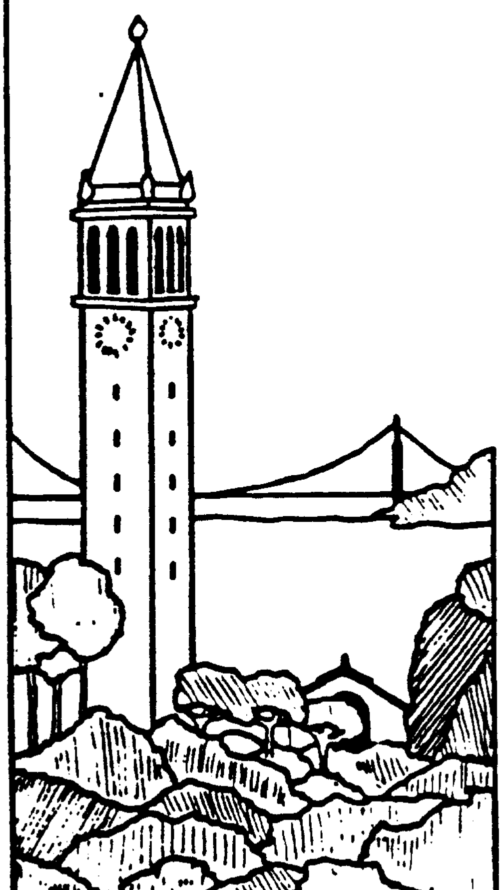
An $\Omega(n^{8/7})$ Lower Bound on the Randomized Complexity of Graph Properties

Valerie King



Report No. UCB/CSD 87/364

July 1987

Computer Science Division (EECS)
University of California
Berkeley, California 94720

An $\Omega(n^{8/7})$ Lower Bound on the Randomized Complexity of Graph Properties

*Valerie King**
U.C. Berkeley

ABSTRACT

A decision tree algorithm determines whether an input graph with n nodes has a property by examining the entries of the graph's adjacency matrix and branching according to the information already gained. All graph properties which are monotone (not destroyed by the addition of edges) and nontrivial (holds for some but not all graphs) have been shown to require $\Omega(n^2)$ queries in the worst case.

In this paper, we investigate the power of randomness in recognizing these properties by considering randomized decision tree algorithms in which coins may be flipped to determine the next entry to be examined. The complexity of a randomized algorithm is the expected number of entries that are examined in the worst case. The randomized complexity of a property is the minimum complexity of any randomized decision tree algorithm which computes the property. We improve Yao's lower bound on the randomized complexity of any monotone nontrivial graph property from $\Omega(n \log^{1/12} n)$ to $\Omega(n^{8/7})$.

1. Introduction

Suppose we would like to determine whether an unknown input graph on nodes V={1,2,...,n} has, for example, an isolated node and we can obtain information only by asking questions of the form "Is edge {i,j} in the graph?". In the *deterministic* decision tree model, the choice of question may depend only on the information gained so far, and the *deterministic* complexity of a problem is the

*Research supported by NSF Grant #DCR-8411954.

number of questions that must be asked in the worst case.

In a *randomized* decision tree algorithm, the choice of question may also depend on coinflips. The cost of the algorithm is measured by the maximum over all input graphs of the expected number of questions asked. The *randomized complexity R(P)* of a property P is the minimum cost of any randomized decision tree algorithm which computes P.

A graph on V={1,2,...,n} may be viewed as a subset of edges E = {{i,j} | i,j ∈ V, i ≠j}. A collection of such graphs is called a *graph property* provided that it is invariant under renumbering of the nodes.

A graph property is *monotone* increasing if it is not destroyed by the addition of edges. It is *nontrivial* if it holds for some but not all graphs.

The deterministic complexity of monotone, nontrivial graph properties has been extensively studied. In 1973, Aanderaa and Rosenberg [Ro] conjectured a lower bound of $\Omega(n^2)$ which was proved by Rivest and Vuillemin [RV]. Their constant factor of 1/16 was subsequently improved by Kleitman and Kwiatkowski [KK], and then Kahn, Saks, and Sturtevant [KSS].

Much less is known about the randomized complexity of monotone nontrivial graph properties. This problem was studied in a 1977 paper by A. Yao [Y1], in which he gives a lower bound of $\Omega(n)$ for all monotone nontrivial graph properties, $\Omega(n^2)$ lower bounds for certain specific graph properties, and develops useful tools for such proofs. No progress was made on the general lower bound until 1986 when Yao showed a lower bound of $\Omega(n \log^{1/12} n)$ [Y2]. In this paper, we show:

Theorem 1: *For any nontrivial, monotone (increasing) graph property P on n nodes, R(P) is greater than $n^{8/7}/18$ for sufficiently large n.*

The gap between the lower bound and upper bound for this problem remains remarkably wide. No monotone, nontrivial graph property is known to have a randomized complexity of less than roughly $n^2/4$. Thus the following conjecture which was posed by Yao in 1977 [Y1] is still open:

Conjecture 1 (Yao): *The randomized complexity of any monotone, nontrivial graph property on n nodes is $\Omega(n^2)$.*

In Sections 3 and 4, we prove the following relationships between the minimum randomized complexity of any monotone nontrivial graph property on n nodes to $b_{k,l}$, the minimum randomized complexity of any monotone, nontrivial bipartite graph property on V and W with $|V|=k$ and $|W|=l$. (A *bipartite graph property* is a collection of subsets of V×W which is invariant under permutations of V and of W.)

Theorem 2: *For any q such that* $1 \le q \le n/2$ *and any monotone nontrivial graph property P on n nodes,* $R(P) \ge \min\{n^2/2q - 3/2n + q, \min_{q \le r \le n/2} b_{n-r,r}\}$.

Theorem 3: *For any monotone, nontrivial graph property P on n nodes,* $R(P) \ge \min\{n^{6/5}/9, b_{\lfloor n/2 \rfloor, \lceil n/2 \rceil}\}$ *for sufficiently large n.*

In Section 5, we prove a lower bound for bipartite graph properties:

Theorem 4: *For any k and l,* $b_{k,l} > (kl)^{4/7}/8$.

Theorems 3 and 4 yield a lower bound of $\Omega(n^{8/7})$, proving Thoerem 1. Theorem 2 is of interest in that it may lead to lower bounds as high as $n^{1.5}$, if improved lower bounds on the complexity of bipartite graph properties can be shown.

In section 6 and 7, we present the proofs of two lemmas and a technique for proving lower bounds on the randomized complexity of graph properties when certain conditions are satisfied. (A 1-certificate is defined in section 2):

Theorem 5: *If P is a monotone nontrivial graph property and P has a 1-certificate with maximum degree d and t nodes of positive degree, then* $R(P) > (t/(d^2+1))^2/32$.

2. Preliminaries

In this section, we review some well-known tools for showing lower bounds on randomized complexity. The following definitions and lemmas are stated in terms of graph properties but are easily extended to bipartite graph properties.

A *1-certificate* for a property P is a minimal set of edges whose presence in a graph proves the graph has the property. I.e., If G_1 is a 1-certificate then $P(G_1) = 1$, and for any proper subset G' of G_1, P(G')=0.

A *0-certificate* for a property P is a minimal set of edges whose absence from a graph proves the graph has the property. I.e., if G_0 is a 0-certificate then $P(\overline{G_0})=0$ and for any proper subset G' of G_0, $P(\overline{G'})= 1$.

The *size* of a certificate refers to the number of edges in it. A clique of size q is the set of all $\binom{q}{2}$ edges on q nodes.

Let π be a 1-1 and onto mapping from nodes V to V'. For any set of edges A on V, we define $\pi(A)$ by $\pi(A) = \{\{\pi(i),\pi(j)\} \mid \{i,j\} \in A\}$. For A a set of edges on V and B a set of edges on V', we say A and B can be *packed* iff there is a 1-1 and onto mapping from V to V' π such that $\pi(A)$ and B have no edges in common.

Lemma 2.1: *a. R(P) is greater than or equal to the size of any 1 or 0-certificate.*

b. No leaf of a decision tree for a property can accept more than one 1-certificate. (Note that this refers to an input graph whose edge set is exactly a 1-certificate.)

c. A 0-certificate and a 1-certificate for a property P cannot be packed.

Lemma 2.2: *Let $P^D(G)= 1$ iff $P(\overline{G})=0$. P^D is called the "dual" of P.*

a. P^D is monotone and nontrivial if P is.

b. The 0-certificates of P are the 1-certificates of P^D and vice versa.

c. $R(P^D) = R(P)$.

The proofs of these lemmas are straightforward.

We note that Lemma 2.2 implies that some results in this paper which are given in terms of 1-certificates are also true for 0-certificates. These include Theorem 5 and Lemmas 4.1 and 4.2.

Theorem 2.3 (Yao) [Y1]: *R(P) equals the maximum over all probability distributions of n-node input graphs of the minimum average cost of a deterministic algorithm on that input.*

3. Reduction to a Bipartite Graph Property--I

To prove Theorem 2, we need the following well-known theorem:

Theorem 2.1 (Turán) [T]: *Let q and n be natural numbers with $q > 2$. Every graph with n nodes and greater than $t_{q-1}(n)$ edges contains a clique of size q,* *where* t_q *equals* $\binom{n}{2} - \sum_{i=0}^{i=q-1} \binom{n_i}{2}$ *where* $n_i = \left\lfloor \frac{n+i}{q} \right\rfloor$.

Theorem 2: *Let P be any monotone, nontrivial graph property on n nodes. For any integer q such that* $1 \leq q \leq n/2$, $R(P) \geq \min\{n^2/2q - 3/2n + q, \min_{q \leq r \leq n/2} b_{n-r,r}\}$.

Proof: We show that any monotone nontrivial graph property P either has a large 0- or 1-certificate or can be reduced to a monotone, nontrivial bipartite graph property.

Let c_1 and c_0 each be the size of the smallest clique which contains a 1-certificate and 0-certificate, respectively, for P.

Case 1: $c_1 \leq q$.

>From Lemma 2.1c, we have that a 0-certificate cannot be packed with a 1-certificate. Hence the complement of any 0-certificate cannot contain a clique of size q. From Turán's Theorem, the complement must be of size less than or equal to t_{q-1}, which implies that every 0-certificate must be of size at least $\binom{n}{2} - t_{q-1} \geq n^2/2q - 3/2n + q$. By Lemma 2.1a, this gives a lower bound for R(P).

Case 2: $c_0 \leq q$.

The proof is similar to the above. A lower bound on the size of any 1-certificate is derived.

Case 3: $c_1 > q$ *and* $c_0 > q$.

Claim: *There is an r such that* $q \leq r \leq n-q$ *and* $r < c_1$ *and* $n-r < c_0$.

Let r = min { $c_1 - 1, n-q$}. We observe that $c_1 + c_0 > n+1$. Otherwise, the two cliques and therefore a 1-certificate and 0-certificate can be packed, since two cliques on two sets of nodes with one node or less in common have no common edges. The claim easily follows.

Let P' be the bipartite graph property defined on V, W with |V| = r and |W| = n-r, as follows: for any B $\subseteq$ V $\times$ W, P'(B) = 1 iff $P(\hat{V} \bigcup B) = 1$, where $\hat{V}$ denotes the set of all edges on V. P' is a monotone bipartite graph property. Since |V| < c_1 and |W| < c_0, we have $P(\hat{V}) = 0$ and $P(\hat{V} \bigcup V \times W) = 1$. Therefore, P' is nontrivial.

For all input graphs containing $\hat{V}$, any randomized algorithm must compute P' in order to determine P. Hence, R(P) is greater than or equal to R(P') which is greater than or equal to $\min_{q \leq r \leq n/2} b_{n-r,r}$.

4. Reduction to a Bipartite Graph Property-II

To prove Theorem 3, we use the following theorem on packing graphs.

Theorem 3.1 (Sauer and Spence)[SS]: *Let A and B each be graphs on n nodes and let m(A) and m(B) be the maximum degree of any node in A and the maximum degree of any node in B, respectively. If m(A)m(B) < n/2 then A and B can be packed.*

In this section, we show:

Theorem 3: *Let P be any monotone nontrivial graph property. For n sufficiently large,*

$$R(P) \geq \min\{n^{6/5}/9,\ b_{\lfloor n/2 \rfloor, \lceil n/2 \rceil}\}.$$

Proof: Let c_1 and c_0 each be the size of the smallest clique that contains a 1-certificate and 0-certificate, respectively, for P. We partition the n nodes into $|V| = \lfloor n/2 \rfloor$ and $|W| = \lceil n/2 \rceil$. We may assume that the size of any 0- or 1-certificate is less than $n^{6/5}/9$ for otherwise, by Lemma 2.1, $R(P) \geq n^{6/5}/9$.

Case 1: $c_1 > \lceil n/2 \rceil$ *and* $c_0 > \lceil n/2 \rceil$.

Then let B be any subset of $V \times W$. We may define a monotone bipartitite graph property P' such that P'(B)= 1 iff $P(\hat{V} \bigcup B)=1$. P' is nontrivial since $\hat{V}$ does not contain a 1-certificate and $\hat{W}$ does not contain a 0-certificate. Since any randomized algorithm to compute P must compute P', $R(P) \geq R(P') \geq b_{\lfloor n/2 \rfloor, \lceil n/2 \rceil}$.

Case 2: $c_1 \leq \lceil n/2 \rceil$.

Then there is a clique of size $\leq c_1$ which contains a 0-certificate for P^D. Hence, we need only consider Case 3.

Case 3: $c_0 \leq \lceil n/2 \rceil$.

Let B be any subset of edges on nodes in W. We define a new property P'as follows: P'(B) = 1 iff P($\hat{V} \bigcup (V \times W) \bigcup B$)= 1. P' is a monotone graph property. P' is also nontrivial since $\hat{W}$ contains a 0-certificate. Any randomized algorithm to compute P must compute P' so that R(P)$\geq$R(P').

We show that there exists a 1-certificate for P' with maximum degree less than $n^{1/5}/4$ and with at least n/4 nodes of positive degree. We can then immediately apply Theorem 5 below to give a lower bound of $n^{6/5}/9$.

Claim 1: *P' has a 1-certificate G' with maximum degree less than $n^{1/5}/4$.*

Let G be any 1-certificate for P. Map the $\lfloor n/2 \rfloor$ nodes of highest degree to nodes in V. The remaining nodes must have degree less than $n^{1/5}/4$, for otherwise, G is of size greater than $n^{6/5}/9$. The set of edges incident to nodes in W contains a 1-certificate for P'. Therefore, we know that P' has a 1-certificate with maximum degree less than $n^{1/5}/4$, which we call G'.

Claim 2: *G' has at least n/4 nodes of positive degree.*

Assume that there are at least n/4 nodes of 0 degree in G'. We use Theorem 3.1 to show that any 0-certificate for P' can be packed with G', giving a contradiction.

Let H be a 0-certificate for P'. We define a permutation σ of W, such that σ(H) and G' are disjoint. Let W' be the set of the n/4 nodes of smallest degree in H. Since the size of H is less than $n^{6/5}/9$, the nodes in W' have degree less than $4n^{1/5}/9$ in H. Let $m_{w'}(H)$ denote their maximum degree.

Let W'' be a set of n/4 nodes which includes all nodes of positive degree in G' and let $m_{w''}(G')$ denote their maximum degree. Since $m_{w'}(H)m_{w''}(G')\leq n^{2/5}/9<n/8$, Theorem 3.1 implies that the subgraph of H induced on W' and the subgraph of G' induced on W'' can be packed. This packing may be extended to a packing of H and G' by arbitrarily mapping W-W' to W-W'', since G' has no edges incident to nodes in W-W".

Since there is a 1-certificate with $n/4$ nodes of positive degree and maximum degree less than $n^{1/5}/4$, we may apply the following:

Theorem 5: *If P is a monotone nontrivial graph property and P has a 1-certificate with maximum degree d and t nodes of positive degree, then R(P) > $(t/(d^2+1))^2/32$.*

Then we have, for sufficiently large n:

$$R(P) \geq \frac{n^2}{512((n^{2/5}/16)+1)^2} > n^{6/5}/9.$$

5. The Randomized Complexity of Bipartite Graph Properties

Theorem 4: *The minimum randomized complexity of any monotone nontrivial bipartite graph property P on V and W, with* $|V|=k$ *and* $|W|=l$, *is at least* $(kl)^{4/7}/8$.

We denote nodes in V and W by v and w, respectively. We may assume that $k \geq l$ and that the size of all 1- and 0-certificates is less than $(kl)^{4/7}/8$. Otherwise, R(P) is at least $(kl)^{4/7}/8$, by Lemma 2.1a.

Let V' be any subset of V with less than k/2 nodes. Then it is not hard to see that either $P(V' \times W) = 0$ or $P^D(V' \times W) = 0$. Since $R(P^D) = R(P)$, we may choose P so that $P(V' \times W) = 0$. It follows that any 1-certificate of P has at least k/2 v's with degree ≥ 1 and that $k/2 < (kl)^{4/7}/8$.

To each 1-certificate for a property P we assign a sequence $(d_1, d_2, \ldots, d_k)$, where each d_i is the degree of w_i in the 1-certificate and the w's have been numbered so that $d_1 \geq d_2 \geq \cdots \geq d_k$. Let G_1 denote a 1-certificate which is lexicographically smallest and let d_{max} denote d_1 for G_1, i.e., the smallest over all 1-certificates of the maximum degree of any w. (If there is more than one lexicographically smallest 1-certificate, we choose one.)

If d_{max} is at least $k^{8/7}l^{-6/7}/4$, we can directly apply a technique from Yao's paper [Y2].

Lemma 4.1: *If P is any monotone nontrivial bipartite graph property on V and W,* $|W| = l$ *and the size of* G_1 *is less than s, then* $R(P) \geq l^2 d_{max}/8s - l/2$.

The proof of Lemma 4.1 is sketched in Section 6.

For $s \leq (kl)^{4/7}/8$ and $d_{max} \geq k^{8/7}l^{-6/7}/4$, Lemma 3.1 gives a lower bound of $(kl)^{4/7}/8$ for R(P).

If d_{max}(P) is less than $k^{8/7}l^{-6/7}/4$, we will show that G_1 has $2(kl)^{2/7}$ v's with nonempty pairwise disjoint neighbor sets. (The *neighbor set of a node v in a graph G* is $\{w \mid \{v, w\} \in G\}$.)

Then Lemma 4.2 below will imply a $(kl)^{4/7}/8$ lower bound for R(P).

Lemma 4.2: *Let G be a 1-certificate for a monotone, nontrivial bipartite graph property P. If G has m v's with nonempty pairwise disjoint neighbor sets, then R(P) is at least $m^2/32$.*

The proof of Lemma 4.2 is given in Section 5.

It remains to prove the following claim:

Claim: *There is a set M of $2(kl)^{2/7}$ v's in G_1 which have nonempty pairwise disjoint neighbor sets.*

Recall that we chose P or P^D so that every 1-certificate had at least k/2 v's with degree at least 1. Of these nodes, less than than k/4 have degree at least $k^{-3/7}l^{4/7}/2$ for, by assumption, the size of each certificate is less than $(kl)^{4/7}/8$. Thus, at least k/4 v's have positive degree less than $k^{-3/7}l^{4/7}/2$.

Let K be a maximal set of these v's which have nonempty pairwise disjoint neighbor sets. We show that if $|K| < 2(kl)^{2/7}$, then K is not maximal.

Let $\Gamma(v)$ denote the neighbor set of v in G_1. Since each v in K has degree less than $k^{-3/7}l^{4/7}/2$, we have:

$$\sum_{v\epsilon K} |\Gamma(v)| < (2(kl)^{2/7})(k^{-3/7}l^{4/7}/2) = (k^{-1/7}l^{6/7}).$$

Each w has degree less than $d_{max} = k^{8/7}l^{-6/7}/4$. Then, the number of v's adjacent to any $w \in \bigcup_{v\epsilon K}\Gamma(v)$ is less than $(k^{-1/7}l^{6/7})(k^{8/7}l^{-6/7}/4) = k/4$. There is at least one v of small positive degree which is not adjacent to any $w \in \bigcup_{v\epsilon K}\Gamma(v)$. Thus, K is not maximal, which contradicts our assumption and proves the claim.

6. Proof of Lemma 4.2 and Theorem 5

Lemma 4.2: *Let G be a 1-certificate for a monotone, nontrivial bipartite graph property P. If G has m v's with nonempty pairwise disjoint neighbor sets, then R(P) is at least $m^2/32$.*

Proof: Let M be the set of v's with nonempty pairwise disjoint neighbor sets. The idea is to reduce the task of finding a 1-certificate to finding a perfect matching between the v's in M and their neighbor sets.

We generate an input distribution for which any deterministic algorithm will require an average cost greater than $m^2/32$. The lower bound on the randomized complexity then follows from Theorem 2.3. For every permutation σ of M, we have a G_σ constructed as follows (where $\Gamma_G(v)$ denotes the neighbor set of v in G):

1. For all $v \notin$ M, {v,w} $\in G_\sigma$ iff $\{v,w\} \in$ G.
2. For all $v_j \in$ M, $\{v_j, w\} \in G_\sigma$ iff $\{v_i, w\} \in$ G, where $\sigma(i)=j$.

Suppose the deterministic algorithm is told about all edges and nonedges described in (1) above, so that the algorithm asks only about edges incident to nodes in M. At each step, if the algorithm asks about an edge $\{v,w\}$ where $w \in \Gamma_G(v_i)$ for some i, the algorithm is told about the entire set of edges $\{\{v, w\} \mid$ for all $w \in \Gamma_G(v_i)\}$ which are either all in the input graph or all absent.

To accept a graph in this distribution, the algorithm must find exactly m "edges". Since no two 1-certificates are accepted by the same leaf in the decision tree, there are at least m! leaves, each corresponding to a different G_σ.

A binary tree of height x can have at most $\begin{pmatrix} x \\ m \end{pmatrix}$ paths with exactly m "yes" branches. Let h be the solution to:

$$\begin{pmatrix} x \\ m \end{pmatrix} = m!/2.$$

Then at least half the leaves accepting the inputs in the distribution must lie at depth greater than h. The average depth of these leaves is at least h/2. By Theorem 2.3, R(P) is at least the minimum average cost of any deterministic algorithm on this input which is at least h/2.

To find a lower bound for h, we note that:

$$\begin{pmatrix} x \\ m \end{pmatrix} < \left(\frac{xe}{m}\right)^m \text{ and } 1/2\left(\frac{m}{e}\right)^m < 1/2m!.$$

Then h is greater than the solution to the following equation:

$$\left(\frac{xe}{m}\right)^m = 1/2\left(\frac{m}{e}\right)^m,$$

which implies that h $> m^2/16$ and R(P) $> m^2/32$.

The lemma may be generalized to arbitrary graph properties by specifying that the v_i must also be independent. Consequently, we have the following theorem:

Theorem 5: *If P is a monotone nontrivial graph property and P has a 1-certificate with maximum degree d and t nodes of positive degree, then* $R(P) > (t/(d^2+1))^2/32$.

Proof: There are at least t / (d^2+1) independent nodes of positive degree which are also pairwise nonadjacent. The proof is the same as for Lemma 4.2.

7. Proof of Lemma 4.1

This lemma is based on a technique discussed in [Y2] and more details may be found there. (A lexicographically smallest 1-certificate is defined in Section 3.)

Lemma 4.1: *Let* G_1 *denote a lexicographically smallest 1-certificate for any monotone nontrivial bipartite graph property P on V and W and* $d_{\max}$ *denote the maximum degree of any w in* G_1. *If* $|W| = l$ *and the size* G_1 *is less than s, then* $R(P) \geq l^2 d_{\max}/8s - l/2$.

Proof: We number the nodes in W so that w_1 is a node of highest degree in G_1 and $w_2, w_3, \ldots, w_{l/2}$ are the l/2 -1 nodes of smallest degree in G_1. The degree of each of these nodes is less than 2s/l, for otherwise, there are l/2 nodes with degree at least 2s/l and at least s edges in G_1. that the size of G_1 is at least s.

We will generate a set of input graphs for which any randomized algorithm will incur an average cost of at least $l^2 d_{\max}/8s - 1/2$.

Let $\Gamma(w_i) = \{ v \mid \{ v, w_i \} \in G_1 \}$.

Each input graph I is constructed as follows:

Start with the edges in G_1 and do the following:

1. Add $\{\{v, w_i\} \mid$ for all $v \in \Gamma(w_{l/2})\}$.
   For each i, $2 \leq i \leq l/2 - 1$, add $\{\{v, w_{i+1} \mid$ for all $v \in \Gamma(w_i)$.
2. Let $T_1 = \Gamma(w_1) - \Gamma(w_{l/2})$
   Let $T_2 = \Gamma(w_1) - \Gamma(w_2)$
   For $3 \leq i \leq l/2$, let $T_i = \Gamma(w_1) - \Gamma(w_i) - \Gamma(w_{i-1})$.
   Now, for all i, $1 \leq i \leq l/2$, add $S_i = \{\{v, w_i\} \mid$ for all $v \in T_i\}$.

3. Randomly remove 4s/l edges from each S_i.

The the following is true about all input graphs I generated in this manner:

Fact 1: *P(I) = 0 because the maximum degree of each w_i in I for $1 \leq i \leq l/2$ is less than d_{max}, and therefore, each I is lexicographically smaller than G_1.*

Fact 2: *If the edges removed from any one S_j in step (3) are replaced in I, the resulting graph I' would have property P.*

Fact 1 is obtained immediately by counting the number of edges incident to each w_i in any I. Fact 2 is observed by noting that I' contains a subgraph isomorphic to G_1 as follows:

a.) w_1 in G_1 may be mapped to any w_j in I' for $1 \leq j \leq l/2$ whose S_j has been restored,

b.) if $j \neq 1$, then each w_i for $l/2 > i \geq j$ in G_1 can be mapped to w_{i+1} in I' and $w_{l/2}$ can be mapped to w_1 in I'.

Thus, to determine that P = 0 on any of these inputs I, an algorithm must find a missing edge in S_i for each i, $1 \leq i \leq l/2$. But this is equivalent to finding one of 4s/l randomly chosen edges out of a total of at least d_{max} - 4s/l, for each i. Any randomized algorithm to compute P will incur an expected cost on the input distribution given by:

$$\text{Expected Cost} \geq \sum_{i=1}^{l/2} \frac{d_{max} - 4s/l}{4s/l} \geq l^2 d_{max}/8s - l/2.$$

It follows that for any randomized algorithm, there is a worst case graph whose expected cost is at least $l^2 d_{max}/8s - l/2$.

Acknowledgements

The author would like to thank her advisor Dick Karp for his helpful comments and suggestions and also Joel Friedman, Lisa Hellerstein, and Danny Soroker. This research was funded by an NSF grant.

References

[KSS] J. Kahn, M. Saks, and D. Sturtevant, A topological approach to evasiveness, *Combinatorica 4* (1984), pp. 297-306.

[KK] D.J. Kleitman and K.J. Kwiatkowski, Further results on the Aanderaa-Rosenberg Conjecture, *J. Combinatorial Theory 28* (1980) pp.85-95.

[RV] R. Rivest and S. Vuillemin, On recognizing graph properties from adjacency matrices, Theor. Comp. Sci. 3 (1978) pp.371-384.

[Ro] A.L. Rosenberg, On the time required to recognize properties of graphs: A problem. *SIG ACT News 5 (4)* (1973), pp.15-16.

[SS] N. Sauer and J. Spencer, Edge-disjoint placement of graphs, *J. Combinatorial Theory*, Ser. B, vol.25, No. 3, (1978) pp.295-302.

[T] P. Turán, On the theory of graphs, *Colloq. Math 3* (1954) pp.19-30.

[Y1] A. Yao, Probabilistic computations: towards a unified measure of complexity, *Proc. 18th Annual Symposium on the Foundations of Computer Science,* (1977), pp.222-227.

[Y2] A. Yao, Lower Bounds to Randomized Algorithms for Graph Properties, (to appear in FOCS 1987).