COMBINATORICA
Akadémiai Kiadó – Springer-Verlag

COMBINATORICA 11 (1) (1991) 23–32

AN $\Omega(n^{5/4})$ LOWER BOUND ON THE RANDOMIZED COMPLEXITY OF GRAPH PROPERTIES

VALERIE KING

Received August 10, 1987
Revised April 11, 1989

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 somes 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 nontrivial monotone graph property from $\Omega(n \log^{1/12} n)$ to $\Omega(n^{5/4})$.

1. Introduction

Suppose we would like to determine whether an unknown input graph on nodes $V = \{1, 2, \ldots, n\}$ 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 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 with no possibility of error.

A graph on $V = \{1, 2, \ldots, n\}$ may be viewed as a subset of the set of edges on V, i.e., $\{\{i, j\} | i, j \in V, i \neq j\}$. 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 nontrivial monotone graph properties has been extensively studied. In 1973, Aanderaa and Rosenberg [6] conjectured a lower bound of $\Omega(n^2)$ which was proved by Rivest and Vuillemin [5]. Their constant factor of 1/16 was subsequently improved by Kleitman and Kwiatkowski [4], and then Kahn, Saks, and Sturtevant [2].

AMS subject classification (1980): 68 C 25, 68 E 10

Much less is known about the randomized complexity of nontrivial monotone graph properties. This problem was studied in a 1977 paper by A. Yao [9], in which he gives a lower bound of $\Omega(n)$ for all nontrivial monotone 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 $\Omega(n \log^{1/12} n)$ [10]. In this paper, we show:

Theorem 1.1. *For any nontrivial, monotone (increasing) graph property P on n nodes, $R(P)$ is greater than $n^{5/4}/44$ for sufficiently large n.*

The gap between the lower bound and upper bound for this problem remains remarkably wide. No nontrivial monotone graph property is known to have a randomized complexity of less than $n^2/4$. Thus the following conjecture which was posed by Yao in 1977 [9] is still open:

Conjecture (Yao). *The randomized complexity of any nontrivial monotone 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 nontrivial monotone graph property on n nodes to $b_{k,l}$, the minimum randomized complexity of a nontrivial monotone bipartite graph property on V and W with $|V| = k$ and $|W| = l$. (A *bipartite graph property* is a collection of subsets of $V \times W$ which is invariant under permutations of V and of W.)

Theorem 1.2. *For any q such that $1 \leq q \leq n/2$ and any nontrivial monotone graph property P on n nodes, $R(P) \geq \min\{n^2/2q - 3/2n + q, \min_{q \leq r \leq n/2} b_{n-r,r}\}$.*

Theorem 1.3. *For any nontrivial monotone graph property P on n nodes, $R(P) \geq \min\{n^{5/4}/16, b_{\lfloor n/2 \rfloor, \lceil n/2 \rceil}\}$ for sufficiently large n.*

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

Theorem 1.4. *For any k and $l, b_{k,l} > k^{3/4} l^{1/2}/18$.*

Theorems 1.3 and 1.4 yield a lower bound of $\Omega(n^{5/4})$, proving Theorem 1.1. Theorem 1.2 is of interest in that it may lead to lower bound as high as $n^{1.5}$, if improved lower bound on the complexity of bipartite graph properties when certain conditions are satisfied.

Theorem 1.5. *If P is a nontrivial monotone graph property and there is a graph in P with maximum degree d, then $R(P) > n^2/512(d^3 + d^2 + d + 1)$.*

2. Preliminaries

In this section, we review some well-known tools for showing lower bound 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. That is, 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 does not have the property. That is, 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 $\pi(A) = \{\{\pi(i), \pi(j)\} | \{i,j\} \in A\}$. 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 π from V to V' 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 edges 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 Lemmas 5.1 and 5.2.

Theorem 2.3 (Yao) [9]. *$R(P)$ 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 1.2, we need the following well-known theorem:

Theorem 3.1 (Turán) [8]. *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 $\binom{n}{2} - \sum_{i=0}^{q-1} \binom{n_i}{2}$ where $n_i = \left\lfloor \frac{n+i}{q} \right\rfloor$.*

Theorem (1.2). *Let P be any nontrivial monotone 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 nontrivial monotone graph property P either has a large 0- or 1-certificate or can be reduced to a nontrivial monotone 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 $n - r < c_0$.*

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 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 $P(\hat{V} \cup B) = 1$, 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 $P(\hat{V} \cup V \times W) = 1$. 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 $\min\limits_{q \leq r \leq n/2} b_{n-r,r}$.

4. Reduction to a Bipartite Graph Property – II

In this section, we show:

Theorem (1.3). *Let P be any nontrivial monotone graph property. For n sufficiently large,*

$$R(P) \geq \min\{n^{5/4}/16, b_{\lfloor n/2 \rfloor, \lceil n/2 \rceil}\}.$$

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 $n^{5/4}/16$ for otherwise, by Lemma 2.1, $R(P) \geq n^{5/4}/16$.

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 bipartite graph property P' such that $P'(B) = 1$ iff $P(\hat{V} \cup B) = 1$. 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 $P(\hat{V} \cup (V \times W) \cup B) = 1$. 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 $n^{1/4}/8$. We can then immediately apply Theorem 1.5 to give a lower bound of $n^{5/4}/16$.

Claim. *P' has a 1-certificate G' with maximum degree less than $n^{1/4}/8$.*

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 $n^{1/4}/8$, for otherwise, G is of size greater than $n^{5/4}/16$. The set of edges incident to nodes in W contains a 1-certificate for P'. Therefore, we known that P' has a 1-certificate with maximum degree less than $n^{1/4}/8$.

5. The Randomized Complexity of Bipartite Graph Properties

Theorem (1.4). *The minimum randomized complexity of any nontrivial monotone bipartite graph property P on V and W, with $|V| = k$ and $|W| = l$, is at least $k^{3/4}l^{1/2}/18$, for sufficiently large k and l.*

Proof. 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 $k^{3/4}l^{1/2}/18$. Otherwise, $R(P)$ is at least $k^{3/4}l^{1/2}/18$, 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 $k/2 < k^{3/4}l^{1/2}/18$.

To each 1-certificate for a property P we assign a sequence $(d_1, d_2, \ldots, d_l)$, where each d_i is the degree of w_i in the 1-certificate and the w's have been numbered so that $d_1 \geq d_2 \geq \cdots \geq d_l$. 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 $k^{3/2}l^{-1}/32$, we can directly apply a technique from Yao's paper [10].

Lemma 5.1. *Let G_1 be a lexicographically smallest 1-certificate for any monotone nontrivial bipartite graph property P on V and W, where $|W| = l$. Let $d_{\max}$ denote the maximum degree of any w node in G_1, and d_{av} be the average degree of any w node in G_1, i.e., $|G_1|/l$. Then $R(P) \geq \frac{l}{2}\frac{d_{\max}-4d_{av}+1}{4d_{av}+1}$.*

The proof of Lemma 5.1 is sketched in Section 7.

For $|G_1| \le k^{3/4}l^{1/2}/18$ and $d_{\max} \ge k^{3/2}l^{-1}/32$, Lemma 5.1 gives a lower bound of $k^{3/4}l^{1/2}/18$ for $R(P)$.

If $d_{\max}(P)$ is less than $k^{3/2}l^{-1}/32$, we will show that G_1 satisfies the conditions of the following lemma with sufficiently high values of t and m. (The *neighbor set of a node v in a graph G is $\{w|\{v,w\} \in G\}$.*)

Lemma 5.2. *Let G be a 1-certificate for a nontrivial monotone bipartite graph property P. If there are t disjoint sets of v's M_1, M_2, ..., M_t such that each M_i contains m v's with nonempty pairwise disjoint neighbor sets in G, then $R(P)$ is at least $m^2t/32$.*

The proof given in Section 6.

We recall that every 1-certificate has at least $k/2$ v's with positive degree. Of these nodes, less than $k/4$ v's with positive degree less than $k^{-1/4}l^{1/2}/4$.

Let S be a set of $k/4$ v's with positive degree less than $k^{-1/4}l^{1/2}/4$.

Claim. *Every subset $S' \subseteq S$ of size $k/8$ contains $16k^{-1/4}l^{1/2}$ v's with pairwise disjoint neighbor sets.*

Proof. Let $M \subseteq S'$ be a maximal set v's with pairwise disjoint neighbor sets, If $|M| < 16k^{-1/4}l^{1/2}$ then we show M is not maximal. Let $\Gamma(v)$ denote the neighbor set of v in G_1. A node v cannot be added to M iff it is adjacent to a node in $\Gamma(v)$ for some v in M. But the number of such v's is bounded above by $\sum\limits_{v \in M} |\Gamma(v)| d_{\max}$ which is less than $(16(k^{-1/4}l^{1/2})(k^{-1/4}l^{1/2}/4)(k^{3/2}l^{-1}/32)) = k/8$. Therefore, some v in S' can be added to M.

Claim 2. *There are $k^{5/4}l^{-1/2}/128$ disjoint sets M_i of v's such that each M_i contains $16k^{-1/4}l^{1/2}$ v's with nonempty pairwise disjoint neighbor sets in G_1.*

Proof. By Claim 1, we can repeatedly remove sets of $16k^{-1/4}l^{1/2}$ v's from S which have nonempty pairwise disjoint neighbor sets in G_1, as long as there are at least $k/8$ nodes remaining in S. Thus, we can remove $(k/8)/(16k^{-1/4}l^{1/2}) = k^{5/4}l^{-1/2}/128$ such sets.

From Lemma 5.2, we have $R(P) \ge k^{3/4}l^{1/2}/16$.

6. Proof of Lemma 5.2 and Theorem 1.5

Lemma (5.2). *Let G be a 1-certificate for a nontrivial monotone bipartite graph property P. If there are t disjoint sets of v's M_1, M_2, $\cdots$, M_t such that each M_i contains m v's with nonempty pairwise disjoint neighbor sets in G, then $R(P)$ is at least $m^2t/32$.*

Proof. The idea is to reduce the task of finding a 1-certificate for P to finding a sequence of perfect matchings between the v's in each M_i and their neighbor sets.

Let G be a 1-certificate which satisfies the conditions of Lemma 5.2 and let $\Gamma_G(v)$ denote the neighbor set of v in G. For any M_i and any $v, v' \in M_i$, we define a *superedge* to be a set of edges $\{\{v,w\}|w \in \Gamma_G(v')\}$ and denote it by $(v, \Gamma_G(v'))$. Note that the superedges are pairwise disjoint.

We generate an input distribution for which any deterministic algorithm will require an average cost greater than $m^2t/32$ and apply Theorem 2.3. Let $\sigma_1, \ldots, \sigma_t$ be a sequence of permutations of M_1, M_2, ..., M_t, respectively. For each such sequence, we form the graph $G_{\sigma_1,\sigma_2,\ldots,\sigma_t}$ which contains exactly the following edges:
1. Let $T = \{\{v,w\}|\{v,w\} \in G$ and $v \notin \cup_i M_i\}$. Then $T \subseteq G_{\sigma_1,\sigma_2,\ldots,\sigma_t}$
2. For $i = 1$ to t and all $v \in M_i$, $(v, \Gamma_G(\sigma_i(v))) \subseteq G_{\sigma_1,\sigma_2,\ldots,\sigma_t}$
Each $G_{\sigma_1,\sigma_2,\ldots,\sigma_t}$ a 1-certificate for P and contains a distinct set of exactly mt superedges.

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 v's contained in M_i's. At each step, if the algorithm asks about any edge in a superedge, the algorithm is told that either every edge in that superedge is present in the input graph or every edge is absent.

Now, any algorithm which computes P must compute P' where P' is defined as follows: for any set A of superedges, $A \in P'$ iff $(\cup_{S \in A} S) \cup T \in P$. Hence, $R(P) \geq R(P')$. P' has $(m!)^t$ 1-certificates of size mt, one for each $G_{\sigma_1,\sigma_2,\ldots,\sigma_t}$.

To accept a graph in this distribution, any algorithm which computes P' must find all its mt superedges and no other edges. It follows that in any decision tree, each graph is accepted by a different leaf which lies at the end of a path with exactly mt "yes" branches.

There are no more than $\binom{h}{mt}$ leaves at the end of paths of length $\leq h$ with exactly mt "yes" branches. If we set $\binom{h}{mt} = (m!)^t/2$, at least half the leaves accepting the inputs in the distribution must lie at depth greater than h. By Theorem 2.3, $R(P)$ is at least the average cost $\geq h/2 > m^2t/32$.

It is easy to see that the techniques used to proved Lemma 5.2 yield an analogous lemma for graph properties:

Lemma 6.1. *Let G be a 1-certificate for a nontrivial monotone graph property P. If there are disjoint sets of nodes M_1, M_2, ..., M_t such each M_i contains m nodes with nonempty pairwise disjoint neighbor sets in G, and no two nodes in the $\cup_i M_i$ are adjacent, then $R(P)$ is at least $m^2t/32$.*

Theorem 1.5 follows from Lemma 6.1 and a packing result of Sauer and Spencer.

Theorem (1.5). *If P is a nontrivial monotone graph property and there is a graph in P with maximum degree d, then $R(P) > n^2/512(d^3 + d^2 + d + 1)$.*

Proof. We show that if there is a graph G in P with maximum degree d, then P has a 1-certificate which satisfies the conditions of Lemma 6.1, for $t = (d^2+1)/(d+1)$ and $m = n/4(d^2+1)$ or P has a 0-certificate of size at least $n^2/16d$. In either case, $R(P) > n^2/512(d^3 + d^2 + d + 1)$.

Let G' be a 1-certificate contained in G.

Claim. *Either there are at least $n/2$ nodes of 0 degree in G', or P has a 0-certificate of size $\geq n^2/16d$.*

Proof. Assume that there are at least $n/2$ nodes of 0 degree in G'. Then any 0-certificate H for P of size $< n^2/16d$ can be packed with G' by mapping the $n/2$

highest degree nodes to the $n/2$ 0-degree nodes of G' and using the following theorem to pack the subgraphs of H and G' induced on the remaining $n/2$ nodes. Note that the $n/2$ lowest degree nodes in H must have degree less than $n/4d$ and that the maximum degree nodes in H must have degree less than $n/4d$ and that the maximum degree of G' is not greater than d:

Theorem 6.2 (Sauer and Spencer) [7]. *Let A and B each be graph on n nodes and let $m(A)$ and $m(B)$ be the maximum degree of any node in A and in B, respectively. If $m(A)m(B) < n/2$, then A and B can be packed.*

Let S be the set of $n/2$ nodes with positive degree in G'. Every subset of S of size $n/4$ contains $(n/4)/(d^2+1)$ nodes such that no two nodes are adjacent and no two neighbor sets intersect.

We can repeatedly removefrom S sets of size $(N/4)/(d^2+1)$ together with all nodes in their neighbor sets, until less than $n/4$ nodes remain in S. This can be done at least $(n/4)/((d+1)(n/4)/(d^2+1)/(d+1)) = (d^2+1)/(d+1)$ times.

7. Proof of Lemma 5.1

This lemma is based on a technique discussed in [10] and more details may be found there. (A lexicographically smallest 1-certificate is defined in Section 3.)

Lemma (5.1). *Let G_1 be a lexicographically smallest 1-certificate for any nontrivial monotone bipartite graph property P on V and W, where $|W| = l$. Let $d_{\max}$ denote the maximum degree of any w in G_1, and $d_{\rm av}$ be the average degree of any w node in G_1, i.e., $|G_1|/l$. Then $R(P) \geq \frac{l}{2}\frac{d_{\max}-4d_{\rm av}+1}{4d_{\rm av}+1}$.*

Sketch of Proof. We may assume that $d_{\max} > 8d_{\rm av}$ since $R(P) \geq l/2$ (see Section 5 and Lemma 2.1(a).)

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 $2d_{\rm av}$, for otherwise, there are more than $l/2$ nodes with degree at least $2d_{\rm av}$.

We will generate a set of input graphs for which any randomized algorithm will incur an average cost of at least $\frac{l}{2}\frac{d_{\max}-4d_{\rm av}+1}{4d_{\rm av}+1}$.

Let $\Gamma(w_i) = \{v|\{v,w_i\} \in G_a\}$.

Each input graph I is construced as follows:

Start with the edges in G_1 and do the following:

1. Add $\{\{v,w_1\}|$ for all $v \in \Gamma(w_{l/2})\}$.
   For each i, $2 \leq i \leq l/2-1$, add $\{\{v,w_{i+1}\}$ | 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 $T_i = \Gamma(w_1) - \Gamma(w_{i-1})$.
   Now, for all i, $1 \leq i \leq l/2$, add $S_i = \{\{v,w_i\}|$ for all $v \in T_i\}$. We note that $|S_i| > d_{\max} - 4d_{\rm av}$.
3. Randomly remove $4d_{\rm av}$ edges from each S_i.
   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 $j \leq i \leq l/2$, 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 $4d_{\text{av}}$ randomly chosen edges out of a total of at least $d_{\max} - 4d_{\text{av}}$, for each i. Any randomized algorithm to compute P will incur an expected cost on the input distribution given by:

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

It follows that for any randomized algorithm, there is a worst case graph whose expected cost is at least $\frac{l}{2}\frac{d_{\max}-4d_{\text{av}}+1}{4d_{\text{av}}+1}$.

8. Remarks

Recently, P. Hajnal has improved the lower bound on the randomized complexity of nontrivial monotone graph properties to $\Omega(n^{4/3})$. The $\Omega(n^2)$ conjecture remains open.

The complexity of randomized algorithms which are allowed to make bounded two-sided errors has been considered in [10]. It has been shown that the complexity of any randomized algorithm which computes a nontrivial monotone graph property on n nodes when the probability of error any input graph is less than $1/5$ is also $\Omega(n^{4/3})$. The $\Omega(n^2)$ conjecture remains open.

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 NSF Grant #DCR-8411954.

References

[1] P. Hajnal: An $\Omega(n^{3/4})$ lower bound on the randomized complexity of graph properties, *The University of Chicago Tech. Report 88–004*, April 1988.

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

[3] V. King,: *Lower bounds on the complexity of graph properties*, Ph. D. Thesis, University of California, Berkeley, (May, 1988).

[4] D. J. KLEITMAN, and K. J. KWIATKOWSKI: Further results on the Aanderaa–Rosenberg conjecture, *J. Combinatorial Theory* **28** (1980), pp. 85–95.

[5] R. RIVEST, and S. VUILLEMIN: On recognizing graph properties from adjacency matrices, *Theor. Comp. Sci.* **3** (1978) pp. 371–384.

[6] A. L. ROSENBERG: On the time required to recognize properties of graph: a problem. *SIGACT News* **5** *(4)* (1973), pp. 15–16.

[7] N. SAUER, and J. SPENCER: Edge-disjoint placement of graphs, *Combinatorial Theory*, Ser. B, **25**, 3, (1978), pp. 295–302.

[8] P. TURÁN: On the theory of graphs, *Colloq. Math.* **3** (1954), pp. 19–30.

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

[10] A. YAO: Lower bounds to randomized algorithms for graph properties, *Proc 28th Annual Symposium on the Foundations of Computer Science*, (1987), pp. 393–400. To appear in *Jour of Comp. Sys. Sci.*

Valerie King

Computer Science Dept.
University of Toronto
Toronto, M5S 1A4
Canada