MY THESIS

by

Valerie King

CHAPTER 1

Introduction

Suppose we would like to determine whether an unknown input graph on nodes V={1,2,...,n} has, for example, a node with n-1 incoming edges and we can obtain information only by asking questions of the form "Is edge {i,j} in the graph?", where the choice of question may depend only on the information gained so far. The *deterministic* complexity $D(P)$ of a property P is the number of questions that must be asked in the worst case. A property is *evasive* if its complexity is the total input size, e.g., $\binom{n}{2}$ for n-node graph properties.

Any algorithm which computes a property in this manner may be represented by a binary decision tree which describes its performance of all possible n-node input graphs. Each internal node corresponds to a query. The algorithm branches to the left or right subtree, depending on the answer to the query, until reaching a leaf which is labelled "accept" or "reject". Then D(P) is the minimum height of any decision tree that computes P.

A graph on V={1,2,...,n} may be viewed as a subset of edges E={{i,j}|for all i,j $\in$ V, i $\neq$j}. A collection of such graphs is called a *graph property* on n nodes provided that it is invariant under renumbering of the nodes. The definition of *digraph property* is the same, except the edges are ordered pairs of nodes.

A *bipartite graph property* on node sets V and W is a collection P of subsets of V$\times$W which is invariant under permutations of V and of W.

A graph property is *nontrivial* if it holds for some but not all graphs.

It is *monotone* (increasing) if it is not destroyed by the addition of edges.

In 1973, Aanderaa and Rosenberg conjectured that the deterministic complexity of any nontrivial monotone graph or digraph property on n nodes is at least εn^2 for some constant ε. Rivest and

Vuillemin proved the conjecture in 1975 [RV]. Their bound of $n^2/16$ was improved by Kleitman and Kwiatkowski [KK] and then by Kahn, Saks, Sturtevant [KSS] to $n^2/4+o(n^2)$. In Chaper 2, we discuss some of the techniques which were used, and we prove a new lower bound on the complexity of any nontrivial monotone digraph property on n nodes of $n^2/4+o(n^2)$. Karp's conjecture, that all nontrivial monotone graph properties are evasive, remains open.

In Chapter 3, we consider the cost of computing when the choice of query may depend on coinflips. A *randomized decision tree algorithm* can be represented by a binary tree whose internal nodes correspond to either queries or coinflips. The algorithm branches to the right or left subtree of a coinflip node depending on the outcome of the coinflip. The cost of the algorithm is 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.

The randomized complexity of nontrivial monotone graph properties was first studied by A. Yao. In 1977, he conjectured a lower bound of $\Omega(n^2)$ and observed a lower bound of $\Omega(n)$ on the randomized complexity of nontrivial monotone n-node graph properties. No progress was made until 1987, when Yao proved a lower bound of $\Omega(n(\log n)^{1/12})$. We improve this to $\Omega(n^{5/4})$. Yao's conjecture remains open, for no nontrivial monotone graph property has been shown to have randomized complexity less than $\frac{1}{2}\binom{n}{2}$

In Chapter 4, we relax the model again by allowing the randomized algorithm to err with maximum probability ε on any input graph. We show that for any constant epsilon $<1/5$ these algorithms have complexity $\Omega(n^{5/4})$.

Below, we define other terms which are used throughout the thesis.

The concepts of deterministic and randomized complexity for graph properties may be extended to any set property. A *set property* is a collection of subsets of an element set X= $\{x_1, x_2, \cdots, x_m\}$. Given a set property S of subsets of X and an input set I which is a fixed but unknown subset of X, we would like to determine whether I $\in$ S by asking questions of the form "Is $x_i \in$ I?" A set property S is *evasive* if m queries must be asked by a decision tree algorithm in the worst case. The definitions of monotone and nontrivial can be naturally extended from graph properties to any set property.

A *bipartite graph property* on node sets V and W is a collection P of subsets of V×W which is invariant under permutations of V and of W.

We review the standard definition of a group action.

A group G *acts on* a set X if there is a mapping from G × X -> X such that the following are true. (The image of (g,x) for g ∈ G, x ∈ X, is denoted by gx.):

(i) For g, g' ∈ G, x ∈ X, g(g'x) = (gg')x.

(ii) Let e be the identity element of G. Then ex=x.

G acts *transitively* on X if for any x,x' ∈ X, there exists a g ∈ G such that gx=x'. The action of G on X induces an action on the set of all subsets of X, e.g., g$\{x_a, x_b, \ldots, x_z\}$ = $\{ gx_a, gx_b, \ldots, gx_z \}$. If S is any collection of subsets of X such that for all I ∈ S and all g ∈ G, gI ∈ S, then we say G *preserves* S or S is *invariant* under G.

A graph property on n nodes can thus be viewed as a set property with element set $E=\{\{i,j\} \mid i,j \in V, i \neq j\}$ which is invariant under the group of permutations of V, where each permutation π maps each edge $\{i,j\}$ to $\{\pi i, \pi j\}$.

CHAPTER 2

Deterministic Complexity

2.1. Overview

The complexity of digraph properties was first investigated by Holt and Reingold, who were seeking to find a lower bound for any cycle detection algorithm [B],[MW]. Lower bounds for other graph properties were proved by Hopcroft and Tarjan, Kirkpatrick, Milner and Walsh, Bollobas, Best, van Emde Boas and H. Lenstra [HT], [K], [MW],[B], [BVL]. Much of the pre-1978 work on the complexity of monotone and non-monotone graph properties is described in *Extremal Graph Properties* by Bollobas [B].

Rosenberg conjectured the existence of a constant ε such that every nontrivial graph or digraph property has complexity at least εn^2. However, Aanderaa showed a counterexample for directed graphs. He observed that it was possible to determine whether a digraph with n nodes contained a "sink", i.e., a node with in-degree $n-1$ and out-degree 0, in $3n$ queries. Together, Aanderaa and Rosenberg formulated the following conjecture which appeared in 1973. (It has also been attributed to Lipton and Snyder [B].)

Aanderaa-Rosenberg Conjecture: *There exists a constant* ε *such that every nontrivial monotone graph or digraph property on n nodes has complexity at least* εn^2.

The first example of a family of (non-monotone) graph properties with complexity less than $\Omega(n^2)$ was shown in 1974 by M. R. Best, P. van Emde Boas, and H. W. Lenstra, Jr. [BVL]. They gave an algorithm with complexity $6n$ which determines whether a graph is a "scorpion" graph, that is, if it has a node b of degree $n-2$, a node t of degree 1, and a node u of degree 2 which is adjacent to both t and b. Edges among the remaining $n-3$ nodes may or may not be present.

The Aanderaa-Rosenberg Conjecture was proved in 1975 by R. Rivest and J. Vuillemin. They showed that the conjecture holds true for $\varepsilon=1/16$. The constant was further improved to $1/9$ by

Kleitman and Kwiatkowski. Both results relied on a similar technique for proving evasiveness of certain set properties. That technique is presented in the next section.

In 1984, Kahn, Saks, and Sturtevant developed a more general method to prove evasiveness of set properties and of graph and digraph properties where the number of nodes is a prime power. Their topological approach is discussed in section 2.3.

By plugging their proof of evasiveness into a recursive formula developed by Kleitman and Kwiatkowski, Kahn, Saks, and Sturtevant raised the lower bound on the complexity of any nontrivial monotone graph property on any number of nodes n. Let M_n and M_n^D denote the minimum complexity of any nontrivial monotone graph or digraph property, respectively, on n nodes. They showed that $M_n^D \geq M_n \geq n^2/4 - o(n^2)$.

In section 2.4, we observe that the $o(n^2)$ term in this lower bound can be made smaller, as an easy consequence of A. Yao's 1986 proof that all nontrivial monotone bipartite graph properties are evasive [Y2]. Yao's proof demonstrates a nice application of the KSS topological approach and is presented in section 2.4.

Finally, in section 2.5, we improve the lower bound of M_n^D to $n^2/2 - o(n^2)$.

The following conjecture of R. Karp remains open, even for graph properties on as few as 10 nodes:

Conjecture 2.1 (Karp): *Every nontrivial monotone graph or digraph property is evasive.*

2.2. Early Results

Let S be any set property with element set X. A key idea of the Rivest-Vuillemin result is their observation (discovered independently by Best, van Emde Boas and H. Lenstra, Jr. [BVL]) that in a decision tree to compute S, every leaf at depth less than |X| accepts the same number of sets with odd cardinality as with even cardinality. Consequently, for a nonevasive set property S, the number of sets in S with odd cardinality equals the number of sets in S with even cardinality.

Rivest-Vuillemin Theorem [RV]: *Let S be a collection of subsets of X, where*

(i) |X| is a prime power p^{α},

(ii) is invariant under G, a group which acts transitively on X,

(iii) $\varnothing$ *or X is in S but not both.*

Then S is evasive.

Proof: Let num_k be the number of sets in S of size k. Let $s(k) = \sum |A|$ over all $A \in S$ where $|A| = k$. Since G acts transitively on X, each x_i appears in the same number of subsets of size k. Thus, $p^{\alpha} \mid s(k)$. But $s(k) = k\,num_k$, so for $0<k<p^{\alpha}$, $p \mid num_k$.

Let $U=\sum_{0}^{p^{\alpha}}(-1)^k num_k$. Since $\varnothing$ or X but not both are in S, $U \equiv 1 \bmod p$.

Since each acceptance leaf of a non-evasive property accepts an equal number of sets with odd and even cardinality, $U \equiv 0 \bmod p$ for non-evasive properties. Then S must be evasive.

The application of this theorem to the Aanderaa-Rosenberg Conjecture is not immediate, for in general, $\binom{n}{2}$ is not a prime power. Rivest and Vuillemin reduce the computation of a graph property to the computation of a set property which satisfies the conditions of their theorem by revealing information about some of the edges in the input graph to the algorithm. This technique of reduction is used several times in proofs presented here. The particular reduction used by Rivest and Vuillemin will not be described here.

In 1975, Kleitman and Kwiatkowski improved the constant in the Aanderaa-Rosenberg Conjecture to $n^2/9$. Using techniques similar to those of Rivest and Vuillemin, they proved evasiveness for a class of bipartite graph properties.

Theorem 2.2 [KK]: *Let P be any monotone bipartite graph property on V and W. If |W| is a prime power, then P is evasive.*

Their lower bound for the complexity of graph properties made use of the following recursive formula:

Theorem 2.3 [KK]: $M_n \geq min(M_{n-1}, y(n-y))$ *where y denotes the prime power closest to n.*

Proof: We sketch the proof. We will reduce the computation of any nontrivial monotone graph property P on n nodes to the computation of a nontrivial monotone graph property on n-1 nodes (in cases (i) and (ii)) or a nontrivial monotone bipartite graph property (case iii). Let V'={2,3,...,n} and, for any set of nodes V, let $\hat{V}$ be the set of all edges on V. Let T = {{1,i}| for all i ∈ V'}

Case (i): V' ∈ P. We reveal that the edges in T are absent from the input graph. Then any algorithm to compute P must compute P' where P' is defined as follows: For B ⊆ $\hat{V'}$, B ∈ P' iff B ∈ P.

Case (ii): $\hat{V'} \notin P$. We reveal that the edges in T are in the input graph. Then any algorithm to compute P must compute P' where P' is defined as follows: For B ∈ $V'hat$, B ∈ P' iff B ∪ T ∈ P.

Case (iii): $T \notin P$ *and* $\hat{V'} \in P$. We partition the n nodes into set A with p^{α} nodes and set B with the remaining nodes. We reveal that $\hat{A}$ is in the input graph and every edge in $\hat{B}$ is absent. Then any algorithm to compute P must compute P', where P' is defined as follows: For any subset C ⊆ A×B, C ∈ P' iff C ∪ $\hat{A}$ ∈ P'. By Theorem 2.2, P' is evasive.

2.3. Topological Approach

A monotone *decreasing* set property is a set property whose complement is monotone (increasing). It is easy to see that the complexity of a set property and its complement are equal.

Kahn, Saks, Sturtevant [KSS] developed a technique for proving evasiveness by observing that results from algebraic topology could be applied. In particular, they observed that for any monotone decreasing set property P with set property X, if the sets P could be accepted by a decision tree of height less than |X|, then P\{∅} is a collapsible abstract simplicial complex.

Lemma 2.4 (KSS): *A monotone decreasing set property P\{ ∅} is an (abstract simplicial) complex, (which we call the "complex P").*

This follows from the definition. An *abstract simplicial complex* is a collection Δ of finite non-empty sets, such that if A is an element of Δ then so is every non-empty subset of A.

Each subset of a complex is called a *face.* The dimension of a face A is |A| -1. Faces of dimension 0 are called *vertices.* The union of the vertices in Δ is called the *vertex set.* (See [Mu].)

A *free face* is a non-maximal face which is contained in only one maximal face. An *elementary collapse* of Δ is the process of removing from Δ some free face, together with all faces containing it. We say Δ is *collapsible* if Δ can be reduced to a vertex by a sequence of elementary collapses.

Lemma 2.5 (KSS): *If a monotone decreasing set property S is nonevasive, then the complex S is collapsible.*

Proof: We describe a sequence of elementary collapses to obtain a vertex by considering the decision tree of any algorithm for P with complexity $< |X|$.

For each accepting leaf L, let L_A be the set of elements known to be in the sets accepted by L. Let L_N be the elements not yet asked about on the path to L. The leftmost leaf $Left$ accepts ∅. If it accepts more than one other subset, expand this leaf into a node and two leaves by asking about an element in $Left_N$ and repeat until the new leftmost leaf $Left'$ accepts only ∅ and a subset containing a single element, i.e., a vertex.

Let $Right$ be the rightmost accepting leaf. If $Right \neq Left'$, then $Right_A$ is a free face contained in the maximal face $Right_A \cup Right_N$ and the sets accepted by $Right$ are exactly the faces containing $Right_A$. Remove these faces from P and $Right$ from the tree. Repeat with the next rightmost accepting leaf, until only a vertex remains in P.

We may characterize a complex by studying group actions on the complex.

Let G be a group which acts on X and preserves Δ. From the induced action of G on Δ, we can define the complex of *fixed points* of Δ denoted Δ_G as:

1. The vertex set Y of $\Delta_G = \{y_A \mid$ A is a minimal G-invariant face of Δ}.

2. The faces of Δ_G are all subsets of Y = $\{y_A, y_B, \ldots, y_Z\}$ such that $A \cup B \cup \cdots \cup Z \in \Delta$.

Let Δ be a complex with vertex set X, |X|=n, and let f_d be the number of faces of dimension d. Then the *Euler characteristic* of Δ is:

$$\sum_{d=0}^{n-1}(-1)^d f_d$$

We are now ready to state a result from algebraic topology, which provides the main tool used here.

Lemma 2.6 (Oliver): *Let G be a group acting on a collapsible complex Δ and let p be prime. If G is cyclic or G has a normal p-subgroup H such that G/H is cyclic, then the Euler characteristic of Δ_G is 1.*

Oliver proves the lemma for complexes which satisfy even weaker conditions. See [O] and [S].

From lemmas 2.4, 2.5, and 2.6, we have:

Theorem 2.7 (KSS): *If the complex S for a monotone decreasing set property is invariant under a group G which is cyclic or has a normal p-subgroup H such that G/H is cyclic and p is prime, and the Euler characteristic of $\Delta_G \neq 1$, then the set property is evasive.*

Theorem 2.8 (KSS): *If P is a nontrivial, monotone graph or digraph property on p^α nodes with p prime, then P is evasive.*

Proof: Let $\bar{P}$ be the complement of P, which is monotone decreasing and nontrivial. Identify the nodes with GF(p^α), the field with p^α elements which has a cyclic multiplicative group. Let G be the group of automorphisms = {x -> ax + b: a,b $\in$ GF(p^α), a $\neq$ 0) }. G has a normal p-group H = {x -> x+b: b $\in$ GF(p^α)} and preserves $\bar{P}$, since $\bar{P}$ is invariant under permutation of the nodes. G maps any pair of nodes to any other pair, and so, maps any edge to any other edge. Then $\bar{P}^G = \emptyset$ with Euler characteristic 0.

2.4. Deterministic Complexity of Graph Properties

As observed by Kahn, Saks and Sturtevant [KSS], the recursive formula of Kleitman and Kwiatkowski (Theorem 2.3) and the Theorem 2.8 combine to show that $M_n \geq q'(q+1-q')$ where q is the largest prime power less than n and q' is the prime power nearest to $(q+1)/2$. The existence of primes sufficiently close to n imply

Theorem 2.9 [KSS]: $M_n \geq n^2/4 + o(n^2)$

In 1987, A. Yao used the KSS topological technique to prove that all nontrivial monotone bipartite graph properties were evasive. An easy consequence of his result is that Kleitman's and Kwiatkowski's recursive formula and consequently, the KSS lower bound on M_n could be slightly improved. The modified recursive formula is $M_n \geq \min\{M_{n-1}, \left\lfloor \frac{n}{2} \right\rfloor, \left\lceil \frac{n}{2} \right\rceil\}$ and the new lower bound is for M_n is $q(q+2)/4$ for q the largest prime power less than n, which is still $n^2/4 + o(n^2)$.

Theorem 2.10 (Yao): *Every monotone, nontrivial bipartite graph property is evasive.*

Proof: Let P be a nontrivial monotone decreasing bipartite graph property on node sets V and W. The idea is to demonstrate an action by a cyclic group on any monotone, nontrivial bipartite graph property P whose fixed points do not have Euler characteristic 1. Then Theorem 2.7 implies that P is not collapsible, and therefore, evasive.

Let G be the cyclic group generated by the function which sends i to (i+1)mod$|W|$ for all i ∈ W. Then the fixed points of the complex P, P_G, correspond to the collection of all sets V'×W ∈ P. That is, the vertices of P_G correspond to the minimal invariant faces {i}×W for all i ∈ V. Similarly, for any j, the faces of P_G of dimension j correspond to the sets V'×W for all V' ⊆ V of cardinality j+1.

Suppose for some V' ⊆ V, V'×W ∈ P. The invariance of P under renumbering of V implies that for every U ⊆ V with |U| = |V'|, U×W ∈ P. Let r be the maximum size of any subset V' such that V'×W ∈ P. Since P is nontrivial, r < |V|.

Case 1: r = 0. Then P has no fixed points; the Euler character of P_G =0.

Case 2: r > 0: Then the number of faces of dimension i, for i < r, in the fixed point complex is $\binom{|V|}{(i+1)}$.

For i ≥ r, it is 0.

The Euler characteristic of P_G is then:

$$\sum_{i=0}^{r-1} (-1)^i \binom{|V|}{(i+1)}$$

which cannot equal 1 [Y2].

2.5. Deterministic Complexity of Digraph Properties

In this section, we will improve the asymptotic bound for M_n^D

$$M_n^D \geq n^2/2 + o(n^2).$$

Thus, for every nontrivial monotone graph or digraph property almost half the edges must be asked about in the worst case.

KSS observed that a lower bound for M_n^D of $n^2/4 + o(n^2)$ immediately follows from:

Proposition 2.11 [KSS]:

(i) $M_n \leq M_n^D$ and

(ii) $M_n^D \leq 2M_n$.

Proof:

(i) Let P be a nontrivial monotone digraph property with complexity M_n^D. For any set of undirected edges S, let B(S)={ (i,j) | {i,j} $\in$ S}. We may define a nontrivial graph property on n nodes P' as follows: for any set of undirected edges S, S $\in$ P' iff B(S)$\in$ P. Let A be an algorithm which computes P in time M_n^D. If we replace every query of (i,j) or {j,i} in A by a query of {i,j}, the resulting algorithm computes P' in time $\leq M_n^D$. Hence, $M_n \leq M_n^D$.

(ii) Let P be a monotone nontrivial graph property on n nodes with complexity M_n^D. Then let P' = {T | B(S) $\subseteq$ T for some S $\in$ P}. Let A be an algorithm which computes P in time M_n. If we replace every query of {i,j} by two queries, of (i,j) and (j,i), then A computes P in time $\leq 2M_n$. It follows that M_n^D <= $2M_n$.

Our proof of the improved lower bound for M_n^D follows the proof of the lower bound for M_n in the previous section. We use the KSS topological approach to prove evasiveness for a special case of nontrivial, monotone bipartite digraph properties, which is then used to prove an analogue of the Kleitman's and Kwiatkowski's recursive formula (Theorem 2.3).

Lemma 2.12: *$M_n^D \geq min(M_{n-1}^D, 2p^\alpha(n-p^\alpha))$, where p^α is the minimum prime power greater than n/2.*

Lemma 2.12 is proved in section 2.5.2.

Combining Lemma 2.12 with Theorem 2.8, we obtain the following:

Theorem 2.13: *Any nontrivial monotone digraph property on n nodes has complexity $\geq n^2/2 - o(n^2)$.*

Proof: Theorem 2.8 implies that $M_n^D = n(n-1)$ for n a prime power. Then, by Lemma 2.12, we see that $M_n^D \geq 2p^\alpha(q^\beta+1-p^\alpha)$ where q^β is the largest prime power less than n and p^α is the smallest prime power greater than $n/2$. The result now follows from an implication of the Prime Number Theorem [HW], that there is a function $\delta(x)=o(x)$ such that for all x there is a prime between x and $x+\delta(x)$.

2.5.1. Deterministic Complexity of Bipartite Digraph Properties

A *bipartite graph property* is a collection P of subsets of (V×W)∪(W×V) which is invariant under renumberings of V and of W.

Yao showed that every monotone, nontrivial bipartite graph property is evasive (Theorem 2.10). The analogous statement for bipartite digraph properties is false. For example, the property of having no edges from V to W can be computed by an algorithm which asks only about the edges from V to W. It need never consider the edges from W to V. We can, however, prove evasiveness for a restricted class of bipartite digraph properties.

Theorem 2.14: *A monotone nontrivial bipartite digraph property on V, W with $|W|=p^\alpha$, p prime, is evasive if either:*

$$\text{(i) } V\times W \in P \text{ and } W\times V \in P,$$
$$\text{or}$$
$$\text{(ii) } V\times W \notin P \text{ and } W\times V \notin P.$$

Proof: Let P be any nontrivial monotone decreasing bipartite digraph property on V and W, where V = $\{v_1, v_2, \cdots, v_{|V|}\}$ and W = $\{w_1, w_2, \cdots, w_{p^\alpha}\}$.

Let G be the group generated by two permutations τ and σ of V∪W,where, for all i:

$\tau(v_i)=v_i$,

$\tau(w_i)=w_{i+1 mod p^\alpha}$;

$\sigma(v_i)=v_{i+1 mod |V|}$,

$\sigma(w_i)=w_i$.

The action of G on V and W induces an action on the edges between V and W, which in turn induces an action on P, since P is invariant under permutations of V and of W. Since τ and σ commute, G has a normal p-subgroup (τ) such that G/<τ> = <σ> is cyclic.

Any G-invariant face of the complex P which contains one edge from V to W (resp., W to V) must contain all of V×W (resp., W×V). Then the possible G-invariant faces are V×W, W×V, and (V×W) ∪ (W×V). The last is not in P since P is nontrivial. Then, since either the first two are both in P or both not in P, the Euler characteristic of P_G = 0 or 2. Hence, P must be evasive.

Remark: The theorem can be extended to the cases where |W| = $p^{\alpha}q^{\beta}$ and |W| = $2p^{\alpha}q^{\beta}$, for p and q primes. We sketch the proof for |W|=$p^{\alpha}q^{\beta}$.

We use a more general lemma of Oliver's [O]:

If G acts on a collapsible complex Δ and G has a normal subgroup G' with G/G' of q-power order, and G' has a normal p-subgroup H with G'/H cyclic, for p and q primes, then the Euler characteristic of $\Delta_G \equiv 1 mod q$.

We denote the elements of W by $w_{i,j}$, where $0 \le i < p^{\alpha}$ and $0 \le j < q^{\beta}$. Then we let G be the group generated by three permutations σ, η, and θ of V∪W, where σ is defined as above, and for all i and j:

$\eta(v_i)=v_i$,

$\eta(w_{i,j})=w_{i,j+1 mod q^{\beta}}$;

$\theta(v_i)=v_i$,

$\theta(w_{i,j})=w_{i+1 mod p^{\alpha},j}$.

Then G satisfies the conditions of the lemma stated above. The G-invariant faces are the same as before, and the Euler characteristic of P_G = 0 or 2 $\neq 1 mod q$.

Open Problem: *Does Theorem 2.14 hold true for any size W ?*

There does not seem to be any easy way of counting up faces, as Yao does in his proof of evasiveness for bipartite graph properties.

2.5.2. The Recursive Formula

Following what is by now a standard technique, we prove a lower bound on the complexity of a a digraph property by revealing information about edges in the input graphs, thereby reducing the computation of the property to the computation of a set property with known complexity.

Let Y be the subset of edges "revealed to be in the graph" and let N be the subset of edges "revealed to be absent from the graph". Then we may define P', the *set property induced by Y and N* as follows: Let U be any set of unrevealed edges. U$\in$ P' iff Y $\cup$ U $\in$ P. Any algorithm to determine whether $Y \cup U$ $\cup$ P must determine whether U $\in$ P'. Hence, the complexity of P is greater than or equal to the complexity of P'.

Lemma 2.12:

$M_n^D \geq \min(M_{n-1}^D, 2p^{\alpha}(n-p^{\alpha}))$ *where* p^{α} *is the minimum prime power greater than v/2.*

Proof: Let P be any monotone decreasing digraph property on n nodes. Let V' denote the set {2,3,...,n}, and, for any set of nodes V, let $\hat{V}$ denote the set of all edges on V.

Case (i): The "bidirected star" = {(1,i)| for all i $\in$ *V'}* $\cup$ *{(i,1)| for all i* $\in$ *V'}* $\in$ *P.*

Then let Y= the bidirected star and N= $\emptyset$. The induced set property P' is a monotone decreasing digraph property on v-1 nodes and it is nontrivial because $\emptyset \in$ P' and $\hat{V'} \notin$ P' (since P is nontrivial). Thus $M_n^D \geq M_{n-1}^D$.

Case (ii): $\hat{V'} \notin P$.

Then let Y= $\emptyset$ and N= the bidirected star. The induced set property P' is a monotone decreasing digraph property on n-1 nodes. It is nontrivial because $\emptyset \in$ P' and $\hat{V'} \notin$ P. Thus $M_n^D \geq M_{n-1}^D$.

For the remaining cases, the bidirected star $\notin$ *P and* $\hat{V'} \in P$.

We partition the n nodes into set B with p^{α} nodes and set A with the remaining nodes.

Case (iii): $\hat{A} \cup \hat{B} \in P$.

There are three subcases:

Case (iiia): $\hat{A} \cup \hat{B} \cup (A \times B) \notin P$ *and* $\hat{A} \cup \hat{B} \cup (B \times A) \notin P$.

Let Y = $\hat{A} \cup \hat{B}$ and N= $\varnothing$. Then P' is a monotone decreasing bipartite digraph property on A,B with |B| a prime power. It is nontrivial becauses P is, and it contains neither A×B nor B×A. By theorem 3.1, P' is evasive. Hence the complexity of P ≥ complexity of P' = $2p^{\alpha}(n - p^{\alpha})$.

Case (iiib): $L = \hat{A} \cup \hat{B} \cup (A \times B) \in P$.

Claim: $\hat{A} \cup (A \times B) \in$ P and $\hat{A} \cup (B \times A) \in$ P.

Proof of Claim: Since P is closed under taking subsets, L $\in$ P implies that $\hat{A} \cup (A \times B) \in$ P.

Let B' be a subset of B containing n-p^{α} nodes. Note that $\hat{B} \subseteq$ L implies that $\hat{B'} \subseteq$ L and that (B-B')×B' $\subseteq$ L. Also, we have A×B' $\subseteq$ L, so $\hat{B'} \cup (((B - B') \cup A) \times B') \subseteq$ L. Since L is in P, any digraph isomorphic to L is in P. In particular, if we map the nodes in B' to A and the nodes in (B-B') $\cup$ A to B, we have that $\hat{A} \cup (B \times A) \in$ P.

Now, let Y= $\hat{A}$ and N=$\hat{B}$. Then the induced set property P' is a monotone decreasing bipartite digraph property on A, B with |B| a prime power and A×B and B×A are both in P'. The complete bipartite digraph $\notin$ P'; otherwise there would be a bidirected star on a node in A. Since $\varnothing \in$ P', P' is nontrivial. Hence, by Theorem 3.1, P' is evasive and the complexity of P ≥$2p^{\alpha}(n - p^{\alpha})$.

Case (iiic): $\hat{A} \cup \hat{B} \cup (B \times A) \in P$.

Similar to case iiib.

Case (iv): $\hat{A} \in P$, $\hat{B} \in P$ *, but* $\hat{A} \cup \hat{B} \notin P$.

There are three subcases:

Case (iva): $\hat{A} \cup (A \times B) \notin P$ *and* $\hat{A} \cup (B \times A) \notin P$.

Let Y = $\hat{A}$ and N = $\hat{B}$. Then P' is a monotone, bipartite digraph on A,B which satisfies the conditions of Lemma 3.1. (It is nontrivial by the same argument as in case iiib.) Hence, the complexity of P ≥ $2p^{\alpha}(n - p^{\alpha})$.

Case (ivb): $\hat{A} \cup (A \times B) \in P$

Let Y = $\hat{A} \cup (A \times B)$ and N = $\varnothing$.

Claim: The induced property P’ is evasive.

Proof: We will use a technique from [KSS].

Identify the nodes in B with GF(p^{α}), the field with p^{α} elements which has a cyclic multiplicative group. Then the group G of automorphisms = {x -> ax + b: a,b $\in$ GF(p^{α}), a $\neq$ 0) } acts on the edges in B and the edges in (B×A) by permuting the nodes in B. Since P is invariant under permutation of nodes, and the nodes in B are isomorphic to each other in the graph given by the "known" edges, P’ is invariant under this action.

G has a normal p-group H = {x -> x+b: b $\in$ GF(p^{α})} = GF(p^{α}) and G/H = $GF(p^{\alpha})^*$, a cyclic multiplicative group.

Since G maps any two nodes in B to any two other nodes, G maps any edge in $\hat{B}$ to any other edge in $\hat{B}$. Therefore, a G-invariant set must contain either all edges in $\hat{B}$ or no edges in $\hat{B}$. Similarly, G maps any edge (b_i, a_j) to any other edge from a node in B to a_j. Thus, any G-invariant set which contains (b_i, a_j) must contain $B \times \{a_j\}$.

By assumption, $\hat{B} \notin$ P’ and a bidirected star $\notin$ P, which implies that $B \times \{a_j\} \notin$ P’. We conclude that P’ has no G-invariant faces. Then the Euler characteristic of P_G = 0≠1. By lemma 2.4, P’ is evasive.

Hence the complexity of P ≥ the complexity of P’= $p^{\alpha}(n-p^{\alpha})+p^{\alpha}(p^{\alpha}-1) \geq 2p^{\alpha}(n-p^{\alpha})$.

Case (ivc): $\hat{A} \cup (B \times A) \in P$.

Similar to Case ivb.

We conclude that $M_n^D \geq \min(M_{n-1}^D, 2p^{\alpha}(n-p^{\alpha}))$.

CHAPTER 3

Randomized Complexity

3.1. Introduction

The randomized complexity of graph properties was first investigated by A. Yao. In 1977, he observed a lower bound of $\Omega(n)$ on the randomized complexity of any (monotone or non-monotone) graph property on n nodes. He posed the following question, which remains open:

Open Problem [Y1]: *Is there a constant* ε *such that for all nontrivial monotone graph properties P, $R(P) \geq \varepsilon n^2$?*

No progress was made on this problem until 1987, when Yao improved the lower bound from $\Omega(n)$ to $\Omega(n(\log n)^{1/12})$ [Y2]. In this chapter, we improve this to $\Omega(n^{5/4})$.

The gap between the lower bound and upper bound for this problem remains remarkably wide. It is not known whether the randomized complexity of a graph property is ever less than one half its deterministic complexity.

A savings of almost a half can be shown for the monotone digraph property of having a node with out-degree $n-1$. A simple adversary argument proves that this property is evasive. The following randomized algorithm which uses only one random bit has complexity $n^2/2$.

If the random bit is 1, then

let i=1, j=1

while $i \leq n$ or until a node with out-degree n-1 is found, do

while $j \leq n$, or until a missing edge is found do

if $i \neq j$ then query (i,j)

j=j+1;

i= i+1.

else

let $i=n$, $j=n$

while $i \geq 1$ *or until a node with out-degree n-1 is found, do*

while $j \geq 1$*, or until a missing edge is found do*

if $i \neq j$ *then query (i,j)*

$j=j-1;$

$i = i-1;$

If the input graph has a node k with out-degree $n-1$, then it will be found after an average of $(n+1)/2$ iterations of the i loops. If the input graph has no node with out-degree $n-1$, then a missing edge will be found after an average of $n/2$ queries for n iterations of the i loop.

For other evasive monotone set properties,, Saks and Wigderson [SW] and Snir [S] have shown that randomization can achieve savings of more than a constant factor. In particular, Saks and Wigderson showed that the family of AND/OR tree functions with input size m has deterministic complexity m and randomized complexity $\Theta(m^{.753...})$. (An AND/OR tree function is described by the values outputed by the root of a complete binary tree in which each input bit is contained in a leaf and each internal node computes either an AND or an OR of its subtrees, depending on whether it is at an odd or even depth in the tree.)

The AND/OR tree function is invariant under a cyclic group which acts transitively on its input bits. Thus when viewed as a set property, it satisfies the criteria for evasiveness in Theorem 2.7. It is still not known if every set property which meets this criteria has randomized complexity at least $m^{.753...}$, where m is the size of its element set, or even, if every evasive set property has this complexity. A bound of $m^{.5}$ is known, and follows from lower bounds on the nondeterministic complexity of set properties.

3.2. Nondeterministic Complexity of Set Properties

Let S be a set property with element set X. Let Y be a set of (queried element, answer) pairs. If every input set which is consistent with Y is in S, then Y may considered a "proof" of membership in S. Similarly, if every input set consistent with Y is not in S, then Y may be considered a proof of non-membership in S.

We call a minimal proof of membership in S a *1-certificate for S* and a minimal proof of non-membership in S a *0-certificate for S.* ship in S. I.e., a proof Y is minimal if any subset of Y is not a proof. The size of a certificate is the number of query pairs in it.

We may define the *nondeterministic complexity of any set property S, N(S),* as the maximum over all input sets of the minimum size proof consistent with the input set. The following two observations are apparent.

Proposition 3.1:

(i) $D(S) \geq R(S) \geq N(S)$.

(ii) Let Y and N be any proof of membership and proof of non-membership, respectively. Then there must be some query Q on which they disagree. I.e, either (Q, yes) $\in$ Y and (Q, no) $\in$ N, or (Q, no) $\in$ N and (Q, yes) $\in$ Y.

Blum has shown that for any set property $N(S) \geq D(S)^{.5}$. The following theorem may also be used to find lower bounds on N(S), in the case where S is invariant under a group which acts transitively on its element set. The proof given here is in fact a generalization of an argument used by Kirkpatrick in 1974 in proving a lower bound on the deterministic complexity of nontrivial monotone graph properties and by Sauer and Spencer in 1978 in proving theorems about packing graphs (see below).

Theorem 3.2: *Let S be any set property with element set X which is invariant under the action of a group G which acts transitively on X. If Y and N are a 1-certificate and a 0-certificate for S, then* $|Y||N| \geq |X|$.

Proof: We prove this by showing that if I and I' are any two sets in S such that $|I||I'| < |X|$, then there is some $g \in G$ such that $gI \cup I' = \emptyset$. The theorem follows as a consequence of Proposition 3.1 (ii). Let

B(I) be the orbit of I under G, i.e., B(I) = {gI| for all g∈ G}. Since G acts transitively on X, every x∈ X appears in the same number of sets in B(I). Thus, |B(I)||I|= k|X| for some k. In particular, every x ∈ I' appears in B(I) k times. If every set in B(I) contains at least one x ∈ I', then |B(I)|≤ k|I'|, which implies that k|X|≤ k|I'||I| or |X|≤|I'||I|.

Corollary 3.3 ([Y1], [K], [SS]): *For any graph property P on n nodes,* $N(P) \geq \binom{n}{2}^{1/2}$.

3.3. Previous Lower Bounds

The first lower bound on the randomized complexity of nontrivial graph properties observed by Yao in 1977 was a consequence of lower bound for the nondeterministic complexity, given above.

In that same paper, Yao introduced some important techniques for proving lower bounds on randomized complexity. One important result which can be applied to analysis in other models of computation is

Theorem 3.4 (Yao) [Y1]: *Let P be any set property. Then*

$$R(P) = \underset{I}{Max}\,\underset{A}{Min}\ (\text{Average Cost of } A \text{ on } I),$$

where I is a probability distribution of input sets and A is a deterministic algorithm to compute P.

Sketch of Proof: An algorithm which flips coins to determine its choices is equivalent to an algorithm which flips all coins first and then selects each possible deterministic algorithm with some fixed probability. R(P) may be viewed as the expected pay-off in a mixed strategy game. Player 1 (the randomized algorithm) selects a vector of p = $p_1 p_2 \cdots p_z$ such that deterministic algorithm j is used with probability p_j. Player 2 (the adversary) selects an input distribution $I = i_1 i_2 \cdots i_w$ such that input k appears with probability i_k. Each entry a_{ij} in the game matrix A is the cost of the deterministic algorithm i on input j. The proof of the theorem follows from Von Neumann's Min-Max theorem [V].

Yao used a theorem similar to the following to prove $\Omega(n^2)$ lower bounds on the randomized complexity on the problems of determining whether a graph on n nodes contains a perfect matching and of determining if it contains a Hamiltonian cycle.

Theorem (Yao): *If S is monotone set property and has k 1-certificates (or 0-certificates) size s, then*

$$\binom{2R(S)}{s} \geq k/2.$$

Sketch of Proof: Suppose f has k 1-certificates. We pick a distribution and prove a lower bound on the average cost that any deterministic algorithm which computes S incurs on that distribution. The distribution is the uniform distribution of the sets of s elements queried in each of the k 1-certificates. We note that since each 1-certificate is a minimal proof, any decision tree algorithm which computes without error must have exactly s of its queries on that input set answered "yes" before it accepts it, and, no two of these sets can be accepted by the same leaf in the decision tree. Then, there are at least k leaves in the decision tree, each corresponding to a different 1-certificate, and each at the end of a path with exactly s "yes" branches.

A binary tree of height h can have at most $\binom{h}{s}$ paths with exactly m "yes" branches. If $\binom{h}{s} = k/2$ 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 3.4, R(P) is at least the minimum average cost of any deterministic algorithm on this input which is at least h/2.

Yao's lower bound of $\Omega(n \log^{1/12} n)$ was proved in two steps. First, following the technique used by Rivest and Vuillemin, he reduced the computation of a graph property to the computation of a bipartite graph property, by revealing information about some of the edges. Second, he showed a lower bound on the randomized complexity of nontrivial monotone bipartite graph properties by considering two cases.

The improved lower bound presented in the next section follows the basic outline of Yao's proof. In step 1, using a different, simpler technique, we show that either a graph property has a high nondeterministic complexity or it can be reduced to a bipartite graph property. We prove a lower bound for bipartite graph properties by considering essentially the same two cases. One case is treated with Yao's technique. However, the other case is handled much differently.

In both cases, we show that we can reduce a bipartite graph property to a set property with either a large number of 1-certificates or a large number of 0-certificates of sufficiently small size and apply Theorem 3.5 above to prove a lower bound on their randomized complexity.

3.4. A New Lower Bound for Graph Properties

We show:

Theorem 3.6: *For any nontrivial monotone graph property P, R(P)>*$n^{5/4}/44$*, for sufficiently large n.*

In Sections 3.4.2 and 3.4.3, we reduce 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:

Theorem 3.7: *For any q such that* $1 \le q \le n/2$ *and any monotone nontrivial graph property P on n nodes, R(P)*$\ge \min\{n^2/3q - 3/2n, \min_{q \le r \le n/2} b_{n-r,r}\}$.

Theorem 3.8: *For any monotone, nontrivial graph property P on n nodes, R(P)* $\ge \min\{n^{5/4}/32, b_{\lfloor n/2 \rfloor, \lceil n/2 \rceil}\}$ *for sufficiently large n.*

In Section 3.4.4, we prove a lower bound for bipartite graph properties:

Theorem 3.9: *For any k and l,* $b_{k,l} > k^{3/4} l^{1/2} / 18$ *for sufficiently large k and l.*

ThIs improves the lower bound for $b_{n,n}$ to $\Omega(n^{5/4})$ from the previously known bound of $\Omega(n(\log n)^{1/4})$ [Y3].

Theorems 3.8 and 3.9 immediately yield Theorem 3.6. Theorem 3.7 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 3.4.6, we give a technique for proving lower bounds for some graph properties:

Theorem 3.10: *If P is a monotone nontrivial graph property and there is a graph G in P with maximum degree d, then R(P) >* $n^2/512(d^3+d^2+d+1)$.

3.4.1. Preliminaries

For the purposes of this section, in which only monotone set properties are discussed, a *1-certificate for P* will refer to *a minimal set of elements whose presence in an input set proves the input set is in P*. A *0-certificate for P* is then *a minimal set of elements whose absence from an input set proves the input set is not in P*.

Let π be a permutation of nodes in V. For any set of edges A on V, let π(A) by $\pi(A) = \{\{\pi(i),\pi(j)\} \mid \{i,j\} \in A\}$. If A and B are sets of edges on V, we say A and B can be *packed* iff there is a permutation π of V such that π(A) and B are disjoint.

The proofs in this section will make frequent use of the following facts which are special cases of Proposition 3.1. Let P be any nontrivial monotone graph property.

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

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

Proposition 3.11: *Let* $G \in P^D$ *iff* $\overline{G} \notin P$, *for* $\overline{G}$ *the complement of G.* 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. $R(P^D) = R(P)$.

3.4.2. Reduction to a Bipartite Graph Property I

The proof of Theorem 3.7 uses:

Turan's Theorem ([T]): *Let q and n be natural numbers with q > 2. Every n-node graph with greater than* $\binom{n}{2} - t_{q-1}(n)$ *edges contains a q-clique, where* $t_q = \sum_{i=0}^{i=q-1} \binom{n_i}{2}$ *where* $n_i = \left\lfloor \frac{n+i}{q} \right\rfloor$.

Equivalently, *Any n-node graph with less than* $t_{q-1}(n)$ *edges can be packed with a q-clique.*

Proof of Theorem 3.7: Let c_1 and c_0 each be the order of the smallest clique which contains a 1-certificate and 0-certificate, respectively, for P. If $c_1 \le q$ or $c_0 \le q$ then Turan's Theorem implies that all 0-certificates, or all 1-certificates, resp. must have size $\ge t_{q-1}(n) \ge n^2/3q - 3/2n$, giving a lower bound for

R(P).

For $c_1 > q$ and $c_0 > q$, let r = min{$c_1 - 1$, $n - q$}. Then $q \le r \le n - q$ and $r < c_1$. We also observe that $c_1 + c_0 > n + 1$, since the two cliques cannot be packed, which implies $n - r < c_0$.

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, B $\in$ P’ iff $\hat{V} \cup B \in$ P, where $\hat{V}$ denotes the set of all edges on V. Since $r < c_1$ and $n - r < c_0$, P’ is nontrivial. We can easily verify that P’ is a monotone bipartite graph property, and that R(P)≥R(P’) ≥ $\min_{q \le r \le n/2} b_{n-r,r}$.

3.4.3. Reduction to a Bipartite Graph Property II

Proof of Theorem 3.8: Let c_1 and c_0 be defined as above. 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 $n^{5/4}/32$.

Case 1: $c_1 > \lceil n/2 \rceil$ *and* $c_0 > \lceil n/2 \rceil$. Let B be any subset of V×W. We define property P’ as follows: B $\in$ P’ iff $\hat{V} \cup B \in$ P. We easily verify that P’ is a nontrivial monotone bipartite graph property and that R(P)≥R(P’)≥$b_{\lfloor n/2 \rfloor, \lceil n/2 \rceil}$.

Case 2: $c_1 \le \lceil n/2 \rceil$. Case 2 reduces to Case 3 by considering P^D.

Case 3: $c_0 \le \lceil n/2 \rceil$. Let B be any subset of edges on nodes in W. We define property P’ as follows: $P'(B)=1$ iff $P(\hat{V} \cup (V \times W) \cup B)=1$. P’ is a monotone nontrivial graph property on $\lceil n/2 \rceil$ nodes and $R(P) \ge R(P')$.

We show that there exists a graph in P’ with maximum degree less than $n^{1/4}/8$ and apply Theorem 3.10 to give a lower bound on R(P’) of $n^{5/4}/32$.

Let G be any 1-certificate for P. Map the $\lfloor n/2 \rfloor$ nodes of highest degree to nodes in V. Then the nodes in W must have degree less than $n^{1/4}/8$, since G has size less than $n^{5/4}/16$, and the subgraph of G induced on W is in P’ and has maximum degree less than $n^{1/4}/8$.

3.4.4. The Randomized Complexity of Bipartite Graph Properties

Theorem 3.9: *$b_{k,l} \geq k^{3/4} l^{1/2}/18$, for sufficiently large k and l.*

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 $k^{3/4} l^{1/2}/16$.

Let V' be any subset of V with less than k/2 nodes. Then it is not hard to see that either $V' \times W \notin$ P or $V' \times W \notin P^D$. Since R(P^D) = R(P), we may choose P so that $V' \times W \notin$ P. It follows that any 1-certificate of P has at least k/2 v's with positive degree and that $k/2 < k^{3/4} l^{1/2}/16$.

Following Yao [Y2] we define a lexicographically smallest 1-certificate for P. 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.

If $d_{\max}$ is at least $k^{3/2} l^{-1}/32$, we can directly apply a technique from [Y3] to prove the following, which yields the desired lower bound:

Lemma 3.12 ([Y3]): *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 then $R(P) \geq l^2 d_{\max}/(8|G_1|+2) - l/2$.*

The proof appears in section 3.4.7.

If $d_{\max}$(P) is less than $k^{3/2} l^{-1}/32$, we 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 $\{w \mid \{v, w\} \in$ G$\}$.

Lemma 3.13: *Let G be a 1-certificate for a monotone, nontrivial 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 $m^2 t/32$.*

The proof is given in Section 3.4.5.

We recall that every 1-certificate has at least k/2 v's with positive degree. Of these nodes, less than k/4 have degree as high as $4|G_1|/k \le k^{-1/4} l^{1/2}/4$.

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

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

Proof: Let M ⊆ S' be a maximal set of 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' is bounded above by $\sum_{v \varepsilon M} |\Gamma(v)| d_{\max}$ which is $<(16(k^{-1/4} l^{1/2})(k^{-1/4} l^{1/2}/4)(k^{3/2} l^{-1}/32)) = k/8$. 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.

3.4.5. Proof of Lemma 3.13

Proof of Lemma 3.13: 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 2.10 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.

Let $\sigma_1, \sigma_2, \cdots, \sigma_t$ be a sequence of permutations of $M_1, M_2, \cdots, M_t$, respectively. For each such sequence, we form the graph $G_{\sigma_1, \sigma_2, \cdots, \sigma_t}$ which contains exactly the following edges:

1. Let T = $\{\{v, w\} \mid$ for all $v \notin \bigcup_i M_i$, $\{v, w\}$ such that $\{v, w\} \in$ G$\}$. Then T $\subseteq G_{\sigma_1, \sigma_2, \cdots, \sigma_t}$

2. For $i = 1$ to t and all $v \in M_i$, $(v, \Gamma_G(\sigma_i(v))) \subseteq G_{\sigma_1, \sigma_2, \cdots, \sigma_t}$

Each $G_{\sigma_1,\sigma_2,\cdots,\sigma_t}$ is 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 that 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 $\left(\bigcup_{S\in A} S\right) \cup T \in$ P. Hence, R(P) ≥ R(P'). P' has $(m!)^t$ 1-certificates of size mt, one for each $G_{\sigma_1,\sigma_2,\cdots,\sigma_t}$.

By Theorem 3.5, the complexity of P' is $\geq h/2$ where h is the solution to $\binom{h}{mt} = (m!)^t/2$. To find a lower bound for h, we note that:

$$\left(\frac{eh}{mt}\right)^m > \binom{h}{mt} = (m!)^t/2 > 1/2\left(\frac{m}{e}\right)^{mt}$$

Then, R(P') $\geq h/2 > e^{-2}m^2t/4 > m^2t/32$.

3.4.6. Proof of Theorem 2.4

The techniques used to prove Lemma 3.13 yield an analogous lemma for graph properties:

Lemma 3.14: *Let G be a 1-certificate for a monotone, nontrivial graph property P. If there are disjoint sets of nodes $M_1, M_2, \cdots, M_t$ such each M_i contains m nodes with nonempty pairwise disjoint neighbor sets in G, and no two nodes in the $\bigcup_i M_i$ are adjacent, then R(P) is at least $m^2t/32$.*

To prove Theorem 3.10, it remains to 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 2.11, for $t=(d^2+1)/(d+1)$ and $m=n/4(d^2+1)$ or P has a 0-certificate of size $\geq n^2/16d$. In either case, $R(P) > n^2/512(d^3+d^2+d+1)$.

Let G_1 be a 1-certificate contained in G.

Claim: *Either there are at least n/2 nodes of positive degree in* G_1*, 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_1. Then any 0-certificate G_0 for P of size $<n^2/16d$ can be packed with G_1 by mapping the n/2 highest degree nodes to the n/2 0-degree nodes of G_1 and using the following theorem to pack the subgraphs of G_0 and G_1 induced on the remaining n/2 nodes. Note that the n/2 lowest degree nodes in G_0 must have degree less than $n/4d$ and that the maximum degree of G_1 is no greater than d:

Theorem 3.15 (Sauer and Spencer)[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 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_1. 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 remove from 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 $(n/4)/((d+1)(n/4)/(d^2+1))=$ $(d^2+1)/(d+1)$ times.

3.4.7. Proof of Lemma 3.12

Lemma 3.12 ([Y3]): *Let* G_1 *denote a lexicographically smallest 1-certificate for any monotone non-trivial bipartite graph property P on V and W and* $d_{\max}$ *denote the maximum degree of any* w *in* G_1*. If* $|W| = l$*, then* $R(P)\geq l^2 d_{\max}/(8|G_1|+2)-l/2$.

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 2 $|G_1|$/l.

We will generate a set of input graphs for which any randomized algorithm will incur an average cost of at least $l^2 d_{\max}/(8|G_1|+2)-1/2$.

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 $\{\{v, w_i\}|$ for all $v \in \Gamma(w_{l/2})\}$.

   For each i, $2 \le i \le l/2-1$, 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 $3 \le i \le l/2$, let $T_i = \Gamma(w_1) - \Gamma(w_i) - \Gamma(w_{i-1})$.

   Now, for all i, $1 \le i \le l/2$, add $S_i = \{\{v, w_i\}|$ for all $v \in T_i\}$.

3. Randomly remove 4 $|G_1|$/l edges from each S_i.

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

Fact 1: *I P because the maximum degree of each w_i in I for $1 \le i \le l/2$ 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 $1 \le j \le l/2$ whose S_j has been restored,

b.) if j≠ 1, then each w_i for $l/2 > i \ge j$ 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 I ∉ P for any of these inputs I, an algorithm must find a missing edge in S_i for each i, $1 \le i \le l/2$. But this is equivalent to finding one of $4|G_1|$/l randomly chosen edges out of a total of at least $d_{\max}$ - $4|G_1|$/l, for each i. Any randomized algorithm to compute P will incur an expected cost on the input distribution given by:

$$\text{Expected Cost} \ge \sum_{i=1}^{l/2} \frac{d_{\max} - 4|G_1|/l + 1}{4|G_1|/l + 1}$$
$$= l^2 d_{\max} / (8|G_1| + 2) - l/2.$$

It follows that for any randomized algorithm, there is a worst case graph whose expected cost is at least $l^2 d_{\max}/(8|G_1|+2) - l/2$.

The analysis given above can be slightly changed to show that P can be reduced to a monotone set property P' which has $\geq \left(\frac{d_{\max} - 4|G_1|/l + 1}{4|G_1|/l + 1} \right)^{l/2}$ 0-certificates of size $l/2$. Then the lower bound implied by Theorem 3.5 is within 1/e of the bounds proved above.

Let G'_1 be the graph constructed from G_1 in steps 1 and 2 above. Arbitrarily partition each S_i into blocks of size $4|G_1|/l$.

Suppose the algorithm is told that every input graph contains all edges in M= $\{\{v,w\} | \{v,w\} \in G_1 \bigcup_i S_i\}$, and contains no edges in $\bar{G}_1 \bigcup_i S_i$, so that the algorithm asks only about edges contained in some S_i. At each step, if the algorithm asks about any edge in a block, the algorithm is told that either that every edge in that block is present in the input graph or every edge is absent.

Now, any algorithm which computes P must compute P' where P' is defined on the blocks as follows: For any set of blocks L, L$\in$ P' iff $\left(\bigcup_{B \in L} B \right) \cup M \in P$. Then R(P)≥R(P'). Facts (1) and (2) imply that every way of choosing one block from each S_i yields a minimal set of blocks whose absence proves the input graph is not in P', i.e., a 0-certificate for P'.

We have observed that every nontrivial monotone graph property has either a high nondeterministic complexity or can be reduced to a nontrivial monotone set property with a high nondeterministic complexity or many 1- or 0-certificates of small size. These observations will be used in the next chapter.

CHAPTER 4

Randomized Complexity with Error

In this chapter, we consider a relaxed model of computation, also studied by A. Yao in 1977, in which the randomized algorithm is permitted to err some of the time. In particular, we show that the lower bounds on the complexity of randomized algorithms proved in the previous chapter hold within a constant factor when the probability of (two-sided) error on any input graph is bounded above by a constant $\varepsilon < 1/5$.

Let $R_\varepsilon(P)$ denote the minimum complexity of any randomized algorithm which computes P where the probablity of error on any input is bounded above by epsilon.

Let $A_\varepsilon(P)$ be the maximum over all probability distributions of inputs of the minimum average cost incurred on that distribution by any deterministic algorithm with average error less than ε on that distribution. Then the following analogue of Theorem 2.7 holds. Yao has stated it for $\delta=2$ in [Y1].

Theorem 4.1: *For any property P and any $\varepsilon < 1$ and any δ such that $1 < \delta < 1/\varepsilon$, $R_\varepsilon(P) \geq (1-1/\delta)$ $A_{\varepsilon\delta}(P)$.*

Proof: The proof involves repeated applications of Von Neumann's Min-Max Theorem [V]. Any randomized algorithm may be viewed as selecting each possible deterministic algorithm i with fixed probability p_i. Let $c_{i,j}$ be the cost of algorithm i on input j and $e_{i,j}=1$ if algorithm i errs on input j and 0 otherwise. Then the expected cost on input j of a randomized algorithm given by a probability vector p is $\sum_i p_i c_{i,j}$, and its probability of error on input j is $\sum_i p_i e_{i,j}$. For any input distribution q, the average cost of deterministic algorithm i on q is $\sum_j q_j c_{i,j}$, and its average error is $\sum_j q_j e_{i,j}$.

Let q' be any probability distribution of the inputs, and let H= $\{i \mid \sum_j q'_j e_{i,j} > \varepsilon\delta\}$, i.e, the set of deterministic algorithms whose average error on q is greater than $\varepsilon\delta$. We show that any randomized algorithm whose error is $\leq\varepsilon$ selects from H with the probability $\leq 1/\delta$.

Let P_H be the set of all probability distributions of algorithms in H and let Q be the set of all probability distributions of the set I of possible inputs. Then the Min-max Theorem yields:

$$\min_{p \in P_H} \max_{j \in I} \sum_{i \in H} p_i e_{i,j} = \max_{q \in Q} \min_{i \in H} \sum_{j \in I} q_j e_{i,j} .$$

By assumption, the right hand side of this equation is at least $\varepsilon\delta$, since every i in H has average error of at least $\varepsilon\delta$ on q'. Thus, for any distribution in P_H, there exists an input such that the probability of error on that input is at least $\varepsilon\delta$. For any randomized algorithm p, if the probability that p selects from H, i.e. $\sum_{i \in H} p_i$, is greater than $1/\delta$, then there exists an input such that the probability that p errs on that input is $>(1/\delta)(\varepsilon\delta)>\varepsilon$. This contradicts our assumption that p has error $\leq\varepsilon$.

We may conclude that for any input distribution, the probability that a randomized algorithm selects from the set of algorithms with average error $\leq\varepsilon\delta$ for that distribution is at least $1\text{-}1/\delta$.

There exists an input distribution $\hat{q}$ such that every deterministic algorithm with average error no greater than $\varepsilon\delta$ on that input distribution incurs an average cost of $A_{\varepsilon\delta}$. Let K = $\{i \mid \sum_j \hat{q}_j e_{i,j} \leq \varepsilon\delta\}$, and let P_K be the set of probability distributions of algorithms in K. Then the Min-max Theorem implies

$$\min_{p \in P_K} \max_{j \in I} \sum_{i \in K} p_i c_{i,j} = \max_{q'} \min_{i \in K} \sum_{j \in I} q'_j c_{i,j} .$$

The right hand side of this equation is, by definition, $A_{\varepsilon\delta}(P)$. Therefore, for every distribution on the algorithms in K, there exists some input such that the expected cost of computing that input is $\geq A_{\varepsilon\delta}$(P). Since every randomized algorithm with error $\leq\varepsilon$ selects from K with probability at least $1-1/\delta$, this implies that there exists some input such that the expected cost of computing that input by the entire randomized algorithm is at least $(1-1/\delta)A_{\varepsilon\delta}(P)$.

The following lemma is similar to a theorem in [Y1].

Lemma 4.2: *Let S be any monotone graph property and* ε *be less than 1/4. If S has a 1-certificate (or 0-certificate) C of size at least* s*, then* A_ε *is at least* $(1-2\varepsilon)s$.

Proof: We consider the distribution on the input sets in which the set of elements C appears with probability 1/2 and, for each $j \in C$, C {j} appears with probability $1/2s$.

Any deterministic algorithm which checks less than $(1-2\varepsilon)s$ elements of C cannot distinguish between C and C {j} for $2\varepsilon s$ different values of j. Hence, the average error of the algorithm is greater than the minimum of {1/4, ε}=ε.

The next lemma extends a result in [Y1] about lower bounds for $A_0(S)$ to lower bounds for $A_\varepsilon(S)$ for ε< 1/5.

Theorem 4.3: *Let S be any monotone property with at least k 1-certificates of size s. Let f(x) be any upper bound on the number of these 1-certificates whose common intersection contains a set of size x. Then, for* ε< 1/5, $A_\varepsilon(P)$ *is bounded below by d/40 where*

$$\binom{d}{(1-4\varepsilon)s} f((1-4\varepsilon)s)=k/20.$$

Proof: We generate a probability distribution on the input graphs as follows:

Each of the k 1-certificates appears with probability 1/2k.

For each element j in each 1-certificate C, C \ {j} appears with probability 1/2ks. (If C \ {j} appears in more than one 1-certificate, its probability is multiplied accordingly.)

Any deterministic algorithm which averages no more ε error must must accept at least $3k/5$ 1-certificates.

Every leaf which accepts a 1-certificate after finding less than $(1-4\varepsilon)s$ of its edges will erroneously accept at least $4\varepsilon s$ inputs of the form C {j}, contributing $2\varepsilon/k$ to the average error. Thus no more than $k/2$ 1-certificates may be accepted by leaves at the end of paths with less than $(1-4\varepsilon)s$ "yes" branches.

So, we may assume that at least k/10 1-certificates are accepted by paths with least $(1-4\varepsilon)s$ "yes" branches. The number of 1-certificates which follow the same path down the decision tree for at least $(1-4\varepsilon)s$ "yes" branches is no greater than $f((1-4\varepsilon)s)$. The number of distinct paths with exactly

$(1-4\varepsilon)s$) "yes" branches of length no more than d is no greater than $\binom{d}{(1-4\varepsilon)s}$. Hence, the maximum number of 1-certificates accepted by paths with at least $(1-4\varepsilon)s$ "yes" branches and at depth no greater than d is bounded above by $\binom{d}{(1-4\varepsilon)s} f((1-4\varepsilon)s)$. If $\binom{d}{(1-4\varepsilon)s} f((1-4\varepsilon)s) = k/20$, then at least k/20 1-certificates must be accepted at depth greater than d which implies that $A_\varepsilon(P) \geq d/40$.

Lemma 4.2 and Theorem 4.3 are used to prove lower bounds on A_ε for all nontrivial monotone graph properties P. The proof of Theorem 3.6 shows that there are only three cases to consider:

1. P has a 1-certificate or 0-certificate of size at least $n^{5/4}/44$ *or P can be reduced to a set property which has.*

In this case, we can immediately apply Lemma 4.2.

2. P or P^D *can be reduced to a nontrivial monotone set property S defined on superedges between nodes in disjoint sets* $M_1, \cdots, M_t$ *of size* m *and their neighbor sets, such that every set of perfect matchings between the nodes in each* M_i *and their neighbor sets is a 1-certificate for S, for a total of* $(m!)^t$ *1-certificates of size* mt.

Note that this reduction was used twice in the proof of Theorem 3.6. First, in the proof of Theorem 3.8, case (iii), when P is reduced to a nontrivial graph property which contains a graph on n/2 nodes with maximum degree less than $n^{1/4}/8$. Theorem 3.10 is invoked, and P is again reduced to a set property which satisfies the description above for $m = n/(n^{1/2}+8)$ and $t = (n^{1/2}+8)/(n^{1/4}+8)$.

The second instance occurs after P is reduced to a nontrivial monotone bipartite graph property on V and W with |V|=|W|= n/2, in the proof of Theorem 3.8, Lemma 3.13. For $k = l = n/2$, the values for m and t are $m = 16(n/2)^{1/4}$ and $t = (n/2)^{3/4}/128$.

Let C be a subset of one of these 1-certificates and let c_i be the number of superedges in C which are adjacent to nodes in M_i. Then C is contained no more than $(m - c_i)!^t$ of these 1-certificates which is $\leq (m - |C|/t)!^t$. For |C| $= (1-4\varepsilon)mt$, this is $\leq (4\varepsilon m)!^t$. Consequently, Theorem 4.3 yields a lower bound of $d/40$ when

$$\binom{d}{(1-4\varepsilon)mt}(4\varepsilon m)!^t = m!^t/20.$$

which occurs when $d > (1-4\varepsilon)^2 m^2 t/20e^2$ For both pairs of values for m and t, this implies $A_\varepsilon \geq (1-4\varepsilon)^2 n^{5/4}/1200e^2$.

3. P or P^D can be reduced to a nontrivial monotone set property S' defined on blocks, where there are n/4 sets of b blocks and any choice of one block from each set forms a 0-certificate for S' for b = $(n/2)^{1/4}/8-1$

This reduction occurs in the proof of Theorem 3.8 in Lemma 3.12. for $k=l=n/2$.

Let C be a subset of one of these 0-certificates. Then C is contained in $b^{n/4-|C|}$ of these 0-certificates. Theorem 4.3 implies that for |C| $=(1-4\varepsilon)n/4$, d/40 is a lower bound on $A_\varepsilon P$) when

$$\binom{d}{(1-4\varepsilon)n/4} b^{4\varepsilon n/4} = b^{n/4}.$$

which occurs when $d \geq (1-4\varepsilon)(n/2)^{5/4}/32$.

Putting all these results together, we can conclude the following:

Theorem 4.4: *For any nontrivial monotone graph property P on n nodes and any* $\varepsilon < 1/5$*, there exists a constant c such that*

$$A_\varepsilon(P) \geq cn^{5/4}.$$

Theorem 4.5: *For any nontrivial monotone graph property P on n nodes and any constant* $\varepsilon < 1/5$ *there exists a constant c' such that*

$$R_\varepsilon(P) \geq c'n^{5/4}.$$

BIBLIOGRAPHY

[BVL]

M. R. Best, P. van Emde Boas, and H.W. Lenstra, Jr. A sharpened version of the Aanderaa-Rosenberg Conjecture, *Report ZW 30/74,* Mathematisch Centrum Amsterdam (1974).

[B] B. Bollobas, *Extremal Graph Theory*. Academic Press (1978).

[HW] G. H. Hardy and E.M. Wright. *An Introduction to the Theory of Numbers,* Clarendon Press (1938).

[KSS]

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

[K] D. Kirkpartick, Determining graph properties from matrix representations, *Proceedings of the 6th SIGACT Conference,* Seattle (1974).

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

[MW]

E. C. Milner and D. J. A. Welsh. On the computational complexity of graph theoretical properties, *Proceedings 5th British Columbia Conference on Combinatorics,* (1975), pp.471-487.

[O] R. Oliver, Fixed-point sets of group actions on finite acyclic complexes, *Comment. Math. Helv. 50* (1975) 155-177.

[RV] R. Rivest and S. Vuillemin, On recognizing graph properties from adjacency matrices, Theor. Comp. Sci. 3 (1976) 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.

[SW] M. Saks and A. Wigderson. Probabilistic Boolean decision trees and the complexity of evalutating game trees, *Proceedings 27th Annual IEEE Symposium on the Foundations of Computer Science (1986) pp.29-38.*

[SS] N. Sauer and J. Spencer, Edge-disjoint placement of graphs, *J. Combinatorial Theory, Ser.B 25*, (1978) pp.295-302.

[S] P.A. Smith, Fixed point theorems for periodic transformations, *Amer. J. of Math. 63* (1941), 1-8.

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

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

J. Von Neumann, Zur Theorie der Gesellschaftsspiele, *Math Annalen 100* (1928) pp. 295-320.

[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, *Proc. 28th Annual Symposium on the Foundations of Computer Science,* (1987), pp.393-400.

[Y3] A. Yao, Monotone bipartite graph properties are evasive (manuscript), (1986).

Abstract

Lower Bounds on the Complexity of Graph Properties

Valerie King

In this simple model, a decision tree algorithm must determine whether an unknown graph on nodes {1,2,...,n} has a given property by asking questions of the form "Is edge <i,j> in the graph?" and branching according to the information gained. The complexity of a property is the number of questions which must be asked in the worst case.

Aanderaa and Rosenberg conjectured that any nontrivial monotone (isomorphism-invariant) n-node graph or digraph property has complexity $\Omega(n^2)$. This lower bound was proved by Rivest and Vuillemin and subsequently improved to $n^2/4+o(n^2)$. We show a lower bound of $n^2/2+o(n^2)$ on the complexity of nontrivial monotone digraph properties on n nodes.

The power of randomness in recognizing these properties is investigated by considering randomized decision tree algorithms in which coins may be flipped to determine the next edge to be queried. A. Yao's lower bound on the randomized complexity of any nontrivial monotone graph property is improved from $\Omega(n \log^{1/12} n)$ to $\Omega(n^{5/4})$, and improved bounds for the complexity of nontrivial monotone bipartite graph properties are shown.

We consider the complexity of randomized algorithms which are permitted to make (2-sided) errors in their computation. The same bounds are shown to hold, within a constant factor, when the probability of error on any input graph is bounded above by a constant less than 1/5.

TABLE OF CONTENTS

1 Introduction 1

2 Deterministic Complexity 4

2.1 Overview 4

2.2 Early Results 5

2.3 Topological Approach 7

2.4 Deterministic Complexity of Graph Properties 9

2.5 Deterministic Complexity of Digraph Properties 11

2.5.1 Deterministic Complexity of Bipartite Digraph Properties 12

2.5.2 The Recusive Formula 14

3 Randomized Complexity 17

3.1 Introduction 17

3.2 Nondeterministic Complexity of Set Properties 19

3.3 Previous Lower Bounds 20

3.4 A New Lower Bound for Graph Properties 22

3.4.1 Preliminaries 23

3.4.2 Reduction to a Bipartite Graph Property I 23

3.4.3 Reduction to a Bipartite Graph Property II 24

3.4.4 The Randomized Complexity of Bipartite Graph Properties 25

3.4.5 Proof of Lemma 3.13 26

3.4.6 Proof of Theorem 3.10 27

3.4.7 Proof of Lemma 3.12 28

4 Randomized Complexity with Error 31

Bibliography 36