CONFERENCE RECORD OF SEVENTH ANNUAL ACM SYMPOSIUM ON THEORY OF COMPUTING

1975

Conference Record

of

SEVENTH ANNUAL ACM SYMPOSIUM ON THEORY OF COMPUTING

Papers Presented at the Symposium

Albuquerque, New Mexico

May 5 - May 7, 1975

Sponsored by the

ASSOCIATION FOR COMPUTING MACHINERY

SPECIAL INTEREST GROUI ON AUTOMATA AND COMPUTABILITY THEORY

With the Cooperation of:

The IEEE Computer Society Technical Committee

on

Mathematical Foundations of Computing

and

The University of New Mexico

1133 Avenue of the Americas, New York, N.Y. 10036

FOREWORD

The papers in this volume were contributed for presentation at the 7th Annual ACM Symposium on the Theory of Computing sponsored by the ACM Special Interest Group on Automata and Computability Theory and by the University of New Mexico. These articles were selected on January 6 at a meeting of the full committee from 87 extended abstracts submitted in response to the call for papers from August to December 1974.

The articles in these Proceedings were selected on the basis of originality and relevance to the theory of computing as described in the call for papers. The Committee wishes to thank those who submitted papers and those colleagues who helped in the evaluation of the many abstracts.

The papers in these Proceedings have not been formally refereed and several papers represent preliminary reports of continuing research. It is anticipated that most of these papers will appear in more polished and complete form in scientific journals.

Program Committee

Ashok K. Chandra
Albert R. Meyer
William C. Rounds, chairman
Richard E. Stearns
Robert E. Tarjan
Shmuel Winograd
Paul R. Young

ORGANIZING COMMITTEE

Program Chairman

William C. Rounds
Computer and Communication Sciences Department
University of Michigan
Ann Arbor, Michigan 48104

Local Arrangements Chairman

Nancy Martin
Division of Computing and Information Science
University of New Mexico
Albuquerque, New Mexico 87131

Publicity Chairman

Jack W. Carlyle
Department of System Science
University of California, Los Angeles
Los Angeles, California 90024

Conference Chairman

Michael A. Harrison
Department of Computer Science
University of California, Berkeley
Berkeley, California 94720

1975 SEVENTH ANNUAL ACM SYMPOSIUM ON THEORY OF COMPUTING

Albuquerque, New Mexico

TABLE OF CONTENTS

May 5

Session I: S. Winograd, Chairman

Session II: A. K. Chandra, Chairman

TABLE OF CONTENTS (continued)

May 6

Session III: P. R. Young, Chairman

Session IV: R. E. Tarjan, Chairman

May 7

Session V: A. R. Meyer, Chairman

TABLE OF CONTENTS (continued)

COMPLEXITY MEASURES AND HIERARCHIES FOR THE EVALUATION OF INTEGERS, POLYNOMIALS, AND N-LINEAR FORMS

Richard J. Lipton[*] and David Dobkin[†]
Department of Computer Science
Yale University
New Haven, Connecticut 06520

1. Introduction

The difficulty of evaluating integers and polynomials has been studied in various frameworks ranging from the addition-chain approach [5] to integer evaluation to recent efforts aimed at generating polynomials that are hard to evaluate [2,8,10]. Here we consider the classes of integers and polynomials that can be evaluated within given complexity bounds and prove the existence of proper hierarchies of complexity classes. The framework in which our problems are cast is general enough to allow any finite set of binary operations rather than just addition, subtraction, multiplication, and division. The motivation for studying complexity classes rather than specific integers or polynomials is analogous to why complexity classes are studied in automata-based complexity: (i): the immense difficulty associated with computing the complexity of a specific integer or polynomial; (ii) the important insight obtained from discovering the structure of the complexity classes. Thus, we are able to prove that under mild restrictions if

$$f(n) > g(n) \text{ a.e.}$$

where f and g are monotone functions, then there are an infinite number of integers (respectively polynomials) that can be evaluated in f(n) steps but not g(n) steps.

The model used here for polynomial evaluation differs from the model used in Strassen [10] and Paterson and Stockmeyer [8]. The difference lies in their allowing scalar multiplications by constant a at a cost of zero or one, while we charge an amount that is a function of a. This amount essentially reflects the complexity of integer a. The motivation for our model is similar to that of Cook [3]: In a "real" machine model it is realistic to say that the cost of $a \cdot p$, where a is an integer and p is some term, is dependent at least on the cost associated with "naming" a. That is, the cost must be at least the amount of information needed to state that the scalar is a and to apply the operation $a \circ$ to p.

The difference between our model and that of Strassen and Paterson and Stockmeyer is most dramatic when one compares the following results:

1) [Strassen] There are polynomials that take ~n/log n steps to evaluate.[‡] They have coefficient $\sim 2^{2^{n^3}}$ in size.
2) [Paterson and Stockmeyer] There are 0,1 coefficient polynomials that take $\sim\sqrt{n}$ steps to evaluate.
3) [Theorem 7, section 4] There are 0,1 coefficient polynomials that take ~n/log n steps to evaluate.

Thus our result would be an improvement of both (1) and (2) if we had assumed that scalars are of cost 1. An open question is: How much does our assumption affect the complexity of polynomial evaluation?

Since our results are proved for any finite set of binary operations it is not surprising that they follow by counting type arguments. The basic counting tools we use are a number of powerful results from number theory on the density of sequences of integers [7]. These tools allow us to establish our hierarchy results. Moreover, they allow us to refine them so that we can show not only that there are, for example, 0,1 polynomials that take ~n/log n steps to evaluation but that "almost all" polynomials take this number of steps.

2. Upper and Lower Bounds

We define an <u>addition chain</u> as a sequence of integers $a_0, a_1, \ldots, a_m$ such that $a_0 = 1$ and, for each i, $a_i = a_j + a_k$ for some $j,k < i$. If $a_m = n$, the chain is said to <u>realize</u> the integer n. We define $C_{\{+\}}(n)$ to be the length of the shortest addition chain realizing n. Brauer [1] obtained the upper bound of

$$\log n + \frac{\log n}{\log\log n} + o\left(\frac{\log n}{\log\log n}\right)$$

on $C_{\{+\}}(n)$ and Erdos [4] showed that for most large n the lower bound of

$$\log n + \frac{\log n}{\log\log n},$$

[†] The work of this author was supported in part by US Army grant DAHC04-75-6-0037.

[*] The work of this author was supported in part by National Science Foundation grant GJ-43157.

[‡] n = degree of the polynomial.

is valid. In the current paper we extend addition chains to B-chains as follows:

Definition: Let B be a finite set of binary operations over N. A B-chain is a sequence $\alpha_0, \ldots, \alpha_m$ such that $\alpha_0 = 1$ and for each i $\alpha_i = \alpha_j \circ \alpha_k$ where $j,k < i$ and o is an operation of B. If $\alpha_m = n$, the B-chain is said to realize n. The length of the shortest B-chain for n is denoted by $C_B(n)$. By convention, $C_B(0)$ and $C_B(1)$ are defined as zero.

We shall denote the operations addition, subtraction, multiplication, division, and exponentiation by +, −, ×, ÷, ↑ in the current paper, where $a \div b = \lfloor \frac{a}{b} \rfloor$. For this notation, the following lower bounds are obtained.

Theorem 1: For all n,

a) $C_{\{+\}}(n) \geq C_{\{+,-\}}(n) \geq \log n$ *

b) $C_{\{+,-,\times,\div\}}(n) > \log \log n$

c) $C_{\{+,-,\times,\div,\uparrow\}}(n) > \log (G(n))$

where G(n) is the number of times the logarithm of n must be taken to yield a value less than or equal to 1.

Proof: In each case, it suffices to consider the largest number achievable in n steps. □

Extensions of Theorem 1 to other basis sets is possible and fairly standard. For example, if for all operations $o \in B$ there exists k such that, for all x and y, x o y is of order $x^k y^k$, then $C_B(n)$ grows asymptotically at least as fast as log log n. We can also obtain the upper bounds.

Theorem 2: For all n,

$$C_{\{+,-,\times,\div,\uparrow\}}(n) \leq C_{\{+,-,\times,\div\}}(n) \leq C_{\{+,\times\}}(n) \leq \frac{2 \log n}{\log \log n} + o(\frac{\log n}{\log \log n}).$$

Proof: Let $n = \sum_{i=0}^{m} \lambda_i \alpha^i$ be the expansion of n in base α for some α; then n can be found by computing 2,...,α−1,α and using Horner's rule to evaluate for n. Thus,

$$C_{\{+,\times\}}(n) \leq \alpha - 1 + 2m = \alpha - 1 + 2[\log_\alpha n].$$

The choice of $\alpha = \frac{\log n}{(\log \log n)^2}$ yields the desired result. □

Next, we study cumulative lower bounds. Rather than consider the complexity of reaching n by a B-chain, we define as $H_B(n)$ the maximum value of $C_B(k)$ for any $k \leq n$. This measure is actually more natural than $C_B(n)$ since $C_B(n)$ may fluctuate greatly. Then we can achieve the surprising result that $H_B(n)$ is asymptotically independent of B if $+,\times \in B$.

Theorem 3: For any choice of B,

$$H_B(n) \approx O(\frac{\log n}{\log \log n}).$$ †

Proof: A simple counting argument shows that the number of B-chains of length $\leq m$ is $\leq |B|^m((m-1)!)^2$. By the definition of $H_B(n)$, we see that a growth rate asymptotic to $\frac{\log n}{\log \log n}$ is necessary. □

Let $h(n) = \frac{\log n}{\log \log n}$ and observe that, for all B, $H_B(n) \approx h(n)$.

3. *Complexity Classes on* N

The results of the previous section pave the way for some interesting questions. We observe that there are constants K_1 and K_2 such that for each n $C_B(n) \leq K_1 h(n)$ and, for some $p \leq n$, $C_B(p) \geq K_2 h(n)$. This leads to interesting questions on the complexity classes into which the integers can be partitioned by B-chains for varied bases B. Before studying such questions, we make contact with some results from elementary number theory.

Definition: For A a subset of N such that $0,1 \in A$, the Schnirelmann density d(A) is

$$d(A) = \inf_{n \geq 1} \frac{A(n)}{n}$$

where A(n) is the number of elements of A less than or equal to n.

We observe that d(A) = 1 if and only if A = N and present the following result on d(A).

Theorem 4: (α-β Theorem [7])

If $C = A + B \overset{\Delta}{=} \{a + b \mid a \in A, b \in B\}$, then $d(c) \geq \min[1, d(A) + d(B)]$.

As a corollary to this theorem, we have the result that if A is any set of positive density then, if

* Throughout this paper, all logarithms are base 2.

† $f(n) \approx g(n)$ if there exist constants m,M such that $0 < m < M < \infty$ with $mf(n) < g(n) < Mf(n)$ for all n.

C is the sum of $\lceil \frac{1}{d(A)} \rceil$ copies of A, C = $\mathbb{N}$. Now we define complexity classes and prove our hierarchy results.

Definition: If f: $\mathbb{N} \to \mathbb{N}$ is a monotone function, then C_f^B, <u>the complexity class of f with respect to B</u>, is defined as $\{n \in \mathbb{N} \mid C_B(n) \le f(n)\}$.

We will not define C_f^B if f is not monotone.

Recall that h(n) is defined as $\frac{\log n}{\log \log n}$. The following lemma yields the hierarchy theorem.

Lemma: If $+ \in B$, f is monotone, and $\lim_{n\to\infty} \frac{f(n)}{h(n)} = 0$, then $d(C_f^B) = 0$.

Proof: Suppose that $d(C_f^B) > 0$ and $\lim_{n\to\infty} \frac{f(n)}{h(n)} = 0$. Then, since every integer can be expressed as the sum of at most $\lceil 1/d(C_f^B) \rceil$ integers, $H_B(n) \le 2\lceil 1/d(C_f^B) \rceil f(n)$ for all n, contradicting theorem 3. □

Thus,

Theorem 5: (Hierarchy Theorem)
Suppose that $+ \in B$ and f and g are monotone integer-valued functions such that

1) $f(n) > g(n)$ a.e.
2) $\lim_{n\to\infty} \frac{h(n)}{g(n)} = \infty$ (i.e. $C_g^B \subsetneq \mathbb{N}$) and
3) g grows sufficiently fast such that C_g^B is infinite. Then $C_f^B - C_g^B$ is infinite.

Proof: It is clear that C_g^B has zero density since g grows asymptotically more slowly than h. Also, there is an integer N_0 such that for all $x \ge N_0$ $1 + g(x) \le f(x)$. Furthermore, there is a choice of $N_1 > N_0$ such that $N_1 \in C_g^B$ and $N_1 + 1 \notin C_g^B$. Now,

$$C_B(N_1 + 1) \le 1 + C_B(N_1) \le 1 + g(N_1) \le f(N_1)$$
$$\le f(N_1 + 1)$$

and hence $N_1 + 1 \in C_f^B$. We may extend this method to form a sequence $\{N_i\}$ such that $N_i > N_{i-1}$ and each $N_i + 1 \in C_f^B - C_g^B$. □

Typical of the applications of this hierarchy result are

Corollary 1: If $B_1 = \{+,-,\times,\div\}$, then

$$C^{B_1}_{\log \log n} \subsetneq C^{B_1}_{(\log \log n)G(n)} \subsetneq \dots \subsetneq$$
$$C^{B_1}_{(\log \log n)G^k(n)} \subsetneq \dots \subsetneq C^{B_1}_{(\log \log n)^2} \subsetneq \dots \subsetneq$$
$$C^{B_1}_{h(n)/G(n)} \subsetneq C^{B_1}_{h(n)}$$
$$= \mathbb{N}.$$

Corollary 2: If $B_2 = \{+,-,\times,\div,\uparrow\}$, then

$$C^{B_2}_{\log(G(n))} \subsetneq \dots \subsetneq C^{B_2}_{\log^2(G(n))} \subsetneq \dots \subsetneq$$
$$C^{B_2}_{\log\dots\log n} \subsetneq \dots \subsetneq C^{B_2}_{\log \log n} \subsetneq \dots \subsetneq$$
$$C^{B_2}_{h(n)/G(n)} \subsetneq C^{B_2}_{h(n)}$$
$$= \mathbb{N}.$$

These results make contact with some interesting results in number theory.

Fact 1: (Landau [6])
Every integer can be expressed as the sum of 67 or fewer primes.

Fact 2: (Waring's problem [7])
For each integer k, there is a number g(k) such that every integer can be expressed as the sum of g(k) or fewer k^{th} powers.

Using these results, we obtain

Corollary 3: For any B, there is an infinite subsequence $\{P_i\}$ of the sequence of primes such that $C_B(P_i)$ grows as $O(\log P_i/\log \log P_i)$.

Corollary 4: For any B and each integer k, there is an infinite sequence $\{x_i^k\}$ such that $C_B(x_i^k)$ grows as
$O(\log x_i^k/\log \log x_i^k) = O(k\log x_i/\log(k\log x_i))$.

<u>*4. Polynomial Evaluation*</u>

The difficulty of polynomial evaluation has been studied in a variety of settings. Lately, a number of authors have focused on finding polynomials that are difficult to evaluate regardless of how much preconditioning of coefficients is allowed [2,8,10]. The results of these studies are hard to evaluate polynomials that have extremely large coefficients. For example, Strassen [10] shows that the evaluation of

$$P_1(x) = \sum_{\delta=0}^{d} 2^{2^{\delta d^2}} x^{\delta}$$

requires either $d/2 - 2$ non-scalar multiplication/divisions or at least $d^2/\log_2 d$ total arithmetics and that the evaluation of

$$P_2(x) = \sum_{\delta=0}^{d} 2^{2^\delta} x^\delta$$

requires at least $\sqrt{d/(3\log d)}$ arithmetics. In the terminology of this paper, however, the computation, from a basis of +,-,×,÷, of single coefficients of $P_1(x)$ (respectively $P_2(x)$) requires d^3 (respectively d) operations, and thus the evaluation cost is unimportant relative to this cost. In this manner, we shall diverge from the methodology of previous studies of polynomial evaluation. We shall try to find the chain requiring the least number of operations from a basis B that, starting from inputs 1 and x_0, generates the value of a polynomial p(x) at the point x_0. We have chosen this model because we feel that it addresses some of the issues not considered in previous studies of this problem. A positive result of lower bounds using this model is that such bounds give lower bounds on the sizes of scalars that must be used in previous models. That is, we define

Definition: If $p(x) \in \mathbb{N}(x)$, then $\underline{\delta_B(p)}$ is the length of the shortest sequence $\alpha_{-1},\ldots,\alpha_k$ (i.e. the least k) such that $\alpha_{-1} = 1$, $\alpha_0 = x$, and, for $1 \le i \le k$, $\alpha_i = \alpha_j \circ \alpha_k$ where $\circ \in B$ and $j,k \le i$.

The following theorem is then immediate.

Theorem 6: $\delta_B(p) \ge C_B(p(n)) - C_B(n)$ for any integer n.

Proof: It is obvious that $\delta_B(p) + C_B(n)$ is an upper bound for $C_B(p(n))$. □

Within our measure, we have the cost for Strassen's polynomials as

Corollary: For $B = \{+,-,\times,\div\}$,

1) $\delta_B(\sum_{i=0}^{d} 2^{2^{id^2}} x^i) \ge d^4/2$

2) $\delta_B(\sum_{i=0}^{d} 2^{2^i} x^i) \ge d^2/2$

We now wish to ask how hard the hardest polynomials are to evaluate in our complexity measure. By defining complexity classes of polynomials, we obtain an extension of a result due to Savage [8] on the complexity of polynomial evaluation.

Theorem 7: Let $D_F^B = \{p \in \mathbb{N}[x] \mid \delta_B(p) \le F(\deg(p))\}$ be a complexity class for polynomials and suppose that D_F^B contains all polynomials with 0,1 coefficients and + is in B; then $F(n) \ge n/\log n$.

Proof: Since D_F^B contains all 0,1 polynomials, we observe that the set $\{p(2) \mid \delta_B(p) \le F(\deg(p))\}$ contains all of $\mathbb{N}$. Now, we define $g(k) = F(\lfloor \log k \rfloor) + 1$ for integer k and claim that $C_g = N$. The proof of this follows since any integers k can be written as $p_k(2)$ where $p_k(x)$ is a polynomial with 0,1 coefficients of degree $\lfloor \log k \rfloor$ and the result of Theorem 6 implies that

$$C_B(k) = C_B(p_k(2)) \le C_B(2) + \delta_B(p_k) \le 1 + \delta_B(p_k)$$
$$\le 1 + F(\lfloor \log k \rfloor) = g(k)$$

for all integers k. Thus, $C_g = \mathbb{N}$. By Theorem 3, however, $g(n) \ge h(n)$ and hence $F(n) \ge n/\log n$. □

The result of this theorem is somewhat surprising, since we have shown the existence of polynomials with 0,1 coefficients whose evaluation by an algorithm using any finite set of basis operations requires at least $O(n/\log n)$ of these operations. For example, as a corollary to this theorem, we have

Corollary: Let $b_1 = +$ and $b_2,\ldots,b_r$ be any set of binary operations. Then there is a family $\{q_n(x)\}$ of polynomials with 0,1 coefficients such that the complexity of evaluating $q_n(x)$ by any algorithm using using the operations $b_1,\ldots,b_r$ grows asymptotically with $O(n/\log n)$.

While we have shown the existence of such a family, we leave its construction as an open problem. We can extend this result to a hierarchy result analogous to Theorem 5.

Theorem 8: (Hierarchy Theorem for Polynomials) Suppose that $\{+,\times\} \in B$ and F and K are functions such that

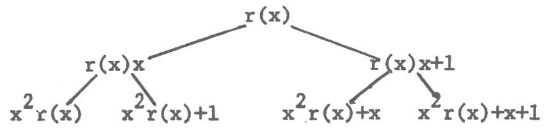
1) $F(n) > K(n) + 1$ a.e.

2) $\lim_{n\to\infty} \frac{K(n)}{\log n} \ge 1$ (i.e. D_K^B is infinite)

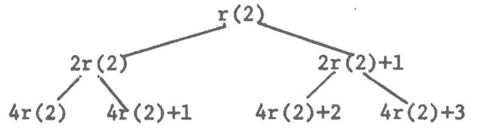
3) $\lim_{n\to\infty} \frac{K(n)}{n/\log n} = 0$ (i.e. $D_K^B \overset{\subset}{+} \mathbb{N}[x]$)

then $D_F^B - D_K^B$ is infinite.

Proof: Define p(x)x and p(x)x+1 to be the successors of $p(x)$. We claim that for any N_0 there is a $p_{N_0}(x) \in D_K{}^B$ such that one of the successors of $p_{N_0}(x)$ is not in $D_G{}^B$ and such that $p_{N_0}(x)$ is of degree at least N_0. Assume not and consider the tree $T(r(x))$ for some $r(x) \in D_K{}^B$



Either our claim is true or every node of the infinite tree $T(r(x))$ belongs to $D_K{}^B$. If every node of the tree $T(r(x))$ is in $D_K{}^B$, then every node of the tree $T'(r(2))$ is in $C_k{}^B$ where $k = K(\lfloor \log n \rfloor) + 1$ and $T'(r(2))$ is given by



But the nodes of $T'(r(2))$ are seen to have positive density and this contradicts the hypothesis of the theorem, since if this were true then for some integer n $C^B_{nk} = N$, contradicting previous results. Thus, either $r(x)x$ or $r(x)x+1$ is not in $D_K{}^B$; if we let the successor of $r(x)$ not in $D_K{}^B$ be $q(x)$, then

$$\delta_B(q(x)) \leq 2 + \delta_B(r(x)) \leq 2 + K(\deg(r(x)))$$
$$\leq F(\deg(r(x)))$$

for large enough N_0. Thus, $q(x) \in D_F{}^B$. By an argument similar to that used in the proof of Theorem 5, we can show that an infinite sequence of polynomials in $D_F{}^B - D_K{}^B$ exists. □

The results of Theorem 7 can be extended to multivariate polynomials and n-linear forms by applying reducibilities to make these problems equivalent to single variable polynomial evaluation.

References

[1] A. Brauer. Bulletin of the AMS 45:736-739, 1939.

[2] A. Borodin and S. Cook. On the number of additions to compute specific polynomials. Conference Record of the Sixth ACM Symposium on the Theory of Computing, Seattle, Washington, May 1974.

[3] S. Cook. Linear time simulation of deterministic two-way push down automata. Proceedings of IFIP Congress 71, TA-2, North-Holland, Amsterdam, 172-179.

[4] P. Erdös. Acta Arithmetica 6:77-81, 1960.

[5] D. Knuth. The Art of Computer Programming, Volume II: Seminumerical Algorithms. Addison-Wesley, Reading, Massachusetts, 1969.

[6] E. Landau. Über einige neuere Fortschritte der additiven Zahlentheorie. Cambridge, 2nd edition, 1937.

[7] I. Niven and H. Zuckerman. An Introduction to the Theory of Numbers. John Wiley and Sons, New York, 2nd edition, 1966.

[8] M. S. Paterson and L. J. Stockmeyer. On the number of nonscalar multiplications necessary to evaluate polynomials. SIAM J. Computing 2(1):60-66, March 1973.

[9] J. Savage. An Algorithm for the computation of linear forms. SIAM J. Computing 3:150-158, 1974.

[10] V. Strassen. Polynomials with rational coefficients which are hard to compute. SIAM J. Computing 3:128-149, 1974.

A GENERALIZATION AND PROOF OF THE AANDERAA-ROSENBERG CONJECTURE[†]

Ronald L. Rivest
Department of Electrical Engineering and Computer Science
Massachusetts Institute of Technology
Cambridge, Massachusetts 02139

Jean Vuillemin
Computer Science Division
Department of Electrical Engineering and Computer Sciences
University of California
Berkeley, California 94720

Abstract: *We investigate the maximum number* $C(P)$ *of arguments of* P *that must be tested in order to compute* P, *a Boolean function of* d *Boolean arguments. We present evidence for the general conjecture that* $C(P) = d$ *whenever* $P(0^d) \neq P(1^d)$ *and* P *is left invariant by a transitive permutation group acting on the arguments. A non-constructive argument (not based on the construction of an "oracle") proves the generalized conjecture for* d *a prime power. We use this result to prove the Aanderaa-Rosenberg conjecture by showing that at least* $v^2/9$ *entries of the adjacency matrix of a* v*-vertex undirected graph* G *must be examined in the worst case to determine if* G *has any given non-trivial monotone graph property.*

1. INTRODUCTION

A fundamental problem of computer science is to determine the relative efficiencies of different data structures for representing a given problem. For example, Hopcroft and Tarjan [4] mention that determining if a v-vertex graph is planar from its adjacency matrix requires $\Omega(v^2)$ operations;[††] this should be contrasted with Tarjan's [11] linear $O(v)$-time algorithm for planarity based on an adjacency-list representation of graphs. Similarly, Holt and Reingold [3] have shown that $(v+1)(v-1)/4$ inspections of the adjacency matrix of a directed graph G are required in the worst case to determine if G contains a directed cycle.

Motivated by these results, Arnold Rosenberg conjectured [10] that, for any nontrivial graph property, representing a graph by an adjacency matrix forces an algorithm which recognizes the property to make $\Omega(v^2)$ inspections of the matrix in the worst case. Aanderaa disproved this conjecture by showing that less than $3v$ inspections are needed to determine if a directed v-vertex graph contains a vertex with in-degree $v-1$ and out-degree 0 (a "sink"). To revive the conjecture, Aanderaa suggests that the graph properties should be constrained to be "monotone": If the property holds for a graph $G = (V,E)$ it must also hold for all graphs $G' = (V,E')$ such that $E \subseteq E'$. This eliminates the "sink" counterexample, and this paper provides a proof to the:

Aanderaa-Rosenberg Conjecture [10]: *In the worst case,* $\Omega(v^2)$ *operations are required to determine from the adjacency matrix of a graph* G *whether it has a property* P *which is (i) nontrivial, (ii) monotone, (iii) independent of the labellings of the vertices, and (iv) independent of the existence of self-loops (see [6]).*

There is in fact no evidence to contradict the stronger conjecture that each of the $v(v-1)/2$ entries of the adjacency matrix of an undirected graph ($v(v-1)$ entries for a directed graph) must be examined in the worst case. In [1], [5], and [7], many properties satisfying (i)-(iv) above are shown to require $\Omega(v^2)$ operations, and Kirkpatrick [5] shows that $\Omega(v \log_2(v))$ operations are always required, giving support to the original conjecture. These results are all obtained by oracle construction techniques, with the exception of Best, Van Emde Boas, and Lenstra [1], who independently discovered the approach we will use here.

In this paper we present a generalization of the Aanderaa-Rosenberg Conjecture, prove this generalized conjecture for Boolean properties having a prime-power number of arguments. We use this result to prove the original Aanderaa-Rosenberg conjecture.

2. DEFINITIONS

Functions and Vectors

Let $P(x_1,\ldots,x_d)$ be a Boolean function (property) mapping $\{0,1\}^d$ onto $\{0,1\}$, denoted $P\colon \{0,1\}^d \mapsto \{0,1\}$. We say "$P(\underset{\sim}{x})$ holds" or "$\underset{\sim}{x}$ has property P" iff $P(\underset{\sim}{x}) = 1$. Let $\underset{\sim}{x} \leq \underset{\sim}{y}$ denote $x_i \leq y_i$ for $1 \leq i \leq d$, with $\underset{\sim}{x}, \underset{\sim}{y} \in \{0,1\}^d$. Let $\underset{\sim}{0}$ (respectively $\underset{\sim}{1}$) represent the d-bit vector of zeros (respectively ones). We say that P is monotone if $\underset{\sim}{x} \leq \underset{\sim}{y}$ implies $P(\underset{\sim}{x}) \leq P(\underset{\sim}{y})$ for all $\underset{\sim}{x}, \underset{\sim}{y}$ in $\{0,1\}^d$. The weight $w(\underset{\sim}{x})$ of a vector $\underset{\sim}{x}$ is the number of ones in $\underset{\sim}{x}$.

Permutation Groups

We denote permutations and permutation groups by lower and upper case Greek letters, respectively.

[†] This work was supported by IRIA-Laboria, 78150 Rocquencourt, France, and by National Science Foundation Grant DCR74-07644-A01.

[††] We use the "omega" notation for lower bounds as the inverse of the "big-O" notation for upper bounds: $f(v) = \Omega(v^2)$ means $v^2 = O(f(v))$ or equivalently $(\exists c > 0)(\forall v) f(v) \geq cv^2$.

The symmetric group of all permutations of degree d is denoted by Σ_d. Let $|\Gamma|$ denote the order of a group Γ, and $\Gamma_1 \leq \Gamma_2$ means that Γ_1 is a subgroup of Γ_2. A permutation group Γ acting on the set $\{1,\ldots,d\}$ is transitive if, for each pair i, j of integers in $\{1,\ldots,d\}$, there is a permutation $\sigma \in \Gamma$ such that $\sigma(i) = j$.

If $P: \{0,1\}^d \mapsto \{0,1\}$, then $\Gamma(P)$ denotes the stabilizer of P:

$$\Gamma(P) = \{\sigma \in \Sigma_d | (\forall \underset{\sim}{x} \in \{0,1\}^d) P(x_1,\ldots,x_d) = P(x_{\sigma(1)},\ldots,x_{\sigma(d)})\}$$

For $\underset{\sim}{x} \in \{0,1\}^d$ and $\Gamma \leq \Sigma_d$ let $\underset{\sim}{x}\Gamma$ represent the orbit of $\underset{\sim}{x}$ under the action of Γ on $\{0,1\}^d$:

$$\underset{\sim}{x}\Gamma = \{\underset{\sim}{y} \in \{0,1\}^d | (\exists \sigma \in \Gamma)(\forall i \in \{1,\ldots,d\}) x_i = y_{\sigma(i)}\}.$$

For example, note that $\underset{\sim}{y} \in \underset{\sim}{x}\Gamma(P)$ implies that $P(\underset{\sim}{x}) = P(\underset{\sim}{y})$, but not conversely in general.

Graphs

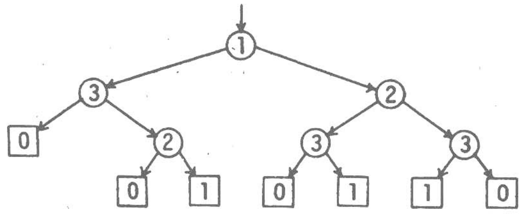
An undirected graph $G = (V,E)$ consists of a vertex set V of size v, and a set $E \subset V^{(2)}$ of edges ($V^{(2)}$ denotes the set of 2-subsets of V). Thus "multiple edges" and "self-loops" are specifically excluded. The adjacency matrix for G is a Boolean vector of length $\binom{v}{2}$, with one position for each edge in $V^{(2)}$, which is 1 iff that edge is in E. The complete graph K_v is $(V,V^{(2)})$, the empty graph E_v is $(V,\emptyset)$.

Let $\Sigma_v^{(2)}$ denote the permutation group acting on $V^{(2)}$ induced by the symmetric group Σ_v acting on V so that $\sigma(\{i,j\}) = \{\sigma(i),\sigma(j)\}$ for each $i, j \in V$ using transparent notation. Two graphs $G = (V,E)$ and $G' = (V,E')$ are isomorphic, written $G \cong G'$, if there exists a permutation $\sigma \in \Sigma_v^{(2)}$ such that $(\{i,j\} \in E) \Leftrightarrow (\sigma(\{i,j\}) \in E')$.

A Boolean function $P: \{0,1\}^d \mapsto \{0,1\}$, where $d = \binom{v}{2}$ is a graph property if $\Sigma_v^{(2)} \leq \Gamma(P)$. Intuitively, this means that P does not depend upon the labelling of the vertices, or, equivalently that $(G \cong G') \Rightarrow (P(G) = P(G'))$. (We use $P(G)$ to mean $P(\underset{\sim}{x})$, where $\underset{\sim}{x}$ is the adjacency matrix of G.)

Algorithms

We consider "decision-tree" algorithms for computing $P(\underset{\sim}{x})$. For a given function $P: \{0,1\}^d \mapsto \{0,1\}$, and an input vector $\underset{\sim}{x} \in \{0,1\}^d$, a decision-tree computes $P(\underset{\sim}{x})$ by successively examining the various components (coordinates) x_i of $\underset{\sim}{x}$. As an example, the following tree determines whether a vector $\underset{\sim}{x} \in \{0,1\}^3$ has exactly two ones:



The algorithm is a binary tree T whose internal nodes are labelled with the indices i of the x_i to be tested. Testing begins with the x_i specified at the root, if it is zero, the algorithm continues with the x_i specified at the root of the left subtree, otherwise it proceeds to the right. The leaf which is eventually reached specifies the value of P for the input vector. Let $c(T,\underset{\sim}{x})$ denote the number of tests made using T to compute $P(\underset{\sim}{x})$. In our example $c(T,000) = 2$ and $c(T,101) = 3$. The depth of a leaf is the number of tests made in order to arrive at that leaf (the path length from the root).

Let $c(T)$ denote the maximum value of $c(T,\underset{\sim}{x})$ for any $\underset{\sim}{x} \in \{0,1\}^d$, and let $C(P)$, the argument complexity of P, be the minimum value of $c(T)$ of all trees T which compute P. Thus $C(P)$ is the minimum number of arguments which must be examined in the worst-case, independent of the algorithm used. If $C(P) = d$ we say that P is exhaustive. Note that $C(P)$ is a lower bound on the time any algorithm recognizing P must take in the worst case, on any model of machine where no two operations can take place at the same time.

3. THE ARGUMENT COMPLEXITY OF ARBITRARY FUNCTIONS

Before attacking the Aanderaa-Rosenberg conjecture directly, let us step back and try to see what are the important parts of the problem. The fact that we are considering graph properties is not essential to the conjecture: matroid or hypergraph properties work as well. Requiring P to be a graph property only means that $\Gamma(P)$ must have a "nice" structure.

Considering P, an arbitrary $\{0,1\}^d \mapsto \{0,1\}$ function, and ignoring for the moment restrictions on $\Gamma(P)$, what can we say about $C(P)$?

Note that a leaf L at depth k in a tree T for P is reached by exactly those 2^{d-k} vectors which vary in all possible ways in the $d-k$ untested positions and which have specified values in the k tested positions. The value of P for each of these vectors is the same. If every leaf $L \in T$ has depth less than d, say $k_0 = \max_{L \in T}(\text{depth}(L)) < d$ then 2^{d-k_0} must divide $|\{\underset{\sim}{x} \in \{0,1\}^d | P(\underset{\sim}{x}) = 1\}|$. From this simple observation, it follows that:

Lemma 1. *If* $|\{\underset{\sim}{x} | P(\underset{\sim}{x}) = 1\}|$ *is odd, then* P *must be exhaustive.*

Proof. An odd number is not the sum of even numbers. □

In order to strengthen this result let the weight polynomial $P^1(z)$ of P be defined as:

$$P^1(z) = \sum_{0 \leq i \leq d} w_i(P) \cdot z^i$$

with $w_i(P) = |\{\underset{\sim}{x} | (P(\underset{\sim}{x}) = 1) \wedge (w(\underset{\sim}{x}) = i)\}|$,

so that the coefficient of z^i is the number of vectors $\underset{\sim}{x}$ of weight i such that $P(\underset{\sim}{x}) = 1$. The contribution of a leaf L at depth k specifying a value 1 for P is $z^j(1+z)^{d-k}$, if j

of the k tests on the path to L gave one as an answer.

Theorem 1. *If* $C(P) \leq k$, *then* $(1+z)^{d-k}$ *divides* $P^1(z)$.

Proof. In the optimal tree T for P, each leaf L specifying 1 for P contributes a multiple of $(1+z)^{d-k}$ to $P^1(z)$. □

Taking $k=d-1$ and $z=1$ in Theorem 1 yields Lemma 1, since $P^1(1) = |\{\underset{\sim}{x} \in \{0,1\}^d | P(\underset{\sim}{x}) = 1\}|$. Theorem 1 also implies that, if $c(P) < d-1$, then $P^1(-1) = 0$, which means that the numbers of even- and odd-weight vectors for which P is true, are equal. Using this observation, it is easy to derive:

Corollary 1. *As* $d \to \infty$, *almost all functions* $P\colon \{0,1\}^d \mapsto \{0,1\}$ *are exhaustive.*

Proof. The number of functions $P\colon \{0,1\}^d \to \{0,1\}$ having

$$|\{\underset{\sim}{x}|\ P(\underset{\sim}{x}) \wedge (w(\underset{\sim}{x}) \text{ odd})\}| = |\{\underset{\sim}{x}|\ P(\underset{\sim}{x}) \wedge (w(\underset{\sim}{x}) \text{ even})\}| = k$$

is $\binom{2^{d-1}}{k}^2$, so that we have

$$\text{Prob}(P \text{ non-exhaustive}) \leq 2^{-2^d} \sum_{0 \leq k \leq 2^{d-1}} \binom{2^{d-1}}{k}^2 = 2^{-2^d} \binom{2^d}{2^{d-1}} \cong (\pi \cdot 2^{d-1})^{-1/2},$$

which goes very rapidly to 0 as $d \to \infty$. □

Since most functions are exhaustive, it seems reasonable to expect that there are large classes of functions, such as those for which $\Gamma(P)$ has a nice structure, which are uniformly exhaustive.

4. THE GENERALIZED AANDERAA-ROSENBERG CONJECTURE

The next question to ask is: If we restrict P to be a graph property $(\Sigma_V^{(2)} \leq \Gamma(P))$, what are the characteristics of $\Sigma_V^{(2)}$ that might enable us to show that P is exhaustive?

The most noticeable feature of $\Sigma_V^{(2)}$, aside from the fact that it is a representation of Σ_V, is that it acts transitively on $V^{(2)}$. Each edge in $V^{(2)}$ is equivalent to (can be mapped into) any other edge, so the testing algorithm has no way of selecting an initial edge which is preferable for testing to any other edge.

Is it possible that the transitivity of $\Sigma_V^{(2)}$ is sufficient? What can be said about functions P such that $\Gamma(P)$ is transitive?

Lemma 2. *If* $\Gamma(P)$ *is transitive, then*

$$w(\underset{\sim}{x}) \cdot |\underset{\sim}{x}\Gamma(P)| = d \cdot b(\underset{\sim}{x}) \qquad (1)$$

where $b(\underset{\sim}{x}) = |\{y \in \underset{\sim}{x}\Gamma(P)|\ y_1 = 1\}|$.

Proof. Let M denote the $|\underset{\sim}{x}\Gamma(P)|$ by d matrix whose rows are the vectors in $\underset{\sim}{x}\Gamma(P)$. The left side of (1) counts the number of ones in M by rows, the right side by columns. By transitivity each column contains $b(\underset{\sim}{x})$ ones, since a permutation of the columns of M by an element $\sigma \in \Gamma(P)$ is equivalent to a permutation of the rows of M. □

Corollary 2. *If* $d = p^\alpha$ *for some prime* p *and integer* α, $\Gamma(P)$ *is transitive, and* $\underset{\sim}{x} \in \{0,1\}^d$, $\underset{\sim}{x} \neq \underset{\sim}{0}$, $\underset{\sim}{x} \neq \underset{\sim}{1}$, *then* p *divides* $|\underset{\sim}{x}\Gamma(P)|$.

Proof. Immediate. Note that $|\underset{\sim}{0}\Gamma(P)| = |\underset{\sim}{1}\Gamma(P)| = 1$ always.

This yields the following result:

Theorem 2. *For* $P\colon \{0,1\}^d \to \{0,1\}$ *if* $\Gamma(P)$ *is transitive,* d *is a prime power and* $P(\underset{\sim}{0}) \neq P(\underset{\sim}{1})$, *then* P *is exhaustive.*

Proof. Consider evaluating $P^1(-1) \bmod p$, where we calculate the number of vectors $\underset{\sim}{x}$ of even and odd weight for which $P(\underset{\sim}{x}) = 1$ on an orbit by orbit basis. From Corollary 2 the only orbits of interest are $\underset{\sim}{0}\Gamma(P)$ and $\underset{\sim}{1}\Gamma(P)$. Thus $P^1(-1) \equiv 1 \bmod p$, unless $P(\underset{\sim}{1}) = 1$ and p is odd, in which case $P^1(-1) \equiv -1 \bmod p$. In either case, $P^1(-1) \neq 0$ and the result follows by Theorem 1. □

Note that $P(\underset{\sim}{0}) \neq P(\underset{\sim}{1})$ is true whenever P is a nontrivial monotone function. Examination of many small cases has led us to the following.

The Generalized Aanderaa-Rosenberg Conjecture. *If* $P\colon \{0,1\}^d \to \{0,1\}$ *is such that* $\Gamma(P)$ *is transitive and* $P(\underset{\sim}{0}) \neq P(\underset{\sim}{1})$, *then* P *is exhaustive.*

By the above remarks the generalized conjecture implies the original Aanderaa-Rosenberg conjecture and Theorem 2 lends support to the generalized conjecture by proving that it holds whenever d is a prime power.

A proof of the generalized conjecture cannot be obtained by a simple extension of the proof of Theorem 2, for the reason that if d is composite, the sizes of the orbits may be any one of many sizes. The result is that there exist functions P satisfying the conditions of the generalized conjecture having $P^1(-1) = 0$, so that the proof technique fails. For the record, we note the smallest such P discovered: Take $d = 12$, and $P(\underset{\sim}{x}) = (\exists \underset{\sim}{y} \in S)(\underset{\sim}{x} \geq \underset{\sim}{y})$ where S contains all vectors in the orbits under the cyclic group C_{12} of $(1^3 0)^3$, $1^7 0^2 1^2 0$, $(1^2 0)^4$, and $(1^4 0^2)^2$. For graphs a similar situation occurs if $P(G)$ is the function: G is not a subgraph of any of the graphs ||||·, ΔΔΔ, or □·⁚⁚, for 9-vertex graphs. Both of these functions are monotonic. Using ad-hoc arguments based upon Theorem 3 below, they can however be shown to be exhaustive; we know of no counterexamples to the generalized conjecture.

While there are functions which are exhaustive and yet have $(1+z)|P^1(z)$ (that is, with $P^1(-1) = 0$), the authors do not know of any satisfying $(1+z)^2|P^1(z)$. This is made relevant by the following:

Theorem 3. *If* $P\colon \{0,1\}^d \mapsto \{0,1\}$ *is a non-exhaustive function with* $\Gamma(P)$ *transitive, then* $(1+z)^2|P^1(z)$.

Proof. Let $Q(\underset{\sim}{x})$ be the Möbius inverse of $P(\underset{\sim}{x})$, so that $P(\underset{\sim}{x}) = \sum_{\underset{\sim}{0} \le \underset{\sim}{y} \le \underset{\sim}{x}} Q(\underset{\sim}{x})$, implying that

$$Q(\underset{\sim}{x}) = \sum_{\underset{\sim}{0} \le \underset{\sim}{y} \le \underset{\sim}{x}} P(\underset{\sim}{x})(-1)^{w(\underset{\sim}{x} \oplus \underset{\sim}{y})}$$ by Möbius inversion,

where $\underset{\sim}{x} \oplus \underset{\sim}{y}$ is component-wise "exclusive-or". Since P is not exhaustive, by Theorem 1 $Q(\underset{\sim}{1}) = P^1(-1) = 0$. By the transitivity of $\Gamma(P)$, each of the restricted functions $P_i(\underset{\sim}{x}) = P(\underset{\sim}{x} | x_i=0)$ for $1 \le i \le d$ must be non-exhaustive, since it makes no difference which argument is tested first. This implies similarly that $Q(1^{i-1}01^{d-i}) = P_i^1(-1) = 0$ for each i. Thus

$$\begin{aligned} P^1(z) &= \sum_{\underset{\sim}{0} \le \underset{\sim}{x} \le \underset{\sim}{1}} P(\underset{\sim}{x}) \cdot z^{w(\underset{\sim}{x})} \\ &= \sum_{\underset{\sim}{0} \le \underset{\sim}{x} \le \underset{\sim}{1}} \; \sum_{\underset{\sim}{0} \le \underset{\sim}{y} \le \underset{\sim}{x}} Q(\underset{\sim}{y}) z^{w(\underset{\sim}{x})} \\ &= \sum_{\underset{\sim}{0} \le \underset{\sim}{y} \le \underset{\sim}{1}} Q(\underset{\sim}{y}) z^{w(\underset{\sim}{y})} (1+z)^{d-w(\underset{\sim}{y})} , \end{aligned}$$

implying the theorem. More generally, if $\Gamma(P)$ is k-transitive and P is not exhaustive then $(1+z)^{k+1}$ divides $P^1(z)$. □

A proof of the general conjecture might be obtainable by showing that if P satisfies the conditions of the conjecture, then $(1+z)^2$ does not divide $P^1(z)$. Theorem 2 is a very strong condition a function must meet to be non-exhaustive. Unfortunately we have to date been unable to apply this result successfully to the general conjecture.

Although Theorem 1 is as we have noted insufficient to prove the general conjecture, it can be used to prove interesting subcases, where we require $\Gamma(P)$ to have more structure than merely be transitive:

Theorem 4. *If* $P: \{0,1\}^d \mapsto \{0,1\}$ *such that* $P(\underset{\sim}{0}) \neq P(\underset{\sim}{1})$ *and* $\Gamma(P)$ *is transitive and Abelian, and* $d \varepsilon E$ *(defined below) then* P *is exhaustive. The set* E *is the smallest set of natural numbers such that* $1 \varepsilon E$ *and* $(n \varepsilon E)(q \text{ prime}) \wedge (q \ge 2^{n-1}) \Rightarrow nq^k \varepsilon E$ *for all natural numbers* k.

Proof. Let $d = nq^k$. The group $\Gamma(P)$ has a normal Sylow subgroup Θ of order $|\Theta| = q^k$. By considering the quotient group $\Gamma(P)/\Theta$, we establish a 1-1 correspondence between the orbits whose size is not a multiple of q, and those of a smaller function $Q: \{0,1\}^n \mapsto \{0,1\}$, satisfying the hypothesis, thus $Q^1(-1) \neq 0$. Since $P^1(-1) \equiv Q^1(-1) \bmod q$ and $|Q^1(-1)| < 2^{n-1}$, the conclusion $P^1(-1) \neq 0$ follows from $d \varepsilon E$, i.e., $q \ge 2^{n-1}$. □

The set E contains all prime powers and many composite numbers (having an arbitrary number of prime factors) but not all natural numbers; it's density in the natural numbers is not significantly greater than that of the primes.

5. THE AANDERAA-ROSENBERG CONJECTURE

We return to the Aanderaa-Rosenberg conjecture and apply the results of the preceding section to show that $C(P) = \Omega(v^2)$ if P is a monotone nontrivial graph property. While we believe that $C(P) = \binom{v}{2}$ is always the case, the results of the preceding sections do not directly apply since $\binom{v}{2}$ is never a prime power unless $v = 2$ or $v = 3$. We have to reduce the problem to one we can handle, at some loss in the strength of results.

It is not difficult to verify that $C(P) = \binom{v}{2}$ for $2 \le v \le 6$ by hand; we have also shown this to be true for $v = 7$, 11, and 13. For the latter cases it suffices to note that $|\underset{\sim}{x}\Gamma(P)| \equiv 0 \bmod v$ unless $\underset{\sim}{x}$ represents a graph with cyclic symmetry (that is, invariant under a cyclic permutation of the vertices). This reduces the calculation of the possible values of $P^1(-1) \pmod v$ to a manageable task.

When v is prime, the remark that $|\underset{\sim}{x}\Gamma(P)| \equiv 0 \bmod v$ unless $\underset{\sim}{x}$ represents a graph with cyclic symmetry allows one to state the following

Lemma 3. *If* v *is prime and* P *is a monotone nontrivial graph property on* v*-vertex graphs such that* $P(H_v) = 1$ *(where* H_v *is a* v*-vertex Hamiltonian circuit), then* P *is exhaustive.*

Proof. Calculate $P^1(-1) \pmod v$. If a nonempty graph has cyclic symmetry it contains H_v as a subgraph. Thus $P^{-1}(-1) \equiv -1 \bmod v$, since E_v is the only orbit with size $\not\equiv 0 \pmod v$ not counted in $P^1(-1)$. □

The preceding gives some cases for which $C(P) = \binom{v}{2}$. To prove the weaker result that $C(P) = \Omega(v^2)$ we proceed in two steps: (1) we show that $C(P) = \Omega(v^2)$ for v a power of 2, and (2) show that $C(P)$ is more or less monotone increasing with v.

We say that a graph G is point (resp. line) -symmetric if for any pair of points (resp. lines) there is an automorphism of G mapping the first into the second. Let nG denote n disjoint copies of a graph G, $G_1 + G_2$, the graph consisting of a copy of G_1 and a (disjoint) copy of G_2, and let $G_1 \times G_2$ denote the graph $G_1 + G_2$ with every point in G_1 joined to every point in G_2.

Suppose $v = 2^n$, and let H_i denote $2^{n-i}K_{2^i}$ (that is, 2^{n-i} copies of the complete graph on 2^i points), so that $H_o = E_v$, $H_n = K_v$, and H_i is a subgraph of H_{i+1} for $0 \le i < n$ (denoted $H_i \le H_{i+1}$). Since P is nontrivial, there is a j such that $P(H_j) = 0$ and $P(H_{j+1}) = 1$. Let J_i be the graph $2^{n-i-1}K_{2^i}$, so that $H_i = J_i + J_i$, and furthermore $H_{i+1} \le J_i \times J_i$. Thus we have $P(J_j+J_j) = 0$ and $P(J_j \times J_j) = 1$ by monotonicity of P.

To show that $C(P) \ge v^2/4$ we will count only the edges that must be examined in $(J_j \times J_j) - (J_j+J_j)$, assuming that the algorithm can determine "free of charge" that the input graph contains a subgraph isomorphic to $J_j + J_j$. More precisely, let $G = (V,E)$ denote the unknown graph (input to the algorithm), where $|V| = 2^n$, $V = V_1 \cup V_2$, with $|V_1| = |V_2| = 2^{n-1}$. Since restricting the possibilities for G can at most decrease $C(P)$ (it can only "help" the algorithm), we consider the case that $G_1 = (V_1, E \cap V_1^{(2)})$ and $G_2 = (V_2, E \cap V_2^{(2)})$ are both isomorphic to J_j. Now P as a function of $E' = E - V_1^{(2)} - V_2^{(2)}$ is still nontrivial by our choice of j. Furthermore $|E'| = 2^{2n-2}$ is a prime power, so we are almost ready to apply Theorem 2 to P as a function of E' (call this function P').

To show that P' must be left invariant by a transitive permutation group acting on E', we note that J_j is point-symmetric. Thus for any pair of edges $e = \{v_1, v_2\}$ and $e' = \{v_1', v_2'\}$ in $V^{(2)} - V_1^{(2)} - V_2^{(2)}$ (where $v_1, v_1' \varepsilon V_1$; $v_2, v_2' \varepsilon V_2$) there is an automorphism of G_1 carrying v_1 into v_1' and an automorphism of G_2 carrying v_2 into v_2', thus an automorphism of $G_1 \times G_2$ carrying e into e'. Since P is invariant under permutations in $\Sigma_V^{(2)}$, it is invariant under any subgroup of $\Sigma_V^{(2)}$, and in particular the automorphism group of $G_1 \times G_2$. Thus P as a function of the edges in $(J_j \times J_j) - (J_j + J_j)$ is left invariant by the transitive permutation group $\Sigma_{v/2} \times \Sigma'_{v/2}$. (Here $\Sigma_{v/2}$ (resp. $\Sigma'_{v/2}$) is the symmetric group on V_1 (resp. V_2), and $(\sigma,\tau)\{v_1,v_2\} = \{\sigma(v_1),\tau(v_2)\}$ for $v_1 \varepsilon V_1$, $v_2 \varepsilon V_2$, $(\sigma,\tau) \varepsilon \Sigma_{v/2} \times \Sigma'_{v/2}$, $\sigma \varepsilon \Sigma_{v/2}$, $\tau \varepsilon \Sigma'_{v/2}$.) We can then apply Theorem 2 to obtain

Theorem 5. *If* $v = 2^n$ *and* P *is a monotone nontrivial graph property on* v*-vertex graphs, then* $C(P) \geq v^2/4$.

It remains to treat the cases where v is not a power of two. Let $C(v)$ denote the minimum value of $C(P)$ as P ranges over all nontrivial monotone properties of v-vertex graphs.

Lemma 4. $C(v) \geq \min(C(v-1), 2^{2k-2})$, *where* $2^k < v < 2^{k+1}$.

Proof. Consider a monotone property P of v-vertex graphs. Then either

(i) $P(K_1 + K_{v-1}) = 1$,

(ii) $P(K_1 \times E_{v-1}) = 0$, or

(iii) neither of the above.

Cases (i) and (ii) directly imply that $C(v) > C(v-1)$ since the algorithm can obtain "free" the information that some vertex is either isolated or connected to all other vertices, and P restricted to the remaining edges is still a monotone nontrivial graph property. Case (iii) implies, using u for 2^{k-1}, that

$$P(E_{v-u} + K_u) = 0$$

since (i) fails, P is monotone, and $E_{v-u} + K_u \leq K_1 + K_{v-1}$. Also $P(E_{v-u} \times K_u) = 1$, since (ii) fails, P is monotone, and $K_1 \times E_{v-1} \leq K_u \times E_{v-u}$. Now we may apply Theorem 2 directly as in the proof of Theorem 5, after "giving away" to the algorithm that the input graph contains a subgraph isomorphic to $E_{v-u} + K_u$, and force it to ask for all the 2^{2k-2} edges linking the two copies of K_u (it is easy to see the transitivity requirement is also met for the restricted function). Thus we have proved by Lemma 4 and

Theorem 6. *If* P *is a nontrivial monotone graph property of* v*-vertex graphs, then* $C(P) \geq v^2/16$.

Dan Kleitman has improved this bound to $C(P) \geq v^2/9$ by proving an equivalent of Theorem 5 showing $C(P) \geq v^2/3$ for v of the form $3 \cdot 2^n$ and then modifying Lemma 4 slightly as well.

6. CONCLUSIONS

The technique introduced in this paper is a new means for establishing the worst-case complexity of Boolean functions, measured in terms of the number of arguments examined. It is not based on the construction of oracles, or on information-theoretic considerations, but rather on a strong necessary condition for $C(P) < d$ to occur. Our generalized conjecture states the minimal conditions that we believe necessary to ensure that $C(P) = d$: namely that $P(\underline{0}) \neq P(\underline{1})$ and $\Gamma(P)$ be transitive. A proof of our generalized conjecture in the case that d is a prime power allows us to settle the Aanderaa-Rosenberg conjecture in the affirmative.

7. ACKNOWLEDGMENTS

We should like to thank the many people who have made helpful suggestions to us during the course of this research: Peter van Emde Boas (who has independently discovered this technique with Best and Lenstra [1]), Joel Coffy, Laurent Hyafil, Richard Karp, David Klarner, Vera Pless (who simplified our earlier proofs by pointing out Lemma 2 to us), Dan Kleitman, and Marc Schutzenberger.

8. REFERENCES

[1] M.R. Best, P. van Emde Boas and H.W. Lenstra, Jr., "A Sharpened Version of the Aanderaa-Rosenberg Conjecture," (preprints from the authors) (1974).

[2] F. Harary, Graph Theory, Addison-Wesley (1969).

[3] R.C. Holt and E.M. Reingold, "On the Time Required to Detect Cycles and Connectivity in Graphs," Math. Systems Theory 6 (1972).

[4] J. Hopcroft and R. Tarjan, "Efficient Planarity Testing," Cornell University Computer Science Tech. Report TR 73-165 (1973).

[5] D. Kirkpatrick, "Determining Graph Properties from Matrix Representations," Proc. 6th SIGACT Conf., Seattle (1974).

[6] R.J. Lipton and L. Snyder, "On the Aanderaa-Rosenberg Conjecture," SIGACT News 6 (1974).

[7] E.C. Milner and D.J.A. Welsh, "On the Computational Complexity of Graph Theoretical Properties," University of Calgary, Dept. of Mathematics, Research Paper No. 232 (1974).

[8] R.L. Rivest and J. Vuillemin, "On the Number of Argument Evaluations Required to Compute Boolean Functions," U.C. Berkeley Electronics Research Laboratory Memorandum ERL-M472 (Oct. 1974).

[9] R.L. Rivest and J. Vuillemin, "On the Time Required to Recognize Properties of Graphs from Their Adjacency Matrices," U.C. Berkeley Electonics Research Laboratory Memorandum ERL-M476 (Nov. 1974).