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 $P: \{0,1\}^d \mapsto \{0,1\}$. We say "$P(x)$ holds" or "x has property P" iff $P(x) = 1$. 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 0 (respectively 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:

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

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 $\{0,1\}^d$:

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

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

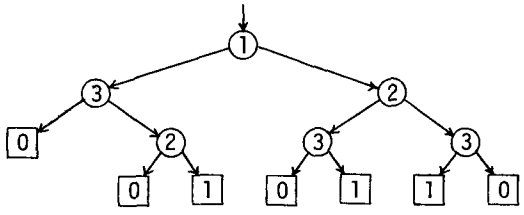
An undirected graph $G = (V,E)$ consists of a vertex set V of size v, and a set $E \subseteq V^{(2)}$ of edges ($V^{(2)}$ denotes the set of 2-subsets of V). Thus "multiple edges" and "self-loops" are specifically excluded. The adjacency matrix for G is a Boolean vector of length $\binom{v}{2}$, with 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 $|\{\underset{\sim}{x} \in \{0,1\}^d \mid P(\underset{\sim}{x}) = 1\}|$. From this simple observation, it follows that:

Lemma 1. *If* $|\{\underset{\sim}{x} \mid P(\underset{\sim}{x}) = 1\}|$ *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 $w_i(P) = |\{\underset{\sim}{x} \mid (P(\underset{\sim}{x}) = 1) \wedge (w(\underset{\sim}{x}) = i)\}|$, 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_j 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* $P: \{0,1\}^d \mapsto \{0,1\}$ *are exhaustive.*

Proof. The number of functions $P: \{0,1\}^d \to \{0,1\}$ 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* $P: \{0,1\}^d \to \{0,1\}$ *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 $P^1(-1)$ mod 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* $P: \{0,1\}^d \to \{0,1\}$ *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 $(1^30)^3$, $1^70^21^20$, $(1^20)^4$, and $(1^40^2)^2$. For graphs a similar situation occurs if $P(G)$ is the function: G is not a subgraph of any of the graphs $||||$., $\Delta\Delta\Delta$, or $\square\cdot\cdot\cdot$, 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* $P: \{0,1\}^d \mapsto \{0,1\}$ *is a nonexhaustive 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* $P(0) \ne P(1)$ *and* $\Gamma(P)$ *is transitive and Abelian, and* $d \in E$ *(defined below) then* P *is exhaustive. The set* E *is the smallest set of natural numbers such that* $1 \in E$ *and* $(n \in E)(q \text{ prime}) \wedge (q \ge 2^{n-1}) \Rightarrow nq^k \in E$ *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 $Q^1(-1) \ne 0$. Since $P^1(-1) \equiv Q^1(-1) \bmod q$ and $|Q^1(-1)| < 2^{n-1}$, the conclusion $P^1(-1) \ne 0$ follows from $d \in E$, 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 $P^1(-1) \bmod v$ 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 $P^1(-1) \bmod v$. 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 $\not\equiv 0 \bmod v$ 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 $H_0 = E_v$, $H_n = K_v$, 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 $v_1, v_1' \in V_1$; $v_2, v_2' \in V_2$) 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 $v_1 \in V_1$, $v_2 \in V_2$, $(\sigma,\tau) \in \Sigma_{v/2} \times \Sigma'_{v/2}$, $\sigma \in \Sigma_{v/2}$, $\tau \in \Sigma'_{v/2}$.) 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 $C(v) \geq C(v-1)$ 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 $P(\tilde{0}) \neq P(\tilde{1})$ 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).

[10] A.L. Rosenberg, "On the Time Required to Recognize Properties of Graphs: A Problem," SIGACT News 5 (1973).
[11] R. Tarjan, "Depth-first Search and Linear Graph Algorithms," SIAM J. on Computing, vol. 1, no. 2 (1972).