Theoretical Computer Science 3 (1976) 371–384.

ON RECOGNIZING GRAPH PROPERTIES FROM ADJACENCY MATRICES*

Ronald L. RIVEST

Laboratory for Computer Science, Massachusetts Institute of Technology, Cambridge, MA 02139, U.S.A.

Jean VUILLEMIN

Computer Science Division, Department of Electrical Engineering and Computer Science, University of California, Berkeley, CA 94720, U.S.A.

Communicated by A. Meyer
Received 31 December 1975
Revised October 1976

Abstract. A conjecture of Aanderaa and Rosenberg [15] motivates this work. 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 invariant under a transitive permutation group acting on the arguments. A non-constructive argument (not based on the construction of an "oracle") settles this question for d a prime power. We use this result to prove the Aanderaa–Rosenberg conjecture: at least $v^2/16$ 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 [6] mention that determining if a v-vertex graph is planar from its adjacency matrix requires $\Omega(v^2)$ operations[1]; this should be contrasted with Tarjan's [16] linear $0(v)$-time algorithm for planarity based on an adjacency-list representation of graphs. Similarly, Holt and Reingold [5] have shown that $(v^2-1)/4$ inspections of the adjacency matrix of a directed graph G are required in the worst case to determine if G contains a directed cycle.

* This work was supported by IRIA-Laboria, 78150 Rocquencourt, France, and by the National Science Foundation under NSF grant number GJ43634X, contract number DCR74-12997-A01, and NSF grant no. MCS76-14294.

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

Motivated by these results, Arnold Rosenberg conjectured [15] 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 fewer 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 leads to the following conjecture.

Aanderaa–Rosenberg Conjecture [15]. 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 [10]).

There is in fact no evidence to contradict the stronger conjecture that each of the $v(v-1)/2$ independent 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 [2], [7], and [11], 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 result 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[2].

In this paper we present a generalization of the Aanderaa–Rosenberg Conjecture, and 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 $P: \{0,1\}^d \to \{0,1\}$. We say "$P(\boldsymbol{x})$ holds" or "$\boldsymbol{x}$ has property P" iff $P(\boldsymbol{x})=1$. Let $\boldsymbol{x} \leqslant \boldsymbol{y}$ denote $x_i \leqslant y_i$ for $1 \leqslant i \leqslant d$, with $\boldsymbol{x}, \boldsymbol{y} \in \{0,1\}^d$. Let $\mathbf{0}$ (respectively $\mathbf{1}$) represent the d-bit vector of zeros (respectively ones). We say that P is *monotone* if $\boldsymbol{x} \leqslant \boldsymbol{y}$ implies $P(\boldsymbol{x}) \leqslant P(\boldsymbol{y})$ for all $\boldsymbol{x}, \boldsymbol{y}$ in $\{0,1\}^d$. The *weight* $w(\boldsymbol{x})$ of a vector $\boldsymbol{x}$ is the number of ones in $\boldsymbol{x}$.

[2] The key observation of the method, summarized in Lemma 1, was also independently made by V. Chvàtal.

Permutation groups

We denote permutations and permutation groups by lower and upper case Greek letters, respectively. The *symmetric group* of all permutations of degree d is denoted by Σ_d. Let $|\Gamma|$ denote the *order* of a group Γ, and $\Gamma_1 \leqslant \Gamma_2$ mean 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 of $\sigma \in \Gamma$ such that $\sigma(i) = j$.

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

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

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

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

For example, note that $\boldsymbol{y} \in \boldsymbol{x}\Gamma(P)$ implies that $P(\boldsymbol{x}) = P(\boldsymbol{y})$, but not conversely in general. A Boolean function $P : \{0,1\}^d \to \{0,1\}$ is said to be *transitive* whenever $\Gamma(P)$ is itself transitive.

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 $(\{i,j\} \in E) \iff (\sigma(\{i,j\}) \in E')$.

A boolean function $P : \{0,1\}^d \to \{0,1\}$, where $d = \binom{v}{2}$, is said to be a *graph property* if $\Sigma_v^{(2)} \leqslant \Gamma(P)$. Intuitively, this means that P does not depend upon the labelling of the vertices, or equivalently that $(G \cong G') \Longrightarrow (P(G) = P(G'))$. (We use $P(G)$ to mean $P(\boldsymbol{x})$, where $\boldsymbol{x}$ is the adjacency matrix of G.) Note that any graph property is transitive.

Algorithms

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

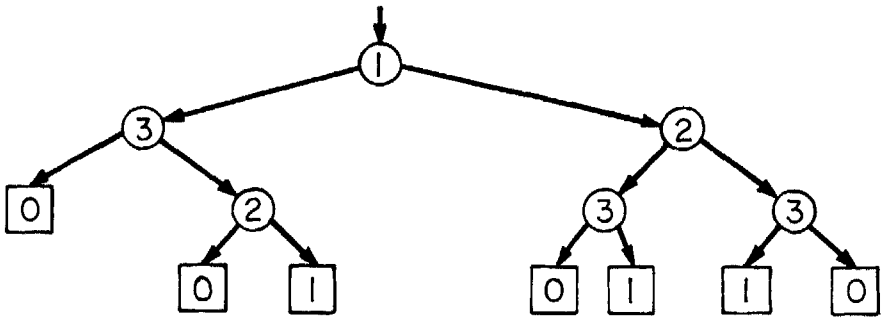

Fig. 1.

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 $c(T, x)$ denote the number of tests made using T to compute $P(x)$. 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 length of the path from the root).

Let $c(T)$ denote the maximum value of $c(T, x)$ for any $x \in \{0, 1\}^d$, 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*. (The term "evasive" is used in [1, 8, 9].) 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 might work as well. Requiring P to be a graph property means only that $\Gamma(P)$ must have a "nice" structure.

Considering P, an arbitrary $\{0, 1\}^d \to \{0, 1\}$ 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 for 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 $k_0 =$

$\max(\text{depth}(L)) < d$ then 2^{d-k_0} must divide $|\{x \in \{0,1\}^d \mid x \text{ arrives at } L\}|$, for any L. From this simple observation, it follows that:

Lemma 3.1. *If* $|\{x \mid P(x)=1\}|$ *is odd, then* P *must be exhaustive.*

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

In order to strengthen this result define the *weight enumerator* $P^1(z)$ of P by

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

where $w_i(P) = |\{x \mid (P(x)=1) \wedge (w(x)=i)\}|$, so that the coefficient of z^i is the number of vectors x of weight i such that $P(x)=1$. The contribution to $P^1(z)$ 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 bits examined on the path to L were ones.

Theorem 3.2. *If* $C(P) \leq k$, *then* $(1+z)^{d-k}$ *divides* $P^1(z)$.

Proof. In an 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 3.2 yields Lemma 3.1, since $P^1(1) = |\{x \in \{0,1\}^d \mid P(x)=1\}|$.

Theorem 3.2 also implies the following corollary, since $C(P) \leq d-1$ implies that $P^1(-1)=0$.

Corollary 3.3. *If* $C(P) \leq d-1$, *then the numbers of even- and odd-weight vectors for which* P *equals* 1, *are equal*:

$$|\{x \mid P(x)=1 \wedge w(x) \text{ odd}\}| = |\{x \mid P(x)=1 \wedge w(x) \text{ even}\}|.$$

Corollary 3.4. *As* $d \to \infty$, *almost all functions* $P: \{0,1\}^d \to \{0,1\}$ *are exhaustive.*

Proof. The number of functions $P: \{0,1\}^d \to \{0,1\}$ such that $|\{x \mid P(x)=1 \wedge w(x) \text{ odd}\}| = k = |\{x \mid P(x)=1 \wedge w(x) \text{ even}\}|$ is $\binom{n}{k}^2$ where $n = 2^{d-1}$; thus

$$\text{Prob}(P \text{ non-exhaustive}) \leq \frac{1}{2^{2n}} \cdot \sum_{0 \leq k \leq n} \binom{n}{k}^2 = \frac{1}{2^{2n}} \cdot \binom{2n}{n} \approx \frac{1}{\sqrt{n}}$$

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 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 to ensure that P is exhaustive? What can be said about functions P such that $\Gamma(P)$ is transitive?

Lemma 4.1. *If $\Gamma(P)$ is transitive, then*

$$w(\boldsymbol{x}) \cdot |\boldsymbol{x}\Gamma(P)| = d \cdot b(\boldsymbol{x})$$

where

$$b(\boldsymbol{x}) = |\{\boldsymbol{y} \in \boldsymbol{x}\Gamma(P) \mid y_1 = 1\}|, \quad \textit{for any } \boldsymbol{x} \in \{0,1\}^d. \tag{1}$$

Proof. Let M denote the $|\boldsymbol{x}\Gamma(P)|$ by d matrix whose rows are the vectors in $\boldsymbol{x}\Gamma(P)$. The left side of (1) counts the number of ones in M by rows, the right side by columns. By transitivity each column contains $b(\boldsymbol{x})$ 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 4.2. *If $d = p^\alpha$ for some prime p and positive integer α, $\Gamma(P)$ is transitive, and $\boldsymbol{x} \in \{0,1\}^d$, then p divides $|\boldsymbol{x}\Gamma(P)|$ unless $\boldsymbol{x} = \mathbf{0}$ or $\boldsymbol{x} = \mathbf{1}$ in which case $|\boldsymbol{x}\Gamma(P)| = 1$.*

Proof. Clearly $|\mathbf{0}\Gamma(P)| = |\mathbf{1}\Gamma(P)| = 1$; otherwise, the result follows from Lemma 4.1 since p^α does not divide $w(\boldsymbol{x})$ unless $\boldsymbol{x} = \mathbf{0}$ or $\boldsymbol{x} = \mathbf{1}$. □

Theorem 4.3. *Any transitive boolean function $P: \{0,1\}^d \to \{0,1\}$ such that d is a prime power $d = p^\alpha$ and $P(\mathbf{0}) \neq P(\mathbf{1})$ is exhaustive.*

Proof. Consider evaluating $P^1(-1) \pmod p$ where we calculate the number of vectors $\boldsymbol{x}$ of even and odd weight for which $P(\boldsymbol{x}) = 1$ on an orbit by orbit basis. From Corollary 4.2 the only orbits of interest are $\mathbf{0}\Gamma(P)$ and $\mathbf{1}\Gamma(P)$. Thus $P^1(-1) \equiv P(\mathbf{0}) + (-1)^d P(\mathbf{1}) \pmod p$; from $P(\mathbf{0}) \neq P(\mathbf{1})$ we obtain $P^1(-1) \equiv \pm 1 \pmod p$. In either case, $P^1(-1) \neq 0$ and the result follows by Theorem 3.2. □

We return to the Aanderaa–Rosenberg conjecture and apply the preceding theorem 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 $2 \leq v \leq 4$ by hand; we have also shown this to be true for $v = 5, 7, 11$, and 13. For the latter cases the following lemma simplifies the calculation considerably.

Lemma 4.4. *If v is prime, then $|x\Gamma(P)| \equiv 0 \pmod{v}$ unless x represents a graph with cyclic symmetry (that is, invariant under a cyclic permutation of the vertices).*

Proof. Observe that $|x\Gamma(P)| = (v!)/|\mathrm{Aut}(x)|$, where

$$\mathrm{Aut}(x) = \{\sigma \in \Sigma_v^{(2)} \mid x = \sigma x\}$$

is the automorphism group of x. By Sylow's theorem (see [2]), if v divides $|\mathrm{Aut}(x)|$ and v is prime, then $\mathrm{Aut}(x)$ contains an element of order v. But the order of an element of $\Sigma_v^{(2)}$ is the lcm of the sizes of the various orbits that it divides the vertices into, so an element of $\Sigma_v^{(2)}$ has order v only if it is a cyclic permuation of the vertices, i.e., it acts transitively on the vertices. □

When v is prime, the fact that $|x\Gamma(P)| \equiv 0 \pmod{v}$ unless x represents a graph with cyclic symmetry implies the following lemma.

Lemma 4.5. *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 $P^1(-1) \pmod{v}$; this is the same as calculating $-(\sim P^1)(-1) \pmod{v}$ since $P^1(z) + (\sim P)^1(z) = (1+z)^d$ where $d = \binom{v}{2}$. If a nonempty graph with a prime number of vertices v has cyclic symmetry, it must contain H_v as a subgraph. Therefore $(\sim P)^1(-1) \equiv 1 \pmod{v}$, since E_v is the only orbit with size not divisible by v that is not counted in $P^1(-1)$; the result then follows again from Theorem 3.2. □

The preceding discussion gives some cases for which $C(P) = \binom{v}{2}$. To prove for all nontrivial monotone graph properties P 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. First we treat the case that v is a power of two.

Theorem 4.6. *If $v = 2^n$ and P is a monotone nontrivial graph property on v-vertex graphs, then $C(P) \geq v^2/4$,*

Proof. For any graphs G, G_1 and G_2 let $m \cdot G$ denote m disjoint copies of G; let $G_1 + G_2$ denote the graph consisting of a copy of G copy of G_2; 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. Let $S_i = 2^{n-i} \cdot K_{2^i}$ represent the graph formed by 2^{n-i} distinct copies of the complete graph on 2^i vertices, so that $S_0 = E_v$, $S_n = K_v$ and S_i is a subgraph of S_{i+1}, denoted $S_i \leqslant S_{i+1}$, for $0 \leqslant i \leqslant n$; finally let $J_i = 2^{n-i-1} \cdot K_{2^i}$ so that $S_i = J_i + J_i$. Since property P is nontrivial and montone, there exists a j such that $P(S_j) = 0$ and $P(S_{j+1}) = 1$. Since $S_j = J_j + J_j$ and $S_{j+1} \leqslant J_j \times J_j$, it follows that $P(J_j + J_j) = 0$ and $P(J_j \times J_j) = 1$.

To show that $C(P) \geqslant v^2/4$ 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 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 4.3 to P as a function of E' (call this function P').

To show that P' must be invariant under a transitive permutation group acting on E', we note that J_j is point-symmetric, i.e., its automorphism group acts transitively on its vertices. 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 4.3 to finish the proof. □

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 4.7. $C(v) \geqslant \min(C(v-1), 2^{2k-2})$, *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 $C(v) \geqslant C(v-1)$ 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.

In case (iii), let $u = 2^{k-1}$ and $r = v - 2u$. As in Theoorem 4.6, we construct from P a property P' satisfying the conditions of Theorem 4.3. First, we restrict attention to graphs G such that $K_u \times K_r + E_u \leq G \leq K_u \times (K_r + E_u)$ and define P' as P restricted to those edges between K_u and E_u for each graphs. Since P' is invariant under independent arbitrary relabelling of vertices within either K_u or E_u, it is left invariant by a transitive permutation group. Since property P is monotone, so is P'; from the conditions

(1) $P(K_1 + K_{v-1}) = 0$ and $K_u \times K_r + E_u \leq K_1 + K_{v-1}$;
(2) $P(K_1 \times E_{v-1}) = 1$ and $K_1 \times E_{v-1} \leq K_u \times (K_r + E_u)$,

it follows by monotonicity of P that P' is nontrivial. Thus all $u^2 = 2^{2k-2}$ edges between K_u and E_u must be examined in the worst case, proving Lemma 4.7. □

From Theorem 4.6 and Lemma 4.7 follows:

Theorem 4.8. *If P is a nontrivial monotone graph property of v-vertex graphs, then $C(P) \geq v^2/16$.*

Kleitman and Smith (alias Kwiatowski) ([8, 9]) have tightened this bound to $C(P) \geq v^2/9$ by showing $C(P) \geq v^2/3$ for v of the form $3 \cdot 2^n$ and improving on Lemma 4.7.

5. The generalized Aanderaa–Rosenberg conjecture

Theorem 4.8 of the preceding section is the main result of this paper. In this section we consider ways in which that result might be strengthened. In particular, we present a generalized version of the Aanderaa–Rosenberg conjecture and consider several approaches towards proving it, together with some examples demonstrating the limitations of the methods of the previous section. We also include an observation by Lovasz to the effect that our generalized conjecture would imply a special case of a well-known open conjecture in graph theory, suggesting the difficulty of this question.

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 transitive and $P(\mathbf{0}) \neq P(\mathbf{1})$ then P is exhaustive.

The generalized conjecture clearly implies the orignal Aanderaa–Rosenberg conjecture, since $P(\mathbf{0}) \neq P(\mathbf{1})$ if P is a nontrivial monotone function. Theorem 4.3

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 4.3, 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 $P(x)=(\exists y \in S)(x \geqslant y)$ 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 $(1^40^2)^2$. The corresponding weight enumerator is

$$P^1(z)=9z^8+52z^9+54z^{10}+12z^{11}+z^{12}.$$

For graphs a similar situation occurs if $P(G)$ is the function: G is not a subgraph of any of the graphs shown in Fig. 2 for 6-vertex graphs. The corresponding weight enumerator is

$$P^1(z)=(1+z)^{15}-15z^7-745z^6-1731z^5-1365z^4-455z^3-105z^2-15z-1.$$

Fig. 2.

Both of these functions are monotonic. Using arguments based upon an application of Lemma 3.1 to the various functions induced from p by fixing some of its arguments, they can, however, be shown to be exhaustive; we know of no counter-examples to the generalized conjecture.

While there are functions which are exhaustive and yet have $(1+z)\,|\,P^1(z)$ (that is, with $P^1(-1)=0$), one might hope that they all satisfy $(1+z)^2 \nmid P^1(z)$. This would be relevant due to the following theorem, although we shall see that this approach is also limited.

Theorem 4.9. *If P is transitive and non-exhaustive, then* $(1+z)^2\,|\,P^1(z)$.

Proof. Let $Q(x)$ be the Möbius inverse of $P(x)$, so that $P(x)=\sum_{0\leqslant y\leqslant x}Q(y)$, implying that $Q(x)=\sum_{0\leqslant y\leqslant x}P(x)(-1)^{w(x\oplus y)}$ by Möbius inversion, where $x\oplus y$ is component-wise "exclusive-or". Since P is not exhaustive, by Theorem 3.2 $Q(\mathbf{1})=P^1(-1)=0$. By the transitivity of $\Gamma(P)$, each of the restricted functions $P_i(x)=P(x\,|\,x_i=0)$ for $1\leqslant i\leqslant d$ 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

$$P^1(z) = \sum_{0 \leq x \leq 1} P(x) \cdot z^{w(x)}$$

$$= \sum_{0 \leq x \leq 1} \sum_{0 \leq y \leq x} Q(y) z^{w(x)}$$

$$= \sum_{0 \leq y \leq 1} Q(y) z^{w(y)} (1+z)^{d-w(y)},$$

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

Unfortunately, there exist many exhaustive functions P with $\Gamma(P)$ transitive such that $(1+z)^2 \mid P^1(z)$. The previously mentioned property of 6-vertex graphs is an example. Thus Theorem 4.9 cannot be used directly to give a proof of the generalized conjecture.

Although Theorem 3.2 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 being transitive.

Theorem 4.10. *Let E denote the smallest set of natural numbers such that $(1 \in E)$ and $(n \in E) \wedge (q \text{ prime}) \wedge (q > 2^{n-1}) \Rightarrow nq^k \in E$ for all natural numbers k. If $P : \{0,1\}^d \to \{0,1\}$ is such that $P(\mathbf{0}) \neq P(\mathbf{1})$, $\Gamma(P)$ is transitive and abelian, and $d \in E$, then P is exhaustive.*

Proof. Let $d = nq^k$, where q is prime, $n \in E$, and $q \geq 2^{n-1}$. Since $\Gamma(P)$ is transitive and abelian, it must also be regular (that is, have order d) [3]. Therefore, for each i, j in $\{1, \ldots, d\}$ there is exactly one permutation $\sigma \in \Gamma(P)$ such that $\sigma(i) = j$. Now $\Gamma(P)$ contains a Sylow subgroup θ of order q^k, and since $\Gamma(P)$ is abelian, θ is normal in $\Gamma(P)$ and θ is the only subgroup of order q^k in $\Gamma(P)$. The action of θ on $\{1, \ldots, d\}$ divides $\{1, \ldots, d\}$ into n blocks of size q^k; i and j are in the same block (denoted $i \sim j$) if $(\exists \sigma \in \theta)(\sigma(i) = j)$.

We calculate $P^1(-1) \pmod q$ on an orbit by orbit basis. Note that $|\boldsymbol{x}\Gamma(P)| = |\Gamma(P)|/|\mathrm{Aut}(\boldsymbol{x})|$, where $\mathrm{Aut}(\boldsymbol{x})$ is the subgroup of $\Gamma(P)$ that fixes $\boldsymbol{x} \in \{0,1\}^d$. If $|\boldsymbol{x}\Gamma(P)| \not\equiv 0 \pmod q$, then $\theta \leq \mathrm{Aut}(\boldsymbol{x})$ follows by Sylow's theorem, since θ is the only subgroup of size q^k in $\Gamma(P)$. Furthermore, if $\theta \leq \mathrm{Aut}(\boldsymbol{x})$, then $(\forall i, j)(i \sim j) \Rightarrow (x_i = x_j)$.

The group $\Gamma(P)/\theta$ is abelian. Its action is to permute the blocks of $\{1, \ldots, d\}$, since $\Gamma(P)$ is the direct product of θ and $\Gamma(P)/\theta$. Clearly $\Gamma(P)/\theta$ must be a transitive group acting on the set of blocks, since $\Gamma(P)$ is transitive. We can create an induced function $Q : \{0,1\}^n \to \{0,1\}$ such that $\Gamma(Q) = \Gamma(P)/\theta$ and $Q(y_1, y_2, \ldots, y_n) = P(x_1, x_2, \ldots, x_d)$ where all of the variables x_j in the i^{th} block are set equal to y_i. Therefore Q satisfies the conditions of the theorem.

To prove P is exhaustive, our inductive assumption will be that $(n \in E) \wedge (q \text{ prime}) \wedge (q \geq 2^{n-1}) \wedge (P : \{0,1\}^{nq^k} \to \{0,1\}) \wedge (\Gamma(P) \text{ transitive and abelian}) \Rightarrow P^1(-1) \neq 0$. By our above remarks $P^1(-1) \equiv Q^1(-1) (\text{mod } q)$. Furthermore, $|Q^1(-1)| \leq 2^{n-1}$, so that $P_1(-1) \neq 0$ follows from $q > 2^{n-1}$. The base case ($n = 1$) follows from Theorem 4.3.

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

The same argument can be used for obtaining the following results: in Theorem 4.10 we can replace "$P(\mathbf{0}) \neq P(\mathbf{1})$" by "$P$ monotone non-trivial" and "E" by "E'", where, in the definition of E', we replace "2^{n-1}" by

$$\text{“}\binom{n-1}{\lfloor \frac{n-1}{2} \rfloor}\text{”};$$

Theorem 4.10 can also be used to settle the Generalized Conjecture when $|\Gamma(P)| = 2 \cdot p^\alpha$ with p prime.

The Generalized Aanderaa–Rosenberg Conjecture seems quite difficult to prove. Lovasz has pointed out to the authors that the generalized conjecture would imply a special case of an open conjecture in graph theory, given in [12].

In a graph $G = (V, E)$ a *clique* is a set of mutually adjacent vertices; a clique C is maximal if, for any vertex $v \notin C$ there exists a vertex in C which is not adjacent to v. A graph is regular if every vertex has the same degree.

Conjecture. If a finite regular graph G is not the complete graph, then for every clique A there exists a maximal clique B which is disjoint from A.

A special case of this conjecture obtains if G is point-symmetric, (and therefore regular); this case is also unsettled.

Lovasz showed that if the special case of the above conjecture is false then so is our generalized conjecture. Let $G_0(V_0, E_0)$ be a point-symmetric graph not equal to $K_{|V_0|}$ containing a clique A_0 which intersects every maximal clique B in G_0. Associate a variable x_i with each vertex v_i in G_0. Define the function f as follows:

$$f(x_1, \ldots, x_{|V_0|}) = 1 \quad \text{iff } \{v_i \mid x_i = 1\} \text{ is a clique.}$$

Clearly f is transitive since G_0 is point-symmetric. Also, f is anti-monotone, and nontrivial since G_0 is not the complete graph. It is never necessary to examine all of the x_i's to compute f. Let C denote the set of vertices $\{v_i \mid x_i = 1\}$. One may examine all the variables corresponding to vertices in $V_0 - A_0$; if we find two nonadjacent vertices in $C \cap (V_0 - A_0)$ then $f(\boldsymbol{x}) = 0$. Otherwise $C \cap (V_0 - A_0)$ is contained in a maximal clique C' which intersects A_0. We next determine

$C \cap (A_0 - C')$; if every vertex in this set is adjacent to every vertex in $C \cap (V_0 - A_0)$, then C must form a clique. The variables corresponding to $A_0 \cap C'$ need not be examined, since any vertices in $C \cap A_0 \cap C'$ must be adjacent to each other and all previously found vertices in C. Since $|A_0 \cap C'| > 0$, f is not exhaustive.

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 $P(\mathbf{0}) \neq P(\mathbf{1})$ 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.

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 4.1 to us), Dan Kleitman, and Marc Schutzenberger.

References

[1] 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).
[2] B. Bollobas, Complete subgraphs are elusive, *J. Combinatorial Theory* **21** (1976) 1–7.
[3] R.D. Carmichael, *Groups of Finite Order* (Dover Publications, NY, 1937).
[4] F. Harary, *Graph Theory* (Addison-Wesley, Reading MA, 1969).
[5] R.C. Holt and E.M. Reingold, On the time required to detect cycles and connectivity in graphs, *Math. Systems Theory* **6** (1972) 103–106.
[6] J. Hopcroft and R. Tarjan, Efficient planarity testing, Cornell University Computer Science Tech. Report TR73–165 (1973).
[7] D. Kirkpatrick, Determining Graph Properties from Matrix Representations, *Proc. 6th SIGACT Conf.*, Seattle (1974) 84–90.
[8] D.J. Kleitman, and D.J. Smith, Further results on the Aanderaa–Rosenberg conjecture, available from authors, Dept. of Mathematics, M.I.T.
[9] D.J. Kwiatkowski, On evasiveness, permutation embeddings, and mapping on sequences, Ph.D. Thesis, Dept. of Mathematics, M.I.T. (May 1975).
[10] R.J. Lipton and L. Snyder, On the Aanderaa–Rosenberg conjecture, *SIGACT News* **6** (1974).

[11] 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). To appear in: J.A. Nash-Williams and J. Sheehan eds., *Proc. Fifth British Conf. on Combinatorics*, Utilitas.
[12] C. Payan, Sur une classe de problèmes de couverture, *C.R. Acad. Sci.* **278** (1974) 233–235.
[13] 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).
[14] R.L. Rivest and J. Vuillemin, On the time required to recognize properties of graphs from their adjacency matrices, U.C. Berkeley Electronics Research Laboratory Memorandum ERL–M476 (Nov. 1974).
[15] A.L. Rosenberg, On the time required to recognize properties of graphs: A problem, *SIGACT News* **5** (1973) 15–16.
[16] R.E. Tarjan, Depth-first search and linear graph algorithms, *SIAM J. Comput.* **1** (2) (1972) 146–159.