ON THE NUMBER OF ARGUMENT EVALUATIONS REQUIRED TO COMPUTE BOOLEAN FUNCTIONS[†]

Ronald L. Rivest
Project M.A.C., Massachusetts Institute of Technology
Cambridge, Massachusetts 02139

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

Abstract:

We consider the number of argument evaluations required to compute a Boolean function which is left invariant by a permutation group of its arguments. A non-constructive (that is, not based on oracle construction) proof method is used to derive that, for many particular functions, every argument must be examined. Evidence is presented for the general conjecture that every argument of $P\colon \{0,1\}^d \to \{0,1\}$ must be examined whenever $P(0^d) \neq P(1^d)$ and the group fixing P acts transitively on $\{1,2,\ldots,d\}$.

I. INTRODUCTION

Trying to relate the computational complexity of a problem to the choice of a particular representation, or data structure, is a natural and important question.

For example, Holt and Reingold [4] have shown that any algorithm deciding whether a v-vertex graph contains a directed cycle from its adjacency matrix representation requires at least

[†] This work was supported by IRIA-LABORIA, 78150, Rocquencourt, France, and by NSF grant GJ-43227X.

$\frac{1}{4}(v + 1)(v - 1)$ inspections of the adjacency matrix in the worst case. Similarly, Hopcroft and Tarjan [5] mention that testing a graph for planarity from its adjacency matrix requires of the order of v^2 operations; this should be contrasted with the linear $O(v)$ algorithm of Tarjan [11], which uses an adjacency list representation of graphs.

Motivated by these results, Arnold Rosenberg conjectured that determining from its adjacency matrix if a v-vertex graph has any particular non-trivial, property requires $\Omega(v^2)$[†] operations.

Aanderaa destroys this conjecture with a clever counterexample: he shows that deciding if a directed v-vertex graph $H = (V,E)$ contains a "sink" requires less than $3v$ probes of the adjacency matrix. A "sink" is a vertex $t \in V$ such that for all vertices $u \in V$, $u \neq t$, there is an edge $(u,t) \in E$ but no edge $(t,u) \in E$. To revive the conjecture, Aanderaa suggests that graph properties should be constrained to be "monotonic", that is, if the property is true of a graph $H = (V,E)$, it must also be true of any graph $H' = (V,E')$ such that $E \subseteq E'$. This eliminates the "sink" counterexample, and in fact, there is no known counterexample to:

Aanderaa-Rosenberg conjecture [10]: Any algorithm for determining from the adjacency matrix of a v-vertex directed graph H having no self-loops whether H has a property which is

(i) non constant,

(ii) monotonic, and

[†] In this paper, we understand the Ω notation as the inverse of the $\mathcal{O}$ notation: $f(v) = \Omega(v^2)$ iff $v^2 = \mathcal{O}(f(v))$, (this is not the standard usage of the notation).

(iii) invariant under renaming of the nodes,

must in the worst case examine all $v(v - 1)$ non-diagonal entries of the adjacency matrix.

Of course, one can replace "directed" by "undirected" and $v(v - 1)$ by $\frac{1}{2}v(v - 1)$ in the statement of the conjecture. In [1], [4], [6], [7] and [8], many properties satisfying (i), (ii) and (iii) are shown to require $\Omega(v^2)$ computational steps, thus providing more evidence towards the conjecture. The only general attempt at solving the problem is reported by Kirkpatrick [6] who establishes $\Omega(v \log v)$ bound.

Except for Best, Van Emde Boas and Lemstra [1] who independently discovered the proof technique we are about to describe, it is worth noting that all the previous results mentioned are obtained by oracle construction techniques.

In this work we present a generalization of the Aanderaa-Rosenberg conjecture and a non-constructive (no oracle construction) proof technique for attacking this type of problem. Although the generalized conjecture is not proved in its full generality, our method yields proofs for many special cases which we feel are of sufficient interest to deserve this exposition. In particular, the authors show in [9] that, as a corollary of Theorem 2 in this report, Kirkpatrick's $\Omega(v \log v)$ bound can be improved to $\Omega(v^2)$, thus settling the question raised by Rosenberg in [10].

II. BASIC DEFINITIONS

In this section we define the concepts and notations necessary for stating the conjecture and presenting the proof technique.

Let $P(x_1,\ldots,x_d)$ be a Boolean function mapping $\{0,1\}^d$ (the set of all d-tuples over $\{0,1\}$) onto $\{0,1\}$, which we denote $P\colon \{0,1\}^d \mapsto \{0,1\}$. Property P is non-constant since the mapping is onto $\{0,1\}$. As usual, we say the $P(\bar{x})$ is "true" for some $\bar{x} \in \{0,1\}^d$ whenever $P(\bar{x}) = 1$.

For any two elements $\bar{x} = (x_1,\ldots,x_d)$ and $\bar{y} = (y_1,\ldots,y_d)$ of $\{0,1\}^d$, we define $\bar{x} \leq \bar{y}$ to mean $x_i \leq y_i$ for $i \in [1,d]$. It follows that $\bar{0} \leq \bar{x} \leq \bar{1}$ for all $\bar{x} \in \{0,1\}^d$. Property P is monotone if $\bar{x} \leq \bar{y}$ implies $P(\bar{x}) \leq P(\bar{y})$ for all $\bar{x},\bar{y} \in \{0,1\}^d$. We denote the vector of d ones (resp. d zeros) by $\bar{1}$ (resp. $\bar{0}$) throughout. The weight $w(\bar{x})$ of a vector $\bar{x} \in \{0,1\}^d$ is the number of ones it contains.

We denote by G_p the (maximal) group of permutations of the argument positions leaving P invariant. By definition:

$$(1)\quad G_p = \{\sigma \in S_d \mid \forall\bar{x} \in \{0,1\}^d\colon\ f(x_1,\ldots,x_d) = f(x_{\sigma(1)},\ldots,x_{\sigma(d)})\},$$

where S_d is the symmetric group on $\{1,2,\ldots,d\}$ (the set of all permutations of d elements). We say that "G fixes P" or rather that "P is invariant under G", for any subgroup $G \leq G_p$.

As an example of the above notation, the adjacency matrix for an undirected graph $H = (V,E)$ with $v = |V|$ vertices is a symmetric $v \times v$ matrix of 0's and 1's whose (i,j) entry is 1 iff $\{i,j\}$ is an edge of H. If H has no self-loop, it can also be described as a vector of $d = \binom{v}{2}$ bits. We say that a property P is "invariant under graph isomorphism", or simply "P is a graph property" if, for all graphs H having v vertices and all permutations $\sigma \in S_v$:

$$(2)\quad P(H) = P(\sigma H),$$

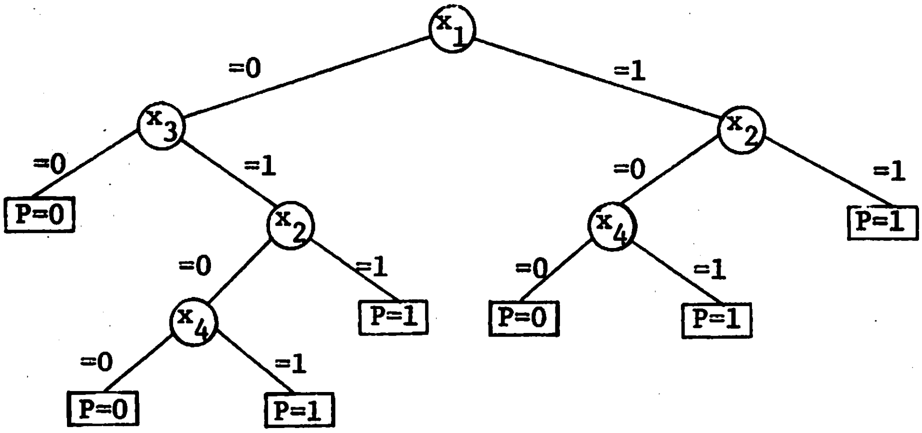
where σH denotes the graph (V,E') such that $\{i,j\} \varepsilon E \Leftrightarrow \{\sigma(i), \sigma(j)\} \varepsilon E'$. If we denote by I_v this permutation group of the edges, saying "P is a graph property" is equivalent to $I_v \leq G_p$. Since we exclude self-loops, I_v is transitive. A permutation group G acting on $X = \{1,2,\ldots,n\}$ is transitive, or equivalently, G acts transitively on X, if for all $i,j \varepsilon X$, there exists $\sigma \varepsilon G$ such that $\sigma(i) = j$.

An algorithm for evaluating $P(x_1,\ldots,x_d)$, henceforth called a P-algorithm, must examine some of the individual arguments x_i, since P is non constant. A P-algorithm can be represented as a binary decision-tree T, whose internal nodes specify arguments to be tested, and whose external nodes are marked true (1) or false (0) according to the appropriate value for P.

As an example, consider the property

(3) $P_3(x_1,x_2,x_3,x_4) \equiv x_1x_2 \vee x_2x_3 \vee x_3x_4 \vee x_4x_1$

and a particular P_3-algorithm:



,

Figure 1.

which in order to simplify notations, is described just as well by:

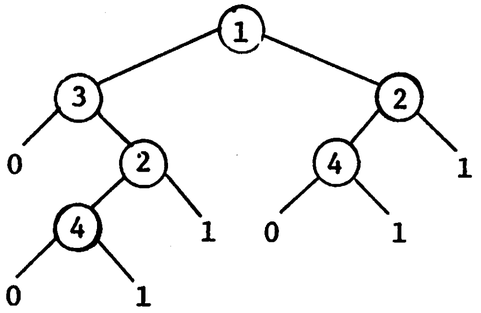


Figure 2.

Here G_{P_3} is the dihedral group D_4 generated by (1234) and (14)(23). We write $G_{P_3} = D_4 = <(1234),(14)(23)>$. To evaluate P_3 for a given input $\bar{x}$ using the P_3-algorithm of Figure 1, we first test the argument x_1 (specified at the root of the tree); depending on whether $x_1 = 0$ or $x_1 = 1$, we proceed to the root of the left or right subtree respectively, continuing in this fashion until we reach the leaf specifying the value $P(\bar{x})$ of P for $\bar{x}$.

In general, we denote by $c(T,\bar{x})$ the number of tests made in determining $P(\bar{x})$ by the P-algorithm T. The maximum number of tests made, $\max_{\bar{x}\varepsilon\{0,1\}^d}\{c(T,\bar{x})\}$, or equivalently the maximum depth of any leaf the tree representation of T, will be our measure of the cost of the P-algorithm T. We define the argument complexity C(P) of P as the cost of the cheapest P-algorithm. In symbols,

$$(4) \quad C(P) \underset{\text{def}}{=} \min_{\substack{T \text{ is a} \\ P\text{-algorithm}}} \max_{\bar{x}\varepsilon\{0,1\}^d} \{c(T,\bar{x})\}.$$

Using example (3) again, we have $c(T,0011) = 4$ for the P_3-algorithm T pictured in Figure 1; the reader can convince himself that in fact $C(P_3) = 4 = d$, so no P_3-algorithm can do better in the worst case.

Let us point out that in this example, $G_{P_3} = D_4$ acts transitively on $\{1,2,3,4\}$.

If we now consider

(5) $P_5(x_1,x_2,x_3,x_4) \equiv x_1x_2 \vee x_2x_3 \vee x_3x_4$,

the following P_5-algorithm

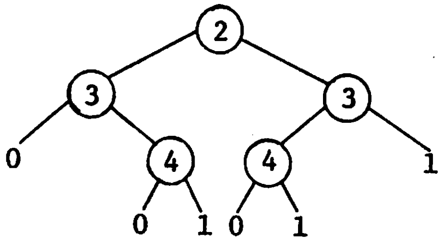


Figure 3.

suffices to show that $C(P_5) \leq 3 < d = 4$. Note that, in this case, $G_{P_5} = <(14)(23)>$ is not transitive.

In general, a property P: $\{0,1\}^d \to \{0,1\}$ is said to be exhaustive if $C(P) = d$, i.e., any P-algorithm must, in the worst case, examine every argument.

Often, a property P will be described in a fashion independent of the size of the input d. For example, the property "is connected" applies to a graph of any size. In this case, we have an overall function P: $\{0,1\}^* \to \{0,1\}$ which may be broken down into an infinite collection of finite functions P_d: $\{0,1\}^d \to \{0,1\}$ for each $d \in N$. If each P_d is exhaustive, we say that P is exhaustive.

Using this vocabulary, we can re formulate the Aanderaa-Rosenberg question as: Is every monotone graph property exhaustive? It is then tempting to ask the more general question: Can one characterize the class of exhaustive properties? As a possible partial answer to this last question, we suggest the following:

Generalized Conjecture: *If property* $P: \{0,1\}^d \to \{0,1\}$ *such that* $P(\bar{0}) \neq P(\bar{1})$ *has a transitive invariance group* G_P *then* P *is exhaustive.*

Note that the requirement $P(\bar{0}) \neq P(\bar{1})$ is weaker than and is implied by monotonicity. Although monotonicity seems to help with some of the proofs, we do not feel that it is an intrinsic requirement of the problem. Needless to say, we know of no non-exhaustive property P (graph property or otherwise) satisfying $P(\bar{0}) \neq P(\bar{1})$ and G_P transitive.

Since $I_v \leq G_P$, if P is a graph property, so that G_P is transitive, this conjecture implies the Aanderaa-Rosenberg conjecture. If one considers a property P_d defined for an infinite sequence of values for d, it is possible to formulate a weaker conjecture which says that $\Omega(d)$ tests are required, as $d \to \infty$. It is proved by the authors in [9] that this is the case for monotone non constant graph properties; the question for arbitrary transitive groups is still unsettled.

III. THE METHOD

As mentioned earlier, our approach is not based upon the explicit construction of oracles, but on a partial characterization of the class of non-exhaustive properties.

Consider an arbitrary decision tree T for a property P, for example the tree T of Figure 1 for P_3 of (3). Without invalidating the fact that T is a P-algorithm, we may extend it into a complete decision tree T', in which all paths have length d. For this, we add new useless but not redundant tests, replacing every leaf of T at depth $d' < d$ by a complete subtree of depth $d - d'$ which computes the constant function which is the value of P for every input which has a corresponding leaf in the subtree. In T', there is a leaf for each of the 2^d possible inputs and each path of T' tests each variable in $\{x_1, x_2, \ldots, x_d\}$ exactly once.

A possible complete tree T' associated with the T of figure 1 is:

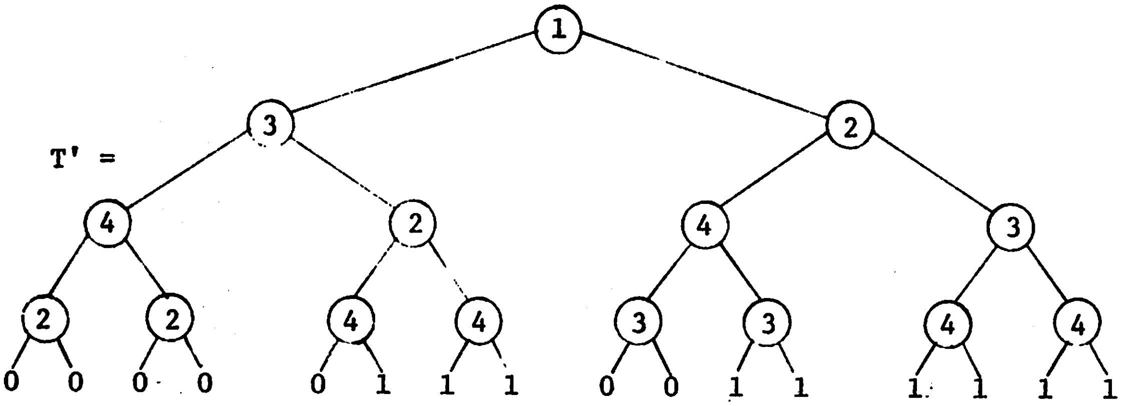


Figure 4.

Conversely, any decision tree for P can be constructed by starting with a complete decision tree T' for P and "pruning off" subtrees which calculate constant functions. The dotted lines of Figure 4 suggest the appropriate pruning operations to turn it into Figure 2.

The following is the essential observation to our method:

Proposition 1: *If $C(P) \leq d - k$ for some $P: \{0,1\}^d \to \{0,1\}$ and $0 \leq k < d$, then there exists a complete decision tree T' for P in which all subtrees of height k, (having 2^k leaves) compute constant functions.*

In order to phrase this observation differently, let $B_d = <\{0,1\}^d, \leq>$ denote the boolean lattice over $\{0,1\}^d$ induced by the relation "$\leq$" defined in §1. Note that the set of inputs corresponding to the leaves of any subtree of height k of a complete decision tree is isomorphic to B_k, since $d-k$ tests have already been made so that only k arguments remain free to vary.

Let $P^o = \{\bar{x} \in \{0,1\}^d | P(\bar{x}) = 0\}$ and $P^1 = \{\bar{x} \in \{0,1\}^d | P(\bar{x}) = 1\}$. Proposition 1 then implies the following:

<u>*Proposition 2*</u>: *If $C(P) \leq d-k$ for some $P: \{0,1\}^d \to \{0,1\}$ and $0 \leq k < d$, then both P^o and P^1 are packable with isomorphic copies of B_k.*

We say a graph G is packable with isomorphic copies of a graph H if the vertices of G can be partitioned into disjoint blocks $\{\pi_i\}$ such that the subgraph of G induced by each π_i is isomorphic to H. The graphs of P^o and P^1 have the specified vectors in $\{0,1\}^d$ as vertices and an edge $(\bar{x},\bar{y})$ whenver $\bar{x}$ and $\bar{y}$ differ in exactly one component. That is, we consider the graph of the covering relation of "$\leq$" in P^o and P^1.

As a simple consequence, we have:

<u>*Corollary 1:*</u> *If $|P^1|$ is odd, then P is exhaustive.*

The function P_3 defined by (3) has $|P_3^1| = 9$ (see Figure 4). It follows from the corollary that P_3 is exhaustive, i.e., $C(P_3) = 4$ as announced earlier.

Not all exhaustive properties P have $|P^1|$ odd however; consider $P \equiv (x_1+x_2+x_3 \geq 2)$ for example. We need a somewhat stronger consequence of Proposition 2. If we consider the case $k = 1$, we see that P^1 must be packable with copies of B_1, in order for P to be non-exhaustive. This means that the graph of the covering relation of "$\leq$" in $B_d \cap P^1$ must contain a perfect matching. Since any $\bar{x} \in B_d$ of even weight $w(\bar{x})$ is adjacent to odd weight $\bar{y}$'s only and conversely, B_d is a bipartite graph. The same remark applies a fortiori to $B_d \cap P^1$. For example, if

(6) $P_6 \equiv (x_1 + x_2 + x_3 \geq 2)$,

then $B_3 \cap P^1_6$ is represented as

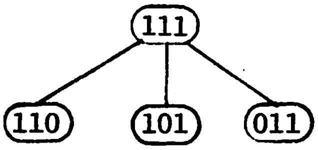


Figure 5.

Since this bipartite graph does not have a perfect matching, P_6 must be exhaustive.

More generally, the existence of perfect matchings in $P^1 \cap B_d$, (or, similarly in $P^o \cap B_d$) can be characterized by Philip Hall's famous SDR theorem. This turns out to be rather difficult to apply, and we opt for a simpler necessary condition for the existence of such a matching, namely that $|P^1_{odd}| = |P^1_{even}|$ where $P^1_{odd} = \{\bar{x} \varepsilon P^1 \mid w(\bar{x}) \text{ is odd}\}$ and $P^1_{even} = \{\bar{x} \varepsilon P^1 \mid w(\bar{x}) \text{ is even}\}$. We shall see that even this simple prerequisite yields non-trivial results.

To express this requirement more elegantly, we introduce the generating function $P^1(z)$ for the set P^1 defined by

(7) $$P^1(z) = \sum_{\bar{x}\varepsilon P'} z^{w(\bar{x})},$$

with $P^o(z)$ defined similarly. Thus the coefficient of z^i in $P^1(z)$ is $|\{\bar{x} \varepsilon P^1 \mid w(\bar{x}) = i\}|$, for $0 \leq i \leq d$, and, clearly, $P^o(z) + P^1(z) = (1 + z)^d$. Our necessary condition for the existence of a perfect matching can thus be expressed as follows:

Corollary 2: If $P^1(-1) \neq 0$, then P is exhaustive.

Proof: The value of $P^1(-1)$ is exactly $|P^1{}_{even}| - |P^1{}_{odd}|$. □

If we are interested in establishing the argument complexity of non-exhaustive functions as well, this result can be strengthened to:

Proposition 3: If $C(P) \leq d - k$ for some $P\colon \{0,1\}^d \to \{0,1\}$ and $0 \leq k < d$, then $(1 + z)^k$ divides $P^1(z)$.

The generating function for $T_k\colon \{0,1\}^k \to \{1\}$ the "ever true" property is $(1 + z)^k$, hence, by proposition 2, $(1 + z)^k \mid P^1(z)$ (and also $(1 + z)^k \mid P^o(z)$). □

Before attempting to use those results for solving special cases of the generalized conjecture, let us point out an interesting consequence of Proposition 2:

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

Proof: A straightforward counting argument yields

$$\mathrm{Prob}(|P^1_{odd}| = k) = \mathrm{Prob}(|P^1_{even}| = k) = \binom{2^{d-1}}{k} \cdot 2^{-2^{d-1}} .$$

Since P non-exhaustive implies $|P^1_{even}| = |P^1_{odd}|$, we have

$$\begin{aligned}\mathrm{Prob}(P \text{ non-exhaustive}) &\leq \mathrm{Prob}(|P^1_{odd}| = |P^1_{even}|)\\ &= \sum_{0 \leq k \leq 2^{d-1}} \binom{2^{d-1}}{k}^2 \cdot 2^{-2^d} = \binom{2^d}{2^{d-1}} \cdot 2^{-2^d} \cong (\pi \cdot 2^{d-1})^{-\frac{1}{2}} .\end{aligned}$$

We see that, indeed, $\mathrm{Prob}(P \text{ non-exhaustive}) \to 0$ as $d \to \infty$. □

Since almost all functions are exhaustive, it seems reasonable to try to characterize classes of exhaustive functions, such as those of our generalized conjecture.

IV. APPLICATION TO THE GENERALIZED CONJECTURE

We now concentrate on properties P for which G_p is transitive.

Let $G \leq G_p$ be a given group which acts transitively on $\{1,2,\ldots,d\}$. Define the action of G on $\{0,1\}^d$ by $\sigma\bar{x} = x_{\sigma(1)}x_{\sigma(2)}\cdots x_{\sigma(d)}$ for $\sigma \in G$ and $\bar{x} \in \{0,1\}$. The orbit $\bar{x}G$ of $\bar{x}$ under this action of G is

$$(8) \quad \bar{x}G = \{\bar{y} \in \{0,1\}^d \mid \exists\sigma \in G\colon\ \bar{y} = \sigma\bar{x}\}.$$

By the fundamental relation of the theory of permutation groups ([2]), we have

$$(9) \quad |G| = |\bar{x}G| \cdot |G_{\bar{x}}|,$$

where $G_{\bar{x}} = \{\sigma \in G \mid \sigma\bar{x} = \bar{x}\}$ is the stabilizer of $\bar{x}$ in G.

The number m of distinct orbits in the action of G on $\{0,1\}^d$ is given by Burnside's formula:

$$(10) \quad m = \frac{1}{|G|} \sum_{\sigma\in G} |\{\bar{x} \in \{0,1\}^d \mid \sigma\bar{x} = \bar{x}\}|.$$

Let $\bar{x}_1, \bar{x}_2,\ldots, \bar{x}_m$ be distinct representatives of each such orbit respectively. The generating function $P^1(z)$ for P^1 can then be computed as follows:

$$(11) \quad P^1(z) = \sum_{1\leq j\leq m} |\bar{x}_jG| \cdot P(\bar{x}_j) \cdot z^{w(\bar{x}_j)}.$$

For example, if $d = 4$ and $G = C_4$ is the cyclic group, the action of C_4 on B_4 can be pictured as:

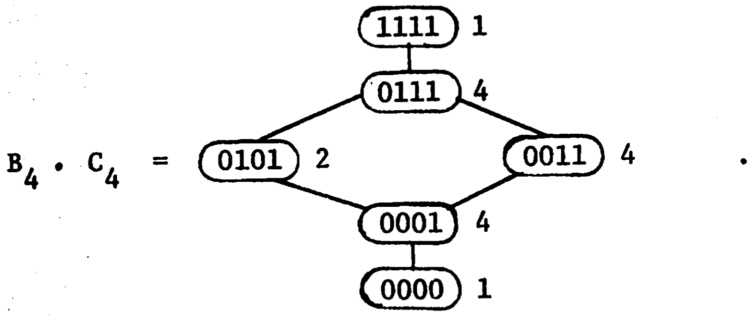


Figure 6.

Here, the number of orbits in the action of C_4 on $\{0,1\}^4$ is $m = 6$. Each property $P\colon \{0,1\}^4 \mapsto \{0,1\}$ such that $C_4 \leq G_P$ is fully described by the values of P on the set $R = \{1111, 0111, 0101, 0011, 0001, 0000\}$ of representative orbits in $B_4 \cdot C_4$. The numbers next to each orbit indicate the size of the orbit. For example, $\boxed{0011}\ 4$ means that $0011 \cdot C_4 = \{0011, 1001, 1100, 0110\}$, the orbit of 0011 in the action of C_4 has size $|0011 \cdot C_4| = 4$.

The generating functions of any $P\colon \{0,1\}^4 \to \{0,1\}$ are then given by:

$$(12)\quad P^1(z) = \Gamma(\bar{0}) + 4P(0001)z + 4P(0011)z^2 + 2P(0101)z^2 + 4P(0111)z^3 + P(\bar{1})z^4 .$$

The calculation of $P^1(z)$ can in general be quite complicated. However, things simplify considerably if we consider $P^1(z)$ mod q, for some natural number q. For example, if we want to compute modulo 2, Figure 6 simplifies to

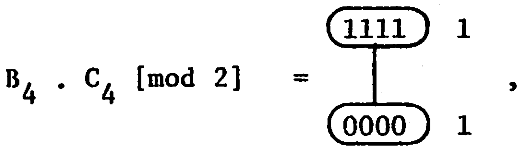


Figure 7.

and formula (12) becomes

$$(13)\quad P^1(z) \equiv P(\bar{0}) + P(\bar{1})z^4 \quad [\text{mod } 2].$$

It follows from $P(\bar{0}) \neq P(\bar{1})$ that $P^1(-1) \equiv \pm 1$ [mod 2], hence $P^1(-1) \neq 0$ and, by Corollary 2 of Proposition 2, any $P\colon \{0,1\}^4 \to \{0,1\}$ such that $C_4 \leq G_p$ and $P(\bar{0}) \neq P(\bar{1})$ must be exhaustive.

This technique generalizes very nicely, and

<u>Theorem 2</u>: The generalized conjecture holds for $d = q^\alpha$, a prime power.

<u>Proof</u>: The general idea is to prove that G_p transitive and $d = q^\alpha$ implies $P^1(-1) \equiv \pm 1$ [mod q], hence P must be exhaustive. It is convenient to decompose the argument in two parts. First, let us show that, from elementary group theory,

<u>Lemma</u>: If G_p acts transitively on $\{1,\ldots,d\}$ with $d = q^\alpha$ a prime power, it admits a Sylow subgroup $S \leq G_p$ such that $|S| = q^\beta$ with $\beta \geq \alpha$, which also acts transitively on $\{1,\ldots,d\}$.

<u>Proof of the Lemma</u>: Since G_p acts transitively on $\{1,2,\ldots,d\}$ and $d = q^\alpha$, we know that $q^\alpha \mid |G_p|$. Suppose q^β is the highest power of the prime q which divides $|G_p|$, thus $\beta = \alpha + r$ with $r \geq 0$. From Sylow's theorem (see [2], page 10) we know that G_p has a subgroup $S \leq G_p$ of order $|S| = q^\beta$. For any $i \in \{1,\ldots,d\}$, let $i \,.\, S$ and $i \,.\, G_p$ denote the orbits of i in S and G_p respectively. From Wielandt ([12], Theorem 3.4, page 6), $q^m \mid |i \,.\, G_p|$ implies $q^m \mid |i \,.\, S|$ for any $m \geq 0$. In particular, this applies to $d = q^\alpha$, hence $|i \,.\, S| = d$ and S is indeed transitive. □

Let m be the number of orbits in the action of S on $\{0,1\}^d$ and $\bar{x}_1,\bar{x}_2,\ldots,\bar{x}_m$ be distinct representative of each such orbit. Since S is transitive, we see that $|\bar{x}_i . S| = 1$ iff $\bar{x}_i = \bar{0}$ or $\bar{x}_i = \bar{1}$ for $1 \leq i \leq m$. Hence, if we assume by convention that $\bar{x}_1 = \bar{0}$ and $\bar{x}_m = \bar{1}$, we have $|\bar{x}_i . S| > 1$ for $1 < i < m$. Since $q^\beta = |S| = |\bar{x}_i . S| \cdot |S_{\bar{x}_i}|$, we have $|\bar{x}_i . S| \equiv 0$ [mod q] for $1 < i < m$. It follows that, modulo q, the generating function for P^1 can be written:

$$(16) \quad P^1(z) \equiv P^1(\bar{0}) + P^1(\bar{1}) . z^d \quad [\text{mod } q],$$

hence $P^1(-1) \equiv P^1(\bar{0}) - P^1(\bar{1}) \not\equiv 0$ [mod q], therefore P must be exhaustive. Theorem 2 is proved. □

As we shall see, if d is not a prime power, there exists properties P such that $P^1(-1) = 0$ and G_P transitive. They are not counterexamples to the generalized conjecture however† and, in order to prove that they are exhaustive, we generalize Proposition 2 as follows:

Proposition 4: *If P: $\{0,1\}^d \to \{0,1\}$ is not exhaustive with G_P transitive, then $(1 + z)^2$ divides $P^1(z)$.*

Proof: We notice that $P^1(-1)$ can be expressed with the Möbius inverse $Q(\bar{x})$ of $P(\bar{x})$, since if $P(\bar{x}) = \sum_{\bar{0} \leq \bar{y} \leq \bar{x}} Q(\bar{y})$, (there is only one such function Q: $\{0,1\}^d \to \mathbb{N}$), then, by Möbius inversion, $Q(\bar{x}) = \sum_{\bar{0} \leq \bar{y} \leq \bar{x}} P(\bar{x})(-1)^{w(\bar{x} \oplus \bar{y})}$, so that $Q(\bar{1}) = P^1(-1)$. Here $\bar{x} \oplus \bar{y}$ denotes the component-wise "exclusive-or" of $\bar{x}$ and $\bar{y}$. Thus, P

† At least for all the examples we discovered.

non-exhaustive implies $Q(1^d) = 0$. Furthermore, if G_P is transitive, then $P^1_{x_i=0} = \{\bar{x} \varepsilon P^1 | x_i = 0\}$ must contain a perfect matching for each $i \varepsilon [1,d]$ since it makes no difference which variable x_i a P-algorithm tests first. A necessary condition for this is $Q(1^{i-1}01^{d-i}) = 0$, for $1 \leq i \leq d$, since this is the appropriate sum within $\{\bar{x} \varepsilon \{0,1\}^d | x_i = 0\}$. Since $P^1(z) = \sum_{\bar{0} \leq \bar{x} \leq \bar{1}} P(\bar{x}) \cdot z^{w(\bar{x})}$, we have

$$P^1(z) = \sum_{\bar{0} \leq \bar{x} \leq \bar{1}} \sum_{\bar{0} \leq \bar{y} \leq \bar{x}} Q(\bar{y}) z^{w(\bar{x})} = \sum_{\bar{0} \leq \bar{y} \leq \bar{1}} Q(\bar{y}) z^{w(\bar{y})} (1+z)^{d-w(\bar{y})} .$$

Proposition 4 follows directly. □

More generally, if P is not exhaustive with G_P k-transitive, then $(1+z)^{k+1}$ divides $P^1(z)$.

V. OTHER APPLICATIONS

We now attempt to solve special cases of the generalized conjecture, by considering functions (properties) which are invariant under some specific transitive group.

a) The Cyclic Group C

Consider for example the function:

(17) $P_{15} \equiv (x_1,\ldots,x_d$ has k consecutive ones) ,

where consecutive means up to circular shift (graphically, we may draw $x_1,x_2,\ldots,x_d$ on a circle so that x_1 and x_d are adjacent). Clearly, $C_d \leq G_{P_{15}}$, where C_d is the cyclic group $C_d = <(12\ldots d)>$. Let us prove that:

Proposition 5: For all $d, k \geq 1$, the function P_{15} defined by (17) is exhaustive.

Proof: Let q_k^d denote the number of vectors $\bar{x} \in \{0,1\}^d$ starting with a zero (i.e., $x_1 = 0$) and having no run of k consecutive ones; let t_k^d denote the number of such x's having no cyclic run of k consecutive ones. By counting strings $\bar{y}$ of the form $01^{i-1}\bar{x}$ where $\bar{x}$ is counted in q_k^{d-i}, we have: $q_k^d = 0$ for $d \leq 0$, $q_k^d = 1$ for $1 \leq d \leq 2$ and $q_k^d = \sum_{1 \leq i \leq k} q_k^{d-i}$ for $d \geq 3$. It follows from counting t_k^d as cyclic shifts (up to i places) of $01^{i-1}\bar{x}$ where $\bar{x}$ is counted in q_k^{d-i}, $1 \leq i \leq k$, that $t_k^d = \sum_{1 \leq i \leq k} i \cdot q_k^{d-i}$, so that either t_k^d is odd -- all cases except k even and $d \equiv 0[\mathrm{mod}\ k+1]$ -- in which case $P_{15}^1(-1) \equiv 1\ [\mathrm{mod}\ 2]$, hence $P_{15}^1(-1) \neq 0$, or q_k^d is odd in which case $\frac{d}{dz}P_{15}^1(-1) \equiv 1\ [\mathrm{mod}\ 2]$, hence $\frac{d}{dz}P_{15}^1(-1) \neq 0$. It follows from Proposition 4 that P_{15} is exhaustive. □

The reader may find it challenging to try and prove the last result through an oracle construction.

This particular example demonstrates that the method can be applied to specific questions as well as to more general problems. We now attempt to prove that all functions which are left invariant by the cyclic group are exhaustive. The smallest d not covered by Theorem 2 is $d = 6$. The graph of $B_6 \cdot C_6$ is drawn in

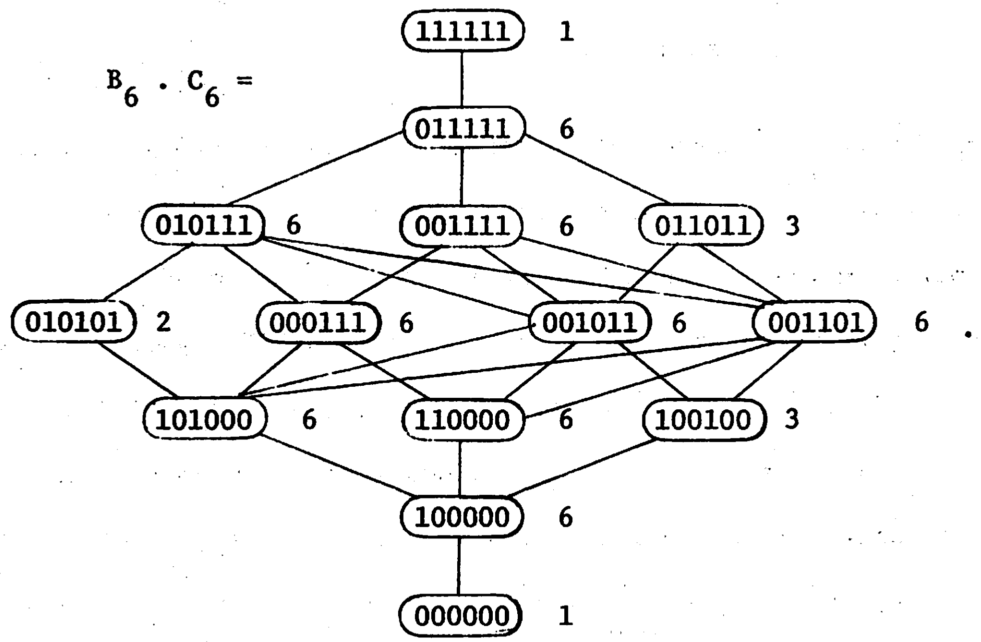


Figure 8.

Since this leaves too many possibilities, we consider the same diagram, omitting the orbits of size 0 modulo 3:

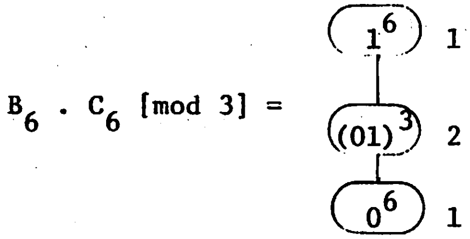


Figure 9.

From this consideration, we see that the generating function $P^1(z)$ for a property $P: \{0,1\}^6 \to \{0,1\}$ such that $C_6 \leq G_P$ is of the form:

$$(18) \quad P^1(z) \equiv P(\bar{0}) + 2P((01)^3)z^3 + P(\bar{1})z^6 \text{ [mod 3]}.$$

The constraint $P(0^6) \neq P(1^6)$ suffices to ensure that $P^1(-1) \equiv \pm 1$ [mod 3], hence $P^1(-1) \neq 0$ and P is exhaustive by Proposition 2, Corollary 2.

We shall generalize this idea, and show that functions which are left invariant by C_d are exhaustive for a large class of values of d. For this purpose, let $\mathbb{E} \subseteq \mathbb{N}$ denote the smallest subset of the natural numbers such that:

(19) (i) $1 \in \mathbb{E}$

(ii) If $n \in \mathbb{E}$ and q is a prime such that $q \geq 2^{n-1}$, then $nq^\alpha \in \mathbb{E}$ for all natural numbers $\alpha \in \mathbb{N}$.

In particular, we see that $\mathbb{E}$ contains all the prime powers, as well as composite numbers, such as $2 \cdot 3 \cdot 31 \cdots$ having an arbitrary number of prime factors. The relevance of this set to our problem appears in:

<u>*Theorem 3*</u>*:* *If $d \in \mathbb{E}$ (the set defined by (19)) then any function $P: \{0,1\}^d \to \{0,1\}$ such that $P(\bar{0}) \neq P(\bar{1})$ and $C_d \leq G_P$ is exhaustive.*

<u>Proof</u>: We prove by induction that $d \in \mathbb{E} \Rightarrow P^1(-1) \neq 0$. Suppose $d = nq^\alpha$ with q prime, $(n,q) = 1$; because of Theorem 2, we may as well assume $n > 1$. Let $C^q = \langle(12\ldots d)^q\rangle$ be the subgroup $C^q \leq C_d$ of order $|C^q| = q^\alpha$ of q-shifts of the inputs. Let m be the number of orbits in the action of C^q on $\{0,1\}^d$, and $R = \{\bar{x}_1 = \bar{0}, \bar{x}_2, \ldots, \bar{x}_{m-1}, \bar{x}_m = \bar{1}\}$ be a set of representative elements in each of these orbits. By (11), we have $P^1(z) = \sum_{1 \leq j \leq m} |\bar{x}_j \,.\, C^q| \,.\, P(\bar{x}_j) \,.\, z^{w(\bar{x}_j)}$.

From the identity $q^\alpha = |C^q| = |\bar{x} \,.\, C^q| . |C^q_{\bar{x}}|$, we see that $|\bar{x}_j C^q| \equiv 0$

[mod q] unless, for all $\sigma \in C^q$: $\sigma(\bar{x}_j) = \bar{x}_j$ in which case $|\bar{x}_j C^q| = 1$. It is easy to see that this last situation can only happen if $\bar{x}_j = (\bar{y}_j)^{q^\alpha}$ is the same pattern $\bar{y}_j$ of n bits, repeated q^α times. Computing $P^1(z)$ modulo q therefore yields:

$$(20) \quad P^1(z) \equiv \sum_{\bar{y} \in \{0,1\}^n} P((\bar{y})^{q^\alpha}) \,.\, z^{w(\bar{y})} \quad [\text{mod } q].$$

To each P: $\{0,1\}^d \mapsto \{0,1\}$, we can associate a Q: $\{0,1\}^n \mapsto \{0,1\}$ defined by $Q(\bar{y}) = P((\bar{y})^{q^\alpha})$ for each $\bar{y} \in \{0,1\}^n$. Formula (20) then becomes $P^1(z) \equiv Q^1(z)$ [mod q]. If we now assume $n \in \mathbb{E}$, we know by induction that $|Q^1(-1)| \geq 1$. Since $|Q^1(-1)| = \text{absval}\,(|Q^1_{\text{even}}| - |Q^1_{\text{odd}}|) \leq 2^{n-1}$, we have $Q^1(-1) \not\equiv 0$ [mod q] as soon as $q > 2^{n-1}$; it follows that $P^1(-1) \neq 0$ if $d \in \mathbb{E}$, thus concluding the proof of Theorem 3. □

The first value for which Theorem 3 does not apply is $d = 12$, and in fact, there exists (monotone) properties P: $\{0,1\}^{12} \mapsto \{0,1\}$ with $P(\bar{0}) \neq P(\bar{1})$ and $C_{12} \leq G_P$ such that $P^1(-1) = 0$. Ad hoc arguments for this case, based on Proposition 4 show that these functions are exhaustive. One should therefore regard this case $(d = 12)$ as a demonstration of the limits of applicability of our proof of Theorem 3 rather than an indication contradicting the Generalized Conjecture. It also gives an idea of the difficulties involved in setting up a computer search for counterexamples. Indeed, the cyclic group is in a sense the "simplest" group, yet the first place to look for a counterexample is $d = 20$!

b) <u>Graph Properties</u>

Let us turn to graph properties, which were the original motivation for this work. We consider undirected graphs having v vertices to be represented by the upper non diagonal part of their adjacency matrices. In this case, the number d of elements permuted by the transitive group I_v is $\frac{1}{2}v(v-1)$ which is never a prime power, except for the trivial cases $v = 2,3$; Theorem 2 does not apply here!

Before describing a more general (unsuccessful) attempt at solving the Aanderaa-Rosenberg conjecture, we point out that, in some cases, it is possible to explicitly compute $P^1(-1)$ for some specific graph properties P. For example:

<u>*Proposition 6:*</u> *The graph property $P_{16}(H)$ = "The edges of H are not contained in a triangle" is exhaustive.*

<u>Proof</u>: If $v = |H|$, hence $d = \frac{1}{2}v(v-1)$, then

$$(21) \quad P^1_{16}(z) = (1+z)^d - (1 + dz + d(v-2)z^2 + \frac{d(v-2)}{3} z^3).$$

Since $P^1_{16}(-1) = \frac{v(v-1)(v-5)}{6} - 1$ is never 0, Proposition 6 is proved. □

This approach has been exploited by Best, van Emde Boas and Lenstra [1] who showed in this way that the graph properties: "Graph H contains a directed cycle", "Graph H is transitive", "Graph H is contained in a star", etc.... are exhaustive.

In order to try and derive general results, consider $B_d \cdot I_v$, for example in the case $v = 4$

$B_6 \cdot I_4 =$

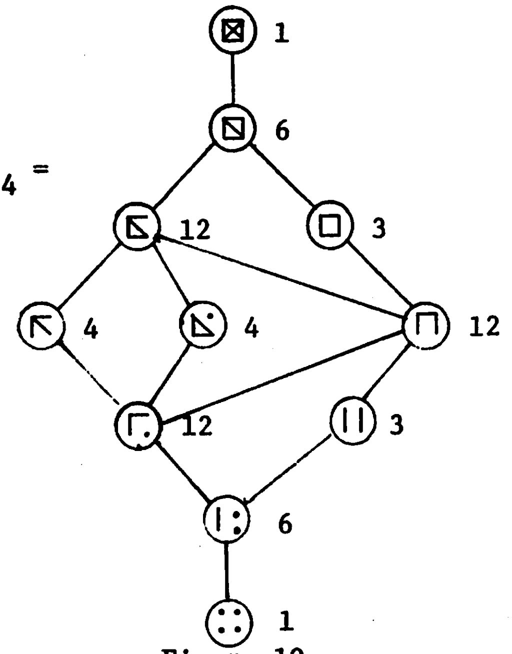
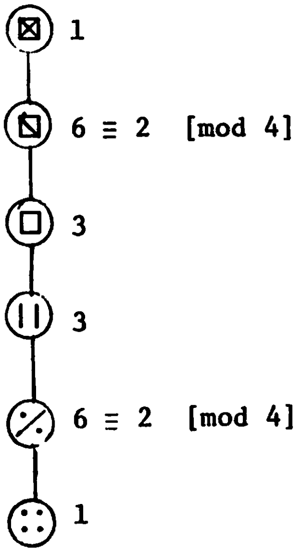


Figure 10.

Here, 4 means that the number of different representations of the graph by adjacency matrices is 4.

Exhaustive inspection of this diagram shows that there is no non-trivial property P such that both P^0 and P^1 admit a perfect matching, hence by Proposition 2, all non-trivial graph properties are exhaustive when $v = 4$. If we restrict ourselves to monotone graph properties, the argument is simplified by the consideration of $B_6 \cdot I_4$ [mod 6]:

$B_6 \cdot I_4$ [mod 6] =



;

Figure 11.

from this, we conclude that $P^1(-1) \equiv \pm 1$ or 2 [mod 6] for any non-trivial monotone graph property P. This technique allows to solve many small cases of the problem, namely:

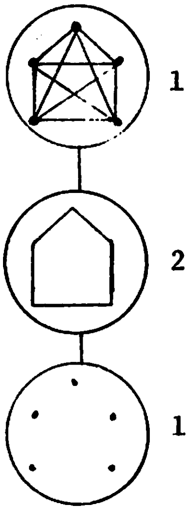
<u>*Proposition 7:*</u> *The Aanderaa-Rosenberg conjecture holds for graphs of size $v = 1,2,3,4,5,11$ and 13.*

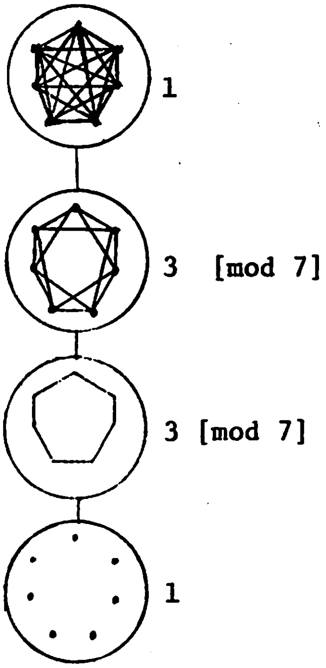
<u>**Proof:**</u> The case $v = 4$ has been treated by an ad-hoc exhaustive inspection. The other values correspond to v prime. In this case, an elegant combinatorial remark by Laurent Hyafil shows that

$$B_{\frac{1}{2}v(v-1)} \cdot I_v \text{ [mod v] is isomorphic to } B_{\frac{1}{2}v(v-1)} \cdot C_{\frac{1}{2}(v-1)} .$$

For example

$B_{10} \cdot I_5$ [mod 5] = and $B_{21} \cdot I_7$ [mod 7] =





<u>Figure 12</u>.

look respectively like

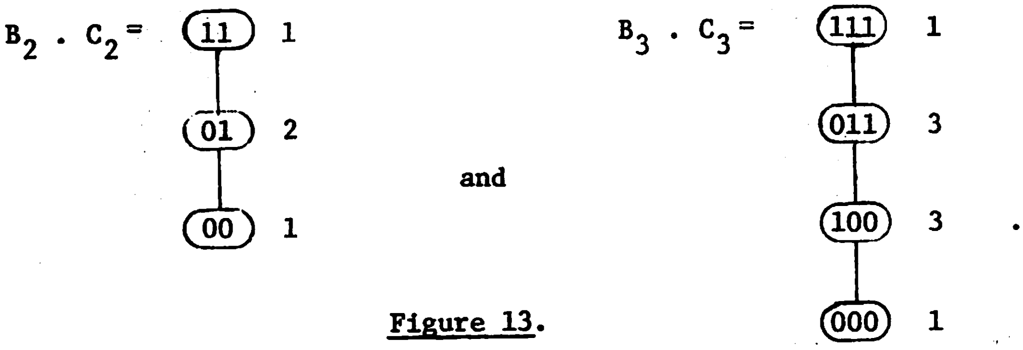


Figure 13.

Using this remark, it is easy to prove Proposition 7, ... and to realize that more involved techniques will be required if one is to prove the conjecture in the other cases. Indeed, for $v = 9$, the property $P(H) \equiv$ "Graph H is not contained in G_1, G_2, or G_3" is such that $P^1(-1) = 0$; where, $G_1 = ||||\cdot$, $G_2 = \Delta\Delta\Delta$ and $G_3 = ⊠ ⁙$. □

In order to salvage part of our effort, let H_n denote a Hamiltonian circuit through n nodes. When n is prime, let $H_n^{(k)}$ for $1 \leq k \leq \frac{1}{2}(n - 1)$ denote the superposition of k edge disjoint Hamiltonian circuits through n nodes; hence, $H_n^{(1)} = H_n$, $H_n^{(\frac{1}{2}(n-1))} = K_n$ the complete graph, and the number of edges in $H_n^{(k)}$ is kn.

<u>*Proposition 8:*</u> *Any non-trivial monotone graph property P of v-nodes graphs such that $P(H_v) = 1$ is exhaustive for v a prime number.*

<u>**Proof**</u>: Consider the subgroup $C^v \leq I_v$ generated by the action on the edges of the graph of the subgroup C_v of cyclic relabelling of the vertices. If v is prime, the orbits $H \cdot C^v$ in the action of C^v

on $\{0,1\}^d$ with $d = \frac{1}{2}v(v-1)$ have size v, unless H is left invariant by C^v. The graphs which are left invariant by C^v are precisely the $H_v^{(k)}$'s. The generating function of a property P satisfying the hypothesis of Proposition 8 therefore satisfies:

$$(22) \quad P^1(z) \equiv (1+z)^d - 1 \quad [\mathrm{mod}\ v], \text{ hence } P^1(-1) \neq 0$$

and P must be exhaustive. □

Of course, there is a general duality principle involved in the problem by which we can replace $P(H_v) = 1$ by $P(\bar{H}_v) = 0$ without affecting the conclusions. Here $\bar{H}_v = H_v^{(\frac{1}{2}(v-1))}$ is the complement of H_v.

c) Subgraphs Properties

Instead of studying properties which apply to all graphs, we now consider properties which are only defined for the family of subgraphs of a given graph H, or a set of given graphs. The invariance group such properties is then a subgroup of I_v, namely the permutation group resulting from the action of the automorphism group $\Gamma(H)$ of H on the edges of H, which we call the edge group of H.

We say that a graph H is edge-transitive (resp. vertex transitive) if the automorphism group $\Gamma(H)$ of H acts transitively on its edges (resp. vertices). Harary [3] calls such graphs line-symmetric (resp. point-symmetric).

In order to ensure that properties P of the family of subgraphs of a given graph H have a transitive invariance group G_p, we therefore insist that H be edge-transitive.

Viewed in this fashion, the graph properties which we previously studied are a special case, namely the properties of the family of subgraphs of K_v, the complete graph with v nodes.

The bipartite graphs form an interesting class of edge-transitive graphs, and we shall study <u>bipartite-properties</u>, i.e., properties which apply to the class of bipartite graphs. More precisely, P is a (n,m) bipartite property if $P: \{0,1\}^d \mapsto \{0,1\}$ with $d = n.m$ and $I_{n,m} \leq G_p$, where $I_{n,m}$ is the permutation group generated on $n \times m$ boolean matrices by arbitrary independent transposition of any two rows or columns.

If q is a prime, α and β natural numbers, we see from Theorem 2 that any (q^{α},q^{β}) bipartite property such that $P(\bar{0}) \neq P(\bar{1})$ is exhaustive. It is not too hard to also show:

<u>*Proposition 9:*</u> *If q is a prime and $n \leq q$ a natural number, any non-trivial monotone (q,n) bipartite property is exhaustive.*

<u>**Proof**</u>: Let P be such a property and $d = q.n$. In the action of $I_{q,n}$ on $\{0,1\}^d$, the orbits $\bar{x}.I_{q,n}$ have all size $|\bar{x}.I_{q,n}| \equiv 0$ [mod q] unless the representation of $\bar{x}$ as a q rows and m columns matrix is such that all columns are either equal to 1^q or 0^q, in which case $|\bar{x}.I_{q,n}| = \binom{n}{k}$, where k is the number of 1^q columns. It follows that

$$(23)\quad P^1(z) \equiv \sum_{1 \leq k \leq m} \binom{m}{k} z^{kq} \text{ [mod q]} \quad \text{for some} \quad i \geq 1 \text{ .}$$

Thus

$$(24)\quad P^1(-1) \equiv \sum_{i \leq k \leq m} \binom{m}{k} (-1)^k \equiv (-1)^i \binom{m}{i} \text{ [mod q];}$$

therefore $P^1(-1) \neq 0$, since $q \geq m$ implies $\binom{m-1}{i} \not\equiv 0$ [mod q]. □

VI. DISCUSSION

We have seen that our non-constructive approach has led to encouraging while not decisive results on the Aanderaa-Rosenberg conjecture. An examination of a generalization of the conjecture seems to indicate that the important requirements are $P(\bar{0}) \neq P(\bar{1})$ and G_p transitive.

It should be interesting to relate, in the case G_p untransitive, the complexity $C(P)$ of P to its dependence upon variables in the various transitivity classes.

VII. ACKNOWLEDGMENTS

We should like to thank Joel Coffy, Laurent Hyafil, Richard Karp, David Klarner and Marc Schutzenberger for their comments and suggestions on preliminary results.

VIII. BIBLIOGRAPHY

[1] M.R. Best, P. van Emde Boas and H.W. Lenstra, Jr., "A Sharpened Version of the Aanderaa-Rosenberg Conjecture", Mathematisch Centrum Report ZW 30/74, Amsterdam, (1974).

[2] N. Biggs, "Finite Groups of Automorphisms", London Mathematical Society Lecture Note Series 6, Cambridge University Press (1971).

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

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

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

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

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

[8] 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).

[9] R.L. Rivest and J. Vuillemin, "On the Time Required to Recognize Properties of Graphs from their Adjacency Matrices", (to appear).

[10] A.L. Rosenberg, "On the Time Required to Recongize 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).

[12] H. Wielandt, *Finite Permutation Groups*, Academic Press, (1964).