

**stichting  
mathematisch  
centrum**



---

AFDELING ZUIVERE WISKUNDE

ZW 30/74

OCTOBER

M. BEST, P. VAN EMDE BOAS & H.W. LENSTRA JR.

A SHARPENED VERSION OF THE AANDERAA-ROSENBERG CONJECTURE

---

**2e boerhaavestraat 49 amsterdam**

BIBLIOTHEEK MATHEMATISCH CENTRUM  
AMSTERDAM

*Printed at the Mathematical Centre, 49, 2e Boerhaavestraat, Amsterdam.*

*The Mathematical Centre, founded the 11-th of February 1946, is a non-profit institution aiming at the promotion of pure mathematics and its applications. It is sponsored by the Netherlands Government through the Netherlands Organization for the Advancement of Pure Research (Z.W.O), by the Municipality of Amsterdam, by the University of Amsterdam, by the Free University at Amsterdam, and by industries.*

A sharpened version of the AANDERAA-ROSENBERG conjecture

by

M.R. Best, P. van Emde Boas and H.W. Lenstra jr.

ABSTRACT

The AANDERAA-ROSENBERG conjecture states that every algorithm which decides whether some graph, which is represented by means of its adjacency-matrix, has some non-trivial monotonic property, must in the worst case probe  $O(n^2)$  entries. We present a number of techniques which enable us to prove for several specific properties (e.g. connectedness) that in order to decide these properties in fact all edges must be probed by the algorithm. Moreover, we present some new examples of properties on undirected graphs, where not all the edges are needed, or even stronger,  $O(n)$  edges are sufficient.

KEYWORDS & PHRASES: *Properties of graphs, analyses of algorithms.*

## 1. INTRODUCTION

For  $n \in \mathbb{N}^*$ , let  $G_n$  be the collection of all graphs<sup>\*\*)</sup> with set of vertices  $\{1, 2, \dots, n\}$ , and let  $G = \bigcup_{n \in \mathbb{N}} G_n$ . Let  $G, H \in G$  and let  $x$  be an edge. Then

$|G|$  denotes the number of edges in  $G$ ;  
 $x \in G$  denotes that  $x$  is an edge of  $G$ ;  
 $G \subset H, G \cap H$ , etc. denote the corresponding expressions for the sets of edges, provided the sets of vertices coincide;  
 $G^c$  denotes the graph complementary to  $G$ ;  
 $G \simeq H$  denotes graph-isomorphism;  
 $E_n$  denotes the totally disconnected graph on  $\{1, 2, \dots, n\}$ ;  
 $K_n$  denotes the complete graph on  $\{1, 2, \dots, n\}$ ;  
 $e_n = |K_n|$ . We write  $e = e_n$  if no confusion arises.

Let  $P$  be a property on  $G$ , and  $G \in G$ . Then in expressions like  $G \in P$ ,  $G_n \cap P$ ,  $G_n \setminus P$ , etc.,  $P$  is identified with the collection of graphs in  $G$  which satisfy  $P$ . We denote  $G_n \cap P$  by  $P_n$ .  $P$  is called a *property on  $G_n$*  if  $P \subset G_n$ . In this case  $P^c$  denotes  $G_n \setminus P$ . A property  $P$  is called a *graph-property* if

$$\forall G \in G \forall H \in G ((G \in P \wedge G \simeq H) \Rightarrow H \in P).$$

Now fix a natural number  $n$  and a property  $P$  on  $G_n$  and consider the following game between two persons, called the hider and the seeker. First the hider takes a graph  $G \in G_n$  in mind. The seeker aims to find out as soon as possible whether  $G \in P$  or not. To do so, each of his moves consists of questioning the hider as to whether some edge  $x$  is in  $G$  or not. The game terminates on the moment that the seeker can decide, using the information gathered so far, whether  $G \in P$ . The hider wins if all edges have been asked for; otherwise the seeker wins.

---

\*) In this note, zero will be called a natural number ( $0 \in \mathbb{N}$ ).

\*\*) For the time being, we leave undecided whether we consider directed or undirected graphs.

In order to avoid trivialities, such as choosing the property "the graph has  $n$  vertices" (one is ready at the beginning), or "the graph has a self-loop" (as LIPTON and SNYDER have computed in [7], this game costs the seeker at most as many moves as there can be self-loops), one should agree:

- I. all graphs are understood to contain no self-loops;
- II. only non-trivial properties on  $G_n$  are to be considered.

A property  $P$  on  $G_n$  is called *non-trivial*, if neither  $P$  nor  $P^c$  is empty. An arbitrary property  $P$  is called *non-trivial on  $G_n$* , if  $P_n$  is non-trivial.

After having lost many games (and being frustrated by his thankless task), the hider becomes perfidious, and modifies the rules of the game. Instead of actually selecting a graph in advance, he only provides answers to the seeker's questions, thus designing a graph which is hard to determine for his opponents decision algorithm.

We denote the number of moves in this modified game, assuming that both opponents play optimally, by  $\mu(P)$ . Now the question is whether there exists a (non-trivial graph) property  $P$  on  $G_n$  such that  $\mu(P) < e_n$ . We call property  $P$  on  $G_n$  for which this is not the case (i.e.  $\mu(P) = e_n$ ), *evasive*. An arbitrary property  $P$  is called *evasive on  $G_n$*  if  $P_n$  is evasive.

The quantity  $\mu(P_n)$  indicates the number of entries of the adjacency matrix of  $G$  any  $P$ -algorithm can be forced to probe, in order to decide whether the graph  $G$  has property  $P$  or not. This explains why the behaviour of  $\mu$  has drawn the attention of several people working in the field of analysis of algorithms. HOLT and REINOLD [4] derived for the properties "is strongly connected" and "contains a directed cycle" lower bounds of respectively  $\frac{1}{2}n(n-1)$  and  $\frac{1}{4}(n+1)(n-1)$ . We show in section 4 that these two properties are actually evasive.

ROSENBERG [8] conjectured that for any non-trivial graph property  $P$  we have  $\mu(P_n) \gg n^2$ . \*) However, AANDERAA provided a counterexample for

---

\*) It is not clear how the assertion " $\mu(P_n) = O(n^2)$ " should be interpreted. The LANDAU-BACHMANN  $O$ -symbol can certainly not be intended. We have chosen for the interpretation  $\mu(P_n) \gg n^2$  (WINOGRADOV's symbol:  $\liminf_{n \rightarrow \infty} \mu(P_n) / n^2 > 0$ ), although the interpretation  $\mu(P_n) = \Omega(n^2)$  (i.e. not  $\mu(P_n) = o(n^2)$ , or  $\limsup_{n \rightarrow \infty} \mu(P_n) / n^2 > 0$ ) can be defended as well.

directed graphs (cf. section 7). Together they formulated the AANDERAA-ROSENBERG conjecture, stating that for any non-trivial monotonic graph property, the estimate  $\mu(P_n) \gg n^2$  holds [8]. A property  $P$  is called *monotonic* if

$$\forall G \in \mathcal{G} \forall H \in \mathcal{G} ((G \in \mathcal{P} \wedge G \subset H) \Rightarrow H \in \mathcal{P}).$$

A number of results can be found in a paper by KIRKPATRICK [6]. He proves  $\mu(P_n) \gg n^2$  for several special properties  $P$ . Furthermore he claims the estimate  $\mu(P_n) \gg n \cdot \log n$  in case  $P$  is monotonic, using a proof which can not convince us (the treatment of case (2) in his lemma 3 is inadequate).

It has already been suggested by HOPCROFT and TARJAN [5] and by R. KARP (cf. [8]), that for many graph properties  $P$ , any  $P$ -algorithm must, in the worst case, inspect all entries of the adjacency matrix. Indeed, it seems reasonable to conjecture that any non-trivial monotonic graph property is evasive.

In this note, we develop a few techniques by which we can prove evasiveness for many special properties. Moreover we present in section 7 some new examples of properties on undirected graphs which are non-evasive, one of them even being a counterexample to the original ROSENBERG conjecture.

## 2. SOME GENERAL REMARKS

I. It follows from a result of KIRKPATRICK that for any non-trivial graph property  $P$  the lower bound  $\mu(P_n) \gg n$  holds. His theorem 1 in [6] states that for directed graphs the inequality

$$\mu(P_n) \geq n(n-1)/k_p + k_p - 1$$

holds for some positive number  $k_p$ . This obviously yields  $\mu(P_n) \geq 2n-2$ .

For undirected graphs corollary 1 in the same paper leads to  $\mu(P_n) \geq n\sqrt{2}-2$  for any non-trivial graph property  $P$ .

II. The AANDERAA-ROSENBERG conjecture implies the existence of a universal constant  $c_0 > 0$  and integer  $n_0 \in \mathbb{N}$  such that for every  $n \geq n_0$  and for every non-trivial monotonic graph property  $P$  on  $G_n$  one has  $\mu(P) > c_0 n^2$ .

This can be seen as follows. Construct a property  $P$  by  $P_0 = P_1 = \emptyset$  and  $P_n$  is a non-trivial monotonic graph property  $Q$  on  $G_n$  for which  $\mu(Q)$  attains its minimal value. This minimum exists by finiteness. By the conjecture one has

$$\exists c_0 > 0 \exists n_0 \in \mathbb{N} \forall n \geq n_0 (\mu(P_n) > c_0 n^2).$$

Now the assertion stated above follows from the minimality of  $\mu(P_n)$ .

III. For each property  $P$  on  $G$  we define the *dual* property  $P^*$  by

$$P^* = \{G \mid G \in G \wedge G^c \notin P\}.$$

It will be clear that  $P^*$  is a graph property (non-trivial, monotonic) if and only if  $P$  is. Furthermore  $\mu(P_n^*) = \mu(P_n)$ .

IV. Let  $G$  be a directed graph on  $\{1, 2, \dots, n\}$ . We define the undirected graphs  $G'$  and  $G''$  on the same vertexset by:

$$(i, j) \in G' \Leftrightarrow (\langle i, j \rangle \in G \wedge \langle j, i \rangle \in G);$$

$$(i, j) \in G'' \Leftrightarrow (\langle i, j \rangle \in G \vee \langle j, i \rangle \in G).$$

Now let  $P$  be a property for undirected graphs. Then we define the properties  $P'$  and  $P''$  for directed graphs by:

$$P' = \{G \mid G' \in P\} \quad \text{and} \quad P'' = \{G \mid G'' \in P\}.$$

The hider can use any strategy for  $P$  also for  $P'$  ( $P''$ ) by giving an edge  $\langle i, j \rangle$  always (never) when  $\langle j, i \rangle$  has not yet been asked for, and otherwise he gives this edge if and only if  $(i, j)$  should have been given in the  $P$ -strategy. Hence  $\mu(P'_n) \geq 2\mu(P_n)$  and  $\mu(P''_n) \geq 2\mu(P_n)$ .

On the other hand, it is clear that the seeker needs both for  $P'$  and  $P''$  at most  $2\mu(P_n)$  questions, by asking every edge in both directions. Hence  $\mu(P'_n) \leq 2\mu(P_n)$  and  $\mu(P''_n) \leq 2\mu(P_n)$ .

Together this yields:

$$\mu(P'_n) = \mu(P''_n) = 2\mu(P_n).$$

In particular  $P'$  is evasive if and only if  $P$  is, and the same holds for  $P''$ .

As an example, we mention that if  $P$  is the property "connectedness" then  $P''$  is "weak connectedness". So if connectedness is evasive (and we shall prove below it is), then the same holds for weak connectedness.

V. For many properties a trivial strategy for the hider can be given, which makes the property evasive. We mention:

"The graph has exactly (at most)  $k$  edges"; the hider gives the first  $k$  edges and thereafter none.

"The graph is point-symmetric" or "the graph is line-symmetric"; the hider gives every edge asked for. Since the complete graph on  $n$  points is both point- and line-symmetric, and the graph with  $e-1$  edges is neither, the seeker has to ask for all edges.

### 3. A STRAIGHTFORWARD STRATEGY

Let  $P$  be the property "the graph contains a cycle" for undirected graphs. Suppose the hider uses for this property the following strategy: he gives every edge asked for, unless that edge should close a cycle. It turns out that this simple strategy is optimal, and that it makes the property evasive (except for  $n = 2$  but then the property is trivial). We will prove this for a more general class of properties.

THEOREM 1. *Let  $n \in \mathbb{N}$  and let  $P$  be a non-trivial monotonic property on  $G_n$  such that for every  $G \in G_n$  and for every  $x \notin G$  with  $G \cup \{x\} \notin P$  there is a  $y \notin G \cup \{x\}$  such that  $G \cup \{y\} \notin P$ . Then  $P$  is evasive.*

PROOF. Let  $G_i$  be the graph consisting of all edges given by the hider in his first  $i$  answers. Thus  $G_0 = E_n$ . The hider's strategy consists of giving an edge  $x$  in his  $i^{\text{th}}$  answer if and only if  $G_{i-1} \cup \{x\} \notin P$ . By induction, it is clear that  $G_i \notin P$  for all  $i$ .



Now suppose  $\mu(\mathcal{P}_n) = m < e$ . Let  $H$  be the set of edges not asked for in the game, and let  $x \in H$ . Then  $G_m \cup H \notin \mathcal{P}$  since otherwise the game was not finished. Put  $G = G_m \cup H \setminus \{x\}$ . Since  $G \cup \{x\} \notin \mathcal{P}$ , there is an edge  $y \notin G \cup \{x\} = G_m \cup H$  such that  $G \cup \{y\} \notin \mathcal{P}$ . This edge  $y$  must have been asked for during the game (in the  $k^{\text{th}}$  move, say), and have been refused by the hider. So  $G_{k-1} \cup \{y\} \in \mathcal{P}$ . Hence, by monotony,  $G \cup \{y\} \in \mathcal{P}$ . Contradiction.  $\square$

EXAMPLE 1. *"The graph contains a cycle" is an evasive property for undirected graphs with at least three vertices.*

It is left to the reader to show that this property satisfies the conditions of theorem 1.

EXAMPLE 2. *"The graph is planar" is an evasive property for undirected graphs with at least five vertices.\*)*

PROOF. Suppose  $G$  is a planar graph with at least five vertices,  $(a,b) \notin G$ , and  $G \cup \{(a,b)\}$  is planar. We claim that there is some edge different from  $(a,b)$  which may be added to  $G$  without disturbing planarity.

We assume that  $G \cup \{(a,b)\}$  is maximal planar, since otherwise our claim is trivial. Now fix some embedding of  $G \cup \{(a,b)\}$  in the sphere. By the maximality, its faces are all triangles, and therefore, the faces of  $G$  are all triangles except for one quadrangle  $(a,c,b,d)$ . Obviously  $G \cup \{(c,d)\}$  is planar, so if  $(c,d) \notin G$ , this yields the desired extension.

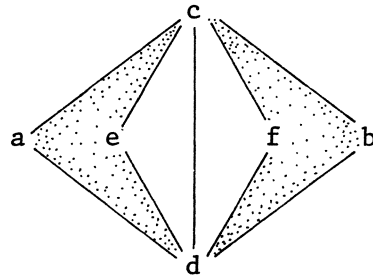
Hence we may assume that  $(c,d) \in G$ . Let the two triangles adjoining  $(c,d)$  be  $(c,d,e)$  and  $(c,d,f)$ . If  $\{e,f\} = \{a,b\}$  then  $(a,c,d)$ ,  $(b,c,d)$  and  $(a,c,b,d)$  are all faces, so  $G$  has only four vertices.

Hence we can assume that  $a \notin \{e,f\}$ .  $(e,f)$  cannot be an edge, since it would intersect either  $(c,d)$  or the path  $(c,a,d)$ . Now we divert  $(c,d)$  as the internal diagonal of the quadrangle  $(a,c,b,d)$ , and  $(e,f)$  may be added to  $G$  without disturbing the planarity.

This proves that for  $\mathcal{P} = \text{"non-planar"}$  the condition of theorem 1 is satisfied.  $\square$

---

\*) This result has been claimed without proof by HOPCROFT and TARJAN [5].



Picture of the graph  $G$ . The quadrangle  $(a,c,b,d)$  has been drawn as the exterior face. Other vertices and edges may be added in the shaded regions, although  $b = f$  is allowed.

By the duality mentioned in section 2, we obtain:

THEOREM 2. *Let  $P$  be a non-trivial monotonic property on  $G_n$  such that for every  $G \in G_n$  and for every  $x \in G$  with  $G \setminus \{x\} \in P$  there is an edge  $y \in G \setminus \{x\}$  such that  $G \setminus \{y\} \in P$ . Then  $P$  is evasive.*

EXAMPLE 3. *"The graph is connected" is an evasive property for undirected graphs.*

The proof is left to the reader.

#### 4. THE ENUMERATION POLYNOMIAL

We call a collection  $\{A,B\}$  of two sets a *pair of neighbours* if  $|A \Delta B| = 1$ . ( $\Delta$  denotes the symmetric difference.) A collection is called *pairable* if it is the disjoint union of pairs of neighbours.

THEOREM 3. *Let  $n \in \mathbb{N}$ ,  $P$  be a non-evasive property on  $G_n$ . Then both  $P$  and  $P^c$  are pairable.*

PROOF. Let  $G^{(i)}$  be the set of all graphs in  $G_n$  which are compatible with the first  $i$  answers of the hider, and let  $P^{(i)} = G^{(i)} \cap P$ . Note that  $G^{(i)}$  is pairable for  $i < e$ . If the game is finished after  $m$  moves, then either  $P^{(m)} = \emptyset$ , or  $P^{(m)} = G^{(m)}$ , so  $P^{(m)}$  is always pairable, unless  $m = e$ .

Now assume that  $P$  is not pairable. Then the hider does nothing except to ensure that for  $i \in \{0, 1, \dots, m\}$ ,  $P^{(i)}$  is not pairable. He may do so, because by assumption  $P^{(0)}$  is not pairable, and by asking the  $i^{\text{th}}$  edge, the seeker actually divides  $P^{(i-1)}$  into two subsets  $Q$  and  $R$ , from which the hider has to make the choice which one will become  $P^{(i)}$ . Since  $Q \cup R = P^{(i-1)}$ , there is at least one choice ( $P^{(i)} = Q$  or  $P^{(i)} = R$ ) for which  $P^{(i)}$  is not pairable. (The disjoint union of pairable sets is again pairable.)

Therefore,  $P^{(m)}$  is not pairable, so  $m = e$ , and  $P$  is evasive on  $G_n$ . Contradiction. So  $P$  is pairable. Similarly  $P^c$  is pairable.  $\square$

Although we do not give here any direct application of this theorem, it might be useful for those who intend to find a counterexample to the conjecture stated above. "Pairable" is quite a strong condition. Up till now, we were not able to find any non-trivial, monotonic, pairable graph property!

REMARK. It is not difficult to generalize theorem 3. A collection  $I$  is called a  $k$ -interval, if there are sets  $A \in I$  and  $B \in I$  such that  $|B \setminus A| = k$ , and  $I = \{C \mid A \subset C \wedge C \subset B\}$ . Thus a 1-interval is a pair of neighbours.

Now the following holds.

Let  $k \in \mathbb{N}$ ,  $n \in \mathbb{N}$ , and  $P$  be a property on  $G_n$  such that  $\mu(P) \leq e - k$ . Then  $P$  is the disjoint union of  $k$ -intervals.

Let  $N \in \mathbb{N}$ . Then  $f(X) = \sum_{k=0}^N a_k X^k$  is called an enumerating polynomial in  $X$  of degree  $N$  if for all  $k \in \{0, 1, \dots, N\}$  one has  $a_k \in \mathbb{N}$  and  $a_k \leq \binom{N}{k}$ . (Note that  $a_N = 0$  is allowed.)

Now let  $n \in \mathbb{N}$  and  $P$  be a property on  $G_n$ . Then we define

$$F(P, X) = \sum_{G \in P} X^{|G|} = \sum_{k=0}^e N(P, k) \cdot X^k,$$

where  $N(P, k)$  denotes the number of graphs in  $P$  with exactly  $k$  edges.

Obviously, for fixed  $P$ ,  $F(P,X)$  is an enumerating polynomial in  $X$  of degree  $e$ , called the *enumeration polynomial*.

THEOREM 4. *Let  $n \in \mathbb{N}$  and  $P$  be a non-evasive property on  $G_n$ . Then  $F(P,X)$  is divisible by  $1+X$  in  $\mathbb{Z}[X]$ , and moreover  $F(P,X)/(1+X)$  is an enumerating polynomial in  $X$  of degree  $e-1$ .*

PROOF. The contribution to the enumeration polynomial of a pair of neighbours is divisible by  $1+X$ . Hence from theorem 3 both  $F(P,X)/(1+X)$  and  $((1+X)^e - F(P,X))/(1+X)$  are polynomials in  $X$  over  $\mathbb{N}$ .  $\square$

COROLLARY 1. *Let  $n \in \mathbb{N}$ , and  $P$  be a property on  $G_n$  such that  $F(P,-1) \neq 0$ . Then  $P$  is evasive on  $G_n$ .*

COROLLARY 2. *Let  $n \in \mathbb{N}$ , and  $P$  be a property on  $G_n$  such that  $|P|$  is odd. Then  $P$  is evasive on  $G_n$ .\*)*

EXAMPLE 4. *"The graph contains a directed cycle" is an evasive property for directed graphs.*

PROOF. We use corollary 2. For  $n \in \mathbb{N}$  let  $A_n$  be the collection of all acyclic digraphs on  $\{1,2,\dots,n\}$ . For  $n \geq 2$  let  $A_n^T$  be the collection of all acyclic digraphs on  $\{1,2,\dots,n\}$  which are invariant under the transposition of the vertices  $n-1$  and  $n$ , and define  $\phi: A_n^T \rightarrow G_{n-1}$  by  $\phi(G)$  is the graph that remains after deleting the vertex  $n$  and all its incident edges from  $G$ . A little reflection shows that  $\phi$  is injective, and that  $\phi(A_n^T) = A_{n-1}$ .

Since  $|A_n \setminus A_n^T|$  is even,  $|A_n| \equiv |A_n^T| = |A_{n-1}| \pmod{2}$ . Since  $|A_0| = |A_1| = 1$ ,  $|A_n|$  is odd for each  $n \in \mathbb{N}$ . Hence "acyclic" is evasive, and so is its negation.  $\square$

EXAMPLE 5. *"The graph is transitive" is an evasive property for directed graphs.*

The proof runs completely similar to that of example 4.

---

\*) This result has been found independently by R.L. RIVEST (personal communication).

A *star* is a bipartite graph such that one part of the bipartition consists of a single vertex, called the *center* of the star. A star is called *maximal* if the bipartite graph is complete.

EXAMPLE 6. *"The graph is a star" is an evasive property for undirected graphs with at least three vertices.*

PROOF. Let  $n \in \mathbb{N}$  and  $P$  be the property to be considered. We evaluate the alternating sum  $F(P_n, -1)$ . Clearly, the center of a star is uniquely determined if the star has at least two edges. Hence

$$\begin{aligned} F(P_n, -1) &= 1 - n(n-1)/2 + n \cdot \sum_{k=2}^{n-1} \binom{n-1}{k} (-1)^k = \\ &= (n-1)(n-2)/2 \neq 0 \end{aligned}$$

for  $n \geq 3$ .  $\square$

EXAMPLE 7. *"The graph contains two disjoint edges" is an evasive property for undirected graphs with at least four vertices.*

PROOF. A graph which does not contain two disjoint edges is either a star, or a triangle. Therefore, the alternating sum for this property becomes

$$(n-1)(n-2)/2 - n(n-1)(n-2)/6 = -(n-1)(n-2)(n-3)/6. \quad \square$$

EXAMPLE 8. *"The graph is connected" is an evasive property for undirected graphs.*

(This was already proved in example 3.)

PROOF. Let  $P$  be the property "connected". Following GILBERT [2], formula (2), we have

$$T_{n+1}(X) = \sum_{k=0}^n \binom{n}{k} C_{k+1}(X) T_{n-k}(X),$$

where

$$T_n(X) = F(G_n, X) = (1+X)^{n(n-1)/2}, \quad C_n(X) = F(P_n, X).$$

For  $X = -1$  this yields

$$1 = C_1(-1),$$

$$0 = C_{n+1}(-1) + nC_n(-1) \text{ if } n \geq 1,$$

so

$$C_n(-1) = (-1)^{n-1}(n-1)! \text{ if } n \geq 1.$$

This is not zero, and therefore the property is evasive.  $\square$

EXAMPLE 9. *"The graph is strongly connected" is an evasive property for directed graphs.*

PROOF. Let  $P$  be the property "strongly connected". Then  $F(P_n, -1) = (n-1)!$  for  $n \geq 1$  (see e.g. BEST & SCHRIJVER [1]). Hence by corollary 1,  $P$  must be evasive.

EXAMPLE 10. *"The graph is bipartite" is an evasive property for directed graphs with at least three vertices.*

PROOF. This also follows by explicit computation of the alternating sum (cf. [1]).

EXAMPLE 11. *Let  $k$  be a natural number. Then the property "the graph has at most  $k$  non-isolated vertices" is evasive for undirected graphs with more than  $k$  vertices.*

PROOF. The contribution to the alternating sum of those graphs which have precisely  $m$  non-isolated vertices, can easily be seen to be a polynomial of degree  $m$  in  $n$ . Adding these contributions for  $0 \leq m \leq k$ , we derive that the alternating sum for the above property is a polynomial in  $n$  of degree  $k$ , say  $A(n)$ .

For  $n \leq k$  the property is trivial. Consequently  $A(0) = A(1) = 1$ , and  $A(m) = 0$  for  $2 \leq m \leq k$ . This completely determines the polynomial  $A$ . Moreover, by ROLLE's theorem, the derivative of  $A$  has a zero in between 0 and 1 and in between  $m$  and  $m+1$  for  $2 \leq m < k$ . This shows that  $A$  is strictly monotonic for  $x \geq k$  and consequently  $A(x)$  has no zeros for  $x > k$ .  $\square$

For graph properties theorem 4 can be sharpened to:

THEOREM 5. Let  $n \in \mathbb{N}$  and let  $P$  be a non-evasive graph property on  $G_n$ .  
Then

$$(1 / (e(1+X))) \frac{d}{dX} F(P,X)$$

and

$$(1 / (1+X)) (F(P,X) - (X/e) \frac{d}{dX} F(P,X))$$

are both enumerating polynomials in  $X$  of degree  $e - 2$ .

PROOF. We use the same notation as in the proof of theorem 3. Suppose the hider answers the first question affirmatively. Then, since it is immaterial which edge is asked for, we have

$$e N(P^{(1)}, k) = k N(P, k) ,$$

hence

$$\begin{aligned} F(P^{(1)}, X) &= \sum_{k=0}^e (k/e) N(P, k) X^k = \\ &= (X/e) \frac{d}{dX} F(P, X) . \end{aligned}$$

Similar to the proof of theorem 3 we find that both  $P^{(1)}$ , and  $G^{(1)} \setminus P^{(1)}$  are pairable. Hence  $F(P^{(1)}, X) / (1+X)$  and  $(X(1+X)^{e-1} - F(P^{(1)}, X)) / (1+X)$  are polynomials over  $\mathbb{N}$ . Since  $F(P^{(1)}, X)$  is divisible by  $X$ , it follows that  $F(P^{(1)}, X) / (X(1+X))$  as well as  $(1+X)^{e-2} - F(P^{(1)}, X) / (X(1+X))$  are polynomials over  $\mathbb{N}$ . This confirms the first assertion.

A negative answer from the hider on the first question leads to the second assertion.  $\square$

COROLLARY 3. Let  $n \in \mathbb{N}$  and let  $P$  be a graph property on  $G_n$ , such that  $F(P, X)$  is not divisible by  $(1+X)^2$ . Then  $P$  is evasive on  $G_n$ .

PROOF. If  $P$  were not evasive on  $G_n$  then both  $F(P, X)$  and its derivative would be divisible by  $1+X$ .  $\square$

COROLLARY 4. Let  $n \in \mathbb{N}$  and let  $P$  be a graph property on  $G_n$  such that  $|P|$  is not a multiple of 4. Then  $P$  is evasive on  $G_n$ .

## 5. THE ENUMERATION POLYNOMIAL OVER A FINITE FIELD

Up till now, the enumeration polynomial has been considered as an element of  $\mathbb{Z}[X]$ . It can be defined however as well over any arbitrary commutative ring  $R$  with unity. It is clear that for non-evasive properties  $P$  on  $G_n$  the relation  $(1+X) \mid F(P,X)$  holds in  $R[X]$  too. In this section we take for  $R$  the finite field  $\mathbb{F}_p$  of prime order  $p$ .

Let  $n \in \mathbb{N}$ , let  $P$  be a graph property on  $G_n$ , and let  $T$  be a subgroup of  $S_n$ , the group of all permutations of the vertices. Then we define:

$$G_n^T = \text{the collection of graphs in } G_n \text{ which are invariant under } T,$$

$$P^T = G_n^T \cap P.$$

Since there is a natural way to regard  $S_n$  as a subgroup of  $S_m$  when  $n < m$  it makes sense to speak of the graphs in  $G_m$  invariant under  $T \subset S_n$  when  $n < m$ .

THEOREM 6. *Let  $n \in \mathbb{N}$ ,  $p$  be a prime,  $P$  be a non-evasive graph property, and let  $T$  be a  $p$ -group contained in  $S_n$ . Then  $(1+X) \mid F(P^T, X)$  in  $\mathbb{F}_p[X]$ .*

PROOF. This relation trivially follows from theorem 4 and the congruence

$$N(P^T, k) \equiv N(P, k) \pmod{p}. \quad \square$$

COROLLARY 5. *Let  $n \in \mathbb{N}$ , let  $P$  be a property, and let  $T$  be a  $p$ -group contained in  $S_n$ , such that  $F(P^T, -1) \not\equiv 0 \pmod{p}$ . Then  $P$  is evasive on  $G_n$ .*

As a first application, we give a very simple proof that strong connectedness is evasive in case the number of vertices is a prime.

EXAMPLE 12. *"The graph is strongly connected" is an evasive property for directed graphs with a prime number of vertices. The same holds for "contains a Hamilton circuit" for both directed and undirected graphs with a prime number of vertices.*

PROOF. Let  $p$  be a prime and let  $T$  be the group generated by the cycle  $(1, 2, \dots, p)$  in  $S_p$ . Clearly each non-empty graph which is invariant under  $T$



is strongly connected (contains a Hamilton circuit). Consequently if we let  $P$  denote the property "is not strongly connected" ("does not contain a Hamilton circuit") then  $F(P_p^T, X) = F(\{E_p\}, X) = 1 \not\equiv 0 \pmod{p}$ .  $\square$

EXAMPLE 13. "The graph contains two adjacent edges" is an evasive property for undirected graphs with at least three vertices.

PROOF. First assume that  $n$  is odd. Let  $p$  be a prime divisor of  $n$ , and  $k = n/p$ . Let  $T$  be the group generated by the cycles  $(1, 2, \dots, p)$ ,  $(p+1, p+2, \dots, 2p)$ ,  $\dots$ ,  $((k-1)p+1, (k-1)p+2, \dots, kp)$ . Clearly every non-empty graph which is invariant under  $T$  contains two adjacent edges. Hence, denoting the negation of the considered property by  $P$ , we have

$$F(P_n^T, X) = F(\{E_n\}, X) = 1 \not\equiv 0 \pmod{p}.$$

If  $n$  is even, then we take  $p$  a prime divisor of  $n-1$ , and  $k = (n-1)/p$  and the same argument holds.  $\square$

## 6. AN APPLICATION OF THE PRINCIPLE OF INCLUSION AND EXCLUSION

Let  $P$  be a monotonic property on  $G$ . A graph  $G$  is called  $P$ -minimal if  $G$  has property  $P$  but no proper subgraph of  $G$  has it. The collection of  $P$ -minimal graphs is denoted by  $M(P)$ , so  $M(P_n) = M(P) \cap G_n$ .

THEOREM 7. Let  $n \in \mathbb{N}$  and let  $P$  be a monotonic, non-evasive property on  $G_n$ . Then

$$\sum_{J \in M(P), UJ=K_n} (-1)^{|J|} = 0.$$

PROOF. Let  $G \in M(P)$ . Then the contribution to  $F(P, X)$  of the graphs containing  $G$  as a subgraph equals  $X^{|G|} (1+X)^{e-|G|}$ .

By adding all these contributions, and using the principle of inclusion and exclusion, we arrive at:

$$F(P, X) = \sum_{J \in M(P), J \neq \emptyset} X^{|UJ|} (1+X)^{e-|UJ|} (-1)^{|J|-1}.$$

Hence

$$F(P, -1) = \sum_{J \in M(P), UJ = K_n} (-1)^{e+|J|-1},$$

which proves the theorem by corollary 1.  $\square$

EXAMPLE 14. *"The graph contains a maximal star" is an evasive property for undirected graphs containing at least two vertices.*

PROOF. The maximal stars themselves are the minimal graphs with this property. The coverings of  $K_n$  by maximal stars consist of either  $n-1$  or  $n$  elements. Consequently

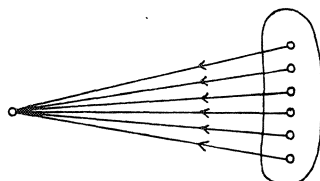
$$\sum_{J \in M(P_n), UJ = K_n} (-1)^{|J|} = \pm(n-1) \neq 0. \quad \square$$

## 7. EXAMPLES OF NON-EVASIVE PROPERTIES AND COUNTEREXAMPLES TO THE ORIGINAL ROSENBERG CONJECTURE

This section contains the example of a non-evasive property on directed graphs given by AANDERAA, and three new examples of non-evasive properties on undirected graphs. The AANDERAA example and the last undirected example are moreover counterexamples of the original ROSENBERG conjecture: The seeker needs at most a number of edges which depends linearly on the number of vertices. The three undirected examples were designed at the Advanced Study Institute on Combinatorics (Breukelen, the Netherlands, July 8-20, 1974) on which occasion the finding of such properties was raised by the authors as an open problem.

EXAMPLE 15. [AANDERAA] Let  $P$  be the property "The graph contains a sink". Then  $\mu(P_n) \leq 3n$ .

(A *sink* in a directed graph on  $n$  vertices is a vertex with indegree  $n-1$  and outdegree zero.)

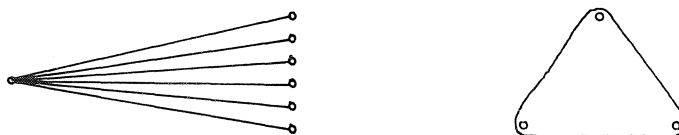


STRATEGY. At each stage of the game we call a vertex a *candidate sink* provided all incoming edges asked for have been given, whereas all outgoing edges asked for have been refused.

If the edge  $\langle i, j \rangle$  is given (refused) by the hider, then vertex  $i$  ( $j$ ) is ruled out as a candidate sink. This makes it possible for the seeker to reduce in  $n-1$  questions the set of candidate sinks, which contains initially all vertices, to a singleton. The verification that the last candidate sink is indeed a sink takes at most  $2(n-1)$  questions.  $\square$

REMARK. It is not difficult to prove that  $\mu(P_n) \leq 3n - \lceil 2 \log n \rceil - 3$  for  $n \geq 1$ . Actually we can show, by means of an information theoretical argument, that equality holds.

EXAMPLE 16. [L. CARTER] Let  $P$  be the property "The graph contains a vertex of valency  $n-4$  and the vertices adjacent to this vertex have valency 1". Then  $\mu(P_n) \leq \frac{1}{2}n(n-1) - 1$  for  $n \geq 9$ .

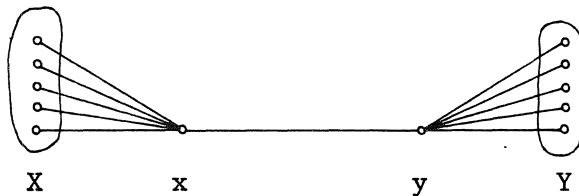


STRATEGY. The seeker divides the set of vertices in two about equal parts, and asks for all edges in between the two parts. This way he can identify, if  $n \geq 9$ , the vertex with valency  $n-4$  (or prove that no such vertex exists or that too many vertices have valency larger than one). Next he asks for all edges incident to this candidate, in this way isolating the three vertices not adjacent to it. At least one edge in between these three vertices

is not yet asked for, and, therefore,  $\mu(P_n) \leq \frac{1}{2}n(n-1) - 1$ .  $\square$

REMARK. By replacing  $n-4$  by e.g.  $4n/5$  in the above example one may produce an example where the number of edges that need not be asked for is a positive fraction of  $n^2$ .

EXAMPLE 17. [D. KLEITMAN] Let  $n$  be an even number and let  $P$  be the property "There are two adjacent vertices  $x$  and  $y$ , each of valency  $n/2$ , such that the sets of vertices in  $\{1, \dots, n\} \setminus \{x, y\}$  adjacent to  $x$  and  $y$ , called  $X$  and  $Y$  respectively, are disjoint, and such that no vertex in  $X$  is adjacent to a vertex in  $Y$ ". Then  $\mu(P_n) \leq 3/8 \cdot n^2 + 1/4 \cdot n - 1$ .



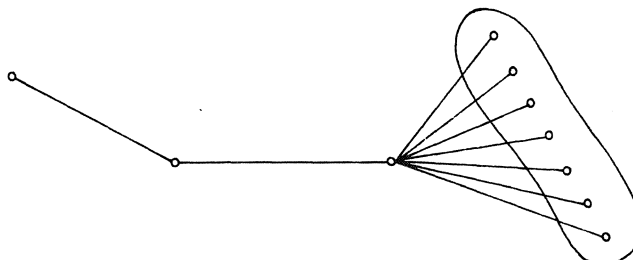
STRATEGY. The seeker selects at random some vertex and asks for all its incident edges. Next the seeker proceeds to one of the vertices adjacent to the first one, and asks for its incident edges. This way the seeker proceeds, always selecting a vertex adjacent to one, which he has investigated before. This way the seeker is able, before having investigated  $n/2 + 2$  vertices, either to isolate the vertices  $x$  and  $y$  and the sets  $X$  and  $Y$ , or to prove that the graph does not have the property. It is clear that, after having isolated  $x$ ,  $y$ ,  $X$ , and  $Y$  none of the vertices in between members of  $X$  or  $Y$  need to be probed. Moreover, no vertex in either  $X$  or  $Y$  has yet been investigated. Therefore, at least  $\frac{1}{2}(\frac{1}{2}n-1)(\frac{1}{2}n-2)$  edges need not be probed.  $\square$

REMARK. The property  $P$  may be extended to odd  $n$  as follows: if  $n$  is odd the graph  $G$  satisfies  $P_n$  if  $G$  consists of an isolated vertex  $n$  and a remaining graph on  $n-1$  vertices which satisfies  $P_{n-1}$  as defined above. Since the isolated vertex costs at most  $n-1$  questions, one has

$$\mu(P_n) \leq 3/8 \cdot n^2 + 1/2 \cdot n - 15/8.$$

A *scorpion graph* on  $n$  vertices contains a vertex  $b$  (the *body*) of valency  $n-2$ , a vertex  $t$  (the *tail*) of valency 1, and a vertex  $u$  of valency 2

which is adjacent to both  $t$  and  $b$ . The remaining  $n-3$  vertices form a set  $S$ , and edges in between members of  $S$  may be present or not.



EXAMPLE 18. If  $P$  is the property "The graph is a scorpion graph" then  $\mu(P_n) \leq 6n$ .

STRATEGY. At each stage of the game we call a vertex a *candidate body* (*candidate tail*) if at most one incident edge has been refused (given). The *weight* of a candidate body (tail) equals two minus the number of incident edges which have been refused (given). Hence a candidate has weight 2 or 1.

First the seeker asks for the edges  $(1,2)$ ,  $(2,3)$ ,  $\dots$ ,  $(n-1,n)$ , and  $(n,1)$ . In this way the set of all vertices is divided into three parts, viz.:

- B, consisting of candidate bodies of weight 2;
- T, consisting of candidate tails of weight 2;
- M, consisting of vertices with one incident edge given by the hider, and one refused.

By asking at most  $|M|$  more questions, such that each vertex in  $M$  is incident to three edges asked for, the seeker divides the set  $M$  into two subsets  $B_1$  and  $T_1$ , consisting of candidate bodies and candidate tails respectively, both of weight 1. At this stage of the game the sum of the weights of all the candidates does not exceed  $2|B|+2|T|+|B_1|+|T_1| = 2n-|M|$ .

Now the seeker asks for edges connecting candidate bodies to candidate tails, thus reducing with each question the sum of the weights by one. This part of the game, which takes at most  $2n-|M|$  questions, terminates when all edges in between the remaining candidate bodies and candidate tails have been asked for. We denote the number of remaining candidate bodies (tails) by  $\beta$  ( $\tau$ ). Since of the connecting edges at most  $\beta$  have been refused

and  $\tau$  have been given, one derives  $\beta + \tau \geq \beta\tau$ , and therefore  $\beta \leq 1$  or  $\tau \leq 1$  or  $\beta = \tau = 2$ .

If  $\beta = 0$  or  $\tau = 0$ , the seeker is ready. If  $\beta = 1$  or  $\tau = 1$ , then  $3n$  further questions are sufficient to determine the property. In case  $\beta = \tau = 2$ , the vertex  $u$  is easily seen to be among the candidate bodies. Now the seeker asks for all edges incident to both the candidate bodies, and then for those incident to the only candidate tail left (if present). This also takes at most  $3n$  questions.  $\square$

#### REFERENCES

- [1] BEST, M.R. & A. SCHRIJVER, *The enumeration of some properties of labelled graphs*, Math. Centre Report, ZW 32/74, Amsterdam 1974.
- [2] GILBERT, E.N., *Enumeration of labelled graphs*, *Canad. J. Math.*, 8 (1956), pp. 405-411.
- [3] HARARY, F., *Graph Theory*, Add. Wesley, 1969.
- [4] HOLT, R.C. & E.M. REINGOLD, *On the time required to detect cycles and connectivity in directed graphs*, *Math. Systems Theory*, 6 (1972), pp. 103-107.
- [5] HOPCROFT, J. & R. TARJAN, *Efficient planarity testing*, TR 73-165, Dept. of Computer Science, Cornell Univ. (April 1973).
- [6] KIRKPATRICK, D., *Determining graph properties from matrix representations*, Proc. 6<sup>th</sup> ACM Symp. on the theory of Computing, Seattle 1974, pp. 84-90.
- [7] LIPTON, R.J. & L. SNYDER, *On the AANDERAA-ROSENBERG conjecture*, SIGACT news, 6 (Jan. 1974).
- [8] ROSENBERG, A.L., *On the time required to recognize properties of graphs: a problem*, SIGACT news, 5 (Oct. 1973).



