ON THE TIME REQUIRED TO RECOGNIZE PROPERTIES
OF GRAPHS FROM THEIR ADJACENCY MATRICES

by
Ronald L. Rivest and Jean Vuillemin

Memorandum No. ERL-M476

November 1974

ELECTRONICS RESEARCH LABORATORY

College of Engineering
University of California, Berkeley
94720
ON THE TIME REQUIRED TO RECOGNIZE PROPERTIES
OF GRAPHS FROM THEIR ADJACENCY MATRICES†

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

and

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

November 1974

Abstract

Let \( P \) be any non-trivial monotone property which applies to the class of \( v \)-vertex graphs. We show that, if graphs are represented by adjacency matrices, any algorithm for deciding if \( P \) holds or not of a given graph must, in the worst case, take time proportional to \( v^2 \). This provides a positive answer to the question raised by Aanderaa and Rosenberg in [5].

†This work was supported in part by National Science Foundation Grants GJ-43318 and DCR-74-07644-A01.
I. Introduction

Trying to relate the computational complexity of graph properties to the data-structure chosen for representing graphs is a natural and important question. Despite its many mathematical advantages, the adjacency matrix representation of graphs does not appear to be a good choice, if one is expecting to produce graph algorithms whose running time is faster than $\Omega(v^2)$, $v$ being the number of vertices (nodes) in the graph.

It has been conjectured by Aanderaa and Rosenberg in [5] that recognizing if a $v$-vertex graph has any particular non-trivial monotone property from its adjacency matrix requires, in the worst case, on the order of $v^2$ operations. A graph property $P$ is nontrivial if adding edges to a graph where $P$ holds does not make $P$ false; it is non-trivial if $P$ holds of the complete graph $K_v$ and does not hold of its complement $E_v = \overline{K}_v$, the empty graph.

In this paper, we provide a proof of the validity of Aanderaa-Rosenberg's conjecture.

II. Notations for Graphs and Groups

Before attempting to establish any result, we need to set up some notations and definitions. We shall usually conform to traditional usage, as defined by Biggs [2] and Harary [3] for example, although this has not always been possible.

\[ f(v) = \Omega(g(v)) \text{ means } g(v) = O(f(v)), \text{ i.e., there exists } K > 0, \text{ for all } v, \ f(v) \geq Kg(v); \text{ it is the natural inverse of the "big-oh" notation.} \]
2.1. Graphs

A \textit{v-graph} or \textit{graph} $G$ (finite undirected labelled graph without
self-loops or multiple edges) is a pair $(V(G), E(G))$ where $V(G)$ is
a finite set of vertices, labelled 1 through $v = |V(G)|$, and
$E(G) \subseteq V(G)^2$ is a subset of $V(G)^2 = \{\{i,j\} | \ 1 \leq i,j \leq v, \ i \neq j\}$ of the
symmetric cartesian product $V(G) \times V(G)$. Elements of $E(G)$ are edges
and, if $e = \{u,v\} \in E(G)$, we say that $e$ \textit{joins} $u$ and $v$. For
example, the complete v-graph $K_v$ has $v = |V(K_v)|$ and $E(K_v) = V(K_v)^2$;
it is composed of $v$ vertices and $\frac{1}{2}v(v-1)$ edges. Its \textit{complement}, the
empty v-graph $E_v = \overline{K_v}$ has $E(E_v) = \emptyset$; the complement $\overline{G}$ of a graph
$G$ is the graph $(V(G), V(G)^2 - E(G))$.

Two v-graphs $G_1$ and $G_2$ are isomorphic if there exists a permuta-
tion $\sigma$ of $\{1, \ldots, v\}$ such that $\{\sigma(u), \sigma(v)\} \in E(G_2)$ if and only
if $\{u,v\} \in E(G_1)$. Graph isomorphism, denoted $G_1 \cong G_2$, is an equiva-
lence relation over the class of v-graphs. An unlabelled graph is an
equivalence class of graphs under isomorphism.

Graph $G_1$ is a subgraph of $G_2$, denoted $G_1 \subseteq G_2$, if there exists
$G'_1 \subseteq G_1$ such that $V(G'_1) = V(G_2)$ and $E(G'_1) \subseteq E(G_2)$. Relation $\subseteq$ is
a partial ordering of v-graphs; it has a minimal element $E_v$ and a
maximal element $K_v$.

The adjacency matrix $M(G) = [m_{i,j}]$ of a v-graph $G$ is a symmetric
$v \times v$ boolean matrix such that $m_{i,j} = 1$ if and only if $\{i,j\} \in E(G)$.
Two v-graphs $G_1$ and $G_2$ are isomorphic $G_1 \cong G_2$ if and only if there
exists a permutation matrix $P$ such that $M(G_1) = P^{-1}M(G_2)P$.

Consider $G_1$ a $v_1$-graph and $G_2$ a $v_2$-graph. Their sum $G_1 + G_2$
is the $(v_1 + v_2)$-graph $G$ formed by placing a $v_1$-graph $G_1$ and a
$v_2$-graph $G_2$ side by side, i.e., $\{i,j\} \in E(G)$ if and only if
(1 \leq i,j \leq v_1 \text{ and } \{i,j\} \in E(G_1)) \text{ or } (v_1 < i,j \leq v_1 + v_2 \text{ and } \\
\{i-v_1,j-v_1\} \in E(G_2))$. The product $G_1 \times G_2$ is obtained from the sum $G_1 + G_2 \text{ by joining every vertex in } G_1 \text{ to every vertex in } G_2$, i.e., $E(G_1 \times G_2) = E(G_1 + G_2) \cup \{\{i,j\} \mid 1 \leq i \leq v_1 < j \leq v_1 + v_2\}$. Clearly, $G_1 + G_2 \leq G_1 \times G_2$ and $G_1 + G_2 = \overline{G}_1 \times \overline{G}_2$; also, $E_n + E_m = E_{n+m}$ while $K_n \times K_m = K_{n+m}$. We denote by $K_{n,m} = E_n \times E_m$ the complete $(n,m)$-bipartite graph. A graph $G$ is bipartite if and only if $G \leq K_{n,m}$ for some $n, m \geq 1$.

2.2. Groups

In order to minimize confusion, we use Greek letters for groups and permutations. If $\Gamma$ is a permutation group on $\{1, \ldots, d\}$, we say that $d$ is the degree of $\Gamma$ and we denote by $|\Gamma|$ the size of $\Gamma$. If $\Gamma_1$ and $\Gamma_2$ are two permutation groups of degree $d$, $\Gamma_1 \leq \Gamma_2$ means that $\Gamma_1$ is a subgroup of $\Gamma_2$. We use $<$ for proper inclusion, and denote by $\Sigma_d$ the symmetric group of degree $d$ and order $|\Sigma_d| = d!$.

Let $\Gamma_1$ and $\Gamma_2$ be two permutation groups of degrees $d_1$ and $d_2$ respectively. The sum $\Gamma_1 + \Gamma_2$ is the group of degree $d_1 + d_2$ and order $|\Gamma_1 + \Gamma_2| = |\Gamma_1| \cdot |\Gamma_2|$ resulting from the action

$$(\sigma_1 + \sigma_2)(i) = \begin{cases} 
\sigma_1(i) & \text{if } 1 \leq i \leq d_1 \\
\sigma_2(i-d_1 + d_1) & \text{if } d_1 < i \leq d_1 + d_2
\end{cases}$$

for $\Gamma_1$ and $\Gamma_2$ on $\{1, \ldots, d_1 + d_2\}$. The product $\Gamma_1 \times \Gamma_2$ is the group of degree $d_1 \times d_2$ and order $|\Gamma_1| \cdot |\Gamma_2|$ resulting from the action

$$(\sigma_1 \times \sigma_2)<i,j> = <\sigma_1(i), \sigma_2(j)> \text{ with } 1 \leq i \leq d_1, \ 1 \leq j \leq d_2,$$

$\sigma_1 \in \Gamma_1$ and $\sigma_2 \in \Gamma_2$, of $\Gamma_1$ and $\Gamma_2$ on $\{1, \ldots, d_1\} \times \{1, \ldots, d_2\}$.
If $\Gamma$ is a permutation group on $\{1,\ldots,d\}$, the pseudo-square $|\Gamma|^{2}$ is the permutation group of degree $\frac{1}{2}d(d-1)$ and order $|\Gamma|^{2} = |\Gamma|$ resulting from the action $\sigma([i,j]) = \{\sigma(i),\sigma(j)\}$ for $1 \leq i,j \leq d$ and $\sigma \in \Gamma$ of $\Gamma$ over $\{1,\ldots,d\}$. If $|\Gamma| > 1$, then $|\Gamma|^{2} < |\Gamma \times \Gamma|$.

A permutation group $\Gamma$ on $\{1,\ldots,d\}$ is transitive if the orbit $i.\Gamma = \{j \mid 1 \leq j \leq d, \exists \sigma \in \Gamma: j = \sigma(i)\}$ of any $i \in \{1,\ldots,d\}$ in $\Gamma$ has size $|i.\Gamma| = d$, i.e., $i.\Gamma = \{1,\ldots,d\}$. For example, $\Sigma_{d}$ and $\Sigma_{d}^{2}$ are both transitive. If $\Gamma$, $\Gamma_{1}$ and $\Gamma_{2}$ are transitive, $\Gamma_{1} \times \Gamma_{2}$ is also transitive but $|\Gamma|^{2}$ is not transitive in general.

An automorphism of a graph $G$ is an isomorphism of $G$ with itself. The set of automorphisms of a $v$-graph $G$ is a permutation group

\[\Gamma(G) = \{\sigma \in \Sigma_{v} \mid \{i,j\} \in E(G) \iff \{\sigma(i),\sigma(j)\} \in E(G)\}\]

called the automorphism group or the point group of $G$. The automorphisms of $G$ also induce a permutation group $|\Gamma(G)|^{2}$ on the edges (lines) of $G$, called the line group of $G$. For example

\[\Gamma(K_{v}) = \Gamma(E_{v}) = \Sigma_{v}
\]

and

\[|\Gamma(K_{v})|^{2} = |\Gamma(E_{v})|^{2} = \Sigma_{v}^{2}\];

\[\Gamma(K_{m,n}) = \Sigma_{m} + \Sigma_{n} \quad \text{and} \quad |\Gamma(K_{m,n})|^{2} = \Sigma_{m} \times \Sigma_{n} \quad \text{if} \quad n \neq m\,.
\]

In general $\Gamma(G) = \Gamma(G)_{G}$.

2.3. Symmetric Graphs

Graph $G$ is point-symmetric (respectively line-symmetric) if $\Gamma(G)$ (respectively $|\Gamma(G)|^{2}$) is transitive. If $G$ is both line and point symmetric, we say that graph $G$ is symmetric. For example, $E_{v}$, $K_{v}$ and $K_{v,v}$ are symmetric. If $n \neq m$, $K_{n,m}$ is line symmetric but not point symmetric, while $(K_{n}^{+}K_{n}) \times (K_{n}^{+}K_{n})$ is point symmetric but not line symmetric for $n > 1$. If $G$ is symmetric, $G + G$ is also symmetric;
if \( G \) is point symmetric, so are \( \overline{G} \), \( G+G \) and \( G \times G \).

We now define a family of symmetric graphs which will be useful later on. Let \( v = 2^p \), where \( p \) is a non-negative integer.

**Definition D1:** For each \( 0 \leq i \leq p \), the graphs \( \bar{B}^i_p \) are defined by:

1. \( \bar{B}^i_p = K^v \) with \( v = 2^p \);
2. \( \bar{B}^i_p = \bar{B}^{i-1}_p + \bar{B}^{i-1}_p \) for \( 0 \leq i < p \).

For example, \( \bar{B}^0_p = \cdot \), \( \bar{B}^1_p = | | \), \( \bar{B}^2_p = \Box \Box \), etc. In general, \( \bar{B}^i_p \) consists of \( 2^{p-i} \) copies of \( K^{2^i} \). It is easy to establish that these graphs have the following properties:

**Lemma 1:** The family \( \{ \bar{B}^i_p | 0 \leq i \leq p \} \) of graphs defined by D1 has the properties:

(a) \( E^p_v = \bar{B}^0_p \) and \( K^v = \bar{B}^p_p \) with \( v = 2^p \);
(b) \( \bar{B}^i_p < \bar{B}^{i+1}_p \) for \( 0 \leq i < p \);
(c) \( \bar{B}^i_p \) is symmetric;
(d) \( \bar{B}^{i+1}_p < \bar{B}^i_p \times \bar{B}^i_p \) for \( 0 \leq i < p \).

### III. The Argument Complexity of Boolean Functions

#### 3.1. Monotone Non-trivial Properties

Let \( \{0,1\}^d \) represent the set of all (boolean) \( d \)-tuples over \( \{0,1\} \). For any two elements \( \overline{x} = <x_1, \ldots, x_d> \) and \( \overline{y} = <y_1, \ldots, y_d> \) of \( \{0,1\}^d \), we write \( \overline{x} \preceq \overline{y} \) whenever \( x_i \leq y_i \) for all \( 1 \leq i \leq d \). For example, a \( v \)-graph \( G \) can be represented by a boolean vector \( g \in \{0,1\}^d \) with

\[
d = \frac{1}{2}v(v-1),
\]

where \( g \) is the upper non-diagonal part of the adjacency matrix \( M(G) \) of \( G \). If another \( v \)-graph \( G' \) is represented in a similar fashion \( g' \), then \( G \succeq G' \) if and only if \( g \preceq cg' \) for some \( c \in \Sigma_{v}^{1} \); similarly, \( G \preceq G' \) if and only if \( g \preceq cg' \) for some \( c \in \Sigma_{v}^{2} \).
Consider a boolean function (property) \( P : \{0,1\}^d \rightarrow \{0,1\} \) mapping the set of boolean \( d \)-tuples into \( \{0,1\} \). If \( \vec{x} \leq \vec{y} \) implies \( P(\vec{x}) \leq P(\vec{y}) \) for all \( \vec{x}, \vec{y} \in \{0,1\}^d \), we say that \( P \) is monotone. We denote by \( M_d = \{ P : \{0,1\}^d \rightarrow \{0,1\} | \text{P monotone, } P(0) = 0, P(1) = 1 \} \) the class of monotone non-trivial properties. "Property" will now mean "monotone non-trivial boolean property".

We say that property \( P \in M_d \) with \( d = \frac{1}{2}v(v-1) \) is "invariant under graph isomorphism", or simply that "\( P \) is a \( v \)-graph property" if, for any \( g \in \{0,1\}^d \) and \( \sigma \in \Sigma_v \), \( P(g) = P(\sigma(g)) \). This boolean vector \( g \in \{0,1\}^d \) can be regarded as the upper non-diagonal part of the adjacency matrix \( M(G) \) of some \( v \)-graph \( G \). We write \( P(G) \) rather than \( P(g) \) or \( P(M(G)) \); this notation however means that graph \( G \) is represented as a boolean vector of \( \frac{1}{2}v(v-1) \) entries. The class of \( v \)-graph properties is denoted by \( P_v = \{ P \in M_d | d = \frac{1}{2}v(v-1), P \) is a \( v \)-graph property\}.

To any property \( P \in M_d \), we can associate a permutation group \( \Gamma(P) = \{ \sigma \in \Sigma_n | \forall \vec{x} \in \{0,1\}^d : P(\vec{x}) = P(\sigma(\vec{x})) \} \) which is the maximal group of permutation of the argument positions leaving \( P \) invariant. For example, \( P \) is a \( v \)-graph property if it is invariant under graph-isomorphism, i.e., \( \Sigma_v \leq \Gamma(P) \).

Similarly, we say that \( P \) is an \((m,n)\)-bipartite property if \( \Sigma_m \times \Sigma_n \leq \Gamma(P) \); the class of \((m,n)\)-bipartite properties is denoted by \( P_{m,n} = \{ P \in M_{m \times n} | \Sigma_m \times \Sigma_n \leq \Gamma(P) \} \).

3.2. Algorithms and Complexity of Properties

An algorithm for evaluating \( P(x_1, \ldots, x_d) \) with \( P \in M_d \) must examine some of the individual arguments \( x_i \), since \( P \) is non-constant.
On any reasonable model of machine, the number of arguments which need to be examined determines a lower bound on the execution time of the algorithm. In order to formalize this idea, we define a decision-tree \( T \) for property \( P \) to be a binary tree whose internal nodes specify arguments to be tested and external nodes are marked according to the appropriate value of \( P \).

For example, if \( P \) is the 3-graph property, \( P(G) \equiv \text{"3-graph } G \text{ is connected"} \), the following is a decision tree for \( P \), where \( \{i,j\} \) in an internal node means the algorithm is to test the entry \( m_{i,j} \) of \( M(G) \).

\[
T = \begin{array}{c}
\{1,2\} \\
\{1,3\} \\
\{2,3\} \\
\{1,3\}
\end{array}
\begin{array}{c}
=0 \\
=0 \\
=0 \\
=0
\end{array}
\begin{array}{c}
=1 \\
=1 \\
=1 \\
=1
\end{array}
\begin{array}{c}
P=0 \\
P=1 \\
P=0 \\
P=1
\end{array}
\[
\begin{array}{c}
P=0 \\
P=1 \\
P=0 \\
P=1
\end{array}
\]

Figure 1

In general, we denote by \( c(T, \overline{x}) \) the number of tests made in determining \( P(\overline{x}) \) according to the decision tree \( T \). For example, if graphs \( G_1 \) and \( G_2 \) are given respectively by the adjacency matrices

\[
M(G_1) = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix} \quad \text{and} \quad M(G_2) = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix},
\]

then \( c(T, G_1) = 2 \) and \( c(T, G_2) = 3 \).

The maximum number of tests made, \( \max_{\overline{x} \in \{0,1\}^d} c(T, \overline{x}) \), or, equivalently, the maximum depth of the tree representation of \( T \) will be our measure
of the cost of a particular decision tree $T$. The argument complexity $C(P)$ of property $P$ will be the cost of the cheapest decision tree $T$ for $P$:

**Definition D2:** The argument complexity $C(P)$ of property $P$ is defined by:

$$C(P) = \min_{T \text{ a decision-tree for } P} \max_{\bar{x} \in \{0,1\}^d} \{c(T,\bar{x})\}.$$ 

As mentioned earlier, the argument complexity of property $P$ is a lower bound on the time complexity of $P$. If $E \subseteq M_d$ is a class of properties, the complexity $C(E) = \min_{P \in E} \{C(P)\}$ is the minimum complexity of properties in the class. We are interested in graphs and bipartite properties:

**Definition D3:** We denote by $F(v)$ and $F(n,m)$ respectively the complexity of the classes of $v$-graph and $(n,m)$-bipartite properties, i.e., $F(v) = \min_{P \in P_v} \{C(P)\}$ and $F(n,m) = \min_{P \in P_{n,m}} \{C(P)\}$.

In general, if a class of functions is defined by an invariance permutation group,

**Definition D4:** The complexity $C(\Gamma)$ of a permutation group is the least complexity

$$C(\Gamma) = \min_{\{P \in M_d \mid \Gamma \leq \Gamma(P)\}} \{C(P)\} \text{ of properties } P \text{ left invariant by } \Gamma.$$

Using this notation gives $F(v) = C(\Sigma_v^2)$ and $F(n,m) = C(\Sigma_m \times \Sigma_n)$.
It follows directly from (D4) that \( \Gamma_1 \leq \Gamma_2 \) and \( \deg(\Gamma_1) = \deg(\Gamma_2) \) implies \( C(\Gamma_1) \leq C(\Gamma_2) \). It is an easy exercise to show for example that \( C(\Sigma_d) = d \).

In [4], Rivest and Vuillemin have shown that:

**Theorem 1:** If the permutation group \( \Gamma \) is transitive and has degree \( d = q^\alpha \) a prime power, then \( C(\Gamma) = d \).

This result has no direct implication as to the complexity of graph properties since the degree \( \frac{1}{2}v(v-1) \) of \( \Sigma_v^2 \) is never a prime power unless \( v = 2 \) or 3. For bipartite properties however, we obtain \( F(q, q^\beta) = q^{\alpha+\beta} \) for any prime \( q \) and \( \alpha, \beta \in \mathbb{N} \) as a corollary. The rest of the paper describes a way to embed some forms of bipartite properties into graph properties, so as to show \( F(v) \geq Kv^2 \) for some constant \( K \).

**IV. Proof of the Main Theorem**

4.1. **Embedding Technique**

The general idea is to extract a subset of the entries in the adjacency matrix, and "give away" the other entries. We must keep enough symmetry into the problem so that \( \Sigma_v^2 \) acts transitively on the chosen subset and we can apply Theorem 1 in order to get \( F(v) \geq Kv^2 \). More precisely, we use:

**Lemma 2:** Let \( P \in P_v \) be a \( v \)-graph property, \( G_1 \) and \( G_2 \) a \( v_1 \)- and \( v_2 \)-graph respectively, with \( v_1 + v_2 = v \). If \( P(G_1 + G_2) = 0 \) and \( P(G_1 \times G_2) = 1 \), then \( C(P) \geq C(\Gamma(G_1) \times \Gamma(G_2)) \).

**Proof:** Let \( E_0 \) denote those edges in \( G_1 \times G_2 \) but not in \( G_1 + G_2 \), i.e. \( E \) is the set of edges joining vertices in \( G_1 \) with vertices in \( G_2 \).
and is a subset of $E(K_{v_1,v_2})$:

$$E_0 = \{(i,j) \mid 1 \leq i \leq v_1 < j \leq v_1 + v_2 \text{ where } v_1 = |V(G_1)|, v_2 = |V(G_2)|\}.$$ 

Consider the function $P'$, a restriction of $P$, mapping subsets $S$ of $E_0$ into $\{0,1\}$ defined by:

$$P'(S) = P(G), \text{ with } G = (V(G_1 + G_2), E(G_1 + G_2) \cup S).$$

By hypothesis, $P'$ is a nontrivial, monotone function of $S$, since $E(G_1 + G_2) \cup E_0 = E(G_1 \times G_2)$. By the definition of $P'$ it follows that $C(P') \leq C(P)$, since any decision tree for $P$ can also be used for $P'$ ($P'$ is just $P$ on a restricted domain).

It remains to show that $C(P') \geq C(\Gamma(G_1) \times \Gamma(G_2))$ by showing $\Gamma(P') \geq \Gamma(G_1) \times \Gamma(G_2)$. Now $P$ is left invariant by $\Gamma(P) \geq \Sigma_v |2|$, thus also by the subgroup $\Gamma'$ of $\Sigma_v |2|$ which fixes $E(G_1 + G_2)$. But $\Gamma' \geq (\Gamma(G_1) + \Gamma(G_2)) |2|$ (acting on $(V(G_1) \cup V(G_2)) |2|$), which contains the subgroup $\Gamma(G_1) \times \Gamma(G_2)$ acting on $E_0$. □

In order to apply Theorem 1, we need that $\Gamma(G_1) \times \Gamma(G_2)$ be transitive and $v_1 \times v_2$ be a prime power. As noticed earlier, it is sufficient, in order for $\Gamma(G_1) \times \Gamma(G_2)$ to be transitive, that $\Gamma(G_1)$ and $\Gamma(G_2)$ be both transitive, i.e., that $G_1$ and $G_2$ be point symmetric. For the requirement $v_1 \times v_2$ is a prime power, we first consider $v$-graphs where $v$ is a power of 2.

4.2. Graphs of Size $2^p$

Using Lemma 2, it is now easy to prove

**Lemma 3:** If $v = 2^p$, $p \geq 1$, then $P(v) \geq \frac{2}{4} v^2$. 

Proof: Consider the graphs $B^i_p$ for $0 \leq i \leq p$ defined by (D1). Any graph property $P \in P_v$ must be such that $0 \leq i \leq j$ implies $P(B^i_p) = 0$ and $j < i \leq p$ implies $P(B^i_p) = 1$ for some $j$ such that $0 \leq j < p$ (this follows from monotonicity of $P$ and Lemma 1, (a) and (b)). In particular, $P(B^j_p) = P(B^{j}_{p-1} + B^j_{p-1}) = 0$ and $P(B^{j+1}_p) = 1$.

Since we proved in Lemma 1, (d) that $B^{j+1}_p \leq B^j_p \times B^j_p$, and $P$ is monotone, $P(B^{j+1}_{p-1} \times B^j_{p-1}) = 1$. Applying Lemma 2 then yields $C(P) > C(T(B^{j}_{p-1}) \times T(B^j_{p-1}))$. As noticed in Lemma 1, (c), graph $B^j_{p-1}$ is symmetric, therefore $T(B^j_{p-1}) \times T(B^j_{p-1})$ is transitive. Since the degree of this group is $2^{p-1} \times 2^{p-1} = 4^{p-1}$ which is a prime power, Theorem 1 gives us $C(P) > \frac{1}{4}v^2$. This bound is valid for any $P \in P_v$, thus $F(v) > \frac{1}{4}v^2$. 

This proves $F(v) \geq Kv^2$ for $v = 2^p$ a power of two. The construction can be adapted (at some cost) to powers of 3, and prime powers in general. What to do with numbers $v$ which are not prime powers is not clear however. Instead of following this approach, we shall prove that $F(v)$ is more or less increasing with $v$, thus obtaining $F(v) > K'v^2$ for all $v$, the constant $K'$ being lower than the one ($K = \frac{1}{4}$) which applies for $v = 2^p$ a power of two.

4.3. General Case

Proving directly that $F(v) \geq F(v-1)$ is not easy, no matter how intuitively obvious this appears to be. We prove the following weaker result, which will be sufficient for our purposes:

As a matter of fact, this question is unresolved as far as the authors are concerned. This might not be much simpler than proving $F(v) = \frac{1}{2}v(v-1)$. 

\[\frac{1}{2}v(v-1)\]
Lemma 4: For all $v \in \mathbb{N}$,

$$F(v) \geq \min(F(v-1),2^{2K-2})$$

where $2^K \leq v < 2^{K+1}$.

Proof: For an arbitrary property $P \in \mathcal{P}_v$, one of three cases holds:

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

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

(iii) neither of the above.

Cases (i) and (ii) imply that $F(v) \geq F(v-1)$ directly, since we may induce a function $P' \in \mathcal{P}_{v-1}$ from $P$ by suitably restricting the domain: $P'(G) = P(K_{1} + G)$ in case (i) and $P'(G) = P(K_{1} \times G)$ in case (ii). In either case $P'$ is a monotone nontrivial graph property.

In case (iii), using $u$ to denote $2^{K-1}$ and $r$ to denote $v-2u$, we have

$$P((K_u \times K_r) + E_u) = 0 \text{ since } P(K_{1} + K_{v-1}) = 0$$

and

$$((K_u \times K_r) + E_u) \leq K_1 + K_{v-1}; \text{ and }$$

$$P((K_r + E_u) \times K_u) = 0 \text{ since } P(K_1 \times E_{v-1}) = 1$$

and

$$((K_r + E_u) \times K_u) \geq K_1 \times E_{v-1}. $$

The function $P'$ defined as $P$ restricted to those edges between $K_u$ and $E_u$ satisfies all the requirements of Theorem 1: We have just shown that it is nontrivial, it is monotone since it is a restriction of the monotone function $P$, and it is invariant under the action of $\Sigma_u \times \Sigma_u$, acting on the vertices of $K_u$ and $E_u$, a transitive group. Since $C(P) \geq C(P')$ and $P'$ is exhaustive, this proves the lemma. $\square$
Combining lemmas 3 and 4 yields directly:

**Theorem 4:** If $P$ is a nontrivial monotone graph property of $v$-graphs, then

$$C(P) > \frac{v^2}{16}.$$ 

**Proof:** If $v = 2^K + r$ with $0 \leq r < 2^K$, then lemmas 3 and 4 give

$$C(P) \geq 2^{2K-2} \geq \frac{v^2}{16}.$$  

Of course, this result also applies to other classes of graphs, directed, or multi-edges. It can be used directly as a lower bound, or the construction can be adapted so as to improve the constant.

**V. Conclusion**

The tantalizing remaining question is the exact value of $F(v)$. It is widely conjectured that $F(v) = \frac{1}{2}v(v-1)$ and this has been proved in [4] for $v = 1,2,4,5,7,11,13$. This is part of a more general problem discussed in [4]: Is it true that any transitive permutation group $\Gamma$ of degree $d$ has complexity $C(\Gamma) = d$? The results of the paper indicate that it might be easier to prove the existence of a constant $K$ such that any transitive $\Gamma$ of degree $d$ has $C(\Gamma) \geq Kd$. 

![Figure 2](image-url)
The monotonicity requirement is also discussed in [4] and, in fact, there is nothing to stop us from believing that $C(P) > K^2_v$ for any (monotone or non-monotone) $v$-graph property, provided $P(E_v) \neq P(K_v)$.

References


†A complete bibliography on the problem can be found in [4].