On the Minimum Order of Graphs with Given Automorphism Group*

By

Gert Sabidussi, New Orleans, La., USA.

(*Received May 16, 1958*)

1. Introduction

Given a finite group G define $\alpha(G)$ to be min $\alpha_0(X)$, the minimum taken over all graphs X whose automorphism group $G(X)$ is isomorphic to G ($\alpha_0(X)$ denotes the number of vertices of X). By a *graph* X we mean a *finite* set $V(X)$ (the set of *vertices* of X) together with a set $E(X)$ (the set of *edges* of X) of unordered pairs of *distinct* elements of $V(X)$. We shall indicate unordered pairs by brackets. The automorphism group of a graph X, i. e. the group of all one-one functions φ of $V(X)$ onto $V(X)$ such that $[x, y] \varepsilon E(X)$ implies $[\varphi x, \varphi y] \varepsilon E(X)$, will be denoted by $G(X)$.

It is known ([1], p. 377) that

$$\alpha(G) = O(mn),$$

where m is the order of G, and n is the minimal number of generators of G. More precisely, $\alpha(G) \leqq 2\,mn$, if $n \geqq 2$. By refining the method of [1] we shall prove:

Theorem 1: $\alpha(G) = O(m \log n)$.

In view of the fact that $n = O(\log m)$ (cf. [1], p. 378) we have: *Corollary*: $\alpha(G) = O(m \log \log m)$.

The proof consists of constructing a graph X such that $G(X) \cong G$, and $\alpha_0(X) = O(m \log n)$. Concerning the construction of X two facts should be emphasized. First, our method always yields a result of the form $\alpha(G) \leqq m\, f(n)$. Hence, no matter how effectively $f(n)$ can be improved upon, one cannot hope to obtain anything like a best possible

* Written with the support of the National Science Foundation of the United States of America.

estimate (for the symmetric group S_m of order $m!$, $\alpha(S_m) = m$, while our method gives $\alpha(S_m) \leqq m!\, f(2)$). Second, it appears that the result $f(n) = O(\log n)$ cannot be further refined in any substantial way; for instance, it seems to be impossible to obtain $f(n) = O(\log \log n)$.

In the simple case that G is the cyclic group Z_m of order m it is known ([1], p. 371) that $\alpha(Z_3) \leqq 10$, and $\alpha(Z_m) \leqq 3\,m$ if $m \geqq 4$.
With little effort one obtains:

Theorem 2:

$$\alpha(Z_m) = \begin{cases} 2, & \text{if } m = 2 \\ 3\,m, & \text{if } m = 3, 4, 5 \\ 2\,m, & \text{if } m = p^e \geqq 7, \text{ where } p \text{ is prime} \\ \alpha(Z_{p_1^{e_1}}) + \ldots + \alpha(Z_{p_r^{e_r}}), & \text{if } m = p_1^{e_1} \ldots p_r^{e_r}, \\ \text{where } p_1, \ldots, p_r \text{ are distinct primes.} \end{cases}$$

2. Proof of Theorem 1

Let w be a given positive integer. By $M_1, \ldots, M_r$, $r = 2^w - 1$, denote the non-empty subsets of the set $M = \{1, \ldots, w\}$, and form all products $M_{i_k} \times M_{j_k}$, $1 \leqq i_k \leqq r$, $1 \leqq j_k \leqq r$, $k = 1, \ldots, r^2$. Given a finite group G of order m, let w be the smallest positive integer for which $r^2 \geqq n$, where n is the minimum number of generators of G. Clearly $w = O(\log n)$.

Now let $\{h_1, \ldots h_n\}$ be a set of generators of G, and define a graph X as follows:

$$V(X) = \{(g, i) \mid g \varepsilon G, 0 \leqq i \leqq w\} \cup \{(g, i') \mid g \varepsilon G, 0 \leqq i \leqq w + 1\},$$

$$\begin{aligned} E(X) = \; & \{[(g, i), (g, i')] \mid g \varepsilon G, 0 \leqq i \leqq w\} \cup \\ & \{[(g, i-1), (g, i')] \mid g \varepsilon G, 1 \leqq i \leqq w + 1\} \cup \\ & \{[(g, 0), (g', 1)], [(g, 1), (g', 1)], [(g, (w+1)'), (g', (w+1)')] \mid \\ & g \varepsilon G, g' = g h_k, \; 1 \leqq k \leqq n\} \cup \\ & \{[(g, x), (g', y)] \mid g \varepsilon G, g' = g h_k, (x, y) \varepsilon M_{i_k} \times M_{j_k}, 1 \leqq k \leqq n\}. \end{aligned}$$

Note that $\alpha_0(X) = m(2\,w + 3) = O(m \log n)$. It remains to prove that $G(X) \cong G$. For any $g' \varepsilon G$ define $\varphi_{g'}: V(X) \to V(X)$ by $\varphi_{g'}(g, x) = (g'\, g, x)$, $g \varepsilon G$. Then clearly $G' = \{\varphi_{g'} \mid g' \varepsilon G\}$ is a subgroup of $G(X)$ isomorphic to G.

It is immediate from the definition of X that each $(g, 0')$, $g \varepsilon G$, is of degree 1; (g, x'), where $g \varepsilon G$, $x = 1, \ldots, w + 1$, is of degree 2; all other vertices of X are of degree $\geqq 2$. Let $\varphi \varepsilon G(X)$. Then $\varphi(g, 0')$ is of degree 1; hence $\varphi(g, 0') = (g', 0')$ for some $g' \varepsilon G$. $(g, 0)$ is the only vertex of X joined with $(g, 0')$. Likewise, $(g', 0)$ is the only vertex joined with $(g', 0')$. Hence $\varphi(g, 0) = (g', 0)$. This in turn implies $\varphi(g, 1') = (g', 1')$, etc., and we obtain $\varphi(g, x) = (g', x)$ for all $x = 0', 0, 1', 1, \ldots, w, (w+1)'$. The crucial fact here is that at least every other vertex in the sequence $(g, 0'), (g, 0), (g, 1'), (g, 1), \ldots, (g, w), (g, (w+1)')$ is of degree 2.

Now let $\varphi \varepsilon G(X)$ be such that $\varphi(g, 0') = (g, 0')$ for some fixed $g \varepsilon G$. By the previous argument, $\varphi(g, x) = (g, x)$, $x = 0', 0, \ldots, w, (w+1)'$. Suppose $g', g'' \varepsilon G$ are such that $[(g, 1), (g', 1)]$ and $[(g, 1), (g'', 1)]$ are edges of X, and suppose that $\varphi(g', 1) = (g'', 1)$. Then either $g' = gh_k$, $g'' = gh_{k'}$ or $g' = gh_k^{-1}$, $g'' = gh_{k'}^{-1}$. Assume $g' = gh_k$. Then $\varphi(g', 1) = (g'', 1)$ implies $\varphi[(g, 0), (g', 1)] = [(g, 0), (g'', 1)] \varepsilon E(X)$. Hence by definition of $E(X)$, $g'' = gh_{k'}$. Similarly, if $g' = gh_k^{-1}$. Now $g' = gh_k$, $g'' = gh_{k'}$, and $g' = gh_k^{-1}$, $g'' = gh_{k'}^{-1}$ each imply $M_{i_k} = M_{i_{k'}}$, $M_{j_k} = M_{j_{k'}}$, whence $k = k'$, so that $g' = g''$. This shows that if (g', y) is joined with some (g, x) then (g', y) is invariant under φ. An inductive argument then proves that φ is the identity on the whole set $V(X)$.

Let $\psi \varepsilon G(X)$, $(g, x) \varepsilon V(X)$, then in view of the fact that $\psi(g, x) = (g', x)$ there is a $g'' \varepsilon G$ such that $\varphi_{g''} \psi(g, x) = (g, x)$. Hence $\varphi_{g''} \psi = 1$, so that $\psi \varepsilon G'$. Hence $G(X) = G' \cong G$.

3. Proof of Theorem 2

In view of the triviality of $\alpha(Z_2) = 2$, we can assume that $m \geqq 3$.

Case (1): $m = p^e \geqq 7$. Let $X(m)$ be the following graph:

$$V(X(m)) = \{1, \ldots, m, 1', \ldots, m'\},$$

$$E(X(m)) = \{[i, i+1], [i, i'], [i+1, i'], [i-2, i'] \mid 1 \leqq i \leqq m\},$$

where addition is modulo m.

Clearly $\psi : V(X(m)) \to V(X(m))$ given by $\psi\, i = i + 1$, $\psi\, i' = (i+1)'$, $i = 1, \ldots, m$, is an automorphism of $X(m)$; hence $G(X(m))$ contains a subgroup isomorphic to Z_m.

Note that the m-circuit C formed the vertices $1, \ldots, m$ is the only m-circuit of $X(m)$ whose vertices are of degree 5 in $X(m)$. Hence C remains invariant under all automorphisms of $X(m)$. In particular, if $\varphi \varepsilon G(X(m))$ is such that $\varphi\, i_0 = i_0$ for some $i_0 \varepsilon V(C)$, then either $\varphi \mid C = 1$ or $\varphi(i_0 + j) = i_0 - j$, $j = 1, \ldots, m$. Note that all 3-circuits of $X(m)$ are of the form $i, i+1, i', 1 \leqq i \leqq m$. Hence if $\varphi(i_0 + j) = i_0 - j$ it follows that $\varphi\, i_0' = (i_0 - 1)'$. But then $\varphi[i_0', i_0 - 2] = [(i_0 - 1)', i_0 + 2] \varepsilon E(X(m))$, a contradiction since $m \geqq 7$. Hence $\varphi \mid C = 1$, and therefore $\varphi = 1$. It follows that $G(X(m)) \cong Z_m$. $\alpha_0(X(m)) = 2\, m$, hence $\alpha(Z_m) \leqq 2\, m$.

To complete the proof that $\alpha(Z_m) = 2\,m$ assume that there is a graph Y with $G(Y) \cong Z_m$ and $\alpha_0(Y) < 2\,m$. Since $m = p^e$ it follows that if $\varphi \varepsilon G(Y)$ and $y \varepsilon V(Y)$, then either $y, \varphi y, \ldots, \varphi^{m-1} y$ are all distinct, or else $\varphi y = y$. In either case $G(Y) \cong D_{2m}$ (= the dihedral group of order $2\,m$), a contradiction. Hence $\alpha(Z_m) = 2\,m$.

Case (2): $m = 3, 4, 5$. Here we define $X(m)$ by

$$V(X(m)) = \{1, \ldots, m, 1', \ldots, m', 1'', \ldots, m''\},$$

$$E(X(m)) = \{[i, i+1], [i, i'], [i+1, i'], [i', i''], [i'', (i+1)''], [i'', i+1] \mid 1 \leqq i \leqq m\} \qquad \text{(addition modulo } m\text{)},\ m = 3, 4, 5.$$

Obviously $\alpha_0(X(m)) = 3\,m$. The proof that $G(X(m)) \cong Z_m$, and that $\alpha(Z_m) = 3\,m$ is similar to that in case (1).

Case (3): $m = p_1^{e_1} \ldots p_r^{e_r}$. Consider the graph

$$X = X(p_1^{e_1}) + \ldots + X(p_r^{e_r}).$$

Since $X(m)$ and $X(m')$ are non-isomorphic whenever $m \neq m'$, it follows that

$$G(X) \cong G(X(p_1^{e_1})) \times \ldots \times G(X(p_r^{e_r})) \cong Z_{p_1^{e_1}} \times \ldots \times Z_{p_r^{e_r}} \cong Z_m.$$

Hence

$$\alpha(Z_m) \leqq \sum_{i=1}^{r} \alpha_0(X(p_i^{e_i})) = \sum_{i=1}^{r} \alpha(Z_{p_r^{e_r}}),$$

and an argument analogous to that in case (1) then shows that there is actual equality.

References

[1] *Frucht, R.*, Graphs of degree 3 with given abstract group. Canad. J. Math. **1** 365—378. (1949).