ON GROUPS AND GRAPHS[1]

BY
CHONG-YUN CHAO

By a graph X we mean a finite set $V(X)$, called the vertices of X, together with a set $E(X)$, called the edges of X, consisting of unordered pairs of distinct elements of $V(X)$. We shall indicate the unordered pairs by brackets. Two graphs X and Y are said to be isomorphic, denoted by $X \simeq Y$, if there is a one-to-one map σ of $V(X)$ onto $V(Y)$ such that $[\sigma a, \sigma b] \in E(Y)$ if and only if $[a, b] \in E(X)$. An isomorphism of X onto itself is said to be an automorphism of X. For each given graph X there is a group of automorphisms, denoted by $G(X)$, where the multiplication is the multiplication of permutations. The complementary graph X^c of X is the graph whose $V(X^c) = V(X)$, and $E(X^c)$ consists of all possible edges which do not belong to $E(X)$. It is easy to see that X and X^c have the same group of automorphisms. A graph consisting of isolated vertices only is called the null graph, and its complementary graph is called the complete graph. Both the null graph and the complete graph of n vertices have S_n, the symmetric group of n letters, as their group of automorphisms. A regular graph of degree k is a graph such that the number of edges incident with each vertex is k. The null graphs and the complete graphs are regular. The graph X is necessarily regular if $G(X)$ is transitive.

In [7], König proposed the following question: "When can a given abstract group be set up as the group of automorphisms of a graph?" The question can be interpreted in two ways. (a) Given a finite group G, can one construct a graph whose group of automorphisms is abstractly isomorphic to G? (b) Given a permutation group G acting on n letters, can one construct a graph of n vertices whose group of automorphisms is G? The former has been answered affirmatively by Frucht in [4] and [5], and many others. Concerning the latter, Kagno in [6] investigated the graphs of vertices $\leqq 6$ and their group of automorphisms. It is known that not every group can have a graph in the sense of (b). For instance, letting

$$G = \left\{ \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} \right\},$$

Presented to the Society, April 20, 1964 under the title *Graphs and groups*; received by the editors February 14, 1964.

(1) A portion of the work was done while the author was at the Research Center, International Business Machines Corporation.

there is no graph of two vertices whose group of automorphisms is G, but the null graph of a single vertex has its group of automorphisms abstractly isomorphic to G. It is also known that there is no graph of n vertices whose group of automorphisms is transitive and abelian for $n > 2$ with one exception [3]. To find a necessary and sufficient condition seems to be very difficult. The purpose here is to study the groups of automorphisms of graphs by using some of the known results and methods in the theory of permutation groups. The definitions concerning permutation groups used here are the same as in [13]. In §1 we center around an algorithm for obtaining $G(X)$ for a given graph X with n vertices,all graphs isomorphic to X (the number of them is equal to the index of $G(X)$ in S_n), and all the isomorphic mappings of X. We also give a sufficient condition for $G(X')$ to be an inavriant subgroup of $G(X)$, where X' is a subgraph of X. We also construct an X and X' such that the factor group $G(X)/G(X')$ is isomorphic to a given abstract group. In §2 we give, based on a theorem of Schur, a simple algorithm for constructing all graphs X of n vertices whose $G(X)$ contain a given transitive permutation group of degree n (a more general result will be followed by the author). In particular, we give an algorithm for constructing all graphs X of p vertices whose $G(X)$ is transitive where p is a prime number, and study the properties of $G(X)$. In §3 we show, by construction, that for each integer $n > 2$ there exists a graph X of n^2 vertices whose $G(X)$ is primitive and not doubly transitive.

1. For each graph X with n vertices (label them by the numbers 1 to n), a matrix $A(X) = (a_{ij}), i, j = 1, 2, \cdots, n$, is determined, and it is called the adjacency matrix of X, where

$$a_{ij} = \begin{cases} 1 & \text{if there is an edge between the } i\text{-vertex and } j\text{-vertex,} \\ 0 & \text{otherwise.} \end{cases}$$

Clearly, $A(X)$ is an $n \times n$ symmetric $(0,1)$-matrix with zero on the diagonal. Conversely, if such a matrix is given, then a graph with n vertices is determined.

LEMMA A. *Let σ be a one-to-one map of $V(X)$ onto $V(Y)$, and $P_\sigma = (p_{ij})$ be the permutation matrix corresponding to σ. Then σ is an isomorphism of X onto Y if and only if $A(X)P_\sigma = P_\sigma A(Y)$.*

Proof. We note that since σ is a one-to-one map of $V(X)$ onto $V(Y)$, σ^{-1} exists and P_σ^{-1} is the transpose matrix of P_σ. For every i and j vertices of $V(X)$ we have, say, $\sigma(i) = k$ and $\sigma(j) = m$. Since P_σ is a permutation matrix, we have

$$\begin{aligned}(A(X)P_\sigma)_{im} &= \sum_r a_{ir} p_{rm} = a_{ik} p_{km} \\ &= \begin{cases} 1 & \text{if } [i, k] \in E(X), \\ 0 & \text{otherwise,} \end{cases}\end{aligned}$$

$$(P_\sigma A(Y))_{im} = \sum_s p_{is} b_{sm} = p_{ij} b_{jm}$$
$$= \begin{cases} 1 & \text{if } [j,m] \in E(Y), \\ 0 & \text{otherwise,} \end{cases}$$

then σ is an isomorphism of X onto Y if and only if $(A(X)P_\sigma)_{im} = (P_\sigma A(Y))_{im}$ for $i, m = 1, 2, \cdots, n$, i.e., if and only if $A(X)P_\sigma = P_\sigma A(Y)$.

COROLLARY A.1. *Let σ be a permutation of $V(X)$ onto $V(X)$, and $P_\sigma = (P_{ij})$ be the permutation matrix corresponding to σ. Then σ is an automorphism of X if and only if $A(X)$ commutes with P_σ.*

THEOREM 1. *Let X be a graph of n vertices and X' be a subgraph of X (i.e., $V(X') = V(X)$ and $E(X') \subseteq E(X)$) such that $G(X') \subseteq G(X)$. Then the number of the isomorphic graphs of X' in X is $\geqq$ the index of $G(X')$ in $G(X)$.*

Proof. Let σ be any element of $G(X)$. We claim that σ is an isomorphism of X' onto some subgraph of X. Since $P_\sigma A(X')P_\sigma^{-1}$ is a symmetric $(0,1)$-matrix with zeros on the diagonal, $P_\sigma A(X')P_\sigma{}^{-1}$ can be considered as the adjacency matrix for some graph Y' with the same number of vertices as X'. By Lemma A, $X' \simeq Y'$. We show that Y' is also a subgraph of X: Let e' be any edge in $E(Y')$, and e be the corresponding edge in $E(X')$. Since σ is an automorphism of X, $e' = \sigma e \in E(X)$, i.e., $E(Y') \subseteq E(X)$. Similarly, $V(Y') = V(X)$.

We also claim that all elements in the same left coset $\sigma G(X')$, where $\sigma \in G(X)$, transform X' alike, and two elements from different left cosets transform X' differently. We shall consider the corresponding matrices. By Corollary A.1, we have $(P_\sigma P_\mu)A(X')(P_\sigma P_\mu)^{-1} = P_\sigma A(X')P_\sigma^{-1}$, irrespective of the elements μ chosen in $G(X')$. On the other hand, if two elements from different cosets did not transform X' differently, we would have $P_\sigma A(X')P_\sigma^{-1} = P_\omega A(X')P_\omega^{-1}$, whence $A(X')$ commutes with $P_\sigma^{-1}P_\omega$ which, by Corollary A.1, means $\sigma^{-1}\omega \in G(X')$ and $\omega \in \sigma G(X')$. That is a contradiction and the number of the isomorphic graphs of X' in X is $\geqq$ the index of $G(X')$ in $G(X)$.

COROLLARY 1.1 *Let X' be a graph of n vertices. Then the number of graphs isomorphic to X' is equal to the index of $G(X')$ in S_n (i.e., equal to $n!$ divided by $|G(X')|$ where $|G(X')|$ is the order of $G(X')$).*

Proof. Let X be the complete graph of n vertices. If $Y' \simeq X'$, then Y' has n vertices and Y' is a subgraph of X. Apply Theorem 1 to complete the proof.

COROLLARY 1.2. *Let X' be a graph of n vertices. Then any permutation in S_n is an isomorphism of X' onto some graph Y' of n vertices.*

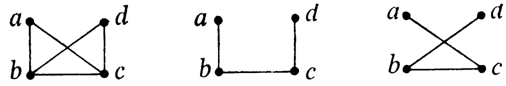
From the preceding discussion it is clear that we have an algorithm for obtaining the group of automorphisms of a given graph X of n vertices, i.e., we can obtain the matrix $A(X)$ accordingly and consider $P_\sigma A(X)P_\sigma^{-1}$, where σ runs through S_n. The permutation σ is an automorphism of X if and only if the matrix $P_\sigma A(X)P_\sigma^{-1}$ is equal to $A(X)$. Similarly, we have an algorithm for obtaining all the graphs isomorphic to X, i.e., when $P_\sigma A(X)P_\sigma^{-1}$ is not equal to $A(X)$, we may consider it as the adjacency matrix of some graph Y which is isomorphic to X. There are $(n!/|G(X)|)-1$ such graphs (not including X itself), and the set of permutations $\{\sigma\mu;\ \mu\in G(X)\}$ consists of all isomorphisms of X onto Y, and is of cardinality $|G(X)|$.

Another immediate consequence of Corollary A.1 is the following.

THEOREM 2. *Let X' be a subgraph of X, and $G(X')\subseteq G(X)$. Then $G(X')$ is an invariant subgroup of $G(X)$ if $G(X')$ is also the group of automorphisms of every graph isomorphic to X' in X (i.e., $G(X')=G(Y')$ for every Y' isomorphic to X' in X).*

Proof. If $G(X') = G(Y')$ for every Y' isomorphic to X' in X, then for every $\mu\in G(X')$ and every $\sigma\in G(X)$, we have $(P_\sigma^{1-}P_\mu P_\sigma)A(X')(P_\sigma^{-1}P_\mu P_\sigma)^{-1} =(P_\sigma^{-1}P_\mu)A(Y')(P_\sigma^{-1}P_\mu)^{-1}=A(X')$ where $A(Y')=(P_\sigma A(X')P_\sigma^{-1}$. By CorollaryA. $\sigma^{-1}\mu\sigma\in G(X')$, i.e., $\sigma^{-1}G(X')\sigma\subseteq G(X')$ for every $\sigma\in G(X)$, and $G(X')$ is invariant in $G(X)$.

In §2 we shall see that there exists no graph of n vertices whose group of automorphisms is a proper invariant subgroup of S_n, i.e., the complete graphs do not have any subgraph X' whose $G(X')$ is a proper invariant subgroup of S_n. However, the following example shows that a graph X containing all possible edges except one can have a subgraph X' whose $G(X')$ is a proper invariant subgroup of $G(X)$ and also illustrates the theorems at this point: Let $V(X) = \{a,b,c,d\}$ and $E(X)$ consists of all possible edges except $[a,d]$. Also let $V(X') = V(X)$ and $E(X')=\{[a,b],\ [b,c],\ [c,d]\}$. Then $G(X) = \{1,\ (ad),\ (bc),\ (ad)(bc)\}$, and $G(X')=\{1,\ (ad)(bc)\}$. Clearly, $G(X')$ is a proper invariant subgroup since $G(X$ is abelian.



X X' Y'

We see that Y' is isomorphic to X', and the isomorphisms are (ad) and (bc).

THEOREM 3. *For any given finite group G of order > 1, there exists a graph X and a subgraph X' of X such that $G(X')$ is a proper invariant subgroup of $G(X)$ and $(G(X)/G(X'))\simeq G$.*

Proof. From Frucht's result in [4] or [5], we know that there exists a graph Y of n vertices, $n>1$, such that $G(Y)\simeq G$. We shall denote the vertices of Y by $x_{11},x_{21},\cdots,x_{n1}$. Let X' be the following graph: $V(X')=\{x_{11},x_{12},x_{21},x_{22}, x_{23},\cdots,x_{i1},x_{i2},\cdots,x_{ii+1},\cdots,x_{n1},x_{n2},\cdots,x_{nn+1}\}$, and $E(X') = E(Y)$

$\cup \{[x_{ki}, x_{kj}];\ i \neq j, i,j = 1,2,\cdots,k+1$, and $k = 1,2,\cdots,n\}$. In other words, we obtain X' from Y by adding a complete graph of $k+1$ vertices at x_{k1} for $k = 1,2,\cdots,n$. It is easy to see that an automorphism of X' leaves each x_{i1} fixed, and may permute x_{ij} among themselves where $j = 2,3,\cdots,i+1$. Hence, $G(X') \simeq S_1 \times S_2 \times \cdots \times S_n$. Let $V(X) = V(X')$ and $E(X) = E(X') \cup \{[x_{ij}, x_{k1}];\ j = 2,3,\cdots,i+1, i \neq k$, and $i,k = 1,2,\cdots,n\}$. Clearly, X' is a subgraph of X and $G(X') \subset G(X) \simeq G(Y) \times S_1 \times S_2 \times \cdots \times S_n$. Since $\sigma\mu\sigma^{-1}$ leaves every x_{i1} fixed for every $\sigma \in G(X)$ and every $\mu \in G(X')$, $G(X')$ is a proper invariant subgroup of $G(X)$, and $(G(X)/G(X')) \simeq G(Y) \simeq G$.

2. Let G be a transitive permutation group acting on n letters, say, $1,2,\cdots,n$, and let the orbits of the subgroup $G_1 = \{\sigma \in G; \sigma 1 = 1\}$ be denoted by $\Delta_1 = \{1\}, \Delta_2, \cdots, \Delta_k$ (since G is transitive, there is no difference by considering G_1 or any $G_i, 2 \leqq i \leqq n$). Associate with each Δ_μ an $n \times n$ matrix $B(\Delta_\mu) = (b_{ij})$, $i,j = 1,2,\cdots,n$, with

$$b_{ij} = \begin{cases} 1, & \text{if there exists a } \sigma \in G \text{ and an } x \in \Delta_\mu \text{ with } \sigma 1 = j \text{ and } \sigma x = i, \\ 0, & \text{otherwise.} \end{cases}$$

It is easy to see that $B(\Delta_1)$ is the identity matrix I, and $\sum_{i=1}^{k} B(\Delta_i) = J$, where J is the $n \times n$ matrix whose entries are all 1. Every row or column of $B(\Delta_i)$ consists of exactly $|\Delta_i|$ ones where $|\Delta_i|$ denotes the number of elements in the orbits Δ_i for $i = 1,2,\cdots,k$.

The following theorem is due to Schur (p. 94 in [13]): Let G be a transitive permutation group acting on n letters regarded as a group of $n \times n$ permutation matrices, let $V(G) = \{M = (m_{ij}),\ i,j = 1,2,\cdots,n;\ m_{ij} \in$ a commutative field F, and for $P_\sigma \in G$, $P_\sigma M = MP_\sigma$ where the multiplication is the ordinary matrix multiplication$\}$, and let $\Delta_1 = \{1\}, \Delta_2, \cdots, \Delta_k$ be the orbits of G_1. Then $V(G)$ is a vector space over F with $B(\Delta_1), B(\Delta_2), \cdots, B(\Delta_k)$ as a basis.

In [13], F is the complex number field. Apparently, the theorem holds for any commutative field since the argument in the proof practically does not have to be changed (See [11]). For our purpose here we shall take F to be GF(2).

Now we may state the algorithm for constructing all graphs X of n vertices whose $G(X) \supseteq G$ where G is a given transitive permutation group of degree n: (1) From the given group G we can easily find all the orbits $\Delta_1 = \{1\}, \Delta_2, \cdots, \Delta_k$ of G_1 where $2 \leqq k \leqq n$. (2) Compute $B(\Delta_i)$ for $i = 2,3,\cdots,k$. (We may ignore $B(\Delta_1)$ since the graphs which we consider have no loops.) (3) Consider each $B(\Delta_i)$ for $i = 2,3,\cdots,k$. If $B(\Delta_i)$ is a symmetric matrix, then a graph X_i can be constructed whose $A(X_i)$ is $B(\Delta_i)$. If it is not symmetric, ignore it temporarily. (4) Consider $B(\Delta_i) + B(\Delta_j), i \neq j, i,j = 2,3,\cdots,k$. If it is symmetric, construct the graphs as in (3). If not, ignore it temporarily. Repeat the same process for all possible sums of $3,4,\cdots,k-1$ different $B(\Delta_i)$ matrices. (5) Include the null graph of n vertices.

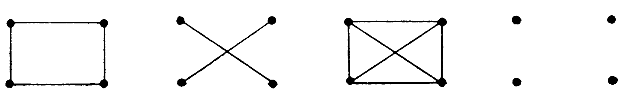
We claim that this process gives us all the graphs each whose group of automorphisms$\supseteq G$. Let X be any graph of n vertices such that $G(X) \supseteq G$, then $A(X)$ is determined by X, and, by Corollary A.1, ($A(X)$ commutes with all $P_\sigma \in G$ (regarded as permutation matrices). That means $A(X) = \sum_{i=1}^{k} a_i B(\Delta_i)$, $a_i \in \mathrm{GF}(2)$. Since $A(X)$ has all zeros on the diagonal, $a_1 = 0$. Hence, X is one of the graphs which we have constructed. Conversely, each of the graphs X which we have constructed by using the algorithm must have its $A(X)$ commute with each of the permutation matrices of G since $A(X)$ is a linear combination of the $B(\Delta_i)$. Hence, by Corollary A.1, $G \subseteq G(X)$.

For convenience, this process shall be called Schur's algorithm on G, where G is a given transitive permutation group.

An example: Let G be the dihedral group of order 8 acting transtitively on four letters 1, 2, 3, 4. The orbits of G_1 are $\Delta_1 = \{1\}$, $\Delta_2 = \{2,4\}$ and $\Delta_3 = \{3\}$, and

$$B(\Delta_2) = \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix} \quad \text{and} \quad B(\Delta_3) = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}.$$

Since $B(\Delta_2)$ and $B(\Delta_3)$ are symmetric and $B(\Delta_2) + B(\Delta_3) = J - I$, the following graphs of four vertices are all the graphs each whose group of automorphisms contains G:



(a) (b) (c) (d)

where the group of automorphisms of graphs (a) and (b) is the dihedral group, and that of (c) and (d) is S_4, which certainly contains G.

THEOREM 4. *Let p be a prime number, and G be the cyclic group generated by $(123\cdots p)$. Then Schur's algorithm on G gives all the graphs of p vertices each whose group of automorphisms is transitive.*

Proof. Each graph X of p vertices obtained by Schur's algorithm acting of G has its $G(X)$ transitive since $G(X)$ contins G. Conversely, let X be a graph of p vertices whose $G(X)$ is transitive, then p divides $|G(X)|$ (see p. 8 in [13]), and $G(X)$ contains an element whose order is p (see p. 47 in [2]). Clearly, this element is a generator of G, i.e., $G(X)$ contains G, and X must be one of the graphs obtained by Schur's algorithm on G.

Let G be the group generated by $(12\cdots p)$ where p is an odd prime. Then none of the $B(\Delta_i)$ is a symmetric matrix, where $\Delta_i = \{i\}$ and $i = 2,3,\cdots,p$, and it is easy to see that $B(\Delta_i) + B(\Delta_j)$ is a symmetric matrix if and only if $j = p - i + 2$ where $i = 2,3,\cdots,(p+1)/2$. Each $B(\Delta_i) + B(\Delta_{p-i+2})$ is the adjacency matrix of an

1-cycle. From Theorem 4 we know that any graph X of p verticles, where p is an odd prime, whose $G(X)$ is transitive must be a regular graph with these 1-cycles combined together.

LEMMA B. *There exists no graph whose group of automorphisms is k-ply transitive for $k \geqq 2$ except the complete graphs and null graphs.*

Proof. Let G be a doubly transitive permutation group, i.e., G_1 is transitive on the remaining $n-1$ letters; then G_1 has only two orbits $\Delta_1 = \{1\}$ and Δ_2 such that $B(\Delta_2) = J - I$. By the algorithm, the graphs whose group of automorphisms contains G are the complete graphs and null graphs. The proof is completed by using the fact that a k-ply ($k \geqq 3$) transitive group certainly is doubly transitive.

We also can prove Lemma B without using the algorithm. If X is not a null graph then there is an edge $[a, b] \in E(X)$, and by the double transitivity of $G(X)$, all edges belong to $E(X)$, i.e., X is a complete graph.

COROLLARY B.1. *There exists no graph of n vertices whose group of automorphisms is a proper invariant subgroup of S_n.*

Proof. Since the alternating group A_n is the only proper invariant subgroup n S_n for $n \neq 4$ and A_n is doubly transitive for $n > 3$, by using Lemma B we complete our proof for $n > 4$. Since the transitive four-group and A_3 are transitive and abelian, we know from [3] that they cannot be the group of automorphisms of any graph with 4 and 3 vertices, respectively.

COROLLARY B.2 (KAGNO [6]). *There exists no graph whose group of automorphisms is A_n.*

THEOREM 5. *Let X be a noncomplete and non-null graph of p vertices, where p is a prime, and $G(X)$ be transitive. Then* (a) *$G(X)$ is solvable.* (b) *$G(X)$ is a Frobenius group.* (c) *$G(X)$ is (3/2)-ply transitive.*

Proof. (a) It follows from Lemma B, and a famous theorem of Burnside [2, p. 339] that every nonsolvable transtive group of prime degree is doubly transitive. (b) Since $G(X)$ is solvable and transitive of prime degree, by a theorem of Galois [1, p. 79] $G(X)_{ab} = (1), a \neq b$. We claim that $G(X)_a \neq (1)$. Suppose $G(X)_a = (1)$; then $G(X)$ would be a regular group, and $|G(X)| =$ the degree of $G(X) = p$. Consequently, $G(X)$ must be a cyclic group, but we know that there exists no graph of n verticles whose $G(X)$ is cyclic for $n > 2$ [6], [3]. For $n = 2, X$ is either the complete graph or the null graph. Hence, $G(X)$ is a Frobenius group. (c) It follows from the fact that every Frobenius group is (3/2)-ply transitive.

3. It is easy to see that Theorem 4 does not hold if p is not a prime. For instance, the Petersen graph [8, p. 241] has 10 vertices, its group of automor-

phisms is transitive and does not contain the cyclic group generated by $(12\cdots 10)$. However, all the non-null and noncomplete graphs obtained by Schur's algorithm on the group generated by $(12\cdots n)$, where n is a composite number, are imprimitive. This fact follows from Lemma B and a theorem of Schur [11] which states that if n is not a prime, and G is a permutation group of degree n containing the cyclic group generated by $(12\cdots n)$, then G is either doubly transitive or imprimitive. Hence, for each composite number n, we can easily construct graphs of n vertices each of whose group of automorphisms is imprimitive. This leads to the question "Does there exist a non-null and noncomplete graph X of n vertices whose $G(X)$ is primitive for any given composite number n?" Since Wielandt [13, p. 110], [12] showed that when $n = 2p$ and $n \neq a^2 + 1$, where p is a prime, a primitive group of degree n is doubly transitive, the answer to our question is negative. Again, to find a necessary and sufficient condition seems to be very difficult. Here, we shall use the cartesian product of graphs (for definition, see below, and, for interesting properties, see [9] and [10]) to show the following.

THEOREM 6. *For every integer $n > 2$ there exists a graph Z of n^2 vertices whose $G(Z)$ is primitive and not doubly transitive.*

DEFINITION. Let X and Y be graphs. $Z = X \times Y$ is said to be the cartesian product graph of X and Y if $V(Z) = V(X) \times V(Y)$ and $E(Z) = \{[(x_1, y_1), (x_2, y_2)];$ $x_1 = x_2$ and $[y_1, y_2] \in E(Y)$ or $y_1 = y_2$ and $[x_1, x_2] \in E(X)\}$.

LEMMA C. *Let $Z = X \times Y$. Then $G(Z)$ is transitive if and only if $G(X)$ and $G(Y)$ are transitive.*

Proof. For each $\sigma \in G(X)$, we define a permutation μ_σ on $V(Z)$ by $\mu_\sigma(x, y) = (\sigma x, y)$. We claim that $\mu_\sigma \in G(Z)$. If $[(x_1, y_1), (x_2, y_2)] \in E(Z)$, then either $x_1 = x_2$ and $[y_1, y_2] \in E(Y)$, or $y_1 = y_2$ and $[x_1, x_2] \in E(X)$. The former indicates $\sigma x_1 = \sigma x_2$, and the latter implies $[\sigma x_1, \sigma x_2] \in E(X)$. Hence, $[(\sigma x_1, y_1), (\sigma x_2, y_2)] \in E(Z)$, i.e., $[\mu_\sigma(x_1, y_1), \mu_\sigma(x_2, y_2)] \in E(Z)$. Conversely, if $[\mu_\sigma(x_1, y_1), \mu_\sigma(x_2, y_2)] \in E(Z)$, then, by using $\sigma \in G(X)$, one can easily show that $[(x_1, y_1), (x_2, y_2)] \in E(Z)$. Hence, $\mu_\sigma \in G(Z)$.

Similarly, for each $\theta \in G(Y)$, we define $\mu_\theta(x, y) = (x, \theta y)$, and show $\mu_\theta \in G(Z)$.

Let (x_1, y_1) and (x_2, y_2) be any two vetrices in $V(Z)$. We know that there exists an $\sigma \in G(X)$ such that $\sigma x_1 = x_2$, and $\theta \in G(Y)$ such that $\theta y_1 = y_2$ If $y_1 = y_2$, then $\mu_\sigma(x_1, y_1) = (x_2, y_1)$. If $x_1 = x_2$, then $\mu_\theta(x_1, y_1) = (x_1, y_2)$. If $x_1 \neq x_2$ and $y_1 \neq y_2$, then $\mu_\theta \mu_\sigma(x_1, y_1) = (x_2, y_2)$. Hence, $G(X)$ is transitive.

Conversely, if $G(Z)$ is transitive, then for every x_i and x_j in $V(X)$, there exists a $\mu \in G(Z)$ such that $\mu(x_i, y_k) = (x_j, y_k)$, i.e., induces a permutation σ on $V(Z)$ such that $\sigma x_i = x_j$. We claim that $\sigma \in G(X)$. $[(x_i, y_k), (x_t, y_k)] \in E(Z)$ if and only if $[x_i, x_t] \in E(X)$. Also, $[(x_i, y_k), (x_t, y_k)] \in E(Z)$ if and only if $[(\sigma x_i, y_k), (\sigma x_t, y_k)] \in E(Z)$, i.e., if and only if $[\sigma x_i, \sigma x_t] \in E(X)$. This implies that $\sigma \in G(X)$. Consequently, $G(X)$ is transitive. Similarly, $G(Y)$ is transitive.

Now the proof of Theorem 6 goes as follows: Let X be the complete graph of n vertices, and label the vertices by $1,2,\cdots,n$. Let $Z = X \times X$. Then $V(Z) = \{(i,j); i,j = 1,2,\cdots,n\}$. For convenience, we shall call i the first coordinate and j the second coordinate of the vertex (i,j). Clearly, Z is a non-null and noncomplete graph. By Lemma C, $G(Z)$ is transitive of degree n^2, and by Lemma B, $G(Z)$ is not doubly transitive.

Let B be a block of $G(X)$ whose length is $t, 1 \leqq t \leqq n^2$; then t must divide n^2. We may assume that B contains the vertex $(1,1)$.

Case 1. $t = n$ Since $Z = X \times X$, there is a permutation μ on $V(Z)$ such that $\mu(i,j) = (j,i)$ for all $i,j = 1,2,\cdots,n$. It is clear that $\mu \in G(Z)$. We claim that $B \neq \{(1,1),(2,1),\cdots,(n,1)\}$. Suppose the contrary; then we would have $\mu B \cap B \neq B, \neq \varnothing$ which contradicts B being a block of $G(X)$. We claim that B cannot contain k vertices whose first coordinates are the same, where $1 < k < n$. Suppose, on the contrary, B contained $(i,i_1), (i,i_2),\cdots,(i,i_k)$; then there would be a j such that B contains no vertex whose first coordinate is j. Since there is a $\rho \in G(X)$ such that $\rho(i) = j$, $\rho(j) = i$ and $\rho(u) = u$ for all $u \neq i,j$ since $n > 2$, such a u exists), ρ induces a $\mu_\rho \in G(Z)$, where $\mu_\rho(t,u) = (\rho t,u)$. Then $\mu_\rho B \cap B \neq B$, and $(1,1) \in (\mu_\rho B \cap B)$. That is a contradiction. We also claim that $B \neq \{(1,1),(2,i_2),\cdots,(n,i_n)\}$. Again, suppose the contrary. We first notice that not all i_r are 1 for $r = 2,3,\cdots,n$, because it would be a previous case. Say $i_s \neq 1$ for some s; then $\mu_\rho B \cap B \neq B, \neq \varnothing$ where $\mu_\rho(t,u) = (\rho t, u)$ and $\rho(1) = i_r, \rho(i_r) = 1$ and $\rho(k) = k$ for all $k \neq 1, i_r$ (since $n > 2$, such a k exists). Hence, B cannot be of length n.

Case 2. $n^2 > t > n$, i.e., $t = sn, 1 < s < n$. If B contains more than s vertices each of whose first coordinate is i, then there must be a j such that $j \neq i, 1 \leqq j \leqq n$, and B contains less than s vertices each of whose first coordinate is j. Consequently, $\mu_\rho B \cap B \neq B, \neq \varnothing$ where $\mu_\rho(t,u) = (\rho t,u)$, and $\rho \in G(X)$ such that $\rho(i) = j$, $\rho(j) = i$ and $\rho(k) = k$ for all $k \neq i,j$ (since $n > 2$ such a k exists). If B contains exactly s vertices each of whose first coordinate is $i, i = 1,2,\cdots,n$, then $\mu B \cap B \neq B$, $\neq \varnothing$, where μ is defined as in Case 1. Hence, B cannot be of length $t, n^2 > t > n$.

Case 3. $n > t > 1$. B cannot contain all the t vertices each of whose first coordinate is 1 since $G(X)$ $(= S_n)$ is primitive. Hence, there exists an $i \neq 1$ such that B contains at least one vertex whose first coordinate is i. Since $n > t$ and $n > 2$, there is a $j \neq 1, i$ such that B contains no vertex whose first coordinate is j. Consequently, $\mu_\rho B \cap B \neq B, \neq \varnothing$, where $\rho \in G(X)$ and $\rho(i) = j, \rho(j) = i$ and $\rho(k) = k$ for $k \neq i,j$. Hence, B cannot be of length $t, 1 < t < n$, either. B must be of trivial length, and $G(Z)$ is primitive.

COROLLARY 6.1. *For every integer $n > 2$, there exists a primitive permutation group of degree n^2 which is not doubly transitive.*

REMARK. (*Added in proof*). R. L. Hemminger points out to me that the following example shows that " > " in Theorem 1 is necessary, and that the converse of Theorem 2 does not hold in general: Let X' be a subgraph of X such that $V(X) = V(X') = \{a, b, c, d\}$, $E(X') = \{[a, b], [b, c]\}$ and $(EX) = \{[a, b], [b, c], [c, d], [d, a], [a, c]\}$. Then $G(X') \subset G(X)$ and the index is 2. But the number of isomorphic graphs of X' in X is greater than 2, and there is a subgraph Y' of X such that $G(Y') \simeq G(X')$ and $G(Y') \neq G(X)'$.

I wish to thank A. J. Hoffman for helpful conversations.

References

1. E. Artin, *Galois theory*, Notre Dame Mathematical Lectures, No. 2, 2nd. ed., Notre Dame, Indiana, 1959.

2. W. Burnside, *Theory of groups of finite order*, 2nd. ed., Chelsea, New York, 1958.

3. C. Y. Chao, *On a theorem of Sabidussi*, Proc. Amer. Math. Soc. (to appear).

4. R. Frucht, *Herstellung von Graphen mit vorgegebener abstrakter Gruppe*, Compositio Math. **6** (1938), 239–250.

5. ———, *Graphs of degree three with a given abstract group*, Canad. J. Math. **1** (1949), 365–378.

6. I. N. Kagno, *Linear graphs of degree* $\leqq$ 6 *and their groups*, Amer. J. Math. **68** (1946), 505–520.

7. D. König, *Theorie der endlichen und unendlichen graphen*, Akademie Verlag, Leipzig, 1936 and Chelsea, New York, 1950.

8. O. Ore, *Theory of graphs*, Amer. Math. Soc. Colloq. Publ. Vol. 38, Amer. Math. Soc., Providence, R. I., 1962.

9. G. Sabidussi, *Graphs with given graph theoretical properties*, Canad. J. Math. **9** (1957), 515–525.

10. ———, *Graph multiplication*, Math. Z. **72** (1962), 446–457.

11. I. Schur, *Zur Theorie der einfach transitiven Permutationsgruppen*, S. B. Preuss. Akad. Wiss. Phys.-Math. Kl. (1933), 598–623.

12. H. Wielandt, *Primitive Permutations-grouppen vom Grad* 2*p*, Math. Z. **63** (1955), 478–485.

13. ———, *Permutation groups*, California Institute of Technology, Pasadena, California, 1962.

University of Pittsburgh,
Pittsburgh, Pennsylvania