

## THE GRAPH EXTENSION THEOREM<sup>1</sup>

ERHEST SHULT

**ABSTRACT.** A sufficient condition is given that a transitive permutation group  $G$  admits a transitive extension  $G^*$ . The condition is graph-theoretic and does not involve any direct algebraic properties of the group being extended. The result accounts for a fairly wide class of doubly transitive groups, including the two doubly transitive representations of the groups  $\text{Sp}(2n, 2)$ , and the doubly transitive representations of the Higman-Sims group, and the Conway group (.3).

The theorem given below gives a sufficient condition for the existence of certain doubly transitive groups. All known doubly primitive groups which are not triply transitive (with the exception of  $\text{PSL}(2, q)$ ,  $q \equiv 3 \pmod{4}$ , acting on  $1+q$  letters, and  $\text{PSL}(2, 11)$  acting on 11 letters) occur by virtue of this theorem. Included in this list of groups are groups involving doubly transitive representations of two recently discovered sporadic simple groups: the Higman-Sims groups acting on 176 letters and the Conway group (.3) acting on 276 letters.

**GRAPH EXTENSION THEOREM.** *Let  $\Omega$  be an undirected graph without loops. Set  $G = \text{Aut}(\Omega)$ , the automorphism group of  $\Omega$ .*

*Assume the following:*

- (a)  *$G$  transitively permutes the vertices of  $\Omega$ .*
- (b) *Given some vertex  $x$  in  $\Omega$ , let  $\Gamma$  denote the set of vertices of  $\Omega$  which are arced to  $x$  and let  $\Sigma = \Omega - (\Gamma \cup \{x\})$ . Then there exist maps  $h_1: \Gamma \rightarrow \Gamma$ , and  $h_2: \Sigma \rightarrow \Sigma$  such that the  $h_i$  induce automorphisms on  $\Gamma$  and  $\Sigma$ , viewed as subgraphs of  $\Omega$ , and such that if  $a \in \Gamma$  and  $b \in \Sigma$ ,  $a$  is arced to  $b$  if and only if  $h_1(a)$  is not arced to  $h_2(b)$ .*

*Then there exists a doubly transitive group  $G_0$  acting on  $|\Omega|+1$  letters, such that the subgroup fixing a letter acts on remaining letters in a manner permutation—isomorphic to  $G$  acting on the vertices of  $\Omega$ . (In other words,  $G_0$  is a transitive extension of  $G$ .)*

---

Received by the editors June 21, 1971.

*AMS 1970 subject classifications.* Primary 20B20, 20B25; Secondary 22B10, 05C30.

*Key words and phrases.* Doubly transitive groups, transitive extension, automorphism groups of graphs.

<sup>1</sup> This theorem was first presented in a group theory seminar at the Princeton Institute for Advanced Study in the spring of 1969. The author was a one-year member that year and gratefully acknowledges the support of grant number NSF GP-7952X.

© American Mathematical Society 1972

PROOF. Let  $\Omega$  and  $\Omega'$  denote two isomorphic copies of the graph  $\Omega$ , and use  $z'$  to denote the element in  $\Omega'$  which corresponds to the element  $z \in \Omega$ , under this isomorphism. We define a new graph  $\Omega^*$  whose vertices are  $\{\alpha\} \cup \Omega \cup \Omega' \cup \{\alpha'\}$ . The vertex  $\alpha$  is arced to every vertex of  $\Omega$ , the vertex  $\alpha'$  is arced to every vertex of  $\Omega'$ , and  $\Omega$  and  $\Omega'$  are to be subgraphs of  $\Omega^*$ . Finally if  $a \in \Omega$ , and  $b' \in \Omega'$ , then  $a$  is arced to  $b'$  if and only if  $a$  is *not* arced to  $b$  in  $\Omega$ . We have defined the arcs of  $\Omega^*$  and it is clear that  $\Omega^*$  is a graph in which every vertex is arced to  $|\Omega|$  other vertices.

Set  $G^* = \text{Aut}(\Omega^*)$ . Clearly, automorphisms of  $\Omega$  can be extended to automorphisms of  $\Omega^*$  leaving both  $\alpha$  and  $\alpha'$  fixed. Thus we have an embedding  $e: G \rightarrow G^*$ . Fix the vertex  $x \in \Omega$  and form the decomposition  $\Omega = \{x\} \cup \Gamma \cup \Sigma$  where  $\Gamma$  is the subgraph of  $\Omega$  whose vertices are all arced to vertex  $x$ , and  $\Sigma$  is the subgraph whose vertices are  $\Omega - (\Gamma \cup \{x\})$ . Let  $\Gamma'$  and  $\Sigma'$  be the corresponding subgraphs of  $\Omega'$ . We define an automorphism  $t_x$  as follows: (a)  $t_x$  transposes  $\alpha$  and  $x$  and transposes  $\alpha'$  and  $x'$ . (b)  $t_x$  stabilizes  $\Gamma$  and induces the mapping  $h_1$  on  $\Gamma$ . Similarly,  $t_x$  stabilizes  $\Gamma'$  and  $t_x(b') = (h_1(b))'$  for all  $b' \in \Gamma'$ . (c) If  $a \in \Sigma$ ,  $t_x(a) = h_2(a)'$ . Similarly, if  $a' \in \Sigma'$ , then set  $t_x(a') = h_2(a)$ . Thus  $t_x$  interchanges the sets  $\Sigma$  and  $\Sigma'$ . It is easy to check that  $t_x$  is an isomorphism of  $\Omega^*$ . Since  $e(G)$  acts on the vertices of  $\Omega^*$  with orbits  $\{\alpha\}$ ,  $\Omega$ ,  $\Omega'$  and  $\{\alpha'\}$ , it follows that  $H = \langle e(G), t_x \rangle$  transitively permutes the set  $X$  of "antipodal" pairs  $\{(\alpha, a') | a \in \{\alpha\} \cup \Omega\}$ . Thus  $|X| = 1 + |\Omega|$ ,  $H$  is transitive on  $X$  and its subgroup  $e(G)$  fixes the pair  $\{(\alpha, \alpha')\}$  and is transitive on the remaining pairs  $\{(x, x') | x \in \Omega\}$ . Thus  $H$  is doubly transitive on  $X$ .

Clearly, the mapping transposing members of each antipodal pair is a central involution  $t$  in  $G^*$  and together with the identity comprises the full kernel of the action  $G^*$  on  $X$ . It follows that  $\langle t, e(G) \rangle \simeq Z_2 \times e(G)$  is the full stabilizer in  $G^*$  of a point in  $X$ . Thus  $G_0 = G^* / \langle t \rangle$  is a doubly transitive group on  $X$  satisfying the conclusion of the theorem. (Note that  $G^* = H$  if  $\Omega$  is not a complete graph.)

We conclude with some examples. In each case we identify the initial graph  $\Omega$ , and the "arc-breaking" map  $h_1 \times h_2: \Gamma \times \Sigma \rightarrow \Gamma \times \Sigma$ .

EXAMPLE 1. *The symmetric groups.* Let  $\Omega$  be the graph having  $n$  vertices and no arcs. Then  $\Gamma$  is empty, and so  $\Gamma \times \Sigma$  is empty. Thus there are no arcs to break, and we may take  $h_2$  to be the identity map on  $\Sigma$ . Then  $\Omega^*$  consists of two sets  $A = \alpha \cup \Omega'$  and  $B = \alpha' \cup \Omega$  each consisting of  $n+1$  vertices and no arcs. There is a 1-1 correspondence between  $A$  and  $B$  such that each vertex in one set is arced to every vertex in the other except the one corresponding to it. Although we must contend in this example with the artificiality that the mapping  $h_1$  and hence  $h_1 \times h_2$  have empty domains, nonetheless the automorphism  $t_x$  of  $\Omega^*$  defined in the proof of the

theorem exists, forcing  $G^* = \text{Aut}(\Omega^*)$  to be doubly transitive on the set  $X$  of antipodal pairs in  $\Omega^*$ . Indeed  $t_x$  induces a single 2-cycle on  $X$ .

EXAMPLE 2. *Groups involving  $\text{P}\Sigma\text{L}(2, q)$  acting on  $1+q$  letters,  $q \equiv 1 \pmod{4}$ .* Let  $Q$  denote the multiplicative group of nonzero squares in the field  $\text{GF}(q)$ ,  $q \equiv 1 \pmod{4}$ . Let the vertices of  $\Omega$  be the elements of  $\text{GF}(q)$  and let  $x$  be arced to  $y$  if and only if  $x-y \in Q$ . Since  $-1$  is a square,  $x-y \in Q$  implies  $y-x \in Q$ , so that the arc relation is symmetric. Clearly, the group  $S$  of semilinear substitutions of the form  $g(x, \beta, \sigma): x \rightarrow \alpha x^\sigma + \beta$  where  $\alpha \in Q$ ,  $\beta \in \text{GF}(q)$ ,  $\sigma \in \text{Aut}(\text{GF}(q))$ , is a group of automorphisms of the graph  $\Omega$ . We isolate the vertex represented by zero, and we set  $\Gamma = Q$  and  $\Sigma = \text{GF}(q) - (Q \cup \{0\})$  the set of nonzero nonsquares. Let  $h_1$  and  $h_2$  be the restrictions of the mapping  $x \rightarrow (1/x)$  to  $Q$  and  $\Sigma$  respectively (this is possible since the reciprocal of a square is a square). Let  $x$  and  $y$  be distinct nonzero elements of  $\text{GF}(q)$ . If  $x$  and  $y$  are either both squares, or nonsquares, then  $xy$  is a square. In that case  $x-y=a$  and  $(1/y)-(1/x)=a/(xy)$  are either both squares or both nonsquares. On the other hand, if only one of  $x$  and  $y$  is a square,  $xy$  is a nonsquare, and so only one of  $x-y=a$  and  $(1/y)-(1/x)=a/(xy)$  is a square. Thus  $h_1$  and  $h_2$  induces automorphisms of the subgraphs  $\Gamma$  and  $\Sigma$ , and  $h_1 \times h_2$  interchanges the set of arcs and the set of nonarcs in  $\Gamma \times \Sigma$ .

The doubly transitive groups  $G_0$  which arise here contain  $\text{P}\Sigma\text{L}(2, q)$  as a doubly transitive group on  $1+q$  letters, where  $\text{P}\Sigma\text{L}(2, q)$  denotes the semidirect product  $\text{PSL}(2, q)$  and the group  $C$  of automorphisms of  $\text{PSL}(2, q)$  induced from the group of field automorphisms. The assertion that  $G_0 \cong \text{P}\Sigma\text{L}(2, q)$  is equivalent to stating that the *full* automorphism group of the graph  $\Omega$  given above coincides with (and is permutation isomorphic to) the group  $H$  of semilinear transformations of the form

$$x \rightarrow \alpha x^\sigma + \beta$$

where  $\sigma \in \text{Aut}(\text{GF}(q))$ ,  $\beta \in \text{GF}(q)$  and  $\alpha$  is a nonzero square. Whether  $\text{Aut}(\Omega)$  is isomorphic to  $H$  or is larger seems to be an open question, although certain cases can be handled. In this connection, see reference [3].

EXAMPLE 3. *Doubly transitive representations of  $\text{Sp}(2n, 2)$ .* Let the vertices of  $\Omega$  be the set of singular vectors in either one of the two non-degenerate orthogonal geometries on the  $2n$ -dimensional vector space over  $\text{GF}(2)$ . Arc two singular vectors if they are perpendicular, with respect to the induced symplectic form. Selecting a vector  $u$ , we let  $\Gamma$  be all singular vectors distinct from  $u$  which are perpendicular to  $u$ . Then  $\Sigma$  is the set of all singular vectors having inner product 1 with  $u$ . Let  $h_1$  be translation by the vector  $u$  (this stabilizes  $\Gamma$ ) and let  $h_2$  represent the identity mapping on  $\Sigma$ . Then  $h_1$  and  $h_2$  satisfy the hypotheses of the theorem. The doubly transitive groups obtained can easily be shown to be the groups  $\text{Sp}(2n, 2)$ . Because

of the way  $h_1$  and  $h_2$  are defined, there exist involutions in these doubly transitive groups, fixing a relatively large number of letters. (For example  $\text{Sp}(6, 2)$  is doubly transitive on 28 letters and contains an involution fixing 16 of these letters.)

EXAMPLE 4. *The semidirect product of  $\text{Sp}(2n, 2)$  and the additive groups of its vector space.* Let the vertices of  $\Omega$  be the nonzero vectors in a nondegenerate symplectic space of dimension  $2n$ , over the field of two elements. Arc two vectors if they are not equal but are perpendicular. Select a vector  $u \in \Omega$ , set  $\Gamma = u^\perp \cap \Omega - \{u\}$  and  $\Sigma = \Omega - (\Gamma \cup \{u\})$ . Let  $h_1$  be translation of elements of  $\Gamma$  by the vector  $u$  (this induces an automorphism of the subgraph  $\Gamma$ ) and let  $h_2$  be the identity mapping on  $\Sigma$ . Then, as in the previous example,  $h_1$  and  $h_2$  satisfy the hypotheses of the theorem.

EXAMPLE 5. *The Higman-Sims group.* Let  $S$  be the graph with 50 vertices defined from the orbital of size 7, as the simple group  $U(3, 5)$  acts as a rank-3 permutation group on the cosets of a subgroup isomorphic to  $A_7$ . The graph  $S$  contains 175 arcs, no triangles, and no quadrilaterals. Two distinct arcs in  $S$  bear one of three relationships: (A) they have a common vertex, (B) they do not have a common vertex and are arcs in a unique pentagon, (C) they lie in no pentagon, and lie in exactly two hexagons, forming there, opposites sides of the hexagon.

Now we define the graph  $\Omega$ . The vertices of  $\Omega$  are the arcs of  $S$ . Two vertices of  $\Omega$  are arced in  $\Omega$  if and only if they represent two arcs of  $S$  in the relation (B). Each vertex in  $\Omega$  is arced to 72 other vertices;  $\Omega$  has diameter 2.

Fix a vertex  $v$  in  $\Omega$  which represents the arc  $(ab)$  in  $S$ . We may redefine the graph  $S$  in the following way. The alternating group on six letters has two conjugate classes  $C_1$  and  $C_2$  of subgroups isomorphic to the alternating group on 5 letters. We label the twelve arcs in  $S$  which have a common vertex with  $(a, b)$  as  $\{(a, x) | x \in C_1\} \cup \{(b, x) | x \in C_2\}$ . Thirty-six further vertices remain in  $S$  and we identify these with the set  $\Lambda$  of 36 5-Sylow subgroups of  $A_6$ . If  $R \in \Lambda$ , we form an arc  $(X, R)$ ,  $X \in C_i$ , if and only if  $R$  is a subgroup of  $X$ . Now each 5-Sylow subgroup lies in just one group from  $C_1$  and one from  $C_2$ . The pairs  $(X, R)$  define 72 arcs in the relation (B) to  $(a, b)$ . Finally, two 5-Sylow subgroups  $R_1$  and  $R_2$  are arced if they do not lie in a common subgroup in  $C_1$  or  $C_2$  and if there exists an involution in  $A_6$  normalizing both  $R_1$  and  $R_2$ . This defines a system of 90 arcs, all with vertices in  $\Lambda$ .

Let  $\Gamma$  be the vertices in  $\Omega$  arced to  $v$ —i.e. they represent 72 arcs in the relation (B) to  $(a, b)$ . Each has the form  $u = (X, R)$  where  $X \in C_1 \cup C_2$ . If  $X \in C_i$  it also is true that  $R$  lies in a unique member  $X'$  of  $C_1 \cup C_2 - C_i$  so that  $u$  has a "twin"  $u' = (X', R)$  which is also one of the 72 arcs of  $S$  represented by vertices in  $\Gamma$ . Define  $h_1: \Gamma \rightarrow \Gamma$  by  $u \rightarrow u'$ , so  $h_1$  is an involution.

Each involution  $t$  in  $A_6$  normalizes exactly four 5-Sylow subgroups,  $R_1, R_2, R_3, R_4$ , where  $\langle R_1, R_2 \rangle, \langle R_3, R_4 \rangle$  are elements of  $C_1$ , and  $\langle R_1, R_4 \rangle, \langle R_2, R_3 \rangle$  are elements of  $C_2$  and  $(R_1, R_3)$  and  $(R_2, R_4)$  are arcs of  $S$ . Thus the 4 points of  $\Lambda$  fixed by  $t$  yield 2 nonmeeting arcs. Conversely given an arc  $(R_i, R_j)$  there exists only one involution  $t$  in  $A_6$  normalizing both  $R_i$  and  $R_j$  and so there is a "twin" to this,  $(R'_i, R'_j)$ , also fixed by  $t$ . Then  $f: (R_i, R_j) \rightarrow (R'_i, R'_j)$  is a well-defined involutory mapping on the set  $\Sigma_1$  of 90 arcs in relation (C) to  $(a, b)$ . Finally let  $\Sigma_2$  be the 12 arcs which meet  $(ab)$  so that  $\Sigma = \Sigma_1 + \Sigma_2$ . Define  $h_2: \Sigma \rightarrow \Sigma$  by letting  $h_2$  be the identity mapping on  $\Sigma_2$  and the mapping  $f$  on  $\Sigma_1$ . Then it can be shown that  $h_2$  is an automorphism of the subgraph  $\Sigma$ ,  $h_1$  is an automorphism of the subgraph  $\Gamma$ , and that  $h_1 \times h_2$  exchanges all arcs and nonarcs in  $\Gamma \times \Sigma$ . Thus the conditions of the graph extension theorem hold for the graph  $\Omega$ .

Although, it is a somewhat tedious verification the group  $G_0$  which arises must be the Higman-Sims simple group. This is achieved by first showing (a) that  $\text{Aut}(\Omega) \cong \text{PSU}(3, 5)$  (i.e. the relation of graphs  $S$  and  $\Omega$  is tight enough that no automorphism group of  $\Omega$  which is rank-3 on its vertices is possible), (b) that in  $G_0$  there is an involution  $t$  interchanging two letters  $\alpha$  and  $\beta$  which centralizes the subgroup fixing both  $\alpha$  and  $\beta$ , and that the action of  $t$  on  $\Omega - \beta$  is unique, and finally, (c) action of a corresponding involution from the Higman-Sims group either agrees with the action of  $t$  in (b) or else fixes more letters than can be allowed from the character table of the Higman-Sims group. (For a description of this permutation representation see [2].)

EXAMPLE 6. *The Conway Group* (.3). Let  $C$  denote the simple Conway group (.3), and let  $Mc$  denote its simple subgroup of index 276, the McLaughlin simple group [1], [4].  $C$  is doubly transitive on a set  $U$  of 276 letters, with  $Mc = C_\alpha$ , the subgroup fixing letter  $\alpha$ .  $Mc$  is a transitive rank-3 permutation group on the remaining 275 letters  $\Omega = U - \{\alpha\}$ , with subdegrees 1, 162, 112. The subgroup of  $Mc$  fixing a letter  $\beta$  in  $\Omega$  is the group  $C_{\alpha\beta} \cong U(3, 4)$ . We construct a graph from  $\Omega$  and  $Mc$  using the orbital of length 162. Thus in the graph  $\Omega$ ,  $\beta$  is arced to a set  $\Gamma$  of 162 vertices, and fails to be arced to a set  $\Sigma$  of 112 points. It is well known [4] that  $Mc$  acts on  $\Gamma \times \Sigma$  in two orbits  $O$  and  $O'$  of equal length and that  $(x, y) \in \Gamma \times \Sigma$  is an arc in  $\Omega$  if and only if  $(x, y) \in O$ . Let  $s$  be an involution in  $Mc$ . Then  $s$  fixes a subgraph  $C_\Omega(s)$  of 35 points. We assume without loss of generality that  $\beta \in C_\Omega(s)$ . Then  $C_{Mc}(s)/\langle s \rangle \cong \gamma_8$ , the symmetric group on 8 letters, acts faithfully on  $C_\Omega(s)$  as a rank-3 permutation group on 35 letters with subdegrees 1-18-16. Let  $t$  be an involution in  $C$  conjugate to  $s$  which interchanges  $\alpha$  and  $\beta$ . Without loss of generality it may be assumed that  $t$  centralizes  $s$ . Then  $C_C(s) = \langle t, C_{Mc}(s) \rangle$  is doubly transitive on the 36 letters  $\alpha \cup C_\Omega(s)$ . Indeed,  $C_C(s)/\langle s \rangle \cong \text{Sp}(6, 2)$  and this transitive extension of  $\gamma_8$

on 35 letters arises from Example 3 above. As a consequence,  $t$  exchanges the set of arcs and the set of nonarcs in the  $18 \times 16$  pairs  $C_1(s) \times C_2(s)$ . Thus  $\langle t, U \rangle$  is transitive on  $\Gamma \times \Sigma$ , and exchanges the orbits  $O$  and  $O'$ . Thus if  $h_1 = t|_\Gamma$  and  $h_2 = t|_\Sigma$ ; the  $h_1 \times h_2$  possesses the "arc-breaking" condition of the graph-extension theorem. An examination of subdegrees of the action of  $U$  on  $\Gamma$  and  $\Sigma$  respectively show that graph-theoretic boundaries in these subgraphs represent orbitals of unique length. Thus  $t$  acts on  $\Gamma$  and  $\Sigma$  by preserving arcs in these subgraphs, whence  $h_1 \in \text{Aut}(\Gamma)$  and  $h_2 \in \text{Aut}(\Sigma)$  as required. Thus  $(\Omega, h_1, h_2)$  fulfills the hypotheses of the graph extension theorem.

In the above examples, just enough details have been presented to show that a graph involved satisfies the conditions of  $\Omega$  in the graph-extension theorem. The actual identification of the doubly transitive groups  $G_0$  which arise in this theorem (although sketched vaguely in some of the above examples) is a fairly tedious process. The unpleasant details of these identifications have been deferred to a mimeographed supplement available to the reader upon request [6].

What doubly transitive groups may arise by virtue of the graph-extension theorem? As a contribution to this question we announce the following

**THEOREM.** *In the graph-extension theorem, if either of the mappings  $h_1$  or  $h_2$  can be taken to be the identity mapping on  $\Gamma$  or  $\Sigma$  respectively (for example by composing it with a suitable mapping induced from an automorphism of  $\Omega$  fixing  $x$ ) then the doubly transitive groups  $G_0$  which appear are the groups  $\text{Sp}(2n, 2)$  in either of its two doubly transitive representations, the semidirect product of  $\text{Sp}(2n, 2)$  and the additive group of its vector space  $V^+$ , or  $\text{PSL}(2, 5)$  acting on six letters.*

This theorem follows from a number of characterization theorems on graphs which will be published elsewhere [5].

The author is grateful to Professor K. Rudvalis who pointed out to the author the possibility that the Higman-Sims group might be an example of this theorem. The author expresses his deep gratitude to Professor W. Kantor for many valuable discussions (including the entire second example!) and for urging the publication of this note.

#### REFERENCES

1. J. H. Conway, *A group of order 8,315,553,613,086,720,000*, Bull. London Math. Soc. **1** (1969), 79-88. MR **40** #1470.
2. G. Higman, *On the simple group of D. G. Higman and C. C. Sims*, Illinois J. Math. **13** (1969), 74-80. MR **39** #1545.

3. D. G. Higman, *Solvability of a class of rank 3 permutation groups*, Nagoya Math. J. **41** (1971), 89–96.
4. J. McLaughlin, *A simple group of order 898.128,000*, Theory of Finite Groups (Symposium, Harvard Univ., Cambridge, Mass., 1968), Benjamin, New York, 1969, pp. 109–111. MR **39** #4268.
5. E. Shult, *Characterizations of certain classes of graphs*, J. Combinatorial Theory (to appear).
6. ———, *Supplement to “The graph extension theorem”*, University of Florida, Gainesville, Fla. (mimeographed notes).

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF FLORIDA, GAINESVILLE, FLORIDA  
32603