A NOTE ON TWO SET-TRANSITIVE
PERMUTATION GROUPS

CHONG-YUN CHAO

In a generalization of permutation groups, Beaumont and Peterson in [1] stated the following definitions: A permutation group \( G \) on \( n \) letters denoted by \( \Omega_n = \{1, 2, \ldots, n\} \) is said to be \( s \) set-transitive \((1 \leq s \leq n-1)\) if for every pair of subsets \( S \) and \( T \) of \( \Omega_n \), each containing \( s \) elements, there exists a permutation in \( G \) which carries \( S \) into \( T \). Also, \( G \) is said to be set-transitive if \( G \) is \( s \) set-transitive for all \( s \) \((1 \leq s \leq n-1)\). They showed that the set-transitive permutation groups on \( n \) letters, other than the symmetric group \( S_n \) and the alternating group \( A_n \), are of degree 5, 6 and 9. All these groups are doubly transitive except \( A_3 \). They also showed that if \( G \) is \( s \) set-transitive for at least one \( s > 1 \) then \( G \) is primitive. It seems natural to ask whether there are \( s \) set-transitive permutation groups which are not doubly transitive for some \( s \) \((1 < s < n-1)\) besides \( A_3 \) and the 2 set-transitive group on \( \Omega_7 \) generated by \((1234567)\) and \((235)(476)\) and its conjugates in \( S_7 \) (see p. 36 in [1]). It is known that, on p. 94 in [2], a primitive group of degree \( n = 2p \) \((p \text{ prime})\) is doubly transitive if \( n \) is not of the form \( a^2 + 1 \). Also, it is not known if \( p \neq 5 \) there are primitive groups of degree \( 2p \) which are not doubly transitive. Hence, the answer to our question depends on \( n \). The purpose of this note is, by using elementary concept of graphs and number theory, to present a constructive proof to the following

Theorem. Let \( p \) be a prime such that \( p \equiv 3 \mod 4 \). Then there exists an \( 2 \) set-transitive permutation group on \( \Omega_p \) which is not doubly transitive.

The graphs which we consider here are finite, directed and loopless, i.e., 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 ordered pairs \([a, b]\) of distinct elements \( a, b \in V(X) \). We also assume that there is at most one directed edge between two ordered vertices. The graph with all possible edges is called a complete graph, and the graph with no edges is said to be a null graph. An automorphism \( \sigma \) of \( X \) is an one-to-one map of \( V(X) \) onto \( V(X) \) such that \([a \sigma, b \sigma] \in E(X)\) if and only if \([a, b] \in E(X)\). The set of automorphisms of \( X \) constitutes a group, denoted by \( G(X) \), where the multiplication is the multiplication of permutations. Let \( H \) be an abstract finite group and \( K \) be a

Received by the editors December 23, 1965.

953
subset of \( H \). The Cayley graph of \( H \) with respect to \( K \) (\( K \) does not contain the identity of \( H \)) is \( X_{H,K} \) with \( V(X_{H,K}) = H \) and \( E(X_{H,K}) = \{ [h, hk] ; h \in H, k \in K \} \). If \( K \) is the empty set \( \emptyset \), then \( E(X_{H,K}) \) is meant to be \( \emptyset \), i.e., \( X_{H,K} \) is a null graph. Clearly, we have

**Lemma 1.** The left regular representations of \( H \) is contained in \( G(X_{H,K}) \) for any subset \( K \) in \( H \).

**Lemma 2.** Let \( X \) be a graph of \( n \geq 3 \) vertices. Then \( G(X) \) is doubly transitive if and only if \( X \) is either the null graph or the complete graph.

**Proof.** Both the null graph and the complete graph have the symmetric group, \( S_n \), as their group of automorphisms. Conversely, if \( X \) is not the null graph, then there is an edge \([a, b] \in E(X)\). By double transitivity of \( G(X) \), all edges belong to \( E(X) \), i.e., \( X \) is a complete graph.

Now the proof of the theorem goes as follows: Let \( H = \{ e = x^0, x^1, x^2, \ldots, x^{p-1} \} \) be the cyclic group of order \( p \) generated by \( x \). We know that the group of automorphisms of \( H \), denoted by \( A(H) \), is a cyclic group of order \( p-1 \) on \( p \) letters leaving \( e \) fixed. Let \( \tau \) be a generator of \( A(H) \) and let \( \sigma = \tau^2 \), then \( \sigma \) is of order \((p-1)/2\). Let \( K = \{ x\sigma, x\sigma^2, \ldots, x\sigma^{(p-1)/2} = x \} \). We claim that none of the elements in \( K \) has an inverse in \( K \). Say, \( x\tau = x^i, 1< \tau \leq p-1 \), then \( x\sigma^i = x^{2i} = (x^i)^2, 1 \leq i \leq (p-1)/2 \). Since \( \sigma \) is of order \((p-1)/2\), \( (t^i)^2 \neq (t^j)^2 \) mod \( p \), \( i \neq j \), \( 1 \leq i, j \leq (p-1)/2 \). Hence, these \((t^i)^2, i = 1, 2, \ldots, (p-1)/2 \), are incongruent quadratic residues of \( p \). Since \( p \equiv 3 \mod 4 \), \( -1 \) is not a quadratic residue. Since the product of a quadratic residue and a quadratic nonresidue is a quadratic nonresidue, \(- (t^i)^2, i = 1, 2, \ldots, (p-1)/2 \), are quadratic nonresidues. Hence, none of \( x^{-2} \) \((= t^3), i = 1, 2, \ldots, (p-1)/2 \), is in \( K \).

We form the Cayley graph, \( X_{H,K} \), of \( H \) with respect to \( K \). Clearly, \( \sigma \) is an automorphism of \( X_{H,K} \). Since \( H \) is abelian, by Lemma 1 the right regular representations (say, generated by \( R_x \)) are also automorphisms of \( X_{H,K} \). Hence, the group, \(( (R_x, \sigma) \) ), generated by \( R_x \) and \( \sigma \) is \( \subseteq G(X_{H,K}) \). By Lemma 2, \(( (R_x, \sigma) \) ) is not doubly transitive since \( X_{H,K} \) is neither null nor complete.

We claim that \(( (R_x, \sigma) \) ) is an 2 set-transitive permutation group. For every pair \( i, j = 1, 2, \ldots, p \) and \( i \neq j \), either \( [x^i, x^j] \in E(X_{H,K}) \) or \( [x^j, x^i] \in E(X_{H,K}) \). If \( [x^i, x^j] = [x^i, x^j] \in E(X_{H,K}) \), i.e., \( x\sigma^r \in K \) where \( x^j = x^i \sigma^r \), then \( x^i(x^j)^{-1} \in K \), i.e., \( [x^i, x^j(x^j)^{-1}] = [x^i, x^jx^j] = [x^i, x^j] \in E(X_{H,K}) \). Any two edges in \( X_{H,K} \) are in the form \( [x^i, x^i(x^j\sigma^r)] \) and \( [x^j, x^j(x^i\sigma^u)] \). We denote them by \( E_1 \) and \( E_2 \) respectively. If \( t = u \), then \( E_iR_x^{t-1} = E_2 \). If \( t \neq u \) then \( \sigma^{u-t} \) followed by \( R_x^t \), for
some $r$, sends $E_1$ onto $E_2$. Hence, $((R_2, \sigma))$ is an 2 set-transitive permutation group and is not doubly transitive.

**Corollary.** Let $p$ be a prime such that $p \equiv 3 \mod 4$. Then there exists an $p - 2$ set-transitive permutation group on $\Omega_p$ which is not doubly transitive.

It follows from our theorem and Theorem 3 in [1].

*Added in proof (June 6, 1966).* After the present note was submitted, Professor R. A. Beaumont informed me that the theorem in this note was also obtained by D. Livingstone and A. Wagner in *Transitivity of finite permutation groups on unordered sets*, Math. Z. 90 (1965), 393–403. However, the methods are different.

**References**


**University of Pittsburgh**