Permutation Groups, Vertex-transitive Digraphs and Semiregular Automorphisms

DRAZEN MARUŠIĆ and RAFFAELE SCAPELLATO

A nonidentity element of a permutation group is said to be semiregular if all of its orbits have the same length. The work in this paper is linked to [6] where the problem of existence of semiregular automorphisms in vertex-transitive digraphs was posed. It was observed there that every vertex-transitive digraph of order \( p^k \) or \( mp \), where \( p \) is a prime, \( k \geq 1 \) and \( m \leq p \) are positive integers, has a semiregular automorphism. On the other hand, there are transitive permutation groups without semiregular elements [4]. In this paper, it is proved that every cubic vertex-transitive graph contains a semiregular automorphism, and moreover, it is shown that every vertex-transitive digraph of order \( 2p^2 \), where \( p \) is a prime, contains a semiregular automorphism.

© 1998 Academic Press

1. INTRODUCTION

By a digraph we mean an ordered pair \( X = (V, A) \) where \( V \) is a finite nonempty set (of vertices) and \( A \) (the set of arcs) is an irreflexive relation on \( V \). In this sense (undirected) graphs are a special case of digraphs with above relation a symmetric one. (All digraphs, as well as graphs, will then be assumed to be finite). Besides, all groups in this paper are assumed to be finite, too. By \( p \) we shall always denote a prime number. We refer the reader to [2, 3, 9] for the terminology not defined here.

Let \( r \geq 1 \) and \( s \geq 2 \) be integers and let \( G \) be a permutation group (on a finite set \( V \)). An element of \( G \) is said to be \((r, s)\)-semiregular if it has \( r \) orbits of length \( s \) and semiregular if it is \((r, s)\)-semiregular for some \( r \) and \( s \).

The following problem was posed independently in [5] and [6].

**PROBLEM 1.1.** Does every vertex-transitive digraph have a semiregular automorphism?

Note that the existence of a semiregular automorphism in a vertex-transitive digraph is equivalent to the existence of a fixed-point-free automorphism of prime order. Of course, it is a direct consequence of the definition that every Cayley digraph has a semiregular automorphism. For non-Cayley digraphs the problem is, by no means, an easy one. Further families of vertex-transitive digraphs, which must necessarily have semiregular automorphisms, include vertex-transitive digraphs of orders \( mp \), where \( m \leq p \), and \( p^k \) (see [6]). On the other hand, no vertex-transitive digraph without a semiregular automorphism is known to us.

Let us also mention the connection between the existence of semiregular automorphisms and the hamiltonicity problem for vertex-transitive graphs. Namely, many existing techniques for constructing hamiltonian cycles in certain classes of vertex-transitive graphs

---

1 Corresponding author. Supported in part by the Commission of the European Communities Research Fellowship, contract no. ERB3510PL923971.6368 and by “Ministrstvo za znanost in tehnologijo Slovenije”, proj. no. J1-7035-0101-95.

2 Supported in part by the Italian Ministry of Research (MURST).
exploit the fact that these graphs possess semiregular automorphisms (see [1]). Finally, we remark that Problem 1.1 cannot be solved by adhering to permutation groups alone, for there exist transitive permutation groups without semiregular automorphisms as we shall see in Section 2. On the other hand, every finite group acting transitively on a set of cardinality at least 2 must necessarily contain an element of prime power order without fixed points (see [4, Theorem 1]).

In this paper we show, first, that every cubic vertex-transitive graph has a semiregular automorphism (Theorem 3.3) and, second, that every vertex-transitive digraph of order 2p², where p is a prime, has a semiregular automorphism (Theorem 4.1).

2. PERMUTATION GROUPS WITHOUT SEMIREGULAR ELEMENTS

If G is a group and g ∈ G we let Cl_G(g) denote the conjugacy class of g in G. The following lemma may be used in the constructions of transitive permutation groups without semiregular elements.

**Lemma 2.1.** Let G be an (abstract) group, let H ≤ G and let H be the set of all right cosets of H in G. The action of G on H by right multiplication is faithful iff, for each g ∈ G\{1}, the class Cl_G(g) is not contained in H. Moreover, if the above action of G is faithful, then G has no semiregular elements iff, for each g ∈ G of prime order, the intersection H ∩ Cl_G(g) is nonempty.

**Proof.** Note that g ∈ G\{1} fixes Hx when Hxg = Hx, that is if xgx⁻¹ ∈ H. Therefore, faithfulness of G means that for each g there is a coset Hx such that xgx⁻¹ ∉ H, that is Cl_G(g) ∉ H. This proves the first part of the lemma.

Suppose now that the action of G on the set H is faithful. The result follows in view of the fact that the absence of fixed-point-free elements g ∈ G of prime order is equivalent to the statement: H ∩ Cl_G(g) = ∅ for all g ∈ G of prime order.

Note that, when the above action in the statement of Lemma 2.1 is faithful, H must be not a nontrivial normal subgroup of G. Using Lemma 2.1 we can now give examples of transitive permutation groups having no semiregular elements. The family of groups given in Example 2.2 is first mentioned in [4, p. 41].

**Example 2.2.** Let G be the group consisting of all affine transformations of GF(p²) of the form x → ax + b, a ∈ GF(p²) \{0}, b ∈ GF(p²), where p is a Mersenne prime. Let H be the subgroup consisting of these transformations where a, b ∈ GF(p), let H be the set of left cosets of H in G and let G act on H by left translation. It may be verified using Lemma 2.1 that every element of prime order in G has a fixed point on H.

**Example 2.3.** Let G be the stabilizer of v = [1, 0, 0]ᵀ in the natural action of PSL(3, 3) on the projective space PG(2, 3). Then G is a group of order 2⁴·3³ and degree 12. Let H = G_w, where w = [0, 1, 0]ᵀ. The typical element g ∈ G, written as a matrix, is

\[
\begin{bmatrix}
\lambda & 0 & U \\
0 & M
\end{bmatrix},
\]

where λ ∈ Z⁺, U is a 2-row, M ∈ GL(2, 3) and λ det M = 1. Moreover, g ∈ H iff M is triangular and the first component of U is 0. Using this description it may be shown that all conjugacy classes of elements of prime order of G intersect H. In view of Lemma 2.1, it follows that G has no semiregular elements.
3. Cubic Vertex-Transitive Graphs

We start this section by giving a simple sufficient condition for a vertex-transitive graph of prime valency to have a semiregular automorphism.

Let $G$ be a permutation group on a set $V$ and let $\alpha \in G$. By $\text{Fix}(\alpha)$ we denote the set of fixed points of $\alpha$ in $V$. Let $X$ be a graph. We define a relation $\mathcal{R}_X$ on $V(X)$ by the rule $u\mathcal{R}_X v$ iff the corresponding sets of neighbors $N(u)$ and $N(v)$ coincide. So $\mathcal{R}_X$ (or $\mathcal{R}$ in short) is an equivalence relation. We let $X/\mathcal{R}$ be the graph with vertex set $V(X)/\mathcal{R}$ and the edges of the form $[u]\mathcal{R}[v]\mathcal{R}$, where $uv$ is an edge of $X$. If $X$ is vertex-transitive, then all classes of $\mathcal{R}$ have equal cardinality, say $r$. Moreover, Aut $X$ is isomorphic to the wreath product $S_r \wr \text{Aut}(X/\mathcal{R})$. Clearly, if $r > 1$, any product of $r$-cycles, one for each class of $\mathcal{R}$, is a semiregular automorphism of $X$. Thus $\mathcal{R} \neq \text{id}$ implies the existence of a semiregular automorphism of $X$.

**Proposition 3.1.** Let $X$ be a connected vertex-transitive graph of prime valency $p$. Let $\alpha, \beta \in \text{Aut}X$, where $\alpha$ has order $p$ and $\text{Fix}(\beta) = V(X) \setminus \text{Fix}(\alpha)$. Then $\mathcal{R} \neq \text{id}$ and so $X$ has a semiregular automorphism.

**Proof.** Since $X$ is connected there are $u \in \text{Fix}(\alpha)$ and $v \in \text{Fix}(\beta)$ such that $v \in N(u)$. Clearly, each $\alpha^i(v)$ belongs to $N(u)$ and so $N(u) = \{v, \alpha(v), \ldots, \alpha^{p-1}(v)\}$. It follows that $N(u) \cap \text{Fix}(\alpha) = \emptyset$, and so $N(u) \subseteq \text{Fix}(\beta)$. Therefore $N(\beta(u)) = \beta(N(u)) = N(u)$, and so $\beta(u) \mathcal{R} u$. But $u \neq \beta(u)$ as $u \in \text{Fix}(\alpha)$. Thus $\mathcal{R} \neq \text{id}$. □

The next lemma will be needed to prove that every cubic vertex-transitive graph has a semiregular automorphism.

**Lemma 3.2.** Let $X$ be a connected vertex-transitive graph of prime valency $p$, let $v \in V(X)$ and let $G$ be a transitive subgroup of $\text{Aut}X$. Then $|G_v|$ is not divisible by $p^2$ nor by any prime greater than $p$.

**Proof.** Let $q$ be a prime dividing $|G_v|$. Then there is an automorphism $\alpha \in G_v$ of order $q$. Of course, any vertex not belonging to $\text{Fix}(\alpha)$ lies in an orbit of $\alpha$ of length $q$. Then, by connectedness, there are vertices $u, v \in V(X)$ such that $\alpha(u) = u$ and the orbit of $\alpha$ containing $v$ has length $q$. On the other hand, this orbit is contained in $N(u)$ which has cardinality $p$. So we have $q \leq p$.

Assume that $p$ divides $|G_v|$. We now prove that $p^2$ does not divide $|G_v|$. Let $P$ be a Sylow $p$-subgroup of $G_v$. We first show that if $\alpha \in P$ fixes some vertex in $N(v)$, then $\alpha = 1$. Since $X$ is connected every two vertices $x, y \in V(X)$ are joined by a path. Denote the distance between $x$ and $y$, that is the minimum length of a path from $x$ to $y$, by $d(x, y)$. Let $u \in V(X)$, with $d(v, u) = i$. By induction on $i$ we now prove that $\alpha(u) = u$. This is clearly true for $i = 0, 1$. Assume that $i \geq 2$ and that the statement is true for all vertices $u'$ such that $d(v, u') \leq i - 1$. Let $z$ and $w$ be the two vertices immediately preceding $u$ in a path of length $i$ from $v$ to $u$. Then $d(v, w), d(v, z) < i$ and so, by induction hypothesis, $\alpha(w) = w$ and $\alpha(z) = z$. It follows that $\alpha \in G_w$ and that $\alpha$ has a fixed point in $N(w)$, that is the vertex $z$. But then, since the valency of $X$ is a prime $p$, it follows that $\alpha$ fixes $N(w)$ pointwise. In particular, $\alpha(u) = u$. We conclude that $\alpha = 1$. In view of this fact we have that the homomorphism associating to an element $\alpha \in P$ its restriction $\alpha^{N(v)}$ to $N(v)$, must be a monomorphism. Hence $P$ is isomorphic to some subgroup of the symmetric group $S_p$.

But $p^2$ does not divide $p! = |S_p|$ and so $|P| = p$. □

**Theorem 3.3.** Every cubic vertex-transitive graph has a semiregular automorphism.
Proposition 3.2, every transitive permutation group of degree \( p^2 \) has a regular subgroup. Now Lemma 3.2 implies that an element of \( \{u, \alpha(u), \alpha^{-1}(u)\} \) is adjacent to any vertex of the set \( \{u, \beta(u), \beta^{-1}(u)\} \). In fact, for \( i = 0, 1, -1 \) and \( j = 0, 1, -1 \), the permutation \( \alpha^i \beta^j \in K \) maps the edge \( uv \) into \( \beta^j(u)\alpha^i(v) \). It follows that \( K_{3,3} \) is a subgraph of \( X \). But then since \( X \) is connected we have \( X \cong K_{3,3} \) and clearly \( X \) has a semiregular automorphism.

4. Digraphs of Order \( 2p^2 \)

Let \( X \) be a digraph and let \( v \in V(X) \) be a vertex of \( X \). We say that a vertex \( u \in V(X) \) is a predecessor of \( v \), and write \( u \rightarrow v \) if \( (u, v) \in A(X) \) is an arc of \( X \). Similarly, a vertex \( u \) is a successor of \( v \) if \( v \rightarrow u \). We use the notation \( P(v) \) and \( S(v) \), respectively, for the sets of predecessors and successors of \( v \). Of course, in a vertex-transitive digraph \( X \) we have that \( |P(v)| = |S(v)| \) for each \( v \in V(X) \).

Furthermore, we adopt the following notation. If \( U \) and \( W \) are disjoint subsets of \( V(X) \) we let \( X[U, W] \) denote the bipartite digraph induced by all those arcs of \( X \) of the form \( (u, w) \) and \( (w, u) \) with \( u \in U \) and \( w \in W \).

Theorem 4.1. A vertex-transitive digraph of order \( 2p^2 \) has a \((2p, p)\)-semiregular automorphism

Proof. In view of [6, Theorems 3.3, 3.4], we may assume that \( X \) is connected. Let \( P \) be a Sylow \( p \)-subgroup of \( \text{Aut} X \). In view of [9, Theorem 3.4], it follows that \( P \) has two orbits of length \( p^2 \), say \( A \) and \( B \). Let \( \alpha \in Z(P) \) be of order \( p \). Assume that \( \alpha \) is not semiregular. Then, without loss of generality, \( \alpha^A \) is semiregular and \( \alpha^B = 1 \). By [7, Proposition 3.2], every transitive permutation group of degree \( p^2 \) has a regular subgroup. Hence let \( Q \leq P \) be such that \( |Q^B| = p^2 \).

Assume first that \( Q^B = Z_{p^2} \). Then let \( \sigma \in Q \) be such that \( \sigma^B \) generates \( Q^B \), that is \( \sigma^B \)
is a \( p^2 \)-cycle. If \( \sigma^A \) is also a \( p^2 \)-cycle, then we obtain a \((2p, p)\)-semiregular automorphism of \( X \) by taking \( \pi = \sigma^p \). If \( \sigma^A \) is not a \( p^2 \)-cycle, then the above holds for \( \pi = \sigma^p \alpha \).

We may now assume that \( Q^B = Z_p \times Z_p \). Then there are elements \( \gamma, \delta \in Q \) such that \( (\gamma \delta)^B = Q^B \) and both \( \gamma^B, \delta^B \) are semiregular of order \( p \). Suppose first that one of \( \gamma^A \) and \( \delta^A \), say \( \gamma^A \), is not a \( p^2 \)-cycle. If \( \gamma^A = 1 \) then \( \pi = \gamma \alpha \) is a \((2p, p)\)-semiregular automorphism of \( X \). Hence we may assume that \( \gamma^A \) has order \( p \) and, moreover, \( \gamma \) has some fixed points in \( A \). But then \( \gamma^A \) must necessarily fix each of the orbits \( A_0, A_1, \ldots, A_{p-1} \) of \( \alpha \) in \( A \). Let \( B_0, B_1, \ldots, B_{p-1} \) be the orbits of \( \gamma^A \) in \( B \). Note that \( \alpha^B = 1 \) for each \( j \). But \( B_j \) is an orbit of \( \gamma \) and \( \gamma(A_i) = A_j \) for each \( i \). It transpires that for each \( i, j \) the arc set of \( X[A_i, B_j] \) is either empty or one of \( A_i \times B_j, B_j \times A_i \) and \( A_i \times B_j \cup B_j \times A_i \). It is then clear that the permutation \( \pi \), defined by the rule

\[
\pi(v) = \begin{cases} 
\alpha(v), & v \in A \\
\gamma(v), & v \in B,
\end{cases}
\]

is the desired automorphism of \( X \).

We are now left with the case where both \( \gamma^A \) and \( \delta^A \) are \( p^2 \)-cycles. If \( (\gamma^A) = (\delta^A) \) then say \( \gamma^A = (\delta^A)^i \) for some \( i \) and so \( (\gamma \delta^{-1})^A = 1 \). Since \( (\gamma \delta^{-1})^B \) has order \( p \), the automorphism \( \pi = \gamma \delta^{-1} \) has the desired form. Assume now that \( (\gamma^A) \neq (\delta^A) \). Note that the orbits of \( \alpha^A \) in \( A \) form an imprimitivity block system for \( P^A \). On the other hand, a cyclic group of order \( p^2 \) has only one imprimitivity block system. More precisely, if \( \gamma^A = (0, 1, \ldots, p^2 - 1) \), then this imprimitivity system consists of residue classes mod \( p \) in \( \{0, 1, \ldots, p^2 - 1\} \). Of course, the same must be true for \( \delta^A \). Without loss of generality we may assume that \( \delta^A(0) = 1 \). Then \( \gamma^A(\delta^A)^{-1} \) fixes 0 and certainly \( \gamma^A(\delta^A)^{-1} \neq 1 \). Hence \( \gamma^A(\delta^A)^{-1} \) has order \( p \). We may now apply the argument in the case where either \( \gamma^A \) or \( \delta^A \) was not a \( p^2 \)-cycle, by replacing \( \gamma \) with \( \gamma \delta^{-1} \). We have that the permutation \( \pi \), defined by the rule

\[
\pi(v) = \begin{cases} 
\alpha(v), & v \in A \\
\gamma \delta^{-1}(v), & v \in B
\end{cases}
\]

is the desired automorphism of \( X \), concluding the proof of Theorem 4.1. \( \square \)

References

D. Marušič
IMFM, Oddelek za matematiko,
Univerza v Ljubljani,
Jadranska 19, 61111 Ljubljana,
Slovenija
E-mail: dragan.marusic@uni-lj.si

R. Scapellato
Dipartimento di Matematica,
Politecnico di Milano,
Piazza Leonardo da Vinci 32,
20133 Milano,
Italy
E-mail: rafsc@mate.polimi.it