Some non-normal Cayley digraphs of the generalized quaternion group of certain orders

Edward Dobson

Department of Mathematics and Statistics
PO Drawer MA
Mississippi State, MS 39762, U.S.A.
dobson@math.msstate.edu

Submitted: Mar 10, 2003; Accepted: Jul 30, 2003; Published: Sep 8, 2003
MR Subject Classifications: 05C25, 20B25

Abstract

We show that an action of $\mathrm{SL}(2,p)$, $p \geq 7$ an odd prime such that $4 \not| (p-1)$, has exactly two orbital digraphs Γ_1, Γ_2, such that $\mathrm{Aut}(\Gamma_i)$ admits a complete block system $\mathcal{B}$ of $p+1$ blocks of size 2, $i = 1,2$, with the following properties: the action of $\mathrm{Aut}(\Gamma_i)$ on the blocks of $\mathcal{B}$ is nonsolvable, doubly-transitive, but not a symmetric group, and the subgroup of $\mathrm{Aut}(\Gamma_i)$ that fixes each block of $\mathcal{B}$ set-wise is semiregular of order 2. If $p = 2^k - 1 > 7$ is a Mersenne prime, these digraphs are also Cayley digraphs of the generalized quaternion group of order 2^{k+1}. In this case, these digraphs are non-normal Cayley digraphs of the generalized quaternion group of order 2^{k+1}.

There are a variety of problems on vertex-transitive digraphs where a natural approach is to proceed by induction on the number of (not necessarily distinct) prime factors of the order of the graph. For example, the Cayley isomorphism problem (see [6]) is one such problem, as well as determining the full automorphism group of a vertex-transitive digraph Γ. Many such arguments begin by finding a complete block system $\mathcal{B}$ of $\mathrm{Aut}(\Gamma)$. Ideally, one would then apply the induction hypothesis to the groups $\mathrm{Aut}(\Gamma)/\mathcal{B}$ and $\mathrm{fix}_{\mathrm{Aut}(\Gamma)}(\mathcal{B})|_B$, where $\mathrm{Aut}(\Gamma)/\mathcal{B}$ is the permutation group induced by the action of $\mathrm{Aut}(\Gamma)$ on $\mathcal{B}$, and $\mathrm{fix}_{\mathrm{Aut}(\Gamma)}(\mathcal{B})$ is the subgroup of $\mathrm{Aut}(\Gamma)$ that fixes each block of $\mathcal{B}$ set-wise, and $B \in \mathcal{B}$. Unfortunately, neither $\mathrm{Aut}(\Gamma)/\mathcal{B}$ nor $\mathrm{fix}_{\mathrm{Aut}(\Gamma)}(\mathcal{B})|_B$ need be the automorphism group of a digraph. In fact, there are examples of vertex-transitive graphs where $\mathrm{Aut}(\Gamma)/\mathcal{B}$ is a doubly-transitive nonsolvable group that is not a symmetric group (see [7]), as well as examples of vertex-transitive graphs where $\mathrm{fix}_{\mathrm{Aut}(\Gamma)}(\mathcal{B})|_B$ is a doubly-transitive nonsolvable group that is not a symmetric group (see [2]). (There are also examples where $\mathrm{Aut}(\Gamma)/\mathcal{B}$ is a solvable doubly-transitive group, but in practice, this is not usually a genuine obstacle in proceeding by induction.) The only known class of examples of vertex-transitive graphs where $\mathrm{Aut}(\Gamma)/\mathcal{B}$ is a doubly-transitive nonsolvable group, have the property that $\mathrm{Aut}(\Gamma)/\mathcal{B}$ is a faithful representation of $\mathrm{Aut}(\Gamma)$ and Γ is not a Cayley graph. In this paper, we give examples of vertex-transitive digraphs that are Cayley digraphs and the action of $\mathrm{Aut}(\Gamma)/\mathcal{B}$ on $\mathcal{B}$ is doubly-transitive, nonsolvable, not faithful, and not a symmetric group.

1 Preliminaries

Definition 1.1 Let G be a permutation group acting on Ω. If $\omega \in \Omega$, then a *sub-orbit of* G is an orbit of $\mathrm{Stab}_G(\omega)$.

Definition 1.2 Let G be a finite group. The *socle* of G, denoted $\mathrm{soc}(G)$, is the product of all minimal normal subgroups of G. If G is primitive on Ω but not doubly-transitive, we say G is *simply primitive*. Let G be a transitive permutation group on a set Ω and let G act on $\Omega \times \Omega$ by $g(\alpha,\beta) = (g(\alpha), g(\beta))$. The orbits of G in $\Omega \times \Omega$ are called the *orbitals* of G. The orbit $\{(\alpha,\alpha) : \alpha \in \Omega\}$ is called the *trivial orbital*. Let Δ be an orbital of G in $\Omega \times \Omega$. Define the *orbital digraph* Δ to be the graph with vertex set Ω and edge set Δ. Each orbital of G has a *paired orbital* $\Delta' = \{(\beta,\alpha) : (\alpha,\beta) \in \Delta\}$. Define the *orbital graph* Δ to be the graph with vertex set Ω and edge set $\Delta \cup \Delta'$. Note that there is a canonical bijection from the set of orbital digraphs of G to the set of sub-orbits of G (for fixed $\omega \in \Omega$).

Definition 1.3 Let G be a transitive permutation group of degree mk that admits a complete block system $\mathcal{B}$ of m blocks of size k. If $g \in G$, then g permutes the m blocks of $\mathcal{B}$ and hence induces a permutation in S_m, which we denote by $g/\mathcal{B}$. We define $G/\mathcal{B} = \{g/\mathcal{B} : g \in G\}$. Let $\mathrm{fix}_{\mathcal{B}}(G) = \{g \in G : g(B) = B \text{ for every } B \in \mathcal{B}\}$.

Definition 1.4 Let G be transitive group acting on Ω with r orbital digraphs $\Gamma_1, \ldots, \Gamma_r$. Define the 2-*closure of* G, denoted $G^{(2)}$ to be $\cap_{i=1}^{r}\mathrm{Aut}(\Gamma_i)$. Note that if G is the automorphism group of a vertex-transitive digraph, then $G^{(2)} = G$.

Definition 1.5 Let Γ be a graph. Define the *complement of* Γ, denoted by $\bar{\Gamma}$, to be the graph with $V(\bar{\Gamma}) = V(\Gamma)$ and $E(\bar{\Gamma}) = \{uv : u, v \in V(\Gamma) \text{ and } uv \notin E(\Gamma)\}$.

Definition 1.6 A group G given by the defining relations

$$G = \langle h, k : h^{2^{a-1}} = k^2 = m, m^2 = 1, k^{-1}hk = h^{-1}\rangle$$

is a *generalized quaternion group*.

Let $p \geq 5$ be an odd prime. Then $\mathrm{GL}(2,p)$ acts on the set $\mathbb{F}_p^2$, where $\mathbb{F}_p$ is the field of order p, in the usual way. This action has two orbits, namely $\{0\}$ and $\Omega = \mathbb{F}_p^2 - \{0\}$. The action of $\mathrm{GL}(2,p)$ on Ω is imprimitive, with a complete block system $\mathcal{C}$ of $(p^2-1)/(p-1) = p+1$ blocks of size $p-1$, where the blocks of $\mathcal{C}$ consist of all scalar multiples of a given vector in Ω (these blocks are usually called *projective points*), and the action of $\mathrm{GL}(2,p)$ on the blocks of $\mathcal{C}$ is doubly-transitive. Furthermore, $\mathrm{fix}_{\mathrm{GL}(2,p)}(\mathcal{C})$ is cyclic of order $p-1$, and consists of all scalar matrices αI (where I is the 2×2 identity matrix) in $\mathrm{GL}(2,p)$. Note that if $m|(p-1)$, then $\mathrm{GL}(2,p)$ admits a complete block system $\mathcal{C}_m$ of $(p+1)m$ blocks of size $(p-1)/m$, and $\mathrm{fix}_{\mathrm{GL}(2,p)}(\mathcal{C}_m)$ consists of all scalar matrices $\alpha^i I$, where $\alpha\in\mathbb{F}_p^*$ is of order $(p-1)/m$ and $i\in\mathbb{Z}$. Each such block of $\mathcal{C}_m$ consists of all scalar multiples $\alpha^i v$, where v is a vector in $\mathbb{F}_p^2$ and $i\in\mathbb{Z}$. Hence $\mathrm{GL}(2,p)/\mathcal{C}_m$ admits a complete block system $\mathcal{D}_m$ consisting of $p+1$ blocks of size m, induced by $\mathcal{C}_m$. Henceforth, we set $m=2$ so that $\mathcal{C}_2$ consists of $2(p+1)$ blocks of size $(p-1)/2$, and $\mathcal{D}_2$ consists of $p+1$ blocks of size 2. Note that as $p\geq 5$, $\mathrm{SL}(2,p)$ is doubly-transitive on the set of projective points, as if $A\in\mathrm{GL}(2,p)$, then $\det(A)^{-1}A\in\mathrm{SL}(2,p)$. Finally, observe that $(-1)I\in\mathrm{SL}(2,p)$. Thus $(-1)I/\mathcal{C}_2\in\mathrm{fix}_{\mathrm{SL}(2,p)/\mathcal{C}_2}(\mathcal{D}_2)\neq 1$ so that $\mathrm{SL}(2,p)/\mathcal{C}_2$ is transitive on $\mathcal{C}_2$. Additionally, as $\mathrm{fix}_{\mathrm{GL}(2,p)}(\mathcal{C}_2)=\{\alpha^i I : |\alpha|=(p-1)/2, i\in\mathbb{Z}\}$, $\mathrm{SL}(2,p)/\mathcal{C}_2\cong\mathrm{SL}(2,p)$. That is, $\mathrm{SL}(2,p)/\mathcal{C}_2$ is a faithful representation of $\mathrm{SL}(2,p)$. We will thus lose no generality by referring to an element $x/\mathcal{C}_2\in\mathrm{SL}(2,p)/\mathcal{C}_2$ as simply $x\in\mathrm{SL}(2,p)$. As each projective point can be written as a union of two blocks contained in $\mathcal{C}_2$, we will henceforth refer to blocks in $\mathcal{C}_2$ as *projective half-points*.

2 Results

We begin with a preliminary result.

Lemma 2.1 *Let $p\geq 7$ be an odd prime such that $4\not|\,(p-1)$, and let $\mathrm{SL}(2,p)$ act as above on the $2(p+1)$ projective half-points. Then the following are true:*

1. *$\mathrm{SL}(2,p)$ has exactly four sub-orbits; two of size 1 and 2 of size p,*
2. *$\mathrm{SL}(2,p)$ admits exactly one non-trivial complete block system which consists of $p+1$ blocks of size 2, namely $\mathcal{D}_2$, formed by the orbits of $(-1)I$.*

Proof. By [4, Theorem 2.8.1], $|\mathrm{SL}(2,p)|=(p^2-1)p$. It was established above that $\mathrm{SL}(2,p)$ admits $\mathcal{D}_2$ as a complete block system of $p+1$ blocks of size 2, and this complete block system is formed by the orbits of $(-1)I$ as $(-1)I\in\mathrm{fix}_{\mathrm{SL}(2,p)}(\mathcal{D}_2)$ and is semi-regular of order 2. As $\mathrm{SL}(2,p)/\mathcal{D}_2=\mathrm{PSL}(2,p)$ is doubly-transitive, there are two sub-orbits of $\mathrm{SL}(2,p)/\mathcal{D}_2$, one of size 1 and the other of size p. Now, consider $\mathrm{Stab}_{\mathrm{SL}(2,p)}(x)$, where x is a projective half-point. Then there exists another projective half-point y such that $x\cup y$ is a projective point z. As $\{x,y\}\in\mathcal{D}_2$ is a block of size 2 of $\mathrm{SL}(2,p)$, we have that $\mathrm{Stab}_{\mathrm{SL}(2,p)}(x)=\mathrm{Stab}_{\mathrm{SL}(2,p)}(y)$. Thus $\mathrm{SL}(2,p)$ has at least two singleton sub-orbits. As $\mathrm{SL}(2,p)/\mathcal{D}_2=\mathrm{PSL}(2,p)$ has one singleton sub-orbit, $\mathrm{SL}(2,p)$ has exactly two singleton sub-orbits. We conclude that every non-singleton sub-orbit of $\mathrm{SL}(2,p)$ has order a multiple of p. As the non-singleton sub-orbits of $\mathrm{SL}(2,p)$ have order a multiple of p, $\mathrm{Stab}_{\mathrm{SL}(2,p)}(x)$ has either one non-singleton orbit of size $2p$ or two non-singleton orbits of size p. As the order of a non-singleton orbit must divide $|\mathrm{Stab}_{\mathrm{SL}(2,p)}(x)|=p(p-1)/2$ which is odd as

$4 \not| (p-1)$, $\mathrm{SL}(2,p)$ must have exactly two non-singleton sub-orbits of size p. Thus 1) follows.

Suppose that $\mathcal{D}$ is another non-trivial complete block system of $\mathrm{SL}(2,p)$. Let $D \in \mathcal{D}$ with v a projective half-point in D. By [3, Exercise 1.5.9], D is a union of orbits of $\mathrm{Stab}_{\mathrm{SL}(2,p)}(v)$, so that $|D|$ is either 2, $p+1$, $p+2$, $2p$, or $2p+1$. Furthermore, as the size of a block of a permutation group divides the degree of the permutation group, $|D| = 2$ or $p+1$. If $|D| = 2$, then D is the union of two singleton orbits of $\mathrm{Stab}_{\mathrm{SL}(2,p)}(v)$, in which case D consists of two projective half-points whose union is a projective point. Thus if $|D| = 2$, then $D \in \mathcal{D}_2$ and $\mathcal{D} = \mathcal{D}_2$. If $|D| = p+1$, then $\mathcal{D}$ consists of 2 blocks of size $p+1$ and D is the union of two orbits of $\mathrm{Stab}_{\mathrm{SL}(2,p)}(v)$, and these orbits have size 1 and p. We conclude that $\cup D$ does not contain the projective point q that contains v.

Now, $\mathrm{fix}_{\mathrm{SL}(2,p)}(\mathcal{D})$ cannot be trivial, as $\mathrm{SL}(2,p)/\mathcal{D}$ is of degree 2 while $|\mathrm{SL}(2,p)| = (p^2-1)p$. Then $|\mathrm{fix}_{\mathrm{SL}(2,p)}(\mathcal{D})| = (p^2-1)p/2$ as $\mathrm{SL}(2,p)/\mathcal{D}$ is a transitive subgroup of S_2. Furthermore, $-I \notin \mathrm{fix}_{\mathrm{SL}(2,p)}(\mathcal{D})$ as no block of $\mathcal{D}$ contains the projective point q that contains v so that $-I$ permutes the two projective half-points whose union is q. Thus $\mathrm{fix}_{\mathrm{SL}(2,p)}(\mathcal{D}_2) \cap \mathrm{fix}_{\mathrm{SL}(2,p)}(\mathcal{D}) = 1$. As $\langle -I\rangle = \mathrm{fix}_{\mathrm{SL}(2,p)}(\mathcal{D}_2)$ and both $\mathrm{fix}_{\mathrm{SL}(2,p)}(\mathcal{D}_2)$ and $\mathrm{fix}_{\mathrm{SL}(2,p)}(\mathcal{D})$ are normal in $\mathrm{SL}(2,p)$, we have that $\mathrm{SL}(2,p) = \mathrm{fix}_{\mathrm{SL}(2,p)}(\mathcal{D}_2) \times \mathrm{fix}_{\mathrm{SL}(2,p)}(\mathcal{D})$. Thus a Sylow 2-subgroup of $\mathrm{SL}(2,p)$ can be written as a direct product of two nontrivial 2-groups, contradicting [4, Theorem 8.3]. □

Theorem 2.2 *Let $p \geq 7$ be an odd prime such that $4 \not| (p-1)$. Then there exist exactly two digraphs Γ_i, $i = 1,2$ of order $2(p+1)$ such that the following properties hold:*

1. *Γ_i is an orbital digraph of $\mathrm{SL}(2,p)$ in its action on the set of projective half-points and is not a graph,*
2. *$\mathrm{Aut}(\Gamma_i)$ admits a unique nontrivial complete block system $\mathcal{D}_2$ which consists of $p+1$ blocks of size 2,*
3. *$\mathrm{fix}_{\mathrm{Aut}(\Gamma_i)}(\mathcal{D}_2) = \langle -I\rangle$ is cyclic of order 2,*
4. *$\mathrm{soc}(\mathrm{Aut}(\Gamma_i)/\mathcal{D}_2)$ is doubly-transitive but $\mathrm{soc}(\mathrm{Aut}(\Gamma_i)/\mathcal{D}_2) \neq A_{p+1}$.*

PROOF. By Lemma 2.1, $\mathrm{SL}(2,p)$ in its action on the half-projective points has exactly four orbital digraphs; one consisting of $p+1$ independent edges (the edges of this graph consists of all edges of the form (v,w), where $\cup\{v,w\}$ is a projective point; thus $\cup\{v,w\}$ is a block of $\mathcal{D}_2$), one which consists of only self-loops (and so is trivial with automorphism group S_{2p+2} and will henceforth be ignored) and two in which each vertex has in and out degree p. The orbital digraph Γ of $\mathrm{SL}(2,p)$ consisting of $p+1$ independent edges is then $\bar{K}_{p+1} \wr K_2$. The other orbital digraphs of $\mathrm{SL}(2,p)$, say Γ_1 and Γ_2, each have in-degree and out-degree p.

If either Γ_1 or Γ_2 is a graph, then assume without loss of generality that Γ_1 is a graph. Then whenever $(a,b) \in E(\Gamma_1)$ then $(b,a) \in E(\Gamma_1)$. As Γ_1 is an orbital digraph, there exists $\alpha \in \mathrm{SL}(2,p)$ such that $\alpha(a) = b$ and $\alpha(b) = a$. Raising α to an appropriate odd power, we may assume that α has order a power of 2, and so $\alpha \in Q$, where Q is a Sylow 2-subgroup of $\mathrm{SL}(2,p)$. As a Sylow 2-subgroup of $\mathrm{SL}(2,p)$ is isomorphic to a generalized quaternion by [4, Theorem 8.3], Q contains a unique subgroup of order 2 (see [4, pg. 29]), which is necessarily $\langle -I\rangle$. If α is not of order 2, then $\alpha^2(a)=a$ and $\alpha^2(b)=b$ so that α has at least two fixed points. However, $(\alpha^2)^c=-I$ for some $c\in\mathbb{Z}$ and $-I$ has no fixed points, a contradiction. Thus α has order 2 and so $\alpha=-I$. Thus $(a,b)\in \bar{K}_{p+1}\wr K_2\neq \Gamma_1$, a contradiction. Hence 1) holds.

We now establish that 2) holds. Suppose that for $i=1$ or 2, $\mathrm{Aut}(\Gamma_i)$ is primitive. We may then assume without loss of generality that $\mathrm{Aut}(\Gamma_1)$ is primitive, and as $\mathrm{Aut}(\Gamma_1)\neq K_{2(p+1)}$, $\mathrm{Aut}(\Gamma_1)$ is simply primitive, and, of course, $\mathrm{SL}(2,p)^{(2)}\leq \mathrm{Aut}(\Gamma_1)$. First observe that by [11, Theorem 4.11], $\mathrm{SL}(2,p)^{(2)}$ admits $\mathcal{D}_2$ as a complete block system. Let v be a projective half-point. By Lemma 2.1, $\mathrm{SL}(2,p)$ has four sub-orbits relative to v, two of size 1, say $\mathcal{O}_1=\{v\}$ and $\mathcal{O}_2=\{w\}$, and two of size p, say $\mathcal{O}_3$ and $\mathcal{O}_4$. By [11, Theorem 5.5 (ii)] the sub-orbits of $\mathrm{SL}(2,p)^{(2)}$ relative to v are the same as the sub-orbits of $\mathrm{SL}(2,p)$ relative to v. Thus the neighbors of v in Γ_1 consist of all elements in one of the sub-orbits $\mathcal{O}_3$ or $\mathcal{O}_4$. Without loss of generality, assume that this sub-orbit is $\mathcal{O}_3$. As $\mathrm{Aut}(\Gamma_1)$ is primitive, by [3, Theorem 3.2A], every non-trivial orbital digraph of $\mathrm{Aut}(\Gamma_1)$ is connected. Then the orbital digraph of $\mathrm{Aut}(\Gamma_1)$ that contains $\vec{vw}$ is connected, and so $\mathcal{O}_2=\{w\}$ is not a sub-orbit of $\mathrm{Aut}(\Gamma_1)$. Of course, $\mathrm{Aut}(\Gamma_1)=\mathrm{Aut}(\bar{\Gamma}_1)$ so that $\mathrm{Aut}(\bar{\Gamma}_1)$ is primitive as well. As if $\mathrm{Aut}(\Gamma_1)$ has exactly two sub-orbits, then $\mathrm{Aut}(\Gamma_1)$ is doubly-transitive and hence $\Gamma_1=K_{2(p+1)}$ which is not true, $\mathrm{Aut}(\Gamma_1)$ has exactly three sub-orbits. Clearly $\mathcal{O}_3$ is a sub-orbit of $\mathrm{Aut}(\Gamma_1)$ so that the only sub-orbits of $\mathrm{Aut}(\Gamma_1)$ relative to v are $\mathcal{O}_1$, $\mathcal{O}_3$, and $\mathcal{O}_2\cup\mathcal{O}_4$. Thus the neighbors of v in $\bar{\Gamma}_1$ are all contained in one sub-orbit of $\mathrm{Aut}(\Gamma_1)$ relative to v. However, one of these directed edges is an edge (as $\bar{\Gamma}_1=\Gamma_2\cup(\bar{K}_{p+1}\wr K_2)$), and so every neighbor of v in $\bar{\Gamma}_1$ is an edge. Thus every neighbor of v in Γ_1 is an edge. However, we have already established that Γ_1 is a digraph that is not a graph, a contradiction. Whence $\mathrm{Aut}(\Gamma_i)$, $i=1,2$, are not primitive, and as $\mathrm{SL}(2,p)\leq\mathrm{Aut}(\Gamma_i)$, we have by Lemma 2.1 that $\mathcal{D}_2$ is the unique complete block system of $\mathrm{Aut}(\Gamma_i)$, $i=1,2$. Thus (2) holds.

If $\mathrm{fix}_{\mathrm{Aut}(\Gamma_i)}(\mathcal{D}_2)$ is not cyclic, then there exists $1\neq\gamma\in\mathrm{fix}_{\mathrm{Aut}(\Gamma_i)}(\mathcal{D}_2)$ such that $\gamma(v)=v$ for some $v\in V(\Gamma_i)$. It is then easy to see that $\mathrm{Aut}(\Gamma_i)$ has only three sub-orbits, two of size 1, and one of size $2p$, a contradiction. Thus (3) holds.

To establish (4), as $\mathrm{SL}(2,p)/\mathcal{D}_2=\mathrm{PSL}(2,p)$ which is doubly-transitive in its action on the blocks (projective points) of $\mathcal{D}_2$, we have that $\mathrm{Aut}(\Gamma_i)/\mathcal{D}_2$ is doubly-transitive. As $\mathrm{PSL}(2,p)\leq\mathrm{Aut}(\Gamma_i)/\mathcal{D}_2$, by [1, Theorem 5.3] $\mathrm{soc}(\mathrm{Aut}(\Gamma_i)/\mathcal{D}_2)$ is a doubly-transitive non-abelian simple group acting on $p+1$ points. Thus we need only show that $\mathrm{soc}(\mathrm{Aut}(\Gamma_i)/\mathcal{D}_2)\neq A_{p+1}$.

Assume that $\mathrm{soc}(\mathrm{Aut}(\Gamma_i)/\mathcal{D}_2)=A_{p+1}$. Recall that as p is odd, a Sylow 2-subgroup Q of $\mathrm{SL}(2,p)$ is a generalized quaternion group. Furthermore, the unique element of Q of order 2, namely $-I$, is contained is every Sylow 2-subgroup of $\mathrm{SL}(2,p)$ and is semiregular. Observe that as $4\not|\,(p-1)$, $4|(p+1)$. Then Q contains an element δ such that $\delta/\mathcal{D}_2$ is a product of $(p+1)/4$ disjoint 4-cycles and $\langle\delta^4\rangle=\mathrm{fix}_{\mathrm{Aut}(\Gamma_i)}(\mathcal{D}_2)=\langle -I\rangle$. Let $\delta/\mathcal{D}_2=z_0\ldots z_{\frac{p+1}{4}-1}$ be the cycle decomposition of $\delta/\mathcal{D}_2$. As $\mathrm{soc}(\mathrm{Aut}(\Gamma_i)/\mathcal{D}_2)=A_{p+1}$, there exists $\omega \in \mathrm{Aut}(\Gamma_i)$ such that $\omega/\mathcal{D}_2 = z_0 z_1^{-1} \ldots z_{\frac{p+1}{4}-1}^{-1}$ (note that if $\omega/\mathcal{D}_2$ is not an even permutation, then $\delta/\mathcal{D}_2$ is not an even permutation, in which case $\mathrm{Aut}(\Gamma_i)/\mathcal{D}_2 = S_{p+1}$ and $\omega \in \mathrm{Aut}(\Gamma_i)$). Then $|\delta\omega/\mathcal{D}_2| = 2$ so that $(\delta\omega)^2 \in \mathrm{fix}_{\mathrm{Aut}(\Gamma_i)}(\mathcal{D}_2)$. Let $\mathcal{O}_0$ be the union of the non-singleton orbits of $\langle z_0\rangle$, and $\mathcal{O}_1$ be the union of the non-singleton orbits of $\langle z_1\rangle$ (note that as $p \geq 7$, $p+1 \geq 8$, so that $(p+1)/4 \geq 2$). Let $D \in \mathcal{D}_2$ such that $D \subset \mathcal{O}_1$. Then $\delta\omega|_D$ has order 1 or 2, so that $(\delta\omega)^2|_D = 1$. Thus if $\omega|_{\mathcal{O}_0} \in \delta|_{\mathcal{O}_0}$, then $(\delta\omega)^2 \in \mathrm{fix}_{\mathrm{Aut}(\Gamma_i)}(\mathcal{D}_2) = \langle -I\rangle$, $(\delta\omega)^2 \neq 1$, but $(\delta\omega)^2$ has a fixed point, a contradiction. Thus $\omega|_{\mathcal{O}_0} \notin \delta|_{\mathcal{O}_0}$. Then $H = \langle\delta,\omega\rangle|_{\mathcal{O}_0}$ has a complete block system $\mathcal{E}$ of 4 blocks of size 2 induced by $\mathcal{D}_2$. Furthermore, $H/\mathcal{E}$ is cyclic of order 4, so that $\mathrm{fix}_H(\mathcal{E})$ has order at least 4. Then $\mathrm{Stab}_H(v) \neq 1$ for every $v \in \mathcal{O}_0$. In particular, $\mathcal{E}$ consists of 4 blocks of size 2, and $\mathrm{Stab}_H(v)$ is the identity on some block of $\mathcal{E}$ while being transitive on some other block. As each block of $\mathcal{E}$ is also a block of $\mathcal{D}_2$, $\mathrm{Stab}_{\mathrm{Aut}(\Gamma)}(v)$ is transitive on some block D_v of $\mathcal{D}_2$. This then implies that $\mathrm{Stab}_{\mathrm{Aut}(\Gamma_i)}(v)$ has three orbits, two of size one and one of size $2(p+1)-2$, a contradiction. □

Corollary 2.3 *Let $p = 2^k - 1 > 7$ be a Mersenne prime. Then there exist exactly two digraphs Γ_i, $i = 1,2$ of order 2^{k+1} such that the following properties hold:*

1. *Γ_i is an orbital digraph of $\mathrm{SL}(2,p)$ in its action on the set of projective half-points and is not a graph,*
2. *$\mathrm{Aut}(\Gamma_i)$ admits a unique complete block system $\mathcal{D}_2$ which consists of 2^k blocks of size 2,*
3. *$\mathrm{fix}_{\mathrm{Aut}(\Gamma_i)}(\mathcal{D}_2)$ is cyclic of order 2,*
4. *$\mathrm{soc}(\mathrm{Aut}(\Gamma_i)/\mathcal{D}_2) = \mathrm{PSL}(2,p)$ is doubly-transitive,*
5. *Γ_i is a Cayley digraph of the generalized quaternion group of order 2^{k+1}.*

PROOF. In view of Theorem 2.2, we need only show that $\mathrm{soc}(\mathrm{Aut}(\Gamma_i)/\mathcal{D}_2) = \mathrm{PSL}(2,p)$ and that each Γ_i is a Cayley digraph of the generalized quaternion group Q of order 2^{k+1}. As $|\mathrm{SL}(2,p)| = 2^k(2^k-1)(2^k-2)$, a Sylow 2-subgroup of $\mathrm{SL}(2,p)$ has order 2^{k+1}, and as p is odd, is isomorphic to a generalized quaternion group of order 2^{k+1}. As a transitive group of prime power order q^ℓ contains a transitive Sylow q-subgroup [10, Theorem 3.4'], a Sylow 2-subgroup Q of $\mathrm{SL}(2,p)$ is transitive and thus regular. It then follows by [9] that each Γ_i is isomorphic to a Cayley digraph of Q. Furthermore, $\mathrm{Stab}_{\mathrm{Aut}(\Gamma_i)/\mathcal{D}_2}(v)$ is of index 2^k in $\mathrm{Aut}(\Gamma_i)/\mathcal{D}_2$. By [5, Theorem 1] we have that either $\mathrm{soc}(\mathrm{Aut}(\Gamma_i)/\mathcal{D}_2)$ is A_{2^k} or $\mathrm{PSL}(2,p)$. As by Theorem 2.2, $\mathrm{soc}(\mathrm{Aut}(\Gamma_i)/\mathcal{D}_2) \neq A_{2^k}$, the result follows. □

References

[1] Cameron, P. J., Finite permutation groups and finite simple groups, *Bull. London Math. Soc.* **13** (1981) 1–22.

[2] Cheng, Y., and Oxley, J., On weakly symmetric graphs of order twice a prime, *J. Comb. Theory Ser. B* **42** 1987, 196-211.

[3] Dixon, J.D., and Mortimer, B., *Permutation Groups*, Springer-Verlag New York, Berlin, Heidelberg, Graduate Texts in Mathematics, **163**, 1996.

[4] Gorenstein, D., *Finite Groups*, Chelsea Publishing Co., New York, 1968.

[5] Guralnick, R. M., Subgroups of prime power index in a simple group, *J. of Algebra* **81** 1983, 304-311.

[6] Li, C. H., On isomorphisms of finite Cayley graphs - a survey, *Disc. Math.*, **246** (2002), 301-334.

[7] Marušič, D., and Scapellato, R., Imprimitive Representations of $\mathrm{SL}(2, 2^k)$ *J. Comb. Theory Ser. B* **58** 1993, 46-57.

[8] Sabidussi, G., The composition of graphs, *Duke Math J.* **26** (1959), 693-696.

[9] Sabidussi, G. O., Vertex-transitive graphs, *Monatshefte für Math.* **68** 1964, 426-438.

[10] Wielandt, H. (trans. by R. Bercov), *Finite Permutation Groups*, Academic Press, New York, 1964.

[11] Wielandt, H., Permutation groups through invariant relations and invariant functions, lectures given at The Ohio State University, Columbus, Ohio, 1969.

[12] Wielandt, H., Mathematische Werke/Mathematical works. Vol. 1. Group theory, edited and with a preface by Bertram Huppert and Hans Schneider, Walter de Gruyter & Co., Berlin, 1994.