J Algebr Comb (2012) 36:21–31
DOI 10.1007/s10801-011-0321-5

Arc-regular cubic graphs of order four times an odd integer

Marston D.E. Conder · Yan-Quan Feng

Received: 16 May 2011 / Accepted: 21 September 2011 / Published online: 19 October 2011

Abstract A graph is arc-regular if its automorphism group acts sharply-transitively on the set of its ordered edges. This paper answers an open question about the existence of arc-regular 3-valent graphs of order $4m$ where m is an odd integer. Using the Gorenstein–Walter theorem, it is shown that any such graph must be a normal cover of a base graph, where the base graph has an arc-regular group of automorphisms that is isomorphic to a subgroup of Aut(PSL$(2,q)$) containing PSL$(2,q)$ for some odd prime-power q. Also a construction is given for infinitely many such graphs—namely a family of Cayley graphs for the groups PSL(2, p^3) where p is an odd prime; the smallest of these has order 9828.

Keywords Arc-regular graph · One-regular graph · Symmetric graph · Cayley graph

1 Introduction

Let X be a finite, simple, undirected graph, with vertex-set $V(X)$, edge-set $E(X)$, arc-set $A(X)$, and (full) automorphism group Aut(X). Note that an *arc* is an ordered edge (an ordered pair of adjacent vertices). An *s-arc* is an ordered $(s+1)$-tuple $(v_0, v_1, \ldots, v_s)$ of vertices such that v_{i-1} is adjacent to v_i for $1 \le i \le s$, and $v_{i-1} \ne v_{i+1}$ for $1 \le i < s$; in other words, a directed walk of length s in which any three consecutive vertices are distinct (so the walk never steps back along an edge just crossed).

M.D.E. Conder (✉)
Department of Mathematics, University of Auckland, Private Bag 92019, Auckland 1142, New Zealand
e-mail: m.conder@auckland.ac.nz

Y.-Q. Feng
Mathematics, Beijing Jiaotong University, Beijing 100044, P.R. China
e-mail: yqfeng@center.njtu.edu.cn

The graph X is said to be *s-arc-transitive* if $\mathrm{Aut}(X)$ is transitive on the set of all s-arcs in X, and *s-arc-regular* if $\mathrm{Aut}(X)$ is regular (that is, sharply-transitive) on the set of all s-arcs in X. In particular, 0-arc-transitive is the same as *vertex-transitive*, and 1-arc-transitive is the same as *arc-transitive*, or *symmetric*. Also the terms s-arc-transitive and s-arc-regular are often abbreviated to just *s-transitive* and *s-regular,* respectively; thus, for example, X is one-regular if $\mathrm{Aut}(X)$ is sharply-transitive on the arcs of X. Furthermore, any subgroup of $\mathrm{Aut}(X)$ that acts transitively (resp., regularly) on the s-arcs of X is said to be s-arc-transitive or s-transitive (resp., s-arc-regular or s-regular) on X.

In any connected s-arc-transitive graph, all vertices have the same valency. Conversely, any s-arc-regular graph in which all vertices have the same positive valency must be connected (for otherwise an s-arc in one component can be fixed by an automorphism moving vertices in another component). A 2-valent regular graph is arc-regular if and only if it is a cycle.

Arc-regular graphs with specific valency greater than 2 have received considerable attention. For example, Chao [2] classified all 4-valent arc-regular graphs of prime order, and Marušič [26] constructed an infinite family of 4-valent arc-regular Cayley graphs for alternating groups. All 4-valent one-regular circulant graphs were classified in [39], and all 4-valent one-regular Cayley graphs on abelian groups were classified in [38]. One may also obtain a classification of 4-valent one-regular Cayley graphs for dihedral groups from the work of Kwak and Oh [19] and Wang et al. [35, 36]. Next, by [3, 25, 27, 29, 30, 37, 38], we know that all 4-valent one-regular graphs of order p or pq (where p and q are primes) are circulant, and a classification of such graphs can be easily deduced from [39]. Furthermore, all 4-valent one-regular graphs of order $2pq$ were classified by Zhou and Feng [43]. On the other hand, Malnič et al. [24] constructed an infinite family of *infinite* one-regular graphs; see also [21, 31] for related results.

The first known example of a cubic (3-valent) one-regular graph is one with 432 vertices constructed by Frucht [15], and much subsequent work has been done in this line as part of a more general programme of investigation of cubic arc-transitive graphs; see [5–8, 10–14, 28], for example. Cheng and Oxley [3] proved that there are infinitely many cubic one-regular graphs of order $2p$ for p prime, and Zhou and Feng [42] classified all cubic one-regular graphs of order $2m$ where m is odd and square-free.

On the other hand, cubic one-regular graphs of order $4m$ where m is odd are more rare. To the best of our knowledge, there has been no previous construction of such graphs. There are no such graphs in the census of connected symmetric cubic graphs on up to 768 vertices complied by Conder and Dobcsányi [4]. Furthermore, Feng and Kwak [13] have shown that there is no cubic one-regular graph of order $4p$ or $4p^2$ for prime p, and Zhou and Feng [42] have shown there is also no such graph of order $4m$ where m is odd and square-free. Indeed in [42], it was conjectured that there is no cubic one-regular graph of order $4m$ for m odd.

In this paper, we will show that this conjecture is not true, by giving several examples. First, we use the Gorenstein–Walter theorem to prove that every one-regular cubic graph of order 4 times an odd integer is a normal cover of a base graph, which itself has a one-regular group of automorphisms isomorphic to a subgroup of Aut(PSL$(2,q)$) containing PSL$(2,q)$ for some odd prime-power q. Then we illustrate this by producing some examples for small values of q. Finally, we construct an infinite family of one-regular cubic Cayley graphs of order $p^3(p^6-1)/2$ for odd primes p. Taking $p \equiv 3$ or 5 (mod 8) gives such graphs with order 4 times an odd integer. The smallest one (for $p=3$) has order $9828 = 4 \times 2457$.

2 Preliminaries

Throughout this paper, we will denote by $\mathbb{Z}_n$ the cyclic group of order n, by D_n the dihedral group of order $2n$, and by S_n and A_n the symmetric group and alternating group of degree n, respectively. Also if G is a permutation group on a set Ω, then we denote by G_α the *stabilizer* of α in G (that is, the subgroup of G fixing the point α), for any $\alpha \in \Omega$. We say that G is *semiregular* on Ω if $G_\alpha = 1$ for every $\alpha \in \Omega$, and *regular* if G is transitive and semiregular on Ω, that is, if G is sharply-transitive on Ω.

We now introduce some preliminary results from the theory of groups. The first is well known, and sometimes called the N/C-theorem. For a subgroup H of a group G, denote by $C_G(H)$ the centralizer of H in G, and by $N_G(H)$ the normalizer of H in G. Conjugation of H by elements of $N_G(H)$ gives a homomorphism from $N_G(H)$ to the automorphism group Aut(H) of H, with kernel $C_G(H)$. In particular, $C_G(H)$ is normal in $N_G(H)$, and we have the following:

Proposition 2.1 [32, I. Theorem 6.11] *The quotient group $N_G(H)/C_G(H)$ is isomorphic to a subgroup of the automorphism group* Aut(H) *of H.*

The next proposition is due to Burnside.

Proposition 2.2 [18, Chap. IV, Theorem 2.6] *Let G be a finite group and let P be a Sylow p-subgroup of G. If $N_G(P) = C_G(P)$, then G has a normal p-complement, that is, a normal subgroup N such that $G = NP$ with $N \cap P = 1$.*

We will also need the Gorenstein–Walter theorem:

Proposition 2.3 [16, Sect. 16.3] *Let G be a finite group with dihedral Sylow 2-subgroups. Let N be the largest normal subgroup of G of odd order. Then G/N is isomorphic to*

(i) *a (dihedral) Sylow 2-subgroup of G, or*
(ii) *A_7, or*
(iii) *a subgroup of* Aut(PSL$(2,q)$) *containing* PSL$(2,q)$ *for some odd q.*

To prove our second main theorem, we need some facts about fields of order p^3:

Proposition 2.4 *For any odd prime p, let $K =$* GF(p^3) *be the field of order p^3, and let $F =$* GF(p) *be the base field of K. Then*

(a) *the multiplicative groups* K^* *and* F^* *of* K *and* F *are cyclic groups of order* p^3-1 *and* $p-1$, *respectively, and* $|K^*:F^*| = p^2+p+1$;
(b) K *has automorphism group of order* 3, *generated by the automorphism* $\alpha\colon x \mapsto x^p$;
(c) *if* $a \in K^*$, *then* $a \in F$ *if and only if* $a + a^{-1} \in F$; *and*
(d) *if* $t \in K$ *but* $t^3 \notin F$, *then* $t^{p-1} \notin F$ *but* $t^{p^2+p+1} \in F$.

Proof First, (a) and (b) are well known, with $\alpha\colon x \mapsto x^p$ the Frobenius automorphism. The "only if" part of (c) is obvious, so suppose that $a + a^{-1} \in F$. Then either $a + a^{-1} = 0$ or $(a + a^{-1})^{p-1} = 1$. If $a + a^{-1} = 0$, then $a^2 = (-a^{-1})^2 = a^{-2}$, so $a^4 = 1$, and then since $|K^*:F^*|$ is odd, this implies that $a \in F$. On the other hand, if $(a + a^{-1})^{p-1} = 1$, then by part (b) or just the fact that K has characteristic p, we find that $a + a^{-1} = (a + a^{-1})^p = a^p + a^{-p}$, so $a - a^p = a^{-p} - a^{-1} = a^{-1-p}(a - a^p)$. Hence either $a - a^p = 0$ or $a^{-1-p} = 1$. In the former case, $a^p = a$, so $a^{p-1} = 1$, and therefore $a \in F^*$. In the latter case, $a^{-1-p} = 1$, so $a^{p+1} = 1$. But $p^3 - 1 = (p+1)(p^2 - p + 1) - 2$, so $\gcd(p+1, p^3-1) = 2$, and hence there are integers s and t such that $2 = (p+1)s + (p^3-1)t$. Thus $a^2 = a^{(p+1)s+(p^3-1)t} = (a^{p+1})^s(a^{p^3-1})^t = 1$, which again implies that $a \in F$. This proves (c). Finally, for part (d), we note that $\gcd(p-1, p^2+p+1) = \gcd(p-1, 3) = 1$ or 3, since $p^2+p+1 = (p-1)(p+2)+3$. In particular, $t^{p-1} \notin F$, because $t^3 \notin F$. On the other hand, $t^{p^2+p+1} \in F$ since $|K^*:F^*| = p^2+p+1$. □

Next, we need the following, which follows from Dickson's classification [9] of subgroups of the projective special linear groups $\mathrm{PSL}(2,q)$; see also [18, II.8.27] or [17, Theorem 2.2].

Proposition 2.5 *Let* $q = p^3$ *where* p *is an odd prime. Then the group* $\mathrm{PSL}(2,q)$ *has four classes of maximal subgroups*:

(a) *subgroups isomorphic to* $\mathrm{PSL}(2,p)$;
(b) *dihedral subgroups of order* $q-1$;
(c) *dihedral subgroups of order* $q+1$;
(d) *subgroups isomorphic to a semidirect product* $\mathbb{Z}_p^3 \rtimes \mathbb{Z}_{\frac{q-1}{2}}$.

We also need some known facts about symmetric graphs and Cayley graphs. First, by a theorem of Tutte [33, 34], every finite connected cubic symmetric graph is s-arc-regular for some $s \le 5$, and the vertex stabilizer in its automorphism group is known:

Proposition 2.6 [10, Proposition 2-5] *Let* X *be a connected symmetric cubic graph, and let* G *be an* s*-regular subgroup of* $\mathrm{Aut}(X)$. *Then the stabilizer* G_v *of* $v \in V(X)$ *in* G *is isomorphic to* $\mathbb{Z}_3$, S_3, $S_3 \times \mathbb{Z}_2$, S_4, *or* $S_4 \times \mathbb{Z}_2$ *for* $s = 1, 2, 3, 4$, *or* 5, *respectively.*

Next, for a finite group G and a subset S of G such that $S = S^{-1}$ and $1 \notin S$, the *Cayley graph* $\mathrm{Cay}(G,S)$ for G with respect to S is defined to have vertex set G and edge set $\{\{g, sg\} \mid g \in G, s \in S\}$. Given $g \in G$, right multiplication $x \mapsto xg$ (for

$x \in G$) is a permutation $R(g)$ on G, and the homomorphism from G to $\mathrm{Sym}(G)$ taking each g to $R(g)$ is called the *right regular representation* of G. The image $R(G) = \{R(g) \mid g \in G\}$ of G is a regular permutation group on G, and is isomorphic to G, which can therefore be regarded as a subgroup of the automorphism group $\mathrm{Aut}(\mathrm{Cay}(G, S))$. In particular, the Cayley graph $\mathrm{Cay}(G, S)$ is vertex-transitive. Moreover, the group $\mathrm{Aut}(G, S) = \{\alpha \in \mathrm{Aut}(G) \mid S^\alpha = S\}$ is a subgroup of $\mathrm{Aut}(\mathrm{Cay}(G, S))$, indeed of the stabilizer $\mathrm{Aut}(\mathrm{Cay}(G, S))_1$ of the vertex 1. Also a Cayley graph $\mathrm{Cay}(G, S)$ is said to be *normal* if $R(G)$ is normal in $\mathrm{Aut}(\mathrm{Cay}(G, S))$.

Proposition 2.7 [40, Propositions 1.3 and 1.5] *A Cayley graph* $X = \mathrm{Cay}(G, S)$ *is normal if and only if* $\mathrm{Aut}(\mathrm{Cay}(G, S))_1 = \mathrm{Aut}(G, S)$, *or equivalently*, *if and only if* $\mathrm{Aut}(X)$ *is isomorphic to the semidirect product* $R(G) \rtimes \mathrm{Aut}(G, S)$.

Automorphism groups of symmetric cubic Cayley graphs for non-abelian simple groups were investigated by Xu et al. in [41], leading to the following remarkable result:

Proposition 2.8 [41, Theorem 1.1] *Let G be a finite non-abelian simple group*, *and let X be a connected symmetric cubic Cayley graph for G. Then either X is a normal Cayley graph*, *or otherwise* $G = A_{47}$ *and* $\mathrm{Aut}(X) = A_{48}$.

Finally, suppose that G is a group of automorphisms acting vertex-transitively on the graph X, and let N be a normal subgroup of G. Then the *quotient graph* X_N of X relative to N is defined as the graph with vertices the orbits of N in $V(X)$, and with two such orbits adjacent in X_N if there is an edge in X between those two orbits. Also X is a *cover* of X_N when the graph induced between two adjacent N-orbits is a perfect matching. (Indeed, it is a *normal cover* of X_N, since N is a normal subgroup of the vertex-transitive group G.) In the special case where X is a symmetric cubic graph and G acts arc-transitively on X, we have the following (from [20, Theorem 9]):

Proposition 2.9 *If N has more than two orbits in $V(X)$*, *then X_N is also a symmetric cubic graph*, *and N is the kernel of the action of G on the set of orbits of N. Moreover*, *the action of N on $V(X)$ is semiregular*, *and G/N is arc-transitive on X_N*.

3 Classification and construction of examples

We begin with a theorem that restricts the structure of the automorphism groups of one-regular cubic graphs of order 4 times an odd integer.

Theorem 3.1 *Let X be a one-regular cubic graph of order* $4m$ *where m is odd. Then X is a normal cover of a base graph Y*, *where Y has an arc-regular group of automorphisms that is isomorphic to a subgroup of* $\mathrm{Aut}(\mathrm{PSL}(2, q))$ *containing* $\mathrm{PSL}(2, q)$ *for some odd prime-power q*.

Proof Let $A=\mathrm{Aut}(X)$. By one-regularity of X, we know that $|A|=3|V(X)|=12m$. Also let P be a Sylow 2-subgroup of A. Then $|P|=4$, so $P\cong\mathbb{Z}_4$ or $\mathbb{Z}_2\times\mathbb{Z}_2$.

Suppose $P\cong\mathbb{Z}_4$. Then by Proposition 2.1, $N_A(P)/C_A(P)\lesssim\mathrm{Aut}(P)\cong\mathrm{Aut}(\mathbb{Z}_4)\cong\mathbb{Z}_2$. Hence $|N_A(P)/C_A(P)|=1$ or 2. If $|N_A(P)/C_A(P)|=2$ then since $C_A(P)$ contains P (which has order 4), we find that $|N_A(P)|$ (and hence $|A|$) is divisible by $2\times 4=8$, a contradiction. Thus $|N_A(P)/C_A(P)|=1$, so $N_A(P)=C_A(P)$, and Proposition 2.2 applies, giving a normal subgroup T in A such that $A=TP$ and $T\cap P=1$. In particular, $|T|=|A|/|P|=12m/4=3m$, and then since $|V(X)|=4m$, it follows that T must have four orbits on $V(X)$, with vertex-stabilizer $T_u\cong\mathbb{Z}_3$ (for some vertex u in any orbit). But on the other hand, Proposition 2.9 implies that T is semiregular on $V(X)$, a contradiction.

Thus $P\cong\mathbb{Z}_2\times\mathbb{Z}_2$. Let N be the largest normal subgroup of A of odd order. Then N has at least four orbits on $V(X)$. By Proposition 2.9, X is a normal cover of the quotient graph X_N and A/N is one-regular on X_N. If $|N|=3m$ then, again by Proposition 2.9, N is semiregular on $V(X)$, which is impossible. Thus $|N|<3m$, and in particular, $A/N\ncong P$. Also $A/N\ncong A_7$, since $|A|$ is not divisible by 8. By Proposition 2.3, we conclude that A/N is isomorphic to a subgroup of $\mathrm{Aut}(\mathrm{PSL}(2,q))$ containing $\mathrm{PSL}(2,q)$, for some odd q. By taking $Y=X_N$, this completes the proof of the theorem. □

We now give some examples of such graphs, for small values of q.

Example 3.2 In the group GL(6, 3), consider the following two matrices:

$$a=\begin{pmatrix}1&0&0&0&0&0\\0&1&0&0&0&0\\1&0&0&0&1&0\\-1&0&0&-1&0&0\\-1&0&1&0&0&0\\0&0&0&0&0&1\end{pmatrix},\qquad b=\begin{pmatrix}0&1&0&0&0&0\\0&0&1&0&0&0\\1&0&0&0&0&0\\0&0&0&0&1&0\\0&0&0&-1&-1&0\\1&1&1&1&1&1\end{pmatrix}.$$

These can be written as $a=\begin{pmatrix}x&0\\0&1\end{pmatrix}$ and $b=\begin{pmatrix}y&0\\v&1\end{pmatrix}$ where x and y are elements of GL(5, 3) satisfying the defining relations for a one-regular group of automorphisms of the graph F220A in the census of symmetric cubic graphs of small order [4]. In particular, $\langle x,y\rangle$ is isomorphic to PSL(2, 11). Also, the element $c=((ab)^3(ab^{-1})^3)^2$ has the form $\begin{pmatrix}I_5&0\\w&1\end{pmatrix}$, and this element and its conjugates by b, b^{-1}, ba and bab generate an elementary abelian subgroup N of order 3^5, which is normal in the group A generated by a and b. In particular, A is isomorphic to an extension of $N\cong(\mathbb{Z}_3)^5$ by PSL(2, 11). Thus A acts regularly on the arcs of a connected cubic graph X of order 53460, which is a 3^5-fold cover of $X_N\cong$ F220A. There is, however, no automorphism of A which takes the generators a and b to their inverses, because $abababab^{-1}ababab^{-1}ab^{-1}$ has order 5 while $ab^{-1}ab^{-1}ab^{-1}abab^{-1}ab^{-1}abab$ has order 15. Hence by observations in [5] or [10], this graph has no 2-arc or 3-arc regular group of automorphisms. It also has no 4- or 5-arc regular group of automorphisms because otherwise, by [7], its automorphism group would have a composition factor isomorphic to PSL$(2,7)$, which is impossible. Thus X is one-regular.

There are many such cubic one-regular covers of F220A obtainable in this way, such as another one with $N \cong (\mathbb{Z}_7)^{11}$. These elementary abelian covers can also be found in a slightly different way, using the technique of lifting symmetries (as described in [23]).

Example 3.3 A similar approach gives cubic one-regular covers of F364A, including one with automorphism group an extension of $(\mathbb{Z}_3)^7$ by PSL$(2,13)$, and another with automorphism group an extension of $(\mathbb{Z}_7)^{14}$ by PSL$(2,13)$.

Example 3.4 The graph F108 in the census [4] is 2-arc regular, with automorphism group an extension G of $(\mathbb{Z}_3)^3$ by S_4, with the index 2 subgroup $H = (\mathbb{Z}_3)^3 \rtimes A_4$ acting regularly on one-arcs. This graph has numerous arc-transitive abelian covers with automorphism group an extension of an abelian normal subgroup by either H or G. Among them there is a one-regular cubic graph X of order $3^6 \cdot 108$ with $\mathrm{Aut}(X) \cong (\mathbb{Z}_3)^6 \rtimes H$. Note that since $A_4 \cong \mathrm{PSL}(2,3)$, the group Aut$(X)$ is an extension by PSL$(2,3)$ of a metabelian 3-group N of order 3^9, and the quotient X_N is the tetrahedral graph K_4. There are other such examples with $\mathrm{Aut}(X) \cong (\mathbb{Z}_3)^k \rtimes H$ for various values of k between 6 and 49, or with $\mathrm{Aut}(X) \cong (\mathbb{Z}_5)^k \rtimes H$ for many values of k (including $k = 6$), and others with different possibilities for N besides these. Details are available from the first author on request.

There are similar examples of cubic one-regular 'covers of covers' of the dodecahedral graph F20A, with Aut(X) an extension of a metabelian 3-group N by $A_5 \cong \mathrm{PSL}(2,5)$.

Next, we note that PSL$(2,q)$ is a quotient of the modular group $\mathrm{PSL}(2,\mathbb{Z}) \cong \mathbb{Z}_2 * \mathbb{Z}_3$ and so acts regularly on the arcs of some cubic graph Y, for all $q \neq 9$; see [22]. When $q \equiv 3$ or 5 (mod 8), the order of this graph Y is 4 times an odd integer. On the basis of the limited evidence provided by the above (and many similar) examples, we conjecture that for every prime-power $q > 9$, there are infinitely many one-regular cubic graphs with automorphism group an extension of a nilpotent group of odd order by PSL$(2,q)$.

Before giving our second main theorem, we need a little more notation. For any matrix $M \in \mathrm{SL}(2,K)$, we will denote by $\overline{M}$ the image of M under the natural homomorphism from SL$(2,K)$ to $\mathrm{PSL}(2,K) = \mathrm{SL}(2,K)/Z(\mathrm{SL}(2,K))$.

Theorem 3.5 *For any odd prime p, let $K = \mathrm{GF}(p^3)$ be the field of order p^3, let α be the Frobenius automorphism of K, and for any element $t \in K$ such that t^3 lies outside the base field $F = \mathrm{GF}(p)$, let*

$$U = \begin{pmatrix} 1 & -2t \\ t^{-1} & -1 \end{pmatrix}, \qquad V = U^\alpha = \begin{pmatrix} 1 & -2t^p \\ t^{-p} & -1 \end{pmatrix}, \quad \textit{and}$$

$$W = V^\alpha = \begin{pmatrix} 1 & -2t^{p^2} \\ t^{-p^2} & -1 \end{pmatrix}.$$

Then

(i) *the images* $\overline{U}$, $\overline{V}$ *and* $\overline{W}$ *generate* $\mathrm{PSL}(2,K)$, *and*
(ii) *the Cayley graph* $\mathrm{Cay}(\mathrm{PSL}(2,K),\{\overline{U},\overline{V},\overline{W}\})$ *is a one-regular cubic graph.*

Proof First, since $\mathrm{Tr}(U)=\mathrm{Tr}(V)=\mathrm{Tr}(W)=0$, the images $\overline{U}$, $\overline{V}$ and $\overline{W}$ in $\mathrm{PSL}(2,K)$ are involutions. Also

$$UV=\begin{pmatrix}1-2t^{1-p} & -2(t^p-t)\\ t^{-1}-t^{-p} & 1-2t^{p-1}\end{pmatrix}\quad\text{and}$$

$$UVW=\begin{pmatrix}1-2t^{1-p}-2t^{p-p^2}+2t^{1-p^2} & -2t+2t^p-2t^{p^2}+4t^{1-p+p^2}\\ t^{-1}-t^{-p}+t^{-p^2}-2t^{-1+p-p^2} & -1+2t^{p-1}-2t^{p^2-1}+2t^{p^2-p}\end{pmatrix},$$

the traces of which are

$$\begin{aligned}\mathrm{Tr}(UV)&=-2\bigl(t^{p-1}+t^{-(p-1)}-1\bigr)\quad\text{and}\\ \mathrm{Tr}(UVW)&=2\bigl(t^{p-1}-t^{1-p}+t^{p^2-p}-t^{p-p^2}+t^{1-p^2}-t^{p^2-1}\bigr)\\ &=2\bigl[\bigl(t^{p-1}-t^{1-p}\bigr)+\bigl(t^{p-1}-t^{1-p}\bigr)^p+\bigl(t^{p-1}-t^{1-p}\bigr)^{p^2}\bigr].\end{aligned}$$

Before proceeding, consider $\mathrm{Tr}(UVW)=2(t^{p-1}-t^{1-p}+t^{p^2-p}-t^{p-p^2}+t^{1-p^2}-t^{p^2-1})$, and suppose that $\mathrm{Tr}(UVW)=0$. For convenience, let $m=t^{p-1}$, which we know does not lie in F, so $m^p\neq 1$ and $m^{p^2}\neq 1$. On the other hand, $m^{p^2+p+1}=t^{(p-1)(p^2+p+1)}=t^{p^3-1}=1$, so $t^{p^2-1}=m^{p+1}=m^{-p^2}$. Now $0=\mathrm{Tr}(UVW)=2(m-m^{-1}+m^p-m^{-p}+m^{-(p+1)}-m^{p+1})$, and it follows that

$$\begin{aligned}m^{-1}(m+1)(m-1)=m-m^{-1}&=m^{-p}-m^{-(p+1)}+m^{p+1}-m^p\\ &=(m-1)\bigl(m^{-(p+1)}+m^p\bigr).\end{aligned}$$

Since $m\neq 1$, this gives $m+1=m(m^{-(p+1)}+m^p)=m^{-p}+m^{p+1}$, which on multiplication by m^p becomes $m^{p+1}+m^p=1+m^{2p+1}$, giving $0=m^{2p+1}-m^{p+1}-m^p+1=(m^p-1)(m^{p+1}-1)$. Since $m^p\neq 1$, we deduce that $m^{p+1}=1$, but then it follows that $m^{p^2}=m^{-(p+1)}=1$, a contradiction. Thus $\mathrm{Tr}(UVW)\neq 0$, and in particular, $\overline{UVW}$ is not an involution.

Now let H be the subgroup of $\mathrm{PSL}(2,K)$ generated by $\overline{U}$, $\overline{V}$ and $\overline{W}$. To prove (i), it suffices to show that H cannot be a subgroup of any of the maximal subgroups of $\mathrm{PSL}(2,K)$ given by the cases (a) to (d) of Proposition 2.5.

By Proposition 2.4, we find that $t^{p-1}\notin F$ and so $\mathrm{Tr}(UV)=-2(t^{p-1}+t^{-(p-1)}-1)\notin F$, which implies that H cannot be isomorphic to $\mathrm{PSL}(2,p)$.

Next, suppose that H is a subgroup of a dihedral group. Since $\mathrm{Tr}(UV)\neq 0$, we know that $\overline{UV}$ has order greater than 2 in $\mathrm{PSL}(2,K)$, and so $\langle\overline{U},\overline{V}\rangle$ must be a dihedral group of order greater than 4, and hence H itself is dihedral, of order $2n$ for some n. Moreover, $\overline{UV}$ lies in the unique cyclic subgroup of order n in $H\cong D_n$, and $\overline{U}$ and $\overline{V}$ cannot commute. Then since $U^\alpha=V$ and $V^\alpha=W$, it follows that also $\overline{V}$ and $\overline{W}$ cannot commute. Thus $\overline{U}$, $\overline{V}$ and $\overline{W}$ are non-commuting involutions in $H \cong D_n$, lying outside of the cyclic subgroup of order n, and hence also $\overline{UVW}$ is an involution, which is impossible. Thus H cannot lie in a dihedral subgroup, and this eliminates cases (b) and (c).

Next, suppose H is a subgroup of a semidirect product $\mathbb{Z}_p^3 \rtimes \mathbb{Z}_{\frac{q-1}{2}}$, as in case (d). Then H has a unique (normal) Sylow p-subgroup P, which is elementary abelian, with cyclic quotient H/P. Since $\langle \overline{U}, \overline{V} \rangle$ is a dihedral group of order more than 4, it follows that $\overline{UV}$ has order p, so $\langle \overline{U}, \overline{V} \rangle$ is a dihedral subgroup of order $2p$. Hence, in particular, conjugation by $\overline{U}$ must invert $\overline{VU}$. Similarly, $\overline{UW}$ has order p and is inverted by conjugation by $\overline{U}$. It follows that also $\overline{VW} = (\overline{VU})(\overline{UW})$ has order 1 or p and is inverted by conjugation by $\overline{U}$, so $(\overline{UVW})^2 = (\overline{VW})^{\overline{U}}\overline{VW} = (\overline{VW})^{-1}\overline{VW} = 1$. Hence $\overline{UVW}$ is an involution, which again is impossible. Thus H cannot be contained in a maximal subgroup from class (d), and therefore $H = \mathrm{PSL}(2, K)$.

Now take $G = \mathrm{PSL}(2, K)$ and $S = \{\overline{U}, \overline{V}, \overline{W}\}$, let X be the Cayley graph $\mathrm{Cay}(G, S)$, and let $A = \mathrm{Aut}(X)$. By observations in the previous section, A has a regular subgroup $R(G)$ isomorphic to G. To prove (ii), it suffices to show that $\mathrm{Aut}(G, S)$ is generated by the automorphism $\overline{\alpha}$ of $G = \mathrm{PSL}(2, K)$ induced by the Frobenius automorphism α of K, of order 3, and that $A = R(G) \rtimes \mathrm{Aut}(G, S)$.

Since $\overline{\alpha} \in \mathrm{Aut}(G, S)$ induces a cyclic permutation of the three neighbours of the identity vertex of X, we know that X is symmetric. By Proposition 2.8, it follows that X is a normal Cayley graph, and then by Proposition 2.7, we find that $A = R(G) \rtimes \mathrm{Aut}(G, S)$. Hence we need only show that $|\mathrm{Aut}(G, S)| = 3$.

To do this, note that $\mathrm{Aut}(G, S)$ is faithful on S (since X is connected), and therefore $|\mathrm{Aut}(G, S)| = 3$ or 6, and accordingly, $|A| = 3|G|$ or $6|G|$. Suppose that $|\mathrm{Aut}(G, S)| = 6$. Let B be the subgroup of A generated by $R(G)$ and $\overline{\alpha}$. This is isomorphic to $\mathrm{P\Sigma L}(2, K)$, of order $3|G|$, and so B has index 2 in A. Now let $C = C_A(B)$, the centralizer of B in A. Then $C \cap B = Z(B)$ which is trivial, so $|C| = 1$ or 2. If $|C| = 2$, then $A \cong B \times C$ so C is central in A, and therefore $\langle \alpha, C \rangle \cong \mathbb{Z}_6$, and $A = R(G) \rtimes \langle \alpha, C \rangle \cong R(G) \rtimes \mathbb{Z}_6$, which gives $A/R(G) \cong \mathbb{Z}_6$. On the other hand, $A = R(G)A_1$ (since $R(G)$ acts regularly on $V(X)$), so $A_1 \cong A/R(G) \cong \mathbb{Z}_6$. But that is impossible, by Proposition 2.6. Thus $|C| = 1$.

In particular, $N_A(B)/C_A(B) = A/C \cong A$, and so Proposition 2.1 tells us that A is isomorphic to a subgroup of $\mathrm{Aut}(B) \cong \mathrm{Aut}(\mathrm{P\Sigma L}(2, K)) \cong \mathrm{P\Gamma L}(2, K)$. Comparing orders, we have $A \cong \mathrm{P\Gamma L}(2, K)$. But this gives $A_1 \cong A/R(G) \cong \mathrm{P\Gamma L}(2, K)/\mathrm{PSL}(2, K) \cong \mathbb{Z}_6$, the same contradiction as above. Thus $|\mathrm{Aut}(G, S)| = 3$, as required. □

Let $p \equiv 3$ or 5 (mod 8). Then $\mathrm{PSL}(2, K)$ has order $p^3(p^3 - 1)(p^3 + 1)/2$, which is 4 times an odd integer. By Theorem 3.5, we have the following corollary.

Corollary 3.6 *There exist infinitely many cubic one-regular graphs of order* $4m$ *where* m *is odd.*

Acknowledgements The authors acknowledge the use of the MAGMA system [1] in helping find examples of cubic one-regular graphs on which the eventual construction was based. The first author's work was supported by the New Zealand Marsden Fund (project number UOA1015), and the second author's work was supported by the National Natural Science Foundation of China (grant 11171020).

References

1. Bosma, W., Cannon, C., Playoust, C.: The MAGMA algebra system I: The user language. J. Symb. Comput. **24**, 235–265 (1997)
2. Chao, C.Y.: On the classification of symmetric graphs with a prime number of vertices. Transl. Am. Math. Soc. **158**, 247–256 (1971)
3. Cheng, Y., Oxley, J.: On weakly symmetric graphs of order twice a prime. J. Comb. Theory, Ser. B **42**, 196–211 (1987)
4. Conder, M.D.E., Dobcsányi, P.: Trivalent symmetric graphs on up to 768 vertices. J. Comb. Math. Comb. Comput. **40**, 41–63 (2002)
5. Conder, M.D.E., Lorimer, P.: Automorphism groups of symmetric graphs of valency 3. J. Comb. Theory, Ser. B **47**, 60–72 (1989)
6. Conder, M.D.E., Nedela, R.: Symmetric cubic graphs of small girth. J. Comb. Theory, Ser. B **97**, 757–768 (2007)
7. Conder, M.D.E., Nedela, R.: A refined classification of symmetric cubic graphs. J. Algebra **322**, 722–740 (2009)
8. Conder, M.D.E., Praeger, C.E.: Remarks on path-transitivity on finite graphs. Eur. J. Comb. **17**, 371–378 (1996)
9. Dickson, L.E.: Linear Groups, with an Exposition of the Galois Field Theory. Dover, New York (1958)
10. Djoković, D.Ž., Miller, G.L.: Regular groups of automorphisms of cubic graphs. J. Comb. Theory, Ser. B **29**, 195–230 (1980)
11. Feng, Y.-Q., Kwak, J.H.: One-regular cubic graphs of order a small number times a prime or a prime square. J. Aust. Math. Soc. **76**, 345–356 (2004)
12. Feng, Y.-Q., Kwak, J.H.: Classifying cubic symmetric graphs of order $10p$ or $10p^2$. Sci. China Ser. A **49**, 300–319 (2006)
13. Feng, Y.-Q., Kwak, J.H.: Cubic symmetric graphs of order a small number times a prime or a prime square. J. Comb. Theory, Ser. B **97**, 627–646 (2007)
14. Feng, Y.-Q., Kwak, J.H., Wang, K.S.: Classifying cubic symmetric graphs of order $8p$ or $8p^2$. Eur. J. Comb. **26**, 1033–1052 (2005)
15. Frucht, R.: A one-regular graph of degree three. Can. J. Math. **4**, 240–247 (1952)
16. Gorenstein, D.: Finite Groups, 2nd edn. Chelsea, New York (1980)
17. Giudici, M.: Maximal subgroups of almost simple groups with socle $\mathrm{PSL}(2,q)$, preprint. Available at http://front.math.ucdavis.edu/math.GR/0703685
18. Huppert, B.: Endliche Gruppen I. Springer, Berlin (1967)
19. Kwak, J.H., Oh, J.M.: One-regular normal Cayley graphs on dihedral groups of valency 4 or 6 with cyclic vertex stabilizer. Acta Math. Sin. Engl. Ser. **22**, 1305–1320 (2006)
20. Lorimer, P.: Vertex-transitive graphs: symmetric graphs of prime valency. J. Graph Theory **8**, 55–68 (1984)
21. Lukacs, A., Seifter, N.: Finite contractions of graphs with polynomial growth. Eur. J. Comb. **22**, 85–90 (2001)
22. Macbeath, A.M.: Generators of the linear fractional groups. In: Number Theory (Proc. Sympos. Pure Math., vol. XII, 1967), pp. 14–32. Am. Math. Soc., Providence (1969)
23. Malnič, A., Marušič, D., Potočnik, P.: Elementary abelian covers of graphs. J. Algebr. Comb. **20**, 71–97 (2004)
24. Malnič, A., Marušič, D., Seifter, N.: Constructing infinite one-regular graphs. Eur. J. Comb. **20**, 845–853 (1999)
25. Marušič, D.: On vertex symmetric digraphs. Discrete Math. **36**, 69–81 (1981)
26. Marušič, D.: A family of one-regular graphs of valency 4. Eur. J. Comb. **18**, 59–64 (1997)
27. Marušič, D., Scapellato, R.: Classifying vertex-transitive graphs whose order is a product of two primes. Combinatorica **14**, 187–201 (1994)
28. Miller, R.C.: The trivalent symmetric graphs of girth at most six. J. Comb. Theory, Ser. B **10**, 163–182 (1971)
29. Praeger, C.E., Wang, R.J., Xu, M.Y.: Symmetric graphs of order a product of two distinct primes. J. Comb. Theory, Ser. B **58**, 299–318 (1993)
30. Praeger, C.E., Xu, M.Y.: Vertex-primitive graphs of order a product of two distinct primes. J. Comb. Theory, Ser. B **59**, 245–266 (1993)
31. Seifter, N., Woess, W.: Approximating graphs with polynomial growth. Glasg. Math. J. **42**, 1–8 (2000)

32. Suzuki, M.: Group Theory I. Springer, New York (1982)
33. Tutte, W.T.: A family of cubical graphs. Proc. Camb. Philos. Soc. **43**, 459–474 (1947)
34. Tutte, W.T.: On the symmetry of cubic graphs. Can. J. Math. **11**, 621–624 (1959)
35. Wang, C.Q., Xu, M.Y.: Non-normal one-regular and 4-valent Cayley graphs of dihedral groups D_{2n}. Eur. J. Comb. **27**, 750–766 (2006)
36. Wang, C.Q., Zhou, Z.Y.: 4-valent one-regular normal Cayley graphs of dihedral groups. Acta Math. Sin. Chin. Ser. **49**, 669–678 (2006)
37. Wang, R.J., Xu, M.Y.: A classification of symmetric graphs of order $3p$. J. Comb. Theory, Ser. B **58**, 197–216 (1993)
38. Xu, J., Xu, M.Y.: Arc-transitive Cayley graphs of valency at most four on abelian groups. Southeast Asian Bull. Math. **25**, 355–363 (2001)
39. Xu, M.Y.: A note on one-regular graphs. Chin. Sci. Bull. **45**, 2160–2162 (2000)
40. Xu, M.Y.: Automorphism groups and isomorphisms of Cayley digraphs. Discrete Math. **182**, 309–319 (1998)
41. Xu, S.J., Fang, X.G., Wang, J., Xu, M.Y.: On cubic s-arc transitive Cayley graphs of finite simple groups. Eur. J. Comb. **26**, 133–143 (2005)
42. Zhou, J.-X., Feng, Y.-Q.: Cubic one-regular graphs of order twice a square-free integer. Sci. China **51**, 1093–1100 (2008)
43. Zhou, J.-X., Feng, Y.-Q.: Tetravalent one-regular graphs of order $2pq$. J. Algebr. Comb. **29**, 457–471 (2009)