J Algebr Comb (2012) 35:173–192
DOI 10.1007/s10801-011-0299-z

An infinite family of biquasiprimitive 2-arc transitive cubic graphs

Alice Devillers · Michael Giudici · Cai Heng Li · Cheryl E. Praeger

Received: 2 March 2011 / Accepted: 6 June 2011 / Published online: 1 July 2011

Abstract A new infinite family of bipartite cubic 3-arc transitive graphs is constructed and studied. They provide the first known examples admitting a 2-arc transitive vertex-biquasiprimitive group of automorphisms for which the index two subgroup fixing each half of the bipartition is not quasiprimitive on either bipartite half.

Keywords 2-arc-transitive graphs · Quasiprimitive · Biquasiprimitive · Normal quotient · Automorphism group

1 Introduction

The study of cubic s-arc-transitive graphs goes back to the seminal papers of Tutte [14, 15] who showed that $s \leq 5$. More generally, Weiss [16] proved that $s \leq 7$ for graphs of larger valency. In [13], the last author introduced a global approach to the study of s-arc-transitive graphs.

Given a connected graph Γ with an s-arc-transitive group G of automorphisms, if G has a nontrivial normal subgroup N with at least three orbits on vertices, then G

The paper forms part of Australian Research Council Federation Fellowship FF0776186 held by the fourth author. The first author is supported by UWA as part of the Federation Fellowship project and the second author is supported by an Australian Research Fellowship.

A. Devillers (✉) · M. Giudici · C.H. Li · C.E. Praeger
Centre for the Mathematics of Symmetry and Computation, School of Mathematics and Statistics,
The University of Western Australia, 35 Stirling Highway, Crawley WA 6009, Australia
e-mail: alice.devillers@uwa.edu.au

M. Giudici
e-mail: michael.giudici@uwa.edu.au

C.H. Li
e-mail: cai.heng.li@uwa.edu.au

C.E. Praeger
e-mail: cheryl.praeger@uwa.edu.au

induces an unfaithful but s-arc-transitive action on the normal quotient Γ_N (defined in Sect. 2). The important graphs to study are then those with no "useful" normal quotients, that is, those for which all nontrivial normal subgroups of G have at most two orbits on vertices. A transitive permutation group for which all nontrivial normal subgroups are transitive is called *quasiprimitive*, while if the group is not quasiprimitive and all nontrivial normal subgroups have at most two orbits we call it *biquasiprimitive*. Thus the basic graphs to study are those which are (G, s)-arc transitive and G is either quasiprimitive or biquasiprimitive on vertices.

Now suppose that our graph Γ were bipartite. Then the *even subgroup* G^+ (the subgroup generated by the vertex stabilisers G_v for all $v \in V\Gamma$) has index 2 in G and is transitive on each of the two bipartite halves of Γ (see, for example, [7, Proposition 1]). Since G^+ is vertex-intransitive, G is not vertex-quasiprimitive and so the basic bipartite graphs are those where G is biquasiprimitive on vertices. The actions of such groups were investigated in [11, 12]. However, when G is biquasiprimitive it may still be possible to find a meaningful quotient of the graph. The subgroup G^+ is what is called locally transitive on s-arcs (see Sect. 2 for a precise definition and [8] for an analysis of such graphs). If G^+ is not quasiprimitive on each bipartite half (note the two actions of G^+ are equivalent) then we can form a G^+-normal quotient and obtain a new (smaller) locally s-arc-transitive graph. The existence of a 2-arc transitive graph with such a group has been regarded as 'problematic' (see [11, Sect. 4]). The main result of this paper is that there do indeed exist $(G, 2)$-arc transitive graphs such that G is biquasiprimitive but G^+ is not quasiprimitive on each bipartite half.

Theorem 1.1 *There exist infinitely many connected bipartite* $(G, 2)$*-arc transitive graphs* Γ *of valency* 3, *where* $G \leq \mathsf{Aut}(\Gamma)$, *such that G is biquasiprimitive on vertices but* G^+ *is not quasiprimitive on either bipartite half.*

Such permutation groups G were described in detail in [11, Theorem 1.1(c)(i)] (see Corollary 9.8) and this theorem gives the first examples of 2-arc-transitive graphs admitting such automorphism groups. (Our graphs are actually 3-arc transitive, but only $(G, 2)$-arc-transitive.) We also provide an infinite family of $(G, 1)$-arc-transitive graphs where G is biquasiprimitive on vertices but G^+ is not quasiprimitive on each orbit (Construction 3.1). The full automorphism group A of such a graph is 2-arc-transitive but A^+ is quasiprimitive on each bipartite half.

Graphs which are s-arc transitive are also s-distance transitive, provided their diameter is at least s. Such graphs were studied in [4] where (G, s)-distance transitive bipartite graphs with G biquasiprimitive on vertices, but G^+ not quasiprimitive on each bipartite half, were referred to as G-basic but not G^+-basic (see [4, Proposition 6.3]). Our infinite family of graphs shows that connected 2-distance transitive graphs with such an automorphism group do indeed exist and so this answers Question 6.4 of [4] in the affirmative for $s = 2$.

We prove Theorem 1.1 by constructing and analysing a new infinite family of finite bipartite $(G, 2)$-arc transitive graphs $\Gamma(f, \alpha)$ of valency 3, where f is a positive integer and α lies in the Galois field $\mathsf{GF}(2^f)$, see Construction 6.1. The group $G \leq \mathsf{Aut}(\Gamma(f, \alpha))$ depends only on f, has order $2^{2f+1}(2^{2f} - 1)^2$, and is biquasiprimitive on vertices, while G^+ is not quasiprimitive on either bipartite half. Indeed we have N (of order $2^f(2^{2f}-1)$) normal in G^+ and intransitive on each bipartite half (Proposition 9.5). These graphs are quite large, indeed their number of vertices is $2^{2f}(2^{2f}-1)^2/3$ (Proposition 6.3). Infinitely many of them are connected (Proposition 8.5). The number of pairwise non-isomorphic connected graphs produced by Construction 6.1 grows exponentially with f (Proposition 8.5); and each connected graph has relatively large girth (at least 10, Proposition 9.2) and diameter (at least $6f-3$, Proposition 6.3).

Note that G is not the full automorphism group of $\Gamma(f,\alpha)$. Moreover, overgroups of biquasiprimitive and quasiprimitive groups are not necessarily biquasiprimitive or quasiprimitive respectively. Indeed we have the following:

Theorem 1.2 *For each connected graph $\Gamma = \Gamma(f,\alpha)$ defined in Construction 6.1, with automorphism group $A = \mathsf{Aut}(\Gamma)$ given in Proposition 8.1, G is an index two subgroup of A, Γ is $(A,3)$-arc-transitive, A is not biquasiprimitive on vertices and A^+ is quasiprimitive on each bipartite half.*

We do not know if there are examples where G is the full automorphism group.

Question 1.3 *Is there a $(G,2)$-arc transitive graph Γ such that $G = \mathsf{Aut}(\Gamma)$ is biquasiprimitive on vertices but G^+ is not quasiprimitive on each bipartite half?*

2 Preliminary graph definitions

We consider simple, undirected graphs Γ, with vertex-set $V\Gamma$ and edge-set $E\Gamma$. A graph is called *cubic* if it is regular of valency 3. For a positive integer s, an *s-arc* of a graph is an $(s+1)$-tuple $(v_0, v_1, \ldots, v_s)$ of vertices such that v_i is adjacent to v_{i-1} for $1 \le i \le s$ and $v_{j-1} \ne v_{j+1}$ for $1 \le j \le s-1$. The *distance* between two vertices v_1 and v_2, denoted by $\mathsf{d}_\Gamma(v_1, v_2)$, is the minimal number s such that there exists an s-arc between v_1 and v_2. For a connected graph Γ, we define the *diameter of* Γ, denoted $\mathsf{diam}(\Gamma)$, as the maximum distance between two vertices of Γ.

We denote a complete graph on n vertices by K_n and a complete bipartite graph with bipartite halves of sizes n and m by $K_{n,m}$. The disjoint union of m copies of Σ is denoted by $m\Sigma$.

Let Γ be a graph, $G \le \mathsf{Aut}(\Gamma)$, and $N \lhd G$. The (*normal*) *quotient graph* Γ_N is the graph with vertex-set the set of N-orbits, such that two N-orbits B_1 and B_2 are adjacent in Γ_N if and only if there exist $v \in B_1$ and $w \in B_2$ with $\{v, w\} \in E\Gamma$.

Tables 1 and 2 describe some properties $\mathcal{P}$ that hold for the G-action on a connected graph Γ, where $G \le \mathsf{Aut}(\Gamma)$ and we require that G be transitive on each set in some collection $\mathcal{P}(\Gamma)$ of sets. For the local variant we require that for each vertex v of Γ, the stabiliser G_v be transitive on each set in a related collection $\mathcal{P}(\Gamma, v)$ of sets. These concepts are sometimes used without reference to a particular group G, especially when $G = \mathsf{Aut}(\Gamma)$.

Next we describe coset graphs, which will be used to describe our family of graphs, and some of their properties.

Table 1 Properties for G-action on a connected graph Γ

Property	$\mathcal{P}(\Gamma) = \{\Delta_i \mid 1 \le i \le s\}$, $\Delta_s \neq \emptyset$
(G, s)-arc transitivity	Δ_i is the set of i-arcs of Γ
G-arc transitivity	$s = 1$ and Δ_1 is as in previous line
(G, s)-distance transitivity	Δ_i is $\{(v, w) \in V\Gamma \times V\Gamma \mid \mathsf{d}_\Gamma(v, w) = i\}$
G-distance transitivity	$s = \mathsf{diam}(\Gamma)$ and Δ_i is as in previous line

Table 2 Local properties for G-action on a connected graph Γ

Local property	$\mathcal{P}(\Gamma, v) = \{\Delta_i(v) \mid 1 \le i \le s\}$, $\Delta_s(v) \neq \emptyset$ for some v
local (G, s)-arc transitivity	$\Delta_i(v)$ is the set of i-arcs of Γ with initial vertex v
local G-arc transitivity	$s = 1$ and $\Delta_1(v)$ is as in previous line
local (G, s)-distance transitivity	$\Delta_i(v)$ is $\Gamma_i(v) := \{w \in V\Gamma \mid \mathsf{d}_\Gamma(v, w) = i\}$
local G-distance transitivity	$s = \mathsf{diam}(\Gamma)$ and $\Delta_i(v)$ is as in previous line

Definition 2.1 Given a group G, a subgroup H and an element $g \in G$ such that $HgH = Hg^{-1}H$, the *coset graph* $\mathsf{Cos}(G, H, HgH)$ is the graph with vertices the right cosets of H in G, with Hg_1 and Hg_2 forming an edge if and only if $g_2g_1^{-1} \in HgH$.

Note that a coset graph is indeed undirected since $g_2g_1^{-1} \in HgH$ if and only if $g_1g_2^{-1} \in Hg^{-1}H$.

Lemma 2.2 *Let* $\Gamma = \mathsf{Cos}(G, H, HgH)$. *Then the following facts hold.*

(a) Γ *has* $|G : H|$ *vertices and is regular with valency* $|H : H^g \cap H|$.
(b) *The group* G *acts by right multiplication on the coset graph with kernel* $\bigcap_{x \in G} H^x$, *and* G *is arc-transitive.*
(c) Γ *is connected if and only if* $\langle H, g\rangle = G$.
(d) *If* $\langle H, g\rangle \le K < G$, *then* $\Gamma = m\Sigma$ *where* $m = |G : K|$ *and* $\Sigma = \mathsf{Cos}(K, H, HgH)$.
(e) Γ *has* $|G : \langle H, g\rangle|$ *connected components, each isomorphic to* $\mathsf{Cos}(\langle H, g\rangle, H, HgH)$.
(f) *For* $\eta \in \mathbf{N}_{\mathsf{Aut}\, G}(H)$, *the map* $\bar{\eta} : Hx \mapsto Hx^\eta$ *is a permutation of* $V\Gamma$ *and induces an isomorphism from* Γ *to* $\mathsf{Cos}(G, H, Hg^\eta H)$.

Proof Statements (a) to (c) can be found in [10].

Assume $\langle H, g\rangle \le K < G$. By Theorem 4(i, iii) of [10], there is no edge of Γ between vertices (that is, H-cosets) lying in distinct K-cosets. On the other hand, by the last paragraph of the proof of that same theorem, for all K-cosets Kx, the graph induced on the H-cosets contained in Kx is isomorphic to $\Sigma = \mathsf{Cos}(K, H, HgH)$. Hence (d) holds. Statement (e) follows from (d) (taking $K = \langle H, g\rangle$) and (c).

Let $\eta \in \mathbf{N}_{\mathsf{Aut}\, G}(H)$ and $\Sigma = \mathsf{Cos}(G, H, Hg^\eta H)$. Then η maps H-cosets to H-cosets and so induces the permutation $\bar{\eta} : V\Gamma \to V\Gamma : Hx \mapsto Hx^\eta$ of $V\Gamma = V\Sigma$.

Let $\{Hx, Hy\}$ be an edge of Γ, that is, $yx^{-1} \in HgH$. Now $y^\eta(x^\eta)^{-1} = (yx^{-1})^\eta \in (HgH)^\eta$. Since η normalises H, we have $(HgH)^\eta = Hg^\eta H$, and so $\{Hx^\eta, Hy^\eta\}$ is an edge of Σ. Conversely, let $\{Hx^\eta, Hy^\eta\}$ be an edge of Σ, so that $y^\eta(x^\eta)^{-1} = (yx^{-1})^\eta \in Hg^\eta H$. Then $yx^{-1} \in (Hg^\eta H)^{\eta^{-1}}$, and since η normalises H, $(Hg^\eta H)^{\eta^{-1}} = HgH$. Therefore $\bar{\eta}$ sends the edge-set of Γ to the edge-set of Σ and (f) holds. □

3 1-arc-transitive examples

In this section, we construct an infinite family of G-arc-transitive graphs such that G is biquasiprimitive on vertices but G^+ is not quasiprimitive on each bipartite half.

Construction 3.1 *Let $H = \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_2$ where $p \equiv 1 \pmod 3$ is a prime. Let a be an element of multiplicative order 3 in $\mathbb{Z}_p$. We define a graph Σ with vertex-set H and edges of the form*

$$\big\{(x,y,0),\ (x+1,y+1,1)\big\},$$
$$\big\{(x,y,0),\ \big(x+a,y+a^2,1\big)\big\},$$
$$\big\{(x,y,0),\ \big(x+a^2,y+a,1\big)\big\}.$$

This yields an undirected bipartite graph with bipartite halves $\Delta_1 = \{(x,y,0) | x,y \in \mathbb{Z}_p\}$ and $\Delta_2 = \{(x,y,1) | x,y \in \mathbb{Z}_p\}$.

Some automorphisms of Σ are:

- $t_{u,v} : (x,y,\epsilon) \mapsto (x+u, y+v, \epsilon) \in \mathsf{Aut}(\Sigma)$, *we denote* $\{t_{u,v} | u,v \in \mathbb{Z}_p\}$ *by* $N \cong \mathbb{Z}_p^2$;
- $\tau : (x,y,\epsilon) \mapsto (ax, a^2y, \epsilon) \in \mathsf{Aut}(\Sigma)$;
- $\sigma : (x,y,\epsilon) \mapsto (y,x,\epsilon) \in \mathsf{Aut}(\Sigma)$;
- $\nu : (x,y,\epsilon) \mapsto (-x,-y,1-\epsilon) \in \mathsf{Aut}(\Sigma)$.

We easily see from this construction that Σ is cubic with the neighbours of the vertex (x,y,ϵ) being $(x+(-1)^\epsilon, y+(-1)^\epsilon, 1)$, $(x+(-1)^\epsilon a, y+(-1)^\epsilon a^2, 1)$ and $(x+(-1)^\epsilon a^2, y+(-1)^\epsilon a, 1)\}$.

Proposition 3.2 *Let $G = N \rtimes \langle \tau, \sigma\nu\rangle \cong \mathbb{Z}_p^2 \rtimes S_3$. Then G is biquasiprimitive on $V\Sigma$ but G^+ is not quasiprimitive on each bipartite half and Σ is $(G,1)$-arc transitive but not $(G,2)$-arc transitive. The full automorphism group of Σ is $A = N \rtimes \langle \tau, \sigma, \nu\rangle \cong \mathbb{Z}_p^2 \rtimes (S_3 \times \mathbb{Z}_2)$. Then Σ is $(A,2)$-arc transitive, A is biquasiprimitive on $V\Sigma$ and A^+ is quasiprimitive on the bipartite halves.*

Proof The group N clearly acts transitively on each bipartite half and $\sigma\nu$ switches Δ_1 and Δ_2, so G is transitive on $V\Sigma$. Moreover, since no nontrivial element of $\langle \tau, \sigma\nu\rangle$ centralises N: and since $\langle \tau, \sigma\nu\rangle$ leaves invariant no subgroup of N of order p, it follows that N is the unique minimal normal subgroup of G and so G is biquasiprimitive on vertices. Now $G^+ = N \rtimes \langle \tau\rangle$ has $\{t_{u,0} | u \in \mathbb{Z}_p\} \cong \mathbb{Z}_p$ as a normal subgroup that is intransitive on Δ_1 and Δ_2. Thus G^+ is not quasiprimitive on each bipartite half. Finally, $G_{(0,0,0)} = \langle \tau \rangle$, which acts regularly on the set of three neighbours of $(0, 0, 0)$, and so Σ is $(G, 1)$-arc transitive but not $(G, 2)$-arc transitive.

Let $A = N \rtimes \langle \tau, \sigma, \nu \rangle$. Then N is also the unique minimal normal subgroup of A and of $A^+ = N \rtimes \langle \tau, \sigma \rangle$. Thus A is biquasiprimitive on vertices and A^+ is quasiprimitive on each bipartite half. Moreover, $A_{(0,0,0)} = \langle \tau, \sigma \rangle \cong S_3$ acts 2-transitively on the set of three neighbours of $(0, 0, 0)$ and so Σ is $(A, 2)$-arc transitive.

Let X be the full automorphism group of Σ. Since A is vertex-transitive, we have $X = AX_\alpha$ (where $\alpha \in V\Sigma$) and so $|X_\alpha|$ divides 48 [14, 15]. Since $|A_\alpha| = 6$, it follows that $|X : A|$ divides 8. Consider the action of X on the set of right cosets of A. If A is core-free in X, it follows that $X \leq S_8$, contradicting p^2 dividing $|A|$ and $p \geq 7$. Thus A contains a normal subgroup M of X. Since N is the unique minimal normal subgroup of A, it follows that $N \leq M$. However, N is the unique Sylow p-subgroup of A and hence of M, and so $N \lhd X$. Hence X has a normal subgroup that acts regularly on each bipartite half and so, by [9, Lemma 2.4], X_α acts faithfully on $\Sigma(\alpha)$. Thus $X_\alpha = A_\alpha = S_3$ and hence $X = A$. □

4 Finite fields

This section contains facts about finite fields that we need later. We denote a field of order q by $\mathsf{GF}(q)$.

Definition 4.1 Let x be an element of a field F. The *subfield generated by x* is the unique smallest subfield containing x. The element x is called a *generator* of F if the subfield generated by x is F, in other words, if x is not contained in any proper subfield of F.

Lemma 4.2 *Let f be an integer and let $\alpha \in \mathsf{GF}(2^f)$. The subfield generated by α is $\mathsf{GF}(2^e)$ if and only if the order of α divides $2^e - 1$ but does not divide $2^s - 1$ for any proper divisor s of e. In particular, α is a generator of $\mathsf{GF}(2^f)$ if and only if the order of α does not divide $2^e - 1$ for any proper divisor e of f.*

Proof Since the multiplicative group of $\mathsf{GF}(2^f)$ is cyclic of order $2^f - 1$, it follows that the multiplicative group of the subfield $\mathsf{GF}(2^e)$ of $\mathsf{GF}(2^f)$ is precisely the subgroup of order $2^e - 1$, with e dividing f. This subgroup is unique, since there is a unique subgroup of each order in a cyclic group. Thus the order of α divides $2^e - 1$ if and only if $\alpha \in \mathsf{GF}(2^e)$. The result follows. □

Lemma 4.3 *Let f be an integer, $f \geq 2$, and let α be a generator of $\mathsf{GF}(2^f)$. Then*

(a) $\alpha^{2^i} \neq \alpha + 1$ *for all positive integers $i < f$ except possibly $i = f/2$ (with f even), and*

(b) $\alpha^{2^i} \neq \alpha$ *for all positive integers $i < f$.*

Proof Suppose $\alpha^{2^i} = \alpha + 1$ for some integer $i < f$. Then since $\mathsf{GF}(2^f)$ has characteristic 2, we have $\alpha^{2^{2i}} = (\alpha^{2^i})^{2^i} = (\alpha + 1)^{2^i} = \alpha^{2^i} + 1 = \alpha$, so $\alpha^{2^{2i}-1} = 1$.

Since $0 \neq \alpha \in \mathsf{GF}(2^f)$, we also have that $\alpha^{2^f-1} = 1$. Hence the order of α divides $\gcd(2^{2i}-1, 2^f-1) = 2^{\gcd(2i,f)}-1$. Since $\gcd(2i, f)$ divides f and α is a generator, Lemma 4.2 implies that $\gcd(2i, f) = f$, that is, f divides $2i$. Since $f > i$, this implies that f is even and $i = f/2$. This proves (a).

Suppose $\alpha^{2^i} = \alpha$ for some positive integer $i < f$. Then $\alpha^{2^i-1} = 1$. Hence the order of α divides $\gcd(2^i-1, 2^f-1) = 2^{\gcd(i,f)}-1$. Since $\gcd(i, f)$ is a divisor of f and α is a generator, Lemma 4.2 implies that $\gcd(i, f) = f$, that is, f divides i, contradicting $f > i$. This proves (b). □

Lemma 4.4 *Let f be an integer, $f \geq 3$. Then the number of generators of* $\mathsf{GF}(2^f)$ *is strictly greater than 2^{f-1}.*

Proof For $f = 3$, all elements of $\mathsf{GF}(2^3) \setminus \{0, 1\}$ are generators, hence there are 6 generators and the claim holds. Assume $f \geq 4$. Let $f = \prod_{i=1}^k p_i^{e_i}$, where the p_i are distinct primes and each $e_i \geq 1$. Let $f_i = f/p_i$. Then all elements which are not generators are in one of the subfields $\mathsf{GF}(2^{f_i})$. Hence the number of generators is $2^f - |\bigcup_{i=1}^k \mathsf{GF}(2^{f_i})|$. We have $|\bigcup_{i=1}^k \mathsf{GF}(2^{f_i})| \leq 1 + \Sigma_{i=1}^k (2^{f_i} - 1)$ since 0 is in all fields. Since $f_i \leq f/2$ for all i, we have $|\bigcup_{i=1}^k \mathsf{GF}(2^{f_i})| \leq 1 + k(2^{f/2} - 1) \leq k2^{f/2}$. Since $f \geq \prod_{i=1}^k p_i \geq 2^k$, we have $k \leq \log_2(f)$, and so $|\bigcup_{i=1}^k \mathsf{GF}(2^{f_i})| \leq \log_2(f)2^{f/2}$. It is easy to check that, for $f \geq 4$, $\log_2(f) \leq 2^{f/2-1}$, and so $\log_2(f)2^{f/2} \leq 2^{f-1}$. We can now conclude that the number of generators is at least $2^f - 2^{f-1} = 2^{f-1}$.

Suppose we get equality. Then we have equality in all our inequalities. In particular $1 + k(2^{f/2} - 1) = k2^{f/2}$, and so $k = 1$, and $k = \log_2(f)$, so $f = 2^k$. Thus $f = 2$, a contradiction. Therefore, the number of generators is greater than 2^{f-1}. □

Lemma 4.5 *Let ℓ be an integer, $\ell \geq 2$. Then the number of generators of* $\mathsf{GF}(2^{2\ell})$ *which do not satisfy the equation $x^{2^\ell} = x + 1$ is strictly greater than $2^\ell(2^{\ell-1} - 1)$.*

Proof By Lemma 4.4, $\mathsf{GF}(2^{2\ell})$ contains more than $2^{2\ell-1}$ generators. Since the equation $x^{2^\ell} = x + 1$ has degree 2^ℓ, it has at most 2^ℓ solutions. Hence the number of generators not satisfying the equation is greater than $2^{2\ell-1} - 2^\ell = 2^\ell(2^{\ell-1} - 1)$. □

5 The group $\mathsf{PSL}(2, 2^f)$

The elements of a group $\mathsf{PSL}(2, q)$ may be viewed as permutations of $X := \mathsf{GF}(q) \cup \{\infty\}$. More precisely, $t_{a,b,c,d}$ is the element

$$t_{a,b,c,d} : x \mapsto \frac{ax + b}{cx + d} \quad \text{for all } x \in X, \tag{1}$$

where $a, b, c, d \in \mathsf{GF}(q)$ are such that $ad - bc$ is a nonzero square of $\mathsf{GF}(q)$. We adopt the convention that ∞ is mapped by $t_{a,b,c,d}$ onto ac^{-1} and that an element of $\mathsf{GF}(q)$ divided by 0 is ∞. For $q = 2^f$, all nonzero elements of $\mathsf{GF}(q)$ are squares, and the automorphism group of $\mathsf{PSL}(2, q)$ is $\mathsf{P\Gamma L}(2, q) = \langle \mathsf{PSL}(2, q), \tau \rangle$, where

$$\tau : t_{a,b,c,d} \mapsto t_{a^2,b^2,c^2,d^2} \quad \text{for each } t_{a,b,c,d} \in \mathsf{PSL}(2, q). \tag{2}$$

In this paper, we will take $T = \mathsf{PSL}(2, 2^f)$ for some $f \geq 1$. For each subfield $\mathsf{GF}(2^e)$ of $\mathsf{GF}(2^f)$, we identify $\mathsf{PSL}(2, 2^e)$ with the subgroup of T of those $t_{a,b,c,d}$ with all of $a, b, c, d \in \mathsf{GF}(2^e)$. In our construction, we will use the following notation for elements of $H = \mathsf{PSL}(2, 2) \leq T$:

$$a = t_{1,1,1,0} : x \mapsto 1 + \frac{1}{x}, \quad b = t_{1,1,0,1} : x \mapsto x + 1. \tag{3}$$

Note that a has order 3, b has order 2, and $H = \langle a \rangle \rtimes \langle b \rangle \cong S_3$. For $\alpha \in \mathsf{GF}(2^f)$, we will also need the following elements of T:

$$u_\alpha = t_{1,\alpha,0,1} : x \mapsto x + \alpha, \quad c_\alpha = a^{u_\alpha} = t_{\alpha+1,\alpha^2+\alpha+1,1,\alpha}. \tag{4}$$

Let P be the Sylow 2-subgroup of T containing the involution $b = u_1$, that is, $P = \{u_\alpha | \alpha \in \mathsf{GF}(2^f)\}$. Then $\mathbf{N}_T(P) \cong \mathsf{AGL}(1, 2^f)$ is the set of permutations $t_{r,s,0,1} : x \mapsto rx + s$ with $r \neq 0$.

Lemma 5.1 *Let $\alpha \in \mathsf{GF}(2^f)$. Using the notation introduced above, the following facts hold.*

(a) $\mathbf{C}_T(b) = P$. *In particular, $u_\alpha b = b u_\alpha = u_{\alpha+1}$ and $\mathbf{C}_H(b) = \langle b \rangle$.*
(b) *For $\alpha \neq 0$, the element $z_\alpha := t_{\alpha^{-1},0,0,1} \in \mathbf{N}_T(P)$. Moreover $u_\alpha = b^{z_\alpha}$ and the order of z_α is equal to the multiplicative order of α.*
(c) *$c_\alpha^{\tau^i} = c_\alpha^{-1}$ if and only if $\alpha^{2^i} = \alpha + 1$.*
(d) $\mathbf{N}_T(H) = H$.
(e) *If the subfield generated by α is $\mathsf{GF}(2^e)$, then $\langle H, u_\alpha \rangle = \mathsf{PSL}(2, 2^e)$.*

Proof (a) The centraliser of b in T is easily computed. Since $u_\alpha \in P$, it then commutes with b, and $b u_\alpha = u_{\alpha+1}$. Also $\mathbf{C}_H(b) = \mathbf{C}_T(b) \cap H = \langle b \rangle$.
(b) A calculation shows that $u_y^{z_\alpha} = u_{\alpha y} \in P$, and so $z_\alpha \in \mathbf{N}_T(P)$. Also $u_\alpha = u_1^{z_\alpha} = b^{z_\alpha}$. Since $z_\alpha^j = t_{\alpha^{-j},0,0,1}$ the rest of the statement follows.
(c) This is a simple calculation left to the reader.
(d) Let $D = \mathbf{N}_T(\langle a \rangle)$. Now D is a dihedral group $D_{2(2^f \pm 1)}$, see [5, Sect. 260]. Since $\langle a \rangle \cong C_3$ is characteristic in $H \cong S_3$, $\mathbf{N}_T(H) \leq \mathbf{N}_T(\langle a \rangle) = D$, and so $\mathbf{N}_T(H) = \mathbf{N}_D(H)$. Since an S_3 subgroup in a dihedral group D_{2n}, n odd, is self-normalising, we have that $\mathbf{N}_D(H) = H$. Thus $\mathbf{N}_T(H) = H$.
(e) Suppose the subfield generated by α is $\mathsf{GF}(2^e)$. If $e = 1$, then $\alpha = 0$ or 1, $u_\alpha \in H$ and $\langle H, u_\alpha \rangle = H = \mathsf{PSL}(2, 2)$. Assume now $e \geq 2$. Since all the subscripts of $u_\alpha = t_{1,\alpha,0,1}$ are in $\mathsf{GF}(2^e)$, we obviously have $\langle H, u_\alpha \rangle \leq \mathsf{PSL}(2, 2^e)$. Suppose that $\langle H, u_\alpha \rangle \leq M$, where M is a maximal subgroup of $\mathsf{PSL}(2, 2^e)$. Since $\langle H, u_\alpha \rangle$ contains a subgroup isomorphic to S_3, M cannot be isomorphic to $\mathsf{AGL}(1, 2^e)$ (for e even, 3 divides $|\mathsf{AGL}(1, 2^e)|$ but no involution in $\mathsf{AGL}(1, 2^e)$ inverts an element of order 3). Also since $\langle H, u_\alpha \rangle$ contains subgroups which are isomorphic to C_2^2, M cannot be isomorphic to $D_{2(2^e \pm 1)}$. It follows from the list of maximal subgroups of $\mathsf{PSL}(2, 2^e)$ (see [5, Sect. 260]) that $M \cong \mathsf{PSL}(2, 2^s)$ for some proper divisor s of e. Since $b, u_\alpha \in M$ commute, they lie in the same Sylow 2-subgroup S of M, so there exists $d \in M$ such that $b^d = u_\alpha$. Hence $b^d = u_\alpha = b^{z_\alpha}$ (by Part (b)), and so $d z_\alpha^{-1}$

centralises b. Since $\mathbf{C}_T(b) = P$ by (a), we obtain that $d \in Pz_\alpha$. Since $z_\alpha \in \mathbf{N}_T(P)$ has order $n := |\alpha|$, it follows that d has order divisible by n. Moreover, d must be in $\mathbf{N}_M(S) \cong \mathsf{AGL}(1, 2^s)$, and so the order of d divides $2^s - 1$. Thus n divides $2^s - 1$, a contradiction to Lemma 4.2. Thus, $\langle H, u_\alpha \rangle = \mathsf{PSL}(2, 2^e)$. □

6 The family of graphs

Let f be a positive integer, and let T, H, a, b, α, z_α (for $\alpha \neq 0$), u_α, and c_α be as in Sect. 5.

Construction 6.1 Let $G = T^2 \rtimes \langle \pi \rangle$, where $\pi \in \mathsf{Aut}(T^2)$ is such that $(x, y)^\pi = (y, x)$, for all elements $(x, y) \in T^2$. Let $L = \langle (a, a), (b, b) \rangle < T^2$, and

$$g_\alpha = (u_\alpha, bu_\alpha)\pi = (u_\alpha, u_\alpha b)\pi = (t_{1,\alpha,0,1}, t_{1,\alpha+1,0,1})\pi. \tag{5}$$

By Lemma 6.2(c) below, $g_\alpha^{-1} = g_\alpha(b, b)$. Thus $Lg_\alpha^{-1}L = Lg_\alpha(b, b)L = Lg_\alpha L$. Define $\Gamma = \Gamma(f, \alpha) = \mathsf{Cos}(G, L, Lg_\alpha L)$.

We shall need information about the following subgroups:

$$X_\alpha = \langle L, g_\alpha \rangle, \quad N_\alpha = \big\langle L, \big(c_\alpha^{-1}, c_\alpha\big)\big\rangle. \tag{6}$$

Lemma 6.2 *The following facts hold.*

(a) $|G| = 2^{2f+1}(2^{2f} - 1)^2$.
(b) $(a, a)^{g_\alpha} = (c_\alpha^{-1}, c_\alpha)$, *where* c_α *is as in* (4) *and has order* 3. *Thus* $N_\alpha \leq X_\alpha$.
(c) $g_\alpha^{-1} = g_\alpha(b, b)$ *and* $(b, b)^{g_\alpha} = (b, b)$.
(d) *For* $f \geq 2$ *and* α *a generator of* $\mathsf{GF}(2^f)$, *either* $N_\alpha = T^2$ *or* $N_\alpha = \{(t, t^\nu) | t \in T\} \cong T$ *for some* $\nu \in \mathsf{Aut}(T)$.

Proof (a) follows from the fact that $|G| = 2|T|^2$.
(b) We have $(a, a)^{g_\alpha} = (a^{u_\alpha}, (a^b)^{u_\alpha})^\pi = (c_\alpha, c_\alpha^{-1})^\pi = (c_\alpha^{-1}, c_\alpha)$, by (4), and hence $N_\alpha \leq X_\alpha$. Since c_α is conjugate to a, it has order 3.
(c) We have $g_\alpha^2(b, b) = (u_\alpha, bu_\alpha)\pi(u_\alpha, bu_\alpha)\pi(b, b) = (u_\alpha, bu_\alpha)(bu_\alpha, u_\alpha)(b, b) = (1, 1)$ since $u_\alpha b = bu_\alpha$ by Lemma 5.1(a). Thus $g_\alpha^{-1} = g_\alpha(b, b)$. We also have $(b, b)^{g_\alpha} = (b^{u_\alpha}, b^{u_\alpha b})^\pi = (b, b)^\pi = (b, b)$, using Lemma 5.1(a) for the second equality.
(d) The projections of N_α onto each of the two coordinates are equal to $\langle a, b, c_\alpha \rangle$. Since $u_\alpha b = bu_\alpha$, the subgroup $\langle a, b, c_\alpha \rangle$ of T is normalised by each of a, b and u_α. Hence $\langle a, b, c_\alpha \rangle \lhd \langle a, b, u_\alpha \rangle$, and $\langle a, b, u_\alpha \rangle = T$ by Lemma 5.1(e). Thus $\langle a, b, c_\alpha \rangle = T$ since T is simple, and so $N_\alpha = T^2$ or $N_\alpha \cong T$. In the latter case, N_α is a diagonal subgroup of T^2 and hence $N_\alpha = \{(t, t^\nu) | t \in T\} \cong T$ for some $\nu \in \mathsf{Aut}(T)$. □

We first describe some general properties of the graphs $\Gamma(f, \alpha)$.

Proposition 6.3 *Let $f \geq 1$ be an integer and α be an element of* $\mathsf{GF}(2^f)$. *Let $\Gamma = \Gamma(f,\alpha)$, G, T, L, π be as in Construction 6.1. Then Γ is bipartite, cubic, and, if Γ is connected, then it has diameter at least $6f-3$. Moreover, $G^+ = T^2$, $G \leq \mathsf{Aut}(\Gamma)$ and $|V\Gamma| = 2^{2f}(2^{2f}-1)^2/3$.*

Proof By Lemma 6.2(b), $(a,a)^{g_\alpha} = (c_\alpha^{-1}, c_\alpha)$, which is not in L since $c_\alpha \neq c_\alpha^{-1}$, and, by Lemma 6.2(c), $(b,b)^{g_\alpha} = (b,b)$. Thus the intersection $L^{g_\alpha} \cap L = \langle (b,b)\rangle \cong C_2$, and so the graph Γ has valency $|L : L^{g_\alpha} \cap L| = 3$ (hence is cubic) by Lemma 2.2(a). Moreover, T^2 has two orbits on the cosets of L, and since $T^2 \cap Lg_\alpha L = \emptyset$, no vertices in the same orbit are adjacent. Hence Γ is bipartite. Since T^2 is an index 2 subgroup of G and its orbits are the two bipartite halves, the even subgroup G^+ is precisely T^2. The number of vertices of Γ is $|G|/|L| = 2^{2f}(2^{2f}-1)^2/3$, with each bipartite half of size $2^{2f-1}(2^{2f}-1)^2/3$.

Suppose Γ is connected and let $d = \mathsf{diam}(\Gamma)$. We have $|\Gamma_1(L)| = 3$ and $|\Gamma_i(L)|$ is at most $2|\Gamma_{i-1}(L)|$ for $2 \leq i \leq d$. Hence the number of vertices of Γ is at most $1 + 3 + 3.2 + \cdots + 3.2^{d-1} = 1 + 3(2^d - 1)$. Therefore $2^{2f}(2^{2f}-1)^2/3 \leq 1 + 3(2^d-1)$, or equivalently, $2^{2f}(2^{2f}-1)^2/9 + 2/3 \leq 2^d$, which implies $2^{2f}(2^{2f}-1)^2/9 < 2^d$. Thus $(2^{2f}-1)/3 < 2^{\frac{d}{2}-f}$. Now for all $f \geq 1$, we have $(2^{2f}-1)/3 \geq 2^{2f}/4 = 2^{2f-2}$, and so $2^{2f-2} < 2^{\frac{d}{2}-f}$. Therefore, $2f-2 < \frac{d}{2} - f$ and $d > 6f-4$. Since $\bigcap_{x\in G} L^x$ is trivial, it follows from Lemma 2.2(b) that G acts faithfully on Γ, and hence $G \leq \mathsf{Aut}(\Gamma)$. □

Note that the bound on the diameter is not tight. For example, for $f = 3$ a MAGMA [2] computation shows that $\Gamma(3,\alpha)$ has diameter 21 for α a generator of $\mathsf{GF}(8)$ (we will see in Corollary 8.6 that the graph is connected in this case).

7 Equality and connectivity

We first have a lemma determining when graphs obtained by Construction 6.1 have the same edge-set.

Proposition 7.1 *Let $f \geq 1$. Let α, β be elements of* $\mathsf{GF}(2^f)$. *Then $\Gamma(f,\alpha) = \Gamma(f,\beta)$ if and only if $\beta \in \{\alpha, \alpha+1\}$.*

Proof Suppose that $\Gamma(f,\alpha) = \Gamma(f,\beta)$. Then the double cosets $Lg_\alpha L$ and $Lg_\beta L$ coincide, and so $g_\beta \in Lg_\alpha L$. Since π centralises L, this implies, using (5), that $(u_\beta, bu_\beta) = (h_1,h_1)(u_\alpha, bu_\alpha)(h_2,h_2)$ for some $h_1, h_2 \in H$. Thus $h_1 bu_\alpha h_2 = bu_\beta = bh_1 u_\alpha h_2$, and so h_1 commutes with b. Since b centralises P by Lemma 5.1(a) and $u_\alpha, u_\beta \in P$, we also have $h_1 u_\alpha b h_2 = u_\beta b = h_1 u_\alpha h_2 b$, and so h_2 also commutes with b. Hence $h_1, h_2 \in \mathbf{C}_H(b) = \langle b \rangle$ by Lemma 5.1(a). If $h_1 = h_2$, then $\alpha = \beta$, and if $h_2 = h_1 b$ then $\beta = \alpha + 1$.

Conversely, if $\beta = \alpha + 1$, then $g_\beta = (u_\beta, u_\beta b)\pi = (u_\alpha b, u_\alpha)\pi = g_\alpha(b,b)$, and so $Lg_\alpha L = Lg_\beta L$. Thus $\Gamma(f,\alpha) = \Gamma(f,\beta)$. □

For $f = 1$ Construction 6.1 yields only one graph.

Lemma 7.2 $\Gamma(1,0)=\Gamma(1,1)=2K_{3,3}$.

Proof Here $T=H$, and by Proposition 7.1, $\Gamma(1,0)=\Gamma(1,1)$ so we may assume $\alpha=0$. Thus $u_\alpha=1$ and $g_\alpha=(1,b)\pi$. It can be computed that $\langle L,g_\alpha\rangle=\{(x,y)|x^{-1}y\in\langle a\rangle\}\cup\{(x,yb)\pi|x^{-1}y\in\langle a\rangle\}$ has index 2 in G. Therefore, by Lemma 2.2(e), $\Gamma(1,0)$ has 2 connected components. Each must be bipartite and have valency 3 by Proposition 6.3, hence the conclusion. □

The next two general results allow us to determine the connected components of $\Gamma(f,\alpha)$.

Lemma 7.3 *Let α be an element of $\mathsf{GF}(2^f)$ and let $\mathsf{GF}(2^e)$ be the subfield generated by α. Then $\Gamma(f,\alpha)\cong m\Gamma(e,\alpha)$, where $m=|T:\mathsf{PSL}(2,2^e)|^2$.*

Proof Let $K=\mathsf{PSL}(2,2^e)^2\rtimes\langle\pi\rangle$ viewed as a subgroup of G. Then $g_\alpha\in K$ and $L\le K$, and so $\langle L,g_\alpha\rangle\le K$. By Lemma 2.2(d), $\Gamma(f,\alpha)=m\Sigma$ where $m=|G:K|$ and $\Sigma=\mathsf{Cos}(K,L,Lg_\alpha L)$. Finally, $m=|G:K|=2|T|^2/(2|\mathsf{PSL}(2,2^e)|^2)=|T:\mathsf{PSL}(2,2^e)|^2$. □

Proposition 7.4 *Let $f\ge 2$ and $\alpha\in\mathsf{GF}(2^f)$ be a generator.*

(a) *If f is odd, or if f is even and $\alpha^{2^{(f/2)}}\ne\alpha+1$, then $\Gamma(f,\alpha)$ is connected.*
(b) *If f is even and $\alpha^{2^{(f/2)}}=\alpha+1$, then $\Gamma(f,\alpha)$ has $|T|$ connected components, each containing $|T|/3$ vertices and isomorphic to $\mathsf{Cos}(\langle T,\nu\rangle,H,Hu_\alpha\nu H)$ where $H=\mathsf{PSL}(2,2)$ and $\nu=\tau^{(f/2)}$.*

Proof We set $X_\alpha=\langle L,g_\alpha\rangle$ and $N_\alpha=\langle L,(c_\alpha^{-1},c_\alpha)\rangle$ as in (6). By Lemma 2.2(e), the number of connected components of $\Gamma(f,\alpha)$ is $|G:X_\alpha|$ and all connected components are isomorphic to $\mathsf{Cos}(X_\alpha,L,Lg_\alpha L)$.

We have $\alpha\notin\{0,1\}$, since α is a generator and $f\ne 1$.

By Lemma 6.2(b), $N_\alpha\le X_\alpha$, and by Lemma 6.2(d), either $N_\alpha=T^2$ or $N_\alpha=\{(t,t^\nu)|t\in T\}$ for some $\nu\in\mathsf{Aut}(T)$. In the latter case, since N_α contains (a,a), (b,b) and (c_α^{-1},c_α), ν must be in $\mathbf{C}_{\mathsf{Aut}(T)}(\langle a,b\rangle)$ and must satisfy $c_\alpha^\nu=c_\alpha^{-1}$. Since $\langle a,b\rangle=\mathsf{PSL}(2,2)$, we have $\mathbf{C}_{\mathsf{Aut}(T)}(\langle a,b\rangle)=\mathbf{C}_{\mathsf{Aut}(T)}(\mathsf{PSL}(2,2))=\mathsf{Aut}(\mathsf{GF}(2^f))=\langle\tau\rangle\cong C_f$, where τ is the Frobenius automorphism described in (2).

Assume f is odd, or f is even and $\alpha^{2^{(f/2)}}\ne\alpha+1$. Then by Lemma 4.3(a), $\alpha^{2^i}\ne\alpha+1$ for all $i<f$, and so by Lemma 5.1(c), $c_\alpha^{\tau^i}\ne c_\alpha^{-1}$ for all $i<f$. Hence there is no $\nu\in\mathbf{C}_{\mathsf{Aut}(T)}(\langle a,b\rangle)$ satisfying $c_\alpha^\nu=c_\alpha^{-1}$. Thus $N_\alpha=T^2$, and so $X_\alpha=G$ since $g_\alpha\notin T^2$. Thus $\Gamma(f,\alpha)$ is connected and (a) holds.

Now assume f is even and $\alpha^{2^i}=\alpha+1$, where $i=f/2$. Let $\nu:=\tau^i$. By Lemma 5.1(c), $\nu\in\mathbf{C}_{\mathsf{Aut}(T)}(\langle a,b\rangle)$ and satisfies $c_\alpha^\nu=c_\alpha^{-1}$, and so $N_\alpha=\{(t,t^\nu)|t\in T\}\cong T$. Notice ν is an involution. We have $N_\alpha\le X_\alpha$, and so $\langle N_\alpha,g_\alpha\rangle\le\langle X_\alpha,g_\alpha\rangle=X_\alpha$. On the other hand, $X_\alpha=\langle(a,a),(b,b),g_\alpha\rangle\le\langle(a,a),(b,b),(c_\alpha^{-1},c_\alpha),g_\alpha\rangle=\langle N_\alpha,g_\alpha\rangle$. Thus $X_\alpha=\langle N_\alpha,g_\alpha\rangle$. Notice that $u_\alpha^\nu=t_{1,\alpha^{2^i},0,1}=u_{\alpha+1}=u_\alpha b$, and so $g_\alpha=(u_\alpha,u_\alpha^\nu)\pi$. Therefore, $\langle N_\alpha,g_\alpha\rangle=\langle N_\alpha,\pi\rangle=N_\alpha\rtimes\langle\pi\rangle$. Hence, $|X_\alpha|=2|N_\alpha|=2|T|$.

Moreover, $X_\alpha = \{(t, t^\nu)\pi^\epsilon | t \in T, \epsilon \in \{0, 1\}\}$. Also the number of connected components is $|G : X_\alpha| = |T|$ by Lemma 2.2(e).

We now prove that X_α is isomorphic to $\langle T, \nu\rangle$. We define

$$\phi : X_\alpha \to \langle T, \nu\rangle : (t, t^\nu)\pi^\epsilon \mapsto t\nu^\epsilon.$$

We first show that ϕ is a homomorphism, that is, that $\phi((t_1, t_1^\nu)\pi^{\epsilon_1}(t_2, t_2^\nu)\pi^{\epsilon_2}) = \phi((t_1, t_1^\nu)\pi^{\epsilon_1})\phi((t_2, t_2^\nu)\pi^{\epsilon_2})$. This clearly holds for $\epsilon_1 = 0$. We now prove the case $\epsilon_1 = 1$.

$$\begin{aligned}
\phi\big((t_1, t_1^\nu)\pi\big(t_2, t_2^\nu\big)\pi^{\epsilon_2}\big) &= \phi\big(\big(t_1, t_1^\nu\big)\big(t_2^\nu, t_2\big)\pi\pi^{\epsilon_2}\big) \\
&= \phi\big(\big(t_1t_2^\nu, t_1^\nu t_2\big)\pi^{1-\epsilon_2}\big) \\
&= t_1t_2^\nu\nu^{1-\epsilon_2} \\
&= t_1\nu t_2\nu\nu^{1-\epsilon_2} \\
&= (t_1\nu)\big(t_2\nu^{\epsilon_2}\big) \\
&= \phi\big(\big(t_1, t_1^\nu\big)\pi\big)\phi\big(\big(t_2, t_2^\nu\big)\pi^{\epsilon_2}\big).
\end{aligned}$$

Thus ϕ is a homomorphism. Clearly, $\mathsf{Ker}\phi = 1$, and $|X_\alpha| = |\langle T, \nu\rangle| = 2|T|$, and so ϕ is a bijection. Therefore, ϕ is an isomorphism.

Notice that $\phi(L) = \langle a, b\rangle = H$ and $\phi(g_\alpha) = u_\alpha\nu$.

By Lemma 2.2(e), each connected component of $\Gamma(f,\alpha)$ is isomorphic to $\mathsf{Cos}(X_\alpha, L, Lg_\alpha L)$, and ϕ induces a graph isomorphism $\mathsf{Cos}(X_\alpha, L, Lg_\alpha L) \cong \mathsf{Cos}(\langle T, \nu\rangle, H, Hu_\alpha\nu H)$. Thus (b) holds. □

Note that the proof of Proposition 7.4 uses the fact that T is simple through Lemma 6.2(d) and hence requires $f \geq 2$.

Putting together Lemma 7.3 and Proposition 7.4, we get the following corollary.

Corollary 7.5 *Let $f \geq 2$ and let $\mathsf{GF}(2^e)$ be the subfield generated by α.*

(a) *If e is odd, or if e is even and $\alpha^{2^{(e/2)}} \neq \alpha + 1$, then $\Gamma(f,\alpha) = m\Gamma(e,\alpha)$, where $m = |T : \mathsf{PSL}(2, 2^e)|^2$ and $\Gamma(e,\alpha)$ is connected.*

(b) *If e is even and $\alpha^{2^{(e/2)}} = \alpha + 1$, then $\Gamma(f,\alpha)$ has $|\mathsf{PSL}(2, 2^e)|^{-1}|\mathsf{PSL}(2, 2^f)|^2$ connected components, each isomorphic to $\mathsf{Cos}(\langle\mathsf{PSL}(2, 2^e), \nu\rangle, H, Hu_\alpha\nu H)$, where $H = \mathsf{PSL}(2, 2)$ and $\nu = \tau^{(e/2)}$.*

We can now deal with the case $f = 2$. Take $\mathsf{GF}(4) = \{a + bi | a, b \in \mathsf{GF}(2), i^2 = i + 1\}$. By Proposition 7.1, Construction 6.1 yields two graphs for $f = 2$, namely $\Gamma(2, 0)$ and $\Gamma(2, i)$.

Corollary 7.6 *The two graphs obtained by Construction 6.1 for $f = 2$ are not connected. More precisely,*

(a) *$\Gamma(2, 0) \cong 200\, K_{3,3}$, and*

(b) $\Gamma(2,i)\cong 60\mathcal{D}$ *where* $\mathcal{D}$ *is the incidence graph of the Desargues configuration, called the Desargues graph* (*it is a double cover of the Petersen graph*).

Proof Consider first $\alpha=0$. By Lemma 7.3, $\Gamma(2,0)\cong m\Gamma(1,0)$, where $m=|\mathsf{PSL}(2,2^2):\mathsf{PSL}(2,2^1)|^2=100$. Part (a) follows from Proposition 7.2.

Now assume $\alpha=i$. Then $\alpha^{2^{(f/2)}}=i^2=i+1=\alpha+1$, so part (b) of Proposition 7.4 holds. Here $u_\alpha=t_{1,i,0,1}$ and $\nu=\tau$. Thus $\Gamma(2,i)$ has $|\mathsf{PSL}(2,2^2)|=60$ connected components, each containing $60/3=20$ vertices and isomorphic to $\mathsf{Cos}(\mathsf{P}\Gamma\mathsf{L}(2,4),H,Hu_\alpha\tau H)$ where $H=\mathsf{PSL}(2,2)$. There are only two arc-transitive cubic graphs on 20 vertices, the Desargues graph and the dodecahedron (see [1, p. 148]). Since $\Gamma(2,i)$ is bipartite by Proposition 6.3, its connected components cannot be dodecahedrons, hence they are Desargues graphs. The Desargues graph has vertices the points and lines of the Desargues configuration, with two vertices adjacent if they form a flag (incident point-line pair) of the configuration. It is a double cover of the Petersen graph. □

8 Automorphism groups and isomorphisms for connected $\Gamma(f,\alpha)$

The remainder of this paper is concerned mainly with the connected graphs $\Gamma(f,\alpha)$ given by Construction 6.1, that is, we may assume from now on that α is a generator and, if f is even, then $\alpha^{2^{(f/2)}}\neq\alpha+1$ (see Corollary 7.5). By Lemma 7.2 and Corollary 7.6, we may assume that $f\geq 3$.

In this section, we determine the full automorphism group A of $\Gamma=\Gamma(f,\alpha)$ and the normaliser of A in $\mathsf{Sym}(V\Gamma)$. This will then enable us to determine a lower bound on the number of non-isomorphic such graphs, for a given f.

Proposition 8.1 *Let $f\geq 3$ be an integer and $\alpha\in\mathsf{GF}(2^f)$. Let $\Gamma=\Gamma(f,\alpha)$, G, T, L, π be as in Construction 6.1 with Γ connected. The full automorphism group of Γ is $A=G\times\langle\sigma\rangle$, where σ is given by $(Lx)^\sigma=L\pi x$ for all $x\in G$. In particular, A does not depend on the choice of α and Γ is $(A,3)$-arc transitive but not $(A,4)$-arc-transitive. Moreover, the stabiliser in A of the vertex L is $L\times\langle\pi\sigma\rangle\cong D_{12}$.*

Proof Let A be the full automorphism group of Γ. By Proposition 6.3, $G\leq A$. Define the map σ on $V\Gamma$ by $(Lx)^\sigma=L\pi x$ for all $x\in G$. This is a well defined bijection, since π centralises L. Consider an edge $\{Lg_1,Lg_2\}$, that is, $g_2g_1^{-1}\in Lg_\alpha L$. Its image under σ is $\{L\pi g_1,L\pi g_2\}$. We have $\pi g_2(\pi g_1)^{-1}=\pi g_2g_1^{-1}\pi\in\pi Lg_\alpha L\pi=L\pi g_\alpha\pi L$. Recall that $g_\alpha=(u_\alpha,u_\alpha b)\pi$ and $u_\alpha b=bu_\alpha$, so $\pi g_\alpha\pi=(u_\alpha b,u_\alpha)\pi=(b,b)g_\alpha$. Thus $L\pi g_\alpha\pi L=Lg_\alpha L$, so $\{Lg_1,Lg_2\}^\sigma$ is an edge, and $\sigma\in A$. We now show that σ centralises G. Indeed, let $h\in G$ and $Lx\in V\Gamma$, then $(Lx)^{h\sigma}=(Lxh)^\sigma=L\pi xh=(L\pi x)^h=(Lx)^{\sigma h}$. Hence $\sigma h=h\sigma$, and $\sigma\in\mathbf{C}_A(G)$. Since $\mathbf{Z}(G)=1$, we have $\sigma\notin G$. Also $\sigma^2=1$. Therefore, $R:=G\times\langle\sigma\rangle\leq A$. The stabiliser of $L\in V\Gamma$ in R is $R_L=L\times\langle\pi\sigma\rangle\cong S_3\times C_2\cong D_{12}$.

By Lemma 2.2(b), Γ is $(G,1)$-arc transitive, and so is $(R,1)$-arc transitive. Tutte [14, 15] proved that the automorphism group of an arc-transitive finite graph with valency 3 acts regularly on s-arcs for some $s\leq 5$, and the stabiliser of a vertex has order 3.2^{s-1}. Since $|R_L| = 12$, R acts regularly on the 3-arcs of Γ (and hence is not transitive on 4-arcs).

Suppose $R < A$. Since both R and A are transitive on $V\Gamma$, the Orbit-Stabiliser Theorem implies that $R_L < A_L$, and so A would act regularly on s-arcs for some $s = 4$ or 5. By Theorem 3 of [7], this is not possible. Hence $A = R$. □

Definition 8.2 Let $\Gamma = \Gamma(f, \alpha)$ (not necessarily connected). We define $\bar{\tau} : V\Gamma \to V\Gamma : L(c,d)\pi^{\epsilon} \mapsto L(c^{\tau}, d^{\tau})\pi^{\epsilon}$ for each $(c,d) \in T^2, \epsilon \in \{0,1\}$, where τ is as defined in (2).

Lemma 8.3 *Let $\Gamma = \Gamma(f, \alpha)$ (not necessarily connected) and let $\bar{\tau}$ be as in Definition 8.2. Then $\bar{\tau}$ induces an isomorphism from Γ to $\Gamma(f, \alpha^2)$. Moreover $\langle \bar{\tau} \rangle \cong C_f$.*

Proof We have τ, as defined in (2), in $\mathsf{Aut}(T)$. We denote by μ the element of $\mathsf{Aut}(G)$ defined by $(c,d)^{\mu} = (c^{\tau}, d^{\tau})$ for all $(c,d) \in T^2$ and by $\pi^{\mu} = \pi$. Then, since μ centralises (a,a) and (b,b), we have that $\mu \in \mathbf{N}_{\mathsf{Aut}\, G}(L)$. Thus we can use Lemma 2.2(f), with $\bar{\mu} : Lx \mapsto Lx^{\mu}$. More precisely for $(c,d) \in T^2, \epsilon \in \{0,1\}$, we have $(L(c,d)\pi^{\epsilon})^{\bar{\mu}} = L(c,d)^{\mu}(\pi^{\epsilon})^{\mu} = L(c^{\tau}, d^{\tau})\pi^{\epsilon}$. Hence $\bar{\mu} = \bar{\tau}$ is a permutation of $V\Gamma$ and induces an isomorphism from $\Gamma = \mathsf{Cos}(G, L, Lg_{\alpha}L)$ to $\mathsf{Cos}(G, L, Lg_{\alpha}^{\mu}L)$ by Lemma 2.2(f). Note that $g_{\alpha}^{\mu} = ((t_{1,\alpha,0,1}, t_{1,\alpha+1,0,1})\pi)^{\mu}$ (see (5)), and so $g_{\alpha}^{\mu} = ((t_{1,\alpha,0,1})^{\tau}, (t_{1,\alpha+1,0,1})^{\tau})\pi = (t_{1,\alpha^2,0,1}, t_{1,\alpha^2+1,0,1})\pi = g_{\alpha^2}$. Therefore, $\mathsf{Cos}(G, L, Lg_{\alpha}^{\mu}L) = \Gamma(f, \alpha^2)$.

For $i \geq 1$, the permutation $\bar{\tau}^i$ of $V\Gamma$ maps the coset $L(c,d)\pi^{\epsilon}$ onto $L(c^{\tau^i}, d^{\tau^i})\pi^{\epsilon}$. Thus $\bar{\tau}$ has the same order as τ, and so $\langle \bar{\tau} \rangle \cong C_f$. □

We now determine $\mathbf{N}_{\mathsf{Sym}(V\Gamma)}(A)$.

Lemma 8.4 *Let $\Gamma = \Gamma(f, \alpha)$ and A be as in Proposition 8.1. Then $\mathbf{N}_{\mathsf{Sym}(V\Gamma)}(A) = A \rtimes \langle \bar{\tau} \rangle \cong A.C_f$, where $\bar{\tau}$ is as defined in Definition 8.2.*

Proof Set $N := \mathbf{N}_{\mathsf{Sym}(V\Gamma)}(A)$ and $N_0 := \langle A, \bar{\tau} \rangle$. We use the notation of Construction 6.1. By Lemma 8.3, $\bar{\tau} \in \mathsf{Sym}(V\Gamma)$. Moreover, it follows from the definitions of $\bar{\tau}$ and σ that $\bar{\tau}^{-1}(c,d)\bar{\tau} = (c^{\tau}, d^{\tau})$ for each $(c,d) \in T^2$, and $[\bar{\tau}, \sigma] = [\bar{\tau}, \pi] = 1$. Thus $N_0 = A \rtimes \langle \bar{\tau} \rangle \leq N$ with $N_0/A \cong \langle \bar{\tau} \rangle \cong C_f$.

Since T^2 is a characteristic subgroup of A, each element of N induces an automorphism of T^2, and we have a homomorphism $\varphi : N \to \mathsf{Aut}(T^2)$ with kernel $K = \mathbf{C}_N(T^2) \leq \mathbf{C}_{\mathsf{Sym}(V\Gamma)}(T^2) = \mathbf{C}$, say. Now K (and hence $\mathbf{C}$) contains $Z(A) = \langle \sigma \rangle \cong C_2$, which interchanges the two orbits of T^2 in $V\Gamma$, and so the subgroup $\mathbf{C}^+$ of $\mathbf{C}$ stabilising each of the T^2-orbits setwise has index 2 in $\mathbf{C}$. The two T^2-orbits are the sets Δ_1 and Δ_2 of L-cosets in T^2 and $T^2 g_{\alpha}$ respectively, and L is the stabiliser in T^2 of the vertex L of Δ_1 and also the stabiliser in T^2 of the vertex $L\pi$ of Δ_2. For $i = 1, 2$, let S_i, L_i denote the permutation groups on Δ_i induced by T^2 and L, respectively. Then by Lemma 5.1(d), $\mathbf{N}_{S_i}(L_i) = L_i$ and by [6, Theorem 4.2A(i)], $\mathbf{C}_{\mathsf{Sym}(\Delta_i)}(S_i) \cong \mathbf{N}_{S_i}(L_i)/L_i = 1$. Thus $\mathbf{C}^+ = 1$ and $K = \mathbf{C} = \langle \sigma \rangle$, of order 2.

Now $\varphi(N)$ contains the inner automorphism group $\varphi(T^2)$ of T^2, and the quotient $\varphi(N)/\varphi(T^2)$ is contained in the outer automorphism group of T^2, which is isomorphic to $\langle \tau \rangle \operatorname{wr} \langle \pi \rangle$. Further, $\varphi(N)/\varphi(T^2)$ normalises $\varphi(A)/\varphi(T^2)$, which corresponds to the subgroup $\langle\pi\rangle$ of $\langle\tau\rangle\,\mathrm{wr}\langle\pi\rangle$, and so the subgroup of $\langle\tau\rangle\,\mathrm{wr}\langle\pi\rangle$ corresponding to $\varphi(N)/\varphi(T^2)$ lies in the normaliser of $\langle\pi\rangle$ in $\langle\tau\rangle\,\mathrm{wr}\langle\pi\rangle$, namely $\langle(\tau,\tau)\rangle\times\langle\pi\rangle\cong C_f\times C_2$. On the other hand, $\varphi(N)/\varphi(T^2)$ contains $\varphi(N_0)/\varphi(T^2)\cong\langle\bar\tau\rangle\times\langle\pi\rangle$. Thus equality holds, and we conclude that $N=N_0$. □

We are now able to determine a lower bound on the number of non-isomorphic connected graphs $\Gamma(f,\alpha)$ for each f. They are obviously not isomorphic for different values of f, so in particular, it follows that there are infinitely many such graphs, as the lower bound is increasing with f.

Proposition 8.5 *Let* $f\geq 3$.

(a) *Let* $\Gamma(f,\alpha)$ *and* $\Gamma(f,\beta)$ *be connected graphs. Then* $\Gamma(f,\alpha)\cong\Gamma(f,\beta)$ *if and only if* $\beta\in\{\alpha^{2^i}\,|\,0\leq i<f\}\cup\{\alpha^{2^i}+1\,|\,0\leq i<f\}$.

(b) *The number of pairwise non-isomorphic connected graphs* Γ *obtained from Construction 6.1 is greater than* $2^{f-2}/f$ *if* f *is odd and greater than* $(2^{f-2}-2^{f/2-1})/f$ *if* f *is even.*

Proof Let $\Gamma=\Gamma(f,\alpha)$ and $\Gamma(f,\beta)$ be connected graphs produced by Construction 6.1. By Corollary 7.5, α and β are generators, and if f is even then $\alpha^{2^{(f/2)}}\neq\alpha+1$ and $\beta^{2^{(f/2)}}\neq\beta+1$.

Suppose that ψ is an isomorphism from $\Gamma(f,\alpha)$ to $\Gamma(f,\beta)$. Since $V\Gamma=V\Gamma(f,\beta)$, the isomorphism ψ is an element of $\mathsf{Sym}(V\Gamma)$ and since, by Proposition 8.1, $\mathsf{Aut}(\Gamma(f,\alpha))=\mathsf{Aut}(\Gamma(f,\beta))=A$, it follows that ψ is an element of $\mathbf{N}_{\mathsf{Sym}(V\Gamma)}(A)$. By Lemma 8.4, $\mathbf{N}_{\mathsf{Sym}(V\Gamma)}(A)=A\rtimes\langle\bar\tau\rangle$. Thus $\Gamma(f,\beta)$ is the image of $\Gamma(f,\alpha)$ under $\bar\tau^i$ for some i such that $0\leq i<f$. We have $\Gamma(f,\beta)=\Gamma(f,\alpha)^{\bar\tau^i}=\Gamma(f,\alpha^{2^i})$ by Lemma 8.3. Therefore, by Proposition 7.1, $\beta=\alpha^{2^i}$ or $\alpha^{2^i}+1$, and so $\beta\in\{\alpha^{2^i}\,|\,0\leq i<f\}\cup\{\alpha^{2^i}+1\,|\,0\leq i<f\}$.

Suppose now that $\beta\in\{\alpha^{2^i}\,|\,0\leq i<f\}\cup\{\alpha^{2^i}+1\,|\,0\leq i<f\}$. Then, by Proposition 7.1, $\Gamma(f,\beta)=\Gamma(f,\alpha^{2^i})$ for some $0\leq i<f$, which, by Lemma 8.3, is equal to $\Gamma(f,\alpha)^{\bar\tau^i}$, where $\bar\tau^i$ is a graph isomorphism. Hence $\Gamma(f,\alpha)\cong\Gamma(f,\beta)$ and part (a) holds.

Let α be a generator such that, if f is even, $\alpha^{2^{(f/2)}}\neq\alpha+1$. We claim that the set $\{\alpha^{2^i}\,|\,0\leq i<f\}\cup\{\alpha^{2^i}+1\,|\,0\leq i<f\}$ has size $2f$. Notice first that all elements x of this set are generators and do not satisfy the equation $x^{2^{(f/2)}}\neq x+1$. Suppose $\alpha^{2^i}=\alpha^{2^j}$ for some i,j such that $0\leq i<j<f$, then $\alpha^{2^i}=(\alpha^{2^i})^{2^{j-i}}$, contradicting Lemma 4.3(b) for the generator α^{2^i}. Hence $\{\alpha^{2^i}\,|\,0\leq i<f\}$ and $\{\alpha^{2^i}+1\,|\,0\leq i<f\}$ both have size f. Now suppose $\alpha^{2^i}=\alpha^{2^j}+1$ for some i,j such that $0\leq i<j<f$ (we can assume $i<j$ without loss of generality, because otherwise we just add 1 to both sides of the equation). Thus $\alpha^{2^i}=(\alpha^{2^i})^{2^{j-i}}+1$. Applying Lemma 4.3(a) to the generator α^{2^i}, we get that f is even, $j-i=f/2$ and $\alpha^{2^i}=(\alpha^{2^i})^{2^{f/2}}+1$. However, since α^{2^i} does not satisfy the equation $x^{2^{(f/2)}}\neq x+1$, this is a contradiction. Thus the claim is proved.

Suppose first f is odd. Then $\Gamma(f,\alpha)$ is connected if and only if α is a generator, by Corollary 7.5. By Lemma 4.4, the number of generators of $\mathsf{GF}(2^f)$ is strictly greater than 2^{f-1}. By the claim and part (a), exactly $2f$ of those generators yield isomorphic graphs, thus the number of pairwise non-isomorphic connected graphs is greater than $2^{f-2}/f$.

Finally, assume f is even. Then $\Gamma(f,\alpha)$ is connected if and only if α is a generator and $\alpha^{2^{(f/2)}} \neq \alpha+1$, by Corollary 7.5. By Lemma 4.5, the number of such elements is greater than $2^{f/2}(2^{f/2-1}-1)$. By the claim and part (a), exactly $2f$ of those generators yield isomorphic graphs, thus the number of pairwise non-isomorphic connected graphs is greater than $2^{f/2-1}(2^{f/2-1}-1)/f = (2^{f-2}-2^{f/2-1})/f$. □

We illustrate this result by considering the case $f=3$ where we obtain the first connected examples. Take $\mathsf{GF}(8) = \{a+bj+cj^2 | a,b,c \in \mathsf{GF}(2), j^3 = j+1\}$. For $f=3$, our construction yields four graphs with different edge-sets, namely $\Gamma(3,0)$, $\Gamma(3,j)$, $\Gamma(3,j^2)$ and $\Gamma(3,j^4)$, by Proposition 7.1.

Corollary 8.6 *Up to isomorphism, Construction 6.1 for $f=3$ yields two graphs, one of which is connected. More precisely,*

(a) $\Gamma(3,0) \cong 14112\, K_{3,3}$, *and*
(b) $\Gamma(3,j) \cong \Gamma(3,j^2) \cong \Gamma(3,j^4)$ *is connected.*

Proof Consider first $\alpha = 0$. By Lemma 7.3, $\Gamma(3,0) \cong m\Gamma(1,0)$, where $m = |\mathsf{PSL}(2,2^8) : \mathsf{PSL}(2,2)|^2 = 84^2$. Part (a) now follows from Proposition 7.2. Now assume $\alpha = j$. By Proposition 7.4, $\Gamma(3,j)$ is connected, and by Proposition 8.5(a), $\Gamma(3,j) \cong \Gamma(3,j^2) \cong \Gamma(3,j^4)$. □

For $f=4$ also, our construction yields just one connected graph and three disconnected ones, up to isomorphism. Take $\mathsf{GF}(16) = \{a+bk+ck^2+dk^3 | a,b,c,d \in \mathsf{GF}(2), k^4 = k+1\}$.

Corollary 8.7 *Up to isomorphism, Construction 6.1 for $f=4$ yields four graphs, one of which is connected. More precisely,*

(a) $\Gamma(4,0) = 924800\, K_{3,3}$,
(b) *For $\alpha \in \{k^5, k^{10}\}$, $\Gamma(f,\alpha) \cong 277440\,\mathcal{D}$, where $\mathcal{D}$ is the Desargues graph,*
(c) *For $\alpha \in \{k,k^2,k^4,k^8\}$, $\Gamma(4,\alpha) \cong \Gamma(4,k)$ has 4080 connected components, and*
(d) *For α a generator not in $\{k,k^2,k^4,k^8\}$, $\Gamma(4,\alpha) \cong \Gamma(4,k^3)$ is connected.*

Proof Consider first $\alpha = 0$. By Lemma 7.3, $\Gamma(4,0) \cong m\Gamma(1,0)$, where $m = |\mathsf{PSL}(2,16) : \mathsf{PSL}(2,2)|^2 = 680^2$. Part (a) now follows from Proposition 7.2.

The element k^5 generates $\mathsf{GF}(4) = \{0,1,k^5,k^{10}\}$, and so by Lemma 7.3, $\Gamma(4,k^5) \cong m\Gamma(2,k^5)$, where $m = |\mathsf{PSL}(2,16) : \mathsf{PSL}(2,4)|^2 = 68^2$. Now $\Gamma(2,k^5)$ is $\Gamma(2,i)$ from Corollary 7.6, and so $\Gamma(4,k^5) \cong 68^2.60\,\mathcal{D} = 277440\,\mathcal{D}$. Now $k^{10} = k^5+1$, and so by Proposition 7.1, $\Gamma(4,k^5) = \Gamma(4,k^{10})$. Thus part (b) holds.

Now assume $\alpha = k$. By Proposition 8.5(a), $\Gamma(4,k) \cong \Gamma(4,k^2) \cong \Gamma(4,k^4) \cong \Gamma(4,k^8)$. Since α is a generator and $\alpha^{2^{(f/2)}} = \alpha^4 = \alpha+1$, by Proposition 7.4, $\Gamma(4,k)$ has $|T| = 4080$ connected components. Thus part (c) holds.

Finally, assume $\alpha = k^3$. Then, by Proposition 8.5(a), $\Gamma(f,\beta) \cong \Gamma(f,k^3)$ if and only if $\beta \in \{\alpha^{2^i} | 0 \le i < f\} \cup \{\alpha^{2^i} + 1 | 0 \le i < f\} = \{k^3, k^6, k^{12}, k^9\} \cup \{k^{14}, k^{13}, k^{11}, k^7\}$, that is, if β is any generator not in $\{k, k^2, k^4, k^8\}$. Moreover, by Proposition 7.4, $\Gamma(4, k^3)$ is connected since $\alpha^4 \neq \alpha + 1$. Thus part (d) holds. □

For $f = 5$, the bound of Proposition 8.5 tells us that there are at least 2 non-isomorphic connected graphs obtained by Construction 6.1. Actually, there are 30 generators, exactly $2f = 10$ of them yielding isomorphic graphs, and so there are 3 pairwise non-isomorphic connected graphs for $f = 5$.

9 Symmetry properties for connected $\Gamma(f,\alpha)$

In this section, we study the symmetry properties described in Tables 1 and 2 possessed by connected graphs $\Gamma(f,\alpha)$. This includes a formal proof of Theorems 1.1 and 1.2. We start by defining the following five groups of automorphisms.

Definition 9.1 We consider the following five subgroups of A, whose inclusions are given in Fig. 1.

1. $A = G \times \langle\sigma\rangle$;
2. $A^+ = T^2 \rtimes \langle\sigma\pi\rangle$;
3. $G = T^2 \rtimes \langle\pi\rangle$;
4. $M = T^2 \times \langle\sigma\rangle$;
5. $G^+ = M^+ = T^2$.

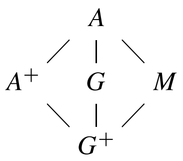
Note that $\sigma\pi$ stabilises the bipartite halves of $\Gamma(f,\alpha)$ setwise and $T^2 \rtimes \langle\sigma\pi\rangle$ is maximal in A, hence it is A^+. By Proposition 6.3, $G^+ = T^2$. Since T^2 is maximal in M, it follows that $M^+ = T^2$.

We have the following results on s-arc transitivity.

Proposition 9.2 *Let $f \ge 3$, $\Gamma(f,\alpha)$ be a connected graph as described in Construction 6.1, and let G, M, A, G^+, A^+ be as in Definition 9.1. Then the following facts hold.*

1. Γ *has girth at least* 10.
2. Γ *is* $(A,3)$*-arc transitive but not* $(A,4)$*-arc transitive.*
3. Γ *is locally* $(A^+,3)$*-arc transitive but not locally* $(A^+,4)$*-arc transitive.*
4. Γ *is* $(G,2)$*-arc transitive but not* $(G,3)$*-arc transitive.*
5. Γ *is* $(M,2)$*-arc transitive but not* $(M,3)$*-arc transitive.*

Fig. 1 Lattice



6. Γ *is locally* $(G^+, 2)$*-arc transitive but not locally* $(G^+, 3)$*-arc transitive.*

Proof See Proposition 8.1 for Fact 2. Since $A_L^+ = A_L$ has order 3.2^2, we have that Γ is locally $(A^+, 3)$-arc transitive but not locally $(A^+, 4)$-arc transitive and Fact 3 holds.

By [3, Theorem 2.1], all the 3-arc transitive finite graphs of girth up to 9 with valency 3 are known. The largest one has 570 vertices. By Theorem 6.3, $|V\Gamma| \geq 2^6(2^6-1)^2/3 = 84672$. Thus Γ has girth at least 10 and Fact 1 holds.

Let $X \in \{G, G^+, M\}$. The stabiliser of the vertex "L" in X is precisely L, acting as S_3 on its three neighbours. Therefore, the stabiliser of a vertex is 2-transitive on its neighbours, and so Γ is locally $(X, 2)$-arc transitive (see for instance Lemma 3.2 of [8]). Since G and M are transitive on $V\Gamma$, Γ is also $(G, 2)$-arc transitive and $(M, 2)$-arc transitive. Since $\mathsf{girth}(\Gamma) > 6$, the number of 3-arcs starting in L is exactly 12, and so X_L, which has order 6, cannot be transitive on the 3-arcs starting in L. Hence Facts 4, 5 and 6 hold. □

The lower bound of 10 on the girth is an underestimate, but is sufficient for our purposes. For example, a computation using MAGMA [2] shows that, for $f = 3$, the unique connected graph $\Gamma(f, j)$ (see Corollary 8.6) has girth 16 and for $f = 4$, the girth of the unique connected graph $\Gamma(3, k^3)$ (see Corollary 8.7) is 30.

Question 9.3 *Is the girth of the connected graphs obtained from Construction 6.1 unbounded?*

Let Γ be a graph of girth g. If $s \leq [\frac{g-1}{2}]$, then Γ is (locally) (G, s)-distance transitive if and only if Γ is (locally) (G, s)-arc transitive [4, Lemma 7.2]. Since $\Gamma(f, \alpha)$ has girth at least 10 we have the following corollary to Proposition 9.2.

Corollary 9.4 *Let* $s \leq 4$, $\Gamma = \Gamma(f, \alpha)$ *and* $X \leq \mathsf{Aut}(\Gamma)$. *Then* Γ *is* (*locally*) (X, s)*-distance transitive if and only if* Γ *is* (*locally*) (X, s)*-arc transitive*

The following proposition determines, for each of the automorphism groups $X \in \{A, G, M\}$, whether X is biquasiprimitive on vertices and whether X^+ is quasiprimitive on each bipartite half. Recall that $M^+ = G^+$.

Proposition 9.5 *Let* $f \geq 3$, $\Gamma = \Gamma(f, \alpha)$ *be a connected graph described in Construction 6.1, and let* G, M, A, G^+, A^+ *be as in Definition 9.1. Then* G *is biquasiprimitive on* $V\Gamma$, *while* M *and* A *are not biquasiprimitive on* $V\Gamma$, *and* A^+ *is quasiprimitive on each bipartite half, while* G^+ *is not.*

Proof We recall that σ centralises G. Since π (respectively, $\sigma\pi$) interchanges the two direct factors of G^+, T^2 is a minimal normal subgroup of G and of A^+, and indeed is the unique minimal normal subgroup. Since T^2 has two orbits on vertices, G is biquasiprimitive on $V\Gamma$. Also A^+ is faithful and quasiprimitive on each of its orbits.

Let $N = 1 \times T$, then N is normal in G^+ and in M. Notice that $|N| = |T| = 2^f(2^{2f}-1)$ is less than the number of vertices in each bipartite half. Hence N

is intransitive on each bipartite half and so Γ_N is nondegenerate. More precisely, $|V\Gamma_N| = 2^f(2^{2f} - 1)/3$ with half the vertices in each bipartite half. Thus G^+ is not quasiprimitive on each bipartite half.

Now let $N' = \langle\sigma\rangle$, then N' is normal in A and in M. Obviously, N' (which has order 2) is intransitive on each bipartite half and so $\Gamma_{N'}$ is nondegenerate. More precisely, $|V\Gamma_{N'}| = |V\Gamma|/2$. Thus A and M are not biquasiprimitive on $V\Gamma$. □

Remark 9.6 As mentioned in the introduction, if G^+ is not quasiprimitive on each bipartite half, which is the case here, then we can form a G^+-normal quotient and obtain a smaller locally s-arc-transitive graph. For $\Gamma = \Gamma(f,\alpha)$, we can quotient by $N = 1 \times T$. Now $G^+/N \cong T$, so this yields a locally $(T,2)$-arc transitive graph Γ_N such that T has two orbits on vertices and the stabiliser of any vertex is isomorphic to S_3. Moreover, by [8, Theorem 1.1], $\Gamma(f,\alpha)$ is a cover of this quotient. Since M normalises N, the group $M/N \cong T \times C_2$ also acts on Γ_N. This action is vertex-transitive and hence Γ_N is $(M/N,2)$-arc transitive. In particular, Γ_N is not semisymmetric.

In general, not all automorphisms of a quotient graph must arise from automorphisms of the original graph.

We can now prove our two main theorems.

Proof of Theorem 1.1 By Proposition 8.5(b), the number of non-isomorphic connected graphs $\Gamma(f,\alpha)$ increases with f odd and with f even, and so there are an infinite number of such graphs. By Proposition 9.2(4) the graphs are $(G,2)$-arc transitive. Moreover, by Proposition 9.5, G is biquasiprimitive on $V\Gamma$ while G^+ is not quasiprimitive on each bipartite half. □

Proof of Theorem 1.2 By Proposition 8.1, G has index 2 in $A = \mathsf{Aut}(\Gamma)$, and by Proposition 9.2(2), Γ is $(A,3)$-arc-transitive. It follows from Proposition 9.5 that A is not biquasiprimitive on vertices and A^+ is quasiprimitive on each bipartite half. □

Next we verify that G is indeed of the type given in [11, Theorem 1.1(c)(i)] as claimed in the introduction. First a definition:

Definition 9.7 A permutation group $G \leq \mathsf{Sym}(\Omega)$ is biquasiprimitive of type (c)(i), as described in Theorem 1.1 of [11], if G is permutationally isomorphic to a group with the following properties.

(a) $|\Omega| = 2m$ and the even subgroup $G^+ \leq S_m \times S_m$ is equal to $\{(h,h^\varphi)|h \in H\}$, where $H \leq S_m$, $\varphi \in \mathsf{Aut}(H)$ and φ^2 is an inner automorphism of H.
(b) H has two intransitive minimal normal subgroups R and S such that $S = R^\varphi$, $R = S^\varphi$, and $R \times S$ is a transitive subgroup of S_m.
(c) $\{(h,h^\varphi)|h \in R \times S\}$ is the unique minimal normal subgroup of G.

Corollary 9.8 *Let $f \geq 3$, $\Gamma = \Gamma(f,\alpha)$ be a connected graph described in Construction 6.1, and let G also be as in Construction 6.1. Then $G \leq \mathsf{Sym}(V\Gamma)$ is of type (c)(i), as described in Theorem* 1.1 *of* [11].

Proof By [11, Theorem 1.2 and Proposition 4.1], a biquasiprimitive group acting 2-arc transitively on a bipartite graph must satisfy the conditions of (a)(i) or (c)(i) of Theorem 1.1 of [11]. For groups satisfying (a)(i), the even subgroup is quasiprimitive on each bipartite half. Since the permutation group induced by the action of $G^+ = T^2$ on a bipartite half is not quasiprimitive, by Proposition 9.5, G satisfies the conditions of (c)(i), and hence is of type (c)(i) as in Definition 9.7. More precisely, we have $m = |V\Gamma|/2$, $H = T^2$, $\varphi = \pi$, $R = 1 \times T$, $S = T \times 1$, and $R \times S = T^2 = G^+$. □

The proof of Proposition 9.5 shows that Γ is an A-normal double cover of its A-normal quotient $\Gamma_{\langle\sigma\rangle}$. We have $\{L, L\pi\} = L^{\langle\sigma\rangle}$. A computation using MAGMA [2] shows that, when $f = 3$, $L\pi$ is the unique vertex at maximal distance from L. In other words, Γ is antipodal with antipodal blocks of size 2.

Question 9.9 *Let $f \geq 3$ and $\Gamma = \Gamma(f, \alpha)$ be a connected graph described in Construction 6.1. Is Γ always antipodal with antipodal blocks of size 2?*

Acknowledgements The authors thank an anonymous referee for advice that included drawing our attention to the construction in Sect. 3.

References

1. Biggs, N.: Algebraic Graph Theory, 52th edn. Cambridge University Press, New York (1992)
2. Bosma, W., Cannon, J., Playoust, C.: The Magma algebra system I: the user language. J. Symb. Comput. **24**(3/4), 235–265 (1997) Also see the MAGMA home page at http://www.maths.usyd.edu.au:8000/u/magma/
3. Conder, M., Nedela, R.: Symmetric cubic graphs of small girth. J. Comb. Theory, Ser. B **97**(5), 757–768 (2007)
4. Devillers, A., Giudici, M., Li, C.H., Praeger, C.E.: Locally s-distance transitive graphs. J. Graph Theory (2011). doi:10.1002/jgt.20574
5. Dickson, L.E.: Linear Groups: With an Exposition of the Galois Field Theory. Dover, New York (1958)
6. Dixon, J.D., Mortimer, B.: Permutation Groups. Graduate Texts in Mathematics, vol. 163. Springer, New York (1996)
7. Djoković, D.Ž., Miller, G.L.: Regular groups of automorphisms of cubic graphs. J. Comb. Theory, Ser. B **29**(2), 195–230 (1980)
8. Giudici, M., Li, C.H., Praeger, C.E.: Analysing finite locally s-arc transitive graphs. Trans. Am. Math. Soc. **356**, 291–317 (2004)
9. Li, C.H.: Finite s-arc transitive Cayley graphs and flag-transitive projective planes. Proc. Am. Math. Soc. **133**, 31–41 (2005)
10. Lorimer, P.: Vertex-transitive graphs: symmetric graphs of prime valency. J. Graph Theory **8**(1), 55–68 (1984)
11. Praeger, C.E.: Finite transitive permutation groups and bipartite vertex-transitive graphs. Ill. J. Math. **47**(1), 461–475 (2003)
12. Praeger, C.E.: On a reduction theorem for finite, bipartite 2-arc-transitive graphs. Australas. J. Combin. **7**, 21–36 (1993)
13. Praeger, C.E.: An O'Nan-Scott theorem for finite quasiprimitive permutation groups and an application to 2-arc transitive graphs. J. Lond. Math. Soc. **47**, 227–239 (1993)
14. Tutte, W.T.: A family of cubical graphs. Proc. Camb. Philos. Soc. **43**, 459–474 (1947)
15. Tutte, W.T.: On the symmetry of cubic graphs. Can. J. Math. **11**, 621–624 (1959)
16. Weiss, R.M.: The nonexistence of 8-transitive graphs. Combinatorica **1**, 309–311 (1981)