Math. Proc. Camb. Phil. Soc. (2014), **157**, 45–61 © *Cambridge Philosophical Society* 2014
doi:10.1017/S0305004114000188
First published online 15 April 2014

Semiregular elements in cubic vertex-transitive graphs and the restricted Burnside problem

BY PABLO SPIGA

Dipartimento di Matematica Pura e Applicata,
University of Milano-Bicocca, Via Cozzi 55, 20126 *Milano, Italy.*
e-mail: pablo.spiga@unimib.it

(*Received* 5 *December* 2012; *revised* 4 *February* 2014)

Abstract

In this paper, we prove that the maximal order of a semiregular element in the automorphism group of a cubic vertex-transitive graph Γ does not tend to infinity as the number of vertices of Γ tends to infinity. This gives a solution (in the negative) to a conjecture of Peter Cameron, John Sheehan and the author [**4**, conjecture 2].

However, with an application of the positive solution of the restricted Burnside problem, we show that this conjecture holds true when Γ is either a Cayley graph or an arc-transitive graph.

For the 60th birthday of Dragan Marušič

1. *Introduction*

In this paper graphs are finite, connected, with no loops and with no multiple edges. A graph Γ is *cubic* if it is regular of valency 3 and *vertex-transitive* if its automorphism group $\mathrm{Aut}(\Gamma)$ acts transitively on the vertices of Γ.

A permutation g of a finite set Ω is said to be *semiregular* if 1 is the only element of the cyclic group $\langle g\rangle$ fixing some point of Ω, that is, in the disjoint cycle decomposition of g all cycles have the same length. By analogy, an automorphism g of a graph Γ is semiregular if g is a semiregular permutation in its action on the vertices of Γ.

An old conjecture of Marušič, Jordan and Klin asserts that every finite vertex-transitive graph admits a non-identity semiregular automorphism. This conjecture was first proposed in 1981 by Marušič [**15**, problem $2\cdot 4$], then was posed again by Jordan [**12**], and was finally refined by Klin [**13**] in 1988. Now, this wide-open conjecture is known as the *Polycirculant conjecture* and is one of the most interesting old-standing problems in the theory of finite permutation groups. We refer to [**2**, **3**] for more details on this beautiful problem and to [**7**, **8**, **14**, **18**] for some remarkable evidence towards this conjecture.

Marušič and Scapellato [**16**] have shown that every cubic vertex-transitive graph admits a non-identity semiregular automorphism and hence they have settled the Polycirculant conjecture for the automorphism group of a cubic vertex-transitive graph. In their nice argument there is little information on the order of the semiregular automorphisms. In fact, their proof allows the existence of cubic vertex-transitive graphs admitting non-identity semiregular automorphisms of order only 2. However, empirical evidence suggests that cubic vertex-transitive graphs do have semiregular automorphisms of large order,as the

https://doi.org/10.1017/S0305004114000188 Published online by Cambridge University Press

number of vertices of the graph grows. To make this statement precise, Cameron, Sheehan and the author have proposed the following conjecture [**4**, conjecture 2].

CONJECTURE 1. There exists a function $f : \mathbb{N} \to \mathbb{N}$ with $\lim_{n\to\infty} f(n) = \infty$ such that, if Γ is a cubic vertex-transitive graph with n vertices, then Γ has a semiregular automorphism of order at least $f(n)$.

A short answer to this open problem is "no".

THEOREM 1·1. *There exists no function f satisfying Conjecture* 1.

However, much lies behind this laconic answer and, in fact, we prove that Conjecture 1 holds true for a large class of cubic vertex-transitive graphs. Let X be a group and let Y be an inverse-closed and identity-free subset of X. The *Cayley graph* $\mathrm{Cay}(X, Y)$ has vertex-set X and two vertices x and x' are adjacent if and only if $x(x')^{-1} \in Y$. We say that a graph Γ is a Cayley graph if $\Gamma \cong \mathrm{Cay}(X, Y)$, for some group X and some subset $Y \subseteq X$. Moreover, a graph Γ is said to be *arc-transitive* if $\mathrm{Aut}(\Gamma)$ acts transitively on the ordered pairs of adjacent vertices of Γ.

The *restricted Burnside problem* [**24**, section $1 \cdot 1$] asks whether there exists a function $g : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ such that, if G is a finite d-generated group of exponent e, then $|G| \leqslant g(d, e)$. In this paper, we use the positive solution of the restricted Burnside problem [**25**, **26**] to prove the following.

THEOREM 1·2. *There exists a function $f : \mathbb{N} \to \mathbb{N}$ with $\lim_{n\to\infty} f(n) = \infty$ such that, if Γ is a cubic Cayley or arc-transitive graph with n vertices, then Γ has a semiregular automorphism of order at least $f(n)$.*

Before concluding this introductory section and moving to the proof of Theorems 1·1 and 1·2 we show that Conjecture 1 is very much related to the restricted Burnside problem with $d = 3$. In fact, for some families of cubic graphs, Conjecture 1 is equivalent to the restricted Burnside problem (for the class of finite groups generated either by three involutions or by one involution and one non-involution).

Recall that a graph is called a *graphical regular representation* or *GRR* if its automorphism group acts regularly on its vertices. Now, if Γ is a GRR, then every element of $\mathrm{Aut}(\Gamma)$ is semiregular. In particular, Conjecture 1 restricted to a cubic GRR Γ asks whether the maximal element order of $\mathrm{Aut}(\Gamma)$ tends to infinity as the number of vertices of Γ tends to infinity. Clearly, as $\mathrm{Aut}(\Gamma)$ acts regularly on the vertices of Γ, we get that Γ has $|\mathrm{Aut}(\Gamma)|$ vertices. Moreover, a moment's thought gives that the maximal element order of $\mathrm{Aut}(\Gamma)$ tends to infinity if and only if the exponent of $\mathrm{Aut}(\Gamma)$ tends to infinity. Finally, as Γ is cubic, the group $\mathrm{Aut}(\Gamma)$ is generated either by three involutions or by one involution and one non-involution. This shows that this particular instance of Conjecture 1 is equivalent to the restricted Burnside problem with $d = 3$: in fact, the exponent of $\mathrm{Aut}(\Gamma)$ tends to infinity if and only if $|\mathrm{Aut}(\Gamma)|$ tends to infinity.

Now, [**20**, theorem $1 \cdot 2$] shows that the class of cubic GRRs is far from being sparse and indeed McKay and Praeger conjecture [**17**] that most cubic vertex-transitive graphs are GRRs. In particular, Conjecture 1 for cubic GRRs is a rather interesting and important case.

Observe that ultimately the proof of Theorem 1·2 relies on the Classification of the Finite Simple Groups. In fact, the Hall–Higman reduction [**10**] of the restricted Burnside problem to the case of prime-power exponent uses the Schreier conjecture. So, since our proof of Theorem 1·2 is inevitably dependent upon the CFSGs, we feel free to use such a powerful tool in other parts of our argument.

https://doi.org/10.1017/S0305004114000188 Published online by Cambridge University Press

Finally, we do not try to optimize the choice of the function f in Theorem 1·2 (which we believe grows rather slowly) and we prove only an "existence" result. For example, using the recent census of cubic vertex-transitive graphs [**19**], we see that there exists a cubic Cayley graph Γ with 1152 vertices and admitting semiregular automorphisms of order at most 6. For a rather more exotic example see Section 2.

We conclude this introductory section, by pointing out the following result that is needed in our proof of Theorem 1·2 and that might be of independent interest. (A graph Γ is said to be *G-vertex-transitive* if G is a subgroup of $\mathrm{Aut}(\Gamma)$ acting transitively on the vertex-set $V\Gamma$ of Γ.)

THEOREM 1·3. *There exists a function* $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ *with*

$$\lim_{n\to\infty} f(n, m) = \infty, \quad \text{for each } m \in \mathbb{N},$$

such that, if Γ *is a cubic* G*-vertex-transitive graph with* n *vertices and* N *is a minimal normal subgroup of* G *with* m *orbits on* $V\Gamma$*, then* G *contains a semiregular element of order at least* $f(n, m)$.

1·1. *Structure of the paper*

The structure of this paper is straightforward. In Section 2, we study a cubic graph related to the Burnside group $B(3, 6)$, this should highlight once again the relationship between Conjecture 1 and the restricted Burnside problem. In Section 3, we collect some basic results on cubic vertex-transitive graphs and on non-abelian simple groups. In Section 4, we first prove Theorem 1·3 and then Theorem 1·2. We prove Theorem 1·1 in Section 5.

2. *The group* $B(3, 6)$ *and one interesting example*

For positive integers d and e, the Burnside group $B(d, e)$ is the freest group on d generators with exponent e. From [**10**], we see that $B(3, 6)$ is actually finite and, in fact, $|B(3, 6)| = 2^{4375}3^{833}$. This gives that the largest group of exponent 6 and generated by an involution and by an element of order 6 is also finite. This group is denoted by $C(2, 6)$ in [**11**] and it is shown that $|C(2, 6)| = 2^4 \cdot 3^7 = 34992$. Moreover, a presentation for $C(2, 6)$ with two generators a and b, where $a^2 = b^6 = 1$, and sixteen relators is given in [**11**, section 5, p. 3633].

Using the computer algebra system `magma` [**1**], we have constructed the Cayley graph $\Gamma = \mathrm{Cay}(C(2, 6), \{a, b, b^{-1}\})$ and the automorphism group $\mathrm{Aut}(\Gamma)$. In particular, we have checked that $|\mathrm{Aut}(\Gamma)| = 2 \cdot |C(2, 6)|$ and hence $\mathrm{Aut}(\Gamma)$ consists merely of the right regular translations by $C(2, 6)$ and of the automorphism φ of $C(2, 6)$ fixing a and mapping b to b^{-1}. With another computation we see that $ab\varphi$ has order 12 and is semiregular. So, the largest order of a semiregular element of $\mathrm{Aut}(\Gamma)$ is 12. This gives that in Theorem 1·2 we have $f(34992) \leqslant 12$. So, although Theorem 1·2 shows that $\lim_{n\to\infty} f(n) = \infty$, we see that the growth rate is conceivably rather slow.

We are confident that the Burnside group $B(3, 6)$ is a rich source of other exotic examples of this form. However, because of the computational complexity, we did not try to construct larger cubic Cayley graphs.

Finally, we stress again that since we only prove the existence of a function f satisfying Theorem 1·2, we do not try (by any means) to obtain the best bounds in the arguments in the next sections.

https://doi.org/10.1017/S0305004114000188 Published online by Cambridge University Press

3. *Some basic results*

A graph Γ is said to be *G-arc-transitive* if G is a subgroup of $\mathrm{Aut}(\Gamma)$ acting transitively on the arcs of Γ, that is, on the ordered pairs of adjacent vertices of Γ.

Given a vertex α of Γ, we let G_α be the vertex-stabiliser of α and we let $G_\alpha^{[1]}$ be the pointwise stabiliser of the neighbourhood Γ_α of α. In particular, $G_\alpha/G_\alpha^{[1]}$ is isomorphic to the permutation group $G_\alpha^{\Gamma_\alpha}$ induced by the action of G_α on Γ_α. Moreover, for a subgroup H of G we write α^H for the H-orbit containing α, that is, $\alpha^H = \{\alpha^h \mid h \in H\}$. Finally, given another vertex β of Γ, we denote by $d(\alpha, \beta)$ the length of a shortest path from α to β.

We start our analysis with some preliminary remarks.

LEMMA 3·1. *Let Γ be a connected cubic G-vertex-transitive graph and let α be a vertex of Γ. Then $G_\alpha^{[1]}$ is a 2-group. Moreover, either G_α is a 2-group, or Γ is G-arc-transitive and $|G_\alpha| = 3 \cdot 2^s$, for some $s \geqslant 0$. In particular, every element of G of order coprime to 2 and 3 is a semiregular element.*

Proof. We start by showing that $G_\alpha^{[1]}$ is a 2-group. We argue by contradiction and we let g be an element of $G_\alpha^{[1]}$ of prime order $p > 2$. Let γ be a vertex of Γ at minimal distance from α with $\gamma^g \neq \gamma$. Write $d = d(\alpha, \gamma)$. As g fixes pointwise Γ_α, we must have $d \geqslant 2$. Let $\alpha = \alpha_0, \ldots, \alpha_{d-1}, \alpha_d = \gamma$ be a path of length d from α to γ in Γ. By minimality, $\alpha_{d-1}^g = \alpha_{d-1}$ and hence g induces a permutation of the neighbourhood $\Gamma_{\alpha_{d-1}}$ fixing α_{d-2}. Since Γ is cubic and since $|g| > 2$, we see that g fixes pointwise $\Gamma_{\alpha_{d-1}}$. However, this contradicts $\gamma^g \neq \gamma$.

Now, $G_\alpha/G_\alpha^{[1]}$ is isomorphic to a subgroup of $\mathrm{Sym}(\Gamma_\alpha)$. As $|\mathrm{Sym}(\Gamma_\alpha)| = 6$, the rest of the proof follows easily.

LEMMA 3·2. *Let Γ be a connected cubic G-vertex-transitive graph. Then G contains a 3-generated subgroup transitive on $V\Gamma$. Moreover, if Γ is also G-arc-transitive, then G contains a 6-generated arc-transitive subgroup.*

Proof. We prove the two parts of this lemma simultaneously. Fix α a vertex of Γ. For each $\beta \in \Gamma_\alpha$, choose $g_\beta \in G$ with $\alpha^{g_\beta} = \beta$. Moreover, if G is arc-transitive, then fix $\beta_0 \in \Gamma_\alpha$ and, for each $\beta \in \Gamma_\alpha$, choose $x_\beta \in G_\alpha$ with $\beta_0^{x_\beta} = \beta$. Write $H = \langle g_\beta \mid \beta \in \Gamma_\alpha \rangle$ and, if G is arc-transitive, write also $K = \langle g_\beta, x_\beta \mid \beta \in \Gamma_\alpha \rangle$. Clearly, H is 3-generated and K is 6-generated .

Write $\Delta = \alpha^H$. Let $\delta \in \Delta$. So, $\delta = \alpha^h$, for some $h \in H$. As $\Gamma_\alpha \subseteq \Delta$, we get $\Gamma_\delta = \Gamma_{\alpha^h} = \Gamma_\alpha^h \subseteq \Delta^h = \Delta$. Since δ is an arbitrary element of Δ, this shows that the subgraph induced by Γ on Δ is cubic. As Γ is connected, we must have $\Delta = V\Gamma$ and hence H is transitive on $V\Gamma$. By construction K_α is transitive on Γ_α and hence K is arc-transitive.

Using a celebrated theorem of Tutte [**23**] one can replace 6 by 3 in the statement of Lemma 3·2. We conclude this section with three lemmas on non-abelian simple groups.

LEMMA 3·3. *There exists a function $\nu : \mathbb{N} \to \mathbb{N}$ with $\lim_{n\to\infty} \nu(n) = \infty$ such that, if T is a non-abelian simple group of order n and R is a $\{2, 3\}$-subgroup of T, then $|T : R| \geqslant \nu(n)$.*

Proof. We argue by contradiction and we assume that there exists no such function ν. This means that there exist.

https://doi.org/10.1017/S0305004114000188 Published online by Cambridge University Press

(i) a positive integer c;
(ii) an infinite family of non-abelian simple groups $\{T_m\}_{m\in\mathbb{N}}$; and
(iii) a family $\{R_m\}_{m\in\mathbb{N}}$ of $\{2, 3\}$-groups;
with $|T_m| < |T_{m+1}|$, $R_m \leqslant T_m$ and $|T_m : R_m| \leqslant c$, for every $m \in \mathbb{N}$.

Observe that by the Burnside's $p^\alpha q^\beta$-theorem, R_m is a proper subgroup of T_m. Let K_m be the core of R_m in T_m. Since T_m is a non-abelian simple group, we have $K_m = 1$. Clearly, $|T_m| = |T_m : K_m| \leqslant |T_m : R_m|! \leqslant c!$. However this contradicts $\lim_{m\to\infty} |T_m| = \infty$.

Given two integers x and f with $x \geqslant 2$ and $f \geqslant 1$, a prime r is said to be a *primitive prime divisor* for $x^f - 1$ if r divides $x^f - 1$ and if r is coprime to $x^s - 1$, for each $1 \leqslant s < f$.

LEMMA 3·4. *Let x and f be integers with $x \geqslant 2$ and $f \geqslant 1$. Then $x^f - 1$ has no primitive prime divisors if and only if either $(x, f) = (2, 6)$ or $(x, f) = (2^y - 1, 2)$ for some $y \in \mathbb{N}$. If r is a primitive prime divisor for $x^f - 1$, then $r \geqslant f + 1$.*

Proof. The first part follows from [**27**]. Now, let r be a primitive prime divisor for $x^f - 1$. A computation shows that r divides $x^m - 1$ if and only if m is a multiple of f. As r divides $x^{r-1} - 1$ by Fermat's little theorem, we deduce that f divides $r - 1$. Thus $r - 1 \geqslant f$ and $r \geqslant f + 1$.

For the proof of the following lemma we recall the definition of Lie rank of a simple group of Lie type G, here we follow [**5**, sections 13·1, 13·2]. Now, G is a group with a (B, N)-pair and the Weyl group W of this (B, N)-pair is a reflection group generated by a set of simple reflections. The number of simple reflections is defined to be the Lie rank of G. So, for instance, $\mathrm{PSU}_3(q)$ has Lie rank 1. (The order of the Weyl group W for untwisted groups is given in [**5**, section 3·6] and for twisted groups is given in [**5**, section 13·3].)

LEMMA 3·5. *There exists a function $\mu : \mathbb{N} \to \mathbb{N}$ with $\lim_{n\to\infty} \mu(n) = \infty$ such that, if T is a non-abelian simple group of order n, then T contains an element t of order coprime to 2 and 3 and with $|t| \geqslant \mu(n)$.*

Proof. We argue by contradiction and we assume that there exists no such function μ. This means that there exist a constant c and an infinite family of non-abelian simple groups $\{T_m\}_{m\in\mathbb{N}}$ such that, $|T_m| < |T_{m+1}|$ and every element of order coprime to 2 and 3 in T_m has order at most c, for every $m \in \mathbb{N}$.

Suppose that $\{T_m\}_{m\in\mathbb{N}}$ contains an infinite subsequence $\{T_{m_s}\}_{s\in\mathbb{N}}$ such that, for every $s \in \mathbb{N}$, the group T_{m_s} is isomorphic either to an alternating group of degree d_s or to a group of Lie type of Lie rank d_s, and $\lim_{s\to\infty} d_s = \infty$.

Let $s_0 \in \mathbb{N}$ with $d_s \geqslant 5$, for every $s \geqslant s_0$. Now, we see that $d_s!/2$ divides the order of T_{m_s} (if $T_{m_s} \cong \mathrm{Alt}(d_s)$, then this is clear, and if T_{m_s} is a group of Lie type of Lie rank d_s, then $d_s!/2$ divides the order of the Weyl group of T_{m_s} and hence the order of T_{m_s}). From Bertrand's postulate, there exists a prime p_s with $d_s/2 < p_s \leqslant d_s$. Observe that we may choose $p_s \notin \{2, 3\}$ for every $s \geqslant s_0$. In particular, for every $s \geqslant s_0$, the group T_{m_s} contains an element of order p_s coprime to 2 and 3. As $\lim_{s\to\infty} p_s = \lim_{s\to\infty} d_s = \infty$, we contradict our choice of $\{T_m\}_{m\in\mathbb{N}}$. This shows that there exists a constant r such that, for every $m \in \mathbb{N}$, the group T_m is either a sporadic simple group, or an alternating group of degree $\leqslant r$, or a group of Lie type of Lie rank $\leqslant r$. In particular, since there are only finitely many sporadic simple groups and alternating groups in the family $\{T_m\}_{m\in\mathbb{N}}$, by replacing $\{T_m\}_{m\in\mathbb{N}}$ with a proper infinite subfamily if necessary, we may assume that every element in $\{T_m\}_{m\in\mathbb{N}}$ is a group of Lie type of Lie rank $\leqslant r$. Moreover, since there is only a finite number of possible ranks for

https://doi.org/10.1017/S0305004114000188 Published online by Cambridge University Press

the groups in $\{T_m\}_{m\in\mathbb{N}}$, there exists a positive integer l such that, by replacing $\{T_m\}_{m\in\mathbb{N}}$ with a proper infinite subfamily if necessary, every element in $\{T_m\}_{m\in\mathbb{N}}$ is a group of Lie type of Lie rank l.

Suppose that $\{T_m\}_{m\in\mathbb{N}}$ contains a subsequence $\{T_{m_s}\}_{s\in\mathbb{N}}$ such that, for every $s \in \mathbb{N}$, the group T_{m_s} is a group of Lie type in characteristic p_s, and $\lim_{s\to\infty} p_s = \infty$. Since T_{m_s} contains an element of order p_s, we contradict our choice of $\{T_m\}_{m\in\mathbb{N}}$. This shows that there exists a constant r such that, for every $m \in \mathbb{N}$, the group T_m is a group of Lie type in characteristic p with $p \leqslant r$. Since there are only finitely many primes $\leqslant r$, arguing as above, we may assume that every element in $\{T_m\}_{m\in\mathbb{N}}$ is a group of Lie type in characteristic p, for a fixed prime p.

Observe that there is only a finite number of Lie types. So, as usual, we may assume that every element in $\{T_m\}_{m\in\mathbb{N}}$ is of the same Lie type.

Summing up, for every $m \in \mathbb{N}$, we have $T_m = L_l(p^{f_m})$, for some $f_m \in \mathbb{N}$ (where we denote by $L_l(p^f)$ the group of Lie type L, of Lie rank l, in characteristic p and defined over the field p^f). Let $m_0 \in \mathbb{N}$ such that $f_m \geqslant 7$, for every $m \geqslant m_0$.

For $m \in \mathbb{N}$, let e_m be the order of the Schur multiplier of T_m (for each group of Lie type the order of the Schur multiplier can be found in [**6**, table 6, page xvi]). Observe that e_m is bounded above by a function of l. Now, from [**6**, table 6, page xvi], we see that $(p^{f_m}-1)/e_m$ divides $|T_m|$. For $m \geqslant m_0$, by Lemma 3·4 there exists a primitive prime divisor r_m for $p^{f_m}-1$ and, moreover, $r_m \geqslant f_m + 1$. As T_m contains an element of order r_m and as $\lim_{m\to\infty} r_m = \lim_{m\to\infty} f_m = \infty$, we obtain a final contradiction.

Lemma 3·6 is inspired by [**21**, lemma 14] and part of its proof is taken directly from [**21**, section 3] (unfortunately we were unable to readily deduce the statement of Lemma 3·6 from [**21**, lemma 14]).

LEMMA 3·6. *Let T be a non-abelian simple group, let $\ell \geqslant 1$, let ℓ' be a divisor of ℓ, let $S_1, \ldots, S_{\ell'}$ be proper subgroups of T and let M be an m-generated subgroup of T^ℓ. Suppose that*

$$T^\ell = M\left((S_1)^{\frac{\ell}{\ell'}} \times \cdots \times (S_{\ell'})^{\frac{\ell}{\ell'}}\right).$$

Then $(\ell/\ell') \leqslant |T|^m$.

Proof. For $j \in \{1, \ldots, \ell\}$, denote by T_j the jth direct factor of T^ℓ. Moreover, for each $i \in \{1, \ldots, \ell'\}$, write

$$N_i = T_{\frac{(i-1)\ell}{\ell'}+1} \times T_{\frac{(i-1)\ell}{\ell'}+2} \times \cdots \times T_{\frac{i\ell}{\ell'}}.$$

Clearly, $N_i \cong T^{\frac{\ell}{\ell'}}$ and $T^\ell = N_1 \times N_2 \times \cdots \times N_{\ell'}$. For $i \in \{1, \ldots, \ell'\}$, denote by $\pi_i : T^\ell \to N_i$ the natural projection and write $M_i = \pi_i(M)$. Clearly, M_i is m-generated and

$$T^{\frac{\ell}{\ell'}} = M_i\, S_i^{\frac{\ell}{\ell'}}. \tag{3·1}$$

This shows that in the proof of this lemma we may assume that $\ell' = 1$.

We argue by contradiction and we suppose that $\ell > |T|^m$. Let $g_1, \ldots, g_m$ be m generators of M. For each $i \in \{1, \ldots, m\}$, we have $g_i = (t_{i,1}, \ldots, t_{i,\ell})$, for some $t_{i,j} \in T$. Since the entries $\{t_{1,j}\}_j$ of the element g_1 are in T and since T has $|T|$ elements, the pigeonhole principle gives that there exist at least $\ell/|T|$ coordinates on which g_1 is constant. In other words, there exists $X_1 \subseteq \{1, \ldots, \ell\}$ with $|X_1| \geqslant \ell/|T|$ and with $t_{1,j} = t_{1,j'}$, for each $j, j' \in X_1$. Arguing in a similar manner with the element g_2 and with the coordinates

https://doi.org/10.1017/S0305004114000188 Published online by Cambridge University Press

labelled from the elements of X_1, we obtain that there exists $X_2 \subseteq X_1$ with $|X_2| \geqslant |X_1|/|T|$ and with $t_{2,j} = t_{2,j'}$, for each $j, j' \in X_2$. In particular, $|X_2| \geqslant \ell/|T|^2$. Now, an inductive argument gives that there exists a subset $X_m \subseteq \{1, \ldots, \ell\}$ with $|X_m| \geqslant \ell/|T|^m$ and with $t_{i,j} = t_{i,j'}$, for every $i \in \{1, \ldots, m\}$ and for every $j, j' \in X_m$.

As we are assuming that $\ell > |T|^m$, we obtain $|X_m| \geqslant 2$. Relabelling the index set $\{1, \ldots, \ell\}$ if necessary, we may assume that $1, 2 \in X_m$. Now, consider $\pi : N \to T^2$ the natural projection onto the first two coordinates and consider the diagonal subgroup $D = \{(t, t) \in T^2 \mid t \in T\}$ of T^2. By construction we have $\pi(M) \leqslant D$. So, by applying π on both sides of (3·1), we obtain

$$T^2 = \pi(M)(S_1 \times S_1) = D(S_1 \times S_1). \tag{3·2}$$

Let t be an element of $T \setminus S_1$. From (3·2), we have $(1, t) = (a, a)(b, c)$ for some $a \in T$ and $b, c \in S_1$. This yields $a = b^{-1} \in S_1$ and $t = ac \in S_1$, a contradiction. This contradiction arose from the assumption $\ell > |T|^m$. Hence $\ell \leqslant |T|^m$ and the lemma is proved.

4. *Proof of Theorems* 1·2 *and* 1·3

Proof of Theorem 1·3. Without loss of generality, we may assume our graphs to be connected. So, let Γ be a connected cubic G-vertex-transitive graph with n vertices and let N be a minimal normal subgroup of G with m orbits on $V\Gamma$.

Let $\mathcal{O}_1, \ldots, \mathcal{O}_m$ be the orbits of N on $V\Gamma$. We show that Γ contains m vertices $\beta_1, \ldots, \beta_m$, with $\beta_i \in \mathcal{O}_i$ for every i, such that the subgraph induced by Γ on $\{\beta_1, \ldots, \beta_m\}$ is connected. Let X be a subset of vertices of Γ of maximal size with the properties:

(i) $|X \cap \mathcal{O}_i| \leqslant 1$ for every $i \in \{1, \ldots, m\}$; and

(ii) the subgraph induced by Γ on X is connected.

If $|X| = m$, then the claim is proved. Suppose then that $|X| = l < m$. Without loss of generality we may assume that $X = \{\beta_1, \ldots, \beta_l\}$. Let γ be a vertex in $\mathcal{O}_{l+1}$. Since Γ is connected, there exists a path $\beta_1 = \gamma_1, \ldots, \gamma_u = \gamma$ in Γ from β_1 to γ. Let i be minimal such that

$$\gamma_i \notin \bigcup_{j=1}^{l} \mathcal{O}_j.$$

In particular, $i \geqslant 2$ and $\gamma_{i-1} \in \mathcal{O}_k$ for some $k \leqslant l$. Since N is transitive on $\mathcal{O}_k$, there exists $g \in N$ such that $\beta_k = \gamma_{i-1}^g$. So, γ_i^g is adjacent to β_k and $\gamma_i^g \notin \bigcup_{j=1}^{l} \mathcal{O}_j$. Set $X' = X \cup \{\gamma_i^g\}$. By construction, $X \subset X'$, the subgraph induced by Γ on X' is connected and X' contains at most one vertex from each $\mathcal{O}_i$. This contradicts the maximality of X. Thus $|X| = m$ and the claim is proved.

Fix $\beta_1, \ldots, \beta_m$, with $\beta_i \in \mathcal{O}_i$ for every $i \in \{1, \ldots, m\}$, such that the subgraph induced by Γ on $\{\beta_1, \ldots, \beta_m\}$ is connected.

For each $i \in \{1, \ldots, m\}$, write $\Gamma_{\beta_i} = \{\beta_{i,1}, \beta_{i,2}, \beta_{i,3}\}$. Now, for each $i \in \{1, \ldots, m\}$ and $j \in \{1, 2, 3\}$, there exists a unique $k_{i,j} \in \{1, \ldots, m\}$ with $\beta_{i,j} \in \mathcal{O}_{k_{i,j}}$. So, choose $g_{i,j} \in N$ with $\beta_{i,j}^{g_{i,j}} = \beta_{k_{i,j}}$ and set

$$M = \langle g_{i,j} \mid i \in \{1, \ldots, m\}, j \in \{1, 2, 3\} \rangle.$$

Observe that M is $3m$-generated.

We claim that the orbits of M on $V\Gamma$ are exactly $\mathcal{O}_1, \ldots, \mathcal{O}_m$. Write $\Delta = \beta_1^M \cup \cdots \cup \beta_m^M$. Observe that from the definition of M, we have $\Gamma_{\beta_i} \subseteq \Delta$, for each $i \in \{1, \ldots, m\}$. From this it follows that $\Gamma_\delta \subseteq \Delta$, for each $\delta \in \Delta$. Now, recalling that the subgraph induced by Γ

https://doi.org/10.1017/S0305004114000188 Published online by Cambridge University Press

on $\{\beta_1, \dots, \beta_m\}$ is connected, it follows from a connectedness argument that the subgraph induced by Γ on Δ is cubic. As Γ is itself cubic, we must have $V\Gamma = \Delta$, from which our claim follows. We obtain

$$N = MN_\gamma, \quad \text{for every } \gamma \in V\Gamma. \tag{4·1}$$

As N is a minimal normal subgroup of G, we have $N = T_1 \times \cdots \times T_\ell$, where $\ell \geqslant 1$ and where $T_1, \dots, T_\ell$ are pairwise isomorphic simple groups (here T_i is possibly abelian).

Suppose that N is soluble, that is, T_i is cyclic of prime order p, for some prime p. Assume that $N_\gamma = 1$, for $\gamma \in V\Gamma$. Thus $M = N$ and hence N is $3m$-generated. Clearly, this gives $\ell \leqslant 3m$ and hence $|N| \leqslant p^{3m}$. In particular, $n = |V\Gamma| \leqslant mp^{3m}$. As the elements of N are semiregular, we see that G contains a semiregular element of order p. Finally, since $p \geqslant (n/m)^{\frac{1}{3m}}$ and since $\lim_{n\to\infty}(n/m)^{\frac{1}{3m}} = \infty$, the lemma follows.

Assume that $N_\gamma \neq 1$. So, $p \in \{2, 3\}$ by Lemma 3·1. Now $|N : N_\gamma| \leqslant |M| \leqslant p^{3m} \leqslant 3^{3m}$. In particular, Γ has order at most $m \cdot 3^{3m}$. As the number of vertices of Γ is bounded above by a function of m, there is nothing to prove in this case.

Suppose that N is not soluble, that is, T_i is a non-abelian simple group, for each $i \in \{1, \dots, m\}$. Denote by $\pi_i : N \to T_i$ the natural projection onto the ith direct factor of N. Denote by K the kernel of the action of G on N-orbits, that is, $K = \bigcap_{\alpha\in V\Gamma}(G_\alpha N)$. In particular,

$$K = K_\gamma N, \quad \text{for every } \gamma \in V\Gamma.$$

As N has m orbits on $V\Gamma$, we have $|G : K| \leqslant m!$.

Since N is a minimal normal subgroup of G, the group G acts transitively by conjugation on the set of the simple direct factors $\{T_1, \dots, T_\ell\}$ of N. Moreover, as $K \trianglelefteq G$ and as $|G : K| \leqslant m!$, we obtain that K has at most $m!$ orbits on $\{T_1, \dots, T_\ell\}$. Denote by ℓ' the number of K-orbits on $\{T_1, \dots, T_\ell\}$. So, $\ell' \leqslant m!$. Moreover, observe that as $K = K_\gamma N$ (for $\gamma \in V\Gamma$) and as N acts trivially by conjugation on $\{T_1, \dots, T_\ell\}$, we have that K and K_γ have exactly the same orbits on $\{T_1, \dots, T_\ell\}$.

Now, fix $\alpha \in V\Gamma$ and write $S_i = \pi_i(N_\alpha)$. Since N_α is a $\{2, 3\}$-group, so is S_i. From the Burnside's $p^\alpha q^\beta$-theorem, we have $S_i \neq T$ and hence S_i is a proper subgroup of T. Clearly, $N_\alpha \leqslant S_1 \times \cdots \times S_\ell$. Since $N_\alpha \trianglelefteq K_\alpha$, we see that K_α acts by conjugation on the set $\{S_1, \dots, S_\ell\}$. Moreover, as K_α has ℓ' orbits on $\{T_1, \dots, T_\ell\}$ each of size ℓ/ℓ', we get that K_α has exactly ℓ' orbits on $\{S_1, \dots, S_\ell\}$ each of size ℓ/ℓ'. Let $S_{i_1}, \dots, S_{i_{\ell'}}$ be representatives for the orbits of K_α on $\{S_1, \dots, S_\ell\}$. Thus we have

$$S_1 \times \cdots \times S_\ell \cong (S_{i_1})^{\frac{\ell}{\ell'}} \times \cdots \times (S_{i_{\ell'}})^{\frac{\ell}{\ell'}}.$$

Observe further that as $N \cong T_1^\ell$ and $\mathrm{Aut}(N) \cong \mathrm{Aut}(T_1) \operatorname{wr} \mathrm{Sym}(\ell)$, the above isomorphism is induced by an automorphism η of the whole of N.

From (4·1), we have

$$N = N^\eta = (MN_\alpha)^\eta = M^\eta N_\alpha^\eta \leqslant M^\eta \left((S_{i_1})^{\frac{\ell}{\ell'}} \times \cdots \times (S_{i_{\ell'}})^{\frac{\ell}{\ell'}}\right) = N$$

and we are in the position to apply Lemma 3·6 (with M replaced by M^η, m replaced by $3m$, and $S_1, \dots, S_{\ell'}$ replaced by $S_{i_1}, \dots, S_{i_{\ell'}}$). We obtain $(\ell/\ell') \leqslant |T|^{3m}$. Recalling that $\ell' \leqslant m!$, we get $\ell \leqslant |T|^{3m}m!$

Observe that each N-orbit has size at most $|N| = |T|^\ell$ and at least $|N : R^\ell| = |T : R|^\ell$, where R is a $\{2, 3\}$-subgroup of maximal size of T. By Lemma 3·3, we get

$$m\nu(|T|)^\ell \leqslant n \leqslant m|T|^\ell.$$

https://doi.org/10.1017/S0305004114000188 Published online by Cambridge University Press

As ℓ is bounded above by a function of $|T|$ and m only, we see that the order of Γ is trapped between two functions depending only on $|T|$ and m. So, the proof follows from Lemma 3·5.

In view of Theorem 1·3, for proving Theorem 1·2 it suffices to remove the dependency on m in the function f.

We now recall the important definition of a normal quotient of a graph. Let Γ be a G-vertex-transitive graph and let N be a normal subgroup of G. Let α^N denote the N-orbit containing $\alpha \in V\Gamma$. Then the *normal quotient* Γ/N is the graph whose vertices are the N-orbits on $V\Gamma$, with an edge between distinct vertices α^N and β^N if and only if there is an edge $\{\alpha', \beta'\}$ of Γ for some $\alpha' \in \alpha^N$ and some $\beta' \in \beta^N$. Observe that the kernel of the action of G on N-orbits is $K = \bigcap_{\alpha \in V\Gamma} G_\alpha N$. Moreover, $\Gamma/K = \Gamma/N$. The group G/K acts faithfully and transitively on the graph Γ/N with vertex-stabilisers $G_\alpha K/K$, for $\alpha \in V\Gamma$. Clearly, if Γ is G-arc-transitive, then Γ/N is (G/K)-arc-transitive.

Proof of Theorem 1·2. We argue by contradiction and we assume this theorem to be false. This means that there exist a constant c_1 and an infinite family of cubic vertex-transitive graphs $\{\Gamma_m\}_{m\in\mathbb{N}}$ such that:

(i) Γ_m is either a Cayley or an arc-transitive graph;
(ii) $|V\Gamma_m| < |V\Gamma_{m+1}|$; and
(iii) every semiregular element of $\mathrm{Aut}(\Gamma_m)$ has order at most c_1,

for every $m \in \mathbb{N}$.

Observe that if Γ_m is disconnected, then its connected components are pairwise isomorphic. Thus, from (iii), Γ_m has at most c_1 connected components. In particular, replacing each Γ_m by one of its connected components Γ'_m we obtain an infinite sequence of cubic vertex-transitive graphs $\{\Gamma'_m\}_{m\in\mathbb{N}}$ satisfying (i) and (iii). Next, replacing $\{\Gamma'_m\}_{m\in\mathbb{N}}$ with a proper infinite subfamily if necessary, we may assume that $|V\Gamma'_m| < |V\Gamma'_{m+1}|$, for every $m \in \mathbb{N}$. This argument shows that we may assume that each Γ_m is connected.

Suppose that there exists an infinite subsequence $\{\Gamma_{m_s}\}_{s\in\mathbb{N}}$ of Cayley graphs. For each $s \in \mathbb{N}$, let X_s be a finite group and let Y_s be a finite subset of X_s with $\Gamma_{m_s} = \mathrm{Cay}(X_s, Y_s)$. Now, every element of X_s has order at most c_1 and hence X_s has exponent at most $c_1!$. By Lemma 3·2, X_s is 3-generated and hence the positive solution of the restricted Burnside problem gives a constant c_2 with $|X_s| \leqslant c_2$, for every $s \in \mathbb{N}$. However, this contradicts the infinitude of $\{\Gamma_{m_s}\}_{s\in\mathbb{N}}$. So, by replacing $\{\Gamma_m\}_{m\in\mathbb{N}}$ with a proper infinite subfamily if necessary, we may assume that Γ_m is arc-transitive, for every $m \in \mathbb{N}$.

For $m \in \mathbb{N}$, write $A_m = \mathrm{Aut}(\Gamma_m)$. By Lemma 3·2, the group A_m contains a 6-generated arc-transitive subgroup G_m. Let N_m be a maximal (with respect to inclusion) normal subgroup of G_m with Γ_m/N_m cubic. Define $\Delta_m = \Gamma_m/N_m$ and $H_m = G_m/N_m$. Observe that by the maximality of N_m, the group H_m acts faithfully on $V\Delta_m$ and hence Δ_m is a cubic H_m-arc-transitive graph. Moreover, as Γ_m/N_m is cubic, it follows from an easy connectedness argument that the normal subgroup N_m acts semiregularly on $V\Gamma_m$.

Suppose that there exists a constant c_2 with $|V\Delta_m| < c_2$, for every $m \in \mathbb{N}$. Since G_m is 6-generated and since $|G_m : N_m| = |H_m| \leqslant |\mathrm{Sym}(V\Delta_m)| \leqslant c_2!$, we see from the Reidemeister–Schreier theorem [**22**, 6·1·8 (ii)] that N_m is $(5c_2! + 1)$-generated. As every semiregular element of G_m has order at most c_1 and as N_m acts semiregularly on $V\Gamma$, we see that N_m has exponent dividing c_1. In particular, the number of generators and the exponent of N_m are both bounded above by constants. So, from the positive solution of the restricted Burnside problem, we see that there exists a constant c_3 with $|N_m| \leqslant c_3$. For every m in

https://doi.org/10.1017/S0305004114000188 Published online by Cambridge University Press

$\mathbb{N}$, we have $|V\Gamma_m| = |V\Delta_m||N_m| \leqslant c_2c_3$, a contradiction. This shows that there exists a subsequence $\{m_s\}_{s\in\mathbb{N}}$ with $|V\Delta_{m_s}| < |V\Delta_{m_{s+1}}|$, for every $s \in \mathbb{N}$.

For each $s \in \mathbb{N}$, let M_{m_s}/N_{m_s} be a minimal normal subgroup of G_{m_s}/N_{m_s}. Write $U_{m_s} = M_{m_s}/N_{m_s}$. Now, the maximality of N_{m_s} yields that

$$\Gamma_{m_s}/M_{m_s} \cong \Delta_{m_s}/U_{m_s}$$

is not cubic.

We claim that U_{m_s} has at most two orbits on the vertices of Δ_{m_s}. Let α be a vertex of Δ_{m_s} and let β and γ be distinct neighbours of α. Since Δ_{m_s} is H_{m_s}-arc-transitive, there exists $h \in (H_{m_s})_\alpha$ with $\beta^h = \gamma$ and, since $U_{m_s} \trianglelefteq H_{m_s}$, we have $(\beta^{U_{m_s}})^h = \gamma^{U_{m_s}}$. This yields that $\beta^{U_{m_s}}$ and $\gamma^{U_{m_s}}$ contain the same number of neighbours of α. As Δ_{m_s} is cubic, we get that $\beta^{U_{m_s}}$ and $\gamma^{U_{m_s}}$ both contain a unique neighbour of α (indeed β and γ, respectively). However this contradicts the fact that Δ_{m_s}/U_{m_s} is not cubic. This gives that the neighbourhood of α is contained in a U_{m_s}-orbit. Now a connectedness argument yields that U_{m_s} has at most two orbits on $V\Delta_{m_s}$.

By Theorem 1·3, H_{m_s} contains a semiregular element $g_{m_s}N_{m_s}$ of order $\geqslant f(|V\Delta_{m_s}|, 2)$. Observe that g_{m_s} acts semiregularly on $V\Gamma_{m_s}$ because N_{m_s} acts semiregularly on $V\Gamma_{m_s}$. Thus G_{m_s} contains a semiregular element of order $\geqslant f(|V\Delta_{m_s}|, 2)$. As $\lim_s |V\Delta_{m_s}| = \infty$, for s sufficiently large G_{m_s} contains a semiregular element of order $> c_1$, a contradiction. This finally proves the theorem.

5. *Proof of Theorem* 1·1

Let $m \geqslant 1$ be an integer. We denote by $\mathbb{F}_3$ the field with 3 elements and we let J be the $(2^m \times 2^m)$-matrix with coefficients in $\mathbb{F}_3$ defined by

$$J_{i,j} = \begin{cases} (-1)^{i-j} & \text{if } i > j, \\ -(-1)^{j-i} & \text{if } j > i, \\ 0 & \text{if } i = j. \end{cases} \tag{5·1}$$

Clearly, the matrix J is antisymmetric, that is, $J_{i,j} = -J_{j,i}$ for every $i, j \in \{1, \dots, 2^m\}$.

We show that J is non-degenerate by performing Gaussian elimination. Keeping the first row of J and, for each $i \in \{2, \dots, 2^m\}$, replacing the ith row with the sum of the $(i-1)$th and of the ith row of J, we obtain the matrix

$$J' = \begin{pmatrix} 0 & 1 & -1 & 1 & -1 & 1 & & \cdots & 1 \\ -1 & 1 & 0 & 0 & 0 & 0 & & \cdots & 0 \\ 0 & -1 & 1 & 0 & 0 & 0 & & \cdots & 0 \\ 0 & 0 & -1 & 1 & 0 & 0 & & \cdots & 0 \\ & & & & & & & & \\ & & & & \cdots & 0 & -1 & 1 & 0 \\ & & & & & \cdots & 0 & -1 & 1 \end{pmatrix}.$$

Observe that the last $2^m - 1$ rows of J' are linearly independent. Moreover, the entries in the first row of J' add up to 1, whilst the entries in the other rows of J' add up to 0. Thus J' is non-degenerate and so is J.

Since J is antisymmetric and non-degenerate, J determines a non-degenerate symplectic form on the 2^m-dimensional vector space $\mathbb{F}_3^{2^m}$. We use this bilinear form to construct an extraspecial 3-group.

https://doi.org/10.1017/S0305004114000188 Published online by Cambridge University Press

Let V be the group given by the presentation

$$V = \big\langle v_1, \dots, v_{2^m}, z \mid v_i^3 = z^3 = [v_i, z] = 1, \quad [v_i, v_j] = z^{J_{i,j}}, \text{ for every } i, j \in \{1, \dots, 2^m\}\big\rangle. \tag{5·2}$$

Observe that V is an extraspecial 3-group of exponent 3 and of order 3^{2^m+1}.

Let $a : \{v_1, \dots, v_{2^m}, z\} \to V$ and $b : \{v_1, \dots, v_{2^m}, z\} \to V$ be the maps defined by

$$v_i \longmapsto v_i^a = \begin{cases} v_{i+1} & \text{if } i \neq 2^m, \\ v_1^{-1} & \text{if } i = 2^m, \end{cases} \quad \text{and} \quad z \longmapsto z^a = z, \tag{5·3}$$

$$v_i \longmapsto v_i^b = \begin{cases} v_{2^m-i+2} & \text{if } i \neq 1, \\ v_1^{-1} & \text{if } i = 1, \end{cases} \quad \text{and} \quad z \longmapsto z^b = z^{-1}. \tag{5·4}$$

We show that a and b preserve the defining relations (5·2) of V and hence they naturally extend to two automorphisms of V, which we will still denote by a and b.

Since both a and b map z to $z^{\pm 1}$ and v_i to an element of the form $v_j^{\pm 1}$, we see that

$$(v_i^a)^3 = (v_i^b)^3 = (z^a)^3 = (z^b)^3 = \big[v_i^a, z^a\big] = \big[v_i^b, z^b\big] = \big[v_i^a, v_i^a\big] = \big[v_i^b, v_i^b\big] = 1,$$

for every $i \in \{1, \dots, 2^m\}$. It remains to show that $[v_i^a, v_j^a] = (z^a)^{J_{i,j}}$ and $[v_i^b, v_j^b] = (z^b)^{J_{i,j}}$, for every two distinct elements $i, j \in \{1, \dots, 2^m\}$. Observe that, as the commutator satisfies the identity $[x, y] = [y, x]^{-1}$, we may assume that $i > j$. Furthermore, as V is a nilpotent group of class 2, we have $[x, y^{-1}] = [x^{-1}, y] = [x, y]^{-1}$, for every $x, y \in V$.

We start by dealing with a. If $i \neq 2^m$, then using (5·1) and (5·3) we obtain

$$\big[v_i^a, v_j^a\big] = [v_{i+1}, v_{j+1}] = z^{J_{i+1,j+1}} = z^{(-1)^{(i+1)-(j+1)}} = z^{(-1)^{i-j}} = z^{J_{i,j}} = (z^a)^{J_{i,j}}.$$

If $i = 2^m$, then, again using (5·1) and (5·3), we get

$$\begin{aligned} \big[v_i^a, v_j^a\big] = \big[v_1^{-1}, v_{j+1}\big] &= [v_1, v_{j+1}]^{-1} = (z^{J_{1,j+1}})^{-1} \\ &= z^{-J_{1,j+1}} = z^{(-1)^j} = z^{J_{i,j}} = (z^a)^{J_{i,j}}. \end{aligned}$$

Now we consider b. If $j \neq 1$, then using (5·1) and (5·4) we have

$$\begin{aligned} \big[v_i^b, v_j^b\big] &= [v_{2^m-i+2}, v_{2^m-j+2}] = z^{J_{2^m-i+2,2^m-j+2}} \\ &= z^{-(-1)^{(2^m-i+2)-(2^m-j+2)}} = z^{-(-1)^{j-i}} = z^{J_{j,i}} = z^{-J_{i,j}} = (z^b)^{J_{i,j}}. \end{aligned}$$

If $j = 1$, then, again using (5·1) and (5·4), we see

$$\begin{aligned} \big[v_i^b, v_j^b\big] = \big[v_{2^m-i+2}, v_1^{-1}\big] &= [v_{2^m-i+2}, v_1]^{-1} = (z^{J_{2^m-i+2,1}})^{-1} \\ &= \left(z^{(-1)^{i-1}}\right)^{-1} = \left(z^{J_{i,j}}\right)^{-1} = z^{-J_{i,j}} = (z^b)^{J_{i,j}}. \end{aligned}$$

Our claim is now proved.

Using (5·3), we see that

$$v_i^{a^{2^m}} = v_i^{-1}, \quad \text{for every } i \in \{1, \dots, 2^m\}. \tag{5·5}$$

In particular, a is an automorphism of V of order 2^{m+1}. By (5·4), the element b^2 fixes every generator of V and hence b is an automorphism of V of order 2. Moreover, combining (5·3) and (5·4), we get

$$z^{bab} = (z^{-1})^{ab} = (z^{-1})^b = z = z^{a^{-1}},$$

https://doi.org/10.1017/S0305004114000188 Published online by Cambridge University Press

$$v_1^{bab} = (v_1^{-1})^{ab} = (v_1^{ab})^{-1} = \left(v_2^{b}\right)^{-1} = v_{2^m}^{-1} = v_1^{a^{-1}},$$
$$v_2^{bab} = (v_{2^m})^{ab} = (v_1^{-1})^{b} = v_1 = v_2^{a^{-1}}$$

and, for $i \in \{3, \dots, 2^m\}$,

$$v_i^{bab} = (v_{2^m-i+2})^{ab} = (v_{2^m-i+3})^{b} = (v_{2^m-(i-1)+2})^{b} = v_{i-1} = v_i^{a^{-1}}.$$

It follows that $bab = a^{-1}$. In particular,

$$Q = \langle a, b \rangle$$

is isomorphic to a dihedral group of order 2^{m+2}.

Now, the group Q acts as a group of automorphisms on the vector space $V/\langle z \rangle$ and hence we may regard $V/\langle z \rangle$ as a Q-module over $\mathbb{F}_3$.

LEMMA 5·1. *The group Q acts irreducibly on $V/\langle z \rangle$.*

Proof. If $m = 1$ or $m = 2$, then the lemma follows from a direct computation. Assume that $m \geqslant 3$. Write $W = V/\langle z \rangle$. We use an additive notation for the elements of W. Let U be an irreducible $\langle a \rangle$-submodule of W and let ℓ be the dimension of U over $\mathbb{F}_3$. Observe that since a^{2^m} acts as the inversion on W by (5·5), we see that a^{2^m} acts faithfully on U and so does a. Hence by [**22**, 9·4·3], we get that $2^{m+1} = |a|$ divides $3^\ell - 1$ and that ℓ is the smallest positive integer with $3^\ell \equiv 1 \pmod{2)^{m+1}$. Now, using the binomial expansion $3^\ell = (1+2)^\ell = \sum \binom{\ell}{i} 2^i$ and using $m \geqslant 3$, a computation shows that

$$3^{2^{m-1}} \equiv 1 \pmod{2)^{m+1},$$
$$3^{2^{m-2}} \equiv 1 + 2^m \pmod{2)^{m+1}.$$

Therefore $2^{m-1} = \ell$ and hence $\dim U = 2^{m-1}$.

By (5·5) the element a^{2^m} acts by inverting each element of W and hence the characteristic polynomial of a in its action on W is $T^{2^m} + 1$. Since the characteristic of W is 3, we obtain

$$T^{2^m} + 1 = (T^{2^{m-1}} + T^{2^{m-2}} - 1)(T^{2^{m-1}} - T^{2^{m-2}} - 1). \tag{5·6}$$

Write

$$W_+ = \{w \in W \mid w^{a^{2^{m-1}} + a^{2^{m-2}} - 1} = 0\},$$
$$W_- = \{w \in W \mid w^{a^{2^{m-1}} - a^{2^{m-2}} - 1} = 0\}.$$

Clearly, W_+ and W_- are $\langle a \rangle$-invariant subspaces of W with $\dim W_+ = \dim W_- = 2^{m-1}$. From the previous paragraph, we see that W_+ and W_- are irreducible $\langle a \rangle$-modules.

Since the characteristic polynomials of the action a on W_+ and W_- are different, we see that W_+ and W_- are non-isomorphic $\langle a \rangle$-modules. Moreover, as the order of $\langle a \rangle$ is coprime to 3, we deduce from Maschke's theorem that W_+ and W_- are the only proper $\langle a \rangle$-submodules of W.

Let U be a non-zero Q-submodule of W. In particular, U is a non-zero $\langle a \rangle$-submodule of W and hence $W_+ \leqslant U$ or $W_- \leqslant U$. We have

$$0 = 0^b = (a^{2^{m-1}} + a^{2^{m-2}} - 1)^b = (a^b)^{2^{m-1}} + (a^b)^{2^{m-2}} - 1$$
$$= a^{-2^{m-1}} + a^{-2^{m-2}} - 1$$

and, multiplying by $-a^{2^{m-1}}$, we obtain $-1 - a^{2^{m-2}} + a^{2^{m-1}} = 0$. This shows that $W_+^b = W_-$. Thus $W = W_+ \oplus W_- \leqslant U$ and hence W is an irreducible Q-module.

https://doi.org/10.1017/S0305004114000188 Published online by Cambridge University Press

Define

$$G = V \rtimes Q. \tag{5·7}$$

In what follows we denote the elements of G as ordered pairs xv, with $x \in Q$ and $v \in V$. In particular, for $x, y \in Q$ and $v, w \in V$, we have $(xv)(yw) = (xy)(v^y w)$. Moreover, we identify Q and V with their corresponding isomorphic copies in G.

Write $H = \langle a^{2^m} \rangle$ and let Ω be the set of right cosets of H in G. Clearly, $H^{v_1} = \langle a^{2^m} v_1^2 \rangle$ by (5·5) and hence $H \cap H^{v_1} = 1$. Thus H is core-free in G and the action by right multiplication of G on Ω endows G of the structure of a permutation group. For the rest of this section we regard G as a subgroup of $\mathrm{Sym}(\Omega)$.

LEMMA 5·2. *A semiregular element of G has order* 1, 2, 3 *or* 6.

Proof. We argue by contradiction and we let g be a semiregular element of order ℓ with $\ell \notin \{1, 2, 3, 6\}$. Since V has exponent 3, ℓ is divisible by 4. So, replacing g by $g^{\ell/4}$, we may assume that $\ell = 4$. Since Q is a Sylow 2-subgroup of G, replacing g by a suitable G-conjugate, we may assume that $g \in Q$. As Q is a dihedral group, we see that $g^2 = a^{2^m} \in H$ and hence g^2 fixes the point H of Ω, a contradiction.

Let Γ be the directed graph with vertex set Ω and with arc set

$$\{(Hg, Habg) \mid g \in G\} \cup \{(Hg, Hbv_1 g) \mid g \in G\} \cup \{(Hg, Hbv_1^{-1} g) \mid g \in G\}. \tag{5·8}$$

LEMMA 5·3. *The graph Γ has $2^{m+1}3^{2^m+1}$ vertices. Moreover, Γ is connected, undirected, cubic and G-vertex-transitive.*

Proof. The vertex set of Γ is Ω and $|\Omega| = |G : H| = |Q||V|/|H| = 2^{m+1}3^{2^m+1}$.

Now ab, bv_1 and bv_1^{-1} have order 2 because $(ab)^2 = abab = aa^{-1} = 1$ and $(bv_1^{\pm 1})^2 = b^2(v_1^{\pm 1})^b v_1^{\pm 1} = (v_1^{\pm 1})^{-1} v_1^{\pm 1} = 1$ by (5·4). Therefore (Hab, H), (Hbv_1, H) and (Hbv_1^{-1}, H) are arcs of Γ. This shows that Γ is undirected.

The vertices of Γ adjacent to H are of the form $Habh$, $Hbv_1 h$ and $Hbv_1^{-1}h$, as h runs through the elements of H. Using (5·5) we get

$$\begin{aligned}
(Hab)a^{2^m} &= Haba^{2^m} = Ha^{2^m}ab = Hab,\\
(Hbv_1)a^{2^m} &= Hba^{2^m}(v_1)^{a^{2^m}} = Ha^{2^m}bv_1^{-1} = Hbv_1^{-1},\\
(Hbv_1^{-1})a^{2^m} &= Hba^{2^m}(v_1^{-1})^{a^{2^m}} = Ha^{2^m}bv_1 = Hbv_1.
\end{aligned}$$

Since $H = \langle a^{2^m} \rangle$, the neighbourhood of H is $\{Hab, Hbv_1, Hbv_1^{-1}\}$ and hence Γ is cubic.

The definition of the arc set (5·8) immediately gives that Γ is G-vertex-transitive. It remains to show that Γ is connected. Write $K = \langle ab, bv_1, bv_1^{-1} \rangle$. Observe that the elements ab, bv_1 and bv_1^{-1} map the vertex H to each of its three neighbours. Therefore, the connected component of Γ containing H is $\{Hk \mid k \in K\}$. Thus it suffices to prove that $G = K$. Now, $(bv_1)(bv_1^{-1}) = b^2 v_1^b v_1^{-1} = v_1^{-2} = v_1$ by (5·4). Thus $v_1 \in K$ and hence $b = (bv_1)(v_1)^{-1} \in K$. Now, $a = (ab)b \in K$. Thus $Q \leqslant K$. Observing that the conjugates of v_1 under Q generate the whole of V, we get $V \leqslant K$ and hence $G = K$.

Write $A = \mathrm{Aut}(\Gamma)$. (As usual, we denote by A_α the stabiliser in A of the vertex α of Γ. In particular, A_H is the stabiliser of the vertex H.)

LEMMA 5·4. *A_H is a 2-group and $|A : G|$ is a 2-power.*

https://doi.org/10.1017/S0305004114000188 Published online by Cambridge University Press

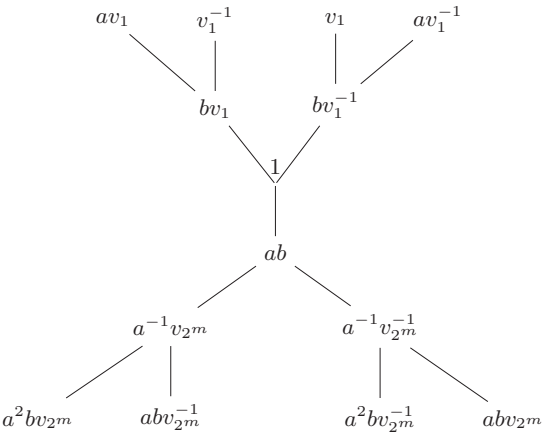


Fig. 1. Local structure of Γ.

Proof. Since G acts transitively on $V\Gamma$, we have $A = A_H G$ and hence it suffices to show that A_H is a 2-group. We argue by contradiction. So A_H acts transitively on Γ_H by Lemma 3·1. Now, it is easy to verify that

$$\left(H, Hbv_1, Hv_1^{-1}, Hb, Hv_1, Hbv_1^{-1}\right)$$

is a cycle of Γ of length 6 passing through the two neighbours Hbv_1 and Hbv_1^{-1} of H. As A_H is transitive on Γ_H, the graph Γ admits a cycle of length 6 passing through the two neighbours Hab and Hbv_1 of H.

Using the definition of Γ and (5·3) and (5·4), we compute all the vertices of Γ at distance $\leqslant 2$ from either H or Hab. Figure 1 depicts this small neighbourhood of Γ and shows that there is no cycle of length 6 containing H, Hab and Hbv_1. (For simplicity, in Figure 1 we write x to denote the vertex Hx.) This contradiction shows that Γ is not arc-transitive.

Before continuing our discussion we need an elementary lemma on the abelian subgroups of the general linear group $\mathrm{GL}_\ell(2)$.

LEMMA 5·5. *An elementary abelian* 3*-subgroup of* $\mathrm{GL}_\ell(2)$ *has size at most* $3^{\ell/2}$.

Proof. Observe $\mathrm{GL}_\ell(2)$ is a group of Lie type. It can be readily checked in [**9**, theorem 4·10·3 (a)] that the maximal order of an elementary abelian 3-subgroup of $\mathrm{GL}_\ell(2)$ is $3^{\lfloor \ell/2 \rfloor}$.

LEMMA 5·6. *Assume that* $G < A$ *and let* T *be a minimal (with respect to inclusion) subgroup of* A *with* $G < T$. *Then* V *is normal in* T.

Proof. As Γ is G-vertex-transitive, from the Frattini argument we have $T = GT_\alpha$, for every $\alpha \in V\Gamma$. Now, since Γ is cubic, T_α is a $\{2, 3\}$-group. Moreover G is a $\{2, 3\}$-group because $G = V \rtimes Q$ with V a 3-group and Q a 2-group. This argument shows that T is a $\{2, 3\}$-group and hence soluble.

Let K be the core of G in T. Since G is a maximal subgroup of T, the group T/K acts primitively on the set Ω of right cosets of G in T. Since T/K is soluble, T/K is of "affine" O'Nan–Scott type. Let S/K be the socle of T/K. By primitivity, S/K (in its action on Ω) is a regular normal elementary abelian p-subgroup of T/K, for some prime $p \in \{2, 3\}$. Therefore $T = SG$, $S \cap G = K$ and $|\Omega| = |T : G| = |S : K|$. By Lemma 5·4, $|A : G|$ is a 2-power and hence so is $|T : G|$. This gives $p = 2$. Let 2^ℓ be the order of S/K. Now,

https://doi.org/10.1017/S0305004114000188 Published online by Cambridge University Press

if $V \leqslant K$, then T/K is a 2-group and hence the primitivity forces $|T : G| = 2$. As V is characteristic in G and $G \trianglelefteq T$, we get $V \trianglelefteq T$.

Suppose that $V \not\leqslant K$. We show that this yields to a contraction. Then $V \cap K$ is a normal subgroup of G properly contained in V. As Q acts irreducibly on $V/\langle z\rangle$ by Lemma 5·1, we must have $V \cap K = 1$ or $V \cap K = \langle z\rangle$. As T/K is a primitive group of affine type with point stabiliser G/K, the group G/K is isomorphic to an irreducible subgroup of $\mathrm{GL}_\ell(2)$. In particular, $\mathrm{GL}_\ell(2)$ contains either an elementary abelian 3-group of order 3^{2^m} (if $V \cap K = \langle z\rangle$) or an extraspecial 3-group of order 3^{2^m+1} (if $V \cap K = 1$). As V contains an elementary abelian 3-subgroup of order $3^{2^{m-1}+1}$, in both cases we see that $\mathrm{GL}_\ell(2)$ contains an elementary abelian 3-subgroup of order at least $3^{2^{m-1}+1}$. So, Lemma 5·5 gives

$$\ell \geqslant 2(2^{m-1} + 1) = 2^m + 2. \tag{5·9}$$

As $|V \cap K| \leqslant 3$ and as V is a Sylow 3-subgroup of T, we see that $|S| = 3^i 2^{\ell'}$, for some $i \in \{0, 1\}$ and some $\ell' \geqslant \ell$. Let R be the largest normal 2-subgroup of S. Clearly, R is the intersection of the Sylow 2-subgroups of S and hence normal in T. By Sylow's theorems, S acts transitively by conjugation on the set $\mathrm{Syl}_2(S)$ of its Sylow 2-subgroups and $|\mathrm{Syl}_2(S)| \in \{1, 3\}$. Thus $|S : R| \leqslant 3! = 6$ and hence $|R| \geqslant 2^{\ell'-1}$. We now distinguish two cases, depending on whether R is semiregular or not.

Assume that R is semiregular. Then RV is a subgroup of T acting semiregularly on $V\Gamma$ because R is semiregular and because A_H is a 2-group by Lemma 5·4. Thus

$$2^{m+1}3^{2^m+1} = |V\Gamma| \geqslant |RV| = |R||V| = |R|3^{2^m+1} \geqslant 2^{\ell'-1}3^{2^m+1}$$

and $m + 1 \geqslant \ell' - 1 \geqslant \ell - 1$. However, this contradicts (5·9).

Assume that R is not semiregular. Let Δ be the normal quotient Γ/R. As R is not semiregular, we see that Δ has valency 2 and hence Δ is a cycle. Let F be the kernel of the action of T on R-orbits. As R and A_H are both 2-groups, so is F. Moreover, as Δ is a cycle, T/F is isomorphic to a dihedral group. However, the 3-group $VF/F \cong V/(V \cap F) = V$ is not isomorphic to a subgroup of a dihedral group, a contradiction.

In the next lemma we denote by $\mathbf{C}_X(Y)$ the centraliser of Y in X, by $\mathbf{N}_X(Y)$ the normaliser of Y in X and by $\mathbf{Z}(X)$ the centre X.

LEMMA 5·7. *$A = G$.*

Proof. We argue by contradiction and we assume that $G < A$. Let T be a minimal, with respect to inclusion, subgroup of A with $G < T$. From Lemma 5·6, we have $V \trianglelefteq T$. Now, T/V is a 2-group by Lemma 5·4 and hence, by minimality, $|T : G| = 2$ and $|T_H| = 4$.

Write $R = \mathbf{C}_T(H)$. We show that R is a Sylow 2-subgroup of T and that $R = QT_H$. Since Q is isomorphic to the dihedral group of order 2^{m+2}, we have $|\mathbf{Z}(Q)| = 2$ and hence $\mathbf{Z}(Q) = H$. Moreover, since $HV/V \cong H$ and $G/V \cong Q$, we get that HV/V is the centre of G/V. Thus HV/V is a characteristic subgroup of G/V and hence normal in T/V. This shows that $HV \trianglelefteq T$. Since H is a Sylow 2-subgroup of HV, from the Frattini argument we obtain $T = \mathbf{N}_T(H)HV = \mathbf{N}_T(H)V$. As $|H| = 2$, we have $\mathbf{N}_T(H) = \mathbf{C}_T(H) = R$. Therefore $T = RV$. Clearly, $R \cap V = \mathbf{C}_V(H) = 1$ and hence R is a Sylow 2-subgroup of T. Finally, note that $Q \leqslant R$ because $H = \mathbf{Z}(Q)$ and $T_H \leqslant R$ because $|T_H : H| = |H| = 2$.

Fix $c \in T_H \setminus H$. Observe that replacing c by an element in the coset Hc, we may assume that c fixes pointwise the neighbourhood $\Gamma_H = \{Hab, Hbv_1, Hbv_1^{-1}\}$ of H. Since c normalises Q and since Q is a dihedral group of order 2^{m+1}, we must have $a^c = a^i$ and $b^c = a^j b$, for some odd $i \in \{1, \ldots, 2^{m+1} - 1\}$ and some $j \in \{0, \ldots, 2^{m+1} - 1\}$.

https://doi.org/10.1017/S0305004114000188 Published online by Cambridge University Press

Given a vertex Hx of Γ, we denote by $(Hx)^c$ the image of Hx under the automorphism c. We have

$$\begin{aligned} Hab = (Hab)^c = H^{abc} = H^{c(c^{-1}abc)} = (H^c)^{(ab)^c} \\ = H^{(ab)^c} = H^{a^c b^c} = H^{a^i a^j b} = Ha^{i+j}b \end{aligned}$$

and hence $a^{i+j-1} \in H$. Thus $i + j = 1$ or $i + j = 1 + 2^m$. Similarly, recalling that c normalises also V, we have

$$\begin{aligned} Hbv_1 = (Hbv_1)^c = H^{bv_1c} = H^{c(c^{-1}bv_1c)} = (H^c)^{(bv_1)^c} \\ = H^{(bv_1)^c} = H^{b^c v_1^c} = H^{a^j b v_1^c} = Ha^j b v_1^c \end{aligned}$$

and hence $a^j \in H$ and

$$v_1^c = v_1. \tag{5·10}$$

In particular, $j = 0$ or $j = 2^m$. In what follows we discuss the various possibilities for i and j.

Suppose that $i = 1$. Write $C = \mathbf{C}_T(c)$. As $i = 1$, we have $a^c = a$ and hence $a \in C$. Since $v_1 \in C$ and since $V = \langle v_1^{a^k} \mid k \rangle$, we obtain $V \leqslant C$. Thus $V\langle a, c\rangle \leqslant C$ and hence $|T : C| \leqslant 2$. Assume that $T = C$. So, c is a central element of T fixing H. As T acts faithfully on $V\Gamma$, we have $c = 1$, a contradiction. Assume that $|T : C| = 2$, that is, $C = V\langle a, c\rangle$. Now C is intransitive on $V\Gamma$ and the C-orbits form a bipartition for Γ. As c centralises C and fixes the vertex H together with its neighbour Hab, we see that c fixes every vertex in $H^C \cup (Hab)^C = V\Gamma$. Thus $c = 1$, a contradiction. This shows that $i = 1 + 2^m$ and $a^c = a^{1+2^m}$.

Suppose that $j = 2^m$, that is, $b^c = a^{2^m} b$. Using (5·3), (5·4), (5·5) and (5·10), we obtain

$$v_1^{-1} = \left(v_1^{-1}\right)^c = \left(v_1^b\right)^c = v_1^{bc} = v_1^{ca^{2^m}b} = v_1^{a^{2^m}b} = \left(v_1^{-1}\right)^b = v_1,$$

a contradiction. Thus $j = 0$ and $b^c = b$.

We are now ready to get a final contradiction. Note that

$$v_2^c = (v_1^a)^c = v_1^{ac} = v_1^{ca^{2^m}a} = v_1^{a^{2^m}a} = \left(v_1^{-1}\right)^a = v_2^{-1},$$

and from this we similarly obtain

$$v_3^c = \left(v_2^a\right)^c = v_2^{ac} = v_2^{ca^{2^m}a} = \left(v_2^c\right)^{a^{2^m}a} = \left(v_2^{-1}\right)^{a^{2^m}a} = v_2^a = v_3.$$

From (5·1) and (5·2), we have $z = [v_1, v_2]$ and hence by applying c on both sides of this equality we get

$$z^c = [v_1, v_2]^c = [v_1^c, v_2^c] = [v_1, v_2^{-1}] = [v_1, v_2]^{-1} = z^{-1}. \tag{5·11}$$

Again from (5·1) and (5·2), we have $z^{-1} = [v_1, v_3]$ and hence by applying c on both sides of this equality we get

$$(z^{-1})^c = [v_1, v_3]^c = [v_1^c, v_3^c] = [v_1, v_3] = z^{-1}$$

and $z^c = z$. Clearly, this contradicts (5·11).

Proof of Theorem 1·1. For every $m \geqslant 1$, let G_m be the group defined in (5·7) and let Γ_m be the graph defined in (5·8). From Lemmas 5·3 and 5·7, Γ_m is a cubic vertex-transitive graph with $2^{m+1}3^{2^m+1}$ vertices and with automorphism group G_m. From Lemma 5·2, every semiregular automorphism of Γ_m has order at most 6. As $\lim_{m\to\infty} |V\Gamma_m| = \infty$, the theorem is proved.

https://doi.org/10.1017/S0305004114000188 Published online by Cambridge University Press

REFERENCES

[**1**] W. BOSMA, J. CANNON and C. PLAYOUST. The Magma algebra system. I. The user language, *J. Symbolic Comput.* **24** (1997), 235–265.

[**2**] P. J. CAMERON. *Permutation groups*. London Mathematical Society Student Texts 45 (Cambridge University Press, 1999).

[**3**] P. CAMERON, M. GIUDICI, G. A. JONES, W. KANTOR, M. KLIN, D. MARUŠIČ and L. A. NOWITZ. Transitive permutation groups without semiregular subgroups. *J. London Math. Soc.* (2) **66** (2002), 325–333.

[**4**] P. CAMERON, J. SHEEHAN and P. SPIGA. Semiregular automorphisms of vertex-transitive cubic graphs. *European J. Combin.* **27** (2006), 924–930.

[**5**] R. W. CARTER. *Simple Groups of Lie Type*. (Wiley Classics Library, John Wiley & Sons, Inc., New York, 1989).

[**6**] J. H. CONWAY, R. T. CURTIS, S. P. NORTON, R. A. PARKER and R. A. WILSON. *Atlas of Finite Groups*. (Claredon Press, Oxford, 1985).

[**7**] E. DOBSON, A. MALNIČ, D. MARUŠIČ and L. A. NOWITZ. Semiregular automorphisms of vertex-transitive graphs of certain valencies. *J. Combin. Theory Ser. B* **97** (2007), 371–380.

[**8**] M. GIUDICI and J. XU. All vertex-transitive locally-quasiprimitive graphs have a semiregular automorphism. *J. Algebraic Combin.* **25** (2007), 217–232.

[**9**] D. GORENSTEIN, R. LYONS and R. SOLOMON. *The Classification of the Finite Simple Groups*, Number 3. Mathematical Surveys and Monographs, Vol. 40. (American Mathematical Society, 1994).

[**10**] P. HALL and G. HIGMAN. On the p-length of p-soluble groups and reduction theorems for Burnside's problem. *Proc. London Math. Soc.* **6** (1956), 1–42.

[**11**] G. HAVAS, M. F. NEWMAN, A. C. NEIMEYER and C. C. SIMS. Groups with exponent six. *Comm. Algebra* **27** (1999), 3619–3638.

[**12**] D. JORDAN. Eine Symmetrieeigenschaft von Graphen, Graphentheorie und ihre Anwendungen. *Dresdner Reihe Forsch.* **9** (Dresden, 1988).

[**13**] M. KLIN. On transitive permutation groups without semi-regular subgroups, ICM 1998: International Congress of Mathematicians. (Berlin, 18–27 August 1998). Abstracts of short communications and poster sessions. (1998), 279.

[**14**] K. KUTNAR and P. ŠPARL. Distance-transitive graphs admit semiregular automorphisms. *European J. Combin.* **31** (2010), 25–28.

[**15**] D. MARUŠIČ. On vertex symmetric digraphs. *Discrete Math.* **36** (1981), 69–81.

[**16**] D. MARUŠIČ and R. SCAPELLATO. Permutation groups, vertex-transitive digraphs and semiregular automorphisms. *European J. Combin.* **19** (1998) 707–712

[**17**] B. MCKAY and C. E. PRAEGER. Vertex-transitive graphs which are not Cayley graphs. I. *J. Austral. Math. Soc. Ser. A* **56** (1994), 53–63.

[**18**] J. MORRIS, P. SPIGA and G. VERRET. Semiregular automorphisms of cubic vertex-transitive graphs. *Submitted*.

[**19**] P. POTOČNIK, P. SPIGA and G. VERRET. Cubic vertex-transitive graphs on up to 1280 vertices. *J. Symbolic Comput.* (2013), 465–477. `http://dx.doi.org/10.1016/j.jsc.2012.09.00`.

[**20**] P. POTOCNIK, P. SPIGA and G. VERRET. Asymptotic enumeration of vertex-transitive graphs of fixed valency. *Submitted*.

[**21**] C. E. PRAEGER, P. SPIGA and G. VERRET. Bounding the size of a vertex-stabiliser in a finite vertex-transitive graph. *J. Combin. Theory Ser. B* **102** (2012), 797–819.

[**22**] D. J. S. ROBINSON. *A course in the theory of groups*. Graduate Texts in Mathematics **20** (Springer-Verlag, 1982).

[**23**] W. T. TUTTE. A family of cubical graphs. *Proc. Camb. Phil. Soc.* **43** (1947), 459–474.

[**24**] M. VAUGHAN–LEE. *The Restricted Burnside Problem*, Second Edition, London Mathematical Society Monographs N.S. 8 (Oxford Science Publications, 2003).

[**25**] E. I. ZELMANOV. The Solution of the Restricted Burnside problem for groups of odd exponent. *Izv. Math. USSR* **36** (1991), 4–60.

[**26**] E. I. ZELMANOV. The solution of the restricted Burnside problem for 2-groups. *Mat. Sb.* **182** (1991), 568–592.

[**27**] K. ZSIGMONDY. Zur theorie der Potenzreste. *Monatsh. Math. Phys.* **3** (1892), 265–284.

https://doi.org/10.1017/S0305004114000188 Published online by Cambridge University Press