THE SEXTET CONSTRUCTION FOR CUBIC GRAPHS

N. L. BIGGS and M. J. HOARE

Received 24 July 1982

We show how to construct cubic graphs which have automorphism groups acting regularly on the s-arcs, $s=4$ or 5.

1. Introduction

In this paper we shall show how to construct families of cubic graphs which have automorphism groups acting regularly on the s-arcs, $s=4$ or 5. It is a famous theorem of Tutte [8] that $s=5$ is the largest value for which this can happen.

Our construction is purely combinatorial, and it yields what we shall call a "sextet graph" $S(p)$ for each odd prime p. In order to describe the automorphism groups of $S(p)$ it is necessary to consider separately the congruence classes of p modulo 16. When $p\equiv 3$, 5, 11, 13 (mod 16) the graph $S(p)$ admits a 5-arc transitive group of automorphisms. The graph $S(3)$ is Tutte's 8-cage with 30 vertices, which is the smallest 5-arc transitive cubic graph. The graph $S(5)$, which has 650 vertices, had previously been noticed (but not published) by J. H. Conway and R. M. Foster. Foster's construction of the graph "by hand" was a remarkable achievement.

No other graphs in the family $S(p)$, $p\equiv 3$, 5, 11, 13 (mod 16) have been noticed before, and it seems that it has not been recognised that an infinite family of 5-arc transitive graphs can be constructed in this way. On the other hand, the group-theoretical counterpart of our construction—the use of octahedral subgroups of projective linear groups—has been known in some cases since the paper of Wong [10] in 1967. Specifically, Wong showed that the only cubic graphs which admit a primitive group acting regularly on the 4-arcs are the graphs $S(p)$ with $p\equiv 1$, 15 (mod 16).

The original motivation for this investigation was a question raised by Djokovic and Miller [4]. In our terminology, they asked for the girth of $S(p)$ in the cases $p\equiv 1$, 15 (mod 16). We conjecture that the girth of $S(p)$ is unbounded as a function of p in all cases, and in Section 5 we prove a result which lends support to this conjecture. One of us (MJH) has computed the girth of $S(p)$ for many values of p. The results tend to confirm the conjecture, and in several cases they provide specific exam-

AMS subject classification (1980): 05 C 25

ples of cubic graphs with relatively large girth. For example, $S(313)$ has girth 30, and its order is 1,277,666, which is approximately 2^{20}. Previously the only known results about cubic graphs with girth 30 were the general theorems stating that about 2^{16} vertices are necessary and about 2^{30} vertices are sufficient.

2. Generalities on cubic graphs

In this section we shall summarise those parts of the general theory of cubic graphs which are required subsequently.

Let Γ be a finite cubic graph with vertex-set V and edge-set E. An edge e which joins the vertices v and w will be written $e=vw$. An *s-arc* in Γ is a sequence of vertices $(v_0, v_1, \dots, v_s)$ such that v_iv_{i+1} is an edge $(0 \leqq i \leqq s-1)$ and $v_i \neq v_{i+2} (0 \leqq i \leqq s-2)$. It has two *successors* $(v_1, v_2, \dots, v_s, w)$ and $(v_1, v_2, \dots, v_s, w')$, where v_{s-1}, w, and w' are the three vertices adjacent to v_s.

Now let Γ_0 be a connected cubic graph and G a group of automorphisms of Γ_0. The pointwise stabilizer of an r-arc $(v_0, v_1, \dots, v_r)$ will be denoted by $G(v_0, v_1, \dots, v_r)$. The following three results may be extracted from Tutte's paper [8].

Proposition A. *If G acts transitively on the s-arcs of Γ_0, but not on the $(s+1)$-arcs' then for any s-arc $(v_0, v_1, \dots, v_s)$ we have*

$$|G(v_0, v_1, \dots, v_i)| = 2^{s-i} \quad (1 \leqq i \leqq s).$$

$$|G(v_0)| = 3 \cdot 2^{s-1}.$$

In particular, the pointwise stabilizer of any s-arc is trivial. (In this situation we say that G acts *s-regularly*.)

Proposition B. *If G acts transitively on the 1-arcs of Γ_0 then it acts s-regularly for some s with $1 \leqq s \leqq 5$. In the case $s=4$, $G(v_0)$ is isomorphic to the octahedral group S_4 while if $s=5$, $G(v_0)$ is isomorphic to $S_4 \times \mathbf{Z}_2$.*

Proposition C. *G acts transitively on the s-arcs of Γ_0 if and only if there are automorphisms "a" and "b" in G which shunt a given s-arc onto its two successors.*

We shall be concerned mainly with the following situation. A standard 4-arc $(v_0, v_1, v_2, v_3, v_4)$ is given in a (not necessarily connected) graph Γ, and a, b are shunt automorphisms taking it onto its two successors. By Proposition C the group $H=\langle a, b\rangle$ must act transitively on the 4-arcs of the component Γ_0 of Γ which contains $(v_0, v_1, v_2, v_3, v_4)$. Furthermore, by Proposition B, H must act s-regularly with $s=4$ or 5. Thus the order of H and the order n of Γ_0 are related by

$$|H| = \begin{cases} 24n & \text{if} \quad s=4; \\ 48n & \text{if} \quad s=5. \end{cases}$$

It follows that in order to determine n we must find both s and $|H|$.

In our study of the *girth* (length of the shortest cycle) of Γ_0 we shall use a relationship between the cycles of Γ_0 and the shunts a, b.

A *word* of *length* l in two non-commuting variables ξ, η is a string of l symbols $w=w_1w_2\dots w_l$ where each w_i is either ξ or η. If ξ, η are members of a monoid $\mathfrak{M}$ then $w(\xi, \eta)$ is also in $\mathfrak{M}$.

Proposition D. *Let Γ_0 be a connected cubic graph, and suppose G is a group of automorphisms acting s-regularly on Γ_0 and generated by the shunt automorphisms a and b with respect to the s-arc $(v_0, v_1, \dots, v_s)$. Then Γ_0 has girth g if and only if the shortest word w such that $w(a, b)$ is the identity in G has length g.*

Proof. Suppose that $w=w(\xi, \eta)$ is a word of length l such that $w(a, b)$ is the identity in G. Let

$$y_i = \begin{cases} a & \text{if} \quad w_i = \xi, \\ b & \text{if} \quad w_i = \eta, \end{cases}$$

and define vertices $v_i (1 \leqq i \leqq l)$ of Γ_0 by the rule

$$v_i = y_1 y_2 \dots y_i(v_0).$$

It can be verified that $v_1, v_2, \dots, v_s$ coincide with the vertices of the standard s-arc previously designated by those symbols. Also $v_i = y_1y_2 \dots y_{i-1}(v_1)$, $v_{i-1} = y_1y_2 \dots \dots y_{i-1}(v_0)$, and since v_1 is adjacent to v_0 it follows that v_i is adjacent to v_{i-1}. Furthermore, $y_1y_2\dots y_l = w(a, b)$ is the identity, so $v_l = v_0$. Hence we have a cycle of length l in Γ_0.

Conversely, suppose C is a cycle whose vertices (in cyclic order) are $u_0, u_1, \dots \dots, u_{r-1}$. Since G acts s-regularly there are unique elements x_i $(1 \leqq i \leqq r)$ in G such that

$$x_i(u_{i-1}, u_i, \dots, u_{i+s-1}) = (u_i, u_{i+1}, \dots, u_{i+s}),$$

where the subscripts are taken modulo r. Let

$$y_i = x_1^{-1}x_2^{-1} \dots x_{i-1}^{-1}x_i x_{i-1} \dots x_1 \quad (1 \leqq i \leqq r).$$

Then it may be verified that each y_i takes the s-arc $(u_0, u_1, \dots, u_s)$ onto one of its successors. Let m be the unique element of G taking $u_0, u_1, \dots, u_s$ onto $v_0, v_1, \dots, v_s$, so that my_im^{-1} takes $(v_0, v_1, \dots, v_s)$ onto one of its sucessors and is consequently either a or b. Define a word w_C of length r by

$$(w_C)_i = \begin{cases} \xi & \text{if} \quad my_im^{-1} = a, \\ \eta & \text{if} \quad my_im^{-1} = b. \end{cases}$$

Then

$$w_C(a, b) = m^{-1}(y_1y_2 \dots y_r)m = m^{-1}(x_rx_{r-1} \dots x_1)m.$$

But $x_rx_{r-1}\dots x_1$ fixes the s-arc $(u_0, u_1, \dots, u_s)$, and so it is the identity. Hence $w_C(a, b)$ is the identity.

We have established a correspondence between the cycles of length l in Γ_0 and the words w of length l such that $w(a, b)$ is the identity in G. From this the required result follows immediately. ▌

3. The Sextet Construction

Let q be an odd prime power, and let $\mathrm{GF}(q)$ denote the field of order q. The projective line $\mathrm{PG}(1, q)$ may be identified with the set $L = \mathrm{GF}(q) \cup \{\infty\}$, with the usual conventions about ∞. We shall say that a *duet* is an unordered pair of points $\{a, b\}$ on L, and a *quartet* is an unordered pair of duets whose cross-ratio is -1. That is, $\{ab|cd\}$ is a quartet if and only if

$$\frac{(a-c)(b-d)}{(a-d)(b-c)} = -1,$$

with the conventions about ∞ being interpreted so that $\{\infty b|cd\}$ is a quartet if and only if

$$\frac{b-d}{b-c} = -1.$$

We define a *sextet* to be an unordered triple of duets $\{ab|cd|ef\}$ such that each of $\{ab|cd\}$, $\{cd|ef\}$, $\{ef|ab\}$, is a quartet.

Lemma 1. *The number of quartets is* $q(q^2-1)/8$. *The number of sextets is* $q(q^2-1)/24$ *if* $q \equiv 1 \pmod 4$ *and zero if* $q \equiv 3 \pmod 4$.

Proof. Recall that the group $\mathrm{PGL}(2, q)$ of projective linear transformations

$$t \mapsto \frac{\alpha t + \beta}{\gamma t + \delta} \quad (\alpha, \beta, \gamma, \delta \in \mathrm{GF}(q),\ \alpha\delta - \beta\gamma \neq 0)$$

acts sharply 3-transitively on L, and its order is $q(q^2-1)$. Clearly $\mathrm{PGL}(2, q)$ acts transitively on the duets, so we may consider the typical duet $\{0, \infty\}$. Now $\{0\infty,|xy\}$ is a quartet if and only if $x+y=0$, so there are $1/2(q-1)$ quartets containing $\{0, \infty\}$. The total number of quartets is therefore $1/2 \cdot 1/2q(q+1) \cdot 1/2(q-1) = q(q^2-1)/8$.

Since the points $0, \infty, 1$, determine the unique quartet $\{0\infty,|1\ -1\}$, and $\mathrm{PGL}(2, q)$ acts 3-transitively on L, it acts transitively on the quartets. The conditions that $\{0\infty|1\ -1|u\,v\}$ be a sextet are $u+v=0$, $uv=1$, so that u, v must be primitive fourth roots of unity in $\mathrm{GF}(q)$. If $q \equiv 1 \pmod 4$ there is a unique pair of solutions $i, -i$, so that each quartet determines a unique sextet. Since each sextet arises from three quartets, the total number of sextets is $q(q^2-1)/24$. If $q \equiv 3 \pmod 4$ there are no primitive fourth roots of unity, and so no sextets. ∎

From now on we shall assume that $q \equiv 1 \pmod 4$ and that $i, -i$ are primitive fourth roots of unity. The following result may be checked by a calculation involving a single sextet, since $\mathrm{PGL}(2, q)$ acts transitively on the sextets.

Lemma 2. *An involution in* $\mathrm{PGL}(2, q)$ *is uniquely determined by two pairs of corresponding points, and, if the two pairs form a quartet, then the fixed points of the involution are the third pair in the unique sextet determined by the given quartet.* ∎

For example, if the quartet is $Q = \{1\ -1|i\ -i\}$, then the involution is given by $j_Q(t) = -t$ and the fixed points are $0, \infty$. The four points of Q may be split into two duets in two other ways, that is, $R = \{1\ i|-1\ -i\}$ and $S = \{1\ -i|-1\ i\}$, where we remark that R and S are not quartets. The correspondin g involutions are

$$j_R(t) = i/t, \quad j_S(t) = -i/t.$$

Solving formally to obtain the fixed points of j_R and j_S we see that we require a square root of i, that is, a primitive eight root of unity.

Suppose then that $q\equiv 1 \pmod 8$ and π is a primitive element of $GF(q)$. If $q=8r+1$ then $\sigma=\pi^r$ is a primitive eighth root of unity, and we may take $i=\sigma^2$. With this notation the fixed points of j_Q, j_R, j_S are $0, \infty; \sigma, -\sigma; \sigma^3, -\sigma^3$. It can easily be checked that this is a sextet.

This remark is the basis for our construction. We must assume that $q\equiv 1$ (mod 8); then we say that the sextets

$$\{\alpha_1\alpha_2|\beta_1\beta_2|\gamma_1\gamma_2\}, \quad \{\alpha_1'\alpha_2'|\beta_1'\beta_2'|\gamma_1'\gamma_2'\}$$

are *adjacent* if $\{\alpha_1', \alpha_2'\}$, $\{\beta_1', \beta_2'\}$ $\{\gamma_1', \gamma_2'\}$ are the fixed points of the involutions j_Q, j_R, j_S, where Q, R and S are given by

$$Q = \{\beta_1\beta_2|\gamma_1\gamma_2\}, \quad R = \{\beta_1\gamma_2|\beta_2\gamma_1\}, \quad S = \{\beta_1\gamma_1|\beta_2\gamma_2\}.$$

It follows from Lemma 2 that $\{\alpha_1', \alpha_2'\}$ is the same as $\{\alpha_1, \alpha_2\}$. There are three sextets adjacent to a given sextet, each having one duet in common with the given sextet. Furthermore, the relation of adjacency is symmetric—it is only necessary to check at one sextet, since we already know that $PGL(2, q)$ acts transitively on the sextets. Thus we have a cubic graph whose vertices the $q(q^2-1)/24$ sextets, with adjacency as defined above. This graph will be denoted by $\Sigma(q)$. In general $\Sigma(q)$ will not be connected, and our major task (in Section 4) will be to determine the size of its components.

Lemma 3. *The group* $PGL(2, q)$ *acts as a group of automorphisms of* $\Sigma(q)$.

Proof. We have already remarked that $PGL(2, q)$ acts on the sextets--that is, the vertices of $\Sigma(q)$. In order to show that an element g of $PGL(2, q)$ is an automorphism of $\Sigma(q)$ we remark that if θ_1, θ_2 are the fixed points of an involution j_Q, then $g\theta_1$, $g\theta_2$ are the fixed points of $gj_Qg^{-1}=j_{gQ}$. Hence g preserves adjacency in $\Sigma(q)$. ▌

At this point we can describe the relationship, mentioned in the introduction, between the sextet construction and the octahedral (S_4) subgroups of $PGL(2, q)$. The stabilizer of a sextet, say $\{0\,\infty|1\ -1|i\ -i\}$ contains the projective linear transformations

$$t\mapsto 1/t, \quad t\mapsto it, \quad t\mapsto (1-t)/(1+t),$$

which generate a subgroup isomorphic to S_4. Indeed, it is possible to think of the elements of a sextet as the vertices of an octahedron, where each duet represents a pair of opposite vertices.

4. Properties of the sextet graphs

The graphs $\Sigma(q)$ constructed in the previous section are not necessarily connected. In this section we shall investigate the size of their components and their automorphism groups.

It will be convenient to work with matrices (elements of $GL(2, q)$) as well as with PGL(2, q). We shall say that a matrix

$$M = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \quad (\alpha, \beta, \gamma, \delta \in \mathrm{GF}(q),\ \alpha\delta - \beta\gamma \neq 0)$$

induces the automorphism m of $\Sigma(q)$ corresponding to the action of the projective linear transformation

$$t \mapsto \frac{\alpha t + \beta}{\gamma t + \beta}$$

on the sextets. Clearly, the matrices M and kM induce the same automorphism for all non-zero k in GF(q).

Let $q = p^n$, p an odd prime, and suppose henceforth that $p^n \equiv 1 \pmod 8$, so that the graph $\Sigma(p^n)$ exists. For each such p^n we shall choose a primitive eighth root of unity in GF(p^n), and denote it by σ. The symbols i and $\sqrt{2}$ will always denote the elements of GF(p^n) defined as follows: $i = \sigma^2$, $\sqrt{2} = \sigma + \sigma^{-1}$.

We shall denote by $\Sigma_0(p^n)$ the component of $\Sigma(p^n)$ containing the vertex (sextet) $k_1 = \{0\ \infty \mid 1\ \ -1 \mid i\ \ -i\}$. Let a, b denote the automorphisms of $\Sigma_0(p^n)$ induced by the matrices

$$A = \begin{bmatrix} \sigma & -\sigma \\ 1 & 1 \end{bmatrix}, \quad B = \begin{bmatrix} \sigma & \sigma \\ 1 & -1 \end{bmatrix},$$

and let k_0, k_1, k_2, k_3, k_4 be the vertices of $\Sigma_0(p^n)$ defined by

$$k_r = a^{r-1}(k_1) \quad (0 \leqq r \leqq 4).$$

It can be verified that k_0, k_1, k_2, k_3, k_4 are the vertices of a 4-arc in $\Sigma_0(p^n)$ and that

$$b^{r-1}(k_1) = k_r \quad (0 \leqq r \leqq 3),$$
$$b^4(k_1) \neq a^4(k_1).$$

Hence a and b are shunt automorphisms for this 4-arc. It follows from Proposition C that a and b generate a group of automorphisms of $\Sigma_0(p^n)$ which acts transitively on the 4-arcs. We shall denote this group by $H = \langle a, b \rangle$. The subgroup of H generated by the elements $a^{1-r} b^r a^{-1}$ $(1 \leqq r \leqq 4)$ fixes k_1; indeed it is just the octahedral subgroup described at the end of Section 2.

As motivation for the first theorem, let us remark that the smallest power of an odd prime p which is congruent to 1 modulo 8, and for which consequently, the sextet constructions works, is either p or p^2.

Theorem 1. *The components* $\Sigma_0(p^n)$ *satisfy*

$$\Sigma_0(p^n) = \begin{cases} \Sigma_0(p) & \text{if} \quad p \equiv 1 \pmod 8 \\ \Sigma_0(p^2) & \text{if} \quad p \equiv 3, 5, 7 \pmod 8). \end{cases}$$

Proof. The eighth root of unity σ in GF(p^n) can be chosen to lie in the subfield GF(p) or GF(p^2), according as p is or is not congruent to 1 modulo 8. The coefficients of a and b lie in this subfield, and the group $H = \langle a, b \rangle$ acts transitively on the vertices of $\Sigma_0(p^n)$. Since the vertex k_1 has elements which lie in the subfield, all vertices of $\Sigma_0(p^n)$ have this property, and the result follows. ▌

For any odd prime p we define the *sextet graph* $S(p)$ to be $\Sigma_0(p)$ or $\Sigma_0(p^2)$, according as p is or is not congruent to 1 modulo 8. In other words, $S(p)$ is a component of the graph $\Sigma(q)$, where $\mathrm{GF}(q)$ is the smallest field of characteristic p for which the sextet construction works.

In the following discussion it will be necessary to consider separately the congruence classes of p modulo 16; we shall use the terminology *Case n* to refer to the case when $p\equiv n \pmod{16}$. The following table may be useful.

Table 1

p (mod 16) Case number	1	3	5	7	9	11	13	15
p^2 (mod 16)	1	9	9	1	1	9	9	1
$S(p)$	$\Sigma_0(p)$	$\Sigma_0(p^2)$			$\Sigma_0(p)$	$\Sigma_0(p^2)$		

By virtue of the remarks about the coefficients of a and b contained in the proof of Theorem 1, the group $H=\langle a, b\rangle$ is a subgroup of $\mathrm{PGL}(2, p)$ in the Cases 1 and 9 and a subgroup of $\mathrm{PGL}(2, p^2)$ in the other cases.

For any odd prime power q, $\mathrm{PGL}(2, q)$ has a subgroup $\mathrm{PSL}(2, q)$ consisting of those projective linear transformations $t\mapsto(\alpha t+\beta)/(\gamma t+\delta)$ for which $\alpha\delta-\beta\gamma$ is a non-zero square in $\mathrm{GF}(q)$. Since the matrices M and kM induce the same projective linear transformation, a member of $\mathrm{PSL}(2, q)$ can be induced by a matrix of determinant 1. Conversely, a matrix whose determinant is any non-zero square induces a member of $\mathrm{PSL}(2, q)$. We have:

$$\det A = 2\sigma, \quad \det B = -2\sigma;$$

and when $q\equiv 1 \pmod 8$ both 2 and -2 are squares $(\sqrt{2}=\sigma+\sigma^{-1},\ \sqrt{-2}=\sigma-\sigma^{-1})$. However σ itself is a square if $q\equiv 1 \pmod{16}$ but not if $q\equiv 9 \pmod{16}$. It follows that $H=\langle a, b\rangle$ is a subgroup of:

$\mathrm{PSL}(2, p)$ in Case 1,
$\mathrm{PSL}(2, p^2)$ in Case 7 and 15,
$\mathrm{PGL}(2, p)$ in Case 9,
$\mathrm{PGL}(2, p^2)$ in Cases 3, 5, 11, 13.

In order to determine H precisely we shall require the list of subgroups of $\mathrm{PSL}(2, q)$. Fortunately, this has been known since the time of L. Dickson: modern treatments are given by Huppert [6] and Suzuki [7].

Proposition E. *If p is an odd prime, then a subgroup of* $\mathrm{PSL}(2, p^n)$ *is isomorphic to one of the following groups.*

(i) *The dihedral groups of order $p^n\pm 1$ and their subgroups.*
(ii) *The semidirect product of an elementary abelian p-group with a (possibly trivial) cyclic group.*
(iii) A_4, S_4, or A_5.
(iv) $\mathrm{PSL}(2, r)$ *or* $\mathrm{PGL}(2, r)$ *where $r=p^m$ divides p^n.*

We remark that no subgroup isomorphic to $S_4 \times \mathbf{Z}_2$ occurs. It is also true that there are no such subgroups of $\mathrm{PGL}(2, p^n)$, since this group itself does occur as a subgroup of $\mathrm{PSL}(2, p^{2n})$ [7, p. 414]. So we have immediately:

Theorem 2. *In all cases* $H=\langle a, b\rangle$ *acts 4-regularly on* $S(p)$.

Proof. We have seen that H acts transitively on the 4-arcs, so that it is either 4-regular or 5-regular. Also H is a subgroup of a PSL or PGL group and so it cannot contain the subgroups of type $S_4 \times \mathbf{Z}_2$ required as the vertex-stabilisers in the 5-regular case. Thus H is 4-regular. ▮

Recalling the remarks following Proposition C, we see that the determination of the order n of $S(p)$ now depends on the order of H: we must have $n=|H|/24$. To find $|H|$ we return to Proposition E, and its useful corollary that a subgroup of $\mathrm{PSL}(2, p^n)$ which strictly contains an S_4 subgroup must be of type (iv).

Theorem 3_1. *In Case 1,* $H=\mathrm{PSL}(2, p)$.

Proof. We know that H contains the S_4 subgroup fixing the vertex k_1, and the element a which does not fix k_1. Hence, by Proposition E, $H=\mathrm{PSL}(2, p)$. ▮

Theorem 3_9. *In Case 9,* $H=\mathrm{PGL}(2, p)$.

Proof. The generators of the stabilizer of k_1 are induced by matrices with square determinants, and so they belong to $H \cap \mathrm{PSL}(2, p)$. The element a^2 also belongs to $H \cap \mathrm{PSL}(2, p)$ and it is not in the stabilizer of k_1, so $H \cap \mathrm{PSL}(2, p)=\mathrm{PSL}(2, p)$. Since H contains the element a not in $\mathrm{PSL}(2, p)$ we must have $H=\mathrm{PGL}(2, p)$. ▮

Theorem 3_{15}. *In Case 15,* $H \approx \mathrm{PSL}(2, p)$.

Proof. Since $p^2 \equiv 1 \pmod{16}$ in this case, we can choose a primitive 16th root of unity τ in $\mathrm{GF}(p^2)$ and put $\sigma=\tau^2$. The matrix $A_0=(\tau\sqrt{2})^{-1}A$ induces the automorphism a, and it has the properties

$$\det A_0 = 1, \quad A_0 A_0^* = I,$$

where A_0^* is the transposed conjugate of A_0 with respect to the field automorphism $x \mapsto x^p$ of $\mathrm{GF}(p^2)$. In other words A_0 belongs to the special unitary group $\mathrm{SU}(2, p^2)$. The same is true for $B_0=(\tau\sqrt{2})^{-1}B$, and so $H=\langle a, b\rangle$ is a subgroup of $\mathrm{PSU}(2, p^2)$. But it is known (see [7, p. 410]) that $\mathrm{PSU}(2, p^2) \approx \mathrm{PSL}(2, p)$. Hence the argument given for Case 1 can be repeated, and $H \approx \mathrm{PSL}(2, p)$. ▮

Theorem 3_7. *In Case 7,* $H \approx \mathrm{PGL}(2, p)$.

Proof. In this case we cannot normalize A so that it is both special and unitary—this is because $\tau^{p+1}=\tau^8=-1$ when $p \equiv 7 \pmod{16}$, whereas $\tau^{p+1}=\tau^{16}=1$ when $p \equiv 15 \pmod{16}$. So we must proceed rather differently.

Let H_1 denote the stabilizer of k_1 and let $K=\langle H_1, a^2, b^2\rangle$. We have seen that H_1 is generated by the elements $a^{1-r}b^r a^{-1}$ $(1 \leq r \leq 4)$, or by the transformations $t \mapsto -1/t$, $t \mapsto it$, $t \mapsto (1-t)/(1+t)$. We can choose matrices representing the transformations as follows:

$$\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \quad \begin{bmatrix} \sigma & 0 \\ 0 & \sigma^{-1} \end{bmatrix}, \quad \begin{bmatrix} -i/\sqrt{2} & i/\sqrt{2} \\ i/\sqrt{2} & i/\sqrt{2} \end{bmatrix},$$

which all belong to $SU(2, p^2)$. Also a^2 and b^2 are induced by the matrices $(2\sigma)^{-1}A^2$, $(-2\sigma)^{-1}B^2$, which belong to $SU(2, p^2)$. Thus, as before, we have $K = PSU(2, p^2) \approx \approx PSL(2, p)$.

Now, for each generator $a^{1-r}b^r a^{-1}$, a^2, b^2 of K the result of conjugating by a is also in K; that is $aKa^{-1} \subseteq K$, or $aK \equiv Ka$. Similarly $bK = Kb$, and since $ba^{-1} \in K$ we must have $aK = bK = Kb = Ka$. It follows that there are just two cosets of K in H, and from Proposition E we deduce that $H \approx PGL(2, p)$. ▮

It must be remarked that in Cases 7 and 15 the group H is not a 'canonical' subgroup $PGL(2, p)$ or $PSL(2, p)$ of $PGL(2, p^2)$: the coefficients of the generators do not lie in $GF(p)$.

Theorem $3_{3,5,11,13}$. *In Case* 3, 5, 11, 13, $H = PGL(2, p^2)$.

Proof. Let $H_0 = H \cap PSL(2, p^2)$. By the usual arguments, the stabilizer of k_1 and th element a^2 belong to H_0, so H_0 is a subgroup of $PSL(2, p^2)$ strictly containing an S_4 subgroup. It follows from Proposition E that H_0 is isomorphic to one of $PSL(2, p)$, $PGL(2, p)$, $PSL(2, p^2)$.

Since it is known [6] that $PSL(2, p)$ contains an S_4 subgroup if and only if $q^2 \equiv 1 \pmod{16}$, it follows that H_0 is not isomorphic to $PSL(2, p)$. If $H_0 \approx PGL(2, p)$ then, since it has index 2 in H, and consequently is normal, and since $PGL(2, p)$ has no outer automorphisms, we must have H isomorphic to $PGL(2, p) \times \mathbf{Z}_2$. A Sylow-2-subgroup S of H is isomorphic to $D_8 \times \mathbf{Z}_2$, and this is the stabilizer of some edge $\{x, y\}$. Since we know that the stabilizer of the 1-arc (x, y) is D_8, there is an automorphism in S which switches x and y and commutes with this D_8. It follows that for some 3-arc (w, x, y, z) we have $H(w, x, y) = H(x, y, z)$, or $H(w, x, y, z) = = H(w, x, y)$, which is impossible (by Proposition A).

Hence $H_0 = PSL(2, p^2)$, and since H contains a, which is not in $PSL(2, p^2)$, $H = PGL(2, p^2)$. (The authors are extremely grateful to the referee for suggesting this simplification of their original proof.) ▮

We can now list the orders of the sextet graphs in all cases. Roughly speaking, in Cases 1 and 9 the construction of $S(p)$ takes place in $GF(p)$ and the graph has the "appropriate" size, while in Cases 3, 5, 11, 13 the construction takes place in $GF(p^2)$ and $S(p)$ again has the appropriate size. However, in Cases 7 and 15 the construction takes place in $GF(p^2)$ but the graph has the size appropriate to a construction in $GF(p)$.

We may also remark that in the cases when H is a PGL group it has a PSL subgroup of index 2, and the orbits of the latter group form a bipartition of $S(p)$.

In those Cases (3, 5, 7, 11, 13, 15) when the construction takes place in $GF(p^2)$ it is reasonable to enquire about the action of the non-trivial field automorphism $\varphi : t \mapsto t^p$ on $S(p)$. If we extend the field automorphism to the projective line by setting $\varphi(\infty) = \infty$, and adjoin φ to the group $PGL(2, p^2)$ we obtain the group usually denoted by $P\Gamma L(2, p^2)$. Since $\varphi(-1) = (-1)^p = -1$ the cross-ratio of a quartet is preserved by φ, and φ induces a permutation of the sextets. Moreover, if j is an involution in $PGL(2, p^2)$ in which α_1, α_2 and β_1, β_2 are corresponding pairs, then $j' = \varphi j \varphi^{-1}$

Table 2

Case	Order of $S(p)$	Bipartite?
1	$p(p^2-1)/48$	No
3, 5, 11, 13	$p^2(p^4-1)/24$	Yes
7	$p(p^2-1)/24$	Yes
9	$p(p^2-1)/24$	Yes
15	$p(p^2-1)/48$	No

is the involution in which $\alpha_1^\varphi, \alpha_2^\varphi$ and $\beta_1^\varphi, \beta_2^\varphi$ are corresponding pairs. Also, if γ_1, γ_2 are the fixed points of j, then $\gamma_1^\varphi, \gamma_2^\varphi$ are the fixed points of j'. Hence φ preserves adjacency in the sextet graph $S(p)$, and $\mathrm{P}\Gamma\mathrm{L}(2, p^2)$ acts as a group of automorphisms of $S(p)$.

In the Cases 7 and 15 it can be verified that φ induces the same automorphism of $S(p)$ as the projective linear transformation $t \mapsto -1/t$. In other words, $\mathrm{P}\Gamma\mathrm{L}(2, p^2)$ does not act faithfully on $S(p)$, and we obtain no new information about the graphs. However, in the other cases φ induces a new automorphism.

Theorem 4. *In Cases 3, 5, 11, 13 the group* $\mathrm{P}\Gamma\mathrm{L}(2, p^2)$ *acts 5-regularly on* $S(p)$.

Proof. Consider the 3-arc (k_0, k_1, k_2, k_3) where k_1 is the sextet $\{0\ \infty | 1\ -1 | i\ -i\}$ and $k_i = a^{i-1}(k_1)$ as usual. If a duet is fixed by an automorphism then that automorphism must either fix or switch the two adjacent sextets having the duet in common. Now φ fixes the duets $\{0, \infty\}$, $\{i, -i\}$, $\{1+\sqrt{2}, 1-\sqrt{2}\}$ which are common to k_0 and k_1, k_1 and k_2, k_2 and k_3 respectively. Thus φ fixes the 3-arc pointwise.

The duet $\{\sigma, -\sigma\}$ is fixed by φ if $p \equiv 5 \pmod 8$ but not if $p \equiv 3 \pmod 8$; however the reverse is true for the duet $\{(3i\sqrt{2}-1)^{-1}, (1-i\sqrt{2})^{-1}\}$. The former duet is common to k_0 and $k_{-1} = a^{-2}(k_1)$, while the latter is common to k_3 and $k_4 = a^3(k_1)$. Thus in both cases φ fixed a 4-arc. But we have shown that $\mathrm{PGL}(2, p^2)$ acts 4-regularly, and so it contains only one automorphism (the identity) fixing a 4-arc. It follows that φ induces a new automorphism, and $\mathrm{P}\Gamma\mathrm{L}(2, p^2)$ acts 5-regularly. ▌

Wong [10] showed that there is only one cubic graph which admits a group acting 5-regularly and primitively. It has 234 vertices and the group is Aut SL(3, 3); an alternative construction may be found in [1, p. 125]. Other constructions of 5-regular cubic graphs are due to Conway (see [1, p. 130]) and Biggs [2]. In both constructions the graphs are coverings of smaller graphs, and so the groups act imprimitively in a corresponding way. However, the groups of the 5-regular sextet graphs act imprimitively in only one, essentially trivial, way, corresponding to the bipartition of the graph. This situation has been called the *semi-primitive* case by Gardiner [5]. We conjecture that the only 5-regular semi-primitive cubic graphs are the sextet graphs $S(p)$ for $p \equiv 3, 5, 11, 13 \pmod{16}$ and an exceptional graph on 468 vertices (a bipartite double cover of Wong's graph).

5. Girth of sextet graphs

In this section we shall prove a result on the girth of $S(p)$ which lends support to the conjecture that the girth tends to infinity as a function of p. We shall use the correspondence, established in Section 2, between the cycles of length l in $S(p)$ and the identity words of length l in the shunt automorphisms a and b.

For simplicity we shall consider only Cases 1 and 9. Thus p will be a prime congruent to 1 modulo 8, and there is a primitive eighth root of unity σ in $\mathbf{Z}_p=\mathrm{GF}(p)$. We shall fix σ for each p.

Let

$$A(t)=\begin{bmatrix} t & -t \\ 1 & 1 \end{bmatrix}, \quad B(t)=\begin{bmatrix} t & t \\ 1 & -1 \end{bmatrix},$$

be elements of the ring R of 2×2 matrices whose terms belong to $\mathbf{Z}[t]$. Let W denote the set of words in two non-commuting variables. For each w in W the matrix

$$w(t)=w(A(t), B(t))=\begin{bmatrix} \alpha_w(t) & \beta_w(t) \\ \gamma_w(t) & \delta_w(t) \end{bmatrix}$$

belongs to the ring R. If w has length l, then $\alpha_w(t)$ and $\beta_w(t)$ are polynomials of degree l, whereas $\gamma_w(t)$ and $\delta_w(t)$ have degree $l-1$. The leading coefficients are all ± 1.

Let $\bar{w}(t)$ denote the matrix $w(t)$ when the coefficients of the polynomials are reduced modulo p; that is, the corresponding polynomials $\bar{\alpha}_w(t)$, $\bar{\beta}_w(t)$, $\bar{\gamma}_w(t)$, $\bar{\delta}_w(t)$ belong to $\mathbf{Z}_p[t]$. The chain $w\to w(t)\to \bar{w}(t)\to \bar{w}(\sigma)$ defines a function from W to $\mathrm{GL}(2, p)$. If we now take the projective linear transformation induced by the matrix by the matrix $\bar{w}(\sigma)$ we have a function

$$e_p\colon W\to \mathrm{PGL}(2, p).$$

The image of the word $w_1(\xi, \eta)=\xi$ is the automorphism a of $S(p)$ and the image of $w_2(\xi, \eta)=\eta$ is b. In general, the value of $e_p(w)$ is the automorphism $w(a, b)$ of $S(p)$.

The following lemma is an immediate corollary of the results in Section 2.

Lemma 4. *$S(p)$ has a cycle of length l if and only if there is a word w of length l for which $e_p(w)=id$, the identity in* $\mathrm{PGL}(2, p)$. ▮

Lemma 5. *Suppose w is a given member of W. If $e_p(w)=id$ for infinitely many primes p, then $e_p(w)=id$ for all p.*

Proof. If $e_p(w)$ is the identity then $\bar{w}(\sigma)$ is a matrix cI, for some c in $\mathbf{Z}_p$. In particular, the polynomial $\bar{\beta}_w(t)$ vanishes when $t=\sigma$. Since $\sigma^4+1=0$ in $\mathbf{Z}_p$, we may say that the polynomials $\bar{\beta}_w(t)$ and t^4+1 have a non-trivial common factor in $\mathbf{Z}_p[t]$. The resultant matrix (see [9]) of these polynomials is a matrix $M_p[w]$ over $\mathbf{Z}_p$ with $l+4$ rows and columns, where l is the length of w. The determinant of $M_p(w)$ vanishes in $\mathbf{Z}_p$ if and only if the polynomials have a non-trivial common factor.

Let $M(w)$ denote the resultant matrix of the polynomials $\beta_w(t)$ and t^4+1 over $\mathbf{Z}$. Then

$$\det M(w)\equiv 0 \pmod{p} \Leftrightarrow \det M_p(w)=0 \quad \text{in} \quad \mathbf{Z}_p.$$

Now if det $M(w) \neq 0$ then it is divisible by only a finite number of primes, Hence, if $e_p(w)$ is the identity for infinitely many primes p, we must have det $M(w)=0$. Consequently det $M_p(w)=0$ for all primes p and $e_p(w)=\mathrm{id}$ for all p. ▌

Theorem 5. *Suppose* $p \equiv 1 \pmod 8$. *Then either*

(i) *there is a "universal" word u such that $e_p(u)=\mathrm{id}$ for all such p, or*
(ii) *the girth of $S(p)$ tends to infinity with p.*

Proof. Suppose that the first alternative does not hold. Then every word w has the property that $e_p(w) \neq \mathrm{id}$ for some p. It follows from Lemma 5 that $e_p(w)=\mathrm{id}$ for only finitely many p. Let $p(w)$ be the largest $p \equiv 1 \pmod 8$ such that $e_p(w)=\mathrm{id}$ (and define $p(w)=1$ if there is no such p). Let

$$p(l) = \max \{p(w) | w \text{ has length } \leqq l\},$$

which is finite since the set of words with length at most l is finite. It follows from Lemma 4 that if $p > p(l)$ then the girth of $S(p)$ is greater than l. ▌

It is hard to believe in the existence of the universal word u. Certainly, it cannot have odd length, since the graphs $S(p)$ are bipartite when $p \equiv 9 \pmod{16}$ and have no odd cycles. Also it must have length at least 30, since $S(313)$ has girth 30.

In Table 3 we tabulate the girths of the sextet graphs $S(p)$ with $p \equiv 1 \pmod 8$ and $p<500$. These values were obtained by explicit computation of the shortest cycle through a specified vertex. The value for $p=433$ is unknown, but it does not exceed 32, since the word $(ab^3a^2baba^6b)^2$ is an identity word in that case. We also give the values of $c=(\log_2 n)/g$, where n is the number of vertices of $S(p)$, that is, $n=p(p^2-1)/48$ or $p(p^2-1)/24$ according as p is congruent to 1 or 9 modulo 16. General theorems [3, pp. 107—110] assert that there is a cubic graph with girth g and $1/2<c<1$ for each g, but no better bounds are known. It is tempting to conjecture that the asymptotic value of c for the sextet graphs is strictly less than 1, but the evidence for this is not wholly convincing. The values of c marked with a star in Table 1 are those for which $S(p)$ is the smallest currently known graph with that girth.

Table 3

p	17	41	73	89	97	113	193	233	241	257	281	313	337	353	401	409	433	449	457
g	9	14	22	22	20	21	25	28	25	25	28	30	27	27	30	30	?	27	30
c	.741	.821	.635*	.674	.711	.708*	.688*	.678*	.826	.737	.707	.676*	.726	.733	.678	.714	?	.772	.722

Table 4

p	3	7	31	71	151
g	8	6	15	20	26
c	.613*	.634*	.618*	.693*	.659*

In Table 4 we give a few results for the sextet graphs with $p \not\equiv 1$ (mod 8). In all the cases listed there the graphs are the smallest currently known with the stated girth.

Note added in proof. A. Weiss has shown that the asymptotic value of c for the sextet graphs with $p \not\equiv \pm 1$ (mod 16) is 3/4.

References

[1] N. L. Biggs, *Algebraic Graph Theory*, Cambridge, 1974.

[2] N. L. Biggs, Constructing 5-arc-transitive cubic graphs. *J. London Math. Soc.* **26** (1982) 193—200.

[3] B. Bollobás, *Extremal Graph Theory*, Academic Press, 1978.

[4] D. Z. Djokovic and G. L. Miller, Regular groups of automorphisms of cubis graphs, *J. Combinatorial Theory (B)* **29** (1980) 195—230.

[5] A. D. Gardiner, Arc transitivity in graphs III, *Quart. J. Math. Oxford (2)* **27** (1976) 313—323.

[6] B. Huppert, *Endliche Gruppen I*, Springer, 1967.

[7] M. Suzuki, *Group Theory I*, Springer, 1982.

[8] W. T. Tutte, A family of cubical graphs, *Proc. Cambridge Philos. Soc.* **43** (1947) 459—474.

[9] B. L. Van der Waerden, *Algebra, vol.* **1**., Ungar—New York, (1970).

[10] W. J. Wong, Determination of a class of primitive permutation groups *Math. Z.* **99** (1967) 235—246.

N. L. Biggs
M. J. Hoare

Royal Holloway College
Egham, Surrey TW20 OEX, U.K.