Geometrical Combinatorics (eds. F.C. Holroyd and R.J. Wilson). London: Pitman, 1984.

N L BIGGS AND JOHN SHAWE-TAYLOR

1 Rotations and graphs with large girth

1. A THEOREM ABOUT ROTATIONS

Consider a triad of mutually orthogonal axes in 3-dimensional Euclidean space. The axes are composed of 6 unit vectors meeting at the origin and can be viewed as an unordered triple of unordered pairs of opposite vertices on the unit sphere. As they are unlabelled a rotation of $\pi/2$ about any one of the axes takes the triad to itself. We define a move on such a triad to be a rotation of $\pi/4$ about the current location of one of its axes. We call a sequence of moves simple if no move of the sequence is the same as the previous move. We now state the main result of this paper.

Theorem Given a simple sequence of moves $M_1, M_2, \ldots, M_k$, the only simple sequence which will regain initial position is the reverse sequence of moves $M_k, M_{k-1}, \ldots, M_2, M_1$.

This theorem may be viewed as a theorem about graphs if we consider the graph obtained by taking the triad positions as vertices and the moves as edges joining two positions. Clearly this graph is cubic and the theorem states that its components are infinite cubic trees. As there are uncountably many triads of axes, the graph will certainly have uncountably many components.

In order to prove the theorem we turn to the algebraic theory of sextets and sextet graphs. In Section 2 we introduce sextets and sextet graphs over a field with eighth roots of unity. In Section 3 the sextet graphs over finite fields as introduced by Biggs and Hoare [1] are considered. Results concerning the girth of these graphs are covered in Section 4. In Section 5 we state the correspondence between sextets and the triads of axes introduced above. This relation enables us to prove the theorem.

2. ALGEBRAIC THEORY OF SEXTETS

Let F be a field containing eighth roots of unity. The projective line over F, PG(1,F), may be considered as the set $L = F \cup \{\infty\}$, with the usual conventions about ∞. We shall call an unordered pair of distinct points {a,b} on L a duet, while a quartet is an unordered pair of duets whose cross-ratio is −1. Thus {{a,b},{c,d}}, or just {ab|cd} for short, is a quartet if and only if

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

A sextet is an unordered triple of duets, denoted by {ab|cd|ef}, such that {ab|cd}, {cd|ef} and {ef|ab} are all quartets.

Let σ be a primitive eighth root of unity in F and $i = \sigma^2$. Hence $i^2 = \sigma^4 = -1$; then $\{0\ \infty|1\ -1|i\ -i\}$ is an example of a sextet of L.

Sextets have appeared in the works of classical geometers, among others, Enriques and Edge [5]. They are sometimes referred to as 'regular sextuples'.

The group PGL(2,F) of projective linear transformations of the form

$$u \longrightarrow \frac{au+b}{cu+d} \quad (a,b,c,d \in F,\ ad-bc \neq 0)$$

can be considered to act on L with the usual conventions about ∞. This group acts sharply 3-transitively on L and maps sextets to sextets as it preserves the cross-ratio.

It is not hard to see that the points $0,\infty,1$ uniquely determine a sextet $\{0\ \infty|1\ -1|i\ -i\}$. Thus given any sextet $\{a_1\ a_2|a_3\ a_4|a_5\ a_6\}$ we can, by choosing the unique $g \in PGL(2,F)$ which maps a_1,a_2,a_3 to $0,\infty,1$ respectively, make g map the second sextet to the first. Hence PGL(2,F) acts transitively on sextets.

Proposition Let Q be a quartet over the field F containing a primitive eighth root of unity σ, and $T = \{a_1\ b_1|a_2\ b_2\}$ one of the three possible pairings of the elements of Q, so not necessarily a quartet. Then T determines an involution j_T of PGL(2,F) which maps a_i to b_i, i=1,2, and this involution has two distinct fixed points.

Proof Since PGL(2,F) preserves cross-ratio and acts transitively on quartets it is sufficient to consider the case when $Q = \{0\ \infty|1\ -1\}$. The three possible pairings of Q are Q itself, $R = \{0\ 1|\infty\ -1\}$ and $S = \{0\ -1|\infty\ 1\}$. The involution j_Q is $u \longrightarrow -1/u$. Its fixed points satisfy $u^2 + 1 = 0$ and so are i and −i. The involution j_R is $u \longrightarrow (1-u)/(1+u)$, so that its fixed points satisfy $u^2+2u-1 = 0$ or $u = -1\pm\sqrt{2}$. The involution j_S is $u \longrightarrow (u+1)/(u-1)$ with fixed points $u = 1\pm\sqrt{2}$. Since $\sqrt{2} = \sigma + \sigma^{-1}$, the two distinct fixed points of j_Q, j_R and j_S all lie in F.∎

We are now in a position to define the sextet graph, S(F), over F. The vertices of S(F) are the sextets of PG(1,F). We define two sextets,

$\{a_1\ a_2|b_1\ b_2|c_1\ c_2\}$ and $\{a_1\ a_2|b_1'\ b_2'|c_1'\ c_2'\}$,

to be adjacent in S(F) if b_1', b_2' are the fixed points of j_R and c_1', c_2' are the fixed points of j_S, where

$R = \{b_1\ c_1|b_2\ c_2\}$ and $S = \{b_1\ c_2|b_2\ c_1\}$.

For example $\{0\ \infty|1\ -1|i\ -i\}$ is adjacent to $\{0\ \infty|\sigma\ -\sigma|\sigma^3\ -\sigma^3\}$ as $\sigma,-\sigma$ are the fixed points of the involution taking $1,-i$ to $i,-1$, respectively, while $\sigma^3,-\sigma^3$ are the fixed points of the involution taking $1,i$ to $-i,-1$, and $\{0\ \infty|\sigma\ -\sigma|\sigma^3\ -\sigma^3\}$ is indeed a sextet.

<u>Proposition</u> If $g \in PGL(2,F)$ and a_1, a_2 are the fixed points of j_R then ga_1, ga_2 are the fixed points of $gj_Rg^{-1} = j_{gR}$. Hence PGL(2,F) acts as a group of automorphisms on the graph S(F). ∎

In fact we shall see in Section 4 that the action of PGL(2,F) is faithful on each component of S(F). By mapping $0,\infty,1$ to $1,-1,i$, respectively, and $0,\infty,1$ to $i,-i,1$, respectively, we obtain two more distinct neighbours of $\{0\ \infty|1\ -1|i\ -i\}$ as the two images of $\{0\ \infty|\sigma\ -\sigma|\sigma^3\ -\sigma^3\}$. Since PGL(2,F) acts transitively on sextets the graph is cubic, and by mapping $0,\infty,1$ to $0,\infty,\sigma$ we see that the definition of adjacency is in fact symmetric.

3. SEXTET GRAPHS OVER FINITE FIELDS

In this section we state briefly the results of Biggs and Hoare [1]. They consider the case of a sextet graph S(F) where F is a finite field GF(q), $g = p^n$. In this case, components of S(F) are isomorphic for all powers of p for which $S(GF(p^n))$ exists. This leads to the definition of the sextet graph S(p) of a prime p:

$$S(p) := \begin{cases} S_0(GF(p)), & p \equiv 1 \pmod 8 \\ S_0(GF(p^2)), & p \equiv 3,5,7 \pmod 8, \end{cases}$$

where $S_0(F)$ is the component of S(F) containing the sextet $\{0\ \infty|1\ -1|i\ -i\}$. Note that the square of p is necessary in the cases $p \equiv 3,5,7 \pmod 8$ in order to guarantee eighth roots of unity in the field.

The order of S(p) for various classes of p (mod 16) and a note as to whether the graph is bipartite or not is presented in Table 1.

p (mod 16)	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

Table 1

As examples of these sextet graphs we consider three primes 7,3,17.

Example 1 (p=7) In this case S(7) is a component of the graph S(GF(49)), which has 4900 sextets and 350 components each of order $|S(7)| = 14$. The graph has girth 6 and is isomorphic to the graph of points and lines of PG(2,2). It is often called Heawood's graph and is in fact 4-arc transitive.

Example 2 (p=3) In this case S(3) is the only component of S(GF(9)), a graph with 30 vertices. The graph is 5-arc transitive and has girth 8. Its vertices can be represented by the partitions into pairs of 6 elements together with the pairs of the elements. Two vertices are adjacent if they represent a pair and a partition containing that pair (Tutte's 8-cage graph).

Example 3 (p=17) In this case S(17) is a component of S(GF(17)). The latter graph has 204 vertices and two components so that $|S(17)| = 102$. S(17) is 4-arc transitive and has girth 9. It is one of the four cubic graphs which are primitive and distance-transitive [2].

4. SYMMETRY AND GIRTH OF SEXTET GRAPHS

Consider the graph S(F) for some field F with an eighth root of unity σ. The maps

$$u \mapsto \frac{\sigma(u-1)}{u+1} \quad \text{and} \quad u \mapsto \frac{\sigma(u+1)}{u-1}$$

are both projective linear transformations and so automorphisms of S(F). We denote them by a and b respectively. The following sequence of vertices is obtained by taking $k_1 = \{0\ \infty | 1\ -1 | i\ -i\}$ and setting

$k_r = a^{r-1}(k_1) = b^{r-1}(k_1)$, $0 \leq r \leq 4$:

$$k_0 = \{1\ -1|-\sigma^3-i-\sigma\ \sigma^3-i+\sigma|\sigma^3+i+\sigma\ -\sigma^3+i-\sigma\}$$
$$k_1 = \{0\ \infty|1\ -1|i\ -i\}$$
$$k_2 = \{0\ \infty|\sigma\ -\sigma|\sigma^3\ -\sigma^3\}$$
$$k_3 = \{-\sigma^3-i+1\ -\sigma^3+i-1|\sigma\ -\sigma|\sigma^3+i-1\ \sigma^3-i+1\}$$
$$k_4 = \{\sigma^3+i+1\ (-\sigma^3-i-1)/3|-\sigma^3-i+1\ -\sigma^3+i-1|\sigma^3-i-1\ (-\sigma^3+i+1)/3\}.$$

As we saw in Section 2, k_1 and k_2 are adjacent and so k_0,k_1,k_2,k_3,k_4 is a 4-arc of S(F). The automorphism a shunts this 4-arc onto one of its successors, while b shunts it onto the other. Hence a and b generate a subgroup H of the automorphism group of S(F) which is 4-arc transitive. Note also that $H \subseteq PGL(2,F)$.

Suppose $e(\neq 1) \in PGL(2,F)$ fixes the 4-arc k_0,k_1,k_2,k_3,k_4. It must then stabilise the duets $\{1\ -1\}$, $\{0\ \infty\}$ and $\{\sigma\ -\sigma\}$ (and indeed $\{-\sigma^3-i+1\ -\sigma^3+i-1\}$ as well). If more than one pair is fixed pointwise then e is the identity. In the case when only $\{0\ \infty\}$ is fixed pointwise, -1 maps to 1, and e is the transformation $u \longrightarrow -u$, which does not fix k_4. So 0 and ∞ must be interchanged by e, and e has the form $u \longrightarrow b/u$, for some $b \in F$. In order for $\{1\ -1\}$ to be stabilised $b = 1$ or -1, while for $\{\sigma\ -\sigma\}$ to be stabilised $b = i$ or $-i$. Hence e cannot be chosen to fix the 4-arc k_0,k_1,k_2,k_3,k_4 and H acts regularly on the 4-arcs. This also implies that PGL(2,F) acts faithfully on $S_0(F)$, and so on each component of S(F); for if g is a non-trivial element which fixes some component S_1 and h maps S_1 to $S_0(F)$, then hgh^{-1} is a non-trivial element fixing $S_0(F)$.

We define a <u>word</u> of length ℓ in two non-commuting variables x and y to be a string of ℓ symbols $w = w_1\ w_2\ \dots\ w_\ell$ where w_i is either x or y. If x and y are members of a monoid M then w(x,y) is also in M.

<u>Proposition</u> Let H be a group of automorphisms acting s-regularly on a graph G with H generated by two shunt automorphisms with respect to some s-arc. Then G has girth g if and only if the shortest word w such that w(a,b) is the identity in H has length g. ∎

This proposition allows us to investigate the girth of an s-regular graph by examining words in its generating automorphisms. Some values of g for various S(p) graphs are tabulated in Table 2. The third column of the table is the value of $c = (\log_2 n)/g$, where n is the number of vertices of S(p).

p	g	$c = (\log_2 n)/g$
3	8	0.613
7	6	0.634
17	9	0.741
31	15	0.618
73	22	0.635
193	25	0.688
233	28	0.678
313	30	0.676

Table 2

The significance of c stems from two known bounds on this parameter for cubic graphs [3]. The first is the trivial lower bound $c > \frac{1}{2}$ for all cubic graphs. The second is given by a general construction of a family of cubic graphs with large girth and gives c as approximately 1 for this family. For many years this was the best general construction for cubic graphs with large girth, but recently Weiss [6] has shown that the sextet graphs give a better value of c.

Theorem [6] Let n be the order and g the girth of the sextet graph S(p). If $p \equiv \pm 3, \pm 5, \pm 7 \pmod{16}$, then

$$\log_2 n \leq 3g/4 + 3/2. \blacksquare$$

Hence Weiss's theorem shows that for infinitely many values of g there is a cubic graph with $c \leq 3/4 + 3/(2g)$, a significant improvement of the value of 1 previously obtained. For our present purposes we need only the obvious corollary that, given any g_0, there is a prime p_0 such that the girth of $S(p_0)$ is at least g_0.

5. TRIADS OF AXES AGAIN

In this section we consider sextet graphs when the field of Section 2 is the complex field $\mathbb{C}$. In this case $L = PG(1,\mathbb{C}) = \mathbb{C} \cup \{\infty\}$, and the points of the projective line can be considered as points on the unit sphere in 3-dimensional Euclidean space. If the cross-ratio of two duets is -1, then the chords joining the two pairs are at an angle of $\pi/2$. So a triad of axes is certainly a sextet. However, not all sextets are triads of axes as the example $\{0\ \infty | 2\ -2 | 2i\ -2i\}$ indicates. In order for a sextet to be a triad of axes its duets must be composed of antipodal points on the sphere; that is, each duet must be of the form $\{z, -1/\bar{z}\}$. We shall show that the component S_0 of $S(\mathbf{C})$ containing the sextet $\{0\ \infty | 1\ -1 | i\ -i\}$ is composed of sextets which are triads of axes, and that adjacency in S_0 corresponds to the rotations described in Section 1. Let θ be the complex number $e^{i\pi/4}$, and let a' and b' denote the automorphisms a and b of Section 4 with σ replaced by θ. Then we have

$$a'(u) = \frac{(1+\bar{\theta})}{(1+\bar{\theta})} a'(u) = \frac{(1+\theta)u - (1+\theta)}{(1+\bar{\theta})u + (1+\bar{\theta})},$$

and hence a' can be represented by the matrix

$$A = \begin{bmatrix} 1+\theta & -(1+\theta) \\ 1+\bar{\theta} & 1+\bar{\theta} \end{bmatrix}.$$

Similarly b' can be represented by the matrix

$$B = \begin{bmatrix} \bar{\theta}-i & \bar{\theta}-i \\ -(\theta+i) & \theta+i \end{bmatrix}.$$

Both of these matrices have the form

$$\begin{bmatrix} x & -y \\ \bar{y} & \bar{x} \end{bmatrix}$$

and so represent rotations (this result goes back to Cayley [4]). Since the composition of two rotations is a rotation, $H = \langle a', b' \rangle$ is a group of rotations. Clearly rotations map antipodal points to antipodal points and so preserve triads of axes. Since the group H acts transitively on the sextets in the component S_0 all these sextets are triads of axes.

Observe that the sextet k_2 of Section 4 with σ replaced by θ is a sextet of L and can be obtained from k_1 by a $\pi/4$ rotation about the axis $0,\infty$. Let this rotation be denoted by r. Since H acts transitively on the 1-arcs of S_0, we can find an element e of H mapping the edge (k_1,k_2) to any other edge (ℓ_1,ℓ_2) of S_0. Then $ere^{-1}(\ell_1) = \ell_2$. But ere^{-1} is a rotation of $\pi/4$ about the axis $e(\{0,\infty\})$, which is one of the duets of ℓ_1. We conclude that adjacency in S_0 corresponds to rotation of a triad about one of its axes by an angle of $\pi/4$.

Hence the theorem of Section 1 reduces to showing that $S_0(\mathbf{C})$ is an infinite cubic tree.

Suppose this is not the case. By the Proposition of Section 4 there is a word w of finite length g such that w(a',b') is the identity in H. For any ring R let $M_2(R)$ denote the ring of 2×2 matrices with elements in R. Consider the matrices

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

which are elements of $M_2(\mathbb{Z}[t])$, where t is an indeterminate. Then $A(\theta)$ and $B(\theta)$ represent the projective linear transformations a' and b' respectively.

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

which is an element of $M_2(\mathbb{Z}[t])$, so that $\alpha_w(t)$, $\beta_w(t)$, $\gamma_w(t)$, $\delta_w(t)$ are polynomials in $\mathbb{Z}[t]$. If w(a',b') is the identity then $w(\theta)$ is a representation of the identity transformation. Hence $\alpha_w(\theta)-\delta_w(\theta) = 0$, $\beta_w(\theta) = 0$, $\gamma_w(\theta) = 0$. This means that t^4+1 divides each of these polynomials:

$$\begin{aligned} \alpha_w(t) - \delta_w(t) &= (t^4+1)q(t), \\ \beta_w(t) &= (t^4+1)r(t), \\ \gamma_w(t) &= (t^4+1)s(t), \end{aligned}$$

for some $q(t), r(t), s(t) \in \mathbb{Z}[t]$. For any $q(t) \in \mathbb{Z}[t]$, let $\tilde{q}(t)$ denote the polynomial q(t) with coefficients taken modulo p, for some fixed prime p. Then

$$\begin{aligned} \tilde{\alpha}_w(t) - \tilde{\delta}_w(t) &= (t^4+1)\tilde{q}(t), \\ \tilde{\beta}_w(t) &= (t^4+1)\tilde{r}(t), \\ \tilde{\gamma}_w(t) &= (t^4+1)\tilde{s}(t). \end{aligned}$$

Let F be a field of characteristic p with σ a primitive eighth root of unity in F, and consider the graph S(F). Let a and b be the transformations of Section 4 over the field F. Note that the following maps are homomorphisms.

$$M_2(\mathbb{Z}[t]) \xrightarrow{\text{mod } p} M_2(\mathbb{Z}_p[t]) \xrightarrow{t=\sigma} M_2(F)$$

This means that the transformation w(a,b) is represented by the matrix

$$\widetilde{w}(\sigma) = \begin{bmatrix} \widetilde{\alpha}_w(\sigma) & \widetilde{\beta}_w(\sigma) \\ \widetilde{\gamma}_w(\sigma) & \widetilde{\delta}_w(\sigma) \end{bmatrix} ,$$

as this is the product $w(A(\sigma),B(\sigma))$ in the ring $M_2(F)$. But substituting σ in our expressions we obtain

$$\widetilde{\alpha}_w(\sigma) - \widetilde{\delta}_w(\sigma) = 0,$$
$$\widetilde{\beta}_w(\sigma) = 0,$$
$$\widetilde{\gamma}_w(\sigma) = 0.$$

So the word $w(a,b)$ represents the identity in the field F. Hence for all primes p, S(p) has a cycle of length g. This contradicts the corollary to Weiss's theorem. We conclude that $S_0(\mathbb{C})$ is indeed an infinite cubic tree, and the theorem of Section 1 follows.

REFERENCES

1. N L Biggs and M J Hoare, The sextet construction for cubic graphs, Combinatorica 3 (1983), 153-165.

2. N L Biggs and D H Smith, On trivalent graphs, Bull. London Math. Soc. 3 (1971), 155-158; MR 44#3902.

3. B Bollobás, Extremal Graph Theory (London Math. Soc. Monograph No. 11), Academic Press, 1978; MR80a:5120.

4. A Cayley, On the correspondence of homographies and rotations, Math. Ann. 15 (1879), 238-240.

5. W L Edge, Conics and orthogonal projectivities in a finite plane, Canad. J. Math. 8 (1956), 362-382; MR18-227.

6. A Weiss, Girths of bipartite sextet graphs, Combinatorica (to appear).

N L Biggs and John Shawe-Taylor,
Royal Holloway College,
Egham,
Surrey, TW20 0EX