Constructions for cubic graphs with large girth

Norman Biggs
Department of Mathematics
London School of Economics
Houghton St., London WC2A 2AE, UK
n.l.biggs@lse.ac.uk

Submitted: October 11, 1997; Accepted: August 31, 1998

Abstract

The aim of this paper is to give a coherent account of the problem of constructing cubic graphs with large girth. There is a well-defined integer $\mu_0(g)$, the smallest number of vertices for which a cubic graph with girth at least g exists, and furthermore, the minimum value $\mu_0(g)$ is attained by a graph whose girth is exactly g. The values of $\mu_0(g)$ when $3 \leq g \leq 8$ have been known for over thirty years. For these values of g each minimal graph is unique and, apart from the case $g = 7$, a simple lower bound is attained.

This paper is mainly concerned with what happens when $g \geq 9$, where the situation is quite different. Here it is known that the simple lower bound is attained if and only if $g = 12$. A number of techniques are described, with emphasis on the construction of families of graphs $\{G_i\}$ for which the number of vertices n_i and the girth g_i are such that $n_i \leq 2^{cg_i}$ for some finite constant c. The optimum value of c is known to lie between 0.5 and 0.75. At the end of the paper there is a selection of open questions, several of them containing suggestions which might lead to improvements in the known results. There are also some historical notes on the current-best graphs for girth up to 36.

MR Subject Numbers: 05C25, 05C35, 05C38.

1. Introduction

The aim of this paper is to give a coherent account of a topic which has been studied in a rather haphazard fashion for many years. There is much that remains to be done, but recent advances, particularly in geometric and computational group theory, promise to throw some light on the darker corners of the subject.

We shall concentrate on *cubic* graphs, that is, graphs in which each vertex has degree three. There are several justifications for this, the first one being that cubic graphs have wide applicability. For example, it follows from a recent result of Malle, Saxl and Weigel [33] that almost every finite simple group has a cubic Cayley graph. Furthermore, the generalisation to graphs of degree $k > 3$ does not appear to be substantially more difficult than the case $k = 3$. Finally, the cubic case is the only one where we have specific examples that improve significantly on the best general results currently available.

The *girth* of a graph is the length of a shortest cycle in the graph. It can be shown that cubic graphs with arbitrarily large girth exist (see Theorem 3.2) and so there is a well-defined integer $\mu_0(g)$, the smallest number of vertices for which a cubic graph with girth at least g exists. It is a standard (but not quite obvious) result [31, p.385] that the minimum value $\mu_0(g)$ is attained by a graph whose girth is *exactly* g, a result which also follows from our Theorem 4.2. We shall assume this result in the following discussion.

The values of $\mu_0(g)$ when $3 \leq g \leq 8$ have been known for over thirty years (see, for example, [47]). For these values of g each minimal graph is unique and, apart from the case $g = 7$, a simple lower bound $\theta_0(g)$ (defined in Section 2) is attained.

The situation for $g \geq 9$ is quite different. Here it is known that $\theta_0(g)$ is attained if and only if $g = 12$. Results for other values of g have been been achieved by a combination of luck, judgement, and years (literally) of computer time. Naturally the first case to attract attention was $g = 9$, where we have $\theta_0(9) = 46$. For many years the smallest number achieved was 60, but in 1979 a graph with 58 vertices was found [10]. In 1984 Brendan McKay showed that there no smaller graphs, so that $\mu_0(9) = 58$, and in 1995 the complete list of 18 minimal graphs was determined [14].

Generally, the problem of finding $\mu_0(g)$ is equivalent to determining the least value of c for which there is a cubic graph with girth g and 2^{cg} vertices. The value of c is known to lie between 0.5 and 0.75, but in practice this leaves considerable room for doubt, since the number of vertices implied by the upper bound is considerably greater than that implied by the lower bound.

In the 1970s a great deal of work was done 'by hand' on the cases $g = 9, 10, 11$, by C. W. Evans, R. M. Foster [15], W. Harries, A. T. Balaban [1,2], and others. Much of this work has remained unpublished, partly because it has been superseded by extensive computations, such as those of McKay referred to above. However, that work contained the germs of several ideas which are useful for dealing with larger values of g. An account of some of these ideas was given in the 1982 thesis of M. A. Hoare, and in a paper [25] by the same author published in 1983. Examples with girth up to 30 were also published at that time [11]. The present author gave a talk on the subject at a conference in 1985, the proceedings of which were published in 1989 [7]. It appears that this paper is not well-known, although it contains results for $g = 13, 14, 15, 16$ which are still the best known in 1998.

Recently there has been some more progress on this problem, and it seems that a fresh account is needed. Indeed, at least one important advance [13] has been made since the preprint of this paper was circulated. A dynamic survey of the current state of knowledge can be found on Gordon Royle's website [37]. This also contains other relevant information, in particular concerning the Foster Census [15] of symmetric cubic graphs.

At the end of the paper there is a selection of open questions, several of which contain suggestions for further work.

2. The naive bound

Let v be any vertex of a cubic graph G with odd girth g. Then v has three neighbours, each of which has two neighbours, and if $g \geq 5$ all six of them are distinct. Generally, the argument can repeated up to the point where there are $3 \times 2^{(g-3)/2}$ distinct vertices in the last step, and so the total number of vertices is at least

$$1 + 3(1 + 2 + 2^2 + \cdots + 2^{(g-3)/2}) = 3 \times 2^{(g-1)/2} - 2.$$

Using a similar argument starting with two adjacent vertices, it can be shown that when g is even the total number of vertices is at least

$$2 + 2^2 + \cdots + 2^{g/2} = 2^{g/2+1} - 2.$$

These two results comprise what we might call the 'very naive bound', denoted by $\theta_0(g)$ in the introduction.

If there is a graph G which attains the very naive bound, G is *distance-regular*, and its intersection array takes a particularly simple form. The theory of distance-regular graphs can be used [4, Chapter 23] to show that this can happen only if $g = 3, 4, 5, 6, 8, 12$. In each case there is a unique graph, and each one is a well-known, highly symmetrical graph.

Since the very naive bound is rarely attained we may say that, almost always, the number of vertices in a cubic graph with girth g strictly exceeds this bound. The number of vertices must be even, so it follows that we can ignore the -2 in the formulae displayed above. For this reason we shall define the *naive bound* $\nu_0(g)$ as follows:

$$\nu_0(g) = \begin{cases} 3 \times 2^{(g-1)/2} & \text{if } g \text{ is odd;} \\ 2^{g/2+1} & \text{if } g \text{ is even.} \end{cases}$$

The conclusion is that, for $g = 7, 9, 10, 11$ and for all $g \geq 13$, the number of vertices in a cubic graph with girth g is at least $\nu_0(g)$. The reason for calling this bound 'naive' can be inferred from the table given below, in which we compare $\nu_0(g)$ with the best results available at the time of writing (1998).

The current results are tabulated as the values of two (time-dependent) functions. The value $\mu(g)$ is the least value for which it has been proved that no smaller cubic graph with girth g can exist. Trivially $\mu(g) \geq \nu_0(g)$, and in cases where there is equality the value of $\mu(g)$ has been omitted. The value $\lambda(g)$ is the smallest number of vertices for which a cubic graph with girth g is known to exist; we shall call such a graph *current-best.* In order to determine $\mu_0(g)$, the minimal possible number of vertices of a cubic graph with girth g, we have to await the time when $\lambda(g) = \mu(g)$; currently this state is achieved only when $g \leq 12$.

g :	7	9	11	13	14	15	16	17	18	19	20
$\nu_0(g)$:	24	48	96	192	256	384	512	768	1024	1536	2048
$\mu(g)$:		58	112	202	258						
$\lambda(g)$:	24	58	112	272	406	620	990	2978	3024	4324	8096

Further details of the current-best graphs and the methods used to construct them will be given in Examples throughout the paper. For convenience, this information is collected in the Historical Notes at the end.

3. Families of graphs with large girth

The naive bound can be written in the following way. For almost all values of g,

$$\nu_0(g) = 2^{\frac{1}{2}g} K_0 \quad \text{where} \quad K_0 = \begin{cases} 3/\sqrt{2} = 2.121... & \text{if } g \text{ is odd;} \\ 2 & \text{if } g \text{ is even.} \end{cases}$$

The value of the constant $1/2$ is crucial. It tells us that, roughly speaking, the number of vertices of a cubic graph with girth g is of the order of $2^{\frac{1}{2}g}$, at least. However, the results quoted above show that known constructions are far from meeting this optimal value. In order to measure how effective these constructions are, it is helpful to define a parameter $c(G)$ which, for a cubic graph G with n vertices and girth g, is given by

$$c(G) = \frac{\log_2 n}{g}.$$

In other words, G has $2^{c(G)\,g}$ vertices. For example, the current-best graph with girth 13 referred to in the table above has $n = 272 = 2^{(0.6221...)g}$ vertices.

Suppose we have constructed a family of cubic graphs $\mathcal{G} = (G_i)$ such that the girth g_i of G_i tends to infinity with i. Then it is quite possible that $c(G_i)$ also tends to infinity with i (see Example 8.2). If the objective is to approach the naive bound, we need a further constraint on the number n_i of vertices of G_i. Define

$$c(\mathcal{G}) = \liminf_{i \to \infty} c(G_i),$$

so that $c(\mathcal{G})$ is the least value of c such that an infinite subsequence (G_j) of $\mathcal{G}$ satisfies

$$n_j < 2^{cg_j}\, K \quad \text{for some constant } K.$$

If $c(\mathcal{G})$ is finite, we say that $\mathcal{G}$ is a *family with large girth.* In this terminology, the aim is to find families for which $c(\mathcal{G})$ is as small as possible and, ideally, close to the optimal value 0.5.

Several authors have succeeded in constructing families $\mathcal{G}$ with large girth – that is, families for which an explicit upper bound for $c(\mathcal{G})$ can be established. However, the optimal value 0.5 has not been approached, and the precise value of $c(\mathcal{G})$ is not known for any of these families. The first result of this kind was obtained by Imrich [27], who constructed a family $\mathcal{I}$ for which he could show that $c(\mathcal{I}) \leq 1.04$. In 1984 Weiss [44] showed that the family of bipartite sextet graphs $\mathcal{S}$ defined by Biggs and Hoare [11] satisfies $c(\mathcal{S}) \leq 0.75$, and this remains the best result obtained so far.

Although the present paper is specifically concerned with graphs of degree 3, it is worth noting what has been achieved for regular graphs of degree $k > 3$. Here it is appropriate to define $c(\mathcal{G})$ to be the lim inf of $(\log_{k-1} n_i)/g_i$. Lubotsky, Phillips and Sarnak [32] constructed families $\mathcal{L}_{p+1}$ of degree $p+1$, where p is a prime congruent to 1 modulo 4, and showed that $c(\mathcal{L}_{p+1}) \leq 3/4$. The fact that the value of $c(\mathcal{L}_{p+1})$ is exactly $3/4$ was established independently by Margulis [34] and Biggs and Boshier [9]. The basic idea of [32] is to use quaternion algebras, and this was extended to cubic graphs by Chiu [16]. Recently, Lazebnik, Ustimenko and Woldar [29, 30] have constructed families $\mathcal{G}_k$ such $c(\mathcal{G}_k) = (3/4)\log_{k-1} k$ for every $k \geq 3$ Unfortunately, their results are weakest for $k = 3$, since the value of c is then $(3/4)\log_2 3 = 1.19\ldots$.

We began with the naive lower bound $\nu_0(g) \leq \mu_0(g)$. The families mentioned above provide upper bounds for some values of $\mu_0(g)$, but not necessarily all values. For example, there are no sextet graphs with girth 9,10, or 11. The following result [31] leads a uniform upper bound.

Lemma 3.1 Let G be a cubic graph with girth $g \geq 3$ having $\mu_0(g)$ vertices. Then the diameter of G does not exceed g.

Proof Suppose that v and w are vertices of G such that the distance $d(v,w) > g$. Construct a new cubic graph G_0 by deleting v, w and the edges which are incident with either of them, and adding new edges which join the three neighbours of v to the three neighbours of w. Then we claim that G_0 also has girth at least g, and since it is smaller than G, we have a contradiction. (Recall our assumption, to be proved in Section 4, that $\mu_0(g)$ is attained by a graph with girth exactly equal to g.)

Clearly it is enough to show that any cycle C_0 in G_0 which contains a new edge has length at least g. If C_0 contains exactly one new edge, then the rest of C_0 is a path in G which (since $d(v,w) \geq g+1$) has length at least $g-1$. Hence the length of C_0 is at least g. If C_0 contains two or three new edges it must also contain at least two paths joining the ends of these edges. Such a path has length at least $g-2$ (if it joins two neighbours of v, or two neighbours of w), and length at least $g-1$ otherwise. Hence the length of C_0 is at least $2 + 2(g-2)$, which is greater than g. $\square$

Applying the simple counting argument used at the beginning of Section 2, we see that any cubic graph with diameter not greater than g has at most

$$1 + 3(1 + 2 + 2^2 + \cdots + 2^{g-1}) = 3 \times 2^g - 2$$

vertices, and so we have the upper bound $3 \times 2^g - 2 \geq \mu_0(g)$.

The preceding result is not constructive, because to apply the technique used in the proof of Lemma 3.1 we must start from a cubic graph with girth g. A truly constructive technique, which leads to the slightly better bound $\mu_0(g) \leq 2^g$, is due to Erdős and Sachs [21] and Sauer [39]. The proof, as given by Bollobás [12], can be converted rather easily into an algorithmic construction, as follows. Start with any regular graph of degree 2, that is, any union of disjoint cycles, which contains no cycle of length less than g; then add new edges, subject to the conditions that (i) only one new edge is incident with each vertex, and (ii) no cycles of length less than g are created. Formally, we have

Theorem 3.2 Let H be a disjoint union of cycles such that: (i) no cycle has length less than g, and (ii) the total number of vertices is 2^g. Then we can add edges to H to form a cubic graph G whose girth is at least g.

Proof [12,21,39] Let $H = (V, E)$ be the given graph, and let D denote the set of all edges (pairs of vertices of H) which are not in E. Let $A \subseteq D$ satisfy the conditions

•1 no vertex is incident with more than one edge in A;

•2 the girth of $H_A = (V, E \cup A)$ is not less than g.

Then we shall show that if $|A| < 2^{g-1}$ there exists $A^+ \subseteq D$ such that $|A^+| = |A|+1$ and A^+ satisfies •1 and •2.

Let d_A be the distance function in H_A (extended, if necessary, by defining the distance between vertices in different components to be infinite). Let $V_2(A) \subseteq V$ denote the set of vertices with degree 2 in H_A, that is, those which are not incident with any edge in A. Given that $|A| < 2^{g-1}$, it follows that $V_2(A)$ has at least two members. If any pair $p, q \in V_2(A)$ is such that $d_A(p, q) \geq g - 1$, then the set $A^+ = A \cup pq$ satisfies the required conditions. Thus it remains to consider the case when all vertices in $V_2(A)$ are within distance $g - 2$ of each other.

Let $D_r(z) = \{v \in V \mid d_A(z, v) \leq r\}$. For any $x \in V_2(A)$, the set $D_{g-2}(x)$ has size at most

$$1 + 2 + 2^2 + \ldots + 2^{g-2} = 2^{g-1} - 1.$$

Consequently, if x, y are any two vertices in $V_2(A)$, and $U = D_{g-2}(x) \cup D_{g-2}(y)$, $I = D_{g-2}(x) \cap D_{g-2}(y)$, we have

$$|U| = |D_{g-2}(x)| + |D_{g-2}(y)| - |I| \ \leq \ 2(2^{g-1} - 1) - |I| = 2^g - 2 - |I|.$$

Let $W = V \setminus U$. Since $|V| = 2^g$, it follows from the preceding inequality that $|W| \geq |I| + 2$. Furthermore, we are considering the case when all vertices in $V_2(A)$

are within distance $g-2$ of each other, so W contains no members of $V_2(A)$. Thus for every $w \in W$ there is a vertex w' defined by $ww' \in A$.

Let $W' = \{w' \mid ww' \in A \text{ and } w \in W\}$. Since vertices in W are at distance $g-1$ (at least) from both x and y, vertices in W' are at distance $g-2$ (at least) from x and y. It cannot be true that all members of W' are at distance exactly $g-2$ from both x and y, since $|W'| = |W| > |I|$. Hence there is a w' for which (say) $d_A(x, w') \geq g-1$. Defining

$$A^+ = A \setminus ww' \cup xw' \cup yw,$$

we have the required result. □

Theorem 3.2 shows that there is a cubic graph with 2^g vertices and girth not less than g which has any prescribed 2-factor. In particular, there is a Hamiltonian graph with these properties.

The proof can be thought of as an algorithm for constructing a sequence of sets

$$\emptyset = A_0 \subset A_1 \subset A_2 \ \ldots \ \subset A_N, \quad N = 2^{g-1},$$

using only two basic operations. If possible A_{i+1} is formed by adding one edge to A_i, but if that is impossible, we delete one edge from A_i and add two new ones. (However, Noga Alon has pointed out that it is not clear in what sense the graphs so constructed are 'explicit'.)

Of course, we might be lucky enough to find that the construction works when the initial graph H has less than 2^g vertices, for example, when H is a cycle of length 2^{cg}, $c < 1$. Since we have families for which $c = 3/4$, the case $c = 2/3$ would be particularly interesting. For simplicity, let $g = 3h$; then we are looking for Hamiltonian cubic graphs of girth $3h$ obtained by adding edges to a cycle of length 2^{2h}. In the cases $h = 1$ and $h = 2$ such graphs are well-known: they are the graphs **4** and **16** in Foster's census [15]. It is probably fairly easy to construct such graphs when $h = 3$ and $h = 4$, but no general construction is known.

4. Excision

In this section we shall show that $\mu_0(g)$, the smallest number of vertices for which there is a cubic graph with girth g, is a strictly increasing function of g. The technique is to construct a graph with girth $g-1$ from one with girth g.

Throughout this section G denotes a cubic connected graph. Let S be a connected subgraph of G, in which the degree of every vertex is either 1 or 3, and the vertices of degree 1 are not adjacent in G. We shall refer to the vertices of degree 1 as the *ends* of S. If we delete from G all the edges of S and its vertices of degree 3, each end y remains adjacent to two vertices that are not in S, say x and z. Replacing the edges xy and yz by a single edge $e_y = xz$, we obtain a cubic graph. We shall denote this graph by $G \ominus S$.

Lemma 4.1 Suppose that s is the diameter of S. If $s < (g-1)/2$ then the girth of $G \ominus S$ is at least $g-1$.

Proof Any cycle C in $G \ominus S$ defines a cycle C^* in G: for each end y such that C contains e_y, C^* contains xy and yz. Hence the length of C is the length of C^* minus the number of ends on C^*. In particular, if C^* contains exactly one end, the length of C is at least $g-1$.

Suppose that C^* contains $k \geq 2$ ends $y_1, y_2, \ldots, y_k$ in cyclic order, and label the neighbours of each y_i as x_i, z_i, so that their cyclic order on C^* is x_i, y_i, z_i. Then C consists of paths π_i of length l_i from z_i to x_{i+1} in $G \ominus S$ (by convention $k+1=1$ here), together with the edges e_y, $y = y_1, y_2, \ldots, y_k$. Let d_S be the distance function in the subgraph S, so that there is a path in S of length $d_S(y_i, y_{i+1}) \leq s$ joining y_{i+1} and y_i. This path, together with the edge $y_i z_i$, the path π_i, and the edge $x_{i+1}y_{i+1}$, forms a cycle in G, and so

$$g \leq d_S(y_i, y_{i+1}) + l_i + 2 \leq s + l_i + 2.$$

It follows that $l_i \geq g - s - 2$. The length of C is $l_1 + l_2 + \cdots + l_k + k$, which is at least $k(g-s-2) + k = k(g-s-1)$. By assumption $k \geq 2$ and $s \leq (g-1)/2$, so the length is at least $g-1$, as claimed. □

From our point of view, the optimum result is obtained by making S as large as possible, consistent with the condition $s \leq (g-1)/2$. This motivates the choices made in the proof of the following theorem.

Theorem 4.2 If there is a cubic graph G with n vertices and girth g then there is a cubic graph G^- with $n - \epsilon(g)$ vertices and girth $g-1$, where

$$\epsilon(g) = \begin{cases} 2^{r+1} - 2 & \text{if } g = 4r \text{ or } 4r+1, \\ 3 \times 2^r - 2 & \text{if } g = 4r+2 \text{ or } 4r+3. \end{cases}$$

Proof Suppose first that $g = 4r$ or $4r+1$. Given any pair v, w of adjacent vertices in G, let S be the subgraph spanned by the vertices whose distance from either v or w does exceed $r-1$. Then S is a tree with diameter $2r-1$, which is less than $(g-1)/2$ in these cases. So, by Lemma 4.1, $G \ominus S$ has girth $g-1$, and the number of its vertices is n minus the number in S, which is $2 + 2^2 + \cdots + 2^r = 2^{r+1} - 2$.

Similarly, if $g = 4r+2$ or $4r+3$, we can take S to be the subgraph spanned by all vertices whose distance from a given vertex v does not exceed r. Then S is a tree with diameter $2r$, which is less than $(g-1)/2$ in both cases. So here again $G \ominus S$ has girth $g-1$, and in this case the number of deleted vertices is $1 + 3(1 + 2 + \cdots + 2^{r-1}) = 3 \times 2^r - 2$. □

Example 4.3 When $g = 6$ the minimal cubic graph is Heawood's graph with 14 vertices. (It is the incidence graph of points and lines in the seven point projective plane.) Excising a tree consisting of a vertex and its three neighbours, we obtain a graph with 10 vertices and girth 5 – Petersen's graph, which is also minimal. In this case both graphs attain the very naive bound. □

Example 4.4 When $g = 8$ the minimal cubic graph is Tutte's graph with 30 vertices. Excising a tree consisting of two adjacent vertices and their neighbours, we obtain a graph with 24 vertices and girth 7. This is McGee's graph, which is minimal and attains the naive bound, but not the very naive bound. □

Example 4.5 When $g = 12$ the minimal cubic graph has 126 vertices, so it attains the very naive bound. Excising a tree on 14 vertices, consisting of two adjacent vertices and all vertices at distance two or less from them, we obtain Balaban's graph with 112 vertices and girth 11. This graph is now known to be minimal [14]. □

Example 4.6 Bray, Parker and Rowley [13] have recently constructed a graph with 3024 vertices and girth 18. In this case the appropriate tree has 46 vertices, so excision yields a graph with 2978 vertices and girth 17. These graphs are current-best, but both are far from attaining the naive bound. □

It is tempting to think that the excision technique could be strengthened, by removing more than one set of vertices. However, this requires that the excised parts be remote from each other, and as yet no one has discovered how to avoid the complications which rapidly outweigh the potential advantages.

The reverse of the excision technique is *insertion*. Here we add a number of new vertices, each of them the 'mid-point' of an existing edge, and join them in pairs to get a cubic graph. The insertion technique produces some pretty constructions: for example, McGee's graph (Example 4.4) can be obtained from the symmetric graph **16** mentioned in the previous section [47, p.79].

5. Permutation groups

Let X be a finite set, and S a set of permutations of X which is closed under inversion and does not contain the identity. These permutations generate a subgroup $\langle S\rangle$ of the symmetric group $\mathrm{Sym}(X)$. (For the avoidance of doubt, we take the group operation to be functional composition on the left: $(st)(x) = s(t(x))$.) We define the *Cayley graph* $\mathrm{Cay}(S)$ to be the graph whose vertices v are the elements of $\langle S\rangle$, with v and w forming an edge if $wv^{-1} \in S$. Thus, if $S = \{\alpha_1, \alpha_2, \dots, \alpha_k\}$, the vertex v is adjacent to the vertices $\alpha_1 v, \alpha_2 v, \dots, \alpha_k v$. Note that the edge joining v and w is undirected, because S is closed under inversion, and hence wv^{-1} is in S if and only if vw^{-1} is in S. (More details about Cayley graphs in general can be found in [4, 15].)

A cycle of length r in $\mathrm{Cay}(S)$ has vertices of the form

$$v,\ \omega_1 v,\ \omega_2\omega_1 v,\ \dots,\ \omega_r \dots \omega_2\omega_1 v = v,$$

where each ω_i is a member of the generating set S, and $\omega_r \dots \omega_2\omega_1$ is the identity permutation. Clearly we must have $\omega_i \neq {\omega_{i+1}}^{-1}$ $(1 \leq i \leq r-1)$, and $\omega_r \neq {\omega_1}^{-1}$. When this holds we say that $\omega_r \dots \omega_2\omega_1$ is an *identity word.* Finding the girth of $\mathrm{Cay}(S)$ is equivalent to finding a shortest identity word in the elements of S, provided we remember to consider identity words which are *reduced*, in the sense that $\omega_i \neq {\omega_{i+1}}^{-1}$ $(1 \leq i \leq r-1)$, and $\omega_r \neq {\omega_1}^{-1}$.

Note that the letters in a word are numbered backwards to conform with our convention for the composition of permutations.

There are two kinds of generating set S which determine a cubic graph $\mathrm{Cay}(S)$. Recall that an *involution* is a permutation π such that π^2 is the identity, or equivalently $\pi^{-1} = \pi$.

- Type 1: $S = \{\alpha, \beta, \gamma\}$, where all three generators are involutions.
- Type 2: $S = \{\alpha, \delta, \delta^{-1}\}$, where α is an involution and δ is not.

Example 5.1 Suppose that $X = \{1, 2, 3, 4\}$ and

$$\alpha = (12), \quad \beta = (13), \quad \gamma = (14).$$

In this case $\mathrm{Cay}(S)$ is a cubic graph of Type 1, and $\langle S \rangle$ is the symmetric group $\mathrm{Sym}(X) = S_4$. Since $\alpha\beta = (132)$, $(\alpha\beta)^3$ is an identity word, and it is easy to check that there no shorter ones. Hence the girth of $\mathrm{Cay}(S)$ is 6. The graph is **24** in Foster's Census [15]. □

Example 5.2 Let X be $\mathbf{Z}/p\mathbf{Z}$, the integers modulo p, where p is prime. Choose $b, c \in X$ such that $c \neq 0$. Then the permutations defined by

$$\alpha(x) = b - x, \quad \delta(x) = cx$$

generate a subgroup of the *affine group* of transformations of $\mathbf{Z}/p\mathbf{Z}$. For example, if $p = 17$, $b = 1$, and $c = 3$ the permutations are

$$\alpha = (0\ 1)(2\ 16)(3\ 15)(4\ 14)(5\ 13)(6\ 12)(7\ 11)(8\ 10)$$
$$\delta = (1\ 3\ 9\ 10\ 13\ 5\ 15\ 11\ 16\ 14\ 8\ 7\ 4\ 12\ 2\ 6).$$

Here we have generators for a Type 2 Cayley graph. The set $S = \{\alpha, \delta, \delta^{-1}\}$ generates the entire group of affine transformations, which has order $17 \times 16 = 272$, so $\mathrm{Cay}(S)$ has 272 vertices. A computer search for identity words reveals that the shortest ones have length 13.

For another example, suppose we take $p = 29$, $b = -1$, $c = 4$. Here we get a graph with $29 \times 14 = 406$ vertices. A shortest identity word is

$$(\alpha\delta^{-2}(\alpha\delta)^2)^2,$$

so the Cayley graph has girth 14.

At this stage it might appear that we have a promising technique for constructing graphs with large girth. However, the promise is short-lived, because it turns out that $\alpha\delta^{-2}(\alpha\delta)^2$ is always an involution, for any permutations α and δ which are defined by the equations given above. Thus the word of length 14 displayed above is a 'universal' identity word for all groups constructed in this way, and all such Cayley graphs have girth $g \leq 14$.

Despite the limited scope of the general construction, it is worth pointing out that the graphs on 272 and 406 vertices described above are the current-best examples for girth 13 and girth 14 (see the Historical Notes.) □

6. Coloured pictures

We shall describe a useful technique for dealing with Cayley graphs of Type 1. In this case each generator is its own inverse, and so a reduced identity word is such that no two consecutive letters are the same, and the first and last ones are different. In the following discussion we shall generally assume that all words under consideration have these properties.

The technique is based on the use of a 'coloured picture' or, more precisely, an edge-coloured graph. We take the vertex-set of this graph to be the set X of objects permuted, and join two vertices x and y by an edge whenever (xy) is a transposition belonging to one of the generators α, β, γ. If we think of α, β, γ as colours, we obtain an edge-coloured graph (no colour appears twice at any vertex), in which each vertex has degree at most 3. Following [5], we shall call it a *picture*.

Example 6.1 Let $X = \{0, 1, 2, \ldots, 9, T, E\}$ and $S = \{\alpha, \beta, \gamma\}$, where

$$\alpha = (01)(23)(56), \quad \beta = (45)(67)(9T), \quad \gamma = (89)(TE)(12).$$

The graph $\mathrm{Cay}(S)$ was first studied by Frucht [22]. The corresponding picture has three components, each of them a path with four vertices.

It is clear that $\langle S \rangle$ must be a subgroup of the direct product of the groups defined by each component of the picture, and in this case these are dihedral groups of order 8. In fact $\langle S \rangle$ has order 64. The shortest identity words are of the form $(\alpha\beta)^4$, so the girth is 8. The graph is **64** in Foster's Census.

For future reference we note that the generators for Frucht's graph satisfy certain identities involving the commutator $[\sigma, \tau] = \sigma^{-1}\tau^{-1}\sigma\tau$ which, when σ and τ are involutions, is just $(\sigma\tau)^2$. In fact, the commutator $[\alpha, \beta] = (\alpha\beta)^2 = (47)(56)$, from which it follows that $[\alpha, \beta]$ commutes with all three generators α, β, γ. By symmetry, we conclude that every commutator in $\langle S \rangle$ commutes with every element of $\langle S \rangle$. The significance of this fact will be explained in Example 8.2. □

Example 6.1 can be regarded as the case $n = 4$ of a general construction, in which we construct permutations which generate a subgroup of the direct product of three dihedral groups of order $2n$. Specifically, we let X be the disjoint union $X_1 \cup X_2 \cup X_3$, where $|X_i| = n$, and set $\alpha = \alpha_1\alpha_2$, $\beta = \beta_2\beta_3$, $\gamma = \gamma_3\gamma_1$, where α_1 and γ_1 are involutions generating a dihedral group on X_1:

$$\langle \alpha_1, \gamma_1 \mid \alpha_1^2 = \gamma_1^2 = (\alpha_1\gamma_1)^n = id \rangle \approx D_{2n},$$

and similarly for β_2, α_2 and γ_3, β_3. Unfortunately, the girth of the graphs constructed in this way is bounded. Since $(\alpha\beta)^2$ fixes the set $X_1 \cup X_3$, which is the set permuted by γ, the two elements commute:

$$[(\alpha\beta)^2, \gamma] = (\beta\alpha)^2\gamma(\alpha\beta)^2\gamma = id.$$

Thus we have an identity word of length 10, which is universal for this construction. It follows that the girth of any graph constructed in this way cannot exceed 10.

At this point, a positive result seems appropriate. The next theorem is a simple, but important, application of coloured pictures.

Theorem 6.2 There are finite Cayley graphs of Type 1 with arbitrarily large girth.

Proof Let P_r denote the 'cubic tree' of finite radius $r \geq 1$. In other words, all vertices at distance less than r from a central vertex x have degree 3, and all vertices at distance r from x have degree 1. Assign three colours to the edges of P_r in any way consistent with the edge-colouring condition, and let α, β, γ be the corresponding involutions.

Suppose we are given any word $\omega_l\omega_{l-1}\ldots\omega_1$ in the generators α, β, γ, which is reduced in the sense explained above. The image of x under ω_1 is a vertex at distance 1 from x. The image of this vertex under ω_2 is a vertex at distance 2 from from x, since $\omega_2 \neq \omega_1$. Repeating the argument, we conclude that if $l \leq r$, the image of x is at distance l from x, and in particular x is not fixed by the given word. Hence no word of length r or less is an identity word, and Cay(S) has girth at least $r + 1$. □

In fact, an obvious continuation of the argument in the proof shows that no word of length $l \leq 2r + 1$ fixes x, so the girth is at least $2r + 2$. We could go further by characterising those words of length $2r + 1$ which do fix x, showing that none of them fix certain other vertices, and so on. Alternatively, for small values of r the girth can be calculated by computer. For example, the girth of the graph when $r = 2$ has been computed to be 20. Note that in this case the permutations generate the entire symmetric group S_{10}, so although we have a graph with $g = 20$, it has $10! = 3\,628\,800$ vertices, which is rather more than the current-best (8096 vertices).

In general, if we choose a set of permutations at random then it is likely that they will generate the entire symmetric or alternating group, and so the Cayley graph will be uncomfortably large. We can avoid this problem by working within a known group, as in Example 6.1. Many interesting groups can be generated by three involutions; for example, it follows from the results of Malle, Saxl and Weigel [33] that almost all finite simple groups can be so generated. Thus cubic Cayley graphs of Type 1 provide a rich source of examples. However, attempts to construct families with large girth often fail because there is a universal identity word, like the word of length 10 which prevented our attempt to generalise Example 6.1.

7. Applications of coloured pictures

Let $P(\alpha, \beta)$ be the subgraph of a picture P spanned by the edges coloured α or β. Then $P(\alpha, \beta)$ consists of a number of components, each of which is either (i) a cycle of even length l, or (ii) a path of length k in which the two end-vertices are fixed by exactly one of α and β. In the first case, the permutation $\alpha\beta$ acts on the vertices of the component as two cycles of length $l/2$, so $(\alpha\beta)^{l/2}$ is the identity permutation on the vertices of this component; in particular, if this is the only component, $(\alpha\beta)^{l/2}$ is an identity word of length l. In the second case $\alpha\beta$ acts on the vertices as a cycle of length k, and $(\alpha\beta)^k$ is the identity permutation on the vertices of this component.

Let $\langle \alpha, \beta \rangle$ denote the group generated by the permutations α and β. For any component C of $P(\alpha, \beta)$, denote by $\langle \alpha, \beta \mid C \rangle$ the group of permutations of the vertices of C induced by $\langle \alpha, \beta \rangle$. The next Lemma follows from the observations in the previous paragraph.

Lemma 7.1 Let C be a component of the picture $P(\alpha, \beta)$. Then if C is a cycle of length l, $\langle \alpha, \beta \mid C \rangle$ is a dihedral group of order l, and if C is path of length k it is a dihedral group of order $2k$. $\square$

The group $\langle \alpha, \beta \rangle$ is the direct product of the groups $\langle \alpha, \beta \mid C \rangle$, each of which is a dihedral group. Thus it is easy to analyse the action of this group. For example, the intersection of $\langle \alpha, \beta \rangle$ with its conjugate $\langle \alpha, \beta \rangle^\gamma$, can be easily determined.

Lemma 7.2 Suppose that a shortest identity word contains an occurrence of γ. If

$$\langle \alpha, \beta \rangle^\gamma \cap \langle \alpha, \beta \rangle = id$$

then this word must contain at least three occurrences of γ.

Proof Note first that the given condition implies that γ does not belong to $\langle \alpha, \beta \rangle$. Suppose that there is an identity word in which γ occurs just once, say $\lambda\gamma\mu = id$, where λ and μ are words in α and β only. Then it follows that $\mu\lambda = \gamma$, contradicting the fact that $\gamma \notin \langle \alpha, \beta \rangle$.

Suppose that there is an identity word in which γ occurs just twice, say $\rho\gamma\sigma\gamma\tau = id$, where ρ, σ and τ are words in α and β, and σ is not the empty word. Then $\tau\rho = \gamma\sigma^*\gamma$, where σ^* is the inverse (= reverse) of σ. Since $\tau\rho$ and σ^* are in $\langle \alpha, \beta \rangle$, this implies that $\gamma\sigma^*\gamma$ is in both $\langle \alpha, \beta \rangle$ and its conjugate $\langle \alpha, \beta \rangle^\gamma$. It follows from the given condition that σ^* is an identity word. Hence the given word cannot be a shortest identity word. $\square$

Example 7.3 Consider the Cayley graph obtained by taking $X = \{1,2,3,4,5\}$ and $S = \{\alpha, \beta, \gamma\}$, where

$$\alpha = (12)(35), \quad \beta = (14)(25), \quad \gamma = (13)(45).$$

Since the generators are even permutations, $\langle S\rangle$ is a subgroup of the alternating group A_5, and it is easy to check that it is 3-transitive, so it is A_5. Hence $\mathrm{Cay}(S)$ has 60 vertices.

The picture $P(\alpha,\beta)$ has one component C_1, a path whose vertices occur in the order $3,5,2,1,4$. So $\langle\alpha,\beta\rangle = \langle\alpha,\beta \mid C_1\rangle$ is a dihedral group of order 10, and it is easy to check that $\langle\alpha,\beta\rangle^\gamma \cap \langle\alpha,\beta\rangle = id$.

The shortest reduced identity word which does not contain γ is $(\alpha\beta)^5$, so 10 is an upper bound for the girth of $\mathrm{Cay}(S)$. But the graph has 60 vertices, and we know that a cubic graph with girth 10 must have at least 64 vertices, so the girth cannot exceed 9. On the other hand, Lemma 7.2 tells us that an identity word which does contain γ must contain at least three occurrences of γ. By symmetry, an identity word must contain at least three occurrences of α and β also, so it must have length at least 9. Hence the girth is exactly 9, and there must be an identity word of length 9, in which each generator occurs three times. Indeed one such word is

$$\alpha\beta\gamma\beta\gamma\alpha\gamma\alpha\beta.$$

This graph was the first cubic graph with 60 vertices and girth 9 to be discovered (by R. M. Foster, see [22]). For many years it remained current-best, although a number of other graphs with these properties were found, and it began to look as if $\mu_0(9) = 60$. However, eventually it turned out [10,14] that the correct value is 58, not 60. □

Example 7.4 Using the MAGMA package, Conder [18] found that the following involutions generate the group $PSL(2,16)$, considered as a permutation group on the 17 points of the projective line over the field $GF(2^4)$.

$$\begin{aligned}\alpha &= (1,9)(2,8)(3,7)(4,6)(10,17)(11,16)(12,15)(13,14)\\ \beta &= (1,11)(2,5)(3,8)(4,14)(6,15)(7,12)(9,17)(10,13)\\ \gamma &= (1,2)(3,13)((5,12)(6,7)(8,11)(9,15)(10,16)(14,17).\end{aligned}$$

The group has order $17\times16\times15 = 4080$, so we have a cubic Cayley graph with that number of vertices, and Conder showed that the girth of this graph is 18. □

Examples 7.3 and 7.4 can be unified, as follows. The multiplicative group of the field $GF(2^{2m})$ is cyclic of order $2^{2m}-1$, which is equal to $3r$, say. If t is a primitive element of the field, $\omega = t^r$ is a cube root of unity.

Consider $PSL(2, 2^{2m})$ as a permutation group, where the permutations are defined by linear fractional transformations on the points of the projective line $PG(1, 2^{2m})$, identified with $GF(2^{2m}) \cup \{\infty\}$. For any k, the transformation

$$x \mapsto \frac{x+1}{kx+1}$$

is an involution, as are its conjugates under the permutations $x \mapsto \omega x$ and $x \mapsto \omega^2 x$. When $m = 1$, the field is $GF(4) = \{0, 1, \omega, \omega^2\}$, where ω itself is a primitive element. Taking $k = \omega$ gives the involutions

$$(\omega)(0\ 1)(\infty\ \omega^2), \quad (\omega^2)(0\ \omega)(\infty\ 1), \quad (1)(0\ \omega^2)(\infty\ \omega).$$

These three involutions generate the group $PSL(2, 4)$, which is isomorphic to the alternating group A_5. The identification with the permutations discussed in Example 7.3 is given by $0 \mapsto 1, 1 \mapsto 2, \omega \mapsto 4, \omega^2 \mapsto 3, \infty \mapsto 5$. The fact the graph is symmetric is an obvious consequence of the fact that the generating involutions are conjugates under an element of period 3.

When $m = 2$ the field $GF(16)$ contains a primitive element t satisfying $t^4+t+1 = 0$, and $t^5 = \omega$ is cube root of unity. Taking $k = t^3$ we get three involutions which can be identified with the ones discovered by Conder. The coloured picture can be drawn so that the threefold symmetry is plain.

It would be gratifying if k could be chosen so that the Cayley graph generated by the three involutions had large girth for all m. Specifically, the two examples might suggest that the girth is $9m$. Since the graphs have about 2^{6m} vertices, that would imply a family with $c = 2/3$. Unfortunately, in the case $m = 3$ the best that can be done is a graph with girth 26, rather than 27. I am (not) grateful to Marston Conder for this computation.

8. Abstract groups generated by three involutions

In this section we consider a group presentation of the form

$$\langle a, b, c \mid a^2 = b^2 = c^2 = 1, r_1, r_2, \ldots, r_m \rangle,$$

where $r_1, r_2, \ldots, r_m$ are relations involving the generators a, b, c. Since the generators are self-inverse, each relation can be written as an identity word $w_1 w_2 \ldots w_l = 1$, where w_i is one of a, b, c, and $w_i \neq w_{i+1}$ $(1 \leq i \leq l-1)$. Furthermore, there is no loss of generality in assuming that the word is *cyclically reduced*, which in this case simply means that, $w_1 \neq w_l$. In general, there is no easy way to ensure that the relations $r_1, r_2, \ldots, r_m$ determine a finite group, although some special cases can be treated theoretically. If the group is indeed finite, the coset enumeration process will verify this fact by terminating (eventually), but we cannot say when.

The *Cayley graph* of the presentation is the graph in which the vertices are the elements of the group, and an edge joins vertices x and y whenever xy^{-1} is one of the generators a, b, c. Since the generators are involutions, this defines an undirected graph, in which each vertex x is joined to the vertices ax, bx, cx. A cycle of length s in the Cayley graph has vertices of the form

$$x,\ u_1x,\ u_2u_1x, \quad \ldots, \quad u_s \ldots u_2u_1x = x,$$

where each u_i is one of the generators, and $u_2 \neq u_1$, $u_3 \neq u_2$, and so on. So $u = u_s \ldots u_2u_1$ is an *identity word*, that is $u = 1$ in the group. This equation is a consequence of the defining relations, but it is not necessarily one of them.

In the special case when there are no relations, the group is the free product of three cyclic groups of order 2,

$$I = \langle a, b, c \mid a^2 = b^2 = c^2 = 1 \rangle.$$

In this case there are no identity words, and the Cayley graph is the infinite cubic tree T. Any set of relations $r_1, r_2, \ldots, r_m$ defines a quotient group of I, and its Cayley graph is a quotient graph of T. However these quotients may well be infinite.

One way to guarantee finiteness has been discussed in Sections 5,6, and 7. We choose a set S of three involutory permutations α, β, γ of a finite set X, in which case the corresponding subgroup $\langle S \rangle$ of the symmetric group $\mathrm{Sym}(X)$ is finite. The homomorphism $\eta : I \to \langle S \rangle$ defined by $a \mapsto \alpha$, $b \mapsto \beta$, $c \mapsto \gamma$ is onto, and its kernel N is such that I/N is isomorphic to $\langle S \rangle$. Choosing the permutations as in Theorem 6.2 we obtain the following basic result.

Lemma 8.1 Given g, there are finite quotients of I whose Cayley graphs have arbitrarily large girth. □

In the language of group theory, this result states that I is *residually finite* [8].

In the rest of this section we shall consider alternative methods of choosing a set of relations $r_1, r_2, \ldots, r_m$ in such a way that the group they define is finite.

Example 8.2 Suppose we add the relations which say that the generators commute: $ab = ba, bc = cb, ca = ac$. Then the group is abelian, and the elementary theory of abelian groups tells us that it is the direct product of three cyclic groups of order two:

$$\langle a, b, c \mid a^2 = b^2 = c^2 = 1, ab = ba, bc = cb, ca = ac \rangle \ = \ \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}.$$

This is a group of order 8. The relations determine cyclically reduced identity words, such as $abab$, which have length 4. There are no shorter identity words, so we get a cubic graph with 8 vertices and girth 4, which is the graph formed by the vertices and edges of a cube. □

Example 8.3 One way to generalise the previous example is to use the *lower central series* of I. Generally, for any group G, a sequence of characteristic subgroups of G is defined by the recursive construction

$$\gamma_1 G = G, \quad \gamma_i = [G, \gamma_{i-1} G],$$

where $[A, B]$ is the group generated by all commutators $[a, b] = a^{-1}b^{-1}ab, a \in A, b \in B$. In particular, $\gamma_2 G = [G, G]$ is the *commutator subgroup* of G, and $G/\gamma_2 G$ is the 'abelianisation' of G. When $G = I$ the quotient $I/\gamma_2 I$ can be presented as

$$\langle a, b, c \mid a^2 = b^2 = c^2 = [a, b] = [b, c] = [c, a] = 1 \rangle,$$

which is the elementary abelian group of order 8 discussed in Example 8.1. More generally, it is known that, for all $i \geq 1$, $\gamma_{i-1} I/\gamma_i I$ is a finite group (see [41] for further details). Consequently, each term $\gamma_i I$ of the lower central series is a normal subgroup of finite index in I, and the Cayley graph of the quotient group $I/\gamma_i I$ is a finite cubic graph, LC_i. Example 8.2 shows that LC_2 is the cube.

The next graph in the series, LC_3, is the Cayley graph of the group

$$\langle a, b, c \mid a^2 = b^2 = c^2 = 1, [[*, *], *] = 1 \rangle.$$

Here the last equation indicates that *every* expression $[[x, y], z]$, with x, y, z words in a, b, c, is an identity word. It turns out that the group has order 2^6. In fact, the graph LC_3 is the one already discussed in Example 6.1 using generating permutations. The shortest identity words are of the form

$$[[a, b], b] = (abab)b(baba)b = abababab,$$

so the girth is 8.

In order to determine the girth g_i of LC_i in general, we have to remember that that a cyclically reduced identity word of minimal length is not necessarily one of the defining relations. It might be thought that the shortest identity words in LC_i are those which correspond to the relations

$$[\ldots [[a, b], b] \ldots, b] = (ab)^{2^{i-1}},$$

which have length 2^i. However, the existence of shorter words can be inferred from the general fact that $[\gamma_i G, \gamma_j G] \leq \gamma_{i+j} G$. For example, when $G = I$, the case $i = j = 2$ tells us that

$$[[a, b], [b, c]] = (abab)(bcbc)(baba)(cbcb) = (aba)(cbc)(baba)(cbcb)$$

is in I_4. So we have a cycle of length 14 in LC_4, which is shorter than the cycle of length 16 defined by the relation $[[[a, b], b], b] = 1$.

More generally, we can argue as follows. Suppose that u and v are cyclically reduced words of minimal length in $\gamma_i I$ and $\gamma_j I$, so that u and v have length g_i and g_j respectively. There is no loss of generality in assuming that the final letter of u is the same as the first letter of v. Then $w = [u, v] = u^{-1}v^{-1}uv$ is in $\gamma_{i+j}I$ and (after cancellation) its length is $2(g_i + g_j - 1)$. Since w is a cyclically reduced, and it is in $\gamma_{i+j}I$ we have

$$g_{i+j} \leq 2(g_i + g_j - 1).$$

A simple induction argument leads to the result that g_i is $O(i^2)$.

It remains to determine n_i, the number of vertices of LC_i. The results of Waldinger [41] and others show that $\gamma_i I/\gamma_{i-1}I$ is an elementary abelian 2-group of order 2^{λ_i}, where λ_i can be effectively computed. In fact,

$$\lambda_2 = 3,\ \lambda_3 = 3,\ \lambda_4 = 5, \text{ and generally } \lambda_n = O(2^n).$$

.

It follows that $n_i = 2^{\lambda_2+\lambda_3+\cdots+\lambda_i}$ is $O(2^{2^i})$. Hence $(\log_2 n_i)/g_i$ is unbounded as $i \to \infty$. Thus, although $g_i \to \infty$ for the family $\mathcal{LC} = \{LC_i\}$, the number of vertices grows so fast that $c(\mathcal{LC}) = \infty$. □

Example 8.4 If we choose a set of cyclically reduced words $w(a, b, c)$ and impose the relations $w = 1$ on I it is unlikely that the resulting group will be finite. For example, prescribing the orders of ab, bc, and ca by means of the relations

$$(ab)^l = (bc)^m = (ca)^n = 1$$

defines a *Coxeter group*, which (except in a few very special cases) is infinite. However, occasionally a happy choice of additional relations will work. For example, the relations

$$abcbcacab = (ab)^5 = (bc)^5 = (ca)^5 = 1$$

are sufficient to define the alternating group A_5 of order 60. The graph is Foster's graph of girth 9 discussed in Example 7.3. □

9. Geometrical constructions

There are several constructions that produce families of cubic graphs with large girth, based on configurations of points on a projective line. The points on the line $PG(1, q)$ (q a prime power) can be identified with the set $GF(q) \cup \{\infty\}$, by using 'homogeneous coordinates'. For simplicity, we shall discuss only the case when $q = p$, a prime.

Any set of four points x_1, x_2, x_3, x_4 on $PG(1, p)$ has a *cross-ratio*

$$\frac{(x_1 - x_3)(x_2 - x_4)}{(x_1 - x_4)(x_2 - x_3)}.$$

Clearly, the cross-ratio is a property of the two unordered pairs x_1, x_2 and x_3, x_4, and when it takes the value -1 we say that the two pairs are *harmonic conjugates*. A *triplet* is simply an unordered triple of points $\{x, y, z\}$ on $PG(1, p)$. Define an adjacency relation on the set of triplets by the rule that $\{x, y, z\}$ is adjacent to the three triplets

$$\{x', y, z\}, \quad \{x, y', z\}, \quad \{x, y, z'\},$$

where x', y', z' are chosen so that x, x' and y, z are harmonic conjugates, y, y' and x, z are harmonic conjugates and z, z' and x, y are harmonic conjugates. We get a cubic graph with $\binom{p+1}{3} = p(p^2-1)/6$ vertices. In the case $p \equiv 1 \pmod 4$ the graph has two components, and when $p \equiv 3 \pmod 4$ it has one component. In either case, we denote a component by $T(p)$; for example, $T(5)$ is Petersen's graph.

One way of studying the triplet graphs [6] depends on a labelling of the infinite cubic tree T which has remarkably far-reaching implications, essentially because it coordinatises the action of the modular group on the upper half-plane. The corresponding geometrical object, sometimes known as the *Farey graph*, was first studied by H. J. S. Smith in 1877 [40]. More recently it has been investigated by Jones, Singerman and Wicks [28], and by Conway [19].

We begin by assigning triples of rational numbers in the closed interval $[0, 1]$ to the vertices of a rooted binary tree B, as follows:

- •1 the root is labelled $(0/1, 1/2, 1/1)$;
- •2 the descendants of the vertex labelled $(a/b, c/d, e/f)$ are labelled

$$(a/b, (a+c)/(b+d), c/d) \quad \text{and} \quad (c/d, (c+e)/(d+f), e/f).$$

It be can shown that the label $(a/b, c/d, e/f)$ of a vertex is uniquely determined by the middle term c/d. Furthermore, the labelling of B can be extended to the cubic tree T as follows. Let P denote a two-way infinite path whose vertices are labelled with the integers $\ldots, -2, -1, 0, 1, 2, \ldots$, in the obvious way. For each integer n let B_n be a copy of B and assign the label $n + \frac{c}{d}$ to the vertex corresponding to the one labelled $\frac{c}{d}$ in B_0. Join the root of B_n, labelled $n + \frac{1}{2}$, to the vertex labelled n in P.

This construction produces a labelling of T that has many remarkable properties, discussed in the references given above. For our purposes the important thing is that when we collapse the labelled tree T modulo a prime p, we obtain the triplet graph $T(p)$. By analysing the labels carefully, we obtain the following result [6].

Theorem 9.1 If $p \equiv 3 \pmod 4$ the triplet graph $T(p)$ is a cubic graph whose girth g_p satisfies

$$F(g_p + 1) \geq p^2,$$

where $F(i)$ denotes the ith Fibonacci number. □

In terms of the parameter c, this implies that the family of triplet graphs $\mathcal{T}$ is such that $c(\mathcal{T}) \leq 1.04\ldots$. The possibility of a subfamily of $\mathcal{T}$ with 'better' girth remains open.

Historically, the first graphs of this kind to be studied were the *sextet graphs* [11]. A *sextet* is a set of three unordered pairs of points on $PG(1,p)$, such that every two pairs are harmonic conjugates. For certain congruence classes of p (mod 8) it is possible to define an adjacency relation on the sextets, such that a cubic graph $S(p)$ is obtained. Weiss [44] proved that the family $\mathcal{S}$ of sextet graphs satisfies $c(\mathcal{S}) \leq 0.75$, and here too an improvement may be possible. Many individual sextet graphs satisfy $c(S(p)) < 0.75$, and the family provides some of the current-best examples. For example, the sextet graph $S(31)$ with 620 vertices is the current-best with girth 15. Further examples will be found in the Historical Notes.

Other families constructed in a similar way, such as the *hexagon graphs*, have been studied by Hoare [26]. The hexagon graph $H(47)$ is the current-best with girth 19.

10. Open questions

The notation is that used in the rest of the paper. Note that not all the questions are independent; for example, a positive answer to Question 2 would provide a solution to Question 1.

1. Find an infinite family $\mathcal{G}$ of cubic graphs for which it can be proved that $c(\mathcal{G})$ is strictly less than 3/4.

2. Is it true that, for all $h \geq 1$, we can add edges to a cycle of length 2^{2h} to get a cubic graph of girth $3h$? In other words, is there a Hamiltonian cubic graph with 2^{2h} vertices and girth $3h$?

3. Suppose $s \geq 4$, and let K consist of 2^s disjoint cycles of length 2^s. Can we add edges to K to form a cubic graph of girth $3s$?

4. Let S be a subgraph of a cubic graph G, with the conditions as in Section 4, except that S may be disconnected. If G has girth g, find suitable conditions under which $G \ominus S$ has girth $g-1$.

5. Find new current-best graphs with girth 13 and 14. (The long tenure of the title of current-best by the graphs with 272 and 406 vertices respectively is becoming an embarrassment.)

6. Under what conditions is there an identity word for a family of cubic Cayley graphs that is 'universal', in the sense described in Examples 5.2 and 6.1? (In fact, we really need conditions which guarantee that no such word exists.)

7. Let T_r be a family of trees with vertices of degree not exceeding 3, each tree with a given edge-3-colouring. Let $\mathcal{P} = (P_r)$ be the family of cubic Cayley graphs defined by the corresponding involutory permutations. Can we construct examples in which the girth of P_r tends to infinity and $c(\mathcal{P})$ is finite?

8. Let $G = PSL(2,q)$ where q is a prime power of the form $3r+1$, and let ω be a cube root of unity in $GF(q)$. Let α be an involution $x \mapsto (x-b)/(cx-1)$ in G, and let β, γ be its conjugates with respect to the maps $x \mapsto \omega x$, $x \mapsto \omega^2 x$. What conditions on b and c guarantee that α, β, γ generate G? If they do generate G, what is the girth of the resulting Cayley graph?

9. Any finite simple group G (except $U_3(3)$) can be generated by three involutions [33]. Define the *girth* of G to be the maximum girth of a Cayley graph of G with respect to a set of three generating involutions. Compute the girth of the classical groups and the sporadic ones.

10. Is it true that the involutions referred to in Problem 9 can be chosen to be conjugate? Can they be chosen to be conjugate under an element of order 3, assuming that G has such an element? (If the answer is yes, we get a symmetric Cayley graph,)

Historical Notes

These brief notes have been compiled with the assistance of many of the people involved, and they are believed to be correct.

Girth 10 The first example with 70 vertices was found by Balaban [1] in 1972. O'Keefe and Wong [36] showed that 70 is the smallest possible number of vertices. There are just three minimal graphs.

Girth 11 A graph with 112 vertices was published by Balaban [2] in 1973. It was obtained by excising a tree with 14 vertices from the minimal graph with 126 vertices and girth 12 (see below). In 1995 it was announced [14] that no smaller graphs exist, but Balaban's graph is not known to be unique.

Girth 12 In this case the very naive bound (126 vertices) is attained by a unique graph. The graph is associated with configurations studied by classical geometers such as Edge [20], and it is also implicit in the 'geometry of triality' studied by Tits [46]. The underlying structure is the Lie algebra of type G_2, which gives rise to the related concept of a *generalised hexagon*. The first explicitly graph-theoretical treatment is due to Benson [3].

Girth 13 A Cayley graph with 272 vertices was discovered by Hoare in 1981. It is described in [25], also in [7]. At first it seemed likely that this graph would soon be superseded, but in 1997 it remains the current-best. Calculations of Royle have confirmed that there are no smaller symmetric graphs or Cayley graphs with this girth. McKay, Myrvold and Nadon [35] have shown that at least 202 vertices are needed.

Girth 14 A Cayley graph with 406 vertices was discovered by Hoare in 1981. It is described in [25], also in [7]. McKay, Myrvold and Nadon [35] have shown that at least 258 vertices are needed.

Girth 15 The sextet graph $S(31)$ with 620 vertices is a member of the family described by Biggs and Hoare [11] in 1983. The fact that its girth is 15 is stated explicitly in that paper.

Girth 16 An explicit construction of a graph with 990 vertices was described by Biggs at the New York conference in 1985, and is published in the proceedings [7]. The fact that such a graph exists is implicit in the work of Goldschmidt [24], and a related configuration was discussed by Chuvaeva [17].

Girth 17 A graph with 2978 vertices is obtained by excising a tree with 46 vertices from a graph with girth 18 (see below).

Girth 18 Bray, Parker, and Rowley [13] have constructed a graph with 3024 vertices. It is a Cayley graph of the direct product of $PSL(2,8)$ with a cyclic group of order 6. (The method looks hopeful, but has not as yet produced any other contenders.) Earlier, Conder [18] had constructed a graph with 4080 vertices as the Cayley graph of three permutations which generate the group $PSL(2,16)$, and this in turn superseded the hexagon graph $H(37)$ with 4218 vertices [26].

Girth 19 The current-best is the hexagon graph $H(47)$ on 4324 vertices [26].

Girth 20 Bray, Parker, and Rowley [13] discovered that constructing Cayley graphs that have triangles, and then collapsing the triangles, can lead to graphs with large girth. Using this 'collapsing method' they obtain a graph with 8096 vertices and girth 20. It supersedes as current-best the bipartite double covering of $H(47)$, which has 8648 vertices.

Girth 21 The current-best is a graph on 16112 vertices obtained by excising a tree with 94 vertices from the sextet graph $S(73)$ (see below). This just beats the hexagon graph $H(73)$ which has 16206 vertices and girth 21.

Girth 22 The sextet graph $S(73)$ has 16206 vertices and its girth is 22, as stated by Biggs and Hoare [11] in 1983. (The graph is also listed in [7], but there it is erroneously stated to be $S(89)$.)

Girth 23 The current-best is a graph with 49482 vertices obtained by excising a tree with 126 vertices from a graph with 49608 vertices and girth 24 (see below). Earlier, Conder [18] had constructed a Cayley graph of Type 1 for the group $PSL(2,53)$ which has order 74412 and girth 23, and subsequently [personal communication, November 1997] he found a graph with 59640 vertices and girth 23.

Girth 24 The collapsing method [13] produces a graph with 49608 vertices.

Girths 25 and 26 The collapsing method [13] produces a graph with 109 200 vertices and girth 26, from which a graph with girth 25 is obtained by excising a tree with 190 vertices. These graphs supersede the sextet graph $S(151)$ which has 143 450 vertices and girth 26 [11], and the graph obtained from it by excising a tree with 190 vertices.

Girth 27 The collapsing method [13] produces a graph with 285 852 vertices and girth 27.

Girth 28 The collapsing method [13] produces a graph with 415 104 vertices and girth 28.

Girth 29 The collapsing method [13] produces a graph with 1 143 408 vertices and girth 29.

Girth 30 The sextet graph $S(313)$ has 1 227 666 vertices and girth 30 [11].

Girths 31 and 32 The collapsing method [13] produces a graph with 3 650 304 vertices and girth 32. Excising a tree with yields a graph with 3 649 794 vertices and girth 31. Earlier, Hoare [unpublished, c.1989] had found that the girth of the hexagon graph $H(373)$ is 32. It has 4 324 562 vertices.

Girths 33 and 34 Hoare [unpublished, c.1989] found that the girth of the sextet graph $S(761)$ is 34. It has $18\,362\,930 = 2^{(0.7097\ldots)g}$ vertices. Excising a tree with 766 vertices produces a graph with girth 33.

Girths 35 and 36 Hoare [unpublished, c.1989] found that the girth of the sextet graph $S(857)$ is 36. It has $26\,225\,914 = 2^{(0.6846\ldots)g}$ vertices. Excising a tree with 1022 vertices produces a graph with girth 35.

References

1. A. T. Balaban, A trivalent graph of girth 10. *J. Combinatorial Theory* 12 (1972) 1–5.
2. A. T. Balaban, Trivalent graphs of girth 9 and 11 and relationships among cages. *Rev. Roum. Math. Pures et Appl.* 18 (1973) 1033–1043.
3. C. T. Benson, Minimal regular graphs of girth 8 and 12. *Canad. J. Math.* 18 (1966) 1091–1094.
4. N. L. Biggs, *Algebraic Graph Theory* (2nd ed.), Cambridge University Press, 1993.
5. N. L. Biggs, Pictures. In: *Combinatorics* (eds. D.J.A.Welsh and D.R. Woodall), Institute of Mathematics and its Applications, 1972, pp. 1–17.
6. N. L. Biggs, Graphs with large girth. *Ars Combinatorica* 25C (1987) 73–80.
7. N. L. Biggs, Cubic graphs with large girth. (In: *Combinatorial Mathematics*: Proceedings of the Third International Conference) *Annals of the New York Academy of Sciences* 555 (1989) 56–62.
8. N. L. Biggs, Girth and residual finiteness. *Combinatorica* 8 (1988) 307–312.
9. N. L. Biggs and A. G. Boshier, Note on the girth of Ramanujan graphs. *Journal of Combinatorial Theory Series B* 49 (1990) 190–194.
10. N. L. Biggs and M. J. Hoare, A trivalent graph with 58 vertices and girth 9. *Discrete Mathematics* 30 (1980) 299–301.
11. N. L. Biggs and M. J. Hoare, The sextet construction for cubic graphs. *Combinatorica* 3 (1983) 153–165.
12. B. Bollobás, *Extremal Graph Theory.* Academic Press, London 1978.
13. J. Bray, C. Parker, and P. Rowley, Graphs related to Cayley graphs and cubic graphs of large girth. Preprint April 16, 1998.
14. G. Brinkmann, B. D. McKay, and C. Saager, The smallest cubic graphs of girth nine. *Combinatorics, Probability and Computing* 5 (1995) 1–13.
15. I. Z. Bouwer, *The Foster Census*, Charles Babbage Research Centre, Winnipeg 1988.
16. P. Chiu, Cubic Ramanujan graphs. *Combinatorica* 12 (1992) 275–285.
17. I. A. Chuvaeva, A combinatorial configuration associated with the group M_{12}. In: *Methods for Complex System Studies* (in Russian). Moscow 1983, pp. 47–52.

18. M. Conder, Small trivalent graphs of large girth. Preprint June 1997.
19. J. H. Conway, The Sensual Quadratic Form. *Carus Mathematical Monographs No. 26* 1997.
20. W. L. Edge, A second note on the simple group of order 6048. *Proc. Cambridge Philos. Soc.* 59 (1963) 1–9.
21. P. Erdős and H. Sachs, Reguläre Graphen gegebene Taillenweite mit minimaler Knotenzahl *Wiss. Z. Univ. Hall Martin Luther Univ. Halle–Wittenberg Math.–Natur.Reine* 12 (1963), 251–257.
22. R. Frucht, A one-regular graph of degree three. *Canad. J. Math.* 4 (1952) 240–247.
23. R. Frucht, Remarks on finite groups defined by generating relations. *Canad. J. Math.* 7 (1955) 8–17. Correction: *ibid.* 413.
24. D. Goldschmidt, Automorphisms of trivalent graphs. *Ann. Math.* 111 (1980) 377–406.
25. M. J. Hoare, On the girth of trivalent Cayley graphs. *Graphs and Other Combinatorial Topics* (Proceedings of the Third Czechoslovak Symposium on Graph Theory, Prague 1982), Teubner, Leipzig 1983, pp.109–114.
26. M. J. Hoare, Triplets and hexagons. *Graphs and Combinatorics* 9 (1993) 225–233.
27. W. Imrich, Explicit construction of regular graphs without short cycles. *Combinatorica* 4 (1984) 53–59.
28. G. A. Jones, D. Singerman and K. Wicks, The modular group and generalised Farey graphs. In: *Groups St Andrews 1989 Volume 2* (eds. C.M. Cambell and E.F. Robertson), Cambridge University Press, 1990, pp 316–338.
29. F. Lazebnik, V. A. Ustimenko, A. J. Woldar, A new series of dense graphs of high girth, *Bulletin of the AMS* 32 (1995), 73–79
30. F. Lazebnik, V. A. Ustimenko, A. J. Woldar, New upper bounds on the order of cages *Electronic Journal of Combinatorics* 4 (1997) R13.
31. L. Lovász, *Combinatorial Problems and Exercises.* North-Holland Amsterdam, 1979.
32. A. Lubotzky, R. Phillips, R. Sarnak, Ramanujan graphs, *Combinatorica* 8 (1988) 261–277.
33. G. Malle, J. Saxl, and T. Weigel, Generators of classical groups. *Geom. Dedicata* 49 (1994) 85–116.
34. G. A. Margulis, Explicit group-theoretical construction of combinatorial schemes and their application to the design of expanders and concentrators. *Journal of Problems of Information Transmission* (1988) 39–46.
35. B. McKay, W. Myrvold, and J. Nadon, Fast backtracking principles applied to find new cages. *Proceedings of the Ninth Annual ACM-SIAM Symposium on Discrete Algorithms* 1998, pp.188–191.

36. M. O'Keefe and P-K. Wong, A smallest graph of girth 10 and valency 3. *J. Combinatorial Theory Series B* 29 (1980) 91–105.

37. G. Royle, Cubic cages, http://www.cs.uwa.edu.au/˜gordon/cages/index.html.

38. H. Sachs, Regular graphs with given girth and restricted circuits, *J. London Math. Society* 38 (1963), 423–429

39. N. Sauer, Extremaleigenschaften regulärer Graphen gegebener Taillenweite, I and II, *Sitzungsberichte Österreich. Acad. Wiss. Math. Natur. Kl.*, S-B II, 176 (1967), 9–25; 176 (1967), 27–43.

40. H. J. S. Smith, Memoire sur les equations modulaires. *Ac. de Lincei* 1877 (= *Collected Papers*, Chelsea, New York 1965, 224–241).

41. H. Waldinger, The lower central series of groups of a special class. *J. Algebra* 14 (1970) 229–244.

42. H. Walther, Eigenschaften von regulären Graphen gegebener Taillenweite und minimaler Knotenzahl, *Wiss. Z. Ilmenau* 11 (1965), 167–168.

43. H. Walther, Über reguläre Graphen gegebener Taillenweite und minimaler Knotenzahl, *Wiss. Z. Techn. Hochsch. Ilmenau* 11 (1965), 93–96.

44. A. Weiss, Girths of bipartite sextet graphs. *Combinatorica* 4 (1984) 241–245.

45. P-K. Wong, Cages – A Survey, *Journal of Graph Theory* 6 (1982) 1–22.

46. J. Tits. Sur la trialité et certains groupes qui s'en deduisent. *Inst. Hautes Etudes Sci. Publ. Math.* 2 (1959) 14–60.

47. W. T. Tutte, *Connectivity in Graphs*. University of Toronto Press, 1966.