THE GIRTH OF CUBIC GRAPHS

A Thesis submitted for the degree of
Doctor of Philosophy
in
the Royal Holloway College
University of London

by

Miles Hoare
ABSTRACT

We start with an account of the known bounds for \( n(3, g) \), the number of vertices in the smallest trivalent graph of girth \( g \), for \( g \leq 12 \), including the construction of the smallest known trivalent graph of girth 9. This particular graph has 58 vertices - the 32 known trivalent graphs with 60 vertices are also catalogued and in some cases constructed.

We prove the existence of vertex-transitive trivalent graphs of arbitrarily high girth using Cayley graphs. The same result is proved for symmetric (that is vertex-transitive and edge-transitive) graphs, and a family of 2-arc-transitive graphs for which the girth is unbounded is exhibited. The excess of trivalent graphs of girth \( g \) is shown to be unbounded as a function of \( g \).

A lower bound for the number of vertices in the smallest trivalent Cayley graph of girth \( g \) is then found for all \( g \leq 9 \), and in each case it is shown that this bound is attained. We also establish an upper bound for the girth of Cayley graphs of subgroups of \( \text{Aff}(p^f) \) the group of linear transformations of the form \( x \rightarrow ax + b \) where \( a, b \) are members of the field with \( p^f \) elements and \( a \) is non-zero. This family contains the smallest known trivalent graphs of girth 13 and 14, which are exhibited.

Lastly a family of 4-arc-transitive graphs for which the girth may be unbounded is constructed using "sextets". There is a graph in this family corresponding to each odd prime, and the family splits into several subfamilies depending on the congruency class of this prime modulo 16. The graphs corresponding to the primes congruent to 3, 5, 11, 13
modulo 16 are actually 5-arc-transitive. The girth of many of these graphs has been computed and graphs with girths up to and including 32 have been found.
<table>
<thead>
<tr>
<th>CONTENTS</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chapter 1</td>
<td>6</td>
</tr>
<tr>
<td>Chapter 2</td>
<td>11</td>
</tr>
<tr>
<td>Chapter 3</td>
<td>19</td>
</tr>
<tr>
<td>Chapter 4</td>
<td>31</td>
</tr>
<tr>
<td>Chapter 5</td>
<td>49</td>
</tr>
<tr>
<td>Appendix</td>
<td>73</td>
</tr>
<tr>
<td>Tables</td>
<td>75</td>
</tr>
<tr>
<td>References</td>
<td>84</td>
</tr>
</tbody>
</table>
ACKNOWLEDGEMENTS

I debated whether to use this page to mention everyone from my hairdresser to Bob Dylan who had contributed however miscellaneously to the completion of this thesis, but in the end I settled for just two people. First I would like to thank Mrs. Marion Brooker who has typed all this very painstakingly and shown great patience all the while.

My main thanks must go to Mr. Norman Biggs my supervisor who has been a constant source of help and ideas throughout my three years at the Royal Holloway College.
Chapter 1

Introduction

1.1 Glossary

At the outset it is necessary to outline some of the basic concepts of graph theory and define some of the notation that will be used. In general we follow the notation used in R.J. Wilson's Introduction to Graph Theory [37] and N.L. Biggs Algebraic Graph Theory [5].

A graph $G$ consists of a set $V(G)$ of elements called vertices and a set $E(G)$ of elements called edges together with a relation of incidence which associates with each edge two vertices called its ends. If none of the edges have coincident ends, and no two edges are incident with the same pair of vertices, then we say $G$ is a simple graph, and indeed we shall be dealing exclusively with simple graphs, or more briefly graphs. The two ends of an edge are said to be adjacent. We define a path of length $\ell$ in $G$ joining $v_i$ to $v_j$ to be a finite sequence of vertices of $G$

$$v_1 = u_0, u_1, \ldots, u_\ell = v_j$$

such that $u_{t-1}$ and $u_t$ are adjacent for $1 \leq t \leq \ell$, and $u_{t-1}$ and $u_{t+1}$ are distinct $1 \leq t \leq \ell-1$. A circuit or cycle is a path in which the endvertices coincide. An $s$-arc is the ordered set of vertices underlying a path of length $s$.

A subgraph of a graph $G$ is simply a graph all of whose vertices belong to $V(G)$ and all of whose edges belong to $E(G)$. A graph $G$ is connected if for each pair of vertices $v_i, v_j$ in $V(G)$, there is a $v_i v_j$ path in $G$. A maximal connected subgraph of $G$ is a component of $G$. The degree or valency of a vertex $v$ is the number of edges incident
with \( v \), and if every vertex in \( G \) is of degree 3 \( G \) is said to be **trivalent** or **cubic**. The **distance** between two vertices \( x, y \) in graph \( G \) is the length of the shortest path between them and will be denoted \( d_G(x, y) \) (or \( d(x, y) \) if there is no ambiguity).

An **automorphism** \( \varnothing \) of a graph \( G \) is a one-to-one mapping of the vertex set \( \nu(G) \) onto itself with the property that \( \varnothing(v) \) and \( \varnothing(w) \) are adjacent if and only if \( v \) and \( w \) are. These automorphisms form a group under composition called the **automorphism group**. We say that a graph \( G \) is **vertex-transitive** if the automorphism group acts transitively on the vertices and **edge-transitive** if the automorphism group acts transitively on the edges. Further if for all vertices \( u, v, x, y \) of \( G \) such that \( u \) is adjacent to \( v \) and \( x \) is adjacent to \( y \) there is an automorphism \( \varnothing \) such that \( \varnothing(u) = x \) and \( \varnothing(w) = y \), \( G \) is called **symmetric**. A graph \( G \) is **s-arc-transitive** \( (s \geq 1) \) if its automorphism group is transitive on the set of \( s \)-arcs in \( G \), but not transitive on the \( (s + 1) \) arcs in \( G \); thus every symmetric graph is at least 1-arc-transitive. Lastly and most importantly the **girth** of a graph \( G \) (which is the subject of this thesis) is the length of the shortest cycle in \( G \).

**Motivation**

It is not easy to find trivalent graphs with large girth. When this work was begun there were no published examples of trivalent graphs with girth more than 12, although the existence of trivalent graphs with arbitrarily high girth had been proved. Tutte [4] and Bollobás [8] have published proofs that are in some sense constructive.
Both start with a graph \(G\) on \(2^g\) vertices with girth \(g\) in which every vertex has degree 2 or 3 and show that if there are any vertices of degree 2 in \(G\) a graph with more edges also of girth \(g\) and every vertex of degree 2 or 3 may be constructed on the same number of vertices. Pisanski and Shawe Taylor [30] have also produced a construction that develops a trivalent graph of girth \(g+1\) from a cycle permutation graph of girth \(g\), while the number of vertices in the new graph is roughly the square of the number of vertices in the original. The central problem examined in this thesis is the enumeration of \(n(3,g)\), the number of vertices in the smallest trivalent graph of girth \(g\). It is known that this value must exceed a number close to \(2^{\frac{g}{2}}\) [34], and as we have seen it is bounded by \(2^g\), so significance will be attached to the value

\[
c(g) = \log_2(n(3,g))/g
\]

which in turn must lie between \(\frac{1}{2}\) and 1. Although it remains a mystery what happens to \(c(g)\) as \(g\) tends to infinity, in Chapter 5 we will exhibit some trivalent graphs with girth up to 32, and so obtain some upper bounds for \(c(g)\), \(g < 32\).

Contents

In Chapter 2 there is an account of the known bounds for \(n(3,g)\) for \(g \leq 12\), and the smallest known trivalent graph of girth 9 is derived. This particular graph has 58 vertices - the thirty two known graphs of girth 9 with 60 vertices are also catalogued and in some cases constructed.

Chapters 3 and 4 are largely concerned with Cayley graphs. A Cayley graph can be obtained from a group \(G\) with a set of generators \(\Omega\)
not containing the identity satisfying the additional property;

\[-1\]

\[x \in \Omega \Rightarrow x \in \Omega.\]

The Cayley graph \( \Gamma = \Gamma(G, \Omega) \) is the simple graph whose vertexset and edge set are

\[V(\Gamma) = G; E(\Gamma) = \{(g, b)|g^{-1}b \in \Omega\}.\]

If \( \Omega \) consists of three involutions, or an involution and an element of order greater than 2 and its inverse, the resulting Cayley graph will be trivalent. A trivalent Cayley graph will be said to be **Type I** if its generating set consists of three involutions and **Type II** otherwise.

Chapter 3 contains a proof that there exist trivalent graphs that are Cayley of arbitrarily large girth and a similar result for symmetric graphs (Cayley graphs are all vertex-transitive [5]). It also contains a result concerning the number of vertices in a vertex-transitive graph with valency \( k \) and girth \( g \).

Chapter 4 contains the construction of the smallest trivalent Cayley graphs of girth \( g \) where \( g \leq 9 \), and some examples of groups and generating sets giving trivalent Cayley graphs of girth up to 17. One particular area of investigation will be the Cayley graphs of the groups denoted \( Z(p, \frac{p-1}{2}, k) \) by Coxeter, Frucht and Powers [11] where \( p \) is an odd prime and \( k \) a primitive root modulo \( p \). There is an upper bound on the girth of such graphs which is established and attained.
Because the girth of an $s$-arctransitive graph must be at least $2s-2$ [34], it would seem that highly arctransitive graphs would be a fertile area to look for graphs of large girth. However there is a wellknown theorem of Tutte which states that there are no trivalent $s$-arctransitive graphs with $s > 5$ [35]. In Chapter 5 we show how to construct a family of graphs that are at least 4-arctransitive for which it is conjectured that the girth is unbounded. There is a one-to-one correspondence between members of this family and the odd primes. The family subdivides into several subfamilies depending on the congruency class of the prime modulo 16. The subfamily of graphs corresponding to primes congruent to 1 or 15 modulo 16 is the same set of graphs as that defined by Wong in terms of primitive subgroups of the projective special linear group $\text{PSL}(2,p)$ [38]. As shall be shown the number of vertices in the graph corresponding to prime $p$ is of the order of $p^3$ if $p$ is congruent to 1 or 7 modulo 8 and of the order of $p^6$ otherwise.

Some of the most interesting results are those portrayed in the numerical tables to be found at the back of the thesis. Firstly there is a table showing the smallest known trivalent graphs of girth $g \leq 17$ and some of their properties. Secondly there is a table giving the girths and degree of arctransitivity of the Cayley graphs of $\text{Z}(p,(p-1)/2,k)$ where $p$ is a prime less than or equal to 23; finally there are various tables associated with the sextet construction of Chapter 5.
Chapter 2

The (3, g) cages 2 ≤ g ≤ 12

A (3, g)-cage is defined as a trivalent graph with girth g such that there are no other graphs with less vertices with these properties. This chapter will be devoted to the search for (3, g)-cages in the cases 2 ≤ g ≤ 12 in particular the case g = 9.

Lower bound for \( n(3, g) \)

There is a lower bound on the number of vertices in a trivalent graph of girth g either obtained by counting the number of vertices at distance strictly less than \( \frac{g+1}{2} \) from a given vertex or by counting those vertices at distances less than \( \frac{g}{2} \) from either endvertex of a given edge [34]. If graph G is trivalent and has girth g and n vertices then

\[
\begin{align*}
    n \geq 3\left(\frac{g-1}{2}\right) - 2 & \quad \text{if } g \text{ is odd}, \\
    n \geq 2^{\frac{g}{2}+1} - 2 & \quad \text{if } g \text{ is even}.
\end{align*}
\]

This minimum is rarely attained. The excess \( e(3, g) \) is defined as the difference between \( n(3, g) \), the number of vertices in a (3, g)cage, and the minimum \( n_o(3, g) \) where

\[
\begin{align*}
    n_o = 3\left(\frac{g-1}{2}\right) - 2 & \quad \text{if } g \text{ is odd}, \\
    n_o = 2^{\frac{g}{2}+1} - 2 & \quad \text{if } g \text{ is even}.
\end{align*}
\]
The Known \((3,g)\) cages

By considering the multiplicities of the eigenvalues of the collapsed adjacency matrices it has now been shown by various authors that the excess \(e(3,g)\) can be zero only if \(g\) is equal to \(3,4,5,6,8,\) or \(12\) (see [5]).

All these values of \(g\) correspond to unique cages with excess zero. The \((3,g)\) cages for \(g = 3,4,5,6,8\) respectively are the complete graph \(K_4\), the complete bipartite graph \(K_{3,3}\), the Petersen graph on 10 vertices, the Heawood graph which has 14 vertices, and the Tutte graph on 30 vertices. Their uniqueness is proved by Tutte [34], as is the uniqueness of the McGee graph which has 24 vertices and girth 7 and consequently has excess 2. The \((3,12)\) cage on 126 vertices is described by Biggs [5] and Benson [4] and was proved unique by Rees [33] and others. O'Keefe and Wong [29] have proved that a \((3,10)\) cage must have 70 vertices and excess 8 and that there are at least 3 of these cages. One of them was found by Balaban, and the other two were discovered by O'Keefe and Wong and independently by Harries and will be referred to here as \(X\) and \(Y\).

Girth 9 and "Tree-Removal"

From the three graphs with 70 vertices, graphs with 60 vertices and girth 9 may be constructed as follows.

Let \(v\) be a vertex in a trivalent graph \(G\) of girth 10 and let \(v_1, v_2, \ldots, v_{12}\) be the 12 vertices at distance 3 from \(v\) such that \(v_i\) is at distance 2 from \(v_{i+1}\) if \(i\) is odd.
Define a new graph $H$ whose vertex-set and edge set are

$$V(H) = V(G) \setminus \{x \in V(G) \mid d_G(v,x) \leq 2\}$$

and

$$E(H) = [E(G) \setminus (V(H) \times V(H))] \cup A$$

where $A$ is the set of edges $\{(v_1,v_2), \ldots, (v_{11},v_{12})\}$.

The new graph $H$ is trivalent; we now prove every cycle in $H$ is

Let $C$ be a cycle in the graph $H$.

If no edges in $C$ are in $A$, then $C$ is a cycle of $G$ and

consequently of length at least 10.

If there is just one edge $(v_i,v_{i+1})$ say which is in both $C$ and $A$,
then there is a circuit $C'$ in $G$ corresponding to $C$ with the edge
$(v_i,v_{i+1})$ replaced by two edges since $v_i$ and $v_{i+1}$ are at distance
2 in $G$. But $G$ has girth 10 so $C'$ has at least 10 edges and $C$
must contain at least nine edges.

If $C$ contains two or more edges in $A$ it must also contain 2 paths
$v_a v_b$ and $v_c v_d$ in $H$ where $v_a, v_b, v_c,$ and $v_d$ are all in $\{v_1, v_2, \ldots, v_{12}\}$.
There are paths from $v_a$ and $v_b$ to $v$ of length 3 in $G$, so there is a $v_a v_b$ path of length at most 6 in $G$ but not in $H$. If there was a $v_a v_b$ path of length less than 4 in $H$, $G$ would contain a cycle with less than 10 edges, so $d_H(v_a, v_b)$ must be at least 4. Similarly $d_H(v_c, v_d)$ must also be at least 4. Hence $C$ contains at least 10 edges, and $H$ has girth at least 9.

This result may be generalized to obtain an upper bound for $n(g, 3)$ in terms of $n(g + k, 3)$ for all $g \geq 6$ as follows.

**Proposition**

$$n(g, 3) \leq n(g + 1, 3) - n_0\left(\left\lceil \frac{(g+2)}{2} \right\rceil, 3\right).$$

**Proof**

Let $G$ be a trivalent graph of girth $g$ and let

$$\Delta_r(x) = \{ v \in V(G) \mid d_G(v, x) = r \}.$$

Then $\bigcup_{r=0}^{s} \Delta_r(x)$ is a tree consisting of all vertices at distance less than $s+1$ from $x$ if $g > 2s$ and we shall say it is rooted at $x$, and has radius $s$. If $\left\lceil \frac{g}{2} \right\rceil$ is odd it is possible to create a graph $H$ of girth at most $g-1$ by replacing the tree rooted at a given vertex $x$ with radius $s = \left\lceil \frac{g-4}{2} \right\rceil$ with edges joining those vertices in $\Delta_s(x)$ at distance 2 from each other.

If $\left\lceil \frac{g}{2} \right\rceil$ is even, if a given edge $(y, x)$ in $E(G)$ is contracted to single vertex $x$ of valency 4, and then the tree $\bigcup_{i=0}^{s} \Delta_i(x)$
where $s = \left\lfloor \frac{g-6}{2} \right\rfloor$ and those vertices in $\Delta_{g+1}(x)$ that were at distance 2 in $G$ joined, the new graph will again be at least $g-1$ in girth.

Balaban used this method, starting from the $(3,12)$ cage and removing fourteen vertices to find the smallest known trivalent graph of girth 11 which has 112 vertices [1]. The $(3,12)$ cage is edgetransitive [4], and the tree to be removed is rooted on an edge so only one such graph can be produced in this way.

**Trivalent Graphs of Girth 9 with 60 Vertices.**

More trivalent graphs of girth 9 with 60 vertices can be created from the $(3,10)$ cages by tree removal as the tree to be removed is rooted at a vertex and the three $(3,10)$ cages Balaban, X and Y have 3, 4 and 8 vertex orbits respectively under the action of their automorphism groups. Just two of the resulting graphs are isomorphic, so 14 trivalent 60 vertex girth 9 graphs have been obtained (Harmies, unpublished). Previously five such graphs were known, two of which are Cayley graphs and will be described in Chapter 4. The other three are named after Foster, Evans and Balaban/Biggs respectively. The Evans graph is the only known trivalent graph of girth 9 on 60 vertices that is vertextransitive but is not a Cayley graph. Only one of these graphs, the Cayley graph named after Foster and Frucht [18], has the property that its diameter, which is the maximum distance between two vertices in a given graph, is 5. Graphs with the property that their diameter is less than or equal to $\frac{3}{2}(g+1)$ where $g$ is their girth, are known as generalized Moore graphs. This is the largest known trivalent generalized Moore graph.
Table 4 contains various details about the thirtytwo known 60 vertex trivalent graphs of girth 9 including the number of 9-cycles they contain, the automorphism group and the value of the smallest eigenvalues of their adjacency matrices.

A Trivalent Graph with 58 Vertices and Girth 9

Only one trivalent graph with 58 vertices and girth 9 is known, that being described in a paper by Biggs and Hoare [6]. This was discovered while examining edgereplacement schemes and can be derived from a 60 vertex trivalent graph (itself derived from X) as follows. In this graph XC there exists a subgraph A,B,C,D,E,F,G,H shown in Figure 2.4 with the property that through the 2-arcs ABC and DEF there are no nine-cycles.

It is possible to remove the vertices B,E,H and add the edges (A,C) and (D,F) to obtain a graph \( \Gamma \) on 57 vertices with girth 9, in which every vertex is of degree three except one vertex (G) which has valency 2. Elsewhere in the graph there is an edge \((X,Y)\) such that \(d_{\Gamma}(X,A) = d_{\Gamma}(Y,A) = 7\). By adding a vertex Z to the vertex set of \( \Gamma \), and replacing the edge \((X,Y)\) by the three edges \((X,Z)\), \((Y,Z)\) and \((G,Z)\) a trivalent graph of girth 9 on 58 vertices is obtained.
The Value \( n(3,9) \).

In the known graph on 58 vertices described above there are 2 2-arcs which are not contained in any 9-cycle but unfortunately no means of removing either of them and reconstructing to obtain a trivalent graph on 56 vertices with girth 9 has yet been discovered. Hence the upper bound for \( n(3,9) \) remains 58. Using a computer McKay has shown that \( n(3,9) \) is at least 54 [28], but at present it cannot be said which of the three possible values 54, 56, 58 corresponds to the true number \( n(3,9) \).
Chapter 3

Some Families with Increasing Girth

In this chapter we shall investigate families of cubic graphs with the property that the girth is increasing. As we have mentioned previously, Tutte and others [34] have shown that given $g$ greater than or equal to 3 there exists a finite trivalent graph with girth at least $g$—we start by showing there is a Cayley graph with these properties. The argument is similar to that used by Evans [16] to show that given $k \geq 2$, $g \geq 3$, there is an embeddable $g$-net of valency $k$.

First we need two lemmas.

Lemma

Let $G$ be a group. If $N_1$ and $N_2$ are normal subgroups of finite index in $G$, then the intersection of $N_1$ and $N_2$ is also a normal subgroup of finite index in $G$.

Proof

By the Second Isomorphism Theorem the quotient group $N_1N_2/N$ is isomorphic to $N_2/N_1 \cap N_2$. Now $N_1N_2$ is a subgroup of $G$, and $N_1$ is of finite index in $G$ so $N_1N_2$ must be finite. Also the order of $N_2/N_1 \cap N_2$ is the same as the order of $N_1N_2/N_1$ so $N_2/N_1 \cap N_2$ is finite. But $N_2$ is of finite index in $G$ so $G/N_1 \cap N_2$ is finite.
Let $G$ be the free product of a finite number of cyclic groups. Then $G$ is residually finite, that is given any non-identity element $g$ in $G$ there is a normal subgroup $N_g$ of finite index in $G$ that does not contain $g$.

Proof

This was proved first by Gruenberg [20]. The neatest proof is in a paper by Baumslag and Tretkoff [3].

Theorem 3.1

If $n$ is an integer larger than 2, there is a finite group whose Cayley graph is trivalent and has girth at least $n$.

Proof

Let $G = \langle R_1, R_2, R_3 | R_1^2 = R_2^2 = R_3^2 = 1_G \rangle$, where $1_G$ is the identity element of $G$. Then by the Lemma $G$ is residually finite. Hence given $g$ a non-identity element of $G$ we can find $N_g$ a normal subgroup of finite index in $G$ not containing $g$.

We now use the set of generators $\{R_1, R_2, R_3\}$ to construct $A$ a Cayley graph of $G$, and we denote the vertex in $V(A)$ corresponding to the element $g$ of $G$ by $v_g$. $A$ is in fact the infinite trivalent tree.

Let $S = \{\gamma | \gamma \in G, 0 < d_A(v_1, v_\gamma) < n\}$, that is the set of words in $G$ of length less than $n$. $S$ is finite.

Now let $N = \bigcap_{\gamma \in S} N_{\gamma}$. Then $N$ is of finite index by the Lemma.
Let \( \Gamma \) be the Cayley graph of quotient group \( G/N \) using \( \{NR_1, NR_2, NR_3\} \) as the generating set. We claim \( \Gamma \) has girth at least \( n \).

For suppose there is a cycle of length \( m \) in \( \Gamma \) where \( m \) is strictly less than \( n \). Then

\[
Nw_1Nw_2 \cdots Nw_m = N
\]

so \( Nw_1w_2w_3 \cdots w_m = N \) since \( Ng = gN \) for all \( g \) in \( G \)

and \( w_1w_2 \cdots w_m \) is in \( N \).

But \( w_1w_2 \cdots w_m \) is in \( S \) since \( m < n \), and thus \( w_1w_2 \cdots w_m \) is not in \( Nw_1 \cdots w_m \) and cannot be in \( N \). Hence there can be no cycles of length less than \( n \) in \( \Gamma \) and \( \Gamma \) must have girth at least \( n \).

If the subgroups referred to in the above proof as \( Ng \) are chosen more carefully we can ensure that the Cayley graph \( \Gamma \) is not just vertex-transitive but also edge-transitive.

**Corollary 3.2**

Given \( n \geq 3 \), there exists a finite trivalent graph that is symmetric and has girth at least \( n \).

**Proof**

Again let \( G = \langle R_1, R_2, R_3 \mid R_1^2 = R_2^2 = R_3^2 = 1_G \rangle \), and let \( \Lambda \) be the Cayley graph constructed from \( G \) using \( \{R_1, R_2, R_3\} \) as the set of generators. As in the previous proof we let \( S = \{\gamma \mid \gamma \in G, 0 < d_{\Lambda}(v, v') < n\} \)

Given \( g = R_{i_1} R_{i_2} R_{i_3} \cdots R_{i_m} \) with \( i_j \in \{1, 2, 3\} \) \( 1 \leq j \leq m \), define
Let $G = R_{\mathfrak{m}_1} R_{\mathfrak{m}_2} \ldots R_{\mathfrak{m}_m}$ where $\mathfrak{m}$ represents the permutation (123). $\mathfrak{m}$ is clearly an automorphism of $G$.

Now given $\gamma$ we choose $N_\gamma$ such that $N_\gamma$ is a normal subgroup of finite index in $G$ not containing $\gamma$ such that

$$N_\gamma = < R_1, R_2, R_3 | R_1^2 = R_2^2 = R_3^2 = W_1 = \ldots = W_n = 1_G > \text{ if and only if }$$

$$N_\mathfrak{m} = < R_1, R_2, R_3 | R_1^2 = R_2^2 = R_3^2 = \mathfrak{m} W_1 = \ldots = \mathfrak{m} W_n = 1_G > .$$

since $\gamma \in S$ if and only if $\mathfrak{m} \gamma \in S$ the image of $N = \bigcup_{\gamma \in S} N_\gamma$ under $\mathfrak{m}$ will be $N$.

Let $\Gamma$ be the Cayley graph of $G/N$ using $\{NR_1, NR_2, NR_3\}$ as the set of generators. Then $\Gamma$ has girth at least $n$; it is just required to show that $\Gamma$ is edgetransitive.

Suppose $N_\gamma$ is adjacent to $N_\delta$ in $\Gamma$. Then $\delta_1 = n \gamma_2 r$ for some $n$ in $N$ and some $r$ in $\{R_1, R_2, R_3\}$. This means

$$\mathfrak{m} \delta_1 = \mathfrak{m} (n \gamma_2 r)$$

$$= n' \mathfrak{m} \gamma_2 \mathfrak{m} r$$

$$= n' \mathfrak{m} \gamma_2 \mathfrak{m} r \text{ where } n' \in N \text{ and }$$

$\mathfrak{m} r$ must be in $\{R_1, R_2, R_3\}$ and so $N \mathfrak{m} \delta_1$ is adjacent to $N \mathfrak{m} \gamma_2$. Hence $\mathfrak{m}$ represents an automorphism of $\Gamma$ and it stabilizes the vertex corresponding to the identity element while cyclically permuting its adjacent vertices. Since $\Gamma$ is a Cayley graph and all Cayley graphs are vertextransitive [5] $\Gamma$ must be symmetric. $
$

The same results can be obtained for $k$-valent graphs where $k > 3$ by similar methods. As we shall see we can also construct trivalent
2-arc-transitive graphs in this way. We use the **Lower Central Series** of the group \( G = \langle R_1, R_2, R_3 | R_1^2 = R_2^2 = R_3^2 = 1_G \rangle \).

**Definitions**

Given \( x, y \) elements in a group \( G \), we write the **commutator** \( x^{-1}y^{-1}xy \) as \((x, y)\). For subgroups \( A, B \) of \( G \) the notation \((A, B)\) will mean the group generated by all \((a, b)\) with \( a \in A, b \in B \). If \( G_0 = G \) and \( G_{n+1} = (G_n, G) \) for \( n \geq 1 \), the series

\[
G = G_0 \geq G_1 \geq G_2 \ldots
\]

is called the **Lower Central Series** of \( G \). If \( g \) is a member \( G_i \) but not a member of \( G_{i+1} \) we say \( g \) is a commutator of weight \( i \). We have that \( G_i \) is a normal subgroup of \( G \) for all \( i \).

Let \( G = \langle R_1, R_2, R_3 | R_1^2 = R_2^2 = R_3^2 = 1_G \rangle \), and let \( G_i \) denote \((G, G_{i-1})\) where \( G_0 = G \), that is the \( i \)th term in the **Lower Central Series** of \( G \). Let \( \Gamma_i \) correspond to the Cayley graph of the quotient group \( G / G_i \) using \( \{G_i R_1, G_i R_2, G_i R_3\} \) as the generating set.

**Theorem**

The girth of \( \Gamma_i \) increases unboundedly.

**Proof**

Mal'cev [27] has shown that \( G \) is an \( N \)-group, that is the infinite intersection \( \bigcap_{i>1} G_i \) is the identity element in \( G \). This means that given an element \( g \) of \( G \), there exists \( r_g \) such that \( g \) is not in \( G_i \) for all \( i \) greater than \( r_g \).
As in the proof of Theorem 3.1, we let $A$ be the Cayley graph of $G$ using generating set $\{R_1, R_2, R_3\}$ and define

$$S_n = \{\gamma | \gamma \in G, 0 < d_A(v_1, v_\gamma) < n\}$$

where $v_\gamma$ represents the vertex in $V(A)$ corresponding to the group element $\gamma$ in $G$.

Now let $r$ be the largest value of $r$ for all $\gamma$ in $S_n$. Then the girth of $\Gamma_r$ must be at least $n$ by a similar argument as that used in Theorem 3.1.

The graphs $\Gamma_r$ are finite. Caglione [19] has shown that $G_i / G_{i+1}$ is elementary Abelian of order $2^{\lambda_n}$ where

$$\lambda_n = \frac{1}{n} \sum_{k|n, k>1} \mu(n/k) (\log k)$$

where $\mu$ is the Möbius function, and

$$a_n = \frac{1}{n!} \left. \frac{d^n}{dx^n} \ln[1 - 2x^3 - 3x^2] \right|_{x=0}$$

From these formulae we can calculate the order of $G_i / G_1$, and hence we find the number of vertices in $\Gamma_i$ is given by

$$2^L \text{ where } L = \sum_{n=1}^{i} \lambda_n$$

The first nontrivial graph in the sequence $\Gamma_i$ is $\Gamma_2$ which is the cube. This has 8 vertices and girth 4. $\Gamma_3$ has 64 vertices and girth 8 [17], while $\Gamma_4$ has $2^{11}$ vertices and has been computed to have girth 14.

**Theorem 3.4**

The girth of $\Gamma_i$ is less than $i^2$ if $i \geq 3$. 

Proof

First we need a result concerning the weight of a commutator. If 
\( u \) is in \( G_i \) and \( v \) is in \( G_j \), then \((u,v)\) is in \( G_{i+j} \) \([21]\),
and the words \((u,v)\) and \((u^{-1},v)\) correspond to cycles in \( \Gamma_{i+j} \).

Choose \( u \) and \( v \) such that the lengths of the words \( u \) and \( v \)
correspond to the girths of \( \Gamma_i \) and \( \Gamma_j \) respectively, and \((u,v)\)
is not the identity element.

Let \( u = R_a \ldots R_b \); \( R_a \neq R_b \) since \( R_a u R_a \) is in \( \Gamma_i \) and would
be of shorter length than \( u \) if \( R_a \) were the same as \( R_b \). Similarly
let \( v = R_c \ldots R_d \) where \( R_c \) is different from \( R_d \).

Then \((u,v) = R_a \ldots R_b \ldots R_c \ldots R_d \). If there is no
cancellation in \((u,v)\), that is \( R_a \neq 1 \), \( R_b \neq 1 \) and \( R_c \neq 1 \),
there must be a cancellation in

\[(u^{-1},v) = R_a \ldots R_b \ldots R_c \ldots R_d \] since \( R_b = R_d \).

Hence if \( g(\Gamma_i) \) represents the girth of the graph \( \Gamma_i \)

\[ g(\Gamma_{i+j}) \leq 2(g(\Gamma_i) + g(\Gamma_j)) - 2 \]

so

\[ g(\Gamma_{2n}) \leq 4g(\Gamma_n) - 2 \]

and

\[ g(\Gamma_{2n+1}) \leq 2(g(\Gamma_n) + g(\Gamma_{n+1})) - 2. \]

Suppose \( g(\Gamma_i) \leq i^2 \) whenever \( 2 \leq i < n \).

Now if \( n = 2i \) \( g(\Gamma_n) \leq 4(g(\Gamma_i)) - 2 \leq n^2 - 2 < n^2 \)
and if \( n = 2i+1 \) \( g(\Gamma_n) \leq 2(g(\Gamma_i) + g(\Gamma_{i+1})) - 2 \leq (2i+1)^2 - 1 < n^2 \).
26.

But \( g(\Gamma_2) = 4 \) and \( g(\Gamma_3) = 8 \) so by induction

\[
g(\Gamma_i) < i^2 \text{ whenever } i \text{ is greater than } 2. \]

We now turn our attention to the values \( c_{\lambda_i} \) if the number of vertices in \( \Gamma_i \) or \( |V(\Gamma_i)| \) is taken to be \( 2^{c_i g(\Gamma_i)} \). Recall that \( \lambda_i \) is given in equation (1) and \( a_i \) is given in equation (2), but \( a_i \) is alternatively seen to be the coefficient of \( x^n \) in the infinite sum

\[
A = 6(x^2 + x) \sum_{i=0}^{\infty} (2x^3 + 3x^2)^i.
\]

Since \( (1-3x^2-2x^3) = (2x-1)(x+1)^2 \) and the nearest zero to the origin is \( x = \frac{1}{2} \), the radius of convergence of \( \sum_{n=0}^{\infty} a_n x^n \) is \( \frac{1}{2} \) and consequently as \( n \to \infty \), \( \frac{a_{n+1}}{a_n} \to 2 \).

But \( a_n \) is much the largest term in the sum

\[
\frac{1}{\lambda_n} \sum_{k=1}^{\infty} \mu(n/k) k a_k
\]

so \( \frac{\lambda_{n+1}}{\lambda_n} \) also tends to 2 as \( n \) tends to infinity.

Thus as \( n \to \infty \) the number of vertices in \( \Gamma_i \) tends to \( 2^{2i} \) and so as \( g(\Gamma_i) < i^2 \) and \( |V(\Gamma_i)| = 2^{c_i g(\Gamma_i)} \) \( c_i \) tends to infinity as \( i \) tends to infinity.

**Theorem 3.5**

The graphs in the family \( \{\Gamma_i\} \) are all s-arctransitive, where \( s \geq 2 \).

**Proof**

Given \( G = R_{i_1} R_{i_2} \ldots R_{i_m} \) with \( i_j \in \{1, 2, 3\} \) \( 1 \leq j \leq m \), define
27.

\[ \pi g = \pi_{i_1}^{Rn} \pi_{i_2}^{Rn} \cdots \pi_{i_m}^{Rn} \]

where \( \pi \) represents an element of the symmetric group of permutations on the set \( \{1, 2, 3\} \). \( \pi \) is an automorphism of \( G \), and the image of \( G_i \) under \( \pi \) is still \( G_i \).

We follow the proof of Corollary 3.2 and find that \( \pi \) corresponds to an automorphism of the graph \( G_i \) fixing the vertex corresponding to the identity element. Because there are six permutations on 3 letters, the order of the stabilizer of a vertex is at least 6 and the graph \( G_i \) must be at least 2-arctransitive.

Additive Excess

Until now in this chapter we have been viewing excess as a multiplicative function of \( g \). We now show that although \( c(g) \) may tend to \( \frac{1}{2} \) as \( g \) becomes large, the additive excess, the actual number of extra vertices required as the girth increases, is unbounded. In this section not only trivalent graphs will be considered but also graphs in which every vertex has degree \( k \), or \( k \)-valent graphs. Biggs has shown that for each odd integer \( k \) the excess \( e_{k,k}(g) \) of a vertex-transitive graph with valency \( k \) and girth \( g \) is unbounded as a function of \( g \) [7].

It will now be shown this is true for all even integers \( k \) as well.

Let \( G \) be a vertex-transitive graph of girth \( g = 2r + 1 \) and valency \( k \), and let \( \Delta_{i}(v) \) denote the set of vertices at distance \( i \) from a given vertex \( v \). Because there are no cycles of length less than \( g \)

\[ |\Delta_{i}(v)| = k(k-1)^{i-1} \quad i \leq r. \]

The number of cycles of length \( g \) through \( v \) is equal to the number of edges in \( E(G) \) which join two members of \( \Delta_{g}(v) \), and as \( G \) is
vertextransitive this number is a constant x independent of v. Let J denote the number of edges from a vertex of \( \Delta_r(v) \) to one in \( \Delta_{r+1}(v) \). The excess of G is given by \( | \bigcup_{s>r} \Delta_s(v) | \), the number of vertices at distance greater than r from vertex v, and will be denoted by e.

**Lemma**

\[ 0 < \frac{(g-1)}{2} k - 2x \leq k e. \]

**Proof**

Each vertex in \( \Delta_r(v) \) is adjacent to one vertex in \( \Delta_{r-1}(v) \) and k - 1 other ones so that

\[ 2x + J = (k - 1) |\Delta_r(v)|. \]

But \( |\Delta_{r+1}(v)| \leq e \), and each vertex in \( \Delta_{r+1}(v) \) has valency k, so we have \( 0 \leq J \leq ke \). Putting \( |\Delta_r(v)| = \frac{(g-3)}{2} k(k-1) \) gives the required result.

**Theorem 3.6**

For each integer \( k \geq 3 \), there is an infinite sequence of values of g such that the excess of any vertextransitive graph with valency k and girth g satisfies \( e > \sqrt{g/k} \).

**Proof**

Firstly if k is odd, Biggs has shown \( e > \frac{g}{k} \) for all g in an infinite set of primes \( S_k \).
Now if \( k \) is even there is an odd prime \( p \) dividing \((k-1)\). Let \( g = p^{2m} \), where \( m \) is a positive integer. Let the number of cycles of length \( g \) in \( G \) be \( N \) and let the number of vertices \( |V(G)| \) be \( n \).

Each of the \( n \) vertices is contained in \( X \) \( g \)-cycles, so \( nX = Ng \), and \( g \) must divide \( nX \). But \( g = p^{2m} \) so either

\[
X \equiv 0 \pmod{p^m} \quad \text{or} \quad n \equiv 0 \pmod{p^m}.
\]

Suppose first \( X \equiv 0 \pmod{p^m} \).

Then \( J = (k-1)(g-1)/2 - 2X \equiv 0 \pmod{p^m} \).

But \( J > 0 \) since \( G \) is connected, so \( J \geq p^m \).

From the lemma we have \( ke \geq p^m \), so \( e \geq \sqrt{\frac{g}{k}} \).

Next suppose \( n \equiv 0 \pmod{p^m} \).

Now

\[
n = \sum_{s=0}^{\infty} |\bigcup_{s=0}^{r} A_s(v)|
\]

\[
= \sum_{s=0}^{r} |\bigcup_{s=0}^{r} A_s(v)| + e
\]

\[
= 1 + \sum_{s=1}^{r} k(k-1)^{s-1} + e
\]

\[
= \frac{k}{k-2} \{(k-1)^{\frac{1}{2}}(g-1)-1\} + (1+e).
\]

Hence \((k-2)n = k\{(k-1)^{\frac{1}{2}}(g-1)-1\} + (e+1)(k-2)\).
But \( n = 0 \mod p^m \) and \((k-1)\sum_{j=1}^{i}(g-1) = 0 \mod p^m\) since 
p divides \(k-1\) so

\[
0 \equiv -k + (e+1)(k-2) \mod p^m.
\]

Hence \( e \equiv \frac{2}{(k-2)} \mod p^m \).

Bannai and Ito have shown \( e > 1 \) for \( k = 4 \) \([2]\),

so

\[
e \geq \frac{2 + p^m}{k - 2} > p^{m/k}.
\]

Thus \( e > \sqrt[k]{g_{/k}} \).
This chapter is devoted to the problem of finding the smallest Cayley graphs of a given girth. It is true that for some small values of the girth the "Cayley Cages" are of similar order to the ordinary cages, but there is no general result of this kind. Since Cayley graphs are all vertex-transitive the results in Chapter 3 concerning the excess of vertex-transitive graphs apply.

The (3,k) Cayley Cages \( k \leq 9 \)

We start by noting that the \((3,4)\) cage \( K_{3,3} \) is the Cayley graph of the group \( S_3 \) using the three involutions as generating set. The Heawood graph, the unique \((3,6)\) cage is also a Cayley graph, the group being a subgroup of the group of linear transformations of the field with seven elements isomorphic to the dihedral group of order 14, the generating set being the three involutions \{1-x, 2-x, 4-x\}. Examining \( C_{10} \) and \( D_{10} \) shows that the unique \((3,5)\) cage the Petersen graph is not a Cayley graph and indeed the \((3,5)\) Cayley cage has considerably more than 10 vertices.

**Theorem 4.1**

Trivalent Cayley graphs of girth 5 have at least 50 vertices.

**Proof**

Let \( G \) be the smallest trivalent graph of girth 5 which is also a Cayley graph, and let it be the Cayley group \( G \) with generating...
set \( \Omega \). We have that \( G \) has more than ten elements.

Consider the cycles of length 5 in the graph. Each such cycle corresponds to an identity word \( W_1 W_2 W_3 W_4 W_5 \) in the generators of \( G \). Suppose \( W_i \neq W_{i+1} \) for some \( i \). Then the five words \( W_1 W_2 W_3 W_4 W_5, W_2 W_3 W_4 W_5 W_1, \ldots, W_5 W_1 W_2 W_3 W_4 \) must all represent different cycles through a given vertex in the Cayley graph.

Let \( \Gamma_r(x) \) denote the set of vertices at distance \( r \) from a given vertex \( x \), and let the subgraph \( \Gamma_r(x) \) have vertex-set and edge-set

\[
V(\Gamma_r(x)) = \bigcup_{i=0}^{r} \Delta_r(x); E(\Gamma_r(x)) = \{(v,w) | (v,w) \in E(\Gamma)\}
\]

There cannot be six edges from \( \Delta_2(x) \) to \( \Delta_2(x) \), or \( \Gamma \) would be the Petersen graph, so there must be exactly 5 edges between vertices in \( \Delta_2(x) \).

Now we show \( x \) is not a cutvertex; this means the graph remains connected when the vertex \( x \) is removed. Every 5-cycle through \( x \) must also pass through 2 members of \( \Delta_1(x) \), and there are at most 2 5-cycles passing through \( x \) and two given members of \( \Delta_1(x) \). Hence there is a path of length 3 between any two members of \( \Delta_1(x) \) not containing \( x \). Thus \( x \) is not a cutvertex. We also have that through any 2-arc there is at least one 5-cycle.

There are six vertices in \( \Delta_2(x) \). Since there are six edges from vertices in \( \Delta_2(x) \) to vertices in \( \Delta_1(x) \) and five edges from \( \Delta_2(x) \) to \( \Delta_2(x) \) there must be exactly 2 edges from \( \Delta_2(x) \) to \( \Delta_3(x) \). Suppose these 2 edges have a coincident end in \( \Delta_2(x) \) vertex \( V \) say. Then there can be no path from \( \Delta_3(x) \) to the
vertex $x$ which does not pass through $V$ and $V$ must be a cutvertex. But $x$ is not a cutvertex so the vertextransitivity of $\Gamma$ is contradicted. Hence $e_1$ and $e_2$ have distinct ends in $\Delta_2(x)$, and similarly they have distinct ends in $\Delta_2(x)$.

Let the edges $e_1, e_2$ be $(V_1, W_1)$ and $(V_2, W_2)$ where $V_1, V_2$ are in $\Delta_2(x)$ and $W_1, W_2$ are in $\Delta_3(x)$. Hence $\Delta_3(x) = \{W_1, W_2\}$. $W_1$ has at most one neighbour in $\Delta_3(x)$, and exactly one neighbour $V_1$ in $\Delta_2(x)$, so there is a vertex $U$ say in $\Delta_4(x)$ joined to $W_1$.

There is a 5-cycle $C$ through the 2-arc $(V_1, W_1, U)$. Any path from $V_1$ to $W_1$ not containing $e_1$ must contain $e_2$ since $e_2$ is the only other edge connecting $\Delta_2(x)$ to $\Delta_2(x)$. Hence $e_2$ is also in $C$. $C$ contains but 5 edges so $(U, W_2)$ and $(V_1, V_2)$ must also be in $E(\Gamma)$. Now consider the subgraph $D_2$ whose vertexset is $\Delta_2(x) \setminus \{V_1, V_2\}$. This is a graph with 4 vertices and 4 edges, which must contain either a 3-cycle or a 4-cycle contradicting the girth.

Hence the only word that could possibly represent a cycle of length 5 in a graph of girth 5 is $S^5$ for some generator $S$. 
Thus $\Gamma$ has 'Type II'. Let $G = \langle R, S \rangle$ where $R^2 = S^5 = 1$ be the group whose Cayley graph is $\Gamma$. Suppose the subgroup generated by $S, \langle S \rangle$ is normal in $G$. Then $RS^aR$ is in $\langle S \rangle$ for all values of $a$ and hence $\langle R, S \rangle$ has ten elements. But $\Gamma$ has more than 10 vertices so $\langle S \rangle$ is not normal in $G$.

Sylow's Theorems state that if the order of a finite group $H$ is $p^m$, where $p$ is a prime not dividing $m$, then all subgroups of $H$ of order $p^n$ are conjugate, and the number of them is congruent to 1 modulo $p$ and divides to order of $H$. Since $R$ is of order 2 and $S$ is of order 5 the order of $G$ must be divisible by 10. By applying Sylow's Theorems we find that any subgroup of order 5 of a group of order 20 or 40 must be normal, and Coxeter and Moser [12] have shown there are no groups of order 30 with 6 Sylow 5 subgroups so again any subgroup of order 5 a group of order 30 must be normal. Hence the order of $G$ is at least 50.

We find that if $G$ is given by the presentation

$$G = \langle R, S \mid R^2 = S^5 = (RS)^2(RS^{-1})^2 = 1 \rangle$$

$G$ is of order 50, and the Cayley graph of $G$ using $\{R, S\}$ as generating set is indeed trivalent and of girth 5.

Corollary

There are no edgetransitive trivalent Cayley graphs of girth 5, nor are there any Cayley graphs of girth 5 of Type I.

Proof

We have already shown that all Cayley graphs which are trivalent and
have girth 5 are Type II. Suppose $\Gamma$ is the Cayley graph of the group $G$ with generating set $\{R, S\}$ where $R^2 = S^5 = 1_G$. Then there is a 5-cycle through any edge labelled $S$ but there is no 5-cycle through an edge labelled $R$, and hence $\Gamma$ cannot be edge-transitive. //

Before examining the trivalent Cayley cages with girth greater than 5, we need a result involving dihedral groups. The dihedral group $D_{2n}$ is the group of symmetries for the regular n-gon. Let $G$ be a dihedral group of order $2n$ and let $G'$ be the cyclic subgroup of $G$ of order $n$. Let $\Omega$ be a generating set of $G$ chosen such that the resulting Cayley graph of $G$ is trivalent.

**Lemma 4.2**

If $\Gamma$ is the Cayley graph of $G$ with generating set $\Omega$ the girth of $\Gamma$ is less than or equal to 6.

**Proof**

Suppose $\Gamma$ is Type I. Then $\Omega$ consists of 3 involutions $\{R, S, T\}$ say, if none of $R, S, T$ are in $G'$, then the product $RST$ is not in $G'$, and $(RST)^2 = 1$ and the graph contains a 6-cycle. At least one member of $\Omega$ is not in $G'$, $R$ say, so if $S$ is in $G'$ $(RS)^2 = 1$ giving a cycle of length 4.

If however $\Gamma$ is Type II, then $\Omega$ consists of one involution $R$ say and an element of order $> 2$ $S$ say and we have $RSRS^{-1} = 1$ and $\Gamma$ contains a 4-cycle.

Hence the girth of $\Gamma$ is at most 6. //
Theorem 4.3

The smallest Cayley graph with degree 3 and girth 7 has 30 vertices.

Proof

First let $\Gamma$ be the Cayley graph of $C_5 \times D_6$ with the generators $A, B$ represented by the permutations

$$A = (1\ 2), \ B = (1\ 2\ 3)\ (4\ 5\ 6\ 7\ 8).$$

The shortest identity word in $A$ and $B$ is $ABAB^4$ and $\Gamma$ has 30 vertices and girth 7.

The unique (3,7) cage, the McGee graph has 24 vertices and is not vertex-transitive and consequently not Cayley. There are only 3 non-Abelian groups which have 26 or 28 elements [12]. Two of these are dihedral groups whose Cayley graphs must have girth less than 7 by the Lemma. The third group is the dicyclic group $Q_{14}$ which contains only one involution, and whose Sylow 7 subgroup is normal. These two properties ensure no generating set may be chosen from this group to give a trivalent Cayley graph that is connected. //

We now examine the cases where the girth is 8 or 9.

First various possibilities have to be eliminated.

Lemma 4.4

The girth of a trivalent Cayley graph on 36 vertices is less than 8.

Proof

We separate the trivalent Cayley graphs into 2 classes. Suppose $G$
is a group with 36 elements, and let $\Gamma$ be the Cayley graph of $G$ using $S$ as generating set.

Suppose $\Gamma$ is Type II. Then $S = \{x,y\}$ where $x$ is of order $n$ and $n$ is greater than 2, and $y$ is an involution. Now either the resultant Cayley graph has girth less than 8 or $n \geq 8$, so we consider the possible values of $n$ where $n > 8$. Let $X$ denote the subgroup generated by $x$.

a) $|X| = 18$ Then $X$ is normal in $G$ being of index 2. Hence $yxy = x^a$ for some $a$. From this we have

$$x^a = (yxy)^a = yx^ay = x.$$  

So $a^2 \equiv 1 \pmod{18}$. There are only two solutions to this $a \equiv \pm 1 \pmod{18}$, and thus $yxyx^{-a}$ is a word of length 4.

b) $|X| = 12$ If $X$ is normal $\langle y,x \rangle$ is a subgroup of order 24 which is not possible. Hence $X$ is not normal, so there are 3 right cosets of $X$, $Xy$ and $Xyx$. $Xy \nmid Xyx$ so $Xyx \nmid Xyx^2$ and thus $Xyx^2 = Xy$ and $yx^2y$ is in $X$. But only two elements $x^2$ and $x^{-2}$ in $X$ are of order 6 so either $yx^2y$ or $yx^{-2}y$ is an identity word and the graph contains a 6-cycle.
c) \( |X| \neq 9 \) If \( X \) is normal, \( \langle x, y \rangle \) contains only 18 elements. Hence \( X \) is not normal. Let \( z = yxy \). The cosets \( Xz^i \) \( (0 \leq i \leq 8) \) are not all distinct (since \( |G| = 36 \)), so \( z^j \) belongs to \( X \) for some \( j \), \( 2 \leq j \leq 4 \), and \( X \cap \langle z \rangle \) is a nontrivial proper subgroup of \( \langle z \rangle \). Hence \( X \cap \langle z \rangle = \langle z^3 \rangle \). Thus \( z^3 = yx^3y \) belongs to \( X \) and must be either \( x^3 \) or \( x^{-3} \).

If \( yx^3y = x^3 \), \( y \) commutes with \( x^3 \) and \( yx^3 \) is of order 6. Since \( G \) contains 4 Sylow-3-subgroups and 3 cyclic groups of order 6 (conjugates of \( \langle yx^3 \rangle \)), counting the elements of \( G \) we find the distinct elements \( xyx^{-1} \), \( x^{-1}yx \), \( y \) must all lie in the unique Sylow-2-subgroup of order 4 and \( xyx^{-2}yxy = 1 \) giving a word of length 7.

On the other hand, if \( yx^3y = x^{-3} \), one of \( (yx)^3 \), \( (yx)^3x^{-3} \) or \( x^{-3}(xy)^3 \) is the identity and again we have a word of length less than 8 corresponding to the identity.
Now suppose $\Gamma$ is Type I. Then $S = \{x, y, z\}$ where $x, y, z$ are all of order 2. Either the girth of $\Gamma$ is less than 8 or each of the products $xy, yz, zx$ are of order greater than 4. Suppose this is the case and that without loss of generality the product $xy$ is of the highest order among them. We now consider the possible order of $A$ the subgroup of $G$ generated by $xy$.

a) $|A| = 18$. Then $G$ is a dihedral group and the girth of $\Gamma$ is at most 6 by Lemma 4.2.

b) $|A| = 9$. Then $\langle x, y \rangle$ is of index 2 and normal in $G$. Hence either $(xyz)^2$ or $yxzyz$ is the identity and $\Gamma$ has girth at most $G$.

c) $|A| = 6$. Suppose $\Gamma$ is of girth 8. Let $M$ denote $\langle x, y \rangle$. $M$ cannot be normal in $G$ since $|\langle x, y, z \rangle|$ is not 24. Hence either $zxz$ or $zyz$ is not in $M$. Suppose $zxz$ is not in $M$. Then $zyxz$ is in $M$ and we have either $(zy)^2$ or $zyxzyzxy$ is the identity and $\Gamma$ contains a 6-cycle.

So let $zyx$ be in $M$. $(zy)^2$ is of order 3 and consequently $(zy)^2 = (zx)^2$. (If $(zy)^2 = (xy)^2 \Gamma$ contains $zyxzyx$ a 6-cycle).

Now consider $N = \langle z, x \rangle$. Similarly we have that exactly one of $zy$ and $yx$ is in $N$. But $z(yzy)x = yxy$ so $zy$ is in $N$ if and only if $yx$ is in $N$. Thus we have a contradiction and $\Gamma$ is of girth less than 8.
Hence Cayley graphs on 36 vertices have girth less than 8. //

Lemma 4.5

The girth of a trivalent graph of order 40 is less than 8 and the girth of a trivalent Cayley graph of order 56 is less than or equal to 8.

Proof

Let $G$ be a group with $8p$ elements with $p=5$ or $p=7$. We know from Sylow's Theorems $G$ contains a normal subgroup of order $p$ or if $p=7$ a normal subgroup of order 8. (In this particular case any Cayley graph of $G$ must be disconnected if $\Gamma$ is of Type I since all involutions lie in the unique Sylow 2 subgroup and of girth less than 8 if it is of Type II since the only elements outside the Sylow 2 subgroup are of order 7). This normal subgroup is unique and cyclic. Let $S$ be a generating set of $G$ such that the resulting Cayley graph $\Gamma$ is trivalent.

Suppose $\Gamma$ is of Type II. Then $S$ consists of an involution $y$ and an element $x$ of order greater than 2. We now consider the possible orders of $X$ the subgroup generated by $x$.

a) $|X| = 4p$. Then $X$ is of index 2 in $G$ and is consequently normal in $G$. Hence $yxy = x^a$ for some $a$. From this we have

$$x^{a^2} = (yxy)^a = yx^ay = x.$$  

Hence $a^2 \equiv 1 \pmod{4p}$, so $a \equiv \pm 1 \pmod{2p}$ and $2a \equiv \pm 2 \pmod{4p}$. Thus either $(yx^2)^2$ or $yx^2yx^{-2}$ is
the identity and $\Gamma$ contains a 6-cycle.

b) $|x| = 2p$  $x^2$ is of order $p$ so the subgroup generated by $x^2$ is normal and cyclic. Again we find either $(yx^2)^2$ or $yx^2yx^{-2}$ is the identity and $\Gamma$ contains a 6-cycle.

c) $|x| = 8$  $X$ is now a cyclic Sylow-2-subgroup of $G$. $y$ is not in $X$ so $y$ must be inside a distinct cyclic subgroup of order 8 generated by $z$, say. Thus $y = z^4$, and since $y$ does not lie in $X$ no power of $z$ can lie in $X$ and the cosets $Xz^i$ ($0 \leq i \leq 7$) must all be distinct. Thus we get a contradiction on the order of $G$, and deduce that there are no groups of order 40 or 56 which are generated by an involution and an element of order 8.

If the order of $X$ is less than 8 $\Gamma$ contains a cycle of length less than 8.

Suppose $\Gamma$ is Type I, and $S$ consists of 3 involutions $x,y,z$. We look at the order of the product $xy$, and by similar arguments to those used above, find the conjugate of $xy$ by $z$ is either $xy$ or $yx$ if $xy$ is of order $4p$, $2p$ or $p$, and $\Gamma$ contains a 6-cycle. Hence either the girth of $\Gamma$ is less than 8 or $(xy)^4 = (yz)^4 = (xz)^4 = 1$.

Suppose $p=5$ and $(xy)^4 = (yz)^4 = (xz)^4 = 1$. Then $G$ contains 5 Sylow 2 subgroups $H_1, H_2, H_3, H_4, H_5$ each isomorphic to $D_5$. Let $H_1 = \langle x, y \rangle$, $H_2 = \langle y, z \rangle$ and $H_3 = \langle z, x \rangle$. Each of these is self-normalizing. Now $xH_1x = H_1$ and $xH_2x = H_3$ and $xH_2x$ is not
Hence the girth of a trivalent Cayley graph is less than 8 if it has 40 vertices and less than 9 if it has 56 vertices.

Lemma 4.6

The girth of a trivalent Cayley graph with 54 vertices is less than 9.

Proof.

There are only two non-Abelian groups of order 27 and in one of them every element is of order 3 [12].

Suppose $G$ is of order 54 and its Sylow 3 subgroup is $H$.

Suppose $H$ is isomorphic to $A$. Let $S$ be a generating set giving a trivalent Cayley graph. If any member of $S$ is in $H$ the Cayley graph contains a triangle; if not and $G$ is of Type II the element in $S$ of order greater than 2 must be of order 6 and the graph contains a 6-cycle, and if the graph is of Type I it also contains a 6-cycle since the product of any two generators is of order 3.

Now suppose $H$ is Abelian. Suppose $Γ$, is the Cayley graph of $G$ is Type I. None of the three involutions generating $G$ lie in $H$, but their products pairwise must all lie in $H$ and $xz . zy . zx . yz = (xyz)^2$ is an identity word. If on the other hand $Γ$ is Type II with generating set $\{x, y\}$ where $x$ is not an involution, then either $yxy^{-1}yx^{-1}y. x$
or \( x^2 . xy . x^{-2} . yx \) is an identity word depending on whether or not \( x \) lies in the subgroup \( H \). \( \Gamma \) has girth at most 8 in this case.

The remaining possibility is that \( H \) is given by the presentation

\[ < S, T | T^3 = T^{-1} STS^2 = 1 > \]

a group of order 27 containing 3 subgroups isomorphic to the cyclic group of order 9, whose centre \( Z \) is of order 3 and generated by the cube of any element of order 9.

Let \( \Gamma \) be a trivalent Cayley graph of \( G \).

Suppose \( \Gamma \) is of Type I, and the generating set is given by \( \{ x, y, z \} \) a set of three involutions. If any of the products \( xy, yz, zx \) which all lie in \( H \) have order 3 \( \Gamma \) contains a 6-cycle so suppose the order of each of these products is 9. Let \( K \) be the dihedral group of order 18 generated by \( x, y \). If \( K \) by \( z \) is the same as \( K \), \( (xz)^2 \) lies in \( K \), \( xz \) commutes with \( xy \) and \( (xyz)^2 = 1 \) so \( \Gamma \) has girth at most 6. Hence there are 3 subgroups of \( G \) all conjugate isomorphic to \( K \) each containing 9 involutions. Since these subgroups intersect in a cyclic subgroup of order 9, these 27 involutions are all distinct, and they must comprise all the elements in \( G \) not in \( H \). But \( xyz \) is not in \( H \) so \( (xyz)^2 = 1 \) and \( \Gamma \) has girth at most 6.

Suppose now instead \( \Gamma \) is of Type II with generating set \( \{ x, y \} \) where \( x \) is not an involution and \( y \) is. If \( x \) is of order 9, \( x^3 \) lies in \( z \) and either \( yx^3 yx^{-3} \) or \( yx^3 yx^3 \) is the identity. If
x is of order 18, coset enumeration swiftly shows $yx^3y$ lies in the subgroup generated by $x$ and again $yx^3yx^{-3}$ or $yx^3yx^3$ is the identity. The only other possible orders of $x$ are less than 9, so $\Gamma$ must contain a cycle of length less than 9.

We are now in a position to establish the number of vertices in the smallest trivalent Cayley graphs of girth 8 and 9.

**Theorem 4.7**

The smallest trivalent Cayley graphs with girth 8 have 42 vertices.

**Proof**

The Tutte graph on 30 vertices is the unique (3,8)cage. Using the fact that this graph is bipartite and that there are 24 8-cycles through each vertex it is verifiable that this is not the Cayley graph of any of the three nonAbelian groups with 30 elements. Biggs and Ito have shown that excess 2 is not feasible in this instance, so there are no trivalent graphs of girth 8 with 32 vertices. The only nonAbelian groups of order 34 or 38 are dihedral so by Lemma 4.2 there are no trivalent Cayley graphs on 34 or 38 vertices with girth more than 6. Lemmas 4.4 and 4.5 rule out 36 and 40 respectively as possible orders for trivalent Cayley cages.

However, the group generated by the permutations

$$A = (1 \ 2), \ B = (1 \ 2 \ 3) \ (4 \ 5 \ 6 \ 7 \ 8 \ 9 \ 10),$$

or alternatively given by the presentation

$$G = \langle A, B \mid A^2 = B^{21} = ABAB^{-8} = 1 \rangle,$$
The smallest trivalent Cayley graphs of girth 9 have 60 vertices.

Proof

As was mentioned in Chapter 2 McKay has shown that any trivalent graph of girth 9 has more than 52 vertices [28]. Lemmas 4.5 and 4.6 show that there are no trivalent Cayley graphs of girth 9 with 54 and 56 vertices and the only non-Abelian group of order 58 is dihedral. Hence the smallest trivalent Cayley graphs of girth 9 have 60 vertices. Two are known.

Firstly the icosahedral group with generating set of permutations

\[(1 2)(3 5), (1 3)(4 5), (1 4)(2 5)\]

has a Cayley graph with girth 9. This is known as Foster's graph [18].

Secondly the group with generating set of permutations

\[(1 2)(4 5), (1 2 3 4)(6 7 8)\]

has a Cayley graph of girth 9. This is an unpublished graph of Coxeter.

The Cayley graphs of \(\text{Aff}(p^f)\)

Given a finite field \(\text{GF}(p^f)\) with \(p^f\) elements consider the group \(\text{Aff}(p^f)\) of affine transformations of the form \(x \mapsto ax+b\), where \(a, b\) are members of \(\text{GF}(p^f)\) and \(a\) is nonzero.
This group is sharply 2-transitive and is of order $p^f(p^f-1)$.

Let $R$ represent the transformation $x \mapsto -1 - x$ and $S$ represent the transformation $x \mapsto ax$ where $a$ is a primitive element of $\text{GF}(p^f)$.

**Theorem 4.9**

$R$ and $S$ generate the entire group $\text{Aff}(p^f)$.

**Proof**

Take any element $T$ of $\text{Aff}(p^f)$ where $Tx = mx + n$ with $m$ nonzero. Since $a$ is primitive $m = -a^i$ for some $i$. Also either $T = S^i$ or $n = -a^j$ for some $j$.

Then

$$mx + n = mx - a^j = a^j(-1 + a^{-j}mx) = a^j(-1 - a^{-j}x)$$

so $Tx = S^j.R.S^{-j}x$ and hence $\text{Aff}(p^f) = \langle R, S \rangle$.//

Hence the group with generating set $\{R, S\}$ has a trivalent Cayley graph with $p^f(p^f-1)$ vertices. We shall be interested in the girth of this graph. Should $p^f$ be congruent to 3 (modulo 4) both $R$ and $S$ correspond to odd permutations of the elements of the field and the graph is bipartite.

**Particular cases**

The girths of all the graphs with $p \leq 23$ are given in Table 2. Certain of the graphs are of special interest.

i) If $p = 11$ choose primitive root 7. Coxeter and Frucht [13] have
shown the resultant Cayley graph which has girth 10 is
3-arctransitive.

ii) If \( p = 17 \) and primitive root 3 is chosen, the Cayley graph
has girth 13. This is the smallest known graph which is
trivalent and has girth 13; it has 272 vertices.

iii) If \( p = 23 \) and if 5, 15 or 17 are chosen as primitive roots
then the girth is 14. The group \( \text{Aff}(23) \) has the presentation
\[
\text{Aff}(23) = \langle A, B | A^2 = B^{22} = AB^5AB^4AB^2 \rangle
\]
and \( A, B \) are equivalent to \( R, S \) when the primitive root is 17.
The Cayley graph with \( \{A, B\} \) as generating set is 4-arctransitive,
as we shall see in Chapter 5.

Although the girth increases initially as the prime power increases
there is an upper bound on the girth of a trivalent Cayley graph
resulting from \( \text{Aff}(p^f) \).

**Theorem 4.10**

If \( G \) is isomorphic to \( \text{Aff}(p^f) \) and \( \Gamma \) is a Cayley graph of degree
3 resulting from \( G \) then the girth of \( \Gamma \) is less than or equal to 14.

**Proof**

The only involutions in \( G \) are of the form \( x \mapsto a-x \) for some \( a \).
All the involutions are contained in the group \( \{x \mapsto aix\} \) which is a
group of order \( 2p^f \). But \( \Gamma \) is the Cayley graph of \( \text{Aff}(p^f) \) and \( \Gamma \)
is trivalent, so \( \Gamma \) is generated by some \( R, S \) where
\[ \begin{align*}
Rx & \mapsto c - x \\
Sx & \mapsto ax + b
\end{align*} \]

where \( a \) is not equal to 0 or \(-1\).

Then
\[ ((RS)^2RS^{-2})x = -a(-1(a^{-1}(a^{-1}x - a^{-1}b) - a^{-1}b)c)b + c) + c) + c = d - x \]

for some \( d \).

Hence \((RS)^2RS^{-2}\)^2 is the identity and \( \Gamma \) contains a cycle of length 14. //

**Theorem 4.11**

The smallest subgroup of a group of the form \( \text{Aff}(p^f) \) to beget a trivalent Cayley graph of girth 14 is of order 406.

**Proof**

Let \( \Gamma \) be the Cayley graph of a group \( G \), a subgroup of \( \text{Aff}(p^f) \) generated by
\[ \begin{align*}
Rx & \mapsto c - x \\
Sx & \mapsto a^{-n}x
\end{align*} \]

where \( a \) is a primitive root of \( p^f \) and \( n > 1 \). Let the order of \( S \) be \( m \). Since \( S^m \) is the identity and the girth of \( \Gamma \) is 14 \( m \geq 14 \).

Now \( nm \equiv -1 \) (modulo \( p^f \)) so \( p^f \geq mn + 1 \).

But \( |V(\Gamma)| = |G| \geq mp^f \geq 14(mn + 1) \geq 14(14.2 + 1) \geq 406 \).
This minimum may be attained if \( p = 29 \) and the generators

\[
\begin{align*}
R & : x \to 28 - x \\
S & : x \to 4x
\end{align*}
\]

are chosen.
Chapter 5

The Sextet Graphs

In this chapter we construct a family of highly transitive graphs for which it is conjectured that there is no upper bound for the girth. I have been unable to prove this conjecture but some partial results are given. The family is also of interest because it yields graphs which are in many cases the smallest known trivalent graphs with their particular girth. The girths and orders of the graphs known to have girth less than 32 are given in the Tables.

The Sextet construction

Let $q$ be an odd prime power.

The projective line $\text{PG}(1,q)$ may be identified with the set $L = \text{GF}(q) \cup \{\infty\}$, where $\text{GF}(q)$ is a finite field with $q$ elements.

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 $-1$.

Thus we shall write

$\{a,b | c,d\}$ is a quartet $\iff \frac{(a-c)(b-d)}{(a-d)(b-c)} = -1$

with the conventions about the element $\infty$ giving

$\{\infty, a | b, c\}$ is a quartet $\iff \frac{(a-b)}{(a-c)} = -1$.

A sextet $\{a,b | c,d | e,f\}$ is an unordered triple of duets such that each of $\{a,b | c,d\}, \{c,d | e,f\}, \{e,f | a,b\}$ is a quartet.

The group $\text{PGL}(2,q)$ of linear fractional transformations
acts sharply 3-transitively on $L$ and its order is $q(q^2 - 1)$.

Lemma 5.1

The number of quartets is $\frac{1}{8} q(q^2 - 1)$. The number of sextets is $\frac{1}{24} q(q^2 - 1)$ if $q \equiv 1 \pmod{4}$ and 0 if $q \equiv 3 \pmod{4}$.

Proof

Clearly $\text{PGL}(2,q)$ acts transitively on the duets so we need only consider a particular duet $\{0, \omega\}$. Now $\{0, \omega | x, y\}$ is a quartet if and only if $x + y = 0$, so there are $\frac{1}{2} (q - 1)$ quartets containing $\{0, \omega\}$. The number of quartets is

$$\frac{1}{2} \cdot \frac{1}{2} q(q + 1) \cdot \frac{1}{2} (q - 1) = \frac{1}{8} q(q^2 - 1).$$

Since the points $\{0, \omega, 1\}$ determine the unique quartet $\{0, \omega|1, -1\}$ and $\text{PGL}(2,q)$ acts 3-transitively on $L$, it acts transitively on the quartets. The condition that $\{0, \omega|1, -1|u, v\}$ be a sextet are

$$u + v = 0, \quad uv = 1,$$

so that $uv$ must be primitive fourth roots of unity $i$ and $-i$. If $q \equiv 1 \pmod{4}$ there are no solutions and consequently there are no sextets. If $q \equiv 1 \pmod{4}$ there is a unique solution. Thus each quartet determines a unique sextet and each sextet arises from three quartets so that the number of sextets is $\frac{1}{24} q(q^2 - 1)$. 

\[
\begin{align*}
t & \mapsto \frac{at + b}{ct + d} \quad (a, b, c, d \in \text{GF}(q), \quad ad - bc \neq 0) \\
\end{align*}
\]
From now on we shall assume \( q \equiv 1 \) (modulo 4).

From Hirschfeld we have that an involution in \( \text{PGL}(2,q) \) is uniquely determined by two pairs of corresponding points, and that if the two pairs from a quartet, then the fixed points of the involution are the third pair in the unique sextet determined by the given quartet [23].

For example if the quartet is \( Q = \{1,-1|i,-i\} \) the involution is \( i_Q(t) = -t \) and the fixed points are \( \{0, \infty\} \). The four points of \( Q \) may be split into two pairs in two other ways, \( R = \{1,-1|-1,i\} \) and \( S = \{1,i|-1,-i\} \) and the corresponding involutions are

\[
i_R(t) = \frac{i}{t}, \quad i_S(t) = -\frac{i}{t}.
\]

Solving formally to obtain the fixed points of \( i_R \) and \( i_S \) we see that we require a square root of \( i \), that is an eighth root of unity. Now if \( q \equiv 1 \) (modulo 8), \( q-1 = 8n \) and \( \tau \) is a primitive element of \( \text{GF}(q) \) then \( \tau^8 = \sigma \) is an eighth root of unity and \( \sigma^2 = i \). So in this case the fixed points of \( i_Q, i_R \) and \( i_S \) are \( \{0, \infty\}, \{\sigma, -\sigma\}, \{\sigma^3, -\sigma^3\} \) and we remark that they form a sextet.

This remark is the basis for the construction of a cubic graph whose vertices are the sextets. We shall suppose that \( q \equiv 1 \) (modulo 8), and let \( \sigma \) denote an element of order 8 in \( \text{GF}(q) \). The sextet \( \{a_1a_2|b_1b_2|c_1c_2\} \) is adjacent to \( \{a_1'a_2'|b_1'b_2'|c_1'c_2'\} \) if

\[
\begin{align*}
   a_1', a_2' & \text{ are the fixed points of the involution determined by } b_1b_2; c_1c_2 \\
   b_1', b_2' & \text{ } b_1c_1; b_2c_2 \\
   c_1', c_2' & \text{ } b_1c_2; b_2c_1.
\end{align*}
\]
In fact \( \{a'_1, a'_2\} \) is the same as \( \{a_1, a_2\} \). Thus there are three sextets adjacent to a given sextet, each having one duet in common with it. Furthermore it cannot be verified that the relation of adjacency is symmetric (since \( \text{PGL}(2, q) \) is transitive on the sextets we need only check one sextet). Thus we have a cubic graph \( S(q) \) with \( \frac{1}{24} q(q^2 - 1) \) vertices.

In order to show that an element \( g \) of \( \text{PGL}(2, q) \) is an automorphism of \( S(q) \) we remark that if \( \theta_1, \theta_2 \) are the fixed points of an involution \( j_Q \) then \( g\theta_1, g\theta_2 \) are the fixed points of \( g j_Q g^{-1} = j_Q \). Hence \( g \) preserves adjacency in \( S(q) \) and the group \( \text{PGL}(2, q) \) acts as a group of automorphisms of \( S(q) \).

The components and automorphisms of \( S(p^f) \).

Now we come to consider the size of the components of \( S(p^f) \). The component of \( S(p^f) \) containing the sextet mentioned previously \( k_0 = \{0, \infty |1, -1|i, -i\} \) will be denoted by \( S_0(p^f) \). We have already established that each element of \( \text{PGL}(2, p^f) \) preserves adjacency and corresponds to an automorphism of \( S(p^f) \).

Let \( A: t \mapsto \frac{\sigma[t - 1]}{[t + 1]} \) and \( B: t \mapsto \frac{\sigma[t + 1]}{[t - 1]} \), where \( \sigma \) denotes an eighth root of unity in the field \( \text{GF}(p^f) \).

Theorem 5.2

The automorphisms \( A, B \) are twin shunts of a 4-arc in \( S(p^f) \).
Proof

We consider the actions of the first five powers of A and B on the sextet \( k_{-1} = \{1, -1 | \frac{1+\sigma}{1-\sigma}, \frac{1-\sigma}{1+\sigma}, \frac{1+\sigma-1}{1+\sigma}, \frac{1+\sigma-1}{1+\sigma} \} \). \( A^i k_{-1} = B^i k_{-1} \) for \( 0 \leq i \leq 4 \) but \( A^5 k_{-1} = B^5 k_{-1} \).

Hence A and B do correspond to twin 4-shunts.

There is a theorem of Tutte [34] which states that given a connected graph G with automorphism group \( \text{Aut}(G) \) and two elements X, Y in \( \text{Aut}(G) \) which both act as shunts on an s-arc then \( \langle X, Y \rangle \), the subgroup of \( \text{Aut}(G) \) generated by X, Y acts at least s-arc transitively on G. Hence \( \langle A, B \rangle \) the subgroup of \( \text{PGL}(2, p^f) \) generated by A, B acts at least 4-arc transitively on \( S_0(p^f) \).

Theorem 5.3

\( S_0(p^f) \) is isomorphic to \( S_0(p^m) \) if \( f \) is greater than \( m \) and \( p^m \equiv 1 (8) \).

Proof

Suppose \( \sigma_p \) an eighth root of unity in \( \text{GF}(p^f) \) lies in a subfield \( \text{GF}(p^m) \) of \( \text{GF}(p^f) \). Then the elements 0, \( \omega, 1, -1, i, -i, \sigma_p, -\sigma_p \) where \( i = \sigma^2 \) must all lie in the subset \( \text{GF}(p^m) \cup \{\omega\} \). As A, B generate a group that is vertex transitive on \( S_0(p^f) \) and A, B are linear fractional transformations involving only powers of \( \sigma_p \) the elements of any sextet in the same component as \( k_0 \) must also be in \( \text{GF}(p^m) \cup \{\omega\} \), and \( S_0(p^f) \) is isomorphic to \( S_0(p^m) \).
Corollary

\[ S_o(p^f) \] is isomorphic to \[ S_o(p^2) \] for all odd primes \( p \) with \( f \) greater than or equal to 2, and \( S_o(p^f) \) is isomorphic to \( S_o(p) \) if \( p \equiv 1 \pmod{8} \).

Proof

\[ p^2 \equiv 1 \pmod{8} \] for all odd primes. 

From now on we will only be concerned with the family of graphs \( S_o(p^2) \), where \( p \) is an odd prime. \( A, B \) will be considered as elements of \( PGL(2,p^2) \) and \( G \) will denote \( \langle A, B \rangle \) the subgroup of \( PGL(2,p^2) \) generated by \( A, B \). \( G \) acts vertex-transitively on \( S_o(p^2) \) and as \( G \) must be isomorphic to one of a small number of subgroups of \( PGL(2,p^2) \) we have a way of calculating the order of \( S_o(p^2) \).

If \( p \equiv 1 \pmod{8} \), we need only consider \( S_o(p) \).

First we consider the cases where \( p \equiv 1 \) or \( 7 \pmod{8} \) when \( A, B \) are both within \( PSL(2,p^2) \) the subgroup of \( PGL(2,p^2) \) consisting of those linear fractional transformations

\[ P : t \mapsto \frac{at+b}{ct+d} \]

where \( ad - bc \) is a square in the field \( GF(p^2) \).

The subgroups of \( PSL(2,p^2) \) were found by Dickson and are listed in [24].

Lemma (Dickson)

The group \( PSL(2,p^f) \) has the following subgroups:

1) Elementary Abelian \( p \)-groups
2) Cyclic groups
3) Dihedral groups
4) Groups isomorphic to $A_4$
5) Groups isomorphic to $S_4$
6) Groups isomorphic to $A_5$
7) Semidirect products of elementary abelian $p$-groups with cyclic groups
8) $\text{PSL}(2, p^m)$ with $m|f$ and $\text{PGL}(2, p^m)$ with $2m|f$.

We remark that there are no subgroups of $\text{PSL}(2, p^n)$ isomorphic to $S_4 \times Z_2$. It is also true that there are no such subgroups of $\text{PGL}(2, p^n)$. Since this group itself occurs as a subgroup of $\text{PSL}(2, p^{2n})$ [14]. So we have immediately:

**Lemma 5.4**

In all cases $G = \langle A, B \rangle$ acts 4-arctransitively on $S(p)$.

**Proof**

We have seen that $G$ acts transitively on the 4-arcs, so $G$ must act either 4-arctransitively or 5-arctransitively. $G$ is a subgroup of a $\text{PGL}$ group and so it cannot contain the subgroups of type $S_4 \times Z_2$ required as the vertex-stabilizers in the 5-arctransitive case. Thus $G$ acts 4-arctransitively. //

Recalling the remarks following the Dickson Lemma, we see that the determination of the order $n$ of $S(p)$ now depends on the order of $G$: we must have $n = |G|/24$.

**Theorem 5.5**

$G = \langle A, B \rangle$ is isomorphic to one of $\text{PSL}(2, p)$, $\text{PGL}(2, p)$, $\text{PSL}(2, p^2)$ or $\text{PGL}(2, p^2)$. 
Proof

G contains the $S_4$ subgroup fixing the sextet $k_0$, and the element $A$ which does not fix $k_0$. The only category of subgroup of $\text{PSL}(2,p^n)$ strictly containing an $S_4$ subgroup is category 8 by the Dickson Lemma. //

Theorem 5.6a

If $p \equiv 1 \pmod{16}$ $G \cong \text{PSL}(2,p)$.

Proof

$A, B$ lie inside $\text{PGL}(2,p)$ and have square determinants. Hence by Theorem 5.5 $G$ must be isomorphic to $\text{PSL}(2,p)$.

Theorem 5.6b

If $p \equiv 9 \pmod{16}$ $G \cong \text{PGL}(2,p)$.

Proof

The generators of the stabilizer of $k_0$ are induced by matrices with square determinants and so they belong to $G \cap \text{PSL}(2,p)$. The element $A^2$ also belongs to $G \cap \text{PSL}(2,p)$ and it is not in the stabilizer of $k_0$ so $G \cap \text{PSL}(2,p) \cong \text{PSL}(2,p)$. Since 4 contains the element $A$ not in $\text{PSL}(2,p)$ we must have $G \cong \text{PGL}(2,p)$. //

Theorem 5.6c

If $p \equiv 15 \pmod{16}$ $G \cong \text{PSL}(2,p)$. 
Proof

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

\[
\det A_0 = 1, \quad A_0 A_0^* = I,
\]

where \( A_0^* \) is transposed conjugate of \( A_0 \) with respect to the field automorphism \( x \mapsto x^p \) of \( \mathbb{GF}(p^2) \). In other words \( A_0 \) belongs to the special unitary group \( SU(2, p^2) \). The same is true for \( B_0 = (\tau^2)^{-1}B \), and so \( G = \langle A, B \rangle \) is a subgroup of \( PSU(2, p^2) \). However it is known that \( PSU(2, p^2) \) is isomorphic to \( PSL(2, p) \). Hence by Theorem 5.5 \( G \) is isomorphic to \( PSL(2, p) \).

Theorem 5.6d

If \( p \equiv 7 \pmod{16} \) \( G \equiv PSL(2, p) \).

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 \( G_0 \) denote the stabilizer of \( k \) and let \( K = \langle G_0, A^2B^2 \rangle \). \( G_0 \) is generated by the elements \( A^{1-r}B^rA^{-1} \) \( (1 \leq r \leq 4) \), or by the transformations \( t \mapsto 1/t, \ t \mapsto it, \ t \mapsto (1-t)/(1+t) \). We can choose matrices representing these transformations as follows:
which all belong to SU(2, p^2). The matrices \( A_o^2 = (2o)^{-1}A^2 \) and 
\( B_o^2 = (-2o)^{-1}B^2 \) induce the same automorphisms as \( A^2 \) and \( B^2 \) respectively 
and both belong to SU(2, p^2). Thus as before we have \( K = \text{PSU}(2, p^2) = \text{PSL}(2, p) \).

Now for each generator \( A^{1-r} B^r A^{-1}, A^2 B^2 \) of \( K \) the result of conjugating 
by \( A \) or \( B \) is also in \( K \). Since \( AB^{-1} \in K \) we must have \( AK = BK = KB = KA \).
It follows that there are just two cosets of \( K \) in \( H \), so from
Theorem 5.5 \( G = \text{PGL}(2, p) \).

It must be remarked that when \( p \equiv 7 \) or \( 15 \) (mod 16) the group \( G \) is not 
a "canonical" subgroup \( \text{PGL}(2, p) \) or \( \text{PSL}(2, p) \) of \( \text{PGL}(2, p^2) \); the 
coefficients of the generators do not lie in \( \text{GF}(p) \).

Case \( p \equiv 3 \) or \( 5 \) (mod 8)

Lemma 5.6c

\( G \) is isomorphic to \( \text{PGL}(2, p^2) \).

Proof

In this case \( p^2 \equiv 9 \) (mod 16) so \( \sigma \) is not a square in the field 
\( \text{GF}(p^2) \). Both \(-1 \) and \( 2 \) are squares however, so neither \( A \) nor \( B \) is 
a member of \( \text{PSL}(2, p^2) \). In a finite field the product of two 
nonsquare elements is always a square. Hence the product of two 
elements of \( \text{PGL}(2, p^2) \) outside \( \text{PSL}(2, p^2) \) must always lie in \( \text{PSL}(2, p^2) \).

Thus if \( G_o \) is the intersection of \( G \) and \( \text{PSL}(2, p^2) \), \( G_o \) must 
contain \( AB^{-1}, A^2 B^{-2}, A^3 B^{-3} \) and \( A^4 B^{-4} \) the elements generating the 
stabilizer of the vertex \( k_o \). \( G_o \) lies inside \( \text{PSL}(2, p^2) \) so we may 
now apply the Dickson Lemma. Since \( G_o \) contains a vertex-stabilizer
The matrices \( A_o^2 = (\sigma)^{-1}A^2 \) and 
\( B_o^2 = (-2\sigma)^{-1}B^2 \) induce the same automorphisms as \( A^2 \) and \( B^2 \) respectively and both belong to \( SU(2, p^2) \). Thus as before we have \( K \cong PSU(2, p^2) \cong PSL(2, p) \).

Now for each generator \( A^{1-r} B^{r} A^{-1}, A^2 B^2 \) of \( K \) the result of conjugating by \( A \) or \( B \) is also in \( K \). Since \( AB^{-1} \in K \) we must have \( AK = BK = KB = KA \).

It follows that there are just two cosets of \( K \) in \( H \), so from Theorem 5.5 \( G \cong PGL(2, p) \).

It must be remarked that when \( p \equiv 7 \) or \( 15 \) (mod 16) the group \( G \) 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 \( GF(p) \).

Case \( p \equiv 3 \) or \( 5 \) (mod 8)

Lemma 5.6c

\( G \) is isomorphic to \( \overline{PGL(2, p^2)} \).

Proof

In this case \( p^2 \equiv 9 \) (mod 16) so \( \sigma \) is not a square in the field \( GF(p^2) \). Both -1 and 2 are squares however, so neither \( A \) nor \( B \) is a member of \( PSL(2, p^2) \). In a finite field the product of two nonsquare elements is always a square. Hence the product of two elements of \( PGL(2, p^2) \) outside \( PSL(2, p^2) \) must always lie in \( PSL(2, p^2) \).

Thus if \( \Go \) is the intersection of \( G \) and \( PSL(2, p^2) \), \( \Go \) must contain \( AB^{-1}, A^2 B^{-2}, A^3 B^{-3} \) and \( A^4 B^{-4} \) the elements generating the stabilizer of the vertex \( k_o \). \( \Go \) lies inside \( PSL(2, p^2) \) so we may now apply the Dickson Lemma. Since \( \Go \) contains a vertex-stabilizer
which is isomorphic to $S_4$ and a further element $A^2$ which is not of order 2, $G_o$ must be isomorphic to either $PSL(2,p)$, $PGL(2,p)$ or $PSL(2,p^2)$.

All elements of $PGL(2,p)$ and $PSL(2,p)$ have order dividing one of $p-1, p^2+p+1$ [24]. We now show $G_o$ is isomorphic to $PSL(2,p^2)$ by showing that the element $A^2$ of $G_o$ cannot be a member of any subgroup isomorphic to $PGL(2,p)$ or $PSL(2,p)$.

The eigenvalues of the matrix $\phi^{-1}(A^2)$ lie in the field $GF(p^4)$ and have order dividing $p^4-1$. The order of these eigenvalues must divide the order of $A^2$. Hence if $A^2$ lies in a subgroup isomorphic to either $PGL(2,p)$ or $PSL(2,p)$ the eigenvalues $\lambda_1, \lambda_2$ of $\phi^{-1}(A^2)$ must have order dividing $p-1$ or $p+1$.

\[
\phi^{-1}(A^2) = \begin{pmatrix}
\frac{\sigma-1}{2} & -\frac{\sigma+1}{2} \\
\frac{\sigma+1}{2\sigma} & \frac{1-\sigma}{2\sigma}
\end{pmatrix}
\]

and the characteristic equation of this matrix is given by

\[
\lambda^2 - \left[ \frac{(\sigma-1)}{2\sigma} \right] \lambda + 1 = 0.
\]

We now use the identity $(\sigma-1)^2 = \sigma(\sqrt{2}-2)$ to obtain

\[
\lambda_1 = \frac{\sqrt{2}-2+\sqrt{(-4\sqrt{2}-10)}}{4}
\]

and

\[
\lambda_2 = \frac{\sqrt{2}-2-\sqrt{(-4\sqrt{2}-10)}}{4}.
\]

Each element of $GF(p^2)$ may be expressed in the form $a+b\sqrt{2}$ for some $a,b$ in $GF(p)$, since $\sqrt{2}$ is contained in $GF(p^2)$ but not in $GF(p)$. $(\sigma+\sigma^{-1})^2 = 2$ so $\sqrt{2} = \sigma+\sigma^{-1}$. Hence
\[ (\sqrt{2})^P = (\sigma + \sigma^{-1})^P = \sigma^3 + \sigma^{-3} = \sigma^4(\sigma^{-1} + \sigma) = -\sqrt{2}. \]

Thus \((a + b\sqrt{2})^P = a - b\sqrt{2}\) if \(a, b \in \text{GF}(p)\).

Suppose \(\lambda_1\) has order dividing \(p - 1\) or \(p + 1\). Because \(\lambda_1\) is in \(\text{GF}(p^2)\), and members of \(\text{GF}(p)\) \(a, b\) may be chosen such that

\[ \lambda_1 = \frac{\sqrt{2} - 2 + a + b\sqrt{2}}{4} \]

and

\[ \lambda_2 = \frac{\sqrt{2} - 2 - a - b\sqrt{2}}{4}. \]

\[ \lambda_1^p = \lambda_1 \text{ or } \lambda_1^{-1}, \text{ and } \lambda_1^{-1} = \lambda_2. \]

But

\[ \lambda_1^p = \frac{-\sqrt{2} - 2 + a - b\sqrt{2}}{4}. \]

Immediately \(\lambda_1^p \not\equiv \lambda_2\). Also there can be no value of \(a\) satisfying

\[ (a - \sqrt{2})^2 = -4\sqrt{2} - 10 \in \text{GF}(p^2) \text{ so } (b + 1) \not\equiv 0 \text{ and } \lambda_1^p \not\equiv \lambda_1. \] Hence the order of \(\lambda_1\) does not divide \(p - 1\) or \(p + 1\).

Hence \(A^2\) lies outside all subgroups of \(\text{PSL}(2, p^2)\) isomorphic to \(\text{PSL}(2, p)\) or \(\text{PGL}(2, p)\) and the group \(G_0\) must be \(\text{PSL}(2, p^2)\).

\(G\) strictly contains \(G_0\) and is a subgroup of \(\text{PGL}(2, p^2)\) and consequently must be isomorphic to \(\text{PGL}(2, p^2)\). \(\lceil\)
The 5-arctransitive Cases

There are further automorphisms of $\text{GF}(p^2)$ under which sextets are preserved, which are not contained in $\text{PGL}(2,p^2)$. The group $\text{PFL}(2,p^2)$ is constructed by adjoining the field automorphism $\phi: x \mapsto x^p$ of $\text{GF}(p^2)$. We need to find the values of $p$ for which $\phi$ induces a new automorphism of $\text{Soc}(p^2)$.

**Theorem 5.7**

The group $\text{PFL}(2,p^2)$ acts transitively on $\text{Soc}(p^2)$ if $p \equiv 3$ or $5 \pmod{8}$.

**Proof**

Let $p \equiv 3$ or $5 \pmod{8}$, and $\omega$ denote an eighth root of unity in $\text{GF}(p^2)$. Now the sextets

\[
\begin{align*}
    k_{-1} &= \{0, \omega, \omega^3, -\omega^3\} \\
    k_0 &= \{0, \omega, i, -i, 1, -1\} \\
    k_1 &= \{i, -i, 1+\sqrt{2}, 1-\sqrt{2}, -1+\sqrt{2}, -1-\sqrt{2}\} \\
    k_2 &= \{1+\sqrt{2}, 1-\sqrt{2}, 3(\sqrt{2}-1)^{-1}, (1-i\sqrt{2})^{-1}, (1+i\sqrt{2})^{-1}\}
\end{align*}
\]

constitute a 3-arc. We now use the fact that $(a+b)^p = a^p + b^p$ in a field of characteristic $p$ to establish that this 3-arc is fixed by the field automorphism $\phi$.

Two adjacent sextets have one duet in common. If a duet $D$ is fixed by an automorphism $\alpha$, then 2 adjacent sextets containing $D$ are either both fixed by $\alpha$ or both moved. It is easily verified that the three duets $\{0, \omega\}, \{i, -i\}, \{1+\sqrt{2}, 1-\sqrt{2}\}$ are all fixed by $\phi$ and consequently so are the sextets $k_{-1}, k_0, k_1, k_2$. The duet $\{\omega, -\omega\}$ is fixed if $p \equiv 5 \pmod{8}$ but not if $p \equiv 3 \pmod{8}$; however the reverse is true...
for the duet \{3(i\sqrt{2} - 1)^{-1}, (1 - i\sqrt{2})^{-1}\} which is fixed if \( p \equiv 3 \pmod{8} \) but not if \( p \equiv 5 \pmod{8} \). Hence if \( p \equiv 3 \) or 5 (mod 8) the automorphism \( \phi \) is nontrivial and it fixes a four-arc (containing the 3-arc \( \overline{k_1k_0k_1k_2} \) and one other sextet) and thus \( S_o(p^2) \) is 5-arctransitive. //

If \( p \equiv 1 \pmod{8} \) then \( S_o(p^2) = S_o(p) \), and \( \phi \) acts trivially on \( S_o(p) \) since it fixes the subfield \( GF(p) \) of \( GF(p^2) \). If \( p \equiv 7 \pmod{8} \) the automorphism of \( S_o(p^2) \) induced by \( \phi \) is the same as that induced by \( \gamma : x \mapsto -1/x \) and so \( PTL(2,p^2) \) induces a group of automorphisms acting 4-arctransitively on \( S_o(p^2) \). Hence the only family of 5-arctransitive sextet graphs is \( \{S_o(p^2) \mid p \equiv 3 \) or 5 (mod 8)\)
The girth of $S_o(p)$.

Now we attempt to find the girth of $S_o(p)$ by examining the constitution of the cycles in the terms of the shunts. The girth of $S_o(p^2)$ has been calculated for various values of $p$ and tabulated in Tables 31 - 35 in the Appendix - here we are interested in the effect on the girth as $p$ becomes large. It is believed the girth tends to infinity.

Definition

We define a **positive word of length** $n$ in $x$ and $y$ $w(x,y)$ to be a string of $n$ letters each of which is either $x$ or $y$. Given a positive word in $x$ and $y$ $w(x,y)$ and a semi-group $H$ containing two elements $u,v$, the element of $H$ $w_H(u,v)$ is obtained from $w(x,y)$ by replacing each $x$ and $y$ in the string by $u$ and $v$ respectively and treating the string as a product in the semi-group $H$.

Suppose $\Gamma$ is a cubic graph on which the group $G$ acts $s$-arctransitively where $s \geq 2$. Let $P_0P_1 \ldots P_s$ be an $s$-arc in $\Gamma$. Then there exist elements of $A,B$ of $G$ representing the twin shunts mapping $P_0P_1 \ldots P_s$ onto its successors $P_1 \ldots P_s P_{s+1}$ and $P_1 \ldots P_s P_{s+1}$.

Theorem 5.8

There is a one-to-one correspondence between the cycles through the $s$-arc $P_0P_1 \ldots P_s$ and the positive words such that $W_G(A,B)$ is the identity in the group $G$. 
Proof

Let $p_0^*,\ldots,p_s^*\ldots,p_g^* = p_0$ be a cycle of length $g$ in $\Gamma$ and let $p_{g+k} = p_k$ for all nonnegative $k$. $p_1^{*} \ldots p^*_{i+s}$ is also an $s$-arc, so by the $s$-arc-transitivity of $G$ there is a unique element $w_i$ of $G$ such that $w_ip_a = p_{a+i}$ for all $0 \leq a \leq s$. For instance $w_0 = 1_G$ is the identity element of $G$. We now find possible expressions for $w_{i+1}$ in terms of $w_i$, given $w_{i+1}p_a = p_{a+i+1}$ for all $0 \leq a \leq s$.

Now $w_{i}p_a = w_{i}p_{a+1} = p_{a+i+1}$ for all $0 \leq a \leq s-1$. The vertices $w_{i}p_a$ and $w_{i}p_{a+1}$ are both adjacent to $w_{i}p_{a-1}$, and $w_{i}p_{a+1} = w_{i}p_{a+2} = w_{i}p_{a+3}$. Hence one of $w_{i}p_a$ and $w_{i}p_{a+1}$ must be $p_{a+i+1}$, and so $w_{i+1}$ is either $w_{i}A$ or $w_{i}B$. Now using induction and the fact that $w_0 = 1_G$ we have $w_i = C_1 C_2 \ldots C_i$ where $C_j$ is either $A$ or $B$ for all $j$ and consequently there is a positive word $W(A,B)$ in $A$ and $B$ such that $w_i = W_i(A,B)$. But $w_g = w_0 = 1_G$ so each cycle corresponds to a positive word $W(A,B)$ in $A$ and $B$ such that $W_g(A,B) = 1_G$.

Conversely, suppose $W_g(A,B) = 1_G$ for some positive word, say $W_g(A,B) = C_1 \ldots C_g = 1_G$ with $C_j$ equal to either $A$ or $B$ for all $j$. Let $w_i = C_1 \ldots C_i$ and $w_0 = 1_G$. Now let $p_{i+s} = w_{i}p_s$, so $p_i = w_{i}p_o = W_{i-1}C_1 p_o$. But $C_1 p_o = p_1$ so $p_i = W_{i-1}p_1$ which is adjacent to $W_{i-1}p_{o} = p_{i-1}$. Hence $p_0, p_1, \ldots, p_g$ is a sequence of vertices with the property $P_i$ is adjacent to $P_{i+1}$ for all $0 \leq i \leq g-1$. Further if $P_{i-1} = P_{i+1}$ then $W_{i-1}p_{o} = W_{i-1}p_2$ which is not possible, so $p_0^*, \ldots, p_g^*$ must be a
cycle \( p_g = p_0 \) because \( W_g = 1_0 \) through the \( s \)-arc \( p_0, \ldots, p_s \).

Let \( \alpha = \begin{pmatrix} x & -x \\ 1 & 1 \end{pmatrix} \) and \( \beta = \begin{pmatrix} x & x \\ 1 & -1 \end{pmatrix} \), elements in the ring \( R \) of \( 2 \times 2 \) matrices whose entries are polynomials with integer coefficients.

Let \( W(X,Y) \) be a positive word of length \( n \).

Then
\[
W = W_R(\alpha,\beta) = \begin{pmatrix} a_w(x) & b_w(x) \\ c_w(x) & d_w(x) \end{pmatrix}
\]
for some \( a_w(x), b_w(x), c_w(x), d_w(x) \) polynomials in \( x \) with integer coefficients. The leading coefficient of each of these polynomials is always \( \pm 1 \), and \( a_w(x) \) and \( b_w(x) \) are of degree \( n \) while \( c_w(x) \) and \( d_w(x) \) are of degree \( n-1 \). This is easily verified by induction.

Given \( p \equiv 1 \pmod{8} \) there exists an element \( \sigma_p \) in \( GF(p) \) of order \( 8 \). Let \( f(x) \) denote the polynomial \( f(x) \) with coefficients reduced modulo \( p \). We define the mapping \( \phi_p \) from the set of positive words in \( \alpha \) and \( \beta \) to the group \( PGL(2,p) \) of linear fractional transformations of \( GF(p) \) as follows. If \( W = W_R(\alpha,\beta) \)
\[
\phi_p(W) : t \mapsto \frac{a_w(\sigma_p)t + b_w(\sigma_p)}{c_w(\sigma_p)t + d_w(\sigma_p)}.
\]

From theorem 5.2 we deduce the following lemma.

Lemma 5.9

When \( \alpha,\beta \) are considered as positive words in \( \alpha \) and \( \beta \) \( \phi_p(\alpha) \)
and \( \phi_\beta \) are twin shunts of a four arc in \( S(p) \).

Let \( I_p \) denote the identity element of the groups \( \text{PGL}(2,p) \) and \( W = w_\alpha(\alpha,\beta) \) an element of \( R \).

**Theorem 5.10**

If \( \phi_p(W) = I_p \) for every \( p \) in an infinite set of primes \( P \) then \( \phi_p(W) = I_p \) for all primes \( p \).

**Proof**

Suppose \( \phi_p(W) = I_p \) for some word \( W \) and prime \( p \).

\[
\phi_p(W) : t \mapsto \frac{a_w(\sigma_p)t + b_w(\sigma_p)}{c_w(\sigma_p)t + d_w(\sigma_p)}, \text{ where } \sigma_p \text{ satisfies } \sigma_p^4 + 1 \equiv 0 \pmod{p}.
\]

\( \phi_p(W) = I_p \) implies \( b_w(\sigma_p) = 0 \), which in turn implies \( \sigma_p \) satisfies the equations \( b_w(x) \equiv 0 \) and \( x^4 + 1 \equiv 0 \pmod{p} \) simultaneously.

Then the polynomials \( b_w(x) \) and \( x^4 + 1 \) when considered as elements of the ring of polynomials with coefficients in \( \mathbb{F}_p \) have a common nonconstant factor. If \( \overline{m} = m \) reduced \( \pmod{p} \)

\[
b_w(x) = b_n x^n + b_{n-1} x^{n-1} + \ldots + b_1 x, \text{ implies } \overline{b_w(x)} = \overline{b_n x^n} + \ldots \overline{b_1 x}.
\]

The resultant of \( \overline{b_w(x)} \) and \( x^4 + 1 \) is the determinant of the \((n+4)\times(n+4)\) matrix
The resultant of two polynomials vanishes if and only if they have a common nonconstant factor \([36]\). Hence \(\det(M_p) \equiv 0 \pmod{p}\).

If \(M = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{bmatrix}\)

then \(\det(M) \equiv \det(M_p) \pmod{p}\). But \(\det(M_p) \equiv 0 \pmod{p}\) so \(p\) divides \(\det(M)\). If \(\det(M)\) is nonzero only a finite number of primes divide \(\det(M)\) and consequently \(\phi_p(M) = 1\) for only a finite number of primes \(p\).
If \( \det M = 0 \) and \( b(x) \) have a common nonconstant factor, and since \( x^4 + 1 \) is the minimal polynomial for each of its roots \( x^4 + 1 \) divides \( b(x) \).

Taking the resultants of \( x^4 + 1 \) and \( c(x) \), and of \( (x^4 + 1) \) and \( a(x) - d(x) \), we obtain the result that either \( \phi_p(W) = I \) for only a finite number of primes \( p \)

or

\[
W = (x^4 + 1)K + g(x)I
\]

where \( K \) is an element of \( R \) and \( I \) is the matrix \( \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \) and \( g(x) \) is a polynomial with integer coefficients.

In this case \( \phi_p(W) = I \) for all primes \( p \).

We are now in a position to examine, firstly, the length of the shortest odd cycle in \( S_o(p) \) and secondly the girth itself, as \( p \) tends to infinity.

**Theorem 5.11**

Given an odd number \( g \) there exists a prime \( p_g \) such that the length of the shortest odd cycle in the graph \( S_o(p) \) is longer than \( g \) if \( p \) is greater than \( p_g \).

**Proof**

We need the fact that if \( p \equiv 9 \pmod{16} \) \( S_o(p) \) is bipartite and contains no odd cycles. Let \( W = w_R(\alpha, \beta) \) be a positive word in \( \alpha \) and \( \beta \) of odd length. Then \( \phi_p(W) \) does not correspond to a cycle in \( S(p) \).
if \( p \equiv 9 \pmod{16} \). Thus by Theorem 5.10 \( \phi_p(W) \) only corresponds to an identity word in \( S(p) \) for a finite number of values of \( p \) and we can define \( p(W) \) to be the largest prime with the property \( \phi_p(W) = I_p \), the identity element in \( \text{FGL}(2,p) \). Since there is only a finite number of positive words of a given length, if \( S_g \) is the set of positive words of odd length less than or equal to \( g \), then all the odd cycles in \( S(p) \) are of length greater than \( g \) if \( p \) is more than \( p(W) \) for all \( W \) in \( S_g \).

**Theorem 5.12**

Either there exists a value \( g \) and a prime \( p_g \) such that if \( p > p_g \), then the girth of \( S(p) \) is \( g \), or given \( g \) there exists \( q_g \) such that if \( p > q_g \) then the girth of \( S(p) \) is greater than \( g \).

**Proof**

As in the previous proof we define \( S_n \) to be the set of positive words of length strictly less than \( n \) and \( p(W) \) is defined for words \( W \) for which there exists a prime \( \pi \) such that \( \phi_\pi(W) \nmid I_\pi \) to be the largest prime with the property \( \phi_{p^{(W)}(W)} = I_{p^{(W)}} \), or 1 if there is no such prime. If \( \ell \) is the length of the shortest word \( W \) such that \( \phi_p(W) = I_p \) for all primes \( p \), then if \( p \) is more than \( p(W) \) for all \( W \) in \( S_\ell \) the girth of \( S(p) \) is \( g \); if no such word exists then given \( g > 0 \) if \( p \) is more than \( p(W) \) for all \( W \) in \( S_g \) the girth of \( S(p) \) is at least \( g \).
Remarks

Hence we have constructed a family of highly transitive graphs for which it is conjectured there is no upper bound to the girth. The family also yields examples of graphs which in many cases are the smallest known trivalent graphs with a given girth. The girths and orders of the shunts of the graphs known to have girth less than 32 are given in the tables on pages 77f; we now take a closer look at some of them.

In the family of 5-arctransitive graphs, the simplest case $p \equiv 3$ yields the graph $S_5^9$ which is Tutte's 8-cage [34]; its group is $\text{Aut}(S_5^9) \cong \text{PFL}(2,9)$. It has 30 vertices. The next graph is the family is $S(25)$ with 650 vertices. This graph was found independently by R.M. Foster and J.H. Conway but it has not been published before. There are only five known 5-arctransitive graphs with less than 1000 vertices; one of the others is a 3-fold covering of $S_5^9$.

No other graphs in the family $S(p^2)$, $p \equiv 3$ or $5 \pmod{8}$ have been previously noticed, and it seems that it has not hitherto been recognized that an infinite family of 5-arctransitive graphs can be constructed in this way. The general idea of using octahedral ($S_4$) subgroups of PSL and PGL groups has been familiar, at least since the paper of Wong [38] in 1967.
The original motivation for this study was a question raised by Djokavic and Miller [15]. In our notation, they asked for a formula for the girth of the graphs $S_o(p^2)$ in the cases $p \equiv 1$ or $15 \pmod{16}$. We have already seen that in these cases $S_o(p^2)$ has $1/48p(p^2-1)$ vertices and its automorphism group is isomorphic to $PSL(2,p)$ and in fact also acts primitively on the graph. The girths of many of the sextet graphs have been computed but no general result has been found. There is, however, apparently no upper bound for the girth. Consequently the sextet graphs provide examples of cubic graphs with given girth $g$ for many values of $g$ for which no specific example is known except as a result of unwieldy general theorems. For example, the graph $S_o(313)$ has girth 30. It has $277,666 = 2^{20}$ vertices, whereas previously it was known only that at least $2^{16}$ vertices are necessary and $2^{30}$ vertices are sufficient [34].

Of the sextet graphs whose automorphism group is isomorphic to $PSL(2,p)$ Ito has shown [25] that only $PSL(2,7)$ and $PSL(2,23)$ can act 4-arctransitively on a Cayley graph so $S_o(49)$ and $S_o(529)$ are the only Cayley graphs in the family. $S_o(49)$ is the Heawood graph with 14 vertices which we have already seen is Cayley in Chapter 4. $S_o(529)$ has 506 vertices and is the Cayley graph of the group $G$ with the presentation:

$$G = \langle R, S \mid R^2 = S^{22} = RS^5RS^2RS^4 \rangle.$$  

We have already encountered this group as $PG(1,23)$ with the generators

$$R : x \mapsto 22-x, \quad S : x \mapsto 17x,$$
and in terms of the shunts the group is generated by

\[ B \text{ and } A^3 B^3 A^4 B^{-4} A^3 B^{-3} A^{-1} \].

This was established using "Cayley" a grouptheoretic computing package.
Appendix

Table 1

Table 1 is a tabulation of the results discussed in Chapter 2 and Chapter 4. \( N(3,g) \) is taken to represent the order of the smallest known trivalent graph with girth \( g \), and \( N^c(3,g) \), the order of the smallest Cayley graph with these properties. If the value given is marked with an asterisk it is not known whether this figure represents the true minimum or not. Either the group attaining the known minimum is named or a reference to a previous chapter or another table is given. The 2-fold coverings mentioned are obtained as follows.

2-fold Coverings

Let \( G \) be a graph of order \( m \) with odd girth \( g \) and vertexset \( V(G) = \{v_1, \ldots, v_m\} \) and edgeset \( E(G) \). Define \( V'(G) = \{v_1', \ldots, v_m'\} \).

Now construct a new graph \( G' \) with vertexset \( V(G') = V(G) \cup V'(G) \) and edgeset

\[
E(G') = \{(v_a, v'_b) \mid (v_a, v_b) \in E(G)\}.
\]

This graph is bipartite and can contain no cycles of length \( g \).

A graph with 6072 vertices and girth 17

Let \( G \) be the Cayley graph of the group \( \text{PSL}(2,23) \), with generating set \( \{R, S\} \) where

\[
R : X \mapsto \frac{1}{X} \quad \text{and} \quad S : X \mapsto X + 2 \pmod{23}
\]
acting on the set $\text{GF}(23) \cup \{\infty\}$ where $\infty + a = \infty$ and $-1/0 = \infty$, $-1/\infty = 0$.

Then it has been verified by computer that the girth of $G$ is 17.

Table 2

Table 2 gives the girth $g$ and diameter $d$ of the Cayley graph of $\text{Aff}(p^f)$ with generating set $\langle R, S \rangle$ where

$$R : x \mapsto -1 - x \text{ and } S : x \mapsto ax \pmod{p}.$$ 

The arctransitivity of the graph is given in the column marked $s$ and the number of vertices in that headed $|V(G)|$.

Tables 3.1 - 3.5

Tables 3.1 - 3.5 give the girth $g$ of $S_o(p^2)$ for odd primes $p$. The constant $c$ represents $g^{-1} \log_2 n$ where $n$ gives the number of vertices in the graph. $|a|$ and $|b|$ represent the shunt orders and $w_g$ gives the identity words of length $g$ where known.

Table 4

Table 4 contains various details about the 32 known 60 vertex trivalent graphs of girth 9. $N$ represents the number of 9 cycles in the graph and $G$ its automorphism group. $\lambda_{\min}$ corresponds to the smallest eigenvalue of the adjacency matrix.
<table>
<thead>
<tr>
<th>g</th>
<th>$n_o(3,g)$</th>
<th>$N(3,g)$ Graph</th>
<th>$N_c(3,g)$ Graph</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>4</td>
<td>4 $K_4$</td>
<td>4 $K_4$</td>
</tr>
<tr>
<td>4</td>
<td>6</td>
<td>6 $K_3,3$</td>
<td>6 $K_3,3$</td>
</tr>
<tr>
<td>5</td>
<td>10</td>
<td>10 Petersen</td>
<td>50 $[C4]$</td>
</tr>
<tr>
<td>6</td>
<td>14</td>
<td>14 Heawood</td>
<td>14 Heawood</td>
</tr>
<tr>
<td>7</td>
<td>22</td>
<td>24 McGee</td>
<td>30 $[C4]$</td>
</tr>
<tr>
<td>8</td>
<td>30</td>
<td>30 Tutte</td>
<td>42 $[C4]$</td>
</tr>
<tr>
<td>9</td>
<td>46</td>
<td>58 $[C2]$</td>
<td>60 $[C4]$</td>
</tr>
<tr>
<td>10</td>
<td>62</td>
<td>70 Balaban &amp; c.</td>
<td>100 $[11]$</td>
</tr>
<tr>
<td>11</td>
<td>94</td>
<td>112 $[1]$</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>126</td>
<td>126 Benson</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>190</td>
<td>272 $[T2]$</td>
<td>272 $[T2]$</td>
</tr>
<tr>
<td>15</td>
<td>382</td>
<td>620 $S_o(31^2)$</td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>510</td>
<td>1240* 2 fold cov.</td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>766</td>
<td>6072*</td>
<td>6072*</td>
</tr>
<tr>
<td>18</td>
<td>1022</td>
<td>12144* 2 fold Cov.</td>
<td>12144*</td>
</tr>
<tr>
<td>19</td>
<td>1534</td>
<td></td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>2046</td>
<td>14910* $S_o(71^2)$</td>
<td></td>
</tr>
<tr>
<td>21</td>
<td>3070</td>
<td></td>
<td></td>
</tr>
<tr>
<td>22</td>
<td>4094</td>
<td>16206* $S(73)$</td>
<td></td>
</tr>
<tr>
<td>25</td>
<td>12286</td>
<td>149768* $S_o(193)$</td>
<td></td>
</tr>
<tr>
<td>28</td>
<td>32766</td>
<td>527046* $S(223)$</td>
<td></td>
</tr>
<tr>
<td>30</td>
<td>65534</td>
<td>1227666* $S(313)$</td>
<td></td>
</tr>
<tr>
<td>32</td>
<td>131070</td>
<td>5892510* $S(521)$</td>
<td></td>
</tr>
</tbody>
</table>

**TABLE 1**
| p  | \( |V(G)| \) | a | g | d | s |
|----|----------------|---|---|---|---|
| 7  | 42             | 3 | 6 | 6 | 1 |
| 11 | 110            | 2 | 10| 7 | 0 |
| 13 | 156            | 2 | 9 | 8 | 0 |
| 17 | 272            | 3 | 13| 8 | 0 |
| 19 | 342            | 2 | 12| 9 | 0 |
| 23 | 506            | 5 | 14| 9 | 0 |
| 29 | 812            | 2 | 12| 10| 0 |
| 31 | 930            | 3 | 12| 12| 0 |

**TABLE 2**
SEXTET GRAPHS

$S(q)$ is defined for $q$ a prime power $\equiv 1 \pmod{8}$

$|S(q)| = N = \frac{1}{24} q(q^2 - 1)$, and $\text{PGL}(2,q)$ acts 4-transitively.

$S(q)$ has $K$ components, all isomorphic, denoted by $S_\circ(q)$.

$|S_\circ(q)| = N_\circ = N/K$ and a group $G_\circ$ acts $S$-arc transitively.

<table>
<thead>
<tr>
<th>$p \pmod{16}$</th>
<th>$p^2 \pmod{16}$</th>
<th>$S(p)$</th>
<th>$S(p^2)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>3</td>
<td>9</td>
<td>PSL(2,p)</td>
<td>2(p^2+1)</td>
</tr>
<tr>
<td>5</td>
<td>9</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>7</td>
<td>1</td>
<td></td>
<td>p(p^2+1)</td>
</tr>
<tr>
<td>9</td>
<td>1</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>11</td>
<td>9</td>
<td>PGL(2,p)</td>
<td>p(p^2+1)</td>
</tr>
<tr>
<td>13</td>
<td>9</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>15</td>
<td>1</td>
<td></td>
<td>2(p^2+1)</td>
</tr>
</tbody>
</table>

So we get five families of connected graphs:

$F_1$ (1) $S(p^2)$, $p \equiv 3,5 \pmod{8}$, 5-transitive, bipartite.

$F_2$ (2) $S_\circ(p)$, $p \equiv 1 \pmod{16}$, 4-transitive, primitive.

$F_3$ (3) $S_\circ(p^2)$, $p \equiv 7 \pmod{16}$, 4-transitive, bipartite.

$F_4$ (4) $S(p)$, $p \equiv 9 \pmod{16}$, 4-transitive, bipartite.

$F_5$ (5) $S_\circ(p^2)$, $p \equiv 15 \pmod{16}$, 4-transitive, primitive.

TABLE 3.0
\[ p \equiv 3, 5, 11, 13 \pmod{16} \]

\[ n = \frac{1}{24} p^2 (p^4 - 1), \quad G_0 = PSL(2, p^2) \]

<table>
<thead>
<tr>
<th>( p^2 )</th>
<th>( g )</th>
<th>( c )</th>
</tr>
</thead>
<tbody>
<tr>
<td>3^2</td>
<td>8</td>
<td>.613</td>
</tr>
<tr>
<td>5^2</td>
<td>12</td>
<td>.779</td>
</tr>
<tr>
<td>11^2</td>
<td>20</td>
<td>.808</td>
</tr>
<tr>
<td>13^2</td>
<td>24</td>
<td>.734</td>
</tr>
<tr>
<td>19^2</td>
<td>28</td>
<td>.746</td>
</tr>
</tbody>
</table>

**TABLE 3.1**

This family contains 5-arctransitive graphs so the order of the shunts \( a, b \) and girth words are not relevant.
\[ p \equiv 7 \pmod{16} \]

\[ n = \frac{1}{24} p(p^2 - 1), \quad G_0 = \text{PGL}(2, p) \]

| p   | g  | c     | |a| | |b| |
|-----|----|-------|-----|-----|-----|
| 7   | 6  | .634  | 6  | 8   | \(a^6\) |
| 23  | 14 | .641  | 24 | 22  | \((aba^{-1}b)^2\) |
| 71  | 20 | .693  | 70 | 72  | \((a^4b^2a^{-1}b^{-1})^2\) |
| 103 | 22 | .703  | 104| 104 | \((a^4b^2a^{-1}b^{-1})^2\) |
| 151 | 26 | .659  | 152| 152 |               |
| 167 | 24 | .733  | 168| 166 |               |

**TABLE 3.3**
\[ p \equiv 15 \pmod{16} \]

\[ n = \frac{1}{48} p (p^2 - 1). \quad G_o = \text{PSL}(2, p^2) \]

| \( p \) | \( g \) | \( c \) | \(|a|\) | \(|b|\) | \( W_g \) |
|-------|-----|-----|-----|-----|-----|
| 31    | 15  | .618| 15  | 16  | \( a^{15} \) |
| 47    | 15  | .738| 23  | 23  | \((a^3b^2)^3\) |
| 79    | 13  | 1.025| 13  | 20  | \( a^{13} \) |
| 127   | 21  | .732| 64  | 32  | \((ab^2)^7\) |
| 191   | 19  | .902| 95  | 19  | \( a^{19} \) |
| 223   | 25  | .712| 111 | 111 | \( ab a^5 ba^2 ba^2 b^5 \) |
| 239   | 21  | .862| 119 | 119 | \((a^2b^2ab)^3\) |
| 271   | 25  | .746| 27  | 135 | \((a^3b^2)^5\) |

**TABLE 3.5**
|    | \( \lambda_{\text{min}} \) | N  | \( |G| \) |
|----|-------------------|----|--------|
| S  | -2.61803          | 60 | 360    |
| T1 | -2.61803          | 60 | 120    |
| T2 | -2.73205          | 80 | 120    |
| BB | -2.56155          | 72 | 48     |
| PF | -2.61803          | 96 | 144    |
| XA | -2.78165          | 84 | 24     |
| XB | -2.78327          | 76 | 8      |
| XC | -2.78686          | 74 | 4      |
| XD | -2.78790          | 75 | 6      |
| YB | -2.78327          | 76 | 8      |
| YC | -2.78686          | 74 | 4      |
| YD | -2.78804          | 75 | 2      |
| YE | -2.78683          | 74 | 1      |
| YF | -2.78790          | 75 | 3      |
| YG | -2.78299          | 76 | 2      |
| YH | -2.78165          | 84 | 6      |
| BALA| -2.78816          | 75 | 2      |
| BALB| -2.78419          | 72 | 4      |
| BALC| -2.78165          | 84 | 8      |
| PS1 | -2.68909          | 76 | 4      |
| PS2 | -2.71199          | 80 | 1      |
| H1 | -2.68867          | 76 | 8      |
| H2 | -2.65527          | 80 | 10     |
| H3 | -2.77253          | 73 | 1      |
| H4 | -2.80734          | 72 | 4      |
| H5 | -2.78804          | 73 | 1      |
| H6 | -2.71397          | 78 | 1      |
| H7 | -2.80592          | 71 | 2      |
| H8 | -2.75372          | 74 | 1      |
| H9 | -2.77178          | 73 | 1      |
| H10| -2.70076          | 75 | 1      |
| H11| -2.78804          | 73 | 1      |

**TABLE 4**
REFERENCES


5. N.L. Biggs, Algebraic Graph Theory CUP (1974).


18. R.M. Frucht, Remarks on Graphs Defined by Generating Relations, Canadian Jour. of Math. 7 (1955) 8-17.


28. B. McKay, Private Communication.


   43 (1947) 459-474.

36. B.L. van der Waerden, Modern Algebra Vol. 1
   - Frederick Ungar Publishing Company (1943).


38. W.J. Wong, Determination of a Class of Primitive Groups,