ELSEVIER
Theoretical Computer Science 204 (1998) 233–248
Theoretical Computer Science

On the structure of Hamiltonian cycles in Cayley graphs of finite quotients of the modular group

Paul E. Schupp

Department of Mathematics, University of Illinois, Urbana, IL 61801, USA

Abstract

It is a fairly longstanding conjecture that if G is any finite group with $|G| > 2$ and if X is any set of generators of G then the Cayley graph $\Gamma(G : X)$ should have a Hamiltonian cycle. We present experimental results found by computer calculation that support the conjecture. It turns out that in the case where G is a finite quotient of the modular group the Hamiltonian cycles possess remarkable structural properties.

1. Introduction

This paper describes some striking properties exhibited by Hamiltonian cycles in Cayley graphs of finite quotients of the modular group. These phenomena were discovered by doing a large amount of computer calculation.

Since we want to discuss the group-theoretical, graph-theoretical and computational setting of the problem we begin a detailed introduction.

In general, if $\Gamma = (V, E)$ is a finite graph, a *Hamiltonian cycle* in Γ is a simple closed path which goes through every vertex of Γ. A graph is *Hamiltonian* if it has at least one Hamiltonian cycle. Deciding whether or not a graph is Hamiltonian is a notorious NP-complete problem and questions about Hamiltonian cycles are thus very linked to current work in computational complexity. See [7, 15] for a detailed discussion of NP-completeness. In practice, NP-completeness means that the only *general* algorithm known for the problem is to "try all the possibilities". This method is soon blocked by the exponential increase in the number of possibilities and the "moral" is that for a feasible computation one must know why the case being considered is a special case and how to take advantage of this information.

In 1878 Cayley [3] described how to associate a graph, $\Gamma(G : X)$, now called the *Cayley graph*, to any group G together with a specified set X of generators of G. The resulting graph is *very* dependent on the set X of generators. In detail, the *vertices* of Γ are the elements of G. If $g \in G$ and $y \in (X \cup X^{-1})$ then there is a *directed*

0304-3975/98/$19.00
PII S0304-3975(98)00041-3

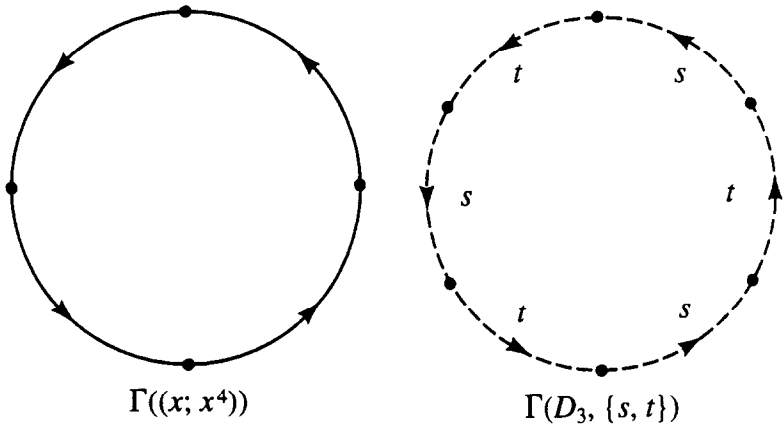

Fig. 1.

edge $e = (g, y, gy)$ in Γ from g to the element gy which has *label* y. We identify the two directed edges (g, y, gy) and (gy, y^{-1}, g) to a single undirected edge. Cayley thought of the edges corresponding to distinct pairs $\{y, y^{-1}\}$ as having different *colors*. The "usual drawing convention" for Cayley graphs is thus to draw one arc for each undirected edge with perhaps an arrow indicating one of its two possible orientations. We stress that for us a Cayley graph is an undirected graph – an edge can always be transversed in either direction and only the label (orientation) changes. One can consider a more general situation with directed graphs. If S is a set of semigroup generators for the group G, that is, every element of G is a product of elements of S but S need *not* be closed under taking inverses, then the *Cayley digraph* $\Gamma(G : S)$ has a directed edge labelled by $s \in S$ from g to gs. Much of the literature about cycles in graphs of groups concerns the digraph case, but we only consider undirected Cayley graphs in this paper.

Even the simplest examples show that the relationship between the algebraic properties of G and the geometric properties of $\Gamma(G : X)$ is not clear. If $G = \langle x; x^m \rangle$ is the cyclic group of order m then $\Gamma(G : \{x\})$ is the cyclic graph C_m. The dihedral group D_n, the group of the $2n$ symmetries of the regular n-gon, has two standard presentations:

$$\langle r, s; r^n, s^2, srs = r^{-1} \rangle$$

and also

$$\langle s, t; s^2, t^2, (st)^n \rangle.$$

(The second presentation is obtained from the first by introducing $t = sr$ and then substituting st for the generator r.) The graph $\Gamma(D_n : \{s, t\})$ is the cyclic graph C_{2n}.

So even Cayley graphs with respect to minimal sets of generators may lose much algebraic information about the group. At the other extreme, if G is any finite group and we take the set X of generators to be the set of all nontrivial elements of G then

$\Gamma(G:X)$ is just the complete graph on $|G|$ vertices and we have effaced all information except the order of the group. In this case $\Gamma(G:X)$ is certainly Hamiltonian.

It is a longstanding question/conjecture that if $\Gamma(G:X)$ is the Cayley graph of a finite group G with $|G|>2$ with X *any* set of generators of G then Γ is Hamiltonian. This was formulated as a question by Rankin [16] in 1948 and has since turned into a conjecture.

Before discussing what is known from the point of view of group theory, we review some results about Hamiltonian graphs. Our basic reference is West [17]. There is a family of theorems which ensure that a graph is indeed Hamiltonian. The most well-known result is probably

Ore's Theorem. *If Γ is a finite graph without loops or multiple edges, $|\Gamma|\geqslant 3$, and for every pair u,v of nonadjacent vertices of Γ*

$$d(u)+d(v)\geqslant|\Gamma|$$

then Γ is Hamiltonian.

To my knowledge, all provably sufficient conditions for a graph to be Hamiltonian are precise versions of the idea that "there are many vertices of large degree". In this paper we shall consider Cayley graphs of two-generator groups $\Gamma=\Gamma(G:\{s,t\})$ where s has order two and t has order three. Such graphs are *cubic* graphs, that is, all vertices have degree three. We are thus in the opposite situation where all vertices have low degree. Incidentally, it is well-known that the problem of deciding if a graph is Hamiltonian remains NP-complete when restricted to considering only cubic graphs.

There is a very simple condition which is necessary for a graph to be Hamiltonian. Namely, if $\Gamma=(V,E)$ is Hamiltonian then for every subset $S\subseteq V$, the graph $\Gamma\backslash S$ has at most $|S|$ components. As far as I know, this condition has not been proven to hold for Cayley graphs.

That every Cayley graph should have a Hamiltonian cycle is an expression of the idea that "A connected extremely symmetric graph is Hamiltonian". In general, a graph Γ is *vertex-transitive* if for every pair u,v of vertices of Γ there is an automorphism φ of Γ with $\varphi(u)=v$. Now a connected vertex-transitive graph Γ need not be Hamiltonian.

The "standard counterexample" of elementary graph theory is the Petersen graph illustrated below. The vertices are the two-element subsets of a set with five elements and there is an edge between two vertices when the sets are disjoint.

That the Petersen graph is vertex-transitive is clear from its definition. The Petersen graph does not have a Hamiltonian cycle but it does have a *Hamiltonian path*, that is, a simple path which visits every vertex of the graph. Lovász [11] has conjectured that every connected vertex-transitive graph has a Hamiltonian path. It is still an open question [2] as to whether or not there are infinitely many finite, connected, vertex-transitive graphs which do not have Hamiltonian cycles.

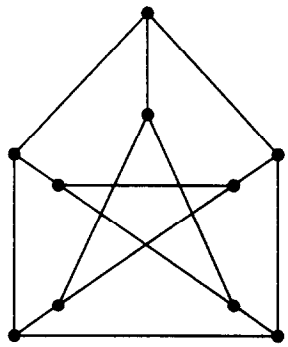

Fig. 2. The Petersen graph.

From the point of view of group theory, asking for a Hamiltonian path in a Cayley graph seems a more natural question. This is equivalent to asking if one can always enumerate the elements of the group without repetition by successive multiplications on the right by the given generators and their inverses. Of course a Cayley graph is "more symmetric" than simply being vertex-transitive. The action of G on $\Gamma(G : X)$ by multiplication on the left is a free action (multiplication by an element $g \neq 1$ moves every vertex) and is a sort of "rigid motion".

There are a few general theorems proving that the conjecture is true for certain special classes of groups. The current state of knowledge is discussed in the survey article of Curran and Gallian [5] from which we cite the following results. Witte [18] proved that if G is a group other than C_2 with prime power order then every Cayley graph of G is Hamiltonian. Keating and Witte [9] proved that if G is a group other than C_2 whose commutator subgroup is cyclic of prime power order then all Cayley graphs of G are Hamiltonian. Jungreis, Friedman and Witte [8] observe that the known results on special orders imply that if G is a group other than C_2 whose order is less than 100 and is not 48, 54, 60, 72, 75, 80, 84, 90 or 96 then every Cayley graph of G is Hamiltonian.

There are also some results concerning groups with particular choices of generators. Conway, Sloane and Wilkes [4] prove that if G is a finite group of isometries of Euclidean n-space and all the given generators are reflections then $\Gamma(G)$ has a Hamiltonian cycle. Glover and Young [6] prove that for the presentation

$$PSL(2, p) = \langle s, u; s^2, u^p, (su)^3 \rangle$$

$\Gamma(PSL(2, p); \{s, u\})$ has a Hamiltonian cycle.

It is difficult to imagine a proof for all presentations of a given class of groups which does not use induction and simple groups thus pose a major obstacle. My original motivation for a computer investigation was to search for a counterexample. But instead of a counterexample, structural properties of Hamiltonian cycles began to emerge.

2. Quotients of the modular group

The *modular group*, $PSL(2,\mathbb{Z})$, is the group of 2×2 integer matrices with determinant 1 modulo the relation that a matrix is identified with its negative. It is well-known that the modular group has generators $s = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 1 \end{smallmatrix}\right)$ of order 2 and $t = \left(\begin{smallmatrix} 0 & 1 \\ -1 & -1 \end{smallmatrix}\right)$ of order 3. Indeed, the modular group is the free product $\langle s : s^2\rangle \star \langle t : t^3\rangle$. (See [13]). By a $(2,3)$-*group* we mean a group G together with a distinguished pair (s,t) of generators where s has order 2 and t has order 3. Thus every $(2,3)$-group is a quotient of the modular group.

Finite quotients of the modular group are very abundant and almost all finite simple groups are $(2,3)$-groups. For the most recent results on this question see Liebeck and Shalev [10]. It is known that any noncyclic finite simple group can be generated by an element of order 2 and one other element. In particular, the fact that all the alternating groups A_n, with $n \geqslant 3$, $n \neq 6,7,8$ are $(2,3)$-groups is a theorem going back to G. A. Miller [14]. The fact that all the projective special linear groups $PSL(2,q)$ with $q \neq 9$ are $(2,3)$-groups is a theorem of Macbeath [12].

A $(2,3)$-group has a presentation $G = \langle s,t; s^2, t^3, R\rangle$ where R is the set of the other defining relations. The *group alphabet* is $\Sigma = \{s,t,t^{-1}\}$. Since every edge in the Cayley graph $\Gamma(G;\{s,t\})$ is labelled by s, t, or t^{-1}, we can describe paths in Γ by words over Σ. A *cyclic word* γ is the set of all cyclic permutations of a linear word and we can describe cycles by cyclic words. By a *subword* of a cyclic word we mean a linear reading of a string of consecutive letters of γ. Note that a cyclic word γ represents a Hamiltonian cycle in the graph $\Gamma(G)$ if and only if the length, $|\gamma|$, of γ is $|G|$ and γ has the property that for every nontrivial proper subword w of γ, the inequality $w \neq 1$ in G holds. We think of cycles as always starting at the identity element of G.

A cycle can, of course, be traversed in either direction. There is thus a natural equivalence relation on Hamiltonian cycles in a Cayley graph Γ. A cycle η is *equivalent* to a cycle γ if η equals γ or γ^{-1} as a cyclic word. Note that this equivalence relation holds between cycles with very different sets of edges. We can start at the identity element and read a Hamiltonian cycle by starting at any letter in either γ or γ^{-1}. The figure below shows two equivalent cycles in the standard presentation of the dihedral group

$$D_3 = \langle s,t; s^2, t^3,\ sts = t^{-1}\rangle$$

which is isomorphic to the symmetric group S_3 with generators $s = (12)$, $t = (123)$. The edges are oriented so that reading successive t-edges traverses the outer triangle clockwise and the inner triangle counterclockwise.

It is a curious fact about cubic graphs that if a cubic graph has a Hamiltonian cycle then it has at least two cycles whose edge sets are different. (See [15]). This is compatible with the fact that there is only one equivalence class of cycles in very small Cayley graphs. In the graph $\Gamma(D_3)$ below, the only equivalence class of Hamiltonian cycles is $(stt)^2$. The graph of the cyclic group C_6 with generators $s = (12)$ and

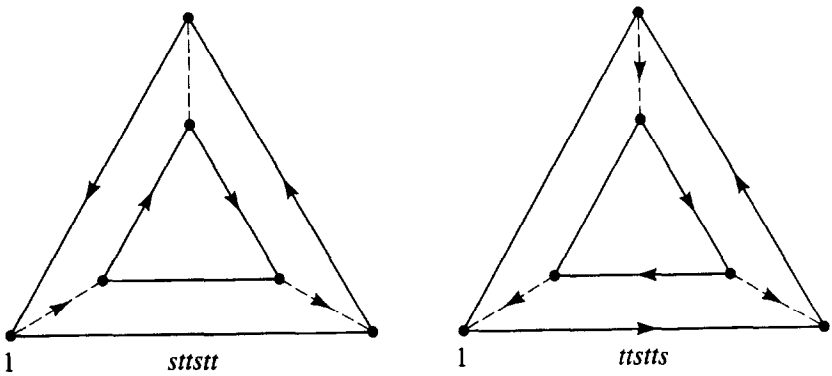

Fig. 3.

$t = (345)$ differs from $\Gamma(D_3)$ only in that the outer and inner-triangles are traversed in the same direction. The only cycle class is $(sttst^{-1}t^{-1})$.

We now start to consecutively number the examples with Roman numerals. Taking D_3 and C_6 as Examples I and II, respectively, we turn to

III. The group A_4 with generators

$$s = (12)(34) \quad \text{and} \quad t = (123)$$

has one cycle class $(sttst^{-1}t^{-1})^2$. In the illustration below the arrows indicate that one reads t in the direction of the arrow.

IV. See Fig. 4. The group $C_3 \times S_3$ of order 18 with generators

$$s = (12)(34)(56) \quad \text{and} \quad t = (135)$$

has cycle classes $(stt)^6$ and $(sttst^{-1}t^{-1})^3$.

After these examples the reader has probably noted a basic fact.

The Subword Lemma. *Let $\Gamma(G : \{s,t\})$ be the Cayley graph of a finite $(2,3)$-group. If γ is a Hamiltonian cycle in Γ then γ is a word $\gamma(stt, st^{-1}t^{-1})$ on the triples stt and $st^{-1}t^{-1}$.*

Proof. We think of the edges labelled by s as being red and the edges labelled by $t^{\pm 1}$ as being black. Since s has order 2 and t has order 3, $\langle s\rangle \cap \langle t\rangle = \{1\}$. The graph Γ thus consists of black triangles with the red edges joining different triangles. Let γ be a Hamiltonian cycle. Since γ cannot revisit any vertices, when γ enters a triangle along a red edge it must leave the triangle by a different red edge. The claim of the lemma is that every time γ enters a triangle along a red edge it must traverse two successive edges of the triangle.

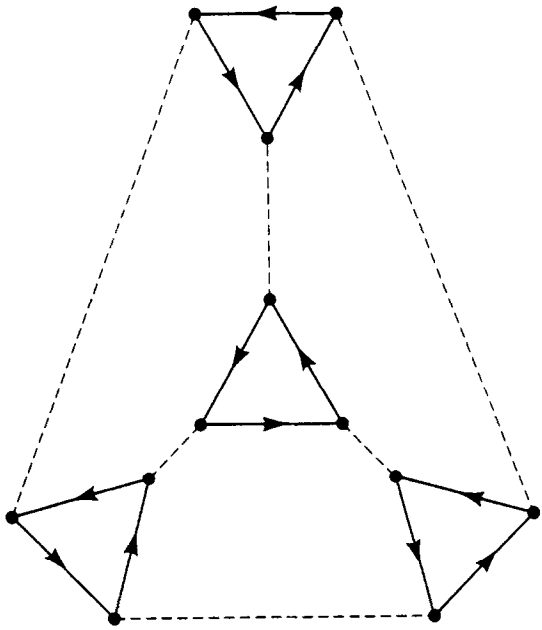

Fig. 4.

If γ traverses only a single black edge before leaving the given triangle Δ then it must revisit Δ later to pick up the remaining vertex. But the second visit must traverse a black edge and thus revisit a vertex already encountered. In short, the figure immediately below is impossible. □

See Fig. 5. The argument given above is, of course, very particular to (2, 3)-groups. From now on we denote stt by A and $st^{-1}t^{-1}$ by B and write all cycles as words on the letters A and B. Since I was searching for a counterexample, the original program stopped as soon as it found a Hamiltonian cycle and did not classify all cycles up to equivalence. Thus although it was, of course, necessary to debug the program on small examples, I did not pay much attention to the form of the cycles and I did not see that the subword lemma was true until after running the original program on A_5, which took twenty-four hours. (Times given for calculations are the amount of time taken until the program finished, not CPU times.) The current version which, of course, takes advantage of the subword lemma, takes three seconds on A_5.

We turn to the next sequence of examples.

V. The group S_4 with generators

$$s = (14) \quad \text{and} \quad t = (123)$$

has only the cycle class

$$(A^2B^2)^2.$$

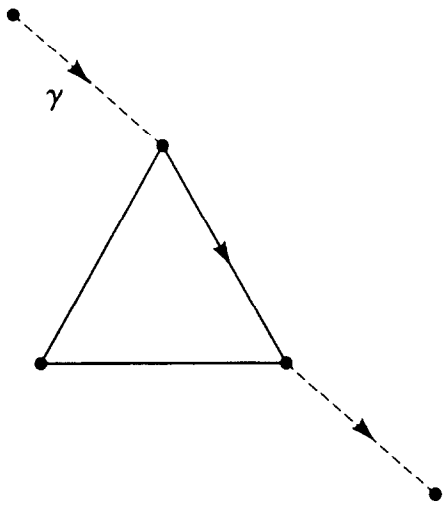

Fig. 5.

VI. The group of order 42 with generators

$$s = (24)(35)(67) \quad \text{and} \quad t = (123)(467)$$

has cycle classes

$$(AB)^7 \quad \text{and} \quad (A^2BA^4B^4AB^2).$$

VII. The group of order 54 with generators

$$s = (18)(27)(36)(45) \quad \text{and} \quad t = (126)(345)(789)$$

has cycle classes

$$(A^2BAB^2)^3,\ (BA^2B^2A)^3,\ (A^4B^2)^3.$$

VIII. The group A_5 of order 60 with generators

$$s = (12)(34) \quad \text{and} \quad t = (135)$$

has cycle classes

$$(A^3BABAB^3)^2 \quad \text{and} \quad (B^3ABABA^3)^2.$$

From even this small number of examples we start to see some remarkable structural properties emerge. We begin with a definition. A cyclic word γ is an *inverse palindrome* if γ equals γ^{-1} as a cyclic word. Since we are considering words on $A = stt$ and

$B = st^{-1}t^{-1}$ we can read γ^{-1} by reading γ from right to left and interchanging A's and B's. Although we try to write words which are inverse palindromes in a linear reading which verifies this fact, we stress that being an inverse palindrome is a cyclic property and that all linear readings must be checked to see if a word is indeed an inverse palindrome. What we notice from these examples is

The Inverse Palindrome Phenomenon: "Many" cycles in Cayley graphs of $(2,3)$-graphs are inverse palindromes.

It is always the case that the inverse of a Hamiltonian cycle is a Hamiltonian cycle, but why so many cycles should read the same in both directions seems a mystery. We can think of A and B as specifying the orientation in which a triangle is traversed. Being an inverse palindrome is an extremely strong "conservation of orientation" condition.

The second thing we notice is

The Proper Power Phenomenon: "Many" Hamiltonian cycles in the Cayley graphs of $(2,3)$-groups are proper powers.

All the cycles which we have seen so far are either inverse palindromes or proper powers and most are indeed proper powers of inverse palindromes. We shall investigate the persistence of these phenomena. Our first examples, D_3 with cycle class A^2 and C_6 with cycle class AB show that there is a certain tension between these two phenomena with certain groups "preferring" one to the other.

There is another algebraic particularity of the $(2,3)$-groups which we consider which is manifested in the form of cycles. Every $(2,3)$-group $G = \langle s,t;\ s^2,t^3,R\rangle$ which we consider has the *reflection automorphism* $\rho : G \to G$ defined by $s \mapsto s,\ t \mapsto t^{-1}$. Applying ρ interchanges A and B and we write $\overline{w}$ for $\rho(w)$, so, for example,

$$\overline{ABABA^2B^2} = BABAB^2A^2.$$

Using some combinatorial group theory it is easy to construct *infinite* quotients of the modular group in which $s \mapsto s,\ t \mapsto t^{-1}$ does not define an endomorphism. (If the map is an endomorphism it is clearly an automorphism since its square is the identity.) I do not know if there are any theorems about the size needed for a finite quotient not to have the reflection automorphism. In any case, all the groups which we discuss in this paper do have the reflection automorphism.

Since the algebraic meaning of a cyclic word γ being a Hamiltonian cycle is that $|\gamma| = |G|$ and no nontrivial proper subword of γ equals the identity in G, it follows that if γ is a Hamiltonian cycle then so is $\overline{\gamma}$. A geometric relationship between γ and $\overline{\gamma}$ does not, however, seem clear at all since they represent very different paths. We say that a cyclic word γ is *self-reflexive* if $\overline{\gamma}$ equals γ or γ^{-1}. It is clear that reflection preserves inverse palindromes. For example, the intriguing similarity between the two cycle classes

$$(A^3BABAB^3)^2 \quad \text{and} \quad (B^3ABABA^3)^2$$

of A_5 is that the second is the reflection of the first. We shall use reflection to cut down on the number of classes which we need to write out.

Before studying larger examples this is perhaps a good place to discuss how we found the permutation representations used and what the programs compute. The computer algebra systems CAYLEY and its successor MAGMA are amazing tools for doing computations with finite permutation groups. All permutation representations of groups larger than A_5 were found by using CAYLEY. The representations were found first by having CAYLEY calculate the action of $PSL(2,\mathbb{Z})$ on cosets of low index subgroups. The authority of any statements made about the algebraic structure of examples larger than A_5 is that "CAYLEY says so." But that the Cayley graph of the group generated by the given generators has the stated cycles does not at all depend on CAYLEY.

After seeing the subword lemma and the inverse palindrome and proper power phenomena I wrote a series of four programs which respectively search for all cycles, cycles which are k-th powers, cycles which are inverse palindromes and finally, only cycles which are k-th powers of inverse palindromes. These programs have *compression factors* respectively of $3, 3k, 6$ and $6k$. The *baselength* β for the calculation of one of these programs on a group G is the order of G divided by its compression factor. The parameter β seems a good rough measure of the time needed for a calculation. Calculations with $\beta \leqslant 25$ are quite feasible. For orders greater than 200, adding one to β roughly doubles the computation time required.

Programs work in three phases. Phase I simply calculates the Cayley graph, as an adjacency list of vertices and the s, t and t^{-1} neighbors of each given vertex. This is very fast. Phase II uses group symmetry to eliminate words that need to be considered. Call a word $w(A,B)$ *good* if it represents a simple path in the Cayley graph. Phase II generates good words out to some *initial length* entered for the calculation. Since the inverse of a cycle is a cycle, if a word generated is the inverse of a word already found it is eliminated. Generating only good words and eliminating inverses keeps the words generated by Phase II down to a reasonable number. For each initial word w generated by Phase II, Phase III calculates all possible (good) extensions of w out to the length baselength. Depending on the program, either the extensions of length baselength, or their k-th powers, or their " doubles" to inverse palindromes or the k-th power of their doubles are checked to see whether or not they are Hamiltonian cycles. The programs which use inverse palindromes will not generate all possible inverse palindromes since Phase II eliminates inverses and Phase III generates only linear extensions of words from Phase II. However, closing under reflection seems to find all the cycles which are inverse palindromes at least for the orders where we can do the computation. Successive programs were debugged on small examples and then checked against the previous programs on larger examples. I later completely rewrote the programs and repeated the whole procedure and checked the results of the second versions against the results of the first versions. The second versions are quite different in the way they use the Cayley graph as a data-structure and I am confident that the results given by the programs are correct.

We return to our examples.

IX. The group $C_3 \times S_4$ of order 72 with generators

$$s = (12)(34)(56) \quad \text{and} \quad t = (125)(347)$$

has only the cycle class

$$(AB^4ABA^4B)^2.$$

X. The solvable group of order 96 with generators

$$s = (34)(57)(68)(9\ 10),\ t = (123)(456)(789)(10\ 11\ 12)$$

has cycle classes
1. $(B^2A^4B^2A^2B^4A^2)^2$,
2. $(A^4B^4)^4$,
3. (A^2BABAB^2),
4. (B^2ABABA^2).

The next example is the first group where we encounter several classes of cycles. We now adopt the following format for tables of cycle classes. At the left we write the number of the class γ. At the right there is a check if the cycle is an inverse palindrome and a ρ if the cycle is self-reflexive. Cycle class 5 is the first cycle we see which is neither an inverse palindrome nor a proper power. Note that the number of A's is very close to the number of B's. It seems that "overloading" one letter in favor of the other, as in $(A^4BA^2B)^5$, occurs only in proper powers. Many classes are still proper powers of inverse palindromes.

XI. The group $C_2 \times A_5$ of order 120 with generators

$$s = (12)(35)(46)(79)(810) \quad \text{and} \quad t = (234)(678)$$

has cycle classes
1. $(A^8BA^2(BA)^3AB^3)^2$
2. $A^2BA^6BA^2BA^4B^2ABA^2B^4AB^2AB^6AB^2$ $(\surd)$
3. $(A^4BA^2B)^5$ (ρ)
4. $(A^4B^4A^2B^2A^4B^4)^2$ $(\surd)$
5. $A^4B^2ABA^3B^3(AB)^2A^3B^2A^3(BA)^2B^3A^3BAB^2$
6. $(A^4B^4)^5$ $(\surd, \rho)$
7. $(A^3BAB^3)^5$ $(\surd)$
8. $(A^2BAB^2A^2B^2ABA^2BAB^2AB)^2$
9. $(AB^2ABA^2B)^5$ $(\surd, \rho)$

plus the reflections of cycles 1, 2, 4 and 7 for a total of 13 cycle classes.

We now turn our attention to linear groups. As a general reference see Alperin and Bell [1]. If F is any field the *projective special linear group*, $PSL(n,F)$, is the group

$SL(n,F)$ modulo the subgroup $\{\lambda I\}$ where $\lambda^n = 1$ in F. A major source of simple groups is the well-known

Theorem. *If $n \geqslant 2$ then $PSL(n,F)$ is simple except when $n = 2$ and $|F|$ is 2 or 3.*

If q is a prime power then $PSL(n,q)$ denotes the group $PSL(n,\mathbb{F}_q)$ where $\mathbb{F}_q$ is the finite field with q elements. There is a very handy formula giving the orders of the groups $PSL(2,q)$.

Theorem.

$$|PSL(2,q)| = \begin{cases} q(q^2-1) & \text{if } 2|q, \\ q\dfrac{(q^2-1)}{2} & \text{if } 2\nmid q. \end{cases}$$

A major ingredient in the proof of simplicity is the fact that $SL(n,F)$ is generated by *transvections*, that is, matrices like $\left(\begin{smallmatrix} 1 & \alpha \\ 0 & 1 \end{smallmatrix}\right)$ which differ from the identity matrix only in a single entry which is not on the main diagonal. It follows that the map $\pi : PSL(2,\mathbb{Z}) \to PSL(2,p)$ defined by reducing entries modulo the prime p is a homomorphism onto $PSL(2,p)$. We can thus make a canonical choice of generators in the matrix groups $PSL(2,p)$ by always taking $s = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 1 \end{smallmatrix}\right)$ and $t = \left(\begin{smallmatrix} 0 & 1 \\ 1 & -1 \end{smallmatrix}\right)$. Note that in the group $PGL(2,p)$ conjugation by the matrix $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ sends s to s and t to t^{-1}. Thus all the groups $PSL(2,p)$ admit the reflection automorphism ρ with our choice of generators.

It is well-known that $PSL(2,2) \simeq S_3$, $PSL(2,3) \simeq A_4$, $PSL(2,5) \simeq A_5$ and $PSL(2,9) \simeq A_6$. As remarked earlier, A_6 is *not* a $(2,3)$-group. The only two noncyclic finite simple groups with order less than 200 are A_5 and $PSL(2,7)$ which has order 168. $PSL(2,7)$ also has a permutation representation with generators

$$s = (12)(34) \quad \text{and} \quad t = (135)(267).$$

This is the largest group for which I have calculated all the cycle classes since the computation took about forty hours. There are thirty classes, eight classes of which are neither proper powers nor inverse palindromes. These classes still have the property that the number of A's is very close to the number of B's. The four classes which are proper powers are

XII. The cycles of $PSL(2,7)$ which are proper powers.

1. $(A^3BAB^2A^2BAB^3)^4$ $(\surd)$
2. $(A^2B^2ABA^2BAB^2(AB)^2A^2BAB^2ABA^2B^2)^2$ $(\surd)$

and their reflections.

For larger groups we can check only cycles which are proper powers. The groups which we consider are all groups of the form $PSL(2,q)$ except for the following group which is a solvable group built up by successive extensions by C_2 or C_3.

XIII. The solvable group G of order 324 with generators

$$s = (15)(38) \text{ and } t = (123)(456)(789)$$

has cycle classes

1. $(A^3B^2A^3B^2AB^2ABAB^2A^2BABA^2BA^2B^3A^2B^3)^3$ (√)
2. $(A^3B^3A^2BAB^2A^3B^3)^6$ (√)
3. $(A^3BA^2BAB^2AB)^9$

and their reflections.

This example is interesting in that it is the only example we have found in which the cycles of the highest power which occurs do not contain a cycle which is a power of an inverse palindrome. All cycles which are 6th powers or 9th powers are listed but we checked only third powers of inverse palindromes so there may be other cycles which are 3rd powers. Looking for cycles which are not proper powers is not feasible.

XIV. The group $PSL(2,8)$ has order 504 and has a permutation representation with generators

$$s = (24)(35)(68)(79) \text{ and } t = (123)(467)(589).$$

The Cayley graph has the following cycles which are 7th powers.

1. $(A^7(BA^2)^2BA^4BAB^2AB)^7$
2. $(A^7(BA^2)^2B^5AB^3AB)^7$
3. $(A^7BA^2BABA^5BAB^2AB)^7$
4. $(A^7BA^2(BA)^2B^4AB^3AB)^7$
5. $(A^4BA(BA^2)^2(B^2A)^2BAB^4)^7$ (√)
6. $(A^4BABA^2(BA)^3B^2ABAB^4)$ (√)
7. $(A^4B^2AB^2ABAB^2AB^3A^3B^3)^7$
8. $((AB^2)^2A^3B^2ABA^2B^3(A^2B)^2)^7$ (√)

and their reflections for a total of 16 classes of cycles which are 7th powers.

XV. $PSL(2,11)$ of order 660 has the following classes of cycles which are 5th powers of inverse palindromes.

1. $(A^5B^3A^3BA^3B^2AB^4A^4BA^2B^3AB^3A^3B^5)^5$
2. $(A^5B^3A^2B(AB^2)^2A^2B^3A^3B^2(A^2B)^2AB^2A^3B^5)^5$
3. $(A^4BA^2B^3AB^3A^3B^4ABA^4B^3A^3BA^3B^2AB^4)^5$

and their reflections.

XVI. The group $PSL(2,13)$ has order 1092. Searching for Hamiltonian cycles in a cubic graph of this size would certainly be impossible without using our structural information. The Cayley graph has no cycles which are 13th powers. A search for Hamiltonian cycles which are 7th powers of inverse palindromes reveals the following list (plus their reflections).

1. $(A^7BA^2BA^3B^3A^4(BA)^5B^4A^3B^3AB^2AB^7)^7$
2. $(A^4BA^4B^3A^4B^2(AB)^2A^3BAB^3(AB)^2A^2B^4A^3B^4AB^4)^7$
3. $(A^4B^2A^3B^4AB^2A^5BA^3BAB^3AB^5A^2BA^4B^3A^2B^4)^7$
4. $(A^3B^2AB(AB^2)^2A^7B^3A^2BAB^2A^3B^7(A^2B)^2ABA^2B^3)^7$

5. $(A^3B^3A^3B^2ABA^3B^5AB^3ABA^3BA^5B^3ABA^2B^3A^3B^3)^7$
6. $(A^3B^3A^3B^3AB^2A^6B^4ABA^4B^6A^2BA^3B^3A^3B^3)^7$
7. $(A^2BA^5BABA^2BA^3BA^2B^3(AB)^3A^3B^2AB^3AB^2ABAB^5AB^2)^7$
8. $(A^2BA^5B^2(AB)^2A^4B^2AB^2(AB)^3A^2BA^2BA^2B^4(AB)^2A^2B^5AB^2)^7$
9. $(A^2BA^5B^3A^3B^4AB^2A^2(BA)^3B^2A^2BA^4B^3A^3B^5AB^2)^7$
10. $(A^2BA^4B^2ABAB^6A^2B^3(AB)^3A^3B^2A^6BABA^2B^4AB^2)^7$

A very interesting question is "What determines which powers occur in cycles?" It may not have escaped the reader that there is a fascinating "numerology" which predicts the highest possible power in the case of the simple groups $PSL(2,p)$.

$$|PSL(2,5)| = 60 = 6.2.5, \quad |PSL(2,7)| = 168 = 6 \cdot 2^2 \cdot 7,$$
$$|PSL(2,11)| = 660 = 6.2.5.11, \quad |PSL(2,13)| = 1092 = 6 \cdot 2 \cdot 7 \cdot 13.$$

We then have the following "rule" for predicting the highest power which occurs as a Hamiltonian cycle in the corresponding Cayley graph.

Power Prediction. *Write the order n of a simple group $PSL(2,p)$ as $n = 6m$. Consider the prime power factorization of m and take the power of the second largest prime which occurs.*

This procedure gives the correct values: 2, 4, 5, 7; for the four examples which we are able to compute. If this "rule" is not an accident then the numbers must be connected with geometries associated to the groups and is thus an important clue as to why there really are cycles. The next test group, $PSL(2,17)$ has order $2448 = 6.2^3.3.17$. Not only has the order increased by a factor of almost two and a half but the predicted power has decreased by the same factor. The baselength parameter β is now 136 and calculation seems totally out of even supercomputer reach. It still is possible to search for cycles which are 17th powers of inverse palindromes in the Cayley graph of $PSL(2,17)$ and, as expected, the search did not find any cycles. It thus seems unlikely that there are any Hamiltonian cycles which are 17th powers.

On the basis of our empirical results one is led to conjecture at least that if G is a noncyclic $(2,3)$-group then the Cayley graph $\Gamma(G : \{s,t\})$ contains a Hamiltonian cycle which is a proper power of an inverse palindrome. Why this should be the case is still a total mystery to the author.

There is another property which seems to be unique to the $(2,3)$-case, namely, the rate of growth of the number of cycle classes as the order of the group increases. The reader has probably noticed that the number of classes which we find is really quite small, only 30 in the complete listing of cycles for $PSL(2,7)$. In general, the number of Hamiltonian cycles might well grow exponentially with the order of the group and this is what we seem to see when we move to other 2-generator groups. Let us consider $(2,4)$-groups with distinguished generators s of order 2 and x of order 4.

XVII. As a $(2,4)$-group S_4 has generators

$$s = (14) \quad \text{and} \quad x = (1234).$$

The cycle classes are

1. $((sx)^2)sx^{-1}sx(sx^{-1})^2)^2$,
2. $((sx)^2sx^{-1}(sx^3sx)^2sx^3sx^{-1})$,
3. $((sx)^2(sx^{-1})^2)^3$,
4. $(sx^3sx^{-3})^3$.

Recall that we are using words in the generators to describe paths so that sx^{-1} and sx^3 are quite different paths. In this particular example the majority of paths are words on $C = sv$ and $D = sv^{-1}$. For successive computations we restrict ourselves *only* to cycles which are words on C and D. We find that even with this restriction the number of cycles grows very quickly with the order of the group.

XVIII. The group of order 48 with generators

$$s = (35)(46) \quad \text{and} \quad x = (1243)(5687)$$

has 26 classes of cycles of which 8 are squares.

XIX. The group of order 64 with generators

$$s = (23)(67) \quad \text{and} \quad x = (12)(3465)(78)$$

has 136 classes of cycles of which 16 classes are squares.

XX. The group of order 72 with generators

$$s = (23) \quad \text{and} \quad x = (12)(3465)$$

has 333 classes of cycles of which 18 are squares. There are no cubes.

Even though we are restricting our attention to cycles of a special form we see a growth rate which is quite different from the case of $(2,3)$-groups.

If we consider an example where the first generator has order greater than two we seem to have even more cycles than in the $(2,4)$-case.

XXI. As a $(3,4)$-group S_4 has generators

$$x = (234) \quad \text{and} \quad u = (1243).$$

There are already 268 different classes of Hamiltonian cycles in the Cayley graph $\Gamma(S_4 : \{x,u\})$.

I take the empirical results described in this article as being a fair amount of evidence for the general conjecture on the existence of Hamiltonian cycles in Cayley graphs. There seem to be fewer cycles in $(2,3)$-groups than in the cases where the generators have bigger orders and finding cycles in the simple group $PSL(2,13)$ of order 1092, indeed at the predicted power, seems to indicate that it is unlikely that one can find a counterexample among $(2,3)$-groups. On the other hand, I still do not really have any better insight into why cycles *should* exist. A sequel to this paper will investigate

the structure of Hamiltonian cycles in graphs of two-generator groups other than the $(2,3)$-case. The proper power phenomenon persists in all the examples which I have been able to compute. It seems to be the case that if G is *any* noncyclic finite two-generator group with generators x and u then $\Gamma(G : \{x,u\})$ has a Hamiltonian cycle which is a proper power.

Acknowledgements

I would first of all like to thank the NSF SCREMS Grant DMS-9505897 for the Sparc 20 workstation in my office without which the computation would certainly not have been done. I would also like to thank my colleagues Nigel Boston, John Gray, Derek Robinson and Joseph Rotman at the University of Illinois and Phillipe Narbel, André Raspaud and Gérard Senizergues at the University of Bordeaux for many helpful and encouraging discussions during this period of computational obsession. I am particularly grateful to Nigel Boston for his patience in showing me how to use the computer algebra system CAYLEY and its successor MAGMA.

References

[1] J.L. Alperin, R.B. Bell, Groups and Representations, Springer, Berlin, 1995.
[2] B. Alspach, C.D. Godsil (Eds.), Cycles in Graphs, Ann. Discrete Math. 27 (1985), 463.
[3] A. Cayley, On the theory of groups Proc. London Math. Soc. 9 (1878) 126–133.
[4] J.H. Conway, N.J.A. Sloane, A.R. Wilks, Gray codes for reflection groups, Graphs Combin. 5 (1989) 315–325.
[5] S.J. Curran, J.A. Gallian, Hamiltonian cycles and paths in Cayley graphs and digraphs – a survey, Discrete Math. 156 (1996) 1–18.
[6] H.H. Glover, T.Y. Yang, A Hamiltonian cycle in the Cayley graph of the $\langle 2,p,3\rangle$ presentation of PSL$(2,p)$, Discrete Math. 160 (1996) 149–163.
[7] J.E. Hopcroft, J.D. Ullman, Introduction to Automata Theory, Languages and Computation, Addison-Wesley, Reading, MA, 1979.
[8] D. Jungreis, E. Freidman, D. Witte, Cayley graphs of groups of low order are Hamiltonian, preprint.
[9] K. Keating, D. Witte, On Hamiltonian cycles in Cayley graphs with cyclic commutator subgroup, in: B.R. Alspach, C.D. Godsil (Eds.), Cycles in Graphs, Ann. Discrete Math. 27 (1985) 89–102.
[10] M.W. Liebeck, A. Shalev, Classical groups, probabilistic methods and the $(2,3)$-generation problem, Ann. Math. 144 (1996) 77–125.
[11] L. Lovász, Problem 11, in: Combinatorial Structures and their Applications, R. Guy, H. Hanani, N. Sauer, J. Schoneheim, (Eds.), Gordan and Breach, London, 1970 p. 197.
[12] A.M. Macbeath, Generators of the linear fractional groups, Proc. Symp. Pure Math. 12 (1967) 14–32.
[13] W. Magnus, Karrass, Solitar, Combinatorial Group Theory, Wiley Interscience, New York, 1966.
[14] G.A. Miller, On the groups generated by two operators, Bull Amer. Math. Soc. 7 (1901) 424–426.
[15] C.H. Papadimtriou, Computational Complexity, Addison-Wesley, Reading, MA, 1994.
[16] R.A. Rankin, A campanological problem in group theory, Proc. Cambridge Phil. Soc. 44 (1948) 17–25.
[17] D.B. West, Introduction to Graph Theory, Prentice–Hall, Englewood Cliffs, NJ, 1996.
[18] D. Witte, Cayley digraphs of prime-power order are Hamiltonian, J. Combin. Theory B 40 (1986) 107–112.