To Peter Hilton, friend and colleague, on his 70^{th} birthday.

ON GROUPS GENERATED BY THREE INVOLUTIONS, TWO OF WHICH COMMUTE

BY MICHAEL CHERKASSOFF AND DENIS SJERVE

ABSTRACT. We completely determine those alternating groups A_n, symmetric groups S_n, and projective groups $PSL_2(q)$ and $PGL_2(q)$, which can be generated by three involutions, two of which commute.

1. INTRODUCTION

In this paper we investigate the possibility of generating certain finite groups G by three involutions, two of which commute. That is, when does G have a presentation of the form

(1) $G \cong \langle R_1, R_2, R_3 | R_1^2 = R_2^2 = R_3^2 = 1, R_1R_2 = R_2R_1 \text{ , ETC } \rangle$?

Here ETC denotes the extra relations needed to present the finite group. To avoid trivial cases we assume throughout this paper that the R_j, as elements of G, are not the identity and are mutually distinct.

Remarks

1. In the trivial cases the groups we obtain are trivial, $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ or dihedral D_{2k}, where k is order of the product of two non-commuting involutions. Note that in particular, when $k = 3$ we get the symmetric group S_3.
2. Without any extra relations the group presented in (1) is the free product $(\mathbb{Z}_2 \oplus \mathbb{Z}_2) * \mathbb{Z}_2$, hence infinite.

We will answer this question for the alternating groups A_n, the symmetric groups S_n, the projective special linear groups $PSL_2(q)$ over finite fields $GF(q)$, and the projective general linear groups $PGL_2(q)$ over $GF(q)$, where $q = p^n$ and p is any prime. Our results are given in the following four theorems.

Theorem 1.1. *The alternating group A_n has a presentation as in* (1) *if, and only if, $n = 5$ or $n \geq 9$.*

Theorem 1.2. *The symmetric group S_n has a presentation as in* (1) *if, and only if, $n \geq 4$.*

Mathematics Department, University of British Columbia, Vancouver, BC, Canada, V6T 1Z2.
E-mail:mikec@math.ubc.ca, sjer@math.ubc.ca.

Theorem 1.3. *The projective special linear group $PSL_2(q)$ has a presentation as in* (1) *if, and only if, $q \neq 2, 3, 7, 9$.*

Theorem 1.4. *The projective general linear group $PGL_2(q)$ has a presentation as in* (1) *if, and only if, $q \neq 2$.*

The motivation for this paper arose in combinatorics, more specifically, in the area of hamiltonian cycles. A conjecture in graph theory, arising from a question of Lovász[7], is that every vertex transitive graph, with just 4 exceptions, has a hamiltonian path. In particular we can consider this conjecture for Cayley graphs associated to finite presentations of finite groups. It turns out that the above presentation on three involutions is very amenable to this conjecture. As far as Cayley graphs are concerned a reasonable conjecture is

CONJECTURE: For any finite presentation of any finite group G (with the trivial exception of $\mathbb{Z}_2$) there is a Hamiltonian cycle in the associated Cayley graph.

The paper [10] by Witte and Gallian contains an excellent survey on this subject.

In Section 2 of this paper we collect the preliminaries and background material we need. Section 3 contains the proofs of Theorems 1.1 and 1.2 and Section 4 contains the proofs of Theorems 1.3 and 1.4. And finally in Section 5 we prove results on the existence of Hamiltonian cycles.

2. PRELIMINARIES

First we give some definitions.

Definition 2.1. The **Projective General Linear Group** over the finite field of $q = p^n$ elements, $PGL_2(q)$, is the quotient group of the group of invertible 2×2 matrices, with entries in the finite field of q elements, by its center.

Definition 2.2. The **Projective Special Linear Group** over the finite field of $q = p^n$ elements, $PSL_2(q)$, is the quotient group of the group of 2×2 matrices of determinant 1, with entries in the finite field of q elements, by its center.

Definition 2.3. Let the group G be generated by distinct elements $g_1, g_2, \ldots, g_n$ all different from the identity. Then **the Cayley graph** for G with this set of generators is the graph with vertices corresponding to the group elements and with vertices s and t connected by an edge if and only if there is i, such that $s = tg_i$.

In the case when g_i is an involution it is customary to consider the graph as having only one edge between s and t.

Definition 2.4. A **Hamiltonian path** in a graph is an edge-path which visits each vertex exactly once.

Definition 2.5. A **Hamiltonian cycle** is a Hamiltonian path having the same vertex as its beginning and end.

Definition 2.6. The **Triangle Group** $T(r,s,t)$ is the group with the presentation

$$\langle x_1, x_2, x_3 | x_1^r = x_2^s = x_3^t = x_1x_2x_3 = 1\rangle$$

It is known that a triangle group is finite if and only if $1/r + 1/s + 1/t > 1$.

The triangle groups are closely related to the geometry of Riemann surfaces. To see this consider the triangle, whose angles are $\pi/r, \pi/s$ and π/t. This triangle is on the sphere if $\frac{1}{r}+\frac{1}{s}+\frac{1}{t} > 1$, the Euclidean plane if $\frac{1}{r}+\frac{1}{s}+\frac{1}{t} = 1$, and the upper half plane in all other cases.

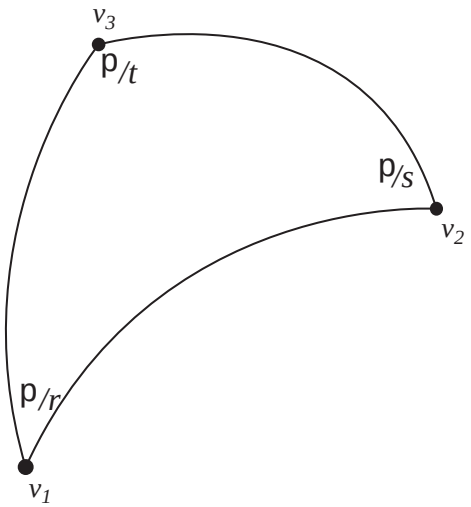


FIGURE 1. Fundamental triangle.

Letting x_1, x_2, x_3 be rotations by $\frac{2\pi}{r}, \frac{2\pi}{s}, \frac{2\pi}{t}$ about the respective vertices, we see that the group generated by x_1, x_2, x_3 is isomorphic to $T(r,s,t)$. It is a group of symmetries of the tesselation produced by repeated reflections of the triangle in free sides.

Secondly, we need some group-theoretic results. The most important result for us is the Dickson classification of subgroups of $PSL_2(q)$ [4, 6, 9].

Theorem 2.7. *The subgroups of $PSL_2(q)$ fall into three types:*

I *(The Projective Subgroups). If $m|n$ then $GF(p^m)$ is a subfield of $GF(q)$ and therefore $PSL_2(p^m)$ is a subgroup of $PSL_2(q)$. If also $2m|n$ and $p > 2$ then $PGL_2(p^m)$ is a subgroup of $PSL_2(q)$. Any subgroup isomorphic to either $PSL_2(p^m)$ or $PGL_2(p^m)$ is called a projective subgroup.*

II *(The Affine Subgroups). Consider the subgroups of $PSL_2(p^{2n})$ which have one of the following forms:*

$$either \left\{ \begin{bmatrix} a & b \\ 0 & a^{-1} \end{bmatrix} : a, b \in GF(q), a \neq 0 \right\},$$

$$or\left\{\begin{bmatrix} \lambda & 0 \\ 0 & \overline{\lambda} \end{bmatrix} : \lambda \in GF(p^{2n})^*, \lambda^{q+1} = 1\right\},$$

where $\lambda \mapsto \overline{\lambda} = \lambda^q$ *is the involution in the field* $GF(p^{2n})$. *Then any subgroup of* $PSL_2(q)$ *isomorphic to a subgroup of one of the above is called an affine subgroup.*

III *(The Exceptional Subgroups). The finite non-cyclic triangle groups are:*
$T(2,2,t)$ = *the dihedral group of order* $2t, t \geq 2$;
$T(2,3,3)$ = *the tetrahedral group* $\cong A_4$;
$T(2,3,4)$ = *the octahedral group* $\cong S_4$;
$T(2,3,5)$ = *the icosahedral group* $\cong A_5$.
Subgroups of $PSL_2(q)$ *isomorphic to one of these are called exceptional groups* ■

We also need a result, due to Dyck, on representations of $PSL_2(q)$ as permutation groups [1, 4]

Theorem 2.8. $PSL_2(q)$ *may be represented as a transitive permutation group on* $q+1$ *symbols but on no fewer, except when* $q = 5, 7, 9, 11$, *for which the minimum number of symbols is* $5, 7, 6, 11$ *respectively* ■

The next two lemmas are obvious and useful in investigating the generation of groups:

Lemma 2.9. *Suppose some permutations* $t_1, .., t_l$, *on the set of symbols* $\{i_1, .., i_k\}$, *generate a subgroup isomorphic to* A_k. *Let* $t=(i_p, i_q, j)$ *be a 3-cycle, where* i_p, i_q *are from this set and* j *is not. Then the permutations* $t_1, .., t_l, t$, *on the set of symbols* $\{i_1, .., i_k, j\}$, *generate a subgroup isomorphic to* A_{k+1} ■

Lemma 2.10. *Suppose we have three involutions, two of which commute, and the third does not commute with them or their product. Then the group these involutions generate is not dihedral* ■

We also need to point out some isomorphisms:

Proposition 2.11. $PSL_2(2) = PGL_2(2) \cong S_3$, $PSL_2(3) \cong A_4$, $PGL_2(3) \cong S_4$, $PSL_2(5) \cong A_5$, $PGL_2(5) \cong S_5$ *and* $PSL_2(9) \cong A_6$ ■

The Cayley graph is a 1-dimensional simplicial complex constructed from the vertex set G by right multiplication by the generators $g_1, \ldots, g_n$. The group G acts on itself by left multiplication, and we can extend this action to the Cayley graph by making it linear on the edges. Thus the Cayley graph has a natural left G-action. We now want to add 2-cells to the Cayley graph to obtain a surface, and then extend the G-action to the surface. We limit our attention to trivalent Cayley graphs, that is graphs such that each vertex has exactly 3 edges coming into it.

A Cayley graph that is trivalent must come from a presentation in one of two ways: either the group is presented by 3 involutions, or it is generated by an involution and one other

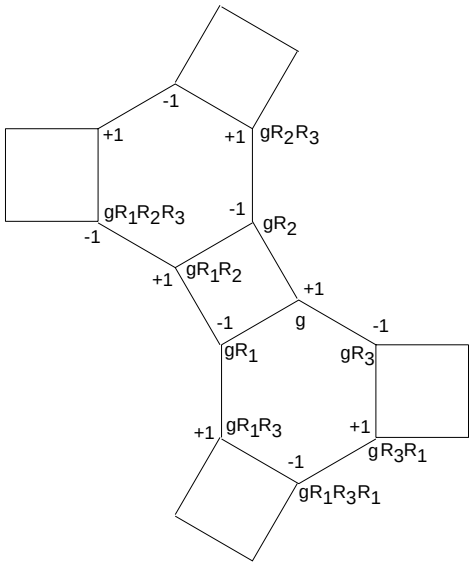
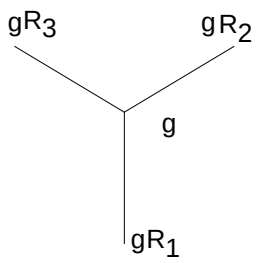


FIGURE 2. The Cayley graph with local orientation.



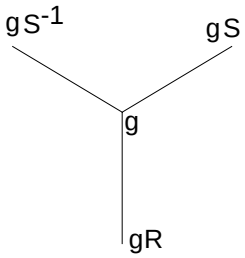


FIGURE 3. $R_1^2 = R_2^2 = R_3^2 = 1$ $\qquad$ $R^2 = 1, S \neq S^{-1}$

element of order bigger than two (see fig. 3); therefore having a presentation of one of the following forms:

$$(a)\ G = \langle R_1, R_2, R_3 | R_1^2 = R_2^2 = R_3^2 = 1, ETC. \rangle$$
$$(b)\ G = \langle R, S | R^2 = S^n = 1, ETC. \rangle, \text{where } n > 2.$$

As far as the first case is concerned let the orders of R_1R_2, R_2R_3 and R_3R_1 be r, s, t respectively. Then we attach three 2-cells to the cycles

$$g, gR_1, gR_1R_2, \ldots, g(R_1R_2)^{r-1}R_1,$$
$$g, gR_2, gR_2R_3, \ldots, g(R_2R_3)^{s-1}R_2,$$
$$g, gR_3, gR_3R_1, \ldots, g(R_3R_1)^{t-1}R_3.$$

Thus the 2-cells attached are $2r$-gons,$2s$-gons and $2t$-gons respectively.

In the second case the relevant cycles are:

$$g, gR, gRS, \dots ,$$
$$g, gR, gRS^{-1}, \dots ,$$
$$g, gS, gS^2, \dots ,$$

and the 2-cells are $2r$-gons, $2r$-gons and s-gons, where r=the order of RS=the order of RS^{-1} and s=the order of S. Thus trivalent Cayley graphs can be completed to surfaces, and the left G-action on the Cayley graph can be extended linearly to the cells. In these cases we refer to the surface as the Cayley surface.

In this paper we are only dealing with case (a). For the presentation of $PSL_2(q)$ as in (b) see [5, 6]. The existence of hamiltonian cycles in case (b) is still open in most of the cases; however, Tzu-Yi Yang[11] has proved that the Cayley graph of the presentation of $PSL_2(p)$ on the generators

$$R = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, S = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

does have hamiltonian cycles.

The Cayley surface of the group G, presented as in (1), is composed of $\frac{|G|}{4}$ 4-gons, $\frac{|G|}{2s}$ $2s$-gons and $\frac{|G|}{2t}$ $2t$-gons where s=the order of R_2R_3 and t= the order of R_3R_1.

It is worth noting which of the Cayley surfaces are non-orientable.

Lemma 2.12. *If a finite group is generated by three involutions, two of which commute, then the Cayley surface of this group is orientable if and only if there is no product of an odd number of generators equal to 1.*

Proof. First we note that the graph is locally planar, so locally we can select an orientation around each vertex. We choose the orientation that crosses the edges R_1, R_2, R_3 in that order. Next note that adjacent edges have opposite orientation (see fig.2).

A word W in the R_j can be represented by a path along the edges of the Cayley graph. This path is a loop, if and only if, $W = 1$ in G. If this word W has odd length in the R_j, then going once around a loop representing W reverses the local orientation, and so the Cayley surface is non-orientable.

Conversely, if the Cayley surface is non-orientable, then there are loops which reverse the orientation. Any such loop can be homotoped to an edge path, which must therefore correspond to a word W in the R_j which has odd length and represents 1 in the group □

Theorem 2.13. *All Cayley surfaces arising from presentation (1) of simple groups are non-orientable.*

Proof. According to lemma 2.12 we have to find a product of an odd number of generators which is equal to 1. Consider the diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & T(2,s,t) & \longrightarrow & \Gamma & \longrightarrow & \mathbb{Z}_2 & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & G' & \longrightarrow & G & \longrightarrow & G/G' & \longrightarrow & 1 \end{array}$$

where $T(2,s,t)$ is the triangle group, Γ is the group generated by reflections through the sides of the triangle with the angles $\pi/2, \pi/s$ and π/t, G is the group generated by three involutions, two of which commute and G' is the subgroup generated by their pairwise products. Then the downarrows are epimorphisms and since $T(2,s,t)$ has index 2 in Γ G' has index 1 or 2 in G. But if G is simple, index 2 can not happen, so $G' = G$. Therefore pairwise products generate the whole group and in particular R_1 can be written as a product of R_1R_2's, R_1R_3's and R_2R_3's. Multiplying both sides by R_1 we obtain a product of an odd number of generators equal to 1. Hence the surface is non-orientable □

3. PERMUTATION GROUPS

In this section we shall prove Theorems 1.1 and 1.2. The proof of Theorem 1.1 has two components. First we show that A_n has a presentation as in (1) if either $n = 5$ or $n \geq 9$, and then we show that the remaining A_n do not have such a presentation (the negative half).

First we want to develop some notation. The symbols R_1, R_2, R_3 will always denote involutions. They will always be chosen so that the R_j are distinct, all are different from the identity, and so that R_1R_2=R_2R_1. The symbols c_i will always denote 3-cycles. All permutations are written in cycle notation.

For technical reasons we deal with the case $n = 5$ separately. In this case it is easy to see, that by choosing:

$$R_1 = (1,2)(3,4),\ R_2 = (1,3)(2,4),\ R_3 = (1,2)(4,5).$$

we generate all of A_5. Indeed let

$$c_1 = R_1R_3 = (3,5,4),\ c_3 = R_2c_1R_2 = (1,5,2),\ c_2 = c_3^2c_1c_3 = (2,4,3),$$

then c_1, c_2, c_3 are clearly generators of A_5. To prove the rest of the positive half of Theorem 1.1 we show that it holds for n = 9,10,11,12,13,14,15, 16 and then we show that it holds for A_{n+8} if it is true for A_n.

Before giving the proof of the inductive step we establish the base case of the induction. In all cases we define three involutions $R_1,\ R_2,\ R_3$ and exhibit an appropriate power $(R_1R_3)^m$ which is a 3-cycle c_1. Then we find another 3-cycle $c_2 = (i_p, i_q, j)$, where $i_p,\ i_q$ are involved in c_1 but j is not. The 3-cycle c_1 generates the group A_3 and adjoining c_2 then gives A_4, according to lemma 2.9. The idea is to then find a succession of 3-cycles $c_3,\ c_4, \ldots$, adjoin them to the previous generators to produce a succession of groups isomorphic to $A_5,\ A_6, \ldots$. These extra 3-cycles are obtained from the previous ones by conjugation. Table 1 contains some of the details.

n	Involutions	Cycles	A_k on
9	$R_1 = (1,2)(3,4)(5,6)(7,8)$ $R_2 = (1,3)(2,4)(5,7)(6,8)$ $R_3 = (4,5)(8,9)$	$c_1 = (R_1R_3)^4 = (7,9,8)$ $c_2 = (R_2c_1^2R_2)c_1(R_2c_1R_2)$ $c_3 = R_2c_1R_2$ $c_4 = R_3(5,6,7)R_3$ $c_5 = R_1(4,5,6)R_1$ $c_6 = R_2(4,5,6)R_2$ $c_7 = R_1(2,3,4)R_1$	$\{7,8,9\}$ $\{6,7,8,9\}$ $\{5,\ldots,9\}$ $\{4,\ldots,9\}$ $\{3,\ldots,9\}$ $\{2,\ldots,9\}$ $G = A_9$
10	$R_1 = (1,2)(3,4)(5,6)(9,10)$ $R_2 = (1,3)(2,4)(5,6)(7,8)$ $R_3 = (1,2)(4,5)(6,7)(8,9)$	$c_1 = (R_1R_3)^5 = (8,10,9)$ $c_2 = R_2c_1R_2$ $c_3 = R_3(7,8,9)R_3$ $\ldots$	$\{8,9,10\}$ $\{7,8,9,10\}$ $\{6,\ldots,10\}$
11	$R_1 = (1,2)(3,4)(5,6)(7,8)$ $R_2 = (1,3)(2,4)(5,6)(9,10)$ $R_3 = (1,11)(4,5)(6,7)(8,9)$	$c_1 = (R_1R_3)^7 = (1,2,11)$ $c_2 = (R_2c_1^2R_2)c_1(R_2c_1R_2)$ $c_3 = R_2c_1R_2$ $\ldots$	$\{1,2,11\}$ $\{1,2,3,11\}$ $\{1,\ldots,4,11\}$
12	$R_1 = (1,2)(3,4)(5,6)(7,8)$ $R_2 = (1,3)(2,4)(9,10)(11,12)$ $R_3 = (4,5)(6,12)(8,9)(10,11)$	$c_1 = (R_1R_3)^{10} = (7,9,8)$ $c_2 = R_2c_1R_2$ $c_3 = R_3c_2R_3$ $\ldots$	$\{7,8,9\}$ $\{7,8,9,10\}$ $\{7,\ldots,11\}$
13	$R_1 = (1,2)(3,4)(5,6)(7,8)(9,10)(11,12)$ $R_2 = (1,3)(2,4)(5,7)(6,8)(9,11)(10,12)$ $R_3 = (1,2)(4,5)(8,9)(12,13)$	$c_1 = (R_1R_3)^4 = (11,13,12)$ $c_2 = (R_2c_1^2R_2)c_1(R_2c_1R_2)$ $c_3 = R_2c_1R_2$ $\ldots$	$\{11,12,13\}$ $\{10,\ldots,13\}$ $\{9,\ldots,13\}$
14	$R_1 = (1,2)(3,4)(5,6)(7,8)$ $R_2 = (1,3)(2,4)(9,10)(11,12)$ $R_3 = (1,14)(4,5)(6,7)(8,9)(10,11)(12,13)$	$c_1 = (R_1R_3)^{14} = (1,14,2)$ $c_2 = (R_2c_1R_2)c_1(R_2c_1^2R_2)$ $c_3 = R_2c_1R_2$ $\ldots$	$\{1,2,14\}$ $\{1,2,4,14\}$ $\{1,\ldots,4,14\}$
15	$R_1 = (1,2)(3,4)(5,6)(7,8)(9,10)(13,14)$ $R_2 = (1,3)(2,4)(5,7)(6,8)(9,10)(11,12)$ $R_3 = (1,15)(2,3)(4,5)(8,9)(10,11)(12,13)$	$c_1 = (R_1R_3)^{35} = (12,14,13)$ $c_2 = R_2c_1R_2$ $c_3 = R_3c_2R_3$ $\ldots$	$\{12,13,14\}$ $\{11,\ldots,14\}$ $\{10,\ldots,14\}$
16	$R_1 = (1,2)(3,4)(5,6)(7,8)(9,10)(11,12)$ $R_2 = (1,3)(2,4)(5,7)(6,8)(9,10)(13,14)$ $R_3 = (1,16)(4,5)(8,9)(10,11)(12,13)(14,15)$	$c_1 = (R_1R_3)^{28} = (1,2,16)$ $c_2 = (R_2c_1^2R_2)c_1(R_2c_1R_2)$ $c_3 = R_1(3,2,1)R_31$ $\ldots$	$\{1,2,16\}$ $\{1,2,3,16\}$ $\{1,\ldots,4,16\}$

TABLE 1. Initial cases for induction.

This establishes the base of the induction. To prove the inductive step we make following hypotheses:

There are involutions R_1, R_2, R_3 in A_n, a partition of $\{1, 2, \ldots, n\}$ into disjoint non-empty subsets S_1, S_2, and elements $i \in S_1, j \in S_2$ so that

(a) R_1R_2=R_2R_1.
(b) $R_1(S_1)$ =S_1, $R_1(S_2)$=S_2, $R_2(S_1)$=S_1, $R_2(S_2)$=S_2.
(c) $(i, j) \in R_3$ and $R_3(S_1\backslash i)$=$S_1\backslash i$, $R_3(S_2\backslash j)$=$S_2\backslash j$.
(d) $(k, i) \in R_1$ for some $k \neq i$ and $R_3(k) = k$.
(e) $(R_1R_3)^m$ is a 3-cycle c, where m is some integer.

Condition (e) is equivalent to the cycle decomposition of R_1R_3 having one 3-cycle and all other cycles having lengths relatively prime to three. Next we extend this data to A_{n+8} as follows:

$$R_1' = R_1(n+1, n+2)(n+3, n+4)(n+5, n+6)(n+7, n+8),$$

$$R_2' = R_2(n+1, n+3)(n+2, n+4)(n+5, n+7)(n+6, n+8),$$

$$R_3' = R_3(i, j)(i, n+1)(n+4, n+5)(n+8, j),$$

$$S_1' = S_1 \cup \{n+1, n+2, n+3, n+4\},$$

$$S_2' = S_2 \cup \{n+5, n+6, n+7, n+8\},$$

$$i' = n+4, j' = n+5, k' = n+3.$$

Proposition 3.1. *The elements R_1', R_2', R_3' are involutions in A_{n+8} satisfying conditions (a)-(e) above.*

Proof. It is clear that R_1' and R_2' are involutions in A_{n+8}. Note that $(i, j) \in R_3$ and so $R_3(i, j)$ is a product of disjoint transpositions involving only elements from the set $\{1, 2, \ldots, n\}\backslash\{i, j\}$. Therefore, R_3 is also an involution in A_{n+8}.

Properties (a),(b),(c) and (d) are easy to check. To prove (e) we compute $R_1'R_3'$:

$$R_1'R_3' = (n+1, n+2, i, k)(n+3, n+5, n+6, n+4)(n+8, n+7, j, \ldots)(\mathit{othercycles}).$$

The "other cycles" in $R_1'R_3'$ are identical to some of those in R_1R_3, specifically those not including i or j.

Now the cycle of R_1R_3 containing j has the form $(i, k, j, j_2, \ldots, j_t)$, where $\{j_2, \ldots, j_t\}$ is a subset (possibly empty)of $S_2\backslash\{j\}$ and $R_1(j_t) = j$ (or $R_1(j) = j$ in which case the above cycle is just the 3-cycle (i, k, j)). The form of $R_1'R_3'$ now reveals that the cycle of $R_1'R_3'$ containing j is $(n+8, n+7, j, j_2, \ldots, j_t)$ and so has the same length as the cycle of R_1R_3 containing j. It now follows that $(R_1'R_3')^{m'}$ is a 3-cycle, where m' =LCM$(4, m)$ □

Remark. . The involutions R_1R_2, R_3 defined in the table for the initial cases n =9,10,11,12,13, 14,15,16 satisfy (a),. . . ,(e) for the following choices of S_1, S_2, i, j, k, m:

n	S_1	i	j	k	m
9	$\{1,2,3,4\}$	4	5	3	4
10	$\{1,2,3,4\}$	4	5	3	5
11	$\{1,2,3,4,11\}$	4	5	3	7
12	$\{1,2,3,4\}$	4	5	3	10
13	$\{1,2,3,4\}$	4	5	3	4
14	$\{1,2,3,4,14\}$	4	5	3	14
15	$\{5,\ldots,14\}$	5	4	6	35
16	$\{1,2,3,4,16\}$	4	5	3	28

S_2 is always the complement of S_1.

Thus it follows that (a),...,(e) hold for A_n if $n \geq 9$. We will show that these involutions generate A_n. The method of proof will be by "extending 3-cycles", as illustrated in the Table. That is, we start with the 3-cycle $c_1 = (R_1R_3)^m$, which generates A_3, and then inductively construct additional 3-cycles $c_2, c_3, \ldots$ so that each c_r involves only one letter different from those present in $c_1, \ldots, c_{r-1}$, each c_r is of the form WcW^{-1} where c is a 3-cycle in the group generated by $c_1, \ldots, c_{r-1}$, and W is a word in R_1, R_2, R_3.

Proposition 3.2. *The involutions R_1, R_2, R_3 generate A_n for $n \geq 9$.*

Proof. The proof is by induction on n. The initial step is provided by the Table, that is for $n = 9, 10, 11, 12, 13, 14, 15, 16$. So assume that A_n is generated by R_1, R_2, R_3 for some value of n. Then we must show that A_{n+8} is generated by R_1', R_2', R_3'.

First note that the 3-cycle $c_1 = (R_1R_3)^m$ does not involve i or j. Therefore $c_1' = (R_1'R_3')^{m'}$ is identical to c_1. Moreover, c_1 involves only letters from either S_1 or S_2, say S_1, the case S_2 being similar.

Now consider the sequence of 3-cycles in A_n up to the point where j is adjoined, say $c_1, c_2, \ldots, c_{r+1}$, where $c_1 = (R_1R_3)^m$ and $c_t = W_t\gamma_t W_t^{-1}, 2 \leq t \leq r+1$, for some word W_t in R_1, R_2, R_3 and some $\gamma_t \in \langle c_1, c_2, \ldots, c_{t-1}\rangle$. Necessarily $\gamma_r = (i_1, i_2, i)$ for some $i_1, i_2 \in S_1\backslash\{i\}$ and $c_{r+1} = (i_3, i_4, j)$ for some $i_3, i_4 \in S_1$.

Examination of the table (the base case of the induction) reveals that we have $W_{r+1} = R_3$ and that all subsequent conjugations are also by generators. We make the inductive assumption that this also occurs for A_n.

Let W_t' denote the word in R_1', R_2', R_3' obtained from W_t by replacing each occurence of R_j by R_j'. Then the 3-cycle $c_t' = W_t'\gamma_t W_t'^{-1}$ is identical to c_t for $2 \leq t \leq r$, and $c_{r+1}' = R_3'\gamma_{r+1}R_3' = (i_3, i_4, n+1)$.

Thus we have added the new letter $n+1$. Then conjugating by $R_1', R_2', R_1', R_3', R_1', R_2', R_1', R_3'$ in turn yields the new letters $n+2, n+4, n+3, n+5, n+6, n+8, n+7, j$ respectively. Notice that all new conjugations are also by generators.

All that remains now is to add the letters in $S_2\backslash\{j\}$. To do this we merely follow the corresponding sequence in A_n, replacing each occurence of R_j in every conjugation by R'_j □

Now the "negative" part.

Proposition 3.3. *A_6,A_7 and A_8 can not be generated by such involutions.*

Proof. The easiest case is A_7. Up to conjugation, the first involution can be chosen only one way - namely (1,2)(3,4). The second is either (1,3)(2,4), or (1,2)(5,6). In both cases we have four subsets stable under both permutations, namely $\{1,2,3,4\},\{5\},\{6\},\{7\}$ and $\{1,2\},\{3,4\},\{5,6\},\{7\}$ respectively. The third involution consists of only two transpositions, so it can not connect all these four subsets into one, therefore we do not have a transitive action on the set $\{1,2,3,4,5,6,7\}$. Hence the subgroup generated by R_1, R_2 and R_3 is not A_7.

In the case of A_6 for the first two involutions we have again only two essentially different choices: R_1=(1,2)(3,4), R_2=(1,2)(5,6) or R_2=(1,3)(2,4). The transitivity argument forces the choice of R_3: R_3=(2,3)(4,5) in the first case and R_3=(1,5)(2,6) in the second. In both cases we compute the order of $\langle R_1, R_2, R_3\rangle$. It is 60 in the first case and 24 in the second. Hence the subgroup is not A_6. This was done by computer.

The most extensive case is A_8. Up to conjugacy there are only two choices for R_1, namely $R_1 = (1,2)(3,4)$ and $R_1 = (1,2)(3,4)(5,6)(7,8)$. Now we must choose an involution R_2 so that $R_1R_2 = R_2R_1$. When choosing R_2 we do not distinguish amongst choices that are conjugate by any conjugation that leaves R_1 invariant. Nor do we distinguish amongst choices that give the same subgroup $\langle R_1, R_2\rangle \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$. There are then only five essentially different choices for R_1 and R_2:

(I) $R_1 = (1,2)(3,4)$ $R_2 = (1,3)(2,4)$
(II) $R_1 = (1,2)(3,4)$ $R_2 = (1,2)(5,6)$
(III) $R_1 = (1,2)(3,4)$ $R_2 = (5,6)(7,8)$
(IV) $R_1 = (1,2)(3,4)$ $R_2 = (1,3)(2,4)(5,6)(7,8)$
(V) $R_1 = (1,2)(3,4)(5,6)(7,8)$ $R_2 = (1,3)(2,4)(5,7)(6,8)$.

In case V there is only one choice for R_2 since any other choice is either equivalent to this one or reduces to case (IV).

We must now choose the third involution R_3. Again we do not distinguish amongst choices that differ only by a conjugation not altering the subgroup $\langle R_1, R_2\rangle = \mathbb{Z}_2 \oplus \mathbb{Z}_2$. These conjugations can be by elements of S_8. Our choices for R_3 are restricted by the fact that the group $\langle R_1, R_2, R_3\rangle$ is supposed to be transitive on $\{1,2,3,4,5,6,7,8\}$. In each choice of R_3 we used a computer to determine the order of the subgroup $\langle R_1, R_2, R_3\rangle$. The maximum order turns out to be 576, and therefore A_8 can not be generated by three involutions as in (1).

	Choice of R_3	order of $\langle R_1, R_2, R_3\rangle$
(I)	$R_3 = (1,5)(2,6)(3,7)(4,8)$	32
(II)	$R_3 = (1,7)(2,3)(4,5)(6,8)$	192
(III)	$R_3 = (1,7)(2,3)(4,5)(6,8)$	48

In case (IV) there are many choices for R_3 leading to groups of different orders. The diagram below indicates how R_1 and R_2 are acting on the eight elements $1, 2, \ldots, 8$.

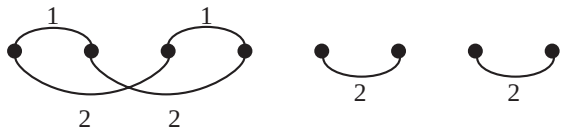


FIGURE 4. R_1, R_2 acting on 8 symbols.Case IV.

R_3 must necessarily involve a transposition containing one letter from $1, 2, 3, 4$ and one from $5, 6, 7, 8$. Up to conjugacy we may assume $(4, 5)$ is in R_3. Since R_3 is an even permutation it must involve either one more transposition or three more. Thus the cases are:

(IVa) $R_3 = (4,5)(1,7)$	48
(IVb) $R_3 = (4,5)(3,7)$	64
(IVc) $R_3 = (4,5)(6,7)$	576

We should point out that either 7 or 8 must be involved in the other transposition and that the choice $R_3 = (4, 5)(2, 7)$ is equivalent to $R_3 = (4, 5)(1, 7)$. To see this note that switching 1 and 2 leaves $\langle R_1, R_2 \rangle$ invariant. The same remarks apply when the choices for R_3 involve 4 disjoint transpositions.

(IVd) $R_3 = (4,5)(1,7)(2,3)(6,8)$	16
(IVe) $R_3 = (4,5)(1,7)(2,6)(3,8)$	16
(IVf) $R_3 = (4,5)(1,7)(2,8)(3,6)$	32
(IVg) $R_3 = (4,5)(3,7)(1,2)(6,8)$	64
(IVh) $R_3 = (4,5)(3,7)(1,6)(2,8)$	16
(IVi) $R_3 = (4,5)(6,7)(1,2)(3,8)$	64
(IVj) $R_3 = (4,5)(6,7)(1,8)(2,3)$	48

In case V the action of R_1, R_2 is given by the following diagram

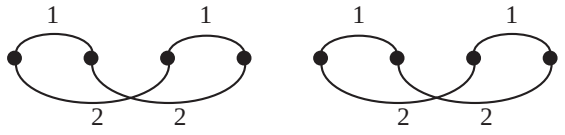


FIGURE 5. R_1, R_2 acting on 8 symbols.Case V.

All choices for R_3 must involve (4,5), at least up to conjugacy. The possibilities are:

(Va)	$R_3 = (4,5)(1,2)$	192
(Vb)	$R_3 = (4,5)(1,6)$	48
(Vc)	$R_3 = (4,5)(1,8)$	16
(Vd)	$R_3 = (4,5)(1,2)(3,6)(7,8)$	16
(Ve)	$R_3 = (4,5)(1,2)(3,7)(6,8)$	24
(Vf)	$R_3 = (4,5)(1,2)(3,8)(6,7)$	24
(Vg)	$R_3 = (4,5)(1,6)(2,3)(7,8)$	24
(Vh)	$R_3 = (4,5)(1,6)(2,7)(3,8)$	8
(Vi)	$R_3 = (4,5)(1,6)(2,8)(3,7)$	32
(Vj)	$R_3 = (4,5)(1,8)(2,3)(6,7)$	16
(Vk)	$R_3 = (4,5)(1,8)(2,6)(3,7)$	8
(Vl)	$R_3 = (4,5)(1,8)(2,7)(3,6)$	8

□

The Symmetric Groups.

Theorem 3.4. *Any symmetric group S_n with $n \geq 4$ can be generated by three involutions, two of which commute.*

Proof. If $n = 2k + 1$ we choose

R_1=(3,4)(5,6) ... $(2k-1, 2k)$,

R_2=(1,2),

R_3=(2,3)(4,5) ... $(2k, 2k+1)$.

Now, (1,3)=$R_3R_2R_3$, (1,4)=R_1(1,3)R_1, (1,5)=R_3(1,4)R_3, etc. So we can produce all (1,i), for 2$\leq i \leq n$, which obviously generate S_n. The case where n is even is similar to this. The cases $n < 4$ are trivial (there are not enough involutions) □

4. THE PROJECTIVE LINEAR GROUPS

In this section we shall prove theorems 1.3 and 1.4. Again we prove the "positive" part first. We start with the case p=2. Thus we must prove the following

Proposition 4.1. *$SL_2(2^n)$ can be generated by three involutions, two of which commute, if $n \geq 2$.*

Proof. Consider the matrices

$$R_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},\ R_2 = \begin{pmatrix} x & 1+x \\ 1+x & x \end{pmatrix},\ R_3 = \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix}.$$

Here x and y are elements of the finite field $GF(2^n)$. We want these matrices to be different from the identity and from each other, and this happens if, and only if, $x \neq 0, 1$ and $y \neq 0$. Thus we need $n \geq 2$ so that such elements exist.

It is easy to check that $R_1R_2 = R_2R_1$ and that R_3 does not commute with any of R_1, R_2, R_1R_2. In fact

$$R_1R_3 = \begin{pmatrix} 0 & 1 \\ 1 & y \end{pmatrix}, \; R_2R_3 = \begin{pmatrix} x & xy+1+x \\ 1+x & y+xy+x \end{pmatrix}, \; R_1R_2R_3 = \begin{pmatrix} 1+x & y+xy+x \\ x & xy+1+x \end{pmatrix}$$

and the respective traces are $y, y+xy$, and xy. Since these traces are not zero it follows that R_3 does not commute with any of R_1, R_2, R_1R_2.

Now we suppose that $y = z + z^{-1}$ for some $z \in GF(2^n)$, where $z \neq 0$ and $z \neq 1$. Again this assumes that $n \geq 2$. Then R_1R_3 is similar to the diagonal matrix

$$\begin{pmatrix} z & 0 \\ 0 & z^{-1} \end{pmatrix}$$

and so its order is the least integer k so that $z^k = 1$. Choosing z to be a primitive root of GF(2^n) we see that the order of R_1R_3 is $2^n - 1$. According to Dickson's theorem (2.7) the possible subgroups of $SL_2(2^n)$ are: A_4 if n is even, A_5 if n is even, the dihedral groups $T(2, 2, t)$ of order $2t$ for $t = 2$ or $t|(2^n - 1)$, the affine groups, and the projective groups $SL_2(2^m)$ for $m|n$. Let G be the subgroup generated by R_1, R_2, R_3.

G can not be dihedral since R_3 does not commute with any of R_1, R_2, R_1R_2 (see lemma 2.10). Also G can not be cyclic since it contains the subgroup $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \cong < R_1, R_2 >$. Thus G must be A_4, A_5, affine or projective. In fact G can not be A_4 according to Theorem 1.1.

Suppose G is affine, that is G is isomorphic to a subgroup of the group

$$A = \left\{ \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} \mid a, b \in GF(2^n), a \neq 0 \right\}$$

There exists a split short exact sequence $1 \to \mathbb{Z}_{2^n} \to A \to \mathbb{Z}_{2^n-1} \to 1$, where the normal subgroup $\mathbb{Z}_{2^n}$ consists of all matrices of the form

$$\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}.$$

Any subgroup of A generated by elements of order 2 would have to be a subgroup of $\mathbb{Z}_2^n$ and therefore be abelian. G is not abelian and so can not be affine. Thus G is A_5 or projective.

For the moment assume that $n > 2$. Then $2^n - 1 \geq 7$ and so G must be projective. The proper projective subgroups $SL_2(2^m)$, where m is a proper divisor of $2^n - 1$, do not have

elements of order $2^n - 1$, and therefore G must be $SL_2(2^n)$. This proves the proposition for $n > 2$.

To prove the proposition for $q = 4$ we can use the isomorphism $SL_2(4) \cong A_5$ and then apply Theorem 1.1. Or we can consider the three matrices

$$R_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \ R_2 = \begin{pmatrix} x & 1+x \\ 1+x & x \end{pmatrix}, \ R_3 = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}.$$

Here x is any element of $GF(4)$ satisfying $x^2 + x + 1 = 0$. Then it is easy to check that the orders of R_1R_3 and R_2R_3 are 5 and 3 respectively. Since the subgroup generated by R_1 and R_2 has order 4 it follows that the order of G is at least 60. On the other hand $SL_2(4)$ has order exactly equal to 60 and so G is all of $SL_2(4)$ □

Now we will prove Theorem 1.3 for odd primes p. The proof is broken down into two cases, the case where -1 is a square in $GF(q)$ and the case where it is not. First we consider the case where -1 is a square. This happens if, and only if, either $p \equiv 1 (\mathrm{mod}\ 4)$ and n is arbitrary, or $p \equiv -1 (\mathrm{mod}\ 4)$ and n is even.

Proposition 4.2. *Suppose p is an odd prime and -1 is a square in $GF(q)$. Then $PSl_2(q)$ can be generated by three involutions, two of which commute, if $q \neq 9$.*

Proof. Let a be any element of $GF(q)$ such that $a^2 = -1$. Then consider the three matrices

$$R_1 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \ R_2 = \begin{pmatrix} a & 0 \\ 0 & -a \end{pmatrix}, \ R_3 = \begin{pmatrix} a & x \\ 0 & -a \end{pmatrix}.$$

Here x is any non-zero element of $GF(q)$. Then we can check that these three matrices are different from the identity and each other. Moreover $R_1R_2 = R_2R_1$ and R_3 does not commute with any of R_1, R_2, R_1R_2. We want to show that G, the subgroup of $PSL_2(q)$ generated by R_1, R_2, R_3, is the entire group, provided x is chosen appropriately.

The idea of the proof is to use Dickson's theorem (2.7) to rule out all proper subgroups. First of all note that G can not be dihedral since if it were R_3 would have to commute with at least one of R_1, R_2, R_1R_2, and it does not. Next we note that G can not be affine since $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ is never a subgroup of an affine group when p is odd. Therefore G must be either projective or exceptional, that is G is isomorphic to one of the following

1. $G \cong PSL_2(p^m)$ for some $m|n$, or $G \cong PGL_2(p^m)$ for some $2m|n$.
2. $G \cong A_4, S_4$, or A_5.

Now consider the matrix

$$R_1R_3 = \begin{pmatrix} 0 & -a \\ -a & -x \end{pmatrix}.$$

We choose x equal to $z + z^{-1}$, for some $z \in GF(q), z \neq 0, \pm 1$. Then the matrix R_1R_3 is similar to

$$\begin{pmatrix} z & 0 \\ 0 & z^{-1} \end{pmatrix}$$

and therefore its order is the least positive integer k so that $z^k = \pm 1$. In particular if we choose z to be a primitive root of $GF(q)$ then the order of R_1R_3 will be $\frac{q-1}{2}$. For the moment assume that $q > 11$ so that $\frac{q-1}{2} > 5$. Thus G can not be exceptional and so must be projective. In fact G must be all of $PSL_2(q)$ since any proper projective subgroup can not have an element of order $\frac{q-1}{2}$. This proves the proposition when -1 is a square, except for $q = 5$.

If $q = 5$ we choose matrices

$$R_1 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \ R_2 = \begin{pmatrix} 2 & 0 \\ 0 & -2 \end{pmatrix}, \ R_3 = \begin{pmatrix} 2 & x \\ 0 & -2 \end{pmatrix},$$

where x is any non-zero element of $GF(5)$. The order of R_2R_3 is 5, the order of the subgroup $< R_1, R_2 >$ is 4, and so the order of G is at least 20. This is sufficient to guarantee that G is all of $PSL_2(5)$. We could also argue as follows:

$$R_1R_3 = \begin{pmatrix} 0 & -2 \\ -2 & -x \end{pmatrix}, \ R_1R_2R_3 = \begin{pmatrix} 0 & -1 \\ 1 & -2x \end{pmatrix}.$$

The respective traces are $-x$ and $-2x$ and so one of these matrices will have order three. Therefore G will have order at least 60, and so must be all of $PSL_2(5)$ since $PSL_2(5)$ has order 60.

Another approach would be to use Theorem 1.1 together with proposition 2.11. This completes the proof of the proposition □

Proposition 4.3. *Suppose $p \equiv -1 (\mathrm{mod}\ 4)$ and n is odd. Then $PSl_2(q)$ can be generated by three involutions, two of which commute, if $q \geq 11$.*

Proof. We choose elements $a, b \in GF(q)$ satisfying $a^2 + b^2 = -1$. This is always possible. Then let R_1, R_2, R_3 be the matrices

$$R_1 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \ R_2 = \begin{pmatrix} a & b \\ b & -a \end{pmatrix}, \ R_3 = \begin{pmatrix} 0 & y \\ -y^{-1} & 0 \end{pmatrix},$$

where y is any element of $GF(q)$ such that $y \neq 0, \pm 1$. For any such y it is easy to check that the R_j are all distinct and different from the identity, $R_1R_2 = R_2R_1$, and R_3 does not commute with any of R_1, R_2, R_1R_2.

Let G denote the group generated by R_1, R_2, R_3. G can not be affine since it contains the subgroup $< R_1, R_2 > \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$. Moreover G can not be dihedral since R_3 does not commute with any of R_1, R_2, R_1R_2 (see lemma 2.10). Therefore G must be projective or one of A_4, S_4, A_5. The actual type of G will depend on how we choose y.

$$R_1R_3 = \begin{pmatrix} -y^{-1} & 0 \\ 0 & -y \end{pmatrix}$$

has order equal to the smallest positive integer k such that $y^k = \pm 1$.

Choosing y to be a primitive root of $GF(q)$ this order will be $\frac{q-1}{2}$. If $\frac{q-1}{2} > 5$ Then G will be projective, and in fact all of $PSL_2(q)$. This proves the proposition, except for $q = 11$.

Now we consider the case $q = 11$. Consider the matrices

$$R_1 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},\ R_2 = \begin{pmatrix} 1 & 3 \\ 3 & -1 \end{pmatrix},\ R_3 = \begin{pmatrix} 1 & -1 \\ 2 & -1 \end{pmatrix}.$$

Then we see that the products

$$R_1R_3 = \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix},\ R_2R_3 = \begin{pmatrix} 7 & -4 \\ 1 & -2 \end{pmatrix}$$

have respective orders 5, 6. Since R_3 does not commute with any of R_1, R_2, R_1R_2 the only possibilities for G are $PSL_2(11)$ and one of A_4, S_4, A_5. But the groups A_4, S_4, A_5 do not have elements of order 6 and so G must be $PSL_2(11)$. □

The "negative" part of the theorem 1.3 is just a combination of previous results.

Proposition 4.4. *$PSL_2(q)$ can not be generated by three involutions two of which commute if $q = 2, 3, 7$ or 9.*

Proof. For q=2 or 3 there are not enough involutions (or we can use proposition 2.11 in conjunction with theorem 1.1). For q=9 we refer to propositions 2.11 and 3.3. For q=7 we refer to theorem 2.8 and the proof of proposition 3.3 noting the fact that any transitive permutation representation $\rho : PSL_2(7) \to S_7$ must have its image in A_7 since $PSL_2(7)$ can be generated by two elements, one of order 3, and the other of order 7. Now, if $PSL_2(7)$ could be generated by three involutions, two of which commute, then it would follow that these involutions in A_7 would act transitively; but the proof of proposition 3.3 shows that this is impossible □

Now we turn our attention to the projective general linear groups $PGL_2(q)$.

Proposition 4.5. *$PGL_2(q)$ can be generated by three involutions, two of which commute, if and only if, $q > 2$.*

Proof. First notice that for even q's the result is theorem 1.3 since $PGL_2(q) \cong PSL_2(q)$. For odd q's we again heavily rely on Dickson's Classfication Theorem (2.7). We choose involutions to be images in $PGL_2(q)$ of

$$R_1 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \; R_2 = \begin{pmatrix} 0 & 1 \\ x & 0 \end{pmatrix}, \; R_3 = \begin{pmatrix} 1 & y \\ 0 & -1 \end{pmatrix},$$

with x and y to be defined later. As in the case of the projective special linear groups, the cyclic, affine and dihedral subgroups are easily eliminated, so long as $y \neq 0$.

We are going to produce an element of order $q-1$ in the subgroup generated by R_1, R_2 and R_3, thus eliminating all proper projective subgroups and all exceptional subgroups for $q \geq 7$. Note that the result for $q = 3$ and $q = 5$ follows from proposition 2.11 and theorem 1.2.

Consider the matrix $A = R_2R_3 = \begin{pmatrix} 0 & -1 \\ x & xy \end{pmatrix}$. It has trace xy and determinant x. We choose x to be a primitive root in $GF(q)$ and $y = 1 + x^{-1}$. Then A is conjugate to $\begin{pmatrix} 1 & 0 \\ 0 & x \end{pmatrix}$ and therefore A has order $q - 1$. Thus R_1, R_2 and R_3 generate all of $PGL_2(q)$. □

5. HAMILTONIAN CYCLES

In this section we shall show that many graphs admit Hamiltonian cycles, thus corroborating the Lovász Conjecture. The graphs we consider are the Cayley graphs of finite groups G having a presentation as in (1). Any such graph is trivalent and so, in some sense, represents the hardest possible case for the existence of Hamiltonian cycles.

Requiring two of the involutions to commute allows us to give a very simple inductive proof for the existence of Hamiltonian cycles. The idea was first mentioned to us by George Maxwell [8], and was also used by Conway, Sloane and Wilks [3] to prove that every finite Coxeter group has Hamiltonian cycles.

Theorem 5.1. *Suppose G has a presentation as in (1). Then the Cayley graph of this presentation has a Hamiltonian cycle.*

Proof. The Cayley graph is trivalent. We can extend the graph to a surface by adding 4-gons, $2s$-gons and $2t$-gons, where s and t are the orders of R_1R_3 and R_2R_3 respectively, as was described in section 2. We will obtain the Hamiltonian cycle as the boundary of a union of faces of the Cayley surface.

The first step is to color all the $2t$-gons, with the same color, and then take the boundary of all colored faces. This will involve all vertices, but in $\frac{1}{2t}|G|$ disjoint cycles.

The next step is to join the colored $2t$-gons by coloring certain 4-gons. Pick any 4-gon and color it. Now the boundary of the union of all colored faces will have one less component, but still involve all vertices. The idea is to repeat this last step until there is only one colored component whose boundary involves all vertices. Suppose at some stage of the construction we still have several colored components. Then there will be a pair of adjacent $2t$-gons in different components, that is there will be an uncolored 4-gon joining these components. Coloring this 4-gon then reduces the number of components. This construction will end in a contractible union of faces whose boundary is a Hamiltonian cycle. □

Note added in proof.

After this paper was written we came upon another paper containing results overlapping with ours. In [2] Conder proves that every A_n, S_n for n sufficiently large, can be generated by three involutions, two of which commute. His proof is different from ours, and the bound on n is not explicit, but much bigger than necessary (see Theorems 1.1 and 1.2).

References

[1] W. Burnside. *Theory of Groups of Finite Order*. Dover Publications Inc., 1955.

[2] Marston Conder. More on generators for alternating and symmetric groups. *Quarterly J. of Math.*, 32:137–163, 1981.

[3] J.H. Conway, N.J.A.Sloane, and Allan R.Wilks. Gray codes for reflection groups. *Graphs and Combinatorics*, 5:315–325, 1989.

[4] Leonard Dickson. *Linear Groups, with an Exposition of the Galois Field Theory*. New York, 1958.

[5] Henry Glover and Denis Sjerve. Representing $PSl_2(p)$ on a riemann surface of least genus. *L'Enseignement Mathématique*, 31:305–325, 1985.

[6] Henry Glover and Denis Sjerve. The genus of $PSl_2(q)$. *Journal reine angew. Math.*, 380:59–86, 1987.

[7] Laslo Lovász. Problem 11. In Richard Guy, Haim Hanani, Norbert Sauer, and Johanan Schonheim, editors, *Combinatorial structures and their applications*. Gordon and Breach,New York, 1970.

[8] George Maxwell. Private communication.

[9] Michio Suzuki. *Group Theory I*. Berlin–Heidelberg–New York, 1982.

[10] D. Witte and J.A Gallian. A survey – hamiltonian cycles in cayley graphs. *Discrete Math.*, 51:293–304, 1984.

[11] Tzu-Yi Yang. PhD thesis, Ohio State University, 1993.