WRITING ELEMENTS OF PSL(2,q) AS COMMUTATORS

DARRYL MCCULLOUGH AND MARCUS WANDERLEY

ABSTRACT. We prove that for $q \ge 13$, an element A of SL(2,q) is the commutator of a generating pair if and only if $A \ne -I$ and the trace of A is not 2. Consequently, when q is odd and $q \ge 13$, every nontrivial element of PSL(2,q) is the commutator of a generating pair, and when q is even, an element of PSL(2,q) is the commutator of a generating pair if and only if its trace is not 0. The proof of these results also leads to an improved lower bound on the number of T-systems of generating pairs of PSL(2,q).

Recently major progress has been made in understanding the commutator map $\alpha: G \times G \to G$ for a finite simple group. In particular, S. Garion and A. Shalev [7] used representation theory and the Witten zeta function to prove that α is almost equidistributed as $|G| \to \infty$. As a consequence, the probability that an element $g \in G$ can be expressed as a commutator g = [x, y] where $\{x, y\}$ is a generating pair of G goes to 1 as $|G| \to \infty$.

In this paper we use elementary arguments to sharpen the latter statement when G is PSL(2, q):

Commutator Theorem. When q is odd and $q \ge 13$, every nontrivial element of PSL(2,q) is a commutator of a generating pair. When q is even, an element of PSL(2,q) is a commutator of a generating pair if and only if its trace is not 0.

The conclusion of the Commutator Theorem is false for q = 3, 5, 7, 9, and 11.

The Commutator Theorem is an immediate consequence of the following statement:

Theorem 2.2. When q = 2, 4, 8 or $q \ge 13$, an element A of SL(2,q) is the commutator of a generating pair if and only if the trace of A is not 2 and $A \ne -I$.

Theorem 2.2 follows from a more technical result, Theorem 2.1, which also provides the following lower bound for the number of T-systems of generating pairs:

Date: March 31, 2008.

²⁰⁰⁰ Mathematics Subject Classification. Primary 20G40.

Key words and phrases. special linear group, T-system, commutator, trace, projective. The first author was supported in part by NSF grant DMS-0102463.

T-system Theorem. Let $q = p^s$, p prime. When q is even or $q \ge 13$, the number of T-systems of generating pairs of PSL(2,q), and hence of SL(2,q), is bounded below by $\Psi_q - 1$, where Ψ_q is the number of orbits of the $Aut(\mathbb{F}_q)$ -action on the field of q elements \mathbb{F}_q . This number is given by the following formula, in which φ denotes the Euler totient function:

$$\Psi_q = \frac{1}{s} \sum_{r|s} \varphi(s/r) \ p^r \ .$$

M. Evans, in his dissertation [5], proved that the number of T-systems of PSL(2, q) goes to ∞ as q does. More precisely, he showed by computation that every element of the field \mathbb{F}_q of q elements other than 0 and 2 appears as the trace of the commutator of a generating pair, and deduced the lower bound $\lceil \frac{q-2}{s} \rceil$ for the number of T-systems. The proof of our main technical result, Theorem 2.1, is similar to Evans' method.

The authors gratefully acknowledge the support of many sources in the course of this work. Travel of the first author was supported by National Science Foundation grant DMS-0102463, by the University of Oklahoma College of Arts and Sciences, and by the University of Oklahoma Office of Research Administration. The work of both authors was supported by the Universidade Federal de Pernambuco Summer in Recife program. We are grateful to Martin Evans for providing us a copy of [5]. We owe a special thanks to Gareth Jones, who provided us with the proof of the formula for Ψ_q that we give below.

1. T-SYSTEMS AND TRACE INVARIANTS

Denote by \mathcal{G}_n the set of generating *n*-tuples of a group *G*. The elements of \mathcal{G}_n can be identified with the surjective homomorphisms from the free group F_n of rank *n* onto *G*. In this way, we may regard $\operatorname{Aut}(F_n) \times \operatorname{Aut}(G)$ as acting on \mathcal{G}_n by $(\phi, \alpha) \cdot \gamma = \alpha \circ \gamma \circ \phi^{-1}$. The orbits of this action are called *T*-systems and the orbits of its restriction to $\operatorname{Aut}(F_n)$ are called *Nielsen classes*.

For an element $(g_1, g_2) \in \mathcal{G}_2(G)$, the union of the conjugacy classes of the commutator $[g_1, g_2] = g_1 g_2 g_1^{-1} g_2^{-1}$ and its inverse is a well-known invariant of the Nielsen class of (g_1, g_2) , called the *Higman invariant*.

From now on, we restrict attention to the case when G is SL(2,q) or PSL(2,q), and n = 2. Observe that for elements $A, B \in PSL(2,q)$, the commutator [A, B] is well-defined in SL(2,q). The commutator and its inverse, as well as all their conjugates, have the same trace, so the trace of [A, B] is a well-defined invariant of the Nielsen class of (A, B), which we call the trace invariant.

The automorphisms of SL(2, q) and PSL(2, q) are well-understood, by the following result due to Schreier and van der Waerden [13] (see also [2], [4], and the appendix to [9]).

Theorem. Every automorphism of SL(2,q) or of PSL(2,q) has the form $A \mapsto PA^{\phi}P^{-1}$, where P is an element of GL(2,q), and A^{ϕ} is the matrix obtained by applying an automorphism ϕ of \mathbb{F}_q to each entry of A.

Conjugation has no effect on the trace invariant, but applying a field automorphism to the coefficients of A and B changes the trace of [A, B] by the field automorphism itself. Therefore the orbit of the trace invariant under $\operatorname{Aut}(\mathbb{F}_q)$ is an invariant of the *T*-system, which we call the *weak trace invariant*.

2. Commutators from trace invariants

In the next section, we will prove the following realization theorem for trace invariants:

Theorem 2.1. For q = 2, 4, 8 or $q \ge 13$, the trace invariants of PSL(2,q), and hence of SL(2,q), are the elements of $\mathbb{F}_q - \{2\}$. In the remaining cases, the trace invariants are as follows:

- 1) For q = 3, q = 9, and q = 11, all elements except 1 and 2.
- 2) For q = 5, only 1 and 3.
- 3) For q = 7, all elements except 0, 1, and 2.

In the remainder of this section, we will use Theorem 2.1 to prove the following result, which as already noted immediately implies the Main Theorem.

Theorem 2.2. When q = 2, 4, 8 or $q \ge 13$, an element A of SL(2, q) is the commutator of a generating pair if and only if the trace of A is not 2 and $A \ne -I$.

First we recall the well-known conjugacy classes in SL(2, q):

Proposition 2.3. If $A, B \in SL(2,q)$ and $tr(A) \neq \pm 2$, then A is conjugate to B if and only tr(A) = tr(B). For each of the traces 2 and -2, there are two conjugacy classes when q is even and three when q is odd.

We will verify the second part, since we need the notation anyway. Consider an element X of SL(2, q) having trace 2ϵ where $\epsilon = \pm 1$. It is conjugate to a matrix of the form $\begin{pmatrix} \epsilon & \mu \\ 0 & \epsilon \end{pmatrix}$, so the nonempty set M(X) of elements μ that appear in such conjugates is a complete invariant of the conjugacy class of X. Conjugation by an element P of SL(2, q) takes $\begin{pmatrix} \epsilon & \mu \\ 0 & \epsilon \end{pmatrix}$ to $\begin{pmatrix} \epsilon & \mu' \\ 0 & \epsilon \end{pmatrix}$ if and only if P is upper triangular. In this case, writing $P = \begin{pmatrix} x & b \\ 0 & x^{-1} \end{pmatrix}$, the effect of conjugation by P is to multiply μ by x^2 . So M(X) is either 0 (when $X = \pm I$), or is the set of nonzero elements that are squares, or is the set of non-squares. Proof of Theorem 2.2. If -I were the commutator of a generating pair, then PSL(2,q) would be abelian. The trace of [A, B] cannot be 2, since then SL(2,q) would fix a 1-dimensional subspace of \mathbb{F}_q^2 (after conjugation [A, B] is an unipotent matrix T, and then ABA^{-1} and TB have the same trace, implying that B and then A are also upper triangular).

Conversely, assume that $X \neq -I$ and $\operatorname{tr}(X) \neq 2$. By Theorem 2.1 there is a generating pair (A, B) with $\operatorname{tr}([A, B]) = \operatorname{tr}(X)$. If $\operatorname{tr}(X) \neq -2$, then Proposition 2.3 gives a C with $X = C[A, B]C^{-1} = [CAC^{-1}, CBC^{-1}]$. This completes the proof for even q, so we assume that q is odd, $\operatorname{tr}(X) = -2$, and $X \neq -I$.

Suppose that $q \equiv 3 \mod 4$. Then -1 is not a square in \mathbb{F}_q , so in the notation used above to verify Proposition 2.3, $M([B, A]) = -M([A, B]) \neq M([A, B])$. Thus the conjugacy classes of [A, B] and [B, A] are distinct and are the two conjugacy classes of matrices of trace -2 other than -I. So X is conjugate to either [A, B] or [B, A], and the result follows as before.

Suppose now that $q \equiv 1 \mod 4$. Then -1 is a square, so M([B, A]) = -M([A, B]) = M([A, B]). By Theorem 2.1, at least one of the conjugacy classes of matrices of trace -2 is a Higman invariant, so we may suppose that X is not conjugate to [A, B].

By conjugation we may choose (A, B) so that $[A, B] = \begin{pmatrix} -1 & t \\ 0 & -1 \end{pmatrix}$ for some nonzero $t \in \mathbb{F}_q$. Conjugating by a matrix in $\mathrm{SL}(2, q^2)$ of the form $\begin{pmatrix} \pi & 0 \\ 0 & \pi^{-1} \end{pmatrix}$, where $\pi^2 \in \mathbb{F}_q$ but $\pi \notin \mathbb{F}_q$, changes (A, B) to a generating pair (A', B') of $\mathrm{SL}(2, q)$ having commutator $\begin{pmatrix} -1 & t\pi^2 \\ 0 & -1 \end{pmatrix}$, which must be conjugate to X.

3. Proof of Theorem 2.1

As already seen in the proof of Theorem 2.2, (A, B) cannot be a generating pair of PSL(2,q) when tr([A, B]) = 2. It remains to show that all elements of $\mathbb{F}_q - \{2\}$ are trace invariants when $q \ge 13$. For $q \le 11$, Theorem 2.1 can be verified by elementary arguments or by direct calculation, say using GAP [6]. A GAP script for these calculations is available at the first author's website [11]. So we may assume that $q \ge 13$.

The subgroups of PSL(2, q) were determined by L. E. Dickson [3]. The following statement, in which $q = p^s$ with p prime and d denotes gcd(2, q-1), is from Theorem 3(6.25) of Suzuki [14].

Theorem 3.1. Every subgroup of PSL(2,q) is isomorphic to (at least) one of the following.

(a) (small subgroups) The dihedral groups of orders $2(q \pm 1)/d$ and their subgroups.

- (b) (triangular subgroups) A group H of order q(q − 1)/d and its subgroups. A Sylow p-subgroup H₀ of H is elementary abelian and normal in H. The quotient H/H₀ is cyclic of order (q − 1)/d.
- (c) (exceptional subgroups) A_4 , S_4 , or A_5 .
- (d) (linear subgroups) $PSL(2, p^r)$ or $PGL(2, p^r)$ where r divides s.

The subgroups H_0 in (b) are also *p*-Sylow subgroups of PSL(2,q), so are conjugate to the subgroup of upper triangular elements.

An element of PSL(2, q) is called *parabolic* if its trace is ± 2 . Parabolic elements have order p. For nonparabolic elements, we have the following information from (2.3) and (2.4) of [8].

Lemma 3.2. The orders of nonparabolic elements of PSL(2,q) are exactly the divisors of (q + 1)/d and (q - 1)/d. In particular, the maximum order of a nonparabolic element of PSL(2,q) is (q + 1)/d.

For $x, y \in \mathbb{F}_q$ with $x \neq 0$, put $H_x = \begin{pmatrix} x & 0 \\ 0 & x^{-1} \end{pmatrix}$ and $J_y = \begin{pmatrix} y+1 & 1 \\ y & 1 \end{pmatrix}$. The next lemma is a straightforward calculation.

Lemma 3.3. Put $D = x - x^{-1}$. Then $[H_x, J_y] = \begin{pmatrix} 1 - Dxy & Dx(y+1) \\ -Dx^{-1}y & 1 + Dx^{-1}y \end{pmatrix}$. Consequently, the trace of $[H_x, J_y]$ is $2 - D^2y$.

The next lemma will ensure that H_x and J_y do not generate a small or triangular subgroup.

Lemma 3.4. Assume that $y \neq 0$, and that $x^4 \neq 1$ and $x^6 \neq 1$. Then $[H_x, J_y]$ and $[H_x^{-1}, J_y]$ do not commute in PSL(2, q).

Proof. Again write $D = x - x^{-1}$, which is nonzero since $x^2 \neq 1$. Now $[H_x^{-1}, J_y] = [H_{x^{-1}}, J_y]$, so $[H_x^{-1}, J_y]$ is obtained from the expression in Lemma 3.3 by replacing each appearance of x with x^{-1} (hence each D with -D). One then calculates

$$[H_x, J_y] [H_x^{-1}, J_y] = \begin{pmatrix} 1 + D^3 x y(y+1) & D^2(y+1) - D^3 x y(y+1) \\ D^2 y + D^3 x^{-1} y^2 & 1 - D^3 x^{-1} y(y+1) \end{pmatrix}$$

Again, by replacing each x by x^{-1} , we obtain

$$[H_x^{-1}, J_y] [H_x, J_y] = \begin{pmatrix} 1 - D^3 x^{-1} y(y+1) & D^2(y+1) + D^3 x^{-1} y(y+1) \\ D^2 y - D^3 x y^2 & 1 + D^3 x y(y+1) \end{pmatrix}$$

If these matrices are equal, then their (2, 1) entries show that $x = -x^{-1}$, in contradiction to the assumption that $x^4 \neq 1$. So assume that $p \neq 2$ and the matrices differ by multiplication by -I. From the (2, 1) entries, we have $1 - Dxy = -1 - Dx^{-1}y$, or $D^2y = 2$. From the (1, 1) entries, we find that $1 - D^3x^{-1}y(y+1) = -1 - D^3xy(y+1)$, which implies that $D^4y(y+1) = -2$, and using $D^2y = 2$ this leads to $D^2 = -3$. But the equation $D^2 = -3$ says that $x^2 - 2 + x^{-2} = -3$, that is, $x^4 + x^2 + 1 = 0$. Multiplying by $x^2 - 1$ shows that $x^6 = 1$, in contradiction to the hypothesis. **Proposition 3.5.** Assume that $q \ge 13$. Suppose that x generates $\mathbb{F}_q - \{0\}$ and that $y \ne 0$. Then H_x and J_y generate SL(2,q).

Proof. Since q > 7, we have $x^4 \neq 1$ and $x^6 \neq 1$. It suffices to show that the images of H_x and J_y in PSL(2, q) generate, so suppose that the subgroup S that they generate is proper. Consider the four possibilities for S given in Theorem 3.1. Small or triangular subgroups have abelian commutator subgroups, so are ruled out by Lemma 3.4. The order of H_x is (q - 1)/2, which is at least 6, so S cannot be exceptional.

Assume that S is a linear subgroup, and consider first the case that S is isomorphic to $PSL(2, p^r)$, where r is a proper divisor of s. By Lemma 3.2 the order of H_x is no more than $(p^r + 1)/d$. Since r < s, this is less than $(p^s - 1)/d$, the known order of H_x .

The remaining possibility is that p > 2 and S is isomorphic to $PGL(2, p^r)$. Since H_x^2 is contained in a subgroup isomorphic to $PSL(2, p^r)$, Lemma 3.2 shows that $(p^s - 1)/2$, the order of H_x , is no more than $p^r + 1$. This can hold only when p = 3 and s = 2, that is, q = 9.

To see that Proposition 3.5 implies Theorem 2.1 in the case $q \ge 13$, let x be a generator of $\mathbb{F}_q - \{0\}$, and put $D = x - x^{-1}$. By Proposition 3.5 and Lemma 3.3, all traces of the form $2 - D^2 y$ with $y \ne 0$ arise as trace invariants of generating pairs for PSL(2, q).

4. Proof of the T-system Theorem

We turn now to *T*-equivalence. Denoting by Ψ_q the number of orbits of the action of $\operatorname{Aut}(\mathbb{F}_q)$ on \mathbb{F}_q , Theorem 2.1 tells us immediately which orbits consist of trace invariants, giving the following counts:

Corollary 4.1. The numbers of orbits of the Frobenius automorphism that occur as weak trace invariants of generating pairs of PSL(2,q) are as follows:

- i) If q = 2, q = 4, q = 8, or $q \ge 13$, then $\Psi_q 1$ orbits occur.
- ii) If q = 3, q = 9, or q = 11, then $\Psi_q 2$ orbits occur.
- iii) If q = 5 or q = 7, then $\Psi_q 3$ orbits occur.

In the remainder of this section, we will prove that

$$\Psi_q = \frac{1}{s} \sum_{r|s} \varphi(s/r) \, p^r$$

The *T*-system Theorem then follows directly from Corollary 4.1.

This formula for Ψ_q is surely well-known, although we have not found an explicit statement in the literature. Experts in finite fields (we thank, in particular, H. Niederreiter) observe that the number of orbits is the same as the number of monic irreducible polynomials over \mathbb{F}_p of degree dividing s, each orbit being the set of roots of one such polynomial. Consequently, the number e(r) of orbits with r elements (which equals the number of monic irreducible polynomials of degree r) satisfies $q = \sum_{r|s} re(r)$, and a

formula for e(s) can be obtained using Möbius inversion (see for example [10, Ch. III.2]). In fact the formula for e(s) is the same as our formula for Ψ_q but with φ replaced by the Möbius function μ . Summing these for r dividing s and then manipulating using the fact (also a consequence of Möbius inversion) that $\frac{\varphi(s)}{s} = \sum_{r|s} \frac{\mu(r)}{r}$ gives the formula for Ψ_q . Rather than writing out the details of that, or worse yet, leaving them to the reader, we will present here an elegant proof shown to us by Gareth Jones, that deduces the formula for Ψ_q in a few lines using Burnside's Lemma and a few of the most elementary properties of \mathbb{F}_q .

Burnside's Lemma says that the number of orbits of a finite group acting on a finite set equals the average number of fixed points of the elements of the group:

Lemma 4.2 (Burnside's Lemma). If a finite group G acts on a finite set Ω , then the number of orbits is given by

$$\frac{1}{|G|} \sum_{g \in G} \pi(g)$$

where $\pi(g)$ is the number of points fixed by g.

Burnside's Lemma can be proven by elementary counting arguments (see for example [1]), and a better name for it is the Burnside-Cauchy-Frobenius formula (see [12]).

Recall that $\operatorname{Aut}(\mathbb{F}_q)$ is a cyclic group generated by the Frobenius automorphism Φ that sends each x to x^p . Also, \mathbb{F}_{p^r} occurs as a subfield of \mathbb{F}_{p^s} if and only if r|s, and that it is the unique subfield of this order.

To obtain the formula for Ψ_q , we will apply Burnside's Lemma with $\Omega = \mathbb{F}_{p^s}$ and $G = \operatorname{Aut}(\mathbb{F}_{p^s})$. Each element Φ^m of G has order s/r, where $r = \operatorname{gcd}(m, s)$, and there are $\varphi(s/r)$ elements of this order for each divisor r of s. Such an element has the same fixed points as Φ^r , since each is a power of the other, and the fixed points of Φ^r are the roots of the polynomial $x^{p^r} - x$. These roots form the subfield F_{p^r} , so $\pi(\Phi^m) = p^r$. Burnside's Lemma now yields the formula for Ψ_q .

The same argument, with q in the role of p, shows that for any prime power q, the number of orbits of the action of the Galois group $\operatorname{Aut}_{\mathbb{F}_q} \mathbb{F}_{q^s}$ on \mathbb{F}_{q^s} is $\frac{1}{s} \sum_{s \to s} \varphi(s/r) q^r$.

Since Φ has order s, the ceiling $\lceil \frac{q}{s} \rceil$ is trivially a lower bound for the number Ψ_q of orbits of $\operatorname{Aut}(\mathbb{F}_q)$, and since Φ fixes each element of the subfield \mathbb{F}_p , $\lceil \frac{q-p}{s} \rceil + p$ is an obvious lower bound. It gives the exact count whenever s is prime (or s = 1), since then all orbits contain s elements except those in the subfield \mathbb{F}_p . But even for composite s this bound is very accurate, apart from a few small values of q, because the vast majority of elements of \mathbb{F}_q do not lie in any proper subfield and consequently almost all orbits have s elements. For example, using GAP [6] we find that for $\Psi_{2^{30}} = 35,792,568$,

the bound of 35, 791, 397 is approximately 99.9967% of the exact value, while the bound of 29, 484, 565, 267, 122, 446 is approximately 99.99999984% of $\Psi_{29^{16}} = 29, 484, 565, 316, 813, 125.$

References

- Kenneth P. Bogart, An obvious proof of Burnside's lemma, Amer. Math. Monthly 98 (1991), 927–928.
- R. Carter, Simple groups of Lie type, Reprint of the 1972 original, Wiley Classics Library, John Wiley & Sons, Inc., New York, 1989.
- 3. L. E. Dickson, Linear groups: with an exposition of the Galois field theory, Leipzig (1901), reprinted by Dover Publications, Inc., New York (1958).
- J. Dieudonné, On the automorphisms of the classical groups, with a supplement by Loo-Keng Hua, Mem. Amer. Math. Soc. 2 (1951), 1–122.
- 5. M. Evans, Ph. D. dissertation at University of Wales, 1985.
- 6. GAP: Groups, Algorithms, and Programming, available at the St. Andrews GAP website http://turnbull.mcs.st-and.ac.uk/~gap/.
- 7. S. Garion and A. Shalev, Commutator maps, measure preservation, and *T*-systems, arXiv:0708.3664.
- H. Glover and D. Sjerve, The genus of PSL₂(q), J. Reine Angew. Math. 380 (1987), 59–86.
- Loo-Keng Hua, On the automorphisms of the symplectic group over any field, Ann. of Math. (2) 49, (1948), 739–759.
- 10. R. Lidl and H. Niederreiter, *Introduction to finite fields and their applications*, Cambridge University Press, Cambridge, (1986).
- 11. D. McCullough, GAP programs for Writing elements of PSL(2,q) as commutators, available at www.math.ou.edu/~dmccullough/
- 12. P. Neumann, A lemma which is not Burnside's, Math. Sci. 4 (1979), 133-141
- O. Schrier and B. L. van der Waerden, Die Automorphismen der projektiven Gruppen, Abh. Math. Sem. Univ. Hamburg 6 (1928), 303–322.
- 14. M. Suzuki, Group Theory, vol. I, Springer-Verlag, 1982.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF OKLAHOMA, NORMAN, OKLAHOMA 73019, USA

E-mail address: dmccullough@math.ou.edu *URL*: www.math.ou.edu/~dmccullough/

DEPARTMENTO DE MATEMATICA, UNIVERSIDADE FEDERAL DE PERNAMBUCO, AV. PROF. LUIZ FREIRE, S/N, CID. UNIVERSITARIA-RECIFE-PE, CEP 50.740-540, BRAZIL *E-mail address*: mvw@dmat.ufpe.br