LMS J. Comput. Math. 16 (2013) 419–423 © 2013 Author
doi:10.1112/S1461157013000193

The minimal generating sets of PSL$(2, p)$ of size four

Sebastian Jambor

Abstract

We show that there are only finitely many primes p such that PSL$(2, p)$ has a minimal generating set of size four.

Supplementary materials are available with this article.

1. *Introduction*

In [**12**], Saxl and Whiston determine upper bounds for the size of a minimax set of $\mathrm{L}_2(q) = \mathrm{PSL}(2, q)$; that is, the size of a minimal generating set of maximal cardinality. They prove that if $q = p$ is a prime, then a minimax set contains at most four elements, and if $p \not\equiv \pm 1 \mod 8$ and $p \not\equiv \pm 1 \mod 10$, then a minimax set contains exactly three elements. For only a small number of primes have minimax sets of $\mathrm{L}_2(p)$ of size four been computed. Recently, Nachman presented a proof that a minimax set contains exactly three elements if $p \not\equiv \pm 1 \mod 10$ and $p \neq 7$, and conjectured that there are only finitely many primes $p \equiv \pm 1 \mod 10$ that allow those extremal minimax sets [**9**]. In this paper, this conjecture is proved, along with a new proof of Nachman's result. Furthermore, a classification of the minimax sets of $\mathrm{L}_2(p)$ of size four is given. The result is as follows.

Theorem 1. *The group* $\mathrm{L}_2(p)$ *has a minimax set of size four if and only if* $p \in \{7, 11, 19, 31\}$. *More precisely, up to automorphisms there are two minimax sets of size four for* $\mathrm{L}_2(7)$, *fourteen for* $\mathrm{L}_2(11)$, *three for* $\mathrm{L}_2(19)$ *and one for* $\mathrm{L}_2(31)$.

The proof is computational, using traces of 2×2 matrices based on the ideas of the L_2-quotient algorithm (cf. [**10**]), as follows. The order of a 2×2-matrix with determinant 1 is uniquely determined by its trace if the order is coprime to the characteristic of the underlying field. Furthermore, the traces of products of 2×2 matrices with determinant 1 satisfy certain polynomial relations that are independent of the prime p (cf. [**3, 4, 6, 10**]). Thus by classifying the orders of the elements in a minimax set and of certain products, we get polynomial conditions on the traces, which can only be satisfied in the characteristics given in the theorem.

We use the notation and results of [**12**]: let $G = \mathrm{L}_2(p)$ for a prime $p > 5$ and let $M(G) = \{g_1, g_2, g_3, g_4\} \subseteq G$ be a minimax set of size four. Set $H_i := \langle M(G) - \{g_i\} \rangle$ for $i = 1, \ldots, 4$. Then every H_i is isomorphic to A_5, S_4 or a dihedral group, and at least two of the H_i are isomorphic to A_5 or S_4 (cf. [**12**]). (It is easy to see that no H_i can be isomorphic to a point stabilizer, that is, a subgroup of $\mathrm{C}_p \rtimes \mathrm{C}_{(p-1)/2}$, since at least two H_i are isomorphic to A_5 or S_4. Cf. also [**9**].)

In the following, we will always assume that H_3 and H_4 are isomorphic to A_5 or S_4.

2. *Restricting possible orders*

Note that $M(G) - \{g_i\}$ is a minimax set of H_i, and it is easy to classify the minimax sets of A_5 and S_4; for example, using GAP [**5**] or Magma [**2**]. In particular, all g_i have order 2 or 3.

Received 20 November 2012; revised 7 June 2013.

2010 Mathematics Subject Classification 20E34, 20G40.

The author was supported by the Alexander von Humboldt Foundation via a Feodor Lynen Research Fellowship.

Lemma 2. *Let H_1 be a dihedral group. Then $|g_ig_j| \leqslant 6$ for $2 \leqslant i < j \leqslant 4$ and $|g_2g_3g_4| \in \{2, 6, 10, 12, 15\}$.*

Proof. The element g_ig_j is contained in the group H_k for some $2 \leqslant k \leqslant 4$. If H_k is isomorphic to A_5 or S_4, then $|g_ig_j| \leqslant 5$. Now assume that H_k is a dihedral group. Recall that an element of a dihedral group is called a rotation if it is contained in the cyclic subgroup of index two, and a reflection otherwise. If g_i and g_j are both rotations, then $|g_ig_j| \leqslant 6$, since $|g_i|, |g_j| \leqslant 3$; if precisely one of g_i and g_j is a reflection, then g_ig_j is a reflection, hence of order 2. Finally, if both g_i and g_j are reflections with $g_i \neq g_j$, then the group $\langle g_i, g_j\rangle$ is not cyclic, so by the proof of [**12**, Lemma 1] it is elementary abelian of order 4, hence $|g_ig_j| = 2$. This concludes the proof that $|g_ig_j| \leqslant 6$. To bound the order of $g_2g_3g_4$, note that if $\{g_2, g_3, g_4\}$ contains an odd number of reflections, then the product $g_2g_3g_4$ is also a reflection, hence of order 2. Otherwise, $g_2g_3g_4$ is a product of two rotations of restricted orders, and the result easily follows. □

Corollary 3. *Let $\{g_1, \dots, g_4\} \subseteq L_2(p)$ be a minimax set of size four for some prime p. There are only finitely many possibilities for the orders of the elements g_i for $1 \leqslant i \leqslant 4$, g_ig_j for $i < j \leqslant 4$ and $g_ig_jg_k$ for $j < k \leqslant 4$.*

All of these possibilities can be easily computed.

3. *Restricting possible traces*

The L_2-quotient algorithm [**10**] uses the fact that an absolutely irreducible representation of the free group on two generators over $\mathbb{F}_q$ is uniquely determined by three traces, up to equivalence. For four matrices, more traces are needed, but the same principles hold.

Definition 4. For a quadruple $m = (m_1, \dots, m_4) \in SL(2, q)^4$ of matrices, let

$$t_m := (t_1, t_2, t_3, t_4, t_{12}, t_{13}, t_{14}, t_{23}, t_{24}, t_{34}, t_{123}, t_{124}, t_{134}, t_{234}) \in \mathbb{F}_q^{14},$$

where $t_i := \operatorname{tr}(m_i)$, $t_{ij} := \operatorname{tr}(m_im_j)$ and $t_{ijk} := \operatorname{tr}(m_im_jm_k)$ for $1 \leqslant i \leqslant 4$, $i < j \leqslant 4$ and $j < k \leqslant 4$. We call t_m the *trace tuple* of m. Conversely, if $t \in \mathbb{F}_q^{14}$ and $m = (m_1, \dots, m_4) \in SL(2, q)^4$ are matrices with $t_m = t$, we call m a *realization* of t.

Proposition 5. *Let q be an odd prime power and $t \in \mathbb{F}_q^{14}$ with realization $m \in SL(2, q)^4$ such that $\langle m_1, \dots, m_4\rangle$ is absolutely irreducible. Then m is unique up to conjugation by an element in* $GL(2, q)$.

Proof. Let w be a word in $m_1, \dots, m_4$. If w has length $\geqslant 4$, then by Procesi's theorem [**11**], $\operatorname{tr}(w)$ can be expressed as a polynomial in traces of words of smaller length (this uses the fact that q is odd). Furthermore, $\operatorname{tr}(m_im_j) = \operatorname{tr}(m_jm_i)$, and $\operatorname{tr}(m_im_km_j)$ can be written as a polynomial in $\operatorname{tr}(m_im_jm_k)$ and traces of words of smaller length (cf. for example [**6**]). Hence the trace of all elements in $\langle m_1, \dots, m_4\rangle$ is uniquely determined by t. Since $\langle m_1, \dots, m_4\rangle$ is finite and absolutely irreducible, it is uniquely determined by its $\mathbb{F}_q$-valued character, up to equivalence. □

(This statement can be proved in a more general form; cf. [**8**].)

Not every 14-tuple of field elements has a realization. The reason is that the traces satisfy certain polynomial relations.

Let $R := \mathbb{Z}[1/2][x_1, x_2, x_3, x_4, x_{12}, x_{13}, x_{14}, x_{23}, x_{24}, x_{34}, x_{123}, x_{124}, x_{134}, x_{234}]$, where the x_i, x_{ij}, x_{ijk} are indeterminates over $\mathbb{Z}[1/2]$. Furthermore, define $y_{ii} := x_i^2/2 - 2$, $y_{ji} := y_{ij} := x_{ij} - x_ix_j/2$ and $y_{ijk} := 2x_{ijk} + x_ix_jx_k - x_ix_{jk} - x_jx_{ik} - x_kx_{ij}$ for $1 \leqslant i \leqslant 4$, $i < j \leqslant 4$, $j < k \leqslant 4$.

PROPOSITION 6 [4, Theorem 2.3]. *Let q be an odd prime power. For every $m \in \mathrm{SL}(2, q)^4$, the trace tuple t_m is a zero of the polynomials*

$$y_{i_1 i_2 i_3} y_{j_1 j_2 j_3} + 2 \det \begin{pmatrix} y_{i_1 j_1} & y_{i_1 j_2} & y_{i_1 j_3} \\ y_{i_2 j_1} & y_{i_2 j_2} & y_{i_2 j_3} \\ y_{i_3 j_1} & y_{i_3 j_2} & y_{i_3 j_3} \end{pmatrix} \in R$$

for $1 \leqslant i_1 < i_2 < i_3 \leqslant 4$, $1 \leqslant j_1 < j_2 < j_3 \leqslant 4$ and

$$y_{i1} y_{234} - y_{i2} y_{134} + y_{i3} y_{124} - y_{i4} y_{123} \in R$$

for $1 \leqslant i \leqslant 4$.

Drensky proves this result for algebraically closed fields of characteristic zero. However, by taking preimages of the m_i over an extension $\mathcal{O}$ of $\mathbb{Z}$ and embedding $\mathcal{O}$ in an algebraically closed field, the result also holds for matrices over finite fields.

Further restrictions on the traces can be imposed by prescribing the order of certain elements, using the following connection between orders and traces.

REMARK 7. For $m \in \mathbb{N}$, denote by $\Psi_m \in \mathbb{Z}[x]$ the minimal polynomial of $\zeta_m + \zeta_m^{-1}$, where ζ_m is a primitive mth root of unity. If $A \in \mathrm{SL}(2, q)$ is an element of finite order $m > 2$, then $\Psi_m(\mathrm{tr}(A)) = 0$.

If $a \in \mathrm{L}_2(q)$ has order ℓ and $A \in \mathrm{SL}(2, q)$ is a preimage, then A has order 2ℓ if ℓ is even and order ℓ or 2ℓ if ℓ is odd.

DEFINITION 8. For $\omega = (\omega_1, \omega_2, \omega_3, \omega_4, \omega_{12}, \omega_{13}, \omega_{14}, \omega_{23}, \omega_{24}, \omega_{34}, \omega_{123}, \omega_{124}, \omega_{134}, \omega_{234}) \in \mathbb{N}^{14}$, let

$$I_\omega := \langle \Psi_{2\omega_j}(x_j) \mid \omega_j \text{ even} \rangle + \langle \Psi_{\omega_j}(x_j) \Psi_{2\omega_j}(x_j) \mid \omega_j \text{ odd} \rangle + J \trianglelefteq R,$$

where j runs over all possible indices and J is the ideal generated by the polynomials in Proposition 6.

REMARK 9. Let $\omega \in \mathbb{N}^{14}$.

(i) If $g = (g_1, \ldots, g_4) \in \mathrm{L}_2(q)^4$ with $|g_i| = \omega_i$, $|g_i g_j| = \omega_{ij}$, $|g_i g_j g_k| = \omega_{ijk}$ for some q and $m = (m_1, \ldots, m_4) \in \mathrm{SL}(2, q)^4$ are preimages of the g_i, then the trace tuple t_m is a zero of I_ω. Conversely, if $t \in \mathbb{F}_q^{14}$ is a zero of I_ω for some q and $m = (m_1, \ldots, m_4) \in \mathrm{SL}(2, q)^4$ is a realization of t, then $|g_i| = \omega_i$, $|g_i g_j| = \omega_{ij}$, $|g_i g_j g_k| = \omega_{ijk}$, where the g_i are images of the m_i in $\mathrm{L}_2(q)$.

(ii) Let $\overline{R} := R/I_\omega$. Every maximal ideal $M \trianglelefteq \overline{R}$ yields a zero $t = (t_1, \ldots, t_{234}) \in \mathbb{F}_q^{14}$ of I_ω, where $\mathbb{F}_q = \overline{R}/M$ is the residue class field of M, by setting $t_j := \overline{x_j} + M$. This defines a bijection between the maximal ideals of $\overline{R}$ and $\mathrm{Gal}(\mathbb{F}_q)$-orbits of zeroes $t \in \mathbb{F}_q^{14}$ of I_ω, where q ranges over all prime powers. The maximal ideals of $\overline{R}$ are in bijection to maximal ideals of R that contain I_ω, and a maximal ideal $M \trianglelefteq R$ contains I_ω if and only if it contains a minimal associated prime ideal of I_ω. In particular, if all associated prime ideals are maximal, then $\overline{R}$ has only finitely many maximal ideals.

For the background on commutative algebra, see [1, Chapter 4]. The minimal associated prime ideals can be computed using [7].

4. *Proof of Theorem 1*

The proof of Theorem 1 works by running through all order tuples ω of Corollary 3 and computing the minimal associated prime ideals of I_ω. For every minimal associated prime ideal that is maximal, compute the unique zero $t \in \mathbb{F}_q^{14}$ (where $\mathbb{F}_q$ is the residue class field of the

https://doi.org/10.1112/S1461157013000193 Published online by Cambridge University Press

maximal ideal) and check whether t has a realization (this can be done using the methods in [10] and the trace bilinear form). If a realization exists, check whether it yields a minimax set.

Example 10. Assume that $H_1 \cong H_2 \cong S_4$ and $H_3 \cong H_4 \cong A_5$. Let $\{h_1, h_2, h_3\}$ be a minimax set of S_4 or A_5 and $\ell := (|h_1|, |h_2|, |h_3|, |h_1h_2|, |h_1h_3|, |h_2h_3|, |h_1h_2h_3|)$. Then there are 37 possibilities for ℓ in the case of S_4 and 62 possibilities for A_5. Together, they yield 34 possibilities for the order tuples ω. We take a closer look at two of those 34 possibilities.

(i) Let $\omega = (2, 2, 2, 2, 3, 3, 2, 2, 3, 5, 4, 4, 5, 5)$. Then I_ω has four minimal associated primes, namely

$$\begin{aligned}&\langle 31, x_1, x_2, x_3, x_4, x_{12} - 1, x_{13} - 1, x_{14}, x_{23}, x_{24} - \delta_1\delta_2, x_{34} + 12\delta_1\delta_2,\\&\quad x_{123} + 8\delta_1, x_{124} + 8\delta_2, x_{134} + 13\delta_2, x_{234} + 13\delta_2\rangle \trianglelefteq R\end{aligned}$$

with $\delta_1, \delta_2 \in \{\pm 1\}$. Hence there are exactly four zeroes of I_ω, all defined in characteristic 31. Possible realizations are given by the matrices

$$m_1 = \delta_1 \begin{pmatrix} 0 & 30 \\ 1 & 0 \end{pmatrix}, \quad m_2 = \delta_1 \begin{pmatrix} 20 & 2 \\ 1 & 11 \end{pmatrix}, \quad m_3 = \delta_1 \begin{pmatrix} 6 & 24 \\ 23 & 25 \end{pmatrix}, \quad m_4 = \delta_2 \begin{pmatrix} 20 & 23 \\ 23 & 11 \end{pmatrix},$$

and each quadruple of matrices yields the same quadruple of elements in $L_2(31)$. It can be easily checked that these elements form a minimax set having the desired subgroups H_i.

(ii) For $\omega = (2, 2, 2, 2, 2, 3, 3, 3, 3, 5, 4, 4, 3, 3)$, the ideal I_ω contains the prime 2. Thus I_ω only has zeroes in characteristic 2, which are not relevant to our problem.

It can happen that I_ω has non-maximal associated primes. In this case, I_ω has zeroes in every characteristic. As it turns out, this happens only if the orders ω come from a configuration where all H_i are isomorphic to S_4 or all are isomorphic to A_5. In these cases, there exist quadruples of elements in S_4 (or in A_5) such that every three-tuple is a minimax set of S_4 (or A_5). Since S_4 and A_5 have representations of degree 2 in every characteristic, these degenerate sets account for infinitely many zeroes of I_ω, that is, the prime ideal of dimension 1, which can therefore be disregarded.

To get a classification of the minimax sets under the automorphism group, note that all quadruples $(\delta_1 m_1, \ldots, \delta_4 m_4)$ with $\delta_i \in \{\pm 1\}$ yield the same quadruple of projective elements. Furthermore, the ordering of the matrices is irrelevant. The actions of $\{\pm 1\}^4$ and S_4 on quadruples of matrices induce an action of $\{\pm 1\}^4 \rtimes S_4$ on the trace tuples, so the automorphism classes of minimax sets correspond to $\{\pm 1\}^4 \rtimes S_4$-orbits of trace tuples.

5. *Source files*

All computations have been done in Magma; the source files are supplied as add-ons to this paper and are available from the publisher's website.

Acknowledgement. I thank the anonymous referee for several helpful comments.

References

1. M. F. Atiyah and I. G. Macdonald, *Introduction to commutative algebra* (Addison-Wesley, Reading, MA, 1969).
2. W. Bosma, J. Cannon and C. Playoust, 'The Magma algebra system. I. The user language', *J. Symbolic Comput.* 24 (1997) 235–265; Computational algebra and number theory (London, 1993).
3. S. Donkin, 'Invariants of several matrices', *Invent. Math.* 110 (1992) 389–401.
4. V. Drensky, 'Defining relations for the algebra of invariants of 2 × 2 matrices', *Algebr. Represent. Theory* 6 (2003) 193–214.
5. The GAP group, 'GAP – groups, algorithms, and programming, Version 4.4.12', 2008.

https://doi.org/10.1112/S1461157013000193 Published online by Cambridge University Press

6. R. D. HOROWITZ, 'Characters of free groups represented in the two-dimensional special linear group', *Comm. Pure Appl. Math.* 25 (1972) 635–649.
7. S. JAMBOR, 'Computing minimal associated primes in polynomial rings over the integers', *J. Symbolic Comput.* 46 (2011) 1098–1104.
8. S. JAMBOR, 'An L_3-U_3-quotient algorithm for finitely presented groups', PhD Thesis, RWTH Aachen University, 2012.
9. B. NACHMAN, 'Generating sequences of PSL$(2, p)$', Preprint, 2012, arXiv:1210.2073 [math.GR].
10. W. PLESKEN and A. FABIAŃSKA, 'An L_2-quotient algorithm for finitely presented groups', *J. Algebra* 322 (2009) 914–935.
11. C. PROCESI, 'The invariant theory of $n \times n$ matrices', *Adv. Math.* 19 (1976) 306–381.
12. J. WHISTON and J. SAXL, 'On the maximal size of independent generating sets of PSL$_2(q)$', *J. Algebra* 258 (2002) 651–657.

Sebastian Jambor
Department of Mathematics
The University of Auckland
Private Bag 92019
Auckland, New Zealand

s.jambor@auckland.ac.nz

https://doi.org/10.1112/S1461157013000193 Published online by Cambridge University Press