Glasgow Math. J. **55** (2013) 481–509. © Glasgow Mathematical Journal Trust 2013.
doi:10.1017/S0017089512000675.

NIELSEN EQUIVALENCE OF GENERATING PAIRS OF SL(2, q)

DARRYL MCCULLOUGH
Department of Mathematics, University of Oklahoma, Norman, OK 73019, USA
e-mail: dmccullough@math.ou.edu

and MARCUS WANDERLEY
Departmento de Matematica, Universidade Federal de Pernambuco, Av. Prof. Luiz Freire, s/n
Cid. Universitaria-Recife-PE, CEP 50.740-540, Brazil
e-mail: marcus@dmat.ufpe.br

(Received 14 December 2011; accepted 28 November 2012; first published online 25 February 2013)

Abstract. We present several conjectures which would describe the Nielsen equivalence classes of generating pairs for the groups SL(2, q) and PSL(2, q). The Higman invariant, which is the union of the conjugacy classes of the commutator of a generating pair and its inverse, and the trace of the commutator play key roles. Combining known results with additional work, we clarify the relationships between the conjectures, and obtain various partial results concerning them. Motivated by the work of Macbeath (A. M. Macbeath, Generators of the linear fractional groups, in *Number theory* (Proc. Sympos. Pure Math., vol. XII, Houston, TX, 1967) (American Mathematical Society, Providence, RI, 1969), 14–32), we use another invariant defined using traces to develop algorithms that enable us to verify the conjectures computationally for all q up to 101, and to prove the conjectures for a highly restricted but possibly infinite set of q.

1991 *Mathematics Subject Classification.* Primary 20F99, Secondary 20G40.

For a two-generator group, two generating pairs are called Nielsen equivalent if one can be obtained from the other by a sequence of operations of replacing one generator by one of its two products with the other or with the inverse of the other. The equivalence classes so obtained have been examined or used in both algebraic contexts [**2**, **5–7**, **8**, **27**, **29**, **30**, **33**] and topological ones [**14–19**, **23**, **25**].

Higman (see [**26**]) observed that the union of conjugacy classes of the commutator of the generators and its inverse forms an invariant of the Nielsen equivalence class. When the group is SL(2, q) or PSL(2, q) for some prime power q, all elements in these conjugacy classes have the same trace, giving an invariant of the Nielsen equivalence class which is a single element of the coefficient field $\mathbb{F}_q$ (note that the commutator of a pair of elements of PSL(2, q) is a well-defined element of SL(2, q)). The main result of [**23**] (stated there for PSL(2, q), but trivially extendible to SL(2, q)) tells precisely which elements occur as trace invariants.

TRACE THEOREM. *The elements of* $\mathbb{F}_q$ *that occur as trace invariants of generating pairs of* SL(2, q) *are as follows*:

i) *For* $q = 2$, $q = 4$, $q = 8$ *and all* $q > 11$, *all elements except* 2 *occur.*
ii) *For* $q = 3$, $q = 9$ *and* $q = 11$, *all elements except* 1 *and* 2 *occur.*

iii) *For $q = 5$, only* 1 *and* 3 *occur.*
iv) *For $q = 7$, all elements except* 0, 1 *and* 2 *occur.*

Thus, apart from a few exceptional values of q, all elements of $\mathbb{F}_q$ other than 2 occur as trace invariants of generating pairs. Understanding the Nielsen equivalence classes then becomes a matter of determining the number of classes that share a given trace invariant. That is the overall goal of this work.

1. A conjectural picture of Nielsen equivalence in $\mathrm{SL}(2, q)$**.** In this section we give an overview of the work in this paper, which develops a conjectural picture of Nielsen equivalence in $\mathrm{SL}(2, q)$ (and $\mathrm{PSL}(2, q)$), and that of a related action of the modular group on triples of elements of $\mathbb{F}_q$. As we present the conjectures, we mention several of our results and explain which parts of the overall picture they verify or support. Finally, we will outline the sections of the paper.

Two ordered pairs of elements of a group K are called equivalent if they are related by a sequence of operations of replacing one element of the pair by one of its products with the other element or its inverse. That is, (A, B) is equivalent to (A, AB), $(A, A^{-1}B)$, (A, BA) and (A, BA^{-1}), as well as to (AB, B), (AB^{-1}, B), (BA, B) and $(B^{-1}A, B)$. These imply that (A, B) is equivalent to (A^{-1}, B), (A, B^{-1}) and (B, A). A convenient alternative definition can be given by regarding a pair (A, B) as an element $\rho_{(A,B)}$ of $\mathrm{Hom}(F_2, K)$, where F_2 is free on two generators a and b and $(\rho_{(A,B)}(a), \rho_{(A,B)}(b)) = (A, B)$. From this viewpoint, equivalence corresponds to being in the same orbit under the left $\mathrm{Aut}(F_2)$-action defined by $\phi \cdot \rho_{(A,B)} = \rho_{(A,B)} \circ \phi^{-1}$.

Equivalence restricts to an equivalence relation on the (possibly empty) set $\mathcal{G}_2(K)$ of generating pairs of K, called *Nielsen equivalence.* The equivalence classes are called *Nielsen classes,* and the set of Nielsen classes is denoted by $\mathcal{N}$.

For an element $x \in K$, the *extended conjugacy class* of x is the union of the conjugacy classes of x and x^{-1}. Sending the generating pair (A, B) to the extended conjugacy class of the commutator $[A, B] = ABA^{-1}B^{-1}$ defines a well-known invariant of Nielsen equivalence called the *Higman invariant.* We regard the Higman invariant as a function $H\colon \mathcal{N} \to \mathcal{E}$, where $\mathcal{E}$ is the set of extended conjugacy classes of K.

From now on, we specialize to the case when K is $\mathrm{SL}(2, q)$. The field with q elements will be denoted by $\mathbb{F}_q$. The trace function induces a function $\mathrm{tr} \circ H\colon \mathcal{N} \to \mathbb{F}_q - \{2\}$, which is the trace invariant mentioned in the introduction.

Our main conjecture says that for $\mathrm{SL}(2, q)$ the Higman invariant is a complete invariant of Nielsen equivalence.

Classification Conjecture *(Higman invariant classifies Nielsen classes).* $H\colon \mathcal{N} \to \mathcal{E}$ is injective.

That is, two generating pairs (A, B) and (A', B') of $\mathrm{SL}(2, q)$ are Nielsen equivalent if and only if $[A, B]$ is conjugate to $[A', B']$ or $[B', A']$. Corollary 5.4 tells the image of H, and consequently the Classification Conjecture gives a full classification of Nielsen classes.

By Corollary 5.6, the Classification Conjecture is equivalent to the following assertion.

Trace Conjecture *(Trace invariant is nearly bijective).* The trace invariant $\mathrm{tr} \circ H\colon \mathcal{N} \to \mathbb{F}_q - \{2\}$ is injective except that it is two-to-one on the pre-image of -2 when $q \equiv 1 \bmod 4$ and $q \neq 9$.

https://doi.org/10.1017/S0017089512000675 Published online by Cambridge University Press

The Trace Theorem shows that tr $\circ H$ is surjective except for $q = 3, 5, 7, 9$ and 11, which are called the *exceptional* q. Thus, apart from the exceptional q, the Classification Conjecture implies that the trace invariant is bijective except that it is two-to-one on the pre-image of -2 when $q \equiv 1 \bmod 4$.

For some applications, Nielsen equivalence is too strong an invariant. More natural is to extend the action of $\mathrm{Aut}(F_2)$ on $\mathrm{Hom}(F_2, G)$ to an action of $\mathrm{Aut}(G) \times \mathrm{Aut}(F_2)$ by letting $(\alpha, \phi) \cdot \rho_{(A,B)} = \alpha \circ \rho_{(A,B)} \circ \phi^{-1}$. The resulting equivalence classes of generating pairs are called *T-systems.* As we explain in Section 4, there is a version of trace invariant that sends each element of the set $\mathcal{T}$ of T-systems to an element of the set $\mathcal{O}_q$ of $\mathrm{Aut}(\mathbb{F}_q)$-orbits of $\mathbb{F}_q$, providing a corresponding version of the Classification Conjecture.

T-Classification Conjecture *(Weak trace invariant classifies T-systems).* For non-exceptional q, the weak trace invariant is a bijection from $\mathcal{T}$ to $\mathcal{O}_q - \{\{2\}\}$.

Corollary 5.7 shows that the Classification Conjecture implies the T-Classification Conjecture.

As we will discuss in some depth in Section 12, we have verified the Classification Conjecture computationally for all $q \leq 101$. In Section 18, using information developed in Sections 13 through 17, we will also verify it for the (almost laughably restrictive, but conceivably infinite) class of all q such that $q - 1$ is prime and $q + 1$ has the form $3p_1$ for some prime p_1.

The *trace* of a pair (A, B) of elements of $\mathrm{SL}(2, q)$ is the ordered triple of elements of $\mathbb{F}_q$ defined by

$$\mathrm{Tr}(A, B) = (\mathrm{tr}(A), \mathrm{tr}(B), \mathrm{tr}(AB)).$$

A result of Macbeath, Theorem 7.1 in this paper, shows that $\mathrm{Tr}\colon \mathrm{SL}(2, q) \times \mathrm{SL}(2, q) \to \mathbb{F}_q^3$ is surjective. A triple is called *essential* when it is the trace of a generating pair.

If we regard $\mathrm{SL}(2, q) \times \mathrm{SL}(2, q)$ as $\mathrm{Hom}(F_2, \mathrm{SL}(2, q))$, then via the trace function the left action of $\mathrm{Aut}(F_2)$ induces a left action of $\mathrm{Aut}(F_2)$ on $\mathbb{F}_q^3$, whose orbits are called *Markov equivalence classes.* Explicitly, Markov equivalence is the relation generated by permutations of three coordinates together with the relation that $(\alpha, \beta, \gamma) \sim (\alpha, \beta, \alpha\beta - \gamma)$. Since the action of $\mathrm{Aut}(F_2)$ on $\mathbb{F}_q^3$ is induced from the action on $\mathrm{Hom}(F_2, \mathrm{SL}(2, q))$ whose orbits are the Nielsen classes $\mathcal{N}$, there is a well-defined trace function

$$\mathrm{Tr}\colon \mathcal{N} \to \mathcal{M}$$

from $\mathcal{N}$ to the set $\mathcal{M}$ of Markov (equivalence) classes of essential triples.

The *Fricke polynomial* $Q\colon \mathbb{F}_q^3 \to \mathbb{F}_q$ is defined by

$$Q(\alpha, \beta, \gamma) = \alpha^2 + \beta^2 + \gamma^2 - \alpha\beta\gamma - 2.$$

A straightforward calculation shows that $\mathrm{tr}([A, B]) = Q(\mathrm{Tr}(A, B))$. As shown in Proposition 8.5, the following conjecture about Q is implied by the Classification Conjecture.

Q-Classification Conjecture $Q\colon \mathcal{M} \to \mathbb{F}_q - \{2\}$ *is injective.*

https://doi.org/10.1017/S0017089512000675 Published online by Cambridge University Press

In summary, the Classification Conjecture implies that, apart from the exceptional values of q, the functions H and Q in the commutative diagram

$$\begin{array}{ccc} \mathcal{N} & \xrightarrow{H} & \mathcal{C} \\ {\scriptstyle \mathrm{Tr}}\downarrow & & \downarrow{\scriptstyle \mathrm{tr}} \\ \mathcal{M} & \xrightarrow{Q} & \mathbb{F}_q - \{2\} \end{array}$$

are bijections. Proposition 5.2 shows that $\mathrm{tr}\colon \mathcal{C} \to \mathbb{F}_q - \{2\}$ is a bijection except that it is two-to-one on the pre-image of -2 when $q \equiv 1 \bmod 4$, so the Classification Conjecture is equivalent to Q-Classification Conjecture together with the assertion that $\mathrm{Tr}\colon \mathcal{N} \to \mathcal{M}$ is bijective except that it is two-to-one on the pre-image of $Q^{-1}(-2)$ when $q \equiv 1 \bmod 4$.

In Section 7 we will present results of Macbeath [**20**] that show that if M is a Markov class then $\mathrm{Tr}^{-1}(M)$ consists of at most two Nielsen classes. We can say a bit more: Theorem 10.1 shows that if $2 - Q(M)$ is not a square in $\mathbb{F}_q$, then $\mathrm{Tr}^{-1}(M)$ is a single Nielsen class.

Macbeath's results [**20**] also show that Tr is a bijection when q is even. Using the fact that tr is also a bijection when q is even, we see in Corollary 8.4 that for even q, the Q-Classification Conjecture is equivalent to the Classification Conjecture.

As will be discussed in Section 19, the Classification Conjecture, and each of our other main conjectures, implies a corresponding assertion for the case of $\mathrm{PSL}(2, q)$, while the corresponding assertion implies a weak form of the conjecture.

Here is a brief outline of the exposition. Sections 2–4 give definitions, some background material and careful statements of the Classification and T-Classification Conjectures. Section 5 compiles useful information about the conjugacy classes in $\mathrm{SL}(2, q)$, and uses it to verify that the Classification Conjecture is equivalent to the Trace Conjecture and implies the T-Classification Conjecture. Dickson's classification [**3**] of the subgroups of $\mathrm{PSL}(2, q)$ and some of Macbeath's results on generating pairs of $\mathrm{SL}(2, q)$ are stated in Sections 6 and 7. More of Macbeath's results are used in Section 8 to obtain the results about the trace function, $\mathrm{Tr}\colon \mathcal{N} \to \mathcal{M}$ that were summarized above.

Section 9 reviews the classification of elements of $\mathbb{F}_q$ into parabolic, hyperbolic and elliptic types that plays a major role in the remainder of the paper. In Section 10, we develop the so-called Fundamental Equation, and use it to show that $\mathrm{Tr}^{-1}(M)$ consists of a single element when $2 - Q(M)$ is a square in $\mathbb{F}_q$.

Our computational verification of the Classification Conjecture for $q \leq 101$ is detailed in Section 12. It requires the ability to identify the essential triples, that is, the elements of $\mathbb{F}_q^3$ that are the image under Tr of a generating pair of $\mathrm{SL}(2, q)$. We provide this in Section 11, which is heavily indebted to Macbeath's work.

Sections 13 through 17 are a more detailed examination of the $\mathrm{Aut}(F_2)$-action on essential triples. This leads to the proof in Section 18 of the Classification Conjecture in the highly restricted case when one of $q + 1$ or $q - 1$ is prime and the other is three times a prime. The details are rather complicated, but we hope the effort will someday be justified by further progress, at least for even q. The restriction to even q arises initially because of the characterization of the hyperbolic elements of $\mathbb{F}_q$, Lemma 15.1, for which no analogue is apparent in odd characteristic.

https://doi.org/10.1017/S0017089512000675 Published online by Cambridge University Press

A possible reason for caution about the conjectures arises in Section 18, where a very important role is played by the 'transitive' elements of $\mathbb{F}_q - \{0\}$, which are the traces of matrices of large orders $q-1$ or $q+1$. For very large q, the proportion of such elements may become arbitrarily small, much smaller than in the cases $q \leq 101$ that we have checked computationally or the cases where $q-1$ and $q+1$ satisfy the very strong primeness assumptions. So in this possibly relevant sense the cases for which the conjectures are known are not representatives of the general case. While this does not suggest that the conjectures are likely to fail, it does say that the accumulated evidence for them may not be as strong as it appears.

Finally, in Section 19 we explain how to adapt our work to PSL(2, q).

The authors are greatly appreciative of the referee's thorough and thoughtful reading of the manuscript. In addition to helping us correct some seriously misleading wording in Section 12, the referee's comments resulted in numerous improvements to our work.

2. Nielsen equivalence. For the free group F_2 on two generators a and b, it is known that $\mathrm{Aut}(F_2)$ is generated by the three involutions defined by

(1) $r(a) = a^{-1}$, $r(b) = b$,
(2) $s(a) = b$, $s(b) = a$,
(3) $t(a) = a^{-1}$, $t(b) = ab$,

where (a, b) is the fixed ordered basis of F_2. One way to see this is to check that Nielsen's standard generators of $\mathrm{Aut}(F_2)$ [**28**] can be written as compositions of these involutions.

Let K be a group. There is a left $\mathrm{Aut}(F_2)$-action on $\mathrm{Hom}(F_2, K) = K \times K$ defined by $\phi \cdot \rho = \rho \circ \phi^{-1}$. Identifying the representation in $\mathrm{Hom}(F_2, K)$ that sends a to A and b to B with the pair $(A, B) \in K \times K$, the corresponding actions of r, s and t on pairs in $K \times K$ are

(1) $r(A, B) = (A^{-1}, B)$,
(2) $s(A, B) = (B, A)$,
(3) $t(A, B) = (A^{-1}, AB)$.

We define two pairs in $K \times K$ to be *equivalent* when they lie in the same orbit for this $\mathrm{Aut}(F_2)$-action. One can check that two pairs are equivalent if and only if each can be obtained from the other by a sequence of operations of replacing an element by its inverse, or pre- or post-multiplying one element by the other or the inverse of the other, or by interchanging the two elements (since these are the effects of the standard generators of $\mathrm{Aut}(F_2)$).

It is not easy to find invariants of equivalence, but two basic ones are obvious. For a pair (A, B) in $K \times K$, denote by $\langle A, B\rangle$ the subgroup of K generated by $\{A, B\}$.

LEMMA 2.1. *Suppose that* (A, B) *and* (A', B') *are equivalent pairs in* $K \times K$.
(i) $\langle A, B\rangle = \langle A', B'\rangle$.
(ii) *If* $X \in \langle A, B\rangle$, *then* (XAX^{-1}, XBX^{-1}) *is equivalent to* (A, B).

Proof. Part (i) is immediate since for ρ in $\mathrm{Hom}(F_2, K)$ and $\phi \in \mathrm{Aut}(F_2)$, the images of ρ and $\rho \circ \phi^{-1}$ are equal. For part (ii), given a representation ϕ sending (a, b) to (A, B) and X in the subgroup of K generated by $\{A, B\}$, choose $x \in F_2$ such that $\phi(x) = X$. For the inner automorphism $\mu(x^{-1})$ of F_2 sending w to $x^{-1}wx$, we then have $\mu(x^{-1}) \cdot (A, B) = (XAX^{-1}, XBX^{-1})$. □

By Lemma 2.1(i), if a pair lies in the set $\mathcal{G}_2(K)$ of generating pairs, then so too does any equivalent pair, and consequently equivalence restricts to an equivalence relation

on $\mathcal{G}_2(K)$ called *Nielsen equivalence.* An equivalence class of generating pairs is called a *Nielsen class,* and the set of Nielsen classes is denoted by $\mathcal{N}$.

3. The Higman invariant.

DEFINITION 3.1. Let $g \in K$. The *extended conjugacy class of* g is the union of the conjugacy classes of g and g^{-1}. The set of extended conjugacy classes of elements of K is denoted by $\mathcal{E}$.

Define $H\colon\ \mathcal{G}_2(K) \to \mathcal{E}$ by sending (A, B) to the extended conjugacy class of $[A, B]$. This is well defined on Nielsen classes, so induces a function $H\colon \mathcal{N} \to \mathcal{E}$, called the *Higman invariant.*

Now specialize to $K = \mathrm{SL}(2, q)$. Then, taking the trace induces a well-defined function $\mathrm{tr}\colon\ \mathcal{E} \to \mathbb{F}_q$. We single out an important subset of $\mathcal{E}$.

DEFINITION 3.2. $\mathcal{C} = \{C \in \mathcal{E} \mid \mathrm{tr}(C) \neq 2 \text{ and } C \neq \{-I\}\}$.

If $[A, B] = -I$, then A and B commute in $\mathrm{PSL}(2, q)$ and hence (A, B) cannot generate $\mathrm{SL}(2, q)$. If $[A, B]$ has trace 2, then again (A, B) cannot generate. This follows from the Trace Theorem, but it can also be seen by elementary means: Supposing that the trace is 2, after conjugation we may assume $[A, B] = T$, where T is of the form $\left(\begin{smallmatrix} 1 & x \\ 0 & 1 \end{smallmatrix}\right)$ with $x \neq 0$ since A and B cannot commute. Since $ABA^{-1} = TB$ and $BAB^{-1} = T^{-1}A$, considering traces shows that A and B are upper triangular as well, so (A, B) cannot generate. We conclude that the image of $H\colon \mathcal{N} \to \mathcal{E}$ lies in $\mathcal{C}$, and $\mathrm{tr} \circ H\colon \mathcal{N} \to \mathbb{F}_q - \{2\}$. Diagrammatically, we have

$$\mathcal{N} \xrightarrow{H} \mathcal{C} \xrightarrow{\mathrm{tr}} \mathbb{F}_q - \{2\}\ .$$

DEFINITION 3.3. A prime power q is called *exceptional* if $q \in \{3, 5, 7, 9, 11\}$, otherwise it is called *non-exceptional.*

Using this notation and terminology, the Trace Theorem becomes the following statement.

THEOREM 3.4. *For non-exceptional* q, $\mathrm{tr} \circ H\colon \mathcal{N} \to \mathbb{F}_q - \{2\}$ *is surjective. For exceptional* q*, the following hold:*

(1) *For* $q = 3$, $q = 9$ *and* $q = 11$, *the image of* $\mathrm{tr} \circ H$ *is* $\mathbb{F}_q - \{1, 2\}$.
(2) *For* $q = 5$, *the image of* $\mathrm{tr} \circ H$ *is* $\mathbb{F}_5 - \{0, 2, 4\}$.
(3) *For* $q = 7$, *the image of* $\mathrm{tr} \circ H$ *is* $\mathbb{F}_7 - \{0, 1, 2\}$.

Our first main conjecture says that the Higman invariant is a complete invariant.

CLASSIFICATION CONJECTURE *(Higman invariant classifies Nielsen classes).* $H\colon \mathcal{N} \to \mathcal{E}$ is injective.

That is, two generating pairs (A, B) and (A', B') of $\mathrm{SL}(2, q)$ are Nielsen equivalent if and only if $[A, B]$ is conjugate to $[A', B']$ or $[B', A']$. For non-exceptional q, Corollary 5.5 shows that $\mathcal{C}$ is the image of H, and the Classification Conjecture becomes the assertion that $H\colon \mathcal{N} \to \mathcal{C}$ is bijective.

Closely related to the Classification Conjecture is the Trace Conjecture.

TRACE CONJECTURE. The trace invariant $\mathrm{tr} \circ H\colon \mathcal{N} \to \mathbb{F}_q - \{2\}$ is injective except that it is two-to-one on the pre-image of -2 when $q \equiv 1 \bmod 4$.

https://doi.org/10.1017/S0017089512000675 Published online by Cambridge University Press

Indeed, we will see in Corollary 5.6 that the Classification Conjecture and the Trace Conjecture are equivalent.

4. T-systems and the weak trace invariant. For some applications, Nielsen equivalence is too strong an invariant. More natural is to extend the action of $\mathrm{Aut}(F_2)$ on $\mathrm{Hom}(F_2, K)$ to an action of $\mathrm{Aut}(K) \times \mathrm{Aut}(F_2)$ by letting $(\alpha, \phi) \cdot \rho = \alpha \circ \rho \circ \phi^{-1}$. The resulting equivalence classes are called *T-systems.*

By a result of Schreier and van der Waerden [**31**] (see also [**4**] and the appendix to [**12**]), $\mathrm{Aut}(\mathrm{SL}(2, q))$ is generated by conjugations by elements of $\mathrm{GL}(2, q)$, which do not change $\mathrm{tr}([A, B])$, together with field automorphisms of $\mathbb{F}_q$ acting on the entries of the elements of $\mathrm{SL}(2, q)$, whose effect is to apply the same field automorphism to $\mathrm{tr}([A, B])$. Thus, the $\mathrm{Aut}(\mathbb{F}_q)$-orbit of $\mathrm{tr} \circ H(A, B)$ in $\mathbb{F}_q$ is an invariant of the T-system of (A, B), called the *weak trace invariant.* Denote the set of T-systems by $\mathcal{T}$ and the set of orbits of $\mathrm{Aut}(\mathbb{F}_q)$ acting on $\mathbb{F}_q$ by $\mathcal{O}_q$.

T-Classification Conjecture *(Weak trace invariant classifies T-systems).* For non-exceptional q, the weak trace invariant is a bijection from $\mathcal{T}$ to $\mathcal{O}_q - \{\{2\}\}$.

Corollary 5.7 is that the Classification Conjecture implies the T-Classification Conjecture.

We mention that the number Ψ_q of $\mathrm{Aut}(\mathbb{F}_q)$-orbits in $\mathbb{F}_q$ is given by the formula

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

No doubt this formula is well known. A proof was given in [**24**, Lemma 4.2]. The Trace Theorem stated in the introduction tells us that, for non-exceptional q, exactly $\Psi_q - 1$ orbits occur as weak trace invariants, and the T-Classification Conjecture would tell us that this is the exact number of T-systems.

5. Comparison between the Higman invariant and trace invariant. In this section we will use the well-known information about conjugacy in $\mathrm{SL}(2, q)$ to show that the Classification Conjecture is equivalent to the Trace Conjecture, and implies the T-Classification Conjecture.

First we must analyse the trace function $\mathrm{tr}\colon \mathcal{C} \to \mathbb{F}_q$, where $\mathcal{C}$ is the set of extended conjugacy classes in Definition 3.2. For this we will need to understand the conjugacy classes in $\mathrm{SL}(2, q)$.

Proposition 5.1. *If $A, B \in \mathrm{SL}(2, q)$ and $\mathrm{tr}(A) \neq \pm 2$, then A is conjugate to B if and only $\mathrm{tr}(A) = \mathrm{tr}(B)$. For each of the traces 2 and -2, there are two conjugacy classes when q is even and three when q is odd.*

Proof. This proposition is well known – one reference is [**9**] – but we will verify the second part since we will need the notation later anyway. Consider an element X of $\mathrm{SL}(2, q)$ having trace 2ϵ where $\epsilon = \pm 1$. It is conjugate to a matrix of the form $\left(\begin{smallmatrix} \epsilon & \mu \\ 0 & \epsilon \end{smallmatrix}\right)$, so the 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 $\mathrm{SL}(2, q)$ takes $\left(\begin{smallmatrix} \epsilon & \mu \\ 0 & \epsilon \end{smallmatrix}\right)$ to $\left(\begin{smallmatrix} \epsilon & \mu' \\ 0 & \epsilon \end{smallmatrix}\right)$ if and only if P is upper triangular. In this case, writing $P = \left(\begin{smallmatrix} x & b \\ 0 & x^{-1} \end{smallmatrix}\right)$, 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

https://doi.org/10.1017/S0017089512000675 Published online by Cambridge University Press

the set of non-zero elements that are squares, or is the set of non-squares. The latter is non-empty exactly when q is odd. □

PROPOSITION 5.2. *The trace function* $\mathrm{tr}\colon \mathcal{C} \to \mathbb{F}_q - \{2\}$ *is nearly bijective, in that*

(1) *for* q *even or* $q \equiv 3 \bmod 4$, $\mathrm{tr}\colon \mathcal{C} \to \mathbb{F}_q - \{2\}$ *is bijective, and*
(2) *for* $q \equiv 1 \bmod 4$ *and* $q \neq 9$, $\mathrm{tr}\colon \mathcal{C} \to \mathbb{F}_q - \{2\}$ *is bijective, except that it is* 2*-to-*1 *on* $\mathrm{tr}^{-1}(-2)$.

Proof. Let X represent an element of $\mathcal{C}$. By Proposition 5.1, we need only examine the case when $\mathrm{tr}(X) = -2$, say $X = \left(\begin{smallmatrix} -1 & x \\ 0 & -1 \end{smallmatrix}\right)$ for some non-zero x, and q is odd. We will continue to use the notation of Proposition 5.1.

Suppose that $q \equiv 3 \bmod 4$. Then -1 is not a square in $\mathbb{F}_q$, so $M(X^{-1}) = -M(X) \neq M(X)$. Thus, the conjugacy classes of X and X^{-1} are distinct and are the two conjugacy classes of matrices of trace -2 other than $\{-I\}$. They form one extended conjugacy class, so $\mathrm{tr}^{-1}(-2)$ contains only one element of $\mathcal{C}$.

Suppose now that $q \equiv 1 \bmod 4$. Then -1 is a square, so $M(X^{-1}) = -M(X) = M(X)$. In this case, there are two extended conjugacy classes of trace -2 other than $\{-I\}$, so $\mathrm{tr}^{-1}(-2)$ consists of two elements of $\mathcal{C}$. □

LEMMA 5.3. *Assume that* q *is odd. Then the two nontrivial conjugacy classes of trace* -2 *are equivalent under an automorphism of* $\mathrm{SL}(2, q)$ *that is a conjugation by an element of* $\mathrm{SL}(2, q^2)$.

Proof. As seen in the proof of Proposition 5.1, each of the nontrivial conjugacy classes of trace -2 contains elements of the form $\left(\begin{smallmatrix} -1 & t \\ 0 & -1 \end{smallmatrix}\right)$ for some non-zero $t \in \mathbb{F}_q$. Conjugating by a matrix in $\mathrm{SL}(2, q^2)$ of the form $\left(\begin{smallmatrix} \pi & 0 \\ 0 & \pi^{-1} \end{smallmatrix}\right)$, where $\pi^2 \in \mathbb{F}_q$ but $\pi \notin \mathbb{F}_q$, changes $\left(\begin{smallmatrix} -1 & t \\ 0 & -1 \end{smallmatrix}\right)$ to $\left(\begin{smallmatrix} -1 & t\pi^2 \\ 0 & -1 \end{smallmatrix}\right)$. Since π^2 is not a square in $\mathbb{F}_q$, this automorphism interchanges the two nontrivial conjugacy classes of trace -2. □

COROLLARY 5.4. *The image of* $H\colon \mathcal{N} \to \mathcal{C}$ *always contains the class or classes of trace* -2*, unless* $q = 3$ *or* $q = 9$*, in which case it contains no class of trace* -2.

Proof. The cases $q = 3$ and $q = 9$ are immediate from the Trace Theorem. Suppose that q is neither of these. By the Trace Theorem, at least one of the nontrivial conjugacy classes of matrices of trace -2 lies in the image of H, that is, there is a generating pair (A, B) having $\mathrm{tr}([A, B]) = -2$. If $q \not\equiv 1 \bmod 4$ then there is only one such class. If $q \equiv 1 \bmod 4$, then for an automorphism φ as in Lemma 5.3, $H(\varphi(A), \varphi(B)) = [\varphi(A), \varphi(B)]$ is the other nontrivial class of trace -2. □

Corollary 5.4 easily implies the following.

COROLLARY 5.5. *If* q *is non-exceptional, then* $H\colon \mathcal{N} \to \mathcal{C}$ *is surjective. For exceptional* q*, the image of* H *consists of all classes not directly excluded by the Trace Theorem.*

Another immediate consequence of Corollary 5.4 is as follows.

COROLLARY 5.6. *The Classification Conjecture is equivalent to the Trace Conjecture.*

Finally, we verify the claim made at the end of Section 3.

COROLLARY 5.7. *The Classification Conjecture implies the* T*-Classification Conjecture.*

https://doi.org/10.1017/S0017089512000675 Published online by Cambridge University Press

Proof. By Corollary 5.4, it suffices to show that for $q \equiv 1 \bmod 4$, the pair of Nielsen classes having trace -2 are T-equivalent. This is immediate from Lemma 5.3. □

6. G_0, G_1 and G, and Dickson's subgroup theorem. Following [**20**], for a fixed value of q we define G_0 to be SL(2, q). There is a natural homomorphism $G_0 \to \mathrm{PSL}(2, q)$.

Let G_1 be the subgroup of SL(2, q^2) consisting of the matrices of the form $\left(\begin{smallmatrix} a & b \\ b^q & a^q \end{smallmatrix}\right)$. This subgroup is conjugate to G_0 in GL(2, q^2) or SL(2, q^4): Fix a generator v of the multiplicative group of non-zero elements of $\mathbb{F}_{q^2}$ so that $(v^q)^q = v$ and $(v^q - v)^q = -(v^q - v)$. If $X = \left(\begin{smallmatrix} 1 & v \\ 1 & v^q \end{smallmatrix}\right)$ (for conjugacy in GL(2, q^2)) or $X = (v^q - v)^{-1/2}\left(\begin{smallmatrix} 1 & v \\ 1 & v^q \end{smallmatrix}\right)$ (for conjugacy in SL(2, q^4)), then sending A to XAX^{-1} carries G_0 to G_1. Following the inverse of this isomorphism by $G_0 \to \mathrm{PSL}(2, q)$ defines a homomorphism $G_1 \to \mathrm{PSL}(2, q)$.

When we write G_i, we mean either one of G_0 or G_1. We write G for PSL(2, q).

A subgroup of G is called *affine* if it is conjugate to a subgroup of the image in G of the subgroup of upper triangular matrices of G_0.

The subgroups of G were determined by Dickson [**3**]; a fine modern reference for that work is Suzuki [**32**]. Here is a list of the possibilities.

THEOREM 6.1. *Write $q = p^s$, and let $d = \gcd(p - 1, 2)$. Every subgroup of* PSL(2, q) *is isomorphic to (at least) one of the following.*

(a) *The dihedral groups of orders $2(q \pm 1)/d$ and their subgroups.*
(b) *A group H of order $q(q - 1)/d$ and its subgroups. A Sylow p-subgroup Q of H is elementary abelian, normal in H, and the factor group H/Q is a cyclic group of order $(q - 1)/d$.*
(c) *A_4, S_4 or A_5.*
(d) PSL(2, p^r) *or* PGL(2, p^r), *where r divides s. The latter subgroup occurs if and only if $p > 2$ and s/r is even.*

The last statement in (d) is from 3(6.18) of [**32**]. The groups H in (b) and their subgroups, together with the subgroups conjugate to diagonal subgroups, are the affine subgroups. The subgroups as in (c) are called *exceptional* subgroups. The particular exceptional subgroups which are contained in a given SL(2, q) are determined by simple congruences involving q [**32**].

7. Traces of G_i-pairs, and the Fricke polynomial. An $\mathbb{F}_q$-*triple* is an ordered triple (α, β, γ) of elements of $\mathbb{F}_q$, that is, an element of the vector space $\mathbb{F}_q^3$.

A G_i-*pair* is an ordered pair (A, B) of elements of G_i. A *conjugate* of the G_i-pair (A, B) is a pair of the form (XAX^{-1}, XBX^{-1}) for some $X \in G_i$, and we write $(A, B) \sim (A', B')$ to mean that (A, B) and (A', B') are conjugate.

The *trace* of a G_i-pair (A, B) is defined to be the $\mathbb{F}_q$-triple

$$\mathrm{Tr}(A, B) = (\mathrm{tr}(A), \mathrm{tr}(B), \mathrm{tr}(AB)).$$

Of course, conjugate pairs have the same trace. Theorem 1 of [**20**] is as follows.

THEOREM 7.1 (Macbeath). $\mathrm{Tr}\colon G_i \times G_i \to \mathbb{F}_q^3$ *is surjective.*

https://doi.org/10.1017/S0017089512000675 Published online by Cambridge University Press

The approach of [**20**] makes use of the *Fricke polynomial* $Q\colon \mathbb{F}_q^3 \to \mathbb{F}_q$, defined by

$$Q(\alpha, \beta, \gamma) = \alpha^2 + \beta^2 + \gamma^2 - \alpha\,\beta\,\gamma - 2.$$

The following computation goes back at least to Fricke (see [**1**]).

PROPOSITION 7.2. *If* (A, B) *is a* G_i*-pair, then* $\operatorname{tr}([A, B]) = Q(\operatorname{Tr}(A, B))$.

The expression $Q(\operatorname{Tr}(A, B))$ appears quite often in our work, and we will abbreviate it to $Q(A, B)$. Note that $Q(A, B) = Q(-A, B) = Q(A, -B) = Q(-A, -B)$, that is, Q is well defined on G-pairs.

Proposition 7.2 says that the following diagram commutes:

$$\begin{array}{ccc} G_i \times G_i & \xrightarrow{H} & \mathcal{E} \\ {\scriptstyle \operatorname{Tr}}\downarrow & & \downarrow{\scriptstyle \operatorname{tr}} \\ \mathbb{F}_q^3 & \xrightarrow{Q} & \mathbb{F}_q \end{array}$$

In the next section, we will refine this diagram.

8. The Markov equivalence. We saw in Section 2 that for any group K, the action of $\operatorname{Aut}(F_2)$ on $K \times K$ is generated by the action of three involutions r, s and t. For any field F, $\operatorname{Aut}(F_2)$ acts on the set of F-triples as follows:

(1) $r(\alpha, \beta, \gamma) = (\alpha, \beta, \alpha\beta - \gamma)$.
(2) $s(\alpha, \beta, \gamma) = (\beta, \alpha, \gamma)$.
(3) $t(\alpha, \beta, \gamma) = (\alpha, \gamma, \beta)$.

Specializing to $K = \mathrm{SL}(2, F)$ for some field F, this action is induced from the $\operatorname{Aut}(F_2)$-action on $G_i \times G_i$ via Tr, that is, $r \circ \operatorname{Tr} = \operatorname{Tr} \circ r$, $s \circ \operatorname{Tr} = \operatorname{Tr} \circ s$ and $t \circ \operatorname{Tr} = \operatorname{Tr} \circ t$. For s and t this is obvious, and for r it is simply the identity $\operatorname{tr}(A^{-1}B) = \operatorname{tr}(A)\operatorname{tr}(B) - \operatorname{tr}(AB)$. We call the equivalence relation on F^3 generated by r, s and t *Markov equivalence*.

Since $\operatorname{Tr} \circ \mu = \operatorname{Tr}$ for any inner automorphism μ of F_2, the $\operatorname{Aut}(F_2)$-action on F^3 induces an action of $\operatorname{Aut}(F_2)/\operatorname{Inn}(F_2) = \mathrm{GL}(2, \mathbb{Z})$ on F^3. Since the element $-I$ of $\mathrm{GL}(2, \mathbb{Z})$ is represented by the automorphism that sends x_i to x_i^{-1} for both basis elements of F_2, it also acts trivially on F^3 and there is an induced action of $\mathrm{PGL}(2, \mathbb{Z})$. Thus, Markov equivalence in F^3 coincides with the orbits of this action of the extended modular group $\mathrm{PGL}(2, \mathbb{Z})$; this was used for $F = \mathbb{R}$ in [**11**].

An $\mathbb{F}_q$-triple or a G_i-pair is called *singular* or *nonsingular* accordingly as Q does or does not assign it the value 2. Theorem 2 of [**20**] identifies the affine subgroups of $\mathrm{PSL}(2, q)$ in terms of Q.

THEOREM 8.1 (Macbeath). *A* G_i*-pair* (A, B) *generates an affine subgroup of* G *if and only if* $Q(A, B) = 2$.

Here, as in many places in our work, we speak of the subgroup of G generated by a G_i-pair. This means the subgroup generated by the images of A and B in G. Note that Theorem 8.1 shows that a singular pair cannot generate G.

Theorem 3 of [**20**] gives important information about Tr.

THEOREM 8.2 *(Macbeath). Let* (α, β, γ) *be a nonsingular* $\mathbb{F}_q$*-triple. If* q *is even, then there is exactly one conjugacy class of* G_i*-pairs whose trace equals* (α, β, γ). *If* q *is odd,*

https://doi.org/10.1017/S0017089512000675 Published online by Cambridge University Press

then there are exactly two conjugacy classes. These classes are conjugate in $\mathrm{SL}(2, \overline{\mathbb{F}}_q)$*, where* $\overline{\mathbb{F}}_q$ *is the algebraic closure of* $\mathbb{F}_q$*, and consequently generate isomorphic subgroups of* G_i*.*

An $\mathbb{F}_q$-triple is called *essential* when it is the trace of a generating pair. The orbits of the action of $\mathrm{Aut}(F_2)$ on $G_i \times G_i$ preserves the generating pairs $\mathcal{G}_2(G_i)$, so the induced action on $\mathbb{F}_q^3$ preserves the essential triples. The orbits of essential triples under the induced action are called *Markov classes,* and the set of Markov classes is denoted by $\mathcal{M}$.

Since the action of $\mathrm{Aut}(F_2)$ on essential triples is induced from the action on generating pairs, there is a well-defined trace function $\mathrm{Tr}\colon \mathcal{N} \to \mathcal{M}$, and we can refine our previous diagram to the following:

$$\begin{array}{ccc} \mathcal{N} & \xrightarrow{H} & \mathcal{C} \\ {\scriptstyle \mathrm{Tr}}\downarrow & & \downarrow{\scriptstyle \mathrm{tr}} \\ \mathcal{M} & \xrightarrow{Q} & \mathbb{F}_q - \{2\}, \end{array}$$

where Tr is surjective, and for non-exceptional q, H, Q and tr are also surjective.

The results collected so far give a very clear picture of how $\mathrm{Tr}\colon \mathcal{N} \to \mathcal{M}$ works:

(1) Since the defining action of $\mathrm{Aut}(F_2)$ for Markov classes is induced from the defining action for Nielsen classes via the trace function, $\mathrm{Tr}\colon G_i \times G_i \to \mathbb{F}_q^3$ carries each Nielsen class surjectively onto a Markov class.

(2) By Theorem 8.2, the pre-image of an essential triple (α, β, γ) under $\mathrm{Tr}\colon G_i \times G_i \to \mathbb{F}_q^3$ consists of one conjugacy class of generating pairs when q is even, and two conjugacy classes when q is odd.

(3) By Lemma 2.1(ii), conjugate generating pairs are Nielsen equivalent. Therefore, statement (2) implies the following:
   (a) When q is even, the pre-image of a Markov class consists of one Nielsen class.
   (b) When q is odd, the pre-image of a Markov class consists of one Nielsen class if its inverse image under $\mathrm{Tr}\colon G_i \times G_i \to \mathbb{F}_q^3$ contains non-conjugate pairs with the same trace, and two if not.

We say that a function is (≤ 2)-to-1 if the pre-image of each element of the codomain contains at most two elements. From statement (3) above, we have the following.

PROPOSITION 8.3. $\mathrm{Tr}\colon \mathcal{N} \to \mathcal{M}$ *is bijective if* q *is even, and is* (≤ 2)*-to-*1 *if* q *is odd.*

We will refine this in Theorem 10.1, which says that the pre-image of the Markov class of (α, β, γ) is a single Nielsen class whenever $2 - Q(\alpha, \beta, \gamma)$ is not a square in $\mathbb{F}_q$.

The next conjecture says that Q classifies Markov classes.

Q-CLASSIFICATION CONJECTURE $Q\colon \mathcal{M} \to \mathbb{F}_q - \{2\}$ is injective.

Proposition 5.2 tells us that $\mathrm{tr}\colon \mathcal{C} \to \mathbb{F}_q - \{2\}$ is a bijection when q is even. Combined with Proposition 8.3, this gives the following.

COROLLARY 8.4. *For* q *even, the Classification Conjecture is equivalent to the Q-Classification Conjecture.*

In general, we have the following.

https://doi.org/10.1017/S0017089512000675 Published online by Cambridge University Press

PROPOSITION 8.5. *The Classification Conjecture implies the Q-Classification Conjecture.*

Proof. Assuming the Classification Conjecture if $q \not\equiv 1 \bmod 4$, then Proposition 5.2 shows that $\mathrm{tr}\colon \mathcal{C} \to \mathbb{F}_q - \{2\}$ is injective, and the proposition is immediate. So we assume that $q \equiv 1 \bmod 4$ so that tr is injective except that it is 2-to-1 on $\mathrm{tr}^{-1}(-2) = \{C, C'\}$. Choose (A, B) representing the Nielsen class with Higman invariant $[A, B] \in C$. By Lemma 5.3, there is a matrix $X \in \mathrm{SL}(2, q^2)$ such that $X[A, B]X = [XAX^{-1}, XBX^{-1}]$ lies in C', that is, the Higman invariant of the Nielsen class of (XAX^{-1}, XAX^{-1}) is C'. Since $\mathrm{Tr}(A, B) = \mathrm{Tr}(XAX^{-1}, XAX^{-1})$, Tr sends the Nielsen classes of (A, B) and (XAX^{-1}, XAX^{-1}) to the same Markov class of $\mathcal{M}$. It follows that Q is also injective. □

9. Parabolic, elliptic and hyperbolic elements. In our remaining work, we will need more information about the fields $\mathbb{F}_q$ and their elements. To set notation, we denote by u a generator of $C_{q-1} = \mathbb{F}_q - \{0\}$. In the software for the computer-assisted calculations that we will discuss in Section 12, we used for u the primitive element denoted by $Z(q)$ in the Computational Group Theory (GAP) computer algebra system [**10**]. For the unique quadratic extension $\mathbb{F}_{q^2}$ of $\mathbb{F}_q$, the group of non-zero elements is $C_{q^2-1} = \mathbb{F}_{q^2} - \{0\}$ and is generated by $Z(q^2)$. The element u is $Z(q^2)^{q+1}$, and we denote by v the element $Z(q^2)^{q-1}$. The latter generates a subgroup $C_{q+1} \subset C_{q^2-1}$, and its powers are exactly the elements of $\mathbb{F}_{q^2}$ that satisfy $x^{q+1} = 1$, that is, the elements of norm 1. For q odd, $C_{q-1} \cap C_{q+1} = C_2$ generated by $u^{(q-1)/2} = v^{(q+1)/2} = -1$. For q even, $C_{q-1} \cap C_{q+1} = \{1\}$. The subgroup of C_{q^2-1} generated by $C_{q-1} \cup C_{q+1}$ is the set of squares, so is all of C_{q^2-1} when q is even and has index 2 when q is odd.

An element α of $\mathbb{F}_q$ is called *elliptic, parabolic* or *hyperbolic* accordingly as equation $\lambda^2 - \alpha\lambda + 1 = 0$ has zero, one or two distinct roots in $\mathbb{F}_q$. An element of $\mathbb{F}_q$ is hyperbolic if and only if it can be written as $u^i + u^{-i}$ with $u^i \neq \pm 1$. The elements $v^j + v^{-j}$ lie in $\mathbb{F}_q$, and for $v^j \neq \pm 1$ are exactly the elliptic elements. We denote the sets of elliptic and hyperbolic elements of a field under discussion by E and H respectively. If q is even, then E contains $\frac{1}{2}q$ elements, H contains $\frac{1}{2}(q-2)$ hyperbolic elements and 0 is the unique parabolic element. If q is odd, then E contains $\frac{1}{2}(q-1)$ elliptic elements, H contains $\frac{1}{2}(q-3)$ hyperbolic elements and 2 and -2 are the parabolic elements.

The following lemma gives a simple criterion to identify the type of an element in fields of odd characteristics. By $\mathbb{F}_q^2$ we denote the set of elements of $\mathbb{F}_q$ that are squares.

LEMMA 9.1. *Let $\alpha \in \mathbb{F}_q$, with q odd.*

(1) *α is parabolic if and only if $\alpha^2 - 4 = 0$.*
(2) *α is hyperbolic if and only if $\alpha^2 - 4 \in \mathbb{F}_q^2 - \{0\}$.*
(3) *α is elliptic if and only if $\alpha^2 - 4 \notin \mathbb{F}_q^2$.*

Proof. It suffices to prove the right-to-left implications in each of the three statements. The parabolic case is immediate. If α is hyperbolic, then writing $\alpha = u^i + u^{-i}$ gives $\alpha^2 - 4 = (u^i - u^{-i})^2 \in \mathbb{F}_q^2 - \{0\}$. If α is elliptic, then $\alpha = v^j + v^{-j}$ produces $\alpha^2 - 4 = (v^j - v^{-j})^2$. If this is the square of an element in $\mathbb{F}_q$, then $v^j - v^{-j} \in \mathbb{F}_q$, so $2v^j \in \mathbb{F}_q$. Since q is odd, this implies that $v^j \in \mathbb{F}_q$, a contradiction. □

10. The fundamental equation. Consider an $\mathbb{F}_q^3$-triple (α, β, γ) with α either hyperbolic or elliptic. Write $\alpha = x + x^{-1}$, with x of the form u^i or v^j accordingly

https://doi.org/10.1017/S0017089512000675 Published online by Cambridge University Press

as α is hyperbolic or elliptic. Since $x \neq x^{-1}$, there is a unique pair (a, d) of elements of $\mathbb{F}_{q^2}$ such that $a + d = \beta$ and $ax + dx^{-1} = \gamma$. Explicitly, $a = (\gamma - \beta x^{-1})/(x - x^{-1})$ and $d = (\beta x - \gamma)/(x - x^{-1})$. In the hyperbolic case, a and d lie in $\mathbb{F}_q$, and we select any b and c in $\mathbb{F}_q$ with $bc = ad - 1$. In the elliptic case, we compute that $d = a^q$. Since $ad - 1 \in \mathbb{F}_q$, we select any $b \in \mathbb{F}_{q^2}$ with $b^{q+1} = ad - 1$, and put $c = b^q$. Then, (α, β, γ) is the trace of a G_i-pair – a G_0-pair when A is hyperbolic, and a G_1-pair when it is elliptic – of the form

$$(A, B) = \left(\begin{pmatrix} x & 0 \\ 0 & x^{-1} \end{pmatrix}, \begin{pmatrix} a & b \\ c & d \end{pmatrix} \right),$$

with a and d uniquely determined by $\mathrm{Tr}(A, B)$ and the choice between x and x^{-1} is considered to be x. We say that such pairs are *in normal form.* We note that this gives a computational proof of Theorem 7.1, but more importantly, for a pair in normal form, it is straightforward to compute the following formula, which we call the *Fundamental Equation*:

$$Q(\alpha, \beta, \gamma) = 2 - bc(\alpha^2 - 4).$$

The Fundamental Equation helps to establish the following result that was mentioned in Section 1.

THEOREM 10.1. *Let (α, β, γ) be an essential triple. If $2 - Q(\alpha, \beta, \gamma)$ is not a square in $\mathbb{F}_q$, then the Markov class of (α, β, γ) is the trace of a unique Nielsen class.*

Since (A, B) is always Nielsen equivalent to (A^{-1}, B^{-1}), Theorem 10.1 follows from Theorem 8.2 (see statement (3) in Section 8) and the following computational lemma.

LEMMA 10.2. *Let (A, B) be a G_i-pair with $Q(A, B) \neq 2$. Then (A, B) is conjugate to (A^{-1}, B^{-1}) if and only if $2 - Q(A, B)$ is a square in $\mathbb{F}_q$.*

It seems interesting to compare Lemma 10.2 with Lemma 3.4.5 of [**11**], which says that for hyperbolic elements A and B in $\mathrm{SL}(2, \mathbb{R})$ the axes of A and B cross if and only if $\mathrm{tr}([A, B]) < 2$. Since $\mathrm{tr}([A, B]) = Q(A, B)$, this condition is equivalent (when $Q(A, B) \neq 2$) to $2 - Q(A, B)$ being a square in $\mathbb{R}$. The isometry of $\mathbb{H}^2$ that rotates through an angle of π fixing the intersection point of the axes conjugates (A, B) to (A^{-1}, B^{-1}), while if the axes do not cross, any isometry preserving the axis of A cannot preserve that of B, so no isometry conjugates (A, B) to (A^{-1}, B^{-1}).

Proof of Lemma 10.2 When q is even, $2 - \mathrm{Tr}(A, B)$ is always a square. On the other hand, since $\mathrm{Tr}(A, B) = \mathrm{Tr}(A^{-1}, B^{-1})$, Theorem 8.2 shows that (A, B) is conjugate to (A^{-1}, B^{-1}), establishing the lemma. So we will assume that q is odd.

Assume first that at least one of A, B or AB is not parabolic. Noting that if (A, B) is conjugate to (A^{-1}, B^{-1}), then the same is true for any pair Nielsen equivalent to (A, B), we may change (A, B) by Nielsen equivalence to assume that A is not parabolic. Conjugate to put (A, B) into normal form.

Suppose first that $A = \left(\begin{smallmatrix} x & 0 \\ 0 & x^{-1} \end{smallmatrix}\right)$ is hyperbolic. Since $x \neq x^{-1}$, we find that $XAX^{-1} = A^{-1}$ exactly when X is of the form $\left(\begin{smallmatrix} 0 & -s \\ s^{-1} & 0 \end{smallmatrix}\right)$. Writing B as $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, the condition that $XBX^{-1} = B^{-1}$ is then equivalent to $b = cs^2$, that is, bc is a square in $\mathbb{F}_q$. By the Fundamental Equation, $bc = (2 - Q(A, B))/(\alpha^2 - 4)$. Since $\alpha^2 - 4 = (x - x^{-1})^2$, bc is a square in $\mathbb{F}_q$ if and only if $2 - Q(A, B)$ is a square.

https://doi.org/10.1017/S0017089512000675 Published online by Cambridge University Press

Suppose now that A is elliptic (so we now work in G_1 rather than G_0), and $B = \left(\begin{smallmatrix} a & b \\ b^q & a^q \end{smallmatrix}\right)$. By Lemma 9.1, $\alpha^2 - 4$ is not a square in $\mathbb{F}_q$, and the Fundamental Equation shows that $2 - Q(A, B) = b^{q+1}(\alpha^2 - 4)$, so we must show that (A, B) is conjugate to (A^{-1}, B^{-1}) if and only if b^{q+1} is not the square of an element of $\mathbb{F}_q$.

The condition that $XAX^{-1} = A^{-1}$ in G_1 is equivalent to X being of the form $\left(\begin{smallmatrix} 0 & s \\ s^q & 0 \end{smallmatrix}\right)$, where $s^{q+1} = -1$, and then $XBX^{-1} = B^{-1}$ exactly when $s^{-2} = b^{q-1}$. So we must show that these two equations hold for some $s \in \mathbb{F}_{q^2}$ if and only if b^{q+1} is not a square in $\mathbb{F}_q$.

If these hold, then raising both sides of the second equation to the power $-(q+1)/2$ gives $s^{q+1} = (b^{q+1})^{(1-q)/2}$. If b^{q+1} were a square in $\mathbb{F}_q$, say $b^{q+1} = c^2$, then we would have $-1 = (c^2)^{(1-q)/2} = c^{1-q} = 1$.

Suppose that b^{q+1} is not a square in $\mathbb{F}_q$. Let $s = b^{(1-q)/2}$. Then $s^{q+1} = (s^2)^{(q+1)/2} = (b^{1-q})^{(q+1)/2} = (b^{q+1})^{(1-q)/2} = -1$.

We may now assume that A and B (and AB, although that is not needed here) are parabolic. We work in G_0, and by conjugating we may assume that A is of the form $\left(\begin{smallmatrix} \epsilon & x \\ 0 & \epsilon \end{smallmatrix}\right)$, with $\epsilon = \pm 1$ and $x \neq 0$. It is straightforward to check that A is conjugate to A^{-1} if and only if -1 is a square in $\mathbb{F}_q$, say, $r^2 = -1$. In this case, any matrix of the form $X = \left(\begin{smallmatrix} r & s \\ 0 & -r \end{smallmatrix}\right)$ conjugates A to A^{-1}. Writing B as $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, the condition that $XBX^{-1} = B^{-1}$ is equivalent to $r(d - a) = sc$. If $c \neq 0$, this can be satisfied, while if $c = 0$, then since B is parabolic, we have $a = d$ and again it can be satisfied. So (A, B) is conjugate to (A^{-1}, B^{-1}) exactly when -1 is a square in $\mathbb{F}_q$. On the other hand, for $\gamma = \mathrm{tr}(AB)$ we have $Q(A, B) = 4 + 4 + \gamma^2 \pm 4\gamma - 2 = 2 + (\gamma \pm 2)^2$, so $2 - Q(A, B)$ is a square if and only if -1 is a square. Again, the criterion holds. □

11. Identifying essential triples. For our computational verification of the Classification Conjecture for $q \leq 101$, described in Section 12, as well as for some of our later theoretical work, we will need to be able to identify the essential triples – those that are traces of generating pairs of $\mathrm{SL}(2, q)$. In this section we develop simple criteria for checking this.

For $(A, B) \in \mathrm{SL}(2, q) \times \mathrm{SL}(2, q)$, denote by $P(A, B)$ the subgroup of $\mathrm{PSL}(2, q)$ generated by $\{A, B\}$. Clearly (A, B) generates a proper subgroup of $\mathrm{SL}(2, q)$ if and only if $P(A, B)$ is a proper subgroup. The subgroups that can occur were described in Theorem 6.1, and can be identified from $\mathrm{Tr}(A, B) = (\alpha, \beta, \gamma)$ as follows:

(1) Since a matrix has order 2 in $\mathrm{PSL}(2, q)$ if and only if its trace is 0, $P(A, B)$ is dihedral if at least two of α, β and γ are 0.
(2) By Theorem 8.1, $P(A, B)$ is affine (which includes the cases when it is cyclic) if and only if $Q(\alpha, \beta, \gamma) = 2$.
(3) The cases when $P(A, B)$ is one of the exceptional subgroups A_4, S_4 or A_5 can be characterized by conditions on $\mathrm{Tr}(A, B) = (\alpha, \beta, \gamma)$, which are stated and verified in [**21**]. It is A_4 exactly when $\alpha, \beta, \gamma \in \{0, \pm 1\}$ and $Q(\alpha, \beta, \gamma) = 0$, and is S_4 exactly when $\alpha, \beta, \gamma \in \{0, \pm 1, \pm\sqrt{2}\}$, where $\sqrt{2}$ denotes a root of $x^2 - 2$, and $Q(\alpha, \beta, \gamma) = 1$. For A_5 the conditions are more complicated (in particular, there are special conditions when the characteristic of $\mathbb{F}_q$ is 3, 11, 19 and 29), and we do not detail them here.
(4) When all three of α, β and γ lie in a proper subfield $\mathbb{F}_{p^r}$, either $P(A, B)$ is affine or $P(A, B)$ is isomorphic to a subgroup of $\mathrm{PSL}(2, p^r)$. For, by Theorem 7.1, there must be a pair (A', B') of elements of $\mathrm{PSL}(2, p^r)$ such that $\mathrm{Tr}(A', B') = (\alpha, \beta, \gamma)$.

https://doi.org/10.1017/S0017089512000675 Published online by Cambridge University Press

If $Q(\alpha, \beta, \gamma) = 2$, then $P(A, B)$ is affine, and if not, then by Theorem 8.2, the subgroups $P(A, B)$ and $P(A', B')$ are isomorphic.

The remaining proper subgroups of SL(2, q) will take a bit more effort. They are included in case (d) in Theorem 6.1, and are described explicitly in (6.18) of [**32**] (also in [**20**], p. 28) as follows: Assume that q is odd, and observe that there is an element of $\mathbb{F}_q - \mathbb{F}_{p^r}$ whose square lies in $\mathbb{F}_{p^r}$ if and only if $\mathbb{F}_{p^{2r}} \subseteq \mathbb{F}_q$, in which case all such elements lie in $\mathbb{F}_{p^{2r}}$. If π is such an element, and $x \in \mathbb{F}_q - \mathbb{F}_{p^r}$, then $x^2 \in \mathbb{F}_{p^r}$ if and only if $x = \pi\delta$ for some some $\delta \in \mathbb{F}_{p^r}$. Write d_π for the matrix $\left(\begin{smallmatrix} \pi & 0 \\ 0 & \pi^{-1} \end{smallmatrix}\right)$.

Let $\widehat{\mathrm{SL}}(2, p^r) = \langle \mathrm{SL}(2, p^r), d_\pi \rangle$. We have $d_\pi^2 \in \mathrm{SL}(2, p^r)$, and d_π normalizes $\mathrm{SL}(2, p^r)$, so $\mathrm{SL}(2, p^r)$ has index 2 in the subgroup $\widehat{\mathrm{SL}}(2, p^r)$.

The trace of $d_\pi^\epsilon A$ is of the form $\pi^\epsilon \delta$ for some $\delta \in \mathbb{F}_{p^r}$. Consequently, if (A, B) is a pair of elements of $\widehat{\mathrm{SL}}(2, p^r)$, then $\mathrm{Tr}(A, B) = (\pi^{\epsilon_1}\alpha, \pi^{\epsilon_2}\beta, \pi^{\epsilon_3}\gamma)$ with $\alpha, \beta, \gamma \in \mathbb{F}_{p^r}$ and $\epsilon_1 + \epsilon_2 + \epsilon_3 \equiv 0 \bmod 2$. Equivalently, $\mathrm{Tr}^2(A)$, $\mathrm{Tr}^2(B)$, $\mathrm{Tr}^2(AB)$ and $\mathrm{Tr}(A)\,\mathrm{Tr}(B)\,\mathrm{Tr}(AB)$ all lie in $\mathbb{F}_{p^r}$. We are prepared for the following variation on Theorem 7.1:

PROPOSITION 11.1. *Let $(\widehat{\alpha}, \widehat{\beta}, \widehat{\gamma})$ be a triple of elements of $\mathbb{F}_q$ such that $\widehat{\alpha}^2$, $\widehat{\beta}^2$, $\widehat{\gamma}^2$, and $\widehat{\alpha}\widehat{\beta}\widehat{\gamma}$ all lie in a proper subfield $\mathbb{F}_{p^r}$ of $\mathbb{F}_q$. Then either $\widehat{\alpha}$, $\widehat{\beta}$, and $\widehat{\gamma}$ all lie in $\mathbb{F}_{p^r}$, or $\mathbb{F}_{p^{2r}} \subseteq \mathbb{F}_q$ and there exists a pair $(A, B) \in \widehat{\mathrm{SL}}(2, p^r)$ such that $\mathrm{Tr}(A, B) = (\widehat{\alpha}, \widehat{\beta}, \widehat{\gamma})$.*

Proof. Our argument is a very slight modification of the proof of Theorem 7.1, given as Theorem 1 in [**20**]. If all three coordinates lie in $\mathbb{F}_{p^r}$, in particular if q is even, then there is nothing to prove. Of the remaining possibilities, we need only consider the case when the triple is of the form $(\pi\alpha, \pi\beta, \gamma)$, with $\alpha, \beta, \gamma \in \mathbb{F}_{p^r}$, since the other cases can then be achieved by applying Nielsen equivalences to a pair (A, B) that we will obtain for this case.

We will seek a pair of the form

$$(A, B) = \left(\begin{pmatrix} 0 & \pi \\ -\pi^{-1} & \pi^{-1}(\pi^2\alpha) \end{pmatrix}, \begin{pmatrix} \pi x & \pi y \\ \pi^{-1}z & \pi^{-1}w \end{pmatrix} \right)$$

for which

$$\begin{aligned} \pi x + \pi^{-1} w &= \mathrm{tr}(B) = \pi\beta, \\ z - y + \alpha w &= \mathrm{tr}(AB) = \gamma, \\ xw - yz &= \det(B) = 1\,. \end{aligned}$$

Eliminating x and then y from these equations reduces them to the condition

$$1 + z^2 + \pi^{-2}w^2 + \alpha zw + \beta(-1)w + \gamma(-1)z = 0.$$

If (X, Y, Z) is a solution of

$$C(X, Y, Z) = X^2 + Y^2 + \pi^{-2}Z^2 + \alpha YZ + \beta XZ + \gamma XY = 0$$

with $X \neq 0$, then putting $(-1, z, w) = (-1, -Y/X, -Z/X)$ satisfies the condition. Since every quadratic form over a finite field has non-zero solutions, we need only consider the case of a non-zero solution of the form $(0, Y_0, Z_0)$. A line through this point and not tangent to the conic $C(X, Y, Z) = 0$ will intersect the conic in a point with $X \neq 0$, giving the desired solution. Such a line exists unless $(0, Y_0, Z_0)$ is a singular point of the conic. But the singularity condition is $0 = \gamma Y_0 + \beta Z_0$, $0 = 2Y_0 + \alpha Z_0$

https://doi.org/10.1017/S0017089512000675 Published online by Cambridge University Press

and $0 = \alpha Y_0 + 2\pi^{-2} Z_0$, and the latter two equations imply that $\pi^2 = (2\alpha^{-1})^2$, in contradiction to the fact that $\pi \notin \mathbb{F}_{p^r}$. □

Equipped with Proposition 11.1, we now consider the remaining type of proper subgroup.

(5) If q is odd and α^2, β^2, γ^2 and $\alpha\beta\gamma$ lie in a proper subfield $\mathbb{F}_{p^r}$ of $\mathbb{F}_q$, but at least one of α, β and γ does not lie in $\mathbb{F}_{p^r}$, then either $P(A, B)$ is affine or $P(A, B)$ is isomorphic to a subgroup of the image of $\widehat{\mathrm{SL}}(2, p^r)$ in $\mathrm{PSL}(2, q)$. For, by Proposition 11.1, there exists a pair (A', B') of elements of $\widehat{\mathrm{SL}}(2, p^r)$ such that $\mathrm{Tr}(A', B') = (\widehat{\alpha}, \widehat{\beta}, \widehat{\gamma})$. If $Q(\alpha, \beta, \gamma) = 2$, then $P(A, B)$ is affine, and if not, then by Theorem 8.2 the subgroups $P(A, B)$ and $P(A', B')$ are isomorphic.

Conditions (1) through (5) make it easy to check when a triple in $\mathbb{F}_q^3$ is essential. One application is a computational proof of the Trace Theorem for the cases when $q \leq 11$: We remove from $\mathbb{F}_q^3$ all the triples satisfying one of the five conditions, then find the values that Q assumes on the remaining subset.

12. Computational verification of the Classification Conjecture for $q \leq 101$. Using GAP [**10**], we have verified the Classification Conjecture for all $q \leq 101$. The scripts used for that work are available at [**22**]. In this section we will describe the method used.

For a given q-value, the number of generating pairs is of the order of $|\mathrm{SL}(2, q)|^2$, i.e. q^6. Consequently, verifying the Classification Conjecture directly requires a great deal of computing capacity, and on typical desktop machines, such as ours, is feasible only for $q \leq 11$. But this does allow us to consider only $q \geq 13$ in the remaining discussion. In particular, all q will be non-exceptional.

The key idea is to first verify the Q-Classification Conjecture for $q \leq 101$, then utilize it to deduce the Classification Conjecture. This dramatically extends the workable range of q-values, since the number of essential triples is only of the order of q^3.

Here is how the program verifies the Q-Classification Conjecture for a fixed q. For each value $\ell \in \mathbb{F}_q - \{2\}$, it uses Section 11 to find all the essential triples with Q-value equal to ℓ, then forms singleton lists each containing one of these triples. Then it combines any two of these lists whenever an element of one is equivalent to an element of the other under one of r, s or t. In all cases with $q \leq 101$, it finishes with only a single list for each of the possible trace invariants listed in the Trace Theorem.

Following the referee's suggestion, we also wrote a script to use GAP's built-in orbit calculator to verify the Q-classification Conjecture. It worked well and verified the conjecture as far as $q = 131$ before exceeding the memory of our ordinary personal computer when attempting $q = 137$. The script was shorter than ours. On the other hand, checking which orbits were actually essential triples required some of our existing software, and consequently (1) the new script was not really so much shorter, and (2) it provides only a partially independent check of the previous computational verification of the Q-classification Conjecture. Future investigation might explore the possibility of using GAP to better understand the action; in particular, it might be interesting to know the elements of $\mathrm{Aut}(F_2)$ that act trivially.

Once the Q-Classification Conjecture has been verified for a given value of q, we verify the Classification Conjecture as follows.

https://doi.org/10.1017/S0017089512000675 Published online by Cambridge University Press

(1) For even q, the Q-Classification Conjecture implies the Classification Conjecture, by Corollary 8.4, so there is nothing more to do.
(2) For odd q, Theorem 8.2 says that each nonsingular triple is the trace of only two conjugacy classes of pairs.
   (a) For the Q-value -2 when $q \equiv 1 \bmod 4$, Corollary 5.4 shows that $H : \mathcal{N} \to \mathcal{C}$ always contains both the classes of trace -2, that is, there are at least two Nielsen classes with trace invariant -2. The Q-classification conjecture implies that there is a unique Markov class with Q-value -2, hence at most two Nielsen classes with trace invariant -2. So there are exactly two, and H carries them to the two elements of $\mathcal{C}$ with trace -2.
   (b) For all Q-values in $\mathbb{F}_q - \{2, -2\}$, and for the Q-value -2 when $q \equiv 3 \bmod 4$, we find two generating pairs that have the same trace – a triple with this particular Q-value – that are Nielsen equivalent but not conjugate. Finding such pairs shows that there is only one Nielsen class mapping to the Markov class of that essential triple. Since the Q-Classification Conjecture tells us there is only one Markov class with the given Q-value, there is only one Nielsen class with trace invariant equal to that Q-value.

Here is the actual algorithm for step 2(b). Fixing an odd q with $13 \leq q \leq 101$ and a value $\ell \in \mathbb{F}_q - \{2, -2\}$, or $\ell = -2$ when $q \equiv 3 \bmod 4$, consider the graph with vertices being the set of generating pairs with Q-value ℓ, with edges labelled by r running from each (A, B) to $r(A, B)$, and similar edges labelled as s and t. (Using instead a graph whose edges correspond to the basic Nielsen transformations will give similar results.) The program chooses a pair (A_0, B_0) for which $Q(A_0, B_0) = \ell$, then takes random walks in the graph, starting from (A_0, B_0). If some walk reaches a pair having trace equal to $\mathrm{Tr}(A_0, B_0)$, but not conjugate to (A_0, B_0), then the two conjugacy classes of pairs with that trace are Nielsen equivalent. From step 2(a), such a walk cannot exist when $q \equiv 1 \bmod 4$ and $\mathrm{tr}([A, B]) = -2$, but in all other cases we found many such walks.

In the cases when $2 - \ell$ was not a square, Lemma 10.2 shows that the Nielsen equivalent pairs (A_0, B_0) and (A_0^{-1}, B_0^{-1}) are non-conjugate. In these cases, the program finds very short walks taking (A_0, B_0) to a conjugate of (A_0^{-1}, B_0^{-1}) (for example, $RSRS(A_0, B_0) = (A_0^{-1}, B_0^{-1})$). When $2 - \ell$ was a square, nearby pairs with $\mathrm{Tr}(A, B) = (A_0, B_0)$ were rarely found, and the conjugacy classes of the pairs (A, B) having $\mathrm{Tr}(A, B) = \mathrm{Tr}(A_0, B_0)$ appeared to vary randomly as one moved through the graph, consistent with an even chance of agreement or disagreement with the conjugacy class of (A_0, B_0). Additional computation would give a more precise picture of what the Nielsen classes look like within the space of essential triples.

13. The geometry of the Q-levels. This section and the following one are presented for arbitrary q, although only used later for even q. In this section, we will examine more closely how the level surfaces of Q meet the 'slices' of $\mathbb{F}_q^3$ having a fixed value for one of the coordinates. Since Q is symmetric, permutations of coordinates preserve the level surfaces, so it suffices to examine the slices with a fixed first coordinate α.

Each slice decomposes into conic sections which are hyperbolas, ellipses or lines, depending upon whether α is hyperbolic, elliptic or parabolic. In this section, we will detail how the stabilizer of the slice under the Markov action acts on these conic sections. Also, the subgroup of $\mathrm{Aut}(F_2)$ generated by r and t preserves each of the slices, and we will examine the action of this subgroup on these conic sections. As our discussion is necessarily rather notation-intensive, it may be helpful to read this

https://doi.org/10.1017/S0017089512000675 Published online by Cambridge University Press

section in tandem with the concrete examples presented in Section 14, and Figure 5 in Section 16.

Sections 15 through 18 are specialized to even values of q. A number of simplifications occur, which allow us to obtain a more workable description of the action within a fixed slice. Even with all this information, our proof of the Classification Conjecture in Section 18 requires further strong assumptions on $q-1$ and $q+1$.

For each $\ell \in \mathbb{F}_q$, we denote $Q^{-1}(\ell)$ by Q_ℓ, and call it a *level surface* of Q, or a *Q-level.* For $\alpha \in \mathbb{F}_q$, define U_α to be the set of $\mathbb{F}_q$-triples whose first entry is equal to α, and for $\ell \in \mathbb{F}_q$, define $U_{\alpha,\ell} = Q_\ell \cap U_\alpha$.

Define $m \in \mathrm{Aut}(F_2)$ by $m = tr$, so $m(a) = a$ and $m(b) = a^{-1}b$, and let $\mathbb{D}$ be the subgroup of $\mathrm{Aut}(F_2)$ generated by $\{r, m\}$. It is an infinite dihedral group, since it is generated by the involutions r and $t = mr$ and their product $m = tr$ has infinite order. We have important formulas for the action of r and m on $\mathbb{F}_q^3$:

$$r(\alpha, \beta, \gamma) = (\alpha, \beta, \alpha\beta - \gamma) \text{ and } m(\alpha, \beta, \gamma) = (\alpha, \gamma, \alpha\gamma - \beta).$$

Since Q is invariant under the action of $\mathrm{Aut}(F_2)$ on $\mathbb{F}_3$, and r and m fix the first coordinate of $\mathbb{F}_q^3$, the action of $\mathbb{D}$ preserves each $U_{\alpha,\ell}$. Any action of $\mathbb{D}$ on a finite set induces an action of a finite quotient of $\mathbb{D}$ that is a dihedral group (allowing the possibilities $D_2 = C_2 \times C_2$, $D_1 = C_2$ and $D_0 = \{1\}$).

Finally, we define another quantity that will play an important role in our work. For $\alpha, \ell \in \mathbb{F}_q$ with $\alpha \neq \pm 2$, define

$$k(\alpha, \ell) = 1 - (\ell - 2)(\alpha^2 - 4)^{-1}.$$

When the values of α and ℓ are fixed, as in the next proposition, we often just write k for $k(\alpha, \ell)$.

PROPOSITION 13.1. *Let $\alpha \in \mathbb{F}_q$ be hyperbolic, and write $\alpha = x + x^{-1}$ for some $x \in \mathbb{F}_q$.*

(1) *When $k \neq 0$, that is, when $\ell \neq \alpha^2 - 2$, $U_{\alpha,\ell}$ is a 'hyperbola' with $q-1$ points. Explicitly, if $C_{\alpha,\ell}$ is the set of pairs $(a, k/a)$ with $a \in \mathbb{F}_q - \{0\}$, then sending $(a, k/a)$ to $(\alpha, a + k/a, ax + (k/a)x^{-1})$ is a bijection from $C_{\alpha,\ell}$ to $U_{\alpha,\ell}$. In these $C_{\alpha,\ell}$-coordinates, the action of $\mathbb{D}$ on $U_{\alpha,\ell}$ becomes $m(a, k/a) = (ax, (k/a)x^{-1})$ and $r(a, k/a) = (k/a, a)$.*

(2) *When $k = 0$, that is, when $\ell = \alpha^2 - 2$, $U_{\alpha,\ell}$ is a 'degenerate hyperbola' with $2q-1$ points, consisting of the two straight lines, $\gamma = x\beta$ and $\gamma = x^{-1}\beta$. The action of $\mathbb{D}$ fixes their intersection point $(\alpha, 0, 0)$, and on the other points it acts by $m(\alpha, \beta, x\beta) = (\alpha, x\beta, x^2\beta)$, $m(\alpha, \beta, x^{-1}\beta) = (\alpha, x^{-1}\beta, x^{-2}\beta)$ and $r(\alpha, \beta, x\beta) = (\alpha, \beta, x^{-1}\beta)$.*

Proof. Assume first that $k \neq 0$. Using the normal form and the Fundamental Equation from Section 10, we find that $U_{\alpha,\ell}$ consists of the set of ordered triples $(\alpha, \beta, \gamma) = (x + x^{-1}, a + d, ax + dx^{-1})$ such that $ad = k$ (with the ordered pair (a, d) uniquely determined by (α, β, γ) and the ordered pair (x, x^{-1})). That is, $\phi\colon C_{\alpha,\ell} \to U_{\alpha,\ell}$ defined by $\phi(a, k/a) = (\alpha, a + k/a, ax + (k/a)x^{-1})$ is a bijection. Using the formulas $r(\alpha, \beta, \gamma) = (\alpha, \beta, \alpha\beta - \gamma)$ and $m(\alpha, \beta, \gamma) = (\alpha, \gamma, \alpha\gamma - \beta)$ and the fact that $\alpha = x + x^{-1}$, one checks that $r\,\phi(a, k/a) = \phi(k/a, a)$ and $m\,\phi(a, k/a) = \phi(ax, (k/a)x^{-1})$.

Changing the choice of which member of the pair $\{x, x^{-1}\}$ is considered to be x does not affect the bijection ϕ or the effects of the actions, since it also interchanges a

https://doi.org/10.1017/S0017089512000675 Published online by Cambridge University Press

and d. The formula $\phi(a, k/a) = (\alpha, a + k/a, ax + (k/a)x^{-1})$ becomes

$$\phi(d, k/d) = (\alpha, d + k/d, dx^{-1} + (k/d)x).$$

The formula for the action r gives $r\phi(d, k/d) = \phi(k/d, d)$ and that for m gives $m\phi(d, k/d) = \phi(dx^{-1}, (k/d)x)$, the same effect as before.

When $k = 0$, the equation $\ell = Q(\alpha, \beta, \gamma)$ works out to $0 = \beta^2 - \alpha\beta\gamma + \gamma^2 = (\beta - x\gamma)(\beta - x^{-1}\gamma)$, giving the two intersecting straight lines for $U_{\alpha,\ell}$. Since $\alpha = x + x^{-1}$, the action of m on the line $\gamma = x\beta$ is

$$m(\alpha, \beta, x\beta) = (\alpha, x\beta, (\alpha x - 1)\beta) = (\alpha, x\beta, x^2\beta)$$

and similarly for the line $\gamma = x^{-1}\beta$. The action of r is

$$r(\alpha, \beta, x^{\pm 1}\beta) = (\alpha, \beta, (\alpha - x^{\pm 1})\beta) = (\alpha, \beta, x^{\mp}\beta).$$

□

PROPOSITION 13.2. *Let $\alpha \in \mathbb{F}_q$ be elliptic, and write $\alpha = x + x^q$ with $x \in \mathbb{F}_{q^2} - \mathbb{F}_q$ and $x^{q+1} = 1$.*

(1) *When $k \neq 0$, that is, when $\ell \neq \alpha^2 - 2$, $U_{\alpha,\ell}$ is an 'ellipse' with $q + 1$ points. Explicitly, if $C_{\alpha,\ell}$ is the set of pairs (a, a^q) with $a \in \mathbb{F}_{q^2}$ and $a^{q+1} = k$, then sending (a, a^q) to $(\alpha, a + k/a, ax + (k/a)x^{-1})$ is a bijection from $C_{\alpha,\ell}$ to $U_{\alpha,\ell}$. In these $C_{\alpha,\ell}$-coordinates, the action of $\mathbb{D}$ on $U_{\alpha,\ell}$ becomes $m(a, k/a) = (ax, (k/a)x^{-1})$ and $r(a, k/a) = (k/a, a)$.*
(2) *When $k = 0$, that is, when $\ell = \alpha^2 - 2$, $U_{\alpha,\ell}$ is a 'degenerate ellipse' consisting only of $(\alpha, 0, 0)$.*

Proof. For $k \neq 0$, calculating as in Proposition 13.1 shows that $U_{\alpha,\ell}$ consists of the set of ordered triples $(\alpha, \beta, \gamma) = (x + x^q, a + a^q, ax + (ax)^q)$ such that $a^{q+1} = k$. In $\mathbb{F}_{q^2}$ there are $q + 1$ choices for a, and the map from $C_{\alpha,\ell}$ to $U_{\alpha,\ell}$ is again seen to be bijective, with the action as described. When $k = 0$, the factorization $0 = (\beta - x\gamma)(\beta - x^{-1}\gamma)$ has the unique solution $(\beta, \gamma) = (0, 0)$ in $\mathbb{F}_q \times \mathbb{F}_q$. □

PROPOSITION 13.3. *Let $\alpha \in \mathbb{F}_q$ be parabolic.*

(1) *For q odd and $\alpha = 2\epsilon$, $Q_{\alpha,\ell}$ is empty if $\ell - 2$ is not a square, while if $\ell - 2 = s^2$, $Q_{\alpha,\ell}$ is the set of triples of the form $(2\epsilon, \beta, \epsilon\beta \pm s)$, which is a pair of disjoint lines if $\ell \neq 2$ and a single line if $\ell = 2$. For $\ell \neq 2$, the action of m is $m(2\epsilon, \beta, \epsilon\beta \pm s) = (2\epsilon, \epsilon\beta \pm s, \epsilon(\epsilon\beta \pm s) \pm \epsilon s)$, so m preserves each line if $\epsilon = 1$ and interchanges them if $\epsilon = -1$, and the action of r is $r(2\epsilon, \beta, \epsilon\beta \pm s) = (2\epsilon, \beta, \epsilon\beta \mp s)$, so r interchanges the two lines. For $\ell = 2$, r acts trivially, and m acts as an involution when $\epsilon = -1$ and trivially when $\epsilon = 1$.*
(2) *For q even and $\ell = s^2$, $Q_{\alpha,\ell}$ is the line consisting of the points of the form $(0, \beta, \beta + s)$. The action of r is trivial and the action of m is $m(0, \beta, \beta + s) = (0, \beta + s, \beta)$, so m is an involution if $\ell \neq 0$ and acts trivially if $\ell = 0$.*

Proof. For q odd and $\alpha = 2\epsilon$, the equation $\ell = Q(\alpha, \beta, \gamma)$ is $\ell - 2 = (\gamma - \epsilon\beta)^2$, so $Q_{\alpha,\ell}$ is empty when $\ell - 2$ is not square. When $\ell - 2 = s^2 \neq 0$, $Q_{\alpha,\ell}$ consists of the two disjoint lines $\gamma = \epsilon\beta \pm s$. We have $m(2\epsilon, \beta, \epsilon\beta \pm s) = (2\epsilon, \epsilon\beta \pm s, \epsilon(\epsilon\beta \pm s) \pm \epsilon s)$, so m preserves each line if $\epsilon = 1$ and interchanges them if $\epsilon = -1$. For r, we have $r(2\epsilon, \beta, \epsilon\beta \pm s) = (2\epsilon, \beta, \epsilon\beta \mp s)$, so r interchanges the two lines. When $\ell - 2 = 0$, we have $\gamma = \epsilon\beta$, and the remarks about the action are easily checked.

https://doi.org/10.1017/S0017089512000675 Published online by Cambridge University Press

1	u	0	0
u	u	0	0
0	1	u	u
$\alpha=0$	0	u	1

1	0	0	u
u	0	u	0
0	u	0	0
$\alpha=u$	0	u	1

1	0	u	0
u	0	0	u
0	u	0	0
$\alpha=1$	0	u	1

Figure 1. Slices for $q = 3$.

1	1	u	u^2	0
u^2	u	1	0	u^2
u	u^2	0	1	u
0	0	u^2	u	1
$\alpha=0$	0	u	u^2	1

1	u	u	1	1
u^2	1	0	0	1
u	0	u	0	u
0	u^2	0	1	u
$\alpha=u$	0	u	u^2	1

1	u^2	1	u^2	1
u^2	0	0	u^2	u^2
u	1	0	0	1
0	u	1	0	u^2
$\alpha=u^2$	0	u	u^2	1

1	0	1	1	0
u^2	u^2	1	u^2	1
u	u	u	1	1
0	1	u	u^2	0
$\alpha=1$	0	u	u^2	1

Figure 2. Slices for $q = 4$.

For q even any ℓ can be written uniquely as s^2. We find $s^2 = Q(\alpha, \beta, \gamma) = (\gamma + \beta)^2$, which says that $\gamma = \beta + s$ and $Q_{\alpha,\ell}$ is a line, and the action works out as stated. □

14. Examples of slices. Figure 1 shows the slices for $\mathbb{F}_3 = \{0, u, 1\}$. For each fixed value of α, the horizontal coordinate is β, the vertical coordinate is γ and the (β, γ)-entry is $Q(\alpha, \beta, \gamma)$.

The 16 triples with $Q(\alpha, \beta, \gamma) = 0$ are the single $\mathrm{Aut}(F_2)$-orbit of traces of generators. The element 0 is a unique elliptic element of $\mathbb{F}_3$, indeed $0 = Z(9)^2 + Z(9)^{-2}$, where $Z(9)$ is the multiplicative generator of $\mathbb{F}_9 - \{0\}$ provided by GAP. The slice for $\alpha = 0$ is as described in Proposition 13.2. We have $k = 1 - (\ell - 2)(0^2 - 4)^{-1} = \ell - 1$, so $k = 0$ occurs for $U_{0,1}$, giving the degenerate ellipse $(0, 0, 0)$, while $U_{0,0}$ and $U_{0,u}$ are ellipses each containing four points. The elements $\alpha = u$ and $\alpha = 1$ are parabolic, and their slices are as described in Proposition 13.3: $U_{u,1}$ and $U_{1,1}$ are empty since $1 - 2 = u$ is not a square, $U_{u,u}$ and $U_{1,u}$ are single lines, and $U_{u,0}$ and $U_{1,0}$ each consist of two lines.

Figure 2 shows the slices for $\mathbb{F}_4 = \{0, u, u^2, 1\}$. The elements u and u^2 are elliptic. There is one parabolic element 0, and one hyperbolic element $1 = u + u^{-1}$. In the slice for $\alpha = 1$, the degenerate hyperbola is $U_{1,1}$, which consists of the straight lines $\{(1, \beta, u\beta)\}$ and $\{(1, \beta, u^2\beta)\}$, which intersect in $(1, 0, 0)$. The level surface U_1 consists of the three inessential triples $(1, 0, 0)$, $(0, 1, 0)$ and $(0, 0, 1)$, and one $\mathrm{Aut}(F_2)$-orbit of length 18.

Finally, Figures 3 and 4 show the slices for $\mathbb{F}_8$ for $\alpha = u$ and $\alpha = u^3$. Since u is elliptic, U_u contains one degenerate ellipse $(u, 0, 0)$ and seven nondegenerate ellipses each containing nine points. The element u^3 is hyperbolic, and U_{u^3} contains one degenerate hyperbola of 15 points and seven nondegenerate hyperbolas of seven points each. In these two figures we have indicated the degenerate conics in boldface.

https://doi.org/10.1017/S0017089512000675 Published online by Cambridge University Press

1	u^6	u^6	0	u^4	0	u^3	u^3	u^4
u^6	u^3	u^6	1	u^6	u^5	u^5	1	u^3
u^5	u^5	u	u^3	u^4	u^4	u	u^5	u^3
u^4	u^4	u^5	1	1	0	u^4	u^5	0
u^3	1	u	u	u^6	1	u^4	u^6	u^4
u^2	u	0	u^3	u	1	u^3	1	0
u	0	u^5	0	u	u^5	u	u^6	u^6
0	$\mathbf{u^2}$	0	u	1	u^4	u^5	u^3	u^6
$\alpha = u$	0	u	u^2	u^3	u^4	u^5	u^6	1

Figure 3. Slice for $q = 8$ and $\alpha = u$.

1	u^2	u^4	$\mathbf{u^6}$	u^2	u^5	$\mathbf{u^6}$	u^5	u^4
u^6	u	$\mathbf{u^6}$	u	0	$\mathbf{u^6}$	0	u^5	u^5
u^5	u^4	u^4	u^3	$\mathbf{u^6}$	u^3	0	0	$\mathbf{u^6}$
u^4	u^5	1	$\mathbf{u^6}$	1	u^3	u^3	$\mathbf{u^6}$	u^5
u^3	0	$\mathbf{u^6}$	u^2	1	1	$\mathbf{u^6}$	0	u^2
u^2	u^3	u	u^2	u^2	$\mathbf{u^6}$	u^3	u	$\mathbf{u^6}$
u	1	u	u	$\mathbf{u^6}$	1	u^4	$\mathbf{u^6}$	u^4
0	$\mathbf{u^6}$	1	u^3	0	u^5	u^4	u	u^2
$\alpha = u^3$	0	u	u^2	u^3	u^4	u^5	u^6	1

Figure 4. Slice for $q = 8$ and $\alpha = u^3$.

15. Parabolic, elliptic and hyperbolic elements in characteristic 2. Recall that if $r = p^m$ is a prime power and $n > 1$, the trace map $\tau\colon \mathbb{F}_{r^n} \to \mathbb{F}_r$ is the $\mathbb{F}_r$-linear transformation defined by $\tau(x) = x + x^{p^m} + x^{p^{2m}} + \cdots + x^{p^{(n-1)m}}$. The trace map has many well-known properties which can be found in texts on finite fields such as [**13**]. In particular, $\tau(xy)$ defines a nondegenerate symmetric $\mathbb{F}_r$-valued bilinear form on $\mathbb{F}_{r^n} \times \mathbb{F}_{r^n}$, making $\mathbb{F}_{r^n}$ an inner product space over $\mathbb{F}_r$. Consequently, every subspace W determines an orthogonal subspace $W^\perp$ of complementary dimension. Since the characteristic is non-zero, W and $W^\perp$ may have nontrivial intersection. The kernel of τ is exactly $\mathbb{F}_r^\perp$.

In characteristic 2, the trace map leads to an elegant and useful description of the sets H and E of hyperbolic and elliptic elements respectively. Let q be even, and for $S \subseteq \mathbb{F}_q - \{0\}$, denote by S^{-1} the set consisting of the inverses of the elements of S. Since 0 is a unique parabolic element when q is even, both H^{-1} and E^{-1} are defined.

LEMMA 15.1. *Let q be even and let $\tau\colon \mathbb{F}_q \to \mathbb{F}_2$ be the trace map to $\mathbb{F}_2$. Then $\tau(\alpha) = 0$ if and only if $\alpha = 0$ or $\alpha \in H^{-1}$, and $\tau(\alpha) = 1$ if and only if $\alpha \in E^{-1}$.*

Proof. Since $\mathbb{F}_q$ is the disjoint union $\{0\} \cup H^{-1} \cup E^{-1}$, it suffices to prove that for $\alpha \neq 0$, $\tau(\alpha) = 0$ if and only if $\alpha^{-1} \in H$.

Fix $\alpha \neq 0$ and suppose first that $\alpha^{-1} \in H$. Then $x^2 + \alpha^{-1}x + 1 = 0$ for some $x \in \mathbb{F}_q$, so $(\alpha x)^2 + (\alpha x) + \alpha^2 = 0$. Since $\tau((\alpha x)^2) = \tau(\alpha x)$, applying τ to this equation gives $\tau(\alpha^2) = 0$ and hence $\tau(\alpha) = 0$.

Conversely, suppose that $\tau(\alpha)$ and hence $\tau(\alpha^2)$ are 0. For any $\beta \in \mathbb{F}_q$, $\tau(\beta^2 + \beta) = 0$, therefore the $q/2$ elements of this form are exactly the kernel of τ. Writing $\alpha^2 = \beta^2 + \beta$ and multiplying by α^{-2} shows that $x^2 + \alpha^{-1}x + 1 = 0$ has a solution, so $\alpha^{-1} \in H$. □

For odd characteristics, we do not know a result analogous to Lemma 15.1.

https://doi.org/10.1017/S0017089512000675 Published online by Cambridge University Press

1	0	u^4	u	u^4	$[u^2]$	$[u^2]$	u	0
u^6	u^4	u^3	u	u^5	u^5	u^3	u^4	u
u^5	u	u^3	u^6	u^6	$[u^2]$	u	u^3	$[u^2]$
u^4	u^3	0	0	u^5	u^3	$[u^2]$	u^5	$[u^2]$
u^3	(u^2)	u^4	u^6	(u^2)	u^5	u^6	u^5	u^4
u^2	u^5	0	u^5	u^6	0	u^6	u	u
u	u^6	u^6	0	u^4	0	u^3	u^3	u^4
0	1	u^6	u^5	(u^2)	u^3	u	u^4	0
$\alpha=1$	(0)	u	u^2	(u^3)	$[u^4]$	$[u^5]$	u^6	$[1]$

Figure 5. The slice for $q = 8$ and $\alpha = 1$. The ellipse U_{1,u^2} consists of two $\mathbb{D}$-orbits, one enclosed in parentheses and the other in brackets. The corresponding β-coordinate sets are also enclosed in parentheses and brackets.

Lemma 15.1 has the following consequences.

COROLLARY 15.2. *Let q be even and let W denote the subspace of $\mathbb{F}_q$ spanned by the subset $\{\kappa_1, \ldots, \kappa_r\}$ of $\mathbb{F}_q$. Then $(\kappa_1 H \cap \cdots \cap \kappa_r H)^{-1} \cup \{0\} = W^\perp$.*

Proof. Using Lemma 15.1, $x \in (\kappa H)^{-1} \cup \{0\} = \kappa^{-1}(H^{-1} \cup \{0\})$ if and only if $\tau(\kappa x) = 0$, that is, $x \in (\kappa\, \mathbb{F}_2)^\perp$. So $(\cap \kappa_i H)^{-1} \cup \{0\} = \cap(\kappa_i\, \mathbb{F}_2)^\perp = W^\perp$. □

COROLLARY 15.3. *Let q be even and suppose that the elements $\kappa_1, \ldots, \kappa_n$ of $\mathbb{F}_q$ are linearly independent over $\mathbb{F}_2$. Then*

(a) *$\cap_{j=1}^n \kappa_j E$ contains $q/2^n$ elements.*
(b) *For $1 \le m \le n$, $(\cap_{i=1}^m \kappa_i H) \cap (\cap_{j=m+1}^n \kappa_j E)$ contains $q/2^n - 1$ elements.*

Proof. Corollary 15.2 shows that $\cap_{i=1}^n \kappa_i H$ has $q/2^n - 1$ elements, which is part (b) for $m = n$. Now, let $K_i = \kappa_i H \cup \{0\}$, so that $\cap_{i=1}^n K_i = \{0\} \cup (\cap_{i=1}^n \kappa_i H)$ has $q/2^n$ elements. Write L_i for $\mathbb{F}_q - K_i$, which is $\kappa_i E$. Inducting on $n - m$, we have $1 + |(\cap_{i=1}^m \kappa_i H) \cap (\cap_{j=m+1}^n \kappa_j E)| = |(\cap_{i=1}^m K_i) \cap (\cap_{j=m+1}^n L_j)| = |(\cap_{i=1}^m K_i) \cap (\cap_{j=m+2}^n L_j)| - |(\cap_{i=1}^{m+1} K_i) \cap (\cap_{j=m+2}^n L_j)| = q/2^{n-1} - q/2^n = q/2^n$, establishing the rest of (b). Part (a) follows from induction and part (b) since $|(\cap_{j=1}^n L_j)| = |(\cap_{j=2}^n L_j)| - |K_1 \cap (\cap_{j=2}^n L_i)| = q/2^{n-1} - q/2^n$. □

16. β-coordinates in characteristic 2. Throughout this section we assume that q is even so that $q = 2^s$ for some s. For x in $\mathbb{F}_q$, we denote the unique square root $x^{q/2}$ of x by $\sqrt{x}$. The value $k = 1 - (\ell - 2)(\alpha^2 - 4)^{-1}$ from Section 13 becomes $k = 1 + \ell\alpha^{-2}$, so $k = 0$ exactly when $\alpha = \sqrt{\ell}$. We introduce the notation

$$\kappa = \kappa(\alpha, \ell) = 1 + \sqrt{\ell}\alpha^{-1}$$

for the square root of k.

The slice in Figure 5 may be helpful in understanding the general description in this section. It shows the slice Q_1 for $q = 8$. For $q = 8$, $1 = v^3 + v^{-3}$ is elliptic. We focus on the ellipse U_{1,u^2}, for which $\kappa = 1 + \sqrt{u^2} \cdot 1 = u^3$.

In characteristic 2, the set of values of the second coordinate β that appear in triples in $U_{\alpha,\ell}$ can be described in a somewhat simpler way. Denote this set by $\beta(U_{\alpha,\ell})$. Suppose first that α is hyperbolic so that Proposition 13.1 applies. When $\kappa = 0$, it

https://doi.org/10.1017/S0017089512000675 Published online by Cambridge University Press

shows that $\beta(U_{\alpha,\ell}) = \mathbb{F}_q$, while for $\kappa \neq 0$ it gives

$$\beta(U_{\alpha,\ell}) = \{a + \kappa^2/a \mid a \in \mathbb{F}_q^*\} = \{\kappa(a/\kappa + (a/\kappa)^{-1}) \mid a \in \mathbb{F}_q^*\} = \kappa H \cup \{0\},$$

where $\mathbb{F}_q^*$ denotes $\mathbb{F}_q - \{0\}$ and as usual H denotes the set of hyperbolic elements of $\mathbb{F}_q$. Similarly, applying Proposition 13.2 when α is elliptic shows that for $\kappa = 0$, $\beta(U_{\alpha,\ell}) = \{0\}$ and for $\kappa \neq 0$

$$\beta(U_{\alpha,\ell}) = \kappa E \cup \{0\},$$

although a couple of details should be mentioned. First, since $\kappa \in \mathbb{F}_q$, we have $(a/\kappa)^{q+1} = k/\kappa^{q+1} = \kappa^2/\kappa^2 = 1$, so $a/\kappa + (a/\kappa)^{-1}$ is indeed elliptic. Second, we obtain 0 in $\beta(U_{\alpha,\ell})$ since $\kappa^{q+1} = \kappa^2 = k$ and $\kappa + k/\kappa = 0$, while the other values of a with $a^{q+1} = k$ do not lie in $\mathbb{F}_q$ so produce the elements of κE.

In the example of Figure 5, $E = \{u, u^2, u^4, 1\}$, and

$$\beta(U_{1,u^2}) = \kappa E \cup \{0\} = u^3\{u, u^2, u^4, 1\} \cup \{0\} = \{0, u^3, u^4, u^5, u^7\}.$$

We will need to understand the β-coordinates of the $\mathbb{D}$-orbits of $U_{\alpha,\ell}$, where $\mathbb{D}$ is the subgroup of $\mathrm{Aut}(F_2)$ generated by $\{r, m\}$ as discussed near the beginning of Section 13. To simplify notation, write

$$h(i) = u^i + u^{-i},$$

noting that $h(i) = h(-i) = h(i \pm (q-1))$ and $h(0) = 0$. Also, the function from $\mathbb{F}_q$ to $H \cup \{0\}$ sending 0 to 0 and x to $x + x^{-1}$ is 2-to-1, so $h(i) = h(j)$ for $0 \leq i, j \leq q-1$ only when $i = j$ or $i = q - 1 - j$.

Now fix a hyperbolic element $\alpha = h(d)$. Denote $\gcd(d, q-1)$ by d_0 so that the order of u^d in $\mathbb{F}_q^*$ is $(q-1)/d_0$, which we denote by d_1. For $n \in \mathbb{Z}$, put

$$H_{d_0}(n) = \{h(d_0 i + n) \mid i \in \mathbb{Z}\}.$$

The next lemma gives some useful properties of the sets $H_{d_0}(n)$.

LEMMA 16.1. *Let* $d_1 = (q-1)/d_0$.

(a) $H_{d_0}(-n) = H_{d_0}(n)$.

(b) $H_{d_0}(n \pm d_0) = H_{d_0}(n)$.

(c) $H_{d_0}(0)$ *contains* $(d_1 + 1)/2$ *elements, and each* $H_{d_0}(n)$ *for* $1 \leq n \leq (d_0 - 1)/2$ *contains* d_1 *elements.*

(d) *The sets* $H_{d_0}(0), \ldots, H_{d_0}(\frac{d_0-1}{2})$ *form a partition of* $H \cup \{0\}$.

Proof. Part (a) follows since $\{h(d_0 i - n) \mid i \in \mathbb{Z}\} = \{h(d_0(-i) - n) \mid i \in \mathbb{Z}\} = \{h(d_0 i + n) \mid i \in \mathbb{Z}\}$, and part (b) is similar. Part (c) follows from the fact that $h(i) = h(j)$ for $0 \leq i, j \leq q-1$ only when $i = j$ or $i = q - 1 - j$, which also shows that the sets in (d) are disjoint and establishes (d). Part (d) also follows since the union of the sets in (d) is $H \cup \{0\}$ by parts (a) and (b), and the numbers of their elements given in (c) sum to $q/2$, the number of elements of $H \cup \{0\}$. □

PROPOSITION 16.2. *Let* $\alpha = h(d)$ *be a hyperbolic element of* $\mathbb{F}_q$. *Put* $d_0 = \gcd(d, q-1)$ *and* $d_1 = (q-1)/d_0$. *Let* ℓ *be one of the* $q-1$ *values for which* $\kappa \neq 0$, *then* $\beta(U_{\alpha,\ell}) = \kappa H \cup \{0\}$. *Moreover:*

https://doi.org/10.1017/S0017089512000675 Published online by Cambridge University Press

(1) *The sets of β-coordinates of the $\mathbb{D}$-orbits of $U_{\alpha,\ell}$ are $\kappa H_{d_0}(0)$, $\kappa H_{d_0}(1), \ldots, \kappa H_{d_0}((d_0-1)/2)$.*
(2) *$\kappa H_{d_0}(0)$ contains $(d_1+1)/2$ elements, and each $\kappa H_{d_0}(n)$ for $1 \le n \le (d_0-1)/2$ contains d_1 elements.*

Proof. The fact that $\beta(U_{\alpha,\ell}) = \kappa H \cup \{0\}$ was noted earlier in this section. Part (2) is immediate from Lemma 16.1. For part (1), let $\kappa h(i) \in \beta(U_{\alpha,\ell})$. From the description of the action of m given in Proposition 13.1, the β-coordinate of the image under m of a point with β-coordinate $\kappa\, h(i) = \kappa u^i + \kappa^2(1/(\kappa u^i))$ is $\kappa u^{d+i} + \kappa^2(1/(\kappa u^{d+i})) = \kappa\, h(d+i)$, so these images produce $\kappa H_{d_0}(i)$. Since r fixes the β-coordinate of each point, the set of β-coordinates of an m-orbit is the same set as the β-coordinates of the $\mathbb{D}$-orbit that contains it. □

For elliptic elements, we put $e(d) = v^d + v^{-d}$, $d_0 = \gcd(d, q+1)$, and

$$E_{d_0}(n) = \{e(d_0 i + n) \mid i \in \mathbb{Z}\}.$$

Analogously to Lemmas 16.1 and 16.2, we have

LEMMA 16.3. *Let $d_1 = (q+1)/d_0$.*
(a) *$E_{d_0}(-n) = E_{d_0}(n)$.*
(b) *$E_{d_0}(n \pm d_0) = E_{d_0}(n)$.*
(c) *$E_{d_0}(0)$ contains $(d_1+1)/2$ elements, and each $E_{d_0}(n)$ for $1 \le n \le (d_0-1)/2$ contains d_1 elements.*
(d) *The sets $E_{d_0}(0), \ldots, E_{d_0}(\frac{d_0-1}{2})$ form a partition of $E \cup \{0\}$.*

PROPOSITION 16.4. *Let $\alpha = e(d)$ be an elliptic element of $\mathbb{F}_q$. Put $d_0 = \gcd(d, q+1)$ and $d_1 = (q+1)/d_0$. Let ℓ be one of the $q-1$ values for which $\kappa \neq 0$. Then $\beta(U_{\alpha,\ell}) = \kappa E \cup \{0\}$. Moreover:*
(1) *The sets of β-coordinates of the $\mathbb{D}$-orbits of $U_{\alpha,\ell}$ are $\kappa E_{d_0}(0)$, $\kappa E_{d_0}(1), \ldots, \kappa E_{d_0}((d_0-1)/2)$.*
(2) *The set $\kappa E_{d_0}(0)$ contains $(d_1+1)/2$ elements, and each $\kappa E_{d_0}(j)$ for $1 \le j \le (d_0-1)/2$ contains d_1 elements.*

In the example of Figure 5, $d = 3$, $d_0 = d_1 = 3$, $E_{d_0}(0) = E_3(0) = \{0, 1\}$ and $E_{d_0}(1) = E_3(1) = \{u, u^2, u^4\}$, so the β-sets for the orbits of $\mathbb{D}$ are

$$\kappa E_3(0) = u^3\{0, 1\} = \{0, u^3\} \text{ and } \kappa E_3(1) = u^3\{u, u^2, u^4\} = \{u^4, u^5, 1\}\,.$$

17. Transitive elements. We continue to assume that q is even. A hyperbolic (respectively, elliptic) element α is called *transitive* exactly when $\alpha = h(d)$ (respectively, $\alpha = e(d)$) with $\gcd(d, q-1) = 1$ (respectively, $\gcd(d, q+1) = 1$). We remark that a matrix $A \in \mathrm{SL}(2, q)$ with hyperbolic or elliptic trace has (respectively) order $q-1$ or $q+1$ in $\mathrm{PSL}(2, q)$ if and only if $\mathrm{tr}(A)$ is transitive. For, since $\mathrm{Tr}(m^k(A, B)) = (\mathrm{tr}(A), \mathrm{tr}(A^{-k}B), \mathrm{tr}(A^{-k+1}B))$, the order of A is the order of m acting on the slice U_α, and Proposition 13.1 or 13.2 shows that this order is $\gcd(d, q-1)$ or $\gcd(d, q+1)$ accordingly as $\alpha = \mathrm{tr}(A)$ is hyperbolic or elliptic.

Write $V_{\alpha,\ell}$ for $U_{\alpha,\ell} - \{(\alpha, 0, 0)\}$. We have $V_{\alpha,\ell} = U_{\alpha,\ell}$ except when $\kappa = 0$, that is, when $\ell = \alpha^2$.

For two subsets X, $Y \subset \mathbb{F}_q^3$, we write $X \sim_M Y$ when every element of X is Markov equivalent to every element of Y.

https://doi.org/10.1017/S0017089512000675 Published online by Cambridge University Press

PROPOSITION 17.1. *Suppose that q is even, $q \geq 16$ and $q-1$ or $q+1$ is prime. Then for each $\ell \neq 0$, there is a Markov equivalence class that contains $V_{\alpha,\ell}$ for every transitive element α of $\mathbb{F}_q$.*

Proof. Fix $\ell \neq 0$. Propositions 13.1 and 13.2 show that for all transitive α, $\mathbb{D}$ acts transitively on each $V_{\alpha,\ell}$, that is, the elements of each $V_{\alpha,\ell}$ are Markov equivalent.

Suppose for now that $q-1$ is prime so that every hyperbolic element is transitive. We fix a hyperbolic element α_1, and will prove that $V_{\alpha_1,\ell} \sim_M V_{\alpha_2,\ell}$ for any transitive element α_2.

Write κ_i for $1+\sqrt{\ell}\alpha_i^{-1}$. Note that $\kappa_i \neq 1$, since $\ell \neq 0$ and $\alpha_i \neq 0$.

It is sufficient to prove that $\beta(V_{\alpha_1,\ell}) \cap \beta(V_{\alpha_2,\ell})$ contains a transitive element α_3. For then, each $V_{\alpha_i,\ell}$ contains a point of the form $(\alpha_i, \alpha_3, \gamma_i)$. The points $(\alpha_3, \alpha_i, \gamma_i)$ lie in $V_{\alpha_3,\ell}$, so are equivalent. Since $(\alpha_i, \alpha_3, \gamma_i) \sim_M (\alpha_3, \alpha_i, \gamma_i)$, $V_{\alpha_1,\ell} \sim_M V_{\alpha_3,\ell} \sim_M V_{\alpha_2,\ell}$.

Suppose that $\kappa_1 = 0$. By Proposition 13.1, $\beta(V_{\alpha_1,\ell}) = \mathbb{F}_q^*$, so $\alpha_2 \in \beta(V_{\alpha_1,\ell})$, that is, $V_{\alpha_1,\ell}$ contains a point of the form $(\alpha_1, \alpha_2, \gamma)$. This is equivalent to $(\alpha_2, \alpha_1, \gamma) \in V_{\alpha_2,\ell}$ so $\alpha_1 \in \beta(V_{\alpha_2,\ell})$. Since also $\alpha_1 \in \beta(V_{\alpha_1,\ell})$, we have $V_{\alpha_1,\ell} \sim_M V_{\alpha_2,\ell}$. The argument is the same if $\kappa_2 = 0$ and α_2 is hyperbolic. If $\kappa_2 = 0$ and α_2 is elliptic, then $V_{\alpha_2,\ell}$ is empty and there is nothing to prove. So we may assume that both κ_i are non-zero.

Since α_1 is hyperbolic, Proposition 16.2 implies that $\beta(V_{\alpha_1,\ell}) = \kappa_1 H$. By Propositions 16.2 and 16.4, $\beta(V_{\alpha_2,\ell})$ is $\kappa_2 H$ if α_2 is hyperbolic and $\kappa_2 E$ if it is elliptic. Since $q \geq 16$, Corollary 15.3 shows that $\kappa_1 H \cap \kappa_2 H \cap H$ and $\kappa_1 H \cap \kappa_2 E \cap H$ are nonempty, so in either case there is a transitive element in $\beta(V_{\alpha_1,\ell}) \cap \beta(V_{\alpha_2,\ell})$. □

18. Proof of the Classification Conjecture in a restricted case. In this section we will use the previous analysis of the Markov orbits in $\mathbb{F}_q^3$ to prove the Classification Conjecture in an extremely restricted case, stated in Theorem 18.2. We finish the section with some comments on the proof and its possible extension to more general cases.

We will use the following easy observation about cyclic groups of prime order.

LEMMA 18.1. *Let C_P be a cyclic group of prime order P, and let $S \subseteq C_P$. Suppose that $x \in C_P$ with $x \neq 1$. If $xS = S$, then S is either empty or $S = C_P$. Suppose that S is a nonempty, proper subset and $xS \subset S \cup \{y\}$. Then S is of the form $\{x^{-1}y, x^{-2}y, \ldots, x^{-n}y\}$ for some n.*

Proof. The first statement is immediate since x must be a generator of C_P. For the second statement, consider the subset $S' = \{x^{-1}y, x^{-2}y, \ldots, x^{-n}y\}$, where $n+1$ is the minimal value for which $x^{-(n+1)}y \notin S$. Then $x(S - S') = S - S'$, so $S' = S$. □

THEOREM 18.2. *Let $q = 2^s$ and suppose that one of $q+1$ or $q-1$ is prime and the other is three times a prime. Then there are exactly $q-1$ Markov classes of essential triples classified by their Q-values.*

Theorem 18.2 is the Q-Classification Conjecture for these values of q, and since we are in characteristic 2, Corollary 8.4 shows that the Q-Classification Conjecture implies the Classification Conjecture.

The only case of Theorem 18.2 for $q+1$ prime is $s = 4$. For numbers of the form $2^{2k+1}+1$ are always divisible by 3, while if $s = 2k$ then $q-1$ factors as $(2^k-1)(2^k+1)$ and is of the form $3p_1$ only when $k = 2$. For $q-1$ prime, Theorem 18.2 applies when $s \in \{3, 5, 7, 13, 17, 19, 31, 61, 127\}$, and perhaps for other values as well. It might apply to infinitely many cases, of course it is a well-known open problem even to determine whether there are infinitely many primes among the Mersenne numbers $2^s - 1$.

https://doi.org/10.1017/S0017089512000675 Published online by Cambridge University Press

Proof of Theorem 18.2. We may assume that $q \geq 16$, since the theorem can be checked by calculation when $q \leq 8$.

Fix $\ell \in \mathbb{F}_q - \{0\}$ and suppose first that $q-1$ is prime and $q+1 = 3p_1$ with p_1 prime. Since $q-1$ is prime, all hyperbolic elements are transitive, and Proposition 17.1 shows that there is a Markov class $M(\ell)$ containing $V_{\alpha,\ell}$ for all transitive elements α.

Any pair with trace $(\alpha, 0, 0)$ generates a dihedral subgroup in $\mathrm{PSL}(2, q)$, so the triple $(\alpha, 0, 0)$ is never essential. Consequently $M(\ell)$ contains all the essential triples in $U_{\alpha,\ell}$ for each transitive α.

Using the notation of Proposition 16.4, the set of nontransitive elements is $E_3(0) \cup E_{p_1}(0)$. Explicitly, $E_{p_1}(0) = \{0, 1 = v^{p_1} + v^{-p_1}\}$ and $E_3(0) = \{v^{3i} + v^{-3i} \mid 0 \leq i \leq (q+4)/6\}$. Therefore, the set of nontransitive elements is $E_3(0) \cup \{1\}$. Since $E_3(0)$ contains $(p_1+1)/2$ elements, $E_3(0) \cup \{1\}$ contains $(p_1+3)/2$ elements (when $q = 8$, which we are excluding, $1 \in E_3(0)$ so $E_3(0) \cup \{1\}$ contains only $(p_1+1)/2$ elements).

Fix an essential triple $(\alpha, \beta, \gamma) \in U_{\alpha,\ell}$ with all coordinates nontransitive. We may assume that α and β are non-zero, and hence elliptic. We must have $\kappa \neq 0$, since otherwise Proposition 13.2 shows that $U_{\alpha,\ell} = \{(\alpha, 0, 0)\}$ contains no essential triple.

Suppose for contradiction that $(\alpha, \beta, \gamma) \notin M(\ell)$. Then none of α, β or γ can be transitive. Since (α, β, γ) is essential, its coordinates do not all lie in a proper subfield, so we may assume that $\alpha \notin \{0, 1\}$, and hence $\alpha \in E_3(0) - E_{p_1}(0)$. Also, we cannot have $\beta = \gamma = 0$, since (α, β, γ) is essential, so we may assume that $\beta \neq 0$.

By Proposition 16.4, the set of β-coordinates for the $\mathbb{D}$-orbit of (α, β, γ) is $\kappa E_3(0) \cup \kappa E_3(1)$, with each of these two sets being the set of β-coordinates for some $\mathbb{D}$-orbit of $U_{\alpha,\ell}$. If $\beta \in \kappa E_3(1)$, then since $\kappa E_3(1)$ contains p_1 values, and there are only $(p_1+3)/2$ nontransitive elements, (α, β, γ) is Markov equivalent to some $(\alpha, \beta', \gamma')$ with β' transitive, so $(\alpha, \beta, \gamma) \in M(\ell)$. So we have $\beta \in \kappa E_3(0)$ and $\kappa E_3(0) \subseteq E_3(0) \cup \{1\}$. Lemma 18.1 shows that $E_3(0)$ is of the form $\{0, \kappa^{-1}, \kappa^{-2}, \ldots, \kappa^{-(p_1-1)/2}\}$.

Now $E_3(0)$ is closed under the Frobenius automorphism, since $(v^{3i} + v^{-3i})^2 = v^{6i} + v^{-6i}$. But κ has order $q-1$, so $(\kappa^{-(p_1-1)/2})^2 = \kappa^{-(p_1-1)}$ is not in $\{0, \kappa^{-1}, \kappa^{-2}, \ldots, \kappa^{-(p_1-1)/2}\}$, giving a contradiction to Lemma 18.1. Therefore, $\kappa E_3(0)$ contains a transitive element, that is, (α, β, γ) is equivalent to some $(\alpha, \beta', \gamma')$ with β' transitive, so $(\alpha, \beta, \gamma) \in M(\ell)$.

Suppose now that $q+1$ is prime and $q-1 = 3p_1$. As noted above, this implies that $q = 16$. The nontransitive elements are 0, $u^5 + u^{-5} = u^{10} + u^{-10} = 1$, $u^3 + u^{-3} = u^{10}$ and $u^6 + u^{-6} = u^5$. That is, the set of nontransitive elements is $\mathbb{F}_4$. Therefore, each coordinate of any triple of nontransitive elements has a trace of an element of $\mathbb{F}_4$, and (as shown in Section 11) such a triple cannot be essential. That is, every essential triple contains a transitive element, so lies in the orbit $M(\ell)$. □

The phenomenon in the last paragraph of the previous proof is unfortunately not universal, as an essential triple need not contain a nontransitive element. For example, when $q = 64$, the element $u^3 + u^{-3} = u^{23}$ is non-transitive, but (by the criteria in Section 11) the triple (u^{23}, u^{23}, u^{23}) is essential.

A roadblock to extending Theorem 18.2 to more values of q is our inability to make some usable statement about the effect of the element m on β-coordinates, specifically about the values of i and j that are obtained when elements of the form $\kappa(a + \kappa/a)$ are rewritten in the form $u^i + u^{-i}$ or $v^j + v^{-j}$. Our approach to Theorem 18.2 seems hopeless for odd q, as it relies on several major simplifications that do not seem to have analogues in the odd case.

https://doi.org/10.1017/S0017089512000675 Published online by Cambridge University Press

As remarked in Section 1, the key role played by transitive elements, while possibly an artifact of our approach to Theorem 18.2, gives some reason for caution about the conjectures. The cases for which they are known to hold, that is, $q \leq 101$ and the cases of Theorem 18.2, all have rather high densities of transitive elements, so in this sense they are not representatives of the general case. For large q not satisfying some hypotheses such as those in Theorem 18.2, this density can be arbitrarily close to 0.

19. The case of PSL(2, q)**.** In this section, we will adapt the conjectures to the case of PSL(2, q). Since PSL(2, q) = SL(2, q) when q is even, we will assume throughout this section that q is odd.

For now, we consider coefficients in an arbitrary field F of characteristic not 2. When (A, B) represents a pair in PSL(2, F) so that A and B are only defined up to sign, the commutator $[A, B]$ is a well-defined element of SL(2, F), and we regard the Higman invariant as $H\colon \overline{\mathcal{N}} \to \mathcal{E}$, where $\overline{\mathcal{N}}$ is the set of Nielsen classes of generating pairs of PSL(2, F) and $\mathcal{E}$ is the set of extended conjugacy classes in SL(2, F). To make the trace function Tr well defined on $\overline{\mathcal{N}}$, it is sufficient to extend Markov equivalence by adding the additional involution $(\alpha, \beta, \gamma) \to (-\alpha, \beta, -\gamma)$ (note that this together with the action of s that sends $(\alpha, \beta, \gamma) \to (\beta, \alpha, \gamma)$ makes (α, β, γ) also equivalent to $(\alpha, -\beta, -\gamma)$). This extends the PGL(2, $\mathbb{Z}$)-action on F^3 to an action of $C_2 \circ$ PGL(2, $\mathbb{Z}$) whose orbits we denote by $\overline{\mathcal{M}}$.

For finite F, at least, the following conjecture seems reasonable:

CONJECTURE P (*No essential difference between* SL *and* PSL). $\mathcal{N} \to \overline{\mathcal{N}}$ and $\mathcal{M} \to \overline{\mathcal{M}}$ are bijections.

Specializing to the case $F = \mathbb{F}_q$, the Classification Conjecture implies that $\mathcal{N} \to \overline{\mathcal{N}}$ is bijective, since $H\colon \mathcal{N} \to \mathcal{C}$ factors as $\mathcal{N} \to \overline{\mathcal{N}} \to \mathcal{C}$ with the first map surjective. Similarly, the Q-Classification Conjecture implies that $\mathcal{M} \to \overline{\mathcal{M}}$ is bijective. Therefore, the Classification Conjecture implies Conjecture P. Similarly, the T-Classification Conjecture implies that $\mathcal{T} \to \overline{\mathcal{T}}$ is a bijection, where $\overline{\mathcal{T}}$ denotes the T-systems of PSL(2, q).

On the other hand, versions of the conjectures for PSL(2, q) imply weak forms of the conjectures for SL(2, q) by means of the following observation.

PROPOSITION 19.1. *The natural maps* $\mathcal{N} \to \overline{\mathcal{N}}$ *and* $\mathcal{M} \to \overline{\mathcal{M}}$ *are* (≤ 2)*-to-*1.

Proof. Suppose that (A, B) and (A', B') in $\mathcal{G}_2(\mathrm{SL}(2, q))$ are Nielsen equivalent as elements of $\mathcal{G}_2(\mathrm{PSL}(2, q))$. A sequence of Nielsen moves changing (A', B') to (A, B) up to signs changes (A', B') to one of (A, B), $(-A, B)$, $(A, -B)$, or $(-A, -B)$.

If A has odd order k, then $(-A)^k = -I$, so $(-A, B) \sim (-A, -B)$, where $\sim$ indicates Nielsen equivalence. On the other hand, if A has even order $2k$, then $A^k = -I$ so $(A, B) \sim (A, -B)$. By the same reasoning applied to B, either $(A, -B) \sim (-A, -B)$ or $(A, B) \sim (-A, B)$. Each of the four possible combinations lead to (at least) three of (A, B), $(-A, B)$, $(A, -B)$ or $(-A, -B)$ being Nielsen equivalent, showing that $\mathcal{N} \to \overline{\mathcal{N}}$ is (≤ 2)-to-1.

Since the four equivalent $\mathbb{F}_q$-triples (α, β, γ), $(-\alpha, \beta, -\gamma)$, $(\alpha, -\beta, -\gamma)$ and $(-\alpha, -\beta, \gamma)$ are the traces of (A, B), $(-A, B)$, $(A, -B)$ and $(-A, -B)$, the previous argument shows that they lie in at most two Markov classes. It follows that $\mathcal{M} \to \overline{\mathcal{M}}$ is (≤ 2)-to-1. □

https://doi.org/10.1017/S0017089512000675 Published online by Cambridge University Press

Consider, for example, the following conjecture:

PROJECTIVE CLASSIFICATION CONJECTURE *(Higman invariant classifies projective Nielsen classes)*. $H\colon \overline{\mathcal{N}} \to \mathcal{E}$ is injective.

The Projective Classification Conjecture together with Proposition 19.1 then imply that $H\colon \mathcal{N} \to \mathcal{E}$ is (≤ 2)-to-1, a weak form of the Classification Conjecture. The patterns are similar for the Q-Classification Conjecture and the T-Classification Conjecture.

ACKNOWLEDGMENT. The first author was supported in part by NSF grant DMS-0102463.

REFERENCES

1. H. Cohn, Approach to Markov's minimal forms through modular functions, *Ann. Math.* **61**(2) (1955), 1–12.

2. D. J. Collins, Generation and presentation of one-relator groups with centre, *Math. Z.* **157** (1977), 63–77.

3. L. E. Dickson, *Linear groups with an exposition of the Galois field theory* (B.G. Tuebner, Leipzig, Germany, 1901; reprinted by Dover Publications, New York, 1958).

4. 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. Dunwoody, On T-systems of groups, *J. Aust. Math. Soc.* **3** (1963), 172–179.

6. M. Dunwoody, Nielsen transformations, in *Computational problems in abstract algebra* (Leech J., Editor) (Proc. Conf. Oxford, 1967) (Pergamon, Oxford, UK, 1970), 45–46. MR 0260852 (41 #5472).

7. M. J. Evans, T-systems of certain finite simple groups, *Math. Proc. Cambridge Phil. Soc.* **113**(1) (1993), 9–22.

8. R. Gilman, Finite quotients of the automorphism group of a free group, *Can. J. Math.* **29** (1977), 541–551.

9. H. Glover and D. Sjerve, The genus of $\mathrm{PSL}_2(q)$, *J. Reine Angew. Math.* **380** (1987), 59–86.

10. GAP – Groups, Algorithms, and Programming. Available at http://www.gap-system.org/, accessed 4 January 2013.

11. W. Goldman, The modular group action on real SL(2)-characters of a one-holed torus, *Geom. Topol.* **7** (2003), 443–486.

12. L.-K. Hua, On the automorphisms of the symplectic group over any field, *Ann. of Math.* **49**(2) (1948), 739–759.

13. R. Lidl and H. Niederreiter, *Introduction to finite fields and their applications* (Cambridge University Press, Cambridge, UK, 1986).

14. M. Lustig, Nielsen equivalence and simple-homotopy type, *Proc. Lond. Math. Soc.* **62**(3) (1991), 537–562.

15. M. Lustig and Y. Moriah, Nielsen equivalence in Fuchsian groups and Seifert fibered spaces, *Topology* **30** (1991), 191–204.

16. M. Lustig and Y. Moriah, Generalized Montesinos knots, tunnels and N-torsion, *Math. Ann.* **295** (1993), 167–189.

17. M. Lustig and Y. Moriah, Generating systems of groups and Reidemeister–Whitehead torsion, *J. Algebra* **157** (1993), 170–198.

18. M. Lustig and Y. Moriah, N-torsion and applications, in *Geometric group theory,* vol. 1 (Proc. of Geometric Group Theory, University of Sussex, 1991), London Mathematical Society Lecture Note Series 181 (Cambridge University Press, Cambridge, UK, 1993), 159–168.

19. M. Lustig and Y. Moriah, On the complexity of the Heegaard structure of hyperbolic 3-manifolds, *Math. Z.* **226** (1997), 349–358.

20. A. M. Macbeath, Generators of the linear fractional groups, in *Number theory* (Proc. Sympos. Pure Math., vol. XII, Houston, Tex., 1967) (American Mathematical Society, Providence, RI, 1969), 14–32.

21. D. McCullough, Exceptional subgroups of SL(2, F). Preprint available at www.math.ou.edu/~dmccullough/research/manuscripts.html, accessed 4 January 2013.

22. D. McCullough, Software for Nielsen equivalence of generating pairs of SL(2,q), GAP script . Available at www.math.ou.edu/~dmccullough/research/software.html, accessed 4 January 2013.

23. D. McCullough and M. Wanderley, Free actions on handlebodies, *J. Pure Appl. Algebra* **181** (2003), 85–104.

24. D. McCullough and M. Wanderley, Writing elements of PSL(2, q) as commutators, *Comm. Algebra* **39** (2011), 1234–1241.

25. Y. Moriah, Heegaard splittings of Seifert fibered spaces, *Invent. Math.* **91** (1988), 465–481.

26. B. H. Neumann, On a question of Gaschütz, *Arch. Math.* (Basel) **7** (1956), 87–90.

27. B. H. Neumann and H. Neumann, Zwei Klassencharakteristischer Untergruppen und ihre Factorgruppen, *Math. Nachr.* **4** (1951) 106–125.

28. J. Nielsen, Die Isomorphismengruppe der allgemeinen unendlichen Gruppe mit zwei Erzeugenden, *Math. Ann.* **78** (1918), 385–397.

29. S. J. Pride, The isomorphism problem for two-generator one-relator groups with torsion is solvable, *Trans. Amer. Math. Soc.* **227** (1977), 109–139.

30. G. Rosenberger, All generating pairs of all two-generator Fuchsian groups, *Arch. Math.* **46** (1986), 198–204.

31. O. Schrier and B. L. van der Waerden, Die Automorphismen der projektiven Gruppen, *Abh. Math. Sem. Univ. Hamburg* **6** (1928), 303–322.

32. M. Suzuki, *Group theory*, vol. I (Springer-Verlag, Berlin, Germany, 1982).

33. P. J. Webb, Minimal relation modules of free nilpotent groups, *Arch. Math.* (Basel) **37** (1981), 193–197.