J. Group Theory **18** (2015), 961–980
DOI 10.1515/jgth-2015-0021

Expansion of conjugacy classes in $\mathrm{PSL}_2(q)$

Shelly Garion

Communicated by Robert M. Guralnick

Abstract. For any conjugacy class $\mathcal{C}$ in $G = \mathrm{PSL}_2(q)$ we compute $\mathcal{C}^2$ and discuss whether or not $\mathcal{C}$ contains a triple of elements whose product is 1 which generate G. Moreover, we determine which elements in G can be written as a product of two conjugate elements that generate G.

1 Introduction

There is a great interest in expansion properties of conjugacy classes in finite simple (non-abelian) groups. Thompson conjectured that every finite simple group G has a conjugacy class $\mathcal{C}$ such that $\mathcal{C}^2 = G$. This conjecture was verified for many families of finite simple groups, including the alternating groups and the sporadic groups, and Ellers and Gordeev [4] proved this conjecture for all finite simple groups of Lie type defined over fields with more than 8 elements, but nevertheless it is still very much open today. On the other hand, the expansion of small enough conjugacy classes $\mathcal{C}$ in sufficiently large finite simple groups, has been investigated by Schul [13]. Moreover, Guralnick and Malle [8] showed that every finite simple group G has a conjugacy class $\mathcal{C}$ that contains a triple of elements which have product 1 and generate G.

In this paper we consider *all* the conjugacy classes in the group $G = \mathrm{PSL}_2(q)$, and extend previous results of Guralnick and Malle [8, Lemma 3.14, Lemma 3.15 and Theorem 7.1].

Theorem 1. *Let $G = \mathrm{PSL}_2(q)$ where $q > 3$ and let $\mathcal{C}$ be a non-trivial G-conjugacy class. Then $\mathcal{C}$ contains elements x, y such that $\langle x, y\rangle = G$, with only the following exceptions:*

- *$\mathcal{C}$ is a conjugacy class of an element of order 2,*
- *$q = 9$ and $\mathcal{C}$ is a conjugacy class of a unipotent element (of order 3).*

The author was supported by the SFB 878 “Groups, Geometry and Actions”.

In addition, $\mathcal{C}$ contains three elements x, y, z such that $xyz = 1$ and $\langle x, y\rangle = G$ if and only if one of the following holds:

- *$\mathcal{C}$ is a conjugacy class of a semisimple element of a q-*minimal *order greater than 3,*
- *$q > 3$ is prime and $\mathcal{C}$ is a conjugacy class of a unipotent element.*

Definition 1. Let $q = p^e$ be a prime power and let $n > 1$ be an integer. Then n is called a *q-minimal* order if

$$e = \min\{f > 0 : p^f \equiv \pm 1 \bmod (\gcd(2, n) \cdot n)\}.$$

(Namely, $\mathrm{PSL}_2(p^e)$ contains an element of order n, but no $\mathrm{PSL}_2(p^f)$ with $f < e$ contains such an element.)

Note that similar results appear in [9–11] regarding generation properties of $\mathrm{PSL}_2(q)$ by a triple of elements (x, y, z) with product 1 and prescribed orders (see also [5, 12]).

Theorem 2. *Let $G = \mathrm{PSL}_2(q)$ where $q > 2$ is even. Let $\mathcal{C}$ be the G-conjugacy class of an element x.*

(i) *If x is a semisimple element whose order divides $q - 1$, then $\mathcal{C}^2 = G$.*

(ii) *If x is a semisimple element whose order divides $q + 1$, then*

$$\mathcal{C}^2 = G \setminus \{\textit{unipotents}\}.$$

(iii) *If x is a unipotent element, then $\mathcal{C}^2 = G$.*

In addition, only a semisimple element in G can be written as a product of two G-conjugate (semisimple) elements that generate G.

Theorem 3. *Let $G = \mathrm{PSL}_2(q)$ where $q > 3$ is odd. Let $\mathcal{C}$ be the G-conjugacy class of an element x.*

(i) *If x is a semisimple element whose order is greater than 2, then $\mathcal{C}^2 = G$.*

(ii) *If x is an element of order 2, then*

$$\mathcal{C}^2 = \begin{cases} G & \text{if } q \equiv 1 \bmod 4, \\ G \setminus \{\textit{unipotents}\} & \text{if } q \equiv 3 \bmod 4. \end{cases}$$

(iii) *If x is a unipotent element, then*

$$\mathcal{C}^2 = \begin{cases} \{\textit{unipotents}\} \cup \{\textit{semisimples of } q\textit{-good orders}\} \cup \{1\}, & q \equiv 1 \bmod 4, \\ \{\textit{unipotents}\} \cup \{\textit{semisimples of } q\textit{-good orders}\}, & q \equiv 3 \bmod 4. \end{cases}$$

*In addition, any non-trivial element in G can be written as a product of two G-conjugate semisimple elements that generate G. And moreover, a semisimple element can be written as a product of two G-conjugate unipotents that generate G if and only if its order is q-*minimal *and q-*good*, where $q \neq 9$.*

Definition 2. Let $q = p^e$ be a prime power and let $n > 1$ be an integer. Then n is called a *q-good* order if one of the following holds:

- n is odd and divides either $q - 1$ or $q + 1$,
- n is even and $4n$ divides either $q - 1$ or $q + 1$.

Corollary 4. *Let $G = \mathrm{PSL}_2(q)$. Let $\mathcal{C}$ be the G-conjugacy class of an element x.*

(i) *If q is even, then*

$$\frac{|\mathcal{C}|}{|G|^{2/3}} \to 1 \quad \textit{and} \quad \frac{|\mathcal{C}^2|}{|G|} \to 1 \quad \textit{as } q \to \infty.$$

(ii) *If q is odd and x is a semisimple element whose order is greater than 2, then*

$$\frac{|\mathcal{C}|}{|G|^{2/3}} \to \sqrt[3]{4} \quad \textit{and} \quad \frac{|\mathcal{C}^2|}{|G|} \to 1 \quad \textit{as } q \to \infty.$$

(iii) *If q is odd and x is an element of order 2, then*

$$\frac{|\mathcal{C}|}{|G|^{2/3}} \to \frac{1}{\sqrt[3]{2}} \quad \textit{and} \quad \frac{|\mathcal{C}^2|}{|G|} \to 1 \quad \textit{as } q \to \infty.$$

(iv) *If q is odd and x is a unipotent element, then*

$$\frac{|\mathcal{C}|}{|G|^{2/3}} \to \frac{1}{\sqrt[3]{2}} \quad \textit{and} \quad \frac{|\mathcal{C}^2|}{|G|} \to \frac{3}{4} \quad \textit{as } q \to \infty.$$

Example 5. For any prime power $q < 30$ the following Table 1 presents *all* the *q-minimal* orders, divided according to whether they are *q-good* or not.

2 Preliminaries – Basic properties of $\mathrm{PSL}_2(q)$

2.1 Elements and conjugacy classes

(See [2, 3, 6, 14].) Let $q = p^e$, where p is a prime number and $e \geq 1$. Recall that the order of $G = \mathrm{PSL}_2(q)$ is $q(q^2 - 1)/d$, where

$$d = \gcd(2, q - 1) = \begin{cases} 1 & \text{if } q \text{ is even,} \\ 2 & \text{if } q \text{ is odd.} \end{cases}$$

q	order of a unipotent	q-minimal orders which are q-good	q-minimal orders which are not q-good
2	2	3	–
3	3	–	2
4	2	3, 5	–
5	5	3	2
7	7	2, 3	4
8	2	7, 9	–
9	3	5	4
11	11	3, 5	2, 6
13	13	3, 7	2, 6
16	2	15, 17	–
17	17	2, 3, 4, 9	8
19	19	3, 5, 9	2, 10
23	23	2, 3, 6, 11	4, 12
25	5	6, 13	4, 12
27	3	7, 13	14
29	29	3, 5, 7, 15	2, 14

Table 1. Orders of elements in $\mathrm{PSL}_2(q)$.

One can classify the elements of $\mathrm{PSL}_2(q)$ according to the Jordan form of their pre-image in $\mathrm{SL}_2(q)$. The following Table 2 lists the three types of elements, according to whether the characteristic polynomial $P(\lambda) := \lambda^2 - \alpha\lambda + 1$ of the matrix $A \in \mathrm{SL}_2(q)$ (where $\alpha = \mathrm{tr}(A)$) has 0, 1 or 2 distinct roots in $\mathbb{F}_q$.

We denote

$$\kappa(\alpha) = \begin{cases} 1 & \text{if } \alpha \neq 0, \\ 2 & \text{if } \alpha = 0. \end{cases}$$

2.2 Subgroups

Table 3 specifies all the subgroups of $G = \mathrm{PSL}_2(q)$ up to isomorphism following [14, Theorems 6.25 and 6.26].

These subgroups can be divided into the following three classes, following Macbeath [11]. The subgroups isomorphic to $\mathrm{PSL}_2(q_1)$ or $\mathrm{PGL}_2(q_1)$ are usually called *subfield* subgroups (since $\mathbb{F}_{q_1}$ is a subfield of $\mathbb{F}_q$). Since A_4, S_4, A_5 and

type	roots of $P(\lambda)$	Jordan form in $\mathrm{SL}_2(\overline{\mathbb{F}}_p)$	order	G-conjugacy classes
unipotent	1 root	$\left(\begin{smallmatrix}\pm 1 & 1\\ 0 & \pm 1\end{smallmatrix}\right)$, $\alpha = \pm 2$	p	d classes in G each of size $(q^2-1)/d$
semisimple split	2 roots	$\left(\begin{smallmatrix}a & 0\\ 0 & a^{-1}\end{smallmatrix}\right)$ where $a \in \mathbb{F}_q^*$ and $a + a^{-1} = \alpha$	divides $(q-1)/d$	for each α: one conjugacy class of size $(q(q+1))/\kappa(\alpha)$
semisimple non-split	no roots	$\left(\begin{smallmatrix}a & 0\\ 0 & a^q\end{smallmatrix}\right)$ where $a \in \mathbb{F}_{q^2}^* \setminus \mathbb{F}_q^*$, $a^{q+1} = 1$ and $a + a^q = \alpha$	divides $(q+1)/d$	for each α: one conjugacy class of size $(q(q-1))/\kappa(\alpha)$

Table 2. Elements in $\mathrm{PSL}_2(q)$.

dihedral groups correspond to the finite triangle groups, that is, triangle groups $T_{r,s,t}$ such that $1/r + 1/s + 1/t > 1$, we will call them *small* subgroups. For convenience we will refer to the other subgroups, namely subgroups of the Borel and cyclic subgroups, as *structural* subgroups.

Macbeath [11] classified the pairs of elements in $\mathrm{PSL}_2(q)$ in a way which makes it easy to determine what kind of subgroup they generate.

Theorem 6 ([11, Theorem 1]). *For every $\alpha, \beta, \gamma \in \mathbb{F}_q$ there exist three matrices $A, B, C \in \mathrm{SL}_2(q)$ satisfying $\mathrm{tr}(A) = \alpha$, $\mathrm{tr}(B) = \beta$, $\mathrm{tr}(C) = \gamma$ and $ABC = I$.*

Definition 3. A triple $(\alpha, \beta, \gamma) \in \mathbb{F}_q^3$ is called *singular* if

$$\alpha^2 + \beta^2 + \gamma^2 - \alpha\beta\gamma - 4 = 0.$$

Theorem 7 ([11, Theorem 2]). *Let $(A, B, C) \in \mathrm{SL}_2(q)^3$ be a triple of matrices satisfying $\mathrm{tr}(A) = \alpha$, $\mathrm{tr}(B) = \beta$, $\mathrm{tr}(C) = \gamma$ and $ABC = I$. Then $(\alpha, \beta, \gamma) \in \mathbb{F}_q^3$ is* singular *if and only if the group generated by the images of A and B is a* structural *subgroup of* $\mathrm{PSL}_2(q)$.

2.3 Orders and traces

For an integer $n > 1$ we denote

$$\mathcal{T}_q(n) = \{\alpha \in \mathbb{F}_q : \alpha = \mathrm{tr}(A), A \in \mathrm{SL}_2(q), |\bar{A}| = n\} \tag{2.1}$$

where $\bar{A}$ denotes the image of the matrix A in $\mathrm{PSL}_2(q)$. It is easy to see from Table 2 that for any prime power q,

$$\mathcal{T}_q(2) = \{0\}, \quad \mathcal{T}_q(3) = \{\pm 1\},$$

type	maximal order	conditions
p-group	q	–
Frobenius (Borel)	$q(q-1)/d$	–
cyclic (split)	$(q-1)/d$	–
dihedral (split)	$2(q-1)/d$	–
cyclic (non-split)	$(q+1)/d$	–
dihedral (non-split)	$2(q+1)/d$	–
$\mathrm{PSL}_2(q_1)$	–	$q = q_1^m$ $(m \in \mathbb{N})$
$\mathrm{PGL}_2(q_1)$	–	q is odd, $q = q_1^{2m}$ $(m \in \mathbb{N})$
A_4	12	q is odd; or $q = 2^e$, e even
S_4	24	$q^2 \equiv 1 \bmod 16$
A_5	60	$p = 5$ or $q^2 \equiv 1 \bmod 5$

Table 3. Subgroups of $\mathrm{PSL}_2(q)$.

and for any odd $q = p^e$,

$$\mathcal{T}_q(p) = \{\pm 2\}.$$

Moreover, when q is odd, then $\alpha \in \mathcal{T}_q(n)$ if and only if $-\alpha \in \mathcal{T}_q(n)$. In fact, for any prime power q and integer $n > 1$, $\mathcal{T}_q(n)$ can be effectively computed as follows.

Proposition 8. *Denote by $\mathcal{P}_q(n)$ the set of primitive roots of unity of order n in $\mathbb{F}_q$.*

- *Let $q = 2^e$ for some positive integer e and let $n > 1$ be an integer. Then*

$$\mathcal{T}_q(n) = \begin{cases} \{0\} & \text{if } n = 2, \\ \{a + a^{-1} : a \in \mathcal{P}_q(n)\} & \text{if } n \text{ divides } q-1, \\ \{b + b^q : b \in \mathcal{P}_{q^2}(n)\} & \text{if } n \text{ divides } q+1, \\ \emptyset & \text{otherwise.} \end{cases} \tag{2.2}$$

- *Let $q = p^e$ for some odd prime p and some positive integer e and let $n > 1$ be an integer. Then*

$$\mathcal{T}_q(n) = \begin{cases} \{\pm 2\} & \text{if } n = p, \\ \{\pm(a + a^{-1}) : a \in \mathcal{P}_q(2n)\} & \text{if } n \text{ divides } (q-1)/2, \\ \{\pm(b + b^q) : b \in \mathcal{P}_{q^2}(2n)\} & \text{if } n \text{ divides } (q+1)/2, \\ \emptyset & \text{otherwise.} \end{cases} \tag{2.3}$$

Proof. We prove the case where q is odd and n divides $(q-1)/2$. The other cases are similar.

Assume first that n is even. Let a be a primitive root of unity of order $2n$. Then $-a$ is also a primitive root of unity of order $2n$, and $(-a)^n = a^n = -1$. Thus the matrices

$$A = \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \quad \text{and} \quad -A = \begin{pmatrix} -a & 0 \\ 0 & -a^{-1} \end{pmatrix}$$

both reduce to the same element $\bar{A} \in G$ of order n. Hence, $a+a^{-1}$ and $-(a+a^{-1})$ both belong to $\mathcal{T}_q(n)$. The set $\mathcal{T}_q(n)$ contains only the elements of the claimed form, since it suffices to consider only the conjugacy classes of elements of G, described in Table 2.

Now assume that n is odd. Then a is a primitive root of unity of order n if and only if $-a$ is a primitive root of unity of order $2n$. In this case,

$$(-a)^n = -a^n = -1.$$

Thus the matrices

$$A = \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \quad \text{and} \quad -A = \begin{pmatrix} -a & 0 \\ 0 & -a^{-1} \end{pmatrix}$$

both reduce to the same element $\bar{A} \in G$ of order n. Hence, $a+a^{-1}$ and $-(a+a^{-1})$ both belong to the set $\mathcal{T}_q(n)$. Again, considering the conjugacy classes appearing in Table 2 shows that $\mathcal{T}_q(n)$ contains only the elements of the claimed form. □

Proposition 9. *Assume that $q = p^e$ is odd. Let $C \in \mathrm{SL}_2(q)$, and denote $\gamma = \mathrm{tr}(C)$ and $t = |\bar{C}|$. Assume that $\gamma \neq \pm 2$ (or equivalently, $t \neq p$). Then t is a q-*good *order if and only if one of $2+\gamma$, $2-\gamma$ is a square in $\mathbb{F}_q$.*

Proof. As $t \neq p$, it follows that t divides either $(q-1)/2$ or $(q+1)/2$.

If t divides $(q-1)/2$, then $\gamma = a+a^{-1}$ or $\gamma = -(a+a^{-1})$, for some primitive root of unity a of order $2t$ in $\mathbb{F}_q$ (see Proposition 8). Hence,

$$\{2+\gamma, 2-\gamma\} = \{a+2+a^{-1}, (-a)+2+(-a)^{-1}\}.$$

Therefore, $2+\gamma$ or $2-\gamma$ is a square in $\mathbb{F}_q$ if and only if $a = c^2$ or $-a = c^2$ for some $c \in \mathbb{F}_q$. Indeed, $a+2+a^{-1}$ is a square if and only if $(a+1)^2/a$ is a square if and only if a is a square in $\mathbb{F}_q$, and similarly for $(-a)+2+(-a)^{-1}$.

Now, one the following necessarily holds:

- If t is even, then $-a$ is also a primitive root of unity of order $2t$. Hence, a is a square in $\mathbb{F}_q$ if and only if $-a$ is a square is $\mathbb{F}_q$. In addition, a is a square in $\mathbb{F}_q$ if and only if $\mathbb{F}_q$ contains a primitive root of unity of order $4t$, namely, if and only if $4t$ divides $q-1$.

- If t is odd and $q \equiv 1 \bmod 4$, then $4t$ divides $q-1$, and so $\mathbb{F}_q$ contains a primitive root of unity of order $4t$. Thus a, which is a primitive root of unity of order $2t$, is a square in $\mathbb{F}_q$, as required.
- If t is odd and $q \equiv 3 \bmod 4$, then $\mathbb{F}_q$ contains a primitive root of unity of order $2t$ but does not contain a primitive root of unity of order $4t$, and so, a is a non-square in $\mathbb{F}_q$. However, $-a$ is a primitive root of unity of order t, and so, it is necessarily a square in $\mathbb{F}_q$, as required.

In conclusion, $a = c^2$ or $-a = c^2$ for some $c \in \mathbb{F}_q$ if and only if either t is odd and divides $q-1$ or t is even and $4t$ divides $q-1$.

If t divides $(q+1)/2$, then $\gamma = a + a^q$ or $\gamma = -(a + a^q)$, for some primitive root of unity a of order $2t$ in $\mathbb{F}_{q^2}$ (see Proposition 8). Hence,

$$\{2+\gamma, 2-\gamma\} = \{a + 2 + a^q, (-a) + 2 + (-a)^q\}.$$

Therefore, $2+\gamma$ or $2-\gamma$ is a square in $\mathbb{F}_q$ if and only if $a = c^2$ or $-a = c^2$ for some $c \in \mathbb{F}_{q^2}$ satisfying $c^{q+1} = 1$.

Now, one the following necessarily holds:

- If t is even, then $-a$ is also a primitive root of unity of order $2t$. Hence, $a = c^2$ for some $c \in \mathbb{F}_{q^2}$ satisfying $c^{q+1} = 1$ if and only if $-a = b^2$ for some $b \in \mathbb{F}_{q^2}$ satisfying $b^{q+1} = 1$. This is equivalent to the condition that $4t$ divides $q+1$.
- If t is odd and $q \equiv 3 \bmod 4$, then $\mathbb{F}_{q^2}$ contains a primitive root of unity b of order $4t$ satisfying $b^{q+1} = 1$. Hence, $a = c^2$ for some $c \in \mathbb{F}_{q^2}$ satisfying $c^{q+1} = 1$, as required.
- If t is odd and $q \equiv 1 \bmod 4$, then $\mathbb{F}_{q^2}$ does not contain a primitive root of unity c of order $4t$ satisfying $c^{q+1} = 1$. However, in this case, $-a = b^2$ for some $b \in \mathbb{F}_{q^2}$ satisfying $b^{q+1} = 1$, as required.

In conclusion, $a = c^2$ or $-a = c^2$ for some $c \in \mathbb{F}_{q^2}$ satisfying $c^{q+1} = 1$ if and only if either t is odd and divides $q+1$ or t is even and $4t$ divides $q+1$. □

2.4 Number of elements

Definition 4. Let q be a prime power and let $\alpha \in \mathbb{F}_q$.

If $\alpha = \pm 2$, we say that α is a *unipotent* trace. If α is a trace of a semisimple split (respectively, non-split) matrix in $\mathrm{SL}_2(q)$ we say that α is *split* (respectively, *non-split*).

Assume that q is odd and $\alpha \neq \pm 2$. If at least one of $2+\alpha$, $2-\alpha$ is a square in $\mathbb{F}_q$, we say that α is a *good* trace. If neither $2+\alpha$ nor $2-\alpha$ is a square in $\mathbb{F}_q$ we say that α is a *bad* trace.

Lemma 10. *The following statements hold.*

(1) *If q is even, then $\mathbb{F}_q$ contains one unipotent, $(q-2)/2$ split and $q/2$ non-split traces.*

(2) *If q is odd, then $\mathbb{F}_q$ contains two unipotent, $(q-3)/2$ split and $(q-1)/2$ non-split traces.*

(3) *If $q \equiv 1 \bmod 4$, then $\mathbb{F}_q$ contains $(q-1)/4$ bad traces.*

(4) *If $q \equiv 3 \bmod 4$, then $\mathbb{F}_q$ contains $(q+1)/4$ bad traces.*

Proof. Statements (1) and (2) are due to [11, Lemma 2].

(3) If $q \equiv 1 \bmod 4$, then $(q-1)/2$ is even, and so all the bad traces are necessarily split. Hence, there are $((q-3)/2+1)/2$ bad traces.

(4) If $q \equiv 3 \bmod 4$, then $(q+1)/2$ is even, and so all the bad traces are non-split. Hence, there are $((q-1)/2+1)/2$ bad traces. □

Now, the following corollaries easily follow from Table 2, Proposition 9 and Lemma 10.

Corollary 11. *If q is even, then $G = \mathrm{PSL}_2(q)$ contains:*

- q^2-1 *unipotent elements,*
- $q(q+1)(q-2)/2$ *semisimple split elements,*
- $q^2(q-1)/2$ *semisimple non-split elements.*

Corollary 12. *If q is odd, then $G = \mathrm{PSL}_2(q)$ contains:*

- q^2-1 *unipotent elements,*
- $q(q+1)(q-3)/4$ *semisimple split elements,*
- $q(q-1)^2/4$ *semisimple non-split elements,*
- $q(q^2-1)/8 = |G|/4$ *semisimple elements whose order is* not q-good.

2.5 Unipotent elements when q is odd

Consider the following matrices in $G_0 = \mathrm{SL}_2(q)$ (where q is odd):

$$U_1 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \qquad U_{-1} = \begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix} = -U_1^{-1},$$

$$U_1' = XU_1X^{-1} = \begin{pmatrix} 1 & x^2 \\ 0 & 1 \end{pmatrix}, \quad U_{-1}' = XU_{-1}X^{-1} = \begin{pmatrix} -1 & x^2 \\ 0 & -1 \end{pmatrix},$$

where $x \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ satisfies that $x^2 \in \mathbb{F}_q$ and

$$X = \begin{pmatrix} x & 0 \\ 0 & x^{-1} \end{pmatrix} \in \mathrm{SL}_2(q^2).$$

Proposition 13. *Let $G_0 = \mathrm{SL}_2(q)$ when q is odd. Then, for any $A \in G_0$, we have $XAX^{-1} \in G_0$. Moreover:*

- *If $A \neq I$ and $\mathrm{tr}(A) = 2$, then A is G_0-conjugate to either U_1 or U_1'.*
- *If $A \neq -I$ and $\mathrm{tr}(A) = -2$, then A is G_0-conjugate to either U_{-1} or U_{-1}'.*

Proof. Indeed, if $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in G_0$, then

$$XAX^{-1} = \begin{pmatrix} a & bx^2 \\ cx^{-2} & d \end{pmatrix} \in G_0.$$

Moreover, U_1 is not G_0-conjugate to $U_1' = XU_1X^{-1}$, since x^2 is not a square of some element in $\mathbb{F}_q$. Hence, any $I \neq A \in G_0$ with $\mathrm{tr}(A) = 2$ is G_0-conjugate to either U_1 or U_1' (see Table 2). □

Corollary 14. *Let $G = \mathrm{PSL}_2(q)$ when q is odd. Then, for any $\bar{A} \in G$, we have that $\bar{X}\bar{A}\bar{X}^{-1} \in G$. If moreover, $\bar{A}$ is unipotent, then it is G-conjugate to either $\bar{U}_1$ or $\bar{U}'_1 = \bar{X}\bar{U}_1\bar{X}^{-1}$. In addition:*

- *If $q \equiv 1 \bmod 4$, then $\bar{U}_1$ and $\bar{U}_{-1}$ are G-conjugate.*
- *If $q \equiv 3 \bmod 4$, then $\bar{U}_1$ and $\bar{U}'_{-1}$ are G-conjugate.*

3 Proof of the main results

Proof of Theorem 1. The proof follows from Propositions 15, 17, 18, Remark 19, Proposition 32 and Remark 33. □

Proof of Theorem 2. The proof follows from Propositions 16, 22–24 and 28. □

Proof of Theorem 3. The proof follows from Propositions 16, 21, 22, 24 and 25, Corollaries 27 and 31 and Proposition 32. □

Proof of Corollary 4. The proof follows from Theorem 2, Theorem 3, Table 2 and Section 2.4.

(i) Let $G = \mathrm{PSL}_2(q)$ when q is even; then $|G| = q(q^2 - 1)$.

- If $\mathcal{C}$ is a conjugacy class of a semisimple split element, then

$$|\mathcal{C}| = q(q+1) \quad \text{and} \quad |\mathcal{C}^2| = q(q^2-1).$$

- If $\mathcal{C}$ is a conjugacy class of a semisimple non-split element, then

$$|\mathcal{C}| = q(q-1) \quad \text{and} \quad |\mathcal{C}^2| = q(q^2-1) - (q^2-1) = (q-1)(q^2-1).$$

- If $\mathcal{C}$ is a conjugacy class of a unipotent element, then

$$|\mathcal{C}| = q^2 - 1 \quad \text{and} \quad |\mathcal{C}^2| = q(q^2-1).$$

Now let $G = \mathrm{PSL}_2(q)$ when q is odd; then $|G| = q(q^2-1)/2$.

(ii) If $\mathcal{C}$ is a conjugacy class of semisimple element whose order is greater than 2, then

$$|\mathcal{C}| = q(q \pm 1) \quad \text{and} \quad |\mathcal{C}^2| = \frac{q(q^2-1)}{2}.$$

(iii) If $\mathcal{C}$ is a conjugacy class of semisimple element x of order 2, then:

- If $q \equiv 1 \bmod 4$, then x is split and so

$$|\mathcal{C}| = \frac{q(q+1)}{2} \quad \text{and} \quad |\mathcal{C}^2| = \frac{q(q^2-1)}{2}.$$

- If $q \equiv 3 \bmod 4$, then x is non-split and so

$$|\mathcal{C}| = \frac{q(q-1)}{2} \quad \text{and} \quad |\mathcal{C}^2| = \frac{q(q^2-1)}{2} - (q^2-1) = \frac{(q-2)(q^2-1)}{2}.$$

(iv) If $\mathcal{C}$ is a conjugacy class of a unipotent element, then by Corollary 12,

$$|\mathcal{C}| = \frac{q^2-1}{2} \quad \text{and} \quad |\mathcal{C}^2| = \frac{q(q^2-1)}{2} - \frac{q(q^2-1)}{8} - \epsilon = \frac{3q(q^2-1)}{8} - \epsilon,$$

where

$$\epsilon = \begin{cases} 0 & \text{if } q \equiv 1 \bmod 4, \\ 1 & \text{if } q \equiv 3 \bmod 4. \end{cases}$$

□

3.1 Generation properties of $\mathcal{C}$

Proposition 15. *Let $G = \mathrm{PSL}_2(q)$ when $q > 3$ and let $\mathcal{C}$ be a conjugacy class of a semisimple element s of order greater than 2. Then $\mathcal{C}$ contains two elements x, y that generate G.*

Proof. Let $s \in G$ be a semisimple element and let $\mathcal{C}$ be the conjugacy class of s. Let $S \in G_0 = \mathrm{SL}_2(q)$ be the pre-image of s. Denote the order of s by n and $\alpha = \mathrm{tr}(S)$, thus $\alpha \notin \{0, \pm 2\}$. Recall that $d = \gcd(2, q-1)$.

If $q \neq 5, 7$, take some $\gamma \in \mathcal{T}_q((q+1)/d)$. If (α, α, γ) is *singular*, then we have that $(2-\gamma)(\alpha^2 - \gamma - 2) = 0$ and so $\gamma = \alpha^2 - 2$. Thus, we may replace γ

by $-\gamma$ (or by another $\gamma \in \mathcal{T}_q((q+1)/d)$) to obtain a non-singular triple (α, α, γ). When $q = 9$, one can moreover make sure that (α, α, γ) does not correspond to a triple of matrices (A, B, C) with $ABC = I$ satisfying $\langle \bar{A}, \bar{B} \rangle \cong A_5$ (see [10]). When $q = 5$ or 7, take $\gamma = -2$, and then the triple $(\alpha, \alpha, -2)$ is also not singular.

By Theorem 6, there exists a triple of matrices (A, B, C) such that $ABC = I$, $\mathrm{tr}(A) = \mathrm{tr}(B) = \alpha$ and $\mathrm{tr}(C) = \gamma$. Moreover, by Theorem 7, $\langle \bar{A}, \bar{B} \rangle$ is not a structural subgroup of G. By considering the possible subgroups of G detailed in Table 3 we see that the only non-structural subgroup containing $\bar{C}$ is G itself, and hence $\langle \bar{A}, \bar{B} \rangle = G$. □

Proposition 16. *Let $G = \mathrm{PSL}_2(q)$ when $q > 3$.*

- *If q is odd, then any non-trivial element in G can be written as a product of two G-conjugate semisimple elements that generate G.*
- *If q is even, then only a semisimple element in G can be written as a product of two G-conjugate (semisimple) elements that generate G.*

Proof. Assume that q is even. Let $Z \in G$ and denote $\gamma = \mathrm{tr}(Z)$. Assume that $Z = XY$ where X is G-conjugate to Y, and let $\alpha = \mathrm{tr}(X) = \mathrm{tr}(Y)$. If Z is unipotent, then $\gamma = 0$. Since $(\alpha, \alpha, 0)$ is *singular*, it follows from Theorem 7 that the subgroup $\langle X, Y \rangle$ is a structural subgroup of G, and so X and Y cannot generate G. If Z is semisimple, then $\gamma \neq 0$, and we can choose some $\alpha \in \mathcal{T}_q(q+1)$ such that $\gamma \neq \alpha^2$ and then (α, α, γ) is not singular.

Assume that q is odd. Let $1 \neq z \in G$ and let $Z \in G_0 = \mathrm{SL}_2(q)$ be the pre-image of z. Denote $\gamma = \mathrm{tr}(Z)$. If $q \neq 5, 7$, take some $\alpha \in \mathcal{T}_q((q+1)/2)$. If (α, α, γ) is *singular*, then $(2-\gamma)(\alpha^2 - \gamma - 2) = 0$ and so $\gamma = 2$ or $\gamma = \alpha^2 - 2$. Thus, we may replace γ by $-\gamma$ to obtain a non-singular triple (α, α, γ). When $q = 9$, one can moreover make sure that (α, α, γ) does not correspond to a triple of matrices (A, B, C) with $ABC = I$ satisfying $\langle \bar{A}, \bar{B} \rangle \cong A_5$ (see [10]). When $q = 5$ or 7, take $\alpha = -2$ (and make sure that $\gamma \neq 2$) and then the triple $(-2, -2, \gamma)$ is also not singular.

By Theorem 6, there exists a triple of matrices (A, B, C) such that $ABC = I$, $\mathrm{tr}(A) = \mathrm{tr}(B) = \alpha$ and $\mathrm{tr}(C) = \gamma$. Moreover, by Theorem 7, $\langle \bar{A}, \bar{B} \rangle$ is not a structural subgroup of G. By considering the possible subgroups of G detailed in Table 3 we see that the only non-structural subgroup containing $\bar{A}$ is G itself, and hence $\langle \bar{A}, \bar{B} \rangle = G$. □

Proposition 17. *Let $G = \mathrm{PSL}_2(q)$ when $q > 3$ and let $\mathcal{C}$ be a conjugacy class of a semisimple element s. Then $\mathcal{C}$ contains three elements x, y, z such that $xyz = 1$ and $\langle x, y \rangle = G$ if and only if the order of s is q-*minimal *and greater than* 3.

Proof. Let $s \in G$ be a semisimple element and let $\mathcal{C}$ be the conjugacy class of s. Let $S \in G_0 = \mathrm{SL}_2(q)$ be the pre-image of s. Denote the order of s by n and $\alpha = \mathrm{tr}(S)$.

If x, y, z are three elements of order 2 (respectively, 3) such that $xyz = 1$, then any finite group generated by x and y is necessarily abelian (respectively, solvable) and so x and y cannot generate G (see Remark 19).

If n is not q-minimal, then α belongs to some proper subfield $\mathbb{F}_{q_1}$ of $\mathbb{F}_q$. In this case, for any three elements $x, y, z \in \mathcal{C}$ satisfying $xyz = 1$, the subgroup $\langle x, y\rangle$ is necessarily contained in a proper subgroup of G isomorphic to $\mathrm{PSL}_2(q_1)$ (see [11] and [9]).

If $n > 3$ is q-minimal, then $\alpha \notin \{0, \pm 1, \pm 2\}$ and hence $(\alpha - 2)^2(\alpha + 1) \neq 0$ implying that the triple (α, α, α) is non-singular. If $q > 5$ and $n = 5$, one can moreover make sure that the triple (α, α, α) does not correspond to a triple of matrices (A, B, C) with $ABC = I$ satisfying $\langle \bar{A}, \bar{B}\rangle \cong A_5$ (see [10]).

Therefore, by Theorems 6 and 7, there exists a triple of matrices (A, B, C) such that $ABC = I$, $\mathrm{tr}(A) = \mathrm{tr}(B) = \mathrm{tr}(C) = \alpha$ and $\langle \bar{A}, \bar{B}\rangle$ is a structural subgroup of G. By the q-minimality of n, s does not belong to any subgroup isomorphic to $\mathrm{PSL}_2(q_1)$ for some proper subfield $\mathbb{F}_{q_1} \subset \mathbb{F}_q$. In addition, if $\langle x, y\rangle = \mathrm{PGL}_2(q_1)$ and $xyz = 1$, then exactly two of x, y, z belong to $\mathrm{PGL}_2(q_1) \setminus \mathrm{PSL}_2(q_1)$ and the third one belongs to $\mathrm{PSL}_2(q_1)$, so x, y, z cannot all have the same order n. Therefore, $\langle \bar{A}, \bar{B}\rangle$ cannot generate a subgroup isomorphic to $\mathrm{PGL}_2(q_1)$, hence $\langle \bar{A}, \bar{B}\rangle = G$ as needed. □

Proposition 18. *Let $G = \mathrm{PSL}_2(q)$ where q is a prime power. Then there exist three G-conjugate unipotent elements A, B and C such that $ABC = 1$ and $\langle A, B\rangle = G$ if and only if $q > 3$ is prime.*

Proof. If $A, B, C \in G$ are three elements of prime order p such that $ABC = 1$, then $\langle A, B\rangle$ is contained in a subgroup isomorphic to $\mathrm{PSL}_2(p)$, implying that necessarily $q = p > 3$ is prime (see [11] and [9]).

Choose some $a \in \mathbb{F}_p \setminus \{0, \pm 2\}$ and consider the following matrices in $\mathrm{SL}_2(p)$:

$$M = \begin{pmatrix} a+1 & -\frac{a}{2} - 1 \\ 2 & -1 \end{pmatrix}, \quad K = \begin{pmatrix} a & -\frac{1}{2} \\ 2 & 0 \end{pmatrix}.$$

Let $A = U_{-1} \in G_0$ be as in Section 2.5, $B = MU_{-1}M^{-1}$ and $C = KU_{-1}K^{-1}$; then $ABC = I$.

As $\mathrm{tr}(U_{-1}) = -2$ and $(-2, -2, -2)$ is a *non-singular* triple, it follows from Theorem 7 that the subgroup generated by the images of A and B is not a structural subgroup of G. By considering the possible subgroups of G detailed in Table 3 we conclude that $\langle \bar{A}, \bar{B}\rangle = G$, as needed. □

Remark 19. Recall that any finite group generated by two non-commuting involutions is dihedral. In addition, the group presented by $\langle x, y \mid x^3 = y^3 = (xy)^3 \rangle$ is an infinite solvable group (see e.g. [1]).

3.2 Basic properties of $\mathcal{C}^2$

Lemma 20. *Let $A, B \in G_0 = \mathrm{SL}_2(q)$ be two non-central matrices such that $\mathrm{tr}(A)$ is equal to $\mathrm{tr}(B)$ or $-\mathrm{tr}(B)$. Let $\mathcal{C}$ be some conjugacy class in $G = \mathrm{PSL}_2(q)$. If $\bar{A} \in \mathcal{C}^2$, then also $\bar{B} \in \mathcal{C}^2$.*

Proof. If $\bar{A} \in \mathcal{C}^2$, then $\bar{A} = z(gzg^{-1})$ for some $z \in \mathcal{C}$, $g \in G$.

If q is even, or if q is odd and $\mathrm{tr}(A) \neq \pm 2$, then necessarily $\bar{B} = h\bar{A}h^{-1}$ for some $h \in G$ (see Table 2), and so $\bar{B} = (hzh^{-1})(hgzg^{-1}h^{-1}) \in \mathcal{C}^2$.

Assume that q is odd, z is semisimple and $\bar{A}$ is unipotent. Let $Z \in G_0$ be the pre-image of z. Then by Corollary 14, either $\bar{B} = h\bar{A}h^{-1}$ or $\bar{B} = h\bar{X}\bar{A}\bar{X}^{-1}h^{-1}$ for some $h \in G$ and a matrix $X \in \mathrm{SL}_2(q^2)$ as in Section 2.5. Moreover, by Proposition 13, $XZX^{-1} \in G_0$, and since $\mathrm{tr}(XZX^{-1}) = \mathrm{tr}(Z)$, we have $\bar{X}z\bar{X}^{-1} \in \mathcal{C}$ (see Table 2). Similarly, $\bar{X}gzg^{-1}\bar{X}^{-1} \in \mathcal{C}$.

Hence, either

$$\bar{B} = h\bar{A}h^{-1} = (hzh^{-1})(hgzg^{-1}h^{-1}) \in \mathcal{C}^2$$

or

$$\bar{B} = h\bar{X}\bar{A}\bar{X}^{-1}h^{-1} = (h\bar{X}z\bar{X}^{-1}h^{-1})(h\bar{X}gzg^{-1}\bar{X}^{-1}h^{-1}) \in \mathcal{C}^2.$$

If q is odd and z is unipotent, then the following Proposition 21 shows that $\mathcal{C}^2$ contains all the unipotent elements in G, as needed. □

Proposition 21. *Let $G = \mathrm{PSL}_2(q)$ when q is odd and let $\mathcal{C}$ be the G-conjugacy class of a unipotent element x. Then $\mathcal{C}^2$ contains all the unipotent elements in G.*

Moreover, $1 \in \mathcal{C}^2$ if and only if $q \equiv 1 \bmod 4$.

Proof. For $q = 5$ this claim can be easily verified. When $q > 5$, there exist two elements $a, b \in \mathbb{F}_q$ such that a, b and $a + 1$ are squares in $\mathbb{F}_q$ but $b + 1$ is a non-square in $\mathbb{F}_q$. Let U_1 be as in Section 2.5, let

$$A = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}.$$

Then

$$U_1 A = \begin{pmatrix} 1 & a+1 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad U_1 B = \begin{pmatrix} 1 & b+1 \\ 0 & 1 \end{pmatrix}.$$

Moreover, A, B and U_1A are conjugate to U_1 in $\mathrm{SL}_2(q)$, while U_1B is conjugate to U_1' in $\mathrm{SL}_2(q)$ (see Proposition 13). By Corollary 14, any unipotent element in G is G-conjugate to either $\bar{U}_1$ or to $\bar{U}_1'$, as needed.

In addition, by Corollary 14, the matrix $\bar{U}_1$ is G-conjugate to $\bar{U}_1^{-1}$ if and if $q \equiv 1 \bmod 4$. □

Proposition 22. *Let $G = \mathrm{PSL}_2(q)$ and let $\mathcal{C}$ be the G-conjugacy class of a semisimple element x. Then $\mathcal{C}^2$ contains all the semisimple elements in G. Moreover, $1 \in \mathcal{C}^2$.*

Proof. Let $z \in G$ be some semisimple element. Let $X, Z \in \mathrm{SL}_2(q)$ be the preimages of x, z respectively. Denote $\alpha = \mathrm{tr}(X)$, $\gamma = \mathrm{tr}(Z)$. By Theorem 6, there exist matrices $X', Y', Z' \in \mathrm{SL}_2(q)$ such that $\mathrm{tr}(X') = \mathrm{tr}(Y') = \alpha$ and $\mathrm{tr}(Z') = \gamma$. By Table 2, $\bar{X}', \bar{Y}' \in \mathcal{C}$ and so $\bar{Z}' \in \mathcal{C}^2$. Hence by Lemma 20, $z \in \mathcal{C}^2$ as needed.

Moreover, since $\mathrm{tr}(X) = \mathrm{tr}(X^{-1})$, we have, according to Table 2, $x^{-1} \in \mathcal{C}$ as well, and so $xx^{-1} = 1 \in \mathcal{C}^2$. □

Note that the previous proposition is a specific case of a more general result of Gow [7].

Proposition 23. *Let $G = \mathrm{PSL}_2(q)$ when q is even and let $\mathcal{C}$ be the G-conjugacy class of a unipotent element x. Then $\mathcal{C}^2 = G$.*

Proof. Let $z \in G$ be any semisimple element and denote $\gamma = \mathrm{tr}(z)$. By Theorem 6, there exist matrices $x', y', z' \in G$ such that $\mathrm{tr}(x') = \mathrm{tr}(y') = 0$, $\mathrm{tr}(z') = \gamma$. Thus $x', y' \in \mathcal{C}$ and so $z' \in \mathcal{C}^2$. Hence by Lemma 20, $z \in \mathcal{C}^2$ as needed.

Moreover, since x has order 2, we have $x^2 = 1 \in \mathcal{C}^2$. Without loss of generality we may assume that

$$x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

and take

$$y = \begin{pmatrix} a+1 & a \\ a & a+1 \end{pmatrix} \in \mathrm{SL}_2(q) \quad (\text{where } a \neq 0, 1).$$

Then

$$xy = yx = \begin{pmatrix} a & a+1 \\ a+1 & a \end{pmatrix}.$$

Since $\mathrm{tr}(x) = \mathrm{tr}(y) = \mathrm{tr}(xy) = 0$, the matrices x, y, xy are unipotents. Hence by Lemma 20, $\mathcal{C}^2$ contains all the unipotent elements. □

3.3 Unipotent elements contained in $\mathcal{C}^2$

Proposition 24. *Let $G = \mathrm{PSL}_2(q)$ and let $\mathcal{C}$ be the G-conjugacy class of a semisimple split element x. Then $\mathcal{C}^2$ contains all the unipotent elements in G.*

Proof. By Table 2, we may assume x is an image of a matrix

$$X = \begin{pmatrix} a & 1 \\ 0 & a^{-1} \end{pmatrix} \in \mathrm{SL}_2(q) \quad (\text{where } a \neq 0, \pm 1).$$

Let

$$Y = \begin{pmatrix} a^{-1} & a^{-1}(1-a) \\ 0 & a \end{pmatrix}.$$

Then its image in $G = \mathrm{PSL}_2(q)$ is G-conjugate to x, and

$$XY = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Hence the class $\mathcal{C}^2$ contains a unipotent element, and the result now follows from Lemma 20. □

Proposition 25. *Let $G = \mathrm{PSL}_2(q)$ when q is odd and let $\mathcal{C}$ be the G-conjugacy class of a semisimple non-split element x of order greater than 2. Then $\mathcal{C}^2$ contains all the unipotent elements in G.*

Proof. By Table 2, we may assume that x is an image of a matrix

$$X = \begin{pmatrix} a & -1 \\ 1 & 0 \end{pmatrix} \in \mathrm{SL}_2(q) \quad (\text{where } a \neq 0).$$

Let

$$Y = \begin{pmatrix} 0 & 1 \\ -1 & -a \end{pmatrix}.$$

Then its image in $G = \mathrm{PSL}_2(q)$ is G-conjugate to x, and

$$XY = \begin{pmatrix} 1 & 2a \\ 0 & 1 \end{pmatrix}.$$

Hence the class $\mathcal{C}^2$ contains a unipotent element, and the result now follows from Lemma 20. □

Proposition 26. *Let $G = \mathrm{PSL}_2(q)$ when q is odd and let $\mathcal{C}$ be the G-conjugacy class of a semisimple non-split element x of order 2. Then $\mathcal{C}^2$ does not contain any unipotent element of G.*

Proof. Assume that $\mathcal{C}^2$ contains a unipotent element $z \in G$. Then $z = xy$ for some non-split elements x, y of order 2. Let $X, Y, Z \in \mathrm{SL}_2(q)$ be the pre-images of x, y, z respectively. Then $\mathrm{tr}(X) = \mathrm{tr}(Y) = 0$ and $\mathrm{tr}(Z) = \pm 2$. Observe that $(0, 0, \pm 2)$ is a *singular* triple. Therefore, by Theorem 7, the subgroup $H = \langle x, y \rangle$ is a *structural* subgroup of G. By observing the possible subgroups of G detailed in Table 3 above, H cannot be a subgroup of the Borel subgroup since it contains a non-split element, and hence cannot contain the unipotent element z, yielding a contradiction. □

Corollary 27. *Let $G = \mathrm{PSL}_2(q)$ when q is odd and let $\mathcal{C}$ be the G-conjugacy class of a semisimple element x of order 2. Then:*

- *If $q \equiv 1 \bmod 4$, then $\mathcal{C}^2$ contains all the unipotent elements in G.*
- *If $q \equiv 3 \bmod 4$, then $\mathcal{C}^2$ does not contain any unipotent element of G.*

Proof. If $q \equiv 1 \bmod 4$, then an element of order 2 is split and the result follows from Proposition 24. If $q \equiv 3 \bmod 4$, then an element of order 2 is non-split and the result follows from Proposition 26. □

Proposition 28. *Let $G = \mathrm{PSL}_2(q)$ when q is even and let $\mathcal{C}$ be the G-conjugacy class of a semisimple non-split element x. Then $\mathcal{C}^2$ does not contain any unipotent element of G.*

Proof. Assume that $\mathcal{C}^2$ contains a unipotent element $z \in G$. Then $z = xy$ for some non-split matrices x, y. It follows that $\mathrm{tr}(x) = \mathrm{tr}(y) = \alpha \neq 0$ and $\mathrm{tr}(z) = 0$. Observe that $(\alpha, \alpha, 0)$ is a *singular* triple. Therefore, by Theorem 7, the subgroup $H = \langle x, y \rangle$ is a *structural* subgroup of G. By observing the possible subgroups of G detailed in Table 3, H cannot be a subgroup of the Borel subgroup since it contains a non-split element, and hence cannot contain the unipotent element z, yielding a contradiction. □

3.4 Unipotent conjugacy classes $\mathcal{C}$ when q is odd

Proposition 29. *Let $G_0 = \mathrm{SL}_2(q)$ when $q = p^e$ is odd, and let $A, B \in G_0$, with $A, B \neq \pm I$, satisfy $\mathrm{tr}(A), \mathrm{tr}(B) \in \{\pm 2\}$. Denote $C = AB$ and $\gamma = \mathrm{tr}(C)$.*

(1) *If $\mathrm{tr}(A) = \mathrm{tr}(B)$, then A is G_0-conjugate to B if and only if $2 - \gamma$ is a square in $\mathbb{F}_q$.*

(2) *If $\mathrm{tr}(A) = -\mathrm{tr}(B)$, then A is G_0-conjugate to $-B$ if and only if $2 + \gamma$ is a square in $\mathbb{F}_q$.*

Proof. Without loss of generality we may assume that $A = U_1$.

(1) If $B = MU_1M^{-1}$ for some matrix $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in G_0$, then

$$\gamma = \mathrm{tr}(C) = \mathrm{tr}(AB) = \mathrm{tr}(U_1MU_1M^{-1})$$
$$= \mathrm{tr}\begin{pmatrix} 1-ac-c^2 & 1+ac+a^2 \\ -c^2 & 1+ac \end{pmatrix} = 2-c^2,$$

and so $2-\gamma$ is a square in $\mathbb{F}_q$.

If $B = MU_1'M^{-1}$ for some matrix $M \in G_0$, then

$$\gamma = \mathrm{tr}(C) = \mathrm{tr}(AB) = \mathrm{tr}(U_1MU_1'M^{-1}) = 2-x^2c^2,$$

and since $x \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$, it follows that $2-\gamma$ is a non-square in $\mathbb{F}_q$.

(2) Similarly, if $B = M(-U_1)M^{-1}$ for some matrix $M \in G_0$, then

$$\gamma = \mathrm{tr}(C) = \mathrm{tr}(AB) = \mathrm{tr}(U_1M(-U_1)M^{-1}) = -2+c^2,$$

and so $2+\gamma$ is a square in $\mathbb{F}_q$.

If $B = M(-U_1')M^{-1}$ for some matrix $M \in G_0$, then

$$\gamma = \mathrm{tr}(C) = \mathrm{tr}(AB) = \mathrm{tr}(U_1M(-U_1')M^{-1}) = -2+x^2c^2,$$

and so $2+\gamma$ is a non-square in $\mathbb{F}_q$. □

Therefore, in order to decide whether $C = AB$, where $A, B \in G$ are G-conjugate unipotent elements and C is of order $t \neq p$, one needs to determine whether for $\gamma \in \mathcal{T}_q(t)$, $2-\gamma$ or $2+\gamma$ is a square in $\mathbb{F}_q$. In Proposition 9 we showed that this is equivalent to decide whether t is a *q-good* order or not (see Definition 2).

Corollary 30. *Let $G = \mathrm{PSL}_2(q)$ when $q = p^e$ is odd. Let $A, B \in G$ be elements of order p and assume that the order of $C = AB$ is $t \neq p$. Then A is G-conjugate to B if and only if t is a* q-good *order.*

Proof. Let $A, B \in G_0 = \mathrm{SL}_2(q)$ and let $C = AB$, and assume that their images $\bar{A}, \bar{B}, \bar{C} \in G = \mathrm{PSL}_2(q)$ have respective orders (p, p, t), $t \neq p$. Put $\gamma = \mathrm{tr}(C)$. Then $\bar{A}$ and $\bar{B}$ are unipotent if and only if $A, B \neq \pm I$ and $\mathrm{tr}(A), \mathrm{tr}(B) \in \{\pm 2\}$. Moreover, $\bar{A}$ and $\bar{B}$ are G-conjugate if and only if either $\mathrm{tr}(A) = \mathrm{tr}(B)$ and A and B are G_0-conjugate or $\mathrm{tr}(A) = -\mathrm{tr}(B)$ and A and $-B$ are G_0-conjugate. From Proposition 29 we deduce that $\bar{A}$ and $\bar{B}$ are G-conjugate if and only if either $2-\gamma$ or $2+\gamma$ is a square in $\mathbb{F}_q$. By Proposition 9, the latter is equivalent to t being a *q-good* order. □

Corollary 31. *Let $G = \mathrm{PSL}_2(q)$ when q is odd and let $\mathcal{C}$ be the G-conjugacy class of a unipotent element x. Let z be a semisimple element in G. Then $\mathcal{C}^2$ contains z if and only if the order of z is* q-good.

Proof. The proof follows from Corollary 30 and Lemma 20. □

Proposition 32. *Assume that $q = p^e$ where p is odd and $5 \leq q \neq 9$. Furthermore, let $G = \mathrm{PSL}_2(q)$. Then there exist two G-conjugate unipotent elements A and B such that $\langle A, B\rangle = G$.*

Moreover, if $C = AB$ is semisimple, then the order of C is q-minimal *and* q-good.

Proof. Let $(A, B, C = AB) \in G^3$ be a triple of respective orders (p, p, t) with $t \neq p$. If t is not q-good, then by Corollary 30, A and B are not G-conjugate. If t is not q-minimal, then the subgroup $\langle A, B\rangle$ is contained in a subfield subgroup isomorphic to $\mathrm{PSL}_2(q_1)$ for some proper subfield $\mathbb{F}_{q_1} \subset \mathbb{F}_q$ (see [11] and [9]).

Now, let t be a q-minimal order which is also a q-good order. By Theorem 6, there exist a triple $(A, B, C) \in G^3$ of respective orders (p, p, t) with $ABC = 1$. By Corollary 30, A is G-conjugate to B.

Let $\gamma \in \mathcal{T}_q(t)$. As $t \neq p$, we have $\gamma \neq \pm 2$ and so $(\gamma \pm 2)^2 \neq 0$ implying that $(2, 2, \gamma)$ is *non-singular*, hence by Theorem 7, $\langle A, B\rangle$ is not a structural subgroup of G. Since t is q-minimal, it follows that $\langle A, B\rangle$ is not isomorphic neither to $\mathrm{PSL}_2(q_1)$ nor to $\mathrm{PGL}_2(q_1)$, for some proper subfield $\mathbb{F}_{q_1}$ of $\mathbb{F}_q$. Moreover, if $5 < q \neq 9$, then either $p > 5$; or $p = 5$ and $e > 1$ implying that $t \neq 2, 3, 5$; or $p = 3$ and $e > 2$ implying that $t > 5$ (see Table 1). Therefore, $\langle A, B\rangle$ cannot be a small subgroup, hence $\langle A, B\rangle = G$. □

Remark 33. Let $G = \mathrm{PSL}_2(9) \cong A_6$, let A and B be two unipotent elements (of order 3) and $C = (AB)^{-1}$. Denote the order of C by t. Then $t \in \{2, 3, 4, 5\}$.

- Clearly, if $t = 2$ or $t = 3$, then $\langle A, B\rangle \neq G$ (see Table 1).
- $t = 4$ is not 9-good and so A and B are not G-conjugate, by Corollary 30.
- $t = 5$ is 9-good, however if A is G-conjugate to B, then one can verify that $\langle A, B\rangle \cong A_5$ is a small subgroup of G (see e.g. [6, Section 2, Theorem 8.4]).

Acknowledgments. The author would like to thank Gili Schul for useful discussions and the editor for his kind assistance.

Bibliography

[1] H. S. M. Coxeter and W. O. J. Moser, *Generators and Relations for Discrete Groups*, Ergeb. Math. Grenzgeb. 14, Springer, Berlin, 1957.

[2] L. E. Dickson, *Linear Groups with an Exposition of the Galois Field Theory*, Teubner, Leipzig, 1901.

[3] L. Dornhoff, *Group Representation Theory. Part A: Ordinary Representation Theory*, Marcel Dekker, New York, 1971.

[4] E. W. Ellers and N. Gordeev, On the conjectures of J. Thompson and O. Ore, *Trans. Amer. Math. Soc.* **350** (1998), 3657–3671.

[5] S. Garion, On Beauville structures for PSL$(2, q)$, preprint (2013), `http://arxiv.org/abs/1003.2792`.

[6] D. Gorenstein, *Finite Groups*, Chelsea Publishing, New York, 1980.

[7] R. Gow, Commutators in finite simple groups of Lie type, *Bull. Lond. Math. Soc.* **32** (2000), no. 3, 311–315.

[8] R. Guralnick and G. Malle, Products of conjugacy classes and fixed point spaces, *J. Amer. Math. Soc.* **25** (2012), 77–121.

[9] U. Langer and G. Rosenberger, Erzeugende endlicher projektiver linearer Gruppen, *Results Math.* **15** (1989), no. 1–2, 119–148.

[10] F. Levin and G. Rosenberger, Generators of finite projective linear groups. II, *Results Math.* **17** (1990), no. 1–2, 120–127.

[11] A. M. Macbeath, Generators of the linear fractional groups, in: *Number Theory* (Houston 1967), Proc. Sympos. Pure Math. 12, American Mathematical Society, Providence (1969), 14–32.

[12] C. Marion, Triangle groups and $\mathrm{PSL}_2(q)$, *J. Group Theory* **12** (2009), 689–708.

[13] G. Schul, *Expansion in finite simple groups*, Ph.D. thesis, in preparation.

[14] M. Suzuki, *Group Theory I*, Springer, Berlin, 1982.

Received August 5, 2013; revised April 23, 2015.

Author information

Shelly Garion, Fachbereich Mathematik und Informatik, Universität Münster,
Einsteinstraße 62, 48149 Münster, Germany.
Current address: IBM Research – Haifa, Haifa University Campus,
Mount Carmel, 3498825 Haifa, Israel.
E-mail: `shelly.garion@mail.huji.ac.il`