Available online at www.sciencedirect.com

SCIENCE DIRECT®

European Journal of Combinatorics 25 (2004) 1077–1085

European Journal of Combinatorics

www.elsevier.com/locate/ejc

Perfect codes in $SL(2, 2^f)$

Sachiyo Terada

Software Development Center, RICOH Tottori Software Technology Co., Ltd, Aishin-Chiyomi Bldg. 1-100 Chiyomi, Tottori 680-0911, Japan

Received 28 November 2001; received in revised form 25 November 2003; accepted 5 December 2003

Available online 16 January 2004

Abstract

It is shown that any subset X which is closed under conjugation does not divide $SL(2, 2^f)$ non-trivially if $f \neq 1$; that is, there exists no perfect code in the Cayley graph of $SL(2, 2^f)$ with respect to X if $f \neq 1$. A list of subsets X closed under conjugation and natural numbers λ such that X possibly divides $\lambda SL(2, 2^f)$ has been established. Moreover, as a case where X is not closed under conjugation, the orbits X of involutions by conjugation of a Singer cycle of $SL(2, 2^f)$ have been considered and it has been determined whether they divide $\lambda SL(2, 2^f)$ non-trivially or not.

1. Preliminaries

For a non-empty subset X of a finite group G and a natural number λ, it is said that X *divides* λG if there is a subset Y of G such that each element g of G is written in exactly λ ways as $g = xy$ with $x \in X$ and $y \in Y$; the subset Y is called a *code* with respect to X and we write $X \cdot Y = \lambda G$. Note that if X divides λG with code Y, then $\lambda = |X||Y|/|G|$ and $\lambda \leq |X|$. It is said X *trivially* divides λG if $X = G$ or $\lambda = |X|$; in the case $X = G$, we have $X \cdot Y = \lambda G$ for any subset Y of cardinality λ, and in the case $\lambda = |X|$, we have $X \cdot Y = \lambda G$ with $Y = G$. For X dividing λG, it could be assumed that $\lambda \leq |X| - 1$; otherwise it is the trivial case. If X is a subgroup of G or a set of representatives of left cosets for some subgroup of G, then X divides G obviously. Suppose that a subset X divides λG with code Y. Then $X \cdot (Yg) = \lambda G$ for any $g \in G$. Therefore if we can take elements $g_1, g_2, \ldots, g_r$ of G such that $Y \cup (Yg_1) \cup (Yg_2) \cup \cdots \cup (Yg_r) =: Y'$ is a disjoint union, then X divides $r\lambda G$ with code Y'.

E-mail address: sachiyo_t-no5@mvb.biglobe.ne.jp (S. Terada).

0195-6698/$ - see front matter © 2003 Elsevier Ltd. All rights reserved.
doi:10.1016/j.ejc.2003.12.001

Table 1
The character table of S_3

Class name	1	$\mathcal{U}$	$\mathcal{S}$
Size	1	3	2
χ_1	1	1	1
χ_2	1	−1	1
χ_3	2	0	−1

Let X be a subset of G such that X does not contain the identity 1 of G and X coincides with $X^{-1} := \{x^{-1} \mid x \in X\}$. Assume that X divides G with code Y. Then Y is partitioned into pairs $\{y_1, y_2\}$ such that $y_1 \in Xy_2$ and $y_2 \in Xy_1$. In particular, $|Y|$ is even.

For a finite group G and its non-empty subset Ω, the *Cayley graph* $\Gamma(G, \Omega)$ is the graph with the vertex set $V\Gamma = G$ and the edge set $E\Gamma = \{(g, h) \mid gh^{-1} \in \Omega\}$. The *distance* $\partial(v, w)$ is the shortest length of paths from w to v; if $X \neq X^{-1}$, we define $\partial(v, w)$ by using directed paths. A subset C of the vertex set $V\Gamma$ is called a *perfect e-code* if for any vertex v, there is a unique c in C such that $\partial(v, c) \leq e$. Perfect e-codes in the Cayley graph $\Gamma(G, \Omega)$ are perfect one-codes in the Cayley graph $\Gamma(G, X)$, where X is the set of vertices x with $\partial(x, 1) \leq e$ in $\Gamma(G, \Omega)$. So when we consider perfect e-codes in a Cayley graph, we may assume that $e = 1$. Note that X divides G with code Y if and only if G is covered by the disjoint sets $\{Xy \mid y \in Y\}$. If $X \cdot Y = G$ and X contains the identity, then Y is a perfect one-code in $\Gamma(G, X\backslash\{1\})$.

Lemma 1. *If a subset X divides λG with code $Y \neq G$, then the Cayley graph $\Gamma(G, X)$ has eigenvalue 0. If in addition X contains the identity, the Cayley graph $\Gamma(G, X\backslash\{1\})$ has eigenvalue -1.*

Proof. Let A be the adjacency matrix of $\Gamma(G, X)$. For a subset Z of G, let Φ_Z be the column vector indexed by the elements of G whose entries are 1 or 0 according as the vertex belongs to Z or not. Then we have $A\Phi_Y = \lambda\Phi_G$ and $A\Phi_G = |X|\Phi_G$. Thus $A(\Phi_Y - \lambda|X|^{-1}\Phi_G) = \mathbf{0}$. Moreover, $\Phi_Y \neq \lambda|X|^{-1}\Phi_G$ since $Y \neq G$. Hence A has eigenvalue 0. □

Lemma 2 ([1, Theorem 7.2]). *Let G be a finite group and $\{C_i\}_i$ the conjugacy classes. Let X be a subset of G closed under conjugation of G: $X = \bigcup_{i\in\mathcal{I}} \mathcal{C}_i$ for some index set $\mathcal{I}$. The eigenvalues of the Cayley graph $\Gamma(G, X)$ are $\sum_{i\in\mathcal{I}} |\mathcal{C}_i|\vartheta(c_i)/\vartheta(1)$, where c_i is a representative of the conjugacy class $\mathcal{C}_i$ and ϑ runs through all irreducible characters of G. Moreover, the multiplicity of an eigenvalue α of $\Gamma(G, X)$ equals the sum of $\vartheta(1)^2$ over all irreducible characters ϑ such that $\alpha = \sum_{i\in\mathcal{I}} |\mathcal{C}_i|\vartheta(c_i)/\vartheta(1)$.*

For example, the character table of S_3 is given in Table 1, where $\mathcal{U}$ and $\mathcal{S}$ are the conjugacy classes corresponding to the partitions $2^1 1^1$ and 3^1, respectively. Let X be a subset of S_3 closed under conjugation. If X divides λS_3 then it can easily be deduced that $X = \mathcal{U}$, $S_3\backslash\mathcal{U}$ or S_3 from Lemmas 1 and 2. In fact, the subsets $\mathcal{U}$ and $S_3\backslash\mathcal{U}$ divide S_3 with code $Y = \{\mathrm{id}, (1\ 2)\}$.

Theorem 3 (An Analogue to [2]). *Let G be a finite group, X its subset (not necessarily closed under conjugation) and λ a natural number. Assume that G has a subgroup H with the property that*

(1) *the order* $|X|$ *of* X *does not divide* $\lambda|H|$, *and*
(2) *the matrix* $P_H(\widehat{X})$ *is non-singular, where* P_H *is the permutation representation of* G *acting on the cosets* $H\backslash G$ *and* $\widehat{X}$ *is the sum of elements of* X *in the group algebra* $\mathbf{C}[G]$ *over the complex field* $\mathbf{C}$.

Then X *does not divide* λG *non-trivially.*

Proof. Assume that $\widehat{X}\widehat{Y} = \lambda\widehat{G}$ in the group algebra $\mathbf{C}[G]$ for some subset Y of G. Then $P_H(\widehat{X})P_H(\widehat{Y}) = P_H(\lambda\widehat{G}) = \lambda P_H(\widehat{G})$. By the assumption (2), there exists the inverse matrix $P_H(\widehat{X})^{-1}$, which can be described as a polynomial of $P_H(\widehat{X})$. Since $P_H(\widehat{G}) = P_H(x)P_H(\widehat{G})$ for any x in G, it is obtained that $P_H(\widehat{Y}) = P_H(\widehat{X})^{-1}\lambda P_H(\widehat{G}) = a\lambda P_H(\widehat{G})$ for some rational number a. Then, by multiplying the last equation by $P_H(\widehat{X})$ from the left, we have $a = |X|^{-1}$. Hence it is obtained that

$$P_H(\widehat{Y}) = \frac{\lambda}{|X|}P_H(\widehat{G}) = \frac{\lambda|H|}{|X|}J,$$

where J is the matrix with all entries 1. This equation contradicts the fact that the matrix $P_H(\widehat{Y}) = \sum_{y\in Y} P_H(y)$ has integral entries. □

Remarks 4. (1) The matrix $P_H(\widehat{X})$ is non-singular if and only if $R(\widehat{X})$ is non-singular for each irreducible representation R appearing in P_H.
(2) X divides λG with code Y if and only if $G\backslash X$ divides μG with code Y, where $\mu = |Y| - \lambda$.

Lemma 5. *Let* X *divide* λG *with code* Y. *Assume that there exists a subgroup* H *of* G *such that the matrix* $P_H(\widehat{X})$ *is non-singular. Then the following hold.*

(1) *The integer* λ *is divisible by* $|X|/\gcd(|X|, |H|)$.
(2) *If* X *is closed under conjugation, then* μ *is divisible by* $(|G| - |X|)/\gcd(|G| - |X|, |H|)$, *where* $\mu = |Y| - \lambda$.

Proof. The claim (1) derives from Theorem 3. Suppose that X is closed under conjugation. Then $\widehat{G\backslash X}$ belongs to the center of $\mathbf{C}[G]$. Thus each irreducible component of $P_H(\widehat{G\backslash X})$ is a scalar by Schur's lemma. Since $\vartheta(\widehat{G\backslash X}) = -\vartheta(\widehat{X}) \neq 0$ for each non-trivial irreducible character ϑ appearing in the character of P_H, the matrix $P_H(\widehat{G\backslash X})$ is non-singular. Therefore the claim (2) of this lemma follows from Theorem 3. □

We consider which X divides $G = SL(2, q)$ for a power q of 2. Note that the special linear group $SL(2, 2)$ is isomorphic to the symmetric group S_3, and so the argument for $q = 2$ is over. Throughout this paper, we assume that q is a power of 2 greater than 2. Let $\mathcal{I}$ and $\mathcal{J}$ be the index sets

$$\mathcal{I} := \{1, 2, \ldots, (q-2)/2\} \qquad \text{and} \qquad \mathcal{J} := \{1, 2, \ldots, q/2\}.$$

The character table of $SL(2, q)$ is given in Table 2, where δ and ε are primitive $(q-1)$st and $(q+1)$st roots of unity in the complex number field $\mathbf{C}$, respectively. For each subgroup H of $SL(2, q)$, the permutation character $1_H^{SL(2,q)}$ is written as

$$1_H^{SL(2,q)} = |H|^{-1}\sum_{\vartheta}\left(\sum_{x\in H}\vartheta(x)\right)\vartheta \tag{1}$$

Table 2
The character table of $SL(2,q)$

Class name Size	1 1	$\mathcal{U}$ q^2-1	$\mathcal{T}_i$ $(i \in \mathcal{I})$ $q(q+1)$	$\mathcal{S}_j$ $(j \in \mathcal{J})$ $q(q-1)$
χ_0	1	1	1	1
χ_1	q	0	1	-1
ψ_m $(m \in \mathcal{I})$	$q+1$	1	$\delta^{mi}+\delta^{-mi}$	0
φ_n $(n \in \mathcal{J})$	$q-1$	-1	0	$-(\varepsilon^{nj}+\varepsilon^{-nj})$

Table 3
The decompositions of $1_H^G (G = SL(2,q)$ and $q = 2^f \geq 4)$

Subgroup H	$\lvert H\rvert$	The decomposition							
1	1	χ_0	$+$	$q\chi_1$	$+$	$(q+1)\sum_m \psi_m$	$+$	$(q-1)\sum_n \varphi_n$
S	$q+1$	χ_0			$+$	$\sum_m \psi_m$	$+$	$\sum_n \varphi_n$
$N_G(S)$	$2(q+1)$	χ_0			$+$	$\sum_m \psi_m$		
$\langle t\rangle$	$q-1$	χ_0	$+$	$2\chi_1$	$+$	$\sum_m \psi_m$	$+$	$\sum_n \varphi_n$
$N_G(\langle t\rangle)$	$2(q-1)$	χ_0	$+$	χ_1	$+$	$\sum_m \psi_m$		
U	q	χ_0	$+$	χ_1	$+$	$2\sum_m \psi_m$		
B	$q(q-1)$	χ_0	$+$	χ_1				

Here S is a Singer cycle of G, t a diagonal matrix of order $q-1$, U the standard unipotent radical $\left\{\begin{bmatrix}1 & \alpha\\ 0 & 1\end{bmatrix} \,\middle|\, \alpha \in \mathrm{GF}(q)\right\}$, $B = N_G(U)$ the standard Borel subgroup and the summations run over $m \in \mathcal{I}$ and $n \in \mathcal{J}$.

by the Frobenius reciprocity, where the first summation $\sum_\vartheta$ runs over all irreducible characters ϑ of $SL(2,q)$. Using Table 2 and Eq. (1), the decomposition of the permutation character $1_H^{SL(2,q)}$ into irreducible characters is obtained in Table 3 for each subgroup H of $SL(2,q)$.

2. The case where X is closed under conjugation

Let us assume that the subset X is closed under conjugation in this section. For an irreducible representation R, $R(\widehat{X})$ is a scalar by Schur's lemma and therefore the condition (2) of Theorem 3 can be checked easily.

Theorem 6. *Suppose that X is a non-trivial subset closed under conjugation of $SL(2,q)$ $(q = 2^f \geq 4)$. Assume that X does not contain the identity and X divides $\lambda SL(2,q)$. Then X is one of the following with λ divisible by λ' in the table.*

Subset X	λ'	*(when $\psi_m(\widehat{X}) \neq 0$ for all $m \in \mathcal{I}$)*
$\mathcal{U}$	$q-1$	
$\left(\bigcup_{i\in\mathcal{I}_0} \mathcal{T}_i\right) \cup \left(\bigcup_{j\in\mathcal{J}'} \mathcal{S}_j\right)$	$\lvert X\rvert/(p_0 q)$	
$\left(\bigcup_{i\in\mathcal{I}'} \mathcal{T}_i\right) \cup \left(\bigcup_{j\in\mathcal{J}_0} \mathcal{S}_j\right)$	$\lvert X\rvert/(p' q)$	$(\lvert X\rvert/2)$,

where $\mathcal{I}_0$ (respectively $\mathcal{J}_0$) is a subset (possibly empty) of the index set $\mathcal{I}$ (respectively $\mathcal{J}$)

such that

$$\sum_{i\in\mathcal{I}_0}({\delta_0}^i+{\delta_0}^{-i})=0\left(\textit{respectively}\sum_{j\in\mathcal{J}_0}({\varepsilon_0}^j+{\varepsilon_0}^{-j})=0\right)$$

for some $(q-1)$*st* (*respectively* $(q+1)$*st*) *root* δ_0 (*respectively* ε_0) *of unity in* $\mathbf{C}$, $\mathcal{I}'$ (*respectively* $\mathcal{J}'$) *is a subset* (*possibly empty*) *of* $\mathcal{I}$ (*respectively* $\mathcal{J}$),

$$p_0 := \gcd(|\mathcal{I}_0|, q-1) \textit{ if } \mathcal{I}_0 \neq \emptyset, \textit{ or } q-1 \textit{ otherwise},$$
$$p' := \gcd(|\mathcal{I}'|, q-1) \textit{ if } \mathcal{I}' \neq \emptyset, \textit{ or } q-1 \textit{ otherwise}.$$

Proof. Subsets X for which the Cayley graphs $\Gamma(SL(2,q),X)$ have eigenvalue 0 will be listed first, and then conditions on λ are considered by taking suitable subgroups H in Theorem 3. Let

$$\widehat{X}=a\widehat{\mathcal{U}}+\sum_{i\in\mathcal{I}}b_i\widehat{\mathcal{T}_i}+\sum_{j\in\mathcal{J}}c_j\widehat{\mathcal{S}_j},$$

where $a, b_i (i\in\mathcal{I}), c_j (j\in\mathcal{J})$ are 0 or 1.

Assume that the eigenvalue corresponding to χ_1 is equal to 0; that is, $\chi_1(\widehat{X})=0$. Then the equation

$$\begin{aligned}0&=0+\sum_{i\in\mathcal{I}}\frac{b_iq(q+1)\cdot 1}{q}+\sum_{j\in\mathcal{J}}\frac{c_jq(q-1)\cdot(-1)}{q}\\&=(q+1)\sum_{i\in\mathcal{I}}b_i-(q-1)\sum_{j\in\mathcal{J}}c_j\end{aligned}$$

is obtained. By considering this equation modulo $q-1$, the set $\{i\in\mathcal{I}\mid b_i=1\}$ has to be empty since $\sum_{i\in\mathcal{I}}b_i\le|\mathcal{I}|=(q-2)/2$. This implies that the index set $\{j\in\mathcal{J}\mid c_j=1\}$ is also empty. Therefore, we have

$$X=\mathcal{U}, \text{ or } \emptyset.$$

To determine λ for $X=\mathcal{U}$, let us set $H=S$. The irreducible representations R appearing in P_S are those affording χ_0, ψ_m $(m\in\mathcal{I})$ and φ_n $(n\in\mathcal{J})$ by Table 3. Since each of the scalar matrices $R(\widehat{\mathcal{U}})$ is not zero by the character table, the matrix $P_S(\widehat{\mathcal{U}})$ is non-singular. If $\mathcal{U}$ divides $\lambda SL(2,q)$, then the integer λ is divisible by $|\mathcal{U}|/\gcd(|\mathcal{U}|,|\mathcal{S}|)=(q^2-1)/\gcd(q^2-1,q+1)=q-1$ by Lemma 5(1).

In the case where $\psi_m(\widehat{X})=0$ for some $m\in\mathcal{I}$, we have $0=(q^2-1)a+q(q+1)\times\sum_{i\in\mathcal{I}}(\delta^{mi}+\delta^{-mi})b_i$. This equation modulo q implies that $a=0$. Thus we have $\sum_{i\in\mathcal{I}}(\delta^{mi}+\delta^{-mi})b_i=0$ and so $\{i\in\mathcal{I}\mid b_i=1\}=\mathcal{I}_0$ for some $\mathcal{I}_0$. Therefore, we have

$$X=\left(\bigcup_{i\in\mathcal{I}_0}\mathcal{T}_i\right)\cup\left(\bigcup_{j\in\mathcal{J}'}\mathcal{S}_j\right).$$

To determine λ for this subset X, let us set $H=B$, the standard Borel subgroup. In that case the matrix $P_B(\widehat{X})$ is non-singular by Tables 2 and 3 and by the argument for the case $\chi_1(\widehat{X})=0$. If X divides $\lambda SL(2,q)$, then integer λ is divisible by $|X|/\gcd(|X|,|B|)=$

$|X|/(p_0 q)$ since $|X| = q((q+1)|\mathcal{I}_0| + (q-1)|\mathcal{J}'|)$ and $|B| = q(q-1)$. Hence the second row of the list is apparent.

In the case where $\varphi_n(\widehat{X}) = 0$ for some $n \in \mathcal{J}$, the equation

$$X = \left(\bigcup_{i \in \mathcal{I}'} \mathcal{T}_i\right) \cup \left(\bigcup_{j \in \mathcal{J}_0} \mathcal{S}_j\right)$$

holds by an argument similar to the previous case. If $\psi_m(\widehat{X}) = 0$ for some $m \in \mathcal{I}$, then the condition on λ is already obtained. Suppose that $\psi_m(\widehat{X}) \neq 0$ for all $m \in \mathcal{I}$ and let us set $H = B$, $H = N_{SL(2,q)}(S)$ and $H = N_{SL(2,q)}(\langle t \rangle)$ in turn. Then the matrix $P_H(\widehat{X})$ is non-singular for each H by Tables 2 and 3. Assume that X divides $\lambda SL(2, q)$ and set $r_0 := \gcd(|\mathcal{J}_0|, q + 1)$ if $\mathcal{J}_0 \neq \emptyset$, or $p + 1$ otherwise. Then the integer λ is divisible by $|X|/(p'q)$, $|X|/\gcd(|X|, 2(q+1)) = |X|/(2r_0)$ and $|X|/\gcd(|X|, 2(q-1)) = |X|/(2p')$ as $|X| = q((q+1)|\mathcal{I}'| + (q-1)|\mathcal{J}_0|)$. In order to take the least common multiple of these three integers, we calculate the greatest common divisor of qp', $2r_0$ and $2p'$. The integer 2 is, however, the greatest common divisor of the last two integers $2r_0$ and $2p'$ since $\gcd(q-1, q+1) = \gcd(q-1, 2) = 1$. Therefore, the integer λ is divisible by $|X|/2$ and hence the theorem is proved. □

Problem. For each X in the table of Theorem 6, determine whether X divides $\lambda SL(2, q)$ or not.

The list in Theorem 6 with $\lambda = 1$ settles the perfect e-code problem in $SL(2, q)$ when $SL(2, q)$ acts on the Cayley graph by conjugation:

Theorem 7. *For a subset X closed under conjugation and a power q of 2, the special linear group $SL(2, q)$ is divided by X non-trivially if and only if $q = 2$ and $X = \mathcal{U}$ or $X = SL(2, 2) \backslash \mathcal{U}$.*

In the following, we shall outline the proof of Theorem 7. When X does not contain the identity, Theorem 7 follows from Theorem 6 and the fact that $|Y|$ is even, where Y is a code of G with respect to X. Assume that X contains the identity. It has already been noticed in Section 1 that $G \backslash X$ divides μG with $\mu = |Y| - \lambda$. Hence $G \backslash X$ must be in the list of Theorem 6. Applying Lemma 5(2), we have the following corollary. The proof is omitted because it is quite similar to that of Theorem 6.

Corollary 8. *Suppose that X is closed under conjugation and X contains the identity. If X divides $\lambda SL(2, q)$, then X is one of the following with λ divisible by λ' in the table.*

Subset X	λ'	*(when $\psi_m(\widehat{X}) = 0$ for all $m \in \mathcal{I}$)*
$SL(2, q) \backslash \mathcal{U}$	$\lvert X\rvert/(q+1)$	
$SL(2, q) \backslash \left(\left(\bigcup_{i \in \mathcal{I}_0} \mathcal{T}_i\right) \cup \left(\bigcup_{j \in \mathcal{J}'} \mathcal{S}_j\right)\right)$	$\lvert X\rvert/(p_0 q)$	
$SL(2, q) \backslash \left(\left(\bigcup_{i \in \mathcal{I}'} \mathcal{T}_i\right) \cup \left(\bigcup_{j \in \mathcal{J}_0} \mathcal{S}_j\right)\right)$	$\lvert X\rvert/(p' q)$	$(\lvert X\rvert/2)$,

where $\mathcal{I}_0$ (respectively $\mathcal{J}_0$) is a subset (possibly empty) of the index set $\mathcal{I}$ (respectively $\mathcal{J}$) such that

$$\sum_{i \in \mathcal{I}_0} ({\delta_0}^i + {\delta_0}^{-i}) = 0 \left(\textit{respectively} \sum_{j \in \mathcal{J}_0} ({\varepsilon_0}^j + {\varepsilon_0}^{-j}) = 0 \right)$$

for some $(q-1)$*st* (*respectively* $(q+1)$*st*) *root* δ_0 (*respectively* ε_0) *of unity in* $\mathbf{C}$, $\mathcal{I}'$ (*respectively* $\mathcal{J}'$) *is a subset* (*possibly empty*) *of* $\mathcal{I}$ (*respectively* $\mathcal{J}$),

$$p_0 := \gcd(|\mathcal{I}_0|, q-1) \text{ if } \mathcal{I}_0 \neq \emptyset, \text{ or } q-1 \text{ otherwise},$$
$$p' := \gcd(|\mathcal{I}'|, q-1) \text{ if } \mathcal{I}' \neq \emptyset, \text{ or } q-1 \text{ otherwise}.$$

It is clear that the integer λ' is greater than 1. Therefore Theorem 7 holds.

3. Some cases where X is not closed under conjugation

We consider an orbit X of an involution by conjugation of a Singer cycle as a case where X is not closed under conjugation.

Let $q = 2^f \geq 4$ and $\mathrm{GF}(q^2)$ be the finite field of q^2 elements. Let ρ be a primitive $(q+1)$st root of unity in the multiplicative group $\mathrm{GF}(q^2)^\times$ and denote $\rho^j + \rho^{-j}$ by η_j. For each $\alpha \in \mathrm{GF}(q)$ with $\alpha \neq 0$, take matrices

$$u_\alpha := \begin{bmatrix} 1 & \alpha \\ 0 & 1 \end{bmatrix} \quad \text{and} \quad s := \begin{bmatrix} \eta_1 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} \rho & 1 \\ 1 & \rho \end{bmatrix} \begin{bmatrix} \rho & 0 \\ 0 & \rho^{-1} \end{bmatrix} \begin{bmatrix} \rho & 1 \\ 1 & \rho \end{bmatrix}^{-1}.$$

Lemma 9. *We have* $\eta_j = \eta_{-j}$, $\eta_{q+1} = \eta_0 = 0$, ${\eta_j}^2 = \eta_{2j}$,

$$\eta_i \eta_j = \eta_{i+j} + \eta_{i-j} \qquad \text{and} \qquad \eta_i + \eta_j = (\eta_{i+j})^{1/2}(\eta_{i-j})^{1/2}.$$

If $\eta_i = \eta_j$, *then we have* $i \equiv \pm j \bmod q+1$. *The order of* s *is* $q+1$; *that is,* s *is a generator of a Singer cycle. By definition,* s^j *can be written as*

$$s^j = {\eta_1}^{-1} \begin{bmatrix} \eta_{j+1} & \eta_j \\ \eta_j & \eta_{j-1} \end{bmatrix}.$$

Moreover, the field $\mathrm{GF}(q)$ *coincides with the set* $\{\eta_j^{-1}\eta_{j+1} \mid j = 1, 2, \ldots, q\}$, *since the matrix* s *acts on the project line* $PG(1,q)$ *regularly.*

Theorem 10. *Let* X_α *be the orbit of the involution* u_α *by conjugation of* $\langle s \rangle$:

$$X_\alpha := \{s^j u_\alpha s^{-j} \mid j = 0, 1, 2, \ldots, q\} \qquad (q = 2^f)$$

for $\alpha \in \mathrm{GF}(q)$ *with* $\alpha \neq 0$. *Then* X_α *does not divide* $\lambda SL(2,q)$ *non-trivially if* $\alpha \neq \eta_1$.

Proof. Let P be the permutation representation of $SL(2,q)$ acting on the projective line $PG(1,q)$. If $P(\widehat{X_\alpha})$ is non-singular, then X_α does not divide $\lambda SL(2,q)$ non-trivially by Theorem 3 with the subgroup H being the standard Borel subgroup B of order $q(q-1)$. Thus, it is sufficient to show that $P(\widehat{X_\alpha})$ is non-singular.

The elements of $PG(1,q)$ can be arranged as

$$v_0 = \left\{ a \begin{bmatrix} 1 \\ 0 \end{bmatrix} \;\middle|\; a \in \mathrm{GF}(q)^\times \right\} \qquad \text{and} \qquad v_i = s^i v_0 \text{ for } i = 1, 2, \ldots, q.$$

Then the (i,j) entry $P(\widehat{X_\alpha})_{i,j}$ of the matrix $P(\widehat{X_\alpha})$ is the number of k's such that $s^k u_\alpha s^{-k} v_j = v_i$. Note that the matrix $P(\widehat{X_\alpha})$ is circulant: $P(\widehat{X_\alpha})_{i,j} = P(\widehat{X_\alpha})_{i-j,0}$ since $s\widehat{X_\alpha}s^{-1} = \widehat{X_\alpha}$, where we understand the index modulo $q+1$.

For $k = 0, 1, 2, \ldots, q$, let

$$s^k u_\alpha s^{-k} v_0 = \left\{ c \begin{bmatrix} a \\ b \end{bmatrix} \;\middle|\; c \in \mathrm{GF}(q)^\times \right\}.$$

We have $b = 0$ if and only if $k = 0$. Assume that $b \neq 0$. Then

$$ab^{-1} = \alpha^{-1} {\eta_k}^{-2} (\eta_2 + \alpha \eta_{k+1} \eta_k) \tag{2}$$

since

$$s^k u_\alpha s^{-k} = {\eta_1}^{-2} \begin{bmatrix} \eta_2 + \alpha \eta_{k+1} \eta_k & \alpha {\eta_{k+1}}^2 \\ \alpha {\eta_k}^2 & \eta_2 + \alpha \eta_{k+1} \eta_k \end{bmatrix}.$$

If the number of indices k satisfying Eq. (2) is even for each $ab^{-1} \in \mathrm{GF}(q)$, then the matrix $P(\widehat{X_\alpha})$ has entries 1 on the diagonal and even integers off the diagonal. Hence the determinant of $P(\widehat{X_\alpha})$ is odd; in particular, $P(\widehat{X_\alpha})$ is non-singular.

Note that Eq. (2) is equivalent to (3) below:

$$\alpha(ab^{-1} \eta_{2k} + \eta_{2k+1} + \eta_1) + \eta_2 = 0 \tag{3}$$

obtained by multiplying each of the terms of (2) by $\alpha {\eta_k}^2$ and using $\eta_{k+1}\eta_k = \eta_{2k+1} + \eta_1$.

Now we would like to show the number of k satisfying (3) is even for each $ab^{-1} \in \mathrm{GF}(q)$. Assume that k satisfies Eq. (3) and take the index i such that $ab^{-1} = {\eta_i}^{-1} \eta_{i+1}$ by Lemma 9. Then $ab^{-1}\eta_i + \eta_{i+1} = 0$ and $0 = (ab^{-1}\eta_i + \eta_{i+1})\eta_{i-2k} = ab^{-1}(\eta_{2i-2k} + \eta_{2k}) + \eta_{2i-2k+1} + \eta_{2k+1}$. Thus

$$\begin{aligned} 0 &= \{\alpha(ab^{-1}\eta_{2k} + \eta_{2k+1} + \eta_1) + \eta_2\} \\ &\quad + \alpha\{ab^{-1}(\eta_{2i-2k} + \eta_{2k}) + \eta_{2i-2k+1} + \eta_{2k+1}\} \\ &= \alpha(ab^{-1}\eta_{2(i-k)} + \eta_{2(i-k)+1} + \eta_1) + \eta_2; \end{aligned}$$

that is, $i - k \pmod{q+1}$ also satisfies Eq. (3). If $i - k \equiv k \bmod q + 1$ then $\eta_i = \eta_{2k}$ and $\eta_{i+1} = \eta_{2k+1}$ by definition of η. Hence we have $\alpha\eta_1 + \eta_2 = 0$ since $ab^{-1} = {\eta_{2k}}^{-1}\eta_{2k+1}$. This contradicts $q \geq 4$ if $\alpha \neq \eta_1$. Therefore, the number of k satisfying Eq. (3) is even if $\alpha \neq \eta_1$. Thus the theorem is proved. □

In the case where $\alpha = \eta_1$, the set X_{η_1} divides $SL(2, q)$ since X_{η_1} is a set of representatives of the cosets $SL(2, q)/B$. Furthermore, Theorem 10 implies the theorem below on conjugation.

Theorem 11. *Let q be a power of 2 greater than 2 and X an orbit of an involution by conjugation of a Singer cycle of $SL(2, q)$. Then X divides $\lambda SL(2, q)$ non-trivially if and only if X is conjugate to X_{η_1}; that is, X is a complete set of representatives of left cosets for a Borel subgroup in $SL(2, q)$.*

Acknowledgement

The author would like to thank Professor Tatsuro Ito, who was her research supervisor.

References

[1] E. Bannai, T. Ito, Algebraic Combinatorics I: Association Schemes, Benjamin-Cummings, California, 1984.
[2] O. Rothaus, J.G. Thompson, A combinatorial problem in the symmetric group, Pacific J. Math. 18 (1966) 175–178.