数理解析研究所講究録 1299 巻 2003 年 103-119

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

Sachiyo Terada (寺 田 幸 代)
Division of Mathematics and Information Science
Graduate School of Natural Science and Technology
Kanazawa University
(金沢大学 自然科学研究科 計算科学講座)

Abstract

We show that the Cayley graph $\Gamma(SL(2,2^f),X)$ of the finite special linear group $SL(2,2^f)$ does not have any perfect code if X is closed under conjugation for a natural integer $f\geq 2$. Moreover, as a case where X is not closed under conjugation, we consider the orbits X of involutions by conjugation of a Singer cycle of $SL(2,2^f)$ and determine whether they divide $\lambda SL(2,2^f)$ non-trivially or not.

1 Introduction

We study a combinatorial problem below in the finite special linear groups $SL(2,2^f)$.

Problem. Determine the existence of perfect codes in a Cayley graph.

Perfect codes have been mainly studied over finite fields. Recently perfect codes are studied in distance-transitive graphs and distance-regular graphs. As a case of a graph which is not distance-regular, we choose a Cayley graph and consider perfect codes in it. Rothaus and Thompson [RT] considered the existence of perfect codes in the Cayley graph $\Gamma(S_n, T_0)$ of the symmetric group S_n with respect to the set T_0 of transpositions. They gave a necessary condition on n for the existence of perfect codes in $\Gamma(S_n, T_0)$ by using representation theory. N. Ito [It] gave more conditions on n by computing the distribution of character values. In this note, we treat a problem below which extends the problem above.

Problem. For a finite group G, determine the pairs of subsets X and natural integers λ such that X divide λG.

If there exists a perfect code in the Cayley graph $\Gamma(G, X)$, then the union $X \cup \{1\}$ divides G. Thus we can settle the existence problem of perfect codes in a Cayley graph if the pairs of X and λ above are determined.

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 $E\Gamma = \{(g, h) \mid gh^{-1} \in \Omega\}$. A subset C of the vertex set $V\Gamma$ of a graph Γ is called a *perfect e-code* if, for any vertex v of Γ, there is a unique codeword c in C such that $\partial(v, c) \leq e$, where $\partial(v, c)$ is the 'distance' from c to v; the shortest length of directed paths from c to v. 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 $e = 1$.

For a non-empty subset X of a group G and a natural integer λ, we say X *divides* λG *(with code* Y*)* and write $X{\cdot}Y = \lambda G$ 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 $y \in Y$. Note that if X divides λG with code Y, then $\lambda = |X||Y|/|G|$. We say X *trivially* divides λG with code Y if $\lambda = |X|$ or $X = G$; equivalently, $Y = G$ or $Y = \{y\}$ for some $y \in G$. As X always divides $|X|G$ trivially, we may assume that $\lambda = 1, 2, \ldots, |X| - 1$. 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'.

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 ([BI, Thm. 7.2, pp. 117], [It]). *Let G be a finite group and $\{C_i\}_i$ the set of conjugacy classes. Let X be a subset of G closed under conjugation of G: $X = \bigcup_{i \in \mathcal{I}'} C_i$. The eigenvalues of the Cayley graph $\Gamma(G, X)$ are $\Sigma_{i \in \mathcal{I}'} |C_i| \vartheta(c_i)/\vartheta(1)$, where c_i is a representative of the conjugacy class C_i and ϑ runs through irreducible characters of G.*

For example, the character table of the symmetric group 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

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

X be a subset of S_3 closed under conjugation. If X divides λS_3 then we can easily deduce that $X = \mathcal{U}$, $S_3 \backslash \mathcal{U}$ or S_3 by Lemma 1 and Lemma 2. In fact, the subset $\mathcal{U}$ and its complement $S_3 \backslash \mathcal{U}$ divide S_3 with code $Y = \{\text{id}, (1\ 2)\}$.

Note that X divides λG with code Y if and only if the complement $G \setminus X$ divides $(|Y| - \lambda)G$ with code Y.

Theorem 3 (An analogue to [RT]). *Let X be a subset (not necessarily closed under conjugation) of a finite group*

G and λ a natural integer. 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 $\mathbf{C}[G]$.*

Then X does not divide λG non-trivially.

Proof. Assume that X divides λG with code Y non-trivially; that is, $X \cdot Y = \lambda G$. 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, we have $P_H(\widehat{Y}) = P_H(\widehat{X})^{-1}\lambda P_H(\widehat{G}) = a\lambda P_H(\widehat{G})$ for some rational integer a. Then, by multiplying the last equation by $P_H(\widehat{X})$ from left, we have $a = |X|^{-1}$. Hence we have

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

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

Corollary 4. *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 integer λ is divisible by*

$$|X|/\gcd(|X|, |H|).$$

Note that 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.

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. In the following, assume that q is a power of 2 greater than 2. Let $\mathcal{I}$ and $\mathcal{J}$ be the index sets

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

The character table of $SL(2,q)$ is given in Table 2, where δ (resp. ε) is a primitive $(q-1)$st (resp. $(q+1)$st) root of unity in the complex number field $\mathbf{C}$.

Table 2: The irreducible characters of $SL(2, 2^f)$.

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

Using Table 2, we have the decomposition of the permutation character ${1_H}^{SL(2,q)}$ into irreducible characters as shown in Table 3 for each subgroup H of $SL(2,q)$, since ${1_H}^{SL(2,q)} = |H|^{-1} \Sigma_\vartheta \left(\Sigma_{x\in H}\, \vartheta(x)\right) \vartheta$ (the first summation runs over all irreducible characters ϑ of $SL(2,q)$) by the Frobenius reciprocity.

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

H $\lvert H\rvert$	The decomposition
I 1	$\chi_0 + q\chi_1 + (q+1)\sum_m \psi_m + (q-1)\sum_n \varphi_n$
S $q+1$	$\chi_0 + \sum_m \psi_m + \sum_n \varphi_n$
$N_G(S)$ $2(q+1)$	$\chi_0 + \sum_m \psi_m$
T $q-1$	$\chi_0 + 2\chi_1 + \sum_m \psi_m + \sum_n \varphi_n$
$N_G(T)$ $2(q-1)$	$\chi_0 + \chi_1 + \sum_m \psi_m$
U q	$\chi_0 + \chi_1 + 2\sum_m \psi_m$
B $q(q-1)$	$\chi_0 + \chi_1$

where S is a Singer cycle of G, T the subgroup of diagonal matrices, U the standard unipotent radical, $B = N_G(U)$ the standard Borel subgroup, and the summations run over $m \in \mathcal{I}$ and $n \in \mathcal{J}$.

2 The results

We first assume that the subset X is CLOSED under conjugation. Then, for an irreducible representation R of a finite group G, the matrix $R(\widehat{X})$ is a scalar by Schur's lemma and so the condition (2) of Theorem 3 can be checked easily.

Theorem 5. *Assume that X is a non-trivial subset closed under conjugation of $SL(2,q)$ $(q = 2^f \geq 4)$ and divides $\lambda SL(2,q)$. Then X is one of the following with λ divisible by λ' in the table. In the case where $\psi_m(\widehat{X}) \neq 0$ for some $m \in \mathcal{I}$, we have better evaluations for λ' as in the raund brackets (( )).*

Subset X	λ'
$\mathcal{U}$	$\}\,\lvert X\rvert/(q+1)$
$SL(2,q)\setminus\mathcal{U}$	
$(\cup_{i\in\mathcal{I}_0}\mathcal{T}_i)\cup(\cup_{j\in\mathcal{J}'}\mathcal{S}_j)$	$\}\ \lvert X\rvert/(p_0q)$
$SL(2,q)\setminus(\cup_{i\in\mathcal{I}_0}\mathcal{T}_i)\cup(\cup_{j\in\mathcal{J}'}\mathcal{S}_j)$	
$(\cup_{i\in\mathcal{I}'}\mathcal{T}_i)\cup(\cup_{j\in\mathcal{J}_0}\mathcal{S}_j)$	$\}\ \lvert X\rvert/(p'q)$ (($\lvert X\rvert/2$)),
$SL(2,q)\setminus(\cup_{i\in\mathcal{I}'}\mathcal{T}_i)\cup(\cup_{j\in\mathcal{J}_0}\mathcal{S}_j)$	

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

$$\sum_{i\in\mathcal{I}_0}\left(\delta_0^{mi}+\delta_0^{-mi}\right)=0 \quad \left(resp.\ \sum_{j\in\mathcal{J}_0}\left({\varepsilon_0}^{nj}+{\varepsilon_0}^{-nj}\right)=0\right)$$

for some $m \in \mathcal{I}$ and $n \in \mathcal{J}$, $\mathcal{I}'$ (resp. $\mathcal{J}'$) is a subset (possibly empty) of $\mathcal{I}$ (resp. $\mathcal{J}$),

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

Proof. We shall first list up subsets X for which the Cayley graph $\Gamma(SL(2,q), X)$ have eigenvalue 0, and then consider conditions on λ 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 we have

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

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

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

To determine 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 $|\mathcal{U}|/|S| = |\mathcal{U}|/(q+1)$ by Corollary 4.

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

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

To determine the integer λ for this subset X, let us set $H = B$. Then the matrix $P_B(\widehat{X})$ is non-singular by Table 3, Table 2 and by the argument for the case where $\chi_1(\widehat{X}) = 0$. If X divides $\lambda SL(2,q)$, then λ is divisible by $|X|/\gcd(|X|,|B|) = |X|/(qp_0)$ since $|X| = q\left((q+1)|\mathcal{I}_0| + (q-1)|\mathcal{J}'|\right)$ and $|B| = q(q-1)$. Hence we have the third row of the list.

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

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

by an argument similar to the previous case. Suppose that $\psi_m(\widehat{X}) = 0$ for some $m \in \mathcal{I}$. Then we get the condition on λ by an argument as before. If $\psi_m(\widehat{X}) \neq 0$ for any m, let us set $H = N_{SL(2,q)}(S)$ and $H = N_{SL(2,q)}(T)$ in turn. Then the matrix $P_H(\widehat{X})$ is non-singular for each H by Table 3 and Table 2. Assume that X divides $\lambda SL(2,q)$. Set $r_0 := \gcd(|\mathcal{J}_0|, q+1)$ if $\mathcal{J}_0 \neq \emptyset$, or $q+1$ otherwise. Then the the integer λ is divisible by $|X|/\gcd(|X|, 2(q+1)) = |X|/(2r_0)$ and $|X|/\gcd(|X|, 2(q-1)) = |X|/(2p')$ as $|X| = q\left((q+1)|\mathcal{I}'| + (q-1)|\mathcal{J}_0|\right)$. In order to take the least common multiple of these two integers, we calculate the greatest common divisor of $2r_0$ and $2p'$. The integer 2 is, however, the greatest common divisor of the two integers since $\gcd(q-1, q+1) = \gcd(q-1, 2) = 1$. Therefore, the integer λ is divisible by $|X|/2$.

The case where X contains the identity, the detailed proof is left to the reader. The argument is similar to the above, or uses Lemma 6. □

Lemma 6. *Keeping the assumptions of Corollary 4, suppose that X is closed under conjugation. Then $\mu|H|$ is divisible by $|G| - |X|$, where $\mu = |Y| - \lambda$.*

Proof. Note that each irreducible component of $P_H(\widehat{G \setminus X})$ is a scalar by Schur's lemma. Since $\vartheta(\widehat{G \setminus X}) = -\vartheta(\widehat{X}) \neq 0$ for each non-trivial irreducible character ϑ appearing in the character of P_H, the matrix $P_H(\widehat{G \setminus X})$ is non-singular. Thus this lemma follows from Theorem 3. □

Problem. For each X in the table of Theorem 5, determine whether X divides $\lambda SL(2, q)$ or not.

The list in Theorem 5 settles the perfect e-code problem in $SL(2, q)$ with $\lambda = 1$ 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 is $\mathcal{U}$ or $SL(2, 2) \setminus \mathcal{U}$. Moreover, for a Cayley graph $\Gamma = \Gamma(SL(2, q), X)$ on which $SL(2, q)$ acts by conjugation, there exists a perfect* *code in* Γ *if and only if* $q = 2$ *and* $X = SL(2,2)\backslash(\mathcal{U}\cup\{1\}) = \mathcal{S}$.

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

Let $q \geq 4$ and $\mathrm{GF}(q^2)$ 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. Note that η_j belongs to $\mathrm{GF}(q)$. For each $\alpha \in \mathrm{GF}(q)$ with $\alpha \neq 0$, take matrices

$$u_\alpha := \begin{bmatrix} 1 & \alpha \\ 0 & 1 \end{bmatrix}$$

and

$$s_1 := \begin{bmatrix} \eta_1 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} \rho & 1 \\ 1 & \rho \end{bmatrix} \begin{bmatrix} \rho & 0 \\ 0 & \rho^{-1} \end{bmatrix} \begin{bmatrix} \rho & 1 \\ 1 & \rho \end{bmatrix}^{-1}.$$

Lemma 8. *By definition of* η, *we have the following.*

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

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

where, for $\alpha \in \mathrm{GF}(q)$, $\alpha^{1/2}$ *is the element of* $\mathrm{GF}(q)$ *whose square equals* α.

(2) *If* $\eta_i = \eta_j$, *then we have* $i \equiv \pm j \bmod q+1$.

(3) *The order of* s_1 *is* $q+1$; *that is,* s_1 *is a generator of a Singer cycle.*

(4) *We have* $s_1{}^j = \eta_1^{-1} \begin{bmatrix} \eta_{j+1} & \eta_j \\ \eta_j & \eta_{j-1} \end{bmatrix}$.

(5) *The field* GF(q) *coincides with the set* $\{\eta_j^{-1}\eta_{j+1} \mid j = 1, 2, \ldots, q\}$, *since the generator* s_1 *of a Singer cycle acts on the projective line* $PG(1,q)$ *regularly.*

Theorem 9. *Let* X_α *be the orbit of the involution* u_α *by conjugation of* $\langle s_1 \rangle$:

$$X_\alpha := \{s_1{}^j u_\alpha s_1^{-j} \mid j = 0, 1, 2, \ldots, q\}.$$

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 the matrix $P(\widehat{X_\alpha})$ is non-singular, then X_α does not divide $\lambda SL(2,q)$ non-trivially by Theorem 3 with the subgroup H to be the standard Borel subgroup B of order $q(q-1)$. Therefore, it is sufficient to show that $P(\widehat{X_\alpha})$ is non-singular.

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

$$\mathbf{v}_0 = \left\{ \gamma \begin{bmatrix} 1 \\ 0 \end{bmatrix} \middle| \gamma \in \mathrm{GF}(q)^\times \right\}$$

and

$$\mathbf{v}_i = s_1^i \mathbf{v}_0 \text{ for } i = 1, 2, \ldots, q.$$

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 $s_1^k u_\alpha s_1^{-k} \mathbf{v}_j = \mathbf{v}_i$. Note that the matrix $P(\widehat{X_\alpha})$ is circulant: $P(\widehat{X_\alpha})_{i,j} = P(\widehat{X_\alpha})_{i-j,0}$ since $s_1 \widehat{X_\alpha} s_1^{-1} = \widehat{X_\alpha}$, where we understand the index modulo $q+1$.

For $k = 0, 1, 2, \ldots, q$, let j be the index such that

$$s_1^k u_\alpha s_1^{-k} \mathbf{v}_0 = \mathbf{v}_j.$$

We have $j = 0$ if and only if $k = 0$. Assume that $j \neq 0$. Then, denoting $\mathbf{v}_j$ by $\left\{ \gamma \begin{bmatrix} b_j \\ 1 \end{bmatrix} \middle| \gamma \in \mathrm{GF}(q)^\times \right\}$, we have

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

since $s_1^k u_\alpha s_1^{-k} = \eta_1^{-2} \begin{bmatrix} \eta_2 + \alpha \eta_{k+1} \eta_k & \alpha {\eta_{k+1}}^2 \\ \alpha {\eta_k}^2 & \eta_2 + \alpha \eta_{k+1} \eta_k \end{bmatrix}$. If the number of indices k satisfying the equation (1) is even for each $b_j \in \mathrm{GF}(q)$, then the matrix $P(\widehat{X_\alpha})$ has entries 1 on diagonal and even integers off diagonal. Hence the determinant of $P(\widehat{X_\alpha})$ is odd, in particular, $P(\widehat{X_\alpha})$ is non-singular.

Note that equation (1) is equivalent to (2) below

$$\alpha(b_j \eta_{2k} + \eta_{2k+1} + \eta_1) + \eta_2 = 0 \tag{2}$$

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

Now we would like to show that the number of k satisfying (2) is even for each $b_j \in \mathrm{GF}(q)$. Assume that k satisfies equation (2) and take the index i such that $b_j = \eta_i^{-1} \eta_{i+1}$ by Lemma 8. Then $b_j \eta_i + \eta_{i+1} = 0$ and $0 = (b_j \eta_i + \eta_{i+1}) \eta_{i-2k} = b_j(\eta_{2i-2k} + \eta_{2k}) + \eta_{2i-2k+1} + \eta_{2k+1}$. Thus

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

that is, $i-k \pmod{q+1}$ also satisfies equation (2). If $i-k \equiv k \mod q+1$, 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 $b_j = \eta_{2k}^{-1}\eta_{2k+1}$. This contradicts that $q \geq 4$ if $\alpha \neq \eta_1$. Therefore, we have the number of k satisfying equation (2) 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 $SL(2,q)/B$, where B is the standard Borel subgroup of $SL(2,q)$. Furthermore, Theorem 9 implies the theorem below by taking conjugation.

Theorem 10. *Let X be the orbit of an involution by conjugation of a Singer cycle. 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 $SL(2,q)$.*

3 In another groups

Finally, we note the known examples for X to divide the symmetric group S_n.

Theorem 11 ([RT]). *Let T_0 be the set of transpositions of S_n.*

(1) *If $1+n(n-1)/2$ is divisible by a prime exceeding $\sqrt{n}+2$, then $T := T_0 \cup \{\mathrm{id}\}$ does not divide S_n.*

(2) *If a prime exceeding* $\sqrt{n}+2$ *divides* $n(n-1)/2$, *then* T_0 *does not divide* S_n.

Remark ([RT]). The numbers $n = 1, 2, 3, 6, 91, 137, 733$ and 907 are the only integers less than $1,000$ which do not have any prime satisfying the assumption of Theorem 11 (1); that is, n is one of the above if T divides S_n $(n \leq 1000)$.

Note that the symmetric group S_3 is not divided by T since the sphere packing condition fails with $|T| = 4$ and $|S_3| = 6$. Moreover, we can prove that T does not divide S_6, using a combinatorial argument or the fact that the graph $\Gamma(S_6, T)$ does not have eigenvalue 0; that is, the graph $\Gamma(S_6, T_0)$ does not have eigenvalue -1.

Theorem 12 ([Ta]). *For a natural number* n, *let* X *be the union of three-cycles and the identity in the symmetric group* S_n *and let* $n_0 :=\max\{i \mid n \geq (3i-1)i\}$. *If a prime exceeding* $1 + n/n_0$ *divides* $1 + n(n-1)(n-2)/3$, *then the set* X *does not divide* S_n.

Remark ([Ta]). The numbers $n = 2, 3, 4, 14$ and $4,065$ are the only integers less than $40,000$ which do not have any prime satisfying the assumption of Theorem 12; that is, n is one of the above if X divides S_n $(n \leq 40000)$. For $n = 4$ and 14, however, X does not divide S_n by the sphere packing condition. For $n = 3$, X divides S_3 as in Theorem 7.

As shown in the examples above, we can easily conjecture that a subset X does not divide G except for the cases in Introduction. We would like to know an example that X divides G with code Y on condition that neither X nor Y is a subgroup of G.

References

[BI] E. Bannai and T. Ito, *Algebraic combinatorics* I: *Association schemes*, Benjamin-Cummings, California, 1984.

[Bi] N. Biggs, *Algebraic graph theory*, Cambridge University Press, 1974.

[It] N. Ito, The spectrum of a conjugacy class graph of a finite group, *Math. J. Okayama Univ.*, **26**(1984), 1–10

[RT] O. Rothaus and J. G. Thompson, A combinatorial problem in the symmetric group, *Pacific J. Math.*, **18**(1966), 175–178.

[Ta] T. Takematsu, A combinatorial problem in the symmetric group, in preparation.

[Te] S. Terada, Perfect codes in $SL(2, 2^f)$, preprint 2001, submitted.