Journal of Mathematical Research & Exposition
Feb., 2008, Vol. 28, No. 1, pp. 177–191
DOI:10.3770/j.issn:1000-341X.2008.01.023
Http://jmre.dlut.edu.cn

Conjugacy Classes of Torsion in 4×4 Integral Symplectic Group

YANG Qing-jie
(School of Information, Renmin University of China, Beijing 100872, China)
(E-mail: yangqj@ruc.edu.cn)

Abstract A complete list of representatives of conjugacy classes of torsion in 4×4 integral symplectic group is given in this paper. There are 55 distinct such classes and each torsion element has order of $2, 3, 4, 5, 6, 8, 10$ and 12.

Keywords integral symplectic group; torsion; symplectic group space; symplectic direct sum; quasi-direct sum; palindromic monic polynomial; symplectic complement.

Document code A
MR(2000) Subject Classification 53D30; 15A36
Chinese Library Classification O151.2

1. Introduction

The problem that we consider in this paper is the determination of the conjugacy classes of torsion matrices in the 4×4 integral symplectic group. Our original motivation for studying this problem came not from algebra but rather from Riemann surfaces[5].

Let $M_n(\mathbb{Z})$ be the set of $n \times n$ matrices over $\mathbb{Z}$. Let I_n be the identity matrix in $M_n(\mathbb{Z})$ and

$$J = \begin{pmatrix} 0 & I_n \\ -I_n & 0 \end{pmatrix}.$$

Definition 1 *The set of $2n \times 2n$ unimodular matrices X in $M_{2n}(\mathbb{Z})$ such that*

$$X'JX = J, \tag{1}$$

where X' is the transpose of X, is called the symplectic group of genus n over $\mathbb{Z}$ and is denoted by $SP_{2n}(\mathbb{Z})$. Two symplectic matrices X, Y of $SP_{2n}(\mathbb{Z})$ are said to be conjugate or similar, denoted by $X \sim Y$, if there is a matrix $Q \in SP_{2n}(\mathbb{Z})$ such that $Y = Q^{-1}XQ$.

A complete set of non-conjugate classes of torsion in $SP_4(\mathbb{Z})$ will be given in this paper.

Given a matrix $X \in M_{2n}(\mathbb{Z})$, we denote the characteristic polynomial of X by

$$f_X(x) = |xI - X|.$$

If $X \in SP_{2n}(\mathbb{Z})$, then $f_X(x)$ is "palindromic" and monic, that is,

$$x^{2n} f(\tfrac{1}{x}) = f(x) \quad \text{and} \quad f(0) = 1. \tag{2}$$

Received date: 2006-02-20; **Accepted date**: 2007-03-22
Foundation item: the Scientific Research Foundation for the Returned Overseas Chinese Scholars, State Education Ministry.

Definition 2 *A polynomial $f(x)$ in $\mathbb{Z}[x]$ of degree $2n$ ($n \geq 1$) is called an S-polynomial if it is a palindromic monic polynomial. An S-polynomial $f(x) \in \mathbb{Z}[x]$ is said to be irreducible over $\mathbb{Z}$, or is an irreducible S-polynomial in $\mathbb{Z}[x]$, if it cannot be expressed as the product of two S-polynomials (in $\mathbb{Z}[x]$) of positive degree. Otherwise, $f(x)$ is called reducible over $\mathbb{Z}$.*

It is known that every S-polynomial is a product of irreducible S-polynomials. Apart from the order of the factors, this factorization is unique.

We consider torsion elements of $SP_4(\mathbb{Z})$. The first question we consider is: for what positive integer d ($d \geq 2$), is there a matrix $X \in SP_{2n}(\mathbb{Z})$ having order d? If X has order d, then its minimal polynomial $m_X(x)$ is a factor of $x^d - 1$, i.e., $m_X(x)$ is a product of some different cyclotomic polynomials, and its characteristic polynomial $f_X(x)$ is a product of some cyclotomic polynomials. Suppose $d = p_1^{s_1} \cdots p_t^{s_t}$, where $p_1, p_2, \ldots, p_t$ are different primes. According to a result of D. Sjerve[4], the degree of $f_X(x)$ is not less than $\varphi(p_1^{s_1}) + \cdots + \varphi(p_t^{s_t}) - 1$, where φ is the Euler totient function, so

$$\varphi(p_1^{s_1}) + \cdots + \varphi(p_t^{s_t}) \leq 2n + 1.$$

We get

(i) If $n = 1$, then d must be 2, 3, 4, 6;

(ii) If $n = 2$, then d must be 2, 3, 4, 5, 6, 8, 10, 12.

We denote by T_d the set of d-torsion elements in $SP_4(\mathbb{Z})$. Let $X \in T_d$. The possible minimal polynomials $m_X(x)$ and characteristic polynomials $f_X(x)$ are as follows:

When $d = 2$,

$$m(x) = (x+1), \quad f(x) = (x+1)^4, \tag{3}$$

$$m(x) = (x-1)(x+1), \quad f(x) = (x-1)^2(x+1)^2. \tag{4}$$

When $d = 3$,

$$m(x) = (x^2+x+1), \quad f(x) = (x^2+x+1)^2, \tag{5}$$

$$m(x) = (x-1)(x^2+x+1), \quad f(x) = (x-1)^2(x^2+x+1). \tag{6}$$

When $d = 4$,

$$m(x) = (x^2+1), \quad f(x) = (x^2+1)^2, \tag{7}$$

$$m(x) = (x-1)(x^2+1), \quad f(x) = (x-1)^2(x^2+1), \tag{8}$$

$$m(x) = (x+1)(x^2+1), \quad f(x) = (x+1)^2(x^2+1). \tag{9}$$

When $d = 5$,

$$m(x) = f(x) = x^4 + x^3 + x^2 + x^1 + 1. \tag{10}$$

When $d = 6$,

$$m(x) = (x^2-x+1), \quad f(x) = (x^2-x+1)^2, \tag{11}$$

$$m(x) = (x-1)(x^2-x+1), \quad f(x) = (x-1)^2(x^2-x+1), \tag{12}$$

$$m(x) = (x+1)(x^2-x+1), \quad f(x) = (x+1)^2(x^2-x+1), \tag{13}$$

$$m(x) = (x+1)(x^2+x+1), \quad f(x) = (x+1)^2(x^2+x+1), \tag{14}$$

$$m(x) = (x^2 - x + 1)(x^2 + x + 1), \quad f(x) = (x^2 - x + 1)(x^2 + x + 1). \tag{15}$$

When $d = 8$,

$$m(x) = f(x) = x^4 + 1. \tag{16}$$

When $d = 10$,

$$m(x) = f(x) = x^4 - x^3 + x^2 - x + 1, \tag{17}$$

When $d = 12$,

$$m(x) = f(x) = (x^4 - x^2 + 1), \tag{18}$$

$$m(x) = f(x) = (x^2 + 1)(x^2 + x + 1), \tag{19}$$

$$m(x) = f(x) = (x^2 + 1)(x^2 - x + 1). \tag{20}$$

I. Reiner gave a list of the non-conjugate classes of involutions in all symplectic groups $SP_{2n}(\mathbb{Z})$[3]. From Reiner's result, there is only one conjugate class of characteristic polynomials (3) and two classes of (4).

The characteristic polynomials (10), (16)–(18) are irreducible over $\mathbb{Z}$. A complete set of conjugacy classes for these cases was given by Q. Yang[6].

The last two characteristic polynomials (19) and (20) are products of two strictly coprime S-polynomials. We have proved that there are four conjugacy classes for each of these cases in another paper.

In Section 2, we shall state our results for all other 10 cases. To prove our results we need to develop some new tools. In Section 3, we shall use symplectic complements to study the case where ± 1 is an eigenvalue of X, i.e., the cases of characteristic polynomials (6), (8)–(9) and (12)–(14). In Section 4, we discuss the case where the minimal polynomial of X is an irreducible quadratic, i.e. the cases of characteristic polynomials (5), (7) and (11). Then in Section 5, we consider the last remaining case of characteristic polynomial (15). We use the program Maple V to calculate most of our results in this paper.

2. Main results

To explain our results, we need to develop some notations. For $A \in M_{n_1}(\mathbb{Z})$, $B \in M_{n_2}(\mathbb{Z})$, we define the direct sum of A and B as

$$A \dot{+} B = \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix} \in M_{n_1+n_2}(\mathbb{Z}). \tag{21}$$

Obviously, when $n_1 = n_2 = n$, $A \dot{+} B \in SP_{2n_i}(\mathbb{Z})$ if and only if $A'B = I$ or $AB' = I$.

Given two matrices

$$X_1 = \begin{pmatrix} A_1 & B_1 \\ C_1 & D_1 \end{pmatrix} \in M_{2n_1}(\mathbb{Z}) \text{ and } X_2 = \begin{pmatrix} A_2 & B_2 \\ C_2 & D_2 \end{pmatrix} \in M_{2n_2}(\mathbb{Z}),$$

we define the symplectic direct sum of X_1 and X_2 by

$$X_1 * X_2 = \begin{pmatrix} A_1 & 0 & B_1 & 0 \\ 0 & A_2 & 0 & B_2 \\ C_1 & 0 & D_1 & 0 \\ 0 & C_2 & 0 & D_2 \end{pmatrix} \in M_{2(n_1+n_2)}(\mathbb{Z}). \tag{22}$$

It is easy to check that $X_1 * X_2 \in SP_{2(n_1+n_2)}(\mathbb{Z})$ if and only if $X_i \in SP_{2n_i}(\mathbb{Z})$, for $i = 1, 2$.

Given two matrices

$$Y_1 = \begin{pmatrix} C_{11} & C_{12} \\ C_{21} & C_{22} \end{pmatrix} \in M_{2n_1 \times 2n_2}(\mathbb{Z}) \quad \text{and} \quad Y_2 = \begin{pmatrix} D_{11} & D_{12} \\ D_{21} & D_{22} \end{pmatrix} \in M_{2n_2 \times 2n_1}(\mathbb{Z}),$$

where $C_{ij} \in M_{n_1 \times n_2}(\mathbb{Z})$, $D_{ij} \in M_{n_2 \times n_1}(\mathbb{Z})$, we define the quasi-direct sum by

$$Y_1 \circ Y_2 = \begin{pmatrix} 0 & C_{11} & 0 & C_{12} \\ D_{11} & 0 & D_{12} & 0 \\ 0 & C_{21} & 0 & C_{22} \\ D_{21} & 0 & D_{22} & 0 \end{pmatrix} \in M_{2(n_1+n_2)}(\mathbb{Z}). \tag{23}$$

By simple calculation, we see that if $n_1 = n_2 = n$, then $Y_1 \circ Y_2 \in SP_{4n}(\mathbb{Z})$ if and only if $Y_1, Y_2 \in SP_{2n}(\mathbb{Z})$.

Definition 3 *A matrix $X \in SP_{2n}(\mathbb{Z})$ is said to be decomposable if it is conjugate to a symplectic direct sum of two symplectic matrices which have smaller genera; otherwise, X is said to be indecomposable. When n is even, X is said to be quasi-decomposable if it is conjugate to $X_1 \circ X_2$ for some X_1, $X_2 \in SP_n(\mathbb{Z})$.*

Our results are given in following theorems. For the cases where 1 is an eigenvalue of X, we have

Theorem 1 *Suppose $X \in SP_4(\mathbb{Z})$ and $m_X(x) = (x-1)(x^2 + \lambda x + 1)$, where $\lambda = 0, \pm 1$. Then X is conjugate to one of two matrices*

$$I * W_\lambda, \qquad I * W'_\lambda,$$

where $W_\lambda = \begin{pmatrix} 0 & -1 \\ 1 & -\lambda \end{pmatrix}$. Moreover, these matrices are not conjugate.

Similarly, for the cases where -1 is an eigenvalue of X, we have

Theorem 2 *Suppose $X \in SP_4(\mathbb{Z})$ and $m_X(x) = (x+1)(x^2 + \lambda x + 1)$, where $\lambda = 0, \pm 1$. Then X is conjugate to one of two matrices*

$$(-I) * W_\lambda, \qquad (-I) * W'_\lambda$$

and these matrices are not conjugate.

Next for the cases when the minimal polynomial is an irreducible quadratic, we obtain

Theorem 3 *Suppose $X \in SP_4(\mathbb{Z})$ and $m_X(x) = x^2 + \lambda x + 1$, where $\lambda = 0, \pm 1$.*

1) If X is decomposable, then X is conjugate to one of

$$W_\lambda * W_\lambda, \qquad W'_\lambda * W'_\lambda, \qquad W_\lambda * W'_\lambda;$$

2) If X is indecomposable, then $\lambda = 0$ and X is conjugate to $(-I_2) \circ I_2$.

Moreover, these matrices are not conjugate.

For the last case characteristic polynomial (15) we have

Theorem 4 *Suppose $X \in SP_4(\mathbb{Z})$ and $m_x(x) = x^4 + x^2 + 1$.*

1) If X is decomposable, then X is conjugate to one of

$$W * (-W), \qquad W * (-W'), \qquad W' * (-W), \qquad W' * (-W');$$

2) If X is quasi-decomposable, then X is conjugate to one of

$$I_2 \circ W, \qquad I_2 \circ W';$$

3) If X is neither decomposable nor quasi-decomposable, then X is conjugate to one of

$$R, \qquad -R,$$

where

$$W = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}, \quad R = \begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}.$$

Moreover, these matrices are not conjugate.

It is clear that $W_1 = W$, $W_{-1} = -W'$ and $W_0 = J_2$. From above theorems and some results before, we obtain the main theorem.

Main Theorem *A complete list of representatives of the conjugacy classes of d-torsion in $SP_4(\mathbb{Z})$ is given as follows:*

$d = 2$

char. poly. (3): $-I_4$; (24)

char. poly. (4): $I_2 * (-I_2)$, $U \dotplus U'$; (25)

$d = 3$

char. poly. (5): $W * W$, $W' * W'$, $W * W'$; (26)

char. poly. (6): $I_2 * W$, $I_2 * W'$; (27)

$d = 4$

char. poly. (7): $J_2 * J_2$, $-(J_2 * J_2)$, $J_2 * (-J_2)$, $(-I_2) \circ I_2$; (28)

char. poly. (8): $I_2 * J_2$, $I_2 * (-J_2)$; (29)

char. poly. (9): $(-I_2) * J_2$, $-(I_2 * J_2)$; (30)

$d = 5$

char. poly. (10): S, S^2, S^3, S^4; (31)

$d = 6$

char. poly. (11): $-(W * W)$, $-(W' * W')$, $-(W * W')$; (32)

char. poly. (12): $I_2 * (-W),\quad I_2 * (-W');$ (33)

char. poly. (13): $-(I_2 * W),\quad -(I_2 * W');$ (34)

char. poly. (14): $(-I_2) * W,\quad (-I_2) * W';$ (35)

char. poly. (15): $W * (-W),\quad W * (-W'),\quad W' * (-W),\quad W' * (-W'),$
$I \circ W,\quad I \circ W',\quad R,\quad -R;$ (36)

$d = 8$

char. poly. (16): $I_2 \circ J_2,\quad I_2 \circ (-J_2),\quad T,\quad -T;$ (37)

$d = 10$

char. poly. (17): $-S,\quad -S^2,\quad -S^3,\quad -S^4;$ (38)

$d = 12$

char. poly. (18): $I_2 \circ (-W),\quad I_2 \circ (-W');$ (39)

char. poly. (19): $J_2 * W,\quad J_2 * W',\quad J_2' * W,\quad J_2' * W';$ (40)

char. poly. (20): $J_2 * (-W),\quad J_2 * (-W'),\quad J_2' * (-W);\quad J_2' * (-W'),$ (41)

where $U = \begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix}$, $S = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & -1 & 1 \\ 1 & 1 & -1 & 0 \end{pmatrix}$ *and* $T = \begin{pmatrix} 0 & -1 & 1 & 0 \\ -1 & 0 & 1 & 1 \\ -1 & 1 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix}$.

The rest of the paper is the proof of the above theorems. First we state some properties of symplectic direct sum and quasi-direct sum,

$$(X_1 * X_2)' = X_1' * X_2',$$
$$(Y_1 \circ Y_2)' = Y_2' \circ Y_1',$$
$$(X_1 * X_2)(Y_1 \circ Y_2) = (X_1Y_1) \circ (X_2Y_2),$$
$$(X_1 \circ X_2)(Y_1 * Y_2) = (X_1Y_2) \circ (X_2Y_1),$$
$$(X_1 * X_2)(Y_1 * Y_2) = (X_1Y_1) * (X_2Y_2),$$
$$(X_1 \circ X_2)(Y_1 \circ Y_2) = (X_1Y_2) * (X_2Y_1).$$

Here we assume that all matrix multiplications are suitable. The following three lemmas are useful.

Lemma 1 *Let X_1, X_2, X_3, Y_1, Y_2 be symplectic matrices. Then*

1) $X_1 * X_2 \sim X_2 * X_1$.

2) $(X_1 * X_2) * X_3 = X_1 * (X_2 * X_3)$.

3) If $X_1 \sim Y_1$ and $X_2 \sim Y_2$, then $X_1 * X_2 \sim Y_1 * Y_2$.

In what follows, we assume that X_1 and X_2 have the same genus

4) $X_1 \circ X_2 \sim X_2 \circ X_1$.

5) $X_1 \circ X_2 \sim (-X_1) \circ (-X_2)$.

6) $X_1 \circ X_2 \sim I \circ (X_1X_2)$.

7) If $X_1 \sim X_2$, then $I \circ X_1 \sim I \circ X_2$.

Proof 2) and 3) are easy. To prove 1), we let $Q = I_{2n_1} \circ I_{2n_2} \in SP_{2(n_1+n_2)}(\mathbb{Z})$, where n_i is

the genus of X_i, $i = 1, 2$. Then $Q^{-1}(X_1 * X_2)Q = X_2 * X_1$. Similarly we prove 4) by using $Q = I \circ I$, 5) by using $Q = I * (-I)$ and 6) by using $Q = I * X_1^{-1}$. For 7), if $X_2 = Q^{-1}X_1Q$, then $(Q^{-1} * Q^{-1})(I \circ X_1)(Q * Q) = I \circ X_2$. □

In general the converse of 3) in Lemma 1 is not true, but we have

Lemma 2 *Suppose X_1, X_2, Y_1 and Y_2 are symplectic matrices, $f_{X_i}(x) = f_{Y_i}(x) = f_i(x)$, for $i = 1, 2$. Suppose $f_1(x)$ and $f_2(x)$ are coprime. Then $X_1 * X_2 \sim Y_1 * Y_2$ if and only if $X_1 \sim Y_1$ and $X_2 \sim Y_2$.*

Proof The sufficiency part has been proved. We consider the necessity.

Note that any $P \in M_{2(n_1+n_2)}(\mathbb{Z})$ can be expressed in the form

$$P = P_1 * P_2 + P_3 \circ P_4,$$

where $P_1 \in M_{2n_1}(\mathbb{Z})$, $P_2 \in M_{2n_2}(\mathbb{Z})$, $P_3 \in M_{2n_1 \times 2n_2}(\mathbb{Z})$, and $P_4 \in M_{2n_2 \times 2n_1}(\mathbb{Z})$ are blocks of P. Let P be a symplectic matrix such that $(X_1 * X_2)P = P(Y_1 * Y_2)$. We obtain $X_1P_1 = P_1Y_1$, $X_2P_2 = P_2Y_2$, $X_1P_3 = P_3Y_2$ and $X_2P_4 = P_4Y_2$. Then $f_2(X_1)P_3 = P_3f_2(Y_1) = 0$, which yields $P_3 = 0$ since $f_2(X_1)$ is invertible. Similarly, we get $P_4 = 0$. Hence P_1, P_2 are symplectic, therefore $X_1 \sim Y_1$ and $X_2 \sim Y_2$. □

Lemma 3 *If $X \in SP_2(\mathbb{Z})$ has order 3 (resp. 4, 6). Then $f_X(x) = m_X(x) = x^2 + \lambda x + 1$, and $X \sim W_\lambda$ or W'_λ and $\lambda = 1$ (resp. $0, -1$).*

For a proof, see Ref. [6] or corollary of Lemma 6.

3. Symplectic complements

A primitive integral $2n \times (j + k)$ matrix

$$(A_{2n\times j} \quad B_{2n\times k}), \quad j, k \le n$$

which satisfies the conditions

$$A'JA = 0, \quad B'JB = 0, \quad \text{and} \quad A'JB = \begin{pmatrix} I_k \\ 0 \end{pmatrix} \text{ or } (I_j \quad 0)$$

(depending on whether $j \ge k$ or $j \le k$) will be called a normal (j, k)-array. According to Ref. [2] every normal (j, k)-array can be completed to a symplectic matrix by placing $n - j$ columns after the first j columns and $n - k$ columns after the last k columns.

Remark 1 Let $\alpha, \beta \in \mathbb{Z}^{2n}$. Clearly, α is $(1, 0)$-array if and only if α is a primitive vector, and (α, β) is a normal $(1, 1)$-array if and only if $\alpha'J\beta = 1$.

Lemma 4 *Suppose that $X \in SP_{2n}(\mathbb{Z})$ and $f_X(1) = 0$. Then*

$$X \sim \begin{pmatrix} 1 & \gamma' & a & \delta' \\ 0 & A & \alpha & B \\ 0 & 0 & 1 & 0 \\ 0 & C & \beta & D \end{pmatrix},$$

where $Y = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in SP_{2(n-1)}(\mathbb{Z})$, $f_X(x) = (x-1)^2 f_Y(x)$, $a \in \mathbb{Z}$, *and* α, β, γ, $\delta \in \mathbb{Z}^{n-1}$ *with*

$$\begin{cases} \alpha &= A\delta - B\gamma, \\ \beta &= C\delta - D\gamma, \\ \gamma &= C'\alpha - A'\beta, \\ \delta &= D'\alpha - B'\beta. \end{cases} \tag{42}$$

Furthermore, if $Y \sim Y_1 = \begin{pmatrix} A_1 & B_1 \\ C_1 & D_1 \end{pmatrix}$, *then*

$$X \sim \begin{pmatrix} 1 & \gamma_1' & a_1 & \delta_1' \\ 0 & A_1 & \alpha_1 & B_1 \\ 0 & 0 & 1 & 0 \\ 0 & C_1 & \beta_1 & D_1 \end{pmatrix}.$$

Proof Since the number 1 is an eigenvalue of X, there is a primitive vector $\eta \in \mathbb{Z}^{2n}$ such that $X\eta = \eta$. We can find an integral symplectic matrix P with η as its first column. Then

$$P^{-1}XP = X_1 = \begin{pmatrix} 1 & \gamma' & a & \delta' \\ 0 & A & \alpha & B \\ 0 & * & b & * \\ 0 & C & \beta & D \end{pmatrix} \in SP_{2n}(\mathbb{Z}).$$

By simple calculation we can see that the $*$'s are 0, $b = 1$, $Y = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in SP_{2(n-1)}(\mathbb{Z})$, and α, β, γ, δ satisfy (42). Thus $f_X(x) = (x-1)^2 g_Y(x)$.

The second part is easy, merely conjugate by $I * Q$, where $Q \in SP_2(\mathbb{Z})$ and $Q^{-1}YQ = Y_1$.

Now we can prove Theorems 1 and 2.

Proof of Theorem 1 It is clear that $I * W_\lambda \nsim I * W_\lambda'$ (cf. Lemma 2).

By Lemma 4, we get

$$X \sim X_1 = \begin{pmatrix} 1 & a_1 & b_1 & c_1 \\ 0 & A & d_1 & B \\ 0 & 0 & 1 & 0 \\ 0 & C & e_1 & D \end{pmatrix},$$

where $Y = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in SP_2(\mathbb{Z})$ with $f_Y(x) = x^2 + \lambda x + 1$. Then, from Lemma 3, we have $Y \sim W_\lambda$ or W_λ'. Without loss of the generality, we assume $Y \sim W_\lambda$. Then

$$X \sim X_2 = \begin{pmatrix} 1 & a_2 & b_2 & c_2 \\ 0 & 0 & a_2 & -1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & \lambda a_2 + c_2 & -\lambda \end{pmatrix} \sim X_3 = \begin{pmatrix} 1 & 0 & b & c \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & c & -\lambda \end{pmatrix},$$

where the last conjugacy is achieved by $Q=\begin{pmatrix}1&-a_2\\0&1\end{pmatrix}\dot{+}\begin{pmatrix}1&0\\a_2&1\end{pmatrix}\in SP_4(\mathbb{Z})$. We obtain $(\lambda+2)b+c^2=0$ since $m_{_X}(x)=(x-1)(x^2+\lambda x+1)$. This implies $(\lambda+2)\mid c$. Now we see that X_3 is decomposable and use Lemma 3 to complete the proof. In fact let

$$P=\begin{pmatrix}1&k&0&k\\0&-1&-k&0\\0&0&1&0\\0&0&k&-1\end{pmatrix}\in SP_4(\mathbb{Z}),$$

where $k=\frac{c}{\lambda+2}\in\mathbb{Z}$. It is easy to check that $P^{-1}X_3P=I*W_\lambda$. The proof is completed. □

Proof of Theorem 2 Since $m_{_{-X}}(x)=(x-1)(x^2-\lambda x+1)$, we have $-X\sim I*W_{-\lambda}$ or $I*W'_{-\lambda}$. Note that $-W_\lambda=W'_\lambda$. Hence $X\sim(-I)*W'_\lambda$ or $(-I)*W_\lambda$. The proof is completed. □

4. Minimal representatives

Let $X\in SP_{2n}(\mathbb{Z})$ and $\eta=(x_1,x_2,\ldots,x_{2n})'\in\mathbb{Z}^{2n}$. If $a=\eta'JX\eta$, then we say that X represents a. The set of values represented by X will be denoted by $q(X)$. It is clear that $q(X)$ is a conjugacy invariant, for if $Y=Q^{-1}XQ$, where $Q\in SP_{2n}(\mathbb{Z})$, then

$$q(Y)=q(Q^{-1}XQ)=\left\{\eta'JQ^{-1}XQ\eta\mid\eta\in\mathbb{Z}^{2n}\right\},$$

and so putting $\xi=Q\eta$ gives

$$\xi'JX\xi=\eta'Q'JXQ\eta=\eta'JQ^{-1}XQ\eta=\eta'JY\eta.$$

Thus $q(Y)=q(X)$. Unfortunately, the converse is not necessarily true.

The set $q(X)$ is a set of integers, and consequently there is a non-zero η_0 in $\mathbb{Z}^{2n}$ such that $|\eta_0'JX\eta_0|$ is least. If both $\eta_0'JX\eta_0$ and $-\eta_0'JX\eta_0=\eta_1'JX\eta_1$ occur, we resolve the ambiguity by choosing the non-negative value. We write $\mu(X)=\eta_0'JX\eta_0$. Clearly, if $\mu(X)\neq 0$, the minimizing vector x_0 must be primitive, and if $\mu(X)=0$, we can also choose a primitive vector η_0 such that $\eta_0'JX\eta_0=0$.

Example If X is quasi-decomposable, then $\mu(X)=0$.

Lemma 5 *Let $f(x)=f_{_X}(x)$ be the characteristic polynomial of X. Then*

$$|\mu(X)|\le(\frac{4}{3})^{n-\frac{1}{2}}\frac{|f(1)f(-1)|^{\frac{1}{2n}}}{2}.\tag{43}$$

Proof Note that $\eta'JX\eta$ is a quadratic form over $\mathbb{Z}$. If M is a symmetric matrix belonging to $M_n(\mathbb{Z})$, and $a=\min\{|\eta'M\eta|\mid\eta\in\mathbb{Z}^n,\eta\neq 0\}$, then

$$a\le(\frac{4}{3})^{\frac{n-1}{2}}|\det M|^{\frac{1}{n}},$$

see Ref. [1]. Clearly, it is also true if M is a rational symmetric matrix.

We know that $\eta'JX\eta=\frac{1}{2}\eta'(JX+(JX)')\eta$, where $\frac{1}{2}(JX+(JX)')$ is a rational symmetric matrix. Because $(JX)'=X'J'=-X'J=-JX^{-1}$, and $|J|=|X|=1$, we see that

$|JX+(JX)'|=|JX-JX^{-1}|=|J||X^{-1}||X^2-I|=f(1)f(-1)$. Hence

$$|\mu(X)|\le(\frac{4}{3})^{n-\frac{1}{2}}\frac{|f(1)f(-1)|^{\frac{1}{2n}}}{2}.$$

Remark 2 Note that if $X\in SP_4(\mathbb{Z})$ is a torsion element, then $|\mu(X)|\le 1$ since $|\mu(X)|$ is integer and the maximum of $|f(1)f(-1)|$ is 16.

Lemma 6 *Suppose $X\in SP_{2n}(\mathbb{Z})$, and $1\in q(X)$. Then*

$$X\sim\begin{pmatrix}0&0&-1&0\\0&A&\alpha&B\\1&\gamma'&a&\delta'\\0&C&\beta&D\end{pmatrix},$$

where $\begin{pmatrix}A&B\\C&D\end{pmatrix}\in SP_{2(n-1)}(\mathbb{Z})$, $a\in\mathbb{Z}$, and $\alpha,\beta,\gamma,\delta\in\mathbb{Z}^{n-1}$ satisfy Eq.(42).

Proof Since there is a primitive vector $\eta\in\mathbb{Z}^{2n}$ such that $\eta'JX\eta=1$, we see that $(\eta,X\eta)$ is a normal $(1,1)$-array. Let P be the completion of the normal $(1,1)$-array $(\eta,X\eta)$ to a symplectic matrix. Then

$$P=\begin{pmatrix}\vdots&*&\vdots&*\\\eta&*&X\eta&*\\\vdots&*&\vdots&*\end{pmatrix}$$

and therefore

$$P^{-1}XP=X_1=\begin{pmatrix}0&*&b&*\\0&A&\alpha&B\\1&\gamma'&a&\delta'\\0&C&\beta&D\end{pmatrix}\in SP_{2n}(\mathbb{Z}).$$

The remainder of the proof is similar to that of Lemma 4. □

Corollary 1 *Suppose $X\in SP_{2n}(\mathbb{Z})$ and $m_{_X}(x)=x^2+\lambda x+1$ with $1\in q(X)$. Then $X\sim W_\lambda * Y$, where $Y\in SP_{2(n-1)}(\mathbb{Z})$ with $m_{_Y}(x)=m_{_X}(x)$.*

Proof Since $X^2\eta=-\lambda X\eta-\eta$, we see that the entries of the matrix in Lemma 6 are: $a=-\lambda$, $\alpha=0$, $\beta=0$, and so $\gamma=0$, $\delta=0$. □

Lemma 7 *Suppose $X\in SP_{2n}(\mathbb{Z})$, and $\mu(X)=0$. Then*

$$X\sim\begin{pmatrix}0&A&\alpha&B\\1&\gamma'&a&\delta\\0&C&\beta&D\\0&0&1&0\end{pmatrix},$$

where $\begin{pmatrix}A&B\\C&D\end{pmatrix}\in SP_{2(n-1)}(\mathbb{Z})$, $a\in\mathbb{Z}$, and $\alpha,\beta,\gamma,\delta\in\mathbb{Z}^{n-1}$ satisfy Eq.(42).

Proof Note that we have a normal $(2,0)$-array $(\eta, X\eta)$, where $\eta \in \mathbb{Z}^{2n}$ is primitive. □

Proof of Theorem 3 Note that $|\mu(X)| \leq 1$. We consider following four cases:

Case 1. If $\mu(X) = 1$, then by Corollary 1, $X \sim W_\lambda * Y$, for some $Y \in SP_2(\mathbb{Z})$, with $m_{_Y}(x) = x^2+\lambda x+1$. From Lemma 3, $Y \sim W_\lambda$ or W'_λ. Then $X \sim W_\lambda * W_\lambda$ or $W_\lambda * W'_\lambda$. But $\mu(W_\lambda * W'_\lambda) = 0$, hence $X \sim W_\lambda * W_\lambda$.

Case 2. If $\mu(X) = -1$, then $\mu(-X) = 1$. It is clear that $m_{_{-X}}(x) = x^2 - \lambda x + 1$, hence $-X \sim W_{-\lambda} * W_{-\lambda}$, and thus $X \sim -(W_{-\lambda} * W_{-\lambda}) = W'_\lambda * W'_\lambda$.

Case 3. If $\mu(X) = 0$ and $1 \in q(X)$, we also have that $X \sim W_\lambda * W_\lambda$ or $W_\lambda * W'_\lambda$ by Corollary 1 and Lemma 3. But $\mu(W_\lambda * W_\lambda) = 1$, hence $X \sim W_\lambda * W'_\lambda$.

Case 4. Now we assume that $\mu(X) = 0$ and $1 \notin q(X)$. By Lemma 7, we get

$$X \sim X_1 = \begin{pmatrix} W_\lambda & Y \\ 0 & W'^{-1}_\lambda \end{pmatrix},$$

where $Y = \begin{pmatrix} a & b \\ b & \lambda b - a \end{pmatrix}$, $a, b \in \mathbb{Z}$.

Let $P = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & b \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$, $Q = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \in SP_4(\mathbb{Z})$ and $X(a) = \begin{pmatrix} 0 & -1 & a & 0 \\ 1 & -\lambda & 0 & -a \\ 0 & 0 & -\lambda & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$.

It is easy to verify that

$$P^{-1}X_1P = X(a) \quad \text{and} \quad Q^{-1}X(a)Q = X(a-2).$$

So we obtain $X \sim X(0)$ or $X(1)$.

It is clear that $1 \in q(X(0))$ if and only if λ is odd, and always $1 \in q(X(1))$. Thus $\lambda = 0$ in the case $1 \notin q(X)$. We get $X \sim X(0) = (-I_2) \circ I_2$, which is indecomposable.

The proof is completed. □

5. The Case of $f(x) = x^4 + x^2 + 1$

In this section we discuss the last case that $X \in SP_4(\mathbb{Z})$ has characteristic polynomial (15), that means $f_{_X}(x) = x^4+x^2+1$ and prove Theorem 4. The first two parts are very easy to verify.

Proof of the first two parts of Theorem 4 If X is decomposable, then X is conjugate to $Y*Z$, where $Y, Z \in SP_2(\mathbb{Z})$ with characteristic polynomials $f_Y(x) = x^2+x+1$ and $f_Z(x) = x^2-x-1$. From Lemma 3, $Y \sim W$ or W', $Z \sim -W$ or $-W'$. Hence X is conjugate to one of four matrices, $W*(-W)$, $W*(-W')$, $W'*(-W)$ and $W'*(-W')$. Clearly, they are not conjugate to each other, see Lemma 2.

If X is quasi-decomposable, then by (6) in Lemma 1, $X \sim I \circ Y$, where $Y \in SP_2(\mathbb{Z})$. Since X has order 6, $(I \circ Y)^2 = Y * Y \neq I$ and $(I \circ Y)^6 = (Y * Y)^3 = Y^3 * Y^3 = I$. Thus $Y \neq I$,

$Y^3 = I$, and then $Y \sim W$ or W'. So according to part 7 in Lemma 1, we have that $X \sim I \circ W$ or $I \circ W'$. Obviously, these two matrices are not conjugate. □

To prove the third part of Theorem 4, we suppose that X is neither decomposable nor quasi-decomposable. Note that $m_{X^2}(x) = x^2 + x + 1$, according to Theorem 3, X^2 is conjugate to one of three non-conjugate matrices

$$W * W, \qquad W^2 * W^2, \qquad W * W^2.$$

Without loss of generality we assume that $X^2 = X_1 * X_2$, where X_1 and X_2 are either W or W^2. We can express X as

$$X = P_1 * P_2 + P_3 \circ P_4, \tag{44}$$

where the P_i's are 2×2 matrices. Then

$$X^3 = X(X_1 * X_2) = P_1X_1 * P_2X_2 + P_3X_2 \circ P_4X_1,$$
$$X^3 = (X_1 * X_2)X = X_1P_1 * X_2P_2 + X_1P_3 \circ X_2P_4.$$

Note that X has order 6, we have $(JX^3)' = X'^3J' = -JX^{-3} = -JX^3$. Therefore,

$$P_1 = aX_1^2, \quad P_2 = -aX_2^2, \quad P_3P_4 = (1-a^2)X_1, \quad P_4P_3 = (1-a^2)X_2, \tag{45}$$

and $\det P_3 = \det P_4 = 1 - a^2$ for some $a \in \mathbb{Z}$. Also, since $X \in SP_4(\mathbb{Z})$, we have

$$\begin{cases} P_1'JP_1 + P_4'JP_4 = J, \\ P_2'JP_2 + P_3'JP_3 = J, \\ P_1'JP_3 + P_4'JP_2 = 0, \end{cases} \quad \text{and} \quad \begin{cases} P_1JP_1' + P_3JP_3' = J, \\ P_2JP_2' + P_4JP_4' = J, \\ P_1JP_4' + P_3JP_2' = 0. \end{cases} \tag{46}$$

We state the following lemmas without proof. They are very easy to verify.

Lemma 8 *Let $P \in M_2(\mathbb{Z})$. We have*

1) *If $PW = WP$, then $P = bI + cW$, for some constants b and c;*
2) *If $PW + WP = 0$, then $P = 0$;*
3) *If $PW = W^2P$, then $P = \begin{pmatrix} b & c \\ b+c & -b \end{pmatrix}$.*

Clearly, if $P = bI + cW$, then $\det(P) = b^2 - bc + c^2$.

If $X^2 = W^l * W^l$, from Eq.(45), we see that $P_3 = bI + cW$, where $b^2 - bc + c^2 = 1 - a^2$, and hence $a = -1, 0, 1$. In this case, when $a = \pm 1$, $b = c = 0$, thus X is decomposable, and when $a = 0$, $P_1 = P_2 = 0$, we have that $X = P_3 \circ P_4$ is quasi-decomposable.

So we only need consider the case that $X^2 = W * W^2$.

Lemma 9 *Suppose that $X^2 = W * W^2$. Then $X \sim X(a, b, c)$, where*

$$X(a,b,c) = \begin{pmatrix} a & b & -a & c \\ -c & 0 & b+c & -a \\ a & b+c & 0 & -b \\ b & a & c & -a \end{pmatrix} \tag{47}$$

for integers a, b, c satisfying $a^2 - 1 = b^2 + bc + c^2$.

Proof From Eq.(45), we see that $X = (-aW^2) * (aW) + P_3P_4$, where $P_3P_4 = (1-a^2)W$ and $P_3W = W^2P_3$. Applying Lemma 8, we get

$$P_3 = \begin{pmatrix} b & c \\ b+c & -b \end{pmatrix} \quad \text{and} \quad P_4 = \begin{pmatrix} -c & b+c \\ b & c \end{pmatrix}.$$

It is clear that $\det P_3 = -(b^2+bc+c^2) = 1-a^2$. □

Remark 3 For any integral solution of $a^2 - 1 = b^2 + bc + c^2$, $X(a,b,c) \in SP_4(\mathbb{Z})$, and its characteristic polynomial is (15). Clearly, $a \neq 0$.

Remark 4 A simple calculation proves that $X^5(a,b,c) \sim X(-a,b,c)$.

Lemma 10 *$X(a,b,c)$ is decomposable if and only if a is odd.*

Proof It is easy to check that $\frac{1}{2}(X^3 - I) \in M_4(\mathbb{Z})$ if and only if a is odd. We have proved that if $X(a,b,c)$ is decomposable if and only if $\frac{1}{2}(X^3 - I) \in M_4(\mathbb{Z})$. □

Lemma 11 *$\mu(X(a,b,c))$ has the same sign as the non-zero number a.*

Proof Let $M = JX(a,b,c) + (JX(a,b,c))'$. We want to prove that M is positive definite if $a > 0$, and M is negative definite if $a < 0$. We see

$$M = \begin{pmatrix} 2a & 2b+c & -a & -b+c \\ 2b+c & 2a & -b+c & -a \\ -a & -b+c & 2a & -b-2c \\ -b+c & -a & -b-2c & 2a \end{pmatrix}.$$

Its principal minors are:

$$M_1 = 2a,$$

$$M_2 = \det \begin{pmatrix} 2a & 2b+c \\ 2b+c & 2a \end{pmatrix} = 4a^2 - 4b^2 - 4bc - c^2 = 4 + 3c^2 > 0,$$

$$M_3 = \det \begin{pmatrix} 2a & 2b+c & -a \\ 2b+c & 2a & -b+c \\ -a & -b+c & 2a \end{pmatrix} = 6(a^3 - ab^2 - abc - ac^2) = 6a,$$

$$M_4 = \det A = 9.$$

Hence M is positive or negative definite dependent according as $a > 0$ or $a < 0$. □

Corollary 2 *$X(a,b,c)$ is quasi-indecomposable.*

Corollary 3 *$X(a_1,b_1,c_1) \not\sim X(a_2,b_2,c_2)$ if $a_1a_2 < 0$.*

If a is even, then $X(a,b,c)$ is also indecomposable. It is known that the Diophantine equation $a^2 - 1 = b^2 + bc + c^2$ has infinitely many solutions with a even. There are infinitely many $X \in SP_4(\mathbb{Z})$, which are neither quasi-decomposable nor decomposable, of the form $X(a,b,c)$.

In the following, we want to show that there are just two classes amongst $X(a,b,c)$, where a is even. For this purpose, we let

$$R(x,y,z)=\begin{pmatrix} 2x & 0 & -y & x \\ 0 & -2x & -x & -z \\ z & x & -x & z \\ -x & y & y & x \end{pmatrix},$$

where

$$\begin{cases} x=a-b-c, \\ y=2a-2b-c, \\ z=2a-b-2c, \end{cases} \quad \text{or} \quad \begin{cases} a=-3x+y+z, \\ b=-2x+z, \\ c=-2x+y. \end{cases}$$

Then $R(x,y,z)=QX(a,b,c)Q^{-1}$, where

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

It is easy to see that $a^2-1=b^2+bc+c^2$ if and only if $yz=3x^2+1$, and a is even if and only if $x+y+z$ is even, and also $a>0$ if and only if $y>0$. Furthermore, we have

Lemma 12 *Let x, y, z be integers satisfying that $yz=3x^2+1$ and $x+y+z$ is even. Then*

1) If $y>0$, then $R(x,y,z)\sim R(0,1,1)$;

2) If $y<0$, then $R(x,y,z)\sim R(0,-1,-1)$.

Proof Suppose $yz=3x^2+1$, and $x+y+z$ is even. If y is even, then $y=4k$, where k is odd. The reason for this is that x is odd, and then z is odd and $3x^2+1=4l$ where l is odd. If p is an odd prime and $y\equiv 0 \pmod p$, then $p\equiv 1 \pmod 3$. This is because $p\neq 3$, and $3x^2+1\equiv 0 \pmod p$. Thus we see that y has the form

$$y=\pm 4^r p_1^{r_1}\cdots p_t^{r_t},$$

where $r=0,1$, $r_i\geq 0$, and the p_i are primes of the form $3k+1$.

Now suppose $y>0$. First we want to prove there is a solution (u,v) of the Diophantine equation $y=3u^2+v^2$ satisfying $u+xv\equiv 0 \pmod y$.

If $y=1$ then $(0,1)$ is a such solution.

If $y=4$, then $x\equiv\pm 1 \pmod 4$. A solution is $(1,\mp 1)$.

If y is an odd prime and $y\equiv 1 \pmod 3$, then it is well known that there are $a,b\in\mathbb{Z}$ such that $3a^2+b^2=y$, which implies $(a-xb)(a+xb)=a^2-x^2b^2=a^2(3x^2+1)-yx^2\equiv 0 \pmod y$. Hence either $a-xb\equiv 0 \pmod y$ or $a+xb\equiv 0 \pmod y$. So either $(a,-b)$ or (a,b) is a such solution.

In general, we use induction on the factors of y. Suppose $y=y_1y_2$, and (u_i,v_i) are solutions

for y_i (for $i = 1, 2$), that is, $y_i = 3u_i^2 + v_i^2$ and $u_i + xv_i \equiv 0 \pmod{y_i}$. Let

$$\begin{cases} u = u_1v_2 + u_2v_1, \\ v = v_1v_2 - 3u_1u_2. \end{cases}$$

Then $3u^2 + v^2 = y$ and

$$\begin{aligned} (u + xv)x &= (u_1v_2 + u_2v_1)x + (v_1v_2 - 3u_1u_2)x^2 \\ &\equiv xv_2(u_1 + xv_1) + u_2v_1x + u_1u_2 \pmod{y} \\ &= (u_1 + xv_1)(u_2 + xv_2) \equiv 0 \pmod{y}. \end{aligned}$$

So $u + xv \equiv 0 \pmod{y}$ since $(x, y) = 1$. Therefore (u, v) is a solution for y.

Now we can complete the proof. Suppose $y = 3u^2 + v^2$ and $u + vx \equiv 0 \pmod{y}$. Then $v - 3xu \equiv v + 3x^2v = (3x^2 + 1)v \equiv 0 \pmod{y}$. Let

$$P = \begin{pmatrix} v & u & -u & v \\ \frac{u+xv}{y} & \frac{v-3xu}{y} & \frac{v-3xu}{y} & -\frac{u+xv}{y} \\ \frac{u+xv}{y} & \frac{3xu-v}{y} & 0 & \frac{2(u+xv)}{y} \\ -v & u & 2u & 0 \end{pmatrix}.$$

Then $P \in SP_4(\mathbb{Z})$ and $PR(0, 1, 1)P^{-1} = R(x, y, z)$. That is, $R(0, 1, 1) \sim R(x, y, z)$.

The second part is similar. □

Remark 5 The u, v in the proof are coprime. We see that there is a primitive solution of the Diophantine equation $3u^2 + v^2 = m$ if m is a product of a power of 4 and odd primes of form $6k + 1$.

We have completed the proof of the third part of Theorem 4.

References

[1] NEWMAN M. *Integral Matrices* [M]. Academic Press, New York, 1972.
[2] REINER I. *Symplectic modular complements* [J]. Trans. Amer. Math. Soc., 1954, **77**: 498–505.
[3] REINER I. *Automorphisms of the symplectic modular group* [J]. Trans. Amer. Math. Soc., 1955, **80**: 35–50.
[4] SJERVE D. *Canonical forms for torsion matrices* [J]. J. Pure Appl. Algebra, 1981, **22**(1): 103–111.
[5] SJERVE D, YANG Qing-jie. *Conjugacy classes of p-torsion in $Sp_{p-1}(\mathbf{Z})$* [J]. J. Algebra, 1997, **195**(2): 580–603.
[6] YANG Qing-jie. *Conjugacy classes in integral symplectic groups* [J]. Linear Algebra Appl., 2006, **418**(2-3): 614–624.