ISSN 1472-2739 (on-line) 1472-2747 (printed)

*Algebraic & Geometric Topology*
Volume 2 (2002) 791–824
Published: 3 October 2002

# On diffeomorphisms over surfaces trivially embedded in the 4-sphere

Susumu Hirose

**Abstract** A surface in the 4-sphere is *trivially* embedded, if it bounds a 3-dimensional handle body in the 4-sphere. For a surface trivially embedded in the 4-sphere, a diffeomorphism over this surface is extensible if and only if this preserves the Rokhlin quadratic form of this embedded surface.

**AMS Classification** 57N10; 57N05, 20F38

**Keywords** Knotted surface, mapping class group, spin mapping class group

*This paper is dedicated to Professor Mitsuyoshi Kato on his 60th birthday.*

## 1 Introduction

We denote the closed oriented surface of genus $g$ by $\Sigma_g$, the mapping class group of $\Sigma_g$ by $\mathcal{M}_g$. Let $\phi\colon\ \Sigma_g \to S^4$ be an embedding, and $K$ be its image. We call $(S^4, K)$ a $\Sigma_g$*-knot* . Two $\Sigma_g$-knots $(S^4, K)$ and $(S^4, K')$ are *equivalent* if there is a diffeomorphism of $S^4$ which brings $K$ to $K'$. *A 3-dimensional handlebody* $H_g$ is an oriented 3-manifold which is constructed from a 3-ball with attaching $g$ 1-handles. Any embeddings of $H_g$ into $S^4$ are isotopic each other. Therefore, $(S^4, \partial H_g)$ is unique up to equivalence. We call this $\Sigma_g$-knot $(S^4, \partial H_g)$ *a trivial* $\Sigma_g$*-knot* and denote this by $(S^4, \Sigma_g)$. For a $\Sigma_g$-knot $(S^4, K)$, we define the following group,

$$\mathcal{E}(S^4, K) = \left\{ \phi \in \pi_0 \mathrm{Diff}^+(K) \,\middle|\, \begin{array}{l} \text{there is an element } \Phi \in \mathrm{Diff}^+(S^4) \\ \text{such that } \Phi|_K \text{ represents } \phi \end{array} \right\},$$

and define a quadratic form (*the Rokhlin quadratic form*) $q_K\colon\ H_1(K;\mathbb{Z}_2) \to \mathbb{Z}_2$: Let $P$ be a compact surface embedded in $S^4$, with its boundary contained in $K$, normal to $K$ along its boundary, and its interior is transverse to $K$. Let $P'$ be a surface transverse to $P$ obtained by sliding $P$ parallel to itself over $K$. Define $q_K([\partial P]) = \#(\mathrm{int}P \cap (P' \cup K))$ mod 2, where int means the interior. This is a well-defined quadratic form with respect to the $\mathbb{Z}_2$-homology intersection form $(\,,)_2$ on $K$, i.e. for each pair of elements $x$, $y$ of $H_1(K;\mathbb{Z}_2)$, $q_K(x+y) = q_K(x) + q_K(y) + (x,y)_2$. For the trivial $\Sigma_g$-knot $(S^4, \Sigma_g)$, let $\mathcal{SP}_g$ be the subgroup of $\mathcal{M}_g$ whose elements leave $q_{\Sigma_g}$ invariant. This group $\mathcal{SP}_g$ is called the *spin mapping class group* [3]. In the case when $g = 1$, Montesinos showed:

**Theorem 1.1** [10] $\mathcal{E}(S^4, \Sigma_1) = \mathcal{SP}_1$.

In this paper, we generalize this result to higher genus:

**Theorem 1.2** *For any $g \geq 1$, $\mathcal{E}(S^4, \Sigma_g) = \mathcal{SP}_g$.*

The group $\mathcal{E}(S^4, K)$ remains unknown for many non-trivial $\Sigma_g$-knots $K$. On the other hand, for some class of non-trivial $\Sigma_1$-knots $(S^4, K)$, Iwase [6] and the author [5] determined the groups $\mathcal{E}(S^4, K)$.

Finally, the author would like to express his gratitude to Professor Masahico Saito for his helpful comments, and to Professor Nariya Kawazumi for introducing him results of Johnson [8]. This paper was written while the author stayed at Michigan State University as a visiting scholar sponsored by the Japanese Ministry of Education, Culture, Sports, Science and Technology. He is grateful to the Department of Mathematics, Michigan State University, for its hospitality.

## 2 Some elements of $\mathcal{E}(S^4, \Sigma_g)$

For elements $a$, $b$ and $c$ of a group, we write $\overline{c} = c^{-1}$, and $a*b = ab\overline{a}$ . Here, we introduce a standard form of the trivial $\Sigma_g$-knot $(S^4, \Sigma_g)$. We decompose $S^4 = D^4_+ \cup D^4_-$ and call $S^3 = D^4_+ \cap D^4_-$ *the equator* $S^3$ , and decompose $S^3 = D^3_+ \cup D^3_-$ and call $S^2 = D^3_+ \cap D^3_-$ *the equator* $S^2$ . Let $P_g$ be a planar surface constructed from a 2-disk by removing $g$ copies of disjoint 2-disks. As indicated in Figure 1, we denote the boundary components of $P_g$ by $\gamma_0, \gamma_2, \ldots, \gamma_{2g}$, and denote some properly embedded arcs of $P_g$ by $\gamma_1, \gamma_3, \ldots, \gamma_{2g+1}$, $\beta_2, \beta_4, \ldots, \beta_{2g-2}$ and $\beta'_2, \beta'_4, \ldots, \beta'_{2g-2}$. We parametrize the regular neighborhood of the equator $S^2$ in the equator $S^3$ by $S^2 \times [-1,1]$, such that $S^2 \times \{0\}$ = the equator $S^2$, $S^2 \times [-1,1] \cap D^3_+ = S^2 \times [0,1]$ and $S^2 \times [-1,1] \cap D^3_- = S^2 \times [-1,0]$. We put $P_g$ on the equator $S^2$. Then, $P_g \times [-1,1] \subset S^2 \times [-1,1]$ is a 3-dimensional handle body, so that, $(S^4, \partial(P_g \times [-1,1]))$ is the trivial $\Sigma_g$-knot. On $\partial(P_g \times [-1,1]) = \Sigma_g$,

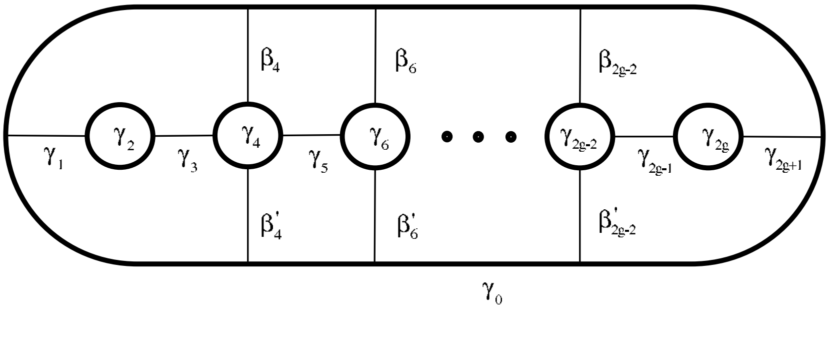

Figure 1

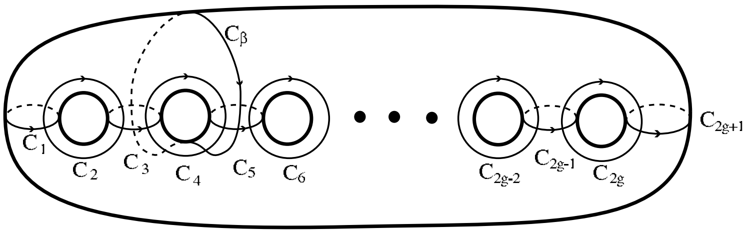

Figure 2

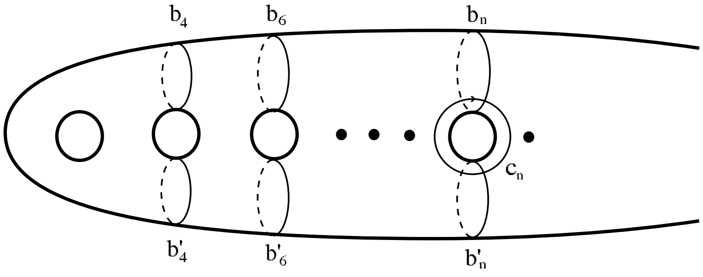

Figure 3

we define $c_{2i-1} = \partial(\gamma_{2i-1} \times [-1,1])$ $(1 \le i \le g+1)$, $b_{2j} = \partial(\beta_{2j} \times [-1,1])$, $b'_{2j} = \partial(\beta'_{2j} \times [-1,1])$ $(2 \le j \le g-1)$, and $c_{2k} = \gamma_{2k} \times \{0\}$ $(1 \le k \le g)$. In Figures 2 and 3, these circles are illustrated and some of them are oriented. For a simple closed curve $a$ on $\Sigma_g$, we denote the Dehn twist about $a$ by $T_a$. The order of composition of maps is the functional one: $T_bT_a$ means we apply

$T_a$ first, then $T_b$. We define some elements of $\mathcal{M}_g$ as follows:

$$\begin{aligned}
&C_i = T_{c_i},\ B_i = T_{b_i},\ B'_i = T_{b'_i},\\
&X_i = C_{i+1}C_i\overline{C_{i+1}}\ ,\ X_i^* = \overline{C_{i+1}}\ C_iC_{i+1}\ \ (1 \le i \le 2g),\\
&Y_{2j} = C_{2j}B_{2j}\overline{C_{2j}}\ ,\ Y_{2j}^* = \overline{C_{2j}}\ B_{2j}C_{2j}\ \ (2 \le j \le g-1),\\
&D_i = C_i^2\ \ (1 \le i \le 2g+1),\\
&DB_{2j} = B_{2j}^2\ \ (2 \le j \le g-1),\\
&T = C_1C_3C_5,\ T_1 = C_1C_3B_4,\ T_2 = B_4C_5C_7\cdots C_{2g+1}.
\end{aligned}$$

When $g \ge 3$, the subgroup of $\mathcal{M}_g$ generated by $X_i$ $(1 \le i \le 2g)$, $Y_{2j}$ $(2 \le j \le g-1)$, $D_i$ $(1 \le i \le 2g+1)$, $DB_{2j}$ $(2 \le j \le g-1)$, $T_1$, and $T_2$ is denoted by $G_g$. It is clear that $X_i^*$ and $Y_{2j}^*$ are elements of $G_g$. When $g = 2$, the subgroup of $\mathcal{M}_2$ generated by $X_i$ $(1 \le i \le 4)$, $D_j$ $(1 \le j \le 5)$, and $T$ is denoted by $G_2$. For two simple closed curves $l$ and $m$ on $\Sigma_g$, $l$ and $m$ are called $G_g$*-equivalent* (denote by $l \underset{G_g}{\sim} m$) if there is an element $\phi$ of $G_g$ such that $\phi(l) = m$. We set a basis of $H_1(\Sigma_g;\mathbb{Z})$ as in Figure 4, then for the quadratic form $q_{\Sigma_g}$ defined in §1, $q_{\Sigma_g}(x_i) = q_{\Sigma_g}(y_i) = 0$ $(1 \le i \le g)$. By the definitions of $q_{\Sigma_g}$ and $\mathcal{SP}_g$, we have:

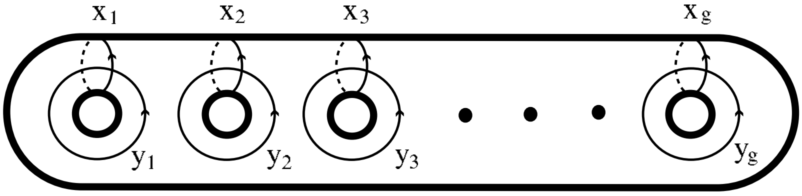

Figure 4

**Lemma 2.1** $\mathcal{E}(S^4, \Sigma_g) \subset \mathcal{SP}_g$.

In this section, we show:

**Lemma 2.2** $G_g \subset \mathcal{E}(S^4, \Sigma_g)$.

As a straightforward corollary of these lemmas, we have:

**Corollary 2.3** $G_g \subset \mathcal{SP}_g$.

If $G_g \supset \mathcal{SP}_g$, then Theorem 1.2 is proved. We prove $G_g \supset \mathcal{SP}_g$ in the next section.

**Proof of Lemma 2.2** First we show that, if $g = 2$, $T = C_1C_3C_5$ is an element of $\mathcal{E}(S^4, \Sigma_2)$. We parametrize the regular neighborhood of the equator $S^3$ in $S^4$ by $S^3 \times [-1, 1]$, such that $S^3 \times \{0\}$ = the equator $S^3$, $S^3 \times [-1, 1] \cap D^4_-$ $= S^3 \times [-1, 0]$, and $S^3 \times [-1, 1] \cap D^4_+ = S^3 \times [0, 1]$. We deform $\Sigma_2$ in $S^4$, in such a way that the surface obtained as a result of this deformation projects onto the equator $S^3$ as indicated in Figure 5. In this figure, there are 6 intersecting circles. For each circle, we take two regular neighborhoods $N_1$ and $N_2$ in $\Sigma_2$. For $0 < \epsilon < 1$, we put $N_1$ into $S^3 \times \{\frac{\epsilon}{2}\}$ and $N_2$ into $S^3 \times \{-\frac{\epsilon}{2}\}$. This deformation defines an orientation preserving diffeomorphism $\Psi_1$ of $S^4$. Let $r(\theta)\colon S^2 \to S^2$ be the angle $\theta$ rotation whose axis passes through $N$. We define $R(\theta)\colon S^3 \to S^3$ by

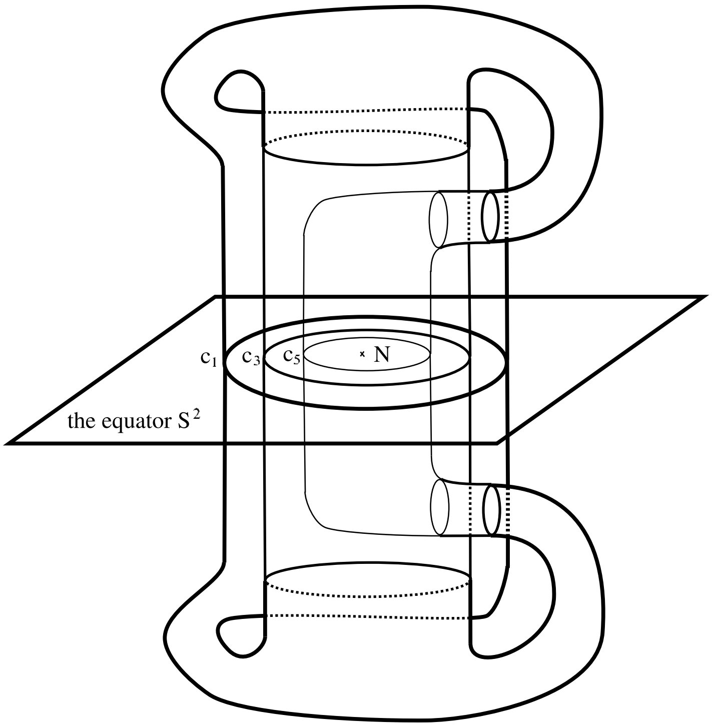

Figure 5

$$R(\theta)(x,t) = (r(t\theta)(x), t) \quad \text{on } S^2 \times [0,1]$$
$$R(\theta) = id \quad \text{on } D^3_-$$
$$R(\theta) = \text{ the angle } \theta \text{ rotation} \quad \text{on } D^3_+ - S^2 \times [0,1].$$

We define an orientation preserving diffeomorphism $\Psi_2$ of $S^4$ by

$$\begin{aligned}
&\Psi_2(x,t) = (R(2\pi)(x),t) \quad \text{on } S^3 \times [-\epsilon,\epsilon],\\
&\Psi_2(x,t) = \left(R(2\pi\frac{1-t}{1-\epsilon})(x),t\right) \quad \text{on } S^3 \times [\epsilon,1],\\
&\Psi_2(x,t) = \left(R(2\pi\frac{t+1}{1-\epsilon})(x),t\right) \quad \text{on } S^3 \times [-1,-\epsilon],\\
&\Psi_2 = id \quad \text{on } S^4 - S^3 \times [-1,1].
\end{aligned}$$

Then $\Psi_1^{-1}\Psi_2\Psi_1|_{\Sigma_2} = C_1C_3C_5$. In the same way as above, we can show for $g \geq 3$ that $T_1$ and $T_2$ are elements of $\mathcal{E}(S^4,\Sigma_g)$.

Next, for $g = 3$, we show that $X_3 = C_4C_3\overline{C_4}$ and $D_3 = C_3^2$ are elements of $\mathcal{E}(S^4,\Sigma_g)$. We review a theorem due to Montesinos [10]. We can construct $S^4$ from $B^3 \times S^1$ and $S^2 \times D^2$ by attaching their boundary with the natural identification. Let $D^2 \times S^1$ be the solid torus trivially embedded in $B^3$. We regard $D^2 \times S^1 \times S^1 \subset B^3 \times S^1 \subset S^4$ as the regular neighborhood of a trivial $\Sigma_1$-knot. Let $E^4$ be the exterior of this trivial $\Sigma_1$-knot. The 3 simple closed curves $l = \partial D^2 \times * \times *$, $r = * \times S^1 \times *$, $s = * \times * \times S^1$ on $\partial E^4$ represent a basis of $H_1(\partial E^4;\mathbb{Z})$. Montesinos showed:

**Theorem 2.4** [10, Theorem 5.3] *Let $g\colon \partial E^4 \to \partial E^4$ be a diffeomorphism which induces an automorphism on $H_1(\partial E^4;\mathbb{Z})$,*

$$g_*(l,r,s) = (l,r,s)\begin{pmatrix} m & a & b\\ n & \alpha & \gamma\\ p & \beta & \delta\end{pmatrix}.$$

*There is a diffeomorphism $G\colon E^4 \to E^4$ such that $G|_{\partial E^4} = g$ if and only if $a = b = 0$ and $\alpha+\beta+\gamma+\delta$ is even.*

Let $p$ be a point on $* \times S^1 \times S^1$ disjoint from $r \cup s$, $N(p)$ be a regular neighborhood of $p$ in the equator $S^3$, then $N = * \times S^1 \times S^1 - N(p)$ in a regular neighborhood of $r \cup s$. Figure 6 illustrates deformation of $\Sigma_g$ into $D^2 \times S^1 \times S^1$. We bring $c_3$ and $c_4$ to $r$ and $s$ and deform as is indicated by arrows. Then, we can deform $\Sigma_3$ in such a way that a regular neighborhood $N'$ of $c_3 \cup c_4$ coincides with $N$ and $\Sigma_3 - N' \subset N(p)$. Let diffeomorphisms $f_1$, $f_2$ over $D^2 \times S^1 \times S^1$ be defined by $f_1 = id_{D^2} \times \begin{pmatrix} 1 & 2\\ 0 & 1\end{pmatrix}$, $f_2 = id_{D^2} \times \begin{pmatrix} 2 & 1\\ -1 & 0\end{pmatrix}$ (where we present diffeomorphisms on $* \times S^1 \times S^1$ by its action on the basis $\{r,s\}$ of $H_1(* \times S^1 \times S^1;\mathbb{Z})$ and $r$ and $s$ are oriented as in Figure 6), then $f_1|_{\Sigma_2} =$

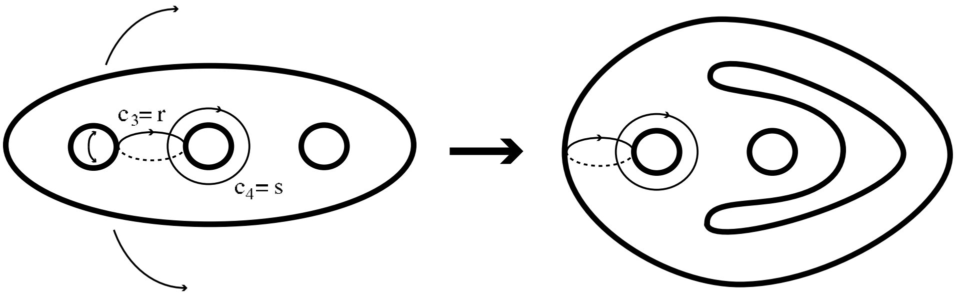

Figure 6

$C_3^2 = D_3$, $f_2|_{\Sigma_2} = C_4 C_3 \overline{C_4} = X_3$. Since the actions of these homeomorphisms on $H_1(\partial E^4;\mathbb{Z})$ are described by

$$(f_1|\partial E^4)_*(l,r,s) = (l,r,s)\begin{pmatrix}1&0&0\\0&1&2\\0&0&1\end{pmatrix},$$

$$(f_2|\partial E^4)_*(l,r,s) = (l,r,s)\begin{pmatrix}1&0&0\\0&2&1\\0&-1&0\end{pmatrix},$$

there are diffeomorphisms $F_1$ and $F_2$ such that $F_1|_{D^2\times S^1\times S^1} = f_1$, $F_2|_{D^2\times S^1\times S^1} = f_2$. These diffeomorphisms $F_1$, $F_2$ are extensions of $f_1$, $f_2$ respectively. By the same method as above, we can show that other $X_i$, $Y_{2j}$, $D_i$, and $DB_{2j}$ are elements of $\mathcal{E}(S^4,\Sigma_g)$ for any $g \geq 2$. □

## 3 A finite set of generators for the spin mapping class group

In Corollary 2.3, we showed that $G_g \subset \mathcal{SP}_g$. In this section, we show that $G_g = \mathcal{SP}_g$. That is to say, we show:

**Theorem 3.1** *If $g = 2$, $\mathcal{SP}_2$ is generated by $C_{i+1}C_i\overline{C_{i+1}}$ $(1 \leq i \leq 4)$, $C_j^2$ $(1 \leq j \leq 5)$, and $C_1C_3C_5$. If $g \geq 3$, $\mathcal{SP}_g$ is generated by $C_{i+1}C_i\overline{C_{i+1}}$ $(1 \leq i \leq 2g)$, $C_{2j}B_{2j}\overline{C_{2j}}$ $(2 \leq j \leq g-1)$, $C_k^2$ $(1 \leq k \leq 2g+1)$, $B_l^2$ $(1 \leq l \leq g-1)$, $C_1C_3B_4$ and $B_4C_5C_7\cdots C_{2g+1}$.*

When $g = 2$, we use Reidemeister–Schreier's method to show this. On the other hand, when $g \geq 3$, we use other methods. We start from the case when $g \geq 3$.

## 3.1 The hyperelliptic mapping class group

Let $\mathcal{H}_g$ be the subgroup of the mapping class group $\mathcal{M}_g$ generated by $C_1, C_2, \ldots, C_{2g+1}$. This group is called *the hyperelliptic mapping class group*. In this group (and also in $\mathcal{M}_g$), $C_i$'s satisfy the following equations:

$$C_iC_{i+1}C_i = C_{i+1}C_iC_{i+1}, \ (1 \leq i \leq 2g)$$
$$C_iC_j = C_jC_i, \ (|i-j| \geq 2).$$

These equations are called *braid equation*. In this paper, we use these relations frequently. In this section, we show the following lemma for $\mathcal{H}_g$.

**Lemma 3.2** *For any $i = 1, 2, \ldots, 2g{+}1$, and any element $W$ of $\mathcal{H}_g$, $WC_iC_i\overline{W}$ is an element of $G_g$.*

**Proof** We call $C_i$ *a positive letter* and $\overline{C_i}$ *a negative letter*. A sequence of positive letters is called *a positive word*. If indices of two letters $C_i$, $C_j$ satisfy $|i-j| = 1$, then we say $C_i$ is *adjacent* to $C_j$. If there is a negative letter $\overline{B}$ in a sequence of letters $W$, which presents an element of $\mathcal{H}_g$, we replace $\overline{B}$ by a sequence of letters $\overline{B}\,\overline{B}\cdot B$. This shows that every element of $\mathcal{H}_g$ is represented by a sequence of positive letters and $\overline{C_j}\,\overline{C_j}$ 's $(1 \leq j \leq 2g+1)$. If there is a sequence of letters $XX$ ( $X = C_i$ or $\overline{C_i}$ ) in $W$, say $W = W_1XXW_2$, then we rewrite,

$$\begin{aligned} WC_iC_i\overline{W} &= W_1XXW_2C_iC_i\overline{W_2}\,\overline{X}\,\overline{X}\,\overline{W_1} \\ &= W_1XX\overline{W_1}\,W_1W_2C_iC_i\overline{W_2}\,\overline{W_1}\,W_1\overline{X}\,\overline{X}\,\overline{W_1}\,. \end{aligned}$$

Therefore, the following claim shows this lemma:

**Claim** *For any positive word $W$ without $C_jC_j (1 \leq j \leq 2g+1)$, $WC_iC_i\overline{W}$ is an element of $G_g$.*

If the word length of $W$ is 0, the above claim is trivial. We assume that the word length of $W$ is at least 1, and we show this claim by the induction on the word length. If the right most letter $L$ of $W$ is not adjacent to $A_i$, and say $W = W'L$, then

$$WC_iC_i\overline{W} = W'LC_iC_i\overline{L}\,\overline{W'} = W'C_iL\overline{L}\,C_i\overline{W'} = W'C_iC_i\overline{W'}\,.$$

By the induction hypothesis, $WC_iC_i\overline{W}$ is an element of $G_g$. Therefore, from here to the end of this proof, we assume that the right most letter of $W$ is adjacent to $C_i$. Let $l$ be the word length of $W$, and $W = x_lx_{l-1}\ldots x_2x_1$. The letter $x_i$ of $W$ is called *a jump*, if $x_{i-1}$ and $x_i$ are not adjacent. The letter $x_j$

of $W$ is called *a turn*, if $x_j$ and $x_{j-1}$ are not jumps and $x_j = x_{j-2}$. Considering jumps and turns, we need to show this claim for the following three cases.

**Case 1** *When there is not any jump or any turn*: Since $x_l$ and $x_{l-1}$ are adjacent, $x_l x_{l-1}\overline{x_l}$ is an element of $G_g$. We rewrite,

$$WC_iC_i\overline{W} = x_lx_{l-1}\overline{x_l} \cdot x_lx_{l-2}x_{l-3}\cdots x_1C_iC_i\overline{x_1}\cdots\overline{x_{l-3}}\,\overline{x_{l-2}}\,\overline{x_l} \cdot x_l\overline{x_{l-1}}\,\overline{x_l}\ .$$

By the induction hypothesis, $WC_iC_i\overline{W}$ is an element of $G_g$.

**Case 2** *When there are jumps, but there is not any turn*: We show in the induction on the number of jumps in $W$. Let $x_j$ be the right most jump in $W$. First we consider the case when $j = 2$, say $W = W'x_2x_1$. If $x_2$ is not adjacent to $C_i$, we rewrite,

$$\begin{aligned} WC_iC_i\overline{W} &= W'x_2x_1C_iC_i\overline{x_1}\,\overline{x_2}\,\overline{W'} \\ &= W'x_1x_2C_iC_i\overline{x_2}\,\overline{x_1}\,\overline{W'} \\ &= W'x_1C_ix_2\overline{x_2}\,C_i\overline{x_1}\,\overline{W'} \\ &= W'x_1C_iC_i\overline{x_i}\,\overline{W'}\ . \end{aligned}$$

By the induction hypothesis on the word length of $W$, $WC_iC_i\overline{W}$ is an element of $G_g$. If $x_2$ is adjacent to $C_i$, we rewrite,

$$\begin{aligned} WC_iC_i\overline{W} &= W'x_2x_1C_iC_i\overline{x_1}\,\overline{x_2}\,\overline{W'} \\ &= W'x_2\overline{C_i}\,x_1x_1C_i\overline{x_2}\,\overline{W'} \\ &= W'x_2\overline{C_i}\,\overline{C_i}\ \cdot C_ix_1x_1\overline{C_i}\ \cdot C_iC_i\overline{x_2}\,\overline{W'} \\ &= W'x_2\overline{C_i}\,\overline{C_i}\,\overline{x_2}\,\overline{W'}\ \cdot W'x_2C_ix_1x_1\overline{C_i}\,\overline{x_2}\,\overline{W'}\ \cdot W'x_2C_iC_i\overline{x_2}\,\overline{W'}\ . \end{aligned}$$

By the induction hypothesis on the word length of $W$, the first and third terms are elements of $G_g$. By the induction hypothesis on the number of jumps in $W$, the second term is an element of $G_g$. Therefore, $WC_iC_i\overline{W}$ is an element of $G_g$. Next, we consider on the case when $j$ is at least 3. If $x_j$ is not adjacent to $x_{j-1}, \ldots, x_1$ then,

$$W = \ldots x_jx_{j-1}\ldots x_1 = \ldots x_{j-1}\ldots x_1x_j.$$

Therefore, it comes down to the case $j = 2$. If there are some letters adjacent to $x_j$ in $\{x_{j-1}, \cdots, x_1\}$, let $x_i$ be the left most element among them. By the definition of jumps, $j > i+1$, and by the definition of $x_i$, $x_j = x_{i-1}$. Therefore,

$$\begin{aligned} W &= \cdots x_j\cdots x_{i+1}x_ix_{i-1}\cdots x_1 \\ &= \cdots x_{i+1}x_jx_ix_{i-1}\cdots x_1 \\ &= \cdots x_{i+1}x_{i-1}x_ix_{i-1}\cdots x_1 \\ &= \cdots x_{i+1}x_ix_{i-1}x_i\cdots x_1. \end{aligned}$$

Since there is not any jump or any turn in the sequence $x_i x_{i-1} \cdots x_1$, $x_i$ commutes with $x_{i-2}, \dots, x_1$. Therefore, $W = \cdots x_1 x_i$ and it comes down to the case $j = 2$.

**Case 3** *When there are turns in $W$*: Let $x_t$ be the right most turn in $W$. By the definition of turn, $t$ is at least 3. By applying the argument for Case 2 to $x_{t-1}x_{t-2}\cdots x_1$, we assume that there is no turn and no jump in $x_{t-1}x_{t-2}\cdots x_1$. Since we assume that $x_1$ is adjacent to $C_i$, there may be a case when $x_2 = C_i$. In that case, we rewrite,

$$\begin{aligned} WC_iC_i\overline{W} &= \cdots x_3x_2x_1C_iC_i\overline{x_1}\,\overline{x_2}\,\overline{x_3}\,\cdots \\ &= \cdots x_3C_ix_1C_iC_i\overline{x_1}\,\overline{C_i}\,\overline{x_3}\,\cdots \\ &= \cdots x_3x_1C_ix_1\overline{x_1}\,\overline{C_i}\,x_1\overline{x_3}\,\cdots \\ &= \cdots x_3x_1x_1\overline{x_3}\,\cdots . \end{aligned}$$

By the induction hypothesis on the word length of $W$, $WC_iC_i\overline{W}$ is an element of $G_g$. If $x_2 \neq C_i$, then $x_{t-1}, x_{t-2}, \cdots, x_2$ are not adjacent to $C_i$. We rewrite,

$$\begin{aligned} W &= \cdots x_tx_{t-1}x_{t-2}x_{t-3}\cdots x_1 \\ &= \cdots x_{t-2}x_{t-1}x_{t-2}x_{t-3}\cdots x_1 \\ &= \cdots x_{t-1}x_{t-2}x_{t-1}x_{t-3}\cdots x_1. \end{aligned}$$

Since we assume that there is no jump and no turn in $x_{t-1}x_{t-2}\cdots x_1$, $x_{t-1}$ is not adjacent to $x_{t-3}, \dots, x_1$. Therefore, $W = \cdots x_{t-1}x_{t-2}x_{t-3}\cdots x_1x_{t-1}$. With remarking that $x_{t-1}$ is not adjacent to $C_i$, we rewrite,

$$\begin{aligned} WC_iC_i\overline{W} &= \cdots x_{t-1}x_{t-2}x_{t-3}\cdots x_1x_{t-1}C_iC_i\overline{x_{t-1}}\,\overline{x_1}\,\cdots\overline{x_{t-3}}\,\overline{x_{t-2}}\,\overline{x_{t-1}}\,\cdots \\ &= \cdots x_{t-1}x_{t-2}x_{t-3}\cdots x_1C_ix_{t-1}\overline{x_{t-1}}\,C_i\overline{x_1}\,\cdots\overline{x_{t-3}}\,\overline{x_{t-2}}\,\overline{x_{t-1}}\,\cdots \\ &= \cdots x_{t-1}x_{t-2}x_{t-3}\cdots x_1C_iC_i\overline{x_1}\,\cdots\overline{x_{t-3}}\,\overline{x_{t-2}}\,\overline{x_{t-1}}\,\cdots . \end{aligned}$$

By the induction hypothesis on the word length of $W$, $WC_iC_i\overline{W}$ is an element of $G_g$. □

### 3.2 The Torelli group $\mathcal{I}_g$

In this subsection, we assume $g \geq 3$. There is a natural surjection $\Phi\colon \mathcal{M}_g \to \mathrm{Sp}(2g, \mathbb{Z})$ defined by the action of $\mathcal{M}_g$ on the group $H_1(\Sigma_g; \mathbb{Z})$. We denote the kernel of $\Phi$ by $\mathcal{I}_g$ and call this *the Torelli group*. In this subsection, we prove the following lemma:

**Lemma 3.3** *The Torelli group $\mathcal{I}_g$ is a subgroup of $G_g$.*

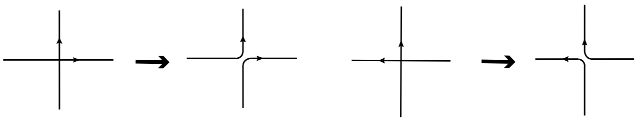

Figure 7

Johnson [7] showed that, when $g$ is larger than or equal to 3, $\mathcal{I}_g$ is finitely generated. We review his result. We orient and call simple closed curves as indicated in Figure 2, and call $(c_1, c_2, \dots, c_{2g+1})$ and $(c_\beta, c_5, \dots, c_{2g+1})$ as *chains*. For oriented simple closed curves $d$ and $e$ which mutually intersect in one point, we construct an oriented simple closed curve $d+e$ from $d \cup e$ as follows: choose a disk neighborhood of the intersection point and in it make a replacement as indicated in Figure 7. For a consecutive subset $\{c_i, c_{i+1}, \dots, c_j\}$ of a chain, let $c_i + \cdots + c_j$ be the oriented simple closed curve constructed by repeated applications of the above operations. Let $(i_1, \dots, i_{r+1})$ be a subsequence of $(1, 2, \dots, 2g+1)$ (Resp. $(\beta, 5, \dots, 2g+1)$). We construct the union of circles $\mathcal{C} = c_{i_1} + \cdots + c_{i_2-1} \cup c_{i_2} + \cdots + c_{i_3-1} \cup \cdots \cup c_{i_r} + \cdots + c_{i_{r+1}-1}$. If $r$ is odd, the regular neighborhood of $\mathcal{C}$ is an oriented compact surface with 2 boundary components. Let $\phi$ be the element of $\mathcal{M}_g$ defined as the composition of the positive Dehn twist along the boundary curve to the left of $\mathcal{C}$ and the negative Dehn twist along the boundary curve to the right of $\mathcal{C}$. Then, $\phi$ is an element of $\mathcal{I}_g$. We denote $\phi$ by $[i_1, \dots, i_{r+1}]$, and call this *the odd subchain map* of $(c_1, c_2, \dots, c_{2g+1})$ (Resp. $(c_\beta, c_5, \dots, c_{2g+1})$). Johnson [7] showed the following theorem:

**Theorem 3.4** [7, Main Theorem] *For $g \geq 3$, the odd subchain maps of the two chains $(c_1, c_2, \dots, c_{2g+1})$ and $(c_\beta, c_5, \dots, c_{2g+1})$ generate $\mathcal{I}_g$.*

We use the following results by Johnson [7].

**Lemma 3.5** [7] (a) *$C_j$ commutes with $[i_1, i_2, \cdots]$ if and only if $j$ and $j+1$ are either both contained in or are disjoint from the $i$'s.*
(b) *If $i \neq j+1$, then $\overline{C_j} * [\cdots, j, i, \cdots] = [\cdots, j+1, i, \cdots]$, and $C_j * [\cdots, j, i, \cdots] = [\cdots, j, i, \cdots][\cdots, j+1, i, \cdots]^{-1}[\cdots, j, i, \cdots]$.*
(c) *If $k \neq j$, then $C_j * [\cdots, k, j+1, \cdots] = [\cdots, k, j, \cdots]$, and $\overline{C_j} * [\cdots, k, j+1, \cdots] = [\cdots, k, j+1, \cdots][\cdots, k, j, \cdots]^{-1}[\cdots, k, j+1, \cdots]$.*
(d) *$[1,2,3,4][1,2,5,6,\dots,2n]B_4 * [3,4,5,\dots,2n] = [5,6,\dots,2n][1,2,3,4,\dots,2n]$, where $3 \leq n \leq g$.*

First we show that some odd subchain maps are elements of $G_g$.

**Lemma 3.6** $[1,2,3,4]$, $[1,3,5,7,\dots,2i+1,\dots,2n-1]$ *($n$ is even, and $4 \le n \le g+1$), and* $[1,2,4,6,\dots,2i,\dots,2n-2]$ *($n$ is even, and $4 \le n \le g+2$) are elements of $G_g$.*

**Proof** In this proof, for a sequence $\{f_i\}$ of elements of $\mathcal{M}_g$, we write,

$$\prod_{i=n}^{m} f_i = \begin{cases} f_n f_{n+1} \cdots f_m, & n \le m, \\ f_n f_{n-1} \cdots f_m, & n \ge m. \end{cases}$$

(1) $[1,2,3,4]$ *is an element of $G_g$:* $[1,2,3,4]$ is equal to $B_4\overline{B'_4}$ . Since $C_4C_3C_2C_1C_1C_2C_3C_4(b_4) = b'_4$,

$$\begin{aligned}[1,2,3,4] &= B_4C_4C_3C_2C_1C_1C_2C_3C_4\overline{B_4}\,\overline{C_4}\,\overline{C_3}\,\overline{C_2}\,\overline{C_1}\,\overline{C_1}\,\overline{C_2}\,\overline{C_3}\,\overline{C_4} \\ &= B_4C_4\overline{B_4}\ \cdot C_3C_2\overline{C_3}\ \cdot C_1C_1 \cdot C_3C_2\overline{C_3}\ \cdot C_3C_3 \cdot B_4C_4\overline{B_4}\ \cdot \overline{C_4}\,\overline{C_3}\,C_4 \cdot \\ &\quad \cdot \overline{C_2}\,\overline{C_1}\,C_2 \cdot \overline{C_2}\,\overline{C_1}\,C_2 \cdot \overline{C_2}\,\overline{C_2}\ \cdot \overline{C_4}\,\overline{C_3}\,C_4 \cdot \overline{C_4}\,\overline{C_4}\ .\end{aligned}$$

Therefore, $[1,2,3,4]$ is an element of $G_g$.
(2) $[1,3,5,7,\dots,2i+1,\dots,2n-1]$ *($n$ is even, and $4 \le n \le g+1$) are elements of $G_g$:* By (b) of Lemma 3.5,

$$[1,3,5,7,\dots,2i+1,\dots,2n-1] = (\prod_{k=n-1}^{1}\prod_{i=2k}^{n+k-1}\overline{C_i}\ ) * [1,2,3,4,\dots,n].$$

Since $[1,2,3,4,\dots,n] = B_n\overline{B'_n}$ , and $b'_n = \prod_{i=n}^{2} C_i \cdot C_1C_1 \cdot \prod_{i=2}^{n} C_i(b_n)$,

$$\begin{aligned}[1,2,3,4,\cdots,n] &= B_n\prod_{i=n}^{2}C_i \cdot C_1C_1 \cdot \prod_{i=2}^{n}C_i \cdot \overline{B_n}\ \cdot \prod_{i=n}^{2}\overline{C_i}\ \cdot \overline{C_1}\,\overline{C_1}\ \cdot \prod_{i=2}^{n}\overline{C_i} \\ &= \prod_{k=2}^{n}\{(B_n\prod_{i=n}^{k}C_i) * (C_{k-1}C_{k-1})\} \cdot B_n * (C_nC_n) \cdot \\ &\quad \cdot \prod_{k=2}^{n}\{(\prod_{i=n}^{k}\overline{C_i}\ ) * (\overline{C_{k-1}}\,\overline{C_{k-1}}\ )\} \cdot \overline{C_n}\,\overline{C_n}\ .\end{aligned}$$

Therefore,

$$\begin{aligned}
[1,3,5,7,\ldots,2n-1] = \prod_{k=2}^{n}\{(\prod_{l=n-1}^{1}\prod_{i=2l}^{n+l-1}\overline{C_i}\ \cdot B_n \cdot \prod_{i=n}^{k} C_i) * (C_{k-1}C_{k-1})\} \cdot \\
\cdot (\prod_{l=n-1}^{1}\prod_{i=2l}^{n+l-1}\overline{C_i}\ \cdot B_n) * (C_nC_n) \cdot \\
\cdot \prod_{k=2}^{n}\{(\prod_{l=n-1}^{1}\prod_{i=2l}^{n+l-1}\overline{C_i}\ \cdot \prod_{i=n}^{k}\overline{C_i}\ ) * (\overline{C_{k-1}}\ \overline{C_{k-1}}\ )\} \cdot \\
\cdot (\prod_{l=n-1}^{1}\prod_{i=2l}^{n+l-1}\overline{C_i}\ ) * (\overline{C_n}\ \overline{C_n}\ ).
\end{aligned}$$

By Lemma 3.2, $\prod_{k=2}^{n}\{(\prod_{l=n-1}^{1}\prod_{i=2l}^{n+l-1}\overline{C_i}\ \cdot \prod_{i=n}^{k}\overline{C_i}\ ) * (\overline{C_{k-1}}\ \overline{C_{k-1}}\ )\}$ and $(\prod_{l=n-1}^{1}\prod_{i=2l}^{n+l-1}\overline{C_i}\ ) * (\overline{C_n}\ \overline{C_n}\ )$ are elements of $G_g$. By braid relations for $\mathcal{M}_g$, (in the following equations $j \leq n-1$)

$$\begin{aligned}
(C_{j-1}\cdot \prod_{i=n}^{j} C_i) * (C_{j-1}C_{j-1}) &= C_{j-1}\prod_{i=n}^{j+1} C_i \cdot C_jC_{j-1}C_{j-1}\overline{C_j}\ \cdot \prod_{i=j+1}^{n}\overline{C_i}\ \overline{C_{j-1}} \\
&= \prod_{i=n}^{j+1} C_i \cdot C_{j-1}C_jC_{j-1}C_{j-1}\overline{C_j}\ \overline{C_{j-1}}\ \cdot \prod_{i=j+1}^{n}\overline{C_i} \\
&= \prod_{i=n}^{j+1} C_i \cdot C_jC_{j-1}C_j\overline{C_j}\ \overline{C_{j-1}}\ C_j \cdot \prod_{i=j+1}^{n}\overline{C_i}\ = (\prod_{i=n}^{j+1} C_i) * (C_jC_j),
\end{aligned}$$

$$\begin{aligned}
(C_{n-1}C_n) * (C_{n-1}C_{n-1}) &= C_{n-1}C_nC_{n-1}C_{n-1}\overline{C_n}\ \overline{C_{n-1}} \\
&= C_nC_{n-1}C_n\overline{C_n}\ \overline{C_{n-1}}\ C_n = C_nC_n.
\end{aligned}$$

By the above equation and the fact that $B_n$ commutes with $C_j$ $(1 \leq j \leq n-1)$,

$$(B_n \cdot \prod_{i=n}^{k} C_i) * (C_{k-1}C_{k-1}) = (\prod_{j=k-2}^{1} C_j \cdot B_n \cdot \prod_{i=n}^{2} C_i) * (C_1C_1) \text{ where } 3 \leq k \leq n,$$

$$B_n * (C_nC_n) = (\prod_{j=n-1}^{1} C_j \cdot B_n \prod_{i=n}^{2} C_i) * (C_1C_1).$$

Since, for $3 \leq k \leq n+1$,

$$\prod_{l=n-1}^{1}\prod_{i=2l}^{n+l-1}\overline{C_i}\ \cdot \prod_{j=k-2}^{1} C_j = \prod_{j=k-2}^{1}(\overline{C_{2j}}\ C_{2j-1}C_{2j}) \cdot \prod_{l=n-1}^{1}\prod_{i=2l}^{n+l-1}\overline{C_i}\ ,$$

we obtain,

$$(\prod_{l=n-1}^{1}\prod_{i=2l}^{n+l-1}\overline{C_i}\cdot\prod_{j=k-2}^{1}C_j\cdot B_n\cdot\prod_{i=n}^{2}C_i)*(C_1C_1)$$

$$=(\prod_{j=k-2}^{1}(\overline{C_{2j}}\,C_{2j-1}C_{2j})\cdot\prod_{l=n-1}^{1}\prod_{i=2l}^{n+l-1}\overline{C_i}\;\cdot B_n\cdot\prod_{i=n}^{2}C_i)*(C_1C_1).$$

Therefore, for showing that $[1,3,5,7,\dots,2n-1]$ is an element of $G_g$, it suffices to show that $(\prod_{l=n-1}^{1}\prod_{i=2l}^{n+l-1}\overline{C_i}\;\cdot B_n\cdot\prod_{i=n}^{2}C_i)*(C_1C_1)$ is an element of $G_g$. Figure 8 illustrates $u=\prod_{l=n-1}^{1}\prod_{i=2l}^{n+l-1}\overline{C_i}\;\cdot B_n\cdot\prod_{i=n}^{2}C_i(c_1)$. We investigate the action of elements of $G_g$ on $u$. As indicated in Figure 9, $X_5^*X_3^*X_1$ acts on $u$. We make $\prod_{i=\frac{n}{2}-2}^{2}X_{4i+1}^*X_{4i-1}^*$ act on this circle. In the middle of this action, $X_{4i+1}^*X_{4i-1}^*$ acts locally as in Figure 10. Hence, $\prod_{i=\frac{n}{2}-2}^{2}X_{4i+1}^*X_{4i-1}^*\cdot X_1(u)$ is as the first of Figure 11. This figure shows that, by the action of $\overline{X_6}\ \overline{X_4}\ \overline{Y_6^*}\ X_{2n-3}^*X_{2n-5}^*$, this curve is changed to the $u$ of $n-4$. Therefore, for our purpose, it suffices to show that $T_uT_u$ is an element of $G_g$ only for $n=4$ or $n=6$. Figure 12 shows that, when $n=4$, $T_uT_u=(\overline{X_1}\ \overline{X_3^*}\ \overline{X_5^*}\ )*(Y_4^*Y_4^*)$.

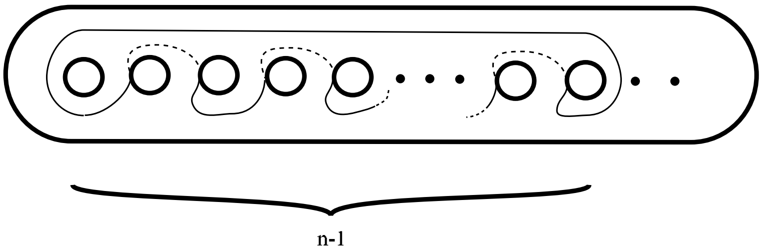

Figure 8

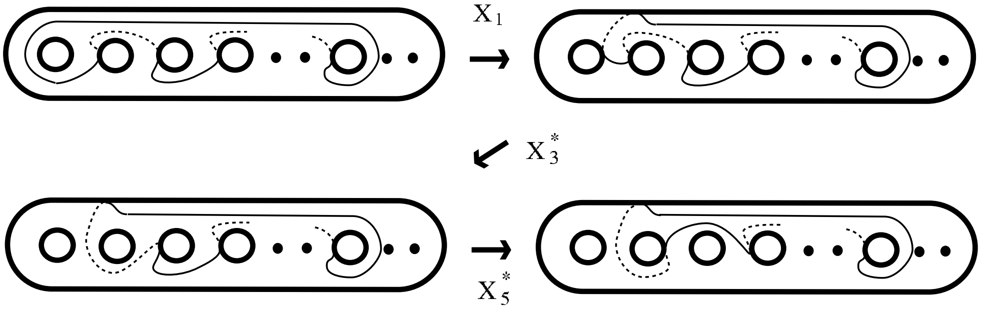

Figure 9

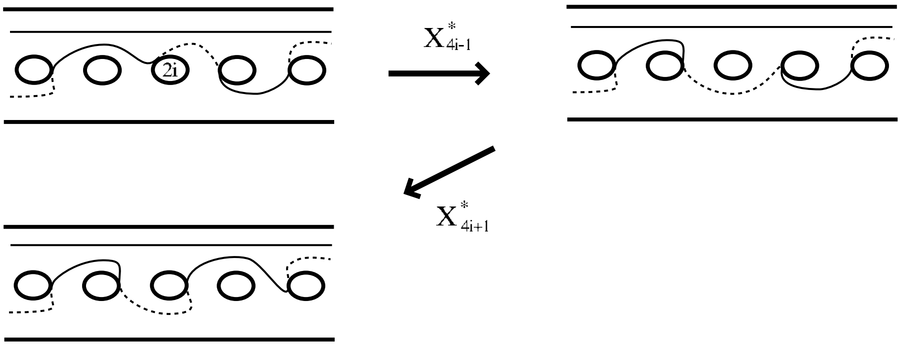

Figure 10

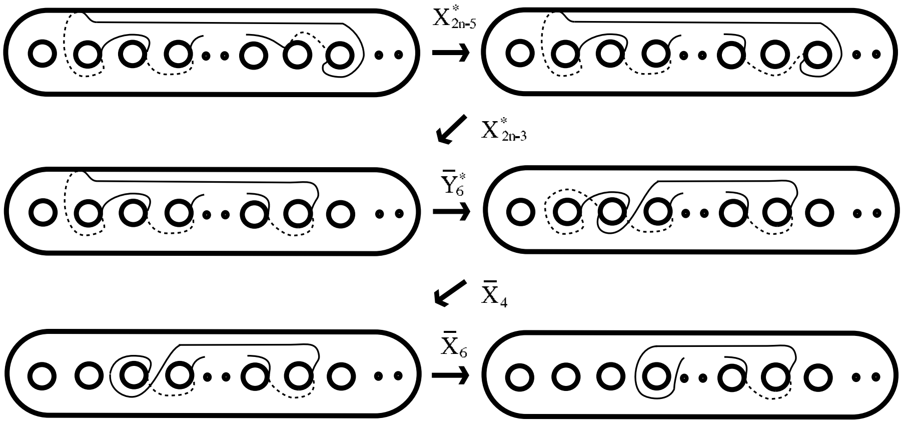

Figure 11

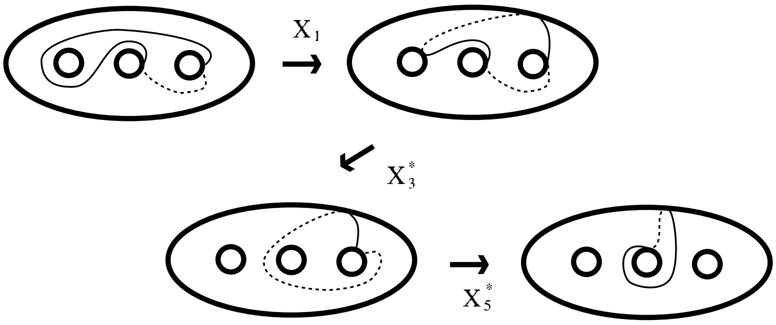

Figure 12

Figure 13 shows that, when $n = 5$, $T_uT_u = (\overline{X_1}\ \overline{X_3^*}\ \overline{X_5^*}\ \overline{X_7^*}\ \overline{X_9^*}\ Y_6^* X_4 X_6) * D_8$.

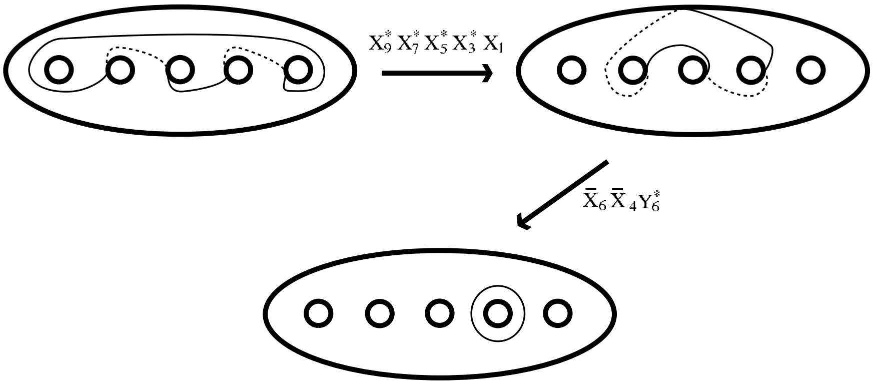

Figure 13

(3) $[1,2,4,6,\dots,2i,\dots,2n-2]$ *($n$ is even, and $4 \le n \le g+2$) are elements of $G_g$:* By (b) of Lemma 3.5,

$$[1,2,4,6,8,\dots,2n-2] = (\prod_{k=n-2}^{1} \prod_{i=2k+1}^{n+k-1} \overline{C_i}\ ) * [1,2,3,4,\dots,n].$$

In the same way as (2),

$$\begin{aligned}[1,2,4,6,8,\dots,2n-2] = &\prod_{k=2}^{n} \{ ( \prod_{l=n-2}^{1} \prod_{i=2l+1}^{n+l-1} \overline{C_i}\ \cdot B_n \cdot \prod_{i=n}^{k} C_i) * (C_{k-1}C_{k-1}) \} \cdot \\ &\cdot ( \prod_{l=n-2}^{1} \prod_{i=2l+1}^{n+l-1} \overline{C_i}\ \cdot B_n) * (C_n C_n) \cdot \\ &\cdot \prod_{k=2}^{n} \{ ( \prod_{l=n-2}^{1} \prod_{i=2l+1}^{n+l-1} \overline{C_i}\ \cdot \prod_{i=n}^{k} \overline{C_i}\ ) * (\overline{C_{k-1}}\ \overline{C_{k-1}}\ ) \} \cdot \\ &\cdot ( \prod_{l=n+2}^{1} \prod_{i=2l+1}^{n+l-1} \overline{C_i}\ ) * (\overline{C_n}\ \overline{C_n}\ ).\end{aligned}$$

By Lemma 3.2, $(\prod_{l=n-2}^{1} \prod_{i=2l+1}^{n+l-1} \overline{C_i}\ \cdot \prod_{i=n}^{k} \overline{C_i}\ ) * (\overline{C_{k-1}}\ \overline{C_{k-1}}\ )$ and $(\prod_{l=n+2}^{1} \prod_{i=2l+1}^{n+l-1} \overline{C_i}\ ) * (\overline{C_n}\ \overline{C_n}\ )$ are elements of $G_g$. By the same method as in (2), but using

$$\prod_{l=n-2}^{1} \prod_{i=2l+1}^{n+l-1} \overline{C_i}\ \cdot \prod_{j=k-2}^{1} C_j = \prod_{j=k-2}^{2} (\overline{C_{2j-1}}\ C_{2j-2}C_{2j-1}) \cdot C_1 \cdot \prod_{l=n-2}^{1} \prod_{i=2l+1}^{n+l-1} \overline{C_i}\ ,$$

in place of,

$$\prod_{l=n-1}^{1}\prod_{i=2l}^{n+l-1}\overline{C_i}\cdot\prod_{j=k-2}^{1}C_j=\prod_{j=k-2}^{1}(\overline{C_{2j}}\,C_{2j-1}C_{2j})\cdot\prod_{l=n-1}^{1}\prod_{i=2l}^{n+l-1}\overline{C_i}\,,$$

we conclude that, for our purpose, it suffices to show that $(\prod_{l=n-2}^{1}\prod_{i=2l+1}^{n+l-1}\overline{C_i}\cdot B_n\cdot\prod_{i=n}^{2}C_i)*(C_iC_i)$ and $(C_1\prod_{l=n-2}^{1}\prod_{i=2l+1}^{n+l-1}\overline{C_i}\cdot B_n\cdot\prod_{i=n}^{2}C_i)*(C_iC_i)$ are elements of $G_g$. Figure 14 illustrates $v=\prod_{l=n-2}^{1}\prod_{i=2l+1}^{n+l-1}\overline{C_i}\cdot B_n\cdot\prod_{i=n}^{2}C_i(c_1)$

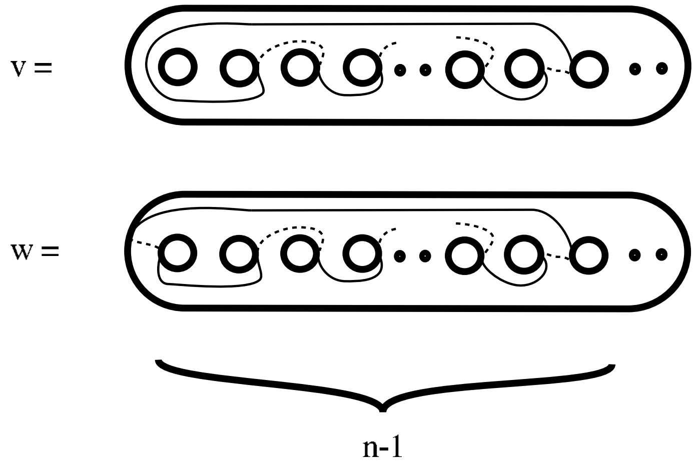

Figure 14

and $w=C_1(v)$. First we investigate the actions of elements of $G_g$ on $v$. In the following argument, we will refer the pictures in Figure 15 and Figure 18 by the number with (). By the action of $T_2\overline{DB_2}$ , $v$ is changed to (0). Now, we show (1) is $G_g$-equivalent to (6). (1) is altered to (2) by the action of $Y_6^*$. We make a sequence of $\overline{X_{4i+1}^*}\,\overline{X_{4i-1}^*}$ 's act on this circle. In the middle of this process, each $\overline{X_{4i+1}^*}\,\overline{X_{4i-1}^*}$ acts locally as indicated in Figure 16. Hence, (2) is $G_g$-equivalent to (3). By the action of $\overline{X_{4m-1}^*}$ , (3) is deformed to (4). In the middle of a sequential action of $\overline{X_{4i+3}^*}\,\overline{X_{4i+1}^*}$ 's, each $\overline{X_{4i+3}^*}\,\overline{X_{4i+1}^*}$ acts locally as shown in Figure 17. Hence, (4) and (5) are $G_g$-equivalent. As a result of the action of $\overline{X_{4m-3}^*}$ , (5) is altered to (6). The above argument shows that (1) is $G_g$-equivalent to (6). For (0), we apply the above process from (1) to (6) repeatedly, then we get (7). The element $\overline{X_5^*}\,\overline{X_7^*}\,\overline{Y_6^*}$ alters (7) into (8). If $\frac{n}{2}$ is even, $DB_4^{\frac{n}{4}-1}$ deforms (8) into (9). Since (9) is changed to (10) by the action of $\overline{X_3}$ , there exists an element $h$ of $G_g$ such that $h*(T_vT_v)=X_1X_1$. If $\frac{n}{2}$ is odd, $DB_4^{\frac{n-2}{4}}$ deforms (8) into (11). Since (11) is changed to (12) by the action

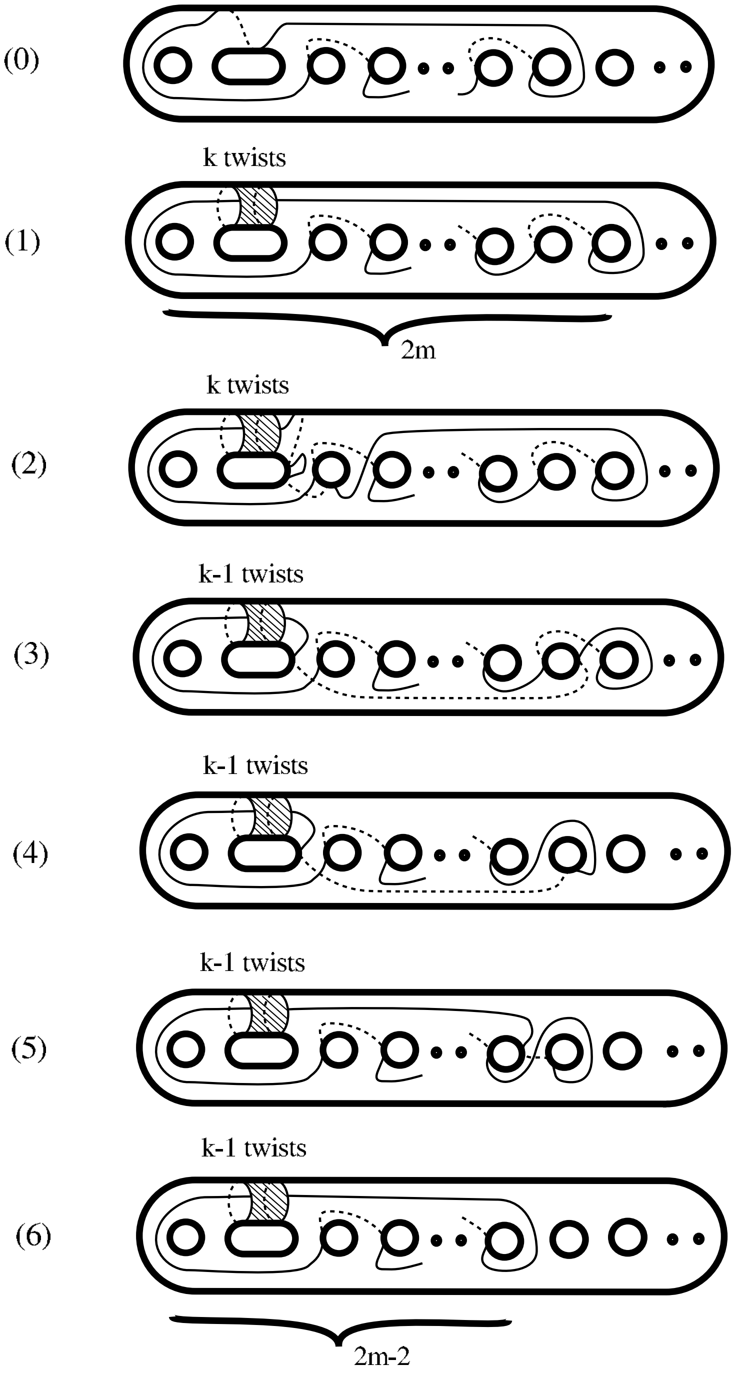
(0)
k twists
(1)
2m
k twists
(2)
k-1 twists
(3)
k-1 twists
(4)
k-1 twists
(5)
k-1 twists
(6)
2m-2

Figure 15

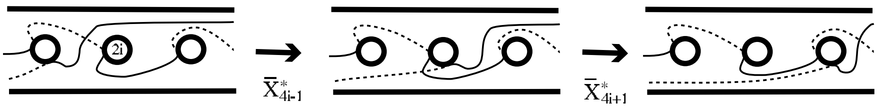

Figure 16

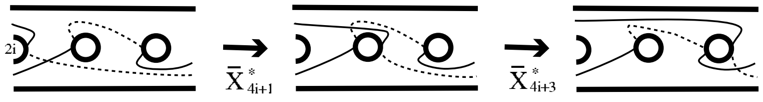

Figure 17

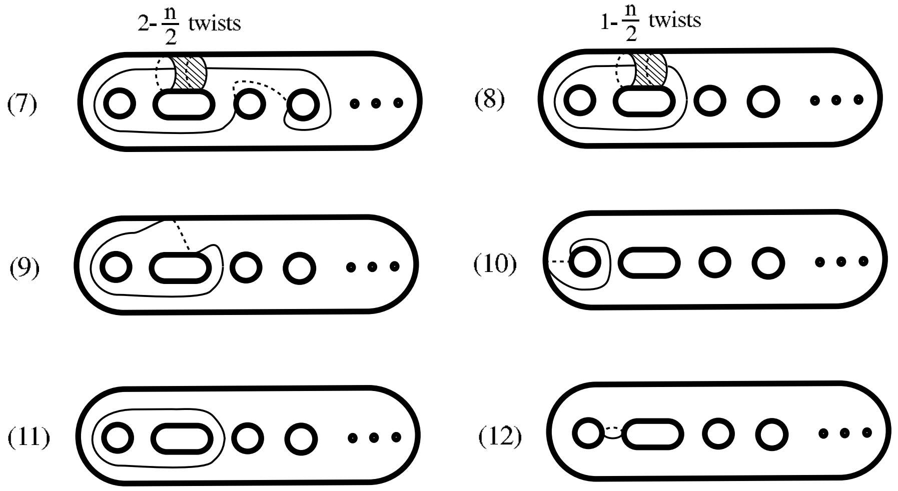

Figure 18

of $X_1\overline{Y_4^*}$ , there exists an element $h$ of $G_g$ such that $h*(T_vT_v) = D_3$. Next, we investigate the actions of $G_g$ on $w$. The action of $\overline{T_1}\ T_2$ deforms $w$ into (1) of Figure 19. After the repeated application of the actions from (1) to (6) of Figure 15, this circle is altered to (2) of Figure 19. By the same argument for $v$, when $\frac{n}{2}$ is even, there is a $h$ of $G_g$ such that $h*(T_wT_w) = D_3$, on the other hand, when $\frac{n}{2}$ is odd, there is a $h$ of $G_g$ such that $h*(T_wT_w) = X_1X_1$. Therefore, $[1, 2, 4, 6, 8, \dots, 2n-2]$ is an element of $G_g$. □

We prove that any odd subchain map of $(c_1, c_2, c_3, \dots, c_{2g+1})$ or $(c_\beta, c_5, c_6, \dots, c_{2g})$ is a product of elements listed on Lemma 3.6 and elements of $G_g$. The following lemma shows that any odd subchain map of $(c_\beta, c_5, c_6, \dots, c_{2g})$ is a product of an odd subchain map of $(c_1, c_2, c_3, \dots, c_{2g+1})$ and elements of $G_g$.

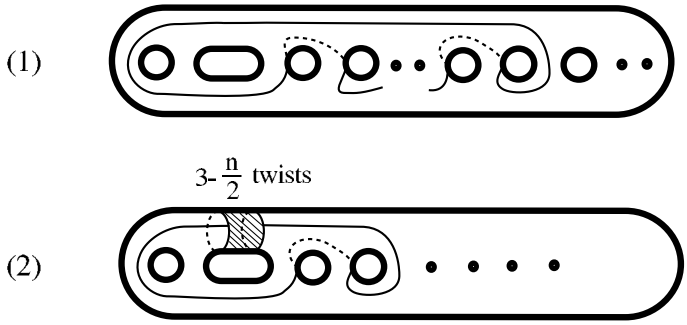

Figure 19

**Lemma 3.7** $D_3\overline{T_1}\,(c_\beta) = c_3 + c_4$.

**Proof** Figure 20 proves this lemma. □

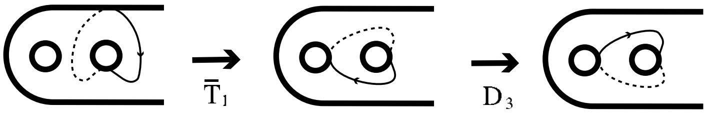

Figure 20

From here to the end of this subsection, odd subchain maps mean only those of $(c_1, c_2, c_3, \ldots, c_{2g+1})$. The following lemma shows that any odd subchain map, whose length is at least 5 and which begins from $1, 2, 3, 4$, is a product of shorter odd subchain maps and elements of $G_g$.

**Lemma 3.8**

$$[1,2,3,4][1,2,3,5]^{-1}[1,2,3,4][1,2,4,6,7,\ldots,2n]\cdot \\ \cdot(C_4B_4\overline{C_4}\,) * [3,4,5,\ldots,2n] = [4,6,7,\ldots,2n][1,2,3,4,\ldots,2n]$$

**Proof** By (a) of Lemma 3.5, $\overline{C_4}\ * [3,4,5,\ldots,2n] = [3,4,5,\ldots,2n]$, and by (d) of Lemma 3.5,

$$[1,2,3,4][1,2,5,6,\ldots,2n]\cdot(B_4\overline{C_4}\,) * [3,4,5,\ldots,2n] = \\ = [5,6,\ldots,2n][1,2,3,4,\ldots,2n].$$

By applying $C_4$ to the above equation, we get the equation which we need. □

For any odd subchain map $[i_1, i_2, \dots , i_r]$, we define a sequence $[[\epsilon_1, \epsilon_2, \dots , \epsilon_{2g+2}]]$ as follows: $\epsilon_k = 1$ if $k$ is a member of $\{i_1, i_2, \dots , i_r\}$, and $\epsilon_k = 0$ if $k$ is not a member of $\{i_1, i_2, \dots , i_r\}$. For this sequence $[[\epsilon_1, \epsilon_2, \dots , \epsilon_{2g+2}]]$, we construct the sequence $[[\delta_1, \delta_2, \dots , \delta_{2g+2}]]$ by the following rule: $(\delta_{2i-1}, \delta_{2i}) = (0, 0)$ if $(\epsilon_{2i-1}, \epsilon_{2i}) = (0, 0)$, $(\delta_{2i-1}, \delta_{2i}) = (1, 0)$ if $(\epsilon_{2i-1}, \epsilon_{2i}) = (0, 1)$, $(\delta_{2i-1}, \delta_{2i}) = (0, 1)$ if $(\epsilon_{2i-1}, \epsilon_{2i}) = (1, 0)$, $(\delta_{2i-1}, \delta_{2i}) = (1, 1)$ if $(\epsilon_{2i-1}, \epsilon_{2i}) = (1, 1)$. The odd subchain map $[j_1, j_2, \dots , j_r]$, which corresponds to the sequence $[[\delta_1, \delta_2, \dots , \delta_{2g+2}]]$, is called *the reversion* of $[i_1, i_2, \dots , i_r]$.

**Lemma 3.9** (1) *For any odd subchain map $c$, there is an element of $G_g$ which brings $c$ to its reversion.*
(2) *When $k \leq i-3$, $(\overline{C_{i-1}}\, C_{i-2}C_{i-1}) * [\dots , k, i, j, \dots ] = [\dots , k, i-2, j, \dots ]$.*
(3) *When $k \leq i-2$, $(C_iC_{i-1}\overline{C_i}\,) * [\dots , k, i, i+1, \dots ] = [\dots , k, i-1, i, \dots ]$.*

**Proof** Lemma 3.5 shows (2) and (3). Since, $\overline{T_1}\, T_2 = \overline{C_1}\, \overline{C_3}\, C_5 \cdots C_{2g+1}$ and $D_{2i-1} = C_{2i-1}C_{2i-1}$ $(1 \leq i \leq g+1)$ are elements of $G_g$, $C_1^{\pm 1}C_3^{\pm 1} \cdots C_{2g+1}^{\pm 1}$ is an elements of $G_g$ for any choice of $\pm 1$'s. Let $[[\epsilon_1, \epsilon_2, \dots , \epsilon_{2g+2}]]$ be the 0-1 sequence corresponding to $[i_1, i_2, \dots , i_r]$. We define $\gamma_i$ $(1 \leq i \leq g+1)$ as follows: $\gamma_i = +1$ if $(\epsilon_{2i-1}, \epsilon_{2i}) = (0, 0), (0, 1)$, or $(1, 1)$, and $\gamma_i = -1$ if $(\epsilon_{2i-1}, \epsilon_{2i}) = (1, 0)$. Then $(C_1^{\gamma_1}C_3^{\gamma_2} \cdots C_{2g+1}^{\gamma_{g+1}}) * [i_1, \dots , i_r]$ is the reversion of $[i_1, \dots , i_r]$. □

By (2) of the above lemma, any odd subchain map is deformed to an odd subchain map $[i_1, i_2, \dots , i_r]$ such that $i_{l+1} - i_l \leq 2$ under the action of $G_g$. If there are at least two disjoint pairs of indices $(i_l, i_{l+1})$ in an odd subchain map $[i_1, i_2, \dots , i_r]$ such that $i_{l+1} = i_l + 1$, then, by (3) of the above lemma, this odd subchain map is altered to the odd subchain map which begins from $1, 2, 3, 4$ under the action of $G_g$. Therefore, by Lemma 3.8, this odd subchain map is a product of shorter odd subchain maps and elements of $G_g$. Hence, it suffices to show that $[1, 3, 5, 7, 9, \dots ]$, $[2, 4, 6, 8, 10, \dots ]$, $[1, 2, 3, 5, 7, \dots ]$, $[1, 2, 4, 6, 8, \dots ]$, and $[1, 2, 3, 4]$ are elements of $G_g$. By (1) of Lemma 3.9, the second ones are changed to the first ones, and the third ones are changed to the fourth ones by the action of $G_g$. On the other hand, we have already shown that $[1, 3, 5, 7, 9, \dots ]$, $[1, 2, 4, 6, 8, \dots ]$, and $[1, 2, 3, 4]$ are elements of $G_g$ in Lemma 3.6. Therefore, Lemma 3.3 is proved.

### 3.3 The level 2 prime congruence subgroup of Sp $(2g, \mathbb{Z})$

In this subsection, we assume $g \geq 3$. Let $\Phi_2$ be the natural homomorphism from $\mathcal{M}_g$ to $\mathrm{Sp}(2g, \mathbb{Z}_2)$ defined by the action of $\mathcal{M}_g$ on the $\mathbb{Z}_2$-coefficient first homology group $H_1(\Sigma_g; \mathbb{Z}_2)$. In this section, we show the following lemma.

**Lemma 3.10** $\ker\Phi_2$ *is a subgroup of* $G_g$.

We denote the kernel of the natural homomorphism from $\mathrm{Sp}(2g,\mathbb{Z})$ to $\mathrm{Sp}(2g,\mathbb{Z}_2)$ by $\mathrm{Sp}^{(2)}(2g)$. We set a basis of $H_1(\Sigma_g;\mathbb{Z})$ as in Figure 4, and define the intersection form $(,)$ on $H_1(\Sigma_g;\mathbb{Z})$ to satisfy $(x_i,y_j)=\delta_{i,j}$, $(x_i,x_j)=(y_i,y_j)=0$ $(1\le i,j,\le g)$. An element $a$ of $H_1(\Sigma_g;\mathbb{Z})$ is called *primitive* if there is no element $n(\neq 0,\pm 1)$ of $\mathbb{Z}$, and no element $b$ of $H_1(\Sigma_g;\mathbb{Z})$ such that $a=nb$. For a primitive element $a$ of $H_1(\Sigma_g;\mathbb{Z})$, we define an isomorphism $T_a\colon H_1(\Sigma_g;\mathbb{Z})\to H_1(\Sigma_g;\mathbb{Z})$ by $T_a(v)=v+(a,v)a$. This isomorphism is the same as the action of Dehn twist about a simple closed curve representing $a$ on $H_1(\Sigma_g;\mathbb{Z})$. We call $T_a^2$ *the square transvection about* $a$. Johnson [8] showed the following result.

**Lemma 3.11** *$Sp^{(2)}(2g)$ is generated by square transvections.*

$\mathrm{Sp}^{(2)}(2g)$ is finitely generated. In fact, we show:

**Lemma 3.12** *$Sp^{(2)}(2g)$ is generated by the square transvections about the primitive elements $\sum_{i=1}^{g}(\epsilon_i x_i+\delta_i y_i)$, where $\epsilon_i=0,1$ and $\delta_i=0,1$.*

We define, for any primitive element $a$ and $b$ of $H_1(\Sigma_g;\mathbb{Z})$, two operation $\boxplus$ and $\boxminus$ by

$$a\boxplus b=a+2(a,b)b,\quad a\boxminus b=a-2(a,b)b.$$

We remark that $T^2_{a\boxplus b}=T_b^{-2}T_a^2T_b^2$, $T^2_{a\boxminus b}=T_b^2T_a^2T_b^{-2}$, and $(a\boxplus b)\boxminus b=a=(a\boxminus b)\boxplus b$. We denote the element $\sum_{i=1}^{g}(a_i^1x_i+a_i^2y_i)$ of $H_1(\Sigma_g;\mathbb{Z})$ by $[(a_1^1,a_1^2),(a_2^1,a_2^2),\cdots,(a_g^1,a_g^2)]$, and call each $(a_i^1,a_i^2)$ as *a block*. For a positive integer $k$, $a(\boxplus b)^k$ is the result of the $k$-fold application of $\boxplus b$ on $a$, and $a(\boxplus b)^{-k}$ is the result of the $k$-fold application of $\boxminus b$ on $a$.

**Lemma 3.13** *For any primitive element $a$ of $H_1(\Sigma_g;\mathbb{Z})$, by applying $\boxplus[(0,0),\dots,(0,0),(1,0),(0,0),\dots,(0,0)]$ or $\boxplus[(0,0),\dots,(0,0),(0,1),(0,0),\dots,(0,0)]$ several times, each block of $a$ is altered to $(0,0)$, $(p,0)$, $(0,p)$, or $(p,p)$.*

**Proof** Let $(m,n)$ be the $i$-th block of $a$. First we consider the case when $|m|>|n|\neq 0$. There is an integer $k$ such that $|m-2kn|\le|n|$. Let $e_i$ be the element of $H_1(\Sigma_g;\mathbb{Z})$, the $i$-th block of which is $(1,0)$, and every other block of which is $(0,0)$. Since, $[\cdots,(m,n),\cdots]\boxplus e_i=[\cdots,(m-2n,n),\cdots]$, and $[\cdots,(m,n),\cdots]\boxminus e_i=[\cdots,(m+2n,n),\cdots]$, we get $[\cdots,(m,n),\cdots](\boxplus e_i)^k=[\cdots,(m-2kn,n),\cdots]$. This means that, by repeated application of $\boxplus e_i$, the $i$-th block $(m,n)$ is altered such that $|m|\le|n|$. Next, we consider the case when

$0 \neq |m| < |n|$. Let $f_i$ be the element of $H_1(\Sigma_g;\mathbb{Z})$, the $i$-th block of which is $(0,1)$, and other blocks of which are $(0,0)$. Since, $[\cdots,(m,n),\cdots] \boxplus f_i = [\cdots,(m,n+2m),\cdots]$, and $[\cdots,(m,n),\cdots] \boxminus f_i = [\cdots,(m,n-2m),\cdots]$, by the same argument as the previous case, by repeated application of $\boxplus f_i$, the $i$-th block is altered such that $|m| \geq |n|$. The above arguments show that, after several application of $\boxplus e_i$ or $\boxplus f_i$, the $i$-th block $(m,n)$ of $a$ is altered to be $|m| = |n|$, or $m = 0$, or $n = 0$. If $n = -m$, the $i$-th block changed to $(m,m)$ by the application of $\boxplus f_i$. For each $i$-th block, we do the same operation as above. Then, this lemma follows. □

For a primitive element of $H_1(\Sigma_g;\mathbb{Z})$, each of whose blocks is $(p,0)$, or $(0,p)$, or $(p,p)$, (where $p$ can be different from block to block) we apply several operations $\boxplus[\ldots,(\epsilon_i,\delta_i),\ldots]$, where $\epsilon_i = 0,1$ and $\delta_i = 0,1$. Then we obtain the following equations, where $\circ\circ\circ$ means a sequence of $(0,0)$, and $\bullet\bullet\bullet$ means the part which is not changed.

$$\begin{aligned}
&[\bullet\bullet\bullet,(p,0),(q,0),\bullet\bullet\bullet] \boxminus [\circ\circ\circ,(1,0),(0,1),\circ\circ\circ] \boxplus [\circ\circ\circ,(0,0),(0,1),\circ\circ\circ] \\
&\qquad = [\bullet\bullet\bullet,(p-2q,0),(q,0),\bullet\bullet\bullet], \\
&[\bullet\bullet\bullet,(p,0),(q,0),\bullet\bullet\bullet] \boxplus [\circ\circ\circ,(1,0),(0,1),\circ\circ\circ] \boxminus [\circ\circ\circ,(0,0),(0,1),\circ\circ\circ] \\
&\qquad = [\bullet\bullet\bullet,(p+2q,0),(q,0),\bullet\bullet\bullet], \\
&[\bullet\bullet\bullet,(p,0),(q,0),\bullet\bullet\bullet] \boxminus [\circ\circ\circ,(0,1),(1,0),\circ\circ\circ] \boxplus [\circ\circ\circ,(0,1),(0,0),\circ\circ\circ] \\
&\qquad = [\bullet\bullet\bullet,(p,0),(q-2p,0),\bullet\bullet\bullet], \\
&[\bullet\bullet\bullet,(p,0),(q,0),\bullet\bullet\bullet] \boxplus [\circ\circ\circ,(0,1),(1,0),\circ\circ\circ] \boxplus [\circ\circ\circ,(0,1),(0,0),\circ\circ\circ] \\
&\qquad = [\bullet\bullet\bullet,(p,0),(q+2p,0),\bullet\bullet\bullet],
\end{aligned}$$

$$\begin{aligned}
&[\bullet\bullet\bullet,(0,p),(0,q),\bullet\bullet\bullet] \boxplus [\circ\circ\circ,(0,1),(1,0),\circ\circ\circ] \boxminus [\circ\circ\circ,(0,0),(1,0),\circ\circ\circ] \\
&\qquad = [\bullet\bullet\bullet,(0,p-2q),(0,q),\bullet\bullet\bullet], \\
&[\bullet\bullet\bullet,(0,p),(0,q),\bullet\bullet\bullet] \boxminus [\circ\circ\circ,(0,1),(1,0),\circ\circ\circ] \boxplus [\circ\circ\circ,(0,0),(1,0),\circ\circ\circ] \\
&\qquad = [\bullet\bullet\bullet,(0,p+2q),(0,q),\bullet\bullet\bullet], \\
&[\bullet\bullet\bullet,(0,p),(0,q),\bullet\bullet\bullet] \boxplus [\circ\circ\circ,(1,0),(0,1),\circ\circ\circ] \boxminus [\circ\circ\circ,(1,0),(0,0),\circ\circ\circ] \\
&\qquad = [\bullet\bullet\bullet,(0,p),(0,q-2p),\bullet\bullet\bullet], \\
&[\bullet\bullet\bullet,(0,p),(0,q),\bullet\bullet\bullet] \boxminus [\circ\circ\circ,(1,0),(0,1),\circ\circ\circ] \boxplus [\circ\circ\circ,(1,0),(0,0),\circ\circ\circ] \\
&\qquad = [\bullet\bullet\bullet,(0,p),(0,q+2p),\bullet\bullet\bullet],
\end{aligned}$$

$$[\bullet\bullet\bullet,(p,0),(0,q),\bullet\bullet\bullet] \boxplus [\circ\circ\circ,(1,0),(1,0),\circ\circ\circ] \boxminus [\circ\circ\circ,(0,0),(1,0),\circ\circ\circ]$$

$$= [\bullet\bullet\bullet, (p-2q,0), (0,q), \bullet\bullet\bullet],$$

$$\begin{aligned}
&[\bullet\bullet\bullet,(p,0),(0,q),\bullet\bullet\bullet] \boxminus [\circ\circ\circ,(1,0),(1,0),\circ\circ\circ] \boxplus [\circ\circ\circ,(0,0),(1,0),\circ\circ\circ] \\
&\qquad = [\bullet\bullet\bullet, (p+2q,0), (0,q), \bullet\bullet\bullet], \\
&[\bullet\bullet\bullet,(p,0),(0,q),\bullet\bullet\bullet] \boxminus [\circ\circ\circ,(0,1),(0,1),\circ\circ\circ] \boxplus [\circ\circ\circ,(0,1),(0,0),\circ\circ\circ] \\
&\qquad = [\bullet\bullet\bullet, (p,0), (0,q-2p), \bullet\bullet\bullet], \\
&[\bullet\bullet\bullet,(p,0),(0,q),\bullet\bullet\bullet] \boxplus [\circ\circ\circ,(0,1),(0,1),\circ\circ\circ] \boxplus [\circ\circ\circ,(0,1),(0,0),\circ\circ\circ] \\
&\qquad = [\bullet\bullet\bullet, (p,0), (0,q+2p), \bullet\bullet\bullet],
\end{aligned}$$

$$\begin{aligned}
&[\bullet\bullet\bullet,(0,p),(q,0),\bullet\bullet\bullet] \boxminus [\circ\circ\circ,(0,1),(0,1),\circ\circ\circ] \boxplus [\circ\circ\circ,(0,0),(0,1),\circ\circ\circ] \\
&\qquad = [\bullet\bullet\bullet, (0,p-2q), (q,0), \bullet\bullet\bullet], \\
&[\bullet\bullet\bullet,(0,p),(q,0),\bullet\bullet\bullet] \boxplus [\circ\circ\circ,(0,1),(0,1),\circ\circ\circ] \boxminus [\circ\circ\circ,(0,0),(0,1),\circ\circ\circ] \\
&\qquad = [\bullet\bullet\bullet, (0,p+2q), (q,0), \bullet\bullet\bullet], \\
&[\bullet\bullet\bullet,(0,p),(q,0),\bullet\bullet\bullet] \boxplus [\circ\circ\circ,(1,0),(1,0),\circ\circ\circ] \boxminus [\circ\circ\circ,(1,0),(0,0),\circ\circ\circ] \\
&\qquad = [\bullet\bullet\bullet, (0,p), (q-2p,0), \bullet\bullet\bullet], \\
&[\bullet\bullet\bullet,(0,p),(q,0),\bullet\bullet\bullet] \boxminus [\circ\circ\circ,(1,0),(1,0),\circ\circ\circ] \boxplus [\circ\circ\circ,(1,0),(0,0),\circ\circ\circ] \\
&\qquad = [\bullet\bullet\bullet, (0,p), (q+2p,0), \bullet\bullet\bullet],
\end{aligned}$$

$$\begin{aligned}
&[\bullet\bullet\bullet,(0,p),(q,q),\bullet\bullet\bullet] \boxminus [\circ\circ\circ,(0,1),(0,1),\circ\circ\circ] \boxplus [\circ\circ\circ,(0,0),(0,1),\circ\circ\circ] \\
&\qquad = [\bullet\bullet\bullet, (0,p-2q), (q,q), \bullet\bullet\bullet], \\
&[\bullet\bullet\bullet,(0,p),(q,q),\bullet\bullet\bullet] \boxplus [\circ\circ\circ,(0,1),(0,1),\circ\circ\circ] \boxminus [\circ\circ\circ,(0,0),(0,1),\circ\circ\circ] \\
&\qquad = [\bullet\bullet\bullet, (0,p+2q), (q,q), \bullet\bullet\bullet], \\
&[\bullet\bullet\bullet,(0,p),(q,q),\bullet\bullet\bullet] \boxplus [\circ\circ\circ,(1,0),(1,1),\circ\circ\circ] \boxminus [\circ\circ\circ,(1,0),(0,0),\circ\circ\circ] \\
&\qquad = [\bullet\bullet\bullet, (0,p), (q-2p,q-2p), \bullet\bullet\bullet], \\
&[\bullet\bullet\bullet,(0,p),(q,q),\bullet\bullet\bullet] \boxminus [\circ\circ\circ,(1,0),(1,1),\circ\circ\circ] \boxplus [\circ\circ\circ,(1,0),(0,0),\circ\circ\circ] \\
&\qquad = [\bullet\bullet\bullet, (0,p), (q+2p,q+2p), \bullet\bullet\bullet],
\end{aligned}$$

$$\begin{aligned}
&[\bullet\bullet\bullet,(p,p),(0,q),\bullet\bullet\bullet] \boxplus [\circ\circ\circ,(1,1),(1,0),\circ\circ\circ] \boxminus [\circ\circ\circ,(0,0),(1,0),\circ\circ\circ] \\
&\qquad = [\bullet\bullet\bullet, (p-2q,p-2q), (0,q), \bullet\bullet\bullet], \\
&[\bullet\bullet\bullet,(p,p),(0,q),\bullet\bullet\bullet] \boxminus [\circ\circ\circ,(1,1),(1,0),\circ\circ\circ] \boxplus [\circ\circ\circ,(0,0),(1,0),\circ\circ\circ] \\
&\qquad = [\bullet\bullet\bullet, (p+2q,p+2q), (0,q), \bullet\bullet\bullet], \\
&[\bullet\bullet\bullet,(p,p),(0,q),\bullet\bullet\bullet] \boxminus [\circ\circ\circ,(0,1),(0,1),\circ\circ\circ] \boxplus [\circ\circ\circ,(0,1),(0,0),\circ\circ\circ] \\
&\qquad = [\bullet\bullet\bullet, (p,p), (0,q-2p), \bullet\bullet\bullet],
\end{aligned}$$

$$\begin{aligned}
&[\bullet\bullet\bullet,(p,p),(0,q),\bullet\bullet\bullet]\boxplus[\circ\circ\circ,(0,1),(0,1),\circ\circ\circ]\boxminus[\circ\circ\circ,(0,1),(0,0),\circ\circ\circ]\\
&\qquad=[\bullet\bullet\bullet,(p,p),(0,q+2p),\bullet\bullet\bullet],
\end{aligned}$$

$$\begin{aligned}
&[\bullet\bullet\bullet,(p,0),(q,q),\bullet\bullet\bullet]\boxminus[\circ\circ\circ,(1,0),(0,1),\circ\circ\circ]\boxplus[\circ\circ\circ,(0,0),(0,1),\circ\circ\circ]\\
&\qquad=[\bullet\bullet\bullet,(p-2q,0),(q,q),\bullet\bullet\bullet],\\
&[\bullet\bullet\bullet,(p,0),(q,q),\bullet\bullet\bullet]\boxplus[\circ\circ\circ,(1,0),(0,1),\circ\circ\circ]\boxminus[\circ\circ\circ,(0,0),(0,1),\circ\circ\circ]\\
&\qquad=[\bullet\bullet\bullet,(p+2q,0),(q,q),\bullet\bullet\bullet],\\
&[\bullet\bullet\bullet,(p,0),(q,q),\bullet\bullet\bullet]\boxminus[\circ\circ\circ,(0,1),(1,1),\circ\circ\circ]\boxplus[\circ\circ\circ,(0,1),(0,0),\circ\circ\circ]\\
&\qquad=[\bullet\bullet\bullet,(p,0),(q-2p,q-2p),\bullet\bullet\bullet],\\
&[\bullet\bullet\bullet,(p,0),(q,q),\bullet\bullet\bullet]\boxplus[\circ\circ\circ,(0,1),(1,1),\circ\circ\circ]\boxminus[\circ\circ\circ,(0,1),(0,0),\circ\circ\circ]\\
&\qquad=[\bullet\bullet\bullet,(p,0),(q+2p,q+2p),\bullet\bullet\bullet],
\end{aligned}$$

$$\begin{aligned}
&[\bullet\bullet\bullet,(p,p),(q,0),\bullet\bullet\bullet]\boxminus[\circ\circ\circ,(1,1),(0,1),\circ\circ\circ]\boxplus[\circ\circ\circ,(0,0),(0,1),\circ\circ\circ]\\
&\qquad=[\bullet\bullet\bullet,(p-2q,p-2q),(q,0),\bullet\bullet\bullet],\\
&[\bullet\bullet\bullet,(p,p),(q,0),\bullet\bullet\bullet]\boxplus[\circ\circ\circ,(1,1),(0,1),\circ\circ\circ]\boxminus[\circ\circ\circ,(0,0),(0,1),\circ\circ\circ]\\
&\qquad=[\bullet\bullet\bullet,(p+2q,p+2q),(q,0),\bullet\bullet\bullet],\\
&[\bullet\bullet\bullet,(p,p),(q,0),\bullet\bullet\bullet]\boxminus[\circ\circ\circ,(0,1),(1,0),\circ\circ\circ]\boxplus[\circ\circ\circ,(0,1),(0,0),\circ\circ\circ]\\
&\qquad=[\bullet\bullet\bullet,(p,p),(q-2p,0),\bullet\bullet\bullet],\\
&[\bullet\bullet\bullet,(p,p),(q,0),\bullet\bullet\bullet]\boxplus[\circ\circ\circ,(0,1),(1,0),\circ\circ\circ]\boxminus[\circ\circ\circ,(0,1),(0,0),\circ\circ\circ]\\
&\qquad=[\bullet\bullet\bullet,(p,p),(q+2p,0),\bullet\bullet\bullet],
\end{aligned}$$

$$\begin{aligned}
&[\bullet\bullet\bullet,(p,p),(q,q),\bullet\bullet\bullet]\boxminus[\circ\circ\circ,(1,1),(0,1),\circ\circ\circ]\boxplus[\circ\circ\circ,(0,0),(0,1),\circ\circ\circ]\\
&\qquad=[\bullet\bullet\bullet,(p-2q,p-2q),(q,q),\bullet\bullet\bullet],\\
&[\bullet\bullet\bullet,(p,p),(q,q),\bullet\bullet\bullet]\boxplus[\circ\circ\circ,(1,1),(0,1),\circ\circ\circ]\boxminus[\circ\circ\circ,(0,0),(0,1),\circ\circ\circ]\\
&\qquad=[\bullet\bullet\bullet,(p+2q,p+2),(q,q),\bullet\bullet\bullet],\\
&[\bullet\bullet\bullet,(p,p),(q,q),\bullet\bullet\bullet]\boxminus[\circ\circ\circ,(0,1),(1,1),\circ\circ\circ]\boxplus[\circ\circ\circ,(0,1),(0,0),\circ\circ\circ]\\
&\qquad=[\bullet\bullet\bullet,(p,p),(q-2p,q-2p),\bullet\bullet\bullet],\\
&[\bullet\bullet\bullet,(p,p),(q,q),\bullet\bullet\bullet]\boxplus[\circ\circ\circ,(0,1),(1,1),\circ\circ\circ]\boxminus[\circ\circ\circ,(0,1),(0,0),\circ\circ\circ]\\
&\qquad=[\bullet\bullet\bullet,(p,p),(q+2p,q+2p),\bullet\bullet\bullet].
\end{aligned}$$

Therefore, by the same argument as the proof of Lemma 3.13, we obtain:

**Lemma 3.14** *For any primitive element $a$ of $H_1(\Sigma_g;\mathbb{Z})$, by applying $\boxplus[(\epsilon_1,\delta_1),\cdots,(\epsilon_g,\delta_g)]$ (where $\epsilon_i = 0,1$, and $\delta_i = 0,1$) several times, $a$ is* *deformed to* $\boxplus[(\epsilon_1,\delta_1),\cdots,(\epsilon_g,\delta_g)]$ *(where* $\epsilon_i = 0,1$*, and* $\delta_i = 0,1$*) or* $[\circ\circ\circ,(-1,0),\circ\circ\circ]$. □

Since $T_{-a}^2(v) = v + 2(-a,v)(-v) = v + 2(a,v)v = T_a^2(v)$, we do not need to consider the elements $[\circ\circ\circ,(-1,0),\circ\circ\circ]$. Hence, Lemma 3.12 follows.

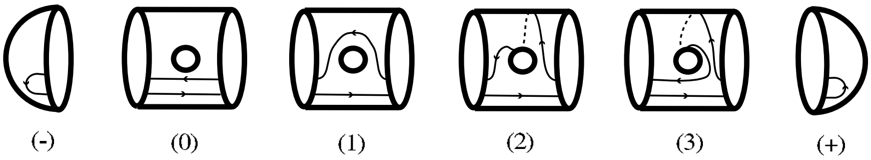

Figure 21

For each element $[(\epsilon_1,\delta_1),\cdots,(\epsilon_g,\delta_g)]$ (where $\epsilon_i = 0,1$, $\delta_i = 0,1$) of $H_1(\Sigma_g;\mathbb{Z})$, we construct an oriented simple close curve on $\Sigma_g$ which represent this homology class. For each $i$-th block, if $(\epsilon_i,\delta_i) = (0,0)$, we prepare (0) of Figure 21, if $(\epsilon_i,\delta_i) = (0,1)$, we prepare (1) of Figure 21, if $(\epsilon_i,\delta_i) = (1,1)$, we prepare (2) of Figure 21, if $(\epsilon_i,\delta_i) = (1,0)$, we prepare (3) of Figure 21. After that, we glue them along the boundaries and cap the left boundary component by (-) of Figure 21 and the right boundary component by (+) of Figure 21. We denote this oriented simple closed curve on $\Sigma_g$ by $\{(\epsilon_1,\delta_1),\cdots,(\epsilon_g,\delta_g)\}$. Here, we remark that the action of $T_{\{(\epsilon_1,\delta_1),\cdots,(\epsilon_g,\delta_g)\}}$ on $H_1(\Sigma_g;\mathbb{Z})$ equals $T_{[(\epsilon_1,\delta_1),\cdots,(\epsilon_g,\delta_g)]}$, and, for any $\phi$ of $\mathcal{M}_g$, $\phi\circ T_{\{(\epsilon_1,\delta_1),\cdots,(\epsilon_g,\delta_g)\}}\circ\phi^{-1} = T_{\phi(\{(\epsilon_1,\delta_1),\cdots,(\epsilon_g,\delta_g)\})}$.

**Lemma 3.15** *For any* $\{(\epsilon_1,\delta_1),\cdots,(\epsilon_g,\delta_g)\}$*, there is an element* $\phi$ *of* $G_g$ *such that*

$$\begin{aligned}\phi(\{(\epsilon_1,\delta_1),\cdots,(\epsilon_g,\delta_g)\}) &= \{(0,1),(0,0),(0,0),\cdots,(0,0)\}\\ \textit{or } &= \{(1,1),(0,0),(0,0),\cdots,(0,0)\}\\ \textit{or } &= \{(0,0),(1,1),(0,0),\cdots,(0,0)\}.\end{aligned}$$

**Proof** If the $i$-th block is (3), by the action of $\overline{Y_{2i}}$ , this block is changed to (1). Therefore, it suffices to show this lemma in the case when each block is not (3). First we investigate actions of elements of $G_g$ on adjacent blocks, say the $i$-th block and the $i+1$-st block. Each picture of Figure 22 shows the action

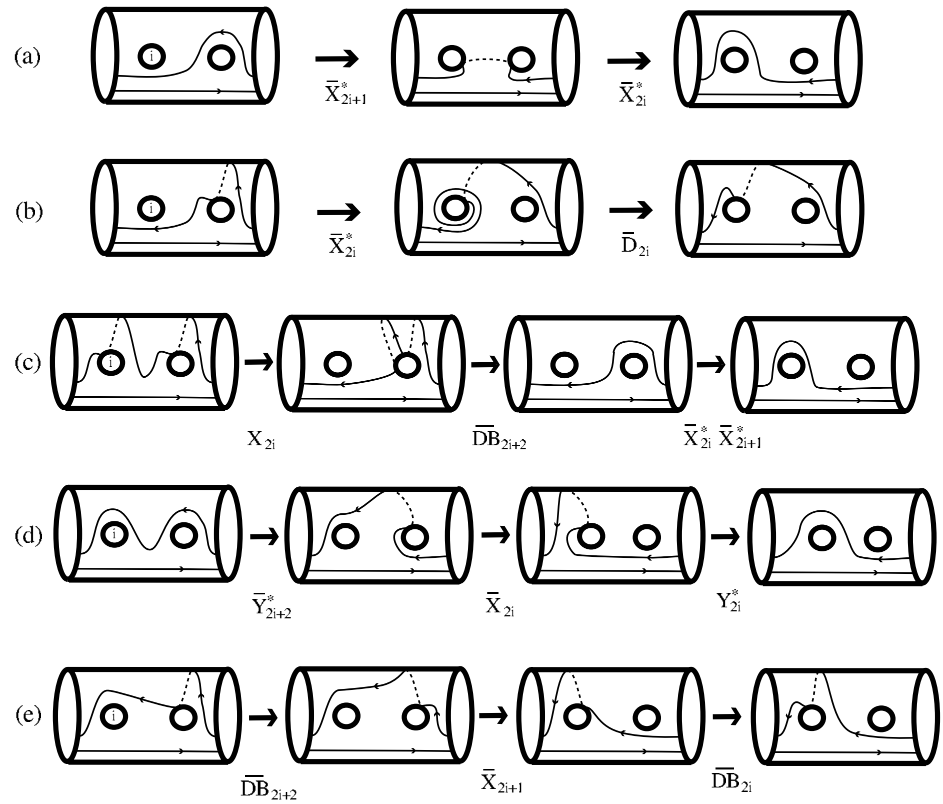

Figure 22

of $G_g$ on this adjacent blocks.

$(a)$ shows $\{\bullet\bullet\bullet,(0,0),(0,1),\bullet\bullet\bullet\} \underset{G_g}{\sim} \{\bullet\bullet\bullet,(0,1),(0,0),\bullet\bullet\bullet\}$,

$(b)$ shows $\{\bullet\bullet\bullet,(0,0),(1,1),\bullet\bullet\bullet\} \underset{G_g}{\sim} \{\bullet\bullet\bullet,(1,1),(0,1),\bullet\bullet\bullet\}$,

$(c)$ shows $\{\bullet\bullet\bullet,(1,1),(1,1),\bullet\bullet\bullet\} \underset{G_g}{\sim} \{\bullet\bullet\bullet,(0,1),(0,0),\bullet\bullet\bullet\}$,

$(d)$ shows $\{\bullet\bullet\bullet,(0,1),(0,1),\bullet\bullet\bullet\} \underset{G_g}{\sim} \{\bullet\bullet\bullet,(0,1),(0,0),\bullet\bullet\bullet\}$,

$(e)$ shows $\{\bullet\bullet\bullet,(0,1),(1,1),\bullet\bullet\bullet\} \underset{G_g}{\sim} \{\bullet\bullet\bullet,(1,1),(0,0),\bullet\bullet\bullet\}$.

For an oriented simple closed curve $x = \{(\epsilon_1,\delta_1),\cdots,(\epsilon_g,\delta_g)\}$, each of whose block is $(0,0)$ or $(0,1)$ or $(1,1)$, let the right most non-$(0,0)$ block be the $j$-th block. By the induction on $j$, we show that $x$ is $G_g$-equivalent to $\{(0,1),(0,0),(0,0),\cdots,(0,0)\}$ or $\{(1,1),(0,0),(0,0),\cdots,(0,0)\}$ or $\{(0,0),(1,1),(0,0),\cdots,$

$(0,0)\}$. If $j = 1$, it is trivial.
*When the $j$-th block is* $(0,1)$. If each block between the first block and the $(j-1)$-st block is $(0,0)$, then, by repeated application of (a), $x$ is $G_g$-equivalent to $\{(0,1),(0,0),\cdots,(0,0)\}$. If there is a block between the first block and the $(j-1)$-st block which is not $(0,0)$, by the induction hypothesis, the sequence from the first block to the $(j-1)$-st block is $G_g$-equivalent to $(0,1),(0,0),(0,0),\cdots,(0,0)$ or $(1,1),(0,0),(0,0),\cdots,(0,0)$ or $(0,0),(1,1),(0,0),\cdots,(0,0)$. In the first case,

$$\begin{aligned}
x &\underset{G_g}{\sim} \{(0,1),(0,0),(0,0),\cdots,(0,0),(0,1),\cdots,(0,0)\}(\text{ by the hypothesis })\\
&\underset{G_g}{\sim} \{(0,1),(0,1),(0,0),\cdots,(0,0),(0,0),\cdots,(0,0)\}(\text{ by (a) })\\
&\underset{G_g}{\sim} \{(0,1),(0,0),(0,0),\cdots,(0,0),(0,0),\cdots,(0,0)\}(\text{ by (d) }).
\end{aligned}$$

In the second case,

$$\begin{aligned}
x &\underset{G_g}{\sim} \{(1,1),(0,0),(0,0),\cdots,(0,0),(0,1),\cdots,(0,0)\}(\text{ by the hypothesis })\\
&\underset{G_g}{\sim} \{(1,1),(0,1),(0,0),\cdots,(0,0),(0,0),\cdots,(0,0)\}(\text{ by (a) })\\
&\underset{G_g}{\sim} \{(0,0),(1,1),(0,0),\cdots,(0,0),(0,0),\cdots,(0,0)\}(\text{ by (b) }).
\end{aligned}$$

In the third case,

$$\begin{aligned}
x &\underset{G_g}{\sim} \{(0,0),(1,1),(0,0),\cdots,(0,0),(0,1),\cdots,(0,0)\}(\text{ by the hypothesis })\\
&\underset{G_g}{\sim} \{(0,0),(1,1),(0,1),\cdots,(0,0),(0,0),\cdots,(0,0)\}(\text{ by (a) })\\
&\underset{G_g}{\sim} \{(1,1),(0,1),(0,1),\cdots,(0,0),(0,0),\cdots,(0,0)\}(\text{ by (b) })\\
&\underset{G_g}{\sim} \{(1,1),(0,1),(0,0),\cdots,(0,0),(0,0),\cdots,(0,0)\}(\text{ by (d) })\\
&\underset{G_g}{\sim} \{(0,0),(1,1),(0,0),\cdots,(0,0),(0,0),\cdots,(0,0)\}(\text{ by (b) }).
\end{aligned}$$

*When the $j$-th block is* $(1,1)$. If every block between the first block and $(j-1)$-st block is $(0,0)$, then,

$$\begin{aligned}
x &\underset{G_g}{\sim} \{(1,1),(0,1),(0,1)\cdots,(0,1),\cdots,(0,0)\}(\text{ by (b) })\\
&\underset{G_g}{\sim} \{(1,1),(0,1),(0,0),\cdots,(0,0),\cdots,(0,0)\}(\text{ by (d) })\\
&\underset{G_g}{\sim} \{(0,0),(1,1),(0,0),\cdots,(0,0),\cdots,(0,0)\}(\text{ by (b) })
\end{aligned}$$

If there is a block between the first block and the $(j-1)$-st block which is not $(0,0)$, by the induction hypothesis, the sequence from the first block to the $(j-1)$-st block is $G_g$-equivalent to $(0,1),(0,0),(0,0),\cdots,(0,0)$ or $(1,1),(0,0),(0,0),\cdots,(0,0)$ or $(0,0),(1,1),(0,0),\cdots,(0,0)$. In the first case,

$$\begin{aligned}
x &\underset{G_g}{\sim} \{(0,1),(0,0),(0,0),(0,0),\cdots,(0,0),(1,1),\cdots,(0,0)\}(\text{ by the hypothesis })\\
&\underset{G_g}{\sim} \{(0,1),(1,1),(0,1),(0,1),\cdots,(0,1),(0,1),\cdots,(0,0)\}(\text{ by (b) })\\
&\underset{G_g}{\sim} \{(0,1),(1,1),(0,1),(0,0),\cdots,(0,0),(0,0),\cdots,(0,0)\}(\text{ by (d) })\\
&\underset{G_g}{\sim} \{(1,1),(0,0),(0,1),(0,0),\cdots,(0,0),(0,0),\cdots,(0,0)\}(\text{ by (e) })\\
&\underset{G_g}{\sim} \{(1,1),(0,1),(0,0),(0,0),\cdots,(0,0),(0,0),\cdots,(0,0)\}(\text{ by (a) })\\
&\underset{G_g}{\sim} \{(0,0),(1,1),(0,0),(0,0),\cdots,(0,0),(0,0),\cdots,(0,0)\}(\text{ by (b) }).
\end{aligned}$$

In the second case,

$$\begin{aligned}
x &\underset{G_g}{\sim} \{(1,1),(0,0),(0,0),(0,0),\cdots,(0,0),(1,1),\cdots,(0,0)\}(\text{ by the hypothesis })\\
&\underset{G_g}{\sim} \{(1,1),(1,1),(0,1),(0,1),\cdots,(0,1),(0,1),\cdots,(0,0)\}(\text{ by (b) })\\
&\underset{G_g}{\sim} \{(1,1),(1,1),(0,1),(0,0),\cdots,(0,0),(0,0),\cdots,(0,0)\}(\text{ by (d) })\\
&\underset{G_g}{\sim} \{(0,1),(0,0),(0,1),(0,0),\cdots,(0,0),(0,0),\cdots,(0,0)\}(\text{ by (c) })\\
&\underset{G_g}{\sim} \{(0,1),(0,1),(0,0),(0,0),\cdots,(0,0),(0,0),\cdots,(0,0)\}(\text{ by (a) })\\
&\underset{G_g}{\sim} \{(0,1),(0,0),(0,0),(0,0),\cdots,(0,0),(0,0),\cdots,(0,0)\}(\text{ by (d) }).
\end{aligned}$$

In the third case,

$$\begin{aligned}
x &\underset{G_g}{\sim} \{(0,0),(1,1),(0,0),(0,0),\cdots,(0,0),(1,1),\cdots,(0,0)\}(\text{ by the hypothesis })\\
&\underset{G_g}{\sim} \{(0,0),(1,1),(1,1),(0,1),\cdots,(0,1),(0,1),\cdots,(0,0)\}(\text{ by (b) })\\
&\underset{G_g}{\sim} \{(0,0),(0,1),(0,0),(0,1),\cdots,(0,1),(0,1),\cdots,(0,0)\}(\text{ by (c) })\\
&\underset{G_g}{\sim} \{(0,0),(0,1),(0,0),(0,1),\cdots,(0,0),(0,0),\cdots,(0,0)\}(\text{ by (d) })\\
&\underset{G_g}{\sim} \{(0,1),(0,1),(0,0),(0,0),\cdots,(0,0),(0,0),\cdots,(0,0)\}(\text{ by (a) })\\
&\underset{G_g}{\sim} \{(0,1),(0,0),(0,0),(0,0),\cdots,(0,0),(0,0),\cdots,(0,0)\}(\text{ by (d) }).
\end{aligned}$$

□

By the fact that $T^2_{\{(0,1),(0,0),\cdots,(0,0)\}} = D_2$, $T^2_{\{(1,1),(0,0),\cdots,(0,0)\}} = (X_1^*)^2$, $T^2_{\{(0,0),(1,1),\cdots,(0,0)\}} = (Y_2^*)^2$, and Lemma 3.3, Lemma 3.10 is proved.

### 3.4 The modulo 2 orthogonal group

In this subsection, we assume $g \geq 3$. As in the previous subsection, let $\Phi_2\colon \mathcal{M}_g \to \mathrm{Sp}(2g, \mathbb{Z}_2)$ be the natural homomorphism. Let $q\colon H_1(\Sigma_g;\mathbb{Z}_2) \to \mathbb{Z}_2$ be the quadratic form associated with the intersection form $(,)_2$ of $H_1(\Sigma_g;\mathbb{Z}_2)$ which satisfies $q(x_i) = q(y_i) = 0$ for the basis $x_i, y_i$ of $H_1(\Sigma_g;\mathbb{Z}_2)$ indicated on Figure 4. We define $\mathrm{O}(2g,\mathbb{Z}_2) = \{\phi \in \mathrm{Aut}(H_1(\Sigma_g;\mathbb{Z}_2)) | q(\phi(x)) = q(x)$ for any $x \in H_1(\Sigma_g;\mathbb{Z}_2)\}$, then $\mathcal{SP}_g = \Phi_2^{-1}(\mathrm{O}(2g,\mathbb{Z}_2))$. Because of Lemma 3.10, if we show $\Phi_2(G_g) = \mathrm{O}(2g,\mathbb{Z}_2)$, then $G_g = \mathcal{SP}_g$ follows. For any $z \in H_1(\Sigma_g;\mathbb{Z}_2)$ such that $q(z) = 1$, we define $\mathbb{T}_z(x) = x + (z,x)_2\, z$. Then $\mathbb{T}_z$ is an element of $\mathrm{O}(2g,\mathbb{Z}_2)$, and we call this a *$\mathbb{Z}_2$-transvection about $z$*. Dieudonné [2] showed the following theorem.

**Theorem 3.16** [2, Proposition 14 on p.42] *When $g \geq 3$, $O(2g,\mathbb{Z}_2)$ is generated by $\mathbb{Z}_2$-transvections.*

Let $\Lambda_g$ be the set of $z$ of $H_1(\Sigma_g;\mathbb{Z}_2)$ such that $q(z) = 1$. For any elements $z_1$ and $z_2$ of $\Lambda_g$, we define $z_1 \Box z_2 = z_1 + (z_2, z_1)_2\, z_2$. Here, we remark that $\mathbb{T}_{z_1}^2 = \mathrm{id}$, $\mathbb{T}_{z_2}\mathbb{T}_{z_1}\mathbb{T}_{z_2}^{-1} = \mathbb{T}_{z_1 \Box z_2}$ and $z_1 \Box z_2 \Box z_2 = z_1$. We denote an element $\epsilon_1 x_1 + \delta_1 y_1 + \cdots + \epsilon_g x_g + \delta_g y_g$ of $H_1(\Sigma_g;\mathbb{Z}_2)$ by $[(\epsilon_1,\delta_1),\cdots,(\epsilon_g,\delta_g)]$, and call each $(\epsilon_i,\delta_i)$ the $i$-th block. $\Lambda_g$ is a set finitely generated by the operation $\Box$. In fact, we have:

**Lemma 3.17** *Under the operation $\Box$, $\Lambda_g$ is generated by $x_i + y_i$ $(1 \leq i \leq g)$, $x_i + y_i + x_{i+1}$ $(1 \leq i \leq g-1)$, and $x_i + x_{i+1} + y_{i+1}$ $(1 \leq i \leq g-1)$.*

**Proof** For an element $[(\epsilon_1,\delta_1),\cdots,(\epsilon_g,\delta_g)]$ of $H_1(\Sigma_g;\mathbb{Z}_2)$, let the $j$-th block be the right most block which is $(1,1)$. When $j \geq 3$, there exist 4 cases of the combination of the $(j-1)$-st block and the $j$-th block: $[\cdots,(1,1),(1,1),\cdots]$, $[\cdots,(0,0),(1,1),\cdots]$, $[\cdots,(0,1),(1,1),\cdots]$, $[\cdots,(1,0),(1,1),\cdots]$. In each case, we can reduce $j$ at least 1. In fact,

$$[\cdots,(1,1),(1,1),\cdots]\Box(x_{j-1}+x_j+y_j) = [\cdots,(0,1),(0,0),\cdots],$$
$$[\cdots,(0,0),(1,1),\cdots]\Box(x_{j-1}+y_{j-1}+x_j) = [\cdots,(1,1),(0,1),\cdots],$$
$$[\cdots,(0,1),(1,1),\cdots]\Box(x_{j-1}+x_j+y_j) = [\cdots,(1,1),(0,0),\cdots],$$
$$[\cdots,(1,0),(1,1),\cdots]\Box(x_{j-1}+y_{j-1})\Box(x_{j-1}+x_j+y_j) = [\cdots,(1,1),(0,0),\cdots].$$

When $j = 2$, since $q([(\epsilon_1, \delta_1), \cdots, (\epsilon_g, \delta_g)])$=1, there are 3 cases of combination of the first block and the second block: $[(0,0),(1,1),\cdots]$, $[(1,0),(1,1),\cdots]$, or $[(0,1),(1,1),\cdots]$. In each case, $j$ can be reduced to 1. In fact,

$$\begin{aligned}&[(0,0),(1,1),\cdots]\Box(x_1+y_1+x_2) = [(1,1),(0,1),\cdots],\\ &[(1,0),(1,1),\cdots]\Box(x_1+y_1)\Box(x_1+x_2+y_2) = [(1,1),(0,0),\cdots],\\ &[(0,1),(1,1),\cdots]\Box(x_1+x_2+y_2) = [(1,1),(0,0),\cdots].\end{aligned}$$

When $j = 1$, if every $i$-th ($i \geq 2$) block is $(0,0)$, then it is $x_1 + y_1$. If there exist at least one of the $i$-th ($i \geq 2$) blocks which are $(1,0)$ or $(0,1)$, then,

$$\begin{aligned}&[\cdots,(0,0),\overset{i}{(1,0)},\cdots]\Box(x_{i-1}+x_i+y_i) = [\cdots,(1,0),(0,1),\cdots],\\ &[\cdots,(1,0),\overset{i}{(0,0)},\cdots]\Box(x_{i-1}+y_{i-1}+x_i) = [\cdots,(0,1),(1,0),\cdots],\\ &[\cdots,(0,0),\overset{i}{(0,1)},\cdots]\Box(x_{i-1}+x_i+y_i) = [\cdots,(1,0),(1,0),\cdots],\\ &[\cdots,(0,1),\overset{i}{(0,0)},\cdots]\Box(x_{i-1}+y_{i-1}+x_i) = [\cdots,(1,0),(1,0),\cdots].\end{aligned}$$

Therefore, we can alter this to an element, each $i$-th ($i \geq 2$) block of which is $(1,0)$ or $(0,1)$. If the $i$-th block of this is $(0,1)$, then

$$[\cdots,(0,1),\cdots]\Box(x_i+y_i) = [\cdots,(1,0),\cdots].$$

Therefore, it suffices to consider the case when the first block is $(1,1)$ and other blocks are $(1,0)$. In this case,

$$[\cdots,(1,0),(1,0)]\Box(x_{g-1}+y_{g-1}+x_g)\Box(x_{g-1}+y_{g-1}) = [\cdots,(1,0),(0,0)].$$

By applying the same operation repeatedly, we get $[(1,1),(1,0),\circ\circ\circ]$ as a result. □

This lemma and Theorem 3.16 show:

**Corollary 3.18** *$O(2g,\mathbb{Z}_2)$ is generated by $\mathbb{T}_{x_i+y_i}$ $(1 \leq i \leq g)$, $\mathbb{T}_{x_i+y_i+x_{i+1}}$ $(1 \leq i \leq g-1)$, and $\mathbb{T}_{x_i+x_{i+1}+y_{i+1}}$ $(1 \leq i \leq g-1)$.* □

Since $G_g$ is a subgroup of $\mathcal{SP}_g$, $\Phi_2(G_g) \subset \mathrm{O}(2g,\mathbb{Z}_2)$. On the other hand, the fact that $\Phi_2(X_{2i}) = \mathbb{T}_{x_i+y_i+x_{i+1}}$ $(1 \leq i \leq g-1)$, $\Phi_2(X_{2i+1}) = \mathbb{T}_{x_i+x_{i+1}+y_{i+1}}$ $(1 \leq i \leq g-1)$, $\Phi_2(X_1) = \mathbb{T}_{x_1+y_1}$, $\Phi_2(Y_{2j}) = \mathbb{T}_{x_j+y_j}$ $(2 \leq j \leq g-1)$, $\Phi_2(X_{2g}) = \mathbb{T}_{x_g+y_g}$, and Corollary 3.18, show $\Phi_2(G_g) \supset \mathrm{O}(2g,\mathbb{Z}_2)$. Therefore we proved that, if $g \geq 3$, then $\mathcal{SP}_g = G_g$.

### 3.5 Genus 2 case: Reidemeister-Schreier method

Birman and Hilden showed the following Theorem.

**Theorem 3.19** [1] *$\mathcal{M}_2$ is generated by $C_1, C_2, C_3, C_4, C_5$ and its defining relations are:*

(1) $C_iC_j = C_jC_i$, *if* $|i-j| \geq 2$, $i, j = 1, 2, 3, 4, 5$,

(2) $C_iC_{i+1}C_i = C_{i+1}C_iC_{i+1}$, $i = 1, 2, 3, 4$,

(3) $(C_1C_2C_3C_4C_5)^6 = 1$,

(4) $(C_1C_2C_3C_4C_5C_5C_4C_3C_2C_1)^2 = 1$,

(5) $C_1C_2C_3C_4C_5C_5C_4C_3C_2C_1 \rightleftarrows C_i$, $i = 1, 2, 3, 4, 5$,

*where $\rightleftarrows$ means "commute with".*

We call (1) (2) of the above relations *braid relations*. We will use the well-known method, called *the Reidemeister–Schreier method* [9, §2.3], to show $\mathcal{SP}_2 \subset G_2$. We review (a part of) this method.

Let $G$ be a group generated by finite elements $g_1, \ldots, g_m$ and $H$ be a finite index subgroup of $G$. For two elements $a$, $b$ of $G$, we write $a \equiv b \bmod H$ if there is an element $h$ of $H$ such that $a = hb$. A finite subset $S$ of $G$ is called *a coset representative system* for $G$ mod $H$, if, for each elements $g$ of $G$, there is only one element $\overline{\overline{g}} \in S$ such that $g \equiv \overline{\overline{g}} \bmod H$. The set $\{sg_i\overline{\overline{sg_i}}^{-1} \mid i = 1, \ldots, m,\ s \in S\}$ generates $H$.

For the sake of giving a coset representative system for $\mathcal{M}_2$ modulo $\mathcal{SP}_2$, we will draw a graph $\Gamma$ which represents the action of $\mathcal{M}_2$ on the quadratic forms of $H_1(\Sigma_2; \mathbb{Z}_2)$ with Arf invariants $0$. Let $[\epsilon_1, \epsilon_2, \epsilon_3, \epsilon_4]$ denote the quadratic form $q'$ of $H_1(\Sigma_2; \mathbb{Z}_2)$ such that $q'(x_1) = \epsilon_1$, $q'(y_1) = \epsilon_2$, $q'(x_2) = \epsilon_3$, $q'(y_2) = \epsilon_4$. Each vertex of $\Gamma$ corresponds to a quadratic form. For each generator $C_i$ of $\mathcal{M}_2$, we denote its action on $H_1(\Sigma_2; \mathbb{Z}_2)$ by $(C_i)_*$. For the quadratic form $q'$ indicated by the symbol $[\epsilon_1, \epsilon_2, \epsilon_3, \epsilon_4]$, let $\delta_1 = q'((C_i)_*x_1)$, $\delta_2 = q'((C_i)_*y_1)$, $\delta_3 = q'((C_i)_*x_2)$, and $\delta_4 = q'((C_i)_*y_2)$. Then, we connect two vertices, corresponding to $[\epsilon_1, \epsilon_2, \epsilon_3, \epsilon_4]$, $[\delta_1, \delta_2, \delta_3, \delta_4]$ respectively, by the edge with the letter $C_i$. We remark that this action is a right action. For simplicity, we omit the edge whose ends are the same vertex. As a result, we get a graph $\Gamma$ as in Figure 23. (Remark: The same graph was in [4, Proof of Lemma 3.1]. ) In Figure 23, the bold edges form a maximal tree $T$ of $\Gamma$. The words $S = \{1,\ C_1,\ C_2,\ C_3,\ C_4,\ C_5,\ C_1C_4,\ C_2C_4,\ C_2C_5,\ C_2C_4C_3\}$, which

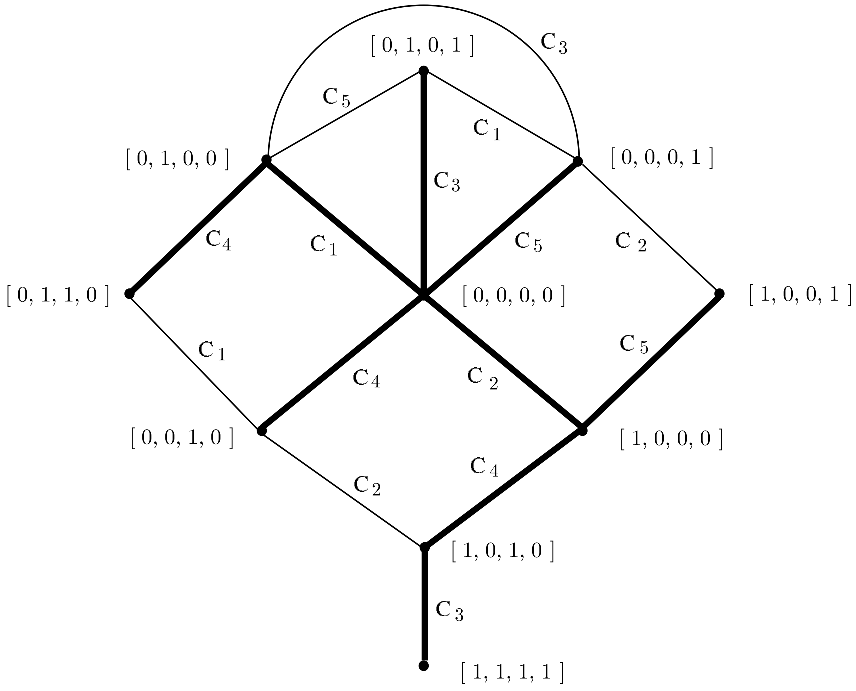

Figure 23

correspond to the edge paths beginning from $[0,0,0,0]$ on $T$, define a coset representative system for $\mathcal{M}_2$ modulo $\mathcal{SP}_2$. For each element $g$ of $\mathcal{M}_2$, we can give a $\overline{\overline{g}} \in S$ with using this graph. For example, say $g = C_2C_4C_5C_2$, we follow an edge path assigned to this word which begins from $[0,0,0,0]$, (note that we read words from left to right) then we arrive at the vertex $[0,0,1,0]$. The edge path on $T$ which begins from $[0,0,0,0]$ and ends at $[0,0,1,0]$ is $C_4$. Hence, $\overline{\overline{C_2C_4C_5C_2}} = C_4$. We list in Table 1 the set of generators $\{sC_i\overline{\overline{sC_i}}^{-1} \mid i = 1,\ldots,5,\ s \in S\}$ of $\mathcal{SP}_g$. In Table 1, vertical direction is a coset representative system $S$, horizontal direction is a set of generators $\{C_1,\ C_2,\ C_3,\ C_4,\ C_5\}$. We can check this table by Figure 23 and braid relations. For example,

$$\begin{aligned} &C_2C_4C_3 \cdot C_1\overline{\overline{C_2C_4C_3 \cdot C_1}}^{-1} = C_2C_4C_3C_1(C_2C_4C_3)^{-1} \\ &= C_2C_4C_3C_1C_3^{-1}C_4^{-1}C_2^{-1} = C_2C_1C_2^{-1} = X_1. \end{aligned}$$

This table shows that $\mathcal{SP}_2 \subset G_2$ .

Table 1: Generators of $\mathcal{SP}_2$

| | $C_1$ | $C_2$ | $C_3$ | $C_4$ | $C_5$ |
|---|---|---|---|---|---|
| $1$ | $1$ | $1$ | $1$ | $1$ | $1$ |
| $C_1$ | $D_1$ | $X_1^*$ | $TD_5^{-1}$ | $1$ | $TD_3^{-1}$ |
| $C_2$ | $X_1$ | $D_2$ | $X_2^*$ | $1$ | $1$ |
| $C_3$ | $TD_5^{-1}$ | $X_2$ | $D_3$ | $X_3^*$ | $TD_1^{-1}$ |
| $C_4$ | $1$ | $1$ | $X_3$ | $D_4$ | $X_4^*$ |
| $C_5$ | $TD_3^{-1}$ | $1$ | $TD_1^{-1}$ | $X_4$ | $D_5$ |
| $C_1C_4$ | $D_1$ | $X_1^*$ | $X_3$ | $D_4$ | $X_4^*$ |
| $C_2C_4$ | $X_1$ | $D_2$ | $1$ | $D_4$ | $X_4^*$ |
| $C_2C_5$ | $X_1$ | $D_2$ | $X_2^*$ | $X_4$ | $D_5$ |
| $C_2C_4C_3$ | $X_1$ | $X_3$ | $(X_2^*)^{-1}D_4X_2^*$ | $X_2^*$ | $X_4^*$ |

## References

[1] **J S Birman**, **H Hilden**, *On the mapping class group of closed surface as covering spaces*, from: "Advances in the theory of Riemann surfaces" Ann. of Math. Studies 66(1971) 81–115

[2] **J Dieudonné**, *La gémmetrie des groupes classiques, (3-rd edn.)*, Ergebnisse der Math. u.i. Grundz. 5, Springer, 1971

[3] **J L Harer**, *Stability of the homology of the moduli spaces of Riemann surfaces with spin structure*, Math. Ann. 287(1990) 323–334

[4] **J L Harer**, *The rational Picard group of the moduli space of Riemann surfaces with spin structure*, Contemp. Math. 150(1993) 107–136

[5] **S Hirose**, *On diffeomorphisms over $T^2$-knot*, Proc. of A.M.S. 119(1993) 1009–1018

[6] **Z Iwase**, *Dehn surgery along a torus $T^2$-knot. II*, Japan. J. Math. 16(1990) 171–196

[7] **D Johnson**, *The structure of the Torelli Group I: A finite set of generators for $\mathcal{I}$*, Annals of Math. 118(1983) 423–442

[8] **D Johnson**, *The structure of the Torelli Group III: The abelianization of $\mathcal{I}$*, Topology 24(1985) 127–144

[9] **W Magnus**, **A Karras**, **D Solitar**, *Combinatorial Group Theory*, Dover 1975

[10] **J M Montesinos**, *On twins in the four-sphere I*, Quart. J. Math. Oxford (2) 34(1983) 171–199

*Department of Mathematics, Faculty of Science and Engineering*
*Saga University, Saga, 840-8502 Japan.*

Email: `hirose@ms.saga-u.ac.jp`

Received: 6 March 2002