Finite index subgroups of mapping class groups

A. J. Berrick, V. Gebhardt and L. Paris

October 29, 2012

Abstract

Let $g \geq 3$ and $n \geq 0$, and let $\mathcal{M}_{g,n}$ be the mapping class group of a surface of genus g with n boundary components. We prove that $\mathcal{M}_{g,n}$ contains a unique subgroup of index $2^{g-1}(2^g-1)$ up to conjugation, a unique subgroup of index $2^{g-1}(2^g+1)$ up to conjugation, and the other proper subgroups of $\mathcal{M}_{g,n}$ are of index greater than $2^{g-1}(2^g+1)$. In particular, the minimum index for a proper subgroup of $\mathcal{M}_{g,n}$ is $2^{g-1}(2^g-1)$.

AMS Subject Classification. Primary: 57M99. Secondary: 20G40, 20E28.

0 Introduction and statement of results

The interaction between mapping class groups and finite groups has long been a topic of interest. The famous Hurwitz bound of 1893 showed that the mapping class group of a closed Riemann surface of genus g has an upper bound of $84(g-1)$ for the order of its finite subgroups, and Kerckhoff showed that the order of finite cyclic subgroups is bounded above by $4g+2$ [19], [20]. The subject of finite index subgroups of mapping class groups was brought into focus by Grossman's discovery that the mapping class group $\mathcal{M}_{g,n} = \pi_0(\mathrm{Homeo}(\Sigma_{g,n}))$ of an oriented surface $\Sigma_{g,n}$ of genus g and n boundary components is residually finite, and thus well-endowed with subgroups of finite index [15]. ($\mathrm{Homeo}(\Sigma_{g,n})$ denotes the space of those homeomorphisms of $\Sigma_{g,n}$ that preserve the orientation and are the identity on the boundary.) This prompts the "dual" question:

What is the minimum index $\mathrm{mi}(\mathcal{M}_{g,n})$ *of a proper subgroup of finite index in* $\mathcal{M}_{g,n}$*?*

Results to date have suggested that, like the maximum finite order question, the minimum index question should have an answer that is linear in g. The best previously published bound is $\mathrm{mi}(\mathcal{M}_{g,n}) > 4g+4$ for $g \geq 3$ (see [26]). This inequality is used by Aramayona and Souto to prove that, if $g \geq 6$ and $g' \leq 2g-1$, then any nontrivial homomorphism $\mathcal{M}_{g,n} \to \mathcal{M}_{g',n'}$ is induced by an embedding [1]. It is also an important ingredient in the proof of Zimmermann [33] that, for $g = 3$ and 4, the minimal nontrivial quotient of $\mathcal{M}_{g,0}$ is $\mathrm{Sp}_{2g}(\mathbb{F}_2)$.

The "headline" result of this paper is the following exact, exponential bound.

Theorem 0.1. *For* $g \geq 3$ *and* $n \geq 0$*,*

$$\mathrm{mi}(\mathcal{M}_{g,n}) = \mathrm{mi}(\mathrm{Sp}_{2g}(\mathbb{Z})) = \mathrm{mi}(\mathrm{Sp}_{2g}(\mathbb{F}_2)) = 2^{g-1}(2^g-1)\,.$$

This exponential bound is all the more surprising since in similar questions we get linear (expected) bounds. For instance, Bridson [5, 6] has proved that a mapping class group of a surface

of genus g cannot act by semisimple isometries, without a global fixed point, on a CAT(0) space of dimension less than g. The exact minimal dimension for such an action is unknown. On the other hand, it has been also shown by Bridson (see [5]) that $\mathcal{M}_{g,n}$ has only finitely many irreducible linear representations over any algebraically closed field, up to dimension $(g+1)$. Later, Funar [14] showed that there is no linear representation with infinite image up to dimension about $\sqrt{g+1}$. However, there is an obvious linear representation of rank $2g$ which comes from the action of $\mathcal{M}_{g,n}$ on the homology of $\Sigma_{g,0}$ (the map $\theta_{g,n}$ defined below). It is expected that this representation is minimal in some sense (see [12]).
The nontrivial quotient of $\mathcal{M}_{g,n}$ of minimal order is unknown, but obviously its order must be at least $\mathrm{mi}(\mathcal{M}_{g,n})$. This quotient is known to be $\mathrm{Sp}_{2g}(\mathbb{F}_2)$ if $(g,n)=(3,0)$ or $(4,0)$ (see [33]). On the other hand, a consequence of the above theorem is the following (proved in [17] in the case $n=0$).

Corollary 0.2. *The group $\mathcal{M}_{g',n'}$ cannot be a quotient of $\mathcal{M}_{g,n}$ if $g > \max(g',2)$.*

Our proof of Theorem 0.1 is constructive, in ways that we now describe. From the surface $\Sigma_{g,n}$ we obtain a closed oriented surface $\widehat{\Sigma}_g$ of genus g by gluing a disk along each boundary component. The embedding $\Sigma_{g,n} \hookrightarrow \widehat{\Sigma}_g$ induces a first epimorphism $\mathcal{M}_{g,n} \twoheadrightarrow \mathcal{M}_{g,0}$. The action of $\mathrm{Homeo}(\widehat{\Sigma}_g)$ on $H_1(\widehat{\Sigma}_g) = \mathbb{Z}^{2g}$ induces a second epimorphism $\mathcal{M}_{g,0} \twoheadrightarrow \mathrm{Sp}_{2g}(\mathbb{Z})$ onto the integral symplectic group, and, passing mod 2, we obtain a third epimorphism $\mathrm{Sp}_{2g}(\mathbb{Z}) \twoheadrightarrow \mathrm{Sp}_{2g}(\mathbb{F}_2)$, where $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$. From now on we denote by $\theta_{g,n} : \mathcal{M}_{g,n} \to \mathrm{Sp}_{2g}(\mathbb{F}_2)$ the composition of these three epimorphisms.

The orthogonal groups $O^+_{2g}(\mathbb{F}_2)$ and $O^-_{2g}(\mathbb{F}_2)$ are subgroups of $\mathrm{Sp}_{2g}(\mathbb{F}_2)$. The cardinalities of $\mathrm{Sp}_{2g}(\mathbb{F}_2)$, $O^+_{2g}(\mathbb{F}_2)$ and $O^-_{2g}(\mathbb{F}_2)$ can be found for instance in [31, pp. 70, 141]; one has

$$\left|\mathrm{Sp}_{2g}(\mathbb{F}_2)\right| = 2^{g^2}\prod_{i=1}^{g}(2^{2i}-1)\ ,$$

$$\left|O^{\pm}_{2g}(\mathbb{F}_2)\right| = 2^{g^2-g+1}(2^g \mp 1)\prod_{i=1}^{g-1}(2^{2i}-1)\ .$$

From this data it is easily shown that, for $g \geq 2$, the indices of $O^+_{2g}(\mathbb{F}_2)$ and $O^-_{2g}(\mathbb{F}_2)$ in $\mathrm{Sp}_{2g}(\mathbb{F}_2)$ are $N^+_g = 2^{g-1}(2^g+1)$ and $N^-_g = 2^{g-1}(2^g-1)$, respectively. The following, more or less known to experts but seemingly unpublished, is the starting-point for our main result (Theorem 0.4). Its proof depends on classification of finite simple groups.

Theorem 0.3. *Let $g \geq 3$.*

(1) $O^-_{2g}(\mathbb{F}_2)$ is the unique subgroup of $\mathrm{Sp}_{2g}(\mathbb{F}_2)$ of index N^-_g, up to conjugation.

(2) $O^+_{2g}(\mathbb{F}_2)$ is the unique subgroup of $\mathrm{Sp}_{2g}(\mathbb{F}_2)$ of index N^+_g, up to conjugation.

(3) All the other proper subgroups of $\mathrm{Sp}_{2g}(\mathbb{F}_2)$ are of index at least $2N^-_g$.

We set $\mathcal{O}^+_{g,n} = \theta^{-1}_{g,n}(O^+_{2g}(\mathbb{F}_2))$ and $\mathcal{O}^-_{g,n} = \theta^{-1}_{g,n}(O^-_{2g}(\mathbb{F}_2))$. Thus, by the above, $\mathcal{O}^-_{g,n}$ is an index N^-_g subgroup of $\mathcal{M}_{g,n}$, and $\mathcal{O}^+_{g,n}$ is an index N^+_g subgroup of $\mathcal{M}_{g,n}$. Here is our main result.

Theorem 0.4. *Let $g \geq 3$ and $n \geq 0$.*

(1) $\mathcal{O}^-_{g,n}$ is the unique subgroup of $\mathcal{M}_{g,n}$ of index N^-_g, up to conjugation.

(2) $\mathcal{O}^+_{g,n}$ is the unique subgroup of $\mathcal{M}_{g,n}$ of index N^+_g, up to conjugation.

(3) If $g = 3$ then all the other proper subgroups of $\mathcal{M}_{3,n}$ are of index strictly greater than $N^+_g = 36$.

(4) If $g \geq 4$ then all the other proper subgroups of $\mathcal{M}_{g,n}$ are of index at least $5N^-_{g-1} > N^+_g$.

Since m is an upper bound for the minimum index of a group G if and only if there is a nontrivial homomorphism from G to the symmetric group $\mathfrak{S}_m$ on m letters, one would like to understand the permutation representations associated to Theorem 0.4.
We denote by $\phi^+_{g,n} : \mathcal{M}_{g,n} \to \mathfrak{S}_{N^+_g}$ (resp. $\phi^-_{g,n} : \mathcal{M}_{g,n} \to \mathfrak{S}_{N^-_g}$) the permutation representation induced by the action of $\mathcal{M}_{g,n}$ on the right cosets of $\mathcal{O}^+_{g,n}$ (resp. $\mathcal{O}^-_{g,n}$). Corresponding to the numerical relations

$$N^+_g = 3N^+_{g-1} + N^-_{g-1}\,, \quad N^-_g = 3N^-_{g-1} + N^+_{g-1}\,,$$

we prove the following.

Theorem 0.5. *(1) Let $g \geq 3$ and $n \geq 1$. Then $\phi^-_{g,n} : \mathcal{M}_{g,n} \to \mathfrak{S}_{N^-_g}$ is, up to equivalence, the unique extension of the representation $(\phi^-_{g-1,n})^3 \oplus \phi^+_{g-1,n}$ from $\mathcal{M}_{g-1,n}$ to $\mathcal{M}_{g,n}$, and $\phi^+_{g,n} : \mathcal{M}_{g,n} \to \mathfrak{S}_{N^+_g}$ is, up to equivalence, the unique extension of the representation $\phi^-_{g-1,n} \oplus (\phi^+_{g-1,n})^3$ from $\mathcal{M}_{g-1,n}$ to $\mathcal{M}_{g,n}$.*

(2) Let $g \geq 3$ and $n \geq 0$. Let b be a nonseparating simple closed curve on $\Sigma_{g,n}$, and let T_b be the Dehn twist around b. Then the cycle structure of the image of T_b under $\phi^-_{g,n}$ is

$$(1)^{2^{2g-2}}(2)^{2^{g-2}(2^{g-1}-1)}\,,$$

and the cycle structure of the image of T_b under $\phi^+_{g,n}$ is

$$(1)^{2^{2g-2}}(2)^{2^{g-2}(2^{g-1}+1)}\,.$$

Remark. Implicit in the statement of Theorem 0.5 is the fact that, if $n \geq 1$, then $\mathcal{M}_{g-1,n}$ naturally embeds into $\mathcal{M}_{g,n}$. This embedding will be described in Section 2. However, there is no natural embedding of $\mathcal{M}_{g-1,0}$ into $\mathcal{M}_{g,0}$, hence Part (1) of the theorem would make no sense for $n = 0$.

We observe that the abelianization of $\mathcal{M}_{g,n}$ is isomorphic to $\mathbb{Z}/12\,\mathbb{Z}$ if $(g,n) = (1,0)$, $\mathbb{Z}^n$ if $g = 1$ and $n \geq 1$, and $\mathbb{Z}/10\,\mathbb{Z}$ if $g = 2$ (see [21]). Hence, the minimum index of $\mathcal{M}_{g,n}$ is 2 if $g = 1$ or 2. Note that $\mathcal{M}_{g,n}$ is perfect if $g \geq 3$ (see [28, 21]). If $g = 2$ we have $N^-_g = 6$ and $N^+_g = 10$, and there are six proper subgroups of index at most 10 in $\mathcal{M}_{g,n}$: one of index 2, one of index 5, two of index 6 and two of index 10. The description of these subgroups as well as the proof of this fact are given in Section 3.

The remainder of the paper is divided into two parts. Part I starts with some preliminaries on permutations (Section 1) and presentations of mapping class groups (Section 2). Then we

determine the subgroups of $\mathcal{M}_{2,n}$ of index at most $10 = N_2^+$ (Section 3) and the subgroups of $\mathcal{M}_{3,n}$ of index at most $36 = N_3^+$ (Section 4). We prove our theorems by induction on the genus. The starting case, $g = 3$, is made in Section 4, and the inductive step is the object of Part II. We first treat the case of a surface with a unique boundary component (Sections 5 to 7) and we extend the result to surfaces with several boundary components in Section 8. Theorem 0.1 is proved in Section 6. This can be read independently from the rest.

Acknowledgements. Many thanks to Derek Holt for his helpful advice. The authors are pleased to acknowledge the financial support of National University of Singapore research grants R-146-000-097-112 and R-146-000-137-112 towards the visits of LP to Singapore in 2007 and 2011 and AJB to Dijon in 2009 and 2010, and the warm hospitality of their hosts. LP is partially supported by the *Agence Nationale de la Recherche* (*projet Théorie de Garside*, ANR-08-BLAN-0269-03). VG acknowledges support under Australian Research Council's Discovery Projects funding scheme (project number DP1094072), and the Spanish Project MTM2010-19355.

Part I
Preliminaries

1 Useful information on permutations

We define the *minimum index* $\mathrm{mi}(G)$ of a nontrivial group G to be the element of the ordered set $2 < 3 < 4 < \cdots < \infty$ corresponding to the minimum among the indices of all proper subgroups of G with finite index, and ∞ when G has no proper finite index subgroup (such a G has been called *counter-finite*).

Permutations are important to our investigation because of the well-known relationship between index m subgroups and maps to $\mathfrak{S}_m$. A homomorphism $\varphi : G \to \mathfrak{S}_m$ is called *transitive* if its image acts transitively on $\{1, \ldots, m\}$. If $\varphi : G \to \mathfrak{S}_m$ is transitive, then $\mathrm{Stab}_\varphi(1) = \{\gamma \in G \mid \varphi(\gamma)(1) = 1\}$ is a subgroup of G of index m. Conversely, if H is a subgroup of G of index m, then there exists a transitive homomorphism $\varphi : G \to \mathfrak{S}_m$ such that $H = \mathrm{Stab}_\varphi(1)$ (take the action of G on the right cosets of H). It follows that $\mathrm{mi}(G)$ is also the smallest $m \geq 2$ such that there exists a nontrivial homomorphism $\varphi : G \to \mathfrak{S}_m$. Of course, if such a homomorphism does not exist for any m, then $\mathrm{mi}(G) = \infty$.

The minimum index has the property that, if $G \twoheadrightarrow H$ is an epimorphism, then $\mathrm{mi}(G) \leq \mathrm{mi}(H)$. (Indeed, the pre-image of an index m subgroup under an epimorphism is an index m subgroup.) From the definition of $\theta_{g,n} : \mathcal{M}_{g,n} \to \mathrm{Sp}_{2g}(\mathbb{F}_2)$ as the composition of epimorphisms

$$\mathcal{M}_{g,n} \twoheadrightarrow \mathcal{M}_{g,0} \twoheadrightarrow \mathrm{Sp}_{2g}(\mathbb{Z}) \twoheadrightarrow \mathrm{Sp}_{2g}(\mathbb{F}_2),$$

we therefore have

$$\mathrm{mi}(\mathcal{M}_{g,n}) \leq \mathrm{mi}(\mathcal{M}_{g,0}) \leq \mathrm{mi}(\mathrm{Sp}_{2g}(\mathbb{Z})) \leq \mathrm{mi}(\mathrm{Sp}_{2g}(\mathbb{F}_2))\,.$$

Since many generators of mapping class groups commute with each other, we need some preliminary results that discuss aspects of commuting permutations. In the following, C_k denotes the cyclic group of order k, and an orbit of cardinality k under the action of a permutation or a permutation group is called a *k-orbit*.

Lemma 1.1. *Let $u \in \mathfrak{S}_m$ have cycle type $(1)^{\ell_1}(2)^{\ell_2}\cdots(m)^{\ell_m}$, and let*

$$I(u) = \{k \in \{1,2,\dots,m\} \mid \ell_k > 0\}\,,$$

so that $\sum_{k\in I(u)} k\ell_k = m$.

(1) The centralizer $C_{\mathfrak{S}_m}(u)$ is isomorphic to

$$\prod_{k\in I(u)} ((C_k)^{\ell_k} \rtimes \mathfrak{S}_{\ell_k}) = \prod_{k\in I(u)} (C_k \wr \mathfrak{S}_{\ell_k})\,.$$

(2) If $P \le C_{\mathfrak{S}_m}(u)$ is nonabelian, then, for some $k \in I(u)$, $\ell_k \ge \mathrm{mi}(P)$.

(3) If further P is perfect, then P is isomorphic to a subgroup of

$$\prod_{k\in I(u)} ((C_k)^{\ell_k} \rtimes \mathfrak{A}_{\ell_k}) = \prod_{k\in I(u)} (C_k \wr \mathfrak{A}_{\ell_k})\,,$$

where $\mathfrak{A}_{\ell_k}$ denotes the alternating group. If $I(P) = \{k \in I(u) \mid P$ acts nontrivially on the union of the k-orbits of $u\}$, then the following numerical constraints hold:

(a) $5 \le \mathrm{mi}(P) \le \ell_k$ whenever $k \in I(P)$;
(b) $m \ge \mathrm{mi}(P)(\sum_{k\in I(P)} k)$; and
(c) if $m < 5\,\mathrm{mi}(P)$, then either $I(P) = \{4\}$ or $I(P) - \{1\} = \{2\}$ or $\{3\}$.

Proof. (1) is left to the reader. Let P_k denote the projection of P to the component $C_k \wr \mathfrak{S}_{\ell_k}$ of $C_{\mathfrak{S}_m}(u)$. Since P is contained in $\prod_{k\in I(u)} P_k$ and P is nonabelian, there exists $k \in I(u)$ such that P_k is nonabelian, and thus $\ell_k \ge \mathrm{mi}(P_k) \ge \mathrm{mi}(P)$. Finally, (3) results from the fact that any nontrivial perfect subgroup of $(C_k)^{\ell_k} \rtimes \mathfrak{S}_{\ell_k}$ (whose support is the union of the k-orbits of u) must have nontrivial perfect image in $\mathfrak{S}_{\ell_k}$. Then $\ell_k \ge 5$ and the image lies in the maximum perfect subgroup $\mathfrak{A}_{\ell_k}$ of $\mathfrak{S}_{\ell_k}$. Then (a), (b) and (c) follow readily. □

For $u \in \mathfrak{S}_m$ we write $\{1,\dots,m\} = F(u) \sqcup S(u)$ for the partition into the fixed set $F(u)$ and support $S(u)$ of the permutation u. Evidently, u restricts to the identity map on $F(u)$, respectively to a bijection on $S(u)$.

Lemma 1.2. *Let $u, v \in \mathfrak{S}_m$ be such that $uvu = vuv$. Then $|S(u)| \le 2\,|S(u) \cap S(v)|$.*

Proof. If $u(i) \in F(v)$, then $(vu)(i) = u(i)$. If also $i \in F(v)$, then

$$u(u(i)) = (uvu)(i) = (vuv)(i) = (vu)(i) = u(i)\,.$$

Thus,

$$i \in u^{-1}(F(v)) \cap F(v) \quad\Longrightarrow\quad i \in u^{-1}(F(u))\,;$$

in other words, $F(v) \cap u(F(v)) \subseteq F(u)$. Therefore,

$$S(u) \cap F(v) \cap u(F(v)) = \emptyset\,;$$

and so $S(u)\cap u(F(v)) \subseteq S(u)\cap S(v)$. However, u maps $S(u)\cap F(v)$ bijectively to $S(u)\cap u(F(v))$. The result is now immediate from the fact that

$$|S(u)| = |S(u)\cap S(v)| + |S(u)\cap F(v)|\,. \quad \square$$

Henceforth, we follow the convention that if u, v are elements of a group G, then $\langle u, v\rangle$ is the subgroup of G that they generate.

Lemma 1.3. *Let $u, v \in \mathfrak{S}_m$ be such that $uvu = vuv$. If $k \in \{2, 3\}$ and all nontrivial orbits of u and $\langle u, v\rangle$ have length k, then $u = v$.*

Proof. We present the argument for $k = 3$; for $k = 2$ it is similar, but simpler. Since u and v are conjugate, they have the same cycle decomposition type. If there are no nontrivial orbits, then $u = v = 1$. So, let O be an orbit of u of length 3. Then O must also be a nontrivial orbit of $\langle u, v\rangle$. Hence, since v is a product of 3-cycles, v acts on O as either $1, u$ or u^2. In each case, the actions of u and v on O commute. Likewise, on each nontrivial orbit of v the actions of u and v commute. Finally, on $F(u)\cap F(v)$, since u and v both act as the identity, the actions of u and v again commute. Hence, $uv = vu$. From $uvu = vuv$, the result follows. $\square$

Lemma 1.4. *Let $u, v_0, v_1 \in \mathfrak{S}_m$ be such that*

(a) $uv_iu = v_iuv_i$ for $i = 0, 1$; and

(b) v_0 and v_1 commute.

If u has order 3 and all nontrivial orbits of $\langle u, v_0\rangle$ and $\langle u, v_1\rangle$ have length 4, then $v_0 = v_1$.

Proof. If u is trivial then the result is immediate from (a). Therefore, we can assume that u contains the 3-cycle (1 2 3) and $\{2, 3, 4\}$ is a nontrivial orbit of v_0. Now, in $\mathfrak{S}_4$

$$(1\ 2\ 3)(4\ 3\ 2)(1\ 2\ 3) = (4\ 3\ 2)(1\ 2\ 3)(4\ 3\ 2) = (1\ 4)(2\ 3)\,;$$

however

$$(1\ 2\ 3)(4\ 2\ 3)(1\ 2\ 3) \neq (4\ 2\ 3)(1\ 2\ 3)(4\ 2\ 3)\,.$$

Thus, v_0 contains the cycle (4 3 2) in its cycle decomposition. Because v_1 commutes with v_0,

$$v_1(4\ 3\ 2)v_1^{-1} = (v_1(4)\ v_1(3)\ v_1(2)) \tag{1.1}$$

is a 3-cycle in the decomposition of v_0. Now, $\langle u, v_1\rangle$ has a 4-orbit of the form $\{1, 2, 3, x\}$, whence, from the above argument in $\mathfrak{S}_4$, v_1 acts on this orbit as $(3)(x\ 2\ 1)$, $(2)(x\ 1\ 3)$ or $(1)(x\ 3\ 2)$. However, in the first case, because $v_1(3) = 3$, Equality (1.1) implies that $v_1(2) = 2$, contradicting $v_1(2) = 1$. Similarly, in the second case, $v_1(2) = 2$ combines with (1.1) to imply that $v_1(3) = 3$, contradicting $v_1(1) = 3$.

This leaves the last case, in which $v_1(3) = 2$, which from (1.1) gives $x = v_1(2) = 4$. That is, (4 3 2) is a 3-cycle in the decomposition of v_1. It follows that the 3-cycles of v_0 and v_1 coincide, whence $v_0 = v_1$. $\square$

Lemma 1.5. *Let $u, v_0, v_1, v_2 \in \mathfrak{S}_m$ be such that*

(a) $uv_iu = v_iuv_i$ for $i = 0, 1, 2$;

(b) v_0, v_1 *and* v_2 *commute pairwise; and*

(c) whenever $\{i,j,k\} = \{0,1,2\}$, *there is an isomorphism* $\gamma_{j,k}$ *from* $\langle u, v_i, v_j\rangle$ *to* $\langle u, v_i, v_k\rangle$ *fixing* u *and* v_i, *and sending* v_j *to* v_k.

If u *is a product of* 4*-cycles (possibly with fixed points) and all nontrivial orbits of each* $\langle u, v_i\rangle$ *have length* 4, *then* $v_0 = v_1 = v_2$.

Proof. Since, by (a), u and v_i are conjugate, they have the same cycle decomposition type, which must be a product of 4-cycles. If there are no nontrivial orbits, then each $v_i = 1$.

Let O be an orbit of u of length 4. Then O must also be a nontrivial orbit of each $\langle u, v_i\rangle$. From (a) it follows that O is also a nontrivial orbit of each v_i. Likewise, a nontrivial orbit of any one v_i must also be a nontrivial orbit of u and thereby of each v_i. Thus, it suffices to restrict attention to the action on each nontrivial orbit O; in effect, $\langle u, v_0, v_1, v_2\rangle \leq \mathfrak{S}_4$. Using (b), from the fact that in $\mathfrak{S}_4$ commuting 4-cycles are either the same or mutually inverse, we must have at least two distinct indices $i, j \in \{0,1,2\}$ such that $v_i = v_j$. Since by (c) $\gamma_{j,k}$ both fixes v_i and sends v_j to v_k, we conclude that $v_i = v_j = v_k$. □

2 Presentation for the mapping class group

Throughout the paper we denote by T_b the Dehn twist about a simple closed curve b. We fix an embedding of $\Sigma_{g,1}$ as well as the simple closed curves $a_0, a_1, \ldots, a_{2g+1}$ illustrated in Figure 2.1, and we set $T_i = T_{a_i}$ for all $0 \leq i \leq 2g+1$. The following result is shown in [24].

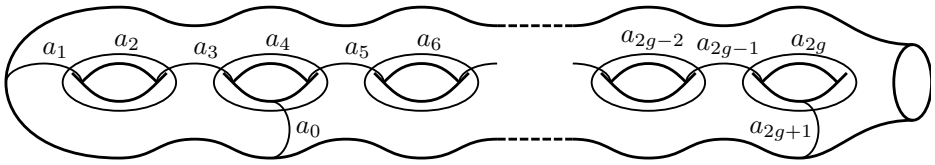

Figure 2.1. Generators for $\mathcal{M}_{g,1}$.

Theorem 2.1. (Matsumoto [24]). *Let* $g \geq 2$.

(a) $\mathcal{M}_{g,1}$ *has a presentation with generators* $T_0, T_1, \ldots, T_{2g}$ *and relations*

$$\begin{gathered} T_iT_jT_i = T_jT_iT_j \quad \text{if } a_i \text{ and } a_j \text{ intersect in a single point,} \\ T_iT_j = T_jT_i \quad \text{if } a_i \cap a_j = \emptyset\,, \\ (T_2T_3T_4T_0)^{10} = (T_1T_2T_3T_4T_0)^6\,, \\ (T_2T_3T_4T_5T_6T_0)^{12} = (T_1T_2T_3T_4T_5T_6T_0)^9 \quad \text{if } g \geq 3\,. \end{gathered}$$

(b) $\mathcal{M}_{g,0}$ *is the quotient of* $\mathcal{M}_{g,1}$ *by the additional relation*

$$T_1^{2g-2} = (T_0T_3T_4\cdots T_{2g-1})^{4g-4}.$$

□

We call k simple closed curves $b_1, \dots, b_k$ in $\Sigma_{g,n}$ a *k-chain* if their intersection numbers satisfy $i(b_i, b_j) = 1$ if $|i - j| = 1$ and $i(b_i, b_j) = 0$ otherwise. Such a k-chain is called *nonseparating* if the complement of $b_1 \cup \dots \cup b_k$ in $\Sigma_{g,n}$ is connected. Note that, if $(b_1, \dots, b_k)$ is a nonseparating k-chain, then each b_i is nonseparating, too. The next lemma follows from the rigidity of closed Riemann surfaces (see, for example, [13] Sections 1.3 and 2.3).

Lemma 2.2. *Let $(b_1, \dots, b_k)$ and $(b'_1, \dots, b'_k)$ be two nonseparating k-chains in $\Sigma_{g,n}$. Then there exists $\alpha \in \mathcal{M}_{g,n}$ such that $\alpha(b_i) = b'_i$ for all $1 \le i \le k$. In consequence, this α satisfies $\alpha T_{b_i} \alpha^{-1} = T_{b'_i}$ for all $1 \le i \le k$.* □

For studying the mapping class group $\mathcal{M}_{g,n}$ with $n \ge 2$ we use the following convention: $a_0, a_2, \dots, a_{2g}, a_{2g+1}$ and $b_1, \dots, b_n$ are the simple closed curves illustrated in Figure 2.2, $T_i = T_{a_i}$ for all $0 \le i \le 2g + 1$, $i \ne 1$, and $T'_j = T_{b_j}$ for all $1 \le j \le n$. In order to unify statements for $n = 1$ and $n > 1$, we make the further convention that, when $n = 1$, b_1 in Figure 2.2 coincides with a_1 in Figure 2.1. Then for $n = 1$ the element T'_1 is simply T_1.

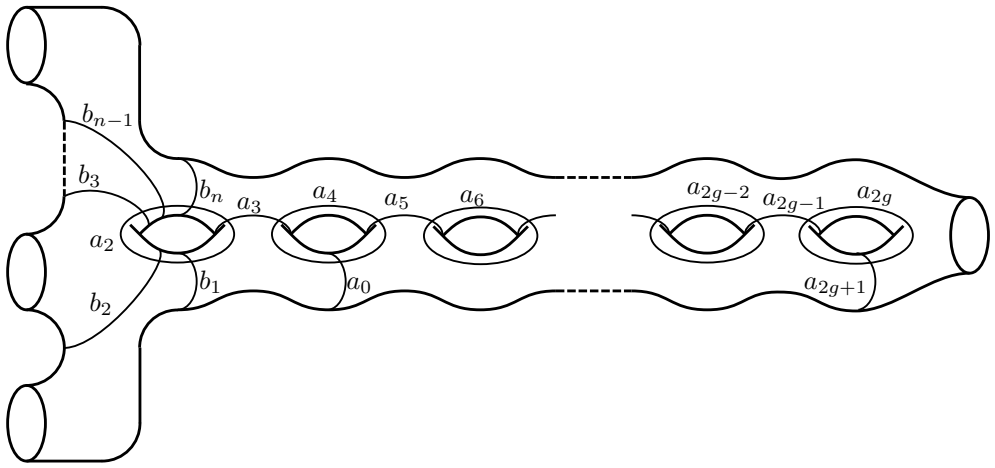

Figure 2.2. Generators for $\mathcal{M}_{g,n}$.

The following is well-known. (It can be found for instance in [22, Prop. 2.10 and Thm. 3.1]).

Proposition 2.3. *Let $g \ge 2$ and $n \ge 1$. Then $\mathcal{M}_{g,n}$ is generated by $T_0, T_2, \dots, T_{2g}, T'_1, \dots, T'_n$.* □

Observation. Let $g \ge 3$ and $n \ge 1$. There is an injective homomorphism $\mathcal{M}_{g-1,n} \to \mathcal{M}_{g,n}$ which sends T'_j to T'_j and T_i to T_i for all $j \in \{1, \dots, n\}$ and $i \in \{0, 2, \dots, 2g - 2\}$. It is easily seen that this homomorphism is induced by some embedding of $\Sigma_{g-1,n}$ into $\Sigma_{g,n}$. From now on we will assume $\mathcal{M}_{g-1,n}$ to be embedded into $\mathcal{M}_{g,n}$ via this homomorphism. Note that such a homomorphism does not exist for $n = 0$.

3 The genus 2 case

In this section we describe all the subgroups of $\mathcal{M}_{2,n}$ of index at most $N_2^+ = 10$ up to conjugation. We will see in particular that the genus $g = 2$ case is different from the genus $g \geq 3$ case.

The first difference comes from the fact that the abelianization of $\mathcal{M}_{2,n}$ is nontrivial, while the group $\mathcal{M}_{g,n}$ is perfect if $g \geq 3$ (see [28], [21]). More precisely, the abelianization of $\mathcal{M}_{2,n}$ is $\mathbb{Z}/10\mathbb{Z}$ [25]. So, if $\mathrm{ab} : \mathcal{M}_{2,n} \to \mathbb{Z}/10\mathbb{Z}$ denotes the projection of $\mathcal{M}_{2,n}$ onto its abelianization, then $\mathrm{ab}^{-1}(\mathbb{Z}/5\mathbb{Z})$ is a subgroup of index 2, $\mathrm{ab}^{-1}(\mathbb{Z}/2\mathbb{Z})$ is a subgroup of index 5, and $\mathrm{Ker}(\mathrm{ab})$ is a subgroup of index 10. Note that all these subgroups contain the commutator subgroup $\mathcal{M}'_{2,n}$. In particular, since $\mathrm{Sp}_4(\mathbb{F}_2)'$ has index 2 in $\mathrm{Sp}_4(\mathbb{F}_2)$, neither $\mathrm{ab}^{-1}(\mathbb{Z}/2\mathbb{Z})$ nor $\mathrm{Ker}(\mathrm{ab})$ is a pre-image under $\theta_{2,n}$ of a subgroup of $\mathrm{Sp}_4(\mathbb{F}_2)$.

The second difference comes from the fact that $\mathrm{Sp}_4(\mathbb{F}_2) = \mathfrak{S}_6$ [10] contains more than two subgroups of index at most 10, up to conjugation. In addition to $O_4^-(\mathbb{F}_2) = \mathfrak{S}_5$ [10] and $O_4^+(\mathbb{F}_2)$, of indices 6 and 10 respectively, it contains the alternating group $\mathfrak{A}_6$ of index 2, and another subgroup of index 6 which can be described as follows. The group $\mathrm{Sp}_4(\mathbb{F}_2) = \mathfrak{S}_6$ has a non-inner automorphism α defined by

$$\alpha : \begin{cases} (1\ 2) \mapsto (1\ 2)(3\ 5)(4\ 6) \\ (2\ 3) \mapsto (1\ 3)(2\ 4)(5\ 6) \\ (3\ 4) \mapsto (1\ 2)(3\ 6)(4\ 5) \\ (4\ 5) \mapsto (1\ 3)(2\ 5)(4\ 6) \\ (5\ 6) \mapsto (1\ 2)(3\ 4)(5\ 6) \end{cases}$$

(Since $\mathrm{Out}(\mathfrak{S}_6)$ has order 2, α is essentially unique.) It turns out that $\alpha(O_4^-(\mathbb{F}_2))$ is a subgroup of $\mathrm{Sp}_4(\mathbb{F}_2)$ of index 6 which is not conjugate to $O_4^-(\mathbb{F}_2)$. On the other hand, $\alpha(O_4^+(\mathbb{F}_2))$ is conjugate to $O_4^+(\mathbb{F}_2)$ (so there are four subgroups and not five), and $\mathrm{ab}^{-1}(\mathbb{Z}/5\mathbb{Z}) = \theta_2^{-1}(\mathfrak{A}_6)$. Note also that $\mathrm{Out}(\mathfrak{S}_n)$ is trivial if $n \neq 6$.

So, we have the following subgroups of index at most 10 in $\mathcal{M}_{2,n}$ up to conjugation:

- $\theta_{2,n}^{-1}(\mathfrak{A}_6) = \mathrm{ab}^{-1}(\mathbb{Z}/5\mathbb{Z})$ of index 2,
- $\mathrm{ab}^{-1}(\mathbb{Z}/2\mathbb{Z})$ of index 5,
- $\theta_{2,n}^{-1}(O_4^-(\mathbb{F}_2))$ of index 6,
- $\theta_{2,n}^{-1}(\alpha(O_4^-(\mathbb{F}_2)))$ of index 6,
- $\mathrm{Ker}(\mathrm{ab})$ of index 10, and
- $\theta_{2,n}^{-1}(O_4^+(\mathbb{F}_2))$ of index 10.

We show that these are all the proper subgroups of index at most 10 in $\mathcal{M}_{2,n}$ up to conjugation.

Let $n \geq 1$, $m \geq 1$ and $w \in \mathfrak{S}_m$. If $w^{10} = 1$, then there is a permutation representation $\mathrm{cycl}_w : \mathcal{M}_{2,n} \to \mathfrak{S}_m$ which sends T_i and T'_j to w for all $i \in \{0, 2, 3, 4\}$ and all $j \in \{1, \ldots, n\}$. Such a representation is called a *cyclic representation* of $\mathcal{M}_{2,n}$. It is transitive if and only if w is a cycle of length m and $m \in \{1, 2, 5, 10\}$.

Lemma 3.1. *For $n \geq 1$, there are exactly three conjugacy classes of non-cyclic transitive permutation representations of $\mathcal{M}_{2,n}$ of degree at most 10, namely, two conjugacy classes of degree 6, and a unique conjugacy class of degree 10. More specifically, up to conjugacy in $\mathfrak{S}_6$, the two transitive permutation representations $\mathcal{M}_{2,n} \to \mathfrak{S}_6$ are given by*

$$\phi_{2,n}^{-} : \begin{cases} T_j' \mapsto (1\ 2) & \text{for } 1 \leq j \leq n \\ T_2 \mapsto (2\ 3) \\ T_3 \mapsto (3\ 4) \\ T_4 \mapsto (4\ 5) \\ T_0 \mapsto (5\ 6) \end{cases}$$

$$\phi_{n}^{\alpha} : \begin{cases} T_j' \mapsto (1\ 2)(3\ 5)(4\ 6) & \text{for } 1 \leq j \leq n \\ T_2 \mapsto (1\ 3)(2\ 4)(5\ 6) \\ T_3 \mapsto (1\ 2)(3\ 6)(4\ 5) \\ T_4 \mapsto (1\ 3)(2\ 5)(4\ 6) \\ T_0 \mapsto (1\ 2)(3\ 4)(5\ 6) \end{cases}$$

and, up to conjugacy in $\mathfrak{S}_{10}$, the unique permutation representation $\mathcal{M}_{2,n} \to \mathfrak{S}_{10}$ is given by

$$\phi_{2,n}^{+} : \begin{cases} T_j' \mapsto (3\ 5)(6\ 8)(9\ 10) & \text{for } 1 \leq j \leq n \\ T_2 \mapsto (2\ 3)(4\ 6)(7\ 9) \\ T_3 \mapsto (1\ 2)(6\ 10)(8\ 9) \\ T_4 \mapsto (2\ 4)(3\ 6)(5\ 8) \\ T_0 \mapsto (4\ 7)(6\ 9)(8\ 10) \end{cases}$$

Proof. In the case $n = 1$, this result can be easily proved with a direct calculation. Using the presentation of $\mathcal{M}_{2,1}$ from Theorem 2.1, one can use coset enumeration techniques to perform a systematic search for representatives of the conjugacy classes of subgroups of $\mathcal{M}_{2,1}$ of index at most K for a (small) integer K; see [30]. When $K = 10$, this systematic search shows that there are exactly six conjugacy classes of proper subgroups of $\mathcal{M}_{2,1}$ of index at most 10; the columns of the coset table for the each of the constructed subgroups yield the images of the generators $T_0, \ldots, T_4$ under the corresponding permutation representation. The computation is very easy and can be performed with any mathematical software such as MAGMA or GAP.
Now suppose that $n \geq 2$. Let $\varphi : \mathcal{M}_{2,n} \to \mathfrak{S}_m$ be a non-cyclic and transitive representation with $m \leq 10$. For $1 \leq j \leq n$, we denote by $\mathcal{M}^{(j)}$ the subgroup of $\mathcal{M}_{2,n}$ generated by T_j', T_2, T_3, T_4, T_0. This group is isomorphic to $\mathcal{M}_{2,1}$ via an isomorphism $\gamma_j : \mathcal{M}_{2,1} \to \mathcal{M}^{(j)}$ which sends T_1 to T_j' and T_i to T_i for all $i \in \{2, 3, 4, 0\}$. We denote by $\varphi_j : \mathcal{M}_{2,1} \to \mathfrak{S}_m$ the composition of γ_j with φ. Observe that

(∗) $\varphi_j(T_i) = \varphi(T_i)$ for all $j \in \{1, \ldots, n\}$ and $i \in \{0, 2, 3, 4\}$.

By the case $n = 1$, for each $j \in \{1, \ldots, n\}$ there is a decomposition $\{1, \ldots, m\} = S_j^{(1)} \sqcup S_j^{(2)} \sqcup S_j^{(3)}$ as follows. Each $S_j^{(k)}$ is invariant under the action of $\varphi_j(\mathcal{M}_{2,1})$; either $S_j^{(1)} = \emptyset$, or φ_j restricted to $S_j^{(1)}$ is equivalent to an element of $\{\phi_{2,1}^{-}, \phi_1^{\alpha}, \phi_{2,1}^{+}\}$; if $S_j^{(2)}$ is nonempty, then there exists $w_j \in \mathfrak{S}_m - \{1\}$ such that $S(w_j) = S_j^{(2)}$ and the restriction of φ_j to $S_j^{(2)}$ is cycl_{w_j}; and $\varphi_j(\mathcal{M}_{2,1})$ acts trivially on $S_j^{(3)}$.

Let $\phi \in \{\phi_{2,1}^-, \phi_1^\alpha, \phi_{2,1}^+\}$ and set $N = N_\phi = 6$ if $\phi = \phi_{2,1}^-$ or ϕ_1^α, and $N = N_\phi = 10$ if $\phi = \phi_{2,1}^+$. The following claims are readily verified from the description of ϕ, using either GAP or MAGMA where necessary:

(1) $\phi(T_2)$ and $\phi(T_3)$ have no common cycle in their decompositions;

(2) $S(\{\phi(T_i) \mid i = 1, 3, 4, 0\}) = \{1, \dots, N\}$, where, for $X \subseteq \mathfrak{S}_N$, $S(X)$ denotes $\cup_{w \in X} S(w)$;

(3) the (simultaneous) centralizer of $\{\phi(T_i) \mid i = 1, 3, 4, 0\}$ in $\mathfrak{S}_N$ is $\{1, \phi(T_1)\}$;

(4) the support of each cycle in the decomposition of $\phi(T_1)$ intersects $S(\{\phi(T_i) \mid i = 0, 2, 3, 4\})$ nontrivially.

We first show that each $S_j^{(2)} = \emptyset$. Whenever $S_j^{(2)} \neq \emptyset$, then by (1) we get that w_j is the product of the common nontrivial cycles of $\varphi_j(T_2)$ and $\varphi_j(T_3)$. However, by $(*)$, these common cycles are independent of choice of j. It follows that for all $j \in \{1, \dots, n\}$, $S_j^{(2)} \neq \emptyset$, $w_j = w_1$ and $S_j^{(2)} = S(w_j) = S(w_1) = S_1^{(2)}$. However, φ is transitive and non-cyclic. Hence, $S_j^{(2)} = \emptyset$ for all $j \in \{1, \dots, n\}$.

It now follows that each $S_j^{(1)} \neq \emptyset$, and therefore, the restriction of each φ_j to $S_j^{(1)}$ is equivalent to an element of $\{\phi_{2,1}^-, \phi_1^\alpha, \phi_{2,1}^+\}$. Since we know by $(*)$ that for each $i \neq 1$ the $\varphi_j(T_i)$ agree, it remains to show that all the $\varphi_j(T_1)$ also coincide, and that each $S_j^{(3)}$ is empty.

Without loss of generality we can assume that $S_1^{(1)} = \{1, \dots, N\}$ and the restriction of φ_1 to $\{1, \dots, N\}$ is an element ϕ in $\{\phi_{2,1}^-, \phi_1^\alpha, \phi_{2,1}^+\}$, where $N = N_\phi$. Let $j \in \{1, \dots, n\}$. Since T_j' commutes with T_1', T_3, T_4, T_0, the permutation $\varphi_j(T_1)$ belongs to the centralizer of $\{\varphi_1(T_i) \mid i = 1, 3, 4, 0\}$. Combining (2) and (3) we get that this centralizer is $\{1, \phi(T_1)\} \times \mathfrak{S}_{m-N}$. On the other hand, by (4), the support of each cycle of $\varphi_j(T_1)$ intersects $S(\{\varphi_j(T_i) \mid i = 0, 2, 3, 4\})$ nontrivially, and, by $(*)$,

$$S(\{\varphi_j(T_i) \mid i = 0, 2, 3, 4\}) = S(\{\varphi_1(T_i) \mid i = 0, 2, 3, 4\}) \subseteq \{1, \dots, N\}.$$

This implies that $\varphi_j(T_1) = \phi(T_1)$ and, therefore, each $\varphi_j(T_1)$ is the same. Then, finally, by transitivity, it must be that $m = N$, and the proof is complete. □

Proposition 3.2. *Let $n \geq 0$. Then $\mathcal{M}_{2,n}$ has precisely six proper subgroups of index at most 10 up to conjugation, namely,* $\mathrm{ab}^{-1}(\mathbb{Z}/5\mathbb{Z}) = \theta_{2,n}^{-1}(\mathfrak{A}_6)$ *of index 2,* $\mathrm{ab}^{-1}(\mathbb{Z}/2\mathbb{Z})$ *of index 5,* $\theta_{2,n}^{-1}(O_4^-(\mathbb{F}_2))$ *of index 6,* $\theta_{2,n}^{-1}(\alpha(O_4^-(\mathbb{F}_2)))$ *of index 6,* $\mathrm{Ker}(\mathrm{ab})$ *of index 10, and* $\theta_{2,n}^{-1}(O_4^+(\mathbb{F}_2))$ *of index 10.*

Proof. For $n \geq 1$, the claim is a direct consequence of Lemma 3.1 together with the description of the subgroups of $\mathcal{M}_{2,n}$ given in the beginning of the section. By Theorem 2.1, $\mathcal{M}_{2,0}$ is a quotient of $\mathcal{M}_{2,1}$ by one additional relation, so for the case $n = 0$ it is sufficient to check that the representations of $\mathcal{M}_{2,1}$ given in Lemma 3.1 satisfy the additional relation of $\mathcal{M}_{2,0}$; this is the case, as can easily be verified. □

4 The genus 3 case

In this section we calculate the subgroups of index at most 36 in $\mathcal{M}_{3,n}$ up to conjugation. (Note that $N_3^- = 28$ and $N_3^+ = 36$.) We argue in the same manner as for the case of genus 2 surfaces (see Section 3), with direct calculations often made with computers. However, we should point out here that, in this case, the computations are far from being elementary, and we often approach the limit of what can currently be done with computers (especially in the proof of Lemma 4.1). Recall also that the case of surfaces of genus $g = 3$ will be the first step in the induction to prove Theorem 0.4.

Lemma 4.1. *For $n \geq 1$, there are exactly two conjugacy classes of nontrivial transitive permutation representations of $\mathcal{M}_{3,n}$ of degree at most 36, namely a unique conjugacy class of degree 28 and a unique conjugacy class of degree 36. More specifically, up to conjugacy in $\mathfrak{S}_{28}$, the unique permutation representation $\mathcal{M}_{3,n} \to \mathfrak{S}_{28}$ is given by*

$$\phi_{3,n}^- : \begin{cases} T_j' \mapsto (14\ 18)(16\ 21)(17\ 22)(19\ 23)(24\ 26)(27\ 28) \text{ for } 1 \leq j \leq n \\ T_0 \mapsto (1\ 3)(2\ 5)(4\ 8)(20\ 25)(24\ 28)(26\ 27) \\ T_2 \mapsto (10\ 14)(12\ 16)(13\ 17)(15\ 19)(20\ 24)(25\ 28) \\ T_3 \mapsto (6\ 10)(7\ 12)(9\ 13)(11\ 15)(24\ 27)(26\ 28) \\ T_4 \mapsto (3\ 6)(4\ 7)(5\ 9)(15\ 20)(19\ 24)(23\ 26) \\ T_5 \mapsto (2\ 4)(5\ 8)(6\ 11)(10\ 15)(14\ 19)(18\ 23) \\ T_6 \mapsto (1\ 2)(3\ 5)(6\ 9)(10\ 13)(14\ 17)(18\ 22) \end{cases}$$

and, up to conjugacy in $\mathfrak{S}_{36}$, the unique permutation representation $\mathcal{M}_{3,n} \to \mathfrak{S}_{36}$ is given by

$$\phi_{3,n}^+ : \begin{cases} T_j' \mapsto (6\ 9)(10\ 13)(14\ 18)(15\ 19)(20\ 22)(21\ 25)(26\ 28)(27\ 30)(31\ 32)(34\ 35) \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{for } 1 \leq j \leq n \\ T_0 \mapsto (1\ 2)(11\ 17)(14\ 22)(16\ 24)(18\ 20)(21\ 28)(23\ 29)(25\ 26)(27\ 32)(30\ 31) \\ T_2 \mapsto (4\ 6)(7\ 10)(11\ 14)(12\ 15)(16\ 21)(17\ 22)(23\ 27)(24\ 28)(29\ 32)(33\ 35) \\ T_3 \mapsto (3\ 4)(5\ 7)(8\ 12)(14\ 20)(18\ 22)(21\ 26)(25\ 28)(27\ 31)(30\ 32)(33\ 36) \\ T_4 \mapsto (2\ 3)(7\ 11)(10\ 14)(12\ 16)(13\ 18)(15\ 21)(19\ 25)(29\ 33)(31\ 34)(32\ 35) \\ T_5 \mapsto (3\ 5)(4\ 7)(6\ 10)(9\ 13)(16\ 23)(21\ 27)(24\ 29)(25\ 30)(26\ 31)(28\ 32) \\ T_6 \mapsto (5\ 8)(7\ 12)(10\ 15)(11\ 16)(13\ 19)(14\ 21)(17\ 24)(18\ 25)(20\ 26)(22\ 28) \end{cases}$$

In particular, $\mathrm{mi}(\mathcal{M}_{3,n}) = 28$.

Proof. In the case $n = 1$, the result is shown by a direct computation. Using the presentation of $\mathcal{M}_{3,1}$ from Theorem 2.1, one can use coset enumeration techniques to perform a systematic search for representatives of the conjugacy classes of subgroups of $\mathcal{M}_{3,1}$ of index at most K for a (small) integer K; see [30]. When $K = 36$, this systematic search shows that there are exactly two conjugacy classes of proper subgroups of $\mathcal{M}_{3,1}$ of index at most 36: exactly one conjugacy class of subgroups of index 28 and exactly one conjugacy class of subgroups of index 36. The columns of the coset table for each of the constructed subgroups yield the images of the generators $T_0, \ldots, T_6$ under the corresponding permutation representations $\phi_{3,1}^-$ of degree 28 and $\phi_{3,1}^+$ of degree 36.

We used the implementation of the low index subgroup search provided in MAGMA [4], filling the coset table in column major order. We ran a development version of MAGMA V2.15. The computation took approximately 47.5 hours on a GNU / Linux system with an Intel E8400 64-bit

CPU (core: 3 GHz, FSB: 1333 MHz) and a main memory bandwidth of 6.5 GB/s (X38 chipset, dual channel DDR2 RAM, memory bus: 1066 MHz). We remark that the use of column major order is crucial for the running time; tests for indices between 10 and 15 suggest a speed-up by a factor between 10^3 and 10^4 compared to row major order.

Now suppose that $n \geq 2$. Let $\varphi : \mathcal{M}_{3,n} \to \mathfrak{S}_m$ be a transitive representation with $m \leq 36$. For $1 \leq j \leq n$, we denote by $\mathcal{M}^{(j)}$ the subgroup of $\mathcal{M}_{3,n}$ generated by $T'_j, T_2, \ldots, T_6, T_0$. This group is isomorphic to $\mathcal{M}_{3,1}$ via an isomorphism $\gamma_j : \mathcal{M}_{3,1} \to \mathcal{M}^{(j)}$ which sends T_1 to T'_j and T_i to T_i for all $i \in \{2, \ldots, 6, 0\}$. We denote by $\varphi_j : \mathcal{M}_{3,1} \to \mathfrak{S}_m$ the composition of γ_j with φ. Observe that

(∗) $\varphi_j(T_i) = \varphi(T_i)$ for all $j \in \{1, \ldots, n\}$ and $i \in \{0, 2, \ldots, 6\}$.

By the case $n = 1$, for each $j \in \{1, \ldots, n\}$ there is a decomposition $\{1, \ldots, m\} = S_j^{(1)} \sqcup S_j^{(2)}$ as follows. Each $S_j^{(k)}$ is invariant under the action of $\varphi_j(\mathcal{M}_{3,1})$; the restriction of φ_j to $S_j^{(1)}$ is equivalent to an element of $\{\phi_{3,1}^-, \phi_{3,1}^+\}$; and $\varphi_j(\mathcal{M}_{3,1})$ acts trivially on $S_j^{(2)}$. (Note here a difference from the $g = 2$ case: because $\mathcal{M}_{3,1}$ is a perfect group [28] it has no cyclic representations.)

Let $\phi \in \{\phi_{3,1}^-, \phi_{3,1}^+\}$ and set $N = N_\phi = 28$ if $\phi = \phi_{3,1}^-$, and $N = N_\phi = 36$ if $\phi = \phi_{3,1}^+$. Again, the following claims may be confirmed from the description of ϕ, using either GAP or MAGMA where necessary:

(1) $S(\{\phi(T_i) \mid i = 1, 3, 4, 5, 6, 0\}) = \{1, \ldots, N\}$, where, for $X \subseteq \mathfrak{S}_N$, $S(X)$ denotes $\cup_{w \in X} S(w)$;

(2) the unique element of the centralizer of $\{\phi(T_i) \mid i = 1, 3, 4, 5, 6, 0\}$ in $\mathfrak{S}_N$ having the same cycle decomposition type as $\phi(T_1)$ is $\phi(T_1)$;

(3) the support of each nontrivial cycle in the decomposition of $\phi(T_1)$ intersects $S(\{\phi(T_i) \mid i = 0, 2, 3, 4, 5, 6\})$ nontrivially.

Without loss of generality we can assume that $S_1^{(1)} = \{1, \ldots, N\}$ and the restriction of φ_1 to $\{1, \ldots, N\}$ is an element ϕ in $\{\phi_{3,1}^-, \phi_{3,1}^+\}$, where $N = N_\phi$. Let $j \in \{1, \ldots, n\}$. Since T'_j commutes with $T'_1, T_3, T_4, T_5, T_6, T_0$, the permutation $\varphi_j(T_1)$ belongs to the centralizer of $\{\varphi_1(T_i) \mid i = 1, 3, 4, 5, 6, 0\}$. By (1), this centralizer is $Z \times \mathfrak{S}_{m-N}$, where Z is the centralizer of $\{\phi(T_i) \mid i = 1, 3, 4, 5, 6, 0\}$ in $\mathfrak{S}_N$. By (3), the support of each nontrivial cycle of $\varphi_j(T_1)$ intersects $S(\{\varphi_j(T_i) \mid i = 0, 2, 3, 4, 5, 6\})$ nontrivially, and, by (∗),

$$\begin{aligned} &S(\{\varphi_j(T_i) \mid i = 0, 2, 3, 4, 5, 6\}) \\ =&S(\{\varphi_1(T_i) \mid i = 0, 2, 3, 4, 5, 6\}) \\ \subseteq&\{1, \ldots, N\}. \end{aligned}$$

Thus, $\varphi_j(T_1) \in Z$. Now, since T'_j and T'_1 are conjugate in $\mathcal{M}_{3,1}$, $\varphi_j(T_1)$ and $\varphi_1(T_1)$ share the same cycle decomposition type; hence, by (2), $\varphi_j(T_1) = \varphi_1(T_1)$. To complete the proof, observe that transitivity forces $m = N$. □

Proposition 4.2. *Let $n \geq 0$. Then $\mathcal{M}_{3,n}$ has precisely two proper subgroups of index at most 36 up to conjugation, namely, $\mathcal{O}_{3,n}^-$ of index 28, and $\mathcal{O}_{3,n}^+$ of index 36.*

Proof. For $n \geq 1$, the claim is a direct consequence of Lemma 4.1 and the definitions of $\mathcal{O}^-_{3,n}$ respectively $\mathcal{O}^+_{3,n}$. By Theorem 2.1, $\mathcal{M}_{3,0}$ is a quotient of $\mathcal{M}_{3,1}$ by one additional relation, so for the case $n = 0$ it is sufficient to check that the representations of $\mathcal{M}_{3,1}$ given in Lemma 4.1 satisfy the additional relation of $\mathcal{M}_{3,0}$; this is the case, as can easily be verified. □

Part II
Induction arguments

We turn now to the proof of our main result, Theorem 0.4. As pointed out before, we argue by induction on the genus. Recall that the case $g = 3$ is proved in Section 4 (see Proposition 4.2). Thus:

- *from now on, we suppose that $g \geq 4$ plus the inductive hypothesis that Theorem 0.4 holds for a surface of genus $g - 1$.*

Recall that we have defined $N_g^- = 2^{g-1}(2^g - 1)$ and $N_g^+ = 2^{g-1}(2^g + 1)$. Throughout the arguments below, we shall rely on the following numerical relationships for $g \geq 4$.

$$N_g^+ = 3\,N_{g-1}^+ + N_{g-1}^-\,, \quad N_g^- = 3\,N_{g-1}^- + N_{g-1}^+\,,$$
$$4\,N_{g-1}^- < N_g^- < N_g^+ < 5\,N_{g-1}^- < 2\,N_g^-\,.$$

(Actually, only the third inequality requires $g \geq 4$; the others hold for $g \geq 2$.)
Theorem 0.3 will be entirely proved in Section 6. Theorem 0.5 will be proved in Sections 7 and 8.

5 Factorization through symplectic groups

Our goal in this section is to prove the following theorem.

Theorem 5.1. *For $g \geq 4$, let $\varphi : \mathcal{M}_{g,1} \to \mathfrak{S}_m$ be a nontrivial homomorphism, with $m < 5\,N_{g-1}^-$. Then there is a homomorphism $\bar{\varphi} : \mathrm{Sp}_{2g}(\mathbb{F}_2) \to \mathfrak{S}_m$ such that the following diagram commutes.*

$$\begin{array}{ccc} \mathcal{M}_{g,1} & & \\ {\scriptstyle \theta_{g,1}}\downarrow & \searrow^{\varphi} & \\ \mathrm{Sp}_{2g}(\mathbb{F}_2) & \xrightarrow[\bar{\varphi}]{} & \mathfrak{S}_m \end{array}$$

The proof strategy is as follows. To show that the kernel of φ contains the kernel of $\theta_{g,1}$, we first prove that the image $w_i = \varphi(T_i)$ has order 2 in $\mathfrak{S}_m$. For this, we consider the cycle decomposition type $(1)^{\ell_1}(2)^{\ell_2}\cdots(m)^{\ell_m}$ of the permutation w_i. We first exclude the possibility of cycles of length at least 5, then of cycles of length 4, and finally – the most delicate case – we exclude cycles of length 3. Hence, w_i is reduced to being an involution after all. It then remains to show that the kernel of $\theta_{g,1}$ is the normal closure of the square of any of our standard generators of $\mathcal{M}_{g,1}$.

Proposition 5.2. *Let $g \geq 4$, and let b be a nonseparating simple closed curve in $\Sigma_{g,1}$. Then the centralizer $\mathcal{Z}_b$ of T_b in $\mathcal{M}_{g,1}$ contains an index 2 subgroup $\mathcal{Z}_b^+$ with the properties:*

(a) $\mathcal{Z}_b^+$ is perfect;

(b) $N_{g-1}^- \leq \mathrm{mi}(\mathcal{Z}_b^+)$; and

(c) $T_b \in \mathcal{Z}_b^+$.

Proof. It is known that $\mathcal{Z}_b$ is the set of mapping classes that fix the curve b up to isotopy (see *e.g.* [27]). We take $\mathcal{Z}_b^+$ to be the subgroup of $\mathcal{Z}_b$ consisting of those classes that also preserve the orientation of b. Evidently, $\mathcal{Z}_b^+$ has index 2 in $\mathcal{Z}_b$ and contains T_b. From [27], $\mathcal{Z}_b^+$ is the image of $\mathcal{M}_{g-1,3}$ in $\mathcal{M}_{g,1}$ under the homomorphism induced by a quotient map $\Sigma_{g-1,3} \to \Sigma_{g,1}$ identifying two boundary circles with the closed curve b. Since by [16] $\mathcal{M}_{g-1,3}$ is perfect, we have (a). From the epimorphism $\mathcal{M}_{g-1,3} \to \mathcal{Z}_b^+$ we know that $\mathrm{mi}(\mathcal{M}_{g-1,3}) \leq \mathrm{mi}(\mathcal{Z}_b^+)$, and by induction we have $\mathrm{mi}(\mathcal{M}_{g-1,3}) = N_{g-1}^-$, thus $N_{g-1}^- \leq \mathrm{mi}(\mathcal{Z}_b^+)$. □

As ever, we consider the simple closed curves $a_0, a_1, \ldots, a_{2g+1}$ illustrated in Figure 2.1, we denote by T_i the Dehn twist about a_i, and write w_i for the image under φ of the Dehn twist T_i $(i = 0, 1, \ldots, 2g+1)$. In the sequel we repeatedly use the fact that, since T_i and T_j are conjugate in the mapping class group, $w_i = \varphi(T_i)$ and $w_j = \varphi(T_j)$ are conjugate in the symmetric group, and so share the same cycle decomposition type, say $(1)^{\ell_1}(2)^{\ell_2}\cdots(m)^{\ell_m}$, where $\sum_{k=1}^m k\ell_k = m$. The fact that $T_i \in \mathcal{Z}_{a_i}^+$ implies that, whenever $\ell_k > 0$ with $k > 1$, $\varphi(\mathcal{Z}_{a_i}^+)$ acts nontrivially on the union of the k-orbits of w_i. Therefore, the above proposition combines with Lemma 1.1 (3) (a), (c) to yield the following.

Corollary 5.3. *For $g \geq 4$, let $\varphi : \mathcal{M}_{g,1} \to \mathfrak{S}_m$ be a nontrivial homomorphism, with $m < 5N_{g-1}^-$. Then there exists $k \in \{2, 3, 4\}$ such that every w_i has the same cycle decomposition type $(1)^{\ell_1}(k)^{\ell_k}$ with $\ell_k \geq N_{g-1}^-$.* □

Lemma 5.4. *For $g \geq 3$, let $\varphi : \mathcal{M}_{g,1} \to \mathfrak{S}_m$ be a group homomorphism. If $S(w_{2g-2}) \cap S(w_{2g}) = \emptyset$, then φ is trivial.*

Proof. First note that, since conjugate permutations have bijective supports, by Lemma 2.2 the cardinality $r = |S(w_i)|$ is independent of choice of i, and for all 3-chains (a_i, a_j, a_k) yields the same cardinalities $s = |S(w_i) \cap S(w_j)|$ and $t = |S(w_i) \cap S(w_k)|$. By assumption, the 3-chain $(a_{2g-2}, a_{2g-1}, a_{2g})$ gives $t = 0$, which implies that

$$(S(w_{2g-2}) \cap S(w_{2g-1})) \sqcup (S(w_{2g-1}) \cap S(w_{2g})) \subseteq S(w_{2g-1})\,,$$

and so $r \geq 2s$. On the other hand, Lemma 1.2 asserts that $r \leq 2s$. Thus, for any 3-chain (a_i, a_j, a_k) we have

$$S(w_j) = (S(w_i) \cap S(w_j)) \sqcup (S(w_j) \cap S(w_k))\,.$$

Turning now to the 3-chains (a_0, a_4, a_3) and (a_0, a_4, a_5) and (a_3, a_4, a_5), we observe that, since $t = 0$, the subsets $S(w_0) \cap S(w_4)$, $S(w_3) \cap S(w_4)$ and $S(w_4) \cap S(w_5)$ of $S(w_4)$ are pairwise disjoint, but each of cardinality half that of $S(w_4)$. For avoidance of contradiction, it must be that $r = s = 0$; whence, since by Theorem 2.1 the image of φ is generated by the w_i, φ is trivial. □

Proposition 5.5. *For $g \geq 4$, let $\varphi : \mathcal{M}_{g,1} \to \mathfrak{S}_m$ with $m < 5N_{g-1}^-$. Then for $i = 0, 1, \ldots, 2g+1$ there are no 4-cycles in the cycle decomposition of w_i.*

Proof. Again write ℓ_k for the number of k-cycles in the decomposition of w_{2g}, and suppose that $\ell_4 > 0$. Then Corollary 5.3 forces the cycle decomposition type of every w_j to be $(1)^{\ell_1}(4)^{\ell_4}$ where $\ell_4 \geq N_{g-1}^-$. The image $\varphi(\mathcal{M}_{g,1})$ contains the subgroup $H = \langle w_{2g}, w_{2g+1}\rangle$, which, since w_{2g} is a product of 4-cycles, is a homomorphic image (via $x_i \mapsto w_{2g+i}$) of the group

$$\widehat{H} = \langle x_0, x_1 \mid x_0^4 = x_1^4 = 1,\ x_0x_1x_0 = x_1x_0x_1\rangle$$

of order 96 (denoted $\langle -2, 3 \,|\, 4\rangle$ in [9, p.74]).
From now on $\mathcal{M}_{g-1,1}$ is considered as the subgroup of $\mathcal{M}_{g,1}$ generated by $T_0, T_1, \ldots, T_{2g-2}$. We write $\widehat{\Omega}_k$ for the union of the orbits $\Omega_{k,i}$ $(i = 1, \ldots, h_k)$ of cardinality k of H. Thus, $|\widehat{\Omega}_k| = kh_k$ and k divides 96. From the fact that the generators w_{2g} and w_{2g+1} of H contain no nontrivial cycles of length less than 4 it follows that $h_2 = h_3 = 0$. Since $\varphi(\mathcal{M}_{g-1,1})$ lies in the centralizer of H, it acts, for any k, both on $\widehat{\Omega}_k$ and on the set $\{\Omega_{k,i} \mid i = 1, \ldots, h_k\}$. The former corresponds to a homomorphism $\psi_k : \mathcal{M}_{g-1,1} \to \mathfrak{S}_{kh_k}$ and the latter to a homomorphism $\nu_k : \mathcal{M}_{g-1,1} \to \mathfrak{S}_{h_k}$.

Claim. *If ν_k is trivial, then so is ψ_k.*

To prove this, since $\nu_1 = \psi_1$ we may assume that $k \geq 4$. Assuming that ν_k is trivial, we observe that each k-orbit $\Omega_{k,i}$ of H must be invariant under the action of $\varphi(\mathcal{M}_{g-1,1})$. Now partition $\Omega_{k,i}$ by means of the orbits of w_{2g}, as

$$\Omega_{k,i} = \mathcal{P}_1 \sqcup \cdots \sqcup \mathcal{P}_p \sqcup F\,,$$

where each orbit $\mathcal{P}_j$ of w_{2g} has length 4, and F consists of the fixed points of w_{2g}. Then $\varphi(\mathcal{M}_{g-1,1})$ acts on $\mathcal{P}_1 \sqcup \cdots \sqcup \mathcal{P}_p$, on $\{\mathcal{P}_1, \cdots, \mathcal{P}_p\}$, and on F. The action on the set $\{\mathcal{P}_1, \ldots, \mathcal{P}_p\}$ must be trivial because

$$p \leq \frac{k}{4} \leq \frac{96}{4} < 2^{g-2}(2^{g-1} - 1) = N_{g-1}^- = \mathrm{mi}(\mathcal{M}_{g-1,1})$$

(by induction). This leaves $\varphi(\mathcal{M}_{g-1,1})$ acting on each 4-orbit $\mathcal{P}_j$, where the action must again be trivial, since certainly $4 < \mathrm{mi}(\mathcal{M}_{g-1,1})$. Hence, the action of $\varphi(\mathcal{M}_{g-1,1})$ on $\Omega_{k,i}$ stabilises $\Omega_{k,i} \cap S(w_{2g})$ pointwise, and likewise $\Omega_{k,i} \cap S(w_{2g+1})$. However, since H is generated by w_{2g} and w_{2g+1}, the union of $\Omega_{k,i} \cap S(w_{2g})$ and $\Omega_{k,i} \cap S(w_{2g+1})$ is equal to $\Omega_{k,i}$. Thus, the action of $\varphi(\mathcal{M}_{g-1,1})$ is trivial on each $\Omega_{k,i}$, and therefore also on their union $\widehat{\Omega}_k$ as required.
In consequence, if $\varphi(\mathcal{M}_{g-1,1})$ acts nontrivially on some $\widehat{\Omega}_k$, then $h_k \geq \mathrm{mi}(\mathcal{M}_{g-1,1})$. Since

$$kh_k = |\widehat{\Omega}_k| \leq m < 5\,N_{g-1}^- = 5\,\mathrm{mi}(\mathcal{M}_{g-1,1})\,,$$

the only possibilities are $k = 1$ or $k = 4$. From Lemma 5.4, $\mathcal{M}_{g-1,1}$ must act nontrivially on some $\widehat{\Omega}_k$ with $k > 1$, and therefore $k = 4$ indeed occurs.
The inequality $h_4 \geq N_{g-1}^-$ implies that $h_1 \leq m - 4h_4 < N_{g-1}^-$, thus $\mathcal{M}_{g-1,1}$ acts trivially on $\widehat{\Omega}_1$. It follows that

$$S(\varphi(\mathcal{M}_{g-1,1})) \subseteq \widehat{\Omega}_4 \subseteq S(H)\,,$$

where, for a subgroup G of $\mathfrak{S}_m$, $S(G)$ denotes its support. Since $S(\varphi(\mathcal{M}_{g-1,1}))$ contains $S(\langle w_1, w_2\rangle)$, which by Lemma 2.2 has the same cardinality as $S(H)$, the above inclusions are indeed equalities.

So, w_{2g} is a product of 4-cycles and all nontrivial orbits of $H = \langle w_{2g}, w_{2g+1}\rangle$ have length 4. Applying again Lemma 2.2, we get that w_4 is a product of 4-cycles and, for $i \in \{0,3,5\}$, all nontrivial orbits of $\langle w_4, w_i\rangle$ have length 4. By Lemma 1.5 we deduce that $w_0 = w_3 = w_5$. But, since $w_3 = w_5$, we also have

$$w_3 = (w_5w_6)w_3(w_5w_6)^{-1} = (w_5w_6)w_5(w_5w_6)^{-1} = w_6\,.$$

Thus $w_5 = w_6$, and therefore $w_0 = w_1 = \cdots = w_{2g}$. It follows that the image of φ is cyclic, and hence, because $\mathcal{M}_{g,1}$ is perfect, φ is trivial – a contradiction. □

Proposition 5.6. *For $g \geq 4$, let $\varphi : \mathcal{M}_{g,1} \to \mathfrak{S}_m$ with $m < 5N^-_{g-1}$. Then for $0 \leq i \leq 2g+1$ there are no 3-cycles in the cycle decomposition of w_i.*

Proof. Suppose to the contrary that $\ell_3 > 0$. In particular, φ cannot be trivial. Then Corollary 5.3 forces the cycle decomposition type of each w_i to be $(1)^{\ell_1}(3)^{\ell_3}$ where $\ell_3 \geq N^-_{g-1}$. The image $\varphi(\mathcal{M}_{g,1})$ contains the subgroup $H = \langle w_{2g}, w_{2g+1}\rangle$, which, since w_{2g} is a product of 3-cycles, is a homomorphic image (via $x_i \mapsto w_{2g+i}$) of the group

$$\widehat{H} = \langle x_0, x_1 \mid x_0^3 = x_1^3 = 1,\ x_0x_1x_0 = x_1x_0x_1\rangle$$

of order 24. Again, we consider $\mathcal{M}_{g-1,1}$ as the subgroup of $\mathcal{M}_{g,1}$ generated by $T_0, T_1, \ldots, T_{2g-2}$. Moreover, we write $\widehat{\Omega}_k$ for the union of the orbits $\Omega_{k,i}$ $(i = 1, \ldots, h_k)$ of cardinality k of H. Thus, $|\widehat{\Omega}_k| = kh_k$ and k divides 24. From the fact that the generators w_{2g} and w_{2g+1} of H contain no nontrivial cycles of length less than 3 it follows that $h_2 = 0$.
Since $\varphi(\mathcal{M}_{g-1,1})$ lies in the centralizer of H, it acts, for any k, both on $\widehat{\Omega}_k$ and on the set $\{\Omega_{k,i} \mid i = 1, \ldots, h_k\}$. The former corresponds to a homomorphism $\psi_k : \mathcal{M}_{g-1,1} \to \mathfrak{S}_{kh_k}$ and the latter to a homomorphism $\nu_k : \mathcal{M}_{g-1,1} \to \mathfrak{S}_{h_k}$.

Claim 1. *If ν_k is trivial, then so is ψ_k.*

Indeed, suppose that ν_k is trivial. Then each k-orbit $\Omega_{k,i}$ of H must be invariant under the action of $\varphi(\mathcal{M}_{g-1,1})$. But

$$|\Omega_{k,i}| = k \leq 24 < 2^{g-2}(2^{g-1}-1) = \mathrm{mi}(\mathcal{M}_{g-1,1})\,,$$

thus $\varphi(\mathcal{M}_{g-1,1})$ acts trivially on each $\Omega_{k,i}$, that is, $\mathcal{M}_{g-1,1}$ acts trivially on $\widehat{\Omega}_k$.

Claim 2. *ψ_k is trivial if $k \geq 5$. Moreover, either ψ_3 or ψ_4 is nontrivial, but not both.*

Indeed, if ψ_k is nontrivial, then ν_k is nontrivial by Claim 1, thus

$$\frac{m}{k} \geq h_k \geq \mathrm{mi}(\mathcal{M}_{g-1,1}) = N^-_{g-1}\,,$$

therefore $k \leq 4$ as $m < 5\,N^-_{g-1}$. If both ψ_3 and ψ_4 are nontrivial, then

$$m \geq 3h_3 + 4h_4 \geq 7N^-_{g-1}\,,$$

which also contradicts $m < 5\,N^-_{g-1}$. Finally, by Lemma 5.4 one of the ψ_k with $k \geq 3$ must be nontrivial, so either ψ_3 or ψ_4 is nontrivial.

Claim 3. *ψ_3 is nontrivial.*

Suppose otherwise that ψ_3 is trivial. Then, by Claim 2, ψ_4 is nontrivial, thus $h_4 \geq N_{g-1}^-$. As $h_1 + 4h_4 \leq m < 5N_{g-1}^-$, it follows that $h_1 < N_{g-1}^-$, thus $\mathcal{M}_{g-1,1}$ acts trivially on $\widehat{\Omega}_1$. So,

$$S(\varphi(\mathcal{M}_{g-1,1})) \subseteq \widehat{\Omega}_4 \subseteq S(H)\,.$$

Since $S(\varphi(\mathcal{M}_{g-1,1}))$ contains $S(\langle w_1, w_2\rangle)$, which has the same cardinality as $S(H)$, the above inclusions are indeed equalities.

So, all nontrivial orbits of H have length 4. Applying Lemma 2.2, we get that w_2 is a product of disjoint 3-cycles and, for $i \in \{1,3\}$, all nontrivial orbits of $\langle w_2, w_i\rangle$ have length 4. By Lemma 1.4 it follows that $w_1 = w_3$. Hence, we also have

$$w_1 = (w_3w_4)w_1(w_3w_4)^{-1} = (w_3w_4)w_3(w_3w_4)^{-1} = w_4\,,$$

thus $w_3 = w_4$, therefore $w_0 = w_1 = \cdots = w_{2g}$. This implies that the image of φ is cyclic, and hence, because $\mathcal{M}_{g,1}$ is perfect, φ is trivial – a contradiction.

Claim 4. *ψ_1 is nontrivial.*

Suppose instead that ψ_1 is trivial. Then we have the inclusions

$$S(\varphi(\mathcal{M}_{g-1,1})) \subseteq \widehat{\Omega}_3 \subseteq S(H)$$

which imply as in the previous claim that $S(H) = \widehat{\Omega}_3$. So, all nontrivial orbits of w_{2g} and $\langle w_{2g}, w_{2g+1}\rangle$ have length 3; thus, by Lemma 1.3, $w_{2g} = w_{2g+1}$. It follows that the image of φ is cyclic, and hence, because $\mathcal{M}_{g,1}$ is perfect, φ is trivial – a contradiction.

The following claim is a direct consequence of the braid relation between w_{2g} and w_{2g+1} (see the proof of Lemma 1.3).

Claim 5. *$\Omega_{3,1}, \ldots, \Omega_{3,h_3}$ are precisely the common 3-orbits of w_{2g} and w_{2g+1}.*

We turn now to conclude the proof of Proposition 5.6 with counting arguments. If $(b_1, \ldots, b_p)$ is a p-chain of nonseparating closed curves, we denote by $c_p(b_1, \ldots, b_p)$ the number of common 3-orbits of $\varphi(T_{b_1}), \ldots, \varphi(T_{b_p})$. We do not assume that the whole chain is nonseparating, but we suppose that each pair (b_i, b_{i+1}) is nonseparating, so that $(T_{b_i}, T_{b_{i+1}})$ is conjugate to (T_{2g}, T_{2g+1}) (see Lemma 2.2). By Claims 1, 3 and 5 we have

$$c_2(b_1, b_2) = c_2(a_{2g}, a_{2g+1}) = h_3 \geq N_{g-1}^-\,,$$

and by Claim 4 we have $h_1 \geq N_{g-1}^-$. Recall also that ℓ_3 is the number of 3-orbits of w_{2g}. Note that the supports of the 3-orbits of w_{2g} that are not included in $\widehat{\Omega}_3$ are included in $X = \{1, \ldots, m\} - (\widehat{\Omega}_3 \sqcup \widehat{\Omega}_1)$; thus there are at most $|X|/3$ of them. Again by Lemma 2.2 it follows that for all $i \in \{2, \ldots, p\}$ among the 3-orbits of $\varphi(T_i)$ there are at most $|X|/3$ that are not 3-orbits of $\varphi(T_{i-1})$. We therefore obtain in turn

$$c_3(b_1, b_2, b_3) \geq h_3 - \frac{|X|}{3}\,, \quad c_4(b_1, b_2, b_3, b_4) \geq h_3 - \frac{2|X|}{3}\,,$$
$$c_5(b_1, b_2, b_3, b_4, b_5) \geq h_3 - \frac{3|X|}{3} = h_3 - |X|\,.$$

Using again the assumption that $m < 5N_{g-1}^-$, we have

$$|X| = m - h_1 - 3h_3 < 4N_{g-1}^- - 3h_3 \leq h_3\,.$$

Hence

$$c_5(b_1, b_2, b_3, b_4, b_5) \geq h_3 - |X| > 0\,.$$

So, there is a common 3-cycle in the decomposition of every generator $w_0, \ldots, w_4$ of $\varphi(\mathcal{M}_{2,1})$. By restricting attention to the support of this 3-cycle, we deduce that φ induces a nontrivial homomorphism from $\mathcal{M}_{2,1}$ to $\mathfrak{S}_3$ whose image is generated by elements of order 3; in other words, from $\mathcal{M}_{2,1}$ onto the cyclic group of order 3. This, however, contradicts Proposition 3.2. □

The last ingredient in our proof of Theorem 5.1 is the following theorem. We knew that it is well-known to experts, but we were not able to find it in the literature, so we included a proof in our first submitted version of the paper. Now, we thank the referee for bringing Humphries' proof of Theorem 5.7 (see [18, Prop 2.1]) to our attention. Note that Proposition 2.1 in [18] is a slightly different statement (it says that the kernel of $\theta_{g,0}$ is the smallest normal subgroup of $\mathcal{M}_{g,0}$ containing T_1^2). However, precisely the same proof proves our Theorem 5.7. The crucial point in Humphries' argument is that the Torelli subgroup of $\mathcal{M}_{g,0}$ is generated by Dehn twists about bounding curves and bounding pairs, and this is also true for the Torelli subgroup of $\mathcal{M}_{g,1}$ (see [28], [3] and [29]).

Theorem 5.7. *Let $g \geq 2$. Then the kernel of $\theta_{g,1}$ is the smallest normal subgroup of $\mathcal{M}_{g,1}$ containing T_1^2.* □

Proof of Theorem 5.1. For $g \geq 4$, let $\varphi : \mathcal{M}_{g,1} \to \mathfrak{S}_m$ be a nontrivial homomorphism, with $m < 5\,N_{g-1}^-$. Thanks to Corollary 5.3 and Propositions 5.5 and 5.6, $w_i = \varphi(T_i)$ is an involution for all $i \in \{0, 1, \ldots, 2g+1\}$. By Theorem 5.7 we conclude that there exists a homomorphism $\bar{\varphi} : \mathrm{Sp}_{2g}(\mathbb{F}_2) \to \mathfrak{S}_m$ such that $\varphi = \bar{\varphi} \circ \theta_{g,1}$. □

6 Large subgroups of $\mathrm{Sp}_{2g}(\mathbb{F}_2)$

The aim of this section is to prove Theorem 0.3, which, together with Theorem 5.1, proves Theorem 0.4 for the case of a surface with $n = 1$ boundary component. The extension to surfaces with several boundary components will be the object of Section 8.

Theorem 6.1. ([23, Theorem 4.1 and § 3]; [2, § 1]) *If H is a maximal subgroup of $\mathrm{Sp}_{2g}(\mathbb{F}_2)$ for $g \geq 1$, then one of the following holds.*

(1) $H = O_{2g}^-(\mathbb{F}_2)$, of order $2^{g^2-g+1}(2^g+1)\prod_{i=1}^{g-1}(2^{2i}-1)$.

(2) $H = O_{2g}^+(\mathbb{F}_2)$, of order $2^{g^2-g+1}(2^g-1)\prod_{i=1}^{g-1}(2^{2i}-1)$.

(3) $|H| \leq 2^{6g}$.

(4) $H \leq \mathfrak{S}_{2g+2}$, of order at most $(2g+2)!$.

(5) H is a group extension with kernel $\mathrm{Sp}_{2k}(\mathbb{F}_{2^r})$ and quotient a cyclic group of order r, where $r > 1$ is a prime divisor of g and $kr = g$. Here, H has order $r \cdot 2^{\frac{g^2}{r}}\prod_{i=1}^{k}(2^{2ri}-1)$.

(6) $H = \mathrm{Sp}_{2k}(\mathbb{F}_2) \wr \mathfrak{S}_r$, *where* $r > 1$ *is a divisor of* g *and* $kr = g$. *Here,* H *has order* $r! \cdot 2^{\frac{g^2}{r}} \prod_{i=1}^{k} (2^{2i} - 1)^r$.

(7) H *is the stabilizer of a totally isotropic subspace of* $\mathbb{F}_2^{2g}$ *under the natural action of* $\mathrm{Sp}_{2g}(\mathbb{F}_2)$. *That is,* H *is a semidirect product*

$$K \rtimes (\mathrm{Sp}_{2g-2k}(\mathbb{F}_2) \times \mathrm{GL}_k(\mathbb{F}_2))$$

for some integer $k \in \{1, \ldots, g\}$, *and* K *is a group extension with kernel an elementary abelian* 2*-group of rank* $\frac{k(k+1)}{2}$ *and quotient an elementary abelian* 2*-group of rank* $2k(g-k)$; *and* H *has order*

$$2^{g^2} \cdot \left(\prod_{i=1}^{g-k} (2^{2i} - 1) \right) \cdot \left(\prod_{i=1}^{k-1} (2^{i+1} - 1) \right) .$$

(8) H *is the stabilizer of a nonsingular subspace of* $\mathbb{F}_2^{2g}$ *under the natural action of* $\mathrm{Sp}_{2g}(\mathbb{F}_2)$. *That is,* H *is* $\mathrm{Sp}_{2k}(\mathbb{F}_2) \times \mathrm{Sp}_{2g-2k}(\mathbb{F}_2)$ *for some* $k \in \{1, \ldots, g-1\}$, *and has order*

$$2^{g^2+2k^2-2gk} \cdot \left(\prod_{i=1}^{g-k} (2^{2i} - 1) \right) \cdot \left(\prod_{i=1}^{k} (2^{2i} - 1) \right) .$$

Moreover, the maximal subgroups falling within case (1) lie in a single conjugacy class, as do the subgroups falling within case (2).

Proof. The first part is shown in [23, Theorem 4.1 and § 3]. Their orders may be found in [31, pp. 19, 70, 141]. For the last two cases, the description of H follows from [32, p. 63], for example. Cases 2 and 1 correspond to the Aschbacher class $\mathcal{C}_8$ [2, § 1], that is, contain the subgroups of $\mathrm{Sp}_{2g}(\mathbb{F}_2)$ stabilizing some quadratic form polarizing to the symplectic bilinear form defining $\mathrm{Sp}_{2g}(\mathbb{F}_2)$; Case 2 corresponds to forms of Witt index g, Case 1 to forms of Witt index $g-1$. By [2, Theorems $B\Delta$ and BO], the action of $\mathrm{Sp}_{2g}(\mathbb{F}_2)$ is transitive on stabilizers of forms of the same similarity type, showing that the groups falling within Case 2, respectively the groups falling within Case 1, form a single conjugacy class. □

Corollary 6.2. *Let* $g \geq 3$ *and let* H *be a subgroup of* $\mathrm{Sp}_{2g}(\mathbb{F}_2)$ *of index (strictly) less than* $2\, N_g^-$. *Then either* $H \cong O_{2g}^-(\mathbb{F}_2)$ *or* $H \cong O_{2g}^+(\mathbb{F}_2)$.

Remark. $SO_{2g}^-(\mathbb{F}_2)$ is an index 2 subgroup of $O_{2g}^-(\mathbb{F}_2)$ and, therefore, an index $2\, N_g^-$ subgroup of $\mathrm{Sp}_{2g}(\mathbb{F}_2)$.

Proof. Recall again that $N_g^- = [\mathrm{Sp}_{2g}(\mathbb{F}_2) : O_{2g}^-(\mathbb{F}_2)]$ and note that the result holds for proper subgroups of $O_{2g}^-(\mathbb{F}_2)$ and $O_{2g}^+(\mathbb{F}_2)$ because $|O_{2g}^+(\mathbb{F}_2)| < |O_{2g}^-(\mathbb{F}_2)|$. Thus, we need consider only maximal subgroups H. For applications, the assertion is presented in terms of the index; however, the data relate to the order, so one needs to check that of the maximal subgroups listed in Theorem 6.1, in all except for the first two cases the order of H is less than

$$\frac{|O_{2g}^-(\mathbb{F}_2)|}{2} = 2^{g^2-g}(2^g + 1) \prod_{i=1}^{g-1} (2^{2i} - 1) .$$

For $g = 3$ the result holds by [7]. (Alternatively, we can compute the conjugacy classes of maximal subgroups of $\mathrm{Sp}_6(\mathbb{F}_2)$ using MAGMA [4]: their orders are 1512, 4320, 4608, 10752, 12096, 23040, 40320, 51840. The maximal subgroups of order 40320 and 51840 can be checked to be isomorphic to $O_6^+(\mathbb{F}_2)$ respectively $O_6^-(\mathbb{F}_2)$, so the claim holds.)

So, assume that $g \geq 4$. In general, it is a routine matter to use the formulae of Theorem 6.1 to check that H has order less than $|O_{2g}^-(\mathbb{F}_2)|/2$. To indicate the flavor of the verification, we discuss the two most delicate cases, namely (6) and (8).

Case (6). First observe that $r! < 2^{(r^2-2r+3)/2}$, and, for r in the range $[2, g]$, the function $(r^2-2r+3)/2+\frac{g^2}{r}$ achieves its maximum value of $(g^2+3)/2$ at the endpoints. Thus, on putting $j = ir$, we have that $|H| = r! \cdot 2^{\frac{g^2}{r}} \prod_{i=1}^{k}(2^{2i}-1)^r$ is bounded above by

$$2^{(g^2+3)/2} \prod_{r|j,\ j\leq g}(2^{2j}-1) < 2^{(g^2+2g+3)/2}(2^g+1) \prod_{r|j,\ j\leq g-1}(2^{2j}-1)\,.$$

Since $2^{(g^2+2g+3)/2} < 2^{g^2-g}(2^2-1)$, and $(2^2-1)\prod_{r|j,\ j\leq g-1}(2^{2j}-1) < \prod_{i=1}^{g-1}(2^{2i}-1)$, we obtain $|H| < |O_{2g}^-(\mathbb{F}_2)|/2$, as required.

Case (8). Since, for k in the range $[1, g-1]$, the function $2k(k-g)$ achieves its maximum of $-2(g-1)$ at the endpoints, we have $2^{g^2+2k^2-2gk} < 2^{g^2-g}$. Meanwhile, using the symmetry of the product below to assume that $k \leq \frac{g}{2}$, and observing that $i < i+g-k = j$ say, gives

$$\begin{aligned}
&\left(\prod_{i=1}^{g-k}(2^{2i}-1)\right)\cdot\left(\prod_{i=1}^{k}(2^{2i}-1)\right)\\
=&(2^{2k}-1)\left(\prod_{i=1}^{g-k}(2^{2i}-1)\right)\cdot\left(\prod_{i=1}^{k-1}(2^{2i}-1)\right)\\
<&(2^g+1)\left(\prod_{i=1}^{g-k}(2^{2i}-1)\right)\cdot\left(\prod_{j=g-k+1}^{g-1}(2^{2j}-1)\right)\,.
\end{aligned}$$

When combined with the exponential inequality above, this again yields $|H| < |O_{2g}^-(\mathbb{F}_2)|/2$. □

Proof of Theorem 0.3. As stated before, we have $[\mathrm{Sp}_{2g}(\mathbb{F}_2) : O_{2g}^-(\mathbb{F}_2)] = N_g^- = 2^{g-1}(2^g-1)$ and $[\mathrm{Sp}_{2g}(\mathbb{F}_2) : O_{2g}^+(\mathbb{F}_2)] = N_g^+ = 2^{g-1}(2^g+1)$ by [31, pp. 70 and 141]. Finally, Corollary 6.2 ensures that the conjugacy classes of $O_{2g}^+(\mathbb{F}_2)$ and $O_{2g}^-(\mathbb{F}_2)$ are the only conjugacy classes of subgroups of $\mathrm{Sp}_{2g}(\mathbb{F}_2)$ of index less than $2\,N_g^-$. □

Now, thanks to Theorem 5.1 and Theorem 0.3, we can prove our main theorem for the case of a surface with $n = 1$ boundary component. However, we have to keep the inductive hypothesis (that Theorem 0.4 holds for a surface of genus $g-1$), as we have used the equality $\mathrm{mi}(\mathcal{M}_{g-1,3}) = N_{g-1}^-$ in the proof of Proposition 5.2.

Proposition 6.3. *Let $g \geq 4$.*

(1) $\mathcal{O}_{g,1}^-$ is the unique subgroup of $\mathcal{M}_{g,1}$ of index $N_g^- = 2^{g-1}(2^g-1)$, up to conjugation.

(2) $\mathcal{O}^+_{g,1}$ is the unique subgroup of $\mathcal{M}_{g,1}$ of index $N^+_g = 2^{g-1}(2^g+1)$, up to conjugation.

(3) All the other proper subgroups of $\mathcal{M}_{g,1}$ are of index at least $5N^-_{g-1} > N^+_g$.

Proof. Let H be a subgroup of $\mathcal{M}_{g,1}$ of index $m < 5\,N^-_{g-1}$. By Theorem 5.1 there is a subgroup $\bar{H}$ of $\mathrm{Sp}_{2g}(\mathbb{F}_2)$ of index m such that $H = \theta^{-1}_{g,1}(\bar{H})$. Since $5\,N^-_{g-1} < 2\,N^-_g$, by Theorem 0.3, we must necessarily have either $\bar{H} = O^-_{2g}(\mathbb{F}_2)$ or $\bar{H} = O^+_{2g}(\mathbb{F}_2)$ up to conjugation, thus either $H = \mathcal{O}^-_{g,1}$ or $H = \mathcal{O}^+_{g,1}$ up to conjugation. □

7 Small symplectic representations of $\mathcal{M}_{g,n}$

The aim of this section is to prove Proposition 7.2, which is the same as Theorem 0.5, except that we do not state that the decompositions in (1) are unique. The uniqueness will follow from Theorem 0.4 proved in Section 8.
The decompositions of $\phi^{\pm}_{g,n}$ in (1) reflect analogous properties of the corresponding representations of $\mathrm{Sp}_{2g}(\mathbb{F}_2)$, which in turn arise in a geometric way; while this result may be more or less known to experts, we could not locate a reference and hence establish it in Lemma 7.1.

We choose a basis $\{\mathbf{e}_1, \dots, \mathbf{e}_{2g}\}$ of $V = \mathbb{F}_2^{2g}$ such that $(\mathbf{e}_i, \mathbf{e}_{2g+1-i})$ for $i = 1, \dots, g$ are the symplectic pairs for the action of $\mathrm{Sp}_{2g}(\mathbb{F}_2)$; we write $\bar{i}$ for $2g+1-i$ to shorten notation. For a vector $\mathbf{x} \in V$, we denote the components of $\mathbf{x}$ with respect to the basis $\{\mathbf{e}_1, \dots, \mathbf{e}_{2g}\}$ by $x_1, \dots, x_{2g}$. We consider $\mathrm{Sp}_{2g-2}(\mathbb{F}_2)$ as a subgroup of $\mathrm{Sp}_{2g}(\mathbb{F}_2)$ via the standard embedding defined by

$$\omega \mapsto \left[\begin{array}{c|ccc|c} 1 & 0 & \cdots & 0 & 0 \\ \hline 0 & & & & 0 \\ \vdots & & \omega & & \vdots \\ 0 & & & & 0 \\ \hline 0 & 0 & \cdots & 0 & 1 \end{array}\right]$$

with respect to the above basis.

For $g \geq 2$ and $\epsilon \in \{\pm\}$, let $\overline{\phi}^{\epsilon}_g : \mathrm{Sp}_{2g}(\mathbb{F}_2) \to \mathfrak{S}_{N^{\epsilon}_g}$ denote the permutation representation induced by the action of $\mathrm{Sp}_{2g}(\mathbb{F}_2)$ on the right cosets of $O^{\epsilon}_{2g}(\mathbb{F}_2)$ (cf. Corollary 6.2).

Lemma 7.1. *Let $g \geq 3$. Then,*

$$\overline{\phi}^{+}_g|_{\mathrm{Sp}_{2g-2}(\mathbb{F}_2)} \cong (\overline{\phi}^{+}_{g-1})^3 \oplus \overline{\phi}^{-}_{g-1} \quad \textit{and} \quad \overline{\phi}^{-}_g|_{\mathrm{Sp}_{2g-2}(\mathbb{F}_2)} \cong (\overline{\phi}^{-}_{g-1})^3 \oplus \overline{\phi}^{+}_{g-1}\,.$$

Proof. It is well-known (see, for example, [11] or [31, ch. 11]) that $\overline{\phi}^{+}_g$ and $\overline{\phi}^{-}_g$ arise from the action of $\mathrm{Sp}_{2g}(\mathbb{F}_2)$ on the two orbits of quadratic forms polarizing to the symplectic form $\langle -, - \rangle$ preserved by $\mathrm{Sp}_{2g}(\mathbb{F}_2)$. The two orbits consist of the quadratic forms of Witt index g (type $+$) respectively Witt index $g-1$ (type $-$).
Let $\mathcal{Q}$ denote the set of quadratic forms polarizing to $\langle -, - \rangle$. The elements of $\mathcal{Q}$ are of the form

$$Q_{\mathbf{b}}(\mathbf{x}) = \sum_{i=1}^{g} x_i x_{\bar{i}} + \langle \mathbf{x}, \mathbf{b} \rangle^2 = \sum_{i=1}^{g} x_i x_{\bar{i}} + \langle \mathbf{x}, \mathbf{b} \rangle \quad \text{for } \mathbf{b} \in V.$$

The symplectic group $\mathrm{Sp}_{2g}(\mathbb{F}_2)$ acts on $\mathcal{Q}$ via $(\omega \cdot Q)(\mathbf{x}) := Q(\omega\mathbf{x})$ for $\omega \in \mathrm{Sp}_{2g}(\mathbb{F}_2)$ and $Q \in \mathcal{Q}$. In particular, $(\omega \cdot Q_{\mathbf{b}})(\mathbf{x}) = Q_{\mathbf{b}^\omega}(\mathbf{x})$ for some $\mathbf{b}^\omega \in V$. It is easy to see that this defines another action of $\mathrm{Sp}_{2g}(\mathbb{F}_2)$ on the set V given by $\omega \cdot \mathbf{b} := \mathbf{b}^\omega$. (Note that this action does not respect the structure of V as a vector space. In particular, it is different from the natural action given by matrix multiplication.) It is easy to verify that the restriction of this action to $\mathrm{Sp}_{2g-2}(\mathbb{F}_2) < \mathrm{Sp}_{2g}(\mathbb{F}_2)$ can be canonically identified with the analogous action of $\mathrm{Sp}_{2g-2}(\mathbb{F}_2)$ on quadratic forms on $\mathbb{F}_2^{2g-2}$.

Now consider the two orbits $\mathcal{Q}^+$ and $\mathcal{Q}^-$ of quadratic forms of type + respectively type − under the action of $\mathrm{Sp}_{2g}(\mathbb{F}_2)$. We will show that $\mathcal{Q}^\epsilon$ ($\epsilon \in \{\pm\}$) splits up into four orbits under the action of $\mathrm{Sp}_{2g-2}(\mathbb{F}_2)$, one for each of the 2^2 possible values of (b_1, b_{2g}), and that three of these orbits have the type ϵ while the remaining orbit has the type $-\epsilon$.

Consider first the orbit $\mathcal{Q}^+$ of quadratic forms of type +, that is, of Witt index g, and define

$$\mathbf{b}_0 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 0 \\ 0 \\ 0 \end{pmatrix}, \quad \mathbf{b}_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \\ 0 \\ 0 \end{pmatrix}, \quad \mathbf{b}_2 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 0 \\ 0 \\ 1 \end{pmatrix}, \quad \mathbf{b}_3 = \begin{pmatrix} 1 \\ 1 \\ 0 \\ \vdots \\ 0 \\ 1 \\ 1 \end{pmatrix}.$$

The quadratic forms $Q_{\mathbf{b}_i}(\mathbf{x})$ for $i = 0, 1, 2, 3$ have Witt index g, that is, are elements of $\mathcal{Q}^+$. Moreover, $\mathcal{Q}^+ = \bigsqcup_{i=1}^4 Q_{\mathbf{b}_i}^{\mathrm{Sp}_{2g-2}(\mathbb{F}_2)}$. It is easy to see that the restriction of $Q_{\mathbf{b}_i}$ to $\mathbb{F}_2^{2g-2}$ is of type + (Witt index $g-1$) for $i = 0, 1, 2$ and of type − (Witt index $g-2$) for $i = 3$. Hence $\overline{\phi}_g^+|_{\mathrm{Sp}_{2g-2}(\mathbb{F}_2)} \cong (\overline{\phi}_{g-1}^+)^3 \oplus \overline{\phi}_{g-1}^-$ as claimed.

The argument for the orbit $\mathcal{Q}^-$ of quadratic forms of type − is analogous. □

Proposition 7.2. *(1) Let $g \geq 3$ and $n \geq 1$. Then $\phi_{g,n}^- : \mathcal{M}_{g,n} \to \mathfrak{S}_{N_g^-}$ is equivalent to an extension of the representation $(\phi_{g-1,n}^-)^3 \oplus \phi_{g-1,n}^+$ from $\mathcal{M}_{g-1,n}$ to $\mathcal{M}_{g,n}$, and $\phi_{g,n}^+ : \mathcal{M}_{g,n} \to \mathfrak{S}_{N_g^+}$ is equivalent to an extension of the representation $\phi_{g-1,n}^- \oplus (\phi_{g-1,n}^+)^3$ from $\mathcal{M}_{g-1,n}$ to $\mathcal{M}_{g,n}$.*

(2) Let $g \geq 3$ and $n \geq 0$. Let b be a nonseparating simple closed curve on $\Sigma_{g,n}$, and let T_b be the Dehn twist around b. Then the cycle structure of the image of T_b under $\phi_{g,n}^-$ is

$$(1)^{2^{2g-2}}(2)^{2^{g-2}(2^{g-1}-1)},$$

and the cycle structure of the image of T_b under $\phi_{g,n}^+$ is

$$(1)^{2^{2g-2}}(2)^{2^{g-2}(2^{g-1}+1)}.$$

Proof. We first consider Part (1). For a simple closed curve c on $\Sigma_{g,1}$, we denote by $[c]$ the class of c in $H_1(\Sigma_{g,1}, \mathbb{Z})$. We consider the curves $u_1, \ldots, u_g, v_1, \ldots, v_g$ indicated in Figure 7.1, and choose $[u_g], [u_{g-1}], \ldots, [u_1], [v_1], [v_2], \ldots, [v_g]$ as basis elements for $H_1(\Sigma_{g,1}, \mathbb{Z})$. With respect

to this ordering, the bilinear form $\langle -, - \rangle$ yielding the algebraic intersection number is given by the matrix

$$M = \begin{bmatrix} 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & \cdots & 1 & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 1 & \cdots & 0 & 0 \\ 1 & 0 & \cdots & 0 & 0 \end{bmatrix}.$$

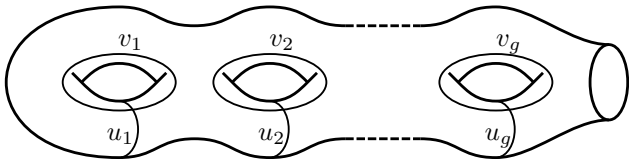

Figure 7.1. Basis for $H_1(\Sigma_{g,1}, \mathbb{Z})$.

The image of the Dehn twist T_b about a simple closed curve b under the epimorphism $\theta_{g,1} : \mathcal{M}_{g,1} \to \mathrm{Sp}_{2g}(\mathbb{F}_2)$ is the map

$$[a] \mapsto [a] + \langle a, b \rangle [b] \,.$$

Since $\mathcal{M}_{g-1,1} < \mathcal{M}_{g,1}$ is generated by $T_0, T_1, \ldots, T_{2g-2}$ and since $a_0, a_1, \ldots, a_{2g-2}$ intersect neither u_g nor v_g, it is clear from the above that $\theta_{g,1}(\mathcal{M}_{g-1,1}) = \mathrm{Sp}_{2g-2}(\mathbb{F}_2) < \mathrm{Sp}_{2g}(\mathbb{F}_2)$, and the restriction of $\theta_{g,1}$ to $\mathcal{M}_{g-1,1}$ coincides with $\theta_{g-1,1} : \mathcal{M}_{g-1,1} \to \mathrm{Sp}_{2g-2}(\mathbb{F}_2) < \mathrm{Sp}_{2g}(\mathbb{F}_2)$.

Let $n \geq 1$. Gluing disks along all boundary components of $\Sigma_{g,n}$ but one, we obtain an embedding $\Sigma_{g,n} \hookrightarrow \Sigma_{g,1}$ that induces a surjective homomorphism $\mu_{g,n} : \mathcal{M}_{g,n} \twoheadrightarrow \mathcal{M}_{g,1}$ (see [27]). More precisely, the epimorphism $\mu_{g,n}$ is defined sending T'_j to T_1 for all $j \in \{1, \ldots, n\}$, and T_i to T_i for all $i \in \{0, 2, \ldots, 2g\}$. Observe that $\theta_{g,n} = \theta_{g,1} \circ \mu_{g,n}$ and the following diagram commutes

$$\begin{array}{ccc} \mathcal{M}_{g-1,n} & \longrightarrow & \mathcal{M}_{g,n} \\ {\scriptstyle \mu_{g-1,n}}\downarrow & & \downarrow{\scriptstyle \mu_{g,n}} \\ \mathcal{M}_{g-1,1} & \longrightarrow & \mathcal{M}_{g,1} \end{array}$$

where $\mathcal{M}_{g-1,n} \to \mathcal{M}_{g,n}$ and $\mathcal{M}_{g-1,1} \to \mathcal{M}_{g,1}$ are the natural embeddings described in Section 2. By the above, it follows that $\theta_{g,n}(\mathcal{M}_{g-1,n}) = \mathrm{Sp}_{2g-2}(\mathbb{F}_2) < \mathrm{Sp}_{2g}(\mathbb{F}_2)$, and the restriction of $\theta_{g,n}$ to $\mathcal{M}_{g-1,n}$ coincides with $\theta_{g-1,n} : \mathcal{M}_{g-1,n} \to \mathrm{Sp}_{2g-2}(\mathbb{F}_2) < \mathrm{Sp}_{2g}(\mathbb{F}_2)$.

We have

$$\overline{\phi}_g^+|_{\mathrm{Sp}_{2g-2}(\mathbb{F}_2)} \cong (\overline{\phi}_{g-1}^+)^3 \oplus \overline{\phi}_{g-1}^- \quad \text{and} \quad \overline{\phi}_g^-|_{\mathrm{Sp}_{2g-2}(\mathbb{F}_2)} \cong (\overline{\phi}_{g-1}^-)^3 \oplus \overline{\phi}_{g-1}^+$$

from Lemma 7.1. By composing with $\theta_{g,n}$ we conclude that

$$\phi_{g,n}^+|_{\mathcal{M}_{g-1,n}} \cong (\phi_{g-1,n}^+)^3 \oplus \phi_{g-1,n}^- \quad \text{and} \quad \phi_{g,n}^-|_{\mathcal{M}_{g-1,n}} \cong (\phi_{g-1,n}^-)^3 \oplus \phi_{g-1,n}^+ \,.$$

Part (2) for $n \geq 1$ follows by induction on g, using the cycle structures $(2)^6\,(1)^{16}$ of $\phi_{3,n}^-(T_b)$ and $(2)^{10}\,(1)^{16}$ of $\phi_{3,n}^+(T_b)$ for $g = 3$ (see Lemma 4.1), and the equivalence $\phi_{g,n}^\epsilon|_{\mathcal{M}_{g-1,n}} \cong (\phi_{g-1,n}^\epsilon)^3 \oplus \phi_{g-1,n}^{-\epsilon}$ proved above for $g \geq 4$.

Gluing a disk along the boundary component of $\Sigma_{g,1}$ we obtain an embedding $\Sigma_{g,1} \hookrightarrow \Sigma_{g,0}$ that induces a surjective homomorphism $\nu : \mathcal{M}_{g,1} \to \mathcal{M}_{g,0}$ (see *e.g.* [27]). Observe that $\theta_{g,1} = \theta_{g,0} \circ \nu$. Thus, if b is a nonseparating simple closed curve in $\Sigma_{g,1}$, then $\theta_{g,1}(T_b) = \theta_{g,0}(T_b)$; therefore $\phi^\epsilon_{g,1}(T_b) = \phi^\epsilon_{g,0}(T_b)$. This proves Part (2) for $n = 0$. □

8 Surfaces with multiple boundary components

We start the section with a geometric interpretation of the decomposition given in Proposition 7.2.

Take $\epsilon \in \{\pm\}$ and consider the representation $\phi^\epsilon_{g,1} : \mathcal{M}_{g,1} \to \mathfrak{S}_{N^\epsilon_g}$. Let w_i denote the image of T_i under $\phi^\epsilon_{g,1}$ for all $i \in \{0, 1, \dots, 2g+1\}$. Set $H = \langle w_{2g}, w_{2g+1} \rangle$. Since w_i has order 2, there is an epimorphism from the group

$$\widehat{H} = \langle x_0, x_1 \mid x_0^2 = x_1^2 = 1,\ x_0x_1x_0 = x_1x_0x_1 \rangle = \mathfrak{S}_3$$

to H which sends x_i to w_{2g+i} for $i \in \{0, 1\}$. In particular, the order of H divides 6.

For $k \geq 1$, let $\widehat{\Omega}_k$ denote the union of the k-orbits $\Omega_{k,i}$ of H, $1 \leq i \leq h_k$. Since the image $\phi^\epsilon_{g,1}(\mathcal{M}_{g-1,1}) = \langle w_0, \dots, w_{2g-2} \rangle$ belongs to the centralizer of H, it acts on the set of orbits $\{\Omega_{k,1}, \dots, \Omega_{k,h_k}\}$ as well as on the whole set $\widehat{\Omega}_k$. The first action induces a homomorphism $\nu_k : \mathcal{M}_{g-1,1} \to \mathfrak{S}_{h_k}$ and the second a homomorphism $\psi_k : \mathcal{M}_{g-1,1} \to \mathfrak{S}_{kh_k}$. The following lemma describes these representations.

Lemma 8.1. *Let $g \geq 3$. With the above notation, the following hold.*

(1) $h_3 = N^\epsilon_{g-1}$, $h_1 = N^{-\epsilon}_{g-1}$, *and* $h_k = 0$ *for all* $k \notin \{1, 3\}$.

(2) $\nu_3 \cong \phi^\epsilon_{g-1,1}$, $\psi_3 \cong (\phi^\epsilon_{g-1,1})^3$, *and* $\nu_1 = \psi_1 \cong \phi^{-\epsilon}_{g-1,1}$.

(3) $\{1, \dots, N^\epsilon_g\} = S(\phi^\epsilon_{g,1}(\mathcal{M}_{3,1}))$, *where, for* $G < \mathfrak{S}_{N^\epsilon_g}$, $S(G)$ *denotes the support of* G, *and* $\mathcal{M}_{3,1}$ *is the subgroup of* $\mathcal{M}_{g,1}$ *generated by* $T_0, T_1, \dots, T_6$.

Proof. We prove by induction on g that $\langle w_1, w_2 \rangle$ has N^ϵ_{g-1} 3-orbits, has no other nontrivial orbit, and has $N^{-\epsilon}_{g-1}$ fixed letters. The case $g = 3$ follows from Lemma 4.1, and the inductive step can easily be derived from the formula $\phi^\epsilon_{g,1}|_{\mathcal{M}_{g-1,1}} \cong (\phi^\epsilon_{g-1,1})^3 \oplus \phi^{-\epsilon}_{g-1,1}$ of Proposition 7.2. Thanks to Lemma 2.2 this proves Part (1).

Let $\Omega_{3,i}$ be a 3-orbit of H. We may write $\Omega_{3,i} = \{a_i, b_i, c_i\}$ so that the restriction of w_{2g} to $\Omega_{3,i}$ is the transposition $(a_i\ b_i)$ and the restriction of w_{2g+1} is $(b_i\ c_i)$. Set $\widehat{\Omega}^1_3 = \widehat{\Omega}_3 - S(w_{2g+1}) = \{a_i; 1 \leq i \leq N^\epsilon_{g-1}\}$, $\widehat{\Omega}^3_3 = \widehat{\Omega}_3 - S(w_{2g}) = \{c_i; 1 \leq i \leq N^\epsilon_{g-1}\}$, and $\widehat{\Omega}^2_3 = \widehat{\Omega}_3 - (\widehat{\Omega}^1_3 \cup \widehat{\Omega}^3_3) = \{b_i; 1 \leq i \leq N^\epsilon_{g-1}\}$. Then $\widehat{\Omega}^\ell_3$ is invariant under the action of $\mathcal{M}_{g-1,1}$ for $\ell = 1, 2, 3$, and the action of $\mathcal{M}_{g-1,1}$ on $\widehat{\Omega}^\ell_3$ is equivalent to ν_3. So,

$$\phi^\epsilon_{g,1}|_{\mathcal{M}_{g-1,1}} \cong \psi_3 \oplus \psi_1 \cong (\nu_3)^3 \oplus \nu_1\,.$$

For the case $g = 3$, one can easily check the equivalences $\nu_3 \cong \phi^\epsilon_{2,1}$ and $\nu_1 \cong \phi^{-\epsilon}_{2,1}$ using Lemma 3.1 and Lemma 4.1, so Part (2) holds in this case and we can assume $g \geq 4$. Recall that $h_3 = N^\epsilon_{g-1}$

and $h_1 = N_{g-1}^{-\epsilon}$. By Lemma 4.1 (if $g = 4$), respectively Proposition 6.3 (if $g > 4$), ν_3 and ν_1 are either trivial or of the form $\nu_3 = \phi_{g-1,1}^{\mu} \oplus \mathbf{1}_q$, respectively $\nu_1 = \phi_{g-1,1}^{\mu'} \oplus \mathbf{1}_{q'}$. Now, the formula of Proposition 7.2 implies that $\phi_{g,1}^{\epsilon}|_{\mathcal{M}_{g-1,1}}$ has no fixed letter, and thus both ν_3 and ν_1 must be nontrivial and we must have $q = q' = 0$, $\mu = \epsilon$, and $\mu' = -\epsilon$. So Part (2) holds.

Part (3) follows by induction on g using Lemma 4.1 for the case $g = 3$ and the equivalence $\phi_{g,1}^{\epsilon}|_{\mathcal{M}_{g-1,1}} \cong (\phi_{g-1,1}^{\epsilon})^3 \oplus \phi_{g-1,1}^{-\epsilon}$ for the inductive step. □

Now, we finish the proof of Theorem 0.4 with the following.

Proposition 8.2. *Let $g \geq 4$ and $n \geq 0$.*

(1) $\mathcal{O}_{g,n}^-$ is the unique subgroup of $\mathcal{M}_{g,n}$ of index $N_g^- = 2^{g-1}(2^g - 1)$, up to conjugation.

(2) $\mathcal{O}_{g,n}^+$ is the unique subgroup of $\mathcal{M}_{g,n}$ of index $N_g^+ = 2^{g-1}(2^g + 1)$, up to conjugation.

(3) All the other subgroups of $\mathcal{M}_{g,n}$ are of index at least $5N_{g-1}^- > N_g^+$.

Proof. Recall that we are under the inductive hypothesis stated at the beginning of Part II, that is, Theorem 0.4 holds for a surface of genus $g - 1$.

The case $n = 1$ is proved in Proposition 6.3, and the case $n = 0$ follows from Proposition 6.3, Theorem 0.3, and the existence of the epimorphisms $\mathcal{M}_{g,1} \twoheadrightarrow \mathcal{M}_{g,0}$, $\mathcal{M}_{g,0} \twoheadrightarrow \mathrm{Sp}_{2g}(\mathbb{F}_2)$ described in Section 0. So, we may assume $n \geq 2$.

Let $\varphi : \mathcal{M}_{g,n} \to \mathfrak{S}_m$ be a nontrivial transitive homomorphism with $m < 5N_{g-1}^-$. As ever, for $i \in \{0, 2, \ldots, 2g+1\}$ and $j \in \{1, \ldots, n\}$, we denote by a_i and b_j the simple closed curves illustrated in Figure 2.2, we denote by T_i the Dehn twist about a_i, by T_j' the Dehn twist about b_j, and we set $w_i = \varphi(T_i)$ and $w_j' = \varphi(T_j')$. For $j \in \{1, \ldots, n\}$, we denote by $\Sigma^{(j)}$ a tubular neighborhood of $b_j \cup a_0 \cup (\cup_{i=2}^{2g} a_i)$. Observe that $\Sigma^{(j)}$ is a subsurface of $\Sigma_{g,n}$ of genus g with a unique boundary component, and the inclusion $\Sigma^{(j)} \hookrightarrow \Sigma_{g,n}$ induces an injective homomorphism $\gamma_j : \mathcal{M}_{g,1} \to \mathcal{M}_{g,n}$ which sends T_1 to T_j' and T_i to T_i for all $i \in \{0, 2, \ldots, 2g\}$. Set $\varphi_j = \varphi \circ \gamma_j : \mathcal{M}_{g,1} \to \mathfrak{S}_m$. By Proposition 6.3, φ_j is of the form $\varphi_j = \psi_j \oplus \mathbf{1}_{q_j}$ where ψ_j is conjugate to an element of $\{\phi_{g,1}^+, \phi_{g,1}^-\}$ and $\mathbf{1}_{q_j} : \mathcal{M}_{g,1} \to \mathfrak{S}_{q_j}$ is the trivial representation.
Let Σ' be a tubular neighborhood of $\cup_{i=0}^{5} a_{2g-i}$. Then Σ' is a subsurface of $\Sigma_{g,n}$ of genus 3 with a unique boundary component, and is included in $\Sigma^{(j)}$ for all $j \in \{1, \ldots, n\}$. Moreover, the inclusion $\Sigma' \hookrightarrow \Sigma_{g,n}$ induces an embedding $\gamma' : \mathcal{M}_{3,1} \to \mathcal{M}_{g,n}$. Set $\varphi' = \varphi \circ \gamma' : \mathcal{M}_{3,1} \to \mathfrak{S}_m$. We have $S(\varphi_j(\mathcal{M}_{g,1})) = S(\varphi'(\mathcal{M}_{3,1}))$ by Lemma 8.1 (3) for all j, and $\bigcup_{j=1}^{n} S(\varphi_j(\mathcal{M}_{g,1})) = S(\varphi(\mathcal{M}_{g,n}))$, thus

$$S(\varphi(\mathcal{M}_{g,n})) = S(\varphi_j(\mathcal{M}_{g,1})) = S(\varphi'(\mathcal{M}_{3,1}))\,.$$

Since φ is transitive, it follows that there exists $\epsilon \in \{\pm\}$ such that $m = N_g^{\epsilon}$ and φ_j is conjugate to $\phi_{g,1}^{\epsilon}$ for all $j \in \{1, \ldots, n\}$.
Set $H = \langle w_{2g}, w_{2g+1} \rangle$; note that $H \subseteq \bigcap_j \gamma_j(\mathcal{M}_{g,1})$. For $k \geq 1$ we denote by $\widehat{\Omega}_k$ the union of the k-orbits $\Omega_{k,i}$ of H, $1 \leq i \leq h_k$. On the other hand, we assume that $\mathcal{M}_{g-1,n}$ is the subgroup of $\mathcal{M}_{g,n}$ generated by $T_1', \ldots, T_n', T_0, T_2, \ldots, T_{2g-2}$. Since the image $\varphi(\mathcal{M}_{g-1,n})$ lies in the centralizer of H, it acts on the set of orbits $\{\Omega_{k,1}, \ldots, \Omega_{k,h_k}\}$ as well as on the whole set $\widehat{\Omega}_k$. The first action induces a homomorphism $\nu_k : \mathcal{M}_{g-1,n} \to \mathfrak{S}_{h_k}$, and the second induces a

homomorphism $\psi_k : \mathcal{M}_{g-1,n} \to \mathfrak{S}_{kh_k}$. Applying Lemma 8.1 (1) to $\varphi_j(\mathcal{M}_{g,1})$ for any j, we get that $h_3 = N_{g-1}^{\epsilon}$, $h_1 = N_{g-1}^{-\epsilon}$, and $h_k = 0$ if $k \notin \{1, 3\}$.
As in the proof of Lemma 8.1, we set $\widehat{\Omega}_3^1 = \widehat{\Omega}_3 - S(w_{2g+1})$, $\widehat{\Omega}_3^3 = \widehat{\Omega}_3 - S(w_{2g})$, and $\widehat{\Omega}_3^2 = \widehat{\Omega}_3 - (\widehat{\Omega}_3^1 \cup \widehat{\Omega}_3^3)$. Then $\widehat{\Omega}_3^\ell$ is invariant under the action of $\mathcal{M}_{g-1,n}$ for $\ell = 1, 2, 3$, and the action of $\mathcal{M}_{g-1,n}$ on $\widehat{\Omega}_3^\ell$ is equivalent to ν_3. Hence,

$$\varphi|_{\mathcal{M}_{g-1,n}} \cong \psi_3 \oplus \psi_1 \cong (\nu_3)^3 \oplus \nu_1 \,.$$

Since $h_3, h_1 \leq N_{g-1}^+$, by induction we have $\nu_3(T_j') = \nu_3(T_1')$ and $\nu_1(T_j') = \nu_1(T_1')$, thus $\varphi(T_j') = \varphi(T_1')$ for all $j \in \{1, \ldots, n\}$. Since φ_1 is conjugate to $\phi_{g,1}^{\epsilon}$, we conclude that φ is conjugate to $\phi_{g,n}^{\epsilon}$. □

Proof of Theorem 0.5. This follows from Proposition 7.2 and Theorem 0.4, proved above. □

References

[1] **J. Aramayona, J. Souto.** *Homomorphisms between mapping class groups.* Geom. Topol., to appear.

[2] **M. Aschbacher.** *On the maximal subgroups of the finite classical groups.* Invent. Math. **76** (1984), no. 3, 469–514.

[3] **J. S. Birman.** *On Siegel's modular group.* Math. Ann. **191** (1971), 59–68.

[4] **W. Bosma, J. Cannon, C. Playoust.** *The* MAGMA *algebra system I: The user language.* J. Symb. Comput. **24** (1997), 235–265, http://magma.maths.usyd.edu.au/magma.

[5] **M. R. Bridson.** *Semisimple actions of mapping class groups on* CAT(0) *spaces.* Geometry of Riemann surfaces, 1–14, London Math. Soc. Lecture Note Ser., 368, Cambridge Univ. Press, Cambridge, 2010.

[6] **M. R. Bridson.** *On the dimension of CAT(0) spaces where mapping class groups act.* J. Reine Angew. Math., to appear. arXiv:0908.0690.

[7] **J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, R. A. Wilson.** *Atlas of finite groups. Maximal subgroups and ordinary characters for simple groups. With computational assistance from J. G. Thackray.* Oxford University Press, Eynsham, 1985.

[8] **B. N. Cooperstein.** *Minimal degree for a permutation representation of a classical group.* Israel J. Math. **30** (1978), no. 3, 213–235.

[9] **H. S. M. Coxeter, W. O. J. Moser.** *Generators and relations for discrete groups.* Springer-Verlag, Berlin-Göttingen-Heidelberg, 1957.

[10] **L. E. Dickson.** *Representations of the general symmetric group as linear groups in finite and infinite fields.* Trans. Amer. Math. Soc. **9** (1908), 121–148.

[11] **R. H. Dye.** *Interrelations of symplectic and orthogonal groups in characteristic two.* J. Algebra **59** (1979), no. 1, 202–221.

[12] **B. Farb.** *Some problems on mapping class groups and moduli space.* Problems on mapping class groups and related topics, 11–55, Proc. Sympos. Pure Math., 74, Amer. Math. Soc., Providence, RI, 2006.

[13] **B. Farb, D. Margalit.** *A Primer on Mapping Class Groups.* Princeton University Press, to appear.

[14] **L. Funar.** *Two questions on mappping class groups.* Proc. Amer. Math. Soc. **139** (2011), no. 1, 375–382.

[15] **E. K. Grossman.** *On the residual finiteness of certain mapping class groups.* J. London Math. Soc. (2) **9** (1974/75), 160–164.

[16] **J. L. Harer.** *Stability of the homology of the mapping class groups of orientable surfaces.* Ann. of Math. (2) **121** (1985), no. 2, 215–249.

[17] **W. J. Harvey, M. Korkmaz.** *Homomorphisms from mapping class groups.* Bull. London Math. Soc. **37** (2005), no. 2, 275–284.

[18] **S. P. Humphries.** *Normal closures of powers of Dehn twists in mapping class groups.* Glasgow Math. J. **34** (1992), no. 3, 313–317.

[19] **A. Hurwitz.** *Über algebraische Gebilde mit eindeutigen Transformationen in sich.* Math. Ann. **41** (1893), 403–442.

[20] **S. P. Kerckhoff.** *The Nielsen realization problem.* Ann. of Math. (2) **117** (1983), no. 2, 235–265.

[21] **M. Korkmaz.** *Low-dimensional homology groups of mapping class groups: a survey.* Turkish J. Math. **26** (2002), no. 1, 101–114.

[22] **C. Labruère, L. Paris.** *Presentations for the punctured mapping class groups in terms of Artin groups.* Algebr. Geom. Topol. **1** (2001), 73–114.

[23] **M. W. Liebeck.** *On the orders of maximal subgroups of the finite classical groups.* Proc. London Math. Soc. (3) **50** (1985), no. 3, 426–446.

[24] **M. Matsumoto.** *A presentation of mapping class groups in terms of Artin groups and geometric monodromy of singularities.* Math. Ann. **316** (2000), no. 3, 401–418.

[25] **D. Mumford.** *Abelian quotients of the Teichmüller modular group.* J. Analyse Math. **18** (1967), 227–244.

[26] **L. Paris.** *Small index subgroups of the mapping class group.* J. Group Theory **13** (2010), no. 4, 613–618.

[27] **L. Paris, D. Rolfsen.** *Geometric subgroups of mapping class groups.* J. Reine Angew. Math. **521** (2000), 47–83.

[28] **J. Powell.** *Two theorems on the mapping class group of a surface.* Proc. Amer. Math. Soc. **68** (1978), no. 3, 347–350.

[29] **A. Putman.** *Cutting and pasting in the Torelli group.* Geom. Topol. **11** (2007), 829–865.

[30] **C. C. Sims.** *Computation with finitely presented groups.* Encyclopedia of Mathematics and its Applications, 48. Cambridge University Press, Cambridge, 1994.

[31] **D. E. Taylor.** *The geometry of the classical groups.* Sigma Series in Pure Mathematics, 9. Heldermann Verlag, Berlin, 1992.

[32] **R. A. Wilson.** *The finite simple groups.* Graduate Texts in Mathematics, 251. Springer-Verlag London, Ltd., London, 2009.

[33] **B. P. Zimmermann.** *A note on minimal finite quotients of mapping class groups.* Preprint. arXiv:0803.3144.

A. Jon Berrick,

Yale-NUS College, 6 College Avenue East, Singapore 138614, SINGAPORE
and
Department of Mathematics, National University of Singapore, 10 Lower Kent Ridge Road, Singapore 119076, SINGAPORE.

E-mail: jon.berrick@yale-nus.edu.sg and berrick@math.nus.edu.sg

Volker Gebhardt,

School of Computing, Engineering and Mathematics, University of Western Sydney, Locked Bag 1797, Penrith NSW 2751, AUSTRALIA.

E-mail: v.gebhardt@uws.edu.au

Luis Paris,

Université de Bourgogne, Institut de Mathématiques de Bourgogne, UMR 5584 du CNRS, B.P. 47870, 21078 Dijon cedex, FRANCE.

E-mail: lparis@u-bourgogne.fr