



ELSEVIER



Journal of Algebra ●●● (●●●●) ●●●-●●●

JOURNAL OF Algebra

www.elsevier.com/locate/jalgebra

# Canonical symplectic representations for prime order conjugacy classes of the mapping-class group <sup>☆</sup>

Jane Gilman

Mathematics Department, Rutgers University, Newark, NJ 07102, USA

Received 14 January 2007

Communicated by Derek Holt

## Abstract

In this paper we find a unique normal form for the symplectic matrix representation of the conjugacy class of a prime order element of the mapping-class group. We find a set of generators for the fundamental group of a surface with a conformal automorphism of prime order which reflects the action the automorphism in an optimal way. This is called an *adapted* homotopy basis and there is a corresponding *adapted presentation*. We also give a necessary and sufficient condition for a prime order symplectic matrix to be the image of a prime order element in the mapping-class group.

© 2007 Published by Elsevier Inc.

**Keywords:** Mapping class group; Symplectic group; Matrix representation; Algorithm; Conformal automorphisms; Riemann surfaces

## Contents

1. Introduction	2
Part I. Summary of terms and prior results	3
2. Preliminaries	3
2.1. Notation and terminology	3
2.2. Equivalent languages	3
2.3. Conjugacy invariants for prime order mapping classes or conformal automorphisms	4
2.4. Homology	4

<sup>☆</sup> Partially supported by grants from the NSA and the Rutgers Research Council and by Yale University.  
E-mail address: gilman@rutgers.edu.

1	2.5. Convention for actions on curves, homotopy, and homology . . . . .	4	1
2	3. Prior results and definitions: matrices and homology bases . . . . .	5	2
3	3.1. Existence of adapted homology bases . . . . .	5	3
4	3.2. Intersection matrix for an adapted homology basis . . . . .	5	4
5	3.3. Matrix forms . . . . .	6	5
6	Part 2. The surface symbol algorithm . . . . .	9	6
7	4. The surface symbol reduction algorithm . . . . .	9	7
8	4.1. How to reduce a linked polygon . . . . .	10	8
9	4.2. Analysis of the algorithm . . . . .	11	9
10	Part 3. Review of rewriting basics, prior results and notation . . . . .	12	10
11	5. Schreier–Reidemeister rewriting and its corollaries . . . . .	12	11
12	5.1. The relation between the action of the homeomorphism and the surface kernel subgroup . . . . .	12	12
13	5.2. The rewriting . . . . .	13	13
14	5.3. Illustration . . . . .	14	14
15	Part 4. Homotopy and the algorithm . . . . .	15	15
16	6. Finding the generators for the fundamental group and the algorithm . . . . .	15	16
17	6.1. The action on the fundamental group of $S_0$ . . . . .	15	17
18	6.2. Calculating with simpler notation . . . . .	15	18
19	6.3. Eliminating generators and relations . . . . .	17	19
20	7. Applying the algorithm . . . . .	19	20
21	7.1. Complexity . . . . .	20	21
22	7.2. Other matrices . . . . .	20	22
23	8. Homotopy when $t = 0$ . . . . .	20	23
24	9. Example, $p = 3, t = 5 (1, 1, 2, 1, 1)$ . . . . .	22	24
25	Acknowledgments . . . . .	25	25
26	References . . . . .	25	26

1. Introduction

This is the second of two papers on prime order conformal automorphisms of compact Riemann surfaces of genus  $g \geq 2$ . The mapping-class group of a surface  $S$  of genus  $g$ , denoted by  $MCG(S)$ , is the set of homotopy classes of self-homeomorphisms of  $S$ . It is well known that the action of a homeomorphism  $h$  of a surface of genus  $g$  on a *canonical homology basis*, a homology basis with certain intersection properties, will give a symplectic matrix,  $M_{hCAN}$ . That is,  $M_{hCAN}$  is an element of  $Sp(2g, \mathbb{Z})$ , the set of  $2g \times 2g$  integer valued matrices that preserve the symplectic form, the non-degenerate skew-symmetric bilinear quadratic form with matrix,  $J = \begin{pmatrix} 0 & I_g \\ -I_g & 0 \end{pmatrix}$  where  $I_g$  denotes the  $g \times g$  identity matrix. The intersection numbers for the curves in a canonical basis is precisely given by the matrix  $J$ . We fix a canonical homology basis and let  $\pi$  denote the surjective map  $\pi : MCG(S) \rightarrow Sp(2g, \mathbb{Z})$ .

In [4,6] we found that corresponding to any conformal automorphism  $h$  of prime order, there exists a special set of generators for the first homology of the surface that reflected the action of the homeomorphism  $h$  in an optimal way. Such a basis was termed an *adapted basis* or equivalently a *basis adapted to  $h$* . In particular the matrix action of the automorphism on the basis had a very simple form. The curves in this homology basis did not form a canonical homology basis. The intersection matrix for the adapted basis was found in [5].

In particular, we have ordered pairs of matrix representations and intersection matrices  $(M_{h_{CAN}}, J)$  and  $(M_A, J_A)$  where  $M_A$  is the matrix of the action on an adapted basis and  $J_A$  the intersection matrix for that basis. For each  $0 < t \leq 2g + 2$  and for each prime  $p \geq 2$ , there is a set of  $t$  integers  $(n_1, \dots, n_t)$  with  $0 < t \leq p - 1$  with  $\sum_{j=1}^t n_j \equiv 0 \pmod{p}$  that determines the conjugacy class of  $h$ . Here  $\equiv \dots \pmod{p}$  denotes equivalence modulo  $p$ . These integers are reflected in each ordered pair. However, in the second pair, these integers are reflected in the intersection matrix and in the first pair, reflected in the matrix of the action of the homeomorphism.

In this paper we present an algorithm to obtain  $M_{h_{CAN}}$  from  $M_A$ . The input to the algorithm is the  $t$ -tuple of integers. The output is a canonical representative for the conjugacy class of  $h$  in  $Sp(2g, \mathbb{Z})$ . Thus the main result of this paper is to describe a canonical representative for each prime order conjugacy class in  $Sp(2g, \mathbb{Z})$  that is the representation of a prime order element of the mapping-class group. All other prime order symplectic matrices are representations of infinite order mapping-classes.

The organization of this paper is as follows: In Part 1, we fix notation and summarize terms and prior results; in Part 2 we develop the tight surface symbol reduction algorithm, and in Part 3 we review the basics of the Schreier–Reidemeister rewriting process. In Part 4, using new calculations we obtain an *adapted presentation of the fundamental group* corresponding to a conformal or finite order mapping class. The main theorems (Theorem 6.4 and Theorems 7.1, 7.2 and 7.3) are proved there in Part 4 and a detailed example is worked out by hand (Section 9).

There is renewed interest in mapping-class groups in regard to computing on Riemann surfaces. In earlier work we noted that in the abstract there was in theory a method for converting the adapted basis to a canonical homology basis and the adapted matrix representation to a symplectic matrix representation, but the formula involved was unwieldy. However, we have recently observed that while the formula is messy for hand computations, it can be implemented as an algorithm whose complexity is bounded by  $O(g^{10})$ .

## Part 1. Summary of terms and prior results

### 2. Preliminaries

#### 2.1. Notation and terminology

We let  $h$  be a conformal automorphism of a compact Riemann surface  $S$  of genus  $g \geq 2$ . Then  $h$  will have a finite number,  $t$ , of fixed points. We let  $S_0$  be the quotient of  $S$  under the action of the cyclic group generated by  $h$  so that  $S_0 = S/\langle h \rangle$  and let  $g_0$  be its genus. If  $h$  is of prime order  $p$  with  $p \geq 2$ , then the Riemann–Hurwitz relation shows that  $2g = 2pg_0 + (p - 1)(t - 2)$ . If  $p = 2$ , of course, this implies that  $t$  will be even.

#### 2.2. Equivalent languages

We emphasize that  $h$  can be thought of in a number or equivalent ways using different terminology. For a compact Riemann surface of genus  $g \geq 2$ , homotopy classes of homeomorphisms of surfaces are the same as isotopy classes. Therefore,  $h$  can be thought of as a representative of a homotopy class or an isotopy class. Further, every isotopy class of finite order contains an element of finite order so that  $h$  can be thought of as a homeomorphism of finite order. For every finite order homeomorphism of a surface there is a Riemann surface on which its action is conformal. A conformal homeomorphism of finite order up to homotopy is finite. We use the language

of conformal maps, but observe that all of our results can be formulated using these other classes of homeomorphisms.

We remind the reader that the mapping-class group of a compact surface of genus  $g$  is also known as the Teichmüller modular group or the Modular group, for short. We write  $MCG(S)$  or  $MCG(S_g)$  for the mapping class group of the surface  $S$  using the  $g$  when we need to emphasize that  $S$  is a compact surface of genus  $g$ . The Torelli Modular group or the Torelli group for short,  $\mathcal{T}(S)$  is homeomorphisms of  $S$  modulo those that induce the identity on homology and the homology of a surface is the abelianized homotopy. There is surjective map  $\pi$  from the mapping-class group onto  $Sp(2g, \mathbb{Z})$  that assigns to a homeomorphism the matrix of its action on a canonical homology basis (see 2.4). The induced map from the Torelli group to the symplectic group is an isomorphism.

It is well known that the map  $\pi$  when restricted to elements of finite order is an isomorphism. An even stronger result can be found in [4,6].

Since  $h$  can be thought of as a finite representative of a finite order mapping-class, we will always treat it as finite. For ease of exposition we use the language of a conformal maps and do not distinguish between a homeomorphism that is of finite order or that is of finite order up to homotopy or isotopy, a finite order representative for the homotopy class, a conformal representative for the class or the class itself. That is, we do not use different notation to distinguish between the topological map, its homotopy class or a finite order representative or a conformal representative.

For ease of exposition in what follows we first assume that  $t > 0$ . We treat the case  $t = 0$  separately in Section 8.

### 2.3. Conjugacy invariants for prime order mapping classes or conformal automorphisms

Nielsen showed that the conjugacy class of  $h$  in the mapping-class group is determined by the set of  $t$  non-zero integers  $\{n_1, \dots, n_t\}$  with  $0 < n_i < p$  where  $\sum_{i=1}^t n_i \equiv 0 \pmod{p}$ .

Let  $m_j$  be the number of  $n_i$  equal to  $j$ . Then we have  $\sum_{i=1}^{p-1} i \cdot m_i \equiv 0 \pmod{p}$  (see [3] for details) and the conjugacy class is also determined by the  $(p-1)$ -tuple,  $(m_1, \dots, m_{p-1})$ .

Topologically we can think of  $h$  as a counterclockwise rotation by an angle of  $\frac{2\pi \cdot s_i}{p}$  about the fixed point  $p_i$ ,  $i = 1, \dots, t$ , of  $h$ . We call the  $s_i$  the *rotation numbers*. The  $n_i$  are the *complementary rotation numbers*, that is,  $0 < s_i < p$  with  $s_i n_i \equiv 1 \pmod{p}$ .

### 2.4. Homology

We recall the following facts about Riemann surfaces.

The homology group of a compact Riemann surface of genus  $g$  is the abelianized homotopy. Therefore, a homology basis for  $S$  will contain  $2g$  homologically independent curves. Every surface has a *canonical homology basis*, a set of  $2g$  simple closed curves,  $a_1, \dots, a_g; b_1, \dots, b_g$  with the property that for all  $i$  and  $j$ ,  $a_i \times a_j = 0$ ,  $b_i \times b_j = 0$  and  $a_i \times b_j = \delta_{ij} = -b_j \times a_i$  where  $\times$  is the algebraic intersection number and  $\delta_{ij}$  is the Kronecker delta.

### 2.5. Convention for actions on curves, homotopy, and homology

A homeomorphism  $h$  of a surface induces an action on the fundamental group of the surface (mapping the fundamental group with base point  $x_0$  to the one with bases point  $h(x_0)$ ) and thus acts as an (outer) automorphism of the fundamental group of  $S$ . It also induces an automorphism

of the first homology group of  $S$ . If  $\gamma$  is any curve on  $S$  or any representative of a free homotopy class or homology class on  $S$ , we adopt the convention that  $h(\gamma)$  denotes either the image curve or the free homotopy class or homology class of the image. It will be clear from the context which we mean.

### 3. Prior results and definitions: matrices and homology bases

Roughly speaking a homology basis for  $S$  is *adapted to  $h$*  if it reflects the action of  $h$  in a simple manner: for each curve  $\gamma$  in the basis either all of the images of  $\gamma$  under powers of  $h$  are also in the basis or the basis contains all but one of the images of  $\gamma$  under powers of  $h$  and the omitted curve is homologous to the negative of the sum of the images of  $\gamma$  under the other powers of  $h$ .

To be more precise

**Definition 3.1.** A homology basis for  $S$  is adapted to  $h$  if for each  $\gamma_0$  in the basis there is a curve  $\gamma$  with  $\gamma_0 = h^k(\gamma)$  for some integer  $k$  and either

- (1)  $\gamma, h(\gamma), \dots, h^{p-1}(\gamma)$  are all in the basis, or
- (2)  $\gamma, h(\gamma), \dots, h^{p-2}(\gamma)$  are all in the basis and  $h^{p-1}(\gamma) \approx^h -(h(\gamma) + h(\gamma) + \dots + h^{p-2}(\gamma))$ . Here  $\approx^h$  denotes is homologous to.

#### 3.1. Existence of adapted homology bases

It is known that

**Theorem 3.2.** (See [4,6].) *There is a homology basis adapted to  $h$ . In particular, if  $g \geq 2$ ,  $t \geq 2$ ,  $g_0$  are as above, then the adapted basis has  $2p \times g_0$  elements of type (1) above and  $(p-1)(t-2)$  elements of type (2).*

And thus it follows that

**Corollary 3.3.** (See [4].) *Let  $M_{\mathcal{A}}(h)$  denote the adapted matrix of  $h$ , the matrix of the action of  $h$  with respect to an adapted basis. Then  $M_{\mathcal{A}}(h)$  will be composed of diagonal blocks,  $2g_0$  of which are  $p \times p$  permutation matrices with 1's along the super-diagonal and 1 in the leftmost entry of the last row and  $t$  are  $(p-1) \times (p-1)$  matrices with 1's along the super-diagonal and all entries in the last row  $-1$ .*

**Remark 3.4.** We adopt the following convention. When we pass from homotopy to homology, we use the same notation for the homology class of the curve as for the curve or its homotopy class, but write  $\approx^h$  instead of  $=$ . It will be clear from the context which we mean.

#### 3.2. Intersection matrix for an adapted homology basis

So far information about  $M_{\mathcal{A}}$  seems to depend only on  $t$  and not upon the  $(p-1)$ -tuple  $(m_1, \dots, m_{p-1})$  or equivalently, upon the set of integers  $\{n_1, \dots, n_t\}$  which determines the conjugacy class of  $h$  in the mapping-class group. However, while the  $2pg_0$  curves can be extended

to a canonical homology basis for  $h$ , the rest of the basis cannot and its intersection matrix,  $J_{\mathcal{A}}$  depends upon these integers.

In [5] the intersection matrix for the adapted basis was computed.

The adapted basis consisted of the curves of type (1):

$$\{A_w, B_w, w = 1, \dots, g_0\} \cup \{h^j(A_w), h^j(B_w), j = 1, \dots, p - 1\}$$

and (some of) the curves of type (2):

$$X_{i,v_i}, h^j(X_{i,v_i}), \quad i = 1, \dots, (p - 1), \quad j = 1, \dots, p - 2, \quad v_i = 1, \dots, u_i.$$

A lexicographical order is placed on  $X_{i,v_i}$  so that  $(r, v_r) < (s, v_s)$  if and only if  $r < s$  or  $r = s$  and  $v_r < v_s$ . The  $t - 2$  curves  $X_{s,v_s}$  with the largest subscript pairs are to be included in the homology basis. Let  $\widehat{s}$  be the smallest integer  $s$  such that  $u_s \neq 0$  and let  $\widehat{q}$  be chosen so that  $\widehat{q}\widehat{s} \equiv 1 \pmod{p}$ . For any integer  $v$  let  $[v]$  denote the least non-negative residue of  $\widehat{q}v$  modulo  $p$ . Thus the integer  $[v]$  satisfies  $0 \leq [v] \leq p - 1$  and  $\widehat{s} \times [v] \equiv v \pmod{p}$ .

**Theorem 3.5.** (See [5].) *If  $(u_1, \dots, u_{p-1})$  determines the conjugacy class of  $h$  in the mapping-class group, then the surface  $S$  has a homology basis consisting of:*

- (1)  $h^j(A_w), h^j(B_w)$  where  $1 \leq w \leq g_0, 0 \leq j \leq p - 1$ .
- (2)  $h^k(X_{s,v_s})$  where  $0 \leq k \leq p - 2$  and for all pairs  $(s, v_s)$  with  $1 \leq s \leq p - 1, 1 \leq v_s \leq u_s$  except that the two smallest pairs are omitted.

The intersection numbers for the elements of the adapted basis are given by

- (a)  $h^j(A_w) \times h^j(B_w) = 1,$
- (b) if  $(r, v_r) < (s, v_s)$ , then

$$h^0(X_{r,v_r}) \times h^k(X_{s,v_s}) = \begin{cases} 1 & \text{if } [k] < [r] \leq [k + s], \\ -1 & \text{if } [k + s] < [r] \leq [k], \end{cases}$$

$$h^0(X_{s,v_s}) \times h^k(X_{s,v_s}) = \begin{cases} 1 & \text{if } [k] \leq [s] < [k + s], \\ -1 & \text{if } [k + s] < [s] < [k]. \end{cases}$$

- (3) All other intersection numbers are 0 except for those that following from the above by applying the identities below to arbitrary homology classes  $C$  and  $D$ ,

$$C \times D = -D \times C,$$

$$h^j(C) \times h^k(D) = h^0(C) \times h^{k-j}(D) \quad (k - j \text{ reduced modulo } p).$$

### 3.3. Matrix forms

We can write the results of Theorems 3.2 and 3.5 and Corollary 3.3 in an explicit matrix form. To do so we fix notation for some matrices. We will use the various explicit forms in subsequent sections.

We let  $M_{\widetilde{\mathcal{A}}}$  denote the matrix of the action of  $h$  on an adapted basis and  $J_{\widetilde{\mathcal{A}}}$  be the corresponding intersection matrix. Further, we let  $M_{h_{CAN}}$  be the matrix of the action of  $h$  on a canonical homology basis. The corresponding intersection matrix is denoted by  $J_{h_{CAN}}$  or  $J$ .

1 However, we prefer to replace  $J$  by the following block matrix where  $q = \frac{(p-1)(t-2)}{2}$  and 1  
 2 where for any integer positive integer  $d$ ,  $I_d$  denotes the  $d \times d$  identity matrix 2  
 3

$$4 \quad J_{h_{CAN}} = \begin{pmatrix} 0 & I_{pg_0} & 0 & 0 \\ 5 \quad -I_{pg_0} & 0 & 0 & 0 \\ 6 \quad 0 & 0 & 0 & I_q \\ 7 \quad 0 & 0 & -I_q & 0 \end{pmatrix} .$$

8 We denote the  $p \times p$  permutation matrix by 8  
 9

$$10 \quad M_{p \times p} = \begin{pmatrix} 0 & 1 & 0 & 0 & \dots & 0 & 0 \\ 11 \quad 0 & 0 & 1 & 0 & \dots & 0 & 0 \\ 12 \quad 0 & 0 & 0 & 1 & \dots & 0 & 0 \\ 13 \quad \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 14 \quad 0 & 0 & 0 & 0 & \dots & 1 & 0 \\ 15 \quad 0 & 0 & 0 & 0 & \dots & 0 & 1 \\ 16 \quad 1 & 0 & 0 & 0 & \dots & 0 & 0 \end{pmatrix} ,$$

17 the  $(p-1) \times (p-1)$  non-permutation matrix of the theorem by 17  
 18  
 19

$$20 \quad N_{(p-1) \times (p-1)} = \begin{pmatrix} 0 & 1 & 0 & 0 & \dots & 0 & 0 \\ 21 \quad 0 & 0 & 1 & 0 & \dots & 0 & 0 \\ 22 \quad 0 & 0 & 0 & 1 & \dots & 0 & 0 \\ 23 \quad \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 24 \quad 0 & 0 & 0 & 0 & \dots & 1 & 0 \\ 25 \quad 0 & 0 & 0 & 0 & \dots & 0 & 1 \\ 26 \quad -1 & -1 & -1 & -1 & \dots & -1 & -1 \end{pmatrix} .$$

27 Thus we have the  $2g_0p \times 2g_0p$  block matrix 27  
 28  
 29

$$30 \quad M_{A_{2g_0, p \times p}} = \begin{pmatrix} M_{p \times p} & 0 & 0 & \dots & 0 & 0 \\ 31 \quad 0 & M_{p \times p} & 0 & \dots & 0 & 0 \\ 32 \quad \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 33 \quad 0 & 0 & 0 & \dots & M_{p \times p} & 0 \\ 34 \quad 0 & 0 & 0 & \dots & 0 & M_{p \times p} \end{pmatrix}$$

35 and the  $(t-2) \cdot (p-1) \times (t-2) \cdot (p-1)$  block matrix  $N_{A_{(t-2), (p-1) \times (p-1)}}$  35  
 36  
 37

$$38 \quad \begin{pmatrix} N_{(p-1) \times (p-1)} & 0 & 0 & \dots & 0 & 0 \\ 39 \quad 0 & N_{(p-1) \times (p-1)} & 0 & \dots & 0 & 0 \\ 40 \quad \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 41 \quad 0 & 0 & 0 & \dots & N_{(p-1) \times (p-1)} & 0 \\ 42 \quad 0 & 0 & 0 & \dots & 0 & N_{(p-1) \times (p-1)} \end{pmatrix}$$

so that the  $2g \times 2g$  matrix  $M_{\mathcal{A}}$  breaks into blocks and can be written as

$$M_{\mathcal{A}} = \begin{pmatrix} M_{\mathcal{A}_{2g_0, p \times p}} & 0 \\ 0 & N_{\mathcal{A}_{(t-2), (p-1) \times (p-1)}} \end{pmatrix}$$

where the blocks are of appropriate size. The basis can be rearranged so that  $2g \times 2g$  matrix  $M_{\tilde{\mathcal{A}}}$  corresponding to the rearranged basis breaks into blocks

$$M_{\tilde{\mathcal{A}}} = \begin{pmatrix} M_{\mathcal{A}_{g_0, p \times p}} & 0 & 0 \\ 0 & M_{\mathcal{A}_{g_0, p \times p}} & 0 \\ 0 & 0 & N_{\mathcal{A}_{(t-2), (p-1) \times (p-1)}} \end{pmatrix}.$$

Here the submatrix

$$\begin{pmatrix} M_{\mathcal{A}_{g_0, p \times p}} & 0 \\ 0 & M_{\mathcal{A}_{g_0, p \times p}} \end{pmatrix}$$

is a symplectic matrix. We obtain the corollary.

**Corollary 3.6.** *Let  $S$  be a compact Riemann surface of genus  $g$  and assume that  $S$  has a conformal automorphism  $h$  of prime order  $p \geq 2$ . Assume that  $h$  has  $t$  fixed points where  $t \geq 2$ . Let  $S_0$  be the quotient surface  $S_0 = S/\langle h \rangle$  where  $\langle h \rangle$  denotes the cyclic group generated by  $h$  and let  $g_0$  be the genus of  $S_0$  so that  $2g = 2pg_0 + (t-2)(p-1)$ .*

*There is a homology bases on which the action of  $h$  is given by the  $2g \times 2g$  matrix  $M_{\tilde{\mathcal{A}}}$ .*

*The matrix  $M_{\tilde{\mathcal{A}}}$  contains a  $2g_0p \times 2g_0p$  symplectic submatrix, but is not a symplectic matrix except in the special case  $t = 2$ .*

**Remark 3.7.** We note that if  $p = 2$ ,  $M_{p \times p}$  reduces to  $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$  and  $N_{(p-1) \times (p-1)}$  to the  $1 \times 1$  matrix  $-1$ .

The point here is that while two automorphisms with the same number of fixed points will have the same matrix representation with respect to an adapted basis, the intersection matrices will not be the same and, therefore, the corresponding two matrix representations in the symplectic group will not be conjugate.

We seek an algorithm to replace  $M_{\tilde{\mathcal{A}}}$  by the symplectic matrix  $M_{h_{CAN}}$  by replacing the  $2g \times 2g$  submatrix  $N_{(t-2), (p-1) \times (p-1)}$  by a symplectic matrix of the same size. We will call this matrix  $N_{\text{symp}} \tilde{\mathcal{A}}$ .

We note that  $J_{\tilde{\mathcal{A}}}$  is of the form

$$\begin{pmatrix} 0 & I_{pg_0} & 0 & 0 \\ -I_{pg_0} & 0 & 0 & 0 \\ 0 & 0 & B_1 & B_2 \\ 0 & 0 & B_3 & B_4 \end{pmatrix}$$

where the blocks  $B_i$  are of the appropriate dimension and we let  $B$  denote the  $2q \times 2q$  matrix

$$\begin{pmatrix} B_1 & B_2 \\ B_3 & B_4 \end{pmatrix}.$$

We also note that  $M_{h_{CAN}}$  will break up into

$$M_{h_{CAN}} = \begin{pmatrix} M_{\mathcal{A}_{g_0, p \times p}} & 0 & 0 \\ 0 & M_{\mathcal{A}_{g_0, p \times p}} & 0 \\ 0 & 0 & N_{h_{CAN}} \end{pmatrix}$$

where  $N_{h_{CAN}}$  is a  $(t - 2)(p - 1) \times (t - 2)(p - 1)$  matrix.

We emphasize that our goal is to find a canonical form for  $N_{\text{symp}} \tilde{\mathcal{A}} = N_{h_{CAN}}$  and an algorithm that produces it from the conjugacy class data. This is found in Section 6. We illustrate this with a detailed example in Section 9.

**Part 2. The surface symbol algorithm**

**4. The surface symbol reduction algorithm**

For a compact Riemann surface of genus  $g \geq 2$ , a presentation for the fundamental group with one defining relation determines a *surface symbol*. There is a standard way to convert any surface symbol to a normal form [1,10] where it is written as the product of the minimal number of commutators. Here we follow the details and notation from Springer (Section 5.5 of [13]).

If we have a compact Riemann surface, we obtain the *surface symbol* homeomorphic to the surface under identifications by cutting along the generators of the fundamental group and labeling the sides appropriately. Let  $\mathcal{P}$  denote the polygon obtained by cutting along the curves. Since  $\mathcal{P}$  is obtained by cutting along curves in the fundamental group, each *side* occurs once in the positive direction and once in the negative direction as one moves along the boundary in the positive (counterclockwise) direction. The surface symbol is the sequence of *sides* that occur. That is it is a sequence of the form  $abc \dots a^{-1} \dots c^{-1} \dots rstb^{-1} \dots$

We define

**Definition 4.1.**

- (1) A polygon is *evenly worded* if for each edge  $a$  that occurs  $a^{-1}$  also occurs.
- (2) A pair of edges  $a$  and  $b$  are *linked* if they appear in the symbol in the order  $\dots a \dots b \dots a^{-1} \dots b^{-1} \dots$
- (3) The polygon is *fully linked* if each edge occurring in the relation is linked to another unique distinct edge.
- (4) The edges  $a$  and  $b$  occurring in the polygon are *optimally linked* if the symbol is of the form  $W_0 a W_1 b W_2 a^{-1} W_3 b^{-1} W_4$  where the  $W_i, i = 0, \dots, 4$ , are words in the edges not involving  $a^{\pm 1}$  or  $b^{\pm 1}$ .
- (5) A pair of edges  $m$  and  $n$  are *tightly linked* if they appear in the symbol in the order  $mnm^{-1}n^{-1}$ .
- (6) A polygon is *tightly worded* if each edge or its inverse is tightly linked to the another edge in the symbol.

Note that a symbol is tightly worded when it can be written as a product of commutators and the product of  $g$  commutators is the normal form for a compact surface of genus  $g$ . Thus it corresponds to a canonical homology basis. Also note that for the symbol we will be tightly linking all linked edges are optimally linked because each edge and its inverse occur only once

in the symbol and the steps we take will not change that. Finally, a surface symbol will always have an even number of edges since each edge and its inverse will occur.

**Remark 4.2.** More generally, one can consider arbitrary polygons with identified sides labeled as  $x$  and  $x^{-1}$ . In that case the polygon may have more than one equivalence class of identified vertices. There is an algorithm for replacing the surface symbol by another surface symbol in a manner that increases the number of vertices in one equivalence class and decreases the number of vertices in the other until one obtains a symbol with only one equivalence class of vertices [13]. Since we are taking our surface symbol from the fundamental group with fixed base point, our surface symbols only have one equivalence class of vertices.

In [13] it is shown that if the symbol has one vertex up to identification, which it does if one takes the fundamental group with fixed base point, then each edge is linked with some other edge.

A surface symbol may possess one or more of the properties described in Definition 4.1.

Our goal is to begin with a surface symbol and obtain a tightly worded polygon.

#### 4.1. How to reduce a linked polygon

Let  $a$  and  $b$  be an optimally linked pair of edges with linking words  $W_0, W_1, W_2, W_3, W_4$  so that the symbol is  $W_0aW_1bW_2a^{-1}W_3b^{-1}W_4\dots$ . Then one can replace  $a$  and  $b$  by new words  $M$  and  $N$  and obtain a new polygon where the new words  $M$  and  $N$  are tightly linked by a standard cutting and pasting replacements. In terms of the surface symbol the words  $M$  and  $N$  now represent edges.

We apply this cutting and pasting procedure in the following informal algorithm. This algorithm does more than tightly link the surface symbol. The algorithm input includes the adapted matrix and its output includes a symplectic matrix representation. We let  $\lambda$  represent the empty word.

#### Ordered recipe for tight linking to a symplectic matrix.

**Step 1. (Initialize)** Assume that the polygon  $\mathcal{P}$  has edges  $e_1, \dots, e_m$  where  $m$  is divisible by 4. Thus  $\mathcal{P} = e_1e_2 \dots e_m$ . Further assume that polygon  $\mathcal{P}$  is evenly worded, that it has only one equivalence class of vertices and that it is fully and optimally linked. The initial matrix is  $M_{\mathcal{A}}$ . Input  $\mathcal{P}$  and  $M_{\mathcal{A}}$ . Set  $\mathcal{M} = M_{\mathcal{A}}$ . Set  $\mathcal{Q} = \lambda$ .

#### Step 2. DO

- (*Free reduction*) If  $aa^{-1}$  or  $a^{-1}a$  occur in  $\mathcal{P}$  they can be removed from the symbol as long as the symbol has at least one other letter. Delete  $a$  and  $a^{-1}$  from the set of edges and renumber the remaining edges. Replace  $\mathcal{P}$  by  $\mathcal{P}$  with  $aa^{-1}$  deleted. Repeat this step wherever possible, until no repeated symbols of the form  $xx^{-1}$  or  $x^{-1}x$  occur. (*Note: We will see that in the case where we apply this algorithm we will always have at least one other letter.*)
- (*Linking and truncation*) Begin with left most occurring letter in the surface symbol,  $\mathcal{P}$ . Let  $a$  be this letter. Let  $b$  be the first edge optimally linked with  $a$ . Write  $\mathcal{P} = aW_1bW_2a^{-1}W_3b^{-1}W_4$  where  $W_1, W_2, W_3$  and  $W_4$  are chosen accordingly. Define  $M = aW_1bW_2a^{-1}$  and  $N = W_3W_2a^{-1}$ . (*Note:  $\mathcal{P}$  can now be written as  $[M, N]W_3W_2W_1W_4$ .*)

Preserving cyclical order rename the edges other than  $a, a^{-1}, b,$  and  $b^{-1}$ . That is, define  $e'_1, \dots, e'_m$  to be the remaining edges that occur in  $W_3W_2W_1W_4$ . (Note: We have the initial ordered basis  $e_1, \dots, e_m$  and new ordered basis  $M, N, M^{-1}, N^{-1}, e'_1, \dots, e'_m$ . In terms of the surface symbol the words  $M$  and  $N$  now represent edges. Note also that  $a, b, a^{-1},$  and  $b^{-1}$  are each one of the original  $e'_j$ 's.)

- (Change of basis) Write down the matrix of the change of basis  $\mathcal{B}$ . Namely,  $\mathcal{B}$  is the identity matrix except that the columns corresponding to  $a$  and  $a^{-1}$  are replaced by the columns whose entries are determined by  $M$  and similarly for  $b$  and  $b^{-1}$  and  $N$ . Compute  $\mathcal{B}\mathcal{M}\mathcal{B}^{-1}$ . Replace the matrix  $\mathcal{M}$  by its conjugate  $\mathcal{B}\mathcal{M}\mathcal{B}^{-1}$ .

Set  $e_i = e'_i, i = 1, \dots, m' = m - 4$ .

Set  $\mathcal{Q} = \mathcal{Q} \cdot [\tilde{a}, \tilde{b}]$ .

Set  $\mathcal{P} = W_3W_2W_1W_4$ .

**UNTIL:**  $\mathcal{P} = \lambda$ .

**Step 3.** Output:  $\mathcal{Q}$  and  $\mathcal{M} = M_{h_{CAN}}$ .

(Note: The output consists of the tightly worded surface symbol and the symplectic matrix.)

#### 4.2. Analysis of the algorithm

The input to the algorithm will be the surface symbol  $\widehat{\mathcal{Q}} \cdot \widehat{\mathcal{LR}}$  and the matrix  $M_{\tilde{A}}$  of Corollary 6.6. Alternately the input to the algorithm can be taken to be (a variant of) the surface symbol  $\widehat{R}$  derived in Section 6. It has length  $m = 4g$ . The free reduction step is  $O(m)$ . It reduces the number of edges. In our application we will begin with  $4g$  edges that represent a surface of genus  $g$ . We know that the final surface symbol must also represent a surface of genus  $g$  so that the final surface symbol will still have  $4g$  edges. Thus we will never encounter a free reduction step (see also Remark 4.3). Each repetition of the loop reduces  $m$  by 4 so the algorithm will stop after at most  $\frac{m}{4} = g$  steps.

We can actually initialize our algorithm with any  $\mathcal{Q}, \mathcal{M},$  and  $\mathcal{P}$  of the correct sizes as long as  $\mathcal{Q}$  is a product of commutators and  $\mathcal{P}$  evenly worded and fully and optimally linked. The length of  $\mathcal{P}$  will be at most  $4g$ .

In the linking step we need to do a search to find the first  $b$  optimally linked to  $a$ . Since we are searching a string of length at most  $m$  the time here is  $O(m^2)$ .

The matrix of the change of basis is of size  $2g \times 2g$  and will only have four columns that differ from the identity matrix, those rows and columns that represent replacing  $a$  by the edge labeled  $M$  and  $b$  by the edge now labeled  $N$ .

We are working with free homotopy classes. These are not necessarily abelian, but when we write down the matrix representation and the matrix of the change of basis, we can cancel any occurrence of a generator (or edge)  $x$  and  $x^{-1}$  in the words  $aW_1bW_2a^{-1}$  and  $W_3W_2a^{-1}$ . The words we are working with are of length at most  $m$ . Thus the matrix of the change of basis can be computed in  $O(m^2)$  time. The matrix multiplications and the inversion for the change of basis step are  $O(m^3)$ .

We conclude that, neglecting the size of the integers involved, the complexity of the tight linking algorithm in the case of interest is  $O(g^3)$ . The size of the input is taken into account in Section 7.1.

**Remark 4.3.** We note that iterating the loop for free reduction and linking is the standard algorithm for finding the normal form for a surface symbol (Section 5.5 of [13]). It can be applied to any evenly worded symbol that comes from the fundamental group of a surface. The symbol does not need to be of length divisible by 4. It is guaranteed to give either a final symbol of the form  $aa^{-1}$  or a product of  $2n$  commutators for some integer  $n$  (Theorems 5–16 of [13]). In our case, since we want to add the truncation and change of basis steps, we have assumed the divisibility by 4 to make the description of these steps simpler. Also we have  $2g$  generators for our fundamental group, those in Eq. (19) of Theorem 6.4 or conjugates of those (Corollary 6.5 or Corollary 6.6). Since each generator and its inverse appear exactly once in our surface symbol, we have  $4g$  edges for the input. We know by construction that this is a surface symbol for a compact surface of genus  $g$ . Therefore, we must end with  $4g$  edges (i.e.  $g$  commutators) so in our implementation of the algorithm, we must never encounter a free reduction step.

### Part 3. Review of rewriting basics, prior results and notation

#### 5. Schreier–Reidemeister rewriting and its corollaries

If we begin with an arbitrary finitely presented group  $G_0$  and a subgroup  $G$ , the Schreier–Reidemeister rewriting process tells one how to obtain a presentation for  $G_0$  from the presentation for  $G$ . In our case the larger group  $G_0$  will correspond to the group uniformizing  $S_0$  and the subgroup  $G$  corresponds to the group uniformizing  $S$ .

In particular, one chooses a special set of coset representatives for  $G$  modulo  $G_0$ , called Schreier representatives, and uses these to find a set of generators for  $G$ . These generators are labeled by the original generators of the group and the coset representative.

##### 5.1. The relation between the action of the homeomorphism and the surface kernel subgroup

We may assume that  $S_0 = U/F_0$  where  $F_0$  is the Fuchsian group with presentation

$$\left\langle a_1, \dots, a_{g_0}, b_1, \dots, b_{g_0}, x_1, \dots, x_t \mid x_1 \cdots x_t \left( \prod_{i=1}^g [a_i, b_i] \right) = 1; x_i^p = 1 \right\rangle. \quad (1)$$

We summarize the result of [3,6] using facts about the  $n$ 's and  $m$ 's defined in Section 2.3. Let  $\phi : F_0 \rightarrow \mathbb{Z}_p$  be given by

$$\phi(a_i) = \phi(b_i) = 0 \quad \forall i = 1, \dots, g_0 \quad \text{and} \quad \phi(x_j) = n_j \neq 0 \quad \forall j = 1, \dots, t.$$

If  $F = \text{Ker } \phi$ , then  $S = U/F$ . Moreover,  $F_0/F$  acts on  $S$  with quotient  $S_0$ . Conjugation by  $x_1$  acts on  $F$  and if  $h$  is the induced conformal map on  $S$ ,  $\langle h \rangle$  is isomorphic to the action induced by this conjugation and the conjugacy class of  $h$  in the mapping-class group is determined by the set of  $n_i$ . The order of the  $n_i$ 's does not affect the conjugacy class. Replacing  $h$  by a conjugate we may assume that  $0 < n_i \leq n_j < p$  if  $i < j$ .

When we need to emphasize the relation of  $h$  to  $\phi$ , we write  $h_\phi$  to mean the automorphism determined by conjugation by  $x_1$ . The conjugacy class of  $h^2$ , would then be determined by the homomorphism  $\psi$  with  $\psi(x_j) \equiv 2\phi(x_j) \pmod{p}$  or by conjugation by  $x_1^2$ .

$F$  is sometimes called the surface kernel and  $\phi$  the surface kernel homomorphism [7,8]. Any other map from  $F_0$  onto  $\mathbb{Z}_p$  with the same  $(m_1, \dots, m_{p-1})$  and with  $\phi(x_j) \neq 0 \forall j$  will yield an automorphism conjugate to  $h$ .

5.2. The rewriting

We want to apply the rewriting process to words in the generators of this presentation for  $F_0$  to obtain a presentation for  $F$ . We choose right coset representatives for  $H = \langle h \rangle$  as  $1, x_1, x_1^2, x_1^3, \dots, x_1^{p-1}$  and observe that this set of elements form a Schreier system (see pp. 88 and 93 of [11]). That is, that every initial segment of a representative is again a representative.

The Schreier right coset function assigns to a word  $W$  in the generators of  $F_0$ , its coset representative  $\overline{W}$  and  $\overline{W} = x_1^q$  if  $\phi(W) = \phi(x_1^q)$ .

If  $a$  is a generator of  $F_0$ , set  $S_{K,a} = K a \overline{K} a^{-1}$ . The rewriting process  $\tau$  assigns to a word that is in the kernel of the map  $\phi$ , a word written in the specific generators,  $S_{K,a}$  for  $F$ . Namely, if  $a_w, w = 1, \dots, r$  are generators for  $F_0$  and

$$U = a_{v_1}^{\epsilon_1} a_{v_2}^{\epsilon_2} \dots a_{v_r}^{\epsilon_r} \quad (\epsilon_i = \pm 1),$$

defines an element of  $F$ , then (Corollary 2.7.2, p. 90 of [11])

$$\tau(U) = S_{K_1, a_{v_1}}^{\epsilon_1} S_{K_2, a_{v_2}}^{\epsilon_2} \dots S_{K_r, a_{v_r}}^{\epsilon_r}$$

where  $K_j$  is the representative of the initial segment of  $U$  preceding  $a_{v_j}$  if  $\epsilon_j = 1$  and  $K_j$  is the coset representative of  $U$  up to and including  $a_{v_j}^{-1}$  if  $\epsilon_j = -1$ .

In our case each  $a_v$  stands for some generator of  $F_0$ ; that is one of the  $a_i$  or  $b_i$  or  $x_j$ . We apply Theorem 2.8 of [11] to see

**Theorem 5.1.** (See [6].) *Let  $F_0$  have the presentation given by Eq. (1). Then  $F$  has presentation*

$$\left\langle S_{K,a_i}, S_{K,b_i}, i = 1, \dots, g_0; S_{K,x_j}, j = 1, \dots, t \right\rangle \tag{2}$$

$$\tau \left( K \cdot x_1 \cdots x_t \left( \prod_{i=1}^{g_0} [a_i, b_i] \right) \cdot K^{-1} \right) = 1, \tau(K x_j^p K^{-1}) = 1 \Big\rangle. \tag{3}$$

Here we let  $K$  run over a complete set of coset representative for  $\phi: F_0 \rightarrow H$  so that  $F$  has generators

$$S_{K,a_i}, S_{K,b_i}, \quad i = 1, \dots, g_0, \\ S_{K,x_j}, \quad j = 1, \dots, t.$$

In [6] we simplified the presentation and eliminated generators and relations so that there is a single defining relation for the subgroup. We first assumed that  $\phi(x_1) = h$  noting that if we can find a homology basis adapted to  $h$ , we can easily find a homology basis adapted to any power of  $h$  and, therefore, this assumption will not be significant. We saw:

**Theorem 5.2.** (See [6].) Let  $F_0$  have the presentation given by Eq. (1). Then  $F$  has

$2pg_0 + (t - 2)(p - 1)$  generators:

$$h^j(A_i), h^j(B_i), \quad i = 1, \dots, g_0, \quad j = 0, \dots, p - 1,$$

$$h^j(X_i), \quad i = 3, \dots, t, \quad j = 0, \dots, p - 2,$$

and a single defining relation:

$$\widehat{R} = 1.$$

Each generator and its inverse occur exactly once in  $\widehat{R}$  and every generator that appears is linked to another distinct generator.  $\widehat{R}$  is given explicitly in terms of these generators.

**Corollary 5.3.** (See [6].) The homology basis obtained by abelianizing the basis in Theorem 5.2 gives a homology basis adapted to  $h$ .

We will give  $\widehat{R}$  explicitly in terms of the generators once we have introduced more notation. In this paper we want to simplify  $\widehat{R}$ . To do so we need to include some of the calculations and notation from the earlier paper and illustrate their use. We then introduce further notation and work to obtain the desired result for homotopy (Theorem 6.4).

### 5.3. Illustration

We illustrate the use of the notation:

If we let  $\phi(x_1) = h$  and  $\phi(K) = \phi(x_1)^r$ , then we have  $S_{K, X_j} = x_1^{r\phi(x_1)} \cdot x_j \cdot \overline{K} \cdot x_j^{-1}$ . Thus if

$$X_j = x_j \cdot \overline{x_j}^{-1}, \quad \text{then } S_{K, x_j} = h^r(X_j). \tag{4}$$

We begin to rewrite the generators and relations using this notation. First we find

$$\tau(\overbrace{x_1 x_1 \cdots x_1}^{p\text{-factors}}) = 1.$$

Since  $X_1 = S_{1, x_1}$  we have

$$\tau(x_1^p) = X_1 \cdot h(X_1) \cdot h^2(X_1) \cdots h^{p-2}(X_1) h^{p-1}(X_1) = 1. \tag{5}$$

Similarly, if  $\phi(x_j) = n_j$ , and we set  $X_j = S_{\overline{1}, x_j}$  and if  $\overline{K} = x_1^s$ , then we can write  $S_{K, x_j} = h^{s \cdot n_j}(X_j)$ .

This tells us that

$$\tau(x_j^{pn_j}) = X_j \cdot h^{n_j}(X_j) \cdot h^{2n_j}(X_j) \cdots h^{(p-2)n_j}(X_j) h^{(p-1)n_j}(X_j) = 1. \tag{6}$$

Note that in deriving all equations we are free to make use of the fact (see [11]) that  $S_{M, x_1} \approx 1 \forall$  Schreier representatives  $M$  where  $\approx$  denotes *freely equal to*. Note that this also eliminates the  $p$  generators,  $S_{x_1^j, x_1}, j = 1, \dots, p-1$ .

Now Eq. (6) is a relation in the fundamental group. We remind the reader that for a compact Riemann surface, homology is abelianized homotopy so that when abelianized, it reduces to

$$h^{p-1}(X_j) \approx^h -X_j - h(X_j) - \dots - h^{p-2}(X_j) \tag{7}$$

where  $\approx^h$  denotes *is homologous to*.

Remember that our goal is to explicitly find the action on the fundamental group given the conjugacy invariants in the mapping class group. To this end we establish more notation to describe  $\widehat{\widehat{R}}$  more simply and precisely.

**Part 4. Homotopy and the algorithm**

**6. Finding the generators for the fundamental group and the algorithm**

While it is easy to see the action of  $h$  on a homology basis, writing explicitly the action of  $h$  on generators for the fundamental groups requires further notation. Our goal is to find a *homotopy basis* adapted to the automorphism  $h$  and its symplectic action on a symplectic basis obtained from this one.

*6.1. The action on the fundamental group of  $S_0$*

First we note that when we rewrite  $x_r^p = 1$  as  $\tau(x_r^p) = 1$ , if  $\phi(x_r) = n_r$ , then if  $s_t \cdot n_t \equiv n_1 \pmod{p}$  with  $0 \leq s_t \leq (p - 1)$  and  $\phi(x_1) = n_1$ , then

$$\tau(x_r^p) = S_{\bar{1},x_r} \cdot S_{\bar{x}_r,x_r} \cdot S_{\bar{x}_r^2,x_r} \cdots S_{\bar{x}_r^{p-2},x_r} \cdot S_{\bar{x}_r^{p-1},x_r} = 1. \tag{8}$$

For each  $r$ , this equation yields the homology relation of Eq. (7) with  $j$  replacing  $r$ .

If  $\phi(x_j) \neq \phi(x_1)$  the relation (8) (or equivalently (6)) determined by  $x_j^p = 1$  is slightly different than that obtained by replacing  $j$  by 1. Up to homology both reduce to the same equation. However, the statement regarding homotopy is more delicate.

We note that if  $\phi(x_1) = n_1$  and  $\phi(x_r) = n_r$  and  $n_1 \cdot s_r \equiv n_r \pmod{p}$  and  $s_r \cdot q_r \equiv 1 \pmod{p}$  so that  $n_r \cdot q_r \equiv n_1 \pmod{p}$ , then  $\phi(x_r)^{s_r} = \phi(x_1)$  and  $\phi(x_r) = \phi(x_1^{q_r})$  and  $x_r^k = x_1^{k \cdot s_r}$ .

If conjugation by  $x_1$  induces the automorphism  $h$  and  $\phi(x_1) = n_1$  and  $\phi(x_j) = n_j$  we let  $n_1 \cdot s_j \equiv n_j \pmod{p}$  so that conjugation by  $x_j$  induces the same action on  $F$  as conjugation by  $x_1^{n_1 \cdot s_j}$ , and conjugation by  $x_j^k$  induces the same action as conjugation by  $x_1^{k \cdot n_1 \cdot s_j}$ . That is

$$S_{x_j^k,x_j} = S_{x_1^{k \cdot s_j},x_j} = h^{k \cdot s_j}(X_j). \tag{9}$$

*6.2. Calculating with simpler notation*

In this section we first assume that  $\phi(x_1) = 1$  so that  $h$  acts as conjugation by  $x_1$  and that  $\phi(x_1) \leq \phi(x_2) \leq \phi(x_j) \forall 3 \leq j \leq t$ . Then  $s_j$  satisfies  $s_j \cdot n_j \equiv 1 \pmod{p}$ .

To simplify the exposition from now on we assume that all exponents are reduced modulo  $p$  and are between 0 and  $p - 1$ . Instead of working with the  $X_j$  described above, we work with the  $Y_j$  defined below. This is done so that the final result is in an optimal form.

We let  $Y_j = S_{\overline{x_1 x_2 \cdots x_{j-1}, x_j}}$  so that

$$h^z(Y_j) = S_{\overline{x_1^z \cdot x_1 x_2 \cdots x_{j-1}, x_j}}, \quad \forall j = 1, \dots, t \text{ and } \forall z = 0, \dots, p - 1.$$

When  $K_r = \overline{x_1 x_2 \cdots x_{r-1}}$ , (8) gives

$$\tau(K_r x_r^p K_r) = S_{\overline{x_1 \cdots x_{r-1}, x_r}} \cdot S_{\overline{K_r \cdot x_r, x_r}} \cdot S_{\overline{K_r \cdot x_r^2, x_r}} \cdots S_{\overline{K_r \cdot x_r^{p-2}, x_r}} \cdot S_{\overline{K_r \cdot x_r^{p-1}, x_r}} = 1$$

or equivalently, where powers of  $h$  are assumed to be reduced modulo  $p$ ,

$$Y_r \cdot h^{s_r}(Y_r) \cdot h^{2s_r}(Y_r) \cdot h^{(p-2)s_r}(Y_r) \cdot h^{(p-1)s_r}(Y_r) = 1. \tag{10}$$

Note that the derivation of these equations uses the fact that the  $S_{K, x_1} \approx 1$  for all coset representatives  $K$ .

We will often drop the subscript  $r$  when it is understood and write (10) as

$$Y h^s(Y) h^{2s}(Y) \cdots h^{(p-2)s}(Y) h^{(p-1)s}(Y) = 1 \tag{11}$$

where the powers of  $h$  are again taken modulo  $p$ .

**Definition 6.1.** *Notation:* For any set of exponents  $u_1, \dots, u_v$  and any element  $U$  of the group  $F$ , we use the shorthand notation  $U^{u_1+u_2+\cdots+u_v}$  and define

$$U^{u_1+u_2+\cdots+u_v} = h^{u_1}(U) h^{u_2}(U) \cdots h^{u_v}(U).$$

Thus (10) becomes

$$Y^{1+s+2s+\cdots+(p-2)s+(p-1)s} = 1. \tag{12}$$

If we choose  $p_r$  so that  $1 \leq p_r \leq p - 1$  and  $p_r \cdot s_r \equiv p - 1 \pmod{p}$ , then we can solve (10) for  $h^{p-1}(Y_r)$  to obtain

$$h^{p-1}(Y_r) = (Y_r^{(p_r+1)s_r+(p_r+2)s_r+\cdots+(p-1)s_r} \cdot Y_r^{1+s_r+2s_r+\cdots+(p-1)s_r})^{-1}. \tag{13}$$

We now make some definitions. The motivation for these definitions will become clear shortly.

**Definition 6.2.** We define  $\mathcal{LR}_0$  by

$$\mathcal{LR}_0 = \left( \prod_{r=2}^t Y_r^{p-1} \right) \left( \prod_{i=1}^{g_0} [h^{p-1}(A_i), h^{p-1}(B_i)] \right).$$

Substituting (13) into this definition, we define

**Definition 6.3.** We define  $\mathcal{LR}$  by

$$\mathcal{LR} = \left( \prod_{r=2}^t (Y_r^{(p_r+1)s_r + (p_r+2)s_r + \dots + (p-1)s_r} \cdot Y_r^{1+s_r+2s_r+\dots+(p_r-1)s_r})^{-1} \right) \cdot \left( \prod_{i=1}^{g_0} [h^{p-1}(A_i), h^{p-1}(B_i)] \right).$$

6.3. Eliminating generators and relations

Recall that  $h^r(Y_1) = S_{x_1, x_1} \approx 1$  for all integers  $r$ . If  $R$  is the relation in the group

$$x_1 \cdots x_t \prod_{i=1}^{g_0} [A_i, B_i] = 1,$$

then with this notation we have:

$$\tau(R) = Y_2 Y_3 \cdots Y_t \prod_{i=1}^g [A_i, B_i] = 1 \quad \text{so that } Y_2^{-1} = Y_3 \cdots Y_t \prod_{i=1}^g [A_i, B_i].$$

Let  $\mathcal{Y} = (Y_3 \cdots Y_t \prod_{i=1}^g [A_i, B_i])^{-1}$ . We have  $\forall v = 1, \dots, p-1$

$$\tau(x_1^v R x_1^{-v}) = h^v(Y_2) h^v(Y_3) \cdots h^v(Y_t) \prod_{i=1}^g [h^v(A_i), h^v(B_i)] = 1. \tag{14}$$

Since  $h$  is a group isomorphism,  $h(TS) = h(S)h(T)$  so that

$$h^v(\mathcal{Y}) = \left( h^v(Y_3) \cdots h^v(Y_t) \prod_{i=1}^g [h^v(A_i), h^v(B_i)] \right)^{-1}. \tag{15}$$

Now  $h^v(Y_2) = h^v(\mathcal{Y})$  so we can eliminate the generator  $Y_2$  and all of its images  $h^v(Y_2)$  and replace these by the expressions on the right-hand side of Eq. (15). Next we replace the relation obtained from Eq. (10) when  $r = 2$  with a relation in the  $h^v(\mathcal{Y})$

$$\mathcal{Y}^{1+s_2+2s_2+\dots+(p-1)s_2} = 1. \tag{16}$$

Recalling that  $p_2$  satisfies  $p_2 \times s_2 \equiv p-1 \pmod{p}$ , we have

$$\mathcal{Y}^{1+s_2+2s_2+\dots+(p_2-1)s_2} \cdot \mathcal{Y}^{(p-1)} \cdot \mathcal{Y}^{(p_2+1)s_2+(p_2+2)s_2+\dots+(p-1)s_2} = 1. \tag{17}$$

We observe that for each  $j \neq 1, 2$ , every  $h^{p-1}(Y_j)$  occurs in  $h^{p-1}(\mathcal{Y})$ . Therefore, we eliminate these  $h^{p-1}(Y_j)$  using (13).

Finally we recall the definition of  $\mathcal{LR}$ , note that it is the same as  $\mathcal{Y}^{p-1}$  and substitute it into (17) to obtain

$$\mathcal{Y}^{1+s_2+2s_2+\dots+(p_r-2)s_2} \cdot \mathcal{LR} \cdot \mathcal{Y}^{(p_r+1)s_2+\dots+(p-1)s_2} = 1. \tag{18}$$

This is now the single defining relation. We have proved

**Theorem 6.4** (Adapted homotopy basis). *If the conjugacy class of  $h$  in the mapping-class group is determined by the  $t$ -tuple  $(n_1, \dots, n_t)$   $t \geq 2$ ,  $n_i \neq 0$ ,  $n_1 = 1 \leq n_2 \leq n_i$ ,  $i \geq 3$ , then  $F$  has an adapted homotopy basis. That is,  $F$  has a presentation with*

generators:

$$\begin{aligned} h^v(Y_w), \quad w = 2, \dots, t-2, \quad v = 0, \dots, p-2, \\ h^v(A_i), \quad i = 1, \dots, g_0, \quad v = 0, \dots, p-1, \\ h^v(B_i), \quad i = 1, \dots, g_0, \quad v = 0, \dots, p-1 \end{aligned} \tag{19}$$

and the single defining relation:

$$\mathcal{Y}^{1+s_2+2s_2+\dots+(p_2-2)s_2} \cdot \mathcal{LR} \cdot \mathcal{Y}^{(p_2+1)s_2+\dots+(p-1)s_2} = 1, \tag{20}$$

where  $\mathcal{Y}$  is the word in the generators:

$$\left( Y_3 \cdots Y_t \cdot \prod_{i=1}^{g_0} [A_i, B_i] \right)^{-1},$$

$\mathcal{LR}$  is the word in the generators:

$$\left( \prod_{r=2}^t (Y_r^{(p_r+1)s_r+(p_r+2)s_r+\dots+(p-2)s_r} Y_r^{1+s_r+2s_r+\dots+(p-1)s_r})^{-1} \right) \cdot \prod_{i=1}^{g_0} [h^{p-1}(A_i), h^{p-1}(B_i)], \tag{21}$$

$s_r$  satisfies  $s_r \cdot n_r \equiv 1 \pmod{p}$  and  $p_r$  satisfies  $p_r \cdot s_r \equiv p-1 \pmod{p}$ .

**Corollary 6.5.** *The fundamental group of  $F$  has a surface symbol  $\mathcal{LR}$  given by Eq. (20) whose unordered edges are the generators given in Eq. (19).*

We let  $\widehat{\mathcal{LR}}$  (respectively  $\widehat{\mathcal{Y}}$ ) be the symbol  $\mathcal{LR}$  (respectively  $\mathcal{Y}$ ) from which all of the occurrences of  $h^v(A_i)$  and  $h^v(B_i)$ ,  $i = 1, \dots, g_0$ ,  $v = 0, \dots, (p-2)$ , have been deleted. We set  $P = \prod_{i=1}^{g_0} [A_i, B_i]$  so that  $h^v(P) = \prod_{i=1}^{g_0} [h^v(A_i), h^v(B_i)]$ . Conjugating  $h^v(A_i)$  and  $h^v(B_i)$  by the same word replaces  $h^v(P)$  by an appropriate conjugate. If we denote the appropriate conjugate by  $[h^v(P)]_v$  and set  $\widehat{Q} = P_0 \cdot [h(P)]_1 \cdots [h^{p-1}(P)]_{p-1}$  we can rewrite

$$\mathcal{Y}^{1+s_2+2s_2+\dots+(p_2-2)s_2} \cdot \mathcal{LR} \cdot \mathcal{Y}^{(p_2+1)s_2+\dots+(p-1)s_2} = 1 \tag{22}$$

as

$$\widehat{Q} \cdot \widehat{Y}^{1+s_2+2s_2+\dots+(p_2-2)s_2} \cdot \widehat{\mathcal{LR}} \cdot \widehat{Y}^{(p_2+1)s_2+\dots+(p-1)s_2} = 1. \tag{23}$$

Setting  $\widehat{\mathcal{LR}} = \widehat{Y}^{1+s_2+2s_2+\dots+(p_2-2)s_2} \cdot \widehat{\mathcal{LR}} \cdot \widehat{Y}^{(p_2+1)s_2+\dots+(p-1)s_2}$  gives the surface symbol  $\widehat{Q} \cdot \widehat{\mathcal{LR}}$ .

With respect to this basis  $h$  now has the matrix of the form

$$M_{\widehat{\mathcal{A}}} \approx \begin{pmatrix} M_{A_{g_0, p \times p}} & 0 & 0 \\ 0 & M_{A_{g_0, p \times p}} & 0 \\ 0 & 0 & N_{\widehat{\mathcal{LR}}} \end{pmatrix}$$

where  $N_{\widehat{\mathcal{LR}}}$  is the matrix of  $h$  with respect to the ordered basis consisting of the edges of  $\widehat{\mathcal{LR}}$ .

**Corollary 6.6.** *The fundamental group has the evenly worded and fully and optimally linked surface symbol  $\widehat{Q} \cdot \widehat{\mathcal{LR}}$  and matrix  $M_{\widehat{\mathcal{A}}}$ .*

### 7. Applying the algorithm

We now combine Theorem 6.4 and Corollary 6.6 with the tight linking algorithm of Section 4.1. Initialize so that  $Q = \widehat{Q}$ ,  $M = M_{\widehat{\mathcal{A}}}$  and  $\mathcal{P} = \widehat{\mathcal{LR}}$  and conclude

**Theorem 7.1.** *Let  $h$  be an element of the mapping-class group of prime order  $p$  and assume that its conjugacy class in the mapping-class group is determined by the  $t$ -tuple  $(n_1, \dots, n_t)$ ,  $t \geq 2$ ,  $n_i \neq 0$ ,  $n_1 = 1 \leq n_2 \leq n_i$ ,  $i \geq 3$ , so that  $F$  has the adapted homotopy basis described above. Then there is an algorithm that inputs  $(n_1, \dots, n_t)$  and outputs a unique symplectic matrix in the conjugacy class of the image of  $h$  in  $Sp(2g, \mathbb{Z})$ .*

**Theorem 7.2.** *Let  $h$  be an element of the mapping-class group of prime order  $p$  and assume that its conjugacy class in the mapping-class group is determined by the  $t$ -tuple  $(n_1, \dots, n_t)$ ,  $t \geq 2$ ,  $n_i \neq 0$ ,  $n_1 \leq n_2 \leq n_i$ ,  $i \geq 3$ . Then there is an algorithm that inputs  $(n_1, \dots, n_t)$  and outputs a unique symplectic matrix in the conjugacy class of the image of  $h$  in  $Sp(2g, \mathbb{Z})$ .*

**Proof.** If  $n_1 = 1$ , this is the previous theorem. If  $n_1 \neq 1$ , let  $s_1$  be the integer with  $n_1 \times s_1 \equiv 1 \pmod{p}$ . Consider the  $t$ -tuple whose  $i$ th entry is  $n_i \times s_1$  (reduced modulo  $p$ , of course). Apply Theorem 7.1 to obtain a symplectic matrix and then output this matrix raised to the power  $n_1$ .  $\square$

We have also shown

**Theorem 7.3.** *Consider an element  $M$  of order  $p$  in  $Sp(2g, \mathbb{Z})$ . For each integer  $t \in \{1, 2, \dots, 2m + 2\}$  if there exists a set of  $t$  integers  $\{n_1, \dots, n_t\}$  with  $1 \leq n_i \leq (p - 1)$  with  $\sum_{i=1}^t n_j \equiv 0 \pmod{p}$  or equivalently a  $p - 1$ -tuple of real numbers  $(m_1, \dots, m_{p-1})$  with  $\sum_{i=1}^{p-1} im_i \equiv 0 \pmod{p}$ , then there is an element in the symplectic group of order  $p$ . The integers  $m_i$  determine its conjugacy class in the symplectic group and the conjugacy class has a unique matrix representative given by the algorithm. We call this matrix the normal form for  $M$ .*

**Remark 7.4.** Note that there can be no  $M$  of prime order for which  $t = 1$ . The canonical form for  $t = 0$  appears in Section 8.

Formulas for determining the number (possibly 0) of distinct  $t$ -tuples of integers that exist for any given  $t$ ,  $p$  and  $g$  that satisfy the hypotheses of the theorem are to be found in [3].

### 7.1. Complexity

We note that replacing the complementary rotation numbers by the rotation numbers requires an application of the Euclidean algorithm  $O(n^2)$ . The calculation of the matrix  $M_{\tilde{A}}$  is  $O(g^2)$  because the words we are looking at are of length at most  $4g$ . Computing the  $p$ th power of a  $4g \times 4g$  matrix is  $O(pg^3)$  but  $p \leq g$  so it is  $O(p^4)$ . The complexity of the tight linking algorithm is  $O(g^3)$ . Thus the complexity of the algorithm in Theorem 7.3 is  $O(g^4)$ .

If  $M$  is an  $n \times n$  matrix, we define the norm of  $M$  to be the maximum of the absolute value of its entries and write  $|M|$ . Multiplying matrices increases their norm and thus will affect the running time. If we let  $A_1, \dots, A_m$  be  $m, n \times n$  matrices, then  $|A_1 \cdots A_m| = O(n^3 \cdot m \cdot \sum_{i=1}^m (1 + \log |A_i|))$ .

We note in all applications that the initial matrix  $M$  has entries that are only 0, 1 and  $-1$  and thus its norm is 1. The matrix of the change of basis at each iteration will also only have entries that are 0, 1 and  $-1$ , so that the norm of it and its inverse is also 1. We can think of the final matrix as being obtained from the initial matrix by conjugating it by at most  $2g$  matrices so that  $m = 4g + 1$ . Thus the norm of the final matrix in the tight linking algorithm is  $O(g^5)$ . We may need to take up to  $p$  powers of this matrix, yielding a matrix of norm  $O(g^{10})$ .

### 7.2. Other matrices

Let  $M$  be a symplectic matrix of prime order  $p \geq 2$  with trace  $T$ . It follows from the results of [6], that the map  $\pi : MCG(S) \rightarrow Sp(2g, \mathbb{Z})$  is injective on elements of finite order. Either every preimage of  $M$  is an infinite order element of the mapping-class group or there is a finite order preimage. In the latter case, we have  $0 \leq t \leq 2g + 2$  and the trace of  $M_{\tilde{A}} = 2 - t$  so since trace is a conjugacy invariant  $T = 2 - t$ . Thus  $M$  must be the image of an element of only infinite order mapping-classes if  $T < -2g$  or  $T \geq 2$ . There are prime order elements of the symplectic group that are not the images of finite order elements of the mapping-class group. If  $-2g \leq T \leq 2$ , then a necessary condition for  $M$  to have a preimage of finite order is that there are integers  $(n_1, \dots, n_t)$  such that  $\sum n_i \equiv 0 \pmod{p}$ . Whether or not there is such a  $t$ -tuple is determined in [3] where the number of such  $t$ -tuples is computed for each  $t$  with  $0 \leq t \leq 2g + 2$ . The algorithm gives a sufficient condition, namely that  $M$  be conjugate to the unique normal form matrix.

## 8. Homotopy when $t = 0$

If the number of fixed points is zero, we can still find an adapted basis. The calculations are slightly different. We have  $2g = 2p(g_0 - 1) + 2$  and the presentation for the group  $F_0$  is simply

$$\left\langle a_1, \dots, a_{g_0}, b_1, \dots, b_{g_0} \mid \left( \prod_{i=1}^{g_0} [a_i, b_i] \right) = 1 \right\rangle. \tag{24}$$

Replacing  $h$  by a conjugate if necessary, the map  $\phi: F_0 \rightarrow \mathbb{Z}_p$  can be taken to be

$$\phi(a_i) = \phi(b_i) = 0 \quad \forall i = 2, \dots, g_0 \quad \text{and} \quad \phi(a_1) = 1 \quad \text{and} \quad \phi(b_1) = 0.$$

Using the rewriting with coset representatives  $1, a_1, \dots, a_1^{p-1}$ , note that  $S_{a_1^k, a_1} \approx 1$  for  $k = 0, \dots, p-2$ . Let  $A = S_{a_1^{p-1}, a_1}$ . Then  $h$  acts on  $\text{Ker } \phi$  via conjugation by  $a_1$ .

We let  $\{h^k(A_j), h^k(B_j), j = 2, \dots, g_0, k = 0, \dots, p-1\}$  be as in (4) with  $a_1$  playing the role and let  $B = S_{1, b_1}$ . We let  $P = \prod_{i=2}^{g_0} [A_i, B_i]$ .

Then we can compute that

$$\begin{aligned} \tau(R) = 1 &\Rightarrow h(B)B^{-1}P = 1, \\ \tau(a_1^k R a_1^{-k}) = 1 &\Rightarrow h^k(B)(h^{k-1}(B))^{-1}h^k(P) = 1 \quad \forall k = 1, \dots, p-2, \quad \text{and} \\ \tau(a_1^{p-1} R a_1^{-(p-1)}) = 1 &\Rightarrow ABA^{-1}(h^{p-1}(B))^{-1}h^{p-1}(P) = 1. \end{aligned} \tag{25}$$

We eliminate generators using (25) and let  $\alpha = A$  and  $\beta = h^{p-1}(B)$  to obtain generators

$$\{\alpha, \beta\} \cup \{h^k(A_j), h^k(B_j), j = 2, \dots, g_0, k = 0, \dots, p-1\}$$

and the single defining relation

$$\beta\alpha\beta^{-1} = h^{p-1}(P)\alpha \prod_{i=k}^{p-2} h^k(P).$$

Further we calculate that  $h(\alpha) = \alpha$  and  $h(\beta) = \beta$ . Note that  $P$  is a product of commutators. Thus the matrix representation for  $h$  on  $S = U/F$  where  $F = \text{Ker } \phi$  is given by  $2(g_0 - 1)$  permutation matrices  $M_{p \times p}$  and one two by two identity matrix. The basis is a canonical homology basis. We have  $\alpha \times \beta = 1$  and we note that the curves  $\alpha$  and  $\beta$  are by default of type (1) in Definition 3.1.

We have proved the following:

**Theorem 8.1.** Assume  $t = 0$  and let  $F$  be the fundamental group of the surface  $S$ .

(1) Then  $F$

(a) has generators:

- (i)  $h^j(A_w), h^j(B_w)$  where  $2 \leq w \leq g_0, 0 \leq j \leq p-1$ ,
- (ii)  $\alpha, \beta$  where  $h^k(\alpha) = \alpha, h^k(\beta) = \beta, 0 \leq k \leq p$ ;

(b) and the single defining relation:

$$[\beta^{-1}, \alpha^{-1}] \cdot h^{p-1}(P^\alpha) \cdot \prod_{k=2}^{p-2} h^k(P)$$

where  $P^\alpha$  denotes the words  $P$  conjugated by  $\alpha$  and  $P = \prod_{i=2}^{g_0} [A_i, B_i]$ .

(2) The corresponding intersection numbers are

- (a)  $h^j(A_w) \times h^j(B_w) = 1$ ;
- (b)  $\alpha \times \beta = 1$ ;



Using  $S_{x_1, x_1}^{-1} \approx 1$ ,  $r = 1, 2, 3$ , and solving for  $(Y_2)^{-1}$  in (28), we have

$$(S_{x_1, x_2})^{-1} = Y_2^{-1} = Y_3 \cdot Y_4 \cdot Y_5 \cdot \left( \prod_{i=1}^{g_0} [A_i, B_i] \right) = 1 \tag{29}$$

and

$$(h(Y_2))^{-1} = h(Y_3) \cdot h(Y_4) \cdot h(Y_5) \cdot \left( \prod_{i=1}^{g_0} [h(A_i), h(B_i)] \right) = 1, \tag{30}$$

$$(h^2(Y_2))^{-1} = h^2(Y_3) \cdot h^2(Y_4) \cdot h^2(Y_5) \cdot \left( \prod_{i=1}^{g_0} [h^2(A_i), h^2(B_i)] \right) = 1. \tag{31}$$

Using  $h^2(Y_2)Y_2h(Y_2) = 1$  and letting  $P = (\prod_{i=1}^{g_0} [A_i, B_i])$ , we have

$$h(Y_3) \cdot h(Y_4) \cdot h(Y_5) \cdot h(P) \cdot Y_3 \cdot Y_4 \cdot Y_5 \cdot P \cdot h^2(Y_3) \cdot h^2(Y_4) \cdot h^2(Y_5) \cdot h^2(P) = 1. \tag{32}$$

We use Eq. (27) to replace the  $h^2(Y_j)$  and obtain the relation

$$h(Y_3) \cdot h(Y_4) \cdot h(Y_5) \cdot h(P) \cdot Y_3 \cdot Y_4 \cdot Y_5 \cdot P \cdot (h(Y_3))^{-1} \cdot (Y_3)^{-1} \cdot (h(Y_4))^{-1} \cdot (Y_4)^{-1} \cdot (Y_5)^{-1} \cdot (h(Y_5))^{-1} \cdot h^2(P) = 1. \tag{33}$$

Equation (33) is the relation  $\widehat{R} = 1$ .

Let  $C_1 = h(Y_3) \cdot h(Y_4) \cdot h(Y_5)$ ,  $C_2 = Y_3 \cdot Y_4 \cdot Y_5$  and  $C_3 = (h(Y_3))^{-1} \cdot (Y_3)^{-1} (h(Y_4))^{-1} \cdot (Y_4)^{-1} \cdot (Y_5)^{-1} \cdot (h(Y_5))^{-1}$ .

Let  $\widetilde{P} = h(P)^{(C_2 C_3)^{-1}} \cdot P^{C_3^{-1}} \cdot h^2(P)$  where if  $X$  and  $Y$  are words  $X^Y$  means the conjugate of  $X$  by  $Y$ .

We can replace the relation (33) by

$$\widetilde{P} h(Y_3) \cdot h(Y_4) \cdot h(Y_5) \cdot Y_3 \cdot Y_4 \cdot Y_5 \cdot P \cdot (h(Y_3))^{-1} \cdot (Y_3)^{-1} \cdot (h(Y_4))^{-1} \cdot (Y_4)^{-1} \cdot (Y_5)^{-1} \cdot (h(Y_5))^{-1} = 1.$$

We use the notation of Section 3.3 in particular the definition of the matrix  $B$  given at the end of that section. We can compute from the formulas for intersection numbers in Theorem 3.5 that the relevant part of the intersection matrix,  $B$ , is the  $6 \times 6$  submatrix that gives the intersection matrix for the curves in the basis given in the order

$$X_{1,3}, h(X_{1,3}), X_{1,4}, h(X_{1,4}), X_{2,1}, h(X_{2,1})$$

1 is

$$B = I_{\widehat{R}} = \begin{pmatrix} 0 & 1 & 1 & 0 & 1 & -1 \\ -1 & 0 & -1 & 1 & 0 & 1 \\ -1 & 1 & 0 & 1 & 1 & -1 \\ 0 & -1 & -1 & 0 & 0 & 1 \\ -1 & 0 & -1 & 0 & 0 & 0 \\ 1 & -1 & 1 & -1 & 0 & 0 \end{pmatrix}.$$

That is, the matrix  $J_{\widehat{A}}$  breaks up into blocks

$$\begin{pmatrix} 0 & I_{pg_0} & 0 \\ -I_{pg_0} & 0 & 0 \\ 0 & 0 & I_{\widehat{R}} \end{pmatrix}.$$

We now rearrange the relation. To simplify the notation we let  $a = Y_3, b = Y_4$  and  $c = Y_5$ . So that the relation becomes

$$h(a) \cdot h(b) \cdot h(c) \cdot h(P) \cdot a \cdot b \cdot c \cdot P \cdot (h(a))^{-1} a^{-1} (h(b))^{-1} \cdot b^{-1} \cdot c^{-1} \cdot (h(c))^{-1} \cdot h^2(P) = 1.$$

We can also make the simplifying assumption, replacing the elements that occur in  $P, h(P)$  and  $h^2(P)$  by conjugates, that we are merely working with the symbol

$$h(a) \cdot h(b) \cdot h(c) \cdot a \cdot b \cdot c \cdot (h(a))^{-1} a^{-1} (h(b))^{-1} \cdot b^{-1} \cdot c^{-1} \cdot (h(c))^{-1} = 1. \quad (34)$$

We replace generators and relations using the algorithm as follows:

Let  $M = h(a) \cdot W_1 \cdot h(b) W_2 \cdot (h(a))^{-1}$  where  $W_1 = \lambda, W_2 = h(c) \cdot a \cdot b \cdot c$ . Set  $W_3 = a^{-1}$  and  $W_4 = b^{-1} \cdot c^{-1} \cdot (h(c))^{-1}$ .

Let  $N = W_3 W_2 (h(a))^{-1}$ . Then

$$h(a) \cdot h(b) \cdot h(c) \cdot a \cdot b \cdot c \cdot (h(a))^{-1} a^{-1} (h(b))^{-1} \cdot b^{-1} \cdot c^{-1} \cdot (h(c))^{-1} = [M, N] W_3 W_2 W_1 W_4 = [M, N] \cdot a^{-1} \cdot h(c) a b c b^{-1} \cdot c^{-1} \cdot (h(c))^{-1} = 1. \quad (35)$$

At this point one can proceed by inspection and let  $[b, c]^*$  denote the conjugate of  $[b, c]$  by  $a^{-1} \cdot h(c) \cdot a$  to obtain

$$[M, N] \cdot [b, c]^* \cdot [a^{-1}, h(c)] = 1.$$

However, to follow the algorithm carefully, we would set  $\widetilde{M} = a^{-1} \cdot h(c) \cdot a$  and  $\widetilde{N} = b \cdot c \cdot a^{-1} \cdot c^{-1} \cdot a$ .

Then Eq. (35) becomes

$$[M, N] \cdot [\widetilde{M}, \widetilde{N}] \cdot [b, c] = 1.$$

Thus the canonical homology basis is given by

$$\{h^j(A_i), h^j(B_i)\}, \quad i = 1, \dots, g_0, \quad j = 0, \dots, p-1 \cup \{M, N, \tilde{M}, \tilde{N}, b, c\}.$$

The reordered basis  $\{M, \tilde{M}, b, N, \tilde{N}, c\}$  has intersection matrix

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

We can compute the action of  $h$  on these last six elements of the homology basis. First we note that  $h(b) \approx^h M - c - b - a - h(c)$  and  $h(a) \approx^h -N + h(c) + b + c$ . Therefore,

$$\begin{aligned} c &\mapsto h(c) \approx^h \tilde{M}, \\ h(c) &\mapsto -c - h(c) \approx^h -c - \tilde{M}, \\ a &\mapsto h(a) \approx^h -N + h(c) + b + c \approx^h -N + \tilde{M} + b + c, \\ b &\mapsto h(b) \approx^h M - c - b - a - h(c) \approx^h M - c - b - \tilde{N} - \tilde{M}, \\ M &\mapsto h(M) \approx^h -\tilde{M} - N, \quad \text{and} \\ N &\mapsto h(N) \approx^h -c + M - N. \end{aligned}$$

Thus the matrix of the action of  $h$  with respect to the ordered basis  $M, \tilde{M}, b, N, \tilde{N}, c$  is the submatrix we have been seeking. Namely,

$$N_{\text{symp}} \tilde{A} = \begin{pmatrix} 0 & 1 & 0 & -1 & 0 & 0 \\ 0 & -1 & 0 & 1 & 0 & -1 \\ 1 & -1 & -1 & -0 & -1 & -1 \\ 1 & 0 & 0 & -1 & 0 & -1 \\ 0 & 1 & 1 & -1 & 0 & -1 \\ 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

One can verify that this  $6 \times 6$  matrix really is a submatrix of a symplectic matrix, as it should be.

**Uncited references**

[2] [9] [12]

**Acknowledgments**

The author thanks Yair Minsky and the Yale Mathematics Department for their hospitality and support while some of this work was carried out. The author also thanks Moira Chas for stimulating conversations and Rubi Rodriguez for some helpful comments.

## References

- [1] Lipman Bers, Introduction of Riemann Surfaces, NYU Lecture Notes, 1957, unpublished.
- [2] J. Gilman, Compact Riemann surfaces with conformal involutions, Proc. Amer. Math. Soc. 37 (1973) 105–107.
- [3] J. Gilman, On conjugacy classes in the Teichmüller modular group, Michigan Math. J. 23 (1976) 53–63.
- [4] J. Gilman, A matrix representation for automorphisms of Riemann surfaces, Linear Algebra Appl. 17 (1977) 139–147.
- [5] J. Gilman, D. Patterson, Intersection matrices for adapted bases, in: Proc. 1978 Stony Brook Conference, in: Ann. of Math. Stud., vol. 97, 1981, pp. 149–166.
- [6] J. Gilman, Prime order automorphisms of Riemann surfaces, in: Proceedings of the Workshop on Teichmüller Theory and Moduli, HRI, Allahabad, India, in press.
- [7] J. Gilman, R. Gilman, On the existence of cyclic surface kernels for pairs of Fuchsian groups, J. London Math. Soc. 30 (1984) 451–464.
- [8] W.J. Harvey, On branch loci in Teichmüller space, Trans. Amer. Math. Soc. 153 (1971) 387–399.
- [9] A.M. MacBeath, Action of automorphisms of a compact Riemann surface on the first homology group, Bull. London Math. Soc. 5 (1973) 103–108.
- [10] A.M. MacBeath, Discontinuous groups, in: Proceedings of the Dundee Summer School, 1961, Lecture notes.
- [11] O. Karrass Magnus, O. Solitar, Combinatorial Group Theory, J. Wiley, 1966, pp. 253–274.
- [12] J. Nielsen, Die Structur periodischer Transformationen von Flächen, D.K. Dan. Vidensk. Selsk. Math.-Fys. Medd. XV (1937) 1–77.
- [13] O. George Springer, Introduction to Riemann Surfaces, Addison–Wesley, 1957.