### Charalampos Stylianakis

#### Abstract

In this paper we give a description of the generators of the prime level congruence subgroups of braid groups. Also, we give a new presentation of the symplectic group over a finite field, and we calculate symmetric quotients of the prime level congruence subgroups of braid groups. Finally, we find a finite generating set for the level-3 congruence subgroup of the braid group on 3 strands.

### 1 Introduction

Let  $B_n$  be the braid group on n strands. By evaluating the (unreduced) Burau representation  $B_n \to \operatorname{GL}_{n-1}(\mathbb{Z}[t^{\pm 1}])$  at t = -1 we obtain a symplectic representation

$$\rho: B_n \to \begin{cases} \operatorname{Sp}_{n-1}(\mathbb{Z}) & \text{ if } n \text{ is odd,} \\ (\operatorname{Sp}_n(\mathbb{Z}))_u & \text{ if } n \text{ is even,} \end{cases}$$

where  $(\operatorname{Sp}_n(\mathbb{Z}))_u$  is the subgroup of  $\operatorname{Sp}_n(\mathbb{Z})$  fixing one vector  $u \in \mathbb{Z}^n$  [17, Proposition 2.1] (see also [9] and [1]).

For a positive integer m, the projection  $\mathbb{Z} \to \mathbb{Z}/m$  induces a representation as follows:

$$\rho_m: B_n \to \begin{cases} \operatorname{Sp}_{n-1}(\mathbb{Z}/m) & \text{ if } n \text{ is odd,} \\ (\operatorname{Sp}_n(\mathbb{Z}/m))_u & \text{ if } n \text{ is even.} \end{cases}$$

Note that if m = 1, then  $\rho_1 = \rho$ . For i > 1 the kernel of  $\rho_m$  is denoted by  $B_n[m]$  and it is called the *level-m congruence subgroup of*  $B_n$ . The kernel of  $\rho$  is called the *braid Torelli* group, and it is denoted by  $\mathcal{BI}_n$ . The group  $\mathcal{BI}_n$  has been extensively studied by Hain [18], Brendle-Margalit [10, 12], and Brendle-Margalit-Putman [11].

For p prime, A'Campo proved that the homomorphism  $\rho_p$  is surjective, by explicitly calculating the image of  $\rho_p$  [1, Theorem 1 (1)]. Wanjryb gave a presentation of  $\operatorname{Sp}_{n-1}(\mathbb{Z}/p)$  and  $(\operatorname{Sp}_n(\mathbb{Z}/p))_u$ as quotients of  $B_n$  [27, Theorem 1]. Let  $PB_n$  be the *pure braid group*, that is, the kernel of the epimorphism  $B_n \to S_n$ , where  $S_n$  is the symmetric group on n letters. Our first result is an analogue of Wanjryb's theorem.

**Theorem A** For p prime, the groups  $\operatorname{Sp}_{n-1}(\mathbb{Z}/p)$  and  $(\operatorname{Sp}_n(\mathbb{Z}/p))_u$  admit a presentation as quotients of the pure braid group  $PB_n$ .

This result is given as Theorem 5.3 in the paper.

A result of Arnol'd shows that  $B_n[2] = PB_n$ , where  $PB_n$  is the pure braid group [2]. Therefore, for every k even, we have that  $B_n[k] \leq PB_n$ . Our second result extends A'Campo's theorem.

**Theorem B** For  $m = 2p_1...p_k$ , where  $p_i \ge 3$  are primes, we have that  $PB_n/B_n[m]$  is isomorphic to  $\bigoplus_{i=1}^k \operatorname{Sp}_{n-1}(\mathbb{Z}/p_i)$  if n is odd, and  $\bigoplus_{i=1}^k (\operatorname{Sp}_n(\mathbb{Z}/p_i))_u$  if n is even.

Theorem B is Theorem 5.1 (see also Theorem 5.2) in the paper.

We also characterize quotient groups of congruence subgroups of braid groups. The braid group  $B_n$  surjects onto the symmetric group  $S_n$ . The kernel of this map is well known to be the pure braid group  $PB_n$ . Also, by a result established by A'rnold [2] the group  $PB_n$  is isomorphic to  $B_n[2]$ . See also [9, Section 2] for further discussion. Therefore, we have  $B_n/B_n[2] \cong S_n$ . We generalize this result as stated in the following theorem.

**Theorem C.** For p prime number, the group  $B_n[p]/B_n[2p]$  is isomorphic to  $S_n$ .

Theorem C is Theorem 6.1 in the paper.

**Topological description of congruence subgroups.** A key part of the paper is a topological interpretation of  $B_n[p]$ , for  $p \ge 3$  prime, given in Section 4. The content of Section 4 was inspired by Powell, who based on Birman's work on the presentation of the symplectic group [8, Theorem 1], to show that the Torelli subgroup of the mapping class group is normally generated by bounding pair maps, and Dehn twists about separating simple closed curves [25, Theorem 2].

Theorems A and B are used to find normal generators for  $B_n[m]$ , where  $m = 2p_1...p_k$  and  $p_i$  is an odd prime. Motivated by Section 4 it would be interesting to find a topological description of the generators of  $B_n[m]$  in the future.

**Related results.** The mapping class group  $\operatorname{Mod}(\Sigma)$  of an orientable surface  $\Sigma$  is the group of isotopy classes of homeomorphisms that preserve the orientation of  $\Sigma$ , fix the boundary pointwise, and preserve the set of marked points setwise. We denote by  $T_c$  a Dehn twist about a simple closed curve c. Let  $\Sigma_g^b$  be a surface of genus  $g \ge 1$  with b boundary components, where  $b \in \{1, 2\}$ . It is a special case of theorem of Birman-Hilden [7] that  $B_{2g+b}$  embeds into  $\operatorname{Mod}(\Sigma_g^b)$  [15, Section 9.4]. We denote the image of this embedding by  $\operatorname{SMod}(\Sigma_g^b)$ . As mentioned in the previous page, the braid Torelli  $\mathcal{BI}_{2g+b}$  is the kernel of the symplectic representation of  $B_{2g+b}$ . Hain conjectured that  $\mathcal{BI}_{2g+b}$  is isomorphic to the group generated by Dehn twists about separating simple closed curves inside  $\operatorname{SMod}(\Sigma_g^b)$  [18]. This conjecture was proved by Brendle-Margalit-Putman [11, Theorem A], and also studied by Brendle-Margalit [10, 12]. By the definitions given in the beginning of the paper, the group  $\mathcal{BI}_{2g+b}$  is a subgroup of  $B_{2g+b}[m]$ , for any  $m \in \mathbb{N}$ .

For  $m \geq 2$ , consider  $B_{2g+b}[m]$  as a subgroup of  $\mathrm{SMod}(\Sigma_g^b) \cong B_{2g+b}$ . A consequence of a work of Arnol'd shows that  $B_{2g+b}[2]$  is isomorphic to the pure braid group  $PB_{2g+b}[2]$  (see [9, Section 2] for explanation of this isomorphism). Combining the latter result with the work of Humphries [19, Theorem 1] we obtain that  $B_{2g+b}[2]$  is isomorphic to the normal closure of a square of a Dehn twist about nonseparating simple closed curve in  $\mathrm{SMod}(\Sigma_g^b)$ . Brendle-Margalit extended the latter result by proving that the normal closure of the 4<sup>th</sup> power of a Dehn twist about a nonseparating simple closed curve in  $\mathrm{SMod}(\Sigma_g^b)$  is isomorphic to  $B_{2g+b}[4]$  [9, Main Theorem].

Let  $\mathcal{T}_{2g+b}(m)$  be the normal closure of the  $m^{th}$  power of a Dehn twist in  $\mathrm{SMod}(\Sigma_g^b)$ , where  $g \geq 1$  and b = 1, 2. Coxeter proved that  $\mathcal{T}_{2g+b}(m)$  is a finite index subgroup of  $\mathrm{SMod}(\Sigma_g^b) = B_{2g+b}$  if and only if (2g+b-2)(m-2) < 4 [14, Section 10]. As mentioned above,  $\mathcal{T}_{2g+b}(2) = B_{2g+b}[2]$ . Furthermore, Humphries gave a complete description of when a group generated by  $\{\mathcal{T}_{2g+b}(m_i) \mid m_i \in \mathbb{N}\}$ , for finite number of  $m_i$ , is of finite index in  $PB_{2g+b}$  [20, Theorem 1]. In addition, Funar-Kohno proved that the intersection of all  $\mathcal{T}_{2g+b}(2m)$ , where  $m \in \mathbb{N}$ , is trivial [16, Theorem 1.1].

Finally, we note a more general definition of congruence subgroups of braid groups. Let  $F_n$  be the free group of rank n. There is an inclusion  $B_n \to \operatorname{Aut}(F_n)$  [5, Theorem 1.9]. Consider a characteristic subgroup H of finite index in  $F_n$ . The kernel of  $\operatorname{Aut}(F_n) \to \operatorname{Aut}(F_n/H)$  is called *principal congruence subgroup*, and any finite index subgroup of  $\operatorname{Aut}(F_n)$  containing a principal congruence subgroup is called *congruence subgroup*. A group G is said to have the *congruence subgroup propery* if every finite index subgroup of G contains a principal congruence subgroup. Asada proved that  $B_n$  satisfies the congruence subgroup property by using the notions of field extensions and profinite groups [3, Theorem 3A, Theorem 5]. In contrast with Asada's techniques, Thurston gave a more elementary proof to the congruence subgroup property of  $B_n$  [22].

**Outline of the paper.** In Section 2 we give basic background on braid groups, hyperelliptic mapping class groups, the symplectic representation of braid groups, and the congruence subgroups of braid groups. In Section 3 we recall some key results about the congruence subgroups of symplectic groups. In Section 4 we give a topological interpretation of the generators of the prime level congruence subgroups of braid groups. In Section 5 we prove Theorems A and B. In Section 6 we prove Theorem C.

Acknowledgments. I would like to thank my PhD supervisor Tara Brendle for her support during my work on this paper.

### 2 Preliminaries

In this section we recall the definition of braid groups, hyperelliptic mapping class groups, and the symplectic representation of braid groups.

#### 2.1 Definitions of braid groups



Figure 1: The action of  $\sigma_3$  on a punctured disc.

**Braid groups.** For detailed description of the following definition, see Birman-Brendle's survey [6]. Let  $\Sigma_{g,n}^b$  denote an orientable surface of genus g with n punctures and b boundary components. If n = 0 we will simply write  $\Sigma_g^b$ . If g = 0 and b = 1 then  $\Sigma_{0,n}^1$  is homeomorphic to a punctured disc. We enumerate the punctures from left to right. The *braid group*  $B_n$  on n strands is defined to be the mapping class group  $Mod(\Sigma_{0,n}^1)$  of  $\Sigma_{0,n}^1$ . For  $1 \le i \le n-1$  we denote by  $\sigma_i$  the mapping classes that interchanges the punctures i, i + 1 as depicted in Figure 1 for i = 3. The mapping classes  $\sigma_i$  are called half-twists. It turns out that  $\sigma_i$  generate the braid group  $B_n$ . In fact we have the following presentation

$$\langle \sigma_1, ..., \sigma_{n-1} \mid \sigma_i \sigma_{i+1} \sigma_i = \sigma_{i+1} \sigma_i \sigma_{i+1}, \sigma_i \sigma_j = \sigma_j \sigma_i \text{ when } |i-j| > 1 \rangle.$$

Consider the symmetric group  $S_n$ , and for  $1 \ge i \ge n-1$  let  $s_i$  denote the generators of  $S_n$ , that is the transpositions (i, i + 1). The map  $B_n \to S_n$  defined by  $\sigma_i \mapsto s_i$  is a well defined homomorphism with kernel the *pure braid group*  $PB_n$ . Let  $1 \le i < j \le n-1$ , we denote by  $a_{i,j}$ the element  $\sigma_{j-1}...\sigma_{j-1}^2...\sigma_{j-1}$ . For  $1 \le i < j \le n-1$  the group  $PB_n$  admits a presentation with generators  $a_{i,j}$  and relations

P1.  $a_{r,s}^{-1}a_{i,j}a_{r,s} = a_{i,j}, 1 \le r < s < i < j \le n \text{ or } 1 \le i < r < s < j \le n$ ,

P2. 
$$a_{r,s}^{-1} a_{i,j} a_{r,s} = a_{r,j} a_{i,j} a_{r,j}^{-1}, \ 1 \le r < s = i < j \le n$$

- P3.  $a_{r,s}^{-1} a_{i,j} a_{r,s} = (a_{i,j} a_{s,j}) a_{i,j} (a_{i,j} a_{s,j})^{-1}, \ 1 \le r = i < s < j \le n,$
- ${\rm P4.} \ \ a_{r,s}^{-1} a_{i,j} a_{r,s} = (a_{r,j} a_{s,j} a_{r,j}^{-1} a_{s,j}^{-1}) a_{i,j} (a_{r,j} a_{s,j} a_{r,j}^{-1} a_{s,j}^{-1})^{-1}, \ 1 \leq r < i < s < j \leq n.$

For more details about definitions and presentations of  $B_n$  and  $PB_n$  see [6, Chapter 1].



Figure 2: Action of the hyperelliptic involution.

Hyperelliptic mapping class groups. Let c be a nonseparating simple closed curve on a surface  $\Sigma_{g,n}^b$ . We denote by  $T_c$  the Dehn twist about the curve c. Dehn twists about nonseparating simple closed curves generate  $\operatorname{Mod}(\Sigma_g^b)$ . Consider a hyperelliptic involution  $\iota$  as depicted in Figure 2. For  $b = 1, 2, \iota$  acts on  $\Sigma_g^b$ . Since  $\iota$  does not fix the boundary components of  $\Sigma_g^b$  pointwise, then  $\iota \notin \operatorname{Mod}(\Sigma_g^b)$ . We have a two fold branched cover  $\Sigma_g^b \to \Sigma_g^b/\iota$ . Topologically  $\Sigma_g^b/\iota$  is homeomorphic to  $\Sigma_{0,2g+b}^1$  (see Figure 2). We note that if  $q_1, q_2$  denote the boundary components of  $\Sigma_g^2$ , then  $\iota(q_1) = q_2$ .



Figure 3: Generators of the hyperelliptic mapping class group.

Consider the curves  $c_i$  depicted in Figure 3, and let  $\sigma_i$  be the generators of  $B_{2g+b}$ . We define a map  $\xi : B_{2g+b} \to \operatorname{Mod}(\Sigma_g^b)$  by  $\xi(\sigma_i) = T_{c_i}$ . Since the braid, and the disjointness relations are satisfied by  $\sigma_i$  and  $T_{c_i}$ , then  $\xi$  is a homomorphism. The image of  $\xi$  is called *hyperelliptic mapping* class group, and it is denoted by  $\operatorname{SMod}(\Sigma_g^b)$ . In fact we have  $B_{2g+b} \cong \operatorname{SMod}(\Sigma_g^b)$  [15, Theorem 9.2] (see also [24]).

#### 2.2 Symplectic representation

In this section we will construct a representation for the braid group  $B_n$ . Firstly, we recall the definition of  $\operatorname{Sp}_{2n}(\mathbb{Z})$ . Let J be the  $2n \times 2n$  matrix

$$\left(\begin{array}{cc} 0 & I_n \\ -I_n & 0 \end{array}\right).$$

The symplectic group with integer coefficients is defined to be

$$\operatorname{Sp}_{2n}(\mathbb{Z}) = \{ A \in \operatorname{GL}(2n, \mathbb{Z}) \mid A^T J A = J \}.$$

We also define the symplectic group with coefficients in  $\mathbb{Z}/m$  to be

$$\operatorname{Sp}_{2n}(\mathbb{Z}/m) = \{A \in \operatorname{GL}(2n,\mathbb{Z}) \mid A^T J A \equiv J \mod(m)\}$$

where  $m \in \mathbb{N}$ . For a fixed  $u \in \mathbb{Z}^{2n}$ , we also recall

$$(\operatorname{Sp}_{2n}(\mathbb{Z}))_u = \{ t \in \operatorname{Sp}_{2n}(\mathbb{Z}) \mid t(u) = u \}.$$

Consider  $g \ge 1$  and b = 1, 2. Since  $B_{2g+b} \cong \text{SMod}(\Sigma_g^b)$ , we will use the action of  $\text{SMod}(\Sigma_g^b)$  on the first homology of  $\Sigma_g^b$  to construct a representation for  $B_{2g+b}$ .



Figure 4: Standard generators for  $H_1(\Sigma_a^1)$ , and  $H_1^P(\Sigma_a^2, \mathbb{Z})$ .

**Construction of the representation.** We denote by  $\iota_a$  the algebraic intersection number between curves of  $\Sigma_g^b$  for  $g \ge 1$  and b = 1, 2. The form  $\iota_a$  is an alternating bilinear and nondegenerate. Every element of the mapping class group preserves  $\iota_a$  [15, Section 6.3]. Consider b = 1; the oriented curves  $x_i, y_i$  of  $\Sigma_g^1$  of Figure 4 form a symplectic basis for  $H_1(\Sigma_g^1; \mathbb{Z})$ . The action of  $SMod(\Sigma_q^1)$  on  $H_1(\Sigma_q^1; \mathbb{Z})$  induces the following representation:

$$\operatorname{SMod}(\Sigma_q^1) \to \operatorname{Sp}_{2q}(\mathbb{Z}).$$

If b = 2, the module  $H_1(\Sigma_g^2; \mathbb{Z})$  is not symplectic. Thus, we will consider a different module. Fix a point on each of the boundaries of  $\Sigma_g^2$ , and denote by Q the set that contains those two points. Denote also by P the set that contains the two boundary components. We set  $H_1^P(\Sigma_g^2; \mathbb{Z}) \cong$  $H_1(\Sigma_g^2, Q; \mathbb{Z})/\langle P \rangle$ . The module  $H_1^P(\Sigma_g^2; \mathbb{Z})$  is symplectic [9, Section 2.1] (see also [26]). The basis of  $H_1^P(\Sigma_g^2; \mathbb{Z})$  is  $x_i, y_i$  as indicated on the right hand side of Figure 4. The action of  $SMod(\Sigma_g^2)$  on  $H_1^P(\Sigma_g^2; \mathbb{Z})$  induces the following representation:

$$\operatorname{SMod}(\Sigma_g^2) \to (\operatorname{Sp}_{2g+2}(\mathbb{Z}))_{y_{g+1}},$$

where  $(\operatorname{Sp}_{2g+2}(\mathbb{Z}))_{y_{g+1}}$  stands for the subgroup of  $\operatorname{Sp}_{2g+2}(\mathbb{Z})$  that fixes the vector  $y_{g+1}$ .

Since the map  $\xi: B_{2g+b} \to \mathrm{SMod}(\Sigma_q^b)$  is an isomorphism, we have a well defined representation

$$\rho: B_{2g+b} \to \begin{cases} \operatorname{Sp}_{2g}(\mathbb{Z}) & \text{if } b = 1\\ (\operatorname{Sp}_{2g+2}(\mathbb{Z}))_{y_{g+1}} & \text{if } b = 2. \end{cases}$$

**Image of the representation.** We denote also by [c] the homology class of a curve c in  $\Sigma_g^b$ . For x, c nonseparating simple closed curves in  $\Sigma_g^b$ , the automorphism  $T_{[c]}([x]) = [x] + \iota_a(x, c)[c]$  is called a transvection [15, Section 6.6.3]. We remark that for every integer m, we have  $T_{[c]}^m([x]) = [x] + m\iota_a(x, c)[c]$ .

Let  $T_{c_i}$  be a Dehn twist about a curve  $c_i$  indicated in Figure 3. The image of  $T_{c_i}$  under the symplectic representation is the transvection  $T_{[c_i]}$ . Also, since  $\xi(\sigma_i) = T_{c_i}$  as explained in the previous section, we have  $\rho(\sigma_i) = T_{[c_i]}$ . We note also that  $\rho(\sigma_i^m) = T_{[c_i]}^m$ .

Kernel of the symplectic representation. Assume that  $b = 1, 2, g \ge 0$ , and recall that  $B_{2g+b} = \text{Mod}(D_{2g+b})$ . The kernel of the symplectic representation  $\rho$  is denoted by  $\mathcal{BI}_{2g+b}$ , and it is called the *braid Torelli*. It is a result by Brendle-Margalit-Putman that  $\mathcal{BI}_{2g+b}$  is generated by Dehn twists about simple closed curves surrounding 3 or 5 number of puncture points [11, Theorem C].

Consider the isomorphism  $\xi : B_{2g+b} \to \text{SMod}(\Sigma_g^b)$ . The image of  $\mathcal{BI}_{2g+b}$  in  $\text{SMod}(\Sigma_g^b)$  under  $\xi$  is denoted by  $\mathcal{SI}(\Sigma_g^b)$ . The latter group is well known as the hyperelliptic Torelli group. Furthermore,  $\mathcal{SI}(\Sigma_g^b)$  is generated by Dehn twists about symmetric separating simple closed curves that bound a subsurface of genus 1 or 2 [11, Theorem A].

#### 2.3 Congruence subgroups of braid groups

Let *m* be a positive integer. The surjective homomorphisms  $H_1(\Sigma_g^1; \mathbb{Z}) \to H_1(\Sigma_g^1; \mathbb{Z}/m)$  and  $H_1^P(\Sigma_g^2; \mathbb{Z}) \to H_1^P(\Sigma_g^2; \mathbb{Z}/m)$  induce the following epimorphisms:

$$\begin{cases} \operatorname{Sp}_{2g}(\mathbb{Z}) \to & \operatorname{Sp}_{2g}(\mathbb{Z}/m) \\ (\operatorname{Sp}_{2g+2}(\mathbb{Z}))_{y_{g+1}} \to & (\operatorname{Sp}_{2g+2}(\mathbb{Z}/m))_{y_{g+1}}. \end{cases}$$

Thus we have a family of representations for the braid groups

$$\rho_m: B_{2g+b} \to \begin{cases} \operatorname{Sp}_{2g}(\mathbb{Z}/m) & \text{if } b = 1\\ (\operatorname{Sp}_{2g+2}(\mathbb{Z}/m))_{y_{g+1}} & \text{if } b = 2, \end{cases}$$

where  $g \ge 1$ . The kernels of the representations  $\rho_m$  are denoted by  $B_{2g+b}[m]$  and they are known as *level-m congruence subgroups of braid groups*.

## 3 Congruence subgroups of Symplectic groups

In this section we examine the structure of the congruence subgroups of symplectic groups.

**Congruence subgroups and generators.** The projection  $\mathbb{Z} \to \mathbb{Z}/m$  induces a surjective homomorphism  $\operatorname{Sp}_{2n}(\mathbb{Z}) \to \operatorname{Sp}_{2n}(\mathbb{Z}/m)$ , whose kernel is the *principal level* m congruence subgroup of  $\operatorname{Sp}_{2n}(\mathbb{Z})$  denoted by  $\operatorname{Sp}_{2n}(\mathbb{Z})[m]$ . The group  $\operatorname{Sp}_{2n}(\mathbb{Z})[m]$  consists of all matrices of the form  $I_{2n} + mA$ ; where  $A \in \operatorname{Sp}_{2n}(\mathbb{Z})$ . Furthermore, if m is a multiple of l then  $\operatorname{Sp}_{2n}(\mathbb{Z})[m] \triangleleft \operatorname{Sp}_{2n}(\mathbb{Z})[l]$ .

Next we give generators for  $\operatorname{Sp}_{2n}(\mathbb{Z})[p]$  when p is any prime number. Let  $r \in \mathbb{Z}$ . We define  $e_{i,j}(r)$  to be the  $n \times n$  matrix with  $(i, j)^{th}$  entry equal to r and 0 otherwise. Let  $\beta_i(r)$  be the  $n \times n$  matrix with  $(i, i)^{th}$  and  $(i, i + 1)^{th}$  entries equal to r,  $(i + 1, i + 1)^{th}$  and  $(i + 1, i)^{th}$  entries equal to -r and 0 otherwise. Define also  $se_{i,j}(r)$  to be the  $n \times n$  matrix with  $(i, j)^{th}$  and  $(j, i)^{th}$  entries equal to r and 0 otherwise. For  $1 \leq i \leq j \leq n$  we define:

$$\mathcal{X}_{i,j}(r) = I_{2n} + \begin{pmatrix} 0 & 0\\ se_{i,j}(r) & 0 \end{pmatrix}, \quad \mathcal{Y}_{i,j}(r) = I_{2n} + \begin{pmatrix} 0 & se_{i,j}(r)\\ 0 & 0 \end{pmatrix}.$$

For  $1 \leq i, j \leq n$  with  $i \neq j$  we define:

$$\mathcal{Z}_{i,j}(r) = I_{2n} + \begin{pmatrix} e_{i,j}(r) & 0\\ 0 & -e_{i,j}(r) \end{pmatrix}$$

For  $1 \leq i < n$ 

$$\mathcal{W}_i(r) = I_{2n} + \left(\begin{array}{cc} \beta_i(r) & 0\\ 0 & -\beta_i(r) \end{array}\right).$$

Finally,

$$\mathcal{U}_1(r) = I_{2n} + \begin{pmatrix} e_{1,1}(r) & e_{1,1}(r) \\ -e_{1,1}(r) & -e_{1,1}(r) \end{pmatrix}$$

The following theorem gives a nice description of  $\operatorname{Sp}_{2n}(\mathbb{Z})[p]$  as a group generated by the matrices above [13, Lemma 5.4].

**Theorem 3.1** (Church-Putman). For  $n \ge 2$  and for a prime number  $p \ge 2$  the congruence subgroup  $\operatorname{Sp}_{2n}(\mathbb{Z})[p]$  is generated by the set

$$\mathcal{S} = \{\mathcal{X}_{i,j}(p), \mathcal{Y}_{i,j}(p), \mathcal{Z}_{i,j}(p), \mathcal{W}_i(p), \mathcal{U}_1(p)\}$$

where i, j are indices defined as above.

We use Theorem 3.1 to prove the lemma below, since we do not know a concise proof in the literature. In particular, we use the generators of Theorem 3.1 to prove that  $\operatorname{Sp}_{2n}(\mathbb{Z}/b)$  can be expressed as a quotient of some congruence subgroup of  $\operatorname{Sp}_{2n}(\mathbb{Z})$  when b is a prime number.

Lemma 3.2. Let a and b two distinct prime numbers. Then the following sequence is exact.

$$1 \to \operatorname{Sp}_{2n}(\mathbb{Z})[ab] \to \operatorname{Sp}_{2n}(\mathbb{Z})[a] \to \operatorname{Sp}_{2n}(\mathbb{Z}/b) \to 1$$

Proof. The map  $\operatorname{Sp}_{2n}(\mathbb{Z})[a] \to \operatorname{Sp}_{2n}(\mathbb{Z}/b)$  sends every matrix  $A \in \operatorname{Sp}_{2n}(\mathbb{Z})[a]$  into its mod(b)reduction. First, we prove the surjectivity of the latter map. The generators of  $\operatorname{Sp}_{2n}(\mathbb{Z}/b)$  are  $\mathcal{X}_{i,j}(1) \mod(b)$  and  $\mathcal{Y}_{i,j}(1) \mod(b)$  where  $1 \leq i < j \leq n$ . Define *n* to be the solution of the equation  $an \equiv 1 \mod(b)$ . Then,  $\mathcal{X}_{i,j}(a)^n \equiv \mathcal{X}_{i,j}(1) \mod(b)$  and  $\mathcal{Y}_{i,j}(a)^n \equiv \mathcal{Y}_{i,j}(1) \mod(b)$ . This proves the surjectivity of the reduction map. The kernel of this reduction map contains matrices which satisfy  $I_{2n} + aA \equiv I_{2n} \mod(b)$ . But since *a* and *b* are relatively primes, the latter equivalence holds if and only if A = bB when *B* is a symplectic matrix.  $\Box$ 

The following proposition gives a useful decomposition of  $\operatorname{Sp}_{2n}(\mathbb{Z}/m)$  [23, Theorem 5].

**Proposition 3.3** (Newman-Smart). Let  $m \in \mathbb{N}$  and write  $m = p_1^{k_1} p_2^{k_2} \dots p_l^{k_l}$ , where  $p_i^{k_i}$  are powers of prime numbers. Then

$$\operatorname{Sp}_{2n}(\mathbb{Z}/m) = \bigoplus_{i=1}^{l} \operatorname{Sp}_{2n}(\mathbb{Z}/p_i^{k_i}).$$

Newman-Smart also proved that the abelian group  $\mathfrak{sp}_{2n}(\mathbb{Z}/l)$  can be expressed as a quotient of congruence subgroups of  $\operatorname{Sp}_{2n}(\mathbb{Z})$ , [23, Theorem 7].

**Proposition 3.4** (Newman-Smart). Let  $l, m \geq 2$  such that l divides m. Then we have the following isomorphism.

$$\operatorname{Sp}_{2n}(\mathbb{Z})[m]/\operatorname{Sp}_{2n}(\mathbb{Z})[ml] \cong \mathfrak{sp}_{2n}(\mathbb{Z}/l).$$

Lemma 3.2 and Propositions 3.3 and 3.4 play crucial role in Section 5, in which we explore the structure of congruence subgroups of braid groups.

# 4 Topological interpretation of prime level congruence subgroups

The purpose of this section is the characterization of the group  $B_{2g+b}[p]$  when p is prime. Since  $B_{2g+b} \cong \mathrm{SMod}(\Sigma_q^b)$ , it is convenient to study the kernel of the map

$$\operatorname{SMod}(\Sigma_g^b) \to \begin{cases} \operatorname{Sp}_{2g}(\mathbb{Z}/p) & \text{if } b = 1, \\ (\operatorname{Sp}_{2g+2}(\mathbb{Z}/p))_{y_{g+1}} & \text{if } b = 2 \end{cases}$$

and we denote the map again by  $\rho_p$ . Also, we denote the kernel of  $\rho_p$  by  $B_{2q+b}[p]$ .

A'Campo proved that the homomorphism  $\rho_p$  is surjective [1, Theorem 1 (1)]. Later Assion gave a presentation for  $\operatorname{Sp}_{2g}(\mathbb{Z}/3)$  and  $(\operatorname{Sp}_{2g+2}(\mathbb{Z}/3))_{y_{g+1}}$  as quotients of braid groups [4]. Wajnryb improved the result of Assion and generalized it for any prime number greater than 2 [27, Theorem 1]. We begin with the theorem of Wajnryb.

**Theorem 4.1** (Wajnryb). Consider the curves  $c_i$  depicted in Figure 3. Let  $G_{2g+b}$  be a group with generators  $T_{c_1}, ..., T_{c_{2g+b-1}}$  and relations R1 to R6 as follows.

R1.  $T_{c_i}T_{c_{i+1}}T_{c_i} = T_{c_{i+1}}T_{c_i}T_{c_{i+1}};$ R2.  $[T_{c_i}, T_{c_i}] = 1, \text{ for } |i-j| > 1;$  R3.  $T_{c_1}^p = 1;$ 

- *R*4.  $(T_{c_1}T_{c_2})^6 = 1$ , for p > 3;
- R5.  $T_{c_1}^{(p-1)/2} T_{c_2}^4 T_{c_1}^{-(p-1)/2} = T_{c_2}^2 T_{c_1} T_{c_2}^{-2}$ , for p > 3; and
- $R6. \ \ (T_{c_1}T_{c_2}T_{c_3})^4 = AT_{c_1}^2A^{-1}, \ \text{for} \ n > 4, \ \text{where} \ A = T_{c_4}T_{c_3}^2T_{c_4}T_{c_2}^{(p-1)/2}T_{c_3}^{-1}T_{c_2}.$

Then  $G_{2g+1}$  is isomorphic to  $\operatorname{Sp}_{2q}(\mathbb{Z}/p)$ , and  $G_{2g+2}$  is isomorphic to  $(\operatorname{Sp}_{2q+2}(\mathbb{Z}/p))_{y_{n+1}}$ .

As a consequence of Theorem 4.1 we obtain elements of  $\text{SMod}(\Sigma_g^b)$  which normally generate  $B_{2g+b}[p]$ .

In the rest of the section we examine the elements of the relations of Theorem 4.1 in order to give a topological description for the generators of  $B_n[p]$ . We note that relations R1 and R2 are the defining relations in the presentation of the braid group.

We denote by  $[c_i]$  the homology class of  $c_i$ , and by  $T_{[c_i]}$  the transvection associated to the Dehn twist  $T_{c_i}$  under the map

$$\mathrm{SMod}(\Sigma_g^b) \to \begin{cases} \mathrm{Sp}_{2g}(\mathbb{Z}/p) & \text{if } b = 1, \\ (\mathrm{Sp}_{2g+2}(\mathbb{Z}/p))_{y_{g+1}} & \text{if } b = 2. \end{cases}$$

By definition, the action of a transvection  $T^m_{[c]}$  on an element  $u \in H_1(\Sigma^1_g, \mathbb{Z})$  (respectively  $H^P_1(\Sigma^2_g, \mathbb{Z})$ ) is defined to be  $T^m_{[c]}(u) = [u] + m\hat{i}(u, [c])[c]$ , where  $\hat{i}$  stands for the algebraic intersection number.

**R3:** Powers of Dehn twists. The  $p^{th}$  powers of Dehn twists about symmetric nonseparating simple closed curves are easy to check by looking at their image in the symplectic group. The symplectic representation sends  $T_{c_1}^p$  into the following matrix:

$$\left(\begin{array}{cc}1&p\\0&1\end{array}\right)\oplus I,$$

where I stands for the identity matrix of dimension depending on g and b (see Section 7.1.3). The mod(p) reduction of the matrix above is the identity. Moreover, every Dehn twist about a non-separating curve is conjugate to  $T_{c_1}$ . As a consequence, every Dehn twist in  $\text{SMod}(\Sigma_g^b)$  raised to the power of p lies in  $B_n[p]$ .

**R4:** Symmetric separating Dehn twists. By the chain relation the element  $(T_{c_1}T_{c_2})^6$  can be represented by a Dehn twist  $T_{\gamma}$ , where  $\gamma$  is the symmetric separating curve bounding the genus 1 subsurface of  $\Sigma_g^b$  as indicated in Figure 5 [15, Proposition 4.12]. We can generalize the relation R4 by considering a symmetric separating curve  $\delta$  of a genus k subsurface of  $\Sigma_g^b$ . By the chain relation there is a maximal chain of curves  $a_1, ..., a_{2k}$  in the subsurface of genus k with boundary  $\delta$  such that  $(T_{a_1}...T_{a_{2k}})^{4k+2} = T_{\delta}$ .

The fact that every symmetric separating simple closed curve  $\delta$  is nullhomologous in  $H_1(\Sigma_g^1)$ (respectively  $H_1^P(\Sigma_g^2)$ ) implies that  $T_{[\delta]}(x) = x + \iota_a(x, [\delta]) = x + 0 = x$  for every  $x \in H_1(\Sigma_g^1)$ (respectively  $H_1^P(\Sigma_g^2)$ ), where  $T_{[\delta]}$  is the corresponding transvection of  $T_{\delta}$  as described in Section 2. Since for every symmetric separating curve  $\delta$  in  $\Sigma_g^b$  and  $T_{\delta} \in B_{2g+b}[p]$  we have that  $(T_{a_1}...T_{a_{2k}})^{4k+2} \in \mathcal{SI}(\Sigma_g^b) \subset B_{2g+b}[p]$ .

**R5:** Mod-p involution maps. We begin by modifying the relation *R*5 of Theorem 4.1.

Lemma 4.2. The relation R5 given above is equivalent to:

$$(T_{c_1}^{(p+1)/2}T_{c_2}^4)^2 = (T_{c_1}T_{c_2})^3$$

in  $\operatorname{Sp}_{2g}(\mathbb{Z}/p)$  (respectively  $(\operatorname{Sp}_{2g+2}(\mathbb{Z}/p))_{y_{g+1}})$ .



Figure 5: The curve  $\gamma$  that bound a surface of genus 1.

*Proof.* We have that  $(T_{c_1}T_{c_2})^3 = T_{c_1}T_{c_2}^2T_{c_1}T_{c_2}^2$ . Then

$$T_{c_1}^{(p-1)/2} T_{c_2}^4 T_{c_1}^{-(p-1)/2} = T_{c_1}^{-1} (T_{c_1}^{(p+1)/2} T_{c_2}^4)^2 T_{c_2}^{-4} = T_{c_2}^2 T_{c_1} T_{c_2}^{-2}.$$

On the other hand

$$(T_{c_1}^{(p+1)/2}T_{c_2}^4)^2 = T_{c_1}T_{c_1}^{(p-1)/2}T_{c_2}^4T_{c_1}^{-(p-1)/2}T_{c_2}^4 = T_{c_1}T_{c_2}^2T_{c_1}T_{c_2}^2.$$

Now we examine the relation of Lemma 4.2.

**RHS.** For  $i = 1, 2, (T_{c_1}T_{c_2})^3([c_i]) = -[c_i]$ , where  $[c_i]$  stands for the homology class of  $c_i$ . Thus, the homeomorphism  $(T_{c_1}T_{c_2})^3$  acts as the hyperelliptic involution on the subsurface bounded by the boundary of the chain  $ch(c_1, c_2)$  (see Figure 5).

LHS. We have

$$(T_{c_1}^{(p+1)/2}T_{c_2}^4)^2([c_1]) = -8p[c_2] + (4p^2 + 2p - 1)[c_1] \equiv -[c_1] \mod (p),$$
  
$$(T_{c_1}^{(p+1)/2}T_{c_2}^4)^2([c_2]) = 2p\frac{p+1}{2}[c_1] - (2p+1)[c_2] \equiv -[c_2] \mod (p)$$

Therefore,  $(T_{c_1}^{(p+1)/2}T_{c_2}^4)^2$  acts as the hyperelliptic involution mod (p) in the subspace of  $H_1(\Sigma_g^1, \mathbb{Z}/p)$  (resp  $H_1^P(\Sigma_g^2, \mathbb{Z}/p)$ ) spanned by  $[c_1], [c_2]$ .

We can generalize Relation R5 as follows. For k even, consider any chain  $ch(a_1, a_2, ..., a_k)$  of symmetric simple closed curves such that  $T_{a_i} \in \mathrm{SMod}(\Sigma_{g,b})$  for all  $i \leq k$ . Choose an  $f \in \mathrm{SMod}(\Sigma_g^b)$  such that  $f([a_i]) = -[a_i]$ . Then  $(T_{a_1}...T_{a_k})^{k+1}f^{-1} \in B_{2g+b}[p]$ . We call this type of element an mod-p involution map.

**R6:** Mod-p center maps. We describe a generalized version of  $(T_{c_1}T_{c_2}T_{c_3})^4(AT_{c_1}^{-2}A^{-1})$ . Let  $A_1$  be the trivial homeomorphism in  $\text{SMod}(\Sigma_q^b)$ . For k odd, and  $k \geq 3$ , define

$$A_{k} = T_{c_{k+1}} T_{c_{k}}^{2} T_{c_{k+1}} T_{c_{k-1}}^{(p-1)/2} T_{c_{k}}^{-1} T_{c_{k-1}} A_{k-2}.$$

First, we deal with the case b = 1. (For b = 2 the process is exactly the same.) Consider the symplectic bases  $\{y_i, x_i\}$  for  $H_1(\Sigma_q^1, \mathbb{Z})$  depicted on Figure 4.

**Lemma 4.3.** For k odd, we have that  $A_k T_{[c_1]} A_k^{-1} = T_{[y_{(k+1)/2}]}$  in  $\text{Sp}_{2g}(\mathbb{Z}/p)$ .

Note that if k = 3, then  $T_{[y_2]} = T_{[d_3]}$ .

*Proof.* We need to prove that  $A_k([c_1]) \equiv [c_1] + [c_3] + ... + [c_k] \in \operatorname{Sp}_{2g}(\mathbb{Z}/p)$ . A direct calculation shows that  $A_3([c_1]) \equiv [c_1] + [c_3] \mod(p)$ . Assume that the theorem is true for k - 2, that is  $A_{k-2}([c_1]) = [c_1] + [c_3] + ... + [c_{k-2}]$ . Then  $T_{c_{k+1}}T_{c_k}^2T_{c_{k+1}}T_{c_{k-1}}^{(p-1)/2}T_{c_k}^{-1}T_{c_{k-1}}([c_{k-2}]) \equiv [c_{k-2}] + [c_k] \mod(p)$ . The proof of the lemma follows.



Figure 6: The chain relation of R6.

Let k be an odd integer, and consider also the odd chain  $ch(c_1, c_2, ..., c_k)$ . By the chain relation we have that  $(T_{c_1}...T_{c_k})^{k+1} = T_{d_k}T_{d'_k}$ , where  $d_k = y_{(k+1)/2}$ , and  $[d_k] = [d'_k] = [y_{(k+1)/2}]$  (see, for example, Figure 6). Thus,  $(T_{[c_1]}...T_{[c_k]})^{k+1} = T^2_{[y_{(k+1)/2}]} \in \operatorname{Sp}_{2g}(\mathbb{Z}/p)$ . On the other hand, according to Lemma 4.3 we have that  $A_k T^2_{[c_1]} A_k^{-1} = T^2_{[y_{(k+1)/2}]} \in \operatorname{Sp}_{2g}(\mathbb{Z}/p)$ . Hence,  $(T_{c_1}...T_{c_k})^{k+1}A_kT^{-2}_{c_1}A_k^{-1} \in B_n[p]$ . Note that if k = 3, the element  $(T_{c_1}...T_{c_k})^{k+1}A_kT^{-2}_{c_1}A_k^{-1}$  is the same one as in the relation 6 of Theorem 4.1.

We can describe a generalized version of  $(T_{c_1}...T_{c_k})^{k+1}A_kT_{c_1}^{-2}A_k^{-1}$ . Consider any odd chain  $ch(a_1, a_2, ..., a_k)$ , such that  $T_{a_i} \in \mathrm{SMod}(\Sigma_g^1)$  for all  $i \leq k$ . Choose a homeomorphism  $h \in \mathrm{SMod}(\Sigma_g^1)$  such that  $h([a_1]) = [a_1] + [a_3] + ... + [a_k] \in \mathrm{Sp}_{2g}(\Sigma_g^1)$ . Then  $(T_{a_1}...T_{a_k})^{k+1}hT_{a_1}^{-2}h^{-1}$  lies on  $B_{2g+1}[p]$ . If we consider  $(T_{a_1}...T_{a_k})^{k+1}$  as the center of the subgroup K of  $\mathrm{SMod}(\Sigma_g^b)$  generated by  $T_{a_1}...T_{a_k}$ , then  $hT_{a_1}^{-2}h^{-1}$  is the center mod(p) of the same group. Note that the choice of h is not unique. We call this type of element an *mod-p center map*.

**Generators for congruence subgroups.** As a corollary of Theorem 4.1 we obtain the following theorem.

**Theorem 4.4.** If p = 3, then  $B_{2g+b}[3]$  is generated by Dehn twists raised to the power of 3, and for 2g + b > 4 by mod-p center maps. For p > 3 the subgroup  $B_{2g+b}[p]$  of  $\mathrm{SMod}(\Sigma_g^b)$  is generated by Dehn twists raised to the power of p, by Dehn twists about symmetric separating curves, by mod-p involution maps, and for 2g + b > 4 by mod-p center maps.

Finite set of generators. It is well known that every finite index subgroup of a finitely generated group, is finitely generated [21, Corollary 2.7.1]. The generating set in Theorem 4.4 is infinite. When p = 3 and g = 1 we can find a finite set of generators.

**Theorem 4.5.** The group  $B_3[3]$  is generated by four elements.

*Proof.* Set  $S = \{T_{c_1}^3, T_{c_2}^3, T_{c_2}T_{c_1}^3, T_{c_2}^{-1}, T_{c_2}^2T_{c_1}^3T_{c_2}^{-2}\}$ . We denote by  $\Gamma$  the subgroup of  $B_3[3]$  generated by S. We prove that if we conjugate elements of S by  $T_{c_1}$  or  $T_{c_2}$ , then the resulting elements lie in  $\Gamma$ . Since  $B_3[3]$  is normally generated by S and since S generates a normal subgroup of  $B_3$ , then  $\Gamma = B_3[3]$ .

In the braid group we have the relation

$$T_{c_j}T_{c_{j-1}}...T_{c_i}^3...T_{c_{j-1}}^{-1}T_{c_j}^{-1} = T_{c_i}^{-1}T_{c_{i+1}}^{-1}...T_{c_j}^3...T_{c_{i+1}}T_{c_i}$$

We prove the theorem in three steps.

**Step 1:** Conjugates of  $T_{c_1}^3, T_{c_2}^3$ :

$$T_{c_2}^{-1}T_{c_1}^3T_{c_2} = T_{c_2}^{-3}T_{c_2}^2T_{c_1}^3T_{c_2}^{-2}T_{c_2}^3 \in \Gamma$$
$$T_{c_1}^{-1}T_2^3T_{c_1} = T_2T_{c_1}^3T_2^{-1} \in \Gamma$$
$$T_{c_1}T_{c_2}^3T_{c_1}^{-1} = T_{c_2}^{-1}T_{c_1}^3T_{c_2} = T_{c_2}^{-3}T_{c_2}^2T_{c_1}^3T_{c_2}^{-2}T_{c_2}^3 \in \Gamma.$$

**Step 2:** Conjugates of  $T_{c_2}T_{c_1}^3T_{c_2}^{-1}$ :

$$T_{c_1}T_{c_2}T_{c_1}^3T_{c_2}^{-1}T_{c_1}^{-1} = T_{c_2}^3 \in \Gamma$$
$$T_{c_1}^{-1}T_{c_2}T_{c_1}^3T_{c_2}^{-1}T_{c_1} = T_{c_1}^{-2}T_{c_2}^3T_{c_1}^2 = T_{c_1}^{-3}(T_{c_1}T_{c_2}^3T_{c_1}^{-1})T_{c_1}^3.$$

The latter is in  $\Gamma$  by step 1.

**Step 3:** Conjugates of  $T_{c_2}^2 T_{c_1}^3 T_{c_2}^{-2}$ :

$$\begin{split} T_{c_1}^{-1} T_{c_2}^2 T_{c_1}^3 T_{c_2}^{-2} T_{c_1} &= T_{c_1}^{-1} T_{c_2}^3 T_{c_2}^{-1} T_{c_1}^3 T_{c_2} T_{c_2}^{-3} T_{c_1} \\ & (T_{c_1}^{-1} T_{c_2}^3 T_{c_1}) (T_{c_1}^{-1} T_{c_2}^{-1} T_{c_1}^3 T_{c_2} T_{c_1}) (T_1^{-1} T_{c_2}^{-3} T_{c_1}) \end{split}$$

The elements  $(T_{c_1}^{-1}T_{c_2}^3T_{c_1}), (T_{c_1}^{-1}T_{c_2}^{-3}T_{c_1})$  are in  $\Gamma$  by step 1.

$$T_{c_1}^{-1}T_{c_2}^{-1}T_{c_1}^3T_{c_2}T_{c_1} = T_{c_2}^3$$

Finally, since  $T_{c_2}^2 T_{c_1}^3 T_{c_2}^{-2} = T_{c_2}^3 T_{c_2}^{-1} T_{c_1}^3 T_{c_2} T_{c_2}^{-3}$ , it suffices to check that  $T_{c_1} T_{c_2}^{-1} T_{c_1}^3 T_{c_2} T_{c_1}^{-1}$  is in  $\Gamma$ . But we have that

$$T_{c_1}T_{c_2}^{-1}T_{c_1}^3T_{c_2}T_{c_1}^{-1} = T_{c_1}^2T_{c_2}^3T_{c_1}^{-2} = T_{c_1}^3T_{c_1}^{-1}T_{c_1}^3T_{c_1}^{-3} = T_{c_1}^3T_{c_2}T_{c_1}^3T_{c_2}^{-1}T_{c_1}^{-3} \in \Gamma.$$

This proves the theorem.

Since  $T_{c_2}^2 T_{c_1}^3 T_{c_2}^{-2} = T_{c_2}^3 T_{c_1}^{-1} T_{c_1}^3 T_{c_2} T_{c_2}^{-3}$  we deduce that  $\{T_{c_1}^3, T_{c_2}^3, T_{c_2} T_{c_1}^3 T_{c_2}^{-1}, T_{c_2}^{-1} T_{c_1}^3 T_{c_2}\}$  is also a generating set for  $B_3[3]$ .

## 5 Symplectic groups and pure braid groups

For  $i \in \mathbb{N}$ , let  $p_i$  denote a prime number greater than 2. In this section we characterize  $B_{2g+b}[m]$ , where  $m = 2p_1p_2...p_k$  and  $m = 4p_1p_2...p_k$ . Our strategy is to find a presentation for  $PB_{2g+b}/B_{2g+b}[m]$ . We recall that  $H_1(PB_{2g+b}, \mathbb{Z}/2)$  is  $\mathfrak{sp}_{2g}(\mathbb{Z}/2)$ , if b = 1 and  $\operatorname{Ann}(y_{g+1})$  if b = 2, where  $\operatorname{Ann}(y_{g+1}) = \{h \in \mathfrak{sp}_{2g+2}(\mathbb{Z}/2) \mid h(y_{g+1}) = 0\}$  [9]. The generators of  $B_{2g+b}$  are denoted by  $\sigma_i$  and the generators of  $PB_{2g+b}$  are denoted by  $a_{i,j}$  as in Section 2.

**Theorem 5.1.** For  $m = 2p_1p_2...p_k$ , where  $p_i \ge 3$  are prime numbers, we have

$$PB_{2g+b}/B_{2g+b}[m] = \begin{cases} \bigoplus_{i=1}^{k} \operatorname{Sp}_{2g}(\mathbb{Z}/p_i) & \text{if } b = 1, \\ \bigoplus_{i=1}^{k} (\operatorname{Sp}_{2g+2}(\mathbb{Z}/p_i))_{y_{g+1}} & \text{if } b = 2. \end{cases}$$

*Proof.* We set  $m = 2p_1p_2...p_k$ . We have the map

$$\rho_m: B_{2g+b} \to \begin{cases} \operatorname{Sp}_{2g}(\mathbb{Z}) \to \operatorname{Sp}_{2g}(\mathbb{Z}/m) & \text{if } b = 1, \\ (\operatorname{Sp}_{2g+2}(\mathbb{Z}))_{y_{g+1}} \to (\operatorname{Sp}_{2g+2}(\mathbb{Z}/m))_{y_{g+1}} & \text{if } b = 2 \end{cases}$$

with kernel  $B_{2g+b}[m]$ . By Lemma 3.3 we know that

$$\operatorname{Sp}_{2g}(\mathbb{Z}/m) = \operatorname{Sp}_{2g}(\mathbb{Z}/2) \bigoplus_{i=1}^{k} \operatorname{Sp}_{2g}(\mathbb{Z}/p_i).$$

If we restrict to the pure braid group, then the image of the map  $PB_{2g+1} \to \operatorname{Sp}_{2g}(\mathbb{Z})$  is the group  $\operatorname{Sp}_{2g}(\mathbb{Z})[2]$ , (see [9, Theorem 3.3]). Furthermore, by Lemma 3.2 we have that the map  $\operatorname{Sp}_{2g}(\mathbb{Z})[2] \to \operatorname{Sp}(\mathbb{Z}/p_i)$  is surjective. Thus, the image of the map

$$\operatorname{Sp}_{2g}(\mathbb{Z}) \to \operatorname{Sp}_{2g}(\mathbb{Z}/m) = \operatorname{Sp}_{2g}(\mathbb{Z}/2) \bigoplus_{i=1}^{k} \operatorname{Sp}_{2g}(\mathbb{Z}/p_i),$$

after we restrict to  $\operatorname{Sp}_{2g}(\mathbb{Z})[2]$ , is the group  $\bigoplus_{i=1}^k \operatorname{Sp}_{2g}(\mathbb{Z}/p_i)$ . Hence, have a short exact sequence

$$1 \to B_{2g+1}[m] \to PB_{2g+1} \to \bigoplus_{i=1}^k \operatorname{Sp}_{2g}(\mathbb{Z}/p_i) \to 1.$$

Likewise, since the image of the map  $PB_{2g+2} \to (\operatorname{Sp}_{2g+2}(\mathbb{Z}))_{y_{g+1}}$  is  $(\operatorname{Sp}_{2g+2}(\mathbb{Z})[2])_{y_{g+1}}$  (see [9, Theorem 3.3]), and since  $(\operatorname{Sp}_{2g+2}(\mathbb{Z}/m))_{y_{g+1}} < \operatorname{Sp}_{2g+2}(\mathbb{Z}/m)$ , we can apply Lemma 3.3 and end up with the following exact sequence.

$$1 \to B_{2g+2}[m] \to PB_{2g+2} \to \bigoplus_{i=1}^k (\operatorname{Sp}_{2g+2}(\mathbb{Z}/p_i))_{y_{g+1}} \to 1.$$

This completes the proof.

In the following statement we slightly generalize Lemma 5.1. The symplectic Lie algebra  $\mathfrak{sp}_{2n}(\mathbb{Z})$  consists of those elements  $A \in \mathfrak{gl}_{2n}(\mathbb{Z})$  which satisfy the relation  $A^T J + J A = 0$ . We define also

$$\operatorname{Ann}(u) = \{ m \in \mathfrak{sp}_{2n}(\mathbb{Z}) \mid m(u) = 0 \},\$$

where Ann(u) stands for the annihilator of the vector u. We have the following theorem.

**Theorem 5.2.** For  $m = 4p_1p_2...p_k$ , where  $p_i \ge 3$  are prime numbers, we have

$$PB_{2g+b}/B_{2g+b}[m] = \begin{cases} \mathfrak{sp}_{2g}(\mathbb{Z}/2) \bigoplus_{i=1}^{k} \operatorname{Sp}_{2g}(\mathbb{Z}/p_{i}) & \text{if } b = 1, \\ \operatorname{Ann}(e) \bigoplus_{i=1}^{k} (\operatorname{Sp}_{2g+2}(\mathbb{Z}/p_{i}))_{y_{g+1}} & \text{if } b = 2. \end{cases}$$

*Proof.* We set  $m = 4p_1p_2...p_k$ . By Lemma 3.3 we have that

$$\operatorname{Sp}_{2g}(\mathbb{Z}/m) = \operatorname{Sp}_{2g}(\mathbb{Z}/4) \bigoplus_{i=1}^{k} \operatorname{Sp}_{2g}(\mathbb{Z}/p_i).$$

We want to characterize the image of the map

$$B_{2g+b} \to \begin{cases} \operatorname{Sp}_{2g}(\mathbb{Z}/4) \bigoplus_{i=1}^{k} \operatorname{Sp}_{2g}(\mathbb{Z}/p_{i}) & \text{if } b = 1, \\ (\operatorname{Sp}_{2g+2}(\mathbb{Z}/4))_{y_{g+1}} \bigoplus_{i=1}^{k} (\operatorname{Sp}_{2g+2}(\mathbb{Z}/p_{i}))_{y_{g+1}} & \text{if } b = 2. \end{cases}$$

For b = 1 we only need to characterize the image of the restriction of the map above to  $PB_{2g+b}$ . In particular, we want to compute the image of the map  $PB_{2g+1} \to \operatorname{Sp}_{2g}(\mathbb{Z}/4)$ . We know that the image of the map  $PB_{2g+1} \to \operatorname{Sp}_{2g}(\mathbb{Z})$  is  $\operatorname{Sp}_{2g}(\mathbb{Z})[2]$ . Consider the inclusion

$$\operatorname{Sp}_{2g}(\mathbb{Z})[2] \hookrightarrow \operatorname{Sp}_{2g}(\mathbb{Z}).$$

We quotient the above inclusion by  $\operatorname{Sp}_{2q}(\mathbb{Z})[4]$ , and we get the following inclusion:

$$\mathfrak{sp}_{2q}(\mathbb{Z}/2) \hookrightarrow \operatorname{Sp}_{2q}(\mathbb{Z}/4).$$

We finally have

$$PB_{2g+1} \to \operatorname{Sp}_{2g}(\mathbb{Z})[2] \to \mathfrak{sp}_{2g}(\mathbb{Z}/2) < \operatorname{Sp}_{2g}(\mathbb{Z}/4)$$

Hence, the image of the map  $PB_{2g+1} \to \operatorname{Sp}_{2g}(\mathbb{Z}/4)$  is the abelian group  $\mathfrak{sp}_{2g}(\mathbb{Z}/2)$ . Thus, we have

$$PB_{2g+b}/B_{2g+b}[m] \cong \mathfrak{sp}_{2g}(\mathbb{Z}/2) \bigoplus_{i=1}^{\kappa} \operatorname{Sp}_{2g}(\mathbb{Z}/p_i).$$

For b = 2, the maps

$$PB_{2g+2} \to (\operatorname{Sp}_{2g+2}(\mathbb{Z})[2])_{y_{g+1}} \to \operatorname{Ann}(y_{g+1})$$

are both surjective, [9, Lemma 3.5]. But  $\operatorname{Ann}(y_{g+1}) < (\operatorname{Sp}_{2g+2}(\mathbb{Z}/4))_{y_{g+1}}$ , and thus, the image of the map

$$PB_{2g+2} \rightarrow (\operatorname{Sp}_{2g+2}(\mathbb{Z}/4))_{y_{g+1}}$$

is the group  $\operatorname{Ann}(y_{g+1})$ . Thus, we get

$$PB_{2g+2}/B_{2g+2}[m] \cong \operatorname{Ann}(y_{g+1}) \bigoplus_{i=1}^{k} (\operatorname{Sp}_{2g+2}(\mathbb{Z}/p_i))_{y_{g+1}}.$$

This completes the proof.

In order to find generators for  $B_{2g+1}[m]$ , it suffices to find a presentation for  $\operatorname{Sp}_{2g}(\mathbb{Z}/p)$  in terms of pure braids. In the next proposition we prove that  $\operatorname{Sp}_{2g}(\mathbb{Z}/p)$  admits a presentation as a quotient of the pure braid group over some relations. These new relations are the generators for  $B_{2g+1}[2p]$ . Recall that the generators of  $PB_n$  are defined to be  $a_{i,j} = \sigma_{j-1}...\sigma_{i+1}\sigma_i^2\sigma_{i+1}^{-1}...\sigma_{j-1}^{-1}$ , where  $1 \leq i < j \leq n$ .

**Proposition 5.3.** Fix a prime number p, and put p = 2k+1. Let  $H_n$  be the group with generators  $\{a_{i,j}\}$  with defining relations as follows:

- $PR1. \ a_{i,i+1}^k a_{i+1,i+2}^k a_{i,i+1}^k = a_{i+1,i+2}^k a_{i,i+1}^k a_{i+1,i+2}^k,$
- *PR2.*  $a_{i,j}^p = 1$ ,
- *PR3.*  $(a_{1,2}a_{1,3}a_{2,3})^2 = 1$  for p > 3,
- $PR4. \ \ a_{r,s}^{-1}a_{i,j}a_{r,s} = a_{i,j}, \ 1 \le r < s < i < j \le n \text{ or } 1 \le i < r < s < j \le n,$
- $PR5. \quad a_{r,s}^{-1}a_{i,j}a_{r,s} = a_{r,j}a_{i,j}a_{r,j}^{-1}, \ 1 \le r < s = i < j \le n,$
- $PR6. \ \ a_{r,s}^{-1}a_{i,j}a_{r,s} = (a_{i,j}a_{s,j})a_{i,j}(a_{i,j}a_{s,j})^{-1}, \ 1 \leq r = i < s < j \leq n,$

$$PR7. \quad a_{r,s}^{-1}a_{i,j}a_{r,s} = (a_{r,j}a_{s,j}a_{r,j}^{-1}a_{s,j}^{-1})a_{i,j}(a_{r,j}a_{s,j}a_{r,j}^{-1}a_{s,j}^{-1})^{-1}, \ 1 \le r < i < s < j \le n,$$

$$PR8. \ \ a_{i,j} = a_{j-1,j}^{k+1} a_{j-2,j-1}^{k+1} ... a_{i,i+1} a_{i+1,i+2}^k ... a_{j-1,j}^k, \ 1 < |i-j| \le n,$$

*PR9.*  $a_{1,2}a_{1,3}a_{2,3} = C$ , where

$$\begin{split} C &= (a_{1,2}^{(p+1)/4}a_{2,3}^2)^2, \text{ if } (p+1)/2 \text{ is even}, \\ C &= a_{1,2}^{(p+3)/4}a_{1,3}^2a_{1,2}^{(p-1)/4}a_{2,3}^2, \text{ if } (p+1)/2 \text{ is odd}. \end{split}$$

*PR10.*  $a_{1,2}a_{1,3}a_{1,4}a_{2,3}a_{2,4}a_{3,4} = Ba_{1,4}B^{-1}$ , where

$$B = a_{3,5}a_{4,5}a_{2,3}^{k/2}a_{3,4}^{-1}, \text{ if } k \text{ is even,}$$
  
$$B = a_{3,5}a_{4,5}a_{2,3}^{k+1}a_{3,4}, \text{ if } k \text{ is odd.}$$

If n = 2g + 1 then  $H_n$  is isomorphic to  $\operatorname{Sp}_{2g}(\mathbb{Z}/p)$ . On the other hand if n = 2g + 2, then  $H_n$  is isomorphic to  $\operatorname{Sp}_{2g+2}(\mathbb{Z}/p)_{y_{g+1}}$ .

Note that relations PR4, PR5, PR6, PR7 are relations in the presentation of the pure braid group given in Chapter 4. We begin with the group  $G_n$  defined in Theorem 4.1, and using Tietze transformations, we obtain the presentation of  $H_n$ .

*Proof.* By Theorem 4.1 the group  $G_n$  has the following presentation:

$$G_n = \langle \sigma_i | R1, R2, R3, R4, R5, R6 \rangle,$$

where  $1 \leq i < 2g+b$ . Let  $a_{i,j} = \sigma_{j-1}...\sigma_{i+1}\sigma_i^2\sigma_{i+1}^{-1}...\sigma_{j-1}^{-1}$  and denote this relation by *PR*11. Then include *PR*11 into the presentation of  $G_n$  and add the generator  $a_{i,j}$  to obtain

$$\langle \sigma_i, a_{i,j} | R1, R2, R3, R4, R5, R6, PR11 \rangle$$
.

Since  $PB_n$  is a subgroup of  $B_n$ , this means that R1 and R2 can be used to deduce the relations PR4, PR5, PR6, PR7.

$$\langle \sigma_i, a_{i,j} | R1, R2, R3, R4, R5, R6, PR4, PR5, PR6, PR7, PR11 \rangle$$

The relation R2 can be deduced by PR11 and R3 and PR4

 $\langle \sigma_i, a_{i,j} | R1, R3, R4, R5, R6, PR2, PR4, PR5, PR6, PR7, PR11 \rangle$ .

We derive two more relations from PR11 and R3.

$$\sigma_i = a_{i,i+1}^{k+1}, \quad \sigma_i^{-1} = a_{i,i+1}^k.$$

Then PR1 is equivalent to R1, PR2 is equivalent to R3, PR3 is equivalent to R4, PR9 is equivalent to R5, PR10 is equivalent to R6, and PR11 is equivalent to PR8. In other words,

 $\langle \sigma_i, a_{i,j} | PR1, PR2, PR4, PR5, PR6, PR7, PR8, PR9, PR10, \sigma_i = a_{i,i+1}^{k+1}, \sigma_i^{-1} = a_{i,i+1}^k \rangle$ 

Finally, for  $1 \le i < j \ge 2g + b$  we have that

$$\langle a_{i,i} | PR1, PR2, PR4, PR5, PR6, PR7, PR8, PR9, PR10 \rangle$$

which is the presentation of  $H_n$ .

As an application of Proposition 5.3, we can obtain generators for  $B_{2g+b}[2p]$ .

**Corollary 5.4.** For k = (p-1)/2, the group  $B_{2g+b}[2p]$  is normally generated by six types of elements:

n

$$\begin{aligned} a_{i,j}^{P}, \\ &(a_{1,2}a_{1,3}a_{2,3})^{2}, \\ &a_{1,2}a_{1,3}a_{2,3}C^{-1}, \\ &a_{1,2}a_{1,3}a_{2,3}a_{2,4}a_{3,4}Ba_{1,4}^{-1}B^{-1}, \\ &a_{i,i+1}a_{i+1,i+2}^{k}a_{i,i+1}^{k}a_{i+1,i+2}^{-k}a_{i,i+1}a_{i+1,i+2}^{-k}, \\ &a_{j-1,j}^{k}a_{j-2,j-1}^{k+1}...a_{i,i+1}a_{i+1,i+2}^{k}...a_{j-1,j}^{k}a_{i,j}^{-1}. \end{aligned}$$

Actually we can use Proposition 5.3 to find normal generators for any  $B_n[m]$ , where m is either  $2p_1...p_k$  or  $4p_1...p_k$  and  $p_i \ge 3$  are prime numbers.

## 6 Symmetric quotients of congruence subgroups

In this section we explore factor groups of congruence subgroups of braid groups. From Section 3 we know that  $B_n[2] \cong PB_n$  and  $B_n/B_n[2] \cong S_n$ . In the next theorem we generalize the latter isomorphism.

**Theorem 6.1.** The quotient  $B_n[p]/B_n[2p]$  is isomorphic to  $S_n$ .

Before we proceed to the proof of Theorem 6.1, we will prove the following lemma.

**Lemma 6.2.** The groups  $B_n[2p]$  and  $B_n[2] \cap B_n[p]$  are isomorphic.

*Proof.* It is obvious that  $B_n[2p] < B_n[2] \cap B_n[p]$ . By Proposition 3.3 we have the decomposition  $\operatorname{Sp}_{2g}(\mathbb{Z}/2p) = \operatorname{Sp}_{2g}(\mathbb{Z}/2) \oplus \operatorname{Sp}_{2g}(\mathbb{Z}/p)$ . By the homomorphism  $\rho : B_n \to \operatorname{Sp}_{2g}(\mathbb{Z}/2p)$  we deduce that  $\rho(B_n[2] \cap B_n[p])$  is trivial. Hence  $B_n[2] \cap B_n[p] < B_n[2p]$ .

Now we can prove the main theorem of the section.

Proof of Theorem 6.1. Denote by  $s_i$  the transposition i, i + 1, that is, the generators of  $S_n$ . We have the following presentation.

$$S_n = \langle s_1, \dots, s_{n-1} \mid s_i^2 = 1, s_i s_{i+1} s_i = s_{i+1} s_i s_{i+1}, s_i s_j = s_j s_i \text{ when } |i-j| > 1 \rangle.$$

Consider the natural epimorphism  $\tau : B_n \to S_n$  defined by  $\tau(\sigma_i) = s_i$ . Fix a prime number p > 2; then the restriction  $\tau : B_n[p] \to S_n$  is a surjective homomorphism as well. Indeed, we have that  $\tau(\sigma_i^p) = s_i^p = s_i$ , and for any other generator  $g \in B_n[p]$  we have  $\tau(g) = 1$ . Finally,  $\ker(\tau) = B_n[2] \cap B_n[p] = B_n[2p]$  by Lemma 6.2.

### References

- N. A'Campo. Tresses, monodromie et le groupe symplectique. Comment. Math. Helv., 54(2):318–327, 1979.
- [2] V. I. Arnol'd. A remark on the branching of hyperelliptic integrals as functions of the parameters. Funkcional. Anal. i Priložen., 2(3):1–3, 1968.
- [3] Mamoru Asada. The faithfulness of the monodromy representations associated with certain families of algebraic curves. *Journal of Pure and Applied Algebra*, 159(23):123 147, 2001.
- [4] J. Assion. Einige endliche Faktorgruppen der Zopfgruppen. Math. Z., 163(3):291–302, 1978.
- [5] J. S. Birman. Braids, links, and mapping class groups. Princeton University Press, Princeton, N.J.; University of Tokyo Press, Tokyo, 1974. Annals of Mathematics Studies, No. 82.
- [6] J. S. Birman and T. E. Brendle. Braids: a survey. In *Handbook of knot theory*, pages 19–103. Elsevier B. V., Amsterdam, 2005.
- [7] J. S. Birman and H. M. Hilden. On the mapping class groups of closed surfaces as covering spaces. In Advances in the theory of Riemann surfaces (Proc. Conf., Stony Brook, N.Y., 1969), pages 81–115. Ann. of Math. Studies, No. 66. Princeton Univ. Press, Princeton, N.J., 1971.
- [8] Joan S. Birman. On siegel's modular group. Mathematische Annalen, 191(1):59–68, 1971.
- [9] T. Brendle and D. Margalit. The level four braid group. Journal fr die reine und angewandte Mathematik (Crelles Journal).
- [10] Tara Brendle and Dan Margalit. Point pushing, homology, and the hyperelliptic involution. Michigan Math. J., 62(3):451–473, 09 2013.
- [11] Tara Brendle, Dan Margalit, and Andrew Putman. Generators for the hyperelliptic Torelli group and the kernel of the Burau representation at t = -1. Invent. Math., 200(1):263–310, 2015.
- [12] Tara E. Brendle and Dan Margalit. Factoring in the hyperelliptic torelli group. Mathematical Proceedings of the Cambridge Philosophical Society, 159(2):207–217, September 2015.
- [13] Thomas Church and Andrew Putman. Generating the Johnson filtration. Geom. Topol., 19(4):2217–2255, 2015.
- [14] H.S.M. Coxeter. Factor groups of the braid group. pages 95–122, 1957.
- [15] B. Farb and D. Margalit. A Primer on Mapping Class Groups (PMS-49). Princeton Mathematical Series. Princeton University Press, 2011.
- [16] Louis Funar and Toshitake Kohno. On burau's representations at roots of unity. Geom. Dedicata, 169:145–163, 2014.
- [17] J. Gambaudo and E. Ghys. Braids and signatures. Bull. Soc. Math. France, 133(4):541–579, 2005.

- [18] Richard Hain. Finiteness and torelli spaces. Problems on Mapping Class Groups and Related Topics, pages 59–73, 2005.
- [19] Stephen P. Humphries. Normal closures of powers of dehn twists in mapping class groups. Glasgow Mathematical Journal, 34:314–317, 9 1992.
- [20] Stephen P. Humphries. Subgroups of pure braid groups generated by powers of dehn twists. Rocky Mountain J. Math., 37(3):801–828, 06 2007.
- [21] Wilhelm Magnus, Abraham Karrass, and Donald Solitar. Combinatorial group theory. Dover Publications, Inc., Mineola, NY, second edition, 2004. Presentations of groups in terms of generators and relations.
- [22] B. McReynolds. The congruence subgroup problem for braid groups: Thurston's proof. New York J. Math, 18:925–942, 2012.
- [23] M. Newman and J. R. Smart. Symplectic modulary groups. Acta Arith, 9:83–89, 1964.
- [24] B. Perron and J. P. Vannier. Groupe de monodromie géométrique des singularités simples. Mathematische Annalen, 306(1):231–245, 1996.
- [25] Jerome Powell. Two theorems on the mapping class group of a surface. Proceedings of the American Mathematical Society, 68(3):347–350, 1978.
- [26] Andrew Putman. Cutting and pasting in the Torelli group. Geom. Topol., 11:829–865, 2007.
- [27] B. Wajnryb. A braidlike presentation of Sp(n, p). Israel J. Math., 76(3):265–288, 1991.

Charalampos Stylianakis, department of Mathematics & Statistics, University of Glasgow, Glasgow, G12 8QW, UK.

E-mail address: c.stylianakis.1@research.gla.ac.uk