CENTRALIZERS OF CENTRALIZERS OF PARABOLIC SUBGROUPS OF BRAID GROUPS

DAVID GARBER, ARKADIUS KALKA, ERAN LIBERMAN AND MINA TEICHER

Abstract. We characterize the centralizer of the centralizer of all parabolic subgroups of the braid group having connected associated Coxeter graphs. We apply this result to provide a new and potentially more efficient solution to the subgroup conjugacy problem for these parabolic subgroups.

1. Introduction

Fenn, Rolfsen and Zhu [FRZ96] determined the centralizer of the standard parabolic subgroup $B_m$ in the braid group $B_n$ ($m < n$) [Ar47]. This result was generalized by Paris [Pa97] who computed generating sets for the centralizer of parabolic subgroups having connected associated Coxeter graphs for Artin groups of type $A$, $B$ and $D$.

In this paper, we characterize the centralizer of the centralizer (also called double centralizer) of a parabolic subgroup $H$ of $B_n$ with a connected associated Coxeter graph, namely we show that $C_{B_n}(C_{B_n}(H)) = Z(B_n) \cdot H$, where $Z(B_n)$ denotes the center of the braid group $B_n$.

Furthermore, we apply this result to the subgroup conjugacy problem for such parabolic subgroups of $B_n$. The conjugacy problem in the braid group $B_n$ was solved in the seminal paper of Garside [Ga69]. A more general problem is the subgroup conjugacy problem for $H \leq B_n$: given two elements $x, y \in B_n$, and a subgroup $H \leq B_n$, decide whether $x$ and $y$ are conjugated by an element in $H$. In general, this problem is presumably undecidable, because $F_2 \times F_2$ can be embedded in $B_n$ for $n \geq 5$ (where $F_2$ is the free group on two generators), and for $F_2 \times F_2$, according to a result of Mihailova [Mi58], even the subgroup membership (or generalized word) problem is unsolvable. Nevertheless, it is interesting to consider the subgroup conjugacy problem for particular natural subgroups of $B_n$. Indeed, even the subgroup conjugacy problem for the natural embedded subgroups $B_m \leq B_n$, for $m \leq n$, has been open for $m \leq n - 2$ until [KLT10].

2010 Mathematics Subject Classification. 20F36.

Key words and phrases. Braid group, centralizer, parabolic subgroup, double centralizer, subgroup conjugacy problem.
case $m = n - 1$ was resolved in [KLT09], which was of particular interest, since the so-called *shifted conjugacy problem* [De06], which was also unknown to be solvable [Det06, LU08, LU09], is equivalent to some subgroup conjugacy problem for $B_{n-1}$ in $B_n$ [LU08, KLT09]. In [KLT09], the subgroup conjugacy problem for $B_{n-1} \leq B_n$ was transformed to an equivalent bisimultaneous conjugacy problem. Then, in [KLT10], the subgroup conjugacy problem for all parabolic subgroups of braid groups, even for all so-called Garside subgroups [Go07] of Garside groups, was solved completely, and deterministic algorithms were provided. The solution in [KLT10] does not resort to a detour via a simultaneous conjugacy problem, but there we cannot apply any cycling and decycling operations (see [EM94]). Therefore, the invariant subsets of the conjugacy class are quite large.

In this paper, we provide a second solution of the subgroup conjugacy problem for parabolic subgroups of $B_n$ having a connected associated Coxeter graph. This solution is a generalization of the approach developed in [KLT09], namely we reduce the problem to an instance of a simultaneous conjugacy problem. Also the invariant subsets of the simultaneous conjugacy class involved in Lee and Lee’s solution [LL02] are relatively big. In [KTV14], we introduce new much smaller invariant subsets of the simultaneous conjugacy class, namely the so-called *Lexicographic Super Summit Sets*. Using these new improved invariant subsets, our new approach to the subgroup conjugacy problem for parabolic subgroups of $B_n$ with a connected associated Coxeter graph, given in Corollary 5.4, is expected to be more efficient than the direct solution (using fractional normal forms) from [KLT10].

Though the subgroup conjugacy problem for standard parabolic subgroups of the braid groups deserves interest on its own, a particular motivation comes from applications in cryptography. Indeed, Dehornoy [De06] proposed an authentication scheme based on the shifted conjugacy problem. We remark that, by using generalized shifted conjugacy operations, it is straightforward to construct shifted conjugacy problems which can be reduced to some subgroup conjugacy problem for $B_m \leq B_n$. Furthermore, the Diffie-Hellman public key exchange based on the braid group, introduced by Ko et al. [KL+00], relies on the subgroup conjugacy problem for $B_m \leq B_n$. Though Gebhardt broke this cryptosystem in [Ge06] with 100% success rate, using his ultra summit sets, introduced in [Ge05], we have to point out that he did not provide a general solution to the subgroup conjugacy problem for $B_m \leq B_n$.

Remark 1.1. As a further application of our main theorem on centralizers of centralizers, we mention the first deterministic solution to the double coset problem for parabolic subgroups (with a connected associated Coxeter graph) of braid groups (see also [KTT14]).
Outline. Section 2 deals with generating sets of the centralizer of $\Delta^2_r$ in $B_n$. We simplify Gurzo’s generating sets in order to determine the algebraic structure of these centralizers. For the convenience of the reader, we include in Section 3 a solution to the subgroup conjugacy problem for $B_{n-2}$ in $B_n$, where we introduce the basic ideas which will be used in greater generality in the subsequent two sections. Then, Section 4 describes the main result concerning centralizers of parabolic subgroups. Finally, Section 5 contains the application to the subgroup conjugacy problem for these subgroups.

2. Gurzo’s Presentation

We use the following definitions. Let $\partial : B_\infty \rightarrow B_\infty$ be the injective shift homomorphism, defined by $\sigma_i \mapsto \sigma_{i+1}$.

**Definition 2.1.** ([De00, Definition I.4.6.]) For $n \geq 2$, define $\delta_n = \sigma_n^{-1} \cdots \sigma_2 \sigma_1$. For $p, q \geq 1$, we set:

$$\tau_{p,q} = \delta_{p+1} \partial(\delta_{p+1}) \cdots \partial^{q-1}(\delta_{p+1}),$$

i.e. the strands $p+1, \ldots, p+q$ cross over the strands $1, \ldots, p$ (see Figure 1).

![Figure 1. $\tau_{p,q}$](image1)

In particular, for $k \geq 0$ and $l \geq 1$ we denote (see Figures 2 and 3):

$$\bar{b}_{[k+1,k+l],1} = \tau_{k,l} \tau_{1,k} \quad \text{and} \quad \bar{b}_{k+1,1} = \bar{b}_{[k+1,k+1],1} = \tau_{k,1} \tau_{1,k}.$$

![Figure 2. $\bar{b}_{[k+1,k+l],1}$](image2)

According to Gurzo [Gu85], for $1 \leq r \leq n-1$, the centralizer or $\Delta^2_r$ is given by:
Proposition 2.2.

\[ C_{B_n}(\Delta^2_r) = B_r \cdot \langle \sigma_{r+1}, \ldots, \sigma_{n-1}, \bar{b}_{r+1,1}, \bar{b}_{[r+1,r+2],1}, \ldots, \bar{b}_{[r+1,n],1} \rangle. \]

Using Nielsen transformations we may simplify this generating set so that we obtain the complete algebraic structure of that centralizer and hence a presentation.

Proposition 2.3. For \( 1 \leq r \leq n-1 \), the centralizer \( C_{B_n}(\Delta^2_r) \) is isomorphic to the direct product of the Artin groups of type \( A_{r-1} \) and \( B_{n-r} \). In particular, we have:

\[ C_{B_n}(\Delta^2_r) = B_r \cdot \langle \bar{b}_{r+1,1}, \sigma_{r+1}, \ldots, \sigma_{n-1} \rangle \cong A(A_{r-1}) \times A(B_{n-r}). \]

Proof. For all \( 2 \leq l \leq n-r \), we have \( \Delta^2_{r+l} = \bar{b}_{[r+1,r+l],1} \cdot \Delta_r^2 \cdot \partial^r(\Delta^2_r) \) (see Figure 4).

![Figure 4](image-url)

**Figure 4.** Decompose \( \Delta^2_{r+l} \) as \( \bar{b}_{[r+1,r+l],1} \cdot \Delta_r^2 \cdot \partial^r(\Delta^2_r) \).

Since \( \Delta^2_r \in B_r \) and \( \partial^r(\Delta^2_r) \in \langle \sigma_{r+1}, \ldots, \sigma_{n-1} \rangle \), we may replace, for \( 2 \leq l \leq n-r \), the elements \( \bar{b}_{[r+1,r+l],1} \) by the elements \( \Delta^2_{r+l} \) in the generating set. Thus, we get:

\[ C_{B_n}(\Delta^2_r) = B_r \cdot \langle \sigma_{r+1}, \ldots, \sigma_{n-1}, \bar{b}_{r+1,1}, \Delta^2_{r+2}, \ldots, \Delta^2_{n} \rangle. \]

Starting with \( \Delta^2_{r+1} = \Delta_r^2 \bar{b}_{r+1,1} \) (see Figure 5), we may prove by induction that, for \( 2 \leq l \leq n-r \),

\[ \Delta^2_{r+l} = \Delta_r^2 \bar{b}_{r+1,1} \bar{b}_{r+2,1} \cdots \bar{b}_{r+l,1}, \]

where all factors commute on the right hand side. Furthermore, starting with \( \bar{b}_{r+2,1} = \sigma_{r+1} \cdot \bar{b}_{r+1,1} \cdot \sigma_{r+1} \), we may prove by induction that, for \( 2 \leq l \leq n-r \) (see Figure 6):

\[ \bar{b}_{r+l,1} = \sigma_{r+l-1} \cdots \sigma_{r+1} \cdot \bar{b}_{r+1,1} \cdot \sigma_{r+1} \cdots \sigma_{r+l-1}. \]

Thus, we may express, for all \( 2 \leq l \leq n-r \), the elements \( \Delta^2_{r+l} \) as words over \( \bar{b}_{r+1,1}, \sigma_{r+1}, \ldots, \sigma_{n-1} \) only, and hence, we may eliminate them from the generating set. Therefore, we have proven that:

\[ C_{B_n}(\Delta^2_r) = B_r \cdot \langle \bar{b}_{r+1,1}, \sigma_{r+1}, \ldots, \sigma_{n-1} \rangle. \]
Consider the map \( B_n \rightarrow B_{n-r+1} \) which removes all but one of the strands 1, \ldots, r, say, all except for strand 1. This map is not a homomorphism, but the restriction \( \eta : \langle \bar{b}_{r+1,1}, \sigma_{r+1}, \ldots, \sigma_{n-1} \rangle \rightarrow B_{n-r+1} \) is an injective homomorphism with image \( \langle \sigma_1^2, \sigma_2, \ldots, \sigma_{n-r} \rangle \). Consider the Artin group \( A(B_{n-r}) \) generated by \( s_1, \ldots, s_{n-r} \) where \( s_1 \) and \( s_2 \) satisfy the 4-relation. A standard embedding \( \iota \) of this \( B \)-type Artin group into the braid group \( B_{n-r+1} \) is given by \( s_1 \mapsto \sigma_1^2 \) and \( s_i \mapsto \sigma_i \) for \( 2 \leq i \leq n-r \). Hence \( \eta^{-1} \circ \iota : A(B_{n-r}) \rightarrow \langle \bar{b}_{r+1,1}, \sigma_{r+1}, \ldots, \sigma_{n-1} \rangle \) is an isomorphism. Since \( B_r \cong A(A_{r-1}) \) commutes with \( \langle \bar{b}_{r+1,1}, \sigma_{r+1}, \ldots, \sigma_{n-1} \rangle \), we conclude that:

\[
C_{B_n}(\Delta_r^2) = B_r \cdot \eta^{-1} \circ \iota(A(B_{n-r})) \cong A(A_{r-1}) \times A(B_{n-r}).
\]

\( \square \)

**Remark 2.4.** Since it it obvious which relations are fulfilled, we will call in the sequel \( B_r \cdot \langle \bar{b}_{r+1,1}, \sigma_{r+1}, \ldots, \sigma_{n-1} \rangle \) *Gurzo’s presentation* of \( C_{B_n}(\Delta_r^2) \).

**3. The subgroup conjugacy problem for \( B_{n-2} \) in \( B_n \)**

We start with the following result concerning the centralizer of \( \Delta_{n-2}^2 \):
Lemma 3.1.

\[ B_{n-1} \cap C_{B_n}(\Delta^2_{n-2}) = B_{n-2} \cdot \langle \bar{b}_{n-1,1} \rangle = B_{n-2} \cdot \langle \Delta^2_{n-1} \rangle. \]

Proof. We start with the left equality. According to Gurzo’s presentation (Proposition 2.3 for \( r = n - 2 \)), we have:

\[ C_{B_n}(\Delta^2_{n-2}) = B_{n-2} \cdot \langle \bar{b}_{n-1,1}, \sigma_{n-1} \rangle. \]

It suffices to show that \( B_{n-1} \cap \langle \bar{b}_{n-1,1}, \sigma_{n-1} \rangle = \langle \bar{b}_{n-1,1} \rangle \). Indeed, since \( \bar{b}_{n-1,1} \in B_{n-1} \) it suffices to show the inclusion \( B_{n-1} \cap \langle \bar{b}_{n-1,1}, \sigma_{n-1} \rangle \subseteq \langle \bar{b}_{n-1,1} \rangle \). Let \( \beta \in B_{n-1} \cap \langle \bar{b}_{n-1,1}, \sigma_{n-1} \rangle \). Recall from the proof of Theorem 2.3 (for \( r = n - 2 \)) the map \( \eta \) which removes the strands 2, \ldots, \( n - 2 \). Hence, \( \eta(\beta) \) lies in \( \eta(B_{n-1} \cap \langle \bar{b}_{n-1,1}, \sigma_{n-1} \rangle) \subseteq \eta(B_{n-1}) \cap \eta(\langle \bar{b}_{n-1,1}, \sigma_{n-1} \rangle) = B_2 \cap \langle \sigma_1^2, \sigma_2 \rangle \).

Now, \( \eta(\beta) \in B_2 \) implies that there exists \( k \in \mathbb{Z} \) such that \( \eta(\beta) = \sigma_1^k \). Since \( \eta(\beta) \) also lies in \( \langle \sigma_1^2, \sigma_2 \rangle \) we may conclude that \( k \) is even, i.e., \( k = 2k' \) for some \( k' \in \mathbb{Z} \). Recall that \( \langle \sigma_1^2, \sigma_2 \rangle \) is the braid group on three strands which fixes the first strand, namely \( \langle \alpha \in B_3 \mid \nu(\alpha)(1) = 1 \rangle \) (see Figure 7), where \( \nu \) denotes the natural homomorphism which maps each braid to its induced permutation on the strands, i.e. \( \nu : \sigma_i \mapsto (i, i + 1) \). Therefore, we may view \( \langle \sigma_1^2, \sigma_2 \rangle \) as the 2-strand braid group of the annulus [Cr99]. However, for odd \( k \), we have \( \nu(\sigma_1^k)(1) = 2 \), contradicting \( \nu(\beta)(1) = 1 \).

\[
\begin{array}{c}
\sigma_1^2 \\
\sigma_2
\end{array}
\]

Figure 7. Generators of \( \langle \alpha \in B_3 \mid \nu(\alpha)(1) = 1 \rangle \)

Thus, we have shown that \( B_2 \cap \langle \sigma_1^2, \sigma_2 \rangle = \langle \sigma_1^2 \rangle \). For the braids in question, \( \eta \) is an isomorphism. Thus we may apply \( \eta^{-1} \), and we obtain

\[ B_{n-1} \cap \langle \bar{b}_{n-1,1}, \sigma_{n-1} \rangle \subseteq \eta^{-1}(\langle \sigma_1^2 \rangle) = \langle \bar{b}_{n-1,1} \rangle, \]

as needed.

The right equality follows from simple Nielsen transformations. Since \( \Delta^2_{n-1} \) generates the center of \( B_{n-1} \) and \( \Delta^2_{n-2} \in B_{n-1} \), we can write:

\[ B_{n-1} \cap C_{B_n}(\Delta^2_{n-2}) \cong \langle B_{n-2}, \bar{b}_{n-1,1} \rangle \cong \langle B_{n-2}, \bar{b}_{n-1,1}, \Delta^2_{n-1} \rangle. \]

Now, since \( \bar{b}_{n-1,1} = \Delta^2_{n-1} \Delta^{-2}_{n-2} \) and \( \Delta^{-2}_{n-2} \in B_{n-2} \), we can omit \( \bar{b}_{n-1,1} \) from the last presentation, and hence we get:

\[ B_{n-1} \cap C_{B_n}(\Delta^2_{n-2}) \cong \langle B_{n-2}, \bar{b}_{n-1,1}, \Delta^2_{n-1} \rangle \cong \langle B_{n-2}, \Delta^2_{n-1} \rangle. \]
Proposition 3.2. For all $x, y \in B_n$, the following are equivalent:

1. There exists $c \in B_{n-2}$ satisfying $y = c^{-1}xc$.
2. There exists $z \in B_n$ satisfying:
   a. $y = z^{-1}xz$
   b. $\Delta^2_{n-1} = z^{-1}\Delta^2_{n-1}z$
   c. $\Delta^2_{n-2} = z^{-1}\Delta^2_{n-2}z$
   d. $\sigma_{n-1}^2 = z^{-1}\sigma_{n-1}z$.

Proof. Since any element in $B_{n-2}$ commutes with $\Delta^2_{n-1}$, $\Delta^2_{n-2}$ and $\sigma_{n-1}$, the implication $(1) \Rightarrow (2)$ is obvious.

Due to Proposition 3 in [KLT09], Conditions (a) and (b) imply that $z = \Delta^2_n c$ where $c \in B_{n-1}$. Hence, $c = \Delta^2_n z$.

Condition (c) implies that $z \in C_{B_n}(\Delta^2_{n-2})$, hence also $c \in C_{B_n}(\Delta^2_{n-2})$. Hence $c \in B_{n-1} \cap C_{B_n}(\Delta^2_{n-2})$. By Lemma 3.1, $c \in \langle B_{n-2}, \Delta^2_{n-1} \rangle$, so we can write: $c = \Delta^2_{n-1} c'$ where $c' \in B_{n-2}$. For finishing the proof, we have to show that $q = 0$.

We have: $z = \Delta^2_n c = \Delta^2_n \Delta^2_{n-1} c'$. So $\Delta^2_{n-1} = \Delta^2_n \Delta^2_{n-1} c'$. Obviously, $\Delta^2_{n-2} = C_{B_n}(\sigma_{n-1})$. By Condition (d), we have $z \in C_{B_n}(\sigma_{n-1})$, and by the construction $c' \in B_{n-2}$ and hence $c' \in C_{B_n}(\sigma_{n-1})$. Therefore, $\Delta^2_{n-1} = \Delta^2_n \Delta^2_{n-1} c'$. It is easy to proof by induction that the left greedy normal forms in $[\text{Th92, EM94}]$ of $\Delta^2_{n-1} \sigma_{n-1}$ and $\sigma_{n-1} \Delta^2_{n-1}$ are

\[
\underbrace{\Delta_{n-1} \cdots \Delta_{n-1}}_{2q-1 \text{ factors}} \cdot (\Delta_{n-1} \sigma_{n-1}) \quad \text{and} \quad (\sigma_{n-1} \Delta_{n-1}) \cdot \underbrace{\Delta_{n-1} \cdots \Delta_{n-1}}_{2q-1 \text{ factors}},
\]

respectively. We conclude that $\Delta^2_{n-1} \notin C_{B_n}(\sigma_{n-1})$ for $q \neq 0$, and since we have $\Delta^2_{n-1} \in C_{B_n}(\sigma_{n-1})$, it implies that $q = 0$, as needed.

4. The centralizer of the centralizer for a parabolic subgroup of $B_n$

Now, we pass to the general case. We need the following result concerning the centralizer of $\Delta^2_n$:

Lemma 4.1. The following holds for all $1 \leq r \leq n - 1$:

\[
B_{r+1} \cap C_{B_n}(\Delta^2_r) = B_r \cdot \langle \bar{b}_{r+1,1} \rangle = B_r \cdot \langle \Delta^2_{r+1} \rangle.
\]

Proof. The proof is a straightforward generalization of the proof of Lemma 3.1. Nevertheless, we provide full details for the convenience of the reader. We start with the left equality. According to Gurzo's presentation (Proposition 2.3), we have:

\[
C_{B_n}(\Delta^2_r) = B_r \cdot \langle \bar{b}_{r+1,1}, \sigma_{r+1}, \ldots, \sigma_{n-1} \rangle.
\]
It suffices to show that $B_{r+1} \cap \langle \bar{b}_{r+1,1}, \sigma_{r+1}, \ldots, \sigma_{n-1} \rangle = \langle \bar{b}_{r+1,1} \rangle$. Indeed, since $\bar{b}_{r+1,1} \in B_{r+1}$ it suffices to show the inclusion $B_{r+1} \cap \langle \bar{b}_{r+1,1}, \sigma_{r+1}, \ldots, \sigma_{n-1} \rangle \subseteq \langle \bar{b}_{r+1,1} \rangle$. Let $\beta \in B_{r+1} \cap \langle \bar{b}_{r+1,1}, \sigma_{r+1}, \ldots, \sigma_{n-1} \rangle$. Consider the map $\eta$ which removes the strands $2, \ldots, r$. Hence, $\eta(\beta)$ lies in

$$\eta(B_{r+1} \cap \langle \bar{b}_{r+1,1}, \sigma_{r+1}, \ldots, \sigma_{n-1} \rangle) \subseteq \eta(B_{r+1}) \cap \eta(\langle \bar{b}_{r+1,1}, \sigma_{r+1}, \ldots, \sigma_{n-1} \rangle) = B_2 \cap \langle \sigma_1^2, \sigma_2, \ldots, \sigma_{n-r} \rangle.$$

Now, $\eta(\beta) \in B_2$ implies that there exists $k \in \mathbb{Z}$ such that $\eta(\beta) = \sigma_1^k$. Since $\eta(\beta)$ also lies in $\langle \sigma_1^2, \sigma_2, \ldots, \sigma_{n-r} \rangle$, we may conclude that $k$ is even, i.e., $k = 2k'$ for some $k' \in \mathbb{Z}$. Recall, that $\langle \sigma_1^2, \sigma_2, \ldots, \sigma_{n-r} \rangle$ is the braid group on $n-r+1$ strands which fixes the first strand, namely $\langle \alpha \in B_{n-r+1} \mid \nu(\alpha)(1) = 1 \rangle$, where $\nu$ denotes the natural homomorphism which maps each braid to its induced permutation on the strands, i.e. $\nu : \sigma_i \mapsto (i, i+1)$. Therefore, we may view $\langle \sigma_1^2, \sigma_2, \ldots, \sigma_{n-r} \rangle$ as the $(n-r)$-strand braid group of the annulus $\Delta^2_{n-r}$. However, for odd $k$, we have $\nu(\sigma_1^k)(1) = 2$, contradicting $\nu(\beta)(1) = 1$.

Thus, we have shown that $B_2 \cap \langle \sigma_1^2, \sigma_2, \ldots, \sigma_{n-r} \rangle = \langle \sigma_1^2 \rangle$. For the braids in question, $\eta$ is an isomorphism. Thus we may apply $\eta^{-1}$, and we obtain

$$B_{r+1} \cap \langle \bar{b}_{r+1,1}, \sigma_{r+1}, \ldots, \sigma_{n-1} \rangle \subseteq \eta^{-1}(\langle \sigma_1^2 \rangle) = \langle \bar{b}_{r+1,1} \rangle,$$

as needed.

The right equality follows from simple Nielsen transformations. \hfill \qed

Remark 4.2. Given a group word over $\{\bar{b}_{r+1,1}, \sigma_{r+1}, \ldots, \sigma_{n-1}\}$ representing an element in $B_{r+1}$, one may find a word over $\{\bar{b}_{r+1,1}\}$ only, either by applying the map $\eta$ as explained above, or one computes the fractional (left) normal form $[\text{Th92}]$ in the $B$-type Artin group $\langle \bar{b}_{r+1,1}, \sigma_{r+1}, \ldots, \sigma_{n-1} \rangle$. Fractional normal forms detect the standard parabolic subgroup in which an element of a finite type Artin group "lives". This generalizes to Garside subgroups of Garside groups $[\text{Go07}]$.

Lemma [4.1] allows us to prove the following crucial result about centralizers:

**Proposition 4.3.** For $1 \leq K \leq n-m$, we have:

$$\bigcap_{k=1}^{K} [C_{B_n}(\Delta^2_{n-k}) \cap C_{B_n}(\sigma_n)] = \langle \Delta^2_{n}, B_{n-K} \rangle,$$

where we define $\sigma_n := 1$ and therefore $C_{B_n}(\sigma_n) = B_n$.

**Proof.** We prove the theorem by induction on $K$. For $K = 1$, according to Gurzo’s presentation, we have:

$$C_{B_n}(\Delta^2_{n-1}) \cap C_{B_n}(\sigma_n) = C_{B_n}(\Delta^2_{n-1}) = \langle B_{n-1}, \bar{b}_{n,1} \rangle = \langle B_{n-1}, \bar{b}_{n,1}, \Delta^2_{n} \rangle = \langle \Delta^2_{n}, B_{n-1} \rangle.$$

The inductive hypothesis is thus verified for $K = 1$. Suppose the result holds for $K = k$, and we wish to prove it for $K = k+1$. Then, for $K = k+1$, we have:

$$\bigcap_{k=1}^{k+1} [C_{B_n}(\Delta^2_{n-k}) \cap C_{B_n}(\sigma_n)] = \langle \Delta^2_{n}, B_{n-(k+1)} \rangle = \langle \Delta^2_{n}, B_{n-k-1} \rangle = \bigcap_{k=1}^{k} [C_{B_n}(\Delta^2_{n-k}) \cap C_{B_n}(\sigma_n)].$$

Thus, by induction, the result holds for any $K$. \hfill \qed
The last equality holds since \( \tilde{b}_{n,1} = \Delta_n^2 \Delta_{n-1}^2 \in \langle \Delta_n^2, B_{n-1} \rangle \).

Now, assume that the equality holds for \( K \) satisfying \( 1 \leq K < n - m \), and we want to prove it for \( K + 1 \). We start by proving the following inclusion:

\[
\bigcap_{k=1}^{K+1} \left[ C_{B_n}(\Delta_{n-k}^2) \cap C_{B_n}(\sigma_{n-k+1}) \right] \subseteq \langle \Delta_n^2 \rangle \cdot B_{n-K-1}
\]

We have:

\[
\bigcap_{k=1}^{K+1} \left[ C_{B_n}(\Delta_{n-k}^2) \cap C_{B_n}(\sigma_{n-k+1}) \right] = \left( \bigcap_{k=1}^{K} \left[ C_{B_n}(\Delta_{n-k}^2) \cap C_{B_n}(\sigma_{n-k+1}) \right] \right) \cap C_{B_n}(\Delta_{n-K}^2) \cap C_{B_n}(\sigma_{n-K}) = \langle \Delta_n^2, B_{n-K} \rangle \cap C_{B_n}(\Delta_{n-K-1}^2) \cap C_{B_n}(\sigma_{n-K}),
\]

where the last equality is by the induction hypothesis. Now, if \( z \in \bigcap_{k=1}^{K+1} \left[ C_{B_n}(\Delta_{n-k}^2) \cap C_{B_n}(\sigma_{n-k+1}) \right] \), then \( z \in \langle \Delta_n^2 \rangle \cdot B_{n-K} \), hence there exist \( c \in B_{n-K} \) and \( p \in \mathbb{Z} \) such that \( z = \Delta_n^{2p}c \).

Since \( z \in C_{B_n}(\Delta_{n-K-1}^2) \) and \( z = \Delta_n^{2p}c \), then \( c \in C_{B_n}(\Delta_{n-K-1}^2) \) too. So \( c \in B_{n-K} \cap C_{B_n}(\Delta_{n-K-1}^2) \) \( \text{Lemma} \) \( B_{n-K-1} \cdot \langle \Delta_n^2 \rangle \).

Hence, there exist \( c' \in B_{n-K-1} \) and \( q \in \mathbb{Z} \) such that \( c = \Delta_n^{2q}c' \). Therefore,

\[
z = \Delta_n^{2q}c' = \Delta_n^{2p} \Delta_n^{2q}c' \text{. Equivalently: }
\]

\[
\Delta_n^{2q} = \Delta_n^{-2p}z \cdot (c')^{-1}.
\]

Recall again that \( z \in \langle \Delta_n^2, B_{n-K} \rangle \cap C_{B_n}(\Delta_{n-K-1}^2) \cap C_{B_n}(\sigma_{n-K}) \), hence: \( z \in C_{B_n}(\sigma_{n-K}) \). Also \( c' \in B_{n-K-1} \), so: \( c' \in C_{B_n}(\sigma_{n-K}) \). Obviously: \( \Delta_n^{-2p} \in C_{B_n}(\sigma_{n-K}) \). Therefore: \( \Delta_n^{2q} \in C_{B_n}(\sigma_{n-K}) \), and hence \( q = 0 \) (since \( \Delta_n^{n-K} \neq \sigma_{n-K} \neq 1 \) for \( i \neq 0 \)).

So we get \( z = \Delta_n^{2p}c' \) where \( c' \in B_{n-K-1} \). Therefore: \( z \in \langle \Delta_n^2 \rangle \cdot B_{n-K-1} \). Since

\[
z \in \bigcap_{k=1}^{K+1} \left[ C_{B_n}(\Delta_{n-k}^2) \cap C_{B_n}(\sigma_{n-k+1}) \right], \text{ we get that: }
\]

\[
\bigcap_{k=1}^{K+1} \left[ C_{B_n}(\Delta_{n-k}^2) \cap C_{B_n}(\sigma_{n-k+1}) \right] \subseteq \langle \Delta_n^2 \rangle \cdot B_{n-K-1}.
\]

The opposite inclusion is obvious, since every element of \( B_{n-K-1} \) and \( \Delta_n^2 \) commute with \( \Delta_n^{2-k} \) and \( \sigma_{n-k+1} \) for \( 1 \leq k \leq K + 1 \). Therefore:

\[
\bigcap_{k=1}^{K+1} \left[ C_{B_n}(\Delta_{n-k}^2) \cap C_{B_n}(\sigma_{n-k+1}) \right] = \langle \Delta_n^2 \rangle \cdot B_{n-K-1}.
\]
This completes the induction step.

**Theorem 4.4.** For $1 \leq m < n$, we have:

$$C_{B_n}(C_{B_n}(B_m)) = \langle \Delta^2_n \rangle \cdot B_m.$$ 

**Proof.** According to [FRZ96], the centralizer of $B_m$ in $B_n$ is:

$$C_{B_n}(B_m) = \langle \Delta^2_{m}, \Delta^2_{m+1}, \ldots, \Delta^2_{n-1}, \sigma_{m+1}, \ldots, \sigma_{n-1} \rangle.$$ 

We conclude that:

$$C_{B_n}(C_{B_n}(B_m)) = \bigcap_{k=1}^{n-m} \left[ C_{B_n}(\Delta^2_{n-k}) \cap C_{B_n}(\sigma_{n-k+1}) \right] = \langle \Delta^2_n \rangle \cdot B_m.$$ 

The right equality is by Proposition 4.3 (where we set $K = n - m$).

We may extend this result to parabolic subgroups of $B_n$ with a connected associated Coxeter graph, in the following sense of Paris [Pa97].

**Definition 4.5.** A subgroup $H$ of the braid group $B_n$ is called parabolic with a connected associated Coxeter graph if it is conjugate to $B_{[k,m]} = \langle \sigma_k, \sigma_{k+1}, \ldots, \sigma_{m-1} \rangle$ for some $1 \leq k < m \leq n$.

**Theorem 4.6.** Let $H$ be parabolic subgroup of $B_n$ with a connected associated Coxeter graph such that $\gamma^{-1} H \gamma = B_{[k,m]}$ for some $\gamma \in B_n$ and $1 \leq k < m \leq n$. Then the centralizer of the centralizer of $H$ is given by:

$$C_{B_n}(C_{B_n}(H)) = \langle \Delta^2_n \rangle \cdot H.$$ 

**Proof.** Recall that $\tau_{m-k+1,k-1}$ is the braid satisfying that the strands $m - k + 2, \ldots, m$ cross over the strands $1, \ldots, m - k + 1$ (see Figure 1). Therefore,

$$B_{[k,m]} = \tau_{m-k+1,k-1} B_{m-k+1} \tau_{m-k+1,k-1}^{-1},$$ 

and we conclude that $H = \gamma \tau_{m-k+1,k-1} B_{m-k+1} \tau_{m-k+1,k-1}^{-1} \gamma^{-1}$. Since $C_G(gHg^{-1}) = gC_G(H)g^{-1}$ for any $g \in G$, for a group $G$ and $H \leq G$, an application of Theorem 4.4 leads to the assertion.

5. **The subgroup conjugacy problem for parabolic subgroups**

We apply the results of the preceding section to reduce the subgroup conjugacy problem to an instance of the simultaneous conjugacy problem.

**Theorem 5.1.** Let $G$ be a group and $H \leq G$ such that $C_G(C_G(H)) = Z(G) \cdot H$ where $Z(G)$ denotes the center of $G$. Furthermore, let $\{g_1, \ldots, g_l\}$ be a generating set of $C_G(H)$. Then, for $x, y \in G$, the following are equivalent:

1. There exists $c \in H$ satisfying $y = c^{-1}xc$. 
Proof. (1) $\Rightarrow$ (2): Set $c' = c \in H \leq G$. Then $c'$ commutes with all elements in $C_G(H)$.

(2) $\Rightarrow$ (1): Conditions (b) implies that $c'$ commutes with all generators of $C_G(H)$. Therefore, $z \in C_G(C_G(H)) = Z(G) \cdot H$, and we may write $c' = zc$ for some $z \in Z(G)$ and $c \in H$. From Condition (a), we conclude that: $y = c'^{-1}xc' = c^{-1}z^{-1}xzc = c^{-1}xc$. \hfill \Box

Remark 5.2. In general, for any pair $(G, H)$, where $G$ is a group and $H \leq G$, we have $C_G(C_G(H)) \supseteq Z(G) \cdot H$. An example of a proper inclusion is the pair $(F_n, F_m)$ for $m < n$, where we have $C_G(C_G(H)) = G$, since $C_G(H) = \{1\}$.

Now, we may reduce the subgroup conjugacy problem for $B_m$ in $B_n$ (for $m < n$) to an instance of the simultaneous conjugacy problem:

**Corollary 5.3.** Let $m < n$. For all $x, y \in B_n$, the following are equivalent:

1. There exists $c \in B_{n-m}$ satisfying $y = c^{-1}xc$.
2. There exists $z \in B_n$ satisfying
   1. $y = z^{-1}xz$,
   2. $\Delta_{n-i}^2 = z^{-1}\Delta_{n-i}^2z$ for all $1 \leq i \leq n-m$,
   3. $\sigma_{n-i+1} = z^{-1}\sigma_{n-i+1}z$, for all $2 \leq i \leq n-m$.

Proof. The proof is just an application of Theorem 5.1 using the presentation

$$C_{B_n}(B_m) = \langle \Delta_m^2, \Delta_{m+1}^2, \ldots, \Delta_{n-1}^2, \sigma_{m+1}, \ldots, \sigma_{n-1} \rangle$$

from [FRZ96]. Also recall that $Z(B_n) = \langle \Delta_n^2 \rangle$ [Ch48]. \hfill \Box

Slightly more general, we may apply that reduction to parabolic subgroups of $B_n$ with a connected associated Coxeter graph:

**Corollary 5.4.** Let $H$ be a parabolic subgroup of $B_n$ with a connected associated Coxeter graph such that $\gamma^{-1}H\gamma = B_{[k,m]}$ for some $\gamma \in B_n$ and $1 \leq k < m \leq n$. Then for all $x, y \in B_n$, the following are equivalent:

1. There exists $c \in H$ satisfying $y = c^{-1}xc$.
2. There exists $z \in B_n$ satisfying
   1. $y = z^{-1}xz$,
   2. $\tau_{m-k+1,k-1}^2 \tau_{m-k+1,k-1}^{-1} \gamma^{-1} = z^{-1}(\tau_{m-k+1,k-1} \Delta_{n-i} \tau_{m-k+1,k-1}^{-1})z$, for all $1 \leq i \leq n - m + k - 1$,
   3. $\tau_{m-k+1,k-1} \sigma_{n-i+1} \tau_{m-k+1,k-1}^{-1} \gamma^{-1} = z^{-1}(\tau_{m-k+1,k-1} \sigma_{n-i+1} \tau_{m-k+1,k-1}^{-1})z$, for all $2 \leq i \leq n - m + k - 1$. 


Proof. This is a straightforward consequence of Theorem 5.1 and Theorem 4.6.

Corollary 5.5. Let $H$ be a parabolic subgroup of $B_n$ with a connected associated Coxeter graph. Then the subgroup conjugacy problem for $H$ in $B_n$ is solvable.

Proof. According to Corollary 5.4, this problem may be reduced to an instance of the simultaneous conjugacy problem in $B_n$. Now, the simultaneous conjugacy problem in braid groups was solved in [LL02]. This implies the solvability of the subgroup conjugacy problem as well.

Acknowledgements. We thank an anonymous referee for finding a gap in a previous version of the proof of the main result. We thank Boaz Tsaban for helpful discussions.

The second author acknowledges financial support by the Minerva Foundation of Germany. The fourth author acknowledges financial support by the Oswald Veblen Fund.

References

[Ar47] E. Artin, Theory of braids, Ann. Math. 48 (1947), 101–126.
[Ch48] W.-L. Chow, On the algebraic braid group, Ann. Math. 49 (1948), 654–658.
[Cr99] J. Crisp, Injective maps between Artin groups, Geom. Group Theory Down Under (Canberra 1996), de Gruyter, Berlin (1999), 119–137.
[De00] P. Dehornoy, Braids and Self-Distributivity, Progress in Math. 192, Birkhauser (2000).
[De06] P. Dehornoy, Using shifted conjugacy in braid-based cryptography, In: L. Gerritzen, D. Goldfeld, M. Kreuzer, G. Rosenberger and V. Shpilrain (Eds.), Algebraic Methods in Cryptography, Contemp. Math. 418 (2006), 65–73.
[EC+92] D. B. A. Epstein, J. W. Cannon, D. F. Holt, S. V. F. Levy, M. S. Paterson and W. P. Thurston, Word processing in groups, Jones and Bartlett (1992).
[EM94] E. A. Elrifai and H.R. Morton, Algorithms for positive braids, Quart. J. Math. 45 (1994), 479–497.
[FRZ96] R. Fenn, D. Rolfsen and J. Zhu, Centralizers in the braid group and singular braid monoid, L’Enseignement Math. 42 (1996), 75–96.
[Ga69] F.A. Garside, The braid group and other groups, Quart. J. Math. Oxford (2) 20 (1969), 235–254.
[Ge05] V. Gebhardt, A new approach to the conjugacy problem in Garside groups, J. Alg. 292(1) (2005), 282–302.
[Ge06] V. Gebhardt, Conjugacy search in braid groups, Applicable Algebra in Engineering, Communication and Computing 17 (2006), 219–238.
[Go07] E. Godelle, Parabolic subgroups of Garside groups, J. Alg. 317 (2007), 1–16.
[Gu85] G.G. Gurzo, Systems of generators for the normalizers of certain elements of the braid group, Math. USSR Izvestiya 24(3), 439–478 (1985).
[KL+00] K.H. Ko, S.J. Lee, J.H. Cheon, J.W. Han, J.-S. Kang and C. Park, New public-key cryptosystem using braid groups, Advances in Cryptology - CRYPTO 2000, LNCS 1880, Springer (2000).
[KLT09] A. Kalka, E. Liberman and M. Teicher, *A note on the shifted conjugacy problem in braid groups*, Groups - Complexity - Cryptology 1(2) (2009), 227–230.

[KLT10] A. Kalka, E. Liberman and M. Teicher, *Solution to the subgroup conjugacy problem for Garside subgroups of Garside groups*, Groups - Complexity - Cryptology 2(2) (2010), 157–174.

[KTT14] A. Kalka, M. Teicher and B. Tsaban, *Double coset problem for parabolic subgroups of braid groups*, preprint: http://arxiv.org/abs/1402.5541

[KTV14] A. Kalka, B. Tsaban and G. Vinokur, *Complete simultaneous conjugacy invariants in Garside groups*, preprint: http://arxiv.org/abs/1403.4622

[LL02] S.J. Lee and E.K. Lee, *Potential weaknesses in the commutator key agreement protocol based on braid groups*, Advances in Cryptology - EUROCRYPT 2002, LNCS 2332, Springer (2002).

[LU08] J. Longrigg and A. Ushakov, *Cryptanalysis of shifted conjugacy authentication protocol*, J. Math. Crypto. 2 (2008), 107–114.

[LU09] J. Longrigg and A. Ushakov, *A practical attack on a certain braid group based shifted conjugacy authentication protocol*, Groups - Complexity - Cryptology 1(2) (2009), 275–286.

[Mi58] K.A. Mihailova, *The occurrence problem for direct products of groups*, Dokl. Akad. Nauk SSSR 119 (1958), 1103–1105. (Russian)

[Pa97] L. Paris, *Centralizers of parabolic subgroups of Artin groups of type A1, B1 and D1*, J. Alg. 196 (1997), 400–435.

[Th92] William Thurston, *Braid groups*, Chapter 9 in [EC+92].

David Garber, Department of Applied Mathematics, Faculty of Sciences, Holon Institute of Technology, 52 Golomb St., PO Box 305, 58102 Holon, Israel
E-mail address: garber@hit.ac.il

Arkadius Kalka, Eran Liberman and Mina Teicher, Department of Mathematics, Bar-Ilan University, 52900 Ramat-Gan, Israel
E-mail address: arkadius.kalka@rub.de, eranyliberman@gmail.com, teicher@macs.biu.ac.il