Reduce Problems From Braid Groups To Braid Monoids.

Abstract. This paper proposes for every n, linear time reductions of the word and conjugacy problems on the braid groups $B_n$ to the corresponding problems on the braid monoids $B_n^+$ and moreover only using positive words representations.

0. Introduction.

Given a group $G$ presented with generators $[g_1, g_2, \ldots]$, a word representation $W$ of an element $g$ of $G$ is said positive if $W$ contains no letter $g_i^{-1}$. A powerful tool in group theory is what we will call a division procedure. That consists to put any word $W$ in an equivalent form $P.Q^{-1}$ where $P$ and $Q$ are both positive. This idea was already present in the work of Garside ([3]). Assume we have such a division method. Two elements of $G$ represented with two words $U$ and $V$ are equal if and only if the word $W = U.V^{-1} \equiv 1$ in $G$. By division of $W$ we obtain the equivalence to $P.Q^{-1} \equiv 1$ that is to say $P \equiv Q$. Hence the word problem on the group $G$ is reduced to the word problem on the monoid $G^+$. Observe that for that aim, one does not need a complete division but only a pseudo-division. That consists to find for any word $W$ some positive words $P$ and $Q$ such that $W \equiv 1$ if and only if $P.Q^{-1} \equiv 1$. That seems easier since $P$ and $Q$ can be taken here in a finite set, for instance:

For $W \equiv 1$, take $P = Q = 1$

For $W \not\equiv 1$, take $P = g_i$ and $Q = 1$ where $g_i \not\equiv 1$.

However, in this paper we will perform divisions that have more semantical power. The key tool of this paper will be a linear time division method for the $n$ strands braid groups $B_n$ presented with standard generators $[\sigma_1, \sigma_2, \ldots, \sigma_{n-1}]$. We will deduce many methods for braids and linear time reductions of problems from the braid groups $B_n$ to the braid monoids $B_n^+$. We obtain the quite surprising result that classical problems on the braid groups are ”easier” than corresponding problems on the braid monoids $B_n^+$. Since the converse is obvious ($B_n^+ \subset B_n$) the problems belong to the same complexity classes. Moreover, since there exists a well-ordering on $B_n^+$ (see [1]), one can use now this strong structure for braids in general. For instance, we directly obtain that the word problem on the group $B_3$ is solvable in linear time since that is the case for $B_3^+$ by computing normal forms in this well-ordering ([1],[2]).
1. Extented Generators of Braid Groups.

Assume we are working with \( n \geq 3 \) strands braids. Denote \( \Delta \) the classical Garside positive braid on \( n \) strands resulting from a positive half-turn of the trivial braid. We have the well known relations:

\[
\begin{align*}
\sigma_i \cdot \Delta &= \Delta \cdot \sigma_{n-i} \\
\sigma_i^{-1} \cdot \Delta &= \Delta \cdot \sigma_{n-i}^{-1}
\end{align*}
\]

and \( \Delta^2 \) belongs to the center of \( B_n \). That is to say, for any \( X \):

\[
X \cdot \Delta^2 = \Delta^2 \cdot X
\]

Definition. (generators). For \( n > i \geq 1 \), let

\[
\begin{align*}
0\sigma_i &:= \sigma_i \\
1\sigma_i &:= \Delta \cdot \sigma_{i}^{-1} \\
2\sigma_i &:= \sigma_{n-i} \\
3\sigma_i &:= \Delta \cdot \sigma_{n-i}^{-1}
\end{align*}
\]

Observe that for every \( n > i \geq 1 \) and \( a \in \{0, 1, 2, 3\} \), \( a\sigma_i \) is a positive braid.

Definition. (conversion). Every braid word \( V \) on standard generators \( \sigma_i \) will be called a standard word. Every braid word \( W \) on extended generators \( a\sigma_i \) will be called an extended word. The extension of a standard word \( V \) is the extended word \( 0V \) obtained by replacing in \( V \) every letter \( \sigma_i \) by \( 0\sigma_i \). The standardization of an extended word \( W \) is the standard word \( S(W) \) obtained by replacing in \( W \):

- every \( 0\sigma_i \) by \( \sigma_i \),
- every \( 1\sigma_i \) by \( D_i \),
- every \( 2\sigma_i \) by \( \sigma_{n-i} \),
- every \( 3\sigma_i \) by \( D_{n-i} \),

where \( D_i \) is some standard positive word of length \( n(n - 1)/2 - 1 \) equivalent to \( \Delta \cdot \sigma_{i}^{-1} \).

Observe that if an extended word \( W \) has \( k \) extended letters \( a\sigma \), its standardization \( S(W) \) will have at most \( k \cdot (n(n - 1)/2 - 1) \leq k \cdot n^2 \) letters \( \sigma \). More precisely, if \( W \) has:

- \( p \) extended letters \( a\sigma \) with \( a \in \{0, 2\} \) and
- \( q \) extended letters \( b\sigma \) with \( b \in \{1, 3\} \)

the length of \( S(W) \) will be exactly \( p + q(n(n - 1)/2 - 1) \).

2. Extended Division in Braid Groups.
Proposition 1. (commutation). For every \( n > i \geq 1 \) and \( n > j \geq 1 \) and \( a \in \{0, 1, 2, 3\} \) and \( b \in \{0, 1, 2, 3\} \), the following relation holds:
\[
a_{\sigma_i} \cdot b\sigma_j^{-1} = a\sigma_i^{-1} \cdot B\sigma_j
\]
where \( A = (a + 1)[4] \) and \( B = (b + 1)[4] \).

**Proof.** First, we verify in all cases that:
\[
a_{\sigma_i} \cdot \Delta^{-1} = a\sigma_i^{-1}
\]
\[
\Delta \cdot b\sigma_j^{-1} = B\sigma_j
\]
That is quite obvious by definition:
\[
o_{\sigma_i} \cdot \Delta^{-1} = 1\sigma_i^{-1}
\]
\[
1_{\sigma_i} \cdot \Delta^{-1} = \Delta \cdot \sigma_i^{-1} \cdot \Delta^{-1} = \Delta \cdot \Delta^{-1} \cdot \sigma_i^{-1} = 2\sigma_i^{-1}
\]
\[
2_{\sigma_i} \cdot \Delta^{-1} = \sigma_{n-i} \cdot \Delta^{-1} = 3\sigma_i^{-1}
\]
\[
3_{\sigma_i} \cdot \Delta^{-1} = \Delta \cdot \sigma_{n-i} \cdot \Delta^{-1} = \Delta \cdot \Delta^{-1} \cdot \sigma_i^{-1} = 0\sigma_i^{-1}
\]
\[
\Delta \sigma_j^{-1} = 1\sigma_j
\]
\[
\Delta \sigma_j^{-1} = \Delta \cdot \sigma_j \cdot \Delta^{-1} = \Delta \cdot \Delta^{-1} \cdot \sigma_j = 2\sigma_j
\]
\[
\Delta \sigma_j^{-1} = \sigma_{n-j} \cdot \Delta^{-1} = 3\sigma_j
\]
\[
\Delta \sigma_j^{-1} = \Delta \cdot \sigma_{n-j} \cdot \Delta^{-1} = \Delta \cdot \Delta^{-1} \cdot \sigma_j = 0\sigma_j
\]
Hence
\[
a_{\sigma_i} \cdot b\sigma_j^{-1} = a_{\sigma_i} \cdot \Delta^{-1} \cdot b\sigma_j^{-1} = a\sigma_i^{-1} \cdot B\sigma_j
\]

Definition. (Shift). For every \( d \in \mathbb{Z}/4\mathbb{Z} \) and every extended letter \( x = a\sigma_j^e \) where \( a \in \mathbb{Z}/4\mathbb{Z} \) and \( e \in \{+1, -1\} \), let \( sh(d, x) \) be the extended letter \( y = A\sigma_j^f \) where \( A = a + d[4] \) and
\[
f = \begin{cases} 
eq & \text{if } d \in \{0, 2\} \\ -e & \text{if } d \in \{1, 3\} \end{cases}
\]
Let \( W = w_1w_2 \ldots w_k \) be an extended braid word and \( L = [d_1, d_2, \ldots, d_k] \) be a list of numbers in \( \mathbb{Z}/4\mathbb{Z} \). The extended braid word \( SH(L, W) \) is \( w_1', w_2', \ldots, w_k' \) where \( w_i' = sh(d_i, w_i) \).

For instance, for \( L = [0, 1, 2, 3] \) and \( W = \sigma_1 \cdot \sigma_2^{-1} \cdot 2\sigma_3^{-1} \cdot 3\sigma_4 \),
\[
SH(L, W) = \sigma_1 \cdot 2\sigma_2 \cdot 0\sigma_3^{-1} \cdot 2\sigma_4^{-1}
\]
In order to obtain linear time algorithms, one must be careful on the counting methods. For instance, given an input word \( W \) with \( k \) letters, working with numbers in the interval \([1, \ldots, k]\) introduces a time factor in \( \log_2(k) \) which may be too much for a real linear time algorithm. That aim motivates for instance to introduce the following notion.
Definition. (Bishift). Let \( W = w_1.w_2 \ldots w_k \) be an extended braid word. For \( 0 \leq p \leq k \), let \( L = [d_1, d_2, \ldots, d_p] \) and \( L' = [d_{p+1}, d_{p+2}, \ldots, d_k] \) be two lists of numbers in \( \mathbb{Z}/4\mathbb{Z} \) and \( \delta \) be another number in \( \mathbb{Z}/4\mathbb{Z} \). Such a triple \((L, \delta, L')\) is called a trip of \( W \). The extended braid word \( SH2(L, \delta, L', W) \) is \( w'_1.w'_2 \ldots w'_k \) where:

\[
w'_1.w'_2 \ldots w'_p = SH(L, w_1.w_2 \ldots w_p) \quad \text{and} \quad w'_q = sh(\delta + d_q, w_q).
\]

The Bishift corresponds to a Shift where all the elements of the second list \( L' \) are translated by the factor \( \delta \). For instance, for \( W = 0\sigma_1.1\sigma_2^{-1}.2\sigma_3^{-1}.3\sigma_4 \)

\[
SH2([0, 1], 2, [0, 1], W) = SH([0, 1, 2, 3], W) = 0\sigma_1.2\sigma_2.0\sigma_3^{-1}.2\sigma_4^{-1}
\]

As usual, for two lists \( L, L' \), denote \( L.L' \) the concatenation of these lists. For instance, \([0, 1].[2, 3] = [0, 1, 2, 3]\).

Definition. (Separation). Let \( W \) be an extended braid word. The separation of \( W \) is a trip \((L, \delta, L')\) of \( W \) defined inductively as follows.

The separation of the empty word is \(([], 0, [])\).

For \((L, \delta, L')\) the separation of \( W \), the separation of \( W.x \) is:

\[
\begin{cases}
(L, \delta, L'.[-\delta]) & \text{if } x \text{ is a negative letter,} \\
(L.[0], \delta, L') & \text{if } L' = [] \text{ and } x \text{ is a positive letter,} \\
(L.[a + \delta + 1], \delta + 2, L''.[3 - \delta]) & \text{if } L' = [a].L'' \text{ and } x \text{ is a positive letter.}
\end{cases}
\]

Observe that with this inductive definition, the separation of \( W \) can be computed in \( O(|W|) \) steps since we only use numbers in \( \mathbb{Z}/4\mathbb{Z} \) and we have to perform a constant number of operations for each letter. Observe also that if \( L' \) is empty, then \( \delta = 0 \) since it is modified if and only if \( L' \) is non empty. Moreover \( \delta \) always belongs to \( \{0, 2\} \) since from the null value, \( \delta \) can only be translated by 2 in \( \mathbb{Z}/4\mathbb{Z} \) and it is obvious that \( \delta = 0 \) if and only \( W \) is positive or the number of positive letters after the first negative letter in \( W \) is even.

Theorem 2. (general extended division). There exists a linear time algorithm \( GED \) that computes for every \( n \) and from every extended word \( W \) of \( B_n \), two extended positive words \( P, Q \) of \( B_n \) such that

\[
W \equiv PQ^{-1}
\]

in \( O(|W|) \) steps. Moreover \( W \) and \( PQ^{-1} \) have exactly the same lengths, the same number of positive letters and the same sequences of right indices.
Proof. Let $W = w_1w_2\ldots w_k$ be an extended word. We are going to show by induction on $k$ that the separation $(L, \delta, L')$ of $W$ satisfies

$$SH2(L, \delta, L', W) = P.q$$

where $P$ is positive, $q$ is negative and for $Q = q^{-1}$ we have the expected properties.

For $W = 1$, that is obvious since $SH2([], 0, [], 1) = 1$.

Assume that for the separation $(L, \delta, L')$ of some $W$, $SH2(L, \delta, L', W) = P.q$.

Let us verify the property for $W.x$.

• If $x$ is negative, we just have to see that $W.x \equiv P.q'$ where $q' = q.x$. Since the separation of $W.x$ is $(L, \delta, L', [\delta])$ the last letter $x$ of $W.x$ will be transformed by $SH2$ in $sh(\delta - \delta, x) = sh(0, x) = x$ and we will obtain $P.q.x$. That was expected.

• If $x$ is positive and $L' = []$ then $W \equiv P.q$ and $q = 1$. Hence $W.x \equiv P'.q$ where $P' = P.x$. Since the separation of $W.x$ is $(L, 0, L')$, the last letter $x$ of $W.x$ will be transformed by $SH2$ in $sh(0, x) = x$ and we will obtain $P.x$. That was expected.

• If $x$ is positive and $L' = [a].L''$ then $W \equiv P.z.q$ where $z = sh(a + \delta, w_{p+1})$ is the first negative letter in $P.z.q$. The positive letter $x$ has to commute with all the negative letters of $z.q$. Applying the commutation principle on $z.q.x$ :

the letter $x$ is translated once and becomes negative,
all the letters in $q$ are translated twice and remain negative,
the letter $z$ is translated once and becomes positive.

Since the separation of $W.x$ is $(L, [a + \delta + 1, \delta + 2, L'', [3 - \delta])]$ and :

$sh(1, z) = sh(a + \delta + 1, w_{p+1})$
$sh(\delta + 2 + 3 - \delta, x) = sh(5, x) = sh(1, x)$

we obtain the expected form. ■

3. Results.

Theorem 3. (fixed standard division). For every $n$, there exists a linear time algorithm $FSD_n$ that computes from every standard word $V$ of $B_n$, two positive standard words $P, Q$ of $B_n$ such that

$$V \equiv P.Q^{-1}$$

in $O(|V|)$ steps.
Proof.

0. Compute the extension $\sigma V$ of $V$ in $|V|$ steps.
1. Perform the general extended division of $\sigma V$ in $P_e.Q_e^{-1}$ in $O(|\sigma V|) = O(|V|)$ steps.
2. Compute $P = S(P_e)$ in $O(|P_e|.n^2) \leq O(|V|.n^2)$ steps.
3. Compute $Q = S(Q_e)$ in $O(|Q_e|.n^2) \leq O(|V|.n^2)$ steps.
Observe that $n$ is fixed, hence $n$ is a constant and $O(|V|.n^2) = O(|V|)$. ■

Observe that, by symmetry one can also compute in $O(|V|)$ steps an equivalent form $Q^{-1}.P$.

**Theorem 4. (general standard division).** There exists an algorithm $GSD$ that computes for every $n$ and from every standard word $V$ of $B_n$, two positive standard words $P,Q$ of $B_n$ such that

\[ V \equiv P.Q^{-1} \]

in $O(|V|.n^2)$ steps.

**Proof.** The method is the same as in $FSD_n$. However, the number of strands $n$ is not constant any more. ■

**Theorem 5. (word problems reduction).** For every $n$, there exists a linear time reduction of the word problem on $B_n$ to the word problem on $B_n^+$ positively presented.

**Proof.** Let $X,Y$ be two standard words of $B_n$. One has $X \equiv Y$ if and only if $V = X.Y^{-1} \equiv 1$. This word $V$ has length $|X| + |Y|$ and is computed in linear time. Compute the fixed standard division $P.Q^{-1}$ of $V$ in $O(|V|)$ steps. One has $X \equiv Y$ in $B_n$ if and only if $P \equiv Q$ in $B_n^+$. ■

Hence, the word problems on $B_n$ and on $B_n^+$ have the same time complexity. Since there exists a linear time algorithm for the word problem on the monoid $B_3^+$, there also exists a linear time algorithm for the word problem on the group $B_3$ (see [2]).

**Theorem 6. (conjugacy decision problems reduction).** For every $n$, there exists a linear time reduction of the conjugacy decision problem on $B_n$ to the following problem on $B_n^+$ positively presented:

Given four positive standard words $A,B,C,D$.

Is there a positive standard word $M$ such that $A.M.B \equiv C.M.D$?
Proof. Let $U, V$ be two standard braid words of $B_n$. They are conjugate if and only if there exists a braid word $X$ such that $U \equiv X.V.X^{-1}$.

First, it is well known that one can also assume that $X$ is positive since any braid word $X$ is equivalent to some $\Delta^{2k}.M$ for $k \in \mathbb{Z}$ and $M$ a positive braid:

\[
U \equiv X.V.X^{-1} \\
\equiv \Delta^{2k}.M.V.M^{-1} \Delta^{-2k} \\
\equiv \Delta^{2k}.\Delta^{-2k}.M.V.M^{-1} \\
\equiv M.V.M^{-1}
\]

1. Compute in $O(|U|)$ steps a division $C^{-1}.A$ of $U$.
2. Compute in $O(|V|)$ steps a division $D.B^{-1}$ of $V$.
3. One obviously have $U \equiv M.V.M^{-1}$ if and only if $A.M.B \equiv C.M.D$

and we immediatly obtain the following

Theorem 7. (conjugacy search problems reduction). For every $n$, there exists a linear time reduction of the conjugacy search problem on $B_n$ to the following problem on $B_n^+$ positively presented:

Given four positive standard words $A, B, C, D$.

Find a positive standard word $M$ such that $A.M.B \equiv C.M.D$

4. Conclusion.

The methods we presented here enable the reductions of problems on braids to equivalent problems on positive braids. First, this general framework could be generalized for other groups $G$ than the braid groups $B_n$. Second, it is likely that the word problems for every $B_n$ (like for $B_3$) have linear time solutions. The fact that $B_n^+$ has a well-ordering that is completely described in term of trees with normal forms defined inductively by blocs give some hope for the generalization of the efficient constructions of normal forms for $B_3^+$. Third, one can expect to reduce the conjugacy problems to simpler problems. A first idea is that if $W$ is divided to $P.Q^{-1}$ which is itself divided in the other way to $R^{-1}.S$, then some non trivial relations hold between $P, Q, R$ and $S$.

References.

[1] S. Burckel, The Well Ordering on Positive Braids, Journal of Pure and Applied Algebra 120 (1997) 1–17.

[2] S. Burckel, Syntactical Methods for Braids of Three Strands, Journal of Symbolic Computation 31(5) (2001) 557–564.
[3] F. Garside, *The braid group and other groups*, Quart. J. Math. Oxford 20 (1969) 235–254.

Serge Burckel.
INRIA-LORIA,
615 rue du Jardin Botanique
sergeburckel@orange.fr