Groups-Complexity-Cryptology
Volume 1 (2009), No. 2, 227–230

A Note on the Shifted Conjugacy Problem in Braid Groups

Arkadius Kalka
Dept. of Mathematics and Computer Science, Bar-Ilan University, Ramat-Gan 52900, Israel
arkadius.kalka@rub.de

Eran Liberman
Dept. of Mathematics and Computer Science, Bar-Ilan University, Ramat-Gan 52900, Israel
manliber@netvision.net.il

Mina Teicher
Dept. of Mathematics and Computer Science, Bar-Ilan University, Ramat-Gan 52900, Israel
teicher@macs.biu.ac.il

Dedicated to Benjamin Fine on the occasion of his 60th birthday.

Received: November 6, 2008
Revised manuscript received: January 22, 2009

It is an open problem whether the shifted conjugacy (decision) problem in B_∞ is solvable. We settle this problem by reduction to an instance of the simultaneous conjugacy problem in B_n for some $n \in \mathbb{N}$.

Recall Artin's presentation of the braid group B_n with $n \geq 2$ strands [1]:

$$B_n = \langle \sigma_1, \ldots, \sigma_{n-1} \mid \sigma_i\sigma_j = \sigma_j\sigma_i \text{ for } |i-j| \geq 2,\ \sigma_i\sigma_j\sigma_i = \sigma_j\sigma_i\sigma_j \text{ for } |i-j| = 1\rangle.$$

The groups B_n ($n \geq 2$) build an inductive system of groups, which has a direct limit: the braid group on infinitely many strands B_∞ is generated by $\{\sigma_1, \sigma_2, \ldots\}$ subject to the same relations.
The *shifted conjugacy operation* $* : B_\infty \times B_\infty \to B_\infty$ defined by [2]

$$x * y = x \cdot \partial y \cdot \sigma_1 \cdot \partial x^{-1},$$

where $\partial : \sigma_i \mapsto \sigma_{i+1}$ denotes the *shift operator*, is an example for a left-selfdistributive operation other than classical conjugacy. The *shifted conjugacy (decision) problem* (ShCP) in B_∞, i.e., given $(x, y) \in B_\infty^2$, decide whether there exists $c \in B_\infty$ such that $y = c * x$ was introduced in [3] and its search version had been been proposed as a base problem for an authentication scheme. According to [3, 9] it is an open problem whether the (decision version of the) ShCP is solvable.

ISSN 1867-1144 / $ 2.50

Immediately after Dehornoy's introduction of the shifted conjugacy problem in the Bochum conference[1], Tsaban pointed out that the memory-length attack [5] should be applicable, heuristically, to this problem. Later, a heuristic centralizer attack on the shifted conjugacy search problem has been performed in [9]. While these attacks are very efficient, none of them solves all instances of the problem. We present a complete algorithm for the ShCP.

Definition 1. For $b \in B_\infty$, we define $N(b)$ to be the minimal number n such that b lies in B_n, i.e., such that b can be expressed in terms of $\{\sigma_1, \ldots, \sigma_{n-1}\}$ and their inverses.

Proposition 2 reduces the ShCP to an instance of the *subgroup conjugacy problem for* $B_{n-1} \leq B_n$, i.e., given $(x, y) \in B_n^2$, decide whether there exists a $c \in B_{n-1}$ such that $y = cxc^{-1}$. This was first noticed in [9]. Indeed, Proposition 2(ii) is a restatement of Proposition 2.1 in [9].

Proposition 2. *Let x, y be two braids in B_∞ and let n be* $\max\{N(x)+1, N(y)\}$.

(i) *The braids x, y are shift-conjugated if and only if they are shift-conjugated by some braid c of B_{n-1}.*

(ii) *Denote $\delta_n = \sigma_{n-1} \cdots \sigma_2 \sigma_1$. For each c in B_{n-1}, the braids x, y are shift-conjugated by c of B_{n-1} if and only if $\partial(x)\sigma_1\delta_n^{-1}$ and $y\delta_n^{-1}$ are conjugated by c in B_n.*

Proof. (i) Suppose there exists such a shifted conjugator $c \in B_\infty$. Recall Definition 1. We want to find an upper bound for $N(\partial(c))$.
Now, we focus on the case of $N(c) > N(x)$. Otherwise $N(\partial(x))$ is an upper bound for $N(\partial(c))$. Since $y = c * x = c\partial(x)\sigma_1\partial(c^{-1}) \Leftrightarrow \partial(c^{-1}) = \sigma_1^{-1}\partial(x^{-1})c^{-1}y$, we get the inequality

$$N(\partial(c^{-1})) = N(\sigma_1^{-1}\partial(x^{-1})c^{-1}y) \leq \max\{N(\partial(x^{-1})), N(c^{-1}), N(y)\} = N(y).$$

Therefore we have $N(y) \geq N(\partial(c))$ in this case. And in all cases we have

$$N(\partial(c)) \leq \max\{N(\partial(x)), N(y)\} = n.$$

This implies $c \in B_{n-1}$. The opposite implication is an obvious embedding.

(ii) Since $\partial(b)\delta_n^{-1} = \delta_n^{-1}b$ for all $b \in B_{n-1}$, we get

$$\begin{aligned} y = c * x &\Leftrightarrow y = c\partial(x)\sigma_1\partial(c^{-1}) \quad | \cdot\delta_n^{-1} \\ &\Leftrightarrow y\delta_n^{-1} = c\partial(x)\sigma_1\partial(c^{-1})\delta_n^{-1} = c\partial(x)\sigma_1\delta_n^{-1}c^{-1}. \end{aligned}$$

□

In the proof to Proposition 2(i) we proved even a stronger statement:

[1]Workshop "Algebraic Methods in Cryptography", Ruhr-Universität Bochum, 17.–18.11.2005.

Proposition 3. *If x, y in B_∞ are shift-conjugated by $c \in B_\infty$, then $N(c) \leq n-1$ with $n = \max\{N(x)+1, N(y)\}$.*

In this respect shifted conjugacy exhibits a different behaviour than usual conjugacy in braid groups. Obviously, there exists no bound for $N(c)$ that holds for all conjugators $c \in B_\infty$ of a given conjugated pair $(x, y) \in B_\infty^2$.
The subgroup conjugacy problem for $B_{n-1} \leq B_n$ can be reduced to some special instances of *simultaneous conjugacy problems* (SCP) in B_n:

Proposition 4. *For $k \in \mathbb{N}$, put $\Delta_k = \sigma_1(\sigma_2\sigma_1)\cdots(\sigma_{k-1}\cdots\sigma_2\sigma_1)$ and $b_k = \sigma_{k-1}\cdots\sigma_2\sigma_1^2\sigma_2\cdots\sigma_{k-1}$. Then, for all $x, y \in B_\infty$ the following are equivalent:*

(1) There exists $c \in B_{n-1}$ satisfying $y = cxc^{-1}$.
(2) There exists $z \in B_n$ satisfying $y = zxz^{-1}$ and $z\Delta_{n-1}^2 z^{-1} = \Delta_{n-1}^2$.
(3) There exists $z \in B_n$ satisfying $y = zxz^{-1}$ and $zb_nz^{-1} = b_n$.

Proof. Since Δ_k^2 generates the center of B_k the implication (1) $\Rightarrow$ (2) is obvious. Further, every $c \in B_{n-1}$ commutes with b_n. This proves (1) $\Rightarrow$ (3). Now, assume (2) or (3), respectively. $z\Delta_{n-1}^2 z^{-1} = \Delta_{n-1}^2$ ($zb_nz^{-1} = b_n$) implies that z lies in the centralizer $C_{B_n}(\Delta_{n-1}^2)$ ($C_{B_n}(b_n)$). According to Theorem 3 and 2 in [8][2] these centralizers are

$$C_{B_n}(\Delta_{n-1}^2) = C_{B_n}(b_n) =< \sigma_1, \ldots, \sigma_{n-2}, b_n >=< B_{n-1}, b_n, \Delta_n^2 > .$$

But, since $\Delta_n^2 = b_n\Delta_{n-1}^2$, we have $< B_{n-1}, b_n, \Delta_n^2 >=< B_{n-1}, \Delta_n^2 >$. Therefore there exist $c \in B_{n-1}$, $l \in \mathbb{Z}$ such that $z = c\Delta_n^{2l}$. This implies $y = zxz^{-1} = c\Delta_n^{2l}x(c\Delta_n^{2l})^{-1} = cxc^{-1}$, i.e. we proved (2) $\Rightarrow$ (1) and (3) $\Rightarrow$ (1). □

Theorem 5. *ShCP is solvable.*

Proof. The SCP can be solved by straightforward generalizations of Garside's solution to the conjugacy problem [4]. An improved solution using minimal simple elements is given in [6]. So an algorithm that decides whether there exists a simultaneous conjugator for the instance pairs $(\partial(x)\sigma_1\delta_n^{-1}, y\delta_n^{-1})$ and $(\Delta_{n-1}^2, \Delta_{n-1}^2)$ in B_n with $n = \max\{N(x)+1, N(y)\}$ provides a solution to the shifted conjugacy instance (x, y) in B_∞. □

Note that as a special case Theorem 5 also settles Question 2.6 in [3].
As a natural generalization it is interesting to consider the subgroup conjugacy problem for $B_m \leq B_n$ with $m < n$. Also it would be nice to settle this problem without making a detour via the SCP. We deal with such subjects in a subsequent paper.

Acknowledgements. This research was partially supported by the Emmy Noether Research Institute for Mathematics and the Minerva Foundation. We thank Boaz Tsaban for fruitful discussions.

[2]In [8] Gurzo computes the centralizers for some certain braids. A complete description of the structure of the centralizer of an arbitrary braid is given in [7].

References

[1] E. Artin: Theory of braids, Ann. Math. 48(2) (1947) 101–126.

[2] P. Dehornoy: Braids and Self-Distributivity, Progress in Math. 192, Birkhäuser, Basel (2000).

[3] P. Dehornoy: Using shifted conjugacy in braid-based cryptography, in: L. Gerritzen et al. (ed.), Algebraic Methods in Cryptography (Mainz, 2005; Bochum, 2005), Contemporary Mathematics 418, AMS, Providence (2006) 65–73.

[4] F. A. Garside: The braid group and other groups, Q. J. Math., Oxf. II. Ser. 20 (1969) 235–254.

[5] D. Garber, S. Kaplan, M. Teicher, B. Tsaban, U. Vishne: Probabilistic solutions of equations in the braid group, Adv. Appl. Math. 35 (2005) 323–334.

[6] J. González-Meneses: Improving an algorithm to solve multiple simultaneous conjugacy problems in braid groups, in: Geometric Methods in Group Theory (Boston, 2002; Seville, 2003), J. Burillo et al. (ed.), Contemp. Math. 372, AMS, Providence (2005) 35–42.

[7] J. González-Meneses, B. Wiest: On the structure of the centralizer of a braid, Ann. Sci. Éc. Norm. Supér. 37(5) (2004) 729–757.

[8] G. G. Gurzo: Systems of generators for the normalizers of certain elements of the braid group, Math. USSR, Izv. 24(3) (1985) 439–478.

[9] J. Longrigg, A. Ushakov: Cryptanalysis of shifted conjugacy authentication protocol, J. Math. Cryptol. 2 (2008) 107–114.