THE CONJUGACY PROBLEM - THEORY AND APPLICATIONS
Jens Harlander (BSU), Hannah Lewis (DSC), Jonathan Siegel (UCSC), and Chao Xu (SBU)

The Conjugacy Problem

Let $G$ be a group. The conjugacy problem in $G$ states: given $g, g' \in G$, decide if they are conjugate, that is, if there is a group element $a$ so that $g = a g' a^{-1}$. The conjugacy search problem states: Given two elements $g_i$ and $g_j$ that are conjugate in $G$, find the conjugator $g$. These problems depend on how the group $G$ is given. Most commonly $G$ is given by a presentation $\langle x_1, \ldots, x_n \mid r_1, \ldots, r_m \rangle$, where the $x_i$ generate the group and the $r_j$ are relations that hold among the generators. For our project we studied the conjugacy problem in the braid group.

Conjugacy Problem Algorithms in the Braid Groups

In 1969 F. Garside found an algorithm for solving the conjugacy problem in braid groups. His algorithm is inefficient, it does not run in polynomial time. In 1988 W. P. Thurston proved that the braid groups are automatic. This insight provided another approach to solving the conjugacy problem, but his algorithm is equally complex. It is not known to this day if there is an efficient algorithm that does the job. This makes braid groups interesting from a cryptography viewpoint.

The braid group $B_3$ is special in many ways. Garside’s and Thurston’s algorithms remain inefficient even in case $n = 3$, but we found algorithms that solve the conjugacy problem in $B_3$ in linear time.

The Elements of the Braid Group

The elements of the braid group $B_n$ are $n$-stranded braids. We multiply braids by concatenation. The braid group has a presentation $\langle \sigma_1, \ldots, \sigma_{n-1} \mid \sigma_i \sigma_i+1 \sigma_i = \sigma_i \sigma_i+1 \sigma_i, \sigma_i \sigma_j = \sigma_j \sigma_i \rangle$, where $i = 1, \ldots, n-2$ and $j = 1, \ldots, n-1$, $|i-j| > 1$.

Key Exchange Protocols Based on the Conjugacy Problem

A key exchange protocol is a procedure by which Alice and Bob can establish a common secret encryption key. The protocol works as follows: Let $A$ and $B$ be subgroups of some group $G$ and $x = \{a_1, \ldots, a_n\} \subseteq A$ and $x' = \{b_1, \ldots, b_n\} \subseteq B$ be subsets. This information is public. $A$ and $B$ and $x$ are posted on Alice’ and Bob’s homepage, respectively. Alice chooses a word $\alpha$ in the $a_i$, $i = 1, \ldots, k$ and Bob chooses a word $\beta$ in the $b_j$, $j = 1, \ldots, l$. The elements $a \in A$ and $\beta \in B$ are Alice’ and Bob’s private keys. Alice sends Bob the set of conjugates $\{ab \alpha^{-1}, \ldots, ab \alpha^{-1}\}$ and Bob send Alice the set of conjugates $\{b \alpha \beta^{-1}, \ldots, b \alpha \beta^{-1}\}$. Alice can then compute $b \alpha \beta^{-1}$ by replacing every $a_i$ in the word $\alpha$ by $b \alpha \beta^{-1}$. Similarly, Bob can compute $\alpha \beta^{-1}$. Alice now computes the secret encryption key $K = (b \alpha \beta^{-1})^{-1}$ and Bob computes the secret encryption key $K' = ((a \alpha \beta^{-1})^{-1})^{-1}$. Note that $K = K'$. An eavesdropper only sees the $a_i$ and the conjugates $b \alpha \beta^{-1}$, but not the conjugator $\beta$. He only sees the $b_j$ and the conjugates $b \alpha \beta^{-1}$, but not the conjugator $\alpha$. Thus, the eavesdropper will have to solve the conjugacy search problem in $A$ and $B$ in order to construct the secret encryption key $K$.

Summary of Results

The standard algorithms by Garside and Thurston do not provide efficient solutions for solving the conjugacy problem in braid groups, even in the three strand braid group $B_3$. However, we have found other algorithms that provide linear time solutions for both the word and conjugacy problems in $B_3$. These algorithms rely on special combinatorial and topological features of $B_3$. The table below summarizes our findings so far. The table also lists findings concerning the word problem, which is a special case of the conjugacy problem. The word problem asks: given a word $w$ expressed in the generators of a group $G$, does it presents the trivial element in $G$?

Questions for Future Work

Do any of the special properties of $B_n$ carry over to $B_n$, $n > 3$? Can geometric ideas be applied to study $B_n$? For which $n$ is $B_n$ non-positively curved? $B_4$ and $B_5$ are known to be non-positively curved. Can this be used for the design of efficient algorithms for the conjugacy problem?

References


Acknowledgements

This work was conducted as part of an REU program on complexity in algebra, geometry and applications at Boise State University in the summer of 2011. We gratefully acknowledge funding from the National Science Foundation (DMS 1062857) and Boise State University.