Tutorials:

Braid Group Cryptography

Second part

Singapore, June 2007

David Garber

Department of Applied Mathematics, School of Sciences
Holon Institute of Technology
Holon, Israel

The underlying (apparently hard) problems

Conjugacy Decision Problem: Given $u, w \in B_n$, determine whether they are conjugate, i.e., there exists $v \in B_n$ such that

$$w = v^{-1}uv$$

Conjugacy Search Problem: Given conjugate elements $u, w \in B_n$, find $v \in B_n$ such that

$$w = v^{-1}uv$$

Decomposition Problem: $u \notin G \leq B_n$. Find $x, y \in G$ such that $w = xuy$.

Attacks using Summit Sets

Basic idea: For an element $x \in B_n$, we look for a subset I_x of the conjugacy class of x satisfying:

1. For every $x \in B_n$, the set I_x is finite, non-empty and only depends on the conjugacy class of x.
2. For each $x \in B_n$, one can compute efficiently $\tilde{x} \in I_x$ and the conjugator $a^{-1}xa = \tilde{x}$.
3. One can construct the whole set I_x for any representative $\tilde{x} \in I_x$.

For solving the Conjugacy Decision Problem and Conjugacy Search Problem for given $x, y \in B_n$, we have to do:

(a) Find $\tilde{x} \in I_x$ and $\tilde{y} \in I_y$.

(b) Using the algorithm from Property (3), compute further elements of I_x (while keeping track of the conjugating elements), until either:
(i) $\tilde{y} \in I_x$, proving x and y are conjugate and providing a conjugating element, or
(ii) $\tilde{y} \notin I_x$, proving that x and y are not conjugate.

Garside (1969): $I_x = \mathrm{SS}(x)$, the Summit Set of x, which is the set of conjugates of x having maximal infimum.

The Super Summit Sets
Elrifai and Morton (1994)

I_x = SSS(x), the Super Summit Set of x, consisting of the conjugates of x having minimal canonical length len(x) (SSS(x) is much smaller than SS(x)).

Definition: Let $x = \Delta^p x_1 \cdots x_r \in B_n$. Cycling of x, $\mathbf{c}(x)$, is:

$$\mathbf{c}(x) = \Delta^p x_2 \cdots x_r \tau^{-p}(x_1).$$

where $\tau(\sigma_i) = \sigma_{n-i}$.
Decycling of x, $\mathbf{d}(x)$, is:

$$\mathbf{d}(x) = x_r \Delta^p x_1 x_2 \cdots x_{r-1} = \Delta^p \tau^{-p}(x_r) x_1 x_2 \cdots x_{r-1}.$$

Properties: $\mathbf{c}(x) = (\tau^{-p}(x_1))^{-1} x (\tau^{-p}(x_1)) \quad ; \quad \mathbf{d}(x) = x_r x x_r^{-1}$

$\inf(x) \leq \inf(\mathbf{c}(x)) \quad ; \quad \sup(x) \geq \sup(\mathbf{d}(x))$

Finding an element in SSS(x): Perform cycling for increasing the infimum, since:

Elrifai-Morton, Birman-Ko-Lee: There exists a positive integer k_1 such that $\inf(\mathbf{c}^{k_1}(x)) > \inf(x)$.

We get: element $\widehat{x}$ of maximal infimum.

Perform decycling for decreasing the supremum, since:

Elrifai-Morton, Birman-Ko-Lee: There exists a positive integer k_2 such that $\sup(\mathbf{d}^{k_2}(\widehat{x})) < \sup(\widehat{x})$.

We get: element in SSS(x).

Complexity (Elrifai-Morton, Birman-Ko-Lee): at most rm (r=length in Artin generators, m=canonical length).

Example (Elrifai-Morton): Let $P = \sigma_1\sigma_2^2\sigma_3\sigma_1\sigma_2^2$.

Left canonical form: $P = (\sigma_1\sigma_2)(\sigma_2\sigma_3\sigma_1\sigma_2)(\sigma_2)$;
$\inf(P) = 0$; $\sup(P) = 3$.

One cycling:

$$\begin{aligned}\mathbf{c}(P) &= (\sigma_2\sigma_3\sigma_1\sigma_2)(\sigma_2)(\sigma_1\sigma_2) = (\sigma_2\sigma_3\sigma_1\sigma_2)(\sigma_2\sigma_1\sigma_2) = \\ &= (\sigma_2\sigma_3\sigma_1\sigma_2)(\sigma_1\sigma_2\sigma_1) = (\sigma_2\sigma_3\sigma_1\sigma_2\sigma_1)(\sigma_2\sigma_1);\end{aligned}$$

$\inf(\mathbf{c}(P)) = 0$, $\sup(\mathbf{c}(P)) = 2$.

One further cycling:

$$\mathbf{c}^2(P) = (\sigma_2\sigma_1)(\sigma_2\sigma_3\sigma_1\sigma_2\sigma_1) = \Delta_4\sigma_2;$$

$\inf(\mathbf{c}^2(P)) = 1$; $\sup(\mathbf{c}^2(P)) = 2$.

Exploring the set SSS(x).

Proposition (Elrifai-Morton, 1994): Let $x \in B_n$ and $V \subset$ SSS(x) be non-empty. If $V \neq$ SSS(x), then there exist $y \in V$ and a permutation braid s such that $s^{-1}ys \in \text{SSS}(x) \setminus V$.

Proposition (Franco, Gonzales-Meneses, 2003): Let $x \in B_n$ and $V \subset$ SSS(x) be non-empty. If $V \neq$ SSS(x), then there exist $y \in V$ such that $\sigma_i^{-1}y\sigma_i \in \text{SSS}(x) \setminus V$.

This exploring algorithm computes a directed graph:
Vertices: the set SSS(x).
Edges: for $y, z \in$ SSS(x), $y \xrightarrow{\sigma_i} z$ if $\sigma_i^{-1}y\sigma_i = z$.

Problem: The size of SSS(x) is very big.

The Ultra Summit Sets
Gebhardt (2005)

$I_x = \text{USS}(x)$, the Ultra Summit Set of x, consisting of the conjugates of x in $\text{SSS}(x)$, which satisfy $\mathbf{c}^m(y) = y$ for some $m > 0$ ($\text{USS}(x)$ is smaller than $\text{SSS}(x)$).

$\text{USS}(x)$ consists of a finite set of disjoint orbits, closed under cycling, decycling and the operator τ.

Examples (Birman, Gebhardt, Gonzales-Meneses, 2006):

• $\mathrm{USS}(\sigma_1) = \mathrm{SSS}(\sigma_1) = \mathrm{SS}(\sigma_1) = \{\sigma_1, \ldots, \sigma_{n-1}\}$, and each element is an orbit under cycling, since $\mathbf{c}(\sigma_i) = \sigma_i$ for $i = 1, \ldots, n-1$.

• $x = \sigma_1\sigma_3\sigma_2\sigma_1 \cdot \sigma_1\sigma_2 \cdot \sigma_2\sigma_1\sigma_3 \in B_4$.
$|\mathrm{USS}(x)| = 6$ while $|\mathrm{SSS}(x)| = 22$.

$\mathrm{USS}(x)$ consists of 2 closed orbits under cycling: $\mathrm{USS}(x) = O_1 \cup O_2$, each one containing 3 **rigid** elements:

$$
\begin{aligned}
O_1 &= \{\sigma_1\sigma_3\sigma_2\sigma_1 \cdot \sigma_1\sigma_2 \cdot \sigma_2\sigma_1\sigma_3, \sigma_1\sigma_2 \cdot \sigma_2\sigma_1\sigma_3 \cdot \sigma_1\sigma_3\sigma_2\sigma_1, \\
&\quad\ \sigma_2\sigma_1\sigma_3 \cdot \sigma_1\sigma_3\sigma_2\sigma_1 \cdot \sigma_1\sigma_2\}, \\
O_2 &= \{\sigma_3\sigma_1\sigma_2\sigma_3 \cdot \sigma_3\sigma_2 \cdot \sigma_2\sigma_3\sigma_1, \sigma_3\sigma_2 \cdot \sigma_2\sigma_3\sigma_1 \cdot \sigma_3\sigma_1\sigma_2\sigma_3, \\
&\quad\ \sigma_2\sigma_3\sigma_1 \cdot \sigma_3\sigma_1\sigma_2\sigma_3 \cdot \sigma_3\sigma_2\}.
\end{aligned}
$$

Note that $O_2 = \tau(O_1)$.

Remark: In **generic** case, $|\mathrm{USS}(x)|$ is either ℓ or 2ℓ ($\ell = \mathrm{len}(x)$) (depends on whether $\tau(O_1) = O_1$) containing rigid braids **(Gebhardt)**. There are exceptions in non-generic case: for $E \in B_{12}$:

$$\begin{aligned} E \;=\; & (\sigma_2\sigma_1\sigma_7\sigma_6\sigma_5\sigma_4\sigma_3\sigma_8\sigma_7\sigma_{11}\sigma_{10}) \cdot (\sigma_1\sigma_2\sigma_3\sigma_2\sigma_1\sigma_4\sigma_3\sigma_{10}) \cdot \\ & \cdot (\sigma_1\sigma_3\sigma_4\sigma_{10}) \cdot (\sigma_1\sigma_{10}) \cdot (\sigma_1\sigma_{10}\sigma_9\sigma_8\sigma_7\sigma_{11}) \cdot (\sigma_1\sigma_2\sigma_7\sigma_{11}) \end{aligned}$$

has an Ultra Summit Set of size 264, instead of the expected size 12 **(Birman, Gebhardt, Gonzales-Meneses)**.

The size and structure of the USS(x) depends on its Nielsen-Thurston type: periodic, reducible or Pseudo-Anosov **(Birman, Gebhardt, Gonzales-Meneses)**.

Finding an element in USS(x): First, perform cycling and decycling for getting an element in $\tilde{x} \in$ SSS(x).

Then start cycling it. We get two integers m_1, m_2 ($m_1 < m_2$), which satisfy:

$$\mathbf{c}^{m_1}(\tilde{x}) = \mathbf{c}^{m_2}(\tilde{x})$$

$\widehat{x} = \mathbf{c}^{m_1}(\tilde{x}) \in$ USS(x), since $\mathbf{c}^{m_2 - m_1}(\widehat{x}) = \widehat{x}$.

Exploring USS(x) from $\hat{x} \in$ USS(x):

Definition: Given $x \in B_n$, $y \in$ USS(x). A permutation braid $s \neq 1$ is a minimal for y with respect to USS(x) if $s^{-1}ys \in$ USS(x), and no proper prefix of s satisfies this property.

Proposition (Gebhardt): Let $x \in B_n$ and $V \subseteq$ USS(x) be non-empty. If $V \neq$ USS(x), then there exist $y \in V$ and a generator σ_i such that $c_y(\sigma_i)$ is a minimal permutation braid for y, and $(c_y(\sigma_i))^{-1}y(c_y(\sigma_i)) \in$ USS(X) $\setminus V$.

Birman, Gebhardt, Gonzales-Meneses (2006): if $x \in$ USS(x) with len(x) $= k > 0$ and s be a minimal simple element for x. Then s is a prefix of either $\iota(x)$ or $\iota(x^{-1})$, or both, where $\iota(x)$ is the first factor of the Garside normal form.

As in Super Summit Sets, the algorithm for USS(x), compute a graph:
Vertices: elements of USS(x).
Edges: for $y, z \in$ USS(x), $y \xrightarrow{s} z$ if $s^{-1}ys = z$, where s is a minimal permutation braid.

Complexity: Although the number of cycling m_2 for finding an element in USS(x) is not known in general, in practice, **the algorithm based on the Ultra Summit Sets is substantially better** for braid groups.

More results: Talk of Gonzales-Meneses in the conference ...

A heuristic algorithm using the Super Summit Sets

Hofheinz-Steinwandt (2002)

Idea: we hope that the representatives in SSS of two conjugated elements will not be too far away (one is a conjugation of the other by a permutation braid).

So, given a pair (x, x') of braids, where $x' = s^{-1}xs$, we do:
1. By a variant of cycling and decycling, we find $\tilde{x} \in \mathrm{SSS}(x)$ and $\tilde{x}' \in \mathrm{SSS}(x')$.
2. Try to find a permutation braid P, such that $\tilde{x}' = P^{-1}\tilde{x}P$. (using the symmetric group).

Remark: In such cases, we can find also the conjugator.

Actually, one can find any $\tilde{s}$ (commuted with r) which satisfies $x' = \tilde{s}^{-1} x \tilde{s}$ which will do the job, since after $r^{-1}pr$ is known:

$$\tilde{s}^{-1} r^{-1} p r \tilde{s} = r^{-1} \tilde{s}^{-1} p \tilde{s} r = r^{-1} x' r$$

which is the shared key.

Success rate: Almost 100% of the cases in the Anshel-Anshel-Goldfeld protocol, and about 80% of the cases in the Diffie-Hellman-type protocol.

Attacks based on linear representations

Idea: map the braid groups into groups of matrices, in which the Conjugacy Search Problem is easy, and lift up the result to the braid group.

Two main representations:
1. **Burau representation** - for $n \geq 5$ is not faithful, but since its kernel is very small - it still might be possible (**Hughes, 2002**). Some variant was broken by **Lee-Lee (2002)**.
2. **Lawrence-Krammer representation** - it is faithful (**Bigelow (2001), Krammer (2002)**), and hence can be used as an attack to Diffie-Hellman-type protocol (**Cheon-Jun, 2003**).

Length-based attack
Hughes-Tannenbaum (2002)

Property: For a **length function** ℓ defined on B_n, usually

$$\ell(a^{-1}ba) > \ell(b)$$

for elements $a, b \in B_n$.

Idea: If $b = x^{-1}ax$ and $x = g_1 \cdot g_2 \cdots g_k$, the following hopefully holds with a non-negligible probability:

$$\ell(g_k x^{-1} a x g_k^{-1}) < \ell(g x^{-1} a x g^{-1})$$

for any generator $g \neq g_k$.

In this way, we try to reveal x by peeling off generator after generator.

Improvements:

- Generalization to solution of equations **(G-Kaplan-Teicher-Tsaban-Vishne, 2005)**
- Memory approach **(G-Kaplan-Teicher-Tsaban-Vishne, 2005)**
- Better length functions **(Hock-Tsaban, 2006)**
- Application to other groups **(Ruinskiy-Shamir-Tsaban, 2007)**

Will be discussed in my conference talk ...

Cycling problem as a potential hard problem

Ko-Lee-Cheon-Han-Kang-Park (2000): **Cycling Problem** might be hard.

Cycling Problem: Given a braid y and a positive integer t such that y is in the image of the operator $\mathbf{c}^t$. Find a braid x such that $\mathbf{c}^t(x) = y$.

Not so hard!

Maffre (2005): Given y, one can find x such that $\mathbf{c}(x) = y$ very fast.

Gebhardt and Gonzales-Meneses (2007): General Cycling Problem has a polynomial solution, since the cycling operation is **surjective**, so apply Maffre's algorithm t times.

Future directions

1. A cryptosystem based on the Shifted Conjugacy Search Problem

Dehornoy (2006)

Let $x, y \in B_\infty$. We define:

$$x * y = x \cdot \mathrm{d}y \cdot \sigma_1 \cdot \mathrm{d}x^{-1}$$

where $\mathrm{d}x$ is the shift of x in B_∞, i.e. $\mathrm{d}(\sigma_i) = \sigma_{i+1}$ for each $i \geq 1$.

Shifted Conjugacy Search Problem: Let $s, p \in B_\infty$ and $p' = s * p$. Find a braid $\tilde{s}$ satisfying $p' = \tilde{s} * p$.

Fiat-Shamir authentication scheme:
S is a set and $(F_s)_{s\in S} : S \to S$ is a family of functions satisfying:

$$F_r(F_s(p)) = F_{F_r(s)}(F_r(p)), \qquad r, s, p \in S$$

Alice is the prover who wants to convince Bob that she knows the secret key s:

Private key: Alice: $s \in S$.
Public keys: Two elements $p, p' \in S$ such that $p' = F_s(p)$.

Alice: Chooses a random $r \in S$ and sends Bob $x = F_r(p)$ and $x' = F_r(p')$.
Bob: Chooses a random bit c and sends it to Alice.
Alice:
If $c = 0$, sends $y = r$ (then Bob checks: $x = F_y(p)$ and $x' = F_y(p')$);
If $c = 1$, sends $y = F_r(s)$ (then Bob checks: $x' = F_y(x)$).

Dehornoy (2006): A **LD-system** is a set S with a binary operation which satisfies: $r * (s * p) = (r * s) * (r * p)$.

The Fiat-Shamir-type authentication scheme on LD-systems:

Private key: Alice: $s \in S$.
Public keys: Two elements $p, p' \in S$ such that $p' = s * p$.

Alice: Chooses a random $r \in S$ and sends Bob $x = r * p$ and $x' = r * p'$.
Bob: Chooses a bit c and sends it to Alice.
Alice:
If $c = 0$, sends $y = r$ (then Bob checks: $x = y * p$ and $x' = y * p'$);
If $c = 1$, sends $y = r * s$ (then Bob checks: $x' = y * x$).

LD-system on braid group: B_∞ with the shifted conjugacy operation.

Further research:

1. **Cryptanalysis direction:** What is the success rate of a length-based attack on this scheme?

2. **Cryptanalysis direction:** Can one develop any theory (like Summit Sets) for the Shifted Conjugacy Search Problem?

3. **Cryptosystem direction:** Can one suggest a LD-system on the braid group, which will be secure for the length-based attack?

4. **Cryptosystem direction:** Can one suggest a LD-system on a different noncommutative group, which will be secure?

2. A cryptosystem based on the shortest braid problem

Settings: B_∞, Generators $\{\sigma_1, \sigma_2, \ldots\}$ subject to the usual braid relations.

Minimal Length Problem (or Shortest Word Problem): Starting with a word w in the $\sigma_i^{\pm 1}$'s, find the shortest word w' which is equivalent to w, i.e., that satisfies $w' \equiv w$.

Paterson and Razborov (1991): The Minimal Length Problem is co-NP-complete.

Hardness for B_n for fixed n is not known.

From the point of view of cryptography, we are interested to construct relatively large families of provably difficult instances in which the keys may be randomly chosen.

Dehornoy (2004): Braids of the form $w(\sigma_1^{e_1}, \sigma_2^{e_2}, \ldots, \sigma_n^{e_n})$ with $e_i = \pm 1$, i.e., braids in which, for each i, at least one of σ_i or σ_i^{-1} does not occur, could be relevant.

Possible problem: The shortest word problem in B_n for a fixed n might be not so hard.

Some indications:
For B_3: **Berger** (Artin), **Wiest** (Artin), **Xu** (BKL).
For B_4: **Kang-Ko-Lee** (BKL).
For B_n, n fixed (small): Conjecture: **Wiest** (Artin), **G-Kaplan-Tsaban** (Artin).

Further research:

1. **Cryptosystem direction**: Suggest a cryptosystem based on the shortest word problem in B_∞, using the hardness result of Paterson-Razborov?

2. **Cryptanalysis direction**: What is the final status of the shortest word problem in B_n for a fixed n?

3. Alternative distributions

Idea: Try to change the distribution of the generators.

Markov walk: the distribution of the choice of the next generator depends on the choice of the current chosen generator.

Maffre (2006): Proposes a new random generator of key which is secure against his attack and the one of Hofheinz-Steinwandt.

Further research: Is it secure from the other attacks too?

4. Cryptosystems based on different non-commutative groups

Further Research: Can one suggest a different non-commutative group where the suggested protocols on the braid group can be applied, and the cryptosystem will be secure?

For applying Diffie-Hellman, one needs **two subgroups which commutes element-wise**.

Some possibilities:

1. Thompson group **(Shpilrain-Ushakov, 2006)**.
2. Miller groups (groups with an abelian automorphism group) **(Mahalanobis, 2005)**.