The Conjugacy Problem: Cryptoanalytic approaches to Dehn's Problem

Boaz Tsaban

Partially joint with

David Garber, Arkadius Kalka, Mina Teicher, Gary Vinokur

Bar-Ilan University

GAGTA-6, July/August 2012 CE

Part I

Key Exchange Protocols

and

Representation attacks

Key Exchange Protocols (KEPs)

Alice and Bob wish to communicate over an insecure channel.

$\exists$ Efficient & secure methods if they share a secret ("key"):
Symmetric encryption (AES,...).

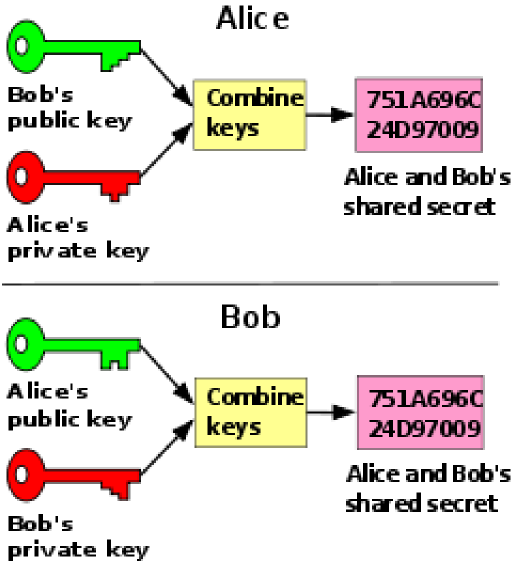
How to decide a shared secret key over an insecure channel?

Diffie–Hellman 1976. Key Exchange Protocol.

The most important breakthrough in cryptography.

In this minicourse: Only passive adversaries.
The kernel on which more involved PKC is built.

Key Exchange Protocol - the concept



Courtesy of Wikipedia

The Diffie–Hellman KEP

Alice	**Public**	**Bob**
$a \in \{0, 1, \ldots, p-1\}$	$G = \langle g \rangle,\ |G| = p$	$b \in \{0, 1, \ldots, p-1\}$

$$\xrightarrow{\boxed{g^a}}$$

$$\xleftarrow{\boxed{g^b}}$$

$$K = \boxed{g^b}^{a} = g^{ab} \qquad\qquad K = \boxed{g^a}^{b} = g^{ab}$$

Exponentiation. $x \mapsto g^x$ via square and multiply, $O(\log_2 p)$.

Security of the Diffie–Hellman KEP

Diffie–Hellman Problem. $(g^a, g^b) \mapsto g^{ab}$.

Discrete Logarithm Problem. $g^x \mapsto x$.

DLP $\geq$ DHP.

Both are ϵ-hard.

Ts 2006. None depends on generator choice.

The Discrete Logarithm Problem

Discrete Logarithm Problem. $g^x \mapsto x$.

Depends on the group!

$G = (\mathbb{Z}_p, +)$. $g = 1$. "g^x" $= x \cdot g = x \cdot 1 = x$.

$G \leq (\mathbb{Z}_p^*, \cdot)$. Quite, but not enough, hard:

NFS. $n := \log_2(p)$: $\quad \mathbf{2}^{\,(1.33 + o(1)) n^{1/3} (\log_2 n)^{2/3}}$.

n	NFS Work Prediction	Year Broken
525	2^{47}	2002
578	2^{49}	2003
664	2^{52}	2005
768	2^{55}	2009
1024	2^{62}	2016?

10,000 bits prime for "eternal" security? Impractical.

The future of cryptography

$G \leq$ Elliptic Curve. Nothing better than $2^{n/2}$. Yet.

ECC. Rich mathematics $\rightarrow \cdots \rightarrow$ algorithmic breakthroughs?

Quantum Computers. Break all Diffie–Hellman KEPs.

Theoretic.

But what is your alternative?

Rivest-Shamir-Adleman (RSA, 1978). As easy as DLP in $\mathbb{Z}_p^*$.

Lattice-based? Maybe.

How about noncommutative groups?

WIN/WIN: New KEP / efficient algorithms.

The Braid Diffie–Hellman KEP

Diffie–Hellman KEP 1976.

Alice	**Public**	**Bob**
$a \in \{0, 1, \ldots, p-1\}$	$G = \langle g \rangle, \ |G| = p$	$b \in \{0, 1, \ldots, p-1\}$

$$\xrightarrow{\boxed{g^a}}$$

$$\xleftarrow{\boxed{g^b}}$$

$$K = \boxed{g^b}^{a} = g^{ab} \qquad\qquad K = \boxed{g^a}^{b} = g^{ab}$$

The Braid Diffie–Hellman KEP

Ko–Lee–Cheon–Han–Kang–Park 2000. G noncommutative.

$g^x := x^{-1} g x$.

Alice	**Public**	**Bob**
$a \in A$	$A, B \leq G, g \in G, [A, B] = 1$	$b \in B$

$$\xrightarrow{\boxed{g^a}}$$

$$\xleftarrow{\boxed{g^b}}$$

$K = \boxed{g^b}^a = g^{ba}$ $\qquad$ $K = \boxed{g^a}^b = g^{ab}$

Dehn's Problems 1911

$G = \langle X \mid R \rangle$.

Word Problem. Decide whether $g = 1$.

Conjugacy Problem. Decide whether g, h are conjugate.
(AKA Generalized Word Problem.)

Isomorphism Problem. Decide whether G, H are isomorphic.

Originally, decision problems. Crypto uses the search versions.

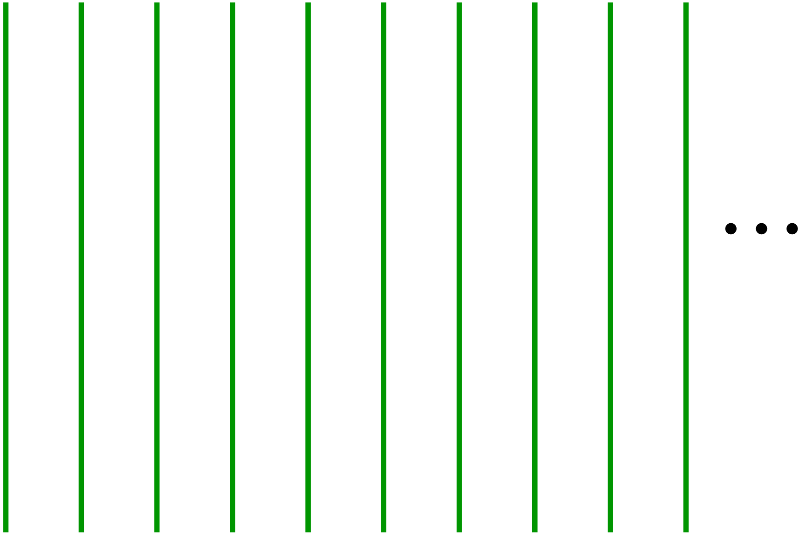
Unlike the decision problems, the search problems are decidable, but we ask for efficient solutions.

Proposed platform. Artin's braid group. (TBD)

Motivated a new line of research in combinatorial group theory.

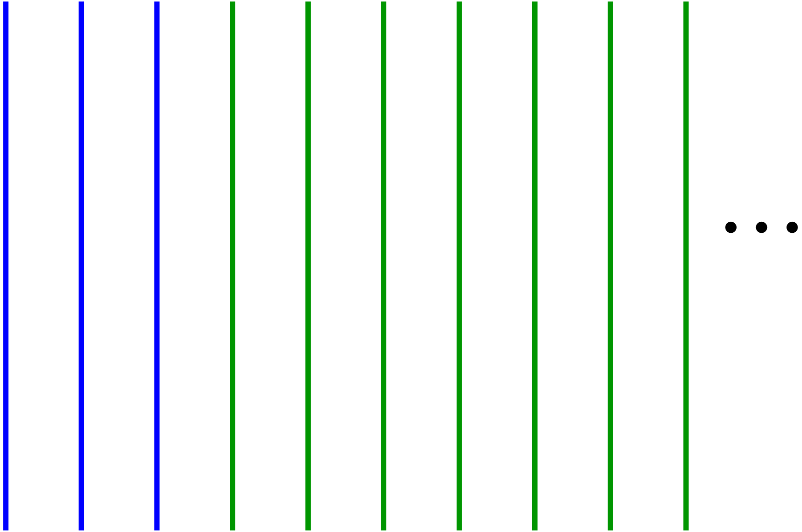
Artin's braid group $\mathbf{B}$

Identity braid:



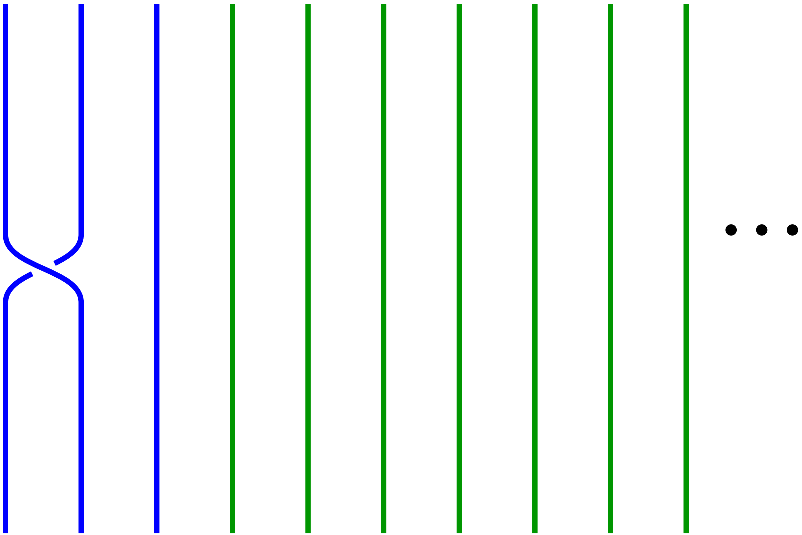
The ordinary braid

1:



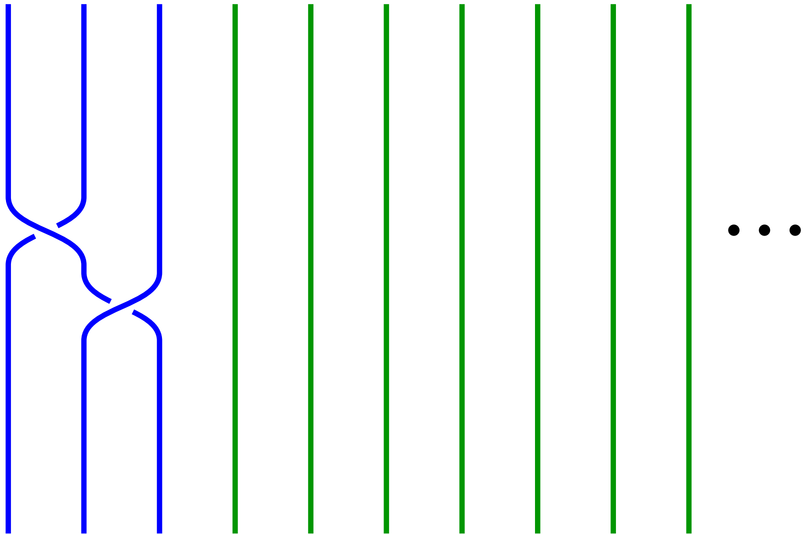
The ordinary braid

σ_1^{-1}:



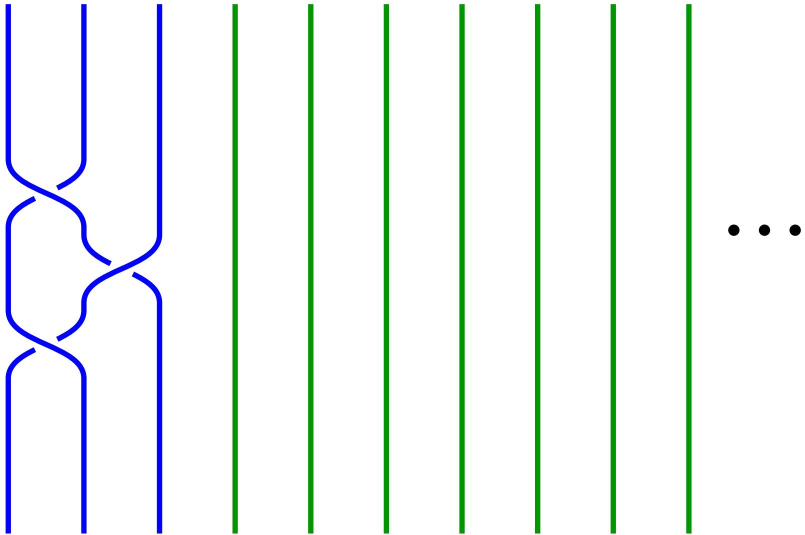
The ordinary braid

$\sigma_1^{-1}\sigma_2$:



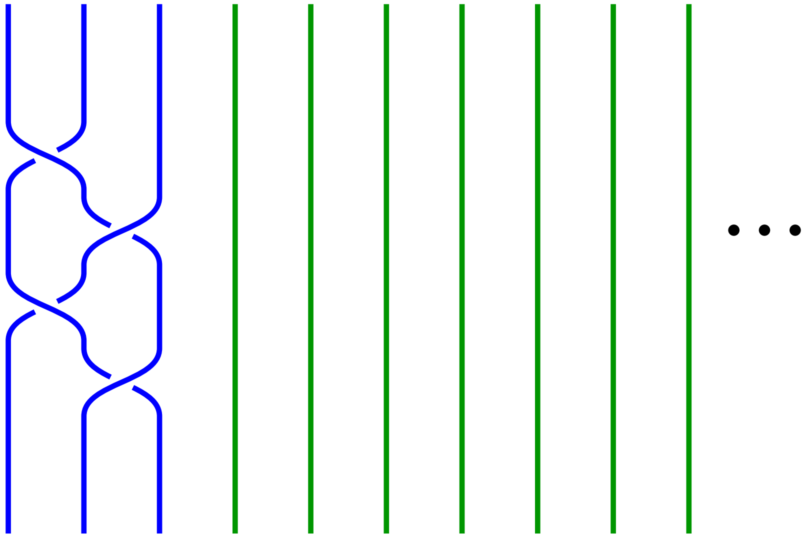
The ordinary braid

$\sigma_1^{-1}\sigma_2\sigma_1^{-1}$:



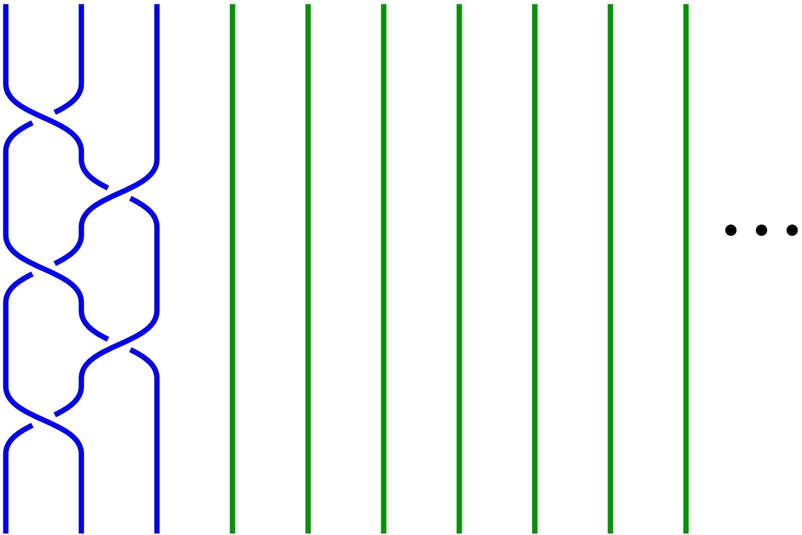
The ordinary braid

$\sigma_1^{-1}\sigma_2\sigma_1^{-1}\sigma_2$:



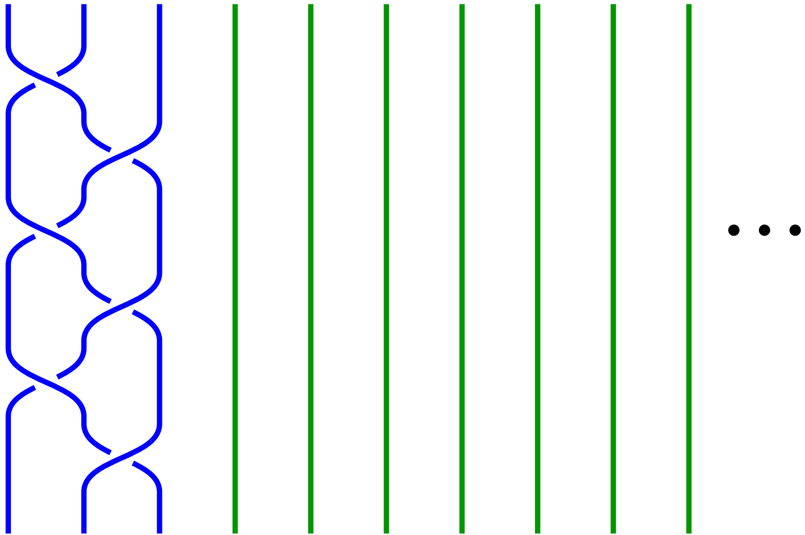
The ordinary braid

$\sigma_1^{-1}\sigma_2\sigma_1^{-1}\sigma_2\sigma_1^{-1}$:



The ordinary braid

$\sigma_1^{-1}\sigma_2\sigma_1^{-1}\sigma_2\sigma_1^{-1}\sigma_2$:



Real life applications

A Challah.

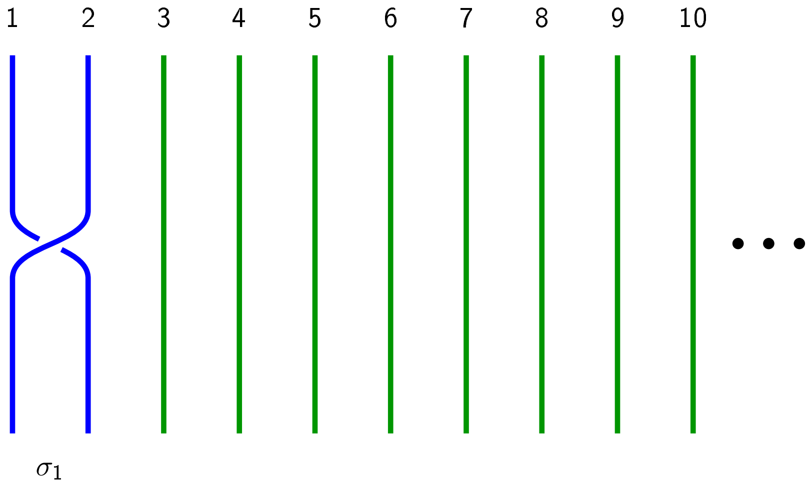
Artin's braid group $\mathbf{B}$

$\mathbf{B}$: Braids / isotopy.

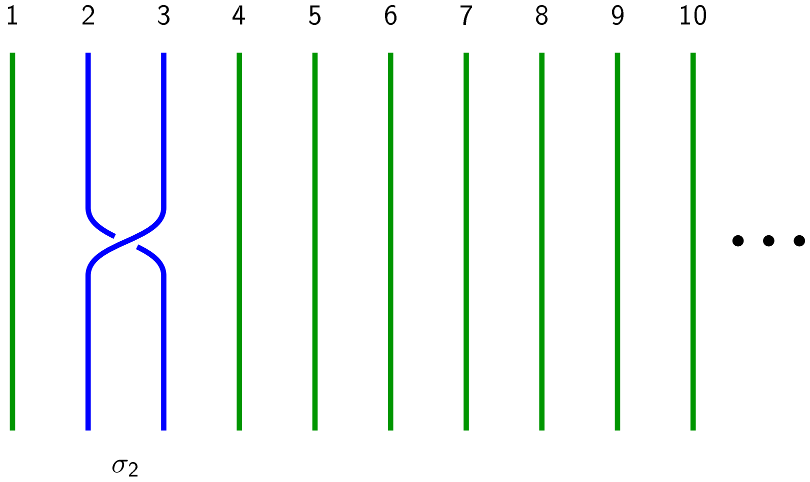
Multiplication: Concatenation of braids.

Inversion: Mirror braid.

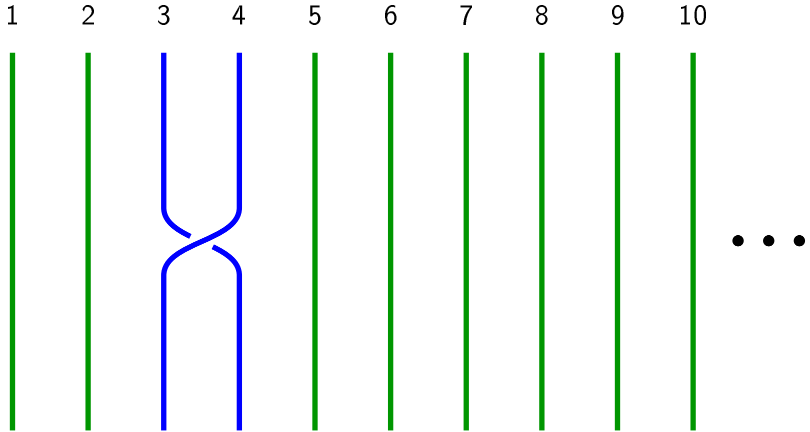
Generators of the braid group



Generators of the braid group

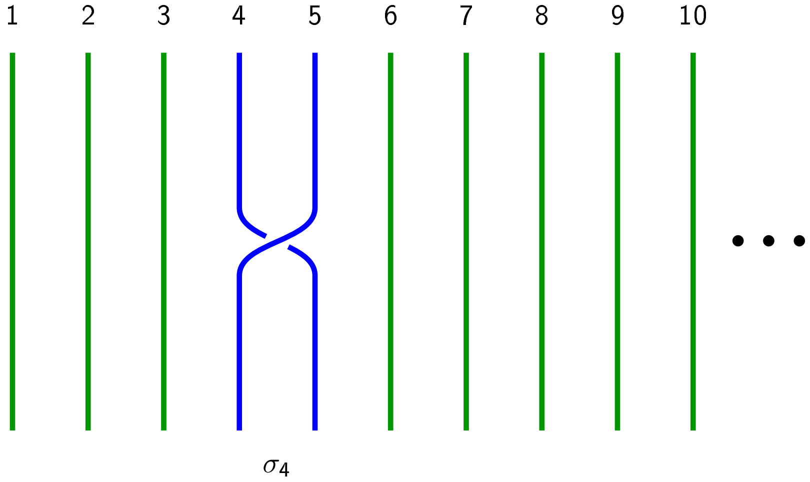


Generators of the braid group

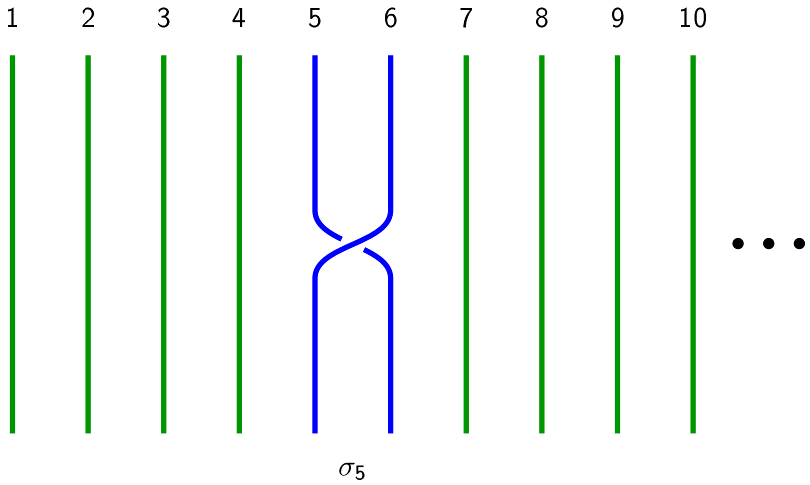


σ_3

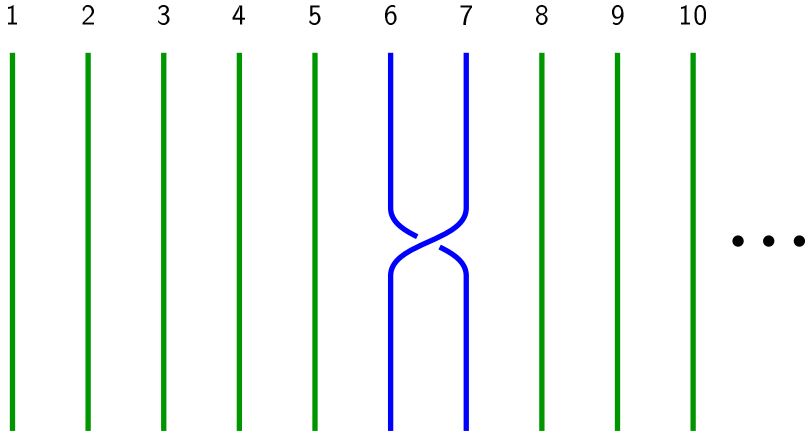
Generators of the braid group



Generators of the braid group

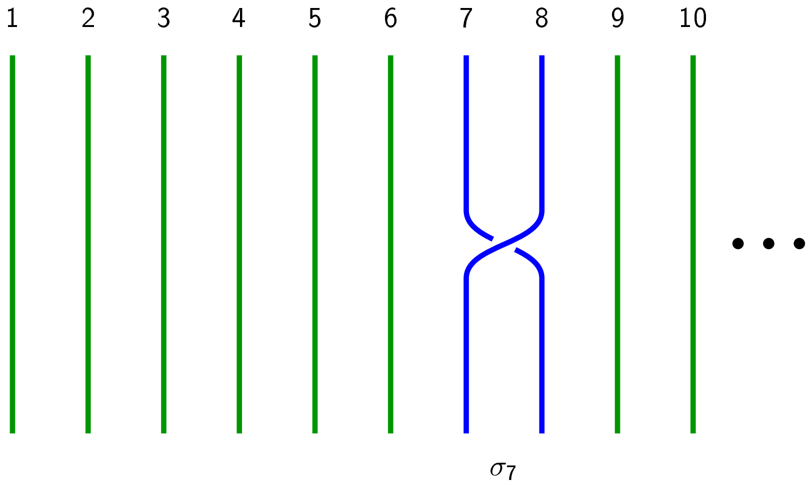


Generators of the braid group

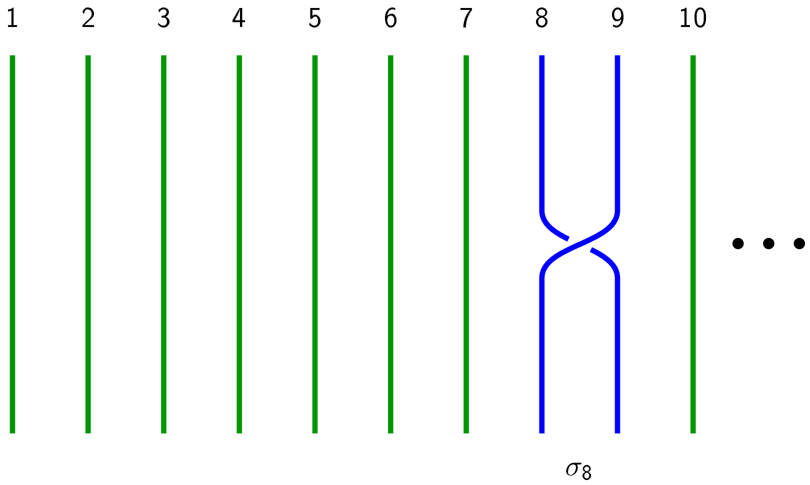


σ_6

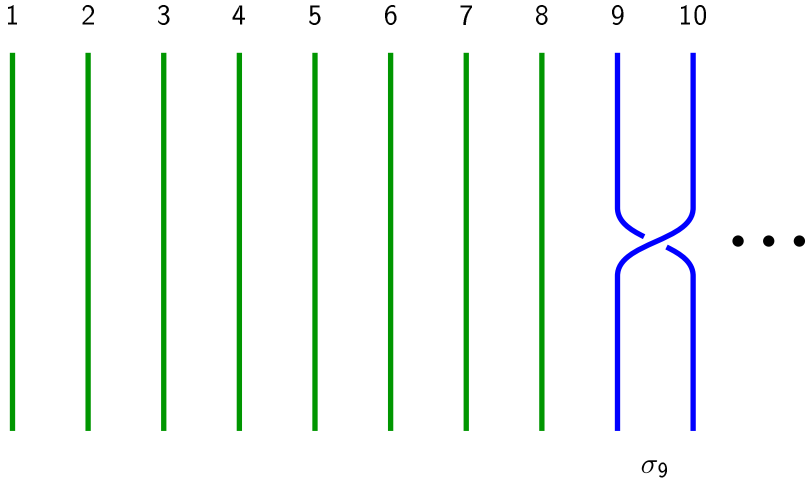
Generators of the braid group



Generators of the braid group

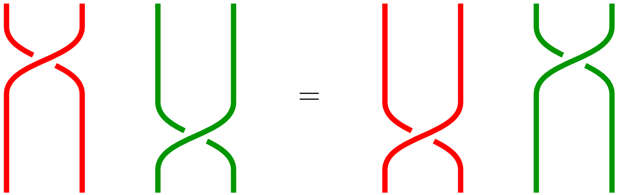


Generators of the braid group

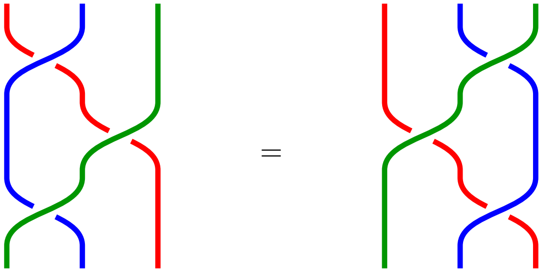


Relations in the braid group

Far Commutativity: $\sigma_i \sigma_j = \sigma_j \sigma_i$ for $i + 1 < j$.



Triple relation: $\sigma_i \sigma_{i+1} \sigma_i = \sigma_{i+1} \sigma_i \sigma_{i+1}$.



Normal forms

Think DH KEP in $(\mathbb{Z}/p\mathbb{Z})^*$ instead of $\mathbb{Z}_p^*$:

1. May not get the same key if choice not canonical!
2. Breakable!

Normal form: $n \mapsto (n \bmod p)$:

1. Ensures same key.
2. Hides the generation info.

Braid Diffie–Hellman KEP uses $\mathbf{B}$ as platform group.

Normal form in $\mathbf{B}$?

The positive monoid $\mathbf{B}^+$

$$\mathbf{B}^+ = \mathrm{Mon}\left\langle \sigma_1, \sigma_2, \ldots \;\middle|\; \begin{array}{rcl} \sigma_i\sigma_j & = & \sigma_j\sigma_i \ (i+1 < j), \\ \sigma_i\sigma_{i+1}\sigma_i & = & \sigma_{i+1}\sigma_i\sigma_{i+1} \end{array} \right\rangle.$$

Garside 1969:

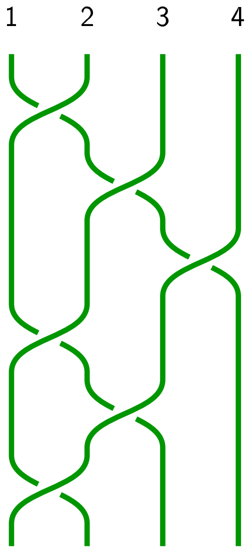
1. Equivalent positive braids are positive-equivalent.
2. $\therefore$ Equivalence classes of positive braids are finite.
3. Lex-minimal representatives are normal forms in $\mathbf{B}^+$.

Not efficient, but the theme will become useful later.

For simplicity, henceforth work in:

$\mathbf{B}_N$: $\langle \sigma_1, \ldots, \sigma_{N-1} \rangle \leq \mathbf{B}$, supported by the leftmost n strands.

The fundamental braid Δ



$\Delta = (\sigma_1\sigma_2\sigma_3)(\sigma_1\sigma_2)\sigma_1$

$$
\begin{array}{rcl}
\sigma_i\Delta & = & \Delta\sigma_{N-i} \\
\Delta^2 & \in & Z(\mathbf{B}_N) \\
\sigma_i\Delta^{-1} & = & \Delta^{-1}\sigma_{N-i} \\
\Delta & \in & \sigma_i\mathbf{B}^+ \\
\Delta & \in & \mathbf{B}^+\sigma_i \\
\Delta\sigma_i^{-1} & \in & \mathbf{B}^+
\end{array}
$$

$\forall b \in \mathbf{B}_N \exists$ minimal $|p|,\ b = \Delta^i \cdot \overset{\substack{\mathbf{B}^+ \\ \cup}}{p}$

p_{lexmin} := lex minimum of these p's

Garside's normal form of $b := \Delta^i \cdot p_{\mathrm{lexmin}}$

inf$(b) := i$ (maximal)

Permutation braids and an efficient normal form

$a \leq b$: $\exists p \in \mathbf{B}_N{}^+,\ ap = b$.

$\mathbf{B}_N{}^+ = \{p \in \mathbf{B}_N\ :\ 1 \leq p\}$.

$p \in S$: $1 \leq p \leq \Delta$.

Permutation braids: $S \cong^{\text{eff}} S_N$.
Canonical expression by transpositions $(i, i+1)$.

Adyan 1984–Thurston 1992–Elrifai–Morton 1994 Normal Form.

$$b = \Delta^{\inf(b)} p_1 p_2 \cdots p_\ell$$

$p_i \in P$ of maximal length, $i = 1, 2, \ldots, \ell$ (left-weighted).

Complexity: $|b|^2 N \log N$.

The Braid Diffie–Hellman KEP

$G = \mathbf{B}_N$.

Alice	**Public**	**Bob**
$a \in A$	$A, B \leq G, g \in G, [A, B] = 1$	$b \in B$

$$\xrightarrow{\boxed{g^a}}$$

$$\xleftarrow{\boxed{g^b}}$$

$K = \boxed{g^b}^a = g^{ba}$ $\qquad$ $K = \boxed{g^a}^b = g^{ab}$

Problems related to the Braid Diffie–Hellman KEP

$A, B \leq G, g \in G, [A, B] = 1.$

BDH Problem. $(g^a, g^b) \mapsto g^{ab}$ $(a \in A, b \in B)$.

Conjugacy Search Problem (CSP). $g^x \mapsto \tilde{x}$, $g^x = g^{\tilde{x}}$ $(g, x \in G)$.

CSP1. $g^a \mapsto \tilde{a} \in C_G(B)$, $g^a = g^{\tilde{a}}$.

CSP2. $g^a \mapsto \tilde{a} \in A$, $g^a = g^{\tilde{a}}$.

CSP2 $\geq$ CSP1 $\geq$ BDH Problem.

Representations of $\mathbf{B}_N$

Burau 1936. $\sigma_i \mapsto I_{i-1} \oplus \begin{pmatrix} 1-t & t \\ 1 & 0 \end{pmatrix} \oplus I_{N-i-1} \in \mathrm{GL}_N(\mathbb{Z}[t^{\pm 1}])$.

Moody 91, Long–Paton 93, Bigelow 99. Not faithful for $N \geq 5$.

Lawrence–Krammer. $\mathrm{LK}\colon \mathbf{B}_N \longrightarrow \mathrm{GL}_{\binom{N}{2}}(\mathbb{Z}[t^{\pm 1}, q^{\pm 1}])$.

Bigelow 2001 (JAMS), Krammer 2002 (Annals):
LK representation is faithful for all N.

Cheon–Jun 2003.

1. LK Evaluation: Fast. Inversion: Roughly N^6 (acceptable).
2. Sufficient to find the key's image κ in a field

$$\mathbb{Z}[t^{\pm 1}, q^{\pm 1}]/\langle p, f(t), g(q)\rangle$$

with $\kappa \bmod \langle p, f(t), g(q)\rangle = \kappa$.

Representation attack

BDH Problem. $(g^a, g^b) \mapsto g^{ab}$ $(a \in A, b \in B)$.

Cheon–Jun 2003. Representation attack.

Assume $G \cong^{\mathrm{eff}}$ matrix group. Think G is a matrix group.

$$\boxed{g^a} = a^{-1} g a \iff a \cdot \boxed{g^a} = g \cdot a$$

Solve

$$\begin{cases} a \cdot \boxed{g^a} & = & g \cdot a \\ a \cdot B & = & B \cdot a \end{cases} \implies \alpha \text{ s.t. } \begin{cases} \alpha \cdot \boxed{g^a} & = & g \cdot \alpha \\ \alpha \cdot B & = & B \cdot \alpha \end{cases}$$

Then $\boxed{g^b}^{\alpha} = g^{b\alpha} = g^{\alpha b} = (g^{\alpha})^b = \boxed{g^a}^{b} = g^{ab} = K$!

Possibly, $\alpha \notin G$, but this works ! Complexity: $(n^2)^3 = N^{12}$.

To resurrect the Braid Diffie–Hellman KEP

Problem. Find G without any representation that is:

1. low-dimensional,
2. faithful, and
3. efficiently computable in both directions.

Second Braid Diffie–Hellman KEP

Cha–Ko–Lee–Han–Cheon 2001.

Alice	**Public**	**Bob**
$a_1 \in A_1, a_2 \in A_2$	$A_1, A_2, B_1, B_2 \leq G, g \in G$	$b_1 \in B_1, b_2 \in B_2$
	$\xrightarrow{\boxed{a_1 g a_2}}$	
	$\xleftarrow{\boxed{b_1 g b_2}}$	
$K = a_1 \boxed{b_1 g b_2} a_2$		$K = b_1 \boxed{a_1 g a_2} b_2$

Cheon–Jun 2003. Similar representation attack:

$$c = a_1 g a_2 \iff \boxed{a_1^{-1}} \cdot c = g \cdot a_2.$$

Finding an invertible solution

Problem. Find an invertible matrix in a subspace of $M_n(\mathbb{F})$.

Cheon–Jun Heuristic. Pick "random" elements until invertible.

Ts. Assume $\operatorname{span}\{A_1, \ldots, A_m\} \cap \mathrm{GL}_n(\mathbb{F}) \neq 0$. Then

$$\Pr(|\alpha_1 A_1 + \cdots + \alpha_m A_m| \neq 0) \geq 1 - \frac{n}{|\mathbb{F}|}.$$

Proof: $f(x_1, \ldots, x_m) := |x_1 A_1 + \cdots + x_m A_m| \in \mathbb{F}[x_1, \ldots, x_m]$, nonzero, degree n.

Schwartz 1980–Zippel 1989 Lemma.
$f(x_1, \ldots, x_m) \in \mathbb{F}[x_1, \ldots, x_m]$ nonzero degree n.

$$\Pr(f(x_1, \ldots, x_m) \neq 0) \geq 1 - \frac{n}{|\mathbb{F}|}.$$

The Shpilrain–Ushakov KEP 2006

Alice	**Public**	**Bob**
$a_1 \in G$	$g \in G$	$b_2 \in G$
	$\xrightarrow{B \leq C_G(a_1)}$	
	$\xleftarrow{A \leq C_G(b_2)}$	
$a_2 \in A$		$b_1 \in B$
	$\xrightarrow{a_1 g a_2}$	
	$\xleftarrow{b_1 g b_2}$	
$K = a_1 b_1 g b_2 a_2$		$K = b_1 a_1 g a_2 b_2$

Linear Centralizer Attack on Shpilrain–Ushakov KEP

Ts (fresh!). Assume $G \leq M = M_n(\mathbb{F})$ (eq., eff. representable).

Key observations.

1. Can't constraint solutions of linear equations to groups, can constraint solutions to subspaces!
2. $H = \langle g_1, \dots, g_k \rangle \leq G \Rightarrow C_G(H) \subseteq C_M(H) = C_M(g_1, \dots, g_k)$.
   $\therefore$ $C_G(H)$ computable by solving
   $$\left\{ \begin{array}{rcl} x g_1 & = & g_1 x \\ & \vdots & \\ x g_k & = & g_k x \end{array} \right.$$
   linear equations in the n^2 entries of x, kn^6 operations.
3. $C_M(g_1, \dots, g_k)$ is a vector subspace of M.
4. $C_M(C_M(H))$ computable: $\dim(C_M(H)) \leq n^2$ equations.

In 2,4: May use instead few random $g \in H$, $C_M(H)$.

Representation attack (continued)

$g, a_1, b_2 \in G$, $B \leq C_G(a_1)$, $A \leq C_G(b_2)$, $a_2 \in A$, $b_1 \in B$.

Shpilrain–Ushakov Problem. $(a_1 g a_2, b_1 g b_2) \mapsto a_1 b_1 g a_2 b_2$.

$a_2 \in A \Rightarrow a_2 \in C_M(C_M(A)) \iff a_2^{-1} \in C_M(C_M(A))$.

$A \leq C_G(b_2) \Rightarrow b_2 \in C_G(A) \subseteq C_M(A) \Rightarrow [C_M(C_M(A)), b_2] = 1$.

Attack (Ts).

1. Compute bases for the subspaces $C_M(B)$, $C_M(C_M(A))$.
2. Solve $a_1 g = \boxed{a_1 g a_2} \cdot a_2^{-1}$
   with $a_1 \in C_M(B), a_2^{-1} \in C_M(C_M(A))$ invertible.
3. $\exists$ solution: (a_1, a_2^{-1}).
4. $\tilde{a}_1 \boxed{b_1 g b_2} \tilde{a}_2 \stackrel{!}{=} b_1 \tilde{a}_1 g \tilde{a}_2 b_2 = b_1 a_1 g a_2 b_2 = K$!
5. Complexity $\leq n^2 \cdot (n^2)^3 = N^{16}$, heuristically N^{12}.
   Not practical, but worst-case polytime.

The Commutator Key Exchange Protocol

Anshel–Anshel–Goldfeld 1999.

Alice	**Public**	**Bob**
$v(x_1, \ldots, x_k) \in F_k$	$\langle a_1, \ldots, a_k \rangle \leq G$	$w(x_1, \ldots, x_k) \in F_k$
$a = v(a_1, \ldots, a_k)$	$\langle b_1, \ldots, b_k \rangle \leq G$	$b = w(b_1, \ldots, b_k)$

$$\xrightarrow{\quad {b_1}^a, \ldots, {b_k}^a \quad}$$

$$\xleftarrow{\quad {a_1}^b, \ldots, {a_k}^b \quad}$$

$K = a^{-1} v({a_1}^b, \ldots, {a_k}^b)$ $\qquad\qquad$ $K = w({b_1}^a, \ldots, {b_k}^a)^{-1} b$

$$a^{-1} v({a_1}^b, \ldots, {a_k}^b) = a^{-1} a^b = a^{-1} b^{-1} a b = (b^a)^{-1} b = w({b_1}^a, \ldots, {b_k}^a)^{-1} b$$

Problems related to the Commutator KEP

$a \in \langle a_1, \ldots, a_k \rangle, b \in \langle b_1, \ldots, b_k \rangle \leq G$.

Commutator KEP Problem.

$$({b_1}^a, \ldots, {b_k}^a, {a_1}^b, \ldots, {a_k}^b) \mapsto a^{-1} b^{-1} ab.$$

Conjugacy Search Problem (CSP). $g^x \mapsto \tilde{x}, \; g^x = g^{\tilde{x}}$.

Multiple CSP. $({g_1}^x, \ldots, {g_k}^x) \mapsto \tilde{x}, \; ({g_1}^x, \ldots, {g_k}^x) = ({g_1}^{\tilde{x}}, \ldots, {g_k}^{\tilde{x}})$.

Multiple CSP is easy in matrix groups.

Polynomial time attack on Commutator KEP

$a \in \langle a_1, \ldots, a_k \rangle, b \in \langle b_1, \ldots, b_k \rangle \leq G$.

Commutator KEP Problem.

$$(b_1{}^a, \ldots, b_k{}^a, a_1{}^b, \ldots, a_k{}^b) \mapsto a^{-1}b^{-1}ab.$$

Ts, Linear Centralizer Attack (fresh!). WLOG G is a matrix group.

1. Compute a base for $C_M(C_M(b_1, \ldots, b_k))$.
2. Solve

$$\begin{array}{rcl} b_1 a & = & a \cdot \boxed{b_1{}^a} \\ & \vdots & \\ b_k a & = & a \cdot \boxed{b_k{}^a} \end{array} \quad ; \quad \begin{array}{rcl} a_1 b & = & b \cdot \boxed{a_1{}^b} \\ & \vdots & \\ a_k b & = & b \cdot \boxed{a_k{}^b} \end{array}$$

   with a invertible, $b \in C_M(C_M(b_1, \ldots, b_k))$ invertible.
3. $\exists$ solution: (a, b).

$$\tilde{a}^{-1}\tilde{b}^{-1}\tilde{a}\tilde{b} = \tilde{a}^{-1}\tilde{b}^{-1}(\tilde{a}a^{-1}a)\tilde{b} = \tilde{a}^{-1}(\tilde{a}a^{-1})\tilde{b}^{-1}a\tilde{b} = a^{-1}a^{\tilde{b}} = a^{-1}a^{b} = K\ !$$

The end of braid-based cryptography?

...and worse: of my lecture series?

Not quite:

1. N^{12} is impractical: 2^{96} (times constants) for $N = 256$.
2. There are additional braid-PKC proposals (Dehornoy, Kalka,...).
3. The other problems (CSP, Multiple CSP,...) remain open.

Linear Centralizer Attacks seem applicable to some of the other KEPs.
Probably not all: Fiat–Shamir Authentication based on CSP, etc.

The only way to rule out (most of) this approach is to solve the CSP.

Part II

Generic length-based algorithms

Solving equations in noncommutative groups

Assume: Finitely generated, efficiently solvable word problem (better: normal form).

Conjugacy Search Problem (CSP). $g^x \mapsto \tilde{x},\ g^x = g^{\tilde{x}}$ $(g, x \in G)$.

Root Search Problem. $x^2 \mapsto \tilde{x},\ x^2 = \tilde{x}^2$.

Double Coset Problem. $agb \in AgB \mapsto \tilde{a} \in A, \tilde{b} \in B,\ agb = \tilde{a}g\tilde{b}$.

$H_1, \ldots, H_k \leq G$, $w(t_1, \ldots, t_{k+m}) \in F_{k+m}$, $p_1, \ldots, p_m \in G$.

Solution Search Problem.
$w(h_1, \ldots, h_k, p_1, \ldots, p_m) \mapsto \tilde{h}_1 \in H_1, \ldots, \tilde{h}_k \in H_k$,
$w(h_1, \ldots, h_k, p_1, \ldots, p_m) = w(\tilde{h}_1, \ldots, \tilde{h}_k, p_1, \ldots, p_m)$.

Generalizes to systems of equations (e.g., Multiple CSP).

Solving equations in noncommutative groups

Solution Search Problem.
$w(h_1, \ldots, h_k, p_1, \ldots, p_m) \mapsto \tilde{h}_1 \in H_1, \ldots, \tilde{h}_k \in H_k$,
$w(h_1, \ldots, h_k, p_1, \ldots, p_m) = w(\tilde{h}_1, \ldots, \tilde{h}_k, p_1, \ldots, p_m)$.

Observations. Suffices to:

1. Find the leading variable.
2. Find a "small" list containing the solution.

Length-based algorithms. Find leading variable + expression in its subgroup.

Too ambitious, but they are heuristic.

Assumptions:

1. $h_1, \ldots, h_k$ sampled (somewhat) independently.
2. $\exists$ "well-behaved" length function: Usually $\ell(hg) > \ell(g)$.

Hughes–Tannenbaum 2002

$G = \langle g_1, \ldots, g_n \rangle$ (symmetric generating set).

Given g^x, $x = g_{i_1} \cdots g_{i_k}$.

$$
\begin{aligned}
g^x &= g_{i_k}^{-1} g_{i_{k-1}}^{-1} \cdots g_{i_1}^{-1} g g_{i_1} \cdots g_{i_{k-1}} g_{i_k} \\
g^{x g_j^{-1}} &= g_j g_{i_k}^{-1} g_{i_{k-1}}^{-1} \cdots g_{i_1}^{-1} g g_{i_1} \cdots g_{i_{k-1}} g_{i_k} g_j^{-1} \\
g^{x g_{i_k}^{-1}} &= g_{i_{k-1}}^{-1} \cdots g_{i_1}^{-1} g g_{i_1} \cdots g_{i_{k-1}}
\end{aligned}
$$

Hopefully, shortest length for g_{i_k}.

Peel off g_{i_k} and continue to $g_{i_{k-1}}$ etc.

May use $\{g_1, \ldots, g_n\}^m$ as generators. Complexity: $\frac{k}{m} \cdot n^m$.

In $\mathbf{B}_N$: Use $\ell(g) =$ length of the normal form of g.

No experimental results given.

Length functions in the braid group

Paterson–Razborov 1991. Minimal length in $\mathbf{B}$ is NP-hard.

Paterson–Razborov 1991. Is Minimal length in $\mathbf{B}_N$ poly-time?

Berger 1994. Yes in $\mathbf{B}_3$.

Birman. Is Minimal length in $\mathbf{B}$ is NP-hard for BKL generators?

Hock–Ts 2010. $\ell(b) \leq \ell_R(b) \leq (|\Delta| - 1)\ell(b)$ in $\mathbf{B}_N$. In particular, $\ell_R(b) = \ell(b)$ in $\mathbf{B}_3$.

Hock–Ts 2010. Approximate Artin length using BKL ℓ_R.

(A.G.) Myasnikov–Shpilrain–Ushakov 2006. Experimentally: Dehornoy handle reduction + Δ-conjugation gives excellent length function.

LBA partial history

Garber–Kaplan–Teicher–Ts–Vishne 2006. Experimentally:

1. Length of rational form better than normal form.
2. Hughes–Tannenbaum LBA succeeds only for toy parameters, with long generators.

Garber–Kaplan–Teicher–Ts–Vishne 2005. Memory-enhanced LBA. Much better, but also needs somewhat long generators.

(A.D.) Myasnikov–Ushakov 2007. Variation of Memory-enhanced LBA: Keep all (and only) the steps reducing length.

Against Commutator KEP in B_{80}:

1. Very successful when $|g_i| \geq 20$.
2. Fails when $|g_i| \leq 10$.

The Commutator KEP was never attacked for $|g_i| \approx 10$.

LBA against CSP in full $\mathbf{B}_N$

The hardest case for LBA:

1. one instance,
2. short generators,
3. many relations.

For reasonable parameters:

Experimental results: 0%.

For all mentioned algorithms.

Classic LBAs assume very specific distributions

Example 1. g conjugate to $h := g^b$ ($g, b \in \mathbf{B}_N$ independent).

Reducing g length won't get us to h!

Example 2. $g := uv$ conjugate to $h := vu$ ($u, v \in \mathbf{B}_N$ independent).

The LBA heuristic is meaningless here.

Kovalyova–Tsaban 2010. Solution:
Meet in the Middle (memory-enhanced) LBA.

LBA*, or: Compression Algorithm (Ts)

Idea similar to A* algorithm for shortest paths in a graph.

Guaranteed success in finite time!

Assumption. $\{h \in g^G : \ell(h) \leq K\}$ finite.

Complexity. Heuristically, $\sqrt{M}$,

$$M = |\{h \in g^G : \ell(h) \text{ (near) minimal}\}|.$$

LBA*, or: Compression Algorithm (Ts)

Algorithm. Input: Conjugate g, h.
$S_g := \emptyset, S_h := \emptyset$.
$g_0 := g, h_0 := h$.
Loop until a computed conjugate of h is in S_g, or vice versa.

1. Add all conjugates of g_0 by generators to S_g.
2. Add all conjugates of h_0 by generators to S_h.
3. $g_0 \in_{\mathrm{rnd}}$ ℓ-minimal elements of S_g not taken before.
4. $h_0 \in_{\mathrm{rnd}}$ ℓ-minimal elements of S_h not taken before.

Finite time. Every dog has its day: $\{h \in g^G : \ell(h) \leq K\}$ finite.

Example. $\mathbf{B}_{16}$, $g, x \in \{\sigma_1^{\pm 1}, \ldots, \sigma_{N-1}^{\pm 1}\}^{32}$, (g, g^x).

ExCAN16L32.txt

Part III
Invariants-based algorithms

Finite invariants of conjugacy classes

Methodology. Efficiently computable:

1. $g \mapsto$ finite $I_g \subseteq g^G$;
2. $g \sim h \Rightarrow I_g = I_h$;
3. x with $g^x \in I_g$;
4. Compute I_g from any single element, by conjugations.

CSP Solution. Given $g \sim h$:

1. Conjugate g into I_g.
2. Conjugate h into $I_h = I_g$.
3. Build I_g by conjugations from g, until h's conjugate is found.

Heuristic. More efficiently, build I_g, I_h until they meet.

For Conjugacy Decision Problem: $I_h \cap I_g$ intersect?

Example: The free group

Think ring. Reduce cyclically (equivalently, cycle).

$$y^{-1}x^{-1}x^{-1}xyyxxy^{-1}xxy$$
$$x^{-1}x^{-1}xyyxxy^{-1}xx$$
$$x^{-1}xyyxxy^{-1}x$$
$$xyyxxy^{-1}$$

$$x^{-1}y^{-1}xxy^{-1}xyyyx$$
$$y^{-1}xxy^{-1}xyyy$$
$$xxy^{-1}xyy$$
$$xy^{-1}xyyx$$
$$y^{-1}xyyxx$$
$$xyyxxy^{-1}$$

$I_g :=$ all cyclic rotations of the cyclically reduced form of g
$=$ Cycle of the cycling orbit of g.

Inf, sup, and canonical length

$b \le c$: $bp = c$, $p \in \mathbf{B}_N{}^+$.

Left invariant: $b \le c \Rightarrow db \le dc$.

$$\Delta^i \le \underbrace{\Delta^i p_1 \cdots p_\ell}_{\text{normal form of } b} \le \Delta^{i+\ell}.$$

Canonical length of b: ℓ.

$$\begin{array}{rcl} \inf(b) & := & i \\ \sup(b) & := & i+\ell \\ b & \in & [i, i+\ell] = [\inf(b), \sup(b)] \end{array}$$

$b \in [i, \infty)$: $i \le \inf(b)$.

Super Summit Sets (a new view)

expsum: $\mathbf{B}_N \to \mathbb{Z}$ sum of exponents. Well-defined; conj-invariant.

Garside 1969. Summit Set: $\mathrm{SS}(b) := \{\Delta^i p \in b^{\mathbf{B}_N} : |p| \text{ minimal}\}$.
Finite nonempty conjugacy invariant.

Cf. LBA!

All elements of $\mathrm{SS}(b)$ have the same inf, $\overline{\inf}(b)$.

Classically, $\overline{\inf}(b) = \max(\inf(b^{\mathbf{B}_N}))$, $\mathrm{SS}(b) := b^{\mathbf{B}_N} \cap [\overline{\inf}(b), \infty)$.

Elrifai–Morton 1994. Minimize also the canonical length of p.

Super Summit Set:
$\mathrm{SSS}(b) := \{\Delta^i p \in b^{\mathbf{B}_N} : p \text{ minimal length and canonical length}\}$.

All elements of $\mathrm{SS}(b)$ have the same sup, $\underline{\sup}(b)$.

Classically, $\underline{\sup}(b) = \min(\sup(\mathrm{SS}(b)))$, $\mathrm{SSS}(b) = b^{\mathbf{B}_N} \cap [\overline{\inf}(b), \underline{\sup}(b)]$.

Conjugating b into SSS(b)

In the free group, cycling brings g to the conjugacy invariant set.

Cycling in $\mathbf{B}_N$:

$$\Delta^i p_1 p_2 \cdots p_\ell = \overline{p_1} \Delta^i p_2 \cdots p_\ell \quad \longmapsto \quad \Delta^i p_2 \cdots p_\ell \overline{p_1},$$

and moving to normal form.

Conjugation by $\overline{p_1} = {p_1}^{\Delta^i}$.

i may only increase, $\ell, |p|$ may only decrease.

Elrifai–Morton 1994, Birman–Ko–Lee 2001. Cycling $|\Delta|$ times increases $\inf(b)$ (if not maximal).

DeCycling:

$$\Delta^i p_1 \cdots p_{\ell-1} p_\ell \quad \longmapsto \quad p_\ell \Delta^i p_1 \cdots p_{\ell-1} = \Delta^i \overline{p_\ell} p_1 \cdots p_{\ell-1}$$

+ normal form. Same results, for sup.

Computing SSS(b) from an element

Elrifai–Morton Convexity. SSS(b) is connected by conjugations by permutation braids.

Complexity: $|\,\mathrm{SSS}(b)| \cdot N!$.

For $a, b \geq 1$: $\exists\ a \wedge b =$ maximal $d \leq a, b$.

Franco–Gonzalez-Meneses 2003. $x, y \in P$,
$g, g^x, g^y \in \mathrm{SSS}(b) \Rightarrow g^{x \wedge y} \in \mathrm{SSS}(b)$.

$\therefore$ Enough to consider minimal permutation braids above $\sigma_1, \ldots, \sigma_{N-1}$.

Complexity: $|\,\mathrm{SSS}(b)| \cdot N = N \cdot |\,\mathrm{SSS}(b)|$. Typically huge!

Ultra Summit Sets and beyond

Gebhardt 2005. Keep cycling!

In the free group, I_g = cycle of the cycling orbit of g.

USS(b) := all cycles of cycling orbits in SSS(g).

Gebhardt. Can move among cycles by minimal permutation braids.

Complexity: $n \cdot |\,\mathrm{USS}(b)|$.

Typically, $|\,\mathrm{USS}(b)|$ is linear in $|b|$. (May be exponential.)

Lee 2000. RSSS(b) intersection of cycling and decycling orbits (no minimal pb's).

Gebhardt–Gonzalez-Meneses 2010. Sliding Circuit SC(b) (with minimal pb's).

$$\mathrm{SC(b)} \subseteq \mathrm{SSSR}(b) \subseteq \mathrm{USS}(b) \subseteq \mathrm{SSS}(b) \subseteq \mathrm{SS}(b).$$

(Typo intentional.)

Dead end?

$$\mathrm{SC(b)} \subseteq \mathrm{SSSR}(b) \subseteq \mathrm{USS}(b) \subseteq \mathrm{SSS}(b) \subseteq \mathrm{SS}(b).$$

An–Ko 2012:

1. CSP for pseudo-Anosov braids boils down to CSP for rigid pseudo-Anosov braids.
2. There, $\mathrm{SC(b)} = \mathrm{RSSS}(b) = \mathrm{USS}(b)$.
3. $\exists$ exponential family with $|\,\mathrm{SC}(b)| \geq 2^{N/2}$.

Ts. Experimentally: Simple, high-entropy distribution on $\mathbf{B}_N$ with $|\,\mathrm{USS}(b)| \geq 2^{N-2}$ in probability $1 - 2^{-N/2}$: Pick

$$b :=_{\mathrm{rnd}} \sigma_{i_1}^{\pm 1} \cdots \sigma_{i_N}^{\pm 1}$$

until $b \in \mathrm{USS}(b)$ and has canonical length $\geq \frac{N}{4}$.

Concentration of measure. $\mathbf{B}_{20}$, $1,000$ tries: $|\,\mathrm{USS}(b)| \geq 2^{17.3}$.

High entropy. No birthday in 2^{14} samples.

Part IV
Dedicated length-based algorithms

Using Vershik's (Right-Angled Artin) group

The computation of USS(b) for

$$b =_{\text{rnd}} \sigma_{i_1}^{\pm 1} \cdots \sigma_{i_N}^{\pm 1} \in \mathbf{B}_N$$

kills my (8-core 8GB RAM) computer already for $N = 32$.

An improvement of LBA*, however, succeeds there.

Homomorphic preimage invariants. On board, IY"H:

1. Vershik's group **V**;
2. Linear time normal form in **V**;
3. Linear time conjugacy normal form in **V**;
4. The hybrid with LBA* in **B**.