Conjugacy of subsets in hyperbolic groups.

Jim Howie (Heriot-Watt University)
(joint work with Martin Bridson, Imperial)
St. Andrews Seminar
17 February, 2005
GROUP-THEORETIC KEY-EXCHANGE PROTOCOL  
(Anshel-Anshel-Goldfield)

Aim: using insecure communication, to set up a secure key known only to Alice & Bob.

Method: Fix a group $G = \langle \text{gens} | \text{rels} \rangle$ and subsets $S_A = \{x_1, \ldots, x_a\}$, $S_B = \{y_1, \ldots, y_b\}$.

Each $x_i, y_j$ given as word in gens.

Alice chooses secret $\alpha = \alpha(x)$, and transmits

\[ z = \alpha y \alpha^{-1} \]

(as a list of words in gens).
Bob chooses secret $\beta = \beta(y)$, and transmits $w = \beta x \beta^{-1}$ (as a list of words in $\text{gens}$).

Each computes secret key

$$[\alpha, \beta] = \alpha(x)\alpha(w)^{-1} = \beta(z)\beta(y)^{-1}.$$ 

To capture the key, a spy must solve one of the two simultaneous conjugacy problems:

$$z = \alpha y \alpha^{-1} \quad \text{(for $\alpha$, given $y, z$)}, \quad \text{OR} \quad w = \beta x \beta^{-1} \quad \text{(for $\beta$, given $x, w$)}.$$
Let $M, M'$ be Riemannian manifolds. A map $u : M \to M'$ is \textit{harmonic} if it is a minimiser of the energy functional

$$E(u) = \int_M \frac{1}{2} g^{ij}(x) \left\langle \frac{\partial u}{\partial x^i}, \frac{\partial u}{\partial x^j} \right\rangle d(\text{vol } M).$$

Thus it is a solution of a PDE $\tau(u) = 0$.

If $M$ is compact and $M'$ has negative sectional curvature, then typically there is at most one harmonic map in any homotopy class.

In general Harmonic maps $\cap$ Conjugacy class \textbf{compact}.
Kappeler, Kuksin and Schroeder consider a perturbed version of the harmonic map equation

\[ \bar{\tau}(u)(x) = \tau(u)(x) + \text{small} \left( x, u(x), \frac{\partial u}{\partial x^i} \right) = 0. \]

**THEOREM** (Kappeler, Kuksin, Schroeder) If \( M \) is compact and \( M' \) has negative sectional curvature, then the solution set of \( \bar{\tau}(u) = 0 \) within any homotopy class is compact.
**Theorem** (Kappeler, Kuksin, Schroeder)
Let $M, M'$ be Riemannian manifolds, such that $M$ is compact and the sectional curvatures of $M'$ are bounded above by $\kappa < 0$.

Let $u, v : M \to M'$ be homotopic maps. Then there exists a homotopy $H : M \times [0, 1] \to M'$ from $u$ to $v$ of width

$$\sup_{m \in M} \text{length}(H(m \times [0, 1])) \leq \text{Constant} \cdot (E(u)^{1/2} + E(v)^{1/2} + 1).$$

**Example** $M = S^1$. $E(u) = \text{length}(u)^2$, so

$$\text{width}(H) \leq \text{linear}(\text{length}(u), \text{length}(v)).$$
$u, v : M \to M'$ homotopic, $M$ compact, $M'$ negative curvature.

**GENERAL CASE** Choose a (finite) metric subgraph $\Gamma \subset M$ such that $\pi_1(\Gamma) \to \pi_1(M)$ is surjective.

(For example, the 1-skeleton of a triangulation of $M$.)

Then

$$E(u)^{1/2} \sim \sum_e \text{length}(u(e)).$$

So the KKS Theorem says

$$\text{width}(H) \leq \text{linear} \left( \sum_e \text{length}(u(e)) + \text{length}(v(e)) \right).$$
**THEOREM** (Bridson, Howie) Let $G$ be a $\delta$-hyperbolic group, with respect to a finite generating set $S$. Let $A, B$ be conjugate finite subsets of $G$. Then there exists a conjugating element $x \in G$ (with $A = B^x$) such that

$$||x|| \leq \text{linear} \left( \max\{||w||; \ w \in A \cup B\} \right).$$

**COROLLARY** The simultaneous conjugacy problem in a hyperbolic group is soluble in linear space.
The linear bound in the BH theorem has coefficients depending on $\delta$ and $|S|$. It is horribly big:

$$B(\mu) \sim \left((2 \cdot |S|)^{2\delta}\right)! \cdot \mu + (2 \cdot |S|)^{8\delta}(2 \cdot |S|)^{8\delta}.$$ 

Compare with the known results for conjugacy of single elements. For example

**THEOREM**

If $a, b$ are conjugate in $G$, then $\exists x \in G$ with $a^x = b$ and

$$||x|| \leq ||a|| + ||b|| + 4\delta.$$ 

If also $a, b$ cyclically geodesic and $\max\{||a||, ||b||\} > 8\delta + 1$,

$$||x|| \leq \frac{1}{2} (||a|| + ||b||) + 2\delta + 1.$$
Computational complexity

In a $\delta$-hyperbolic group $G$:

1. The word problem is soluble in linear time, using Dehn’s algorithm to reduce to geodesic representatives.

The set of relators of length $\leq 16\delta + 1$ is a finite set of defining relations.

Using a pair of push-down stacks to keep track of the word, read word from left to right, search presentation for length-reducing string rewrites (of subwords of length $\leq 8\delta + 1$).

Bounded $(8\delta + 1)$ backtracking and bounded bookkeeping after each rewrite means

$$\text{time } \leq \text{constant} \cdot \text{length}.$$
Dehn’s linear-time algorithm

INPUT

- - - - - p+2  p+1

STACK 1

k

1

STACK 2

k+1

p
II. The conjugacy problem is soluble in time $O(n \log(n))$ (Epstein and Holt).

III. The simultaneous conjugacy problem for lists of $m$ elements of lengths $\leq \mu$ is soluble in time $O(m \mu^2)$, provided $G$ is torsion-free (Bridson and Howie).

IV BUT: the (theoretical) leading coefficient is enormous

$$\sim 75\delta \cdot (2 \cdot |S|)^{23\delta} \cdot \left[ (2 \cdot |S|)^{2\delta} \right]^2 .$$
A geodesic in a metric space \((X, d)\) is \(\gamma : [a, b] \rightarrow X, -\infty \leq a < b \leq +\infty, d(\gamma(s), \gamma(t)) = |s - t| \ \forall \ s, t.\)

\((X, d)\) is geodesic if every pair of points \(x, y \in X\) is joined by a geodesic \([x, y]\) (not necessarily unique).

\((X, d)\) is \(\delta\)-hyperbolic if \((X, d)\) is geodesic, and for any geodesic triangle \([x, y, z]\),

\([x, y] \subset N_\delta([x, z] \cup [z, y]).\)

(The \(\delta\)-thin triangle property.)
A $\delta$-thin triangle

A $\delta$-thin triangle refers to a geometric configuration where the distance between any two points in the triangle is less than a certain threshold $\delta$. This concept is often used in the study of hyperbolic groups, where the geometry of space is negatively curved, and the notion of thin triangles helps in understanding the structure and properties of these groups.
A group, $S$ a (finite) generating set for $G$. Recall the Cayley graph $\Gamma(G, S)$:
vertex set $G$; edge set $G \times S$.

$\Gamma(G, S)$ is a geodesic metric space, where each edge has length 1. $G$ acts (by isometries) on $\Gamma(G, S)$ via left multiplication.

$G$ is hyperbolic if $\Gamma(G, S)$ is $\delta$-hyperbolic for some $\delta \geq 0$. 
**REMARK** The definition of $\delta$-hyperbolic is independent of the finite generating set $S$ (but $\delta$ may vary with $S$).

**EXAMPLES** Free groups, finite groups, $\pi_1(M)$, $M$ a Riemannian manifold with negative sectional curvature (e.g., surface groups).

**USEFUL PROPERTY** Geodesic quadrilaterals are $2\delta$ thin.

**KEY PROPERTY** $g \in G$ of $\infty$ order preserves a *finite* set $S(g)$ of *special geodesics* joining two points $g^{\pm\infty} \in \partial G$. 
Idea of proof - linear space

If $a_1^x = a_1^y = b_1$, then $xy^{-1} \in C_G(a_1) \subset N_B(S(a_1))$, where $B = B(\delta, |S|)$.

$a_1^\infty \neq a_2^{\pm \infty} \Rightarrow N_B(S(a_1)) \cap N_B(S(a_2))$ compact, so

$$||x|| \leq \text{linear} \left( \max \{ ||a_1||, ||a_2||, ||b_1||, ||b_2|| \} \right).$$

If $a_i^{\pm \infty}$ are the same $\forall i$, then $gp(a)$ (virtually) cyclic. $N_B(S(a_1))$ compact modulo $C_G(a)$, so . . .

Hard case – $a_i$ all torsion. Uses fact that torsion is bounded.
Idea of proof - quadratic time

1) Dehn-like algorithm – in linear time, reduce $a_1, b_1$ to cyclically $12\delta$-reduced form.

2) If $a_1 \sim b_1$, $\exists x$ of bounded length with $a_1^x$ a cyclic conjugate of $b_1$. Test $||b_1|| \cdot \text{constant}$ equations, each in linear time, using Dehn’s algorithm.

3) If yes, let $r$ be linear space bound. Then $\exists$ linear bound on $|C_G(a_1) \cap \text{Ball}_{r+||x||}(1)|$. There is an algorithm which lists this set ($Q$, say) in quadratic time.

4) $\forall q \in Q$, $\forall i$, test if $a_i^{qx} = b_i$ in linear time by Dehn. Since $2 \leq i \leq m$, $|Q|$ linear and $\max\{||xq||; q \in Q\}$ linear, this algorithm runs in time $O(m\mu^2)$, $\mu = \max\{||g||; g \in a \cup b\}$. 
The AAG protocol in hyperbolic groups

EXAMPLE
\[ G = \langle a_1, b_1, a_2, b_2 \mid [a_1, b_1][a_2, b_2] = 1 \rangle. \ |S| = 4, \ \delta = 3. \]

Theoretically,

\[ \text{time}(BH) \sim 10^{2.7 \times 10^6} m^2. \ (\text{time}(\text{time}) \sim 120 \text{ seconds}). \]

In principle, not a practical algorithm!

In practice: given \( \alpha = \alpha(x) \) and \( \beta = \beta(y) \) as geodesic words in \( \{a_1, b_1, a_2, b_2\} \), the expected amount of cancellation in \( z_i = \alpha y_i \alpha^{-1} \) or \( w_i = \beta x_i \beta^{-1} \) is small, so \( z_i \) will be long, and \( \alpha \) will be close to the prefix of \( z_i \) of length \( (\|z_i\| - \|y_i\|)/2. \)
A random computation

I used a random number generator to generate five random words of expected length 9 (before cancellation):

\[ x_1 = b_1^{-1}a_1^{-1}b_2^{-1}a_1^{-1}a_2^{-1}b_2^{-1}a_1^{-1} \]

\[ x_2 = a_1b_2^{-1} \]

\[ x_3 = a_2^{-1}a_2 \]

\[ x_4 = b_1b_2a_2^{-1}b_2^{-1} \]

\[ y_1 = a_2^{-1}a_1^{-1}a_1^{-1}a_2^{-1}b_2b_2 \]

and a word \( \alpha \) of expected length 18 in the \( x_i \):

\[ \alpha = x_3^{-1}x_2^{-1}x_1^{-1}x_3x_2x_3^{-1}x_4x_4^{-1}x_3x_2x_2x_1x_2x_2^{-1}x_1^{-1}x_3^{-1}x_3^{-1}x_1 \]
A random computation II

After free cancellation, \( z_1 = \alpha y_1 \alpha^{-1} = \)

\[
b_2 b_2 a_2 a_1 b_2 a_1 b_1 a_1 b_2^{-1} a_1 b_2^{-1} a_1 b_1^{-1} a_1^{-1} b_2^{-1} a_1^{-1} a_2^{-1} b_2^{-1} a_1^{-1} a_2^{-1} a_1^{-1} a_2^{-1} a_1^{-1} a_2^{-1} a_1^{-1} b_2^{-1} a_1^{-1} a_2^{-1} b_2^{-1},
\]

a unique geodesic word. The prefix of length \( 20 = (\|z_1\| - \|y_1\|)/2 \) is exactly \( \alpha \).

**CONCLUSION** Hyperbolic groups are probably not a good choice for the AAG protocol.

**QUESTION** Does it make a difference if the alphabets \( A, B \) and the words \( \alpha, \beta \) are chosen intelligently?