Length-based cryptanalysis of the braid group and its applications

David Garber

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

Singapore, June 2007

Braid Group B_n

Artin generators: $\sigma_1, \ldots, \sigma_{n-1}$

with the relations:

$$\begin{aligned} \sigma_i \sigma_{i+1} \sigma_i &= \sigma_{i+1} \sigma_i \sigma_{i+1}, \\ \sigma_i \sigma_j &= \sigma_j \sigma_i \text{ when } |i-j| > 1 \end{aligned}$$

B_n has geometric-topological interpretations.

B_n is infinite and nonabelian.

The underlying (apparently hard) problems

The Conjugacy 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 $u, w \in B_n$, 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 $w = xuy$.

Key-agreement protocol
Anshel-Anshel-Goldfeld (1999)

$G = \langle g_1, g_2, \ldots, g_n \rangle \leq B_N$ publicly known.

Secret keys: Alice: $a \in G$. Bob: $b \in G$.

Alice's public key: $ag_1a^{-1}, ag_2a^{-1}, \ldots, ag_na^{-1}$.
Bob's public key: $bg_1b^{-1}, bg_2b^{-1}, \ldots, bg_nb^{-1}$.

Bob knows $b = g_{k_1}^{i_1} g_{k_2}^{i_2} \cdots g_{k_m}^{i_m} \quad \Rightarrow \quad aba^{-1} \quad \Rightarrow \quad K = (aba^{-1})b^{-1}$.

Similarly, Alice knows $bab^{-1} \quad \Rightarrow \quad ba^{-1}b^{-1} \quad \Rightarrow \quad K = a(ba^{-1}b^{-1})$.

Parameters: B_{80} with $m = 20$ and g_i of length 5 or 10 Artin generators.

Diffie-Hellman-type key-exchange protocol
Ko-Lee-Cheon-Han-Kang-Park (2000)

$LB_n = \langle \sigma_1, \ldots, \sigma_{m-1} \rangle; \quad UB_n = \langle \sigma_{m+1}, \ldots, \sigma_{n-1} \rangle$ where $m = \lfloor \frac{n}{2} \rfloor$

Public key: a braid $p \in B_n$.
Private keys: Alice: $s \in LB_n$; Bob: $r \in UB_n$.

Alice: Sends Bob publicly: $p' = sps^{-1}$.
Bob: Sends Alice publicly: $p'' = rpr^{-1}$

Shared secret key: $K = srpr^{-1}s^{-1}$

K shared: Alice: $K = sp''s^{-1} = srpr^{-1}s^{-1}$.
Bob: $K = rp'r^{-1} = rsps^{-1}r^{-1}$.

Parameters: B_{80}, with braids of canonical length 12.

Length-based attack
Hughes-Tannenbaum (2002)

Assumption: Exists a **length function** ℓ defined on B_n, such that 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 hold 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.

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

Candidates for length functions

G-Kaplan-Teicher-Tsaban-Vishne (2004-5)

Garside normal form of $w \in B_n$: The unique presentation:

$$w = \Delta_n^r \cdot p_1 \cdots p_k$$

where r is maximal, $p_k \neq \varepsilon$ and $p_1, \ldots, p_k$ are permutation braids in left canonical form.

Garside length $\ell_{\mathsf{G}}(w)$: number of Artin generators in Garside normal form of w.

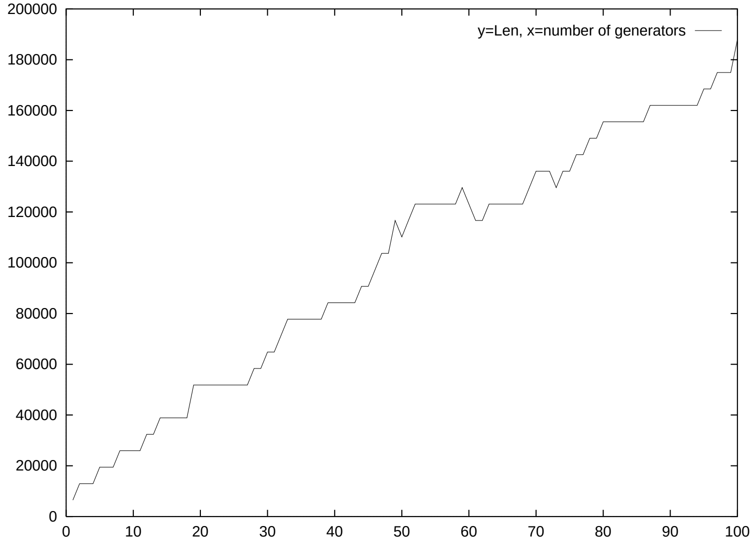
Reduced length function: For each permutation braid p, $\tilde{p} := p^{-1}\Delta_n$ is a permutation braid. So replace: $\Delta_n^{-1}p_1$ with $\tilde{p}_1^{-1}$.

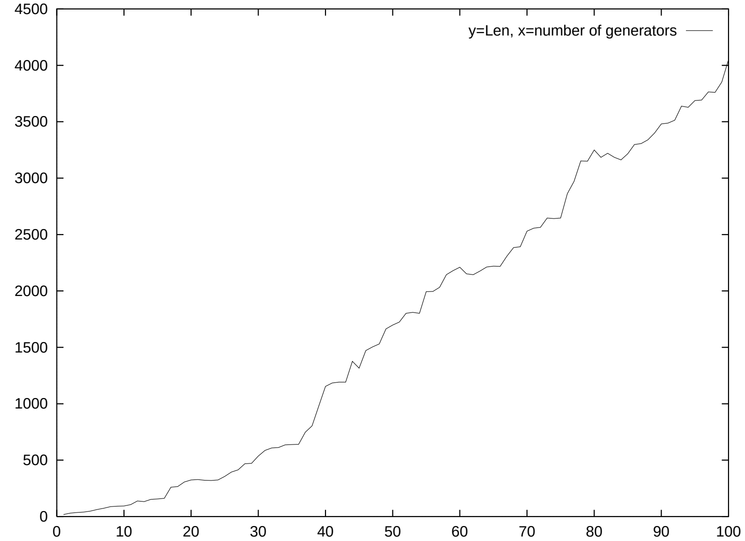
$$\begin{aligned} w &= \Delta_n^{-r} \cdot p_1 \cdots p_k = \Delta_n^{-(r-1)} \cdot \tilde{p}_1^{-1} p_2 \cdots p_k = \\ &= \Delta_n^{-(r-2)} \cdot (\tilde{p}_1')^{-1} \Delta_n^{-1} p_2 \cdots p_k = \cdots \end{aligned}$$

Reduced Garside length (or Mixed Garside length) of w:

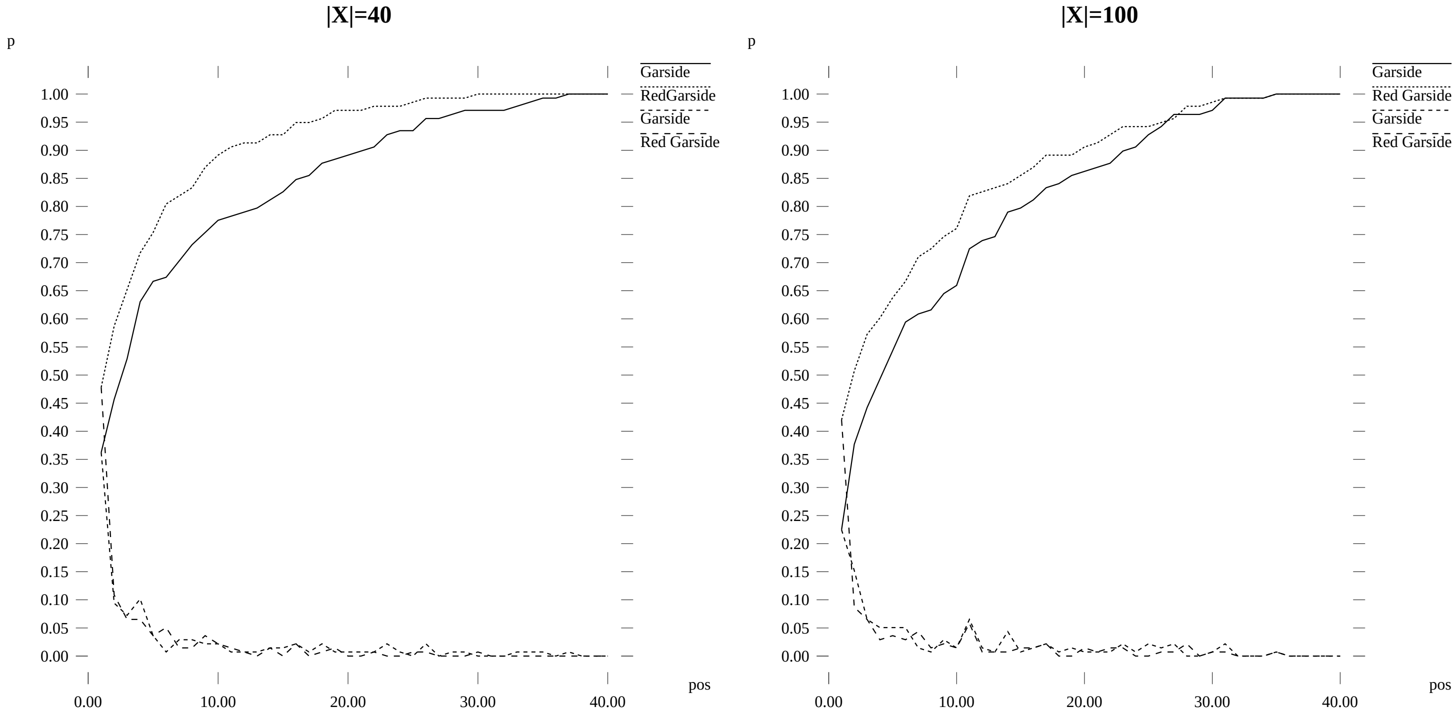
$$\ell_{\mathsf{RG}}(w) = \ell_{\mathsf{G}}(w) - 2 \sum_{i=1}^{\min\{r,k\}} |p_i|$$

Comparison between length functions





The growth of $\ell_{\mathsf{G}}(w)$ and $\ell_{\mathsf{RG}}(w)$



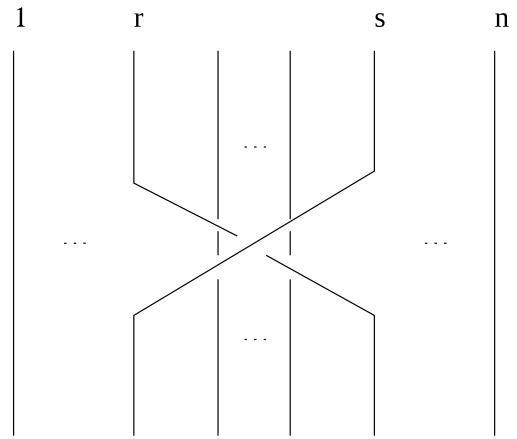
Position of correct generator ℓ_{G} and ℓ_{RG}

Parameters: B_{81}, 20 generators, 200 conjugates, 138 different X

More candidates for length functions
Hock-Tsaban (2007)

Idea: Use the Birman-Ko-Lee presentation (1998) instead of the Artin presentation.

Band generators:



a_{sr}

The band generators satisfies the following relations:

- $a_{ts}a_{rq} = a_{rq}a_{ts}$ if $[s,t] \cap [q,r] = \emptyset$ or $[s,t] \subset [q,r]$ or $[q,r] \subset [s,t]$.
- $a_{ts}a_{sr} = a_{tr}a_{ts} = a_{sr}a_{tr}$ for $1 \leq r < s < t \leq n$.

Birman-Ko-Lee normal form:

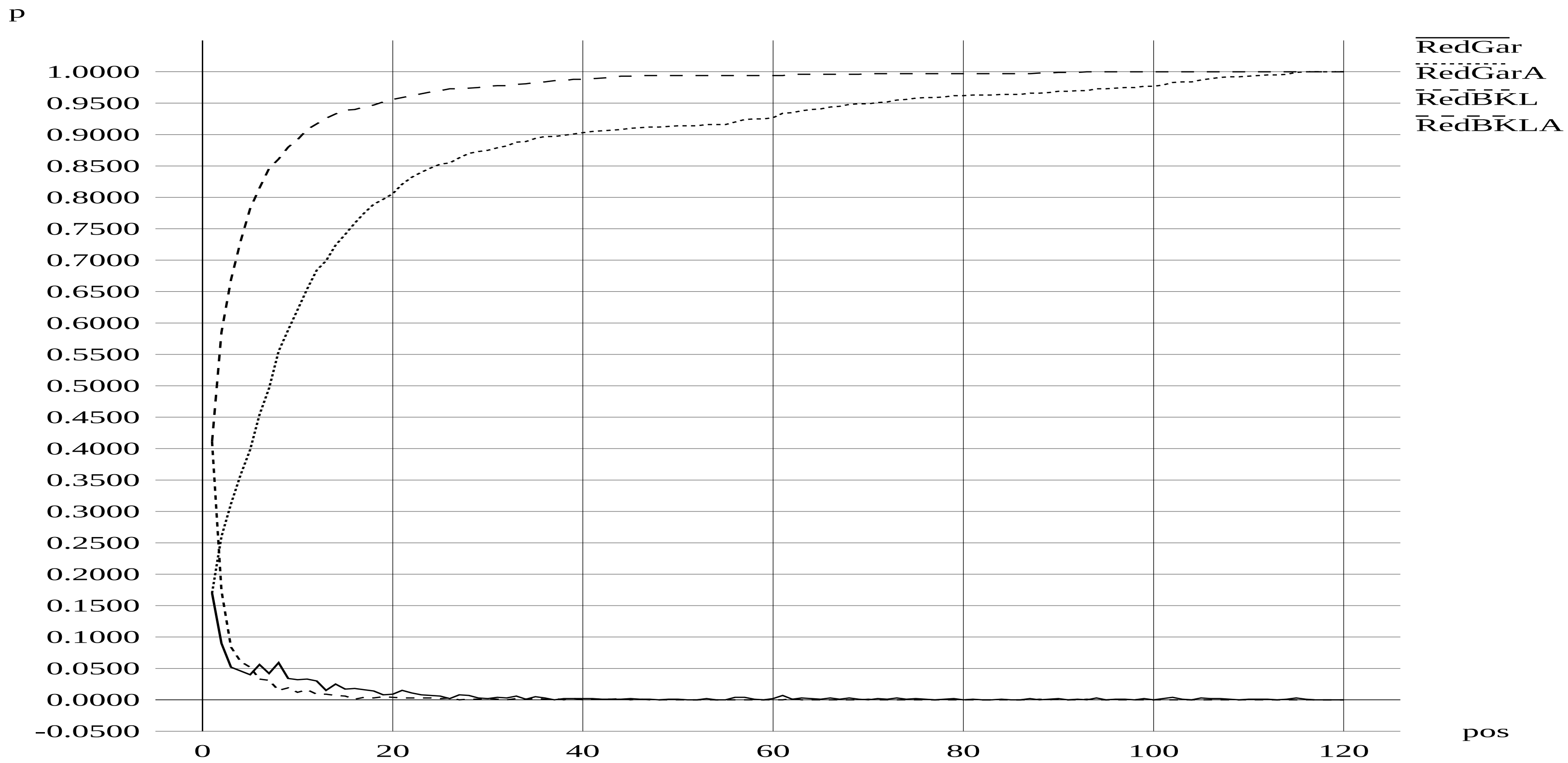
$$w = \delta_n^j A_1 A_2 \cdots A_k,$$

where $A = A_1 A_2 \cdots A_k$ is positive, j is maximal and k is minimal.

BKL length / Reduced BKL length: Similar to Garside.

Reduced BKL is better than Reduced Garside

In $G = \langle g_1, \ldots, g_{60} \rangle \leq B_{80}$, one conjugate, $|x| = 60$:



Improved length-based approach
G-Kaplan-Teicher-Tsaban-Vishne (2004-5)

The general problem:

G: A noncommutative group.
D: Distribution on G, with finite support $\{x_1, \ldots, x_k\} \subseteq G$.
w: Unknown element of G.
x: Product of $\leq n$ D-random elements x_i.
$a = xw$ is given.

Problem. Find a short list of elements of $\langle x_1, \ldots, x_k \rangle \leq G$ (with their presentation), containing x with nontrivial probability.

Can be generalized to a system of equations, etc.

The algorithm

- First step:
  - For each $j = 1, \ldots, m, \quad \sigma \in \{1, -1\}$, compute

$$a_j^{-\sigma} b_i = a_j^{-\sigma} X W_i, \quad i = 1, \ldots, k$$

  - Give (j, σ) the score

$$\sum_{i=1}^{k} \ell(a_j^{-\sigma} b_i)$$

  - Keep in memory the M elements with the least scores.

- Step $s > 1$:
  - For each sequence out of the M sequences, compute:
  $$a_{j_s}^{-\sigma_s}(a_{j_{s-1}}^{-\sigma_{s-1}} \cdots a_{j_1}^{-\sigma_1} b_i) = a_{j_s}^{-\sigma_s} a_{j_{s-1}}^{-\sigma_{s-1}} \cdots a_{j_1}^{-\sigma_1} X W_i,$$
  over $i = 1, \ldots, k$.
  - Assign the resulting score to the longer sequence.
  - Keep in memory the M sequence with the least scores.

Halting condition:

- Length n - step n, or
- The sum of the M scores increases rather than decreases.

Complexity:

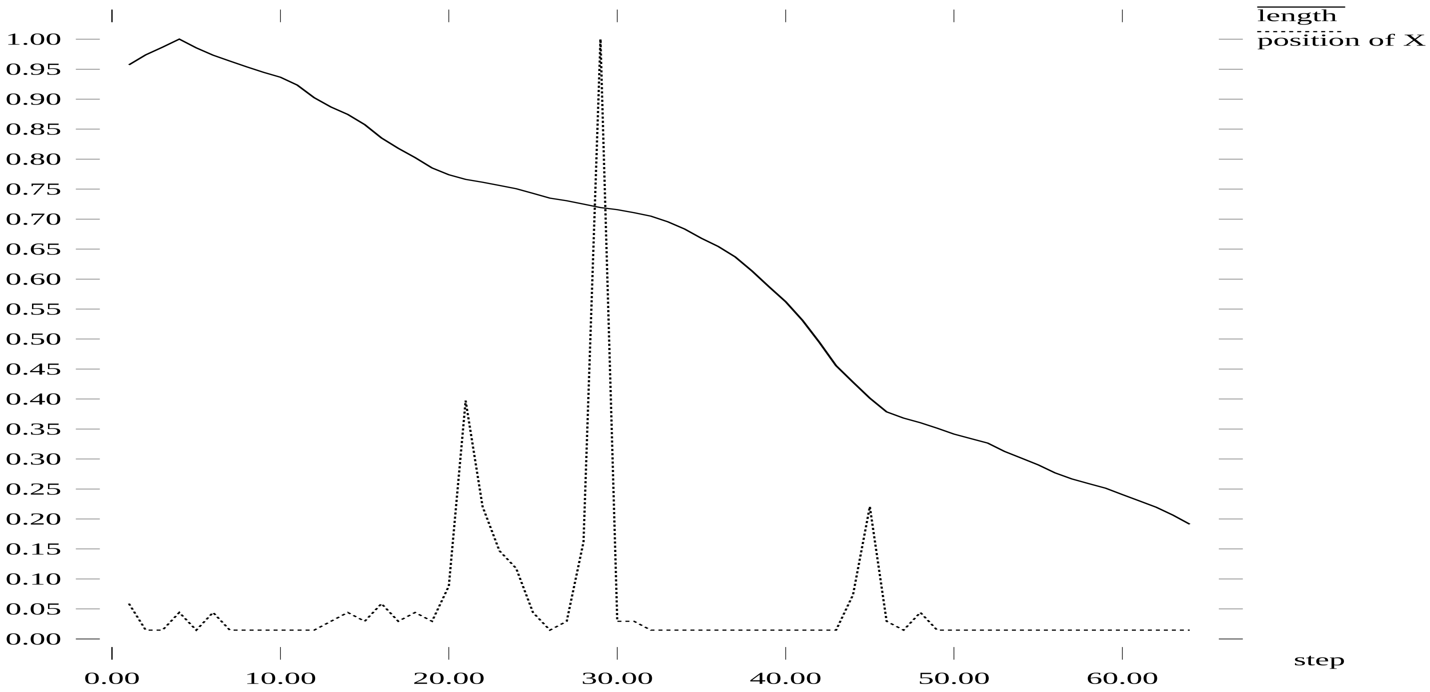
$$\sum_{s=1}^{n} kM(s+2m) = n(n+4m+1)kM/2$$

where:
M = length of the final list.
m = number of the generators of the group.
k = number of equations.

Applications of the improved approach

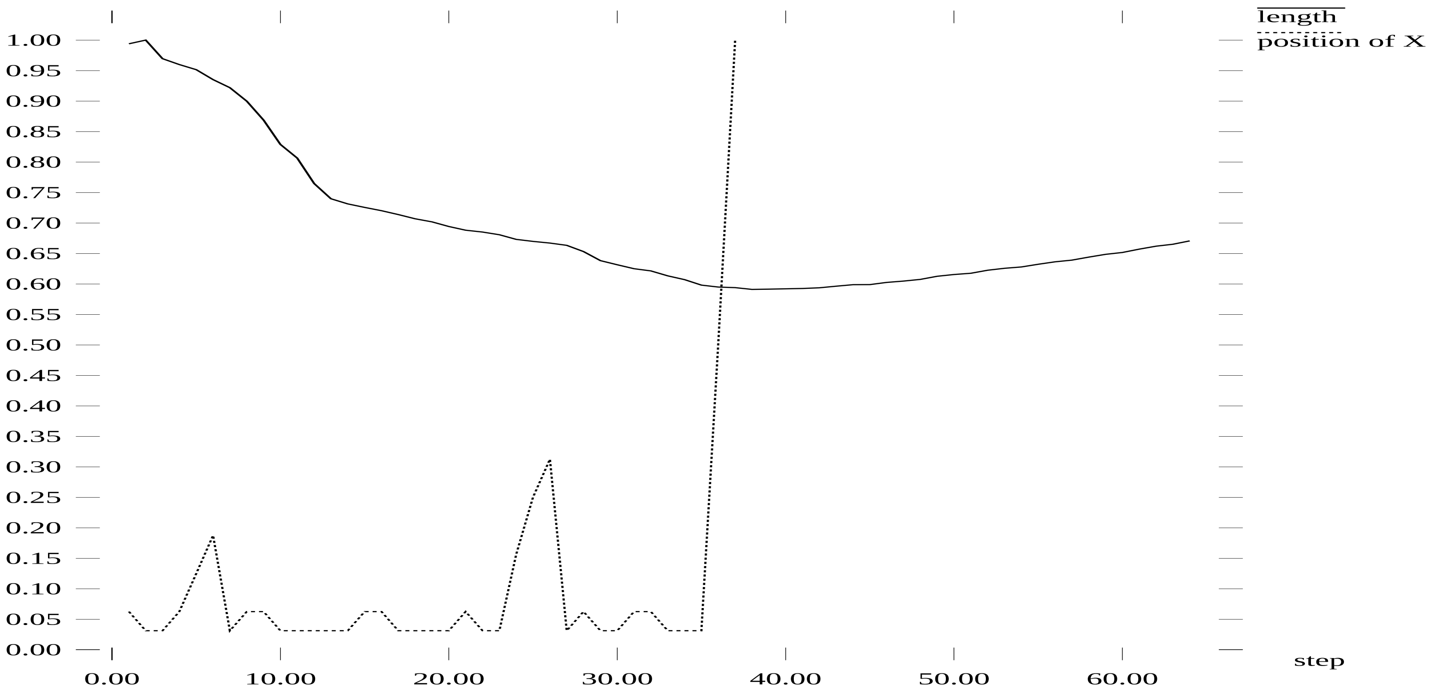
- Parametric equations.
- The Conjugacy Problem and its variants.
- Shifted conjugacy problem.
- Group Membership and Shortest Presentation problems.

Experimental results



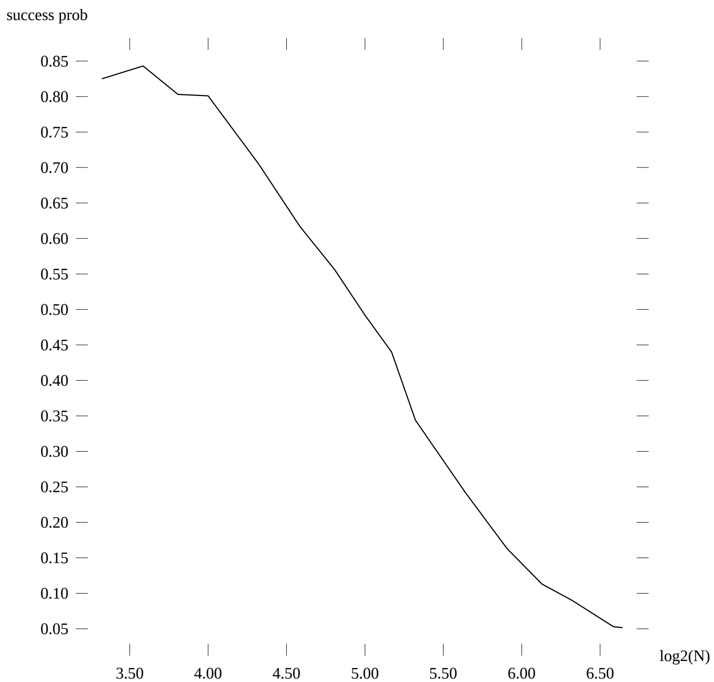
Position of correct prefix in successful runs

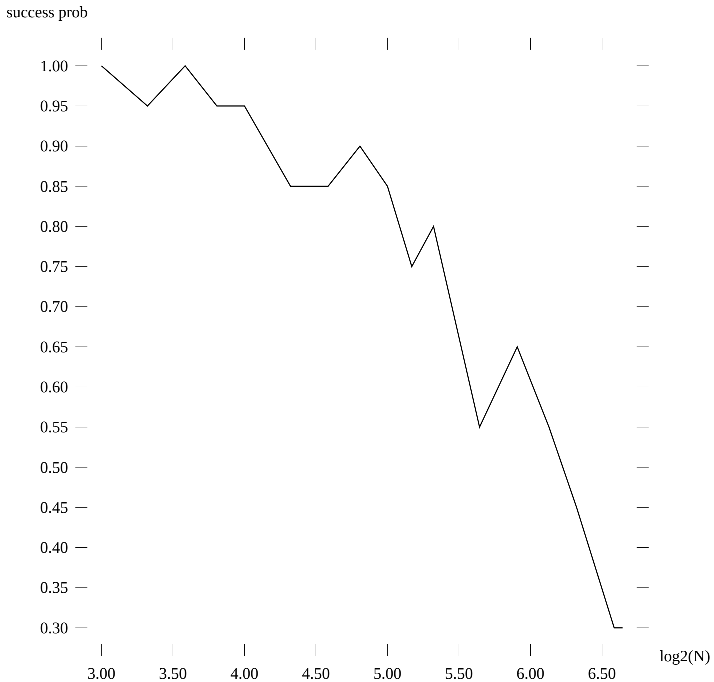
Parameters: B_8, (2,64,8,8,128) - 2 generators for the subgroup, length of X - 64, 8 equations, length of W_i - 8, size of memory - 128.



Position of correct prefix in unsuccessful runs

Parameters: B_8, (2,64,8,8,128)





Success probability for $(2, 16, 8, 8, 2)$ (left) and for $(8, 16, 8, 8, 128)$ (right)

Public-key Cryptosystem on the Thompson group
Shpilrain-Ushakov (2005)

Thompson's group

$$F = \left\langle \quad x_0, x_1, x_2, \ldots \quad \middle| \quad x_k x_i = x_i x_{k+1} \quad (k > i) \quad \right\rangle$$

Fix $s \in \{3, 4, \ldots\}$.
The following subgroups commute elementwise:
$A = \langle\, x_0 x_1^{-1},\ \ldots,\ x_0 x_s^{-1} \,\rangle \leq F$; $B = \langle\, x_{s+1},\ x_{s+2},\ \ldots,\ x_{2s} \,\rangle \leq F$

Public: s (thus also A, B); $w \in F$.
Private: Alice: $a_1 \in A, b_1 \in B$. Bob: $a_2 \in A, b_2 \in B$.

They send publicly. $u_1 = a_1 w b_1$ (Alice), $u_2 = b_2 w a_2$ (Bob).

Shared Key. (Alice) $a_1 u_2 b_1 = a_1 b_2 w a_2 b_1 = K = b_2 a_1 w b_1 a_2 = b_2 u_1 a_2$ (Bob).

$\forall w \in F$, there exists (efficient) normal form NF(w).

$$\ell_{\mathsf{NF}}(w) := |\mathsf{NF}(w)|.$$

Generating the key. Fix a length parameter $L \in \{256, 258, \ldots\}$. Multiply random generators (possibly inverted) until $\ell_{\mathsf{NF}}(x) = L$.

F is far from free: Any nontrivial relation added makes it **abelian**.

Preliminary length-based attack **(Shpilrain-Ushakov)**: 0% success rate.

Matucci (2006): Special attack to Shpilrain-Ushakov cryptosystem.

Improved Length-based attack
Ruinskiy-Shamir-Tsaban (2007)

Using memory:
$|M| \leq 64$ - 0% success rate.
$|M| = 1024$ - 11% success rate.

Why? Probably due to the similarity to abelian groups.

Reasons for improving:
1. Make length-based algorithms applicable to more cases.
2. Deal with iterated systems (Agree on k independent keys in parallel, and XOR them all to obtain the shared key **(Shpilrain)**).

Main improvements

Avoiding repetitions: Do not consider again a candidate tested beforehand (using a hash list). Note that it is a generalization of avoiding loops for the case of no memory.

Finding equivalent solutions: suffice to find $\tilde{a}w\tilde{b} = u = awb$.

Results:
$|M| = 64$ - 62% success rate.
$|M| = 1024$ - 80% success rate.

Subgroup distance based cryptanalysis
Ruinskiy-Shamir-Tsaban (2007)

Idea: Instead of looking for shorter words, look for distance from target.

Application: We are given $w \in G$ and $u = awb$ where $a \in A$ and $b \in B$. We look for $\tilde{a} \in A$ and $\tilde{b} \in B$, such that $\tilde{a}w\tilde{b} = awb$.

Given a candidate $\tilde{a} \in A$, its score will be: $d(w^{-1}\tilde{a}^{-1}u, B)$ for $d(x, B)$ a distance function of x to B (Example: $d(x, B)$ is the number of generators in x which are not in B).

Results:
$|M| = 1$ - 48% success rate.