Time-Memory Analysis of Parallel Collision Search Algorithms
Monika Trimoska, Sorina Ionica, Gilles Dequen

Collision search

Collision
Given a random map \( f : S \to S \) on a finite set \( S \) of cardinality \( N \), we call collision any pair \( R, R' \) of elements in \( S \) such that \( f(R) = f(R') \).

Pollard’s Rho method

\[
\begin{align*}
&x_0, x_1, x_2, \ldots, x_k, x_{k+1}, \\
&\vdots \\
&x_t, x_{k+t}
\end{align*}
\]

- Expected number of steps until the collision is found:

\[
\sqrt{\frac{\pi N}{2}}.
\]

Parallel Collision Search

- Distinguished points: a set of points having an easily testable property. ex. The x-coordinate has 3 trailing zero bits: 10101101000.
- Only distinguished points are stored in memory.

Data structure

Requirements:
- Space efficient
- Thread-safe
- Fast look-up and insertion

Commonly used structure: Hash table.
Alternative: Packed Radix-Tree-List (PRTL).

Packed Radix-Tree-List

- Construct a radix tree up to certain level.
- Add the points to linked lists, each list starting from a leaf on the tree.

PRTL implementation

- Saving space on common prefixes.
- The stored data is packed in a single vector.
- We can estimate the optimal branching level.

Collision search applications

One collision application
- (Elliptic Curve) Discrete Logarithm Problem.

Multi-collision applications
- Attack on the 3-DES with three independent keys.
- (EC)DLP in the multi-user setting.
- Supersingular Fixed-Degree Isogeny Path Problem.

Time complexity analysis

Theorem. In the parallel collision search algorithm, the expected running time to find \( m \) collisions with a memory constraint of \( w \) words is:

\[
\frac{1}{L} \left( \frac{w}{\theta} + \frac{w^2}{2\theta^2 N} \theta N \right) + \frac{2m}{\theta}.
\]

\( L \) - number of used processors. 
\( \theta \) - proportion of distinguished points in \( S \). 
\( N \) - number of elements in \( S \).