UNIVERSITÉ de Picardie Jules Verne

Radboud Universiteit

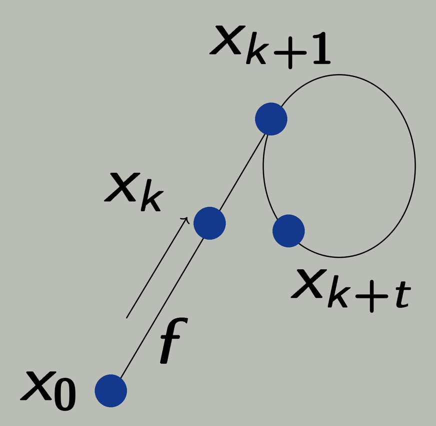
Time-Memory Analysis of Parallel Collision Search Algorithms

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 $f(R) = f(R')$.

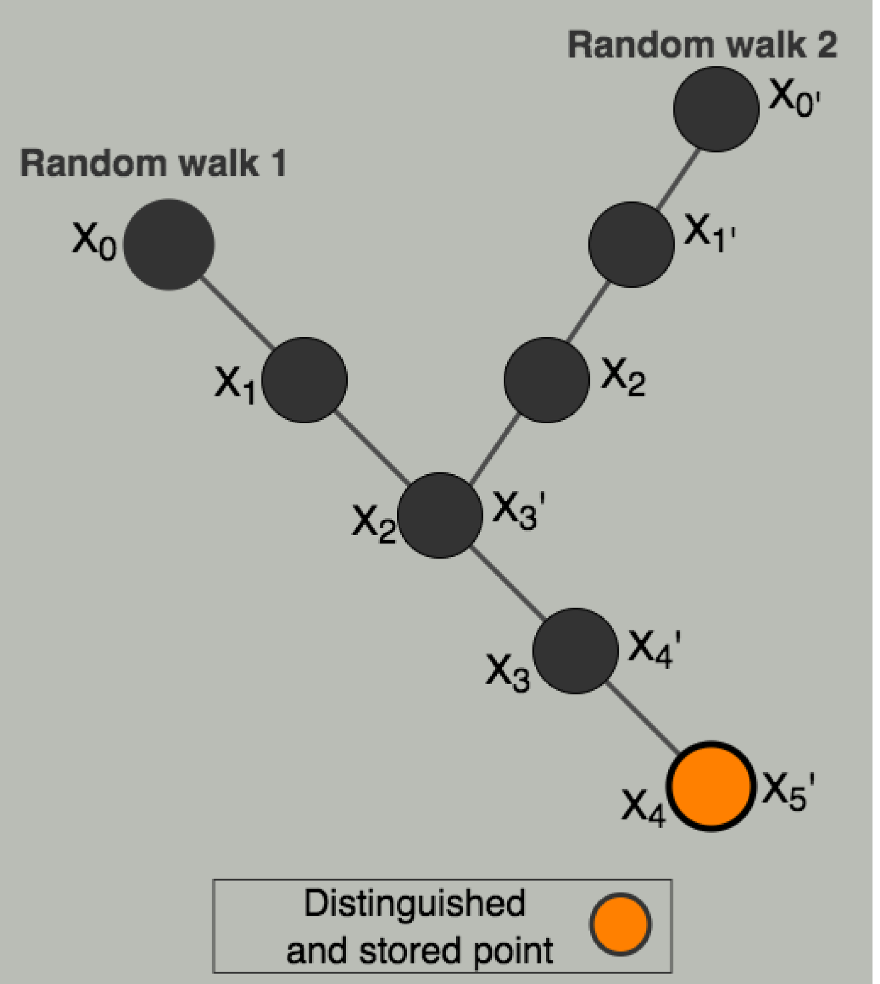
Pollard's Rho method



- Expected number of steps until the collision is found:
$$\sqrt{\frac{\pi N}{2}}.$$

Parallel Collision Search

- Proposed by van Oorschot & Wiener (1996).
- Distinguished points : a set of points having an easily testable property.
ex. The x-coordinate has 3 trailling zero bits: 10101101000.
- Only distinguished points are stored in memory.



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:

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

expected number of iterations needed to find and store w points

number of collisions found after storing w points

expected number of iterations needed to find one collision when w points are stored

L - number of used processors.
θ - proportion of distinguished points in S.
N - number of elements in S.

Data structure

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

Commonly used structure:
Hash table.

Alternative:
Packed Radix-Tree-List (PRTL).

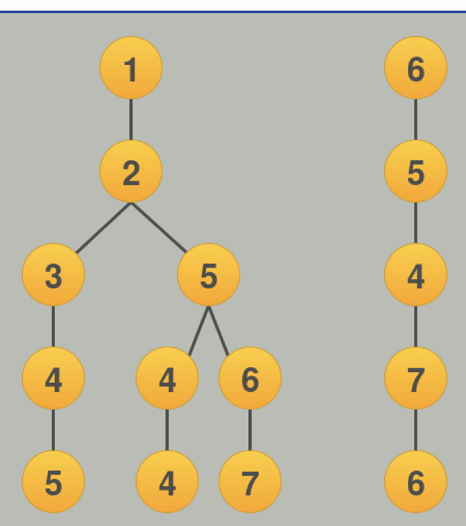


Figure: Example of a radix tree holding the set 12345, 12544, 12567, 65476.

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.

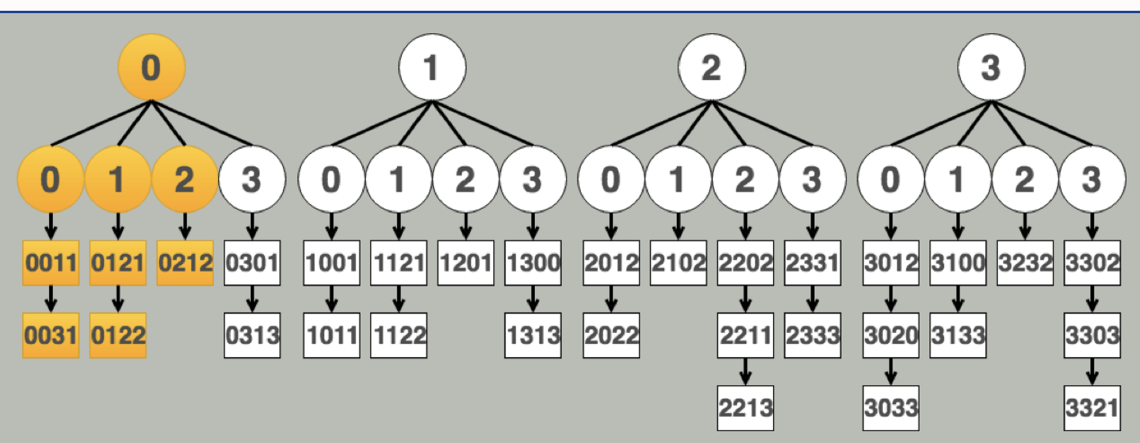
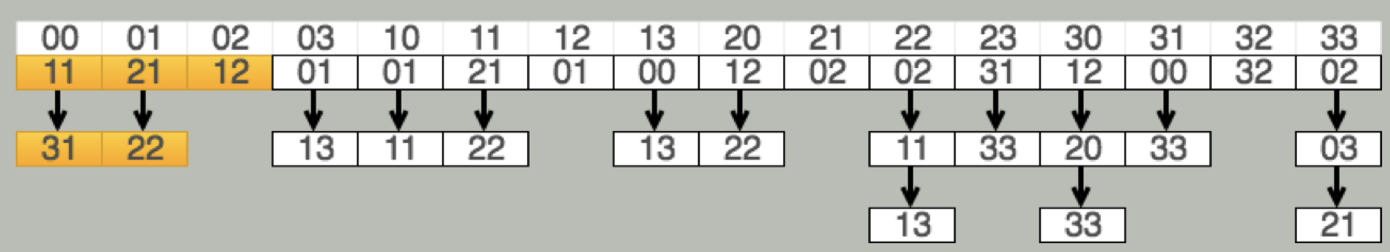


Figure: Example of a PRTL holding the set 0011, 0031, 0121, 0122, 0212, etc.

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.

Paper

Artifact