COLLISION OF RANDOM WALKS FOR DISCRETE LOGARITHM

九州大学
KYUSHU UNIVERSITY

University of Massachusetts
UMASS Lowell

By: Shuji Kijima and Ravi Montenegro

One-way function: Discrete Exponential and Logarithm

Easy

- Compute $\mathrm{h} = g^x$ for given g, h, x

Hard

- Solve $\mathrm{h} = g^x$ for given g, h
- Brute force: $O(N)\ \ steps$

Encryption

- Encrypt: Require g, x.
- Decrypt: Require discrete log.

How hard is Discrete Logarithm?

- *Upper bound*: Certainly $N = |\langle g \rangle|$ steps suffice.
- *Shoup* (‘97): $\Omega(\sqrt{N})$ for generic algorithm.

- *Deterministic Square-root*: $O(\sqrt{N})$ space
  Shanks baby step - giant step.

- *Randomized Square-root methods*: O(1) space
  Pollard’s Rho, Pollard’s Kangaroo (Lambda).

Birthday Attack on Discrete Log: Pollard's Rho

Problem

- Solve $\mathrm{h} = g^x$ in group of order $\mathrm{N} = |\langle g \rangle|$

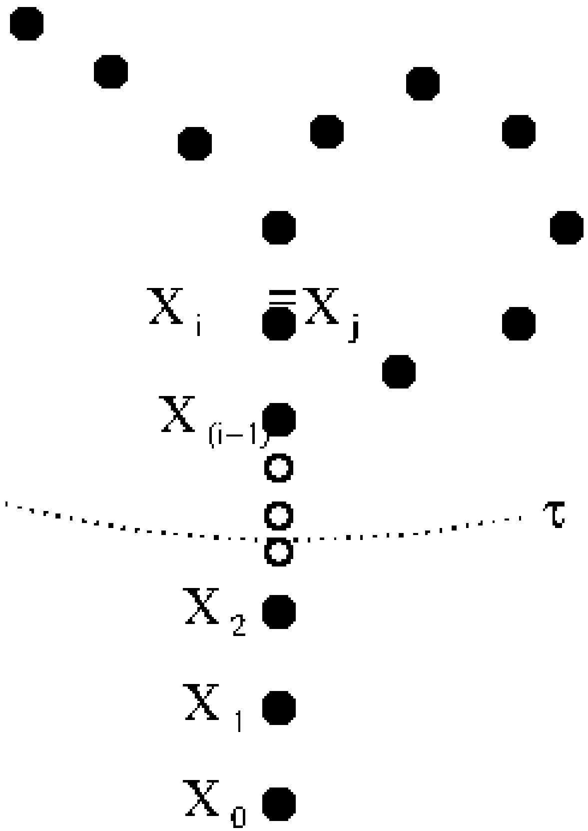
Birthday

- Heuristic: Average $\sqrt{\frac{\pi}{2} N}$ random values until "collision" of a walk.

Algorithm

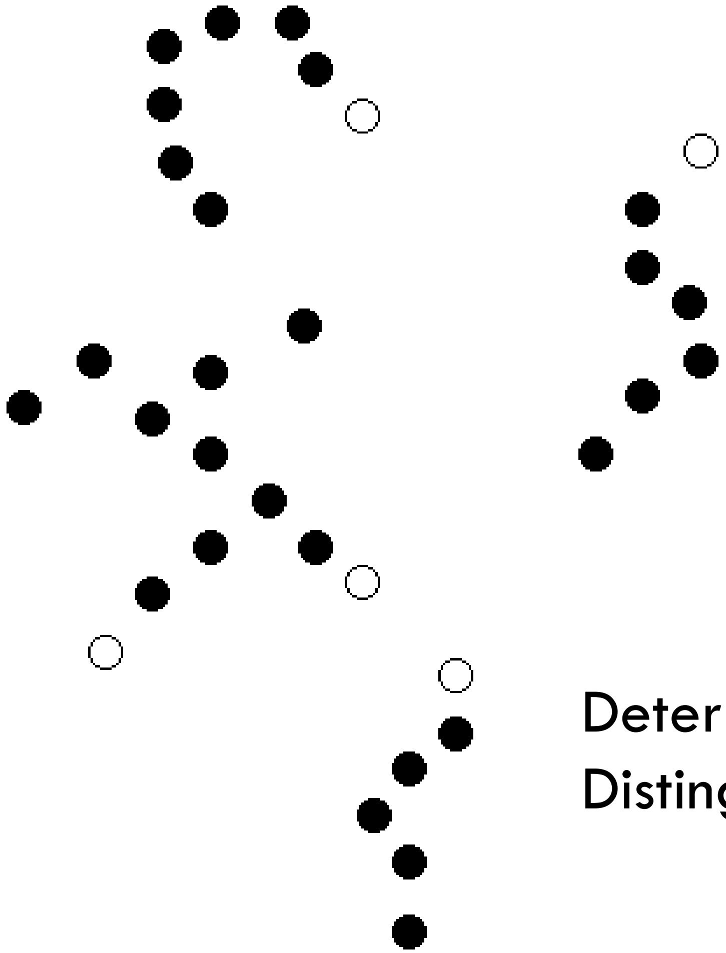
- Choose "random" $(a_0, b_0), (a_1, b_1)$, …
- Then $g^{a_i} h^{b_i} \equiv g^{a_j} h^{b_j}$ in $\sqrt{\frac{\pi}{2}|G|}$ steps
- $\rightarrow g^{a_i + b_i x} \equiv g^{a_j + b_j x}$
- $\rightarrow x \equiv (a_i - a_j)\,(b_j - b_i)^{-1}$

Pollard's Rho



Deterministic?

Pollard's Rho - parallel



Deterministic?

Distinguished points?

Collision Attack on Discrete Log: Pollard's Kangaroo

Problem

- DLog: Solve $h \equiv g^x$
  With condition: if we know that $x \in \{a, a+1, \ldots, b\}$.
  Can we do better than $\sqrt{\frac{\pi}{2}|G|}$?

Kruskal / Kangaroo

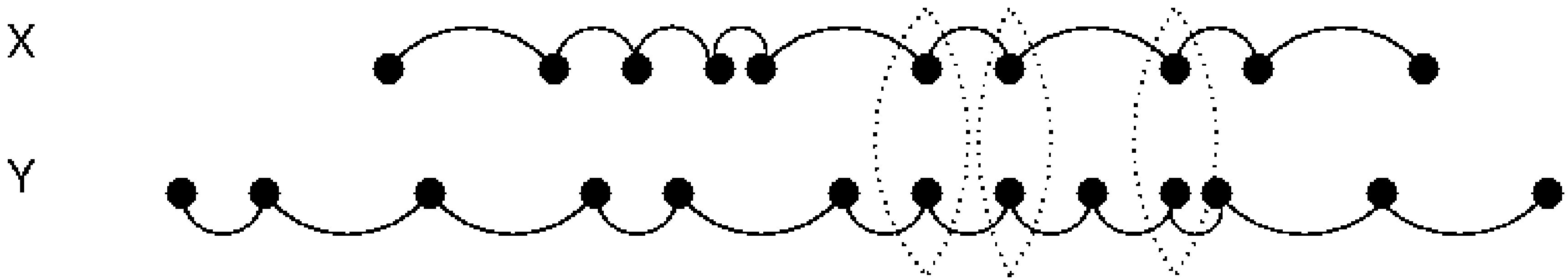
- Kruskal Count: Collision of two monotone walks in

$$(catch\ up\ time) + m$$

Algorithm

- Algorithm:
  -- Start tame kangaroo @ $g^{(a+b)/2}$.
  -- Hop some # of steps. Keep track of exponent.
  -- Place trap: Location @ $g^{\frac{a+b}{2}+\alpha}$.
  -- Run wild until $g^{x+\beta} = g^{\frac{a+b}{2}+\alpha}$
  $\rightarrow x \equiv \frac{a+b}{2} + \alpha - \beta$
- Complexity?

Pollard's Kangaroo

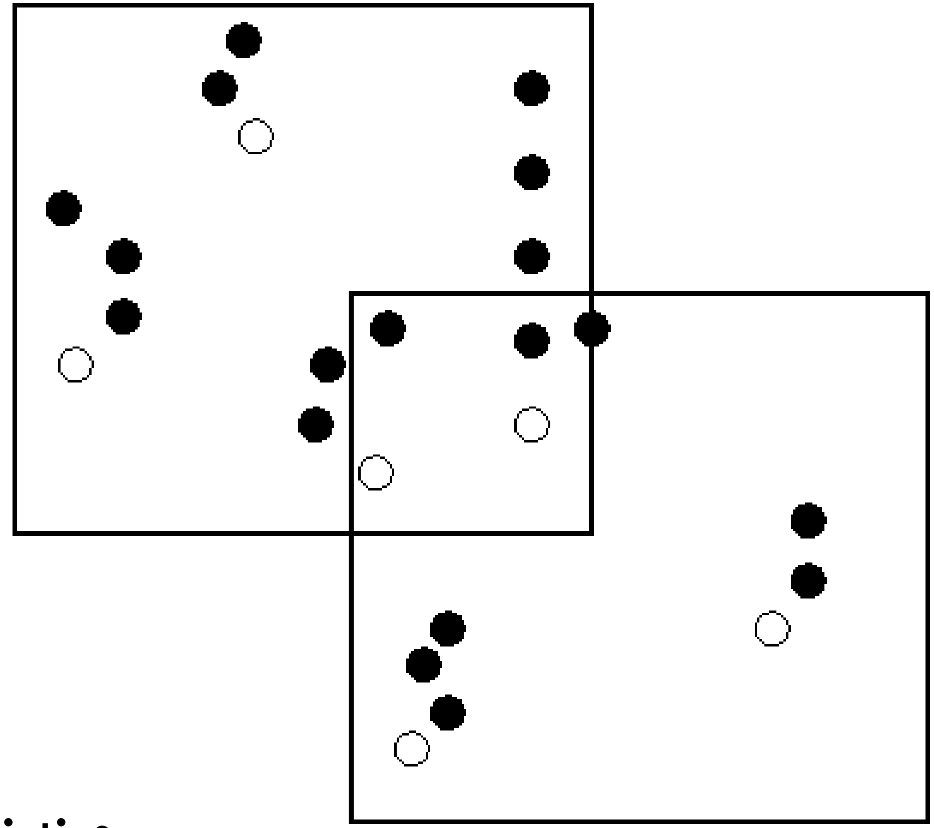


$r \sim 0.5 \log_2 N$ step types

$m \sim 0.5\, N^{0.5}$ step size

Deterministic?

Gaudry-Schost



Deterministic?

Birthday Attack on Discrete Log: Pollard's Rho

Problem

- Solve $\mathrm{h} = g^x$ in group of order $\mathrm{N} = |\langle g \rangle|$

Birthday

- Average $\sqrt{\frac{\pi}{2} N}$ random values until birthday "collision."

Algorithm

- "Random" walk $X_0, X_1, \ldots$
- $X_{i+1} = F(X_i)$ with $F(X)$
- Proceed until "collision" $X_i = X_j$.

- Note: F is deterministic pseudo-random.
- Note: F is low degree (Pollard: r=3, Teske: r=20).

Birthday Heuristic for Rho

- <u>*Heuristic*</u>: Almost all X_i and X_j are "independent."
- $\rightarrow$ a.e. collision involves "independent" states.
- So performs like a birthday problem.

- <u>Birthday</u>: Run time $\approx 1.253\sqrt{N}$
- <u>Simulations</u>: As bad as $1.625\sqrt{N}$

Birthday Heuristic for Rho

- Problem: Low degree dependencies
  $X_{i+1} = F(X_i)$ with $F(X)$ of degree r.
- Pollard: $F(X) = \begin{cases} X * g \\ X * h \\ X^2 \end{cases}$
- Teske:
  $F(X) = X * g^{a_i} h^{b_i} \quad with\, i \in_{uar} \{1,2,\cdots,r\}$

Results for Pollard's Rho (N=$|G|$)

- Birthday heuristic: $\sqrt{\frac{\pi}{2}N} \approx 1.253\sqrt{N}$
- "Rigorous" results: Pollard's walk
  - Miller and Venkatesan: $O\left(\sqrt{N}(\log N)^3\right)$
  - Kim, Montenegro, Peres, Tetali: $\leq 52.5\sqrt{N}$
- Heuristic results: Teske's walk
  - Blackburn and Murphy (also Brent and Pollard; Bailey et.al.)

$$\sqrt{\frac{\pi}{2}\frac{N}{1-1/r}}$$

  - Bernstein and Lange

$$\sqrt{\frac{\pi}{2}\frac{N}{1-\frac{1}{r}-\frac{1}{r^2}-\frac{2}{r^3}-\cdots}}$$

Birthday Heuristic

- State X_i is "independent" of most prior states.
  -- if $|i-j| \geq \tau$ then $P(X_i = X_j) \approx \frac{1}{N}$

- $P(X_i = some\ prior\ X_j) \approx \frac{i-\tau}{N}$

- Collision in: $\sqrt{\frac{\pi}{2}N} \approx 1.253\sqrt{N}$

Our approach

- “Independent” blocks

Rare collisions

- Fix a value k.
- If $T = o(\sqrt{N})$ then prob. 0 first collision has
  $|i - j| < T$ with $X_i = X_j$
  $\rightarrow$ prob. 0 of collision in $\{X_k, X_{k+1}, \cdots, X_{k+T}\}$

- If $T = o(\sqrt{N})$ then prob. 0 first collision involves a state in $\{X_k, X_{k+1}, \cdots, X_{k+T}\}$

- Conclusion:
  -- Can ignore some $o(\sqrt{N})$ states completely.
  -- Can ignore potential collisions closer than $o(\sqrt{N})$.

Our Method: Step 1

- Break walk into blocks with $T = o(\sqrt{N})$

$$\{X_0, X_1, \cdots, X_{T-1}\}$$
$$\{X_T, X_{T+1}, \cdots, X_{2T-1}\}$$
$$\cdots$$
$$\left\{X_{kT}, X_{kT+1}, \cdots, X_{(k+1)T-1}\right\}$$

- Ignore potential collisions within a block.

Our Method: Step 2

- Randomize between blocks: $T = o(\sqrt{N}), \tau = o(T)$

$$\{X_\tau, X_1, \cdots, X_{T-1}\}$$
$$\{X_{T+\tau}, X_{T+\tau+1}, \cdots, X_{2T-1}\}$$
$$\cdots$$
$$\{X_{kT+\tau}, X_{kT+\tau+1}, \cdots, X_{(k+1)T-1}\}$$

- Ignore potential collisions within a block.

  Ignore "randomization" states between blocks.

Our approach

- “Independent” blocks

“Rigorous” Analysis

- Block
$$B_k = \{X_{kT+\tau}, X_{kT+\tau+1}, \cdots, X_{(k+1)T-1}\}$$
is “independent” of all prior blocks.
- If $j < k$ then $P(B_k \cap B_j \neq \emptyset) = p$ (p=TBD).
- $P(\exists j < k : B_k \cap B_j \neq \emptyset) = kp$
- Collision in $\sqrt{\frac{\pi}{2}\frac{1}{p}}$ blocks.
- Collision in $\sqrt{\frac{\pi}{2}\frac{1}{p}}\,T$ steps.

"Rigorous" Analysis: Part 2

- If $B_k \cap B_j \neq \emptyset$

- $P(B_k \cap B_j \neq \emptyset) = \frac{E[|B_k \cap B_j|]}{E[|B_k \cap B_j| : |B_k \cap B_j| > 0]}$

$$= \frac{(T-\tau)^2 \frac{1}{N}}{C_\tau} = p$$

where $C_\tau = E[\#collisions\ in\ \tau\ steps\ when\ X_0 = Y_0]$

“Rigorous” Analysis: Conclusion

- Collision in

$$\sqrt{\frac{\pi}{2}\frac{N}{(T-\tau)^2/C_\tau}}\,T=\sqrt{\frac{\pi}{2}NC_\tau}$$

- Pollard’s walk: $C_\tau = 1.68221$

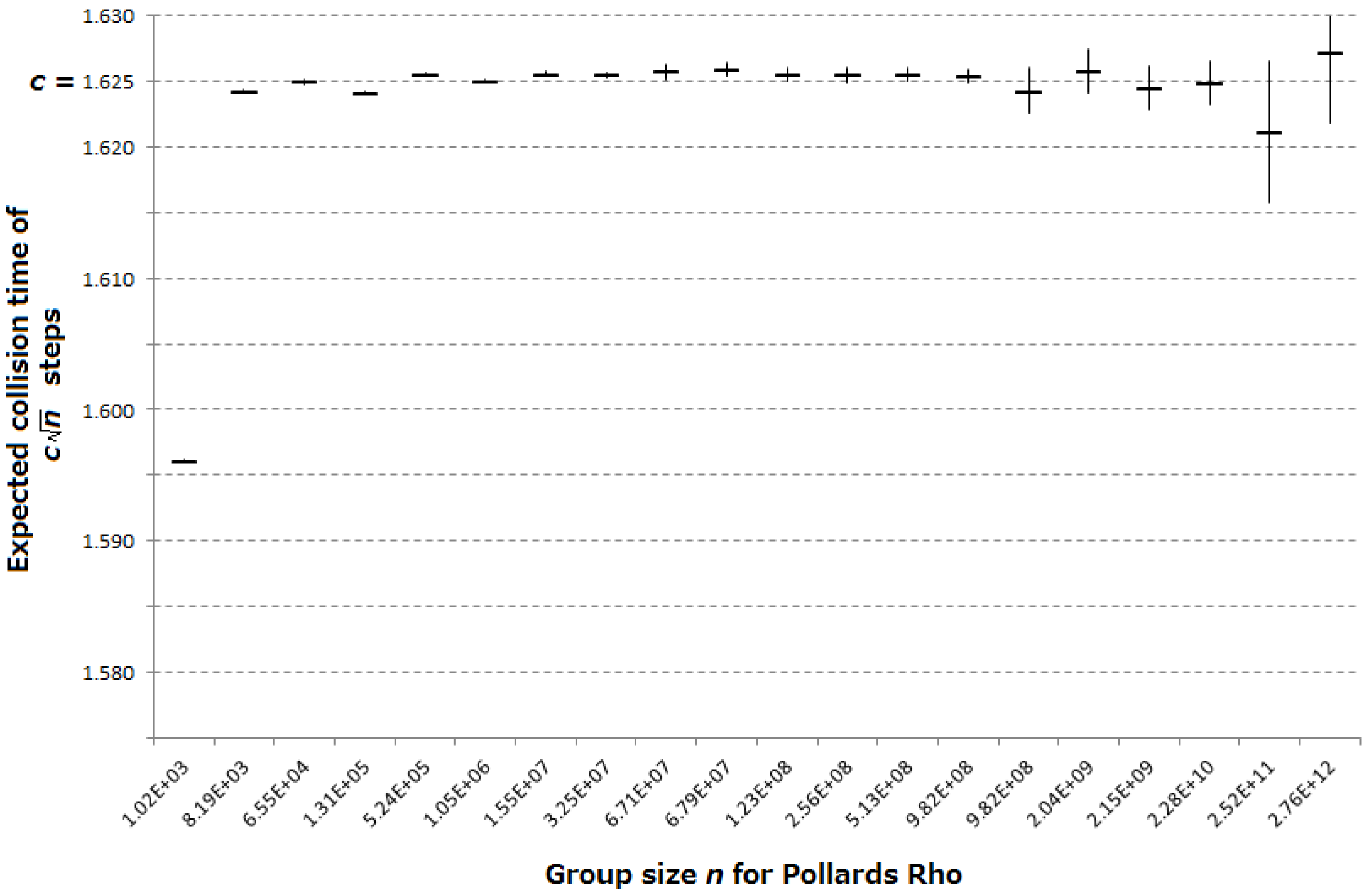
- Teske’s walks: $C_\tau = \frac{1}{1-\frac{1}{r}-\frac{1}{r^2}-\frac{2}{r^3}-\cdots}\ \ if\ N \geq 6$

Rho: r=3 Pollard vs r=3 Teske

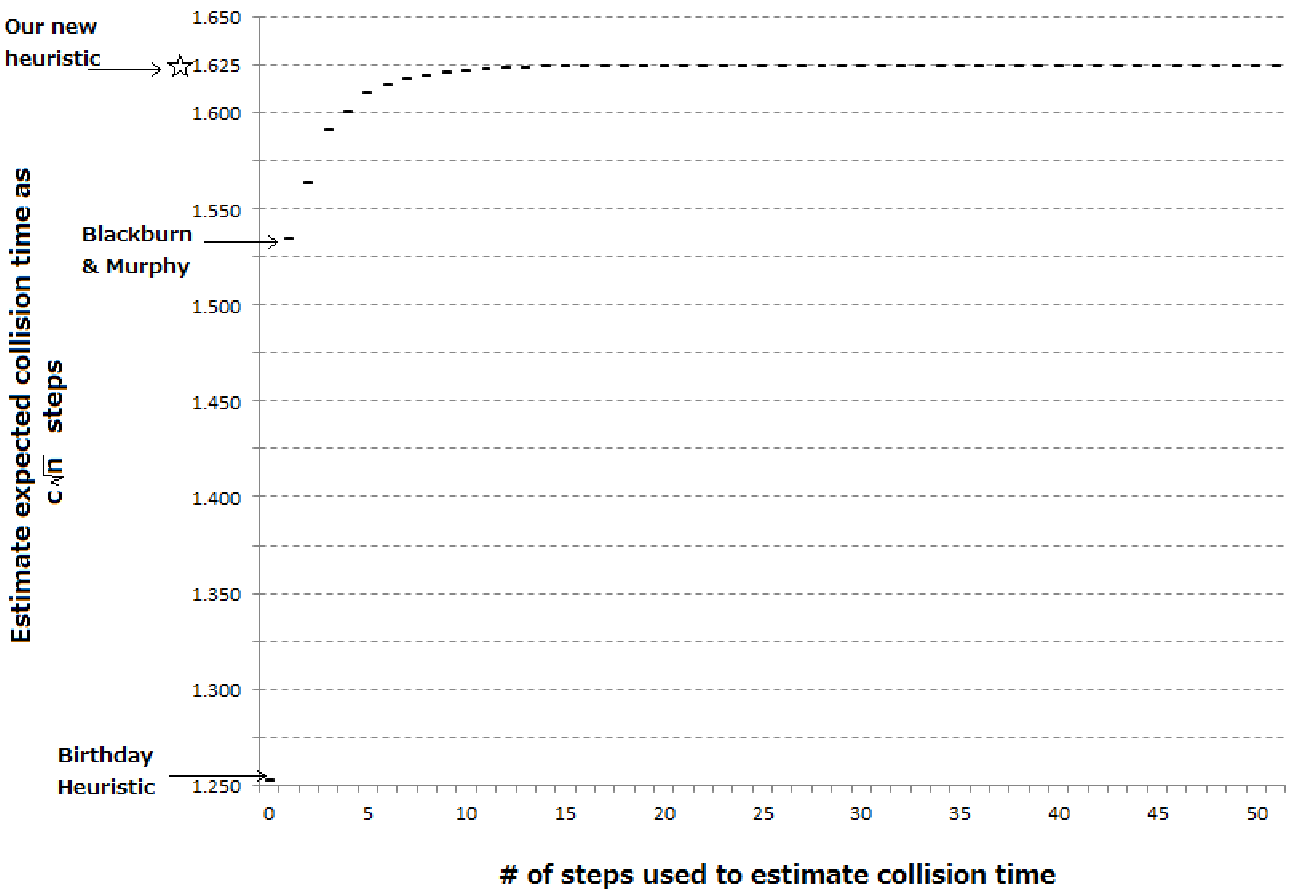
- Pollard:

- Additive:

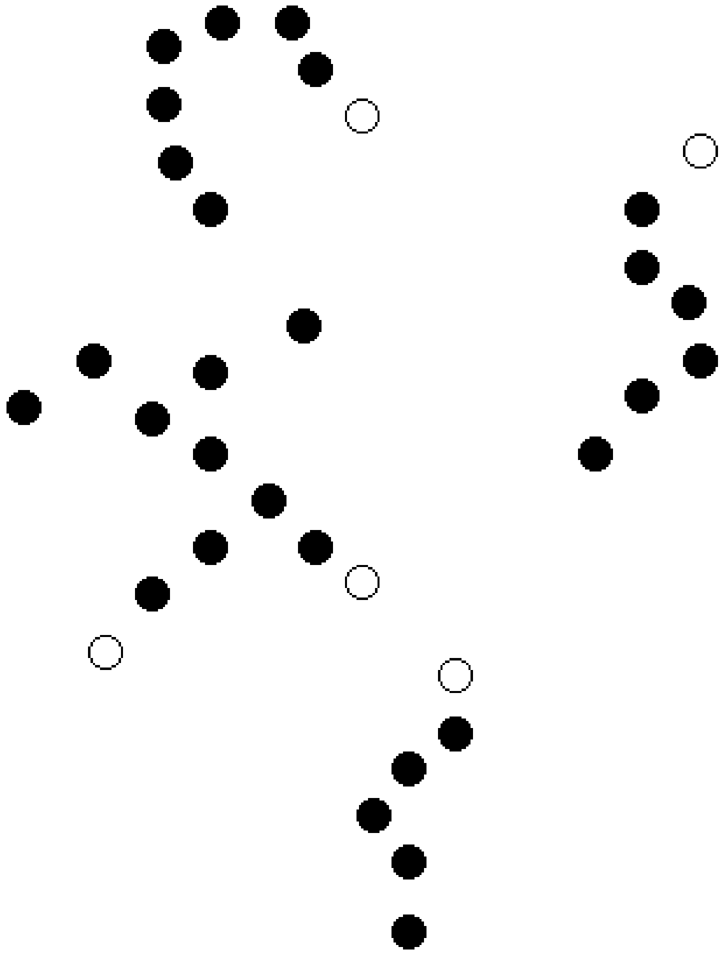
Pollard's Rho: Simulations



Pollard's Rho: Our heuristic



Pollard's Rho - parallel

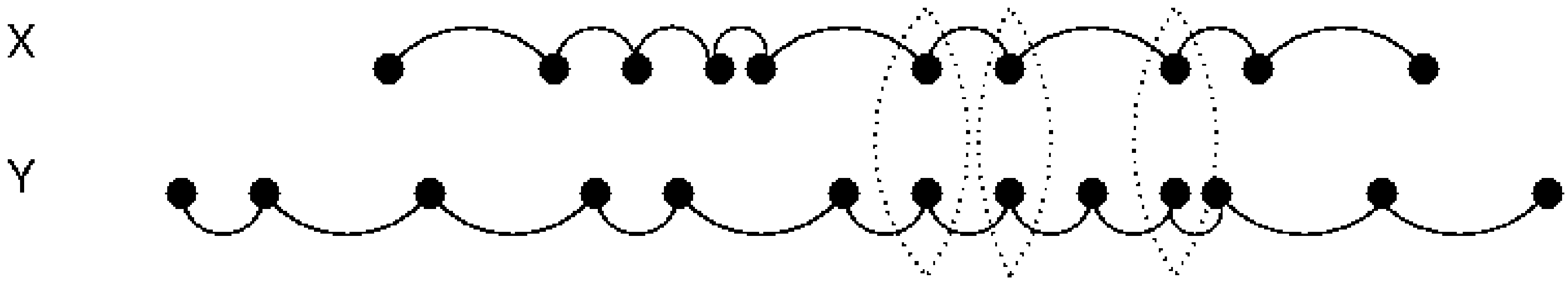


Parallel Rho: Analysis

- If M processors then collision in

$$\sqrt{\frac{\pi}{2}\frac{N}{(T-\tau)^2/C_\tau}\frac{T}{M}} = M^{-1}\sqrt{\frac{\pi}{2}NC_\tau}$$

Pollard's Kangaroo

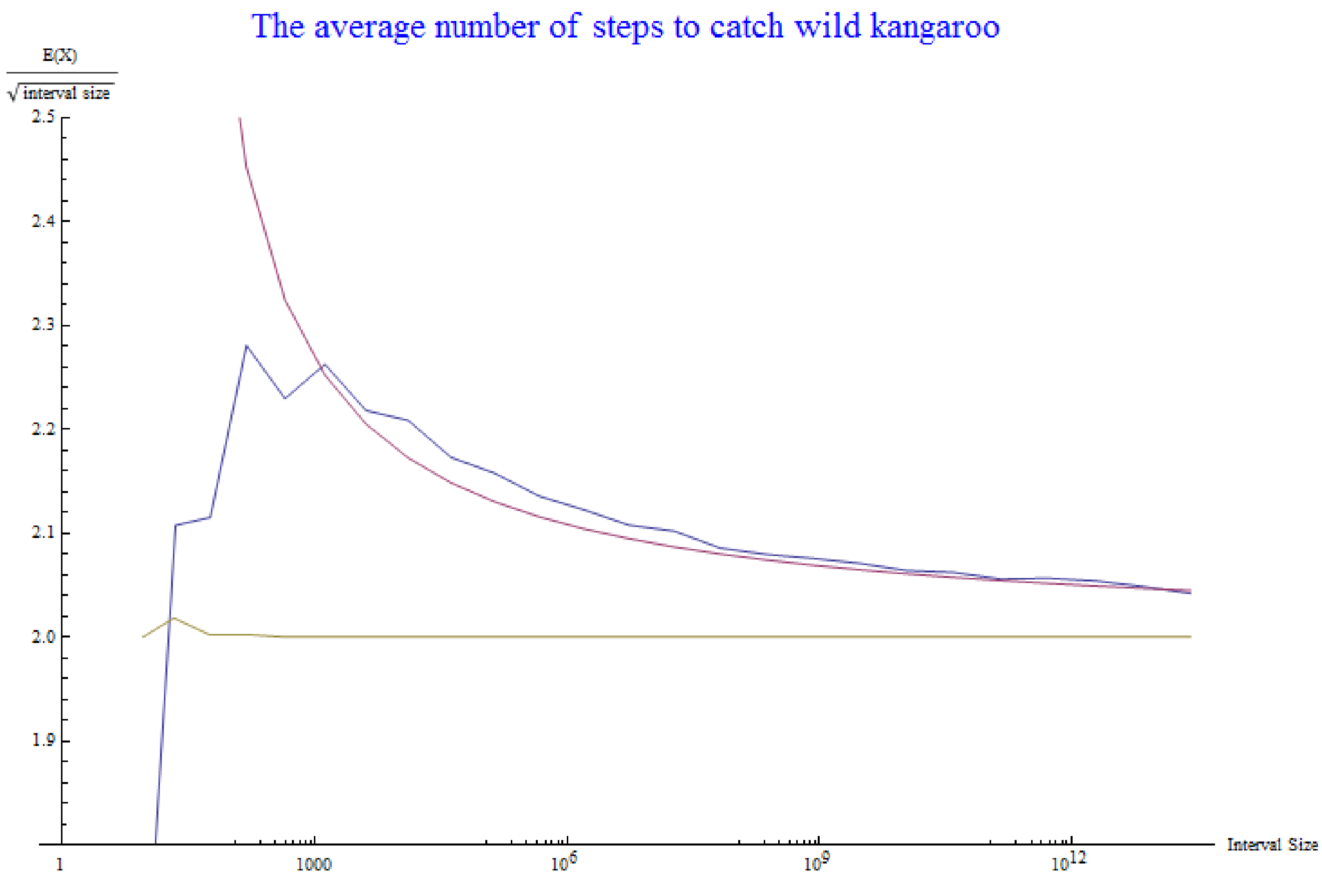


$r \sim 0.5 \log_2 N$ step types

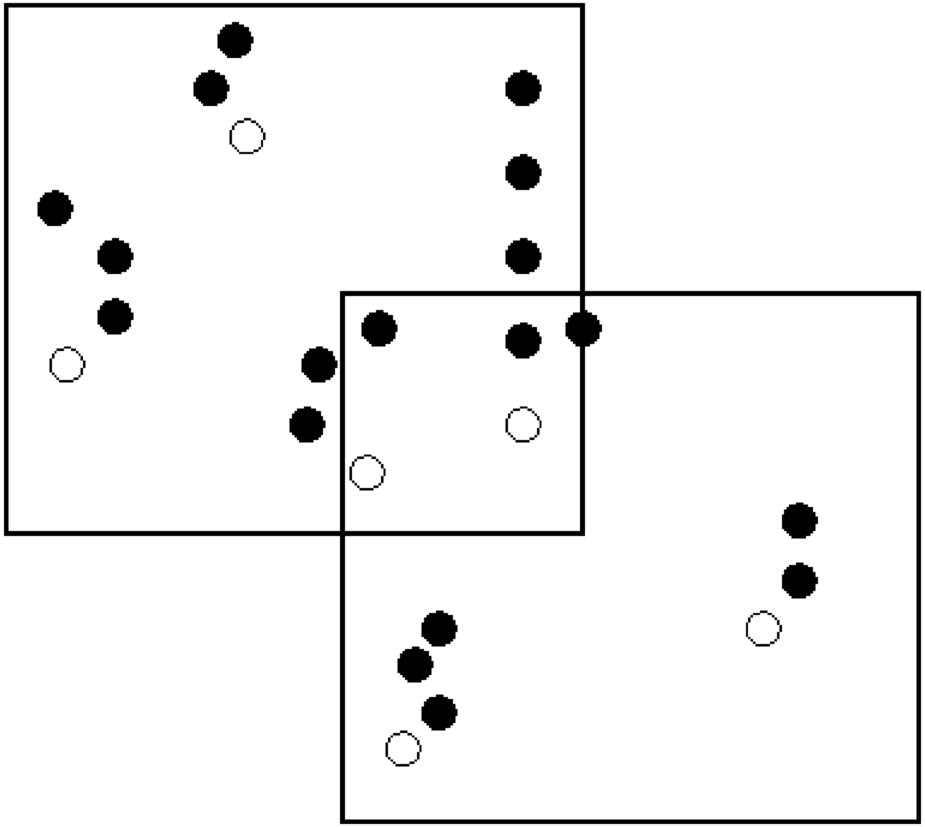
$m \sim 0.5 N^{0.5}$ step size

Pollard's Kangaroo

- Run time $\left(2 + \frac{2}{log_2 N} + \frac{14}{(log_2 N)^2} + \cdots\right)\sqrt{N}$



Gaudry-Schost



Gaudry-Schost

- Galbraith, Pollard, Ruprai: 1-d, 3 or 4 walkers.
  "Improved 3 set" version: Heuristic time $1.761\sqrt{N}$.

- Simulations suggest $1.795\sqrt{N}$
  Interval: $(1.790, 1.799)\sqrt{N}$

- Our improvement: $1.761\sqrt{\frac{N}{1-\frac{1}{r}-\frac{1}{r^2}-\cdots}} = 1.790\sqrt{N}$.
- Error: Boundary effects?

Summary

- Given heuristic for collision of walk(s).
- Break walk(s) into independent blocks.
- Ignore rare collisions involving:
  -- block with itself
  -- mixing states between blocks
- Heuristic (usually) becomes rigorous, with correction

$$C_\tau = E[\#collisions\ in\ \tau\ steps\ when\ X_0 = Y_0]$$