A Birthday paradox for Markov Chains and an optimal bound for Pollard's Rho to solve discrete log

Jeong Han Kim[1] Ravi Montenegro[2]
Yuval Peres[3] Prasad Tetali[4]

[1]Yonsei University
[2]University of Massachusetts at Lowell
[3]Microsoft Research and UC Berkeley
[4]Georgia Institute of Technology

ANTS 2008

Outline

Crypto and Discrete Log

El Gamal Encryption

- Alice chooses cyclic group $G = \langle g \rangle$ with prime order p, and $x \in \{0, 1, \dots, p-1\}$.
  Public Key: $G, g, p, h = g^x$. Private Key: x.

Crypto and Discrete Log

El Gamal Encryption

- Alice chooses cyclic group $G = \langle g \rangle$ with prime order p, and $x \in \{0, 1, \ldots, p-1\}$.
  Public Key: $G, g, p, h = g^x$. Private Key: x.
- Bob converts message m into group element $m \in G$.
  Chooses random $y \in \{0, 1, \ldots, p-1\}$.
  Sends $c_1 = g^y$, $c_2 = m\,h^y$.

Crypto and Discrete Log

El Gamal Encryption

- Alice chooses cyclic group $G = \langle g \rangle$ with prime order p, and $x \in \{0, 1, \ldots, p-1\}$.
  Public Key: $G, g, p, h = g^x$. Private Key: x.
- Bob converts message m into group element $m \in G$.
  Chooses random $y \in \{0, 1, \ldots, p-1\}$.
  Sends $c_1 = g^y$, $c_2 = m\, h^y$.
- Alice reads message $m = c_2\, c_1^{-x}$.

Pollard's Rho Algorithm

Sketch of Algorithm

- Given cyclic group $G = \langle g \rangle$.
  For $h \in G$ find $x = \log_g h$, i.e. solve $g^x = h$.

Pollard's Rho Algorithm

Sketch of Algorithm

- Given cyclic group $G = \langle g \rangle$.
  For $h \in G$ find $x = \log_g h$, i.e. solve $g^x = h$.
- *Pollard:* Choose $(a_i, b_i) \in \mathbb{Z}_{|G|}^2$ until some $g^{a_i} h^{b_i} = g^{a_j} h^{b_j}$.

Pollard's Rho Algorithm

Sketch of Algorithm

- Given cyclic group $G = \langle g \rangle$.
  For $h \in G$ find $x = \log_g h$, i.e. solve $g^x = h$.
- *Pollard:* Choose $(a_i, b_i) \in \mathbb{Z}_{|G|}^2$ until some $g^{a_i} h^{b_i} = g^{a_j} h^{b_j}$.
- *Collision:* Then $x = (a_i - a_j)(b_j - b_i)^{-1} \mod |G|$.

Pollard's Rho Algorithm

Sketch of Algorithm

- Given cyclic group $G = \langle g \rangle$.
  For $h \in G$ find $x = \log_g h$, i.e. solve $g^x = h$.
- *Pollard:* Choose $(a_i, b_i) \in \mathbb{Z}^2_{|G|}$ until some $g^{a_i} h^{b_i} = g^{a_j} h^{b_j}$.
- *Collision:* Then $x = (a_i - a_j)(b_j - b_i)^{-1} \mod |G|$.
- *Birthday Paradox:* Requires $\sqrt{\frac{\pi}{2}\,|G|} \approx 1.25\sqrt{|G|}$ samples.

Pollard's Rho Algorithm

The Algorithm

- *Floyd's:* Fix random function $f : \mathbb{Z}_{|G|}^2 \to \mathbb{Z}_{|G|}^2$.
  Let $(a_{i+1}, b_{i+1}) = f(a_i, b_i)$.
  Then $(a_i, b_i) = (a_{2i}, b_{2i})$ in a few more steps.

Pollard's Rho Algorithm

The Algorithm

- *Floyd's:* Fix random function $f : \mathbb{Z}^2_{|G|} \to \mathbb{Z}^2_{|G|}$.
  Let $(a_{i+1}, b_{i+1}) = f(a_i, b_i)$.
  Then $(a_i, b_i) = (a_{2i}, b_{2i})$ in a few more steps.
- *Pollard:* Partition G into T_1, T_2, T_3.
  Let $f(a, b) = (a + 1, b)$, $(a, b + 1)$, *or* $(2a, 2b)$
  if $g^a h^b \in T_1$ or T_2 or T_3 respectively.

Pollard's Rho Algorithm

The Algorithm

- *Floyd's:* Fix random function $f : \mathbb{Z}^2_{|G|} \to \mathbb{Z}^2_{|G|}$.
  Let $(a_{i+1}, b_{i+1}) = f(a_i, b_i)$.
  Then $(a_i, b_i) = (a_{2i}, b_{2i})$ in a few more steps.
- *Pollard:* Partition G into T_1, T_2, T_3.
  Let $f(a, b) = (a + 1, b)$, $(a, b + 1)$, *or* $(2a, 2b)$
  if $g^a h^b \in T_1$ or T_2 or T_3 respectively.
- *Teske:* Fix (random) partition, random start $\to 1.6\sqrt{|G|}$.
  (ranges from $0.86\sqrt{|G|}$ to $2.8\sqrt{|G|}$).

Pollard's Rho Algorithm

The Algorithm

- *Floyd's:* Fix random function $f : \mathbb{Z}_{|G|}^2 \to \mathbb{Z}_{|G|}^2$.
  Let $(a_{i+1}, b_{i+1}) = f(a_i, b_i)$.
  Then $(a_i, b_i) = (a_{2i}, b_{2i})$ in a few more steps.
- *Pollard:* Partition G into T_1, T_2, T_3.
  Let $f(a, b) = (a + 1, b)$, $(a, b + 1)$, *or* $(2a, 2b)$
  if $g^a h^b \in T_1$ or T_2 or T_3 respectively.
- *Teske:* Fix (random) partition, random start $\to 1.6\sqrt{|G|}$.
  (ranges from $0.86\sqrt{|G|}$ to $2.8\sqrt{|G|}$).
- *Markov chain:* Random partition $\to$ random walk
  (until collision).

Theoretical Results

General DLOG

- *Pohlig-Helman ('78):* Suffices to assume $N = |G|$ prime.
- *Shoup ('97):* Generic algorithm requires $\Omega(\sqrt{N})$ steps.

Theoretical Results

General DLOG

- *Pohlig-Helman ('78):* Suffices to assume $N = |G|$ prime.
- *Shoup ('97):* Generic algorithm requires $\Omega(\sqrt{N})$ steps.

Pollard Rho specific

- *Miller-Venkatesan (ANTS '06): Random walk* converges in $O(\log^3 N)$ and collision in $O(\sqrt{N}(\log^3 N))$.

Theoretical Results

General DLOG

- *Pohlig-Helman ('78):* Suffices to assume $N = |G|$ prime.
- *Shoup ('97):* Generic algorithm requires $\Omega(\sqrt{N})$ steps.

Pollard Rho specific

- *Miller-Venkatesan (ANTS '06): Random walk* converges in $O(\log^3 N)$ and collision in $O(\sqrt{N}(\log^3 N))$.
- *MV (PC):* a.e. N, random start $\rightarrow$ non-degenerate $1 - o(1)$.

Theoretical Results

General DLOG

- *Pohlig-Helman ('78):* Suffices to assume $N = |G|$ prime.
- *Shoup ('97):* Generic algorithm requires $\Omega(\sqrt{N})$ steps.

Pollard Rho specific

- *KMT (FOCS '07):* $O(\log N \log\log N)$ and $O(\sqrt{N \log N \log\log N})$.

Theoretical Results

General DLOG

- *Pohlig-Helman ('78):* Suffices to assume $N = |G|$ prime.
- *Shoup ('97):* Generic algorithm requires $\Omega(\sqrt{N})$ steps.

Pollard Rho specific

- *KMPT (ANTS '08):* Collision in $(1 + o(1))52.5\sqrt{N}$.

Theoretical Results

General DLOG

- *Pohlig-Helman ('78):* Suffices to assume $N = |G|$ prime.
- *Shoup ('97):* Generic algorithm requires $\Omega(\sqrt{N})$ steps.

Pollard Rho specific

- *MV (PC):* a.e. N, random start $\to$ non-degenerate $1 - o(1)$.
- *KMPT (ANTS '08):* Collision in $(1 + o(1))52.5\sqrt{N}$.

Theoretical Results

Remarks

- *Past heuristic:* After a while the walk looks random so Birthday Paradox applies; ignores dependencies between states.

Theoretical Results

Remarks

- *KMPT (ANTS '08):* Assumes random partition; requires $O(N)$ memory. Should suffice to use some pseudo-random partition (e.g. a hash function $f : \mathbb{Z}_N \to \{1, 2, 3\}$).

Outline

Birthday Paradox

Normal

N objects, choose with repetition $\rightarrow$ something twice in $O(\sqrt{N})$.

Birthday Paradox

Normal

N objects, choose with repetition $\rightarrow$ something twice in $O(\sqrt{N})$.

Markov

Uniform walk on K_N has collision in $O(\sqrt{N})$.

Birthday Paradox for Markov Chains: FOCS

Theorem

Finite, ergodic, uniform, $\frac{1/2}{N} \leq P^T(u,v)$ then collision in

$$2\sqrt{2cTN}$$

steps with prob $1 - e^{-c}$.

Birthday Paradox for Markov Chains: New

Theorem: Birthday Paradox for Markov Chains

Finite, ergodic, uniform, $\frac{1/2}{N} \leq P^T(u,v) \leq \frac{2}{N}$, then collision in

$$2\sqrt{N \max\{A_T,\, A_T^*\}} + 2T$$

steps with prob $1/32$.

$A_T = E(\#\text{collisions two iid walks, } T \text{ steps, same start})$
$A_T^* = \text{same for } P^*$

Birthday Paradox for Markov Chains: New

Theorem: Birthday Paradox for Markov Chains

Finite, ergodic, uniform, $\frac{m}{N} \leq P^T(u,v) \leq \frac{M}{N}$, then collision in

$$2\sqrt{\frac{2N}{M}\max\{A_T,\, A_T^*\}} + 2T$$

steps with prob $m^2/2M^2$.

$A_T = E(\#\text{collisions two iid walks, } T \text{ steps, same start})$
$A_T^* = \text{same for } P^*$

Application to Rho Walk

Block Walk

- Stop after $(a, b) \longrightarrow (2a, 2b)$ step.

Application to Rho Walk

Block Walk

- Stop after $(a, b) \rightarrow (2a, 2b)$ step.
- $T = \log^2 N + o(1) \rightarrow$

$$\frac{1 - o(1)}{N} \leq P^T(u, v) \leq \frac{1 + o(1)}{N}$$

Application to Rho Walk

Pre-Mixing

- A_T, A_T^* small if walk diffuses quickly:

$$A_T, A_T^* \leq 2 \sum_{j=0}^{T} (j+1) \max_{u,v} P^j(u,v)$$

Application to Rho Walk

Pre-Mixing

- A_T, A_T^* small if walk diffuses quickly:

$$A_T, A_T^* \leq 2 \sum_{j=0}^{T} (j+1) \max_{u,v} P^j(u,v)$$

- Large "tree-like" spanning subgraph

$$P^j(u,v) \leq \begin{cases} (2/3)^j & j \leq \lfloor \log_2 N \rfloor \\ \frac{3/2}{N^{1-\log_2 3}} \leq \frac{3/2}{\sqrt{N}} & \textit{otherwise} \end{cases}$$

Application to Rho Walk

Collision Time

- Block: $A_T, A_T^* \leq (1 + o(1))\,18$.

Application to Rho Walk

Collision Time

- Block: $A_T, A_T^* \leq (1 + o(1))\, 18$.
- Block: $(1 + o(1))24\sqrt{N}$; Rho: $(1 + o(1))72\sqrt{N}$.

Application to Rho Walk

Collision Time

- Block: $A_T, A_T^* \leq (1 + o(1))\,18$.
- Block: $(1 + o(1))24\sqrt{N}$; Rho: $(1 + o(1))72\sqrt{N}$.
- Improved proof $\rightarrow$ Rho in $(1 + o(1))52.5\sqrt{N}$

Proving the Key Tools

- *Birthday Paradox:*

  Let $S = \#\text{collisions} \geq 2T$ steps apart.

  Then $P(S > 0) \geq \frac{E(S)^2}{E(S^2)}$, i.e. second moment.

Proving the Key Tools

- *Birthday Paradox:*
  Let $S = \#\text{collisions} \geq 2T$ steps apart.
  Then $P(S > 0) \geq \dfrac{E(S)^2}{E(S^2)}$, i.e. second moment.
- *Mixing Time:*
  canonical paths, strong stationary time,
  Fourier, character/quadratic form.

Proving the Key Tools

- *Birthday Paradox:*
  Let $S = \#\text{collisions} \geq 2T$ steps apart.
  Then $P(S > 0) \geq \frac{E(S)^2}{E(S^2)}$, i.e. second moment.
- *Mixing Time:*
  canonical paths, strong stationary time,
  Fourier, character/quadratic form.
- *Fast probability diffusion:*
  Early steps of a SST (a strong form of coupling),
  or Fourier analysis.

Open Question

When can we celebrate Birthday?

- Suppose P is *reversible*: $\pi(x)P(x,y) = \pi(y)P(y,x)$, for every pair of states $x, y \in \Omega$.
  If π: uniform over Ω, with $|\Omega| = N$, then do we have a collision in $O(\sqrt{N})$ whp?

Open Question

When can we celebrate Birthday?

- Suppose P is *reversible*: $\pi(x)P(x,y) = \pi(y)P(y,x)$, for every pair of states $x, y \in \Omega$.
  If π: uniform over Ω, with $|\Omega| = N$, then do we have a collision in $O(\sqrt{N})$ whp?
- Not true in general: *Nonreversibility* requires an additional assumption, such as ours.

Mixing Time

Canonical Paths

- *Mihail, Fill:* Mixing time upper bounded in terms of $\lambda_{PP^*}^{-1}$.
  Reversal $\pi(x)P^*(x,y) = \pi(y)P(y,x)$.
  If lazy then $\lambda_{PP^*} \geq \lambda_P$.

Mixing Time

Canonical Paths

- *Mihail, Fill:* Mixing time upper bounded in terms of $\lambda_{PP^*}^{-1}$.
  Reversal $\pi(x)P^*(x,y) = \pi(y)P(y,x)$.
  If lazy then $\lambda_{PP^*} \geq \lambda_P$.
- *Sinclair, Diaconis & Strook:* Spectral gap λ_P lower bounded using paths along edges of P.

Mixing Time

Canonical Paths

- *Mihail, Fill:* Mixing time upper bounded in terms of $\lambda_{PP^*}^{-1}$.
  Reversal $\pi(x)P^*(x,y) = \pi(y)P(y,x)$.
  If lazy then $\lambda_{PP^*} \geq \lambda_P$.
- *Sinclair, Diaconis & Strook:* Spectral gap λ_P lower bounded using paths along edges of P.
  $\Rightarrow$ Mixing time bound using paths along edges of PP^*.

Mixing Time

Canonical Paths

- *Mihail, Fill:* Mixing time upper bounded in terms of $\lambda_{PP^*}^{-1}$.
  Reversal $\pi(x)P^*(x,y) = \pi(y)P(y,x)$.
  If lazy then $\lambda_{PP^*} \geq \lambda_P$.
- *Sinclair, Diaconis & Strook:* Spectral gap λ_P lower bounded using paths along edges of P.
  $\Rightarrow$ Mixing time bound using paths along edges of PP^*.
- *Montenegro:* Better path method when non-reversible, non-lazy and $\min_{P(x,y)>0} P(x,y)$ is small (non-constant); based on Evolving Sets, a consequence of Diaconis-Fill.

Mixing Time

Canonical Paths

Finite, ergodic, $\pi P = \pi$, $\pi(x)P^*(x,y) = \pi(y)P(y,x)$,

$$\forall u \neq v \in \Omega : \; path \; \gamma_{uv} \; along \; PP^*$$

Mixing Time

Canonical Paths

Let

$$A = \max_{x \neq y : PP^*(x,y) \neq 0} \frac{1}{\pi(x) PP^*(x,y)} \sum_{\gamma_{ab} \ni (x,y)} \pi(a)\pi(b)|\gamma_{ab}| \,.$$

Mixing Time

Canonical Paths

If $\pi_* = \min_{v\in\Omega} \pi(v)$ then

$$T \geq 2\,A\,\log\frac{1}{\epsilon\pi_*} \quad \Rightarrow \quad \pi(v)(1-\epsilon) \leq P^T(u,v) \leq \pi(v)(1+\epsilon)$$

Mixing Time

Canonical Paths

Finite, ergodic, $\pi P = \pi$, $\pi(x)P^*(x,y) = \pi(y)P(y,x)$,

$$\forall u \neq v \in \Omega : \; path\ \gamma_{uv}\ along\ PP^*$$

Let

$$A = \max_{x \neq y : PP^*(x,y) \neq 0} \frac{1}{\pi(x)PP^*(x,y)} \sum_{\gamma_{ab} \ni (x,y)} \pi(a)\pi(b)|\gamma_{ab}|\,.$$

If $\pi_* = \min_{v \in \Omega} \pi(v)$ then

$$T \geq 2\,A \log \frac{1}{\epsilon \pi_*} \quad \Rightarrow \quad \pi(v)(1-\epsilon) \leq P^T(u,v) \leq \pi(v)(1+\epsilon)$$

Mixing Time

Paths

- Observe $BB^*(u,\cdot)$ is concentrated near u, $u \pm k$, *etc*.

Mixing Time

Paths

- Consider $B_{1+\delta} = (1-\delta)B + \delta B^2$ for small δ.

Mixing Time

Paths

- Consider $B_{1+\delta} = (1-\delta)B + \delta B^2$ for small δ.
- $$\begin{aligned} & B_{1+\delta}B^*_{1+\delta}(u,2u) \\ \geq \quad & B_{1+\delta}(u,4u)B^*_{1+\delta}(4u,2u) \\ \geq \quad & \frac{\delta}{9}\frac{1-\delta}{3} \geq \frac{\delta(1-\delta)}{81} \end{aligned}$$

Mixing Time

Paths

- Consider $B_{1+\delta} = (1-\delta)B + \delta B^2$ for small δ.
- $$\begin{aligned} & B_{1+\delta}B^*_{1+\delta}(u, 2u) \\ \geq \quad & B_{1+\delta}(u, 4u)B^*_{1+\delta}(4u, 2u) \\ \geq \quad & \frac{\delta}{9}\frac{1-\delta}{3} \geq \frac{\delta(1-\delta)}{81} \end{aligned}$$
- $$\begin{aligned} & B_{1+\delta}B^*_{1+\delta}(u, 2u+1) \\ \geq \quad & B_{1+\delta}(u, 4u+2)B^*_{1+\delta}(4u+2, 2u+1) \\ \geq \quad & \frac{\delta}{27}\frac{1-\delta}{3} = \frac{\delta(1-\delta)}{81} \end{aligned}$$

Mixing Time

Paths

- Observe $RR^*(u,\cdot)$ is at u, $u+1-k$,$u+k-1$, $2u-1$, $2u-k$, $\frac{u}{2}+\frac{1}{2}$, $\frac{u}{2}+\frac{k}{2}$.
- Consider $R^2R^{*2}(u,\cdot)$.

Mixing Time

Paths

- *Paths from* $u \to v$: Set $n = \lceil \log_2 N \rceil$.

Mixing Time

Paths

$$x = (v - 2^n u) \mod N = (x_0 x_1 \cdots x_{n-2} x_{n-1})_2.$$

Mixing Time

Paths

Path $u_0 = u$, $u_{i+1} = 2u_i + x_i$, so $u_n \equiv 2^n\,u + x \equiv v$.

Mixing Time

Paths

- *Paths from* $u \to v$: Set $n = \lceil \log_2 N \rceil$.
  $x = (v - 2^n\, u) \mod N = (x_0 x_1 \cdots x_{n-2} x_{n-1})_2$.
  Path $u_0 = u$, $u_{i+1} = 2u_i + x_i$, so $u_n \equiv 2^n\, u + x \equiv v$.

Mixing Time

Paths

- *Congestion*: Edge (a, b) with $b \equiv 2a + \{0, 1\} \mod N$.
  (a, b) is ith edge of γ_{uv} for $2^{i-1} \times 2^{n-i}$ choices of u, v.
  $\Rightarrow$ at most $n\,2^{n-1} \leq n\,N$ paths include edge (a, b).

Mixing Time

Paths

- *Conclusion*: If $T \geq \frac{486}{\delta(1-\delta)} \lceil \log_2 N \rceil^3$ then

$$\forall u, v \in \mathbb{Z}_N : \frac{1}{N}(1 - 1/N^2) \leq B_{1+\delta}^{T}(u, v) \leq \frac{1}{N}(1 + 1/N^2)$$

Outline

Further Reading

J.H. Kim, R. Montenegro, Y. Peres, P. Tetali.
A Birthday Paradox for Markov chains, with an optimal bound for collision in the Pollard Rho Algorithm for Discrete Logarithm.
http://www.ravimontenegro.com/research/prho.pdf