MPRI – Cours 2.12.2

F. Morain

Lecture I: groups

2015/09/14–21

The slides are available on `http://www.lix.polytechnique.fr/Labo/Francois.Morain/MPRI/2015`

Contents

I. Which groups?

Why? finite groups are used everywhere in crypto (and elsewhere).

Which tasks?

- representing elements;
- drawing elements at random;
- efficient group laws;
- computation of cardinality;
- structure (with generators);
- etc.

Some groups

- $(\mathbb{Z}/N\mathbb{Z})^*$;
- finite fields $\mathbb{F}_{q^n}$ and subfields;
- algebraic curves (elliptic, hyperelliptic, any genus) over finite fields;
- class groups;
- etc.

Case study: order in a *generic* group

$(G, \circ, 1_G)$, Abelian, finite, of order N; computable $\circ$.

Def. $\mathrm{ord}_G(a) = \min\{k > 0, a^k = 1_G\}$.

Thm. (Lagrange) $\mathrm{ord}_G(a) \mid N$.

Coro. $a^{-1} = a^{N-1}$.

Def. $\mathrm{Exp}(G) = \min\{k > 0, \forall\, a \in G, a^k = 1_G\}$.

Prop.
1. $\mathrm{Exp}(G) \mid N$;
2. $\mathrm{Exp}(G) = \mathrm{lcm}(\mathrm{ord}_G(a), a \in G)$.

It can happen that $\mathrm{Exp}(G) < N$, see later.

Finding the order of an element

Pb. $G = \langle g \rangle$, $N = \mathrm{ord}(g)$; what is the order ω of a in G?

Thm. (Lagrange) $\omega \mid N$.

Rem. If N is small, we can enumerate in $O(N)$ or its divisors.

Prop. a is of order ω if and only if
i) $a^\omega = 1_G$;
ii) for all prime $p \mid \omega$, $a^{\omega/p} \neq 1_G$.

Proof:

In practice, if N *and* its factorization are known, easy.

What if we don't know N (completely)? E.g., (hyper)elliptic curves.

Baby-steps giant-steps

Fundamental algorithm in ANT/crypto; due to Shanks.

Write:

$$\omega = cu + d, \quad 0 \le d < u, \quad 0 \le c < N/u.$$
$$a^\omega = 1 \Leftrightarrow (a^{-u})^c = a^d.$$

Number of group operations: $C_o = u + N/u$ minimized for $u = \sqrt{N}$, hence $2\sqrt{N}$ group operations.

Set operations: u insertions in $\mathcal{B}$ and N/u membership tests in the worst case.

$\Rightarrow \mathcal{B}$ must be a hash table, where both operations take $O(1)$.

Complexity: $O(\sqrt{N})$ in time and space.

Function *BSGS(G, g, N, a)*
- **Input** : $G \supset \langle g \rangle$, g of order N
- **Output**: $\omega = \mathrm{ord}(a)$
- $u \leftarrow \lceil \sqrt{N} \rceil$;
- `// Step 1 (baby steps)`
- initialize a table $\mathcal{B}$ for storing u pairs (elt of G, int $< N$);
- store($\mathcal{B}$, $(1_G, 0)$);
- $H \leftarrow a$; store($\mathcal{B}$, $(H, 1)$);
- **for** $d := 2$ **to** $u - 1$ **do**
  - $H \leftarrow H \circ a$; store($\mathcal{B}$, (H, d));
- `// Step 2 (giant steps)`
- $H \leftarrow H \circ a$; $f \leftarrow 1/H = a^{-u}$;
- $H \leftarrow 1_G$;
- **for** $c := 0$ **to** N/u **do**
  - // $H = f^c$
  - **if** $\exists (H', d) \in \mathcal{B}$ *such that* $H = H'$ **then**
    - // $H = f^c = a^d$ hence $\omega = cu + d$
    - **return** $cu + d$;
  - $H \leftarrow H \circ f$;

Exercises

Exo1-1. Decrease the average time by remarking that $c \approx N/(2u)$ on average.

Exo1-2. What if computing $1/x$ is free?

Exo1-3. Design a variant which takes $O(\max(c,d))$ operations. What is its average running time?

II. The ring $(\mathbb{Z}/N\mathbb{Z})^*$

Thm. $\mathbb{Z}$ is an euclidean domain: $a = bq + r$, $0 \leq r < |b|$.

Def. $\mathbb{Z}/N\mathbb{Z} = \{0, 1, \ldots, N-1\}$ set of equivalence classes of $x\mathcal{R}y \iff x - y \in N\mathbb{Z}$ or $x \equiv y \bmod N$; can be equipped with ring operations.

Prop. $(\mathbb{Z}/N\mathbb{Z})^* = \{x \in \mathbb{Z}/N\mathbb{Z}, \exists y, xy \equiv 1 \bmod N\}$
$= \{x \in \mathbb{Z}/N\mathbb{Z}, \gcd(x, N) = 1\}$.

Thm. (Euler totient function)
$\varphi(N) := \mathrm{Card}((\mathbb{Z}/N\mathbb{Z})^*) = \prod_{i=1}^k \varphi(p_i^{\alpha_i}) = \prod_{i=1}^k p_i^{\alpha_i - 1}(p_i - 1)$ where $N = \prod_{i=1}^k p_i^{\alpha_i}$.

Thm. (Carmichael function) $\mathrm{Exp}((\mathbb{Z}/N\mathbb{Z})^*) = \lambda(N) = \mathrm{lcm}_{i=1}^k \lambda(p_i^{\alpha_i})$ where

$$\lambda(p_i^{\alpha_i}) = \begin{cases} \varphi(p_i^{\alpha_i}) = p_i^{\alpha_i - 1}(p_i - 1) & \text{if } p_i \text{ odd or } \alpha_i \leq 2, \\ 2^{e-2} & \text{if } e \geq 3. \end{cases}$$

More properties

Thm. $\mathbb{Z}/N\mathbb{Z}$ is a field iff N is prime.

Thm. $\mathbb{Z}/N\mathbb{Z} \simeq \prod_{i=1}^k \mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}$.

Rem. Chinese Remaindering Theorem (CRT) Given $(x_i)_{1 \leq i \leq k}$ with $x_i \in \mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}$, $\exists$ unique $x \in \mathbb{Z}/N\mathbb{Z}$, $x \equiv x_i \bmod p_i^{\alpha_i}$ for all i.

Thm. $(\mathbb{Z}/N\mathbb{Z})^*$ is cyclic iff $N = p^\alpha$ or $2p^\alpha$ for odd p, or $N = 2, 4$.

Justification of RSA

Prop. If N is squarefree, then for all $a \in \mathbb{Z}$, $a^{\lambda(N)+1} \equiv a \bmod N$.
Proof:

Coro. RSA is valid: for all x, $x^{ed} \equiv x \bmod N$.
Proof:

Quadratic reciprocity (1/2)

Legendre symbol: for prime odd p and $a \in \mathbb{Z}$

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } p \mid a \\ 1 & \text{if } \exists\, x \text{ s.t. } a \equiv x^2 \bmod p \\ -1 & \text{otherwise.} \end{cases}$$

Easy properties:
(i) $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \bmod p$;
(ii) $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$;
(iii) $\left(\frac{a}{p}\right) = \left(\frac{a \bmod p}{p}\right)$;
(iv) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$;

Quadratic reciprocity (2/2)

Not so easy properties: (Gauss)
(v) $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$;
(vi) (Quadratic reciprocity law) p and q odd primes:

$$\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \times \frac{q-1}{2}} \left(\frac{p}{q}\right).$$

Jacobi symbol: $n \in \mathbb{Z}$, $m = \prod_{i=1}^{k} p_i \in \mathbb{Z}$ odd,

$$\left(\frac{n}{m}\right) = \prod_{i=1}^{k} \left(\frac{n}{p_i}\right).$$

Properties: same as for the Legendre symbol.

Ex. Show that $\left(\frac{n}{m}\right) = 0$ iff $\gcd(n, m) > 1$.

III. Finite fields

Thm. (characteristic) Let $\mathbb{F}$ be a finite field.
a) There exists a smallest $p > 1$ s.t. $p.1_{\mathbb{F}} = 0$; p is prime.
b) The set $\{k.1_{\mathbb{F}}, 0 \le k < p\}$ is the smallest subfield of $\mathbb{F}$; it is isomorphic to $\mathbb{F}_p$ (prime subfield of $\mathbb{F}$).

Thm.

$$\begin{array}{ccc} \mathbb{F} \times \mathbb{F} & \to & \mathbb{F} \\ (x, y) & \mapsto & x + y \end{array} \quad \text{and} \quad \begin{array}{ccc} \mathbb{F}_p \times \mathbb{F} & \to & \mathbb{F} \\ (a, x) & \mapsto & ax \end{array}$$

turn $\mathbb{F}$ into a $\mathbb{F}_p$-vector space. If n is the dimension of this space, $\mathbb{F}$ has p^n elements.

Thm. $\mathbb{F}^\times$ is cyclic.

Frobenius

Thm.

$$\begin{array}{rccc} \sigma_F : & \mathbb{F} & \to & \mathbb{F} \\ & x & \mapsto & x^p. \end{array}$$

It is a field automorphism, i.e.

$$\sigma_F(1) = 1, \quad \sigma_F(x + y) = \sigma_F(x) + \sigma_F(y), \quad \sigma_F(xy) = \sigma_F(x)\sigma_F(y).$$

Fixed points are the elements of $\mathbb{F}_p$.
Proof:

Properties of $\mathbf{K}[X]$

Thm. for all $A, B \in \mathbf{K}[X]$, $B \neq 0$. there exists a unique pair (Q, R) in $\mathbf{K}[X]$ s.t.

$$A = BQ + R, \quad \text{with} \quad R = 0 \text{ or } \deg(R) < \deg(B).$$

Thm. (Bézout) There exists U and V in $\mathbf{K}[X]$ s.t.

$$AU + BV = \gcd(A, B).$$

Def. $A(X)$ is irreducible if its degree is ≥ 1, and all its divisors are constant, or $aA(X)$ with $a \in \mathbf{K}^*$.
Thm. We may factor polynomials

$$P = a \prod_{i=1}^{r} P_i^{\alpha_i},$$

where $a \in \mathbf{K}$, P_i monic irreducible and $\alpha_i > 0$.

Quotient ring

Def. $A \equiv B \pmod f$ iff $A - B$ is a multiple of f.

Def. $\mathbf{K}[X]/f\mathbf{K}[X]$ or $\mathbf{K}[X]/(f)$

Let $\overline{P}$ be the class of P. $\mathbf{K}[X]/(f)$ together with
$\overline{A} + \overline{B} = \overline{A+B}$, $\overline{A}\,\overline{B} = \overline{AB}$, is a ring.
Canonical representant: for all P, there is a unique R of degree $n-1$ s.t. $P \equiv R \bmod f$.

With

$$\lambda \cdot \overline{A} = \overline{\lambda A},$$

$\mathbf{K}[X]/(f)$ is $\mathbf{K}$-vector space of dimension n. The set $\{\overline{1}, \overline{X}, \ldots, \overline{X^{n-1}}\}$ is a basis for this vector space.

Thm. A is invertible modulo f iff $\gcd(A, f) = 1$.

Coro. $\mathbf{K}[X]/(f)$ is a field iff f is irreducible. Moreover, if $\mathbf{K} = \mathbb{F}_p$, $\mathbb{F}_p[X]/(f)$ is a field of cardinality $p^{\deg(f)}$.

Building finite fields

Thm. (the canonical way)
Let $f(X)$ be an irreducible polynomial of degree n over $\mathbb{F}_p$.
Then $\mathbb{F}_p[X]/(f(X))$ is a finite field of degree n and cardinality p^n, noted $\mathbb{F}_{p^n}$.

Example

Build $\mathbb{F}_{41^2}$, using a quadratic non-residue modulo 41.

$$\begin{aligned}\left(\tfrac{7}{41}\right) &= (-1)^{(41-1)/2\times(7-1)/2}\left(\tfrac{41}{7}\right)\\ &= \left(\tfrac{41}{7}\right) = \left(\tfrac{41 \bmod 7}{7}\right)\\ &= \left(\tfrac{6}{7}\right) = \left(\tfrac{2}{7}\right)\left(\tfrac{3}{7}\right) = \left(\tfrac{3}{7}\right) = (-1)\left(\tfrac{7}{3}\right)\\ &= -\left(\tfrac{1}{3}\right) = -1\end{aligned}$$

$\Rightarrow \mathbf{K}_1 = \mathbb{F}_{41^2} \sim \mathbb{F}_{41}[X]/(X^2 - 7)$.
This is a vector space of dimension 2 over $\mathbb{F}_{41}$.
Let $\theta = \overline{X}$. All elements can be written $a + b\theta$ where a, b are in $\mathbb{F}_{41}$.
$\theta^2 - 7 = \overline{X^2 - 7} = 0$. We get

$$\theta^2 = 7, \theta^3 = 7\theta, \theta^4 = 8, \ldots, \theta^{80} = 1,$$

so that θ does not generate $\mathbf{K}^*$, but $\theta + 10$ does.

Application (1/2)

Pb. Given $\left(\frac{a}{p}\right) = 1$, compute $\sqrt{a} \bmod p$.

Case $p \equiv 3 \bmod 4$**:** $r = a^{(p+1)/4} \bmod p$.

Case $p \equiv 1 \bmod 4$**:** find b s.t. $\Delta = b^2 - 4a$ is not a square.

$$\alpha = (-b + \sqrt{\Delta})/2 \quad \Rightarrow \alpha^p = (-b - \sqrt{\Delta})/2 \quad \Rightarrow \alpha\alpha^p = a$$

since $\sqrt{\Delta}^p = \left(\frac{\Delta}{p}\right)\sqrt{\Delta}$.
Let $\beta = \alpha^{(p+1)/2} \bmod (p, X^2 + bX + a)$. Then

$$\beta^2 = \alpha^{p+1} = a;$$

$$\beta^p = \beta(\beta^2)^{(p-1)/2} = \beta a^{(p-1)/2} = \beta$$

$\Rightarrow \beta \in \mathbb{F}_p$.

Application (2/2)

Let $a = 2 \bmod 41$, which is a square;
$b = 1$ is s.t. $\Delta = 1 - 4 \times 2 = -7$ which is not a square; hence $\mathbb{F}_{41^2} \sim \mathbb{F}_{41}[X]/(X^2 + X + 2)$.

$$\alpha = X, \quad \alpha^p = 40X + 40, \quad \alpha\alpha^p = 2.$$

$$\beta = X^{(p+1)/2} = 17, \quad 17^2 \equiv 2 \bmod 41.$$

IV. Generic DLP

DLP: given $h \in G = \langle g \rangle$ of order N, find an integer n, $0 \leq n < N$ such that $h = g^n$.

Z) The Pohlig-Hellman reduction.

A) Enumeration; baby-steps, giant steps (adaptation as exercises).

B) RHO.

C) Kangaroos.

D) Nechaev-Shoup.

Z) The Pohlig-Hellman reduction

Idea: reduce the problem to the case N prime.

$$N = \prod_i p_i^{\alpha_i}$$

Solving $g^n = h$ is equivalent to knowing $n \bmod N$, i.e. $n \bmod p_i^{\alpha_i}$ for all i (chinese remainder theorem).

Idea: let $p^\alpha \mid\mid N$ and $m = N/p^\alpha$. Then $b = h^m$ is in the cyclic group of ordre p^α generated by g^m. We can find the log of b in this group, which yields $n \bmod p^\alpha$.

Cost: $O(\max(DL(p^\alpha))) = O(\max(DL(p)))$.

Consequence: for DH, N must have at least one large prime factor.

B) The RHO method

Basic model: birthday paradox
Let E be a finite set of cardinality m.

Thm. Suppose we draw uniformly n elements from E with replacement. The probability that all n elements are distinct is $\text{Proba} = \frac{1}{m}\prod_{k=1}^{n-1}\left(1-\frac{k}{m}\right)$.

Taking logarithms, and assuming $n \ll m$, we get

$$\log \text{Proba} \approx \log(n/m) - \frac{n(n-1)}{2m}.$$

$\Rightarrow$ taking $n = O(\sqrt{m})$ will give a somewhat large value for this probability.

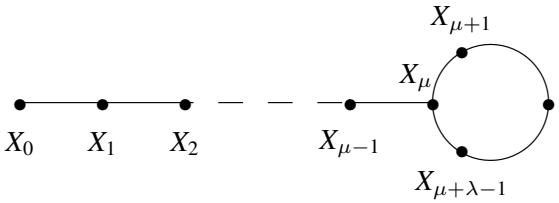
A very simple algorithm

Function *NaiveDL(G, g, N, h)*
  Input : $G \supset \langle g \rangle$, g of order N
  Output: $0 \le n < N$, $g^n = h$
  initialize a table $\mathcal{L}$ for storing u triplets (elt of G, two ints $< N$);
  repeat
    draw u and v at random modulo N;
    $H \leftarrow g^u \circ h^v$;
    if $\exists (H', u', v') \in \mathcal{L}$ *such that* $H = H'$ **then**
      // $H = g^u \circ h^v = g^{u'} \circ h^{v'}$
      // hence $n(v - v') = u' - u \bmod N$
      if $v - v'$ *is invertible modulo* N **then**
        return $(u' - u)/(v - v') \bmod N$;
    else
      store($\mathcal{L}$, (H, u, v));
  until *a collision is found*;

Complexity: $O(\sqrt{n}\log n)$ on average, together with a space $O(\sqrt{n})$, which is no better than BSGS.

Functional digraphs

Let $f : E \to E$ be a function on E.
Consider $X_{n+1} = f(X_n)$ for some starting point $X_0 \in E$.
The functional digraph of X is built with vertices X_i's; an edge is put between X_i and X_j if $f(X_i) = X_j$.

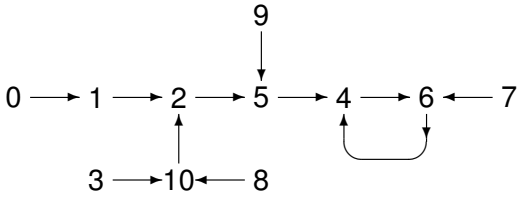


The first part of the sequence is the set of X_i's that are reached only once and there are μ of them.
The second part forms a loop containing λ distinct elements.
Rem. λ and ν cannot be too large on average (use $n = \lambda + \mu$ in the Theorem).

Examples

1) $E = G$ finite group, $f(x) = ax$ and $x_0 = a \Rightarrow (x_n)$ purely is periodic, i.e., $\mu = 0$, and $\lambda = \text{ord}_G(a)$.

2) Take $E = \mathbb{Z}/11\mathbb{Z}$ and $f : x \mapsto x^2 + 1 \bmod 11$



Typical shape: a cycle and trees plugged on the structure.

Epact

Goal: find λ and μ.

Prop. There exists a unique $e > 0$ (epact) s.t. $\mu \leq e < \lambda + \mu$ and $X_{2e} = X_e$.
It is the smallest non-zero multiple of λ that is $\geq \mu$: if $\mu = 0$, $e = \lambda$ and if $\mu > 0$, $e = \lceil \frac{\mu}{\lambda} \rceil \lambda$.

Proof:

Floyd's algorithm

Function *epact(f, x_0)*
Input : A function f, a starting point x_0
Output: The epact of (x_n) defined by $x_{n+1} = f(x_n)$
$x \leftarrow x_0$; $y \leftarrow x_0$; $e \leftarrow 0$;
repeat
  $e \leftarrow e + 1$;
  $x \leftarrow f(x)$;
  $y \leftarrow f(f(y))$;
until $x = y$;
return e.

Cost: $3e$ evaluations of f and e comparisons. For decreasing the number of evaluations, see Brent (and Montgomery).

Asymptotic statistics

Convenient source: Flajolet & Odlyzko (EUROCRYPT 1989).

Thm. When $m \to \infty$

$$\overline{\lambda} \sim \overline{\mu} \sim \sqrt{\frac{\pi m}{8}} \approx 0.627\sqrt{m}.$$

Thm. $\overline{e} \sim \sqrt{\frac{\pi^5 m}{288}} \approx 1.03\sqrt{m}$.

Fundamental coro. A collision is expected to be found after $O(\sqrt{m})$ computations.

Application to DL

Pollard: build a function f from G to G appearing to be random, i. e., the epact of f is $c\sqrt{N}$ for some small c.

. . . **Teske**:

- precompute r random elements $z_i = g^{\gamma_i} \circ h^{\delta_i}$ for $1 \leq i \leq r$ for some random exponents (say $r = 20$);
- use some hash function $\mathcal{H} : G \to \{1, \ldots, r\}$;
- define $f(y) = y \circ z_{\mathcal{H}(y)}$ so that

$$x_i = g^{c_i} \circ h^{d_i},$$

  where (c_i) and (d_i) are two integer sequences.

Ex. if G contains integers, we may simply use $\mathcal{H}(x) = 1 + (x \bmod r)$.

Application to DL (cont'd)

When e is found:

$$g^{c_{2e}} \circ h^{d_{2e}} = g^{c_e} \circ h^{d_e}$$

or

$$g^{c_{2e}-c_e} = h^{d_e-d_{2e}}$$

i.e.,

$$n(c_{2e} - c_e) \equiv (d_e - d_{2e}) \bmod N.$$

Function *Iterate(G, N, $\mathcal{H}$, $(z_i, \gamma_i, \delta_i)$, x, u_x, v_x)*
  Input : $\mathcal{H} : G \to \{1, \ldots, r\}$; $(z_i)_{1 \le i \le r}$ random powers $z_i = g^{\gamma_i} \circ h^{\delta_i}$ of G; $x = g^{u_x} h^{v_x}$
  Output: $f(x, u_x, v_x) = (w, u_w, v_w)$ s.t. $w = g^{u_w} \circ h^{v_w}$
  $i \leftarrow \mathcal{H}(x)$;
  return $(x \circ z_i, u_x + \gamma_i \pmod N, v_x + \delta_i \pmod N)$.

The algorithm

Function *RHO(G, g, N, h, $\mathcal{H}$, $(z_i, \gamma_i, \delta_i)$)*
  Input : $\mathcal{H} : G \to \{1, \ldots, r\}$; $(z_i)_{1 \le i \le r}$ random powers $z_i = g^{\gamma_i} \circ h^{\delta_i}$ of G
  Output: $0 \le n < N$, $g^n = h$
  if $h = 1_G$ **then**
    return 0
  $x \leftarrow h$; $u_x \leftarrow 0$; $v_x \leftarrow 1$;
  $y \leftarrow x$; $u_y \leftarrow u_x$; $v_y \leftarrow v_x$;
  repeat
    // invariant: $x = g^{u_x} \circ h^{v_x}$, $y = g^{u_y} \circ h^{v_y}$
    $(x, u_x, v_x) \leftarrow$ Iterate(G, N, $\mathcal{H}$, $(z_i, \gamma_i, \delta_i)$, x, u_x, v_x);
    $(y, u_y, v_y) \leftarrow$ Iterate(G, N, $\mathcal{H}$, $(z_i, \gamma_i, \delta_i)$, y, u_y, v_y);
    $(y, u_y, v_y) \leftarrow$ Iterate(G, N, $\mathcal{H}$, $(z_i, \gamma_i, \delta_i)$, y, u_y, v_y);
  until $x = y$;
  // $g^{u_x} \circ h^{v_x} = g^{u_y} \circ h^{v_y}$
  if $v_x - v_y$ *is invertible modulo* N **then**
    return $(u_y - u_x)/(v_x - v_y) \pmod N$;
  else
    return *Failure*.

Parallel RHO (1/3)

Goal: if we have p processors, want a gain of p.

We cannot use the notion of epact (all epacts have the same size).

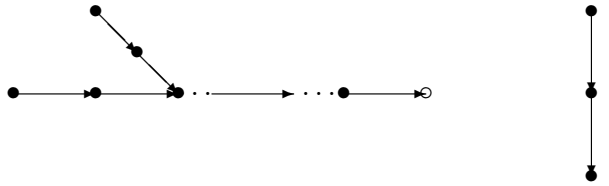
More asymptotic parameters:

- Number of components: $\frac{1}{2} \log m$;
- component size of ν: $2m/3$;
- tree size containing ν: $m/3$ (maximal tree rooted on a circle containing ν);
- number of cyclic nodes: $\sqrt{\pi m/2}$.

$\Rightarrow$ giant component that contains almost everybody.

Parallel RHO (2/3)

Use the same f and store distinguished elements, i.e., elements having a special form.



If $\theta < 1$ is the proportion of distinguished elements, the time to reach one of these will be $1/\theta$.

Parallel RHO (3/3)

Function *DistinguishedPath(*f*,* x_0*)*
Input : A function f, a starting point x_0
Output: The first distinguished element found starting at x_0,
$x \leftarrow x_0$; **repeat**
  $x \leftarrow f(x)$;
until x *is distinguished*;
return x.

Rem. Many subttle points (cycles, automorphisms, etc.).

Prop. The expected running time is $\sqrt{\pi N/2}/p + 1/\theta$ group operations.

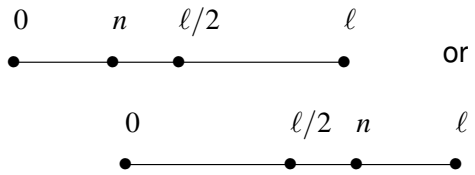
C) Kangaroos

Pb: solve DLP when $n \in [0, \ell]$ with $\ell \leq N$.
Goal: algorithm with running time $O(\sqrt{\ell})$ instead of $O(\sqrt{N})$. The idea is to have two processes, traditionnaly called kangaroos:

- We use a sequence of integer increments $(\delta_i)_{1 \leq i \leq r}$ whose mean size is m. Then, we iterate: $f(x) = x \circ g^{\delta_{\mathcal{H}(x)}}$.
- The tame kangaroo follows a random path starting from $g^{\ell/2}$;
- The wild kangaroo starts from $h = g^n$ and uses the same random function.
- $T = g^{d_T}$ and $W = h \circ g^{d_W}$ for two integer sequences d_T and d_W that are updated when computing f.
- When hitting a distinguished element, it is stored in a list depending on its character (tame or wild).
- When a collision occurs, the discrete logarithm is found.

(Heuristic) analysis

The original positions of K_T and K_W can be either



In either case: back kangaroo (B) and a front kangaroo (F) heading right.
They are at mutual distance $\approx \ell/4$ at the beginning.
Since the average distance between two points is m, B needs $\ell/(4m)$ jumps to reach the initial position of F. After that, B needs m jumps to reach a point already reached by F. The total number of jumps is therefore $2(\ell/(4m) + m)$, which is minimized for $m = \sqrt{\ell}/2$, leading to a $2\sqrt{\ell}$ cost.

The algorithm

Function *Kangaroo(*G*,* g*,* N*,* h*,* ℓ*)*
Input : $G \supset \langle g \rangle$, g of order N
Output: $0 \leq n < \ell$, $g^n = h$
$m \leftarrow \lceil \sqrt{\ell}/2 \rceil$;
compute positive increments $(\delta_i)_{1 \leq i \leq r}$ of mean value m;
initialize two tables $\mathcal{T}$ and $\mathcal{W}$ for storing pairs (elt of G, int $< N$);
$T \leftarrow g^{\ell/2}$; $d_T \leftarrow \ell/2$;
$W \leftarrow h$; $d_W \leftarrow 0$;
while *true* **do**
  $(T, d_T) \leftarrow f((\delta_i), T, d_T)$;
  if $\exists (W', d') \in \mathcal{W}$ *such that* $W' = T$ **then**
    // $T = g^{d_T}$, $W' = h \circ g^{d'}$
    return $(d_T - d') \pmod N$;
  $(W, d_W) \leftarrow f((\delta_i), W, d_W)$;
  if $\exists (T', d') \in \mathcal{T}$ *such that* $T' = W$ **then**
    // $T' = g^{d'}$, $W = h \circ g^{d_W}$
    return $(d' - d_W) \pmod N$;

Parallel kangaroos

Idea: start p kangaroos that will discover and store distinguished elements.

Pollard: we assume $p = 4p'$, and select $u = 2p' + 1$, $v = 2p' - 1$, so that $p = u + v$.

- Increments of the jumps will be $(uvs_1, \ldots, uvs_k)$ for small s_i's, insisting on the mean to be $\approx \sqrt{\ell/(uv)}$;
- i-th tame kangaroo will start at $g^{\ell/2+iv}$ for $0 \leq i < u$;
- i-th wild kangaroo W_i will start from $h \circ g^{iu}$, $0 \leq i < v$;
- a collision will be $\ell/2 + iv = n + ju \bmod (uv)$ and the solution is unique. This prevents kangaroos from the same herd to collide.

The final running time is effectively divided by p.

D) Nechaev/Shoup

Thm. Any generic group DL algorithm requires $\Theta(\sqrt{N})$ group operations.

Rough idea: given DL's for $h_1, h_2, \ldots, h_k$, we can only build new DL's for $O(k^2)$ elements of G. To cover G, we need $k \approx \sqrt{N}$.

Take home messages

To have a better than square-root algorithm for DL, you need specific ideas for specific groups.

Many crypto problems of size n may have solution algorithms in $O(\sqrt{n})$ (time and/or space; deterministic or probabilistic).