Shor's algorithm

Some computational problems

- Factoring: Given N, find prime factors
  - ↳ Important in crypto: If you can factor, you can break RSA
- Discrete log problem:
  Given a group G (integers mod p), generator $g \in G$, given $y \in G$. Find: x s.t. $y = g^x$
  - ↳ Important: Can break (unif.) Elliptic Curve Crypto
- Period finding: (or something else)
  Given $f: \mathbb{Z} \to X$
  find a smallest p s.t. f is p-periodic ($\forall a: f(a) = f(a+p)$)
  - ↳ Important for crypto: Solves the probs above

RSA secret key: p, q primes, d $\quad$ $d \cdot e \equiv 1 \bmod \varphi(N) = (p-1)(q-1)$
public key: $N = pq$, e s.t.

$\mathrm{Enc}(m) = m^e \bmod N$; $\mathrm{Dec}(c) = c^d \bmod N$

$m = 0, \dots, N-1$

$\mathrm{Dec}(\mathrm{Enc}(m)) = m^{ed} \bmod N$
$= m^{k\varphi(N)+1} \bmod N$
$= m^1 \bmod N = m$

How to break? N factor $\to p, q \to \varphi(N) \to d$ (ext. Eucl.)
e

ElGamal encryption

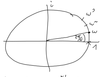
Group G (e.g. mod p, or EC), generator g
secret key: x
public key: $h = g^x$
$\mathrm{Enc}(m) := (g^r, m \cdot h^r)$ (pick random r)
$\mathrm{Dec}(c_1, c_2)$: • $c_1 = g^r \Rightarrow (g^r)^x = (g^x)^r = h^r$
• $c_2 / h^r = m$

Attack: $h = g^x$ (dlog) $\to x$ $\quad$ Enc: g^r (dlog) $\to r$, $m = c_2 / h^r$

Overview:
- Show for period finding (with some simplifications)
- How to use period finding for factoring / dlog

Discrete Fourier Transform ($N \in \mathbb{N}$)

$\mathrm{DFT}_N = \left(\frac{1}{\sqrt{N}} \omega^{kl}\right)_{k,l=0,\dots,N-1} \in \mathbb{C}^{N \times N}$ $\quad$ $\omega := e^{\frac{-2\pi i}{N}}$



$\omega^N = 1$
$\omega^{kN} \neq 1$

Properties
- Unitary
- DFT maps a signal (i.e. vector) to frequency spectrum
- Given N-vector, compute DFT_N in $O(N \log N)$ steps (classically) (primitive root of 1)
- Given N-dim q state (e.g. $N = 2^n$, n qubits), we can apply DFT_N in q steps.
- Takes $O(n^2)$ q gates (if $N = 2^n$)

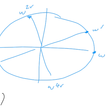
DFT & Frogs

Say: $\psi = (1\,0\,0\,0\,0\,1\,0\,0\,0\,0\,1\,0\,0\,0\,0 \dots 1\,0\,0\,0)^T \in \mathbb{C}^N$
(assume $r \mid N$)

What is $\mathrm{DFT}_N \psi =: \phi$

$\phi_k = \sum_{l=0}^{N-1} (\mathrm{DFT}_N)_{kl} \psi_l = \frac{1}{\sqrt{N}} \omega^{kl} \cdot 1$ iff $r \mid l$

$= \frac{1}{\sqrt{N}} \sum_{l \mid r} \omega^{kl} = \begin{cases} 0 & \text{otherwise} \\ 1 & l = \text{multiple of } \frac{N}{r} \end{cases}$ (multiple of r)

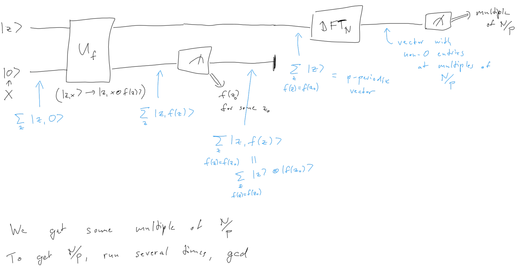


$\Rightarrow \phi = (1\,0\,0\,\underbrace{1\,0\,0}_{N/r}\,1\,0\,0 \dots 1\,0\,0)$

Facts: If ψ is shifted, get same ϕ (up to phase factors)

Shor's algo

Given $f: \mathbb{Z} \to X$ with period p
Assume $p \mid N$ (simplification)



$\sum_a |a, f(a)\rangle \overset{\text{measure}}{\to} \sum_{a : f(a)=f(a+p)} |a, f(a)\rangle = \sum_a |a\rangle \otimes |f(a)\rangle$

$\Rightarrow$ We get some multiple of $\frac{N}{p}$
To get $\frac{N}{p}$, run several times, gcd

Thm: Alg., given p-periodic f, finds p assuming $p \mid N$, N known
(also $N = 2^n$ if we want simple DFT)

It also works if $p \nmid N$ but $N \gg p$.
(Using classical postproc. still get p)

$\Rightarrow$ Period finding solved.
(wk gates for DFT + 1 eval of U_f)

Factoring from period finding

Algo: Input $N \in \mathbb{N}$ (not prime)
- Pick $a \in \{1, \dots, N-1\}$ coprime with N
- Compute $r := \mathrm{ord}(a) \bmod N$ (period of $a \mapsto a^a \bmod N$)

With prob $\geq \frac{1}{2}$: r even (else: restart)

- $(a^{r/2} - 1)(a^{r/2} + 1) \equiv a^r - 1 \equiv 0 \bmod N$
  $\Rightarrow N \mid (a^{r/2} - 1)(a^{r/2} + 1)$
  With prob $\geq \frac{1}{2}$: $N \nmid (a^{r/2} - 1)$, $N \nmid (a^{r/2} - 1)$
  (else restart)
  $\Rightarrow a^{r/2} - 1$ contains some but not all prime factors of N
  $\Rightarrow \gcd(a^{r/2} - 1, N)$ is a nontrivial factor of N

Discrete log Given g, y, find x s.t. $g^x = y$

$f(a,b) = g^a / y^b$

$f(a,b) = f(\tilde{a}, \tilde{b}) \Leftrightarrow g^a / y^b = g^{\tilde{a}} / y^{\tilde{b}}$
$\Leftrightarrow g^{a-\tilde{a}} = y^{b-\tilde{b}} = g^{x(b-\tilde{b})}$
$\Leftrightarrow (a - \tilde{a}) - x(b - \tilde{b}) = 0 \bmod |G|$

Eg: $\tilde{b} = b + 5$
$\tilde{a} = a + 5x$
$\Rightarrow f(ab) = f(\tilde{a}\tilde{b})$

$\Rightarrow f$ is $(x, 1)$-periodic

$\Rightarrow$ period finding (generalized) gives us $(x, 1) \to x = \log_g y$.