Overview

Quantum Algorithms - ~~Difficulty~~ circuits

Classical Algorithms - TM, RAM, etc

Complexity -

- coming up with good quantum algs seems to be diff.
- want qalgs to be better than the best known classical algs
- Intuition suited to classical algs

n bits ↔ n qubits

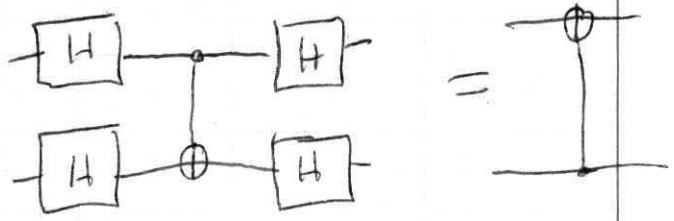
Classical

Number field sieve

$\left[e^{\Theta(n^{1/3} \log^{2/3} n)} \right]$

Shor's

$O(n^2 \log n \log\log n)$



Thinking abt problems with classical intuition yields classical algorithms

→ An example of a "good" qalg

I Num Theory
Divisibility, gcd, congruences

II Order finding
reduction of factoring to OF

III Intro Q Algs
gates as a computational model

IV DFT and QFT

Product Representation of QFT

Circuit realization

V Phase Estimation

use of QFT

→ Approximating eigenvalues of a unitary operator

VI Q Order Finding

Use of Phase Est

I. Number Theoretic Introduction

A. Divisibility

Let $a, b \in \mathbb{Z}$, $a \neq 0$.

a divides b (or b is a multiple of a) if

$\exists\, q \mid q = ba$

Then we write $a \mid b$ — a is a divisor of b

- $a \mid b \rightarrow a \mid kb \quad \forall k$
- $a \mid b, b \mid a \rightarrow a = \pm b$
- $a \mid b, b \mid c \quad a \mid sb + tc$
- $\forall k \neq 0, \quad a \mid b \iff ka \mid kb$

Division Thm $a, b \in \mathbb{Z}$, $a > 0$, then

$\exists!\, q, r \mid b = qa + r$ and $0 \leq r < a$

q quotient, r remainder C, C++

Proof. Set $\{x \mid x > b - \lfloor b/a \rfloor a\}$ has a least element t, $q = t - 1$

B.

Def Largest positive integer dividing a, b is "gcd" a, b — $\gcd(a, b)$

Thm $\gcd(a, b)$ is the smallest positive integer that can be expressed as a linear combination of a and b: $as + bt$

Cor if $c \mid a$, $c \mid b$ then $c \mid \gcd(a, b)$

Proof: $d = sa + tb \rightarrow d \mid \gcd$

Proof $\exists$ min $m = as + bt$
Division $\rightarrow a = qm + r$
$r = a - qm = a - q(sa + bt)$
$= (1 - qs)a + (-qt)b$
r a l.c. of a, b, $r < m \rightarrow r$
$a = qm$, $m \mid a$ $m \mid b$
$d \mid m \rightarrow d \leq m \rightarrow d =$

Co-Primality (relatively Prime)

Def integers a, b are said to be rel prim if $\gcd(a,b) = 1$

skip { Integers $m_1, m_2, \ldots, m_x$ are pairwise relatively prime if $\gcd(m_i, m_j) = 1$ whenever $i \neq j$

GCD Algorithm

$$\gcd(a,b) = \gcd(b,r)$$

r remainder when a is divided by b

```
Euclid(a, b)
{
    if (b = 0) return a
    return Euclid(b, a % b)
}
```

Euclid (30, 21)
= Euclid (21, 9)
= E (9, 3)
= E (3, 0) = 3

Prime number is an integer $p > 1$ that has no divisors other than 1 and itself. others composit

Fundamental Theorem of Arth

Each integer $n > 1$ is a product of primes
This is unique up to the order of factors

(5) Congruences

Let $m \in \mathbb{Z}_+$. If $m \mid (a-b)$ we say

$a \equiv b \pmod m$ otherwise $a \not\equiv b \pmod m$

m modulus, b = "residue of "a" modulo m"

Eqv $a = b + km$ (for some k)

Two numbers are congruent modulo m if they leave the same remainder when divided by m

"Modular arithmetic" ← we only pay attn to remainders

$$\begin{cases} a \equiv b \pmod m \\ b \equiv a \pmod m \end{cases}$$ equivalent

Examples

$a \equiv b \ m, \ b \equiv c \ m \rightarrow a \equiv c \ m$

$a \equiv b \ m, \ c \equiv d \ m \rightarrow a \pm c \equiv b \pm d \ \text{mod} \ m$

etc.

$a \equiv b \pmod m$ and $c \equiv d \pmod m$

$ac \equiv bd \pmod m$

"modular multiplication"

$a \equiv b \pmod m \rightarrow a^n \equiv b^n \pmod m$

"mod exp"

D. Euler's ϕ-function

$\forall m > 1$

$\phi(m) \equiv$ the number of positive integers $\le m$ less than m such that $\gcd(m, n) = 1$

$\phi(1) = 1$

skip

Properties:

$\phi(m) \le m - 1$

$\phi(m) = m - 1$ iff m is prime

3:25

II Order finding

Suppose N is a positive integer, x is relatively prime to N. $1 \le x < N$

The order of x modulo N is defined to be the least positive integer r s.t. $x^r \equiv 1 \pmod N$

$N \in \mathbb{Z}_+$ $\gcd(x, N) = 1$, $1 \le x < N$, then

The order of $x \bmod N$ is the least positive integer

$$r \mid x^r \equiv 1 \pmod N$$

Given x, N, the "order-finding" problem is to determine r.

ex
$3^1 \equiv 3 \bmod 5$
$3^2 = 9 \equiv 4 \bmod 5$
$3^3 = 0 \equiv 2 \bmod 5$
$3^4 = 81 \equiv 1 \bmod 5$
3 is order 4 mod 5

A. Reduction of factoring to order finding

1. Show we can find a factor of n if we can solve (nontrivially) $x^2 \equiv 1 \pmod N$
2. a random $y \mid \gcd(N, y) = 1$ likely has an order r modulo n which is even and s.t. $y^{r/2} \not\equiv \pm 1 \pmod N$

1. Trivial solutions

$$x \equiv 1 \pmod N, \quad x \equiv -1 \pmod N$$
$$(x = N-1)$$

But, if $x^2 \equiv 1 \bmod N$ (nontrivial...)

$$N \mid (x^2 - 1) \rightarrow N \mid (x+1)(x-1)$$

{ N must share at least one factor with either $x+1$ or $x-1$ ($p|ab \rightarrow p|a$ or $p|b$ and N is a product of primes)

Since $1 < x < N-1$

$x-1 < x+1 < N$ so the common factor cannot be N.

→ compute $\gcd(x-1, N)$ $\gcd(x+1, N)$

one of these gives a nontrivial factor

2. $P(r \text{ is even and } y^{r/2} \neq -1 \pmod N) \geq 1 - \frac{1}{2^m}$

m is number of unique prime factors of N

(B) Decomposition

```
Find-factor(N)
  if N even
      return 2
      Remove the degenerate cases, where possible
  x ← Random (1, N-1)   exclusive
      if gcd(x, N) > 1
          return gcd(x, N)
  Find the order r of x modulo N
  if r even, and x^{r/2} ≠ -1 Mod N
      Compute gcd(x^{r/2} - 1, N)
      Compute gcd(x^{r/2} + 1, N)
          return nontrivial factor
```

3.35

III Quantum Algorithms

(A) Quantum computer ⟷ quantum circuit

1) quantum part, classical part. (to make things simple)

2) State space

Insert →

n qubits → 2^n-dimensional complex Hilbert space

product states of the form

$$|x_1\rangle \otimes |x_2\rangle \otimes \cdots \otimes |x_n\rangle \longleftrightarrow |x_1 x_2 \cdots x_n\rangle$$

$x_i = 0, 1$

are called <u>computational basis</u> states

"Analogy" with n-d vector

essentially a sequence of complex numbers

3) Quantum gates

Apply to any subset of qubits

$$X = \begin{bmatrix} |0\rangle & |1\rangle \\ 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{matrix} |0\rangle \\ |1\rangle \end{matrix}$$

action of X on basis states

some gate sets are universal

4) Ability to perform measurements in the basis

→ collapses state space

(B) Review

Single qubit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

α, β complex, $|\alpha|^2 + |\beta|^2 = 1$

IV DFT and QFT

(A) Recall $\mathcal{DFT}(\langle x_0, x_1, \cdots, x_{N-1}\rangle) \to \langle y_0, y_1, \cdots, y_{N-1}\rangle$

$$y_k \equiv \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j e^{2\pi i j\cdot k/N}$$

Used in Signal Processing, etc

Here $\langle x_0, x_1, \cdots, x_n\rangle$ is some vector of complex numbers.

(B) QFT is exactly the same thing

Instead of a vector of complex numbers we have coefficients for each basis state of computational

$$\langle x_0, x_1, \cdots x_n\rangle \longrightarrow \langle y_0, y_1, \cdots y_n\rangle$$

Quantum

$$x_0|000\cdots0\rangle + x_1|000\cdots1\rangle + \cdots x_n|111\cdots1\rangle \longrightarrow y_0|0\cdots0\rangle + y_1|000\cdots1\rangle + \cdots + y_n|111\cdots1\rangle$$

↑ binary representation of subscript

y_n's are as before.

To define QFT we (use Dirac not.)

$$|j\rangle \longrightarrow \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi i jk/N}|k\rangle$$

define its action on basis states

Just like C-NOT, etc.

This is like the "truth table" (bit not)

Equivalently for an arbitrary state

$$\sum_{j=0}^{N-1} x_j|j\rangle \to \sum_{k=0}^{N-1} y_k|k\rangle \qquad (y_k \text{ are DFT of } x_k)$$

Example:

$$|000\ldots0\rangle \rightarrow \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi i \cdot 0 \cdot k/N} |k\rangle$$

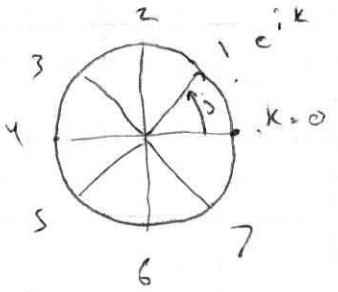
$2^n = N$

$$\rightarrow \frac{1}{\sqrt{N}} \left[|000\rangle + |0001\rangle + |0010\rangle + \ldots + |1111\rangle \right]$$

$n=3$

$N = 2^n = 8$

$$|001\rangle \rightarrow \frac{1}{\sqrt{8}} \sum_{k=0}^{7} e^{2\pi i \cdot k/8} |k\rangle$$



Explain: frequency?

$$\rightarrow \frac{1}{\sqrt{8}} \left[|000\rangle + e^{i\pi/4} |001\rangle + e^{i\pi/2} |002\rangle + e^{i3\pi/4} |111\rangle \right]$$

A natural question is that if we can compute $\mathcal{F}$ of some state $|\psi\rangle$ can we leverage this to speed up any algorithm requiring $\mathcal{F}$ (signal processing)

NO → measurement is probabilistic, disturbs remaining system

Notation

$$j = j_1 j_2 \ldots j_n \quad j_k \in \{0,1\}$$

$$0.j_l j_{l+1} \ldots j_m \longleftrightarrow j_l/2 + j_{l+1}/4 + \ldots + j_m/2^{m-l+1}$$

3rd

⑥ Product Representation

$$|j\rangle \to \frac{1}{2^{n/2}} \sum_{k=0}^{2^n-1} e^{2\pi i j k/2^n} |k\rangle$$

$k = k_1 2^{n-1} + k_2 2^{n-2} + \cdots k_n$

n qubits

$\frac{k}{2^n} = \frac{k_1}{2^1} + \frac{k_2}{2^2} + \cdots \frac{k_n}{2^n}$

Break this sum up

$$\frac{1}{2^{n/2}} \sum_{k=0}^{2^n-1} e^{2\pi i j \left(\sum_{l=1}^{n} k_l 2^{-l}\right)} |k_1 \ldots k_n\rangle$$

$e^{a+b} = e^a e^b$

$$\frac{1}{2^{n/2}} \sum_{k=0}^{2^n-1} e^{2\pi i j \frac{k_1}{2}} e^{2\pi i j \frac{k_2}{2^2}} \cdots e^{2\pi i j \frac{k_n}{2^n}} |k_1\rangle \otimes |k_2\rangle \otimes$$

$$= \frac{1}{2^{n/2}} \sum_{k=0}^{2^n-1} \bigotimes_{l=1}^{n} e^{2\pi i j k_l / 2^l} |k_l\rangle$$

$$= \frac{1}{2^{n/2}} \sum_{k_1=0}^{1} \sum_{k_2=0}^{1} \cdots \sum_{k_n=0}^{1} \bigotimes_{l=1}^{n} e^{2\pi i j k_l / 2^l} |k_l\rangle$$

$$= \frac{1}{2^{n/2}} \bigotimes_{l=1}^{n} \left[\sum_{k_l=0}^{1} e^{2\pi i j 2^{-l}} |k_l\rangle \right]$$

$$= \frac{1}{2^{n/2}} \bigotimes_{l=1}^{n} \left[|0\rangle + e^{2\pi i j 2^{-l}} |1\rangle \right]$$

$$= \frac{\left(|0\rangle + e^{2\pi i 0.j_n} |1\rangle\right)\left(|0\rangle + e^{2\pi i 0.j_{n-1} j_n} |1\rangle\right) \cdots \left(|0\rangle + e^{2\pi i 0.j_1 j_2 \ldots j_n} |1\rangle\right)}{2^{n/2}}$$

(D) Using product rep allows an efficient circuit.

Define $R_k \equiv \begin{bmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^k} \end{bmatrix}$

- we want to map $|j_1, j_2, \cdots j_n\rangle \rightarrow$

$$(|0\rangle + e^{2\pi i\, 0.j_n}|1\rangle)(|0\rangle + e^{2\pi i\, 0.j_{n-1}, j_n}|1\rangle) \otimes (|0\rangle + e^{2\pi i\, 0.j_{n-2}, j_{n-1}, j_n}|1\rangle)$$

$$|j_n\rangle \otimes |j_{n-1}\rangle \otimes \cdots \otimes |j_1\rangle$$

Hadamard

$$\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \longrightarrow \quad |0\rangle \rightarrow \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

$$|1\rangle \rightarrow \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

Basis state

$$|j\rangle \rightarrow \frac{1}{\sqrt{2}}\left(|0\rangle + (-1)^j |1\rangle\right)$$

"computational basis"

$$|j\rangle \rightarrow \frac{1}{\sqrt{2}}\left(|0\rangle + e^{j\pi i}|1\rangle\right)$$

Thus to map $j_n \rightarrow$ we apply —[H]—

What about $\left(|0\rangle + e^{2\pi i\, 0.j_{n-1}, j_n}|1\rangle\right)$

j_{n-1} — H — $\rightarrow \left(|0\rangle + e^{2\pi i 0.j_{n-1}} |1\rangle \right)$

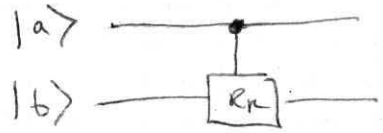
Action of R_k on basis states

$$R_k \equiv \begin{bmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^k} \end{bmatrix}$$

$|0\rangle \rightarrow |0\rangle$

$|1\rangle \rightarrow e^{2\pi i/2^k} |1\rangle$

Controlled-R_k — almost what we want



a	b	
0	0	0 0
0	1	0 1
1	0	1 0
1	1	1 $e^{2\pi i/2^k}$ |1⟩

if $a = 1$ apply R_k

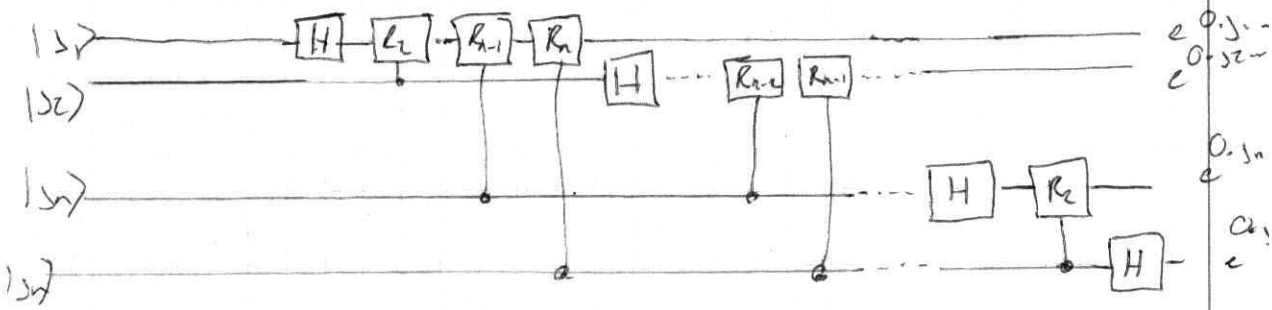
$\rightarrow |0\rangle \rightarrow |0\rangle$

$|1\rangle \rightarrow e^{2\pi i a/2^k} |1\rangle$

j_{n-1} — H — $\rightarrow \left(|0\rangle + e^{2\pi i 0.j_{n-1}} |1\rangle \right)$ — R_k — $\left(|0\rangle + e^{2\pi i 0.j_n j_{n-1}} |1\rangle \right)$ ✓

(j_n controls R_k)

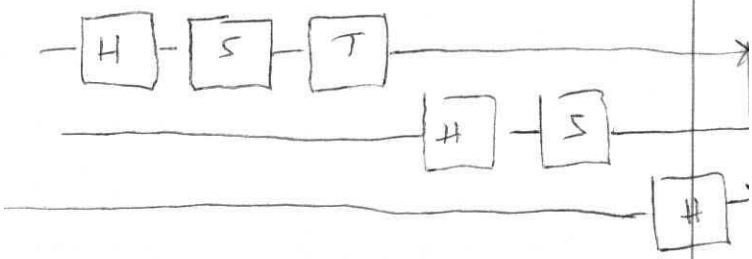
QFT circuit — $n(n+1)/2$ gates



(E) Three qubit QFT Box 5.1 NLC

$e^{\pi i/2} = i$ $R_2 = S$

$e^{\pi i/4}$ $R_3 = T$



4:20 V Phase Est.

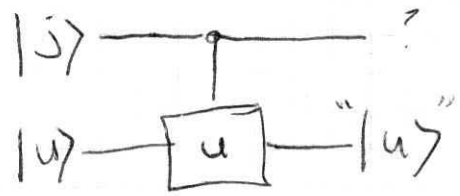
Given a unitary U, eigenvector $|u\rangle$

$$U|u\rangle = e^{2\pi i \varphi}|u\rangle$$

The goal of phase est is to estimate φ

Assume $\exists$ a black box performing U, register in $|u\rangle$

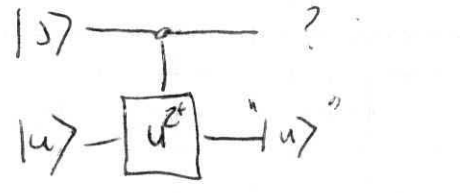
(A) Consider controlled-U acting on an eigenstate



$|0\rangle|u\rangle \to |0\rangle|u\rangle$

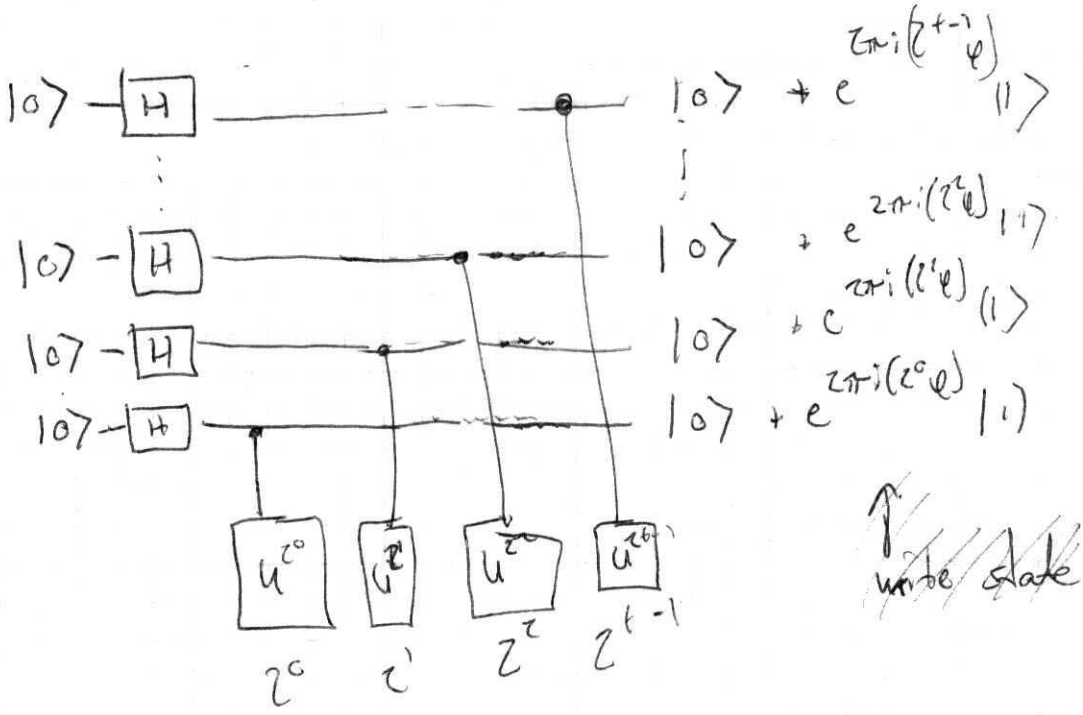
$|1\rangle|u\rangle \to |1\rangle|u\rangle \cdot e^{2\pi i \varphi}$

Eigenvalue has appeared, but how can we get more information?



$|0\rangle|u\rangle \to |0\rangle|u\rangle$

$|1\rangle|u\rangle \to e^{2\pi i \varphi 2^t}|1\rangle|u\rangle$



(B) How is this useful?

Suppose φ can be written exactly in t bits

$$0.\varphi_1\varphi_2\varphi_3\ldots\varphi_t$$

Then state is

$$\left(|0\rangle + e^{2\pi i(\ell^{t-1}\varphi)}|1\rangle\right) \otimes \left(|0\rangle + e^{2\pi i(\ell^0\varphi)}|1\rangle\right)$$

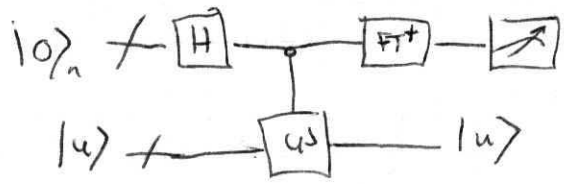
$$\downarrow$$

$$\frac{\left(|0\rangle + e^{2\pi i 0.\varphi_t}|1\rangle\right)\left(|0\rangle + e^{2\pi i 0.\varphi_{t-1}\varphi_t}|1\rangle\right)\cdots\left(|0\rangle + e^{2\pi i 0.\varphi_1\cdots\varphi_t}|1\rangle\right)}{2^{n/2}}$$

This looks like QFT! apply inverse QFT $\longrightarrow$

get basis state $|\varphi_1\ldots\varphi_t\rangle$ with probability $\underline{1}$.

Measure in computational basis $\longrightarrow \varphi$



This works even if φ is not exact, instead producing accuracy to

$$t - \left\lceil \log\left(2 + \frac{1}{2\epsilon}\right) \right\rceil \text{ bits}$$

with probability $1-\epsilon$

Let $|\tilde{\varphi_u}\rangle$ be an approx (proof ~~s.t.~~ in the book

---

(C) QPEst

init $|0\rangle_n |u\rangle$

$H \rightarrow \frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} |j\rangle|u\rangle$ sup

$\rightarrow \frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} |j\rangle U^j|u\rangle$ apply c-Black Box

$= \frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} e^{2\pi i j \varphi_u} |j\rangle|u\rangle$ res

$\rightarrow |\tilde{\varphi}_u\rangle|u\rangle$ $FT^\dagger$

$\rightarrow \tilde{\varphi}_u$

Quantum Order finding

(C) Need) black box $U'_{x,N}$ which performs

$$|j\rangle|k\rangle \to |j\rangle|x^j k \bmod N\rangle$$

$t = 2L+1$ qubits to get 's/r'

L qubits $\to |1\rangle$

1) $|0\rangle_t |1\rangle_L$

2) $\to \frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} |j\rangle|1\rangle$ — create superposition — $\boxed{H}$

3) $\to \frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} |j\rangle|x^j \bmod N\rangle$ — apply U', recall $U' \to U^{2^t}$

$$\approx \frac{1}{\sqrt{r2^t}} \sum_{s=0}^{r-1} \sum_{j=0}^{2^t-1} e^{2\pi i s j/r} |j\rangle|u_s\rangle$$

4. $\to \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |\widetilde{s/r}\rangle|u_s\rangle$ — $FT^\dagger$

5 $\to \widetilde{s/r}$

6 $\to r$ (Continued fractions alg)

Caveats

(1) 1) Small Mod exp circuit

2) computer $|u_s\rangle$ requires knowing r !!

Notice

$$\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |u_s\rangle = |1\rangle$$

Bugs:

1. ~~bad estimate to s/r~~ ?

what if $\gcd(s, r) \neq 1$?

then we have a factor of r, not r

a → i. algorithm is random,

repeat it.

b →

use $x^{r'} \equiv x^{r'} \pmod N$

then the order of $x^{r'}$ is (r/r')

$$x^{r'(r/r')} \equiv x^{r} \pmod{(N)} \equiv 1 \pmod N$$

c. ~~Do Phase Est → $r's'$, $r''s''$~~