The Quantum Fourier Transform

Classical Algorithm:

Prime factorization of n-bit integer requires

$e^{(\Theta(n^{\frac{1}{3}}\log^{\frac{2}{3}} n))}$ operations

using number field sieve.

Quantum Algorithm:

requires

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

exponentially faster.

... any more problems?

Quantum Fourier Transform (QFT),

is key ingredient for factoring algorithm.

.... but...

QFT does not speed up classical task of computing Fourier transforms of classical data.

QFT is also used for...

phase estimation
- eigenvalue approximation for unitaries

order-finding problem

counting solutions to a search problem
- combined with quantum search

hidden subgroup problem
- including discrete log problem.

Discrete Fourier Transform (DFT):

$(y_0, y_1, \ldots y_{N-1})$
$=$
$DFT(x_0, x_1, \ldots x_{N-1})$

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

Quantum Fourier Transform (QFT):

.... the same... but different notation.

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

Equivalently, $\sum_{j=0}^{N-1} x_j |j\rangle \rightarrow \sum_{k=0}^{N-1} y_k |k\rangle$, where $y = DFT(x)$.

The DFT is a unitary transform

$$\begin{pmatrix} y_0 \\ y_1 \\ \vdots \\ y_{N-1} \end{pmatrix} = \frac{1}{\sqrt{N}} \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \alpha & \alpha^2 & \cdots & \alpha^{N-1} \\ 1 & \alpha^2 & \alpha^4 & \cdots & \alpha^{N-2} \\ \vdots & & & & \\ 1 & \alpha^{N-1} & \alpha^{N-2} & \cdots & \alpha \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \\ \vdots \\ x_{N-1} \end{bmatrix},$$

where $\alpha = e^{2\pi i/N}$.

e.g.

$$QFT\left(|00\ldots0\rangle\right) = \frac{1}{\sqrt{N}} \sum_j |j\rangle,$$

$$\frac{1}{\sqrt{N}} \begin{bmatrix} 1 \\ 1 \\ \vdots \\ \vdots \\ 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \alpha & \alpha^2 & \cdots & \alpha^{N-1} \\ 1 & \alpha^2 & \alpha^4 & \cdots & \alpha^{N-2} \\ \vdots & & & & \vdots \\ \vdots & & & & \vdots \\ 1 & \alpha^{N-1} & \alpha^{N-2} & \cdots & \alpha \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ \vdots \\ 0 \end{bmatrix}$$

QFT - another definition

Let $N = 2^n$.

Write the state $|j\rangle$ using $j = \sum_{k=1}^{n} j_k 2^{n-k}$.

Let $0.j_l j_{l+1} \cdots j_m$ represent the binary fraction, $j_l/2 + j_{l+1}/4 + \cdots + j_m/2^{m-l+1}$.

Then, QFT is:

product representation

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

Another Way of Saying the Same Thing

$$\begin{bmatrix} y_0 \\ y_1 \\ y_2 \\ \vdots \\ y_{2^n-1} \end{bmatrix} = 2^{-n/2} \begin{bmatrix} (1,1) \otimes (1,1) \otimes \cdots \otimes (1,1) \\ (1,\alpha) \otimes (1,\alpha^2) \otimes \cdots \otimes (1,\alpha^{2^{n-1}}) \\ (1,\alpha^2) \otimes (1,\alpha^4) \otimes \cdots \otimes (1,\alpha^{2^n-2}) \\ (1,\alpha^3) \otimes (1,\alpha^6) \otimes \cdots \otimes (1,\alpha^{2^n-1}) \\ \vdots \\ (1,\alpha^{2^n-1}) \otimes (1,\alpha^{2^n-2}) \otimes \cdots \otimes (1,\alpha^{2^{n-1}}) \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ \vdots \\ x_{2^n-1} \end{bmatrix},$$

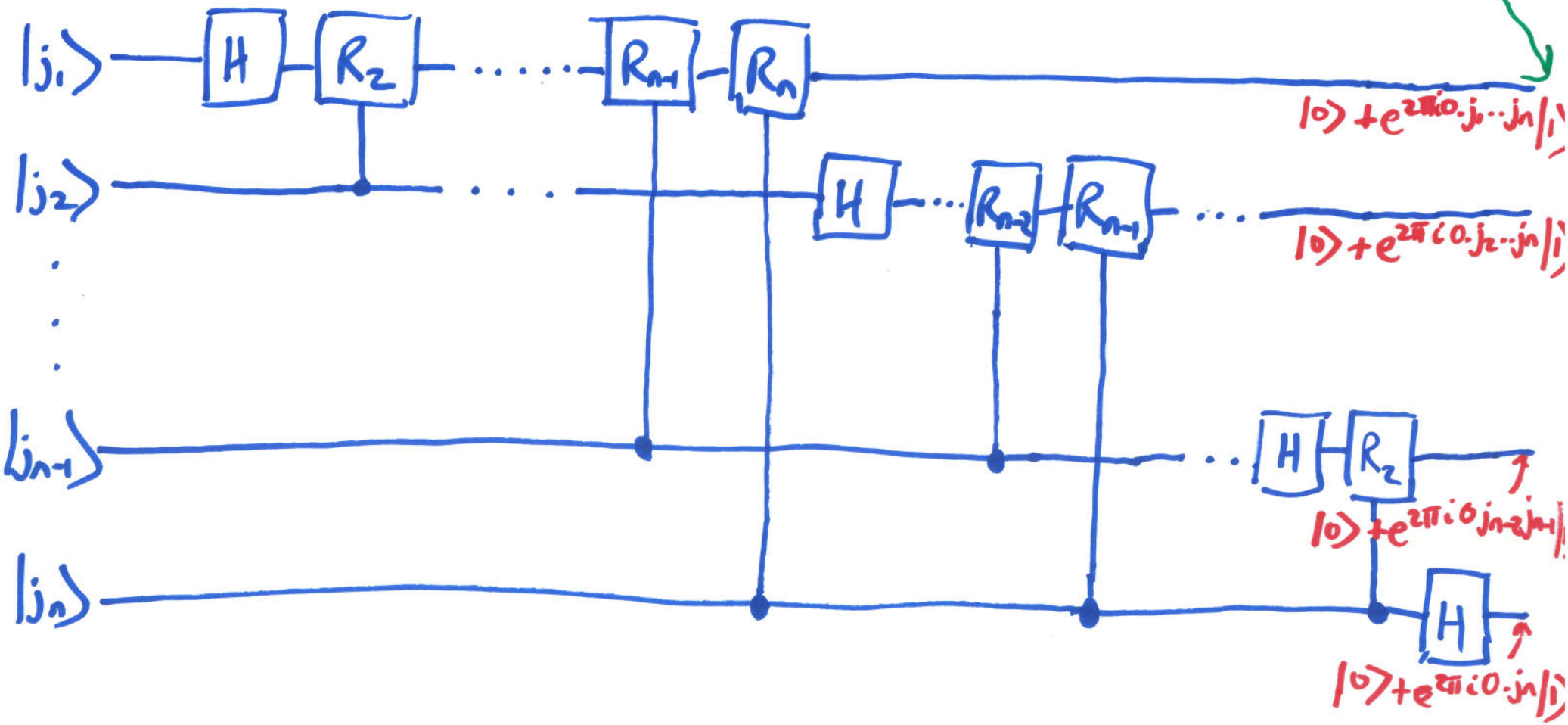
where $\alpha^{2^n} = 1$.

QFT Circuit

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

swap gates required to reverse order of qubits

QFT:



Explanation of QFT Circuit

Input: $|j_1 \cdots j_n\rangle$.

Apply H to first qubit:

$$\rightarrow \frac{1}{2^{\frac{1}{2}}}\left(|0\rangle + e^{2\pi i 0.j_1}|1\rangle\right)|j_2 \cdots j_n\rangle$$

Apply controlled-R_2:

$$\rightarrow \frac{1}{2^{\frac{1}{2}}}\left(|0\rangle + e^{2\pi i 0.j_1 j_2}|1\rangle\right)|j_2 \cdots j_n\rangle$$

Apply controlled-$R_3, \ldots R_n$:

$$\rightarrow \frac{1}{2^{\frac{1}{2}}}\left(|0\rangle + e^{2\pi i 0.j_1 j_2 \cdots j_n}|1\rangle\right)|j_2 \cdots j_n\rangle$$

Apply H, then controlled-$R_2, \ldots R_{n-1}$:

$$\rightarrow \frac{1}{2^{\frac{1}{2}}}\left(|0\rangle + e^{2\pi i 0.j_1 j_2 \cdots j_n}|1\rangle\right)\left(|0\rangle + e^{2\pi i 0.j_2 \cdots j_n}|1\rangle\right)$$
$$|j_3 \cdots j_n\rangle$$

$\ldots$ etc $\ldots$

How Many Gates?

$\frac{n(n+1)}{2}$ gates plus $n/2$ swaps

... each swap requires three C-NOT gates.

$\Rightarrow$

$\Theta(n^2)$ algorithm for QFT.

QFT: $\tilde{\Theta}(n^2)$ gates.

In Contrast...

Classical Fast Fourier Transform (FFT)

requires,

$\tilde{\Theta}(n2^n)$ gates

... exponentially more operations.

... unfortunately, quantum amplitudes cannot be accessed at input or output.

Complementary "Sequences"

Let $(x_0, x_1, \ldots x_{2^n-1})$ be a Golay sequence.

It can be shown that, for,

$$y = \left(\bigotimes_{j=0}^{n-1} U_j \right) x, \quad \text{then } |y_k|^2 \leq 2^{1-n}, \ \forall k \quad (1)$$

where $\alpha_j = e^{2\pi i / t_j}$.

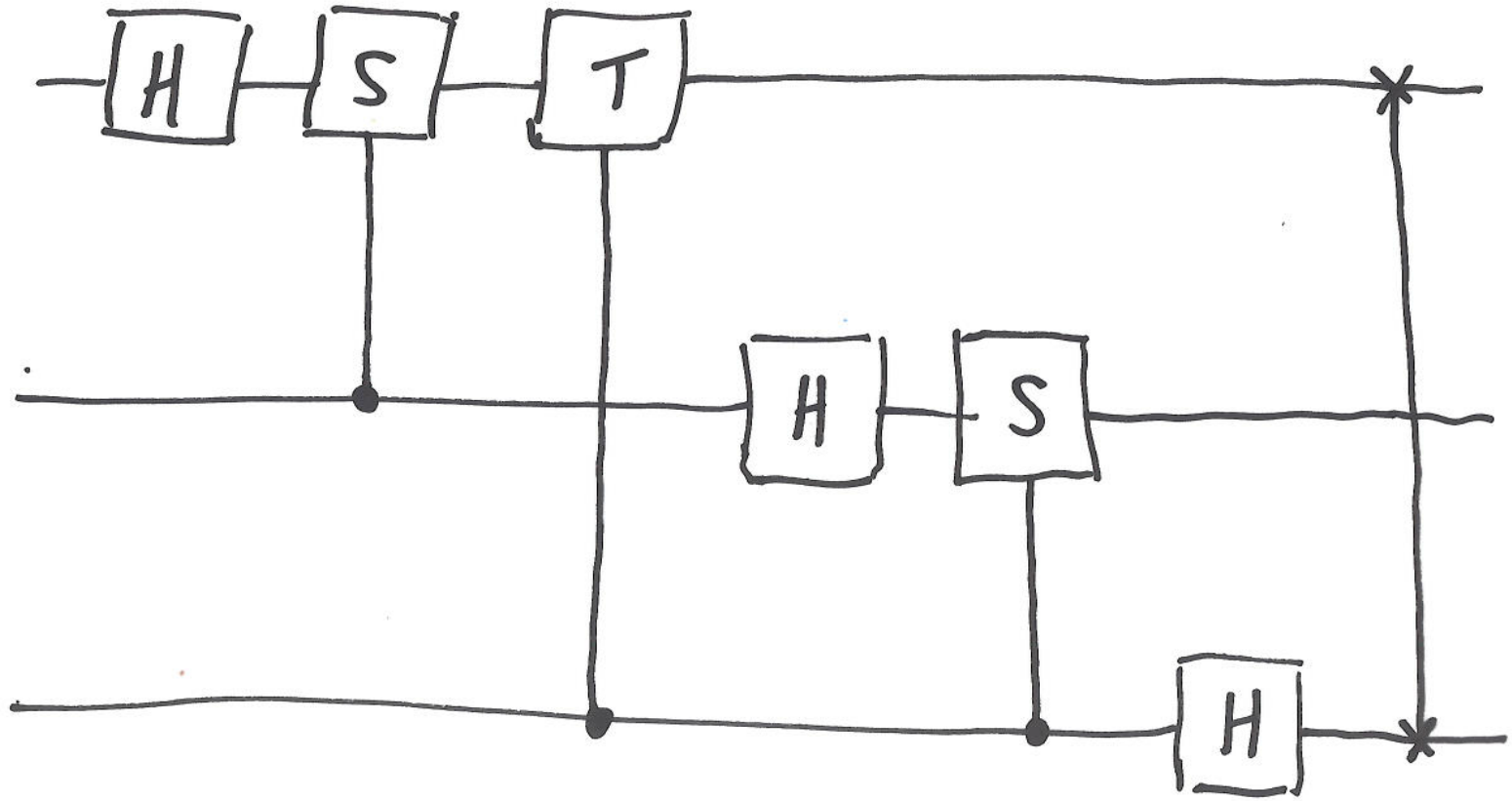
iff $U_j = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & \alpha_j \\ 1 & -\alpha_j \end{bmatrix}, \ \forall j$.

But, previously, the bound was only known wrt 2^n-point DFT.

It is easy to show that (1) implies bound wrt QFT.

... but (1) is a much stronger property.

Three Qubit QFT



Approximate QFT

Circuit requires gates of exponential precision.

... so approximate controlled-R_k gates...

Let U be the exact QFT

Let V be approximate QFT

with controlled-R_k gates to precision $\Delta = \frac{1}{p(n)}$.

Then, $E(U,V) = \max_{|\psi\rangle} \|(U-V)|\psi\rangle\|$ scales as $\Theta(n^2/p(n))$.

Phase Estimation

Problem: Let unitary U have eigenvector $|u\rangle$ with eigenvalue $e^{2\pi i \varphi}$.

φ is unknown....

...estimate φ...

It is assumed that black boxes (oracles) prepare $|u\rangle$ and perform U^{2^j}.

Quantum Phase Estimation

First register : t qubits in state $|0\rangle$.

Second register : state $|u\rangle$.

First Stage : Apply circuit on registers to obtain

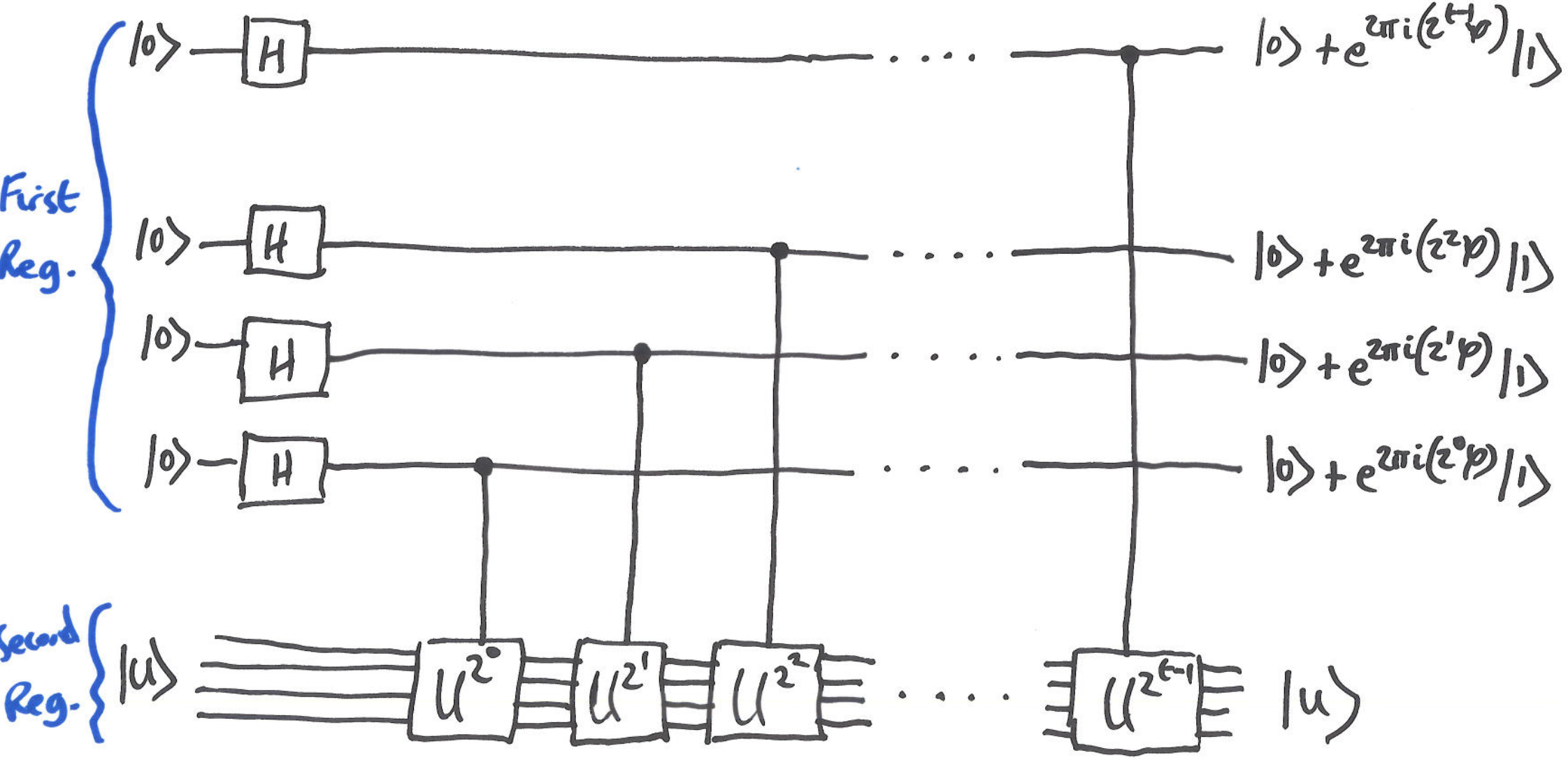
First register: $\frac{1}{2^{t/2}}\left(|0\rangle + e^{2\pi i 2^{t-1}\varphi}|1\rangle\right)\left(|0\rangle + e^{2\pi i 2^{t-2}\varphi}|1\rangle\right)\ldots$

$\ldots\left(|0\rangle + e^{2\pi i 2^{0}\varphi}|1\rangle\right)$

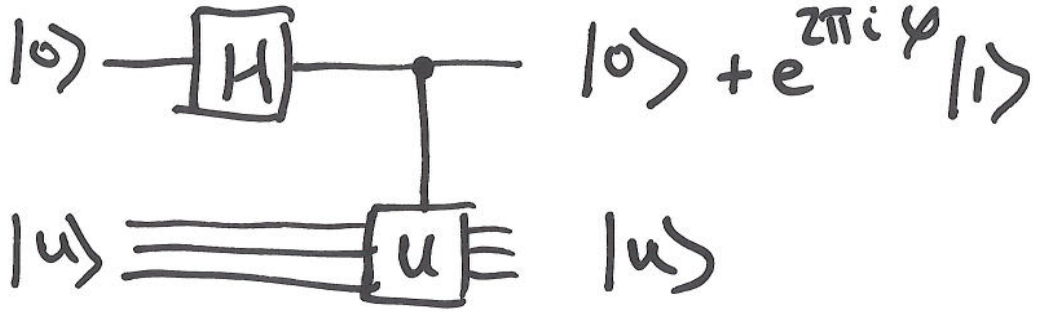
$= \frac{1}{2^{t/2}}\sum_{k=0}^{2^t-1} e^{2\pi i \varphi k}|k\rangle.$

Second register: unchanged.

First Stage of Phase Estimation



Why Does this Work?



We know that $U|u\rangle = e^{2\pi i\varphi}|u\rangle$,

...so...

$$(1,0)\otimes|u\rangle \rightarrow \tfrac{1}{\sqrt{2}}(1,1)\otimes|u\rangle \rightarrow \tfrac{1}{\sqrt{2}}(1, e^{2\pi i\varphi})\otimes|u\rangle$$

... using matrices...

$$\begin{bmatrix}|u\rangle\\ 0\end{bmatrix} \rightarrow \tfrac{1}{\sqrt{2}}\begin{bmatrix}|u\rangle\\ |u\rangle\end{bmatrix} \rightarrow \tfrac{1}{\sqrt{2}}\begin{bmatrix}I & 0\\ 0 & U\end{bmatrix}\begin{bmatrix}|u\rangle\\ |u\rangle\end{bmatrix} = \begin{bmatrix}|u\rangle\\ e^{2\pi i\varphi}|u\rangle\end{bmatrix}$$

Second Stage

Apply inverse QFT to first register...

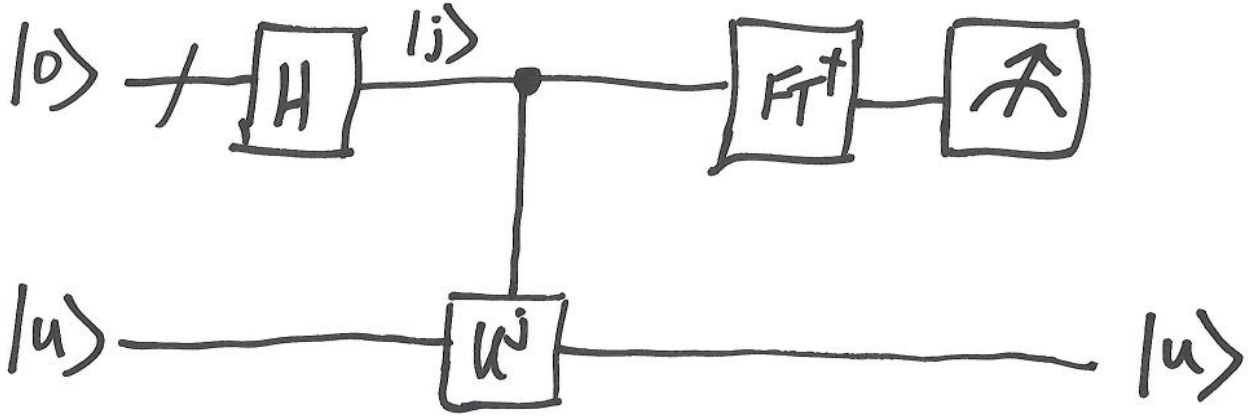
...just reverse QFT circuit...

Third Stage

Measure first register in computational basis

to obtain estimate of φ.

Phase Estimation Procedure



Measures ϕ to within $t - \lceil \log(2 + \frac{1}{2\varepsilon}) \rceil$ bits,

with success probability $\geq 1 - \varepsilon$.

Why?

Suppose $\varphi = 0.\varphi_1 \cdots \varphi_t$.

Then the result of first stage is,

$$\frac{1}{2^{t/2}}\left(|0\rangle + e^{2\pi i 0.\varphi_t}|1\rangle\right)\left(|0\rangle + e^{2\pi i 0.\varphi_{t-1}\varphi_t}|1\rangle\right)\cdots\left(|0\rangle + e^{2\pi i 0.\varphi_1\varphi_2\cdots\varphi_t}|1\rangle\right)$$

...

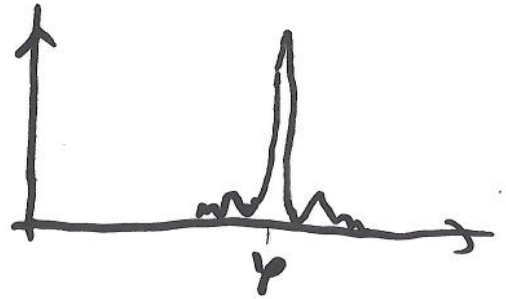
then inverse QFT gives,

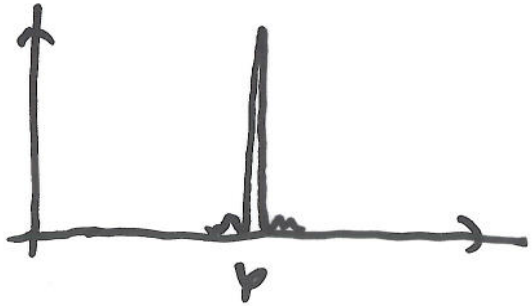
$$|\varphi_1 \cdots \varphi_t\rangle,$$

which is exactly φ.

Another Explanation

Phase estimation : $|u\rangle$ → 

Inverse QFT :  → 

Measure : 

→ $\approx \varphi$

Accuracy?

Let $0 \leq b \leq 2^t - 1$,

where,

$b/2^t = 0.b_1 \ldots b_t$ is the closest t-bit approximation to b, less than b.

Then,

difference $\delta \equiv \varphi - b/2^t$ satisfies,

$$0 \leq \delta \leq 2^{-t}$$

... show that measurement produces result close to b, with high probability.

Result of IQFT is,

$$\frac{1}{2^t} \sum_{k,l=0}^{2^t-1} e^{\frac{-2\pi i k l}{2^t}} e^{2\pi i \beta k} |l\rangle .$$

Let α_l be amplitude of $|(b+l).\ \mathrm{mod}\ 2^t\rangle$.

Then,

$$\alpha_l = \frac{1}{2^t} \sum_{k=0}^{2^t-1} \left(e^{2\pi i (\varphi - (b+l)/2^t)} \right)^k$$

$$\Rightarrow \quad \alpha_l = \frac{1}{2^t} \left(\frac{1 - e^{2\pi i (2^t \varphi - (b+l))}}{1 - e^{2\pi i (\varphi - (b+l)/2^t)}} \right) = \frac{1}{2^t} \left(\frac{1 - e^{2\pi i (2^t \delta - l)}}{1 - e^{2\pi i (\delta - l/2^t)}} \right).$$

Remember: $\alpha_l = \frac{1}{2^t}\left(\frac{1-e^{2\pi i(2^t\delta - l)}}{1-e^{2\pi i(\delta - l/2^t)}}\right)$

We will bound the probability of measuring m, such that,

$$|m-b| > e.$$

$$p(|m-b|>e) = \sum_{-2^{t-1} < l \leq f(e+1)} |\alpha_l|^2 + \sum_{e+1 \leq l \leq 2^{t-1}} |\alpha_l|^2$$

But, $|1-e^{i\theta}| \leq 2$, so,

$$|\alpha_l| \leq \frac{2}{2^t |1-e^{2\pi i(\delta - l/2^t)}|}$$

It can be shown that,

$$|1-e^{i\theta}| \geq \frac{2|\theta|}{\pi} \quad \text{when } -\pi \leq \theta \leq \pi.$$

Remember: $|\alpha_\ell| \le \dfrac{2}{2^t \left|1 - e^{2\pi i(\delta - \ell/2^t)}\right|}$

$|1 - e^{i\theta}| \ge \dfrac{2|\theta|}{\pi}, \quad -\pi \le \theta \le \pi$

$-2^{t-1} < \ell \le 2^{t-1}$,

$p(|m-b| > e) = \sum_{-2^{t-1} < \ell \le -(e+1)} |\alpha_\ell|^2 + \sum_{e+1 \le \ell \le 2^{t-1}} |\alpha_\ell|^2$

therefore $-\pi \le 2\pi(\delta - \ell/2^t) \le \pi$

$\Rightarrow |\alpha_\ell| \le \dfrac{1}{2^{t+1}(\delta - \ell/2^t)}$

so,

$$p(|m-b| > e) \le \frac{1}{4}\left[\sum_{\ell=2^{t-1}+1}^{-(e+1)} \frac{1}{(1-2^t\delta)^2} + \sum_{\ell=e+1}^{2^{t-1}} \frac{1}{(1-2^t\delta)^2}\right]$$

... but $0 \le 2^t\delta \le 1$, .. so ...

$$p(|m-b| > e) \le \frac{1}{4}\left[\sum_{\ell=2^{t-1}+1}^{-(e+1)} \frac{1}{\ell^2} + \sum_{\ell=e+1}^{2^{t-1}} \frac{1}{(-1)^2}\right] \le \frac{1}{2}\sum_{\ell=e}^{2^{t-1}-1} \frac{1}{\ell^2} \le \int_{e-1}^{2^{t-1}-1} d\left(\frac{1}{\ell^2}\right) = \frac{1}{2(e-1)}.$$

Remember: $p(|m-b|>e) \leq \frac{1}{2(e-1)}$.

To approximate φ to accuracy 2^{-n},

we choose $e = 2^{t-n} - 1$.

Using $t = n+p$ qubits,

$$p(|m-b| \leq e) \geq 1 - \frac{1}{2(2^p-2)}.$$

... so...

to obtain φ accurate to n bits with $pr \geq 1-\varepsilon$,

we choose,

$$t = n + \left\lceil \log\left(2 + \frac{1}{2\varepsilon}\right) \right\rceil.$$

Replace Eigenstate with General State, $|\psi\rangle$

Phase estimation algorithm requires preparation of eigenstate $|u\rangle$, of U.

What if we prepare $|\psi\rangle$ instead of $|u\rangle$.

$|\psi\rangle$ can always be written,

$$|\psi\rangle = \sum_u c_u |u\rangle,$$ using the eigenbasis of U.

Phase estimation gives,

$$\simeq \sum_u c_u |\tilde{\varphi}_u\rangle |u\rangle,$$

Measure gives $\tilde{\varphi}_u$ with probability $|c_u|^2$...

... so phase estimation of random eigenstate achieved.

Summary of Phase Estimation

Inputs: Black-box for U^j, eigenstate $|u\rangle$ of U

$t = n + \lceil \log(2 + \frac{1}{2\varepsilon}) \rceil$ qubits initialized to $|0\rangle$.

Outputs: n-bit $\tilde{\varphi}_u$.

Runtime: $O(t^2)$ + one call to controlled-U^j.

Success Probability: $1 - \varepsilon$.

Procedure:

1. $|0\rangle|u\rangle$ — init. state
2. $\to \frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} |j\rangle|u\rangle$ — superposition
3. $\to \frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} |j\rangle U^j|u\rangle = \frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} e^{2\pi i j \varphi_u} |j\rangle|u\rangle$ — black box
4. $\to |\tilde{\varphi}_u\rangle|u\rangle$ — IQFT
5. $\to |\tilde{\varphi}_u\rangle$. — measure.

Order-Finding

order of $x \mod N$,

is,

least +ve integer, r, such that

$$x^r = 1 \mod N.$$

Problem:

Given x and N,

find r.

Order-Finding believed to be hard

"... no classical algorithm known to solve problem using resources polynomial in

$O(L)$ bits,

where $L = \lceil \log(N) \rceil$.

Quantum Algorithm for Order-Finding

Phase estimation algorithm applied to U, where

$$U|y\rangle = |xy \bmod N\rangle, \quad y \in \{0,1\}^L.$$

(assume U acts non-trivially only when $0 \leq y < N$).

Eigenstates of U are,

$$|u_s\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{\frac{-2\pi i s k}{r}} |x^k \bmod N\rangle, \quad 0 \leq s < r.$$

Why? because,

$$U|u_s\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{\frac{-2\pi i s k}{r}} |x^{k+1} \bmod N\rangle = e^{\frac{2\pi i s}{r}} |u_s\rangle.$$

Remember: eigenstates of U are,

$$|u_s\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{\frac{-2\pi i s k}{r}} |x^k \bmod N\rangle$$

eigenvalues are,

$$e^{\frac{2\pi i s}{r}}.$$

Phase Estimation obtains,

$$e^{2\pi i s/r}$$ with high accuracy,

from which r can be obtained.

Requirements for Phase Estimation

1. Efficient implementation of controlled-U^{2^j} gate.

2. Efficient preparation of $|u_s\rangle$ with a non-trivial eigenvalue, or at least a superposition of eigenstates

Use modular exponentiation to satisfy first requirement.
...requires $O(L^3)$ gates.

Second requirement: preparing $|u_s\rangle$ requires that we know r,
so not possible..

Preparing $|u_s\rangle$

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

...so...

use $t = 2L+1 + \lceil \log(2 + \frac{1}{2\varepsilon}) \rceil$ qubits

prepare second register in $|1\rangle$

... for each $0 \leq s < r$,

measure $\varphi \approx s/r$ accurate to $2L+1$ bits

with $p_r = 1 - \frac{\varepsilon}{r}$.

Observe:

Remember: $|u_s\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{\frac{-2\pi i s k}{r}} |x^k \bmod N\rangle$

Before we used,

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

More generally,

$$\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} e^{2\pi i s k/r} |u_s\rangle = |x^k \bmod N\rangle .$$

Continued Fraction Expansion

We have obtained $\varphi \approx s/r$, via phase estimation.

How does one then obtain r?

We know φ up to $2L+1$ bits accuracy

We know that φ is a rational number,

...So...

computing the nearest fraction to φ

might give us r.

Continued Fractions Algorithm

Suppose s/r is rational, where

$$\left|\frac{s}{r} - \varphi\right| \leq \frac{1}{2r^2}.$$

Then s/r is a convergent for the continued fraction of φ,

and can therefore be computed in $O(L^3)$ operations.

Remember: Condition

$$\left|\frac{s}{r} - \varphi\right| \leq \frac{1}{2r^2}$$

Since φ approximates s/r to $2L+1$ bits,

then,

$$\left|s/r - \varphi\right| \leq 2^{-2L-1} \leq \frac{1}{2r^2}, \text{ as } r \leq N \leq 2^L.$$

.... so s/r **is** a convergent

of the continued fraction for φ.

To summarise:

Given φ, the continued fractions algorithm efficiently produces s' and r' with no common factor, such that,

$$s'/r' = s/r.$$

Then compute (classically) $x^{r'} \bmod N$, to see if $r' = r$.

Two Possibilities for Failure

1. Phase estimation produces bad estimate for s/r,

&

with $pr \leq \varepsilon$.

ε can be made small at negligible cost to circuit size.

2. If s and r share a non-trivial factor, then r' is a factor of r.

... three ways round this problem.

Problem when $\gcd(r,s) > 1$

1. For random $0 \leq s < r$, $\Pr(\gcd(r,s)=1)$ is very high

   ... repeating algorithm $2\log(N)$ will ensure, with high probability that $\gcd(r,s)=1$.

2. If $r' \neq r$, then $r' | r$ (unless $s=0$).

   Order of $a' = a^{r'} \bmod N$ is r/r'.

   Repeat algorithm to compute order of a'.

   Then order of $a = r = r' \times r/r'$.

   If $r'' \neq r/r'$, then $r'' | r/r'$

   Order of $a'' = (a')^{r''} \bmod N$ is $(r/r')/r''$

   ... and so on.

at most $\log(r) = O(L)$ iterations required.

Problem when $\gcd(r,s) > 1$ - third method

3. Repeat phase-estimation/continued-fractions twice

Obtain, r_1', s_1' and r_2', s_2'.

If $\gcd(s_1', s_2') = 1$, then $r = \text{lcm}(r_1', r_2')$.

$$\Pr(\gcd(s_1', s_2') = 1) = 1 - \sum_q p(q|s_1') p(q|s_2'),$$

where sum is over primes.

.. but ..

$p(q|s_1') \leq p(q|s_1) \leq \frac{1}{q}$. Similarly, $p(q|s_2') \leq \frac{1}{q}$

$$\Rightarrow \Pr(\gcd(s_1', s_2') = 1) \geq 1 - \sum_q \frac{1}{q^2}.$$

. . . an upper bound is easily derived, so. $1 - \frac{\varepsilon}{2}\frac{1}{q^2}$??

$$\Pr(\gcd(s_1', s_2') = 1) \geq \frac{1}{4}$$

. . . . so probability of obtaining the correct r is at least $\frac{1}{4}$.

Resources for Order-Finding?

Hadamard transform: $O(L)$ gates

IQFT: $O(L^2)$ gates

Modular Exponentiation: $O(L^3)$ gates

Continued Fractions: $O(L^3)$ gates

Repeat a constant number of times: $O(L^3)$ gates

(third method)

Total: $O(L^3)$ gates.

Quantum Order-Finding

Inputs: Black box $U_{x,N} : |j\rangle|k\rangle \to |j\rangle|x^j k \bmod N\rangle$

$t = 2L + 1 + \lceil \log(2 + \frac{1}{2\varepsilon}) \rceil$ qubits set to $|0\rangle$

L qubits set to $|1\rangle$

Outputs: $r > 0$, such that $x^r = 1 \pmod N$ ... r a minimum..

Runtime: $O(L^3)$ steps. Succeeds with $pr = O(1)$.

Procedure:

1. $|0\rangle|1\rangle$ — init.
2. $\to \frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} |j\rangle|1\rangle$ — superposition
3. $\to \frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} |j\rangle|x^j \bmod N\rangle \propto \frac{1}{r\sqrt{2^t}} \sum_{s=0}^{r-1} \sum_{j=0}^{2^t-1} e^{2\pi i s j / r} |j\rangle|u_s\rangle$ — apply $U_{x,N}$
4. $\to \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |s/r\rangle|u_s\rangle$ — IQFT
5. $\to s/r$ — measure
6. $\to r$ — continued fraction.