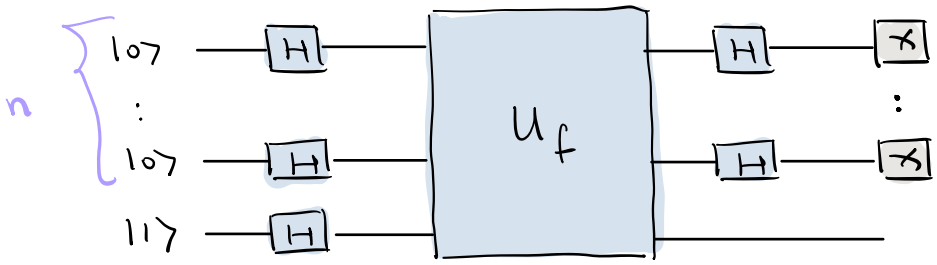
QUANTUM ALGORITHMS

Deutsch - Jozsa algorithm

Given $f: \mathbb{B}^n \to \mathbb{B}$ determine whether

1) f is constant, or → $|f(\mathbb{B}^n)| = 1$.
2) f is balanced. $|f^{-1}(0)| = |f^{-1}(1)|$.

The circuit



where $U_f : (\mathbb{C}^2)^{\otimes(n+1)} \to (\mathbb{C}^2)^{\otimes(n+1)}$ defined by

$$U_f |x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle \qquad x \in \mathbb{B}^n,\ y \in \mathbb{B}.$$

Notation: It is sometimes more convenient to use the natural number corresponding to a bit string:

$$\mathbb{B}^n \hookrightarrow \mathbb{N}$$

$$\langle x \rangle = b_1 \cdots b_n \longmapsto x = \sum_{i=1}^{n} b_i 2^{n-i}.$$

omit $\langle - \rangle$

Lem: $$H^{\otimes n} |x\rangle = \frac{1}{2^{n/2}} \sum_{x'=0}^{2^n-1} (-1)^{x \cdot x'} |x'\rangle$$

$x \cdot x' = \sum_i b_i b'_i$

Proof: Let $\langle x \rangle = b_1 \dots b_n$.

We will do induction on n.

If $n = 1$ then

$$H|b_1\rangle = \frac{1}{2^{1/2}} \sum_{x'=0}^{1} (-1)^{b_1 \cdot x'} |x'\rangle .$$

Let y be such that $\langle y \rangle = b_2 \dots b_n$.

$$H^{\otimes n} |b_1\rangle|y\rangle = H|b_1\rangle H^{\otimes (n-1)} |y\rangle$$

$$= \frac{|0\rangle + (-1)^{b_1}|1\rangle}{\sqrt{2}} \underbrace{\frac{1}{2^{(n-1)/2}} \sum_{x'=0}^{2^{n-1}-1} (-1)^{y \cdot x'} |x'\rangle}_{\text{by induction}}$$

$$= \frac{1}{2^{n/2}} \left(\sum_{x'=0}^{2^{n-1}-1} (-1)^{y \cdot x'} |0\rangle|x'\rangle + \sum_{x'=0}^{2^{n-1}-1} (-1)^{y \cdot x' + b_1} |1\rangle|x'\rangle \right)$$

$$= \frac{1}{2^{n/2}} \sum_{x'=0}^{2^n-1} (-1)^{x \cdot x'} |x'\rangle$$

□

We compute the circuit:

$$(H^{\otimes n} \otimes \mathbb{1})\, U_f\, H^{\otimes (n+1)} |0\cdots0\rangle|1\rangle$$

$$= (H^{\otimes n} \otimes \mathbb{1})\, U_f\, \frac{1}{\sqrt{2}^n} \sum_{x=0}^{2^n-1} |x\rangle \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

$$= \frac{1}{\sqrt{2}^n} H^{\otimes n} \otimes \mathbb{1} \sum_x (-1)^{f(x)} |x\rangle \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

$$= \frac{1}{2^n} \sum_x \sum_y (-1)^{f(x)+x\cdot y} |y\rangle \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

$$= \sum_y \frac{1}{2^n} \sum_x (-1)^{f(x)+x\cdot y} |y\rangle \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

If f is constant:

$$(H^{\otimes n} \otimes \mathbb{1})\, U_f\, H^{\otimes (n+1)} |0\cdots0\rangle|1\rangle$$

$$= \sum_y (-1)^{f(x)} \underbrace{\frac{1}{2^n} \sum_x (-1)^{x\cdot y}}_{S_{y,0}} |y\rangle \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

Assume $y \neq 0$ i.e. $\exists i$ s.t. $y_i = 1$ $\Rightarrow$ $\frac{1}{2^n}\left(\sum_{x:\, x\cdot y=0} 1 - \sum_{x:\, x\cdot y=1} 1\right) = 0$

$x \longmapsto x_1 \cdots \neg x_i \cdots x_n$

$$= (-1)^{f(x)} |0\rangle \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

meaning first n-qubit:

$$p(0\cdots0) = 1.$$

2) f is balanced :

$$(H^{\otimes n} \otimes \mathbb{1})\, U_f\, H^{\otimes (n+1)} |0\cdots0\rangle|1\rangle$$

$$= \sum_y \underbrace{\frac{1}{2^n} \sum_x (-1)^{f(x)+x\cdot y}}_{\text{coefficient of } |0\rangle \text{ is}} |y\rangle \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

$$\frac{1}{2^n}\sum_x (-1)^{f(x)} = 0 \quad \text{since } f \text{ is balanced.}$$

meaning first n-qubit :

$$p(0\cdots0) = 0.$$

We solved the problem by a single evaluation of f via U_f.

Deterministic classical algorithm requires $2^{n-1}+1$ evaluations of f.

There exists a probabilistic classical algorithm which solves this problem with 2 evaluations of f with success probability $\geq 1/2$

↳ Choose two randomly chosen bit strings $x_1 \neq x_2$. Output

1) constant if $f(x_1) = f(x_2)$

2) balanced if $f(x_1) \neq f(x_2)$.

Simon's algorithm

Given $f : \mathbb{B}^n \to \mathbb{B}^n$ such that

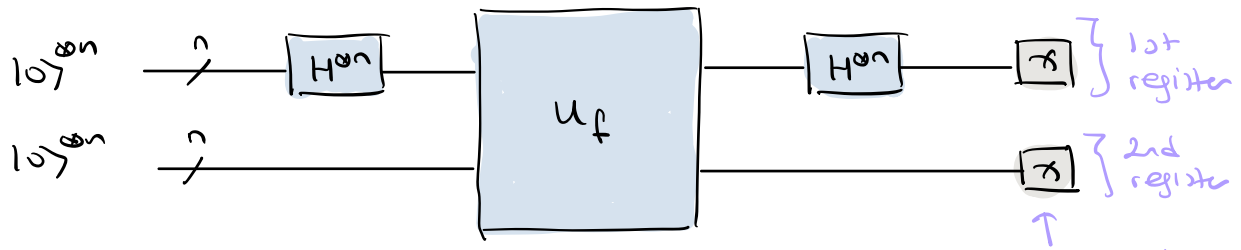
$$f(x) = f(y) \iff y = \begin{cases} x \\ x \oplus a \end{cases} \quad \text{or,}$$

for some fixed $a \in \mathbb{B}^n$, $a \neq 0 \ldots 0$,

determine a.

↳ called the period of f.

The circuit



We can give meaning to the principle of deferred measurement.

where $U_f |x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle$.

We compute

$$U_f \, H^{\otimes n} \otimes \mathbb{1}^{\otimes n} \, |0\rangle^{\otimes n} |0\rangle^{\otimes n}$$

$$= U_f \frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} |x\rangle |0\rangle^{\otimes n}$$

$$= \frac{1}{2^{n/2}} \sum_x |x\rangle |f(x)\rangle$$

Measure the second register:

If outcome is $f(x_0)$ then the post-measurement state is given by

$$\frac{1}{\sqrt{2}} \left(|x_0\rangle + |x_0 \oplus a\rangle \right) |f(x_0)\rangle$$

Then we have

$$H^{\otimes n} \otimes \mathbb{I}^{\otimes n} \frac{1}{\sqrt{2}} \left(|x_0\rangle + |x_0 \oplus a\rangle \right) |f(x_0)\rangle$$

$$= \frac{1}{\sqrt{2}^{n+1}} \sum_y \left((-1)^{x_0 \cdot y} + (-1)^{(x_0 \oplus a) \cdot y} \right) |y\rangle |f(x_0)\rangle$$

$$= \begin{cases} 0 & \text{if } a \cdot y = 1 \\ 2(-1)^{x_0 \cdot y} & \text{if } a \cdot y = 0. \end{cases}$$

$$= \frac{1}{\sqrt{2}^{n-1}} \sum_{y : a \cdot y = 0} (-1)^{x_0 \cdot y} |y\rangle |f(x_0)\rangle$$

Now measuring the first register

$$p(y) = \begin{cases} 0 & \text{if } a \cdot y = 1 \\ \frac{1}{2^{n-1}} & \text{if } a \cdot y = 0. \end{cases}$$

We run the algorithm $n-1$ times to obtain

$$S = \{ y_1, \cdots, y_{n-1} \}.$$

If S is linearly independent over $\mathbb{Z}_2$ then we can find a by solving

$$\begin{aligned} a \cdot y_1 &= 0 \\ &\vdots \\ a \cdot y_{n-1} &= 0. \end{aligned}$$

a is the unique non-zero solution.

Gaussian elimination is polynomial in n.

It suffices to do $O(n)$ queries. (HW).

The classical counterpart requires an exponential number of queries.

↳ $2^{n/2}$ for probabilistic.

$2^{n-1}+1$ for a deterministic algorithm.

Quantum Fourier Transform

The quantum Fourier transform is the unitary operator

$$F : \mathbb{C}^N \longrightarrow \mathbb{C}^N$$

defined by

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

where $\{|j\rangle\}_j$ is the canonical basis.

Notation: An integer $0 \le j < N$ will be represented by $j_1 j_2 \cdots j_n$ where $j_i \in \mathbb{B}$, that is

$$j = \sum_{\ell=1}^{n} j_\ell \, 2^{n-\ell}.$$

The expression $0.j_\ell j_{\ell+1} \cdots j_m$ will stand for

$$\frac{j_\ell}{2} + \cdots + \frac{j_m}{2^{m-\ell+1}} = \sum_{k=\ell}^{m} \frac{j_k}{2^{k-\ell+1}}$$

Let $N = 2^n$ for some $n \ge 1$.

Using this notation:

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

$$= \frac{1}{2^{n/2}} \sum_{k_1} \cdots \sum_{k_n} \underbrace{e^{2\pi i j \left(\sum_{\ell=1}^{n} k_\ell 2^{-\ell}\right)} |k_1\rangle \cdots |k_n\rangle}_{\bigotimes_{\ell=1}^{n} e^{2\pi i j k_\ell 2^{-\ell}} |k_\ell\rangle}$$

$$= \frac{1}{2^{n/2}} \bigotimes_{\ell=1}^{n} \left(\sum_{k_\ell=0}^{1} e^{2\pi i j \, c_\ell 2} \, |k_\ell\rangle \right)$$

$$= \frac{1}{2^{n/2}} \bigotimes_{\ell=1}^{n} \left(|0\rangle + e^{2\pi i j 2^{-\ell}} |1\rangle \right)$$

$$j 2^{-\ell} = \left(\sum_{i=1}^{n} j_i 2^{n-i} \right) 2^{-\ell}$$

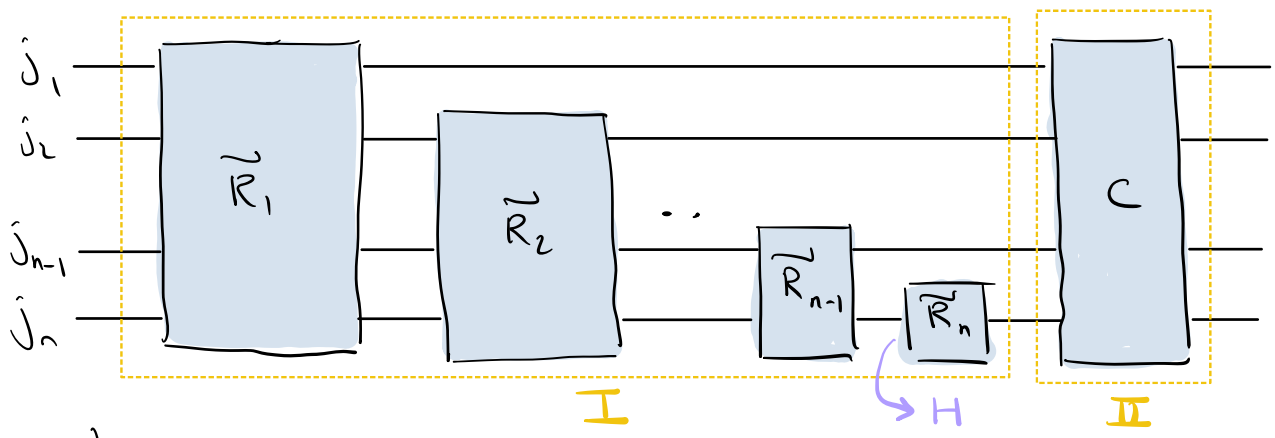
$$= \underbrace{j_1 2^{n-1-\ell} + \cdots + j_{n-\ell} 2^{0}}_{\text{applying } e^{2\pi i (-)} \text{ gives } 1} + \underbrace{j_{n-\ell+1} 2^{-1} + \cdots + j_n 2^{-\ell}}_{0 . j_{n-\ell+1} \cdots j_n}$$

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

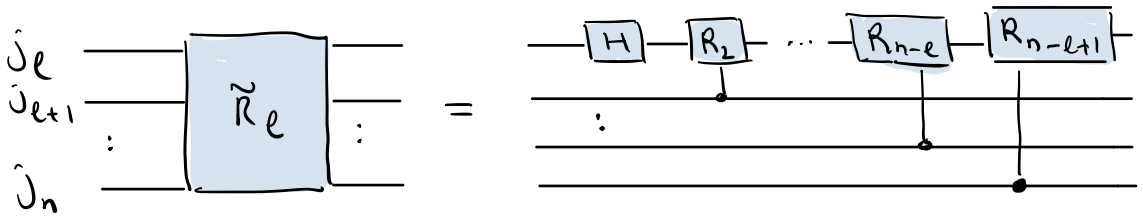
$$= \frac{\left(|0\rangle + e^{2\pi i \, 0 . j_n} |1\rangle\right)\left(|0\rangle + e^{2\pi i \, 0 . j_{n-1} j_n} |1\rangle\right) \cdots \left(|0\rangle + e^{2\pi i \, 0 . j_1 \cdots j_n} |1\rangle\right)}{2^{n/2}}$$

product representation of QFT.

Pr: $F: \mathbb{C}^{2^n} \longrightarrow \mathbb{C}^{2^n}$ can be implemented as the following circuit:

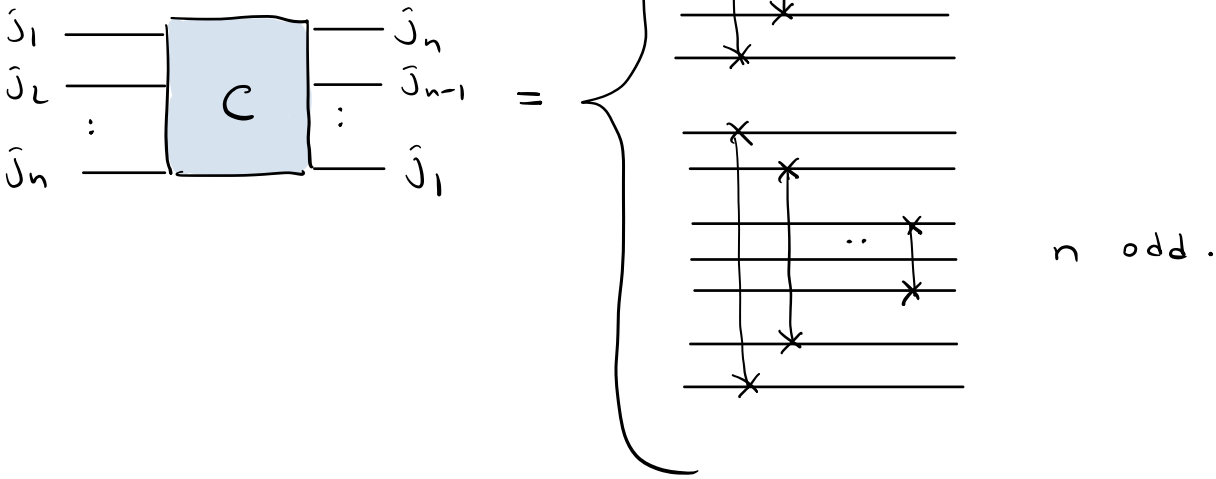


where



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

and



Proof: The result follows from computing $\tilde{R}_\ell$:

control target

$$C(R_{n-\ell+1})_{n,\ell} \cdots C(R_2)_{\ell+1,\ell} \; H_{(\ell)} \; |j_\ell\rangle |j_{\ell+1}\rangle \cdots |j_n\rangle$$

acting on ℓ-th qubit

$$= C(R_2)_{\ell+1,\ell} \; \frac{|0\rangle + (-1)^{j_\ell}|1\rangle}{\sqrt{2}} \; |j_{\ell+1}\rangle$$

$$= \frac{|0\rangle + (-1)^{j_\ell} e^{2\pi i j_{\ell+1}/2^2}|1\rangle}{\sqrt{2}} \; |j_{\ell+1}\rangle$$

$$= \frac{|0\rangle + e^{2\pi i \, 0.j_\ell j_{\ell+1}}|1\rangle}{\sqrt{2}} \; |j_{\ell+1}\rangle$$

$$= \frac{|0\rangle + e^{2\pi i 0.j_l j_{l+1} \cdots j_n}|1\rangle}{\sqrt{2}} |j_{l+1}\rangle \cdots |j_n\rangle. \quad \square$$

Cor: $F : \mathbb{C}^{2^n} \to \mathbb{C}^{2^n}$ can be implemented using $O(n^2)$ gates from $U(\mathbb{C}^2) \cup \{CNOT\}$.

Proof: Each $\tilde{R}_l$ uses 1 single qubit and $n-l$ controlled unitaries, each of which uses 1 CNOT and 4 single qubit unitaries. In total we need at most

$$n + \sum_{l=1}^{n-1} 5(n-l) + 3\left\lceil \frac{n}{2} \right\rceil = O(n^2) \text{ gates.}$$

- n: Hadamards
- $5(n-l)$: each $C(U)$ needs 1 CNOT $\times$ 4 single qubit
- $3\lceil \frac{n}{2} \rceil$: 3 CNOT for each SWAP

$$= 5 \sum_{l=0}^{n-1} l = 5 \frac{n(n-1)}{2} \quad \square$$

Note that Solovay–Kitaev implies that we need

$$O(n^2 \log^c(n^2/\epsilon)) \quad \text{HW}$$

i.e. polynomial number of gates from $\tilde{A}_q$.

Complexity of the discrete FT:

$$F\left(\sum_{j=0}^{2^n-1} \alpha_j |j\rangle\right) = \sum_k \underbrace{\frac{1}{\sqrt{N}} \sum_j \alpha_j e^{2\pi i jk/N}}_{P_k} |k\rangle$$

The set $\{\beta_1, \ldots, \beta_{2^n}\}$ is called the discrete FT of $\{\alpha_1, \ldots, \alpha_{2^n}\}$.
Best classical circuit can compute this using $O(n 2^n)$, i.e., exponential number of gates.

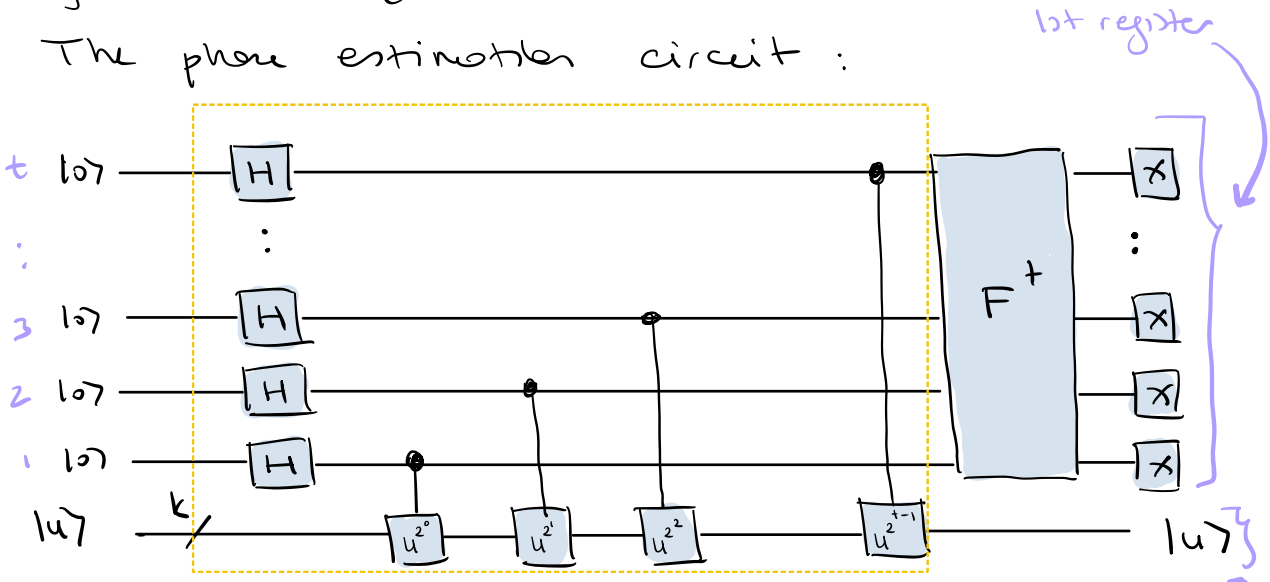
Phase estimation

Let $U : (\mathbb{C}^2)^{\otimes k} \to (\mathbb{C}^2)^{\otimes k}$ be a unitary. Let $|u\rangle \in (\mathbb{C}^2)^{\otimes k}$ be a unit vector such that

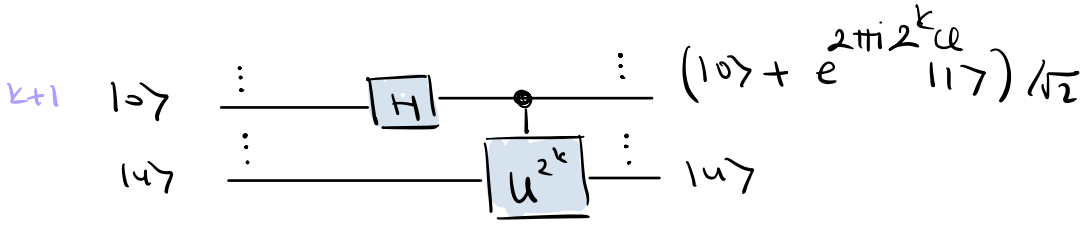
$$U|u\rangle = e^{2\pi i \varphi}|u\rangle$$

for some $\varphi \in [0,1)$.

The phase estimation circuit:



The state just before $F^\dagger$ can be computed easily:



$$C(U^{2^k})\, H \otimes \mathbb{I}\, |0\rangle|u\rangle = C(U^{2^k})\, \frac{|0\rangle+|1\rangle}{\sqrt{2}}\,|u\rangle$$

$$= \frac{|0\rangle + e^{2\pi i 2^k \varphi}|1\rangle}{\sqrt{2}}\,|u\rangle$$

Case I:

Let $\varphi = \varphi_1/2 + \varphi_2/2^2 + \cdots + \varphi_t/2^t$

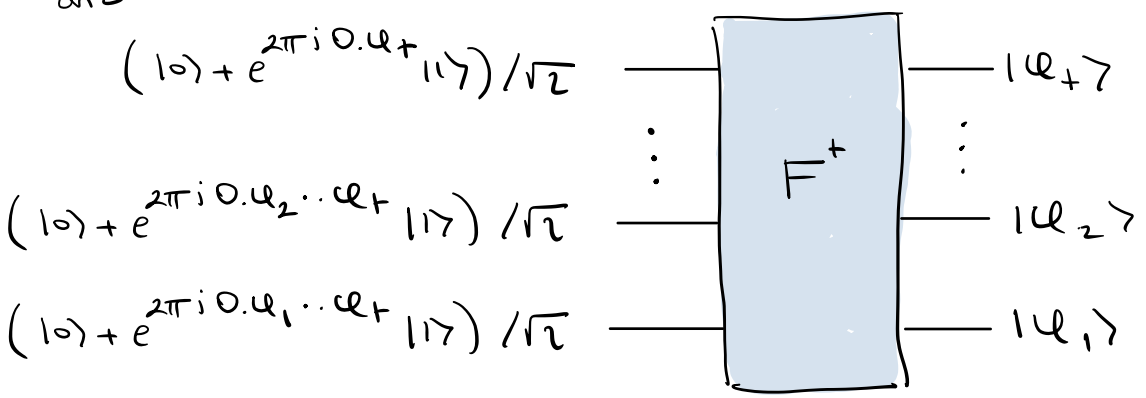
where $\varphi_i \in \mathbb{B}$.

Then

$$e^{2\pi i 2^k \varphi} = e^{2\pi i (\varphi_{k+1}/2 + \cdots + \varphi_t/2^{t-k})}$$

$$= e^{2\pi i \, 0.\varphi_{k+1} \cdots \varphi_t}$$

and



Therefore before the measurement the state is

$$|\varphi_1 \cdots \varphi_t\rangle |u\rangle$$

and measuring the first register outputs $\varphi_1 \cdots \varphi_t$ with probability 1.

Case II:

Let $\widetilde{\varphi} = \varphi_1/2 + \varphi_2/2^2 + \cdots + \varphi_t/2^t$.

Assume $\varphi \neq \widetilde{\varphi}$.

Lem: Let $F: \mathbb{C}^N \to \mathbb{C}^N$ denote the QFT.

Then $G: \mathbb{C}^N \to \mathbb{C}^N$ defined by

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

satisfies $G = F^\dagger$.

Proof: We have

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

$$= \frac{1}{N} \sum_{k,\ell} e^{2\pi i (j-\ell)k/N} |\ell\rangle$$

$$= \sum_\ell \underbrace{\frac{1}{N} \sum_k e^{2\pi i (j-\ell)k/N}}_{} |\ell\rangle$$

Let $\Delta = j - \ell$ and $\omega = e^{2\pi i \Delta/N}$.

Then

$$\frac{1}{N} \sum_{k=0}^{N-1} \omega^k = \begin{cases} 1 & \Delta = 0 \\ 0 & \Delta \neq 0 \end{cases}$$

where $\Delta \neq 0$ comes from

$$\sum_{k=0}^{N-1} \omega^k = \frac{1-\omega^N}{1-\omega} \quad \text{and} \quad \omega^N = 1.$$

$$= \sum_\ell \delta_{j\ell} |\ell\rangle = |j\rangle. \qquad \blacksquare$$

We have

$$F^{\otimes t} C(U^{2^{t-1}}) \cdots C(U^{2^0}) (H^{\otimes t} \otimes \mathbb{1}) |0\cdots0\rangle |u\rangle$$

$$= \frac{1}{2^{t/2}} F^{\otimes t} \left[(|0\rangle + e^{2\pi i 2^{t-1} \ell} |1\rangle) \cdots (|0\rangle + e^{2\pi i 2^0 \ell} |1\rangle) \right] |u\rangle$$

$$= \frac{1}{2^{t/2}} \sum_{k=0}^{2^t-1} e^{2\pi i \ell \left(\sum_{i=1}^{t} k_i 2^{t-i} \right)} F^{\otimes t} |k_1 \cdots k_t\rangle |u\rangle$$

(k under the sum; k under $|k_1 \cdots k_t\rangle$)

$$= \frac{1}{2^t} \sum_{k,\ell} e^{2\pi i \ell k} e^{-2\pi i k \ell / 2^t} |\ell\rangle |u\rangle$$

$$= \sum_{\ell} \underbrace{\frac{1}{2^t} \sum_{k} e^{2\pi i k (\ell - \ell/2^t)}}_{\alpha_{\ell - b}} |\ell\rangle |u\rangle$$

Let $b \in \{0, 1, \ldots, 2^t - 1\}$ such that

$$\boxed{0 < \underbrace{\ell - b/2^t}_{\delta} \leq 2^{-t}.}$$

Then

$$\alpha_\ell = \frac{1}{2^t} \sum_k \left[\underbrace{e^{2\pi i (2^t \ell - (b+\ell))/2^t}}_{\omega} \right]^k$$

$\frac{1 - \omega^{2^t}}{1 - \omega}$ since $\omega \neq 1$ ($\ell \neq \tilde{\ell}$)

$$= \frac{1}{2^t} \frac{1 - e^{2\pi i (2^t \delta - \ell)}}{1 - e^{2\pi i (\delta - \ell/2^t)}}$$

Note α_ℓ is a function of ℓ mod 2^t.

For $m \in \{0,1,\dots,2^t-1\}$ and $e>1$ let

$$p(|m-b|>e)$$

denote the probability of obtaining m as the outcome of the first register such that $|m-b|>e$.

Note that $p(|m-b|\le e) = 1 - p(|m-b|>e)$.

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

Proof: Let us write $m = b+\ell$ for some $\ell \ge 0$. Then

$$p(|m-b|>e) = p(|\ell|>e)$$

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

We have

$$|\alpha_\ell| = \frac{|1 - e^{2\pi i (2^t s - \ell)}|}{2^t |1 - e^{2\pi i (s - \ell/2^t)}|}$$

$|1-e^{2\pi i \theta}| \le 1 + |e^{2\pi i \theta}| = 2$

$$\le \frac{1}{2^{t-1} |1 - e^{2\pi i (s - \ell/2^t)}|}$$

$|1-e^{i\gamma}| \ge \frac{2|\gamma|}{\pi}$ if $-\pi \le \gamma \le \pi$ (calculus)

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

since $-2^{t-1} < \ell \le 2^{t-1}$ and $0 < \delta \le 2^{-t}$.

$\rightarrow -2^{t-1} \le \ell - 2^t\delta \le 2^{t-1}$

$$\le \frac{1}{2^{t-1}\,\frac{2\,|2\pi(\delta - \ell/2^t)|}{\pi}} = \frac{1}{2^{t+1}\,|\delta - \ell/2^t|}$$

Then

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

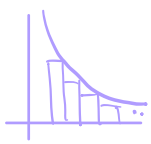
$$\le \frac{1}{4} \sum_{-2^{t-1} < \ell \le -(e+1)} 1/(2^t\delta - \ell)^2 + \sum_{e+1 \le \ell \le 2^{t-1}} 1/(2^t\delta - \ell)^2$$

$\ell^2 \le (2^t\delta + (-\ell))^2$ since $e+1 \le -\ell < 2^{t-1}$ and $0 < 2^t\delta \le 1$

$(\ell-1)^2 \le (2^t\delta - \ell)^2$

$$\le \frac{1}{4} \sum_{e+1 \le \ell \le 2^{t-1}-1} 1/\ell^2 + \sum_{e+1 \le \ell \le 2^{t-1}} 1/(\ell-1)^2$$

$$\le \sum_{e \le \ell \le 2^{t-1}-1} 1/\ell^2 \qquad \sum_{e \le \ell \le 2^{t-1}-1} 1/\ell^2$$



$$\le \frac{1}{2} \sum_{\ell=e}^{2^{t-1}-1} 1/\ell^2 \underbrace{\le}_{e>1} \frac{1}{2} \int_{e-1}^{\infty} \frac{1}{\ell^2}\, d\ell$$

$$= \frac{1}{2(e-1)}$$

∎

Pro : Given $n \geq 0$ and $\epsilon > 0$, if the number of qubits in the first register is

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

then

$$p(|m - b| \leq e) \geq 1 - \epsilon \quad \text{(success probability)}$$

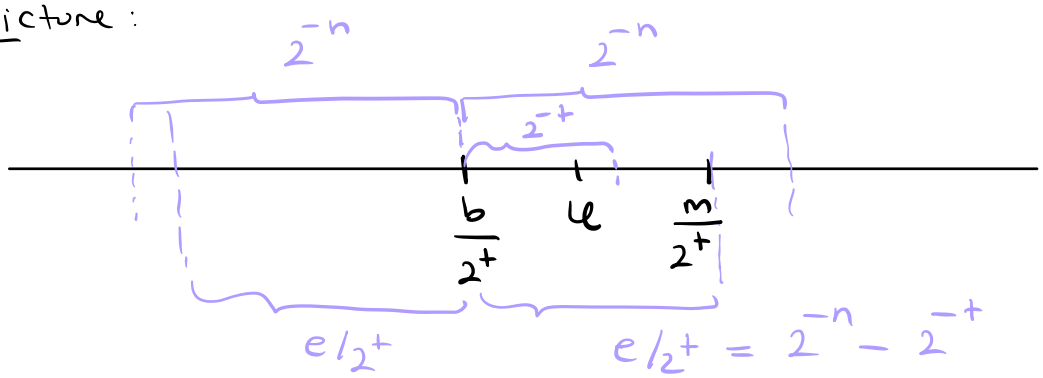
$$0 < \underbrace{\varphi - \frac{b}{2^t}}_{\delta} \leq 2^{-n} \quad \text{(accuracy)}$$

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

Proof : Choose $t \geq n$ and write

$$t = n + p, \quad p \geq 0.$$

Picture :



Given $\epsilon > 0$ let

$$p = \lceil \log\left(2 + \frac{1}{2\epsilon}\right) \rceil \quad \text{and} \quad e = 2^p - 1.$$

Then

$$0 < \varphi - b/2^t \leq 2^{-t} = 2^{-n-p} \leq 2^{-n}$$

since $p \geq 1$ and

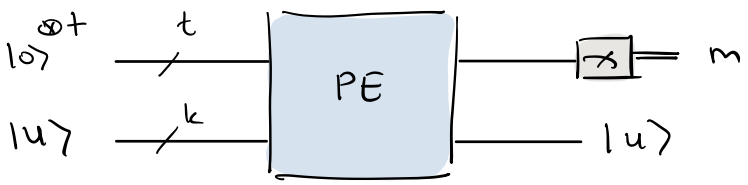
$$p(|m-b| \le e) = 1 - p(|m-b| > e)$$

$$\ge 1 - \frac{1}{2(e-1)} \ge 1 - \frac{1}{2\left(\frac{1}{2\epsilon}\right)} = 1-\epsilon.$$

$$e = 2^{\lceil \log(2+1/2\epsilon) \rceil} - 1 \ge 1 + \frac{1}{2\epsilon}$$

∎

Let us write $\tilde{u} = m_1/2 + m_2/2^2 + \cdots + m_t/2^t$ where m is the outcome of the circuit.



Cor: If $t = n + \lceil \log(2 + \frac{1}{2\epsilon}) \rceil$ then $\tilde{u}$ is an approximation of u accurate to n bits: $|u - \tilde{u}| \le 2^{-n}$.

Proof: We have

$$|u - \tilde{u}| = |u - \frac{m}{2^t}|$$

$$m = m_1 2^{t-1} + m_2 2^{t-2} + \cdots + m_t 2^0$$

and $\tilde{u} = \frac{m}{2^t}$

$$\le \underbrace{|\frac{b}{2^t} - \frac{m}{2^t}|}_{e/2^t} + 2^{-t}$$

$$\le 2^{-n} - 2^{-t} + 2^{-t} = 2^{-n}.$$

∎

Order finding algorithm

Given positive integers $x < N$ with $\gcd(x, N) = 1$ find the order of x mod N, i.e., the smallest positive integer r such that

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

Let $L = \lceil \log N \rceil$.

Define a linear operator

$$U : (\mathbb{C}^2)^{\otimes L} \longrightarrow (\mathbb{C}^2)^{\otimes L}$$

$$U|y\rangle = \begin{cases} |xy \mod N\rangle & \text{if } 0 \le y \le N-1 \\ |y\rangle & \text{if } N \le y \le 2^L - 1. \end{cases}$$

U is unitary since $\gcd(x, N) = 1$:

$\exists\ 0 \le z \le N-1$ such that $z \cdot x = 1 \mod N$.

$\gcd(x,N)=1 \iff \exists\ z, y \in \mathbb{Z} :\ zx + yN = 1.$

Then $U^\dagger$ is given by

$$U^\dagger|y\rangle = \begin{cases} |zy \mod N\rangle & \text{if } 0 \le y \le N-1 \\ |y\rangle & \text{if } N \le y \le 2^L - 1. \end{cases}$$

Also, $U^r = \mathbb{1}$ since $x^r = 1 \mod N$.

This implies that eigenvalues λ of U satisfy $\lambda^r = 1$, i.e., they are of the form

$$e^{2\pi i s / r} \quad \text{where } 0 \le s \le r-1.$$

An eigenvector corresponding to $e^{2\pi i s/r}$ is given by

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

(mod N will be dropped)

$$U|u_s\rangle = \frac{1}{\sqrt{r}} \sum_k e^{-2\pi i s k/r} U|x^k\rangle$$

$U|x^k\rangle = |x^{k+1}\rangle$ since $0 \le x^k \le N-1$

$$= e^{2\pi i s/r} \frac{1}{\sqrt{r}} \sum_k e^{-2\pi i s(k+1)/r} |x^{k+1}\rangle$$

$= |u_s\rangle$ since $|x^r\rangle = |1\rangle$.

$$= e^{2\pi i s/r} |u_s\rangle.$$

We can use phase estimation to find s/r.

Let $\{|u\rangle\}_u$ be an orthonormal basis of eigenvectors of U such that

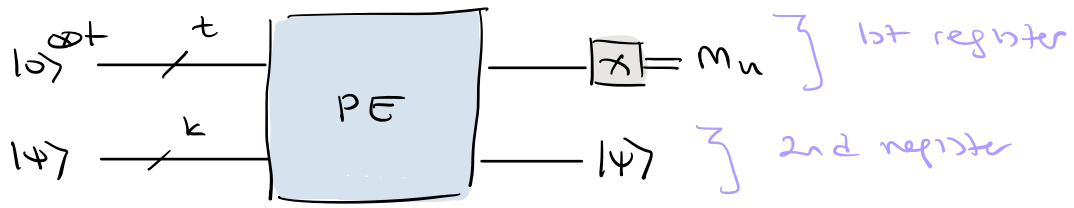
$$U|u\rangle = e^{2\pi i \varphi_u} |u\rangle.$$

Consider the unit vector

$$|\psi\rangle = \sum_u c_u |u\rangle, \quad c_u \in \mathbb{C}.$$

Pro: Let $t = n + \lceil \log(2 + \frac{1}{2\epsilon}) \rceil$ and $\epsilon = 2^{n-t} - 1$.

Then the circuit



will output $\tilde{u}_u$, an approximation for u_u accurate to n-bits, with probability $\geq |c_u|^2 (1-\epsilon)$.

Recall $\tilde{u} = m_1/2 + m_2/2^2 + \cdots + m_t/2^t$

Proof: By the principal of implicit measurement, the outcome probabilities of the 1st register are not affected by measuring the 2nd register.

Apply the projective measurement $\{|u\rangle\langle u|\}_u$ to the 2nd register.

We can further move this measurement to the beginning of the circuit since the controlled unitary commute with $|u\rangle\langle u|$'s.

Therefore we first measure $|0\cdots0\rangle|\psi\rangle$ to obtain $|0\cdots0\rangle|u\rangle$ with probability $|c_u|^2$.

Then the phase estimation produces a good estimator for u_u with probability at least $1-\epsilon$. ∎

Continued fraction algorithm

Given positive integers $a_0, \cdots, a_N$ the continued fraction expansion is the expression given by

$$[a_0, \cdots, a_N] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\cdots + \cfrac{1}{a_N}}}}$$

Any rational number has a continued fraction expression. The algorithm consists of split & invert steps until an integer a_N is obtained. Then there are two expressions

$$[a_0, \cdots, a_{N-1}, a_N]$$

and $$[a_0, \cdots, a_{N-1}, a_N - 1, 1]$$

One of them has even length & the other odd.

Ex:
$$\frac{31}{13} = 2 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1}}}}} \to 2$$

$$31/13 = [2, 2, 1, 1, 1, 1]$$

$$31/13 = [2, 2, 1, 1, 2].$$

The n-th convergent of $[a_0, \cdots, a_N]$ is defined to be $[a_0, \cdots, a_n]$.

Lem: $[a_0, \dots, a_n] = \dfrac{q_n}{p_n}$ where

$n=0$: $p_0 = a_0$, $q_0 = 1$

$n=1$: $p_1 = 1 + a_0 a_1$, $q_1 = a_1$

$2 \le n \le N$: $p_n = a_n p_{n-1} + p_{n-2}$

$q_n = a_n q_{n-1} + q_{n-2}$.

Moreover, $\gcd(p_n, q_n) = 1$.

Proof: The statement holds for $n = 0, 1$.

Assume $n \ge 2$ and consider the n-th convergent

$$[a_0, \dots, a_n] = a_0 + \cfrac{1}{\dots \cfrac{1}{a_{n-2} + \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}}$$

Let $\tilde{a}_{n-1} = a_{n-1} + \dfrac{1}{a_n}$.

Then

$$[a_0, \dots, a_n] = [a_0, \dots, a_{n-2}, \tilde{a}_{n-1}].$$

$$= \frac{\tilde{p}_{n-1}}{\tilde{q}_{n-1}} \quad \text{(by induction)}$$

$$= \frac{\tilde{a}_{n-1} p_{n-2} + p_{n-3}}{\tilde{a}_{n-1} q_{n-2} + q_{n-3}}$$

p_{n-1} →

$$= \frac{a_{n-1} p_{n-2} + p_{n-3} + p_{n-2}/a_n}{a_{n-1} q_{n-2} + q_{n-3} + q_{n-2}/a_n}$$

q_{n-1} →

$$= \frac{(a_n p_{n-1} + p_{n-2})\, a_n}{(a_n q_{n-1} + q_{n-2})\, a_n} = \frac{p_n}{q_n}.$$

Finally $\gcd(p_n, q_n) = 1$ since

$$q_n p_{n-1} - p_n q_{n-1} = (-1)^n.$$

This is proved by induction:

$n=1$: $q_1 p_0 - p_1 q_0 = a_1 a_0 - (1 + a_0 a_1) \cdot 1$

$= -1$

$n \geq 2$:

$(a_n q_{n-1} + q_{n-2}) p_{n-1} - (a_n p_{n-1} + p_{n-2}) q_{n-1}$

$= a_n (q_{n-1} p_{n-1} - p_{n-1} q_{n-1}) - (-1)^{n-1}$

$= (-1)^n.$ ☒

Thm: Let x and p/q be rational numbers satisfying $|p/q - x| \leq \frac{1}{2q^2}$.

Then p/q is a convergent of x and can be computed using $O(L^3)$ gates.

Proof: Assume $x \neq p/q$, otherwise the statement holds. Let $p/q = [a_0, \dots, a_n]$ and define p_i, q_i for $0 \le i \le n$.

Let $\delta = 2q^2 (x - p/q)$.

If we let

$$\lambda = 2\left(\frac{q_n p_{n-1} - p_n q_{n-1}}{\delta} \right) - \frac{q_{n-1}}{q_n}$$

($(-1)^n$ over the numerator; δ in the denominator)

$$|\delta| = 2q^2 \left| x - p/q \right| \le 2q^2 / 2q^2 = 1$$

then

$$x = \frac{\lambda p_n + p_{n-1}}{\lambda q_n + q_{n-1}}$$

(p_{n+1} over the numerator; q_{n+1} over the denominator)

HW: verify.

This means that

$$x = [a_0, a_1, \dots, a_n, a_{n+1}], \quad a_{n+1} = \lambda.$$

Here we chose n even if $\delta > 0$ & n odd if $\delta < 0$ so that

$$\lambda = \frac{2(-1)^n}{\delta} - \frac{q_{n-1}}{q_n} = \frac{2}{|\delta|} - \frac{q_{n-1}}{q_n}$$

$$> \frac{2}{1} - \frac{1}{1} = 1.$$

$q_n = a_{n-1} q_{n-1} + q_{n-2}$

$\Rightarrow q_n > q_{n-1}$.

Let $\lambda = [b_0, \dots, b_m]$. Then

$$x = [a_0, \dots, a_n, b_0, \dots, b_m].$$

($a_0, \dots, a_n$: n-th convergent is p/q.)

Next we determine the number of steps.

Let p/q be such that $p > q$ and $\gcd(p,q) = 1$.
In the expansion

$$p/q = [a_0, \ldots, a_N]$$

we have

$$p > q \geq 2^{\lfloor N/2 \rfloor}.$$

since $q_n = a_n q_{n-1} + q_{n-2} \geq 2 q_{n-2}$
(similarly $p_n \geq 2 p_{n-2}$.)

Therefore if p & q are L-bit integers then

$$2^L \geq p > q \geq 2^{\lfloor N/2 \rfloor}$$

and $N \geq O(L)$.

To compute $[a_0, \ldots, a_N]$ we need to perform $O(L)$ split & invert steps each of which requires $O(L^2)$ gates. ☒

The order-finding algorithm

Given $x < N$ with $\gcd(x, N) = 1$, find the order of x mod N:

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

Let $L = \lceil \log N \rceil$.

1) Apply the phase estimation alg. to the unitary ($O(L^a)$)

$$U : (\mathbb{C}^2)^{\otimes L} \longrightarrow (\mathbb{C}^2)^{\otimes L}$$

$$U|y\rangle = \begin{cases} |xy\rangle & 0 \le y \le N-1 \\ |y\rangle & N \le y \le 2^L - 1 \end{cases}$$

with

$$t = 2L+1 + \lceil \log(2 + 1/2\epsilon) \rceil$$

and initial state $|0\ldots0\rangle|1\rangle$,

where

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

$$U|u_s\rangle = e^{2\pi i \varphi_s} |u_s\rangle$$

to estimate $\varphi_s = s/r$ accurate to $2L+1$ bits, i.e.,

$$|s/r - \tilde{\varphi}| \le 2^{-(2L+1)}.$$

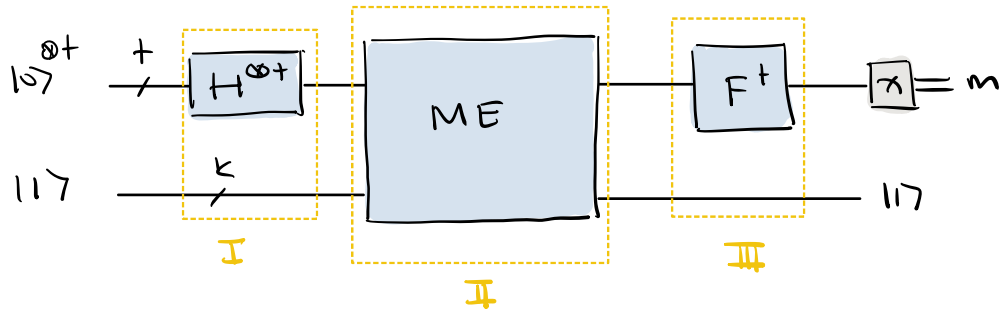
Verification:

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

$$= \sum_k \underbrace{\left(\frac{1}{r} \sum_s e^{-2\pi i sk/r} \right)}_{\delta_{k,0}} |x^k\rangle$$

$$= |1\rangle$$

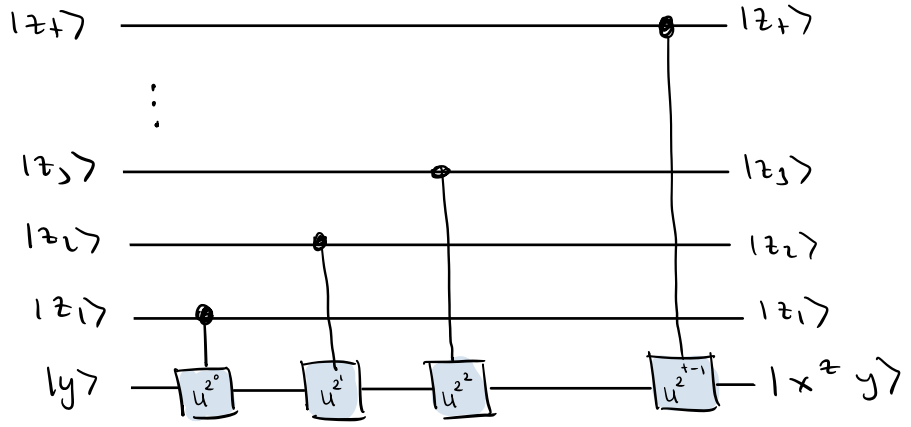
The PE circuit consists of three parts



Parts I and III can be implemented using polynomial number of gates (in L) using $\tilde{A}_Q = \{H, T, T^+, CNOT\}$

Modular exponentiation (For Part II)

Consider the following circuit



For $0 \le y \le N-1$ we have

$$c(U^{2^{t-1}}) \cdots c(U^{2^0}) \, |z_t \cdots z_1\rangle |y\rangle$$

$$= |z_t \cdots z_1\rangle \, U^{z_t 2^{t-1}} \cdots U^{z_1 2^0} |y\rangle$$

$$= |z_t \cdots z_1\rangle \, |\underbrace{x^{z_t 2^{t-1}} \cdots x^{z_1 2^0} y}\rangle$$

can be implemented classically

The numbers $x^{z+2^{t-1}}, \ldots, x^{z,2^0}$ can be computed using $t-1$ squaring operations: $O(L^3)$ gates. Multiplying these numbers requires $O(L^3)$ gates.

Therefore ME uses $O(L^3)$ gates.

2) Apply the continued fraction algorithm:

$O(L^b)$, $b = 3$

$$\left|\frac{s}{r} - \tilde{q}\right| \leq 2^{-(2L+1)} \leq \frac{1}{2r^2}$$

$$2^{-(2L+1)} = \frac{1}{2(2^L)^2} \leq \frac{1}{2r^2}$$

since $r \leq N \leq 2^L$

By the theorem s/r is a convergent of $\tilde{q}$:

$$\exists n : \quad \frac{s}{r} = \frac{p_n}{q_n}. \qquad \text{(n-th convergent)}$$

a) If $\gcd(s,r) = 1$ then

$$\boxed{r = q_n.}$$

Order is found!

b) If $\gcd(s,r) \neq 1$ then repeat the algorithm.

The probability $p(\gcd(s,r) = 1)$ that $\gcd(r,s) = 1$ satisfies

$$p(\gcd(s,r) = 1) \geq p(s \leq r \ \& \ s \text{ prime})$$

$$= \frac{\pi(r)}{r}$$ } number of primes $\leq r$

$\pi(r) \geq \frac{r}{2\log(r)}$

NC Problem 4.1 "prime number theorem"

$$\geq \frac{\frac{r}{2\log(r)}}{r}$$

$$= \frac{1}{2\log r} = \frac{1}{2L}.$$

By repeating the algorithm $O(L^b)$ times we observe with high probability $\varphi_s = s/r$ with $\gcd(s,r) = 1$.

Therefore we can extract r with high probability in polynomial time.

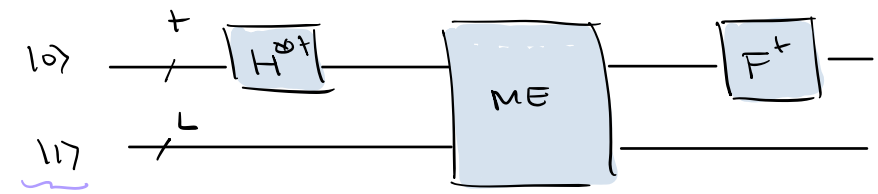
by the Amplification lemma

Summary of order-finding

Given $x < N$ with $\gcd(x,N) = 1$ find the order r of x mod N.

Algorithm:

1) Apply PE algorithm



$|0\ldots0\rangle$

to obtain $\tilde{\varphi}_s$, a good estimate of s/r.

$t = O(L)$ where $L = \lceil \log N \rceil$

$$U|y\rangle = \begin{cases} |xy\rangle & 0 \le y \le N-1 \\ |y\rangle & N \le y \le 2^L - 1 \end{cases}$$

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

$$U|u_s\rangle = e^{2\pi i s/r}|u_s\rangle$$

2) Apply CF algorithm to find s/r as a convergent of $\tilde{q}_s$, the outcome of the circuit.

Shor's factoring algorithm

Factoring problem: Given a composite integer N find a nontrivial factor.

We will reduce this problem to order-finding.

Lemma: Let $0 \leq N \leq 2^L - 1$ be a composite number. If $1 < x < N-1$ is a solution to

$$x^2 = 1 \mod N$$

then at least

$$\gcd(x-1, N) \quad \text{or} \quad \gcd(x+1, N)$$

is a non-trivial factor of N.

This factor can be computed in $O(L^3)$ gates.

Proof: Since $x^2 = 1 \mod N$, N divides

$$x^2 - 1 = (x-1)(x+1).$$

We have

$$\underbrace{0 < x-1 < x+1 < N}$$

Recall $1 < x < N-1$.

Thus, N has a common factor either with $x-1$ or $x+1$.

common factor → positive integer $< N$.

We can compute

$$\gcd(x-1, N) \quad \text{or} \quad \gcd(x+1, N)$$

using Euclid's algorithm.

To find $\gcd(a,b)$ with $a > b$ we need to compute

$$
\begin{aligned}
a &= k_1 b + r_1 \\
b &= k_2 r_1 + r_2 \\
r_1 &= k_3 r_2 + r_3 \\
&\vdots \\
r_i &= k_{i+2} r_{i+1} + r_{i+2} \\
&\vdots \\
r_m &= k_{m+2} r_{m+1} + 0.
\end{aligned}
$$

$O(L)$

each step $O(L^2)$

$\hookrightarrow \gcd(a,b)$

The number of steps is at most $2 \lceil \log a \rceil$. This follows from $r_{i+2} \leq r_i / 2$.

1) $r_{i+1} \leq r_i/2 \Rightarrow r_{i+2} \leq r_{i+1} \leq r_i/2$

2) $r_{i+1} > r_i/2 \Rightarrow$

$$r_i = 1 \cdot r_{i+1} + r_{i+2}$$

$$\Rightarrow r_{i+2} = r_i - r_{i+1} \leq r_i/2.$$

$\square$

Notation: We will write

$$\mathbb{Z}_N = \{0, 1, \dots, N-1\} \quad \text{and}$$

$$\mathbb{Z}_N^\times = \{0 \le k \le N-1 : \gcd(k, N) = 1\}.$$

Chinese remainder theorem:
Let $N = p_1^{\alpha_1} \cdots p_m^{\alpha_m}$ where p_i's are distinct prime numbers.
Then

$$\mathbb{Z}_N \longrightarrow \mathbb{Z}_{p_1^{\alpha_1}} \times \cdots \times \mathbb{Z}_{p_m^{\alpha_m}}$$

$$x \longmapsto (x \bmod p_1^{\alpha_1}, \dots, x \bmod p_m^{\alpha_m})$$

is a bijection

Cor: This bijection restricts to a bijection

$$\mathbb{Z}_N^\times \longrightarrow \mathbb{Z}_{p_1^{\alpha_1}}^\times \times \cdots \times \mathbb{Z}_{p_m^{\alpha_m}}^\times.$$

The Euler function $\varphi(N)$ is defined by

$$\varphi(N) = |\mathbb{Z}_N^\times|.$$

Ex: By the Cor. we have

$$\varphi(N) = \prod_{i=1}^{m} \varphi(p^{\alpha_i}).$$

We can show that $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$:

$$\begin{aligned}\varphi(p^\alpha) &= |\mathbb{Z}_{p^\alpha}^\times| \\ &= |\mathbb{Z}_{p^\alpha} - \{vp : v = 0, 1, \dots, (p^{\alpha-1}-1)\}| \\ &= p^\alpha - p^{\alpha-1} \\ &= p^{\alpha-1}(p-1).\end{aligned}$$

Lem: Let p be an odd prime. There exists $k \in \mathbb{Z}_N^\times$ such that

$$\mathbb{Z}_N^\times = \{k^i : 1 \le i \le \varphi(N)\}.$$

Lem: Let p be an odd prime and 2^d be the largest power of 2 dividing $\varphi(p^\alpha)$. Then the largest power of 2 dividing the order r of $k^i \in \mathbb{Z}_{p^\alpha}$ is given by

1) 2^d if i is odd,
2) 2^k where $k \le d-1$ if i is even.

Proof: We have

$$\mathbb{Z}_{p^\alpha}^\times = \underbrace{\{k^i : i \text{ odd}\}}_{A} \cup \underbrace{\{k^i : i \text{ even}\}}_{B}$$

($\cdot k$ maps A into B; $\cdot k^{-1}$ maps B into A)

A and B are in bijective correspondence.

For $k^i \in A$ we have

$$(k^i)^r = 1 \bmod p^\alpha \Rightarrow \varphi(p^\alpha) \mid ir$$

($\mid$: divides)

$$\Rightarrow 2^d \mid r \text{ since } i \text{ is odd.}$$

Here 2^d is the largest power of 2 dividing r.

For $k^i \in B$ we have

$$(k^i)^{\varphi(p^\alpha)/2} = \left(k^{\varphi(p^\alpha)}\right)^{i/2} = 1 \bmod p^\alpha.$$

Thus $r \mid \varphi(p^\alpha)/2$ and $2^d \nmid r$. ∎

Theorem: Let N be a composite odd positive integer with prime factorization:

$$N = p_1^{\alpha_1} \cdots p_m^{\alpha_m}.$$

Let $x \in \mathbb{Z}_N^*$ be chosen uniformly at random and r be the order of x modulo N.

Then the probability that r is even and $x^{r/2} \neq -1 \bmod N$ is at least $1 - 1/2^{m-1}$:

$$p(r \text{ even } \& \; x^{r/2} \neq -1 \bmod N) \geq 1 - \frac{1}{2^{m-1}}.$$

Proof: We will show that

$$p(r \text{ odd or } x^{r/2} = -1 \bmod N) \leq \frac{1}{2^{m-1}}.$$

By the Chinese remainder theorem, choosing $x \in \mathbb{Z}_N$ uniformly is the same as choosing $x_j \in \mathbb{Z}_{p_j^{\alpha_j}}$ uniformly for each $j = 1, \ldots, m$.

Let r_j be the order of $x_j \bmod p_j^{\alpha_j}$.

Let 2^{d_j} (and 2^d) be the largest power of 2 dividing r_j (and r).

Claim: If r is odd or $x^{r/2} = -1 \bmod N$ then $d_1 = d_2 = \cdots = d_m = d$.

1) r is odd:

Since $r_j \mid r \ \forall j$ each r_j is odd. Therefore $d_1 = \cdots = d_m = d = 0$.

2) $x^{r/2} = -1 \bmod N$:

Then $x^{r/2} = -1 \bmod p_j^{\alpha_j} \ \forall j$, and hence $r_j \nmid r/2$. But since $r_j \mid r$ we have $d_j = d$.

Now, we choose $x_1 \in \mathbb{Z}_{p_1^{\alpha_1}}^{\times}$ uniformly at random. By the Lemma at most half of the elements in $\mathbb{Z}_{p_2^{\alpha_2}}^{\times}$ will have $2^{d_2} = 2^{d_1}$ as the largest power of 2 dividing its order.

Therefore x_2 can be chosen from at most half of the elements in $\mathbb{Z}_{p_1^{\alpha_1}}^{\times}$. Similarly $x_3, \dots, x_m$ can be chosen among half of the elements in $\mathbb{Z}_{p_3^{\alpha_3}}^{\times}, \dots, \mathbb{Z}_{p_m^{\alpha_m}}^{\times}$, respectively.

Therefore

$$p(r \text{ is odd } \& \; x^{r/2} = -1 \bmod N) \leq \frac{1}{2^{m-1}}. \qquad \blacksquare$$

Algorithm for reducing factoring to order-finding

1) If N is even then return 2.
2) If $N = a^b$ for integers $a \geq 1$ and $b \geq 2$ then return a.

   ($*$ of prime factors of N)

   When we reach step 3, N is odd & ($m \geq 2$).
3) Choose $2 \leq x \leq N-1$ uniformly at random. If $\gcd(x, N) > 1$ then return $\gcd(x, N)$; otherwise proceed to step 4.

   When we move to step 4, $\gcd(x, N) = 1$.
4) Use the order-finding algorithm to find the order r of $x \bmod N$. (Quantum part)
5) If r even and $x^{r/2} \neq -1 \bmod N$ then compute

   ↳ prob. of this $\geq 1 - \frac{1}{2^{m-1}} \geq \frac{1}{2}$

   $\gcd(x^{r/2} - 1, N)$ and $\gcd(x^{r/2} + 1, N)$

↳ By the first lemma one of them is a non-trivial factor of N.

Return the non-trivial factor.

This algorithm uses polynomial number of gates. Its success probability is $O(1)$.

We proved Shor's theorem:

Theorem: FACTORING $\in$ BQP.

Hidden subgroup problem

A group G is a set together with a binary operation $\cdot : G \times G \to G$ satisfying

1) Closure: $g, h \in G \Rightarrow g \cdot h \in G$

2) Associativity: $\forall\, g, h, k \in G$
$(g \cdot h) \cdot k = g \cdot (h \cdot k)$.

3) Identity: $\exists\, 1 \in G$:
$g \cdot 1 = 1 \cdot g = g$, $\forall\, g \in G$.

4) Inverse: For every $g \in G$, $\exists\, \bar{g}^{1} \in G$:
$g \cdot \bar{g}^{1} = \bar{g}^{1} \cdot g = 1$.

G is called Abelian if

5) $\forall\, g, h \in G$
$g \cdot h = h \cdot g$.

A subset $H \subset G$ is called a subgroup if it forms a group under the operation $\cdot$.

A function $f : G \to H$ is called a group homomorphism if
$f(g \cdot g') = f(g) \cdot f(g')$ $\forall g, g' \in G$.

A bijective group homomorphism is called a group isomorphism. We write

$$G \cong H.$$

Ex: 1) $\mathbb{Z}_N = \{0, 1, \dots, N-1\}$ under addition

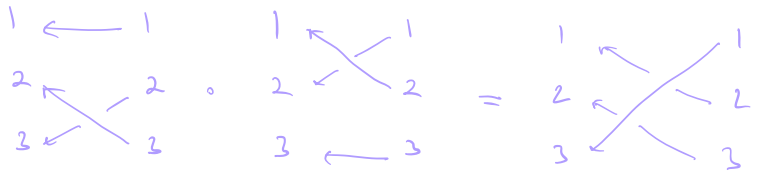
$$\mathbb{Z}_N^\times = \{1 \le k \le N-1 : \gcd(k, N) = 1\}$$

under multiplication

Both groups are Abelian.

2) Σ_n : permutations of $\{1, \dots, n\}$ under composition.

Σ_n is not abelian for $n \ge 2$:



3) $U(\mathbb{C})$ under matrix multiplication.

Given two groups G and H the direct product $G \times H$ is the group consisting of pairs (g, h), where $g \in G$ and $h \in H$, with the binary operation

$$(g, h) \cdot (g', h') = (g \cdot g', h \cdot h').$$

The identity element is given by $(1,1)$ and the inverse of (g,h) is (g^{-1}, h^{-1}).

We will only consider finite Abelian groups and write $+$ for the binary operation $\cdot$ in the case of Abelian groups.

Theorem: Let G be a finite Abelian group and $|G| = p_1^{\alpha_1} \cdots p_m^{\alpha_m}$.
Then

$$G \cong \mathbb{Z}_{p_1^{\alpha_1}} \times \cdots \times \mathbb{Z}_{p_m^{\alpha_m}}.$$

A group homomorphism

$$\chi : G \longrightarrow U(\mathbb{C})$$

is called a character.

Ex: 1) Trivial character $\chi : G \to U(\mathbb{C})$
$g \mapsto 1 \quad \forall g \in G.$

2) $\chi : \mathbb{Z}_N \hookrightarrow U(\mathbb{C})$
$x \longmapsto \omega^x$ where $\omega = e^{2\pi i/N}$.

Pro: Every character of $\mathbb{Z}_N$ is of the form

$$\chi_y : \mathbb{Z}_N \longrightarrow U(\mathbb{C}), \; y \in \mathbb{Z}_N,$$
$$\chi_y(x) = e^{2\pi i xy/N}.$$

Proof: A character $\chi : \mathbb{Z}_N \to U(\mathbb{C})$ satisfies

$$\chi(x) = \chi(\underbrace{1 + \cdots + 1}_{x}) = \chi(1)^x.$$

In particular, $\chi(1)^N = \chi(N) = \chi(0) = 1$.
Therefore χ is determined by $\chi(1) \in U(\mathbb{C})$ satisfying $\chi(1)^N = 1$, i.e., by $\chi(1) = e^{2\pi i y/N}$ for some $y \in \mathbb{Z}_N$.
Conversely given $e^{2\pi i y/N}$ we can define a character by setting $\chi(1) = e^{2\pi i y/N}$.

□

Cor: Every character of $\mathbb{Z}_{N_1} \times \mathbb{Z}_{N_2} \times \cdots \times \mathbb{Z}_{N_k}$ is of the form

$$\chi_{y_1 \cdots y_k}(x_1, \cdots, x_k) = \chi_{y_1}(x_1)\, \chi_{y_2}(x_2) \cdots \chi_{y_k}(x_k).$$

Proof: A character $\chi : \mathbb{Z}_{N_1} \times \cdots \times \mathbb{Z}_{N_k} \to U(\mathbb{C})$ is determined by the values

$$\chi(0, \cdots, 0, 1, 0, \cdots, 0).$$
$$\uparrow i\text{-th}.$$

That is,

$$\chi(x_1, \cdots, x_k) = \chi(1, 0, \cdots, 0)\, \chi(0, 1, 0, \cdots, 0) \cdots \chi(0, \cdots, 0, 1).$$

Each $\chi(0, \cdots, 0, x_i, 0, \cdots, 0)$ is a character of $\mathbb{Z}_{N_i}$, hence is of the form $\chi_{y_i}(x_i)$

□

Consider the vector space $\mathbb{C}^G$ of functions

$$f : G \longrightarrow \mathbb{C}.$$

Given two functions $f_1, f_2 : G \longrightarrow \mathbb{C}$ we define the inner product

$$(f_1, f_2) = \frac{1}{|G|} \sum_{g \in G} \overline{f_1(g)}\, f_2(g)$$

Lem: Let χ and χ' be characters of G. Then

$$(\chi, \chi') = \delta_{\chi,\chi'}. \quad \text{(character orthogonality)}$$

Proof: We have $G \cong \mathbb{Z}_{p_1^{\alpha_1}} \times \cdots \times \mathbb{Z}_{p_m^{\alpha_m}}$.

Then χ, χ' are of the form

$$\chi_{y_1,\ldots,y_m} \times \chi_{y_1',\ldots,y_m'}.$$

We have

$$(\chi_{y_1 \cdots y_m}, \chi_{y_1' \cdots y_m'})$$

$$= \frac{1}{|G|} \sum_{g \in G} \overline{\chi_{y_1 \cdots y_m}(g)}\, \chi_{y_1' \cdots y_m'}(g)$$

$$= \frac{1}{|\mathbb{Z}_{p_1^{\alpha_1}}| \cdots |\mathbb{Z}_{p_m^{\alpha_m}}|} \sum_{\substack{x_1 \in \mathbb{Z}_{p_1^{\alpha_1}} \\ \vdots \\ x_m \in \mathbb{Z}_{p_m^{\alpha_m}}}} \overline{\chi_{y_1}(x_1)} \cdots \overline{\chi_{y_m}(x_m)}\, \chi_{y_1'}(x_1) \cdots \chi_{y_m'}(x_m)$$

$$= (\chi_{y_1}, \chi_{y_1'}) \cdots (\chi_{y_m}, \chi_{y_m'}).$$

Therefore we reduce to $G = \mathbb{Z}_N$.
In this case

$$(\chi_y, \chi_{y'}) = \frac{1}{N} \sum_{x=0}^{N-1} e^{2\pi i (y'-y)/N}$$

$$= \frac{1}{N} \sum_{x=0}^{N-1} \omega^x = \begin{cases} \frac{1}{N} \cdot N & y = y' \\ \frac{1}{N} \cdot \frac{1-\omega^N}{1-\omega} & y \neq y' \end{cases}$$

$$= \delta_{y,y'}. \qquad \blacksquare$$

Cor: The set $\{\chi : G \to U(\mathbb{C}) \subset \mathbb{C}\}$ of characters is an orthonormal basis of $\mathbb{C}^G$. (with respect to $(-,-)$).

The Fourier transform of a function $f : G \to \mathbb{C}$ is the function $\hat{f} : G \to \mathbb{C}$ defined by

$$\hat{f}(y) = \frac{1}{\sqrt{|G|}} \sum_x \chi_y(x) f(x)$$

$$= \sqrt{|G|}\, (\overline{\chi}_y, f).$$

Quantum Fourier Transform

The QFT over G is the unitary operator

$$F_G : \mathbb{C}^G \longrightarrow \mathbb{C}^G$$

defined by

$$F_G |x\rangle = \frac{1}{\sqrt{|G|}} \sum_{y \in G} \chi_y(x) |y\rangle$$

(where $|x\rangle$ stands for e_x).

Note that

$$F_G \sum_x f(x) |x\rangle = \sum_x \frac{1}{\sqrt{|G|}} \sum_y f(x) \chi_y(x) |y\rangle$$

$$= \sum_y \frac{1}{\sqrt{|G|}} \sum_x f(x) \chi_y(x) |y\rangle$$

$$= \sum_y \hat{f}(y) |y\rangle$$

Pro: If $G = \mathbb{Z}_{N_1} \times \cdots \times \mathbb{Z}_{N_k}$ then

$$F_G = F_{\mathbb{Z}_{N_1}} \otimes \cdots \otimes F_{\mathbb{Z}_{N_k}}.$$

Proof: Direct verification:

$$F_G |x\rangle = \frac{1}{\sqrt{|G|}} \sum_{y \in G} \chi_y(x) |y\rangle$$

$$= \frac{1}{\sqrt{N_1}\cdots\sqrt{N_k}} \sum_{y_1\cdots y_k} \chi_{y_1}(x_1)\cdots\chi_{y_k}(x_k)\,|y_1\cdots y_k\rangle$$

$$= \bigotimes_{i=1}^{k} \frac{1}{\sqrt{N_i}} \sum_{y_i} \chi_{y_i}(x_i)\,|y_i\rangle$$

$$= \bigotimes_{i=1}^{k} F_{\mathbb{Z}_{N_i}}\,|y_i\rangle$$

$\square$

Let $H \subset G$ be a subgroup.

A <u>left coset</u> is a set of the form

$$g+H = \{\, g+h \;:\; h\in H \,\}, \quad g\in G.$$

<u>Lem</u>: $g+H \cap g'+H = \begin{cases} g+H & g-g'\in H \\ \emptyset & \text{otherwise.} \end{cases}$

<u>Proof</u>: Assume $g+H \cap g'+H \neq \emptyset$, i.e.,

$\exists\ k \in g+H \cap g'+H$.

Then

$$k = g+h = g'+h' \quad \text{for some } h,h'\in H,$$

$$\Rightarrow\ g' = g+h-h'$$

$$\Rightarrow\ g'+H = g+h-h'+H$$

$$= g+H$$

$\square$

Note that for $h \in H$ we have $h+H = H$:

$\forall\ h' \in h+H \Rightarrow h' = h + h'' \in H.$

$\forall\ h' \in H \Rightarrow h' = h - h + h' \in h+H.$

A set $S = \{g_1, \dots, g_\ell\} \subset G$ is said to generate G if every element of G can be written as a finite product of elements in S.

Ex: 1) $\mathbb{Z}_{p^\alpha}$ can be generated by any element $1 \le k \le p^\alpha - 1$ such that $\gcd(k, p^\alpha) = 1$.

More generally, $\mathbb{Z}_N \cong \mathbb{Z}_{p_1^{\alpha_1}} \times \dots \times \mathbb{Z}_{p_m^{\alpha_m}}$ can be generated by m elements $k_1, \dots, k_m$ such that $\gcd(k_i, p_i^{\alpha_i}) = 1$.

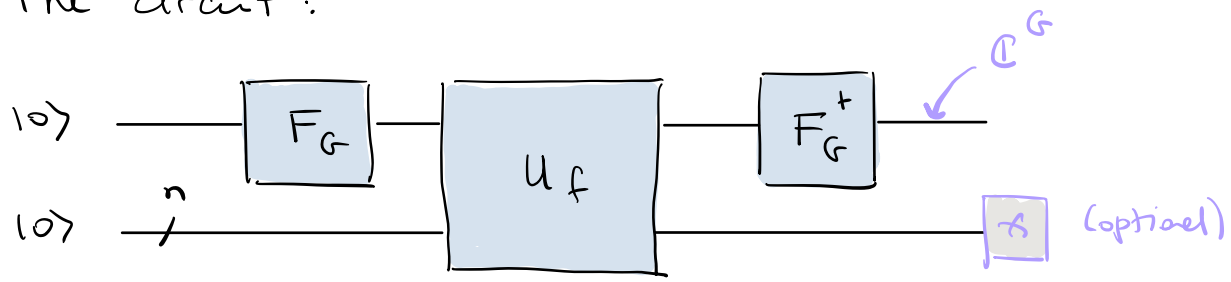
2) Σ_n is generated by transpositions, that is, permutations that swap two elements and fix the rest.

Hidden subgroup problem:

Let $f: G \to \mathcal{H}_2$ be a function such that $f(g) = f(g') \iff g+H = g'+H$.

Find a generating set for H.

The circuit:



where $U_f : \mathbb{C}^G \otimes (\mathbb{C}^2)^{\otimes n} \to \mathbb{C}^G \otimes (\mathbb{C}^2)^{\otimes n}$

$$U_f |x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle.$$

We have

$$U_f F_G |0\rangle|0\rangle = U_f \frac{1}{\sqrt{|G|}} \sum_y \underbrace{\chi_y(0)}_{1} |y\rangle|0\rangle$$

$$= \frac{1}{\sqrt{|G|}} \sum_y |y\rangle|f(y)\rangle.$$

Measuring the second register, if the outcome is $f(y)$ then the post-measurement state is

$$|y+H\rangle|f(y)\rangle$$

where

$$|y+H\rangle = \frac{1}{\sqrt{|H|}} \sum_{x \in H} |y+x\rangle .$$

Assume $G = \mathbb{Z}_{N_1} \times \cdots \times \mathbb{Z}_{N_k}$.

Let

$$H^\perp = \{ t \in G : \chi_t|_H = 1 \}$$

$$\chi_t(s) = e^{2\pi i t_1 s_1/N_1} \cdots e^{2\pi i t_k s_k/N_k}$$

$$= e^{2\pi i \sum_i t_i s_i/N_i} = 1 \qquad \forall s \in H$$

$$= \{ t \in G : \underbrace{\sum_{i=1}^{k} \frac{t_i s_i}{N_i} = 0 \bmod 1}, \ \forall s \in H \}$$

equivalently this sum is an integer.

Lem:

$$F_G^+ |y+H\rangle = \frac{1}{\sqrt{|H^\perp|}} \sum_{t \in H^\perp} \overline{\chi_t(y)}\, |t\rangle.$$

$\chi_{t_1}(x_1) \cdots \chi_{t_k}(x_k)$

Proof: First note that

$$F_G^+ |x\rangle = \frac{1}{\sqrt{|G|}} \sum_y \overline{\chi_y(x)}\, |y\rangle$$

Verification:

$$F_G F_G^+ |x\rangle = \frac{1}{|G|} \sum_y \sum_z \overline{\chi_y(x)}\, \chi_z(y)\, |z\rangle$$

$$= \sum_z \frac{1}{|G|} \sum_y \overline{\chi_x(y)}\, \chi_z(y)\, |z\rangle$$

$$= \sum_z \delta_{x,z}\, |z\rangle = |x\rangle.$$

Then

$$F_G^+ \frac{1}{\sqrt{|H|}} \sum_{z \in H} |y+z\rangle = \frac{1}{\sqrt{|H|\,|G|}} \sum_{z \in H} \sum_{x \in G} \overline{\chi_x(y+z)}\, |x\rangle$$

$$= \sqrt{\frac{|H|}{|G|}} \sum_x \underbrace{\frac{1}{|H|} \sum_z \overline{\chi_x(y+z)}}_{\overline{\chi_x(y)}\ (\chi_x|_H,\ \chi_0)_H}\ |x\rangle$$

Here $\chi_x|_H$ is the restriction of $\chi_x : G \to U(\mathbb{C})$ to H. We have $\chi_x|_H = \chi_h$ for some

$h \in H$. In particular, $h = 0 \iff x \in H^\perp$.

Therefore

$$(\chi_x|_H, \chi_0)_H = \begin{cases} 0 & x \notin H^\perp \\ 1 & x \in H^\perp. \end{cases}$$

$$= \sqrt{\frac{|H|}{|G|}} \sum_{x \in H^\perp} \overline{\chi_x(y)} \, |x\rangle$$

HW: $|H^\perp| = \frac{|G|}{|H|}$

$$= \frac{1}{|H^\perp|} \sum_{x \in H^\perp} \overline{\chi_x(y)} \, |x\rangle$$

□

Measuring the first register:

$$p(x) = \begin{cases} 1/|H^\perp| & x \in H^\perp \\ 0 & \text{otherwise.} \end{cases}$$

Running the algorithm many times we obtain

$$t_1, t_2, \ldots, t_m \in H^\perp.$$

A generating set for H can be found by solving

$$\sum_{i=1}^{k} \frac{(t_j)_i \, s_i}{N_i} = 0 \mod 1 \qquad j = 1, \ldots, m.$$

let $M = \mathrm{lcm}(N_1, \ldots, N_k)$ and

$$(t_j')_i = \frac{M}{N_j} (t_j)_i \in \mathbb{Z}.$$

Then we have

$$\sum_{j=1}^{k} (t_j')_i s_i = 0 \mod M.$$

The idea is similar to Simon's algorithm.

Run time: $\log^m |G|$

Examples:

Deutsch's problem

$$f: \mathbb{Z}_2 \longrightarrow \mathbb{Z}_2, \quad H = \begin{cases} 0 & f \text{ balanced} \\ \mathbb{Z}_2 & f \text{ constant} \end{cases}$$

Simon's problem

$$f: \mathbb{Z}_2^n \longrightarrow \mathbb{Z}_2^n, \quad H \cong \mathbb{Z}_2$$

Period-finding

$$f: \mathbb{Z}_N \longrightarrow \mathbb{Z}_2^n, \quad H = r\mathbb{Z}_N$$

$$f(x) = f(x') \iff \underbrace{x - x' \in r\mathbb{Z}_N}_{x = x' + rk}$$

Order-finding

$$f: \mathbb{Z}_N \longrightarrow \mathbb{Z}_N^{\times} \subset \mathbb{Z}_2^n, \quad H = r\mathbb{Z}_N$$

$$k \longmapsto x^k$$