Quantum computation: lecture 9

Shor's algorithm: conclusion

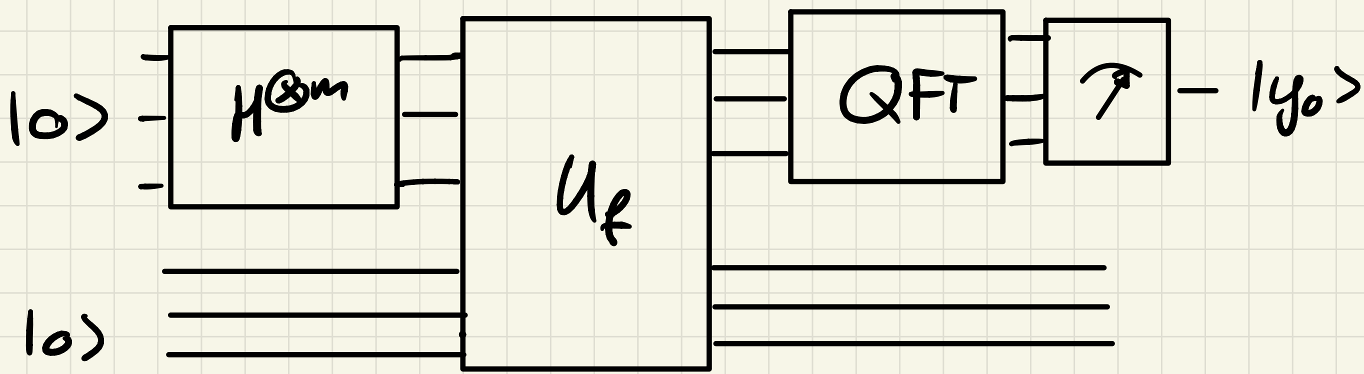
Reminder:

We are looking for the period $r \in \{1..N-1\}$ of a function $f: \mathbb{Z} \longrightarrow \mathbb{Z}$ defined as

$$f(x) = a^x \bmod N$$

where $a \in \{1..N-1\}$ is some fixed integer.

For this, we take $M = 2^m$ for some integer $m \geq 1$ such that $M \geq N^2$ (justification later) and use Shor's quantum circuit with $2m$ qubits:



As seen last week, the output of the circuit is a number $y \in \{0..M-1\}$ such that

$$\mathbb{P}(y \in I) \geq \frac{2}{5}$$

where $I = \bigcup_{k=0}^{r-1} I_k$, $I_k = \left[k \cdot \frac{M}{r} - \frac{1}{2}, k \cdot \frac{M}{r} + \frac{1}{2}\right]$

i.e. $\exists\, 0 \leq k \leq r-1$ s.t. $\left| y - k \cdot \frac{M}{r} \right| \leq \frac{1}{2}$

let us divide by M : $\left| \frac{y}{M} - \frac{k}{r} \right| \leq \frac{1}{2M}$

Here, the choice of $M \sim N^2 \geq r^2$ matters, as this implies: $\left|\frac{y}{M} - \frac{k}{r}\right| \leq \frac{1}{2r^2}$

<u>Task</u>: Find in an effective manner all rational approximations of the form $\frac{k}{r}$ that are at most $\frac{1}{2r^2}$ away from the measured value $\frac{y}{M}$.

Parenthesis: continued fractions

Pick a real number, for example $\frac{263}{189}$

One-digit approximation: 1

So $\frac{263}{189} = 1 + \frac{74}{189} = 1 + \frac{1}{189/74}$

$$\frac{189}{74} = 2 + \frac{41}{74} = 2 + \frac{1}{74/41}$$

So $\frac{263}{189} = 1 + \cfrac{1}{2 + \cfrac{1}{74/41}}$

This leads finally to $\dfrac{263}{189} = 1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{4 + \cfrac{1}{8}}}}}$

$$\left(\frac{74}{41} = 1 + \frac{1}{41/33},\ \frac{41}{33} = 1 + \frac{1}{33/8},\ \frac{33}{8} = 4 + \frac{1}{8} \right)$$

Please note $\dfrac{8}{1} = 7 + \dfrac{1}{1}$ so this could go on forever, but we choose the shortest development.

Note also that if the initial number is irrational then the development is infinite.

<u>Notation:</u> $\dfrac{263}{189} = [1, 2, 1, 1, 4, 8]$

Convergents (toward $\frac{263}{189} \simeq 1{,}391\ldots$)

	value	error
$[1]$	1	$\left\lvert \frac{263}{189} - 1 \right\rvert < \frac{1}{2}$
$[1,2]$	$1 + \frac{1}{2} = \frac{3}{2} = 1{,}5$	$\left\lvert \frac{263}{189} - \frac{3}{2} \right\rvert < \frac{1}{9}$
$[1,2,1]$	$1 + \frac{1}{2 + \frac{1}{1}} = \frac{4}{3} = 1{,}\overline{3}$	$\left\lvert \frac{263}{189} - \frac{4}{3} \right\rvert < \frac{1}{18}$
$[1,2,1,1]$	$\vdots$	$\vdots$
$[1,2,1,1,4]$	$\vdots$	$\vdots$
$[1,2,1,1,4,8]$	$\frac{263}{189}$	0

<u>Legendre</u>: Let α be a real number

Let p, q be so that $\left|\alpha - \frac{p}{q}\right| < \frac{1}{2q^2}$

Then $\frac{p}{q}$ is a convergent of α.

<u>Algorithm</u>:

- Given y, compute the continued fraction of $\frac{y}{M}$
- Look at all convergents: check if any of the denominators is a valid period. If yes, we are done; if not, try again with another measurement.

Note: As $\left|\frac{y}{M} - \frac{k}{r}\right| \leq \frac{1}{2M^2}$, we know by Legendre's lemma that $\frac{k}{r}$ must be a convergent of $\frac{y}{M}$, which justifies the previous algorithm!

Complexity:
- computing the convergents of $\frac{y}{M}$ is actually Euclid's algorithm for computing $\gcd(y, M)$: at most $O(\log_2 M) = O(m)$ steps
- each division costs $O(m^2)$

$\Longrightarrow O(m^3)$ complexity in total.

Circuit for the QFT

$$\mathrm{QFT}\,|x\rangle = \frac{1}{2^{m/2}} \sum_{y=0}^{2^m-1} e^{2\pi i x y / 2^m} \, |y\rangle$$

$\underline{m=1}$: $\mathrm{QFT}\,|x\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{\frac{2\pi i x}{2}}\,|1\rangle\right)$

$$= \frac{1}{\sqrt{2}}\left(|0\rangle + (-1)^x\,|1\rangle\right) = H\,|x\rangle$$

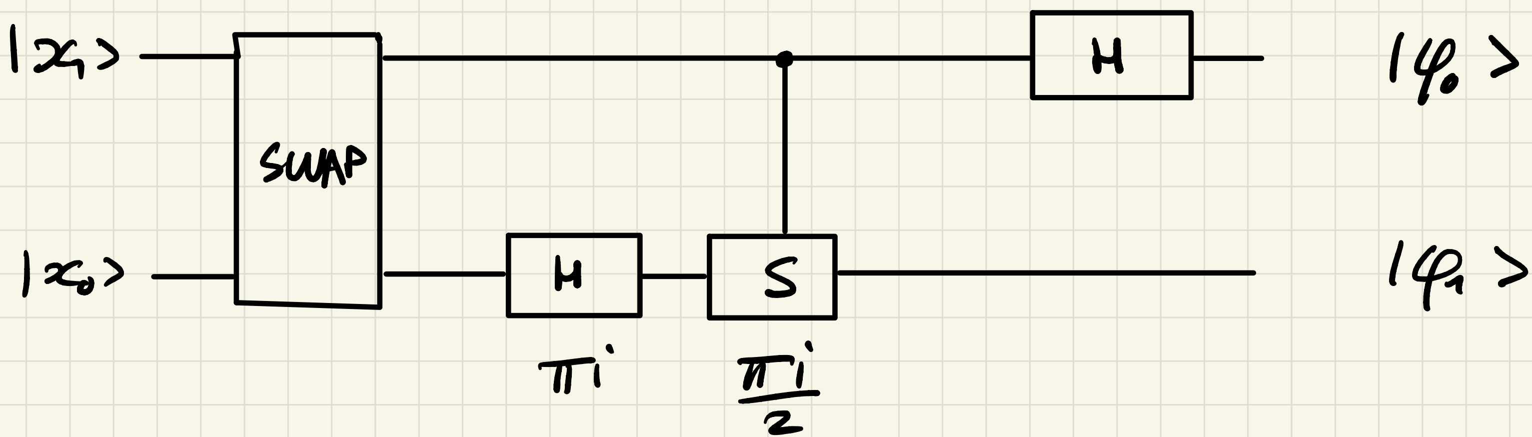
$\underline{m=2}$: $\mathrm{QFT}\,|x\rangle = \frac{1}{2}\left(\underset{\uparrow}{|0\rangle}^{00} + e^{\frac{\pi i x}{2}}\underset{\uparrow}{|1\rangle}^{01} + e^{\pi i x}\underset{\uparrow}{|2\rangle}^{10} + e^{\frac{3\pi i x}{2}}\underset{\uparrow}{|3\rangle}^{11}\right)$

$$= \frac{1}{\sqrt{2}}\left(|0\rangle + e^{\pi i x}\,|1\rangle\right) \otimes \frac{1}{\sqrt{2}}\left(|0\rangle + e^{\frac{\pi i x}{2}}\,|1\rangle\right)$$

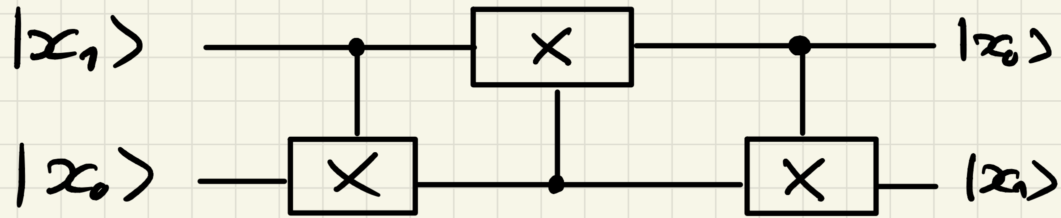
Write $x = (x_1, x_0) = 2x_1 + x_0$ (binary expansion)

$$\Rightarrow QFT\,|x\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{\pi i x_0}|1\rangle\right) \qquad |\varphi_0\rangle$$

$$\otimes \frac{1}{\sqrt{2}}\left(|0\rangle + e^{\pi i x_1 + \frac{\pi i x_0}{2}}|1\rangle\right) \qquad |\varphi_1\rangle$$



SWAP gate:



This procedure generalizes to all values of m (see next slides)

Circuit complexity:

- $3m$ gates for the swap operations
- $m + (m-1) + (m-2) + \ldots + 1 = \frac{m(m+1)}{2} = O(m^2)$ gates for the other part

General m:

Claim: $$QFT\,|x\rangle = \bigotimes_{\ell=1}^{m}\left(\frac{1}{\sqrt{2}}\left(|0\rangle + e^{\frac{2\pi i x}{2^{\ell}}}|1\rangle\right)\right)$$

$m=1$: $$\frac{1}{\sqrt{2}}\left(|0\rangle + e^{\pi i x}|1\rangle\right)$$

$m=2$: $$\frac{1}{\sqrt{2}}\left(|0\rangle + e^{\pi i x}|1\rangle\right) \otimes \frac{1}{\sqrt{2}}\left(|0\rangle + e^{\pi i x/2}|1\rangle\right) \checkmark$$

general m:

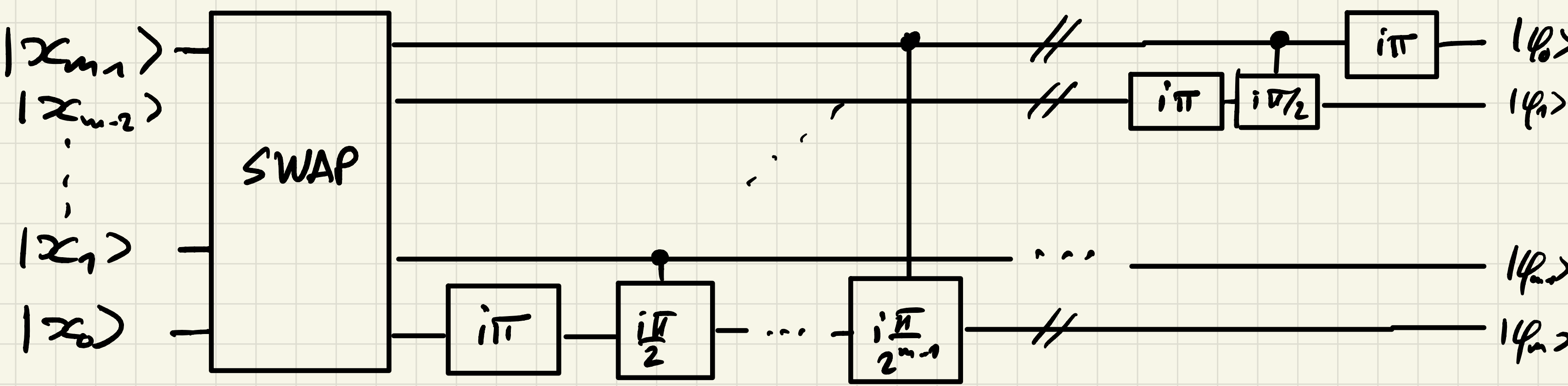
$$\frac{1}{2^{m/2}}\left(|0\rangle + e^{\pi i x}|1\rangle\right)\otimes\left(|0\rangle + e^{\frac{\pi i x}{2}}|1\rangle\right)\otimes \dots \otimes\left(|0\rangle + e^{\frac{\pi i x}{2^{m-1}}}|1\rangle\right)$$

$$x = (x_{m-1}, \dots, x_0) = x_{m-1} 2^{m-1} + \dots + x_1 2 + x_0 \quad (\text{bin. exp})$$

$$\Rightarrow \mathrm{QFT}\,|x\rangle$$

$$= \frac{1}{2^{m/2}} \underbrace{\left(|0\rangle + e^{\pi i x_0}|1\rangle\right)}_{|\psi_0\rangle} \otimes \underbrace{\left(|0\rangle + e^{\pi i x_1 + \frac{\pi i x_0}{2}}|1\rangle\right)}_{|\psi_1\rangle}$$

$$\otimes \dots \otimes \underbrace{\left(|0\rangle + e^{\pi i x_{m-1} + \frac{\pi i x_{m-2}}{2} + \dots + \frac{\pi i x_0}{2^{m-1}}}|1\rangle\right)}_{|\psi_{m-1}\rangle}$$



Check of the claim:

$$QFT\,|x\rangle = \frac{1}{2^{m/2}} \sum_{y=0}^{2^m-1} e^{\frac{2\pi i x y}{2^m}} |y\rangle$$

For $y = y_0 + 2y_1 + \dots + 2^{m-1} y_{m-1}$, the corresponding phase is: $e^{\pi i x \cdot y_{m-1}} \cdot e^{\frac{\pi i x}{2} \cdot y_{m-2}} \cdots e^{\frac{\pi i x}{2^{m-1}} \cdot y_0}$

and one can check for a given sequence of bits $y_{m-1}, \dots, y_0$, the phases match in the above expression and that given by the claim. #