Quantum computation: lecture 6

Plan for the next 3 lectures:

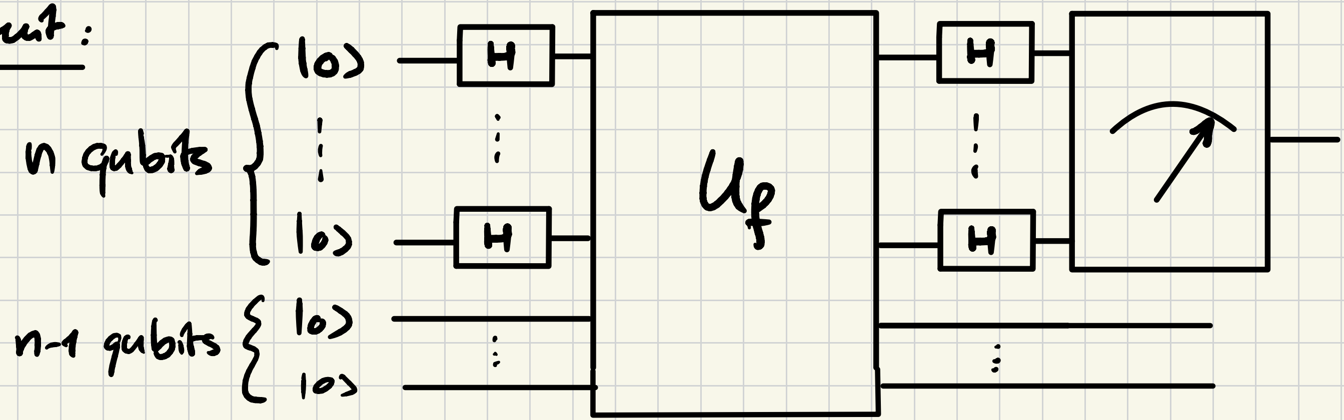
1. Recap of Simon's algorithm
2. Order finding algorithm
   - principle
   - QFT
   - details
3. Shor's factorization algorithm

Recap of Simon's algorithm (in the case $k=1$; $H=\{0,a\}$)

We are given a function $f:\{0,1\}^n \to \{0,1\}^{n-1}$ such that $\exists_{a \neq 0}\, a \in \{0,1\}^n$ with $f(x \oplus a) = f(x)\ \forall x$

The aim is to identify the vector a (= period of f)

Circuit:



Output of the algorithm:

a vector $y \in \{0,1\}^n$ uniformly distributed in the set $H^\perp = \{ z \in \{0,1\}^n : z \cdot a = 0 \}$

$= $ dot product $z_1 a_1 + z_2 a_2 + \ldots + z_n a_n$

(⚠ $\neq$ inner product)

so after sufficiently many runs of the algorithm, it is possible to identify the vector a.

Here is a slight variation of the problem

Given a periodic function $f : \mathbb{Z} \to \mathbb{Z}$, identify the period $r \geq 1$ of the function f (i.e. the smallest value of $r \geq 1$ such that

$$f(x+r) = f(x) \quad \forall x \in \mathbb{Z})$$

Here, $\mathbb{Z}$ is infinite: this adds a difficulty!

In particular, we will be interested in the function f defined as follows:

- Let N be a (large) positive integer

  $a \in \{2 .. N-1\}$ be such that $\gcd(a,N)=1$

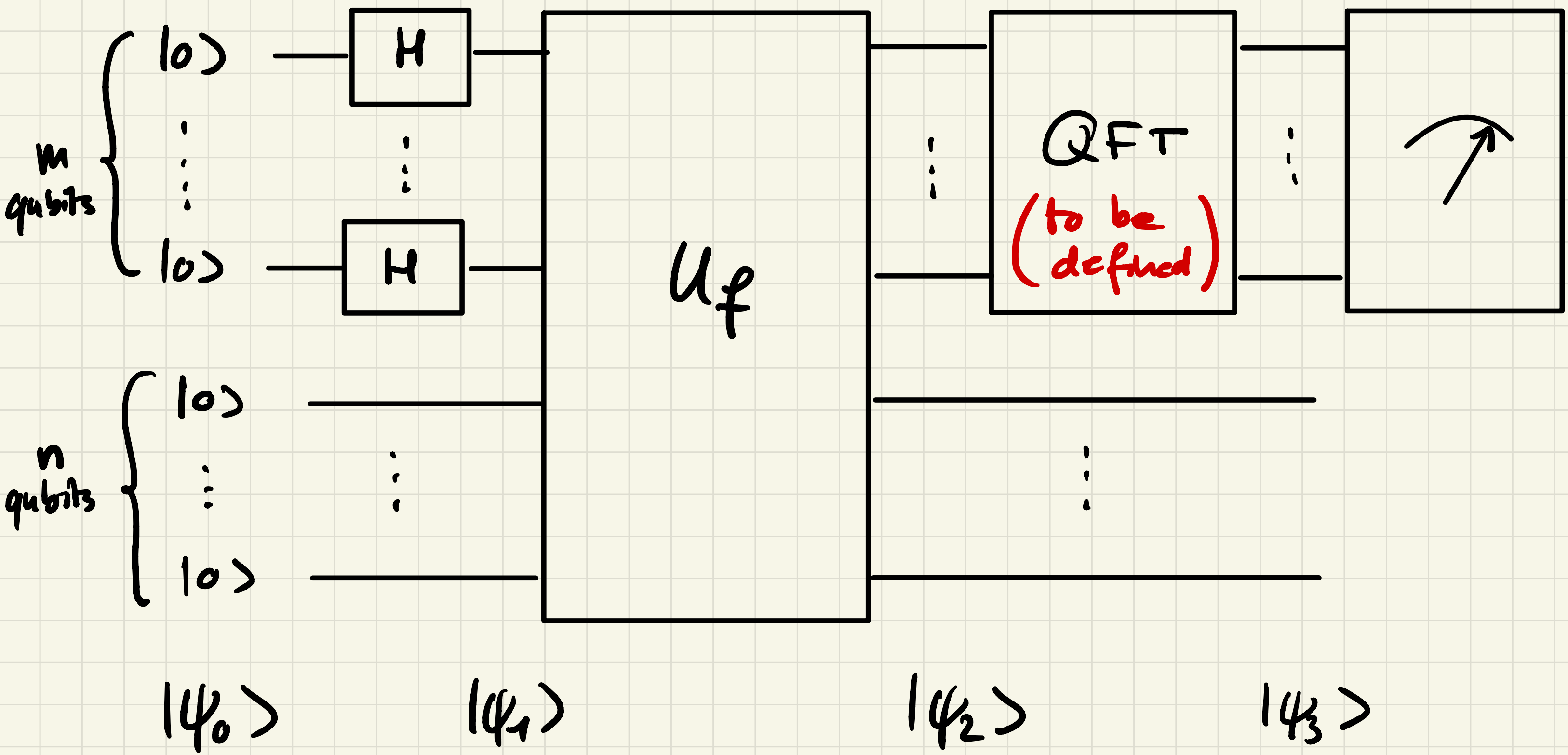
  $$f(x) = a^x \pmod N \qquad x \in \mathbb{Z}$$

- Finding the period of f amounts here to finding its <u>order</u>, i.e. the smallest value of $r \geq 1$ such that $a^r \pmod N = 1$

In order to deal with the fact that $|\mathbb{Z}| = \infty$:

- Let $n = \lceil \log_2(N) \rceil$ be the number of bits needed in the binary decomposition of numbers $\to N-1$
- Let also $M = 2^m$ with $m \geq 1$ be such that $M \simeq N^2$ (so $M >> r$ also, as $r \leq N$) and view $f : \{0..M-1\} \longrightarrow \{0..N-1\}$
- Let us also assume for now (! strange assumption!) that $M = k \cdot r$ for some $k \geq 1$.

Quantum circuit (order finding algorithm)



- $|\psi_0\rangle = \underbrace{|0\ldots0\rangle}_{m \text{ times}} \otimes \underbrace{|0\ldots0\rangle}_{n \text{ times}}$

- $|\psi_1\rangle = \underbrace{H|0\rangle \otimes \ldots \otimes H|0\rangle} \otimes |0\ldots0\rangle$

$$= \frac{1}{2^{m/2}} \sum_{x_1 \ldots x_m \in \{0,1\}} |x_1 \ldots x_m\rangle \otimes |0\ldots0\rangle$$

$\left(\begin{array}{c}\text{short-hand} \\ \text{notation}\end{array}\right) = \dfrac{1}{\sqrt{M}} \displaystyle\sum_{x=0}^{M-1} |x\rangle \otimes |0\ldots0\rangle$

<u>Reminders</u>: - $x_1 \ldots x_m$ = binary representation of x

- $\{|x\rangle,\ 0 \leq x \leq M-1\}$ = computational basis of $\mathbb{C}^M$

Recall also that the oracle U_f acts as:

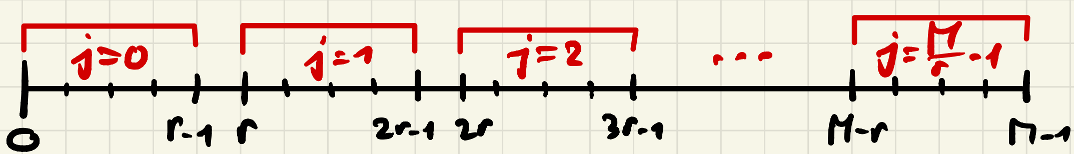
$$U_f\left(|x\rangle \otimes |y\rangle\right) = |x\rangle \otimes |y \oplus f(x)\rangle$$

so $$|\psi_2\rangle = \frac{1}{\sqrt{M}} \sum_{x=0}^{M-1} |x\rangle \otimes |f(x)\rangle$$

$$= \frac{1}{\sqrt{M}} \sum_{x_0=0}^{r-1} \sum_{j=0}^{\frac{M}{r}-1} |x_0 + jr\rangle \otimes |\underbrace{f(x_0+jr)}_{=f(x_0)}\rangle$$

by assumption

(decomposition of the sum:



)

Quantum Fourier Transform

ordinary product!

$$\mathrm{QFT}\,|x\rangle = \frac{1}{\sqrt{M}} \sum_{y=0}^{M-1} \exp\left(\frac{2\pi i x y}{M}\right) |y\rangle$$

This is a unitary operation:

$$\mathrm{QFT}^{\dagger} \cdot \mathrm{QFT}\,|x\rangle = \frac{1}{\sqrt{M}} \sum_{y=0}^{M-1} \exp\left(\frac{2\pi i x y}{M}\right) \mathrm{QFT}^{\dagger}|y\rangle$$

$$= \frac{1}{M} \sum_{y=0}^{M-1} \exp\left(\frac{2\pi i x y}{M}\right) \sum_{z=0}^{M-1} \exp\left(-\frac{2\pi i y z}{M}\right) |z\rangle$$

$$= \sum_{z=0}^{M-1} \Bigg(\underbrace{\frac{1}{M} \sum_{y=0}^{M-1} \exp\left(\frac{2\pi i (x-z) y}{M}\right)}_{=\,\delta_{xz}} \Bigg) |z\rangle = |x\rangle \quad \checkmark$$

We will study more deeply the QFT next week. For now, let us pursue our computation:

$$|\psi_2\rangle = \frac{1}{\sqrt{M}} \sum_{x_0=0}^{r-1} \sum_{j=0}^{\frac{M}{r}-1} |x_0 + jr\rangle \otimes |f(x_0)\rangle$$

so

$$|\psi_3\rangle = (QFT \otimes I_n)|\psi_2\rangle$$

$$= \frac{1}{\sqrt{M}} \sum_{x_0=0}^{r-1} \sum_{j=0}^{\frac{M}{r}-1} \underbrace{QFT|x_0 + jr\rangle}_{= \frac{1}{\sqrt{M}} \sum_{y=0}^{M-1} \exp\left(\frac{2\pi i (x_0 + jr) y}{M}\right) |y\rangle} \otimes |f(x_0)\rangle$$

$$|\psi_3\rangle = \frac{1}{M} \sum_{x_0=0}^{r-1} \sum_{j=0}^{\frac{M}{r}-1} \sum_{y=0}^{M-1} \exp\left(\frac{2\pi i (x_0 + jr) y}{M}\right) |y\rangle \otimes |f(x_0)\rangle$$

$$= \frac{1}{r} \sum_{x_0=0}^{r-1} \sum_{y=0}^{M-1} \exp\left(\frac{2\pi i x_0 y}{M}\right) \underbrace{\left(\frac{r}{M} \sum_{j=0}^{\frac{M}{r}-1} \exp\left(\frac{2\pi i j y}{M/r}\right)\right)}_{= \begin{cases} 1 & \text{if } y = \text{multiple of } \frac{M}{r} \\ 0 & \text{otherwise} \end{cases}} |y\rangle \otimes |f(x_0)\rangle$$

So we should only retain the terms $y = k \cdot \frac{M}{r}$, with $0 \le k \le r-1$:

$$|\psi_3\rangle = \frac{1}{r} \sum_{x_0=0}^{r-1} \sum_{k=0}^{r-1} \exp\left(\frac{2\pi i x_0 k}{r}\right) |k \tfrac{M}{r}\rangle \otimes |f(x_0)\rangle$$

<u>Claim 1</u>: After the measurement of the first m qubits, the state $|\varphi_3\rangle$ is projected uniformly at random onto one of the states $|k \cdot \frac{M}{r}\rangle$ with $0 \leq k \leq r-1$

(please note the similarity with Simon's algorithm)

<u>Claim 2</u>: From this measurement, it is possible to extract the value of r with probability $\geq \frac{1}{4\ln(\ln M)}$.

Once proven the above two claims, we can declare victory, as $O(\ln(\ln M))$ measurements will lead to the result with probability approaching 1 (cf. Simon's algo).

<u>But</u>: All this has been done under the (slightly absurd) simplifying assumption $M = k \cdot r$ for some $k \geq 1$. We still need to deal with this also ...

Proof of Claim 1

Measuring the first m qubits in the computational basis leads to the output state

$$(*) \qquad |\psi_4\rangle = \frac{P_{y_0}|\psi_3\rangle}{\| P_{y_0}|\psi_3\rangle \|} \quad \text{where } P_{y_0} = |y_0\rangle\langle y_0| \otimes I_n$$

$$0 \leq y_0 \leq M-1$$

with probability

$$\text{prob}(y_0) = \langle \psi_3 | P_{y_0} | \psi_3 \rangle$$

[(*) Note that this looks more complex than necessary:
The output state of the first m qubits is simply $|y_0\rangle$]

Let us compute this probability:

$$\mathrm{prob}(y_0) = \langle \psi_3 | P_{y_0} | \psi_3 \rangle$$

$$= \left(\frac{1}{r} \sum_{x_0, k=0}^{r-1} \exp\left(-\frac{2\pi i x_0 k}{r}\right) \langle \tfrac{k\Pi}{r} | \otimes \langle f(x_0) | \right) \left(|y_0\rangle\langle y_0| \otimes I_m \right)$$

$$\cdot \left(\frac{1}{r} \sum_{x_0', k'=0}^{r-1} \exp\left(\frac{2\pi i x_0' k'}{r}\right) | k' \tfrac{\Pi}{r} \rangle \otimes | f(x_0') \rangle \right)$$

$$= \frac{1}{r^2} \sum_{x_0, k, x_0', k_0'=1}^{r-1} \exp\left(\frac{2\pi i (x_0' k' - x_0 k)}{r}\right) \cdot \overbrace{\langle \tfrac{k\Pi}{r} | y_0 \rangle}^{= \delta_{\frac{k\Pi}{r}, y_0}} \cdot \overbrace{\langle y_0 | \tfrac{k'\Pi}{r} \rangle}^{= \delta_{\frac{k'\Pi}{r}, y_0}}$$

$$\cdot \underbrace{\langle f(x_0) | f(x_0') \rangle}_{= \delta_{x_0 x_0'}}$$

(f differs across $0 \le x \le r-1$)

Therefore, among the above four sums over x_0, k, x_0', k' only the one over x_0 remains, so

prob(y_0)

$$= \begin{cases} \frac{1}{r^2} \sum_{x_0=0}^{r-1} 1 = \frac{1}{r} & \text{if } \exists\, 0 \le k \le r-1 \text{ with } y_0 = \frac{kM}{r} \\ 0 & \text{otherwise} \end{cases}$$

proving Claim 1 #

Proof of Claim 2

The output of the circuit is a number $y_0 = \frac{k \cdot M}{r}$ $\left(\text{with } 0 \le k \le r-1\right)$

So $\frac{y_0}{M} = \frac{k}{r}$

known k & r are not known a priori.

- If $\gcd(k, r) = 1$, then simplifying the fraction $\frac{y}{M}$ leads to $\frac{k}{r}$ and looking at the denominator, we find r.

- If $\gcd(k, r) \neq 1$, then this procedure fails.

Note that in practice, we do not know a priori whether $\gcd(k, r) = 1$ or not (because we don't know k & r), but we can still simplify the fraction $\frac{y_0}{M}$ and test whether the resulting denominator is indeed a period of $f(x) = a^x \pmod{N}$ or not (if $\gcd(k, r) \neq 1$, it won't be).

As $0 \leq k \leq r-1$ is uniform, the success probability of this procedure is

$$\text{prob}\left(\gcd(k,r)=1\right) = \frac{\varphi(r)}{r}$$

where $\varphi(r) = \#\{0 \leq k \leq r-1 : \gcd(k,r)=1\}$

$$= \text{Euler's function}$$

<u>Ex</u>: $\varphi(10) = \#\{1,3,7,9\} = 4$

It can be shown that $\varphi(r) \geq \frac{r}{4\ln\ln(r)}$,

so $\text{prob}(\text{success}) \geq \frac{1}{4\ln(\ln r)} \geq \frac{1}{4\ln(\ln N)}$, proving Claim 2

#