Quantum computation: lecture 7

Done last week:

order finding algorithm $\left(\begin{array}{l}\text{smallest value of } r \\ \text{such that } a^r \pmod N = 1\end{array}\right)$

under the strange assumption:

$$M = 2^m \quad \underline{\text{and}} \quad M = k \cdot r$$

Plan for today:

- QFT
- getting rid of → ($M = k \cdot r$)

Definition: The QFT is the unitary transformation on m qubits defined as:

$$QFT\,|x\rangle = \frac{1}{2^{m/2}} \sum_{z=0}^{2^m-1} \exp\left(\frac{2\pi i\, xz}{2^m}\right) |z\rangle$$

where $|x\rangle$ is an element of the computational basis (with $0 \leq x \leq 2^m - 1$)

Note: xz above is the classical product of the numbers x & z

Remark

The QFT is a "true" complex-valued transformation (except in the case $m=1$); its usage may therefore lead to quantum algorithms outperforming classical ones.

Claim

The action of the QFT on a basis vector $|x\rangle$, with $x \in \{0,1\}^m$, may also be rewritten as

$$QFT\,|x\rangle = \bigotimes_{j=1}^{m} \left(\frac{1}{\sqrt{2}} \left(|0\rangle + \exp(2\pi i x / 2^j) |1\rangle \right) \right)$$

Proof of the claim

Let us start from the definition:

$$QFT\,|x\rangle = \frac{1}{2^{m/2}} \sum_{z=0}^{2^m-1} \exp\left(\frac{2\pi i x z}{2^m}\right) |z\rangle$$

Observe that $z = \sum_{j=1}^{m} z_j 2^{m-j}$, where $z_1 .. z_m$ is the binary decomposition of $z \in \{0 .. 2^m-1\}$

(please pay attention that the order chosen for the bits $z_1 .. z_m$ is somehow unconventional here)

So we find successively that:

- $$\exp\left(\frac{2\pi i x z}{2^m}\right) = \exp\left(2\pi i x \sum_{j=1}^{m} z_j \cdot 2^{-j}\right)$$
$$= \prod_{j=1}^{m} \exp\left(2\pi i x z_j 2^{-j}\right)$$

- $$\exp\left(\frac{2\pi i x z}{2^m}\right)|z\rangle = \bigotimes_{j=1}^{m} \exp\left(2\pi i x z_j 2^{-j}\right)|z_j\rangle$$

- $$QFT\,|x\rangle = \bigotimes_{j=1}^{m}\left(\frac{1}{\sqrt{2}} \sum_{z_j \in \{0,1\}} \exp\left(2\pi i x z_j 2^{-j}\right)|z_j\rangle\right)$$
$$= \bigotimes_{j=1}^{m}\left(\frac{1}{\sqrt{2}}\left(|0\rangle + \exp\left(2\pi i x 2^{-j}\right)|1\rangle\right)\right)$$

#

Construction of the circuit for the QFT

$$x = \sum_{k=1}^{m} x_k 2^{m-k}$$ binary decomposition (same conv. as for z)

$$\exp(2\pi i x 2^{-j}) = \exp\left(2\pi i \sum_{k=1}^{m} x_k 2^{m-k-j}\right)$$

Observe that $x_k 2^{m-k-j}$ is an integer for $k \leq m-j$

So $\exp(2\pi i x_k 2^{m-k-j}) = 1$ in this case:

$$\mathrm{QFT}|x\rangle = \bigotimes_{j=1}^{m}\left(\frac{1}{\sqrt{2}}\left(|0\rangle + \exp\left(2\pi i \sum_{k=m-j+1}^{m} x_k 2^{m-k-j}\right)|1\rangle\right)\right)$$

Still written differently:

rotation by $i\pi x_m$

$$QFT\,|x\rangle = \left(\frac{1}{\sqrt{2}} \left(|0\rangle + \exp(2\pi i\, x_m 2^{-1}) |1\rangle \right) \right) \quad [= |\psi_1\rangle]$$

$$\otimes \left(\frac{1}{\sqrt{2}} \left(|0\rangle + \exp(2\pi i\,(x_{m-1} 2^{-1} + x_m 2^{-2})) |1\rangle \right) \right) \quad [= |\psi_2\rangle]$$

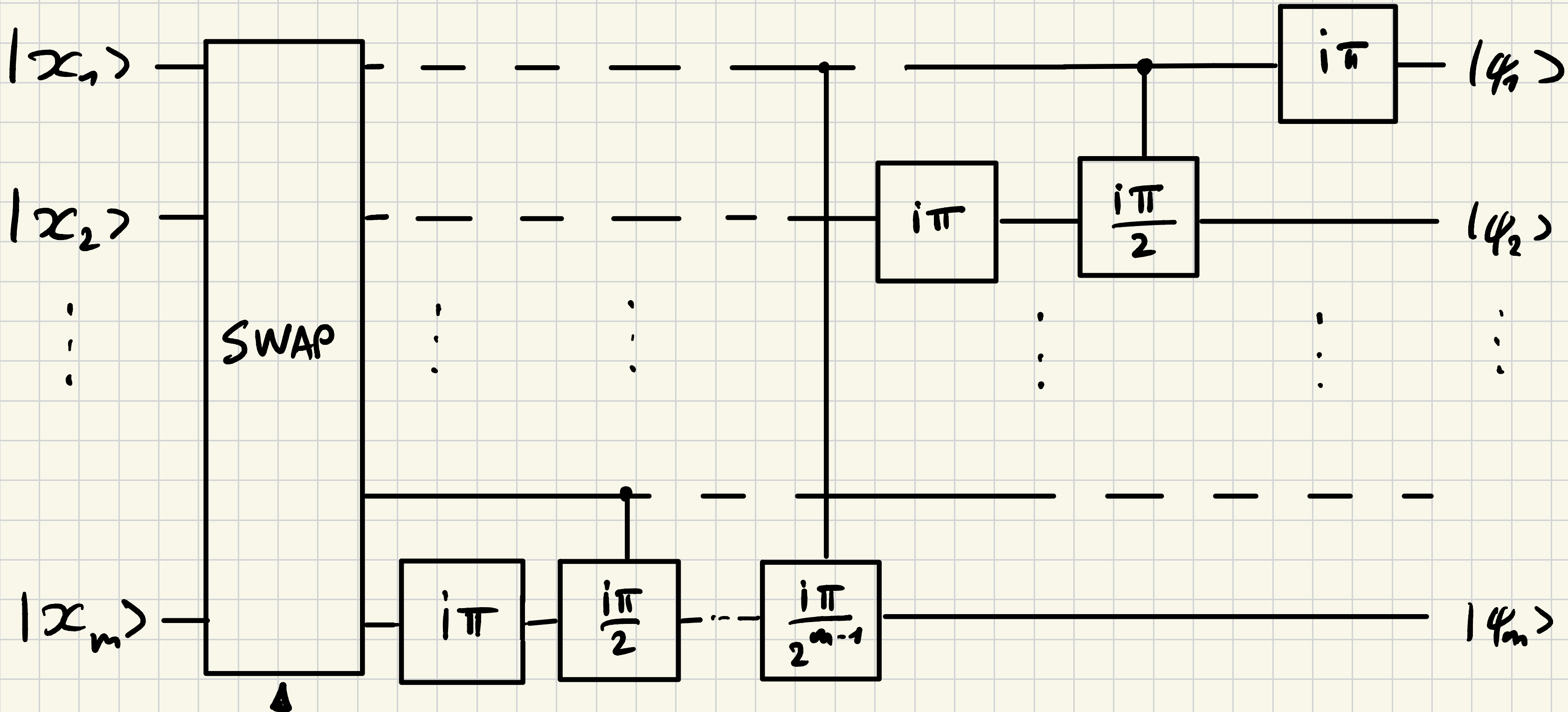
$$\otimes \; \ldots$$

rotation by $i\pi x_{m-1}$

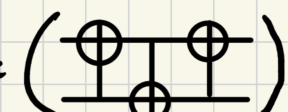
Controlled rotation by $i\pi x_m/2$

Now we can finally draw the circuit!

QFT circuit



generalization of the 2-qubit SWAP gate



Inverse circuit $QFT^\dagger$

$$QFT(|x_1\rangle \otimes \ldots \otimes |x_m\rangle) = |\psi_1\rangle \otimes \ldots \otimes |\psi_m\rangle$$

in short-hand notation: $QFT\,|x\rangle = |\psi\rangle$

As QFT is unitary, it is possible to invert it easily: $QFT^\dagger\,|\psi\rangle = |x\rangle$

with $QFT^\dagger\,|z\rangle = \dfrac{1}{2^{m/2}} \displaystyle\sum_{x=0}^{2^m-1} \exp\left(-\dfrac{2\pi i\, x z}{2^m}\right)|x\rangle$

(z ↑ basis element)

Let us now try to get rid of the weird assumption $M = k \cdot r$ (and see where this goes...)

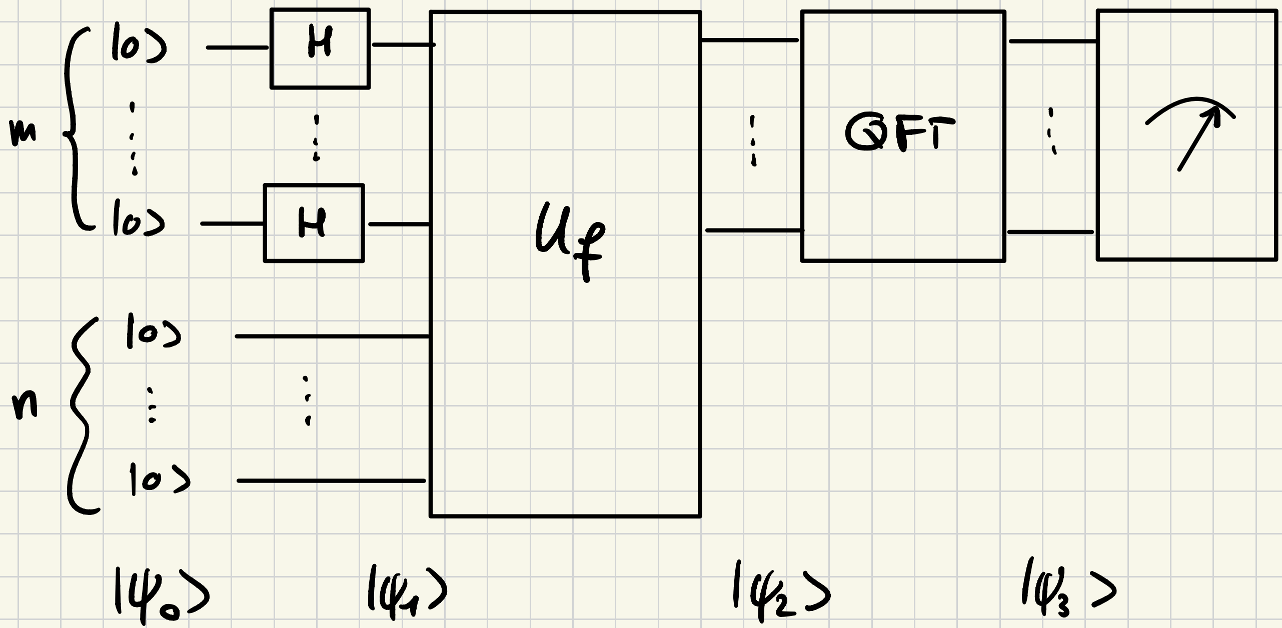
So remember we are looking for the smallest value of $r \geq 1$ s.t. $f(r) = a^r \pmod{N} = 1$

with $2 \leq a \leq N-1$ s.t. $\gcd(a, N) = 1$

and $M = 2^m$, $m \geq 1$ is such that $M \geq N^2$

f viewed as $f: \{0..M-1\} \to \{0..N-1\}$

Let us recall Shor's circuit:



(recall $n = \lceil \log_2(N) \rceil$)

Some things remain the same:

$$|\psi_0\rangle = |0\ldots0\rangle \otimes |0\ldots0\rangle$$

$$|\psi_1\rangle = \frac{1}{\sqrt{M}} \sum_{x=0}^{M-1} |x\rangle \otimes |0\ldots0\rangle$$

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

Define now, for $0 \leq x_0 \leq r-1$:

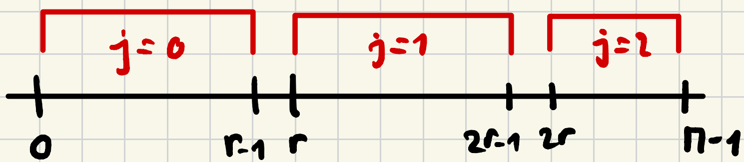
$$A(x_0) = \inf\{ j \geq 1 : x_0 + jr > M-1 \}$$

(when $M = k \cdot r$, $A(x_0) \equiv \frac{M}{r} \quad \forall x_0$)

So we can split the sum, as before:

$$|\varphi_2\rangle = \frac{1}{\sqrt{n}} \sum_{x_0=0}^{r-1} \sum_{j=0}^{A(x_0)-1} |x_0 + jr\rangle \otimes |\underbrace{f(x_0+jr)}_{=f(x_0)}\rangle$$

Ex: $\begin{pmatrix} r=6 \\ n=16 \end{pmatrix}$



$A(x_0=1) = 3$, while $A(x_0=5) = 2$

Let us proceed now and compute $|\varphi_3\rangle$

$$|\psi_3\rangle = \frac{1}{r}\sum_{x_0=0}^{r-1}\sum_{y=0}^{M-1} \exp\left(\frac{2\pi i x_0 y}{M}\right)\underbrace{\left(\frac{r}{M}\sum_{j=0}^{A(x_0)-1}\exp\left(\frac{2\pi i j y}{M/r}\right)\right)}_{\text{this is not anymore 0 or 1 !}} |y\rangle \otimes |f(x_0)\rangle$$

After the measurement of the first m qubits, the state of the first m qubits is $|y_0\rangle$ $(0 \le y_0 \le M-1)$ with probability

$$\text{prob}(y_0) = \langle\psi_3|\, |y_0\rangle\langle y_0| \otimes I_n \,|\psi_3\rangle$$

Let us compute this probability...

$$\mathrm{prob}(y_0) =$$

$$\frac{1}{r}\sum_{x_0=0}^{r-1}\sum_{y=0}^{M-1}\exp\left(-\frac{2\pi i x_0 y}{M}\right)\left(\frac{r}{M}\sum_{j=0}^{A(x_0)-1}\exp\left(-\frac{2\pi i j y}{M/r}\right)\right)\langle y|\otimes\langle f(x_0)|\cdot$$

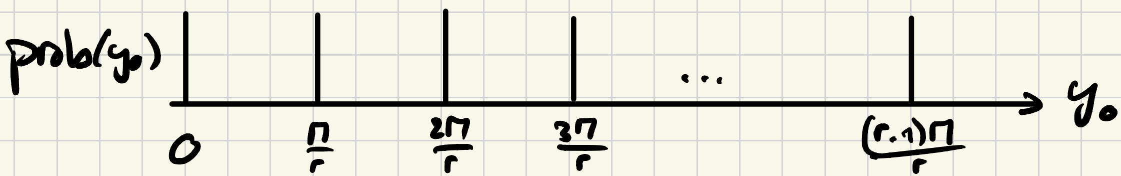
$$\cdot\left(|y_0\rangle\langle y_0|\otimes I_n\right)\cdot \qquad \longrightarrow \delta_{y_0 y}\,\delta_{y_0 y'}\,\delta_{x_0 x_0'}$$

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

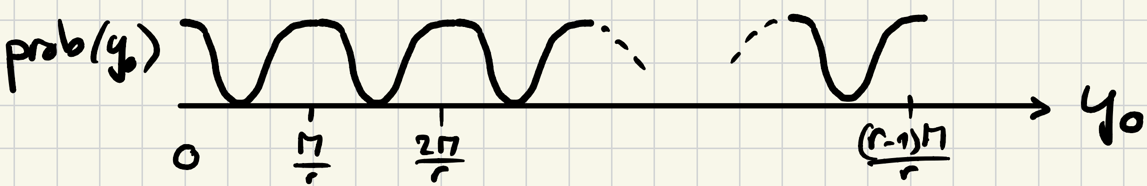
$$= \frac{1}{r^2}\sum_{x_0=0}^{r-1}\left|\frac{r}{M}\sum_{j=0}^{A(x_0)-1}\exp\left(\frac{2\pi i j y_0}{M/r}\right)\right|^2$$

$$\text{prob}(y_0) = \frac{1}{r^2} \sum_{x_0=0}^{r-1} \underbrace{\left| \frac{r}{M} \sum_{j=0}^{A(x_0)-1} \exp\left(\frac{2\pi i\, j\, y_0}{M/r} \right) \right|^2}$$

In the case $M = k \cdot r$, this expression is equal to 1 for y_0 multiple of $\frac{M}{r}$, and 0 otherwise:



In the general case, the situation is as follows:

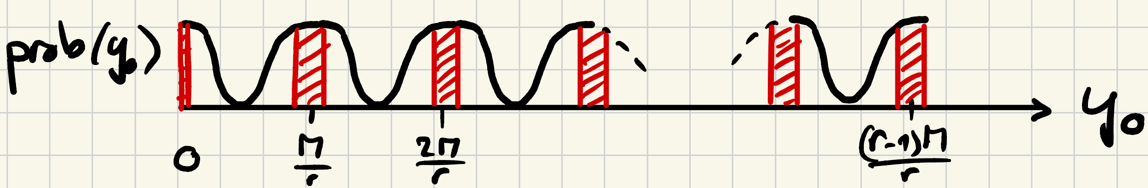


So the output y_0 of the circuit is not necessarily a multiple of $\frac{M}{r}$ anymore.

Nevertheless, we can show the following:

> Let $I = \bigcup_{k=0}^{r-1} I_k$ with $I_k = \left[k\frac{M}{r} - \frac{1}{2}, k\frac{M}{r} + \frac{1}{2} \right]$
>
> Then $\text{prob}(y_0 \in I) \geq \frac{2}{5}$

NB: $|I_k| = 1 \quad \forall k$



Plan for next week:

- last details for the order finding algorithm:
  - how to recover r from $y_0 \in I$?
    (→ convergents)
  - how to build the oracle gate U_f ?
    (→ modular exponential)
- Shor's factoring algorithm