21/11/24

Quantum Fourier Transform

I - Discrete Fourier transform

We give a refresher on the discrete Fourier transform (DFT)

<u>Def</u>: for $N \in \mathbb{N}^*$, $\mathcal{F}^c_N$ defined by

$$\forall 0 \leq j \leq N-1, \quad (\mathcal{F}^c_N x)_j = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2i\pi \frac{jk}{N}} x_k \quad \text{where } x = \begin{bmatrix} x_0 \\ \vdots \\ x_{N-1} \end{bmatrix}.$$

<u>Remark</u>: the DFT in the canonical basis is the matrix

$$F_N = \frac{1}{\sqrt{N}} \begin{bmatrix} 1 & \cdots & & 1 \\ 1 & \omega & \omega^2 \cdots & \omega^{N-1} \\ 1 & \omega^2 & \omega^4 \cdots & \omega^{2(N-1)} \\ \vdots & \vdots & \vdots & \vdots \\ 1 & \omega^{N-1} & \cdots & \omega^{(N-1)(N-1)} \end{bmatrix} \quad \text{where } \omega = e^{\frac{2i\pi}{N}}.$$

- $$(F_N^* F_N)_{ij} = \frac{1}{N} \sum_{k=0}^{N-1} (\omega^*)^{ik} \omega^{kj} = \begin{cases} 1 & \text{if } i=j \\ \frac{1}{N}\frac{\omega^N - 1}{\omega - 1} = 0 & \text{if } i \neq j. \end{cases}$$

  $\Rightarrow \mathcal{F}^c_N$ is an isometry.

- for $x \in \mathbb{C}^N$, $F_N x$ can be performed in $O(N \log N)$ multiplications (better than $O(N^2)$ of a naive matrix-vector multiplication).

II - Reminder on quantum computing

* quantum computer stores a state $|\psi\rangle \in \bigotimes_{i=1}^{n} \mathbb{C}^2 \simeq \mathbb{C}^{2^n}$.
  where $|\psi\rangle$ is normalised (i.e. $\| \psi \|_2 = 1$).
- computational basis = canonical basis of $\bigotimes_{i=1}^{n} \mathbb{C}^2$

$= \{ \underbrace{e_{i_1} \otimes \cdots \otimes e_{i_n}}_{= |i_1 \cdots i_n\rangle} , \ i_k \in \{0,1\} \}$

- $|\psi\rangle$ in the computational basis: $|\psi\rangle = \sum_{i_k \in \{0,1\}} c_{i_1 \cdots i_n} |i_1 \cdots i_n\rangle$ with $\sum_{i_k} |c_{i_k}|^2 = 1$.

→ notation: by writing $j \in [\![0, 2^n - 1]\!]$ in binary, we can write

$$|\psi\rangle = \sum_{j=0}^{2^n-1} \alpha_j |j\rangle \quad \text{where } \alpha_j = c_{i_1 \cdots i_n} \text{ for } j = \sum_{k=1}^{n} 2^{k-1} i_k.$$

* measurement:

- $|\psi\rangle$ "collapses" on the computational basis i.e.

measurement operator → $M|\psi\rangle = |i_1 \cdots i_n\rangle$ with probability $|c_{i_1 \cdots i_n}|^2$.

- partial measurement: suppose $|\psi\rangle = c_0 |0\rangle \otimes |\Phi_0\rangle + c_1 |1\rangle \otimes |\Phi_1\rangle$ where $|\Phi_0\rangle, |\Phi_1\rangle \in \bigotimes_{i=1}^{n-1} \mathbb{C}^2$, then the partial measurement over the first copy of $\mathbb{C}^2$ is the operator

$$M_1 |\psi\rangle = \begin{cases} |0\rangle \otimes |\Phi_0\rangle & \text{with probability } |c_0|^2 \\ |1\rangle \otimes |\Phi_1\rangle & \text{———————— } |c_1|^2. \end{cases}$$

* "computation" on a quantum computer
= unitary transformation U (to preserve the norm).

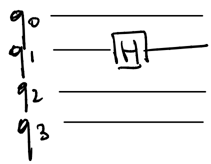
- particular transformations:
  - * 1-qbit gates i.e. acting on $\mathbb{C}^2$
    → examples: Pauli gates X, Y, Z
    Hadamard $H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$
    phase S
    ⋮
  - * 2-qbit gates: acting on $\mathbb{C}^2 \otimes \mathbb{C}^2 = \mathbb{C}^4$
    → examples: CNOT $= \begin{array}{c} 00 \\ 01 \\ 10 \\ 11 \end{array} \begin{bmatrix} 1 & & & \\ & 1 & & \\ & & 0 & 1 \\ & & 1 & 0 \end{bmatrix}$ $\quad CU = \begin{bmatrix} I_2 & \\ & U \end{bmatrix}$

    SWAP $= \begin{array}{c} 00 \\ 01 \\ 10 \\ 11 \end{array} \begin{bmatrix} 1 & & & \\ & 0 & 1 & \\ & 1 & 0 & \\ & & & 1 \end{bmatrix}$.

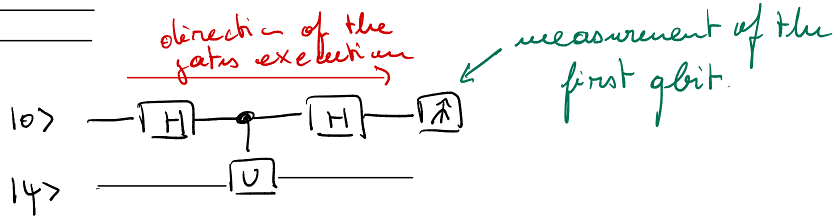
* <u>circuit</u>: 1 qbit or 2 qbit gates can be applied on $\bigotimes_{i=1}^{\sim} \mathbb{C}^2$ by acting on the relevant copies of $\mathbb{C}^2$.

Mathematically, if H is applied on the k-th copy then the operation on $\bigotimes_{i=1}^{\sim} \mathbb{C}^2$ is $\underbrace{I_{k-1}}_{\text{identity on } \mathbb{C}^{2^k}} \otimes H \otimes \underbrace{I_{n-k-1}}_{\text{identity on } \mathbb{C}^{2^{n-k-1}}}$

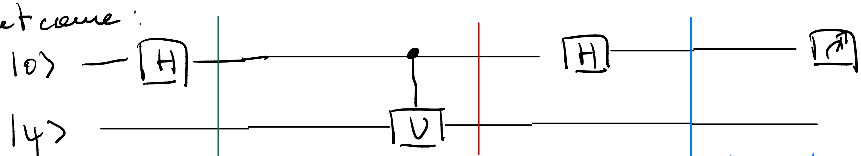
This operation can be represented in a circuit (here $k=2$, $n=4$)



Example:



* outcome:



$\frac{1}{\sqrt{2}}(|0\rangle \otimes |\psi\rangle + |1\rangle \otimes |\psi\rangle)$ $\quad$ $\frac{1}{\sqrt{2}}(|0\rangle \otimes |\psi\rangle + |1\rangle \otimes U|\psi\rangle$ $\quad$ $\frac{1}{2}(|0\rangle \otimes (|\psi\rangle + U|\psi\rangle) + |1\rangle \otimes (|\psi\rangle - U|\psi\rangle))$

$\to$ if $U|\psi\rangle = e^{i\theta}|\psi\rangle$, then we get the state $|1\rangle \otimes |\psi\rangle$ with probability $\left|\frac{1}{2}(1-e^{i\theta})\right|^2 = \sin^2\frac{\theta}{2}$.

$\to$ suppose we have $\theta \simeq 0$ and we want to estimate θ: then $\theta = \pm \arcsin\sqrt{p(1)}$. Then using the empiric estima for $\frac{\#|1\rangle}{N_{samples}}$ has a variance $\frac{p(1)(1-p(1))}{N_{samples}}$

$\Rightarrow N_{samples} \gg \frac{1}{p(1)}$ s.t. we have an accurate estimation of $p(1)$.

III - Quantum Fourier transform

We define the QFT on a quantum state as the unitary transformation applying the DFT on the coefficients of $|\psi\rangle$ in its computational basis.

Definition (QFT)

The QFT_{2^n} is the unitary transformation such that for any $|\psi\rangle \in \bigotimes_{i=1}^{n} \mathbb{C}^2$, $|\psi\rangle = \sum_{j=0}^{2^n-1} c_j |j\rangle$,

$$QFT_{2^n}|\psi\rangle = \frac{1}{\sqrt{2^n}} \sum_{j,k=0}^{2^n-1} c_j \, e^{\frac{2i\pi}{2^n} jk} |k\rangle.$$

Remark: for $|0\rangle \in \bigotimes_{i=1}^{n} \mathbb{C}^2$, then $QFT_{2^n}|0\rangle = \frac{1}{2^n} \sum_{j=0}^{2^n-1} |j\rangle$

$$= (H \otimes \cdots \otimes H)|0\rangle.$$

Towards an implementation of the QFT

Let $j = j_{n-1} 2^{n-1} + \cdots + j_0 2^0$, then $\frac{j}{2^n} = \frac{j_{n-1}}{2} + \frac{j_{n-2}}{2^2} + \cdots + \frac{j_0}{2^n}$,

thus

$$\frac{kj}{2^n} = k_{n-1} 2^{n-1} \frac{j}{2^n} + k_{n-2} 2^{n-2} \frac{j}{2^n} + \cdots + k_0 \frac{j}{2^n}$$

$$= k_{n-1} \left(2^{n-2} j_{n-1} + \cdots + j_1 + \frac{j_0}{2}\right)$$

$$+ k_{n-2} \left(2^{n-3} j_{n-1} + \cdots + j_2 + \frac{j_1}{2} + \frac{j_0}{4}\right)$$

$$\vdots$$

$$+ k_0 \left(\frac{j_{n-1}}{2} + \frac{j_{n-2}}{2^2} + \cdots + \frac{j_0}{2^n}\right)$$

Hence after exponentiation:

$$\exp\left(2i\pi \frac{kj}{2^n}\right) = \exp\left(2i\pi \left[k_{n-1} \frac{j_0}{2} + k_{n-2}\left(\frac{j_1}{2} + \frac{j_0}{4}\right) + \cdots + k_0\left(\frac{j_{n-1}}{2} + \frac{j_{n-2}}{2^2} + \cdots + \frac{j_0}{2^n}\right)\right]\right)$$

Injecting in the expression of QFT_{2^n}, we have

$$QFT_{2^n}|j\rangle = \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} \exp\left(2i\pi \frac{kj}{2^n}\right) |k\rangle$$

$$= \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} \exp\left(2i\pi \, k_0 \left(\frac{j_{n-1}}{2} + \frac{j_{n-2}}{2^2} + \cdots + \frac{j_0}{2^n}\right)\right)$$

$$\cdots \exp\left(2i\pi\, k_{n-2}\left(\frac{j_1}{2}+\frac{j_0}{4}\right)\right)\exp\left(2i\pi k_{n-1}\frac{j_0}{2}\right)|k\rangle$$

Using that $|k\rangle = |k_0\cdots k_{n-1}\rangle = |k_0\rangle\otimes|k_1\rangle\otimes\cdots\otimes|k_{n-1}\rangle$, we have:

$$QFT_{2^n}|j\rangle = \frac{1}{\sqrt{2^n}}\sum_{k=0}^{2^n-1}\exp\left(2i\pi\, k_0\left(\frac{j_{n-1}}{2}+\frac{j_{n-2}}{2^2}+\cdots+\frac{j_0}{2^n}\right)\right)|k_0\rangle$$
$$\otimes\cdots\otimes\exp\left(2i\pi\, k_{n-2}\left(\frac{j_1}{2}+\frac{j_0}{4}\right)\right)|k_{n-2}\rangle$$
$$\otimes\exp\left(2i\pi\, k_{n-1}\left(\frac{j_0}{2}\right)\right)|k_{n-1}\rangle.$$

$$=\sum_{k_0\cdots k_{n-1}=0}^{1}\frac{1}{\sqrt{2}}\left(|0\rangle+\exp\left(i\pi\left(j_{n-1}+\frac{j_{n-2}}{2}+\cdots+\frac{j_0}{2^{n-1}}\right)\right)|1\rangle\right)$$
$$\otimes\cdots\otimes\frac{1}{\sqrt{2}}\left(|0\rangle+\exp\left(i\pi\left(j_1+\frac{j_0}{2}\right)\right)|1\rangle\right)\otimes\frac{1}{\sqrt{2}}\left(|0\rangle+\exp(i\pi j_0)|1\rangle\right).$$

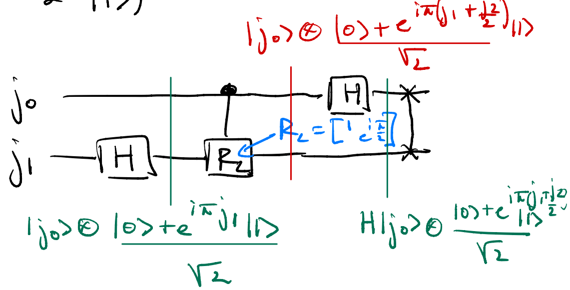
For $n=1$: $\frac{1}{\sqrt2}\left(|0\rangle+e^{i\pi j_0}|1\rangle\right)$: $*\ |j_0\rangle=0 \Rightarrow \frac{1}{\sqrt2}\left(|0\rangle+e^{i\pi j_0}|1\rangle\right)=\frac{1}{\sqrt2}(|0\rangle+|1\rangle)$

$*\ |j_0\rangle=1 \Rightarrow \frac{1}{\sqrt2}\left(|0\rangle+e^{i\pi j_0}|1\rangle\right)=\frac{1}{\sqrt2}(|0\rangle-|1\rangle)$

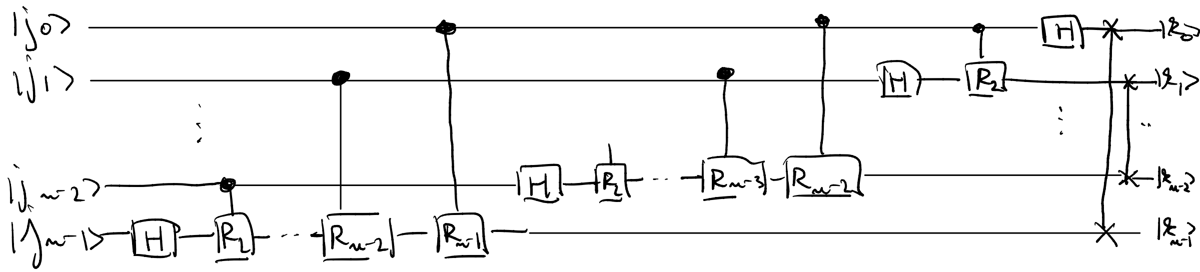
$$\Rightarrow \frac{1}{\sqrt2}\left(|0\rangle+e^{i\pi j_0}|1\rangle\right)=H|j_0\rangle.$$

For $n=2$: $\frac{1}{\sqrt2}\left(|0\rangle+e^{i\pi\left(j_1+\frac{j_0}{2}\right)}|1\rangle\right)$

Corresponding circuit:



For general n:



$\to$ number of gates:

n Hadamard + $\underbrace{[(n-2)+(n-3)+\dots+1]}_{=\frac{(n-2)(n-1)}{2}}$ controlled gates

$+ \lfloor \frac{n}{2} \rfloor$ SWAP $= \mathcal{O}(n^2)$ gates.

This means that the complexity of the QFT is of order $\underline{\mathcal{O}((\log N)^2)}$.

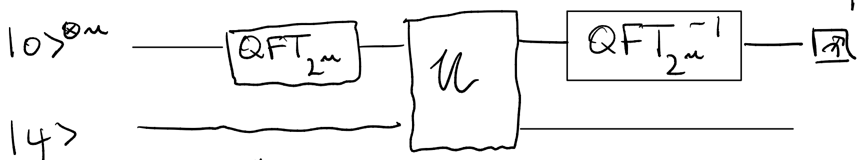
<u>Remark</u>: the same construction holds by substituting $e^{2i\pi/2^n}$ by any other 2^n-th root of the unity. For -1, the circuit simplifies to $H \otimes \dots \otimes H$.

IV - Quantum phase estimation

<u>Assumption</u>: let $U|\psi\rangle = e^{2i\pi\theta}|\psi\rangle$ with $\theta = \frac{k}{2^n}$ for $k \in [\![0, 2^n-1]\!]$.

$|\psi\rangle \in \bigotimes_{i=1}^{m} \mathbb{C}^2$

Consider the circuit



where $\mathcal{U} = \sum_{j=0}^{2^n-1} |j\rangle\langle j| \otimes U^j$

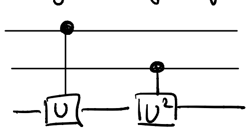
One can check that
$$\mathcal{U}^* \mathcal{U} = \left(\sum_{j=0}^{2^n-1} |j\rangle\langle j| \otimes (U^*)^j\right)\left(\sum_{k=0}^{2^n-1} |k\rangle\langle k| \otimes U^k\right)$$
$$= \sum_{j,k} |j\rangle\underbrace{\langle j|k\rangle}_{=\delta_{jk}}\langle k| \otimes (U^*)^j U^k$$
$$= \sum_{j=0}^{2^n-1} |j\rangle\langle j| \otimes I_m = I_n \otimes I_m.$$

Thus $\mathcal{U}$ is indeed <u>unitary</u>.

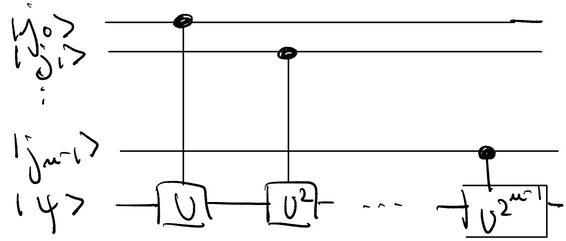
Now we have
$$\mathcal{U} = \sum_{j=0}^{2^n-1} |j\rangle\langle j| \otimes U^j = \sum_{j_0 \dots j_{n-1}=0}^{1} |j_0\rangle\langle j_0| \otimes \dots \otimes |j_{n-1}\rangle\langle j_{n-1}| \otimes U^{j_0+2j_1+\dots+2^{n-1}j_{n-1}}$$

$\to$ for $n=1$: $\mathcal{U} = |j_0\rangle\langle j_0| \otimes U^{j_0} = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes U$
$= $ Control-U.

$\to$ for $n=2$: $\mathcal{U} = |j_0\rangle\langle j_0| \otimes |j_1\rangle\langle j_1| \otimes (U^{j_0} U^{2j_1})$

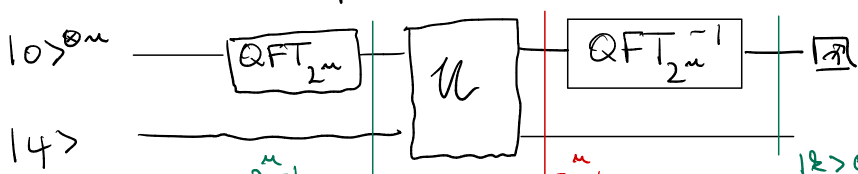
$=$ 

The transformation $\mathcal{U}$ can be efficiently represented using controlled gates:



$\Rightarrow$ # gates = n controlled gates.

Thus the output of the circuit is given by:



$$\frac{1}{\sqrt{2^n}}\sum_{j=0}^{2^n-1}|j\rangle\otimes|\psi\rangle$$

$$\frac{1}{\sqrt{2^n}}\sum_{j=0}^{2^n-1}|j\rangle\otimes\underbrace{U^j|\psi\rangle}_{=e^{2i\pi j\theta}|\psi\rangle}$$

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

$$|k\rangle\otimes|\psi\rangle.$$

This means that the measure is deterministic and we need a single measurement to retrieve the value k and thus $\theta=\frac{k}{2^n}$.

Cost of the eigenvalue estimation: $\mathcal{O}(n^2)=\mathcal{O}((\log N)^2)$ gates.

Limitations:

* $\theta \simeq \frac{k}{2^n}$: then instead of having a Dirac at $|k\rangle$, we have a distribution of values centred at k.
* if $|\psi\rangle$ is not an eigenfunction:
  suppose that $|\psi\rangle=\sum_{j=0}^{2^n-1}c_j|\psi_j\rangle$ where $U|\psi_j\rangle=e^{2i\pi\theta_j}|\psi_j\rangle$.
  Suppose that $\theta_j=\frac{k_j}{2^n}$, $k_j\in[0,2^n]$, with $0<\theta_0\leq\cdots\leq\theta_{2^n-1}<1$
  by linearity:
  $$QPE(|0\rangle^{\otimes n}\otimes|\psi\rangle)=\sum_{j=0}^{2^n-1}c_j|k_j\rangle\otimes|\psi_j\rangle$$
  $\Rightarrow$ we have the lowest eigenvalue $2\pi\frac{k_0}{2^n}$ with probability $|c_0|^2$.

V - HHL algorithm

The goal of the HHL algorithm is to solve a linear system $Ax = b$ where A is Hermitian.

The idea is to decompose A in its eigenvalue decomposition $A = \sum_{i=0}^{2^n-1} \lambda_i |v_i\rangle\langle v_i|$

and $b = \sum_{i=0}^{2^n-1} \beta_i |v_i\rangle$.

Assumption:

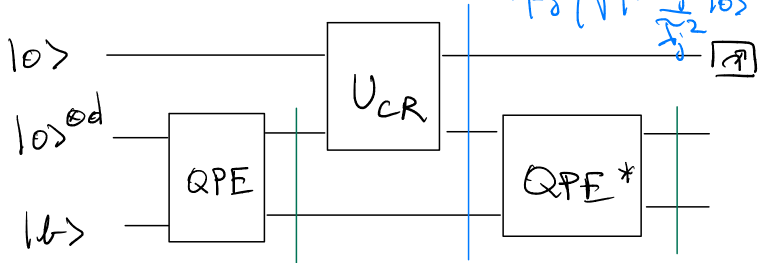
(i) $\sum_{i=0}^{2^n-1} |\beta_i|^2 = 1$ (i.e. $|b\rangle$ is a quantum state)

(ii) $0 < \lambda_0 \leq \dots \leq \lambda_{2^n-1} \leq 1$ are exactly representable on d bits.

$$\sum \beta_j \left(\sqrt{1 - \frac{C_j^2}{\tilde{\lambda}_j^2}} |0\rangle + \frac{C}{\tilde{\lambda}_j} |1\rangle \right) \otimes |\lambda_j\rangle \otimes |v_j\rangle$$

prescribed by user

approximation of λ_j



$$\sum \beta_j |\lambda_j\rangle \otimes |v_j\rangle$$

$$\sum \beta_j \left(\sqrt{1 - \frac{C^2}{\tilde{\lambda}_j^2}} |0\rangle + \frac{C}{\tilde{\lambda}_j} |1\rangle \right) \otimes |0\rangle^{\otimes d} \otimes |v_j\rangle$$

If the 1^{st} qbit measured is $|1\rangle$, then we have the state

$$\frac{\sum_{j=0}^{2^n-1} \frac{\beta_j}{\tilde{\lambda}_j} |0\rangle^{\otimes d} \otimes |v_j\rangle}{\left\| \sum_{j=0}^{2^n-1} \frac{\beta_j}{\tilde{\lambda}_j} |0\rangle^{\otimes d} \otimes |v_j\rangle \right\|} = \frac{|0\rangle^{\otimes d} \otimes \sum_{j=0}^{2^n-1} \frac{\beta_j}{\tilde{\lambda}_j} |v_j\rangle}{\left\| |0\rangle^{\otimes d} \otimes \sum_{j=0}^{2^n-1} \frac{\beta_j}{\tilde{\lambda}_j} |v_j\rangle \right\|} = \frac{|0\rangle^{\otimes d} \otimes x}{\|x\|} =: |0\rangle^{\otimes d} \otimes |x\rangle$$

We thus obtain x up to a normalisation constant. This constant can be retrieved by noticing that the probability to get $|1\rangle$ in the 1^{st} qbit is equal to $\sum_{j=0}^{2^n-1} C^2 \frac{\beta_j^2}{\tilde{\lambda}_j^2} = C^2 \|x\|^2 =: P(|1\rangle)$

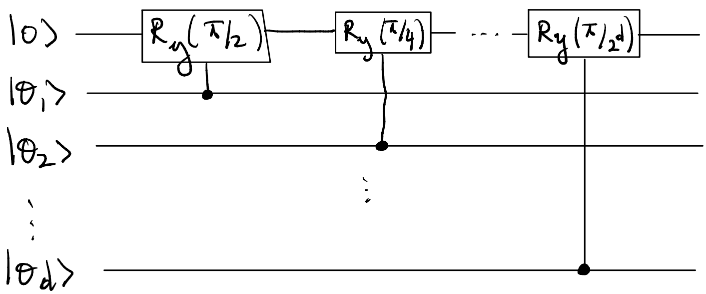
Thus $x = \frac{|x\rangle}{C} P(|1\rangle)$.

Implementation of U_{CR}:

U_{CR} is defined as: $U_{CR}|0\rangle\otimes|\theta\rangle = (\cos(\pi\theta)|0\rangle + \sin(\pi\theta)|1\rangle)\otimes|\theta\rangle$

where $\theta = 0.\theta_1\cdots\theta_d$ in binary.

$\rightarrow$ U_{CR} is implementable by



$|0\rangle$

as $\cos(\pi\theta)|0\rangle + \sin(\pi\theta)|1\rangle = \begin{bmatrix}\cos(\pi\theta) & -\sin\pi\theta \\ \sin(\pi\theta) & \cos(\pi\theta)\end{bmatrix}|0\rangle = \prod_{j=1}^{d}\begin{bmatrix}\cos(\pi\theta/2^j) & -\sin\left(\frac{\pi\theta}{2^j}\right) \\ \sin(\pi\theta/2^j) & \cos\left(\frac{\pi\theta}{2^j}\right)\end{bmatrix}|0\rangle$

Back to HHL: for HHL, we need $\sin(\pi\theta_j) = \frac{C}{\lambda_j}$ for all $j = 0,\dots,2^n-1$

$$\iff \theta_j = \frac{1}{\pi}\arctan\left(\frac{C}{\lambda_j}\right).$$

$\rightarrow$ this means that $C \leq \lambda_0 = \min_{0\leq j\leq 2^n-1}\lambda_j$

Remark: the computation of the angles is only approximate as λ_j and θ_j are represented on d-bits.

Remark: as $p(|1\rangle) = C^2\|x\|^2$ we want to pick $C = \lambda_0$ (i.e. the largest possible)

This means that $p(|1\rangle) = \lambda_0^2\|x\|^2 = \lambda_0^2\|A^{-1}b\| = O\left(\frac{\lambda_0^2}{\lambda_{2^n-1}^2}\right) = \frac{1}{(\mathrm{cond}_2 A)^2}$

$\rightarrow$ if $\mathrm{cond}_2 A \gg 1$, then $p(|1\rangle)$ is very small

This issue can be alleviated using the amplitude amplification as we have $U_{HHL}|0\rangle^{\otimes(d+1)}\otimes|b\rangle = \sqrt{p(1)}\,|1\rangle\otimes|\psi_{good}\rangle + \sqrt{1-p(1)^2}\,|0\rangle\otimes|\psi_{bad}\rangle$.

VI – Period search problem

① Simon's problem

In this problem, we have an oracle (i.e. a function) $f : \{0,1\}^n \to \{0,1\}^n$ such that $\exists s \in \{0,1\}^n : \forall x \neq y \quad f(x) = f(y) \iff y = x \oplus s$

$\iff y_i = x_i \oplus s_i \quad \forall_{1 \leq i \leq n}$

$a \oplus b = a + b \bmod 2.$

The period s is unknown and we would like to design an algorithm to find the period s.

[Note: there is only a pair (x,y) s.t. $f(x) = f(y)$ as $x = x \oplus s \oplus s = y \oplus s$]

→ the function is different than in the Deutsch–Jozsa algorithm, as the output of the function in DJ is in $\{0,1\}$.

We suppose that we have a quantum gate acting on $\bigotimes_{i=1}^{n} \mathbb{C}^2 \otimes \bigotimes_{i=1}^{n} \mathbb{C}^2$

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

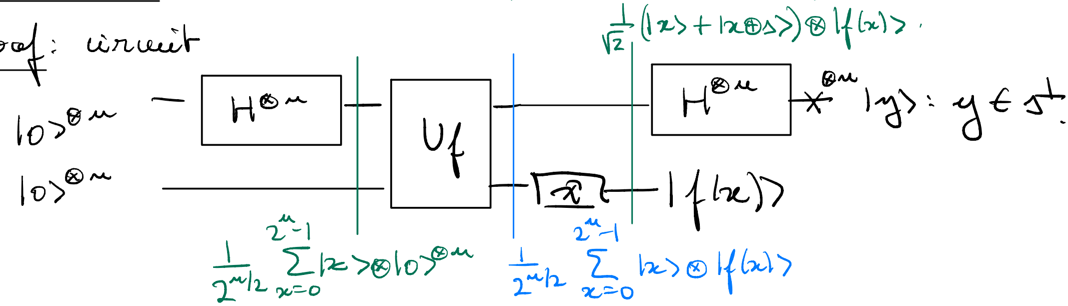
We check that $U_f^* = U_f = U_f^{-1}$: $U_f^2 |x\rangle \otimes |w\rangle = |x\rangle \otimes \underbrace{|w \oplus f(x) \oplus f(x)\rangle}_{= |w\rangle}$

thus U_f is indeed a unitary transformation.

Classical cost : $\mathcal{O}(2^{n/2})$ to determine s.

Quantum cost : $\mathcal{O}(n)$ [⇒ exponential advantage]

proof: circuit



By a direct calculation:

$$\frac{1}{\sqrt{2}} H^{\otimes n}|x\rangle + H^{\otimes n}|x \oplus s\rangle = \frac{1}{\sqrt{2}}\left(\bigotimes_{i=1}^{n} \left(\frac{|0\rangle + (-1)^{x_i}|1\rangle}{\sqrt{2}} \right) + \bigotimes_{i=1}^{n} \frac{|0\rangle + (-1)^{x_i + s_i}|1\rangle}{\sqrt{2}} \right)$$

$$= \frac{1}{2^{\frac{n+1}{2}}} \sum_{i=1}^{\tilde{n}} 2|0\rangle + \underbrace{\left((-1)^{x_i} + (-1)^{x_i+s_i}\right)}_{=0 \text{ if } x_i \neq s_i} |1\rangle .$$

$$= \frac{1}{2^{\frac{n-1}{2}}} \sum_{y \cdot s = 0} |y\rangle .$$

We measure $n+k$ samples of the first register, we then obtain $(n+k)$ vectors $y_1, \dots, y_{n+k}$.

→ with probability $\geq 1 - \frac{1}{2^k}$, $(y_1, \dots, y_{n+k})$ generates $s^\perp$

thus we can solve $\begin{cases} y_1 \cdot s = 0 \\ \vdots \\ y_{n+k} \cdot s = 0 \end{cases}$ □

② Order finding

In the order finding problem, we have two numbers a, N s.t. a and N are coprime (i.e. their common greatest divisor is 1), and we want to find the smallest integer $r > 0$ s.t. $a^r = 1 \bmod N$.

Remark: if we have such an algorithm, where r is even, then we can deduce efficiently a prime factor of N.

We suppose that $M = \ell r$, $\ell \in \mathbb{N}^*$ (for simplicity) and that we can define a QFT_M with a circuit with $O((\log M)^2)$ gates.

Let $f_a : [\![0, M-1]\!] \to [\![0, N-1]\!]$, $x \mapsto a^x\ [N]$. and U_{f_a} a unitary on $\mathbb{C}^M \otimes \mathbb{C}^N$ s.t. $U_{f_a}|x\rangle \otimes |0\rangle = |x\rangle \otimes |a^x \bmod N\rangle$

Circuit:

$$\frac{1}{\sqrt{M}} \sum_{j=0}^{M-1} |j\rangle \otimes |0\rangle^{\otimes N}$$

$$\frac{1}{\sqrt{M}} \sum_{j=0}^{M-1} |j\rangle \otimes |\underbrace{a^j \bmod N}_{a^{t+\ell r} = a^t \bmod N \quad 0 \leq t < r}\rangle .$$

$$= \sqrt{\frac{r}{M}} \sum_{\ell=0}^{M/r - 1} |j + \ell r\rangle\, |a^x \bmod N\rangle .$$

Now by the QFT:

$$QFT_M \left(\sqrt{\frac{r}{M}} \sum_{\ell=0}^{M/r-1} |j + \ell r\rangle \right) = \frac{\sqrt{r}}{M} \sum_{y=0}^{M-1} \sum_{\ell=0}^{M/r-1} \omega_M^{(j+\ell r)y}\, |y\rangle$$

$$= \frac{\sqrt{r}}{n} \sum_{y=0}^{n-1} \omega_n^{jy} \underbrace{\sum_{q=0}^{n/r-1} \left(\omega_n^{yr}\right)^q}_{=0 \text{ if } \omega_n^{yr} \neq 1} |y\rangle.$$

$\Leftrightarrow yr = 0 \mod n.$

→ la mesure du 1^er qbit permet de déterminer $y = \frac{sn}{r}$ for $0 \leq s \leq r-1$

$\in \mathbb{N}$ by assumption.

→ if $y \neq 0$, then with high probability $\frac{y}{n} = \frac{s}{r}$ is irreducible thus we have r.

← output of the algorithm.

← chosen at the beginning