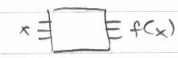
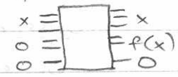
c191: Quantum information 10/28/03



Exponential speedup by quantum computation

① f is easy to compute classically, then there is an efficient reversible circuit

$\Rightarrow$ there is an efficient quantum circuit



on input $\sum_{x \in \{0,1\}^n} \alpha_x |x\rangle$, output is $\sum_x \alpha_x |x\rangle |f(x)\rangle$

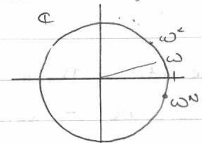
example: $n=1$, $f(x)=x$

input $= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, output $= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ just a CNOT gate

② Quantum Fourier transform

Discrete Fourier transform: modulo N, an $N \times N$ unitary matrix, $\omega = e^{2\pi i}$

$$\begin{array}{cc} & \begin{array}{ccccc} & & y & & \end{array} \\ \frac{1}{\sqrt{N}} \; x & \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & \cdots & \omega^{N-1} \\ 1 & \omega^2 & \omega^{xy} & & \\ 1 & \omega^3 & & & \\ 1 & \omega^{N-1} & & & \end{pmatrix} \end{array}$$



$\bar{\omega} = \omega^{-1}$

standard basis $\begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$ $\begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$ $\cdot$ $\begin{pmatrix} \\ \\ \end{pmatrix}$ jth

$\downarrow \qquad \downarrow \qquad \downarrow$

Fourier basis $\frac{1}{\sqrt{N}}\begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix}$ $\frac{1}{\sqrt{N}}\begin{pmatrix} 1 \\ \omega \\ \vdots \\ \omega^{N-1} \end{pmatrix}$ jth column

inner product between ith & jth column

$$\frac{1}{N}\begin{pmatrix} 1 \\ \omega^i \\ \vdots \end{pmatrix}^{\dagger}\begin{pmatrix} 1 \\ \omega^j \\ \vdots \end{pmatrix} = \frac{1}{N}\sum_k \omega^{(j-i)k} = \begin{cases} 0 & \text{unless } i=j \\ 1 & \text{if } i=j \end{cases}$$

since if $\ell \not\equiv 0 \pmod N$ then $1 + \omega^\ell + \omega^{2\ell} + \cdots + \omega^{(N-1)\ell} = 0$

if $\ell \equiv 0 \pmod N$ $\quad 1 + \omega^\ell + \cdots + \omega^{(N-1)\ell} = N$

computing the discrete Fourier transform is essential for digital signal processing — naive matrix multiplication takes $\Theta(N^2)$ steps

the FFT (Fast Fourier Transform) takes only $O(N \log N)$ steps (!)

how? Assume $N = 2^n$. Split the matrix into four parts, rearrange the columns into even and odd ones
(classically)

$$\begin{array}{cc} & \begin{array}{cc} 2y & 2y+1 \end{array} \\ \begin{array}{c} x \\ \\ \frac{N}{2}+x \end{array} & \left(\begin{array}{c|c} \omega^{2xy} & \omega^x \cdot \omega^{2xy} \\ \hline \omega^{2xy} & -\omega^x \omega^{2xy} \end{array}\right) \end{array} \begin{pmatrix} z_0 \\ \hline z_1 \end{pmatrix} = \begin{pmatrix} F_{\frac{N}{2}} z_0 + \omega^x F_{\frac{N}{2}} z_1 \\ \hline F_{\frac{N}{2}} z_0 - \omega^x F_{\frac{N}{2}} z_1 \end{pmatrix}$$

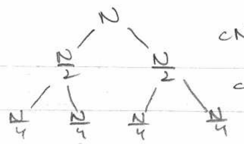
$\omega^{(\frac{N}{2}+x)2y} = \omega^{2xy}$ since $\omega^{\frac{N}{2}} = -1$

write $\omega = \omega_N$. $\omega_N^2 = \omega_{N/2} = e^{2\pi i/(N/2)}$

time to solve problem of size N is

$$T(N) = 2T\left(\tfrac{N}{2}\right) + O(N) \longrightarrow T(N) = O(N \log N)$$

$\longrightarrow$



cN

$c(\frac{N}{2}) + c(\frac{N}{2}) = cN$

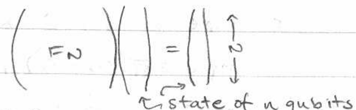
$\log N$ levels, each taking $O(N)$ time $\longrightarrow O(N \log N)$

<u>Classical</u>

$O(N \log N)$ steps

<u>Quantum</u>

$N = 2^n$

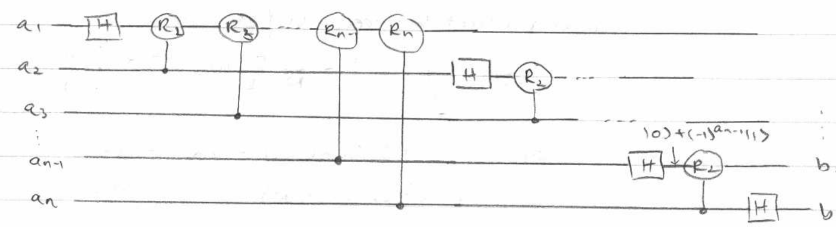


we'll find a quantum circuit of size $O(n^2) = O(\log^2 N)$.

exponential speedup

What's the catch? The output is $\sum_x \alpha_x |x\rangle$, whereas classically you'd get the whole list $\alpha_0, \alpha_1, \dots, \alpha_{N-1}$. All we can do is Fourier sampling: measure to get x with probability $|\alpha_x|^2$. Even with this restriction, the quantum Fourier transform is quite powerful.

We want $\underset{a_1 a_2 \cdots a_n}{|a\rangle} \longrightarrow \frac{1}{N} \sum_b \omega^{ab} |b\rangle$



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

$$|a_1 \cdots a_n\rangle \xrightarrow{F.T.} \underbrace{(|0\rangle + e^{2\pi i (0.a_n)}|1\rangle)}_{b_1} \otimes \underbrace{(|0\rangle + e^{2\pi i (0.a_{n-1}a_n)}|1\rangle)}_{b_2} \otimes \cdots \otimes \underbrace{(|0\rangle + e^{2\pi i (0.a_1 a_2 \cdots a_n)}|1\rangle)}_{b_n}$$

$0.a_n = \frac{a_n}{2}$ = drop integer part of $a/2$ ...; $0.a_{n-1}a_n = \frac{2a_{n-1}+a_n}{4}$; $0.a_1 a_2 \cdots a_n = \frac{a}{2^n}$

what is the coefficient of $\underset{b_1 b_2 \cdots b_n}{|b\rangle}$?

$0110 \cdots 0 = 010 \cdots 0 + 0010 \cdots 0 + \cdots$

eg. if $b_1 = 1$, get extra phase of $e^{2\pi i \frac{a_n}{2}} = e^{\frac{2\pi i}{N} \cdot \frac{N}{2} \cdot a}$

Why does the circuit do this?

$b_1 = |0\rangle + e^{2\pi i \frac{a_n}{2}}|1\rangle$ $\qquad a_n = 0: \ |0\rangle + |1\rangle$
$\qquad\qquad\qquad\qquad\qquad\qquad a_n = 1: \ |0\rangle - |1\rangle$

$b_2 = |0\rangle + e^{2\pi i \frac{2a_{n-1}+a_n}{4}}|1\rangle$

$= |0\rangle + (-1)^{a_{n-1}} \omega_4^{a_n} |1\rangle$ ✓