Quantum computation

Lecture: 2

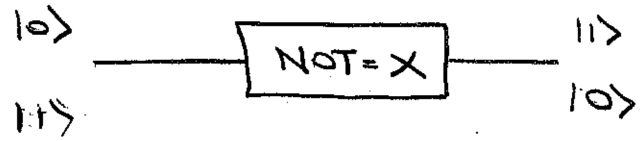
Quantum circuit model: Introduction

Quantum circuits:

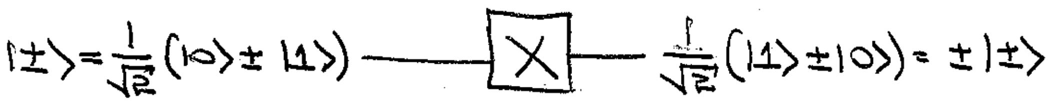
bit strings $\longrightarrow$ state vectors — Superpositions

gates $\longrightarrow$ unitary operators — universal gate sets

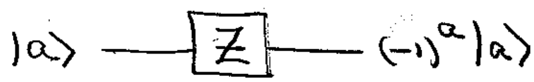
measurements $\longrightarrow$ Born rule for probabilities



$$X|a\rangle = |\bar{a}\rangle = |1 \oplus a\rangle$$



$$X|\pm\rangle = \pm|\pm\rangle$$

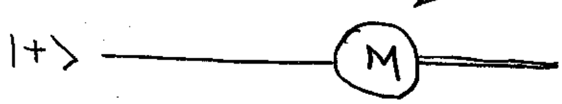


$$Z|a\rangle = (-1)^a|a\rangle$$

$$Z|\pm\rangle = |\mp\rangle$$

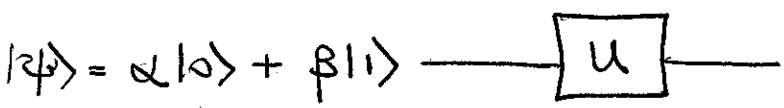
Measurement:

We later generalize this to include post-measurement qubit



$0, \quad p_0 = |\langle 0|+\rangle|^2 = \frac{1}{2}$

$1, \quad p_1 = |\langle 1|+\rangle|^2 = \frac{1}{2}$



$$\alpha U|0\rangle + \beta U|1\rangle$$
$$= \alpha(U_{11}|0\rangle + U_{21}|1\rangle) + \beta(U_{12}|0\rangle + U_{22}|1\rangle)$$
$$= (\alpha U_{11} + \beta U_{12})|0\rangle + (\alpha U_{21} + \beta U_{22})|1\rangle$$

$$\begin{pmatrix} U_{11} & U_{12} \\ U_{21} & U_{22} \end{pmatrix}\begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

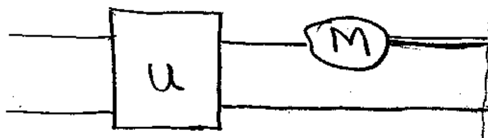
Conservation of probabilities

$$(\alpha^* \ \beta^*)\begin{pmatrix} \alpha \\ \beta \end{pmatrix} = 1$$

$$(\alpha^* \ \beta^*)U^\dagger U\begin{pmatrix} \alpha \\ \beta \end{pmatrix} = 1$$

$\Rightarrow U^\dagger U = I$, U is unitary

$|\psi\rangle = c_{00}|00\rangle + c_{01}|01\rangle + c_{10}|10\rangle + c_{11}|11\rangle$



0, $p_0 = |c'_{00}|^2 + |c'_{01}|^2$

1, $p_1 = |c'_{10}|^2 + |c'_{11}|^2$

If 0, $(c'_{00}|0\rangle + c'_{01}|1\rangle)/\sqrt{p_0}$

If 1, $(c'_{10}|0\rangle + c'_{11}|1\rangle)/\sqrt{p_1}$

$$|\psi'\rangle = U|\psi\rangle \longrightarrow \begin{pmatrix} c'_{00} \\ c'_{01} \\ c'_{10} \\ c'_{11} \end{pmatrix} = U \begin{pmatrix} c_{00} \\ c_{01} \\ c_{10} \\ c_{11} \end{pmatrix}$$

What we're not doing:

$$U\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x' \\ y' \end{pmatrix}$$

What we are doing: turning the space of strings into a complex vector space. Original strings are the <u>computational basis</u>.

① An arbitrary classical gate M becomes a linear operator A:

$$A|x\rangle = |Mx\rangle, \quad \langle y|A|x\rangle = \delta_{y,Mx}$$

② A reversible classical gate becomes a <u>permutation</u> unitary

③ There are many more unitaries than reversible classical gates.

④ Born rule for measurements.

$$p_0 = |\langle 00|U|\psi\rangle|^2 + |\langle 01|U|\psi\rangle|^2$$
$$= \langle\psi|U^\dagger|00\rangle\langle 00|U|\psi\rangle + \langle\psi|U^\dagger|01\rangle\langle 01|U|\psi\rangle$$
$$= \langle\psi|U^\dagger P_0 \otimes I\, U|\psi\rangle = \mathrm{tr}(U\rho U^\dagger P_0 \otimes I)$$

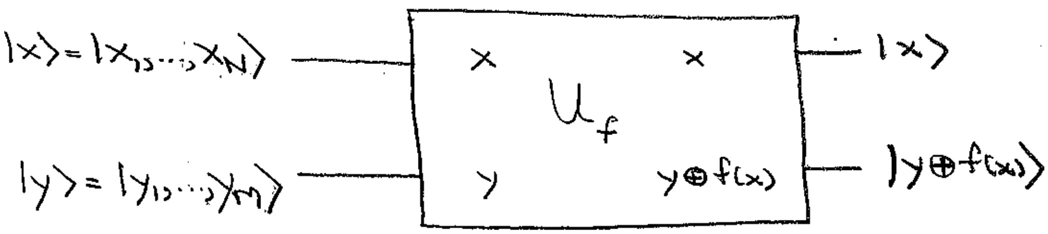
$\rho = |\psi\rangle\langle\psi|$

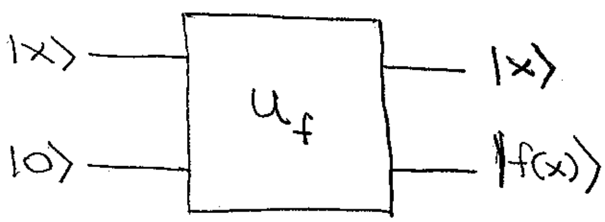
$$P_0 = |0\rangle\langle 0| \otimes I = |00\rangle\langle 00| + |01\rangle\langle 01|$$

If 0, $(P_0 \otimes I)U|\psi\rangle/\sqrt{p_0}$

Function evaluation in quantum circuits:

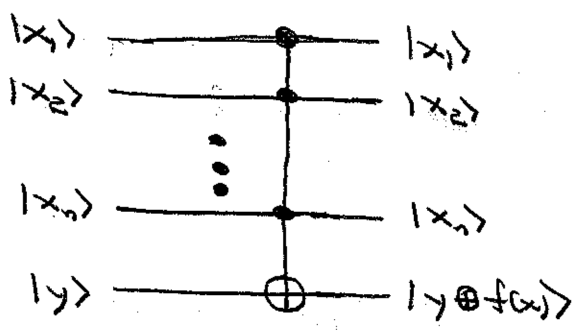
reversible classical circuit acting on computational basis.





If f is a Boolean function, U_f is a controlled bit-flip operation. The input qubits $|x_1\rangle \otimes \ldots \otimes |x_n\rangle$ are the control, but the control is determined by the value of the function $f(x)$. If $f(x) = 0$, the target qubit stays the same, and if $f(x) = 1$, the target qubit flips.

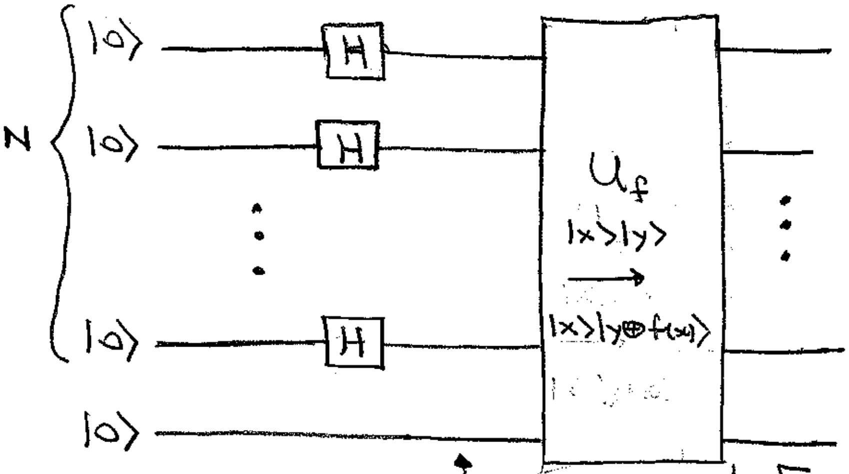
$$U_f |x\rangle |y\rangle = |x\rangle |y \oplus f(x)\rangle$$
$$= |x\rangle \otimes X^{f(x)} |y\rangle$$



$$f(x) = \begin{cases} 1, & x = 11\ldots1 \\ 0, & \text{otherwise} \end{cases}$$

Quantum parallelism: f an N-bit Boolean function

Hadamard gate $H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, $H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$



$$|\psi\rangle = \frac{1}{\sqrt{2^N}} \sum_x |x\rangle |f(x)\rangle$$

All values of f calculated "in parallel."

$$|\psi\rangle = \frac{1}{\sqrt{2^N}} \sum_x |x\rangle|0\rangle$$

$H^{\otimes N}$ — Walsh-Hadamard transform

$$H^{\otimes N}|0\rangle^{\otimes N} = \left[\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\right]^{\otimes N} = \frac{1}{\sqrt{2^N}} \sum_x |x\rangle$$

AND of x and y

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

$$\underset{\substack{\uparrow \\ \text{bit string}}}{H^{\otimes N}|z\rangle} = H^{\otimes N}|z_1, \dots, z_N\rangle = \frac{1}{\sqrt{2^N}} \sum_{x_1,\dots,x_N} (-1)^{z_1 x_1 + z_2 x_2 + \dots + z_N x_N} |x_1, \dots, x_N\rangle$$

$$x \cdot y = \sum_{j=1}^{N} x_j y_j$$

$$H^{\otimes N}|z\rangle = \frac{1}{\sqrt{2^N}} \sum_x (-1)^{z \cdot x} |x\rangle$$

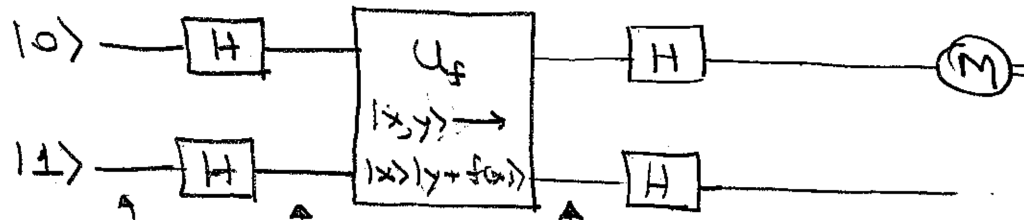
Notice that $U_f|x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle = |x\rangle \otimes X^{f(x)}|y\rangle$

$$U_f \underbrace{|x\rangle|\pm\rangle}_{\text{eigenstates of } U_f} = |x\rangle \otimes X^{f(x)}|\pm\rangle = (\pm 1)^{f(x)} |x\rangle|\pm\rangle$$

Value of f written into the phase if $|-\rangle$

phase kickback

Deutsch's algorithm: $f: \{0,1\} \longrightarrow \{0,1\}$ 1-bit Boolean function



$f(0) \oplus f(1)$ with probability 1

One-shot determination of <u>parity</u> of f.

$|\psi_0\rangle = |0\rangle|1\rangle$

$|\psi_3\rangle = (-1)^{f(0)} |f(0)\oplus f(1)\rangle |1\rangle$

$|\psi_1\rangle = \frac{1}{2}(|0\rangle + |1\rangle)(|0\rangle - |1\rangle)$

$$|\psi_2\rangle = \frac{1}{2}\left(|0\rangle|f(0)\rangle - |0\rangle|\overline{f(0)}\rangle + |1\rangle|f(1)\rangle - |1\rangle|\overline{f(1)}\rangle\right)$$

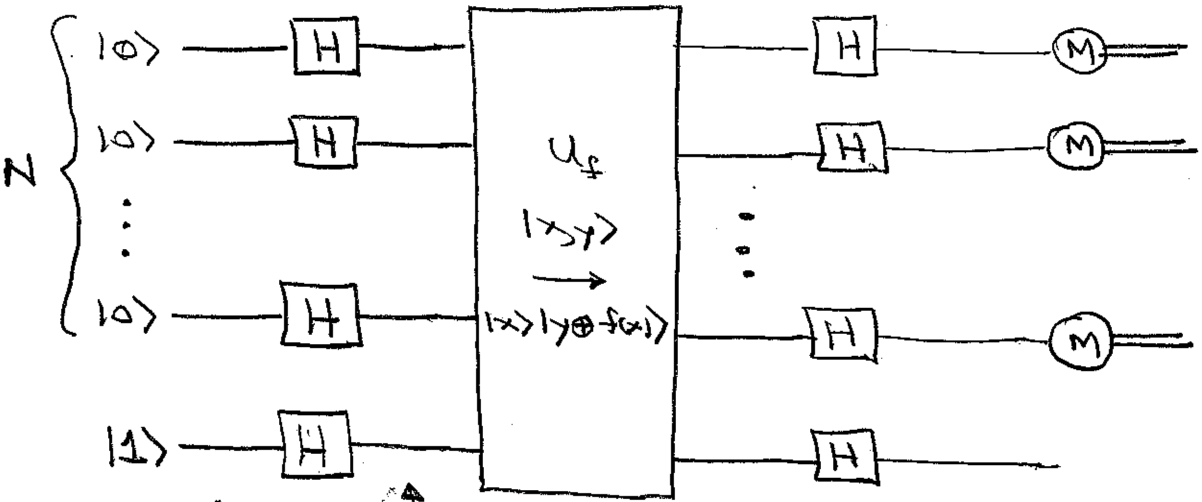
$$= \begin{cases} \frac{1}{2}(|0\rangle+|1\rangle)(|0\rangle-|1\rangle), & f(0)=f(1)=0 \\ \frac{1}{2}(|0\rangle-|1\rangle)(|0\rangle-|1\rangle), & f(0)=0, f(1)=1 \\ \frac{1}{2}(-|0\rangle+|1\rangle)(|0\rangle-|1\rangle), & f(0)=1, f(1)=0 \\ \frac{1}{2}(-|0\rangle-|1\rangle)(|0\rangle-|1\rangle), & f(0)=f(1)=1 \end{cases}$$

$$= \frac{1}{2}(-1)^{f(0)}\left(|0\rangle + (-1)^{f(0)\oplus f(1)}|1\rangle\right)(|0\rangle - |1\rangle)$$

Deutsch's algorithm determines the parity of f in one shot, which is the same as determining whether f is constant or balanced. The D-J algorithm generalizes this latter feature to arbitrary N.

Deutsch-Jozsa algorithm: N-bit Boolean function $f:\{0,1\}^N \to \{0,1\}$, which is either <u>constant</u> or <u>balanced</u>.

Number of classical calls to be sure is $\sim 2^N/2 = 2^{N-1}$



$$|\psi_0\rangle = |0\rangle^{\otimes N}|1\rangle$$

$$|\psi_1\rangle = H^{\otimes N}|0\rangle^{\otimes N} \otimes H|1\rangle$$

$$= \frac{1}{\sqrt{2^N}}\sum_x |x\rangle \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

$$|\psi_2\rangle = \frac{1}{\sqrt{2^N}}\sum_x |x\rangle \frac{1}{\sqrt{2}}\left(|f(x)\rangle - |\overline{f(x)}\rangle\right)$$

$$= \underbrace{\left(\frac{1}{\sqrt{2^N}}\sum_x (-1)^{f(x)}|x\rangle\right)}_{|\phi\rangle} \otimes \underbrace{\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)}$$

ancilla qubit left unentangled.

function value written in phase

$$\langle \phi^{\text{constant}} | \phi^{\text{balanced}} \rangle = \pm \frac{1}{2^N}\sum_x (-1)^{f(x)} = 0$$

$$|\psi_3\rangle = \underbrace{\left(\frac{1}{\sqrt{2^N}}\sum_{x,y} (-1)^{f(x)+x\cdot y}|y\rangle\right)}_{|\chi\rangle} \otimes |1\rangle$$

f constant: $|\chi_0\rangle = \pm|0\rangle^{\otimes N}$

f balanced:

$${}^{\otimes N}\langle 0|\chi\rangle = \frac{1}{2^N}\sum_x (-1)^{f(x)} = 0$$

One-shot determination of whether function is constant or balanced.