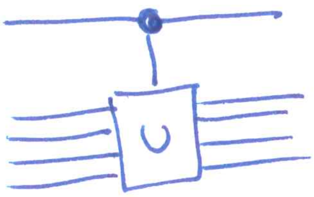
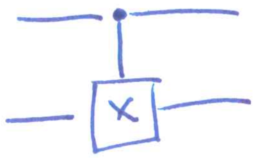
- controlled-U gate: extension of U gate
  - if control bit 0 ⇒ do nothing
  - if control bit 1 ⇒ apply U to rest of system (target)

notation

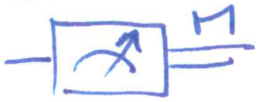


for controlled-X gate



- quantum circuits can also have measurement devices: $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

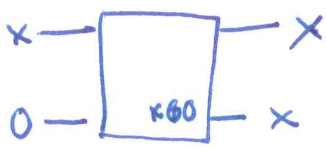
notation



if input $|\psi\rangle$ → output $|0\rangle$ or $|1\rangle$ with probabilities $|\alpha|^2, |\beta|^2$

Qubit copying circuit?

classical copying use CNOT with 0 as target input



in quantum computing copying qubit is not possible

-proof: suppose there exists $\hat{U}$-gate such that $\hat{U}|\Psi\rangle|s\rangle \to |\Psi\rangle|\Psi\rangle$

acting on state $|\Phi\rangle$ we have

$$\hat{U}|\Phi\rangle|s\rangle \to |\Phi\rangle|\Phi\rangle$$

$$\langle s|\langle\psi|U^{+}U|\varphi\rangle|s\rangle = \langle\psi|\varphi\rangle$$

$$\langle\psi|\langle\psi||\varphi\rangle|\varphi\rangle = (\langle\psi|\varphi\rangle)^2$$

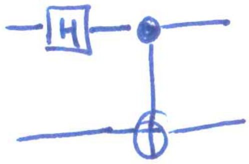
$$\Rightarrow \quad \langle\Psi|\Phi\rangle = (\langle\Psi|\Phi\rangle)^2$$

only holds for $\langle\Psi|\Phi\rangle = 0$ or 1

→ general quantum cloning device is impossible

Bell states

circuit :



→ produces Bell states (EPR pairs)

↓

correlated 2-qubits

$$|0\rangle|0\rangle \xrightarrow{H} \left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)|0\rangle \xrightarrow{CNOT} \frac{|00\rangle+|11\rangle}{\sqrt{2}} = |\beta_{00}\rangle$$

$$|0\rangle|1\rangle \xrightarrow{H} \left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)|1\rangle \xrightarrow{CNOT} \frac{|01\rangle+|10\rangle}{\sqrt{2}} = |\beta_{01}\rangle$$

$$|1\rangle|0\rangle \xrightarrow{H} \left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)|0\rangle \xrightarrow{CNOT} \frac{|00\rangle-|11\rangle}{\sqrt{2}} = |\beta_{10}\rangle$$

$$|1\rangle|1\rangle \xrightarrow{H} \left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)|1\rangle \xrightarrow{CNOT} \frac{|01\rangle-|10\rangle}{\sqrt{2}} = |\beta_{11}\rangle$$

Quantum teleportation

Problem: Alice and Bob met long ago, but now they are apart. While together they generated an EPR pair, each taking one qubit when they separated. Many years later Bob is in hiding, Alice has to deliver a qubit $|\psi\rangle$ to Bob. She does not know state of qubit, and she can only send classical information to Bob.

Can she do it?

Issues: if she measures qubit $\Rightarrow$ qubit is lost

Solution: outline

1.) Alice interacts qubit $|\psi\rangle$ with her half of EPR pair

2.) measures the two qubits in her possession $\Rightarrow$ results 00, 01, 10, 11

3.) She sends result (00, 01, 10, 11) to Bob

4.) Bob performs one of four operations on ~~qubit~~ his half of EPR pair $\Rightarrow$ recovers $|\psi\rangle$

in more detail:

$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ — qubit to be "delivered"

EPR pair: $|\beta_{00}\rangle = \frac{(|00\rangle + |11\rangle)}{\sqrt{2}}$

1.) - interact qubit with EPR pair

$$|\psi_0\rangle \rightarrow |\psi\rangle|\beta_{00}\rangle = \frac{1}{\sqrt{2}}\left[\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|00\rangle + |11\rangle)\right]$$

first two qubits - Alice
third qubit - Bob

2.) - ~~send~~ Alice sends her two qubits through C-NOT gate

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}\left[\alpha|0\rangle \frac{(|00\rangle + |11\rangle)}{\cancel{\sqrt{2}}} + \beta|1\rangle(|10\rangle + |01\rangle)\right]$$

3.) Alice sends first qubit through a Hadamard gate

$$|\psi_2\rangle = \frac{1}{2}\left[\alpha(|0\rangle + |1\rangle)(|00\rangle + |11\rangle) + \beta(|0\rangle - |1\rangle)(|10\rangle + |01\rangle)\right]$$

$$\cancel{= \frac{1}{2}[\alpha(|00\rangle + |10}$$

$$= \frac{1}{2}\left[\alpha(|00\rangle|0\rangle + |01\rangle|1\rangle + |10\rangle|0\rangle + |11\rangle|1\rangle) + \beta(|01\rangle|0\rangle + |00\rangle|1\rangle - |11\rangle|0\rangle - |10\rangle|1\rangle)\right]$$

$$= \frac{1}{2}\left[|00\rangle(\alpha|0\rangle + \beta|1\rangle) + |01\rangle(\alpha|1\rangle + \beta|0\rangle) + |10\rangle(\alpha|0\rangle - \beta|1\rangle) + |11\rangle(\alpha|1\rangle - \beta|0\rangle)\right]$$

4.) now, Alice makes a measurement on $|\psi_2\rangle$

→ measures first two qubits!

depending on the result of measurement the third qubit will remain in some state, which can be manipulated so that original qubit is reproduced

result of measurement	state of 3rd qubit
00	$\alpha|0\rangle + \beta|1\rangle$
01	$\alpha|1\rangle + \beta|0\rangle$
10	$\alpha|0\rangle - \beta|1\rangle$
11	$\alpha|1\rangle - \beta|0\rangle$

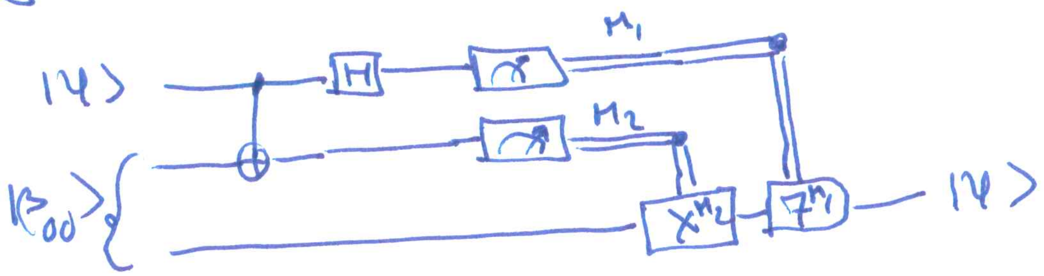
00 → original state reproduced

01 → Bob can apply X gate $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

10 → Bob can apply Z gate $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

11 → Bob can apply XZ

diagram of circuit

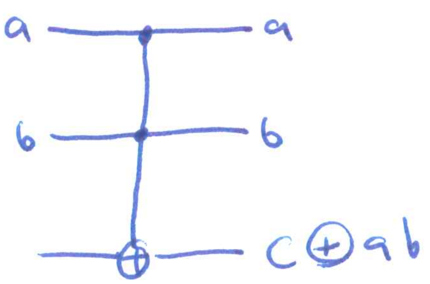


- does teleportation allow transmission of information faster than light?
  - not really: Alice must transmit her results through classical channels ⇒ limited by speed of light
- does quantum teleportation copy a qubit?
  - no → α, β become part of 3rd qubit
    1st qubit (and 2nd) are destroyed by measurement
- applications of quantum teleportation:
  - build quantum gates resistant to noise
  - quantum error correcting

Quantum algorithms

- what computations can quantum circuits perform?
- are they faster/more efficient than classical circuits?

- Classical computations on a quantum computer
  - can we simulate a classical logic circuit using a quantum computer?
  - difficulty: quantum logic gates are reversible, & some classical ones are not
- solution: Toffoli gate – allows simulation of any classical circuit, contains only reversible elements
  - two control bits, one target bit
    - if both control bits are 1 gate NOTs target bit



Input a	Input b	Input c	Output a'	Output b'	Output c'
0	0	0			0
0	0	1			1
0	1	0			0
0	1	1			1
1	0	0			0
1	0	1			1
1	1	0			1
1	1	1			0

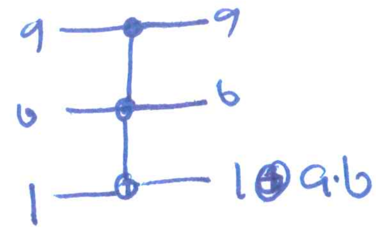
$a' = a$

$b' = b$

inverse of Toffoli gate – itself

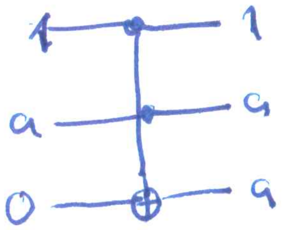
Toffoli gate can simulate NAND/FANOUT

NAND:



	a	b
a	1	1
b	1	0

FANOUT



- can be written as 8 × 8 matrix
- ensures that quantum computer can perform all classical operations
- probabilistic/random algorithms also possible
- so, anything a classical computer can do can also be done by a quantum computer

BUT, is there anything a quantum computer does better than a classical one?

Quantum parallelism

- allows state with many values of some variable x and function f(x) be stored simultaneously
- suppose: $f(x): \{0,1\} \to \{0,1\}$

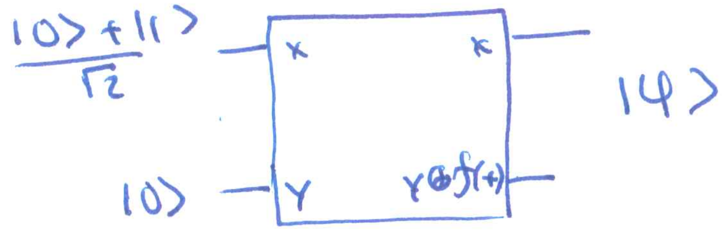
  function with one-bit domain range

computing function on quantum computer

$$|x\, y\rangle \xrightarrow{U_f} |x, y \oplus f(x)\rangle$$

U_f - gate that accomplishes mapping
- can be considered a black box

- compute function at two values:



$$|\psi\rangle = \frac{|0, f(0)\rangle + |1, f(1)\rangle}{\sqrt{2}}$$

state includes two values of $f(x)$
$\Rightarrow$ quantum parallelism $\Rightarrow$ not possible on classical computer

can generalize quantum parallelism to multiple qubits:

$$|0\rangle|0\rangle \xrightarrow{H^{\otimes 2}} \left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)$$

$$= \frac{|00\rangle + |01\rangle + |10\rangle + |11\rangle}{2}$$

$H^{\otimes 2} \rightarrow$ tensor product of $H \otimes H$

states	$\|00\rangle$	$\|01\rangle$	$\|10\rangle$	$\|11\rangle$
binary	0	1	2	3

can produce state $|\psi\rangle = \frac{1}{\sqrt{2^n}} \sum_x |x\rangle$

$x = 0, \ldots, 2^n - 1$

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

- so it appears that quantum computers can store a whole function in one state (qubit) $\Rightarrow$ <u>but</u>! data is not easily accessible
  measurement will "collapse" state into <u>one</u> value of <u>x</u>
- extracting information is not easy

<u>Deutsch algorithm</u>

- demonstrates use of quantum mechanical concept of interference

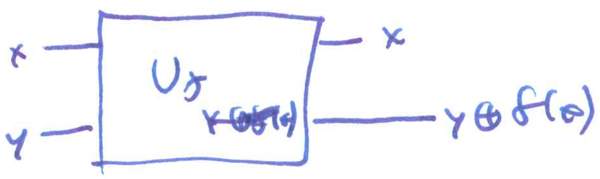
start: $|\psi_0\rangle = |01\rangle$

apply two Hadamard gates

$$|\psi_1\rangle = \left[\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$$

*

$$U_f\,|x\rangle\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) = (-1)^{f(x)}\,|x\rangle\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$



$x = 0$

$$U_f\,|0\rangle\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$

$$= \frac{1}{\sqrt{2}}\left[U_f|00\rangle - U_f|01\rangle\right]$$

$$= \frac{1}{\sqrt{2}}\left[|0\,f(0)\rangle - |0\,1 \oplus f(0)\rangle\right]$$

if $f(0) = 0$

$$= \frac{1}{\sqrt{2}}\left[|0\,0\rangle - |0\,1\rangle\right]$$

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

if $f(0) = 1$

$$= \frac{1}{\sqrt{2}}(|0\,1\rangle - |00\rangle) = \frac{1}{\sqrt{2}}(-1)^{f(0)}|0\rangle(|0\rangle - |1\rangle)$$

- do for all cases $x = 0, 1$; $f(0) = 0, 1$ $f(1) = 0, 1$ 25

result: $(-1)^{f(x)} |x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right)$

$$U_f |\psi_1\rangle = \frac{1}{\sqrt{2}} \left[(-1)^{f(0)} |0\rangle + (-1)^{f(1)} |1\rangle \right] \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right]$$

$$|\psi_2\rangle = \begin{cases} \pm \left[\frac{|0\rangle + |1\rangle}{\sqrt{2}} \right] \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right] & \text{if } f(0) = f(1) \\ \pm \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right] \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right] & \text{if } f(0) \neq f(1) \end{cases}$$

Final Hadamard transform $H \cancel{\otimes} |\psi_2\rangle = |\psi_3\rangle$

$$|\psi_3\rangle = \begin{cases} \pm |0\rangle \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right] & f(0) = f(1) \\ \pm |1\rangle \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right] & f(0) \neq f(1) \end{cases}$$

$$= |f(0) \oplus f(1)\rangle \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right]$$

measuring first qubit => measures $f(0) \oplus f(1)$ => ~~a~~ glob

$f(0) \oplus f(1) \rightarrow$ global property

in classical case two evaluations would be necessary

Deutsch - Jozsa Algorithm

solves a toy problem:

problem: Alice in Amsterdam selects a number in range $0, 2^n-1$, mails it in letter to Bob. Bob ~~applies~~ uses x to calculate function $f(x)$ with result either 0 or 1.

Bob can only use one of two functions:

$f(x)$ = constant (all zeroes or ones)

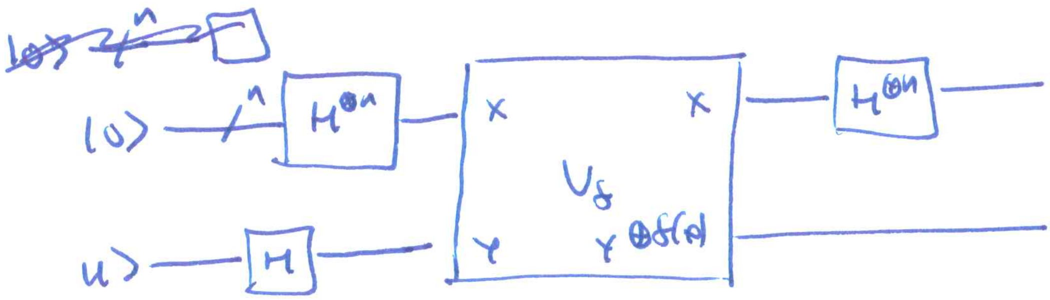
or $f(x)$ = balanced (equal number of zeroes or ones)

how many times must she send to tell whether function is constant or balanced?

classically: $\frac{2^n}{2}+1 \Rightarrow$ gives answer with <u>certainty</u>

in quantum case: One <u>qubit</u> is necessary only!!!

sketch of algorithm



start with $|\psi_0\rangle = |0\rangle^{\otimes n} |1\rangle$

Hadamard transform $H^{\otimes n+1}$

$$|\psi_1\rangle = \sum_{x\in\{0,1\}} \frac{|x\rangle}{\sqrt{2^n}} \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$$

$$|\psi_2\rangle = U_f|\psi_1\rangle = \sum_x \frac{(-1)^{f(x)}|x\rangle}{\sqrt{2^n}} \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$$

Hadamard transform on query qubits (first n)

can write it as: example $n=1$

$|x\rangle \Rightarrow x = 0, 1$

$$H|x\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}} = \sum_z \frac{(-1)^{xz}|z\rangle}{\sqrt{2}}$$

in general $$H^{\otimes n}|x\rangle = \sum_z \frac{(-1)^{x\cdot z}|z\rangle}{\sqrt{2^n}}$$

$\Downarrow$

$$|\psi_3\rangle = H^{\otimes n}|\psi_2\rangle = \underbrace{\sum_{xz} \frac{(-1)^{x\cdot z + f(x)}|z\rangle}{2^n}}_{\downarrow} \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$$

- investigate amplitude of state $|z\rangle = |0, \dots, 0\rangle$ in query register

$$A = \sum_x \frac{(-1)^{f(x)}}{2^n} \rightarrow$$ if $f(x)$ constant $A = 1$ or -1

$\Downarrow$

$|\psi_3\rangle$ – normalized, $A=1, A=-1 \Rightarrow$ all zero state is the only contribution to wave-function

if $f(x)$ – balanced $\Rightarrow$ this is not the case

$\rightarrow A = 0 \Rightarrow$ no contribution from all zero state

- can distinguish <u>constant or balanced</u> function based on <u>one</u> measurement
- caveat: problem does not seem to have application

Application oriented examples exist

- Fourier transform
- Quantum search algorithms

<u>Realizing quantum bits</u>

Stern - Gerlach experiment