GGI School on
"Quantum Computation and Sensing"

Quantum Algorithms and Protocols

LECTURE 2

Elisa Ercolessi

Theory and Phenomenology of Fundamental Interactions

UNIVERSITY AND INFN · BOLOGNA

Istituto Nazionale di Fisica Nucleare

Sezione di Bologna

- Compositions of two bits

  classical: all 4 possibilities

  quantum: computational basis

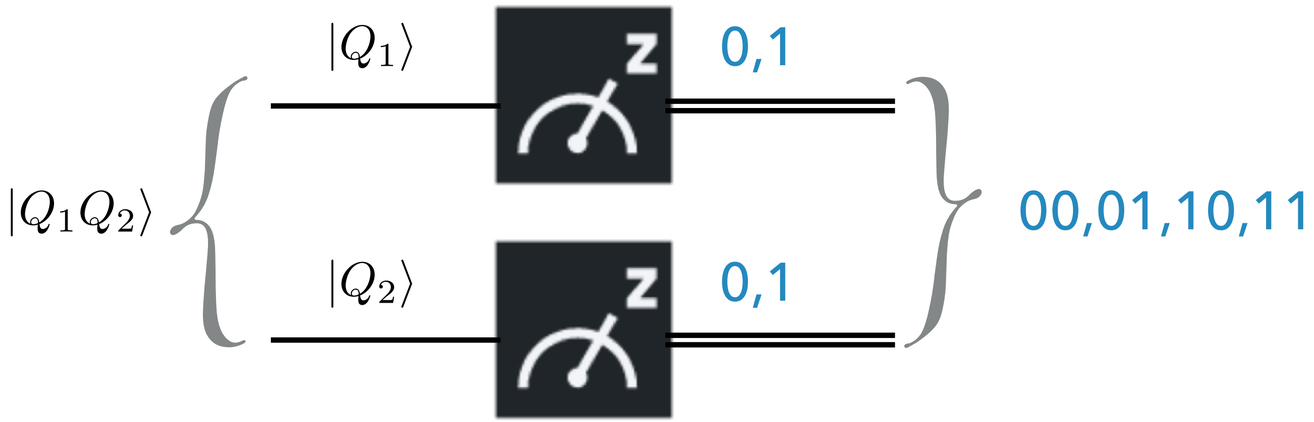
bit 1 \ bit 2	0	1
0	00	01
1	10	11

- Superposition principle:

$$|Q_1 Q_2\rangle = a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle = \begin{pmatrix} a_{00} \\ a_{01} \\ a_{10} \\ a_{11} \end{pmatrix}$$

$$|a_{00}|^2 + |a_{01}|^2 + |a_{10}|^2 + |a_{11}|^2 = 1$$

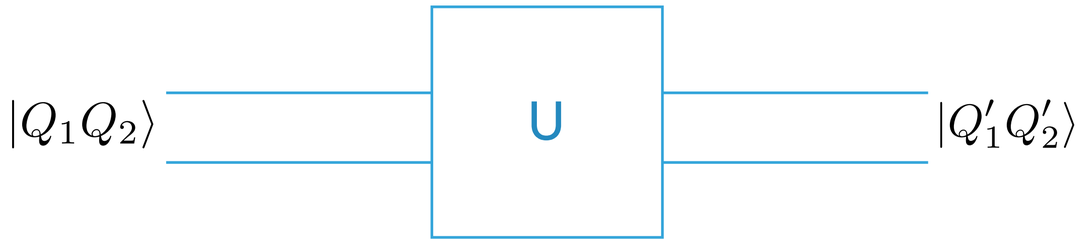
- The physical meaning of the coefficients is linked to measurements



- The outcome is:
  - not deterministic
  - destructive

outcome	probability	state after
00	$p_{00} = \|a_{00}\|^2$	$\|00\rangle$
01	$p_{01} = \|a_{01}\|^2$	$\|01\rangle$
10	$p_{10} = \|a_{10}\|^2$	$\|10\rangle$
11	$p_{11} = \|a_{11}\|^2$	$\|11\rangle$

- Linear (and unitary) transformation



$$|Q_1Q_2\rangle = a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle$$

$$\downarrow \mathrm{U}$$

$$|Q'_1Q'_2\rangle = a'_{00}|00\rangle + a'_{01}|01\rangle + a'_{10}|10\rangle + a'_{11}|11\rangle$$

which is represented by a unitary 4x4 matrix U,

$$\begin{pmatrix} a_{00} \\ a_{01} \\ a_{10} \\ a_{11} \end{pmatrix} \xrightarrow{U} \begin{pmatrix} a'_{00} \\ a'_{01} \\ a'_{10} \\ a'_{11} \end{pmatrix} = \begin{pmatrix} A & B & C & D \\ E & F & G & H \\ I & J & K & L \\ M & L & N & P \end{pmatrix} \begin{pmatrix} a_{00} \\ a_{01} \\ a_{10} \\ a_{11} \end{pmatrix}$$

with $U\,U^\dagger = U^\dagger\,U = \mathbb{I}$

CZ

(controlled Z)

IN	OUT
$\|\underline{0}0\rangle$	$\|00\rangle$
$\|\underline{0}1\rangle$	$\|01\rangle$
$\|\underline{1}0\rangle$	$\|10\rangle$
$\|\underline{1}1\rangle$	$-\|11\rangle$

control bit

target bit, on which Z acts iff the control bit is 1

$$\begin{pmatrix} a_{00} \\ a_{01} \\ a_{10} \\ a_{11} \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} \begin{pmatrix} a_{00} \\ a_{01} \\ a_{10} \\ a_{11} \end{pmatrix} = \begin{pmatrix} a_{00} \\ a_{01} \\ a_{11} \\ a_{10} \end{pmatrix}$$

NB. It is symmetric: it is not necessary to distinguish between control and target

CNOT

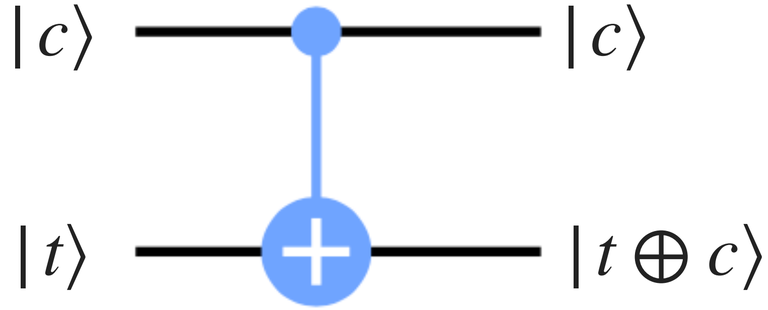
(controlled NOT)

IN	OUT
$\|\underline{0}0\rangle$	$\|00\rangle$
$\|\underline{0}1\rangle$	$\|01\rangle$
$\|\underline{1}0\rangle$	$\|11\rangle$
$\|\underline{1}1\rangle$	$\|10\rangle$

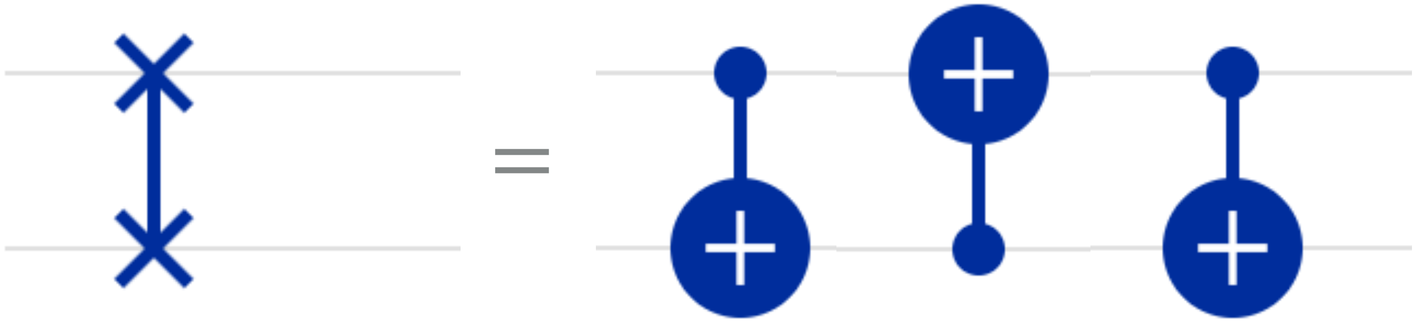
control bit

target bit, on which NOT acts iff the control bit is 1

$$\begin{pmatrix} a_{00} \\ a_{01} \\ a_{10} \\ a_{11} \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} a_{00} \\ a_{01} \\ a_{10} \\ a_{11} \end{pmatrix} = \begin{pmatrix} a_{00} \\ a_{01} \\ a_{11} \\ a_{10} \end{pmatrix}$$



SWAP

$|IN\rangle = |Q_1 Q_2\rangle$  $|IN\rangle = |Q_2 Q_1\rangle$

Example: $|IN\rangle = |01\rangle$.

EXERCISE: $|IN\rangle = |00\rangle, |10\rangle, |11\rangle$.

- A set S is said to be universal if we can *approximate* any unitary transformation on an arbitrary number of qubits, with any desired precision, by composing gates from S only. There are many such sets.

Example: CNOT

$$R_{\pi/8} = \begin{bmatrix} \cos \pi/8 & -\sin \pi/8 \\ \sin \pi/8 & \cos \pi/8 \end{bmatrix} \qquad P = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$$

Solovay-Kitaev theorem. If S is closed under inversion, we can approximate any gate for n qubits with precision ε using a number of gates of order O(4n polylog $1/\varepsilon$).

Therefore complexity scales as $\log(1/\varepsilon)$.

Can we do classical computation on a quantum computer?

Recall that NAND+COPY are sufficient to implement any classical algorithm.

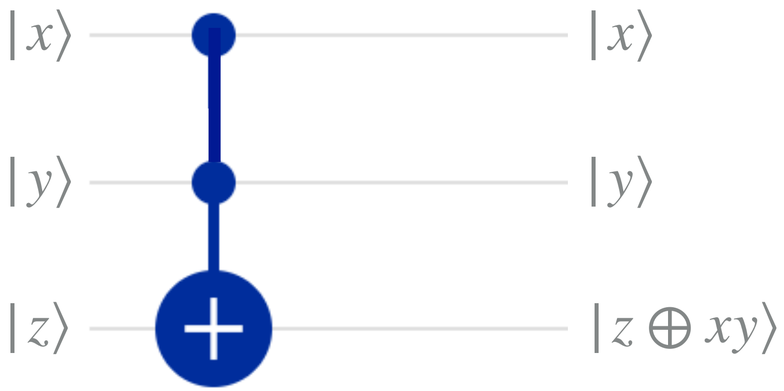
NAND: $(x, y) \mapsto 1 - xy$ COPY : $x \mapsto (x, x)$

This is not a trivial question since:

- quantum computation is reversible - but NAND is not

- in QM we have the “no cloning theorem” = it is impossible to have a unitary transformation whose (only) effect is to copy a state.

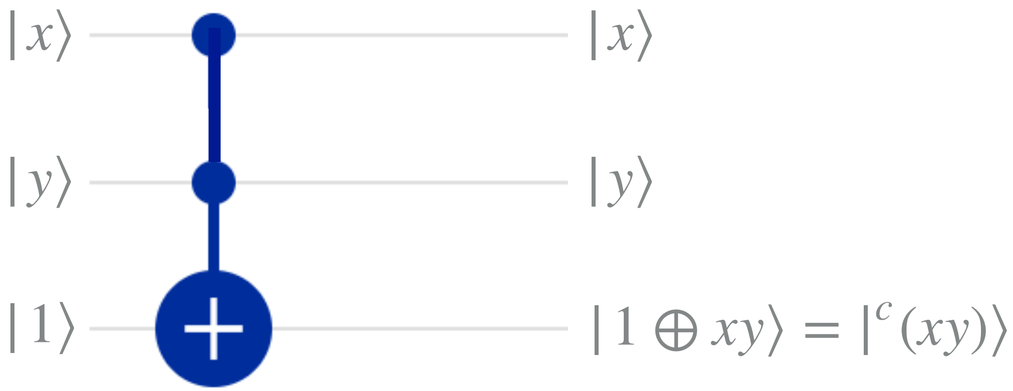
C-C-NOT



reversible classical computation

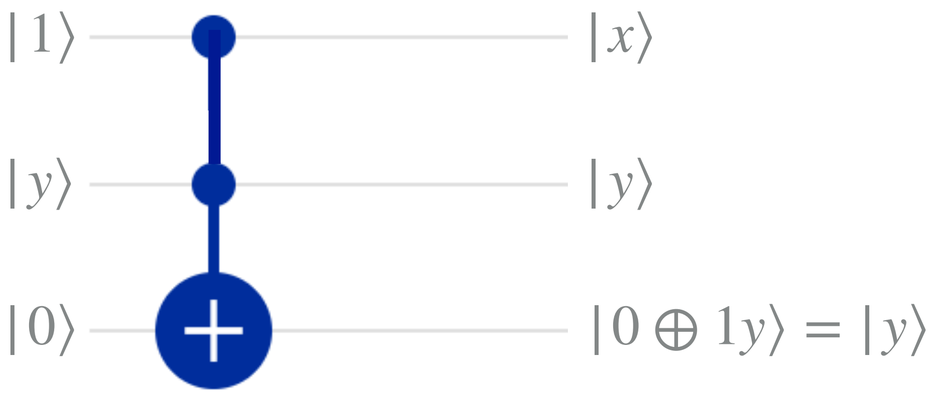
INPUT			OUTPUT		
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0
		↑			↑
		$\|z_{IN}\rangle$			$\|z_{OUT}\rangle$

NAND



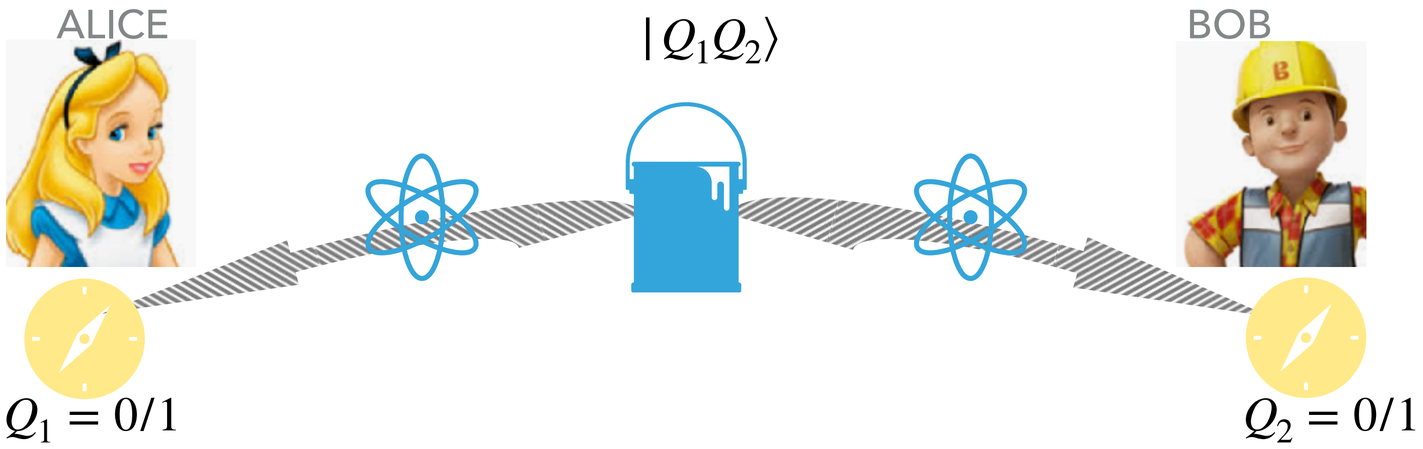
INPUT			OUTPUT		
~~0~~	~~0~~	~~0~~	~~0~~	~~0~~	~~0~~
0	0	1	0	0	1
~~0~~	~~1~~	~~0~~	~~0~~	~~1~~	~~0~~
0	1	1	0	1	1
~~1~~	~~0~~	~~0~~	~~1~~	~~0~~	~~0~~
1	0	1	1	0	1
~~1~~	~~1~~	~~0~~	~~1~~	~~1~~	~~1~~
1	1	1	1	1	0

COPY (fanout)



INPUT			OUTPUT		
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0

QUESTION. Is this violating the “no cloning theorem”?



- Product state: $|Q_1Q_2\rangle = |Q_1\rangle|Q_2\rangle$

initial 2-qubit state	final state	measure on Q_1	measure on Q_2	$Q_1 = Q_2$
$\|Q_1Q_2\rangle = (\|00\rangle + \|01\rangle/\sqrt{2}$ $= \|0\rangle(0\rangle + \|1\rangle/\sqrt{2}$	$\|00\rangle$, $p_{00} = 1/2$ $\|01\rangle$, $p_{01} = 1/2$	0 0	0 1	YES NO

no correlation between Q_1 and Q_2

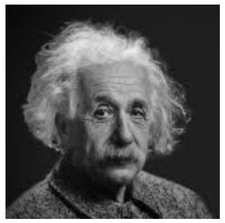
- Entangled state: $|Q_1Q_2\rangle \neq |Q_1\rangle|Q_2\rangle$

initial 2-qubit state	final state	measure on Q_1	measure on Q_2	$Q_1 = Q_2$
$\|Q_1Q_2\rangle = (\|00\rangle + \|11\rangle/\sqrt{2}$ $\neq \|Q_1\rangle\|Q_2\rangle$	$\|00\rangle$, $p_{00} = 1/2$ $\|11\rangle$, $p_{11} = 1/2$	0 1	0 1	YES YES

both measurements cannot be predicted with certainty

perfect correlation between Q_1 and Q_2

EXERCISE: what happens with the state $|Q_1Q_2\rangle = (|00\rangle + |01\rangle + |11\rangle/\sqrt{3}$. Is it entangled?



"spooky action at a distance"

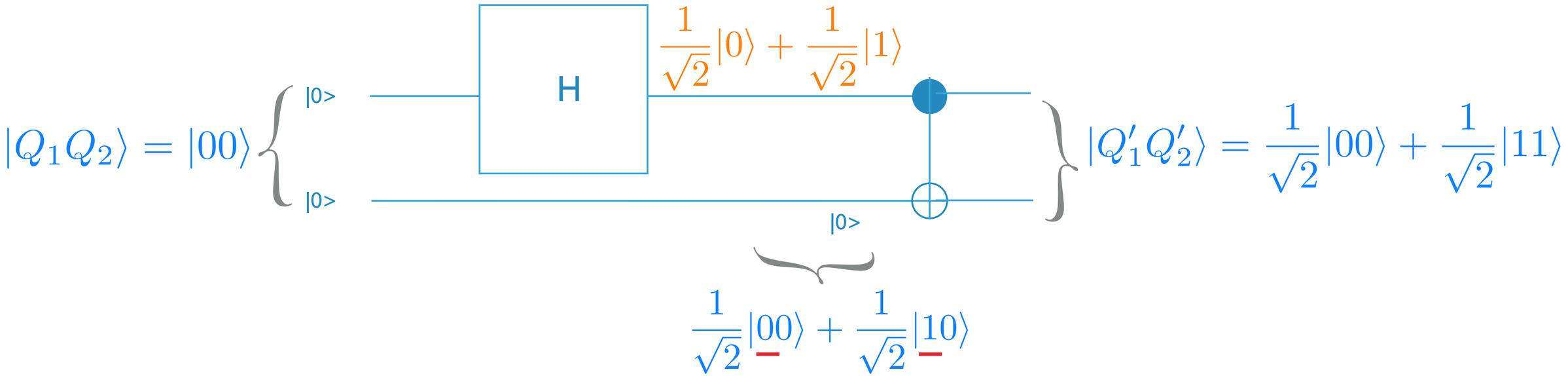
no matter how far away the two qubits are

and instantaneously

EPR paradox, hidden variables, Bell's inequalities …

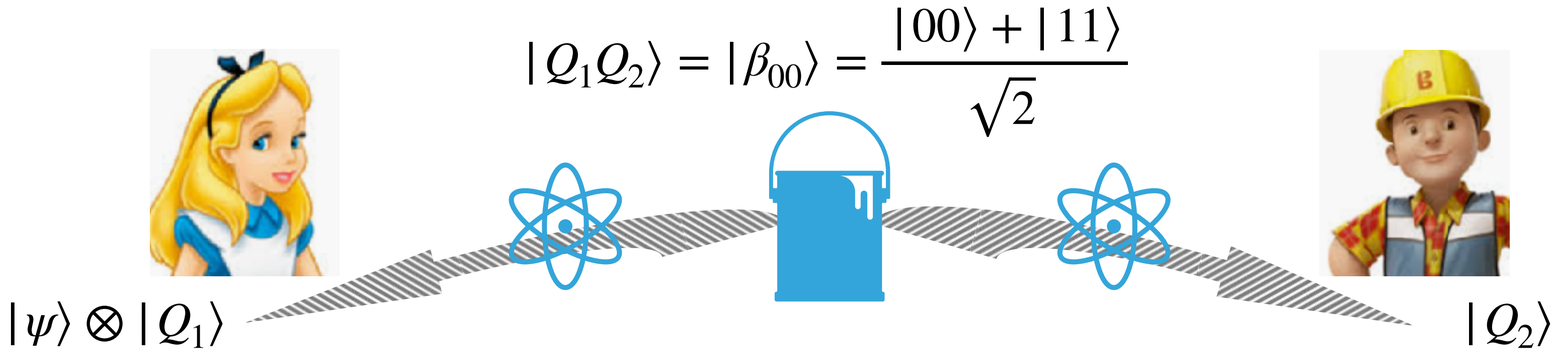
- Examples of maximally entangled states

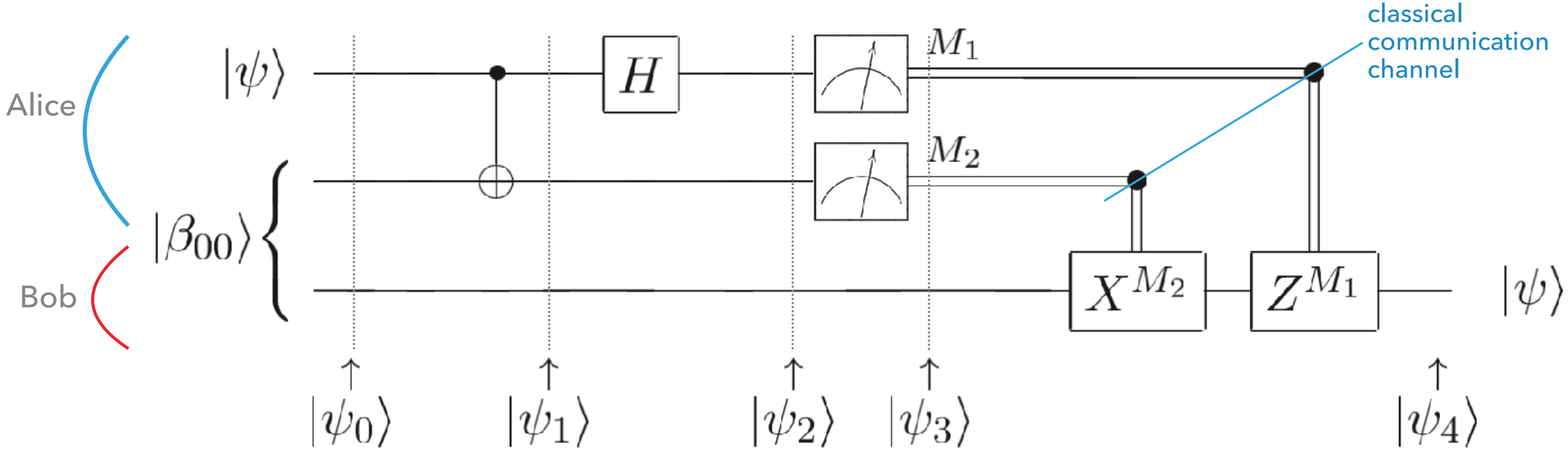
$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$$
$$|\Phi^-\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle - |11\rangle\right)$$
$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle + |10\rangle\right)$$
$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle - |10\rangle\right)$$



EXERCISE: $|Q_1Q_2\rangle = |01\rangle, |10\rangle, |11\rangle.$

- Protocol to teleport an *unknown quantum state* (not a qubit!) from Alice to Bob





$$|\psi_0\rangle = |\psi\rangle \otimes |\beta_{00}\rangle$$

$$= \frac{1}{\sqrt{2}}\left[a|0\rangle(|00\rangle + |11\rangle) + b|1\rangle(|00\rangle + |11\rangle)\right]$$

(ψ A B; c t t c t t)

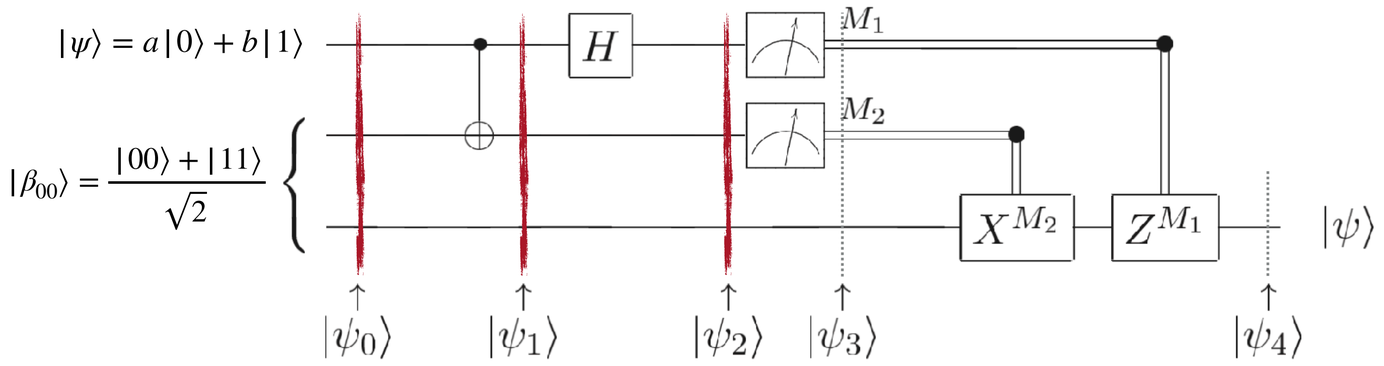
CNOT

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

H

(ψ A B)

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



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

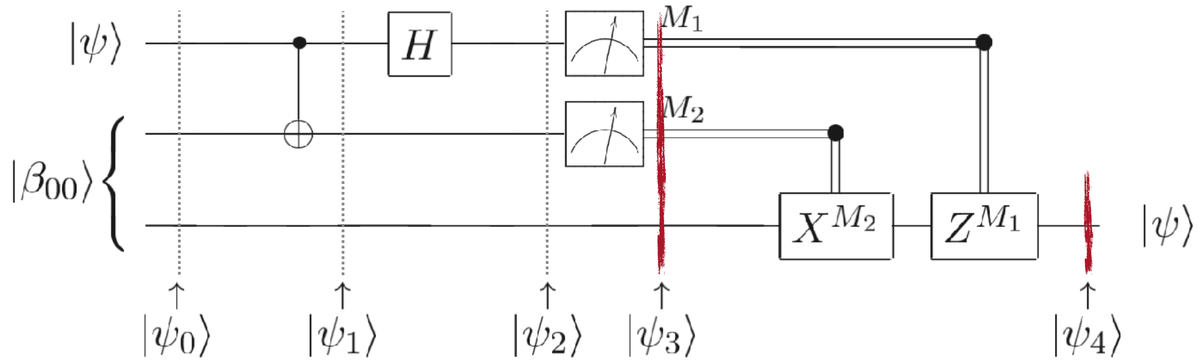
(ψ A B)

Now Alice makes a measurements on the computational basis on its two qubits, getting the results (M_1, M_2): $|\psi_3\rangle = |\psi_3^A\rangle \otimes |\psi_3^B\rangle$

(M_1, M_2)	$\|\psi_3^A\rangle$	$\|\psi_3^B\rangle$	$\|\psi\rangle =$
(0,0)	$\|00\rangle$	$a\|0\rangle + b\|1\rangle$	$\mathbb{I}(a\|0\rangle + b\|1\rangle)$
(0,1)	$\|01\rangle$	$b\|0\rangle + a\|1\rangle$	$X(b\|0\rangle + a\|1\rangle)$
(1,0)	$\|10\rangle$	$a\|0\rangle - b\|1\rangle$	$Z(a\|0\rangle - b\|1\rangle)$
(1,1)	$\|11\rangle$	$-b\|0\rangle + a\|1\rangle$	$ZX(-b\|0\rangle + a\|1\rangle)$

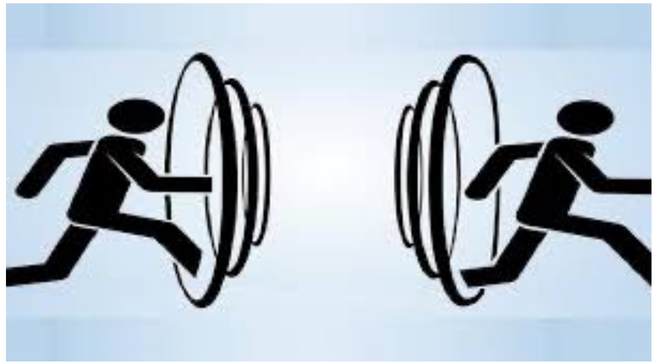
Finally Alice uses a *classical communication channel* to tell Bob the values of (M_1, M_2) and Bob makes the transformation:

$$|\psi_4\rangle = Z^{M_1} X^{M_2} |\psi_3^B\rangle = |\psi\rangle$$



Thus: entanglement is not a “spooky” characteristics of quantum mechanics.

It is actually a **resource** to build protocols that are more efficient or even do not exist in classical computation.



QUESTIONS.

Are we violating relativity because we can teleport faster than light?

Is this protocol violating the no-cloning theorem?

Quantum teleportation across the Danube

Rupert Ursin, Thomas Jennewein, Markus Aspelmeyer, Rainer Kaltenbaek, Michael Lindenthal, Philip Walther & Anton Zeilinger

Nature **430**, 849(2004) | Cite this article

Ground-to-satellite quantum teleportation

Ji-Gang Ren, Ping Xu, [...] Jian-Wei Pan

Nature **549**, 70–73(2017) | Cite this article

6382 Accesses | **224** Citations | **1018** Altmetric | Metrics

PRX QUANTUM **1**, 020317 (2020)

Teleportation Systems Toward a Quantum Internet

Raju Valivarthi,[1,2] Samantha I. Davis,[1,2] Cristián Peña,[1,2,3] Si Xie,[1,2] Nikolai Lauk,[1,2] Lautaro Narvácz,[1,2] Jason P. Allmaras,[4] Andrew D. Beyer,[4] Yewon Gim,[2,5] Meraj Hussein,[2] George Iskander,[1] Hyunseong Linus Kim,[1,2] Boris Korzh,[4] Andrew Mueller,[1] Mandy Rominsky,[3] Matthew Shaw,[4] Dawn Tang,[1,2] Emma E. Wollman,[4] Christoph Simon,[6] Panagiotis Spentzouris,[3] Daniel Oblak,[6] Neil Sinclair,[1,2,7] and Maria Spiropulu[1,2,*]

- Two c-bits (x_1, x_2), and a Boolean function $f(x_1, x_2) \rightarrow 0,1$ which can be

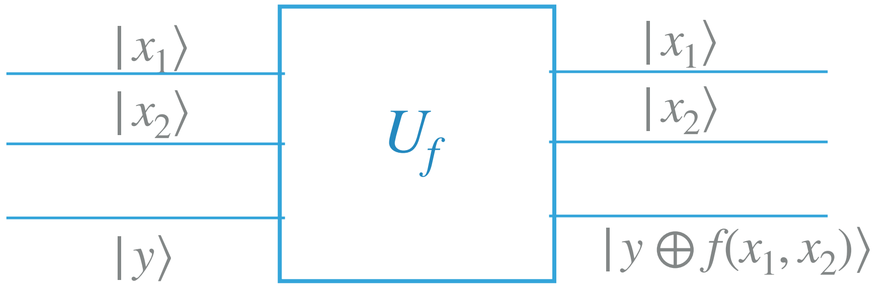
  either constant $f(x_1, x_2) \equiv 0,1$

  or balanced $f(x_1, x_2) = 0(1)$ for half of the possible inputs

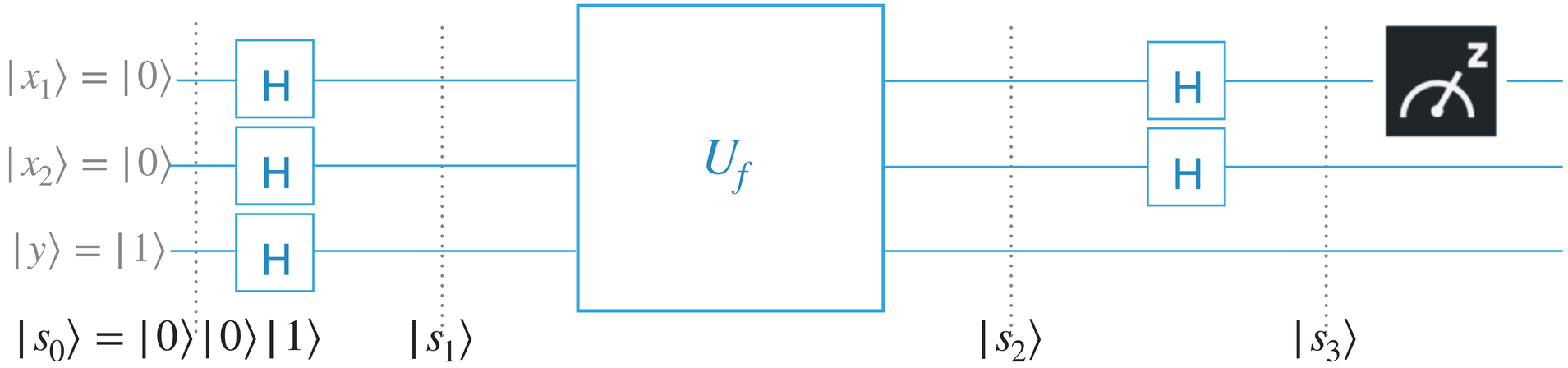
- Classically, to determine whether f is constant or balanced, we have to try 3 of the 4 possibilities $(x_1, x_2) = (0,0), (0,1), (1,0), (1,1)$
- A quantum algorithm can do it just in one shot (quantum parallelism)

for each Boolean function $(x_1, x_2) \rightarrow f(x_1, x_2)$

we can construct the quantum gate "controlled-f"



EXERCISE: do the calculations that are outlined in the following.



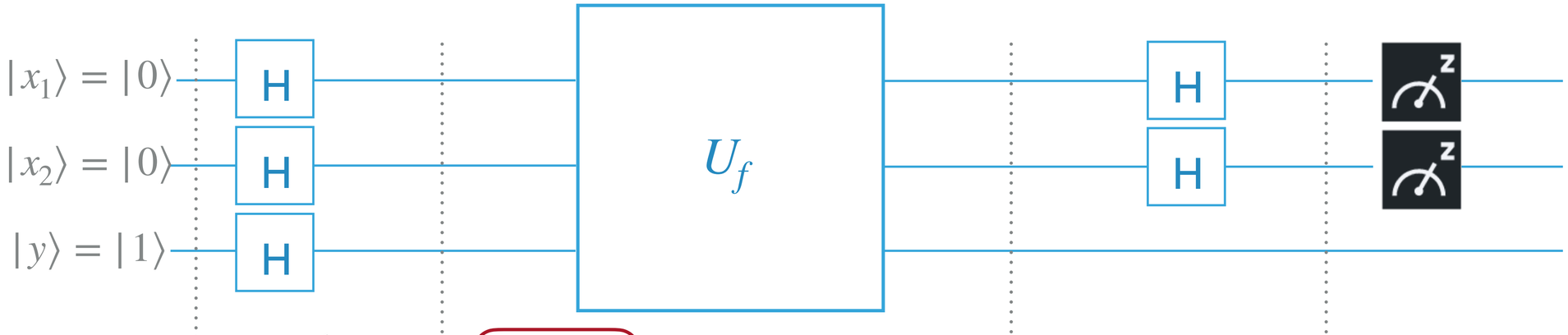
$$|s_1\rangle = \frac{1}{2^{3/2}}\left(|0\rangle+|1\rangle\right)\left(|0\rangle+|1\rangle\right)\left(|0\rangle-|1\rangle\right) = \frac{1}{2^{3/2}}\left(|00\rangle+|01\rangle+|10\rangle+|11\rangle\right)\left(|0\rangle-|1\rangle\right)$$

$$= \frac{1}{2^{3/2}}\sum_{x_1,x_2=0,1}|x_1x_2\rangle\left(|0\rangle-|1\rangle\right)$$

$$|s_2\rangle = \frac{1}{2^{3/2}}\left[|00\rangle|0\oplus f(0,0)\rangle+|01\rangle|0\oplus f(0,1)\rangle+|10\rangle|0\oplus f(1,0)\rangle+|11\rangle|0\oplus f(0,0)\rangle\right]$$

$$-\frac{1}{2^{3/2}}\left[|00\rangle|1\oplus f(0,0)\rangle+|01\rangle|1\oplus f(0,1)\rangle+|10\rangle|1\oplus f(1,0)\rangle+|11\rangle|1\oplus f(0,0)\rangle\right]$$

$$= \frac{1}{2^{3/2}}\sum_{x_1,x_2=0,1}(-1)^{f(x_1,x_2)}|x_1x_2\rangle\left(|0\rangle-|1\rangle\right)$$



- $f = f_0 = 0/1$ *const.*

$$|s_2\rangle = \frac{(-1)^{f_0}}{2^{3/2}} \left[\sum_{x_1,x_2=0,1} |x_1 x_2\rangle \right] \left(|0\rangle - |1\rangle\right)$$

$$|s_3\rangle = (-1)^{f_0} |x_1 = 0, x_2 = 0\rangle \left(|0\rangle - |1\rangle\right)/\sqrt{2}$$

since $H^2 = I$

measure of Q_1, Q_2 *on* $|s_3\rangle$ *yields* 00 *with probability* 1

- f *balanced*

$$(-1)^{f(x_1,x_2)} = \pm 1 \text{ twice each}$$

$$|s_3\rangle = \sum_{x_1,x_2=0,1 (x_1,x_2)\neq(0,0)} (\cdots) |x_1, x_2\rangle \left(|0\rangle - |1\rangle\right)/\sqrt{2}$$

measure of Q_1, Q_2 *on* $|s_3\rangle$ *yields* 00 *with probability* 0