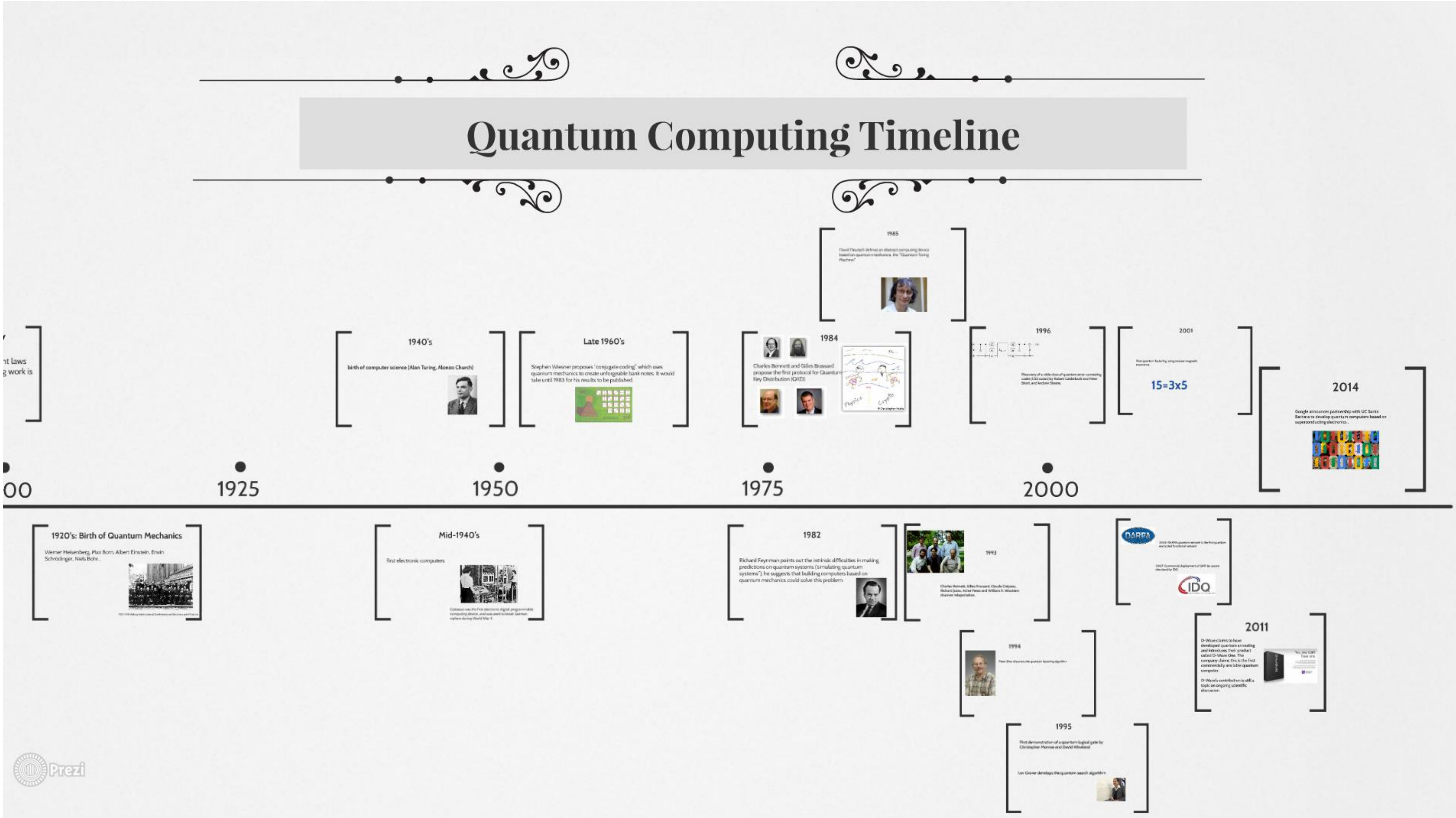
CROSSING Winter School on Quantum Cryptography

- Lecture 1 & 2: Basics of Quantum Information

Presented by: Anne Broadbent, January 25, 2016



[see my Prezi presentation (online)](http://bit.ly/1vOr6f1)

http://bit.ly/1vOr6f1

Quantum Cryptography

- the art and science of exploiting quantum mechanical effects in order to perform cryptographic tasks.

Fundamental advantages compared to classical (non-quantum):

- Uncloneable money
- Quantum Key Distribution
- Bit Commitment
  ⟹Oblivious Transfer
- Device-Independent Cryptography
- ....

Unique limitations and challenges:

- Impossibility of Quantum Bit Commitment
- Quantum Rewinding
- Superposition Access to Oracles
- …

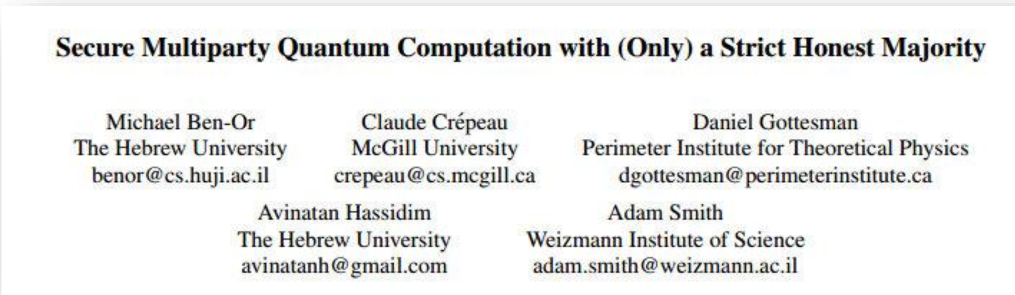
Survey paper: *Quantum Cryptography Beyond Quantum Key Distribution* (with C. Schaffner) Designs, Codes and Cryptography (2016). E-print: 2015/1242. arXiv:1510.06120

Quantum Overload

Quantum bit commitment

using quantum information in order to achieve a classical functionality.

Quantum multiparty computation



Secure Multiparty Quantum Computation with (Only) a Strict Honest Majority

Michael Ben-Or, The Hebrew University, benor@cs.huji.ac.il
Claude Crépeau, McGill University, crepeau@cs.mcgill.ca
Daniel Gottesman, Perimeter Institute for Theoretical Physics, dgottesman@perimeterinstitute.ca
Avinatan Hassidim, The Hebrew University, avinatanh@gmail.com
Adam Smith, Weizmann Institute of Science, adam.smith@weizmann.ac.il

using quantum information in order to achieve a quantum functionality.

Universally Composable Quantum Multi-party Computation*

Dominique Unruh

Saarland University

… or using quantum information in order to achieve a classical functionality.

Roadmap

- Introduction to the simplest mathematical formalism for quantum information: the pure state formalism.

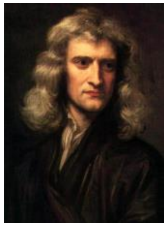
- Prerequisites: linear algebra (matrices, vectors, linear transformations); complex numbers

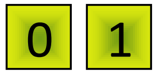
- Objectives:
  - Understand the essential technical tools in the pure state formalism for quantum information.
  - Appreciate quantum information at an intuitive level.
  - Apply the technical tools in simple applications.

Warning: the density matrix formalism is a much more elegant and expressive model for quantum information
See lectures by Serge Fehr this afternoon!

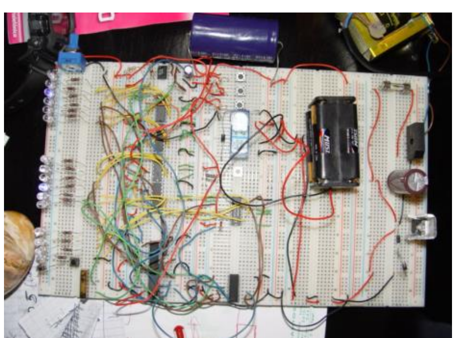
“Classical” = “Non-Quantum”

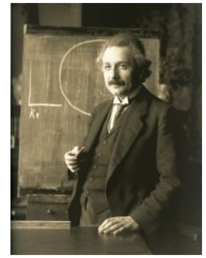
Information is physical

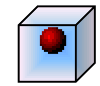




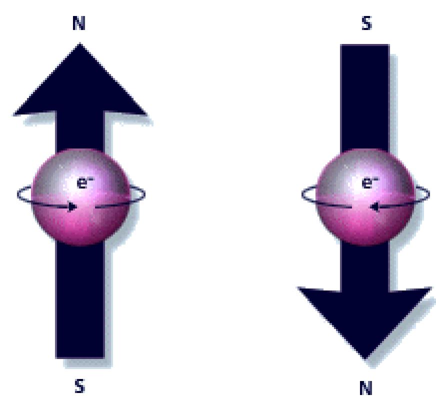
- bit: can be represented by an electrical voltage in an electronic circuit.
- Obeys the laws of classical physics







- **qu**antum **bit** (qubit): can be represented by electron spin, photon polarization, quantum dot, etc.
- Obeys the laws of quantum physics



Qubits ("quantum states")

$|0\rangle$: a column vector in Dirac notation; "ket".

$\langle 0|$: a row vector in Dirac notation; "bra".

$$\langle\psi|\,|\phi\rangle \equiv \langle\psi|\phi\rangle$$

"bra-ket"
(=inner product)

A *pure qubit* can be in one of the basis states:

$$|0\rangle \equiv \begin{pmatrix}1\\0\end{pmatrix} \qquad |1\rangle \equiv \begin{pmatrix}0\\1\end{pmatrix}$$

It can also be in a *superposition*,

$$\alpha\,|0\rangle + \beta\,|1\rangle = \begin{pmatrix}\alpha\\ \beta\end{pmatrix}$$

where $\alpha, \beta \in \mathbb{C}, |\alpha|^2 + |\beta|^2 = 1$.

Systems of qubits are combined with the tensor product:

$$\begin{pmatrix}\alpha_1\\ \beta_1\end{pmatrix} \otimes \begin{pmatrix}\alpha_2\\ \beta_2\end{pmatrix} \equiv \begin{pmatrix}\alpha_1\alpha_2\\ \alpha_1\beta_2\\ \beta_1\alpha_2\\ \beta_1\beta_2\end{pmatrix}$$

e.g. $|0\rangle \otimes |1\rangle \equiv |01\rangle = \begin{pmatrix}0\\1\\0\\0\end{pmatrix}$

More generally, an n-qubit pure system can be in an arbitrary superposition of 2^n basis states: $|00\cdots0\rangle, |00\cdots1\rangle, \ldots, |11\cdots1\rangle$,

$$\sum_x \alpha_x\,|x\rangle\,, \sum_x |\alpha_x|^2 = 1$$

Transformations

Postulate: quantum evolutions are linear

$\Longrightarrow$transformations are given by matrix multiplication.

Q: Which types of matrices are valid quantum transformations?

A: Those that map quantum states to quantum states!

e.g. Suppose $U(\alpha|0\rangle + \beta|1\rangle) = \alpha'|0\rangle + \beta'|1\rangle$

Then U is a valid quantum operation if:

$$|\alpha|^2 + |\beta|^2 = 1 \Rightarrow |\alpha'|^2 + |\beta'|^2 = 1$$

Definition: A matrix is unitary if it preserves the Euclidean norm.

Claim: A matrix U over $\mathbb{C}$ is unitary if and only if $UU^\dagger = I$, where $U^\dagger = (U^T)^*$.

Therefore, in the pure state formalism, unitary matrices are the valid quantum transformation.

Examples of 1-qubit unitaries

Identity

$$\mathsf{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Not (aka Pauli-X)

$$\mathsf{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$\mathsf{X}\,|0\rangle = |1\rangle$$
$$\mathsf{X}\,|1\rangle = |0\rangle$$

Pauli-Z

$$\mathsf{Z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$\mathsf{Z}\,|+\rangle = |-\rangle$$
$$\mathsf{Z}\,|-\rangle = |+\rangle$$

Hadamard

$$\mathsf{H} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

$$\mathsf{HH}^\dagger = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} = \mathsf{I}$$

$$\mathsf{H}|0\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \equiv |+\rangle$$
$$\mathsf{H}|1\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle \equiv |-\rangle$$

Phase shift

$$\mathsf{R}_\theta = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix}$$

$$\mathsf{R}_\theta \mathsf{R}_\theta{}^\dagger = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & e^{-i\theta} \end{pmatrix} = \mathsf{I}$$

$$\mathsf{R}_\theta\,|0\rangle = |0\rangle$$
$$\mathsf{R}_\theta\,|1\rangle = e^{i\theta}\,|1\rangle\ (\equiv |1\rangle)$$

Global phase is irrelevant

relative phase <u>is</u> relevant

$$\mathsf{R}_\theta\,|+\rangle = \frac{1}{\sqrt{2}}(|1\rangle + e^{i\theta}\,|1\rangle)$$

Multi-qubit unitaries

Controlled-Not

$$\text{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

$$|00\rangle \mapsto |00\rangle$$
$$|01\rangle \mapsto |01\rangle$$
$$|10\rangle \mapsto |11\rangle$$
$$|11\rangle \mapsto |10\rangle$$

Tensor products of single-qubit unitaries:

e.g.

$$X \otimes X = \begin{pmatrix} 0[X] & 1[X] \\ 1[X] & 0[X] \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

In general, the matrix tensor product is:

$$A_{m\times n} = (a_{ij}),\ B_{k\times \ell},\ A \otimes B_{(mk)\times(n\ell)} = \begin{pmatrix} a_{11}[B] & a_{12}[B] & \cdots & a_{1,n}[B] \\ a_{21}[B] & \ddots & & \vdots \\ \vdots & & & \\ a_{m,1}[B] & \cdots & & a_{m,n}[B] \end{pmatrix}$$

Measurements: qubits $\longrightarrow$ bits

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

measurement outcomes:

0 with probability $|\alpha|^2$

1 with probability $|\beta|^2$

Measuring a quantum system will not, in general, give a complete description of the state:

Measurement destroys the quantum state.

$$e.g.\ \text{measure } |0\rangle \to 0$$

$$e.g.\ \text{measure } |+\rangle \to \begin{cases} 0 \text{ ,prob. } \frac{1}{2} \\ 1 \text{ ,prob. } \frac{1}{2} \end{cases} \qquad \left(|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right)$$

$$\sum_x \alpha_x |x\rangle \to x,\ \text{prob. } |\alpha_x|^2$$

Partial measurements (later)

Can measure in any basis. (later)

Summary

Two things we can do to qubits:

1. Unitary operations: U unitary $\Leftrightarrow$ $UU^\dagger = I$ $\Leftrightarrow$ $U^{-1} = U^\dagger$
   U $\Leftrightarrow$ invertible.

Reversible!

2. Measurements:

$$\alpha |0\rangle + \beta |1\rangle \Rightarrow \begin{cases} 0 \text{ with probability } |\alpha|^2, \\ 1 \text{ with probability } |\beta|^2 \end{cases}$$

Not reversible!

Warning. According to the density matrix formalism, quantum Information allows other types of operations!

Example

Suppose you are given one of the following two states:

$$|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|0\rangle$$
$$|-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|0\rangle$$

But you are not told which one. How can you determine which one it is?

- Measuring right away does not help. (why?)

- Do a Hadamard, then measure:

$$\mathrm{H}|+\rangle = |0\rangle \rightarrow 0$$
$$\mathrm{H}|-\rangle = |1\rangle \rightarrow 1$$

Notation:

$$\begin{aligned} \langle 0|\psi\rangle &= \langle 0| (\alpha|0\rangle + \beta|1\rangle) \\ &= \alpha\langle 0|0\rangle + \beta\langle 0|1\rangle \\ &= \alpha \cdot 1 + \beta \cdot 0 \\ &= \alpha \end{aligned}$$

Hence: $|\langle 0|\psi\rangle|^2$: probability of observing 0 when measuring $|\psi\rangle$.
In general, $|\langle\phi|\psi\rangle|^2$: probability of observing $|\phi\rangle$ when measuring $|\psi\rangle$.

e.g. measure $|+\rangle$ in the Hadamard basis $\{|+\rangle, |-\rangle\}$; obtain "$|+\rangle$" with certainty since $\langle +|+\rangle = 1$.

Partial measurements (by example)

Given $|\psi\rangle = \frac{1}{2}|00\rangle - \frac{i}{2}|10\rangle + \frac{1}{\sqrt{2}}|11\rangle$, what happens if you measure the first qubit only?

- What are possible outcomes and associated probabilities?
- What is the remaining quantum state for qubit 2?

Write: $|\psi\rangle = |0\rangle|\phi_0\rangle + |1\rangle|\phi_1\rangle$

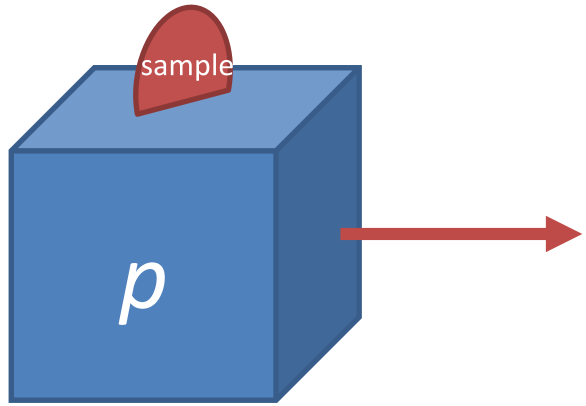
i.e. $|\psi\rangle = |0\rangle\left(\frac{1}{2}|0\rangle\right) + |1\rangle\left(\frac{-i}{2}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right)$

$\Pr[\text{outcome is } 0] = \||\phi_0\rangle\|^2 = \frac{1}{4}$. Remaining state is: $\frac{1}{\||\phi_0\rangle\|}|\phi_0\rangle = |0\rangle$.

$\Pr[\text{outcome is } 1] = \||\phi_1\rangle\|^2 = \frac{3}{4}$. Remaining state is: $\frac{1}{\||\phi_1\rangle\|}|\phi_1\rangle = \frac{-i}{\sqrt{3}}|0\rangle + \sqrt{\frac{2}{3}}|1\rangle$.

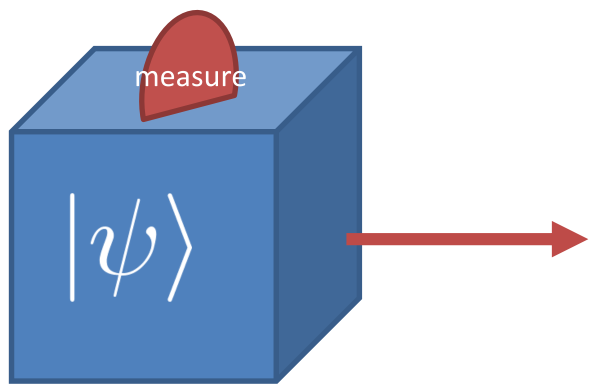
First Analogy: quantum states as generalized probability distributions

p: a probability distribution over $\{0,1\}^n$.



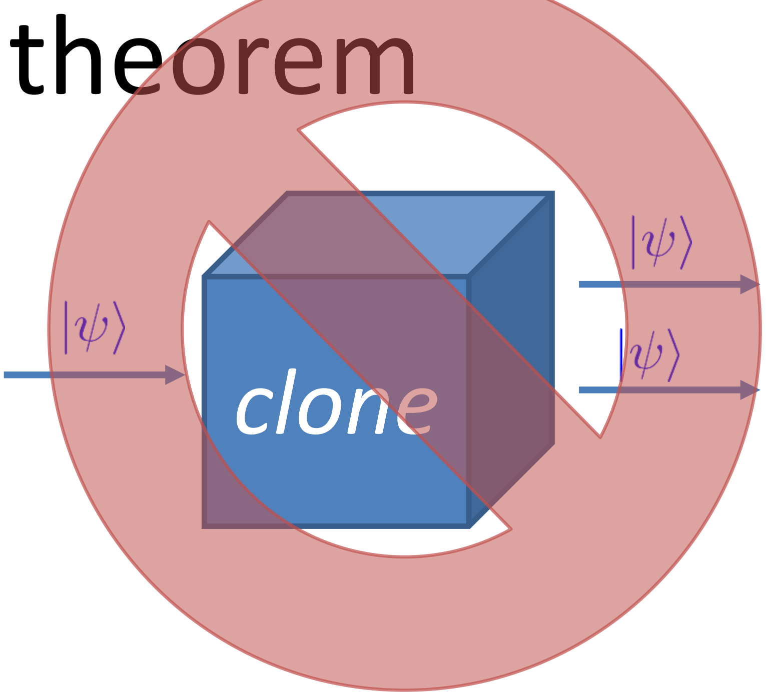
$x \in \{0,1\}^n, \ \text{prob. } p(x)$

$|\psi\rangle = \sum_{x\in\{0,1\}^n} \alpha_x \, |x\rangle$



$x \in \{0,1\}^n, \ \text{prob. } |\alpha_x|^2$

No-cloning theorem

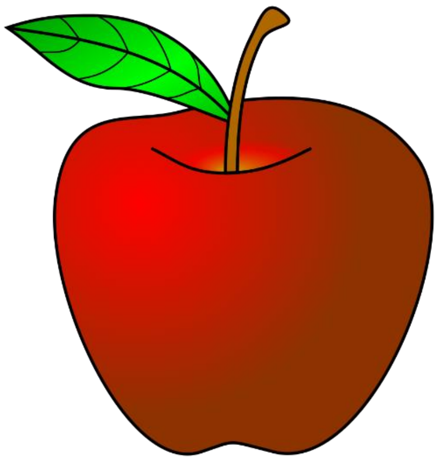


Theorem (no-cloning theorem) No two-qubit unitary U exists such that for all single-qubit $|\psi\rangle$, $U|\psi\rangle|0\rangle = |\psi\rangle|\psi\rangle$.

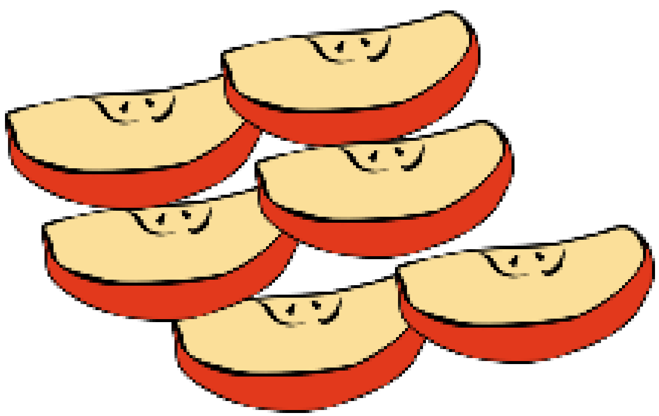
Proof. Suppose such a U exists. Let $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. Then:
$U|\psi\rangle|0\rangle = |\psi\rangle|\psi\rangle = (\alpha|0\rangle+\beta|1\rangle)\otimes(\alpha|0\rangle+\beta|1\rangle) = \alpha^2|00\rangle+\alpha\beta|01\rangle+\beta\alpha|10\rangle+\beta^2|11\rangle$.
Also:
$U|0\rangle|0\rangle = |00\rangle$
$U|1\rangle|0\rangle = |11\rangle$

By linearity, $U(\alpha|0\rangle + \beta|1\rangle)|0\rangle = \alpha U|00\rangle + \beta U|10\rangle = \alpha|00\rangle + \beta|11\rangle$.
This contradicts the first expression for $U|\psi\rangle|0\rangle$ (*e.g.* take $\alpha = \beta = \frac{1}{\sqrt{2}}$).

Second Analogy: Quantum States as physical objects.



$$\approx |\psi\rangle$$



Very powerful tool for quantum cryptography!

Entanglement

A quantum state is entangled over subsystems *A & B* if it cannot be written as a tensor product between sub-systems in *A* and *B*.

For instance, the *EPR-pair* $|\Phi^+\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$ is entangled:
Proof by contradiction. Suppose

$$\begin{aligned}\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle &= (\alpha_1|0\rangle + \beta_1|1\rangle) \otimes (\alpha_2|0\rangle + \beta_2|1\rangle) \\ &= \alpha_1\alpha_2|00\rangle + \alpha_1\beta_2|01\rangle + \beta_1\alpha_2|10\rangle + \beta_1\beta_2|11\rangle \\ &\Rightarrow (\alpha_1 = 0 \vee \beta_2 = 0) \wedge (\beta_1 = 0 \vee \alpha_2 = 0) \\ &\rightarrow\!\leftarrow\end{aligned}$$

The classical equivalent of entanglement is correlation.

Consequences of quantum entanglement:

- Nonlocal games (Bell inequalities)
- Teleportation
- ...

Teleportation

Suppose Alice has a qubit that she wants to send to Bob:

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$$

Question: How many classical bits are required to accomplish this?

Answer 1: depends on the desired precision; α and β are arbitrary complex numbers, but Alice can send an approximation of these values to Bob.

Answer 2: no number of classical bits will suffice:

- Alice may not know (α, β); she cannot perform a measurement to extract (α, β)
- Alice's qubits may be entangled with others; no classical communication can transmit the entanglement.

Teleportation

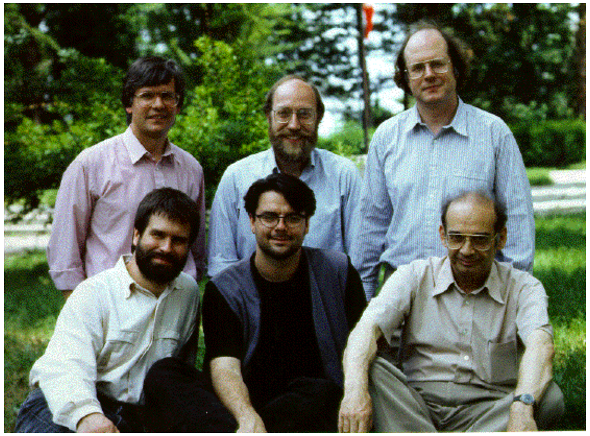
Suppose Alice has a qubit that she wants to send to Bob:

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$$

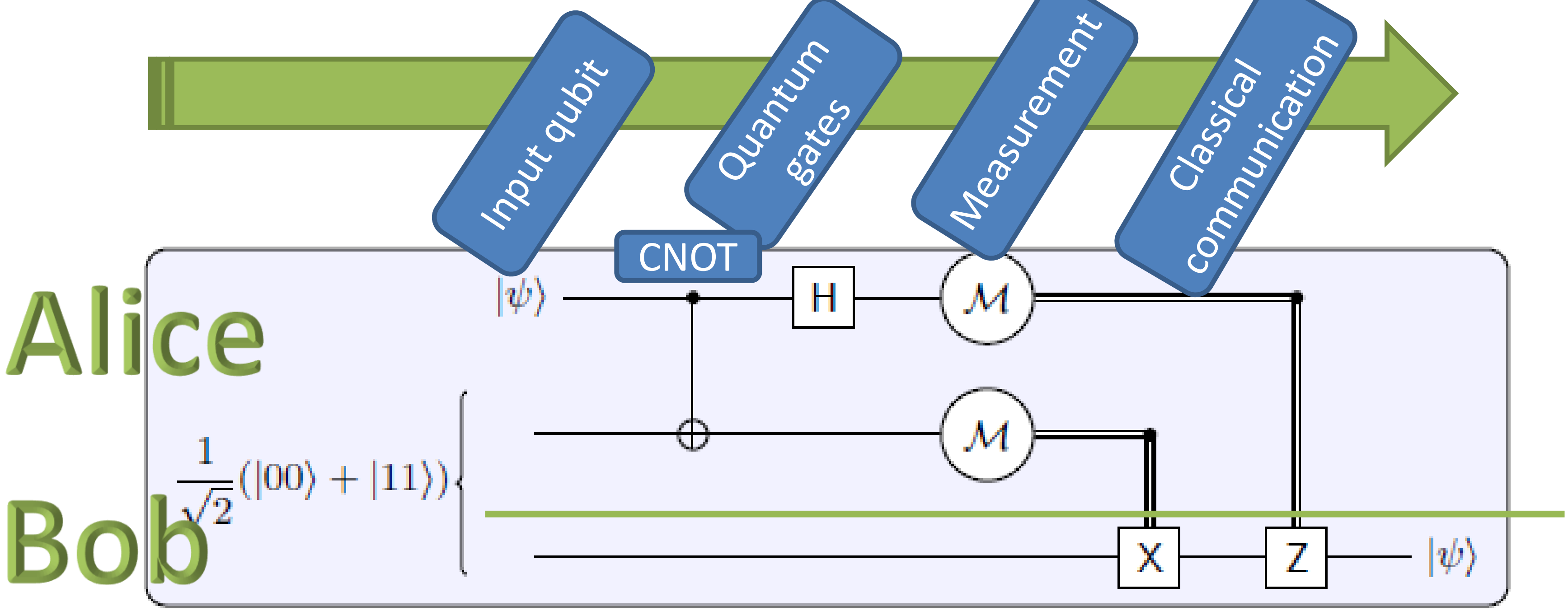
Question: How many classical bits are required to accomplish this, if we allow Alice and Bob to share entanglement ahead of time?

Answer: two bits of classical communication suffice if Alice and Bob share entanglement ahead of time.

Charles H. Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres, and William K. Wootters,



Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels.
Physical Review Letters (1993)



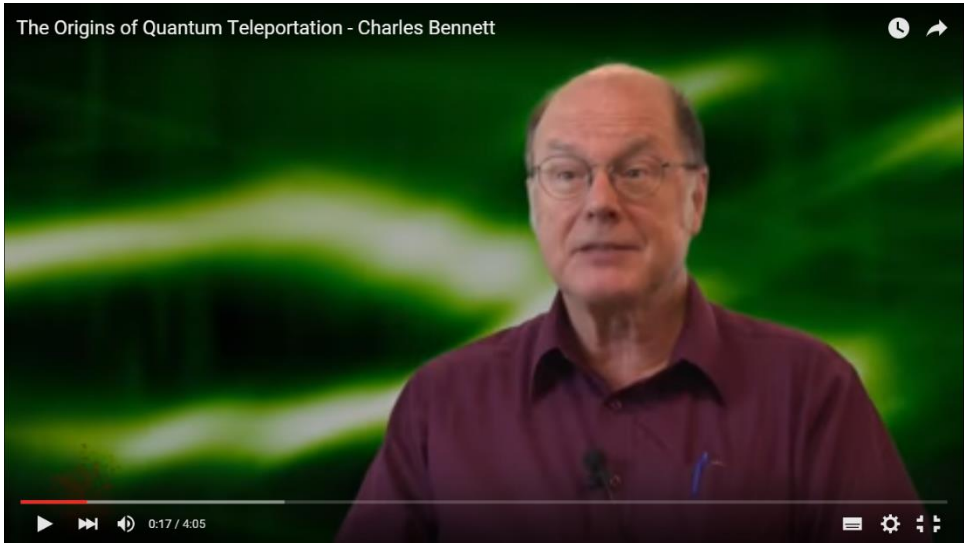
$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

$$(\alpha|0\rangle + \beta|1\rangle) \otimes \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(\alpha|000\rangle + \alpha|011\rangle + \beta|100\rangle + \beta|111\rangle)$$

$$\xrightarrow{\text{CNOT}\otimes\text{I}} \frac{1}{\sqrt{2}}(\alpha|000\rangle + \alpha|011\rangle + \beta|110\rangle + \beta|101\rangle)$$

$$\xrightarrow{\text{H}\otimes\text{I}\otimes\text{I}} \frac{1}{\sqrt{2}}(\alpha(|000\rangle + |100\rangle + |011\rangle + |111\rangle) + \beta(|010\rangle - |110\rangle + |001\rangle - |101\rangle)$$

$$= \frac{1}{\sqrt{2}}(|00\rangle\underbrace{(\alpha|0\rangle + \beta|1\rangle)}_{|\psi\rangle} + |01\rangle\underbrace{(\alpha|1\rangle + \beta|0\rangle)}_{\text{X}|\psi\rangle} + |10\rangle\underbrace{(\alpha|0\rangle - \beta|1\rangle)}_{\text{Z}|\psi\rangle} + |11\rangle\underbrace{(\alpha|1\rangle - \beta|0\rangle)}_{\text{XZ}|\psi\rangle})$$



[Charles Bennett](#) on the origins of teleportation (4min.)

[Gilles Brassard](#) on the meaning of teleportation (2.5min.)

Quantum Information Textbooks

- *Quantum Computation and Quantum Information* by Michael Nielsen and Isaac Chuang (Cambridge University Press, 2000)

- *An Introduction to Quantum Computing* by Philip Kaye, Raymond Laflamme and Michele Mosca (Oxford University Press, 2007)

- *Quantum Computing: A Gentle Introduction* by Eleanor Rieffel and Wolfgang Polak (MIT Press, 2011)

Quantum Information online references

- Courses/lecture notes
  - Ronald de Wolf's lecture notes http://homepages.cwi.nl/~rdewolf/qcnotes.pdf
  - John Watrous lecture notes https://cs.uwaterloo.ca/~watrous/LectureNotes.html
- Textbooks
  - Mark Wilde's *Quantum Information Theory* http://arxiv.org/abs/1106.1445
  - John Watrous's *Theory of Quantum Information* https://cs.uwaterloo.ca/~watrous/TQI/
- Pre-print server
  - arxiv.org/archive/quant-ph
- Wikis
  - Quantum Algorithms Zoo math.nist.gov/quantum/zoo/
  - Complexity Zoo https://complexityzoo.uwaterloo.ca/Complexity_Zoo
  - Quantiki https://quantiki.org/

Thank you!