Introduction to quantum computing and simulability

General overview of the field

Daniel J. Brod

Leandro Aolita

Ernesto Galvão

Instituto de Física
Universidade Federal Fluminense

Outline: General overview of the field

- What is quantum computing?
  - A bit of history;
- The rules: the postulates of quantum mechanics;
- Information-theoretic-flavoured consequences;
  - Entanglement;
  - No-cloning;
  - Teleportation;
  - Superdense coding;

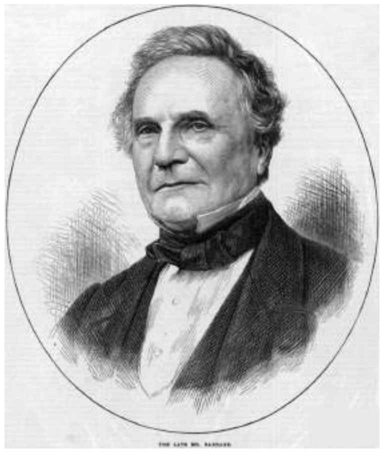
What is quantum computing?

- Computing **paradigm** where information is processed with the rules of quantum mechanics.
- **Extremely** interdisciplinary research area!
  - Physics, Computer science, Mathematics;
  - Engineering (the thing looks nice on paper, but building it is **hard**!);
  - Chemistry, biology and others (applications);
- Promised speedup on certain computational problems;
- New *insights* into foundations of quantum mechanics and computer science.

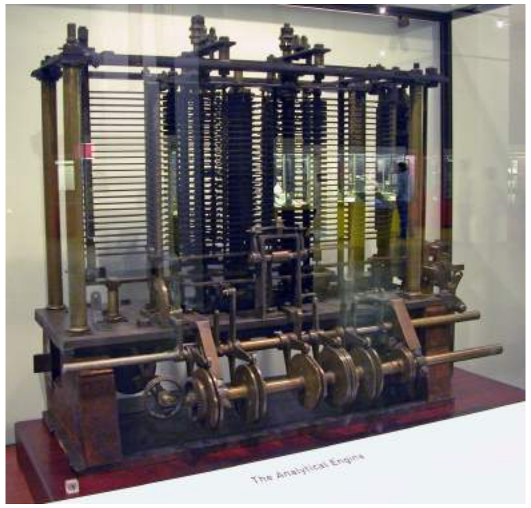
Let’s begin with some history!

Timeline of (classical) computing

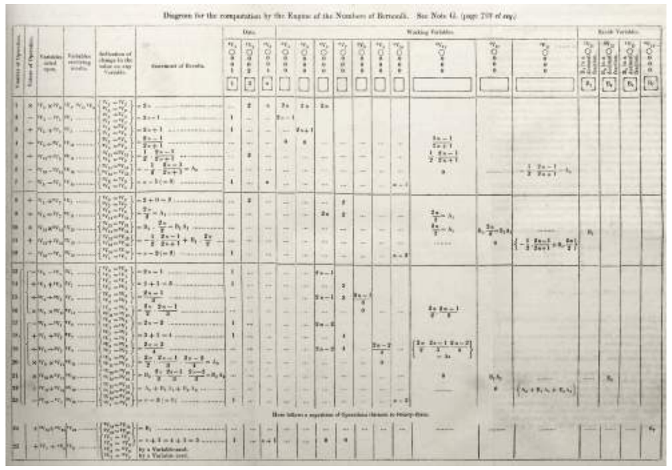
Charles Babbage
(1791-1871)



Ada Lovelace
(1815-1852)



Analytical Engine (1837)
First proposed general purpose mechanical computer. Not completed by lack of money ☹

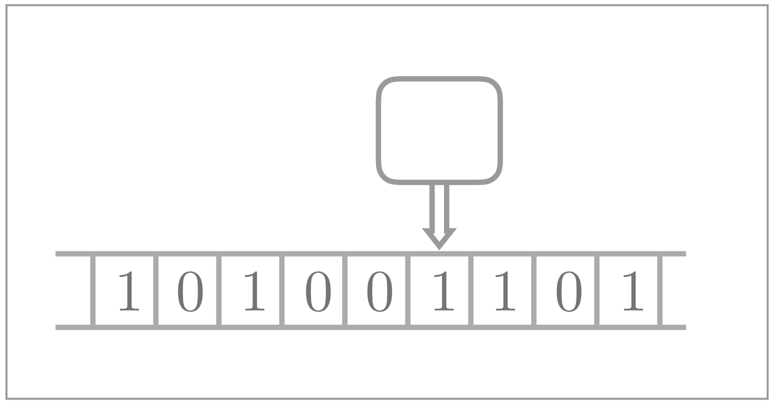


First computer program (1843)
Written by Ada Lovelace for the Analytical engine. Computes Bernoulli numbers.

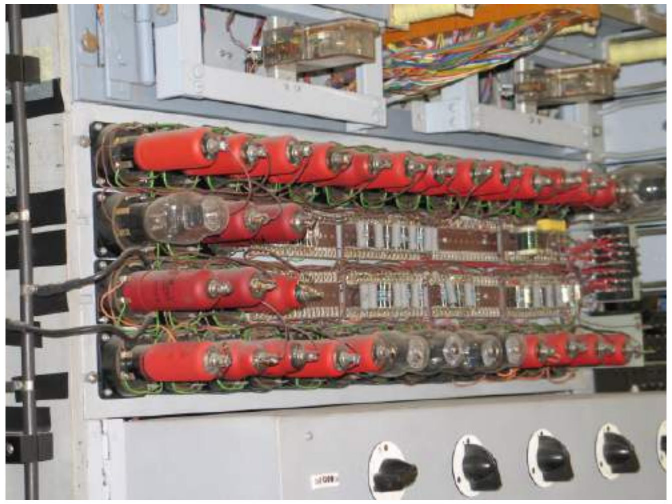
Timeline of (classical) computing

Alonzo Church
(1903-1995)

Alan Turing
(1912-1954)

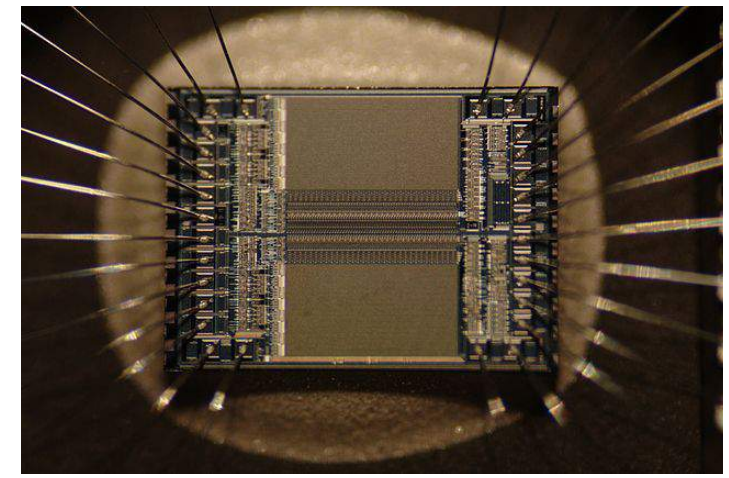


Turing Machine (1936)
Abstract model for a **universal** computing device.



World War II
Colossus, Bombe, Z3/Z4 and others;
- Decryption of secret messages;
- Ballistics;

Timeline of (classical) computing



Intel® 4004 (1971)
2.300 transistors.
Intel® Core™ (2010)
560.000.000 transistors.

Transistor (1947)
Replaces valves in previous computers
Kickstarted flurry of miniaturisation!

Physics!

Physics and computing

Landauer's Principle (1961)
"Any irreversible logical manipulation of information, such as erasing a bit, releases heat"

Rolf Landauer
(1927-1999)

Reversible computation (1973)
A universal computer can be both logically and thermodynamically reversible

Charles Bennett
(1943 -)

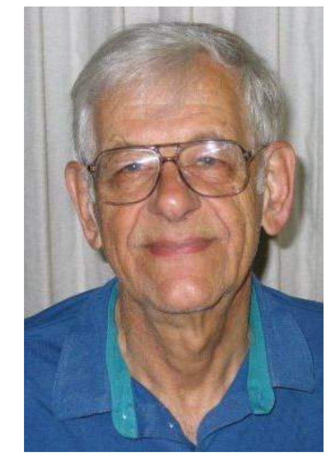
The birth of quantum computing (1980-1982)

“First Conference on the Physics of Computation”

Feynman: simulating a quantum system on a computer is hard. What if we used another quantum system to do the simulation?

Benioff: First recognisable theoretical framework for a quantum computer

Paul Benioff
(1930-)



Richard Feynman
(1918-1988)

Quantum Criptography (1984)

First proposal to use quantum mechanics for distribution of cryptographic keys (BB84 scheme)
(Leandro will talk more about this!)

Giles Brassard
(1955-)

Charles Bennett
(1943 -)

Quantum Turing machine (1985)

First proposal of a universal quantum computer that can solve problems faster than a classical computer

David Deutsch
(1953-)

<u>Shor's algorithm</u> (1994)

Algorithm for factoring large integers exponentially faster than known classical algorithms.
Could break many cryptosystems used today!

Peter Shor
(1959-)

<u>Quantum error correction</u> (1995)

Shor and Steane propose the first quantum error correction protocols. Quantum computers are now feasible <u>in principle</u>.

Andrew Steane

<u>Grover's algorithm</u> (1996)

Algorithm that quadratically speeds up database search. Useful for a large variety of problems.

Lov Grover
(1961-)

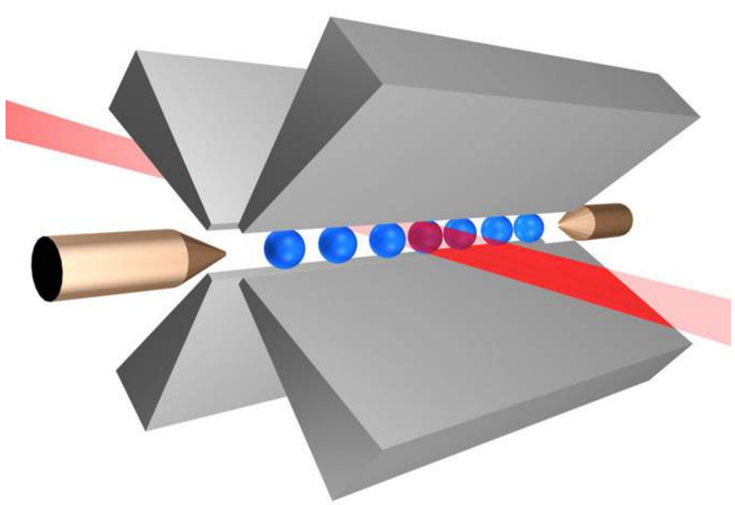
Experiments!

Many other developments
(that we will discuss
throughout the week)!

Experimental quantum computing

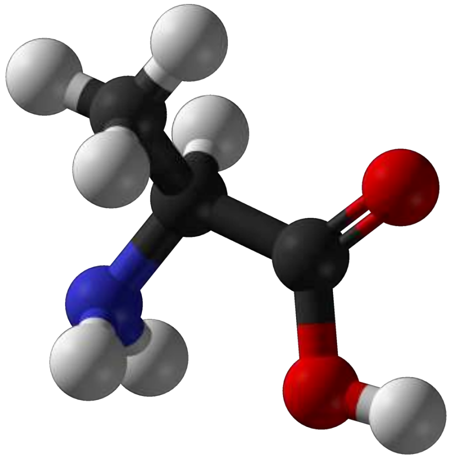
1995
NIST (Boulder, Colorado)

First quantum logic gate (CNOT) using trapped ions



1998
Oxford, IBM + Stanford + MIT

First quantum algorithms (Deutch-Jozsa and Grover) using NMR qubits



Experimental quantum computing

2007 - Today
D-Wave Systems (Vancouver)

D-Wave claims to have first alleged commercial quantum computers
28 (2007) to 2048 qubits (2017)
Some controversy ensued!

2011
Bristol

Record implementation of Shor's algorithm:

21 = 3 x 7

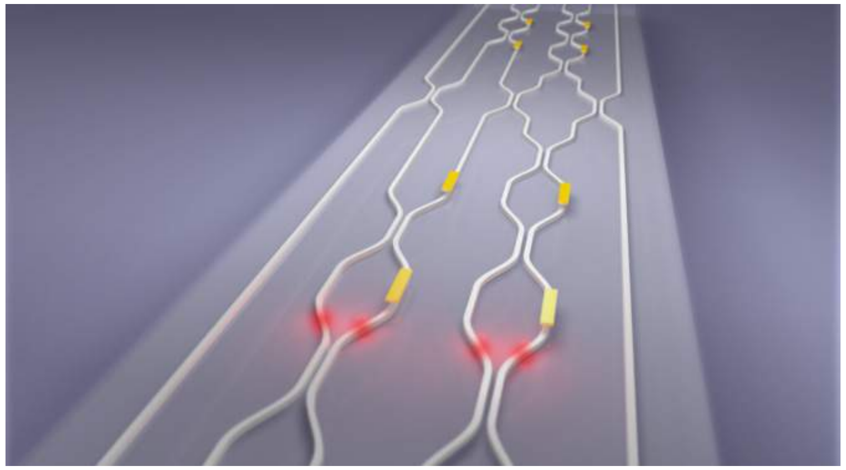
(with high probability!)

Experimental quantum computing

2012
Oxford, Vienna, Brisbane and Rome

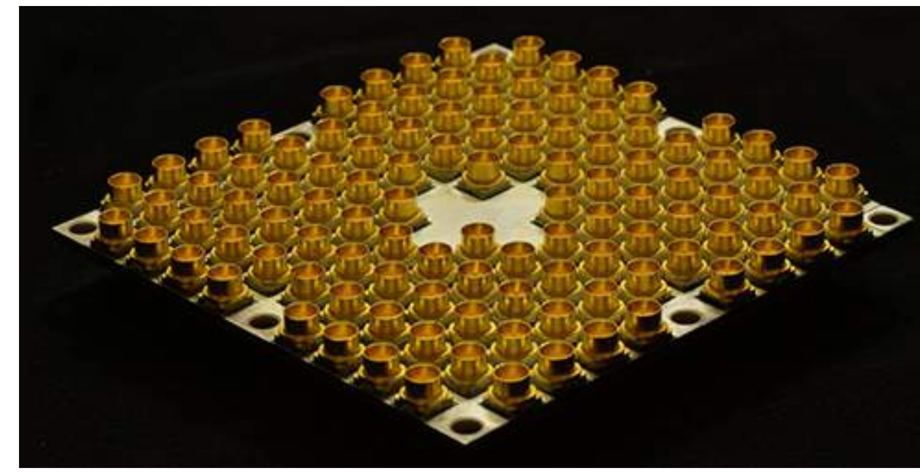
First demonstration of “Quantum advantage” experiments (BosonSampling)

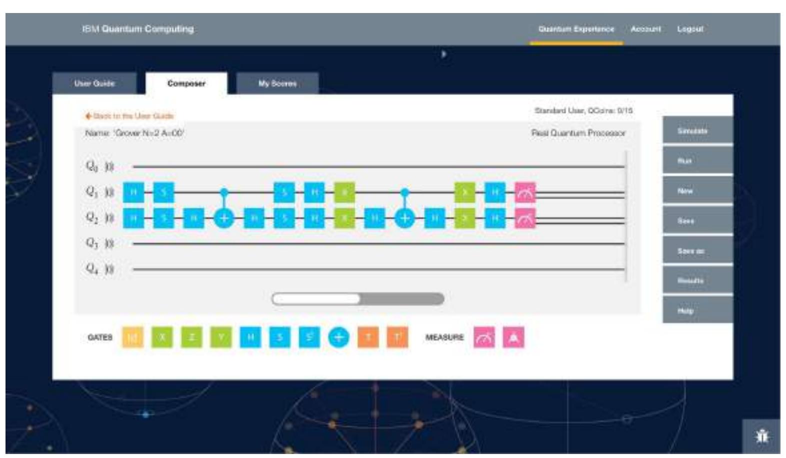
I’ll focus on this on Thursday and Friday!



Experimental quantum computing

Intel’s Tangle Lake
49 qubits





IBM
16 qubits that you can play with!

Google + UCSB’s Bristlecone
49 qubits, to shortly become 72!

Outline: General overview of the field

- What is quantum computing?
  - A bit of history;
- The rules: the postulates of quantum mechanics;
- Information-theoretic-flavoured consequences;
  - Entanglement;
  - No-cloning;
  - Teleportation;
  - Superdense coding;

Postulate 1: The states

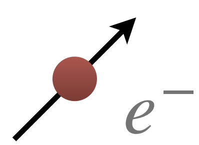
Postulate 1

To any isolated physical system we can associate a complex vector space with inner product. *States* of the system are unit vectors in this state space.

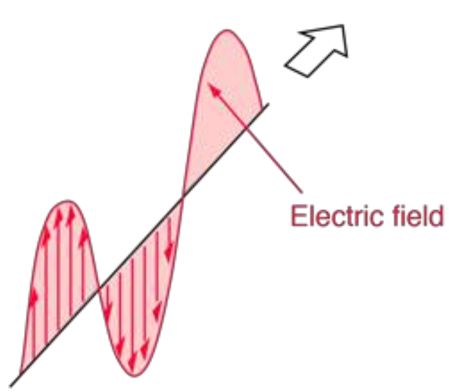
Postulate 1: The states

- Examples

dim = 2

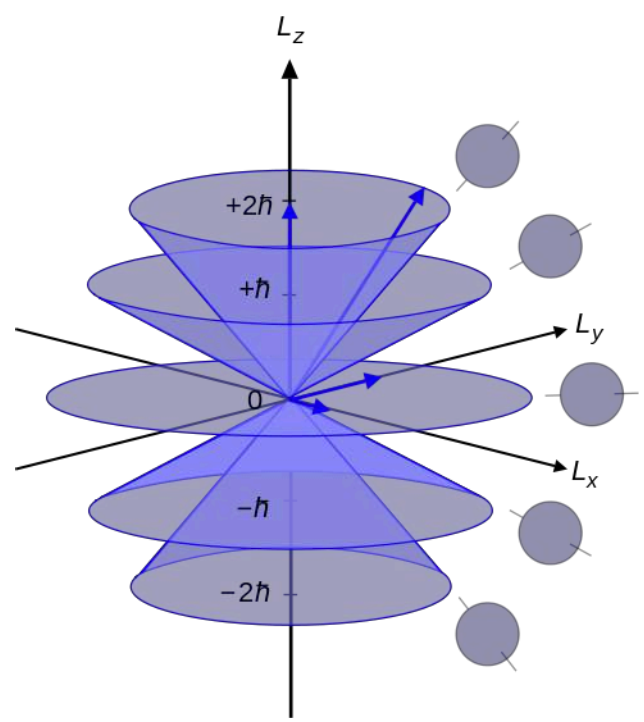


$|\uparrow\rangle, |\downarrow\rangle$



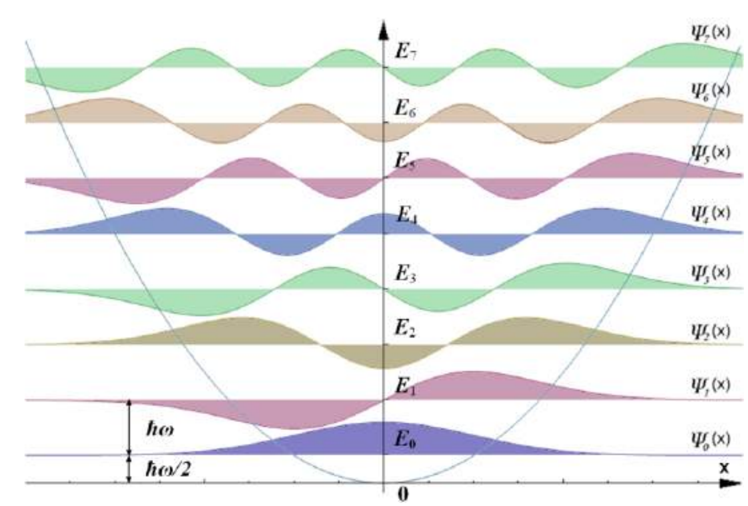
$|H\rangle, |V\rangle$

dim = $2l+1$



$|-l\rangle, |-l+1\rangle \ldots |+l\rangle$

dim = ∞



$|0\rangle, |1\rangle, |2\rangle \ldots$

Postulate 1: The states

- Here we (often) abstract away the physical system.
- Meet your new friend: **the qubit!**
  - Orthonormal basis:

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

  - This special basis is known as the **computational** basis;
  - Arbitrary state:

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

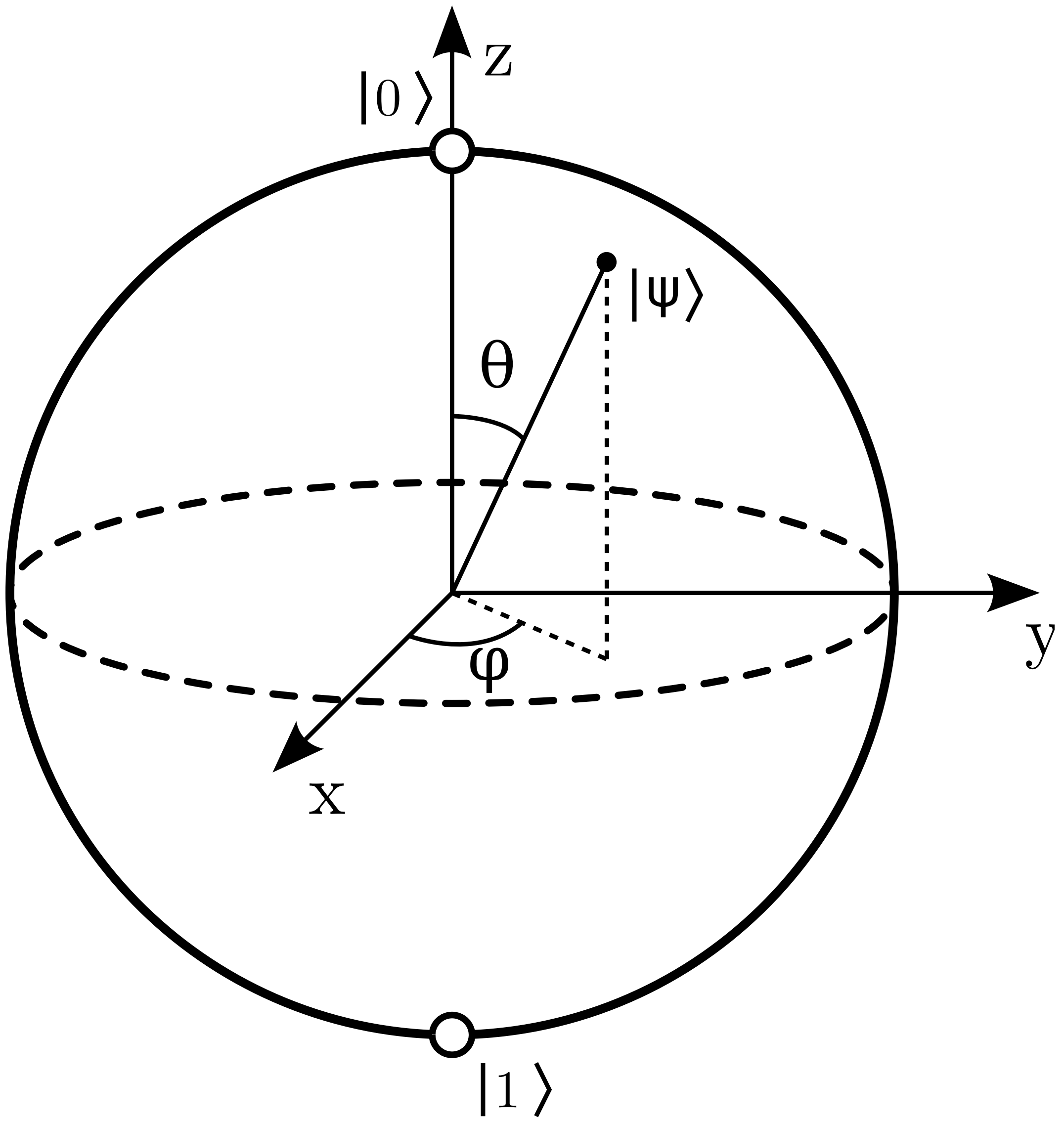
$$\Rightarrow |\alpha|^2 + |\beta|^2 = 1$$

Postulate 1: The states

- Here we (often) abstract away the physical system.
- Meet your new friend: **the qubit!**
- Why restrict to qubits?
    - Abstract representation lets us focus on general results.
    - For computation, qubits are more than enough.

Postulate 1: The states

- Useful geometrical picture: the Bloch sphere



$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\phi}\sin\left(\frac{\theta}{2}\right)|1\rangle$$

Postulate 2: Dynamics

Postulate 2

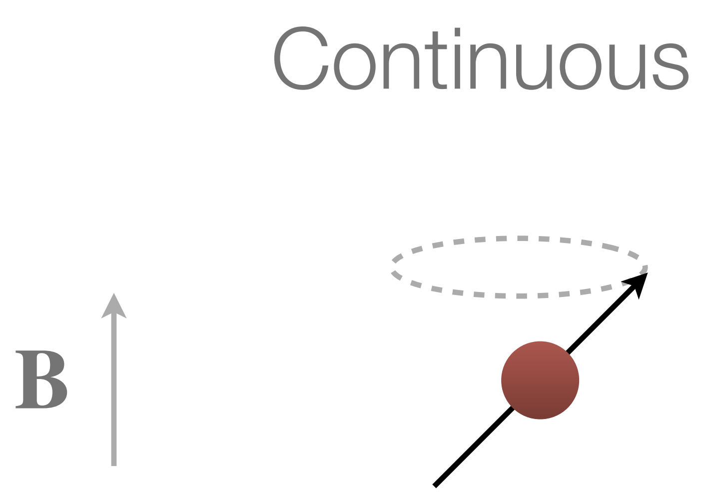
The evolution of a **closed** quantum system is described by unitary transformations.

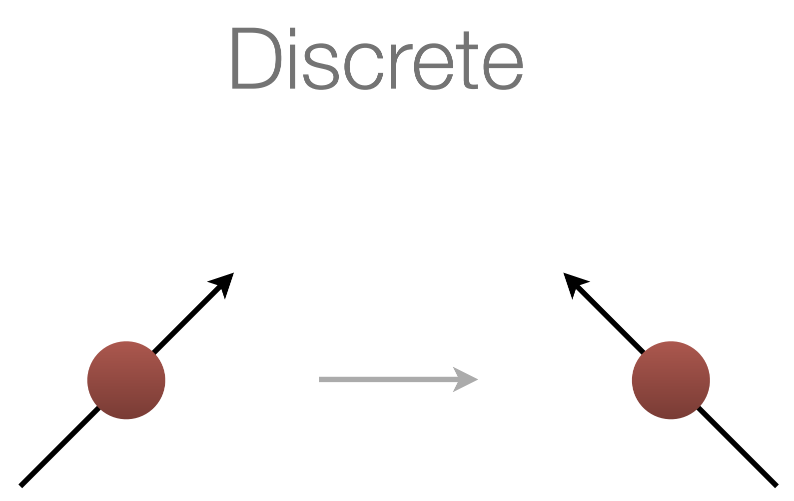
Postulate 2: Dynamics

- For quantum system of dimension d, **any** dynamics can be written as:

$$|\psi_f\rangle = U|\psi_i\rangle, \;\; UU^\dagger = I_d$$

- This is a **discrete-time** version of the dynamics postulate.
    - It is equivalent **in every way** to the Schrödinger equation.





Postulate 3: Measurements

Postulate 3 (for qubits)

A measurement has two classical outcomes, a and b, and corresponds to an orthonormal basis for the state space, e.g. $\mathcal{B} = \{|a\rangle, |b\rangle\}$. The probabilities for both outcomes are given by the Born rule, and the post-measurement state is the basis state corresponding to the outcome.

Postulate 3: Measurements

- For an arbitrary state:

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

- Outcomes of a computational-basis measurement:

0, with prob. $|\alpha|^2$ and post-measurement state $|0\rangle$

1, with prob. $|\beta|^2$ and post-measurement state $|1\rangle$

Postulate 3: Measurements

- For an arbitrary state:

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

- Outcomes of a measurement in basis $\{|a\rangle, |b\rangle\}$:
- Decompose state in this basis:

$$|\psi\rangle = \gamma|a\rangle + \delta|b\rangle$$

- Then measurement results are:

a, with prob. $|\gamma|^2$ and post-measurement state $|a\rangle$

b, with prob. $|\delta|^2$ and post-measurement state $|b\rangle$

Postulate 4: System composition

Postulate 4

The state space of a composite physical system is the tensor product of the state spaces of the componente systems.

Postulate 4: System composition

- Single system basis: $|i\rangle$

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

- Two-system computational basis: $|i\rangle \otimes |j\rangle = |ij\rangle$

$$|00\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \qquad |01\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \qquad |10\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \qquad |11\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

Outline: General overview of the field

- What is quantum computing?
  - A bit of history;
- The rules: the postulates of quantum mechanics;
- Information-theoretic-flavoured consequences;
  - Entanglement;
  - No-cloning;
  - Teleportation;
  - Superdense coding;

Separable and entangled states

- A two-qubit state can be a product of two single-qubit states:

$$
\begin{aligned}
|\psi\rangle &= \left(a|0\rangle + b|1\rangle\right)\left(c|0\rangle + d|1\rangle\right) \\
&= ac|00\rangle + ad|01\rangle + bc|10\rangle + bd|11\rangle
\end{aligned}
$$

- In this case, we call it a **product** state.
- The most general state is not of that form:

$$
|\psi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle
$$

- If a state is not separable, it is **entangled**.

Separable and entangled states

- Examples:

$$\frac{1}{\sqrt{2}}\left(|00\rangle + |01\rangle\right)$$

$$= |0\rangle\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)$$

Separable!

Separable and entangled states

- Examples:

$$\frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$$

$$\neq |\psi\rangle|\phi\rangle$$

Entangled!

Separable and entangled states

- Examples: the **Bell** states

$$\frac{1}{\sqrt{2}}\big(|00\rangle + |11\rangle\big) \qquad \frac{1}{\sqrt{2}}\big(|01\rangle + |10\rangle\big)$$

$$\frac{1}{\sqrt{2}}\big(|00\rangle - |11\rangle\big) \qquad \frac{1}{\sqrt{2}}\big(|01\rangle - |10\rangle\big)$$

The most common maximally entangled two-qubit states;

Outline: General overview of the field

- What is quantum computing?
  - A bit of history;
- The rules: the postulates of quantum mechanics;
- Information-theoretic-flavoured consequences;
  - Entanglement;
  - No-cloning;
  - Teleportation;
  - Superdense coding;

The no-cloning theorem

- Suppose we want to **clone** the state of qubit A onto qubit B.
  - We want an unitary U that does this:

$$|\psi\rangle_A|0\rangle_B \rightarrow |\psi\rangle_A|\psi\rangle_B$$

    for arbitrary $|\psi\rangle$.

  - Suppose one exists. Then:

$$\left.\begin{array}{l} U|\phi\rangle_A|0\rangle_B = |\phi\rangle_A|\phi\rangle_B \\ U|\psi\rangle_A|0\rangle_B = |\psi\rangle_A|\psi\rangle_B \end{array}\right\} \quad \langle\phi|_A\langle 0|_B U^\dagger U|\psi\rangle_A|0\rangle_B = \langle\phi|_A\langle\phi|_B|\psi\rangle_A|\psi\rangle_B$$

$$\langle\phi|\psi\rangle\langle 0|0\rangle = \langle\phi|\psi\rangle\langle\phi|\psi\rangle$$

$$\langle\phi|\psi\rangle = \langle\phi|\psi\rangle^2$$

$$\Rightarrow \langle\phi|\psi\rangle = 0 \text{ or } 1$$

The no-cloning theorem

- Suppose we want to **clone** the state of qubit A onto qubit B.
    - We want an unitary U that does this:

      $$|\psi\rangle_A|0\rangle_B \to |\psi\rangle_A|\psi\rangle_B$$

      for arbitrary $|\psi\rangle$.
    - Suppose one exists. Then:

      $$\begin{aligned} U|\phi\rangle_A|0\rangle_B &= |\phi\rangle_A|\phi\rangle_B \\ U|\psi\rangle_A|0\rangle_B &= |\psi\rangle_A|\psi\rangle_B \end{aligned} \quad \Rightarrow \langle\phi|\psi\rangle = 0 \text{ or } 1$$

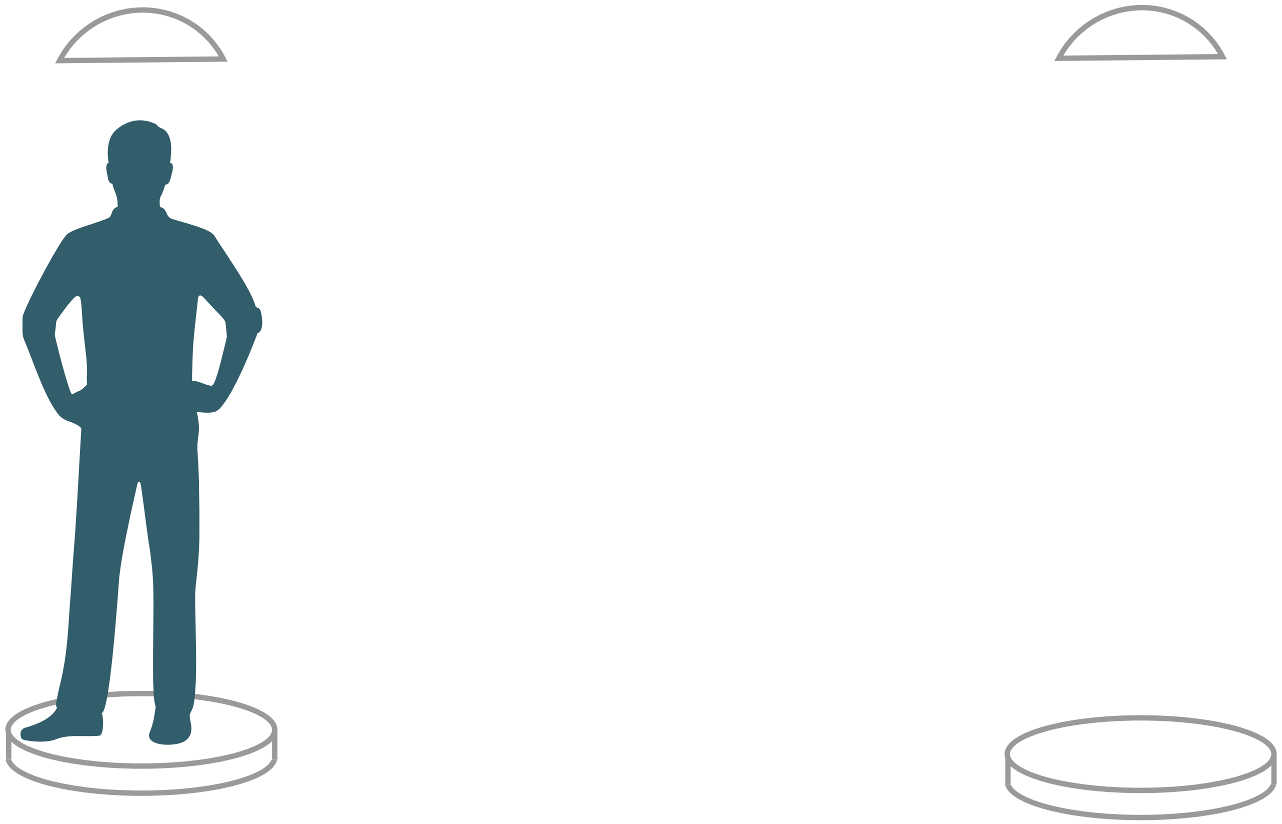
- Conclusion: we cannot clone **arbitrary** states!
    - This makes error correction **really** tricky!

Outline: General overview of the field

- What is quantum computing?
  - A bit of history;
- The rules: the postulates of quantum mechanics;
- Information-theoretic-flavoured consequences;
  - Entanglement;
  - No-cloning;
  - Teleportation;
  - Superdense coding;

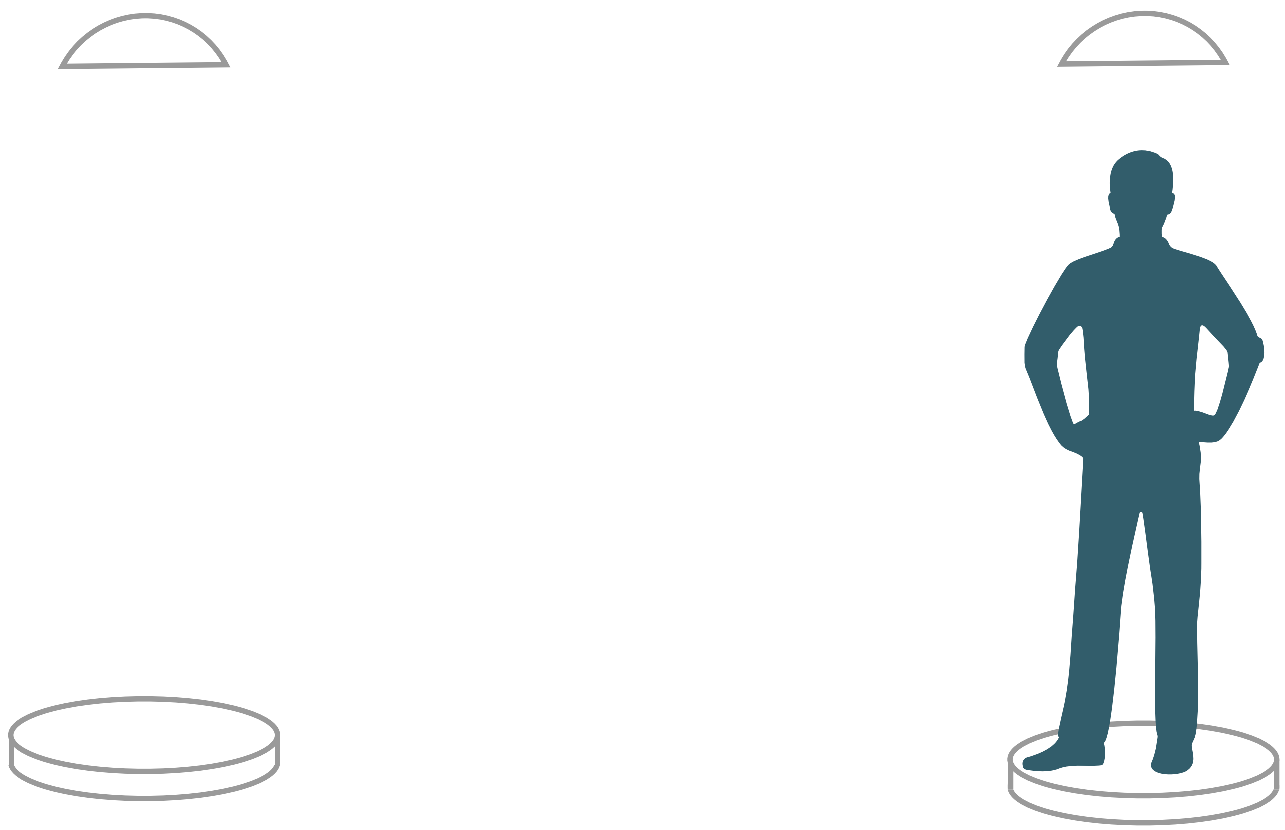
Quantum teleportation

- Suppose we want to send someone far away:



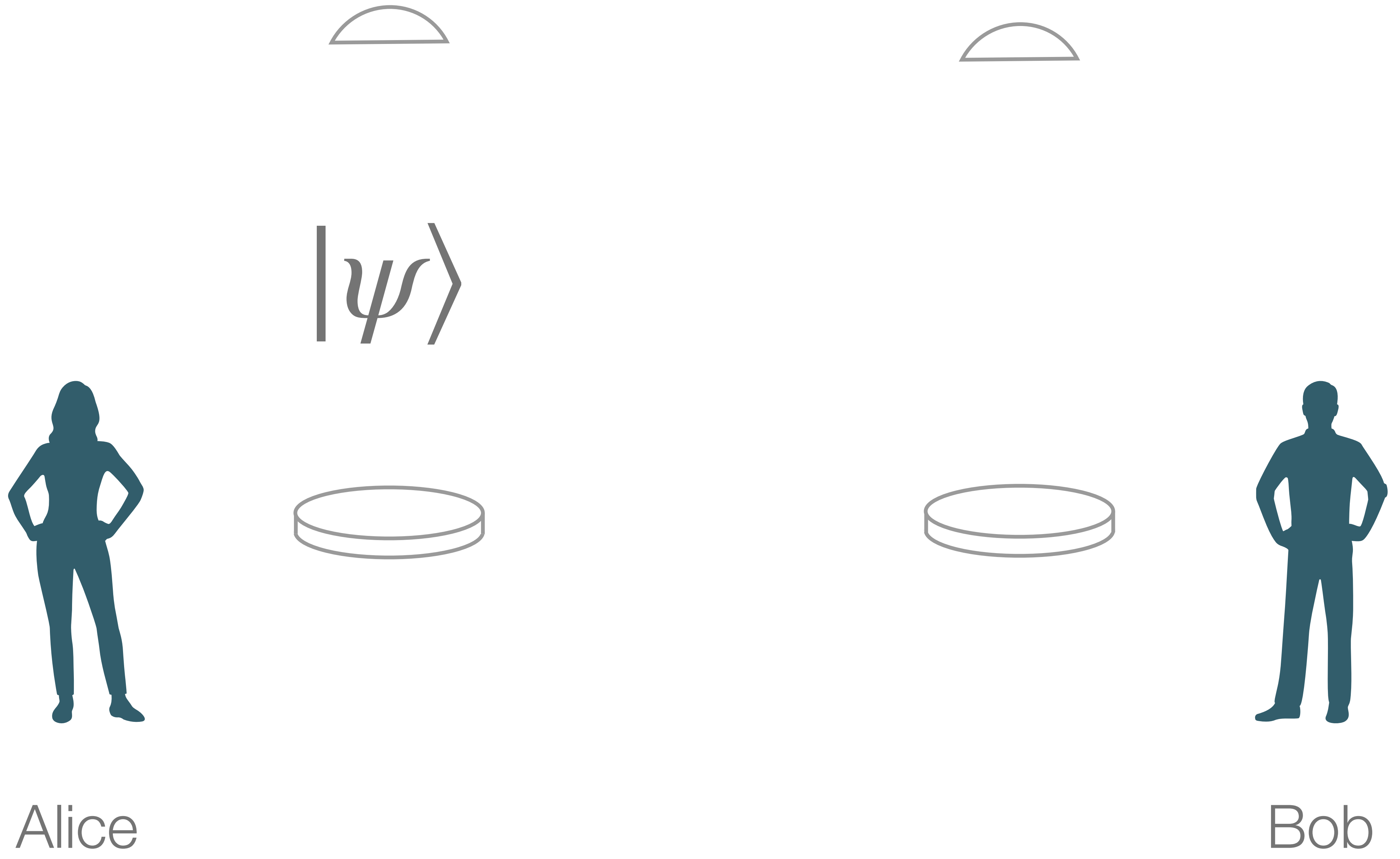
Quantum teleportation

- Suppose we want to send someone far away:



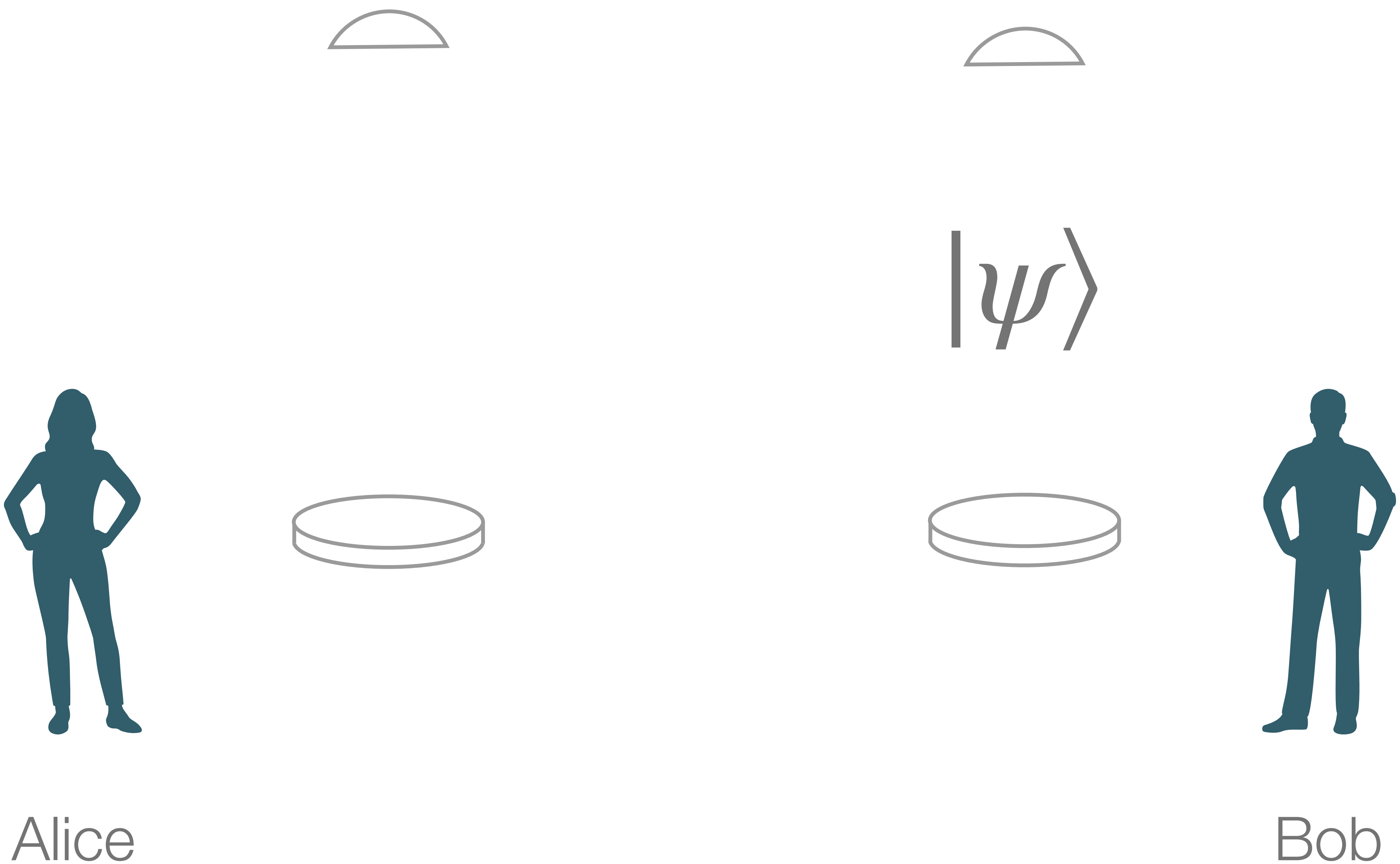
Quantum teleportation

- Suppose we want to send a **qubit** to someone far away:



Quantum teleportation

- Suppose we want to send a **qubit** to someone far away:



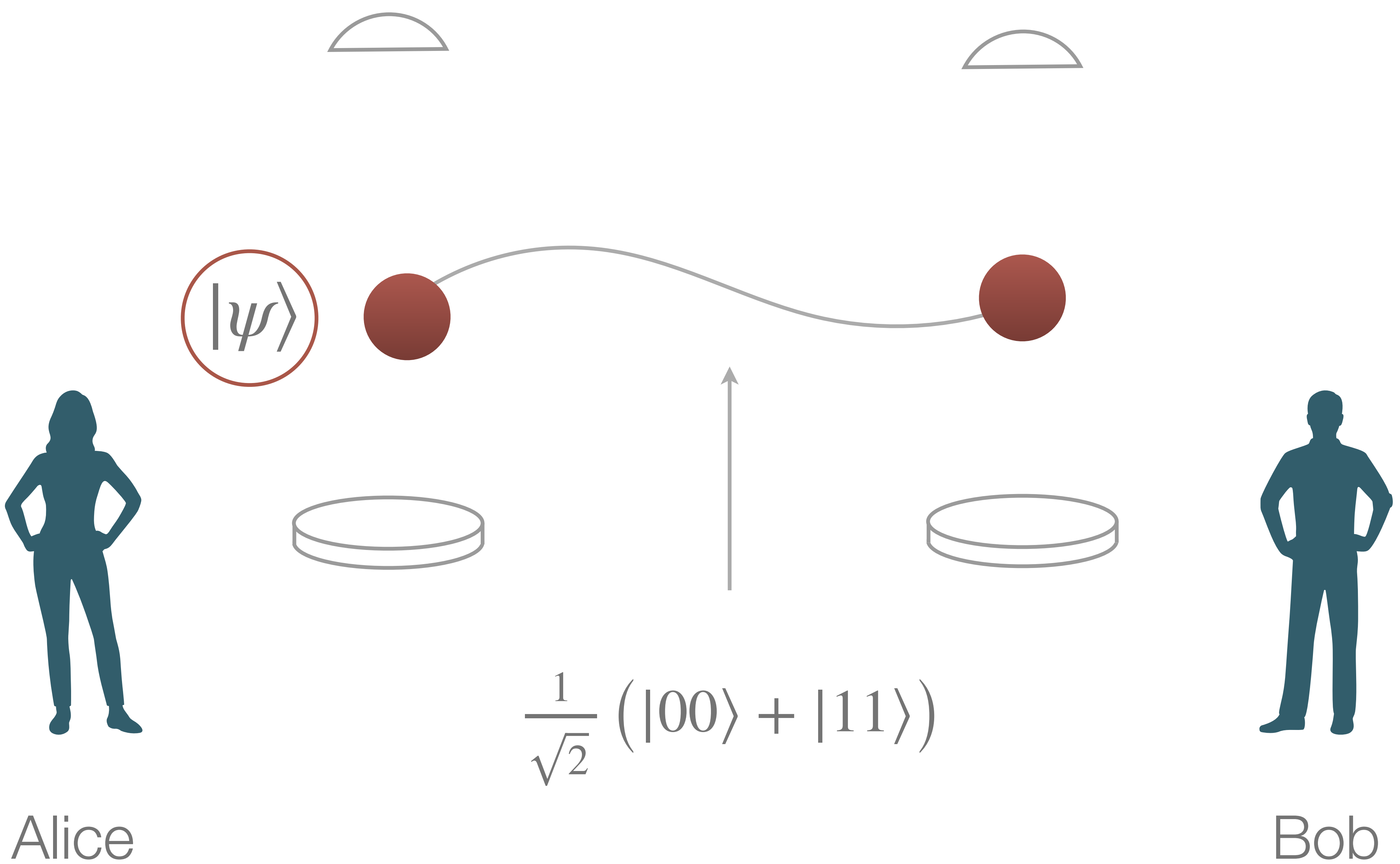
Quantum teleportation

- Suppose we want to send a **qubit** to someone far away:
  - Step 1: A and B share a Bell state, and A wants to send a state to B.

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

$$|\Phi^+\rangle_{AB} = \frac{1}{\sqrt{2}}\left(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B\right)$$

Quantum teleportation



Quantum teleportation

- Suppose we want to send a **qubit** to someone far away:
  - Step 1: A and B share a Bell state, and A wants to send a state to B.
  - Step 2: A applies a transformation to her two qubits and measures them in the 0/1 basis.

$$\frac{1}{\sqrt{2}}\left(\alpha|0\rangle_A + \beta|1\rangle_A\right)\left(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B\right)$$

She applies $$U = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & -1 & 0 \\ 1 & 0 & 0 & -1 \end{pmatrix}$$

Quantum teleportation

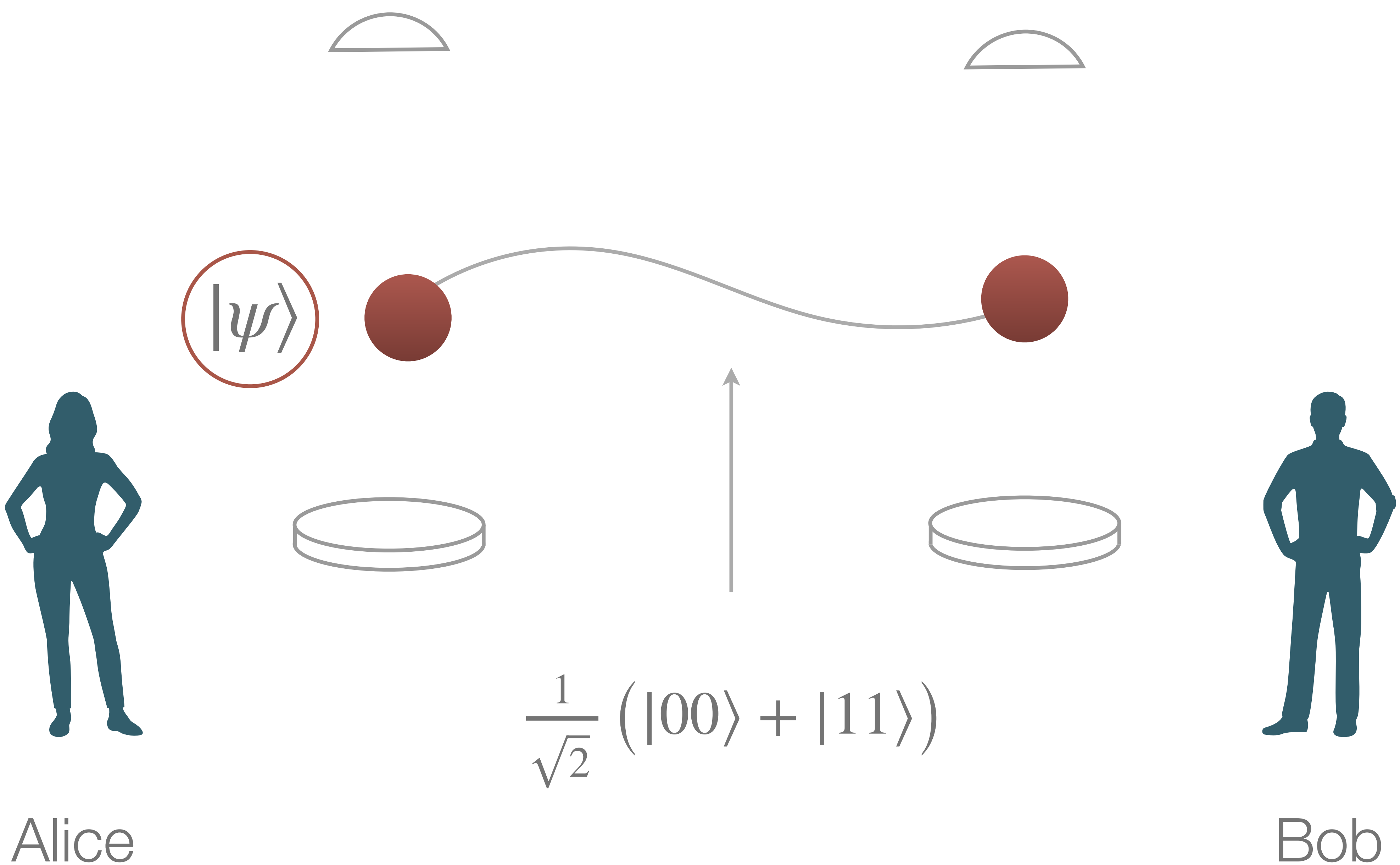
- Suppose we want to send a **qubit** to someone far away:
  - Step 1: A and B share a Bell state, and A wants to send a state to B.
  - Step 2: A applies a transformation to her two qubits and measures them in the 0/1 basis.

Measurement has 4 outcomes, which leave B with the following states*

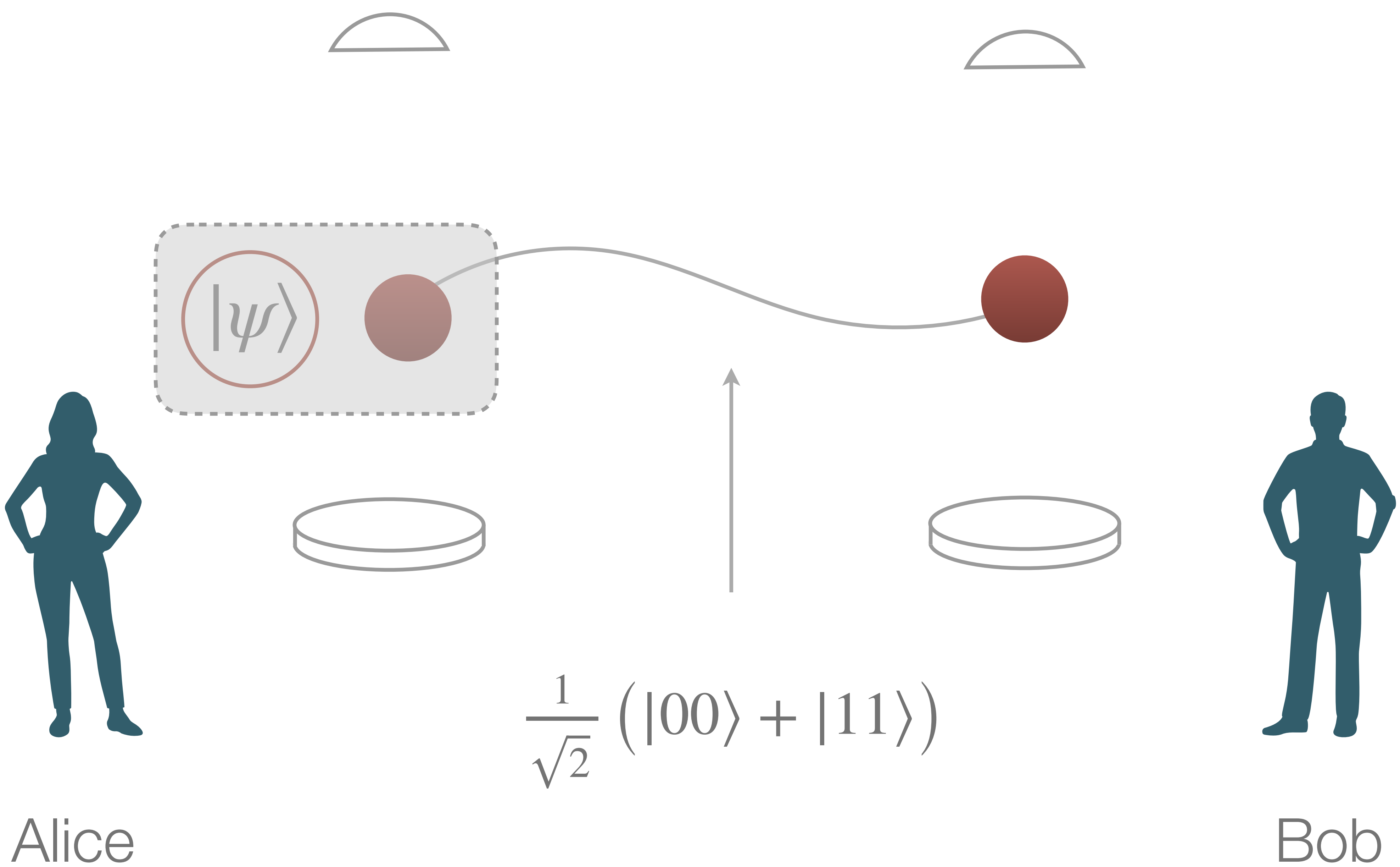
A	B
00	$\longrightarrow \alpha\|0\rangle_B + \beta\|1\rangle_B$
01	$\longrightarrow \alpha\|1\rangle_B + \beta\|0\rangle_B$
10	$\longrightarrow \alpha\|1\rangle_B - \beta\|0\rangle_B$
11	$\longrightarrow \alpha\|0\rangle_B - \beta\|1\rangle_B$

* Homework: Work this out!

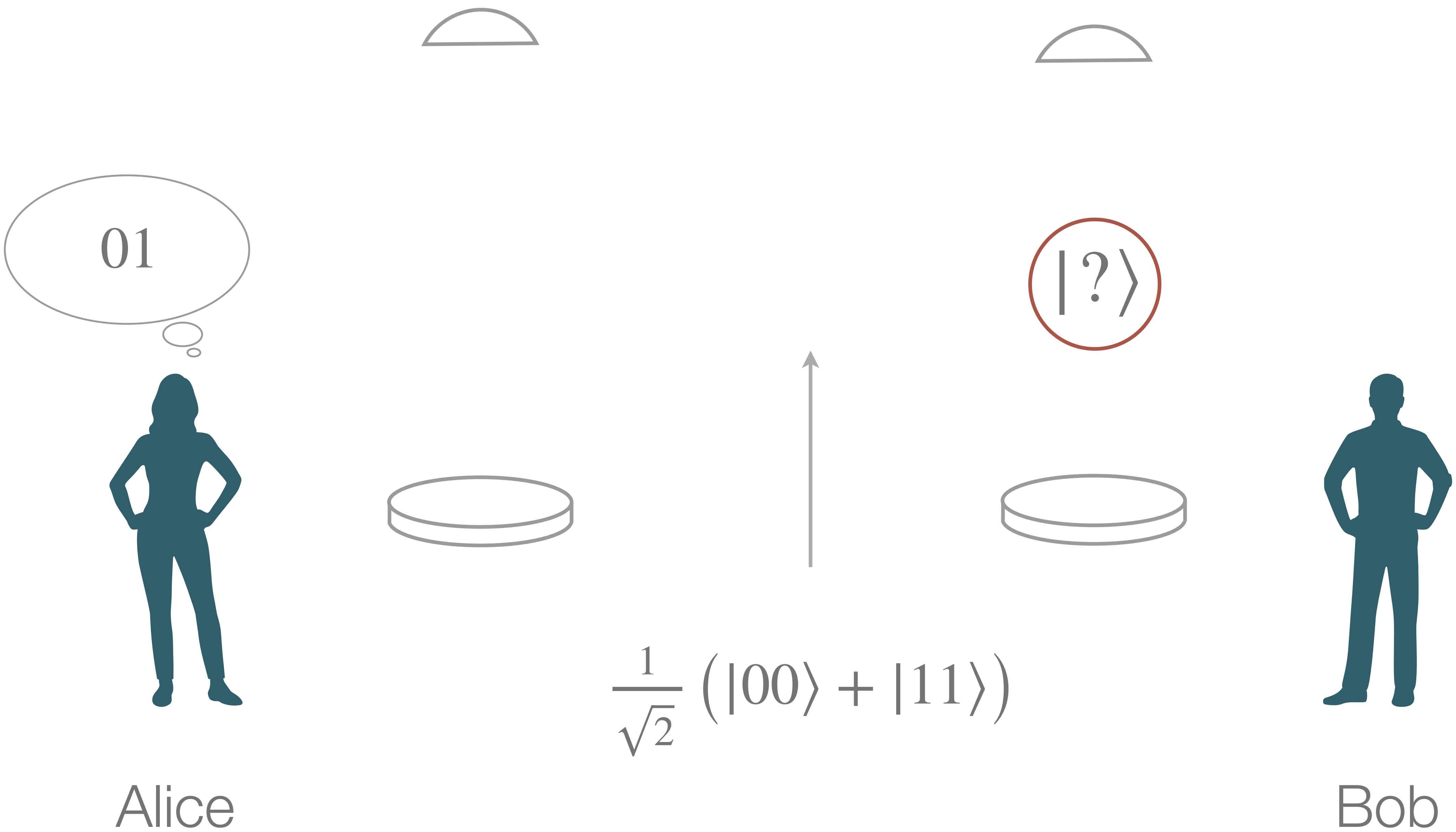
Quantum teleportation



Quantum teleportation



Quantum teleportation



Quantum teleportation

- Suppose we want to send a **qubit** to someone far away:
  - Step 1: A and B share a Bell state, and A wants to send a state to B.
  - Step 2: A applies a transformation to her two qubits and measures them in the 0/1 basis.
  - Step 3: A calls B and sends him the result of her measurement.

$$00 \longrightarrow \alpha|0\rangle_B + \beta|1\rangle_B \qquad 10 \longrightarrow \alpha|1\rangle_B - \beta|0\rangle_B$$

$$01 \longrightarrow \alpha|1\rangle_B + \beta|0\rangle_B \qquad 11 \longrightarrow \alpha|0\rangle_B - \beta|1\rangle_B$$

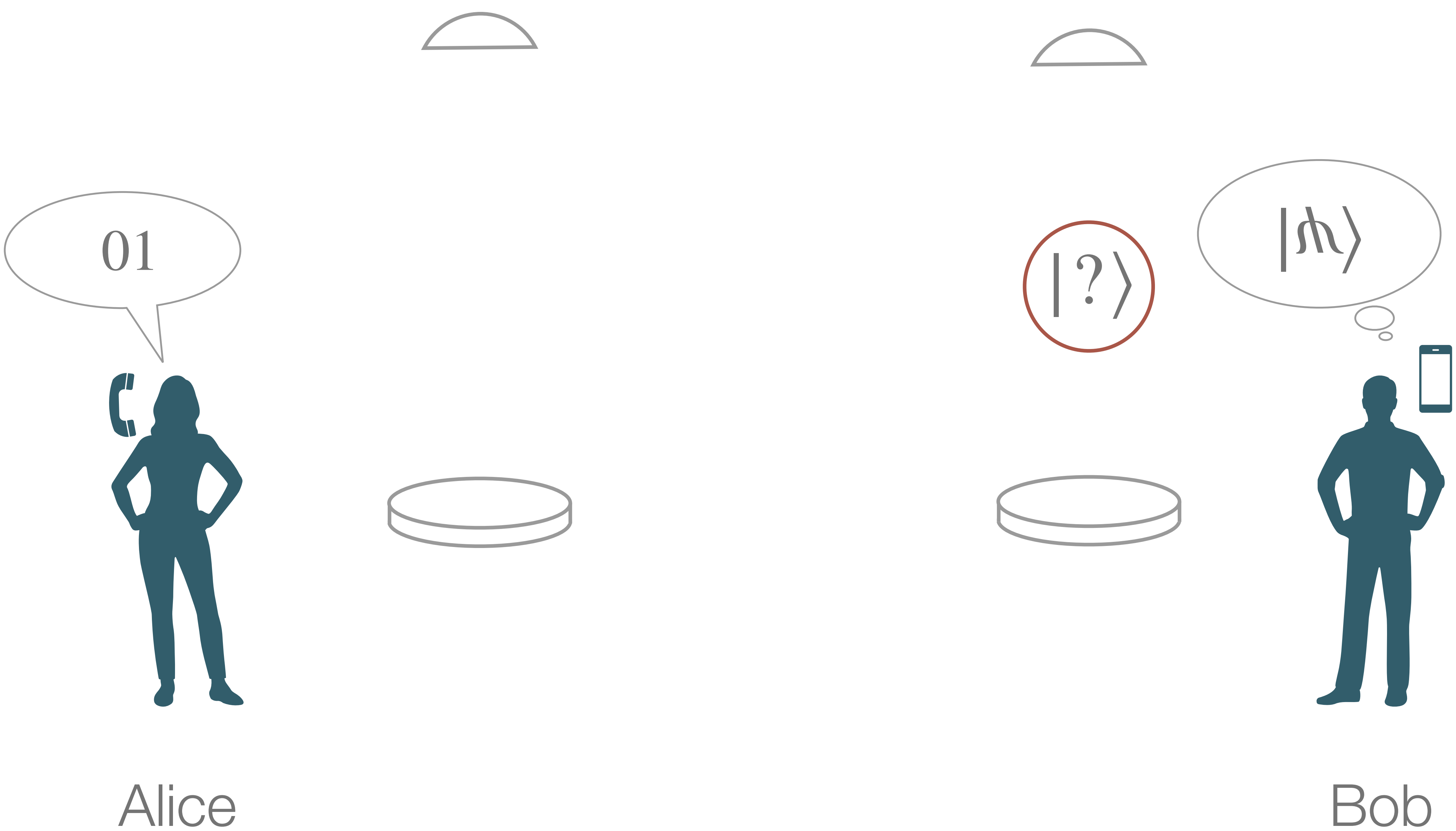
Quantum teleportation

- Suppose we want to send a **qubit** to someone far away:
  - Step 1: A and B share a Bell state, and A wants to send a state to B.
  - Step 2: A applies a transformation to her two qubits and measures them in the 0/1 basis.
  - Step 3: A calls B and sends him the result of her measurement.
  - Step 4: B applies a transformation to correct his state.

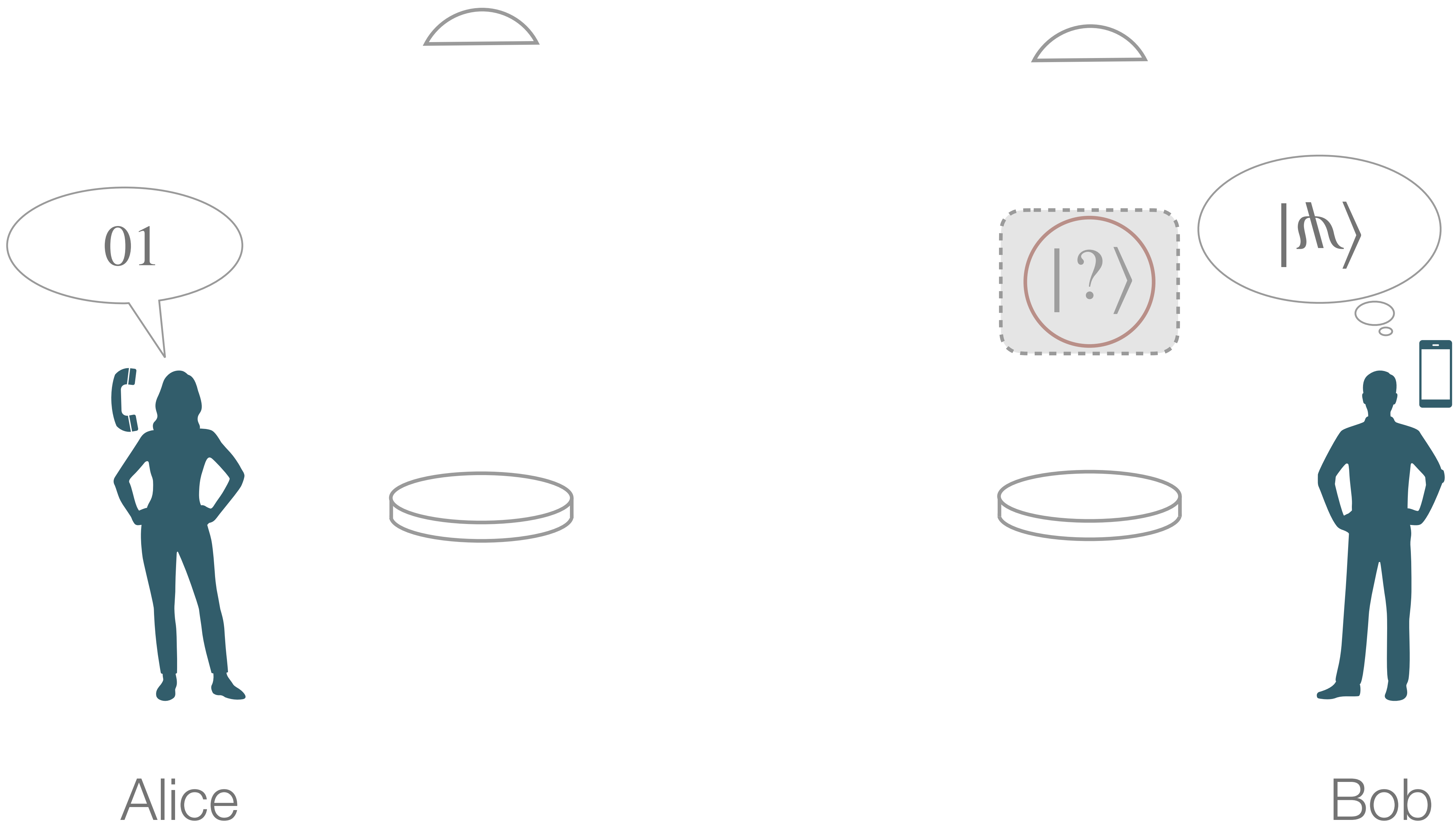
For example: A got $01 \longrightarrow \alpha|1\rangle_B + \beta|0\rangle_B$

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

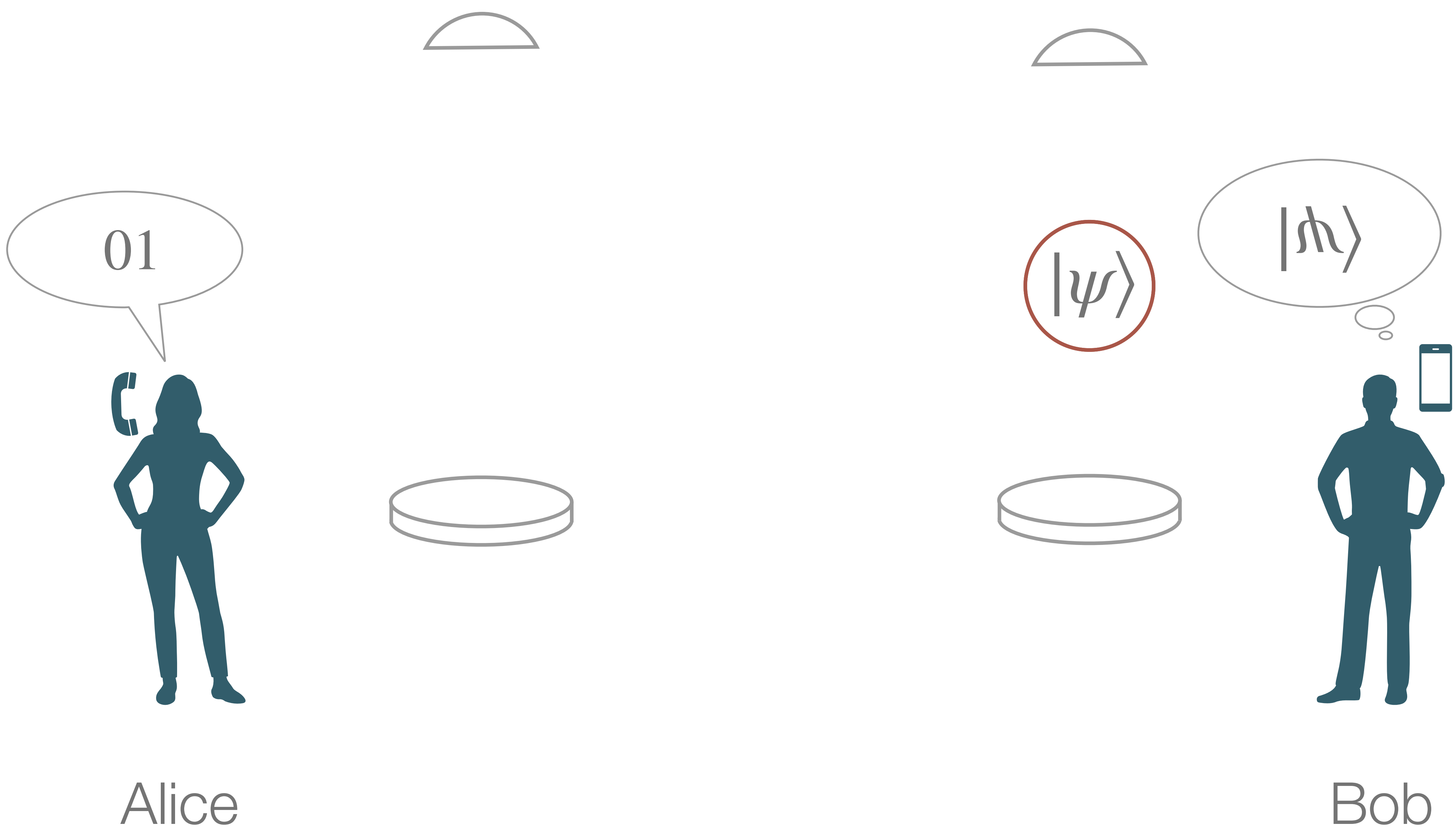
Quantum teleportation



Quantum teleportation



Quantum teleportation



Quantum teleportation

- Can this actually be done? Yes!
  - Demonstration of basic concepts: 1998
  - Teleportation over 600 m using optical fibers: 2004
  - Teleportation over 143km in free space: 2012 (between Canary islands)
  - **Record** - 1400km using ground-to-satellite teleportation (2017)!
- Has been done with photons, atoms, atomic clouds, electrons and superconducting circuits.
- Besides being neat, is a quantum computing primitive!
  - Ernesto will talk more about this!

Outline: General overview of the field

- What is quantum computing?
  - A bit of history;
- The rules: the postulates of quantum mechanics;
- Information-theoretic-flavoured consequences;
  - Entanglement;
  - No-cloning;
  - Teleportation;
  - Superdense coding;

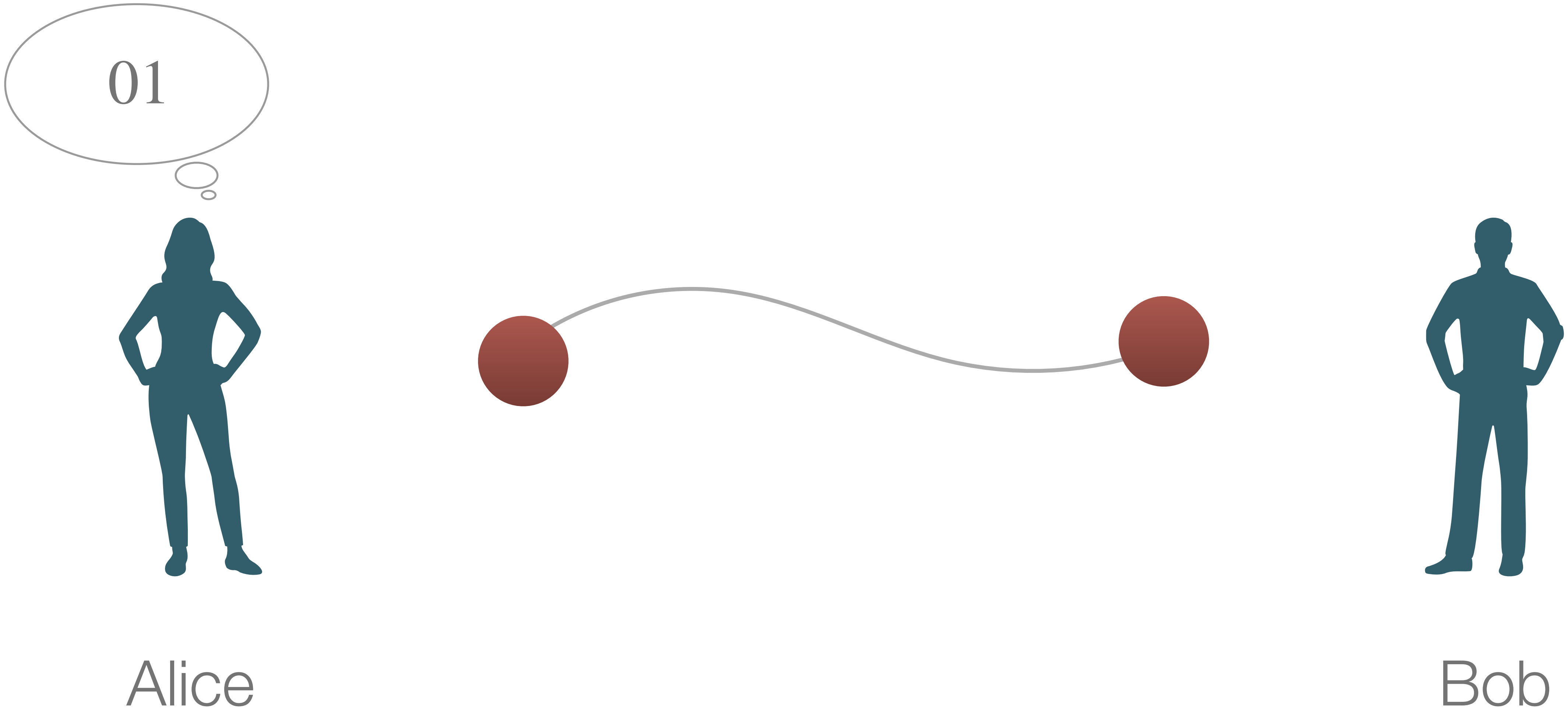
Superdense coding

- **Task**: A wants to sent a two-bit message to B (00, 01, 10 or 11).

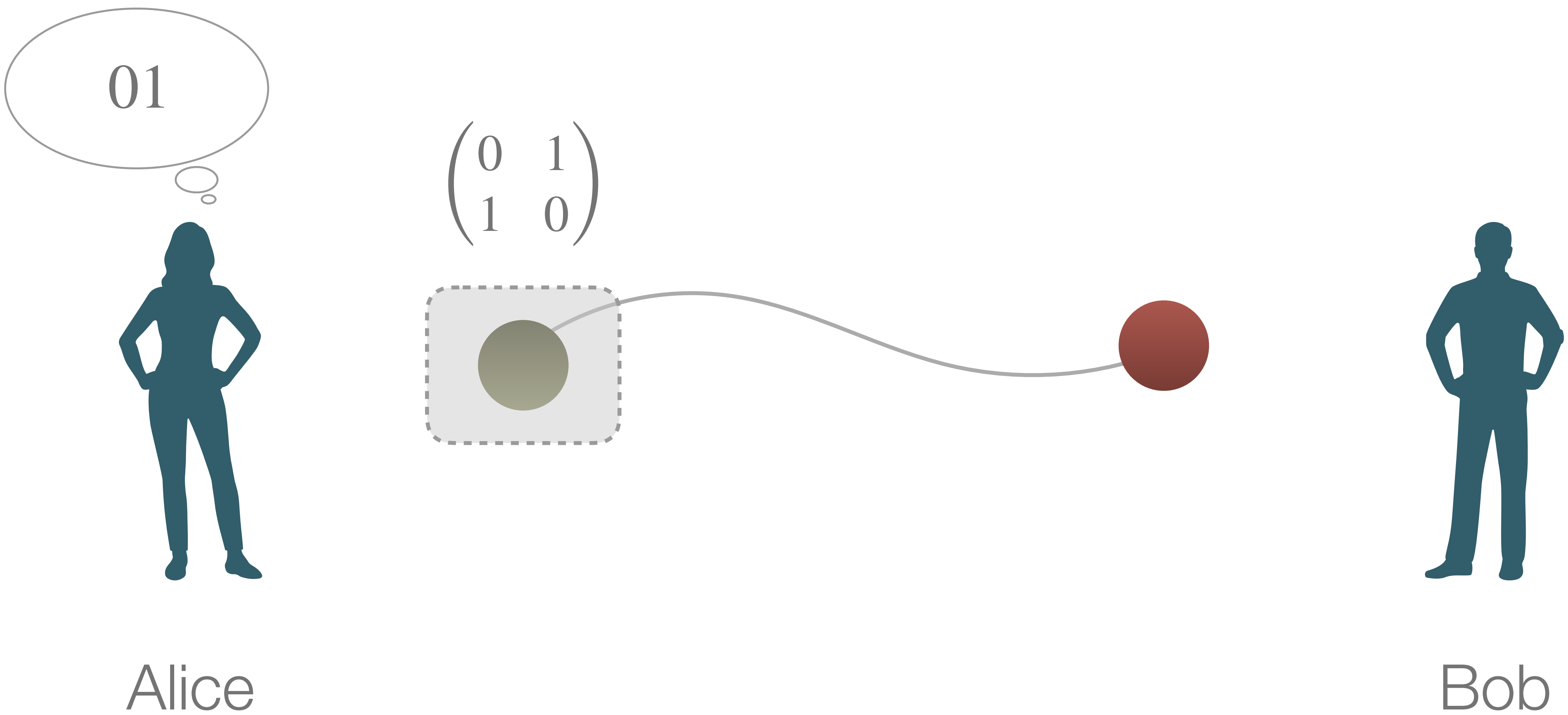
Initial shared state: $\frac{1}{\sqrt{2}}\left(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B\right)$

Message	A applies	Final state
00	$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	$\frac{1}{\sqrt{2}}\left(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B\right)$
01	$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	$\frac{1}{\sqrt{2}}\left(|1\rangle_A|0\rangle_B + |0\rangle_A|1\rangle_B\right)$
10	$Y = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$	$\frac{1}{\sqrt{2}}\left(|1\rangle_A|0\rangle_B - |0\rangle_A|1\rangle_B\right)$
11	$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$	$\frac{1}{\sqrt{2}}\left(|0\rangle_A|0\rangle_B - |1\rangle_A|1\rangle_B\right)$

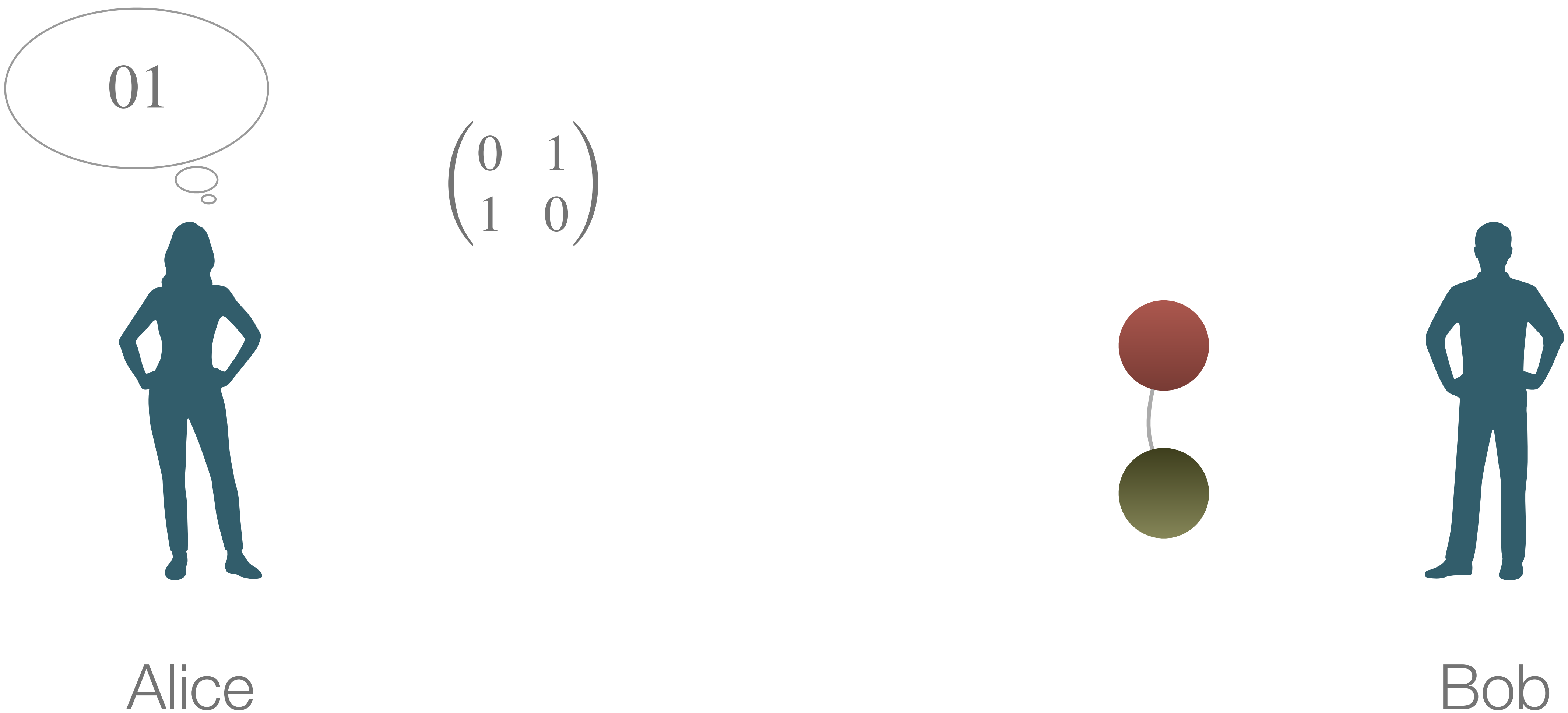
Superdense coding



Superdense coding



Superdense coding



$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Superdense coding

- **Task**: A wants to sent a two-bit message to B (00, 01, 10 or 11).

Bob's state	Bob applies	Final state
$\frac{1}{\sqrt{2}}\big(\vert 00\rangle + \vert 11\rangle\big)$		$\vert 00\rangle$
$\frac{1}{\sqrt{2}}\big(\vert 10\rangle + \vert 01\rangle\big)$	$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & -1 & 0 \\ 1 & 0 & 0 & -1 \end{pmatrix}$	$\vert 01\rangle$
$\frac{1}{\sqrt{2}}\big(\vert 10\rangle - \vert 01\rangle\big)$		$\vert 10\rangle$
$\frac{1}{\sqrt{2}}\big(\vert 00\rangle - \vert 11\rangle\big)$		$\vert 11\rangle$

Superdense coding

Superdense coding

Alice   Bob

Coming soon!

- This is just the beginning! Stay tuned for:

Computation driven by measurement

A zoo of complexity

Classical simulation

Tensor networks

Quantum circuits

"Quantum supremacy"

Blind quantum computation

Neural networks

Verifying quantum technologies