Lecture 10
Entanglement as a computational resource

Luís Soares Barbosa
www.di.uminho.pt/~lsb/



Universidade do Minho





UNU EGOV

Quantum Data Science
Universidade do Minho
2026-2027

Separable and entangled states

State $\frac{1}{\sqrt{2}}(|00\rangle + |01\rangle)$ can be decomposed as $|0\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$

But this not true for $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ which is called an entangled state.

Actually, most states are entangled:

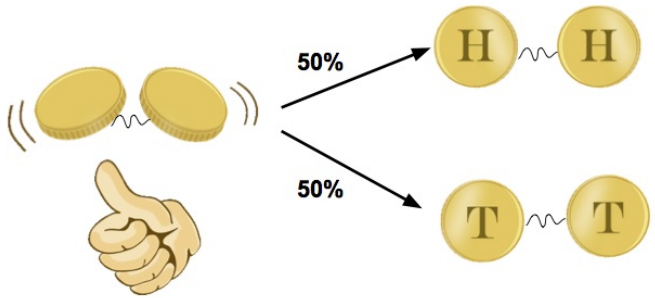
- To express a composition of n qubits requires $2n$ complex numbers (two amplitudes per qubit)
- But how many states $|b_1, b_2, \cdots, b_n\rangle$ are there in a Hilbert space dimension n?

  Each of them is labelled by a binary string of length n, and there are 2^n such strings

$$\boxed{2^n \gg 2n}$$

Entanglement

Entanglement express correlations between subsystems:



"I would not call it one but rather the characteristic trait of quantum mechanics, the one that enforces its entire departure from classical lines of thought"

(Erwin Schrödinger, 1935)

Indeed, it emerges from interaction between parts of a system ...

Example: An entangled state

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \;=\; \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$$

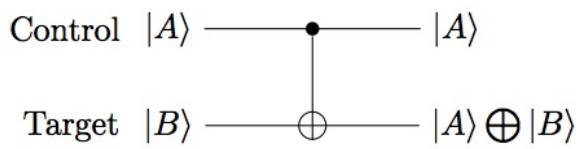
Actually, to make $|\Phi^+\rangle$ equal to

$$(\alpha_1|0\rangle+\beta_1|1\rangle)\otimes(\alpha_2|0\rangle+\beta_2|1\rangle) \;=\; \alpha_1\alpha_2|00\rangle+\alpha_1\beta_2|01\rangle+\beta_1\alpha_2|10\rangle+\beta_1\beta_2|11\rangle$$

would require that $\alpha_1\beta_2 = \beta_1\alpha_2 = 0$ which implies that either

$$\alpha_1\alpha_2 = 0 \;\text{ or }\; \beta_1\beta_2 = 0$$

The *CNOT* gate entails such an interaction



In general: Conditional X

$$CNOT|x\rangle|y\rangle \quad = \quad |x\rangle|x \oplus y\rangle$$

Particular case: The 'spy' gate

$$CNOT|x\rangle|0\rangle \quad = \quad |x\rangle|x\rangle$$

CNOT: conditional X

This paradigmatic two-qubit gate acts on the standard basis for a 2-qubit system flipping the second bit if the first bit is 1 and leaving it unchanged otherwise.

$$\begin{aligned} CNOT &= |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X \\ &= |0\rangle\langle 0| \otimes (|0\rangle\langle 0| + |1\rangle\langle 1|) + |1\rangle\langle 1| \otimes (|1\rangle\langle 0| + |0\rangle\langle 1|) \\ &= |00\rangle\langle 00| + |01\rangle\langle 01| + |11\rangle\langle 10| + |10\rangle\langle 11| \end{aligned}$$

$$= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

A source of entanglement

CNOT generates entanglement e.g.

$$\begin{aligned} CNOT(H \otimes Id)|00\rangle &= CNOT\left(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle\right) \\ &= CNOT\left(\frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)\right) \\ &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \end{aligned}$$

Being its own inverse, also takes an entangled to an unentangled one.

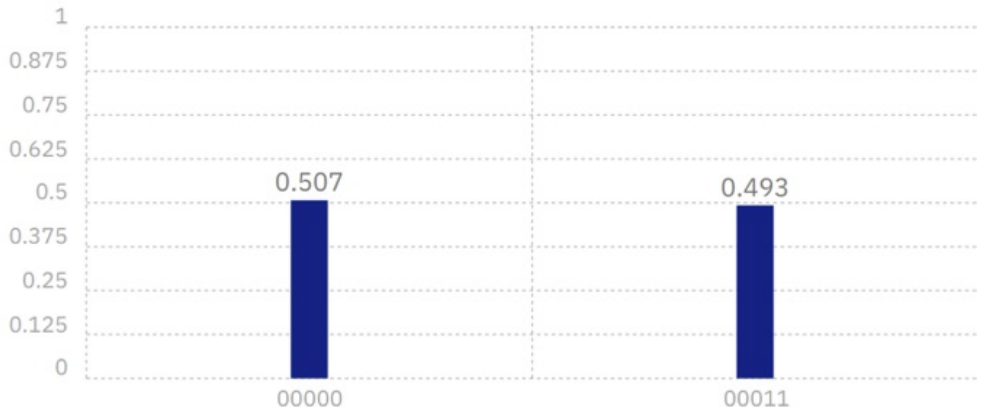
Note that entanglement is not a local property in the sense that transformations that act separately on two or more subsystems cannot affect the entanglement between those subsystems:

$(U \otimes V)\,|v\rangle$ is entangled iff $|v\rangle$ is

A source of entanglement

The Bell states

$$
\begin{aligned}
CNOT(H \otimes Id)|00\rangle &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\
CNOT(H \otimes Id)|01\rangle &= \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \\
CNOT(H \otimes Id)|10\rangle &= \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \\
CNOT(H \otimes Id)|11\rangle &= \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)
\end{aligned}
$$



They are maximally entangled states and form a basis for a two-dimension Hilbert space

Shared randomness

Let's now discuss how entanglement can be used as (another) computational resource.

A protocol

Let two agents, Alice and Bob, in different (possibly distant) locations, share a sequence of Bell pairs

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

When Alice measures her qubit in the pair, she immediately becomes aware of what the result of a measurement by Bob will be when he decides to make it: the global state has already collapsed.

Shared randomness

- Of course there is no communication at all involved in this protocol as the value measured by Alice is perfectly random and to communicate one needs first to know what is to be communicated.
- However, by repeating this process for all shared Bell pairs two identical sequences of completely random binary values will be produced in both locations, which is an important resource in e.g. cryptographic protocols, For example,

$$0\ 1\ 1\ 0\ \cdots 0$$
$$0\ 1\ 1\ 0\ \cdots 0$$

Teleportation

Aim: to transmit, using two classical bits, the state of a single qubit.

Surprisingly, the protocol

- shows that two classical bits suffice to communicate a qubit, which has an infinite number of configurations
- provides a mechanism for the transmission of an unknown quantum state, in spite of the no-cloning theorem

Teleportation

Relevance

Indeed, there is no way to transmit quantum information resorting only to classical communication.

If this was possible, the same classical information shared between Alice and Bob could be reached by a third party (because classical information can easily be copied). The latter could then acquire a copy of the quantum data being shared. But this would violate the non cloning theorem.

Note that the original state cannot be preserved (precisely because of the no-cloning result), which motivates the name of the protocol ...

Teleportation

Strategy:

- Alice and Bob share a Bell state

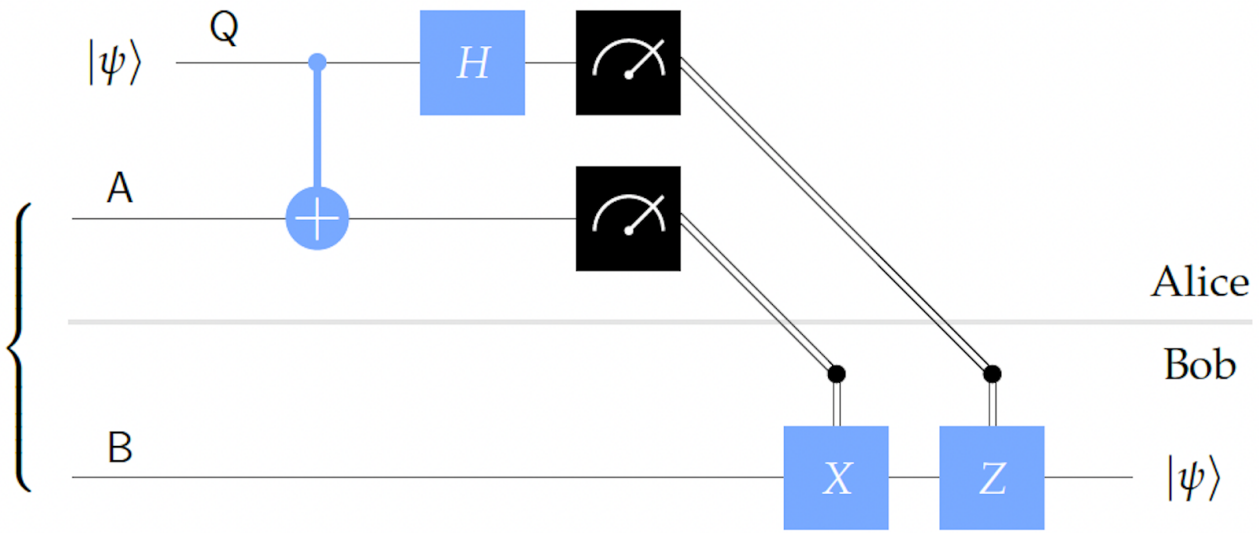
$$|r\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle$$

created ahead in time when both qubits were together and could be made to interact to produce an entangled state (through e.g. a *CNOT* gate).

- This entangled state becomes a resource which remains available when one qubit is taken away from the other.
- Then Alice encodes the unknown qubit with her part of the Bell pair, measures and transmits the (classical) result of the measurement.
- Finally, Bob decodes its part of the Bell pair based on the (classical) information received

Teleportation

The circuit



The Bell pair

is the real resource

also named EPR pair after Einstein, Podolsky, and Rosen, from the *hidden-variable* controversy

Teleportation

Alice

... has a qubit whose state $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$ she ignores, but wants to send to Bob through classical channels.

The starting point is the 3-qubit state whose first 2 qubits are controlled by Alice and the last by Bob:

$$\begin{aligned} |\phi\rangle \otimes |r\rangle &= \frac{1}{\sqrt{2}}(\alpha|0\rangle \otimes \overbrace{(|00\rangle + |11\rangle)}^{\text{entangled}} + \beta|1\rangle \otimes \overbrace{(|00\rangle + |11\rangle)}^{\text{entangled}}) \\ &= \frac{1}{\sqrt{2}}(\alpha|000\rangle + \alpha|011\rangle + \beta|100\rangle + \beta|111\rangle) \end{aligned}$$

Teleportation

Alice

... applies $CNOT \otimes I$ and $H \otimes I \otimes I$ to obtain

$$
\begin{aligned}
&(H \otimes I \otimes I)(CNOT \otimes I)(|\phi\rangle \otimes |r\rangle) \\
&= (H \otimes I \otimes I)\frac{1}{\sqrt{2}}(\alpha|000\rangle + \alpha|011\rangle + \beta|110\rangle + \beta|101\rangle) \\
&= \frac{1}{2}(\alpha(|000\rangle + |011\rangle + |100\rangle + |111\rangle) + \beta(|010\rangle + |001\rangle - |110\rangle - |101\rangle)) \\
&= \frac{1}{2}(|00\rangle(\alpha|0\rangle + \beta|1\rangle) \\
&\quad + \frac{1}{2}(|01\rangle(\alpha|1\rangle + \beta|0\rangle) \\
&\quad + \frac{1}{2}(|10\rangle(\alpha|0\rangle - \beta|1\rangle) \\
&\quad + \frac{1}{2}(|11\rangle(\alpha|1\rangle - \beta|0\rangle)
\end{aligned}
$$

Teleportation

Alice

Alice measures the first two qubits and obtains one of the four standard basis states, $|00\rangle, |01\rangle, |10\rangle, |11\rangle$, with equal probability.

For example,

$$\text{Prob}_{|11\rangle} = \left|\frac{1}{2}\alpha\right|^2 + \left|\frac{1}{2}\beta\right|^2 = \frac{1}{4}(|\alpha|^2 + |\beta|^2) = \frac{1}{4}$$

Teleportation

Alice

Therefore, depending on the result of her measurement, the state of Bob's qubit is projected to

$$\alpha|0\rangle + \beta|1\rangle,\ \alpha|1\rangle + \beta|0\rangle,\ \alpha|0\rangle - \beta|1\rangle,\ \alpha|1\rangle - \beta|0\rangle$$

Then, Alice sends the result of her measurement as two classical bits to Bob.

After these transformations, crucial information about the original state $|\phi\rangle$ is contained in Bob's qubit, Alice's being destroyed ...

Teleportation

Bob

When Bob receives the two bits from Alice, he knows how the state of his half of the entangled pair compares to the original state of Alice's qubit.

Bob can reconstruct the original state of Alice's qubit, $|\phi\rangle$, by applying the appropriate decoding transformation to his qubit, originally part of the entangled pair.

Bits received	Bob's state	Decoder
00	$\alpha\|0\rangle + \beta\|1\rangle$	I
01	$\alpha\|1\rangle + \beta\|0\rangle$	X
10	$\alpha\|0\rangle - \beta\|1\rangle$	Z
11	$\alpha\|1\rangle - \beta\|0\rangle$	ZX

After decoding, Bob's qubit will be in the state $|\phi\rangle$

A note on Pauli gates

Identity $\quad I = |0\rangle\langle 0| + |1\rangle\langle 1| = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

Bit-flip $\quad X = |1\rangle\langle 0| + |0\rangle\langle 1| = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$

Phase-flip $\quad Z = |0\rangle\langle 0| - |1\rangle\langle 1| = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = P_\pi$

BitPhase-flip $\quad Y = i(-|1\rangle\langle 0| + |0\rangle\langle 1|) = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$

- Operators X, Y and Z correspond to rotations in the Bloch sphere along the x, y and z axis, respectively.
- Any 1-qubit unitary operator can be expressed as a linear combination of Pauli operators.

Superdense coding

Aim: encode and transmit two classical bits with one qubit and a shared Bell pair.

This result is surprising, since only one bit can be extracted from a qubit

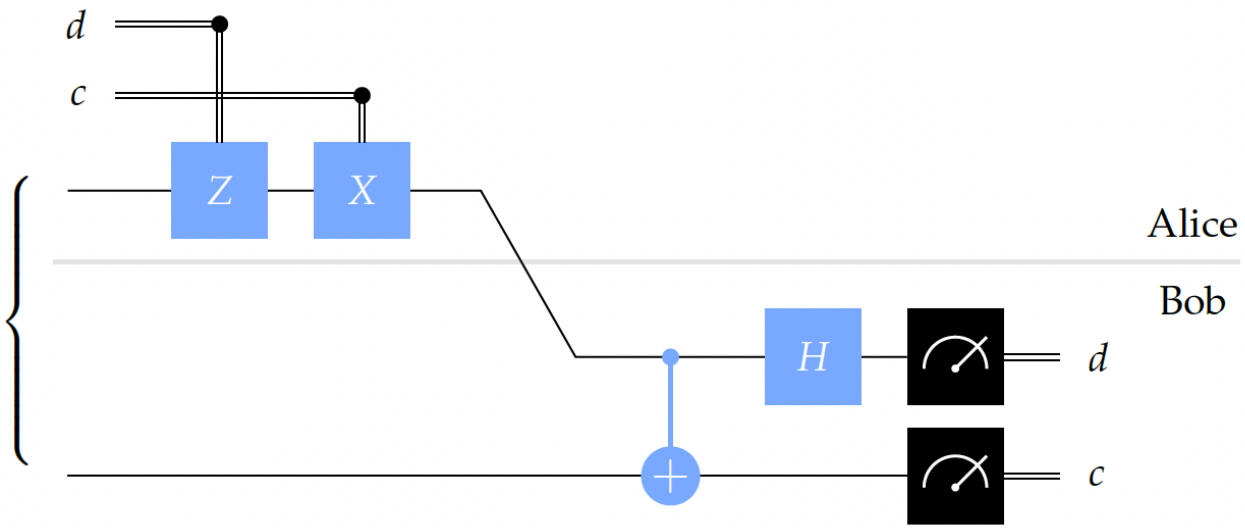
The idea is that, since entangled states can be distributed ahead of time, only one qubit needs to be physically transmitted to communicate two bits of information.

Let Alice (Bob) be sent and operate the first (second) qubit of the EPR pair

$$|r\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Superdense coding

The circuit



Superdense coding

Alice

wishes to transmit the state of two classical bits encoding one of the numbers 0 through 3. Depending on this number, Alice performs one of the Pauli transformations on her qubit of the entangled pair $|r\rangle$, and sends her qubit to Bob.

	Encoder	New state
0	$(I \otimes I)\|r\rangle$	$\frac{1}{\sqrt{2}}(\|00\rangle + \|11\rangle)$
1	$(X \otimes I)\|r\rangle$	$\frac{1}{\sqrt{2}}(\|10\rangle + \|01\rangle)$
2	$(Z \otimes I)\|r\rangle$	$\frac{1}{\sqrt{2}}(\|00\rangle - \|11\rangle)$
3	$(XZ \otimes I)\|r\rangle$	$\frac{1}{\sqrt{2}}(\|10\rangle - \|01\rangle)$

Superdense coding

Bob

decodes the information applying a *CNOT* gate to the two qubits of the entangled pair and then H to the first qubit:

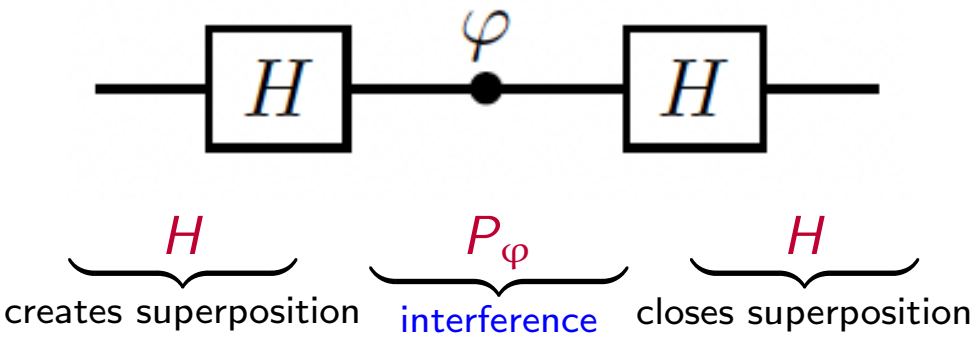
$$CNOT \longrightarrow \begin{bmatrix} \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) \\ \frac{1}{\sqrt{2}}(|11\rangle + |01\rangle) \\ \frac{1}{\sqrt{2}}(|00\rangle - |10\rangle) \\ \frac{1}{\sqrt{2}}(|11\rangle - |01\rangle) \end{bmatrix} = \begin{bmatrix} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle \\ \frac{1}{\sqrt{2}}(|1\rangle + |0\rangle) \otimes |1\rangle \\ \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \otimes |0\rangle \\ \frac{1}{\sqrt{2}}(|1\rangle - |0\rangle) \otimes |1\rangle \end{bmatrix}$$

$$H \otimes I \longrightarrow \begin{bmatrix} |00\rangle \\ |01\rangle \\ |10\rangle \\ -|11\rangle \end{bmatrix}$$

Bob then measures the two qubits in the standard basis to obtain the 2-bit binary encoding of the number Alice wished to send.

The golden pattern

Recall from Lecture 3:



a basic pattern in quantum computation combining superposition and iterference.

$$HP_\varphi H|0\rangle = \cos\frac{\varphi}{2}|0\rangle + -i\sin\frac{\varphi}{2}|1\rangle$$
$$HP_\varphi H|1\rangle = -i\sin\frac{\varphi}{2}|0\rangle + \cos\frac{\varphi}{2}|1\rangle$$

Decoherence

In the same lecture, we discussed this is the behaviour when the quantum system is perfectly isolated.

Otherwise, in the presence of decoherence, interference can be greatly reduced or even eliminated, and, consequently, the system's behaviour becomes more and more classical ...

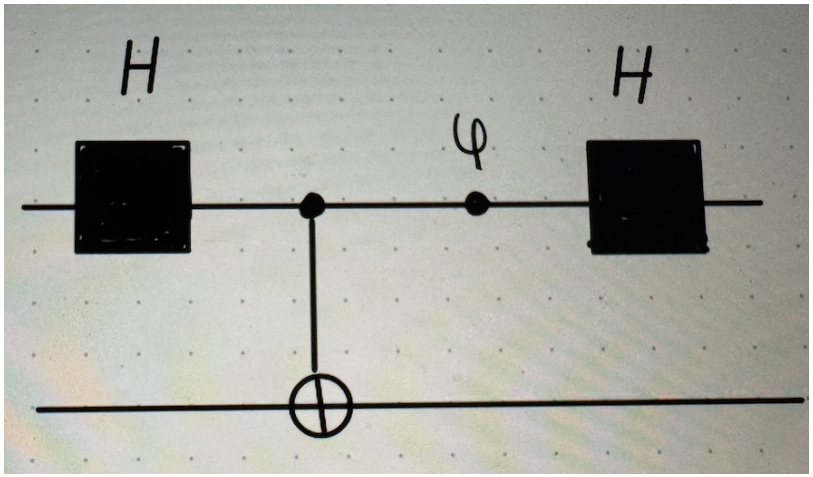
But what is decoherence, after all?

... the (unavoidable) result of the establishment of a strong interaction with the environment, i.e. an entanglement situation.

Let's illustrate this by observing the effect of entanglement in the golden pattern.

Entanglement and Interference

Let's combine the interference and the entanglement patterns:



and apply it to $|00\rangle$:

$$(H \otimes I)(P_\varphi \otimes I)\,CNOT\,(H \otimes I)\,|00\rangle$$

Entanglement and Interference

$$(H \otimes I)(P_\varphi \otimes I)\,CNOT\,(H \otimes I)\,|00\rangle$$

- Before P_φ the system is in the first Bell state; after it becomes

$$\frac{1}{\sqrt{2}}(|00\rangle + e^{i\Phi}|11\rangle)$$

- The second H closes superposition yielding

$$\frac{1}{2}(|00\rangle+|10\rangle+e^{i\varphi}|01\rangle-e^{i\varphi}|11\rangle \;=\; |0\rangle\left(\frac{|0\rangle + e^{i\varphi}|1\rangle}{2}\right)+|1\rangle\left(\frac{|0\rangle - e^{i\varphi}|1\rangle}{2}\right)$$

Entanglement and Interference

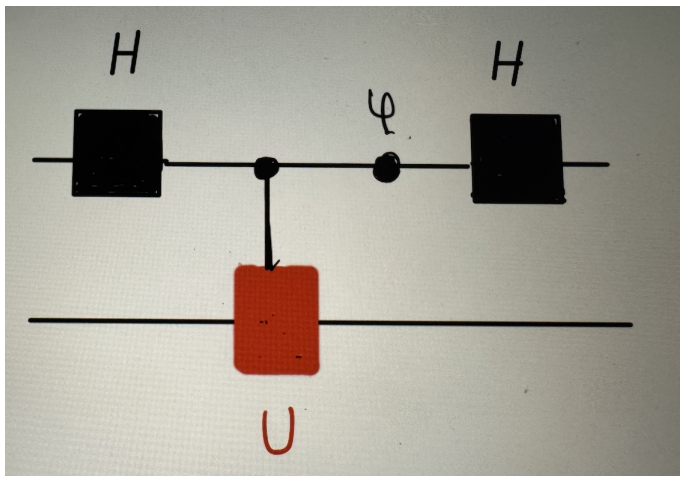
An easy calculation shows that the probabilities of measuring 0 or 1 are $\frac{1}{2}$ in each case.

Interference (via P_φ) was cancelled by entanglement: Indeed the second qubit learnt the first one, becoming aware of which path in the superposition was taken.

The *CNOT* gate, the spy gate, destroyed interference

Entanglement and Interference

Let's go general: replacing *CNOT* by a controlled C_U for an arbitrary unitarian U:



$$(H \otimes I)(P_\varphi \otimes I)C_U(H \otimes I)\,|00\rangle$$

Entanglement and Interference

$$C_U = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes U$$

- If the control qubit is $|0\rangle$, the target qubit remains $|0\rangle$
- if not it is rotated from $|0\rangle$ to $U|0\rangle$

As before, if $U = CNOT$ the rotation is π: the new state becomes orthogonal to the previous one.
The second qubit acquired full knowledge about the first one.

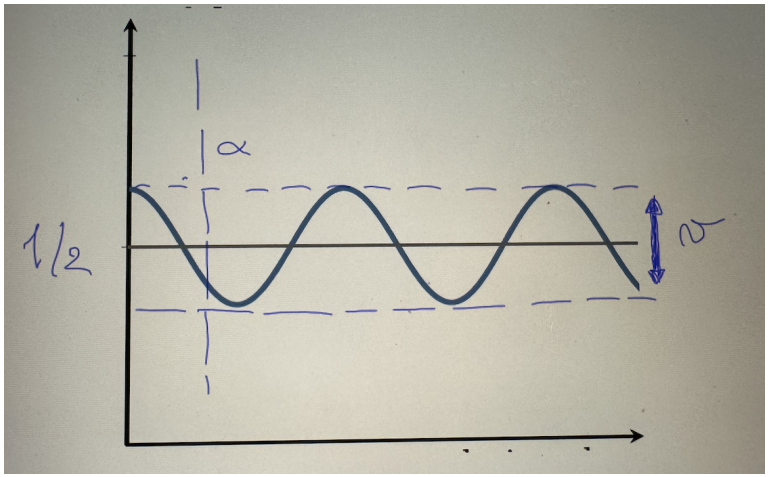
In general, however, the acquired knowledge may be imperfect:

$$\boxed{\langle 0|U|0\rangle = ve^{-i\alpha}}$$

recall: the inner product measures the similarity between states

Entanglement and Interference

$$\langle 0|U|0\rangle = ve^{-i\alpha}$$



Special cases

$\langle 0|X|0\rangle = 0$ Interference completely suppressed: the curve becomes flat at $\frac{1}{2}$.

$\langle 0|Id|0\rangle = 1$ Full interference: probabilities oscillate as $\cos\frac{\varphi}{2}$.

Entanglement as an adversary

Suppose our system corresponds to the first qubit and consists of the typical interference circuit: $HP_\varphi H$.

Interacting with the environment it becomes open and easily goes into an entanglement situation, e.g. as in the previous of the diagram.

However, the system now has no control over the environment.

This may lead to reduction, or even suppression, of interference and therefore to the collapse of quantum computational power.

Remember the fridge?



Decoherence of our quantum system starts here ...

... leading to a much longer story