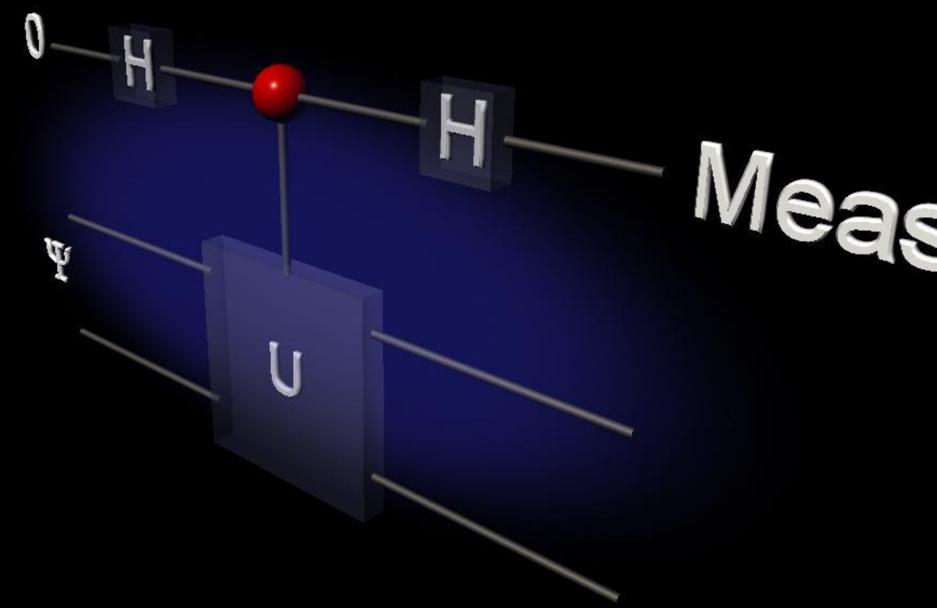
Introduction to Quantum Information Processing

CO481 CS467 PHYS467

Michele Mosca

Lecture 4 (17 January 2013) by Dr. David Gosset

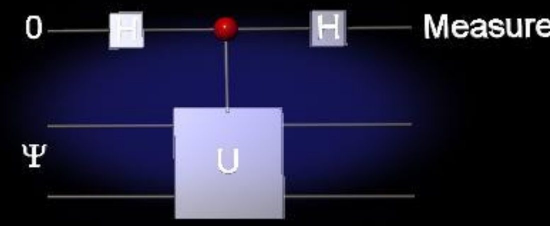


Institute for Quantum Computing

UNIVERSITY OF WATERLOO

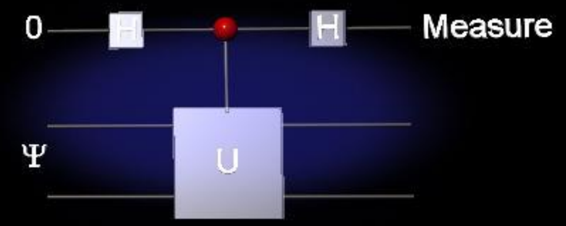
PERIMETER INSTITUTE FOR THEORETICAL PHYSICS

Overview



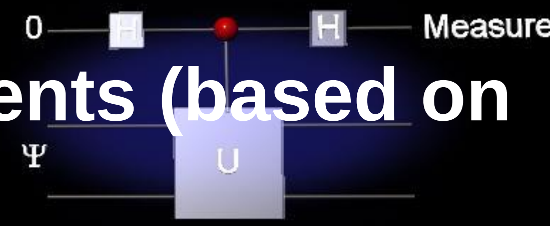
- Some circuit notation for measurements
- Holevo’s theorem
- Bell Basis and Superdense Coding
- Implementing Bell measurements
- Postulates of Quantum Mechanics
- Quantum teleportation

(sections 3.1-3.4, 4.1,4.5,5.1,5.2, Appendix A.8)



Some circuit notation for measurements

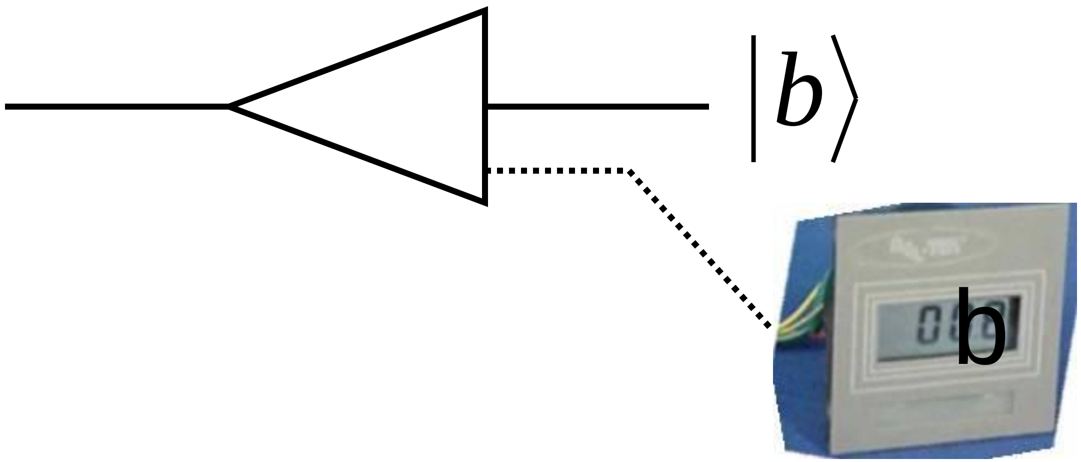
Circuit notation for measurements (based on KLM book)



Consider a one-qubit measurement in the computational basis

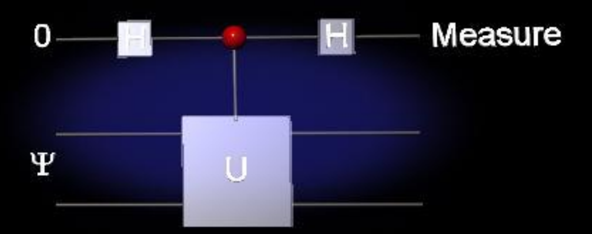
with probability $|\alpha_b|^2 = |\langle b|\psi\rangle|^2$

$$|\psi\rangle = \sum_k \alpha_k |k\rangle$$



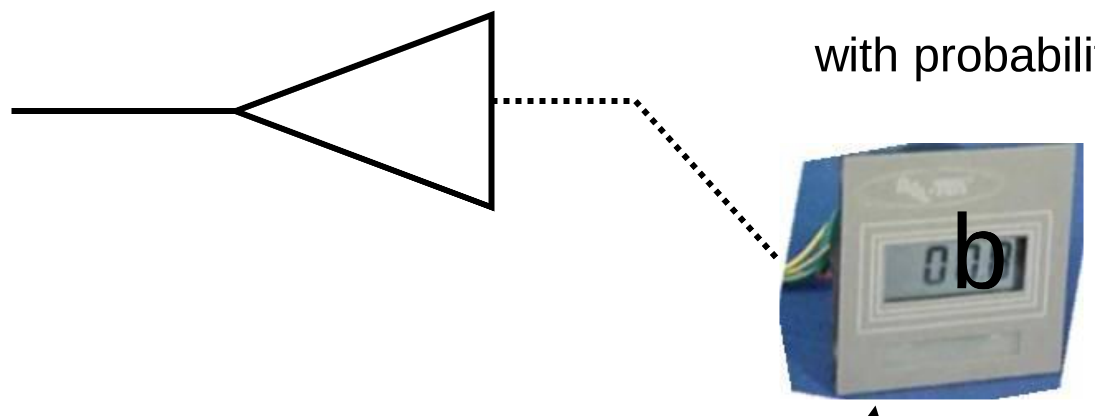
$$|b\rangle$$

classical display



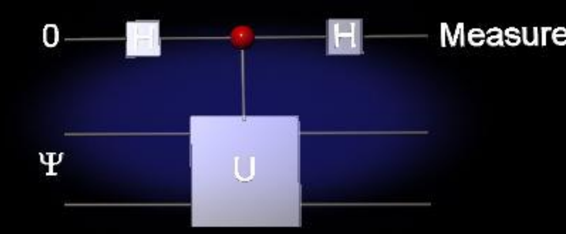
If the quantum output is discarded (e.g. via a “destructive measurement”) we can drop the quantum part

$|\psi\rangle$

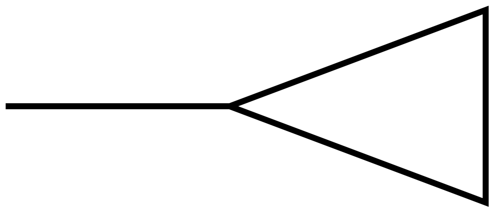


with probability $\left|\langle b|\psi\rangle\right|^2$

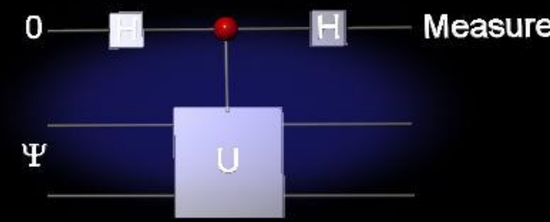
classical display



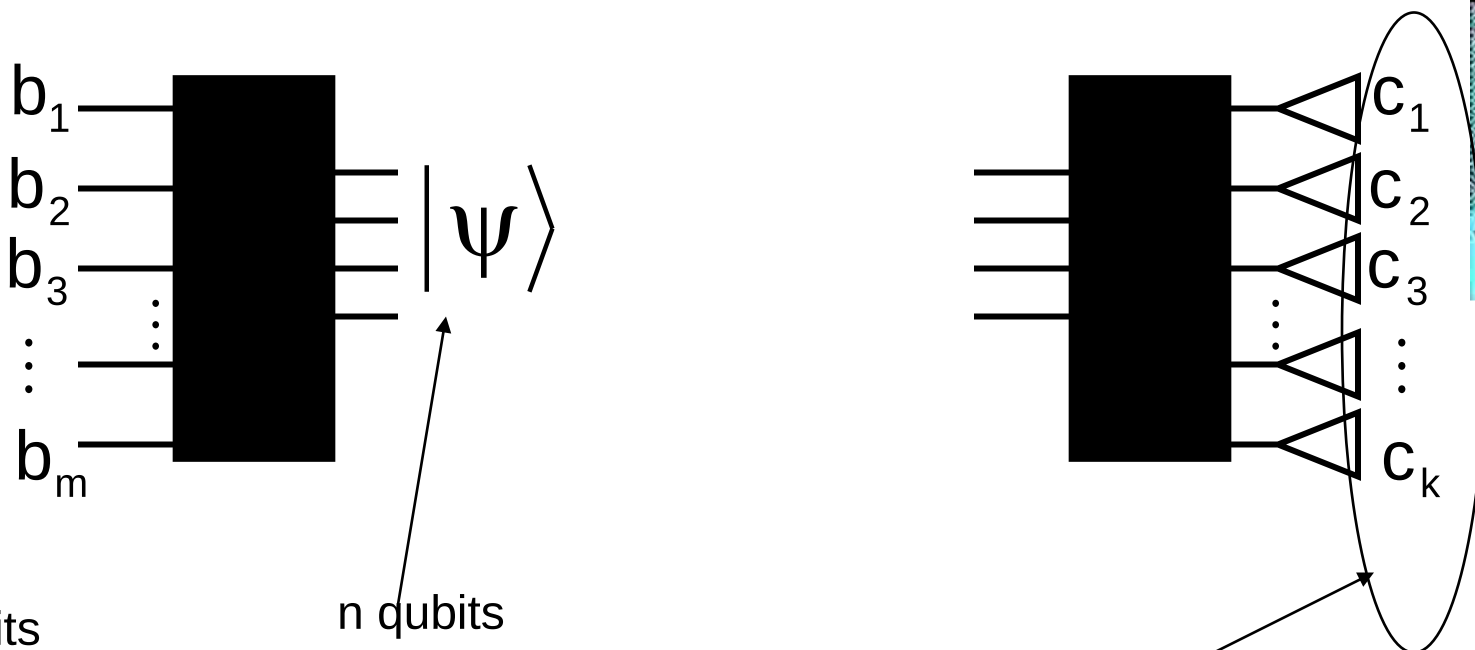
Or just:

$|\psi\rangle$  b with probability $\left|\langle b|\psi\rangle\right|^2$

Holevo's Theorem



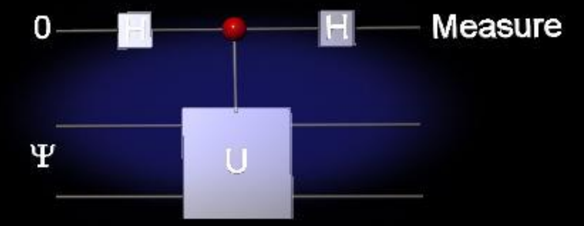
"n qubits cannot convey more than n classical bits of information"



This "no-go" theorem was further generalized by Nayak (Random Access Code Theorem).

Cannot convey more than n bits of information

Can shared randomness help?

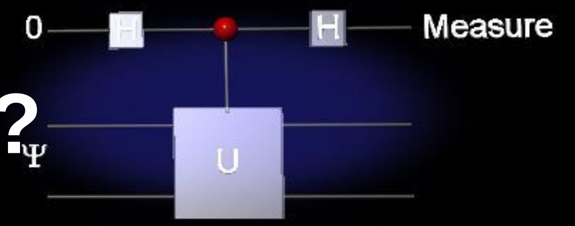


$r_1 r_2 r_3 r_4 r_5 r_6 \cdots$

$r_1 r_2 r_3 r_4 r_5 r_6 \cdots$

NO!

Can shared entanglement help?

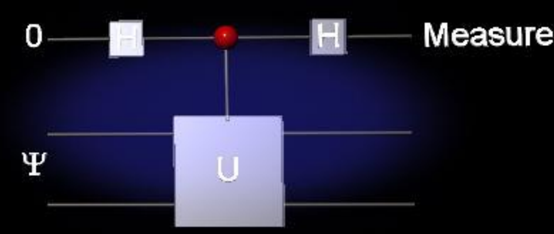


$$\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$$

$$\frac{1}{\sqrt{2}}|0\cdots \;\cdots\; \cdots \;\cdots 0\rangle + \frac{1}{\sqrt{2}}|1\cdots \;\cdots\; \cdots \;\cdots 1\rangle$$

We'll see!

New tool: Bell basis change

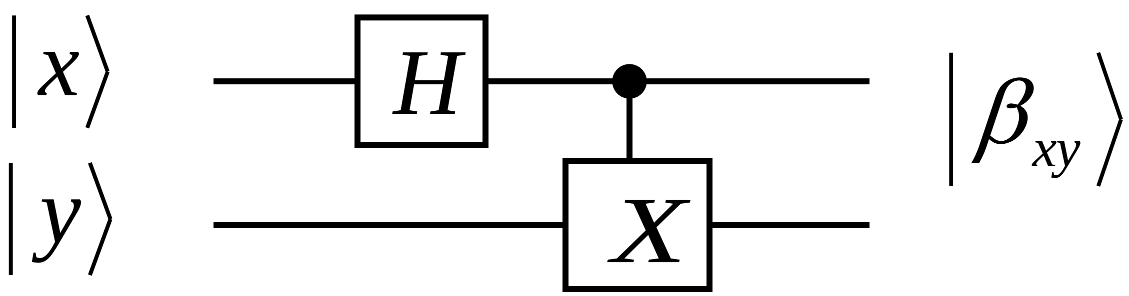


Consider the orthonormal basis consisting of the “Bell” states

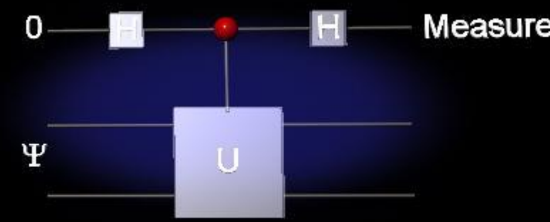
$$|\beta_{00}\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle \qquad |\beta_{01}\rangle = \frac{1}{\sqrt{2}}|01\rangle + \frac{1}{\sqrt{2}}|10\rangle$$

$$|\beta_{10}\rangle = \frac{1}{\sqrt{2}}|00\rangle - \frac{1}{\sqrt{2}}|11\rangle \qquad |\beta_{11}\rangle = \frac{1}{\sqrt{2}}|01\rangle - \frac{1}{\sqrt{2}}|10\rangle$$

Note that



New tool: Bell basis change

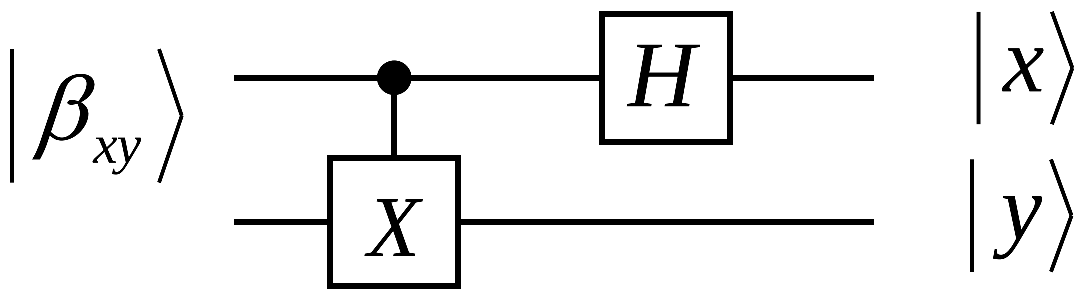


Consider the orthonormal basis consisting of the “Bell” states

$$|\beta_{00}\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle \qquad |\beta_{01}\rangle = \frac{1}{\sqrt{2}}|01\rangle + \frac{1}{\sqrt{2}}|10\rangle$$

$$|\beta_{10}\rangle = \frac{1}{\sqrt{2}}|00\rangle - \frac{1}{\sqrt{2}}|11\rangle \qquad |\beta_{11}\rangle = \frac{1}{\sqrt{2}}|01\rangle - \frac{1}{\sqrt{2}}|10\rangle$$

Also,

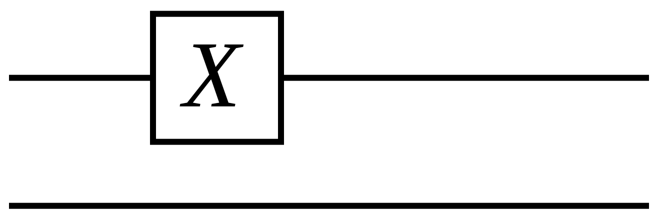


Important fact about the Bell basis

It is possible to change between any two Bell basis states with only a *local* operation.

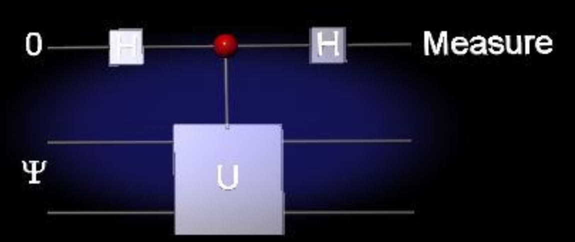
e.g.

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



$$|\beta_{01}\rangle = \frac{1}{\sqrt{2}}|01\rangle + \frac{1}{\sqrt{2}}|10\rangle$$

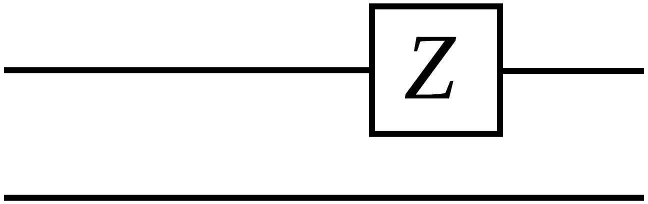
Important fact about the Bell basis



It is possible to change between any two Bell basis states with only a *local* operation.

e.g.

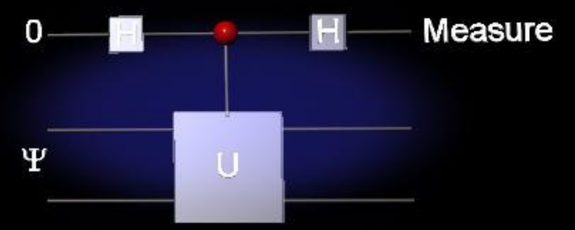
$$|\beta_{00}\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$$



$$|\beta_{10}\rangle = \frac{1}{\sqrt{2}}|00\rangle - \frac{1}{\sqrt{2}}|11\rangle$$

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

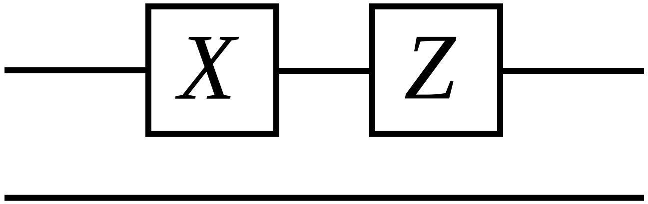
Important fact about the Bell basis



It is possible to change between any two Bell basis states with only a *local* operation.

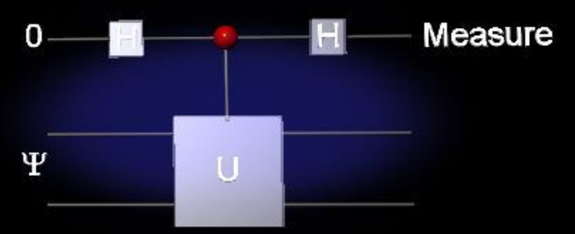
e.g.

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



$$|\beta_{11}\rangle = \frac{1}{\sqrt{2}}|01\rangle - \frac{1}{\sqrt{2}}|10\rangle$$

Important fact about the Bell basis

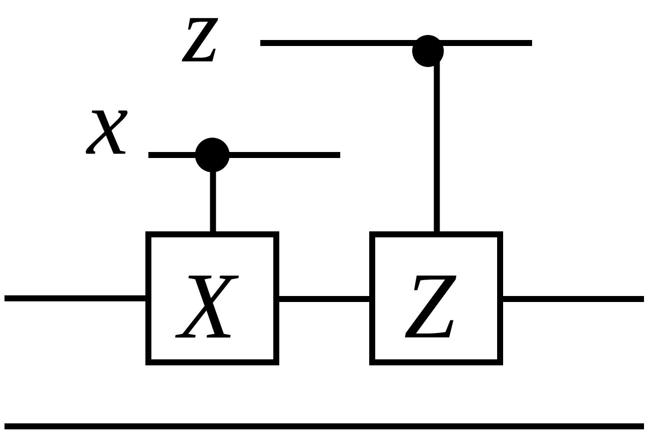


It is possible to change between any two Bell basis states with only a *local* operation.

in general

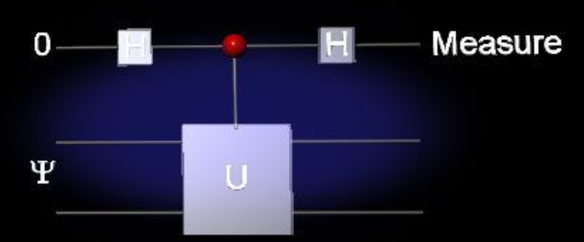
$$x, z \in \{0,1\} \quad X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

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



$$|\beta_{zx}\rangle$$

Important fact about the Bell basis



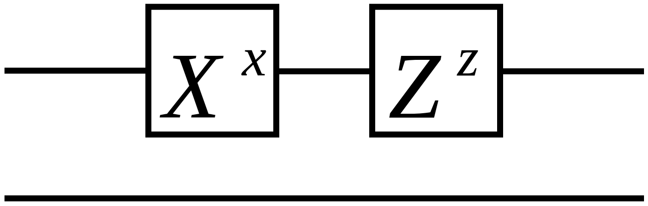
It is possible to change between any two Bell basis states with only a *local* operation.

equivalently

$$x, z \in \{0,1\} \quad X^0 = I, \quad X^1 = X$$

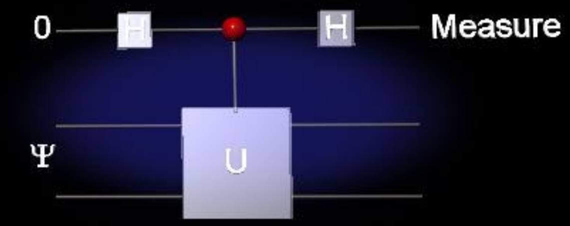
$$Z^0 = I, \quad Z^1 = Z$$

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



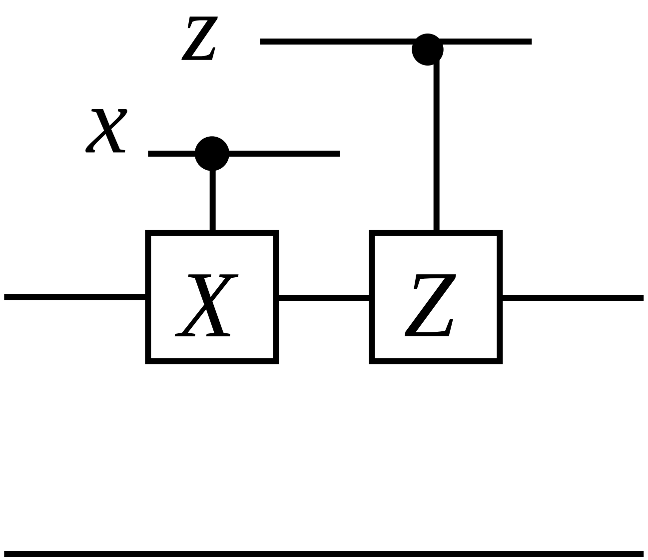
$$|\beta_{zx}\rangle$$

Superluminal signaling?



It is possible to change between any two Bell basis states with only a *local* operation.

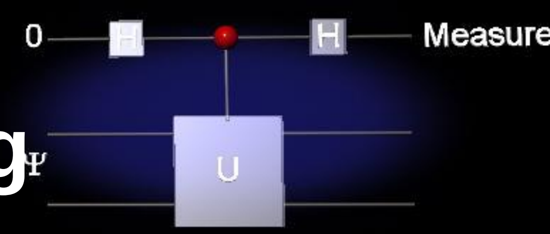
$$|\beta_{00}\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$$



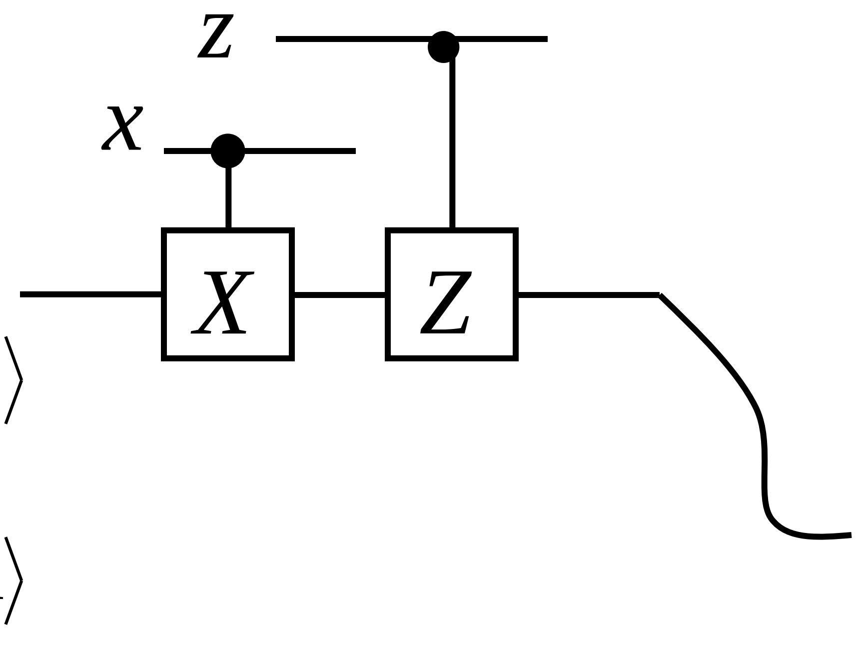
$$|\beta_{zx}\rangle$$

Note that this does not allow non-local (or superluminal) signalling. Why not?

Application: superdense coding

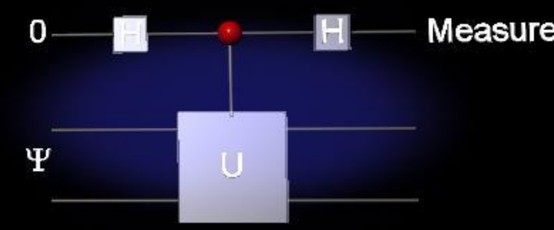


$$\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$$

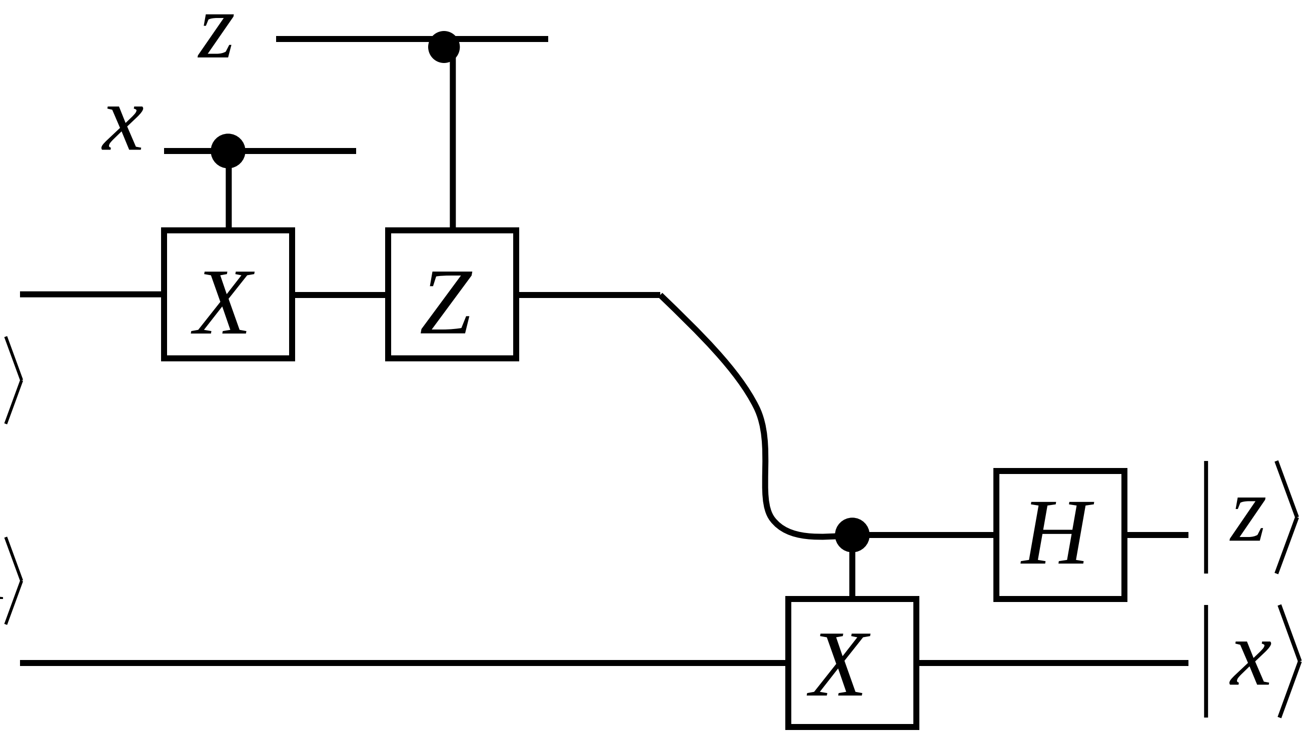


$$|\beta_{zx}\rangle$$

Application: superdense coding



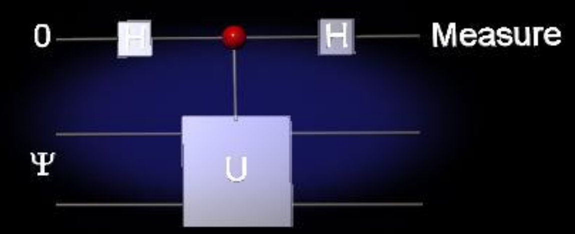
$$\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$$



With prior entanglement:

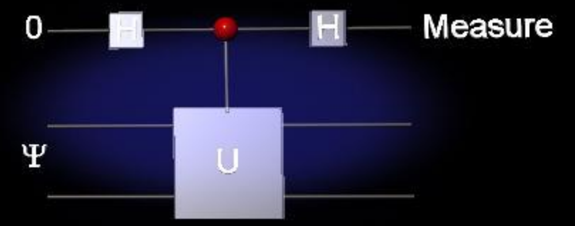
Can send 2 classical bits by sending 1 qubit

(We can't do any better)



Postulates of quantum mechanics

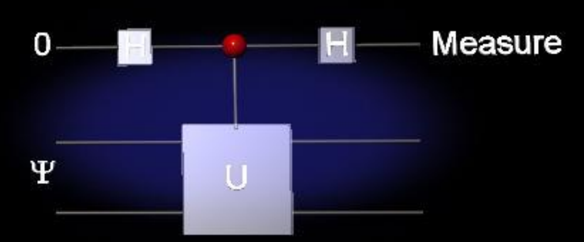
Postulate 1: state space



The state of a system is described by a unit vector in a complex* vector space H.

(*Usually referred to as a *Hilbert space,* which is an inner product space that is complete with respect to the norm defined by the inner product. Finite dimensional complex vector spaces are trivially Hilbert spaces. We will restrict attention to finite dimensional spaces for most of this course.)

Postulate 2: evolution



The time-evolution of a closed quantum system is described by a unitary operator.

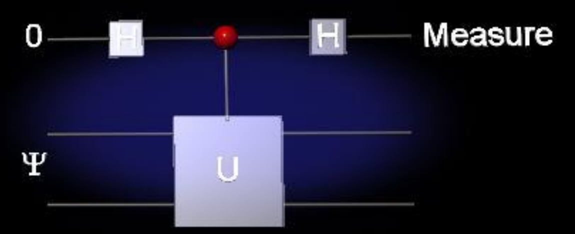
That is, for any evolution of the closed system there exists a unitary operator U such that if the initial state of the system is $|\psi_1\rangle$, then after the evolution the state of the system will be

$$|\psi_2\rangle = U|\psi_1\rangle$$

A linear operator U is unitary if $U^{-1}=U^{\dagger}$ (where $\dagger$ denotes the conjugate transpose)

(if we want a linear evolution that preserves the norm, then we must have unitary evolution)

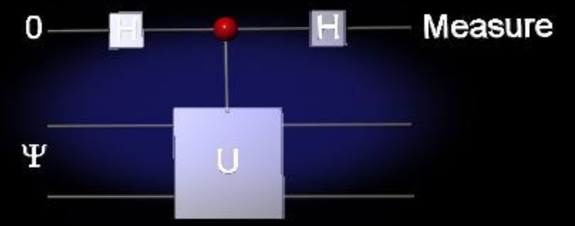
Postulate 3: composite systems



When two physical systems are treated as one combined system, the state space of the combined physical system is the tensor product space $H_A \otimes H_B$ of the state spaces H_A, H_B of the component subsystems.

If the first system is in state $|\psi_1\rangle$ and the second system is in the state $|\psi_2\rangle$, then the combined system is in the state $|\psi_1\rangle \otimes |\psi_2\rangle$.

Postulate 4: measurements

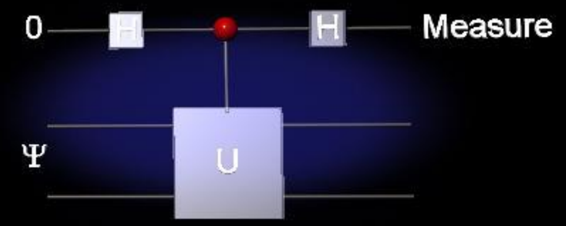


For a given orthonormal basis $B = \{|\varphi_i\rangle : i = 1,2,...\}$ of a state space H_A for a system A, it is possible to perform a Von Neumann measurement on the system with space H_A with respect to the basis B that, given a state

$$|\psi\rangle = \sum_i \alpha_i |\varphi_i\rangle$$

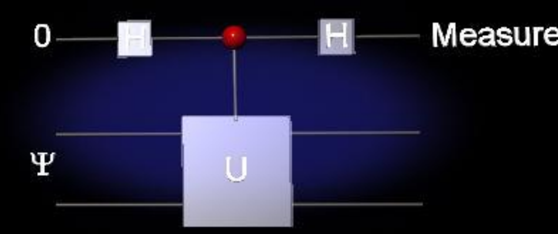
outputs a label “i” with probability $|\alpha_i|^2$ and leaves the system in state $|\varphi_i\rangle$.

Postulate 4: measurements



Furthermore, given a state $|\psi\rangle = \sum_i \alpha_i |\varphi_i\rangle |\gamma_i\rangle$ from a bipartite state space (the $|\varphi_i\rangle$ are orthonormal), then performing a Von Neumann measurement on system A will yield outcome “i” with probability $|\alpha_i|^2$ and leave the bipartite system in state $|\varphi_i\rangle|\gamma_i\rangle$.

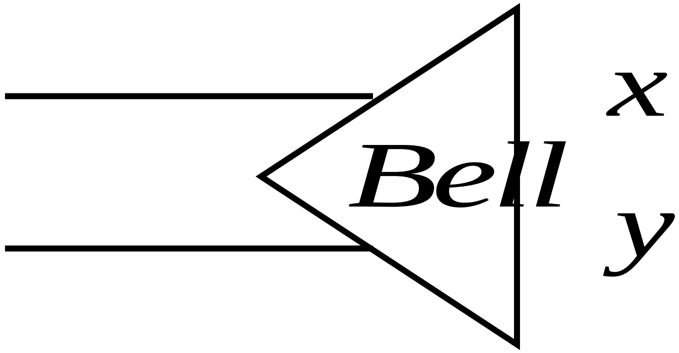
Bell measurement



Note that the Bell states form an orthonormal basis for the 2-qubit states, and we can implement a measurement of the following form.

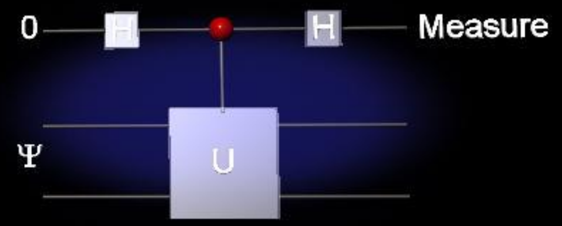
(known as a "Von Neumann measurement" with respect to the Bell basis)

$$|\psi\rangle = \sum_{x,y} \alpha_{x,y} |\beta_{xy}\rangle$$



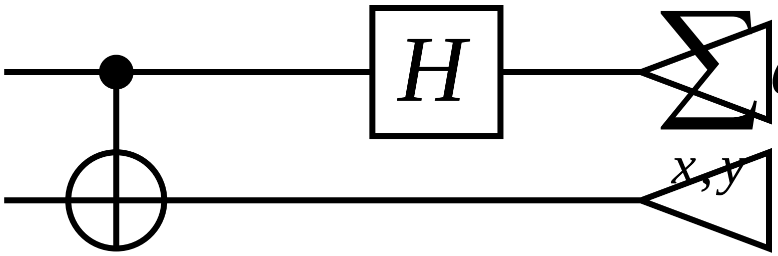
$prob \, |\alpha_{xy}|^2$

Implementing a Bell measurement



We can "destructively" measure

$$\sum_{x,y} \alpha_{x,y} \left| \beta_{xy} \right\rangle$$



$$\sum_{x,y} \alpha_{x,y} \left| xy \right\rangle$$

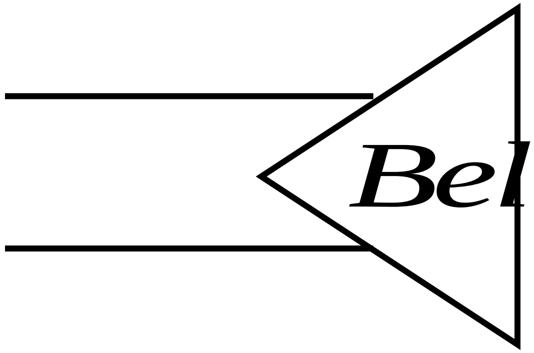
x

y

$prob \left| \alpha_{xy} \right|^2$

$$\equiv$$

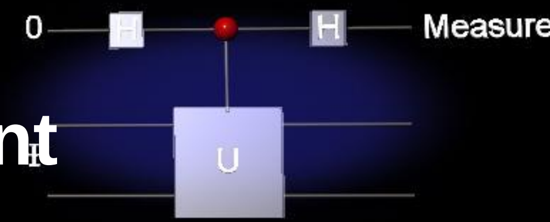
$$\left| \psi \right\rangle = \sum_{x,y} \alpha_{x,y} \left| \beta_{xy} \right\rangle$$



x

y

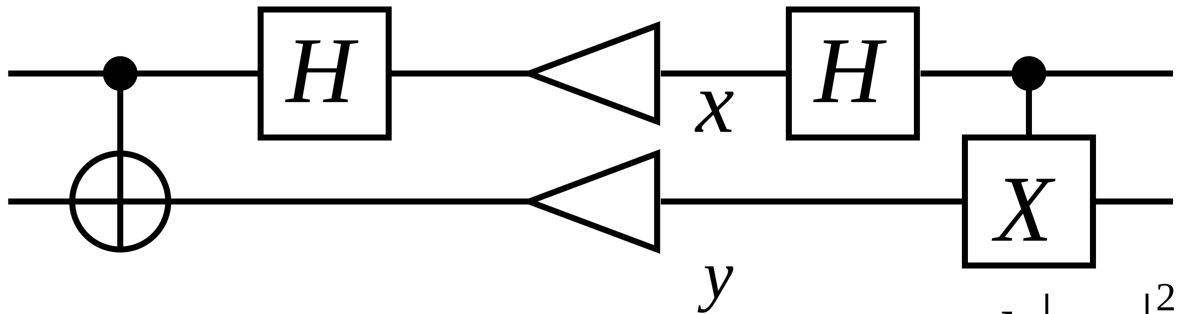
$prob \left| \alpha_{xy} \right|^2$



Implementing a Bell measurement

We can “non-destructively” measure

$$\sum_{x,y}\alpha_{x,y}\left|\beta_{xy}\right\rangle$$

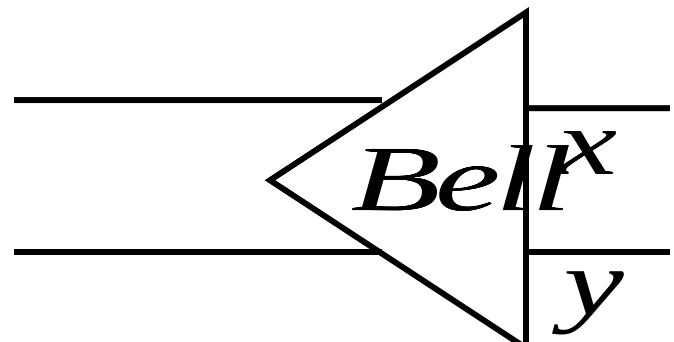


$$\left|\beta_{xy}\right\rangle$$

$$prob\left|\alpha_{xy}\right|^2$$

$$\equiv$$

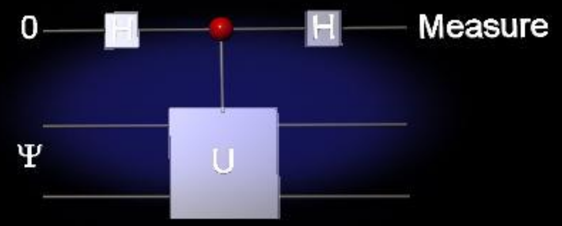
$$\left|\psi\right\rangle=\sum_{x,y}\alpha_{x,y}\left|\beta_{xy}\right\rangle$$



$$\left|\beta_{xy}\right\rangle$$

$$prob\left|\alpha_{xy}\right|^2$$

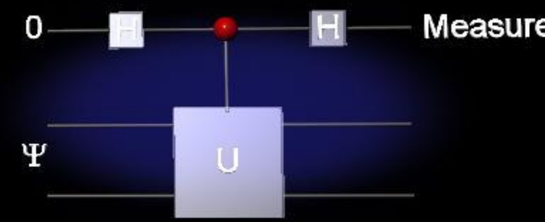
Example 1



Yet another way to implement a Bell measurement

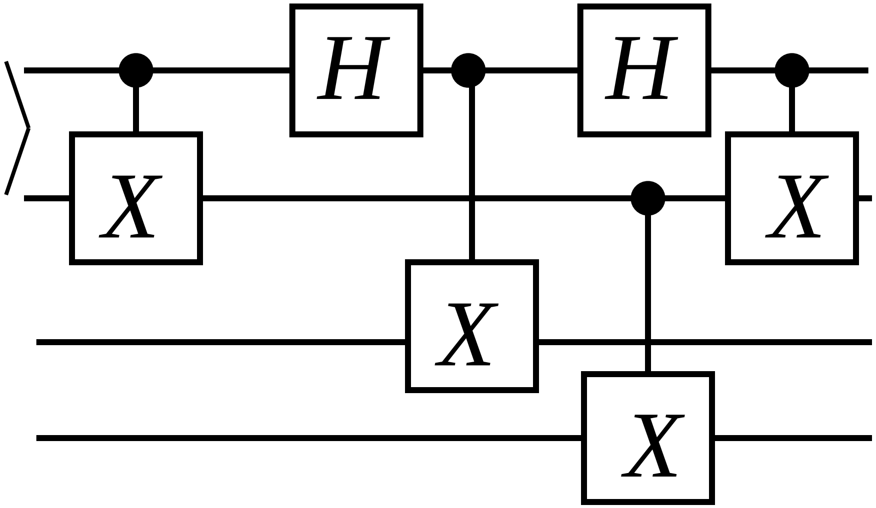
(e.g. suppose your physical measurements are destructive, but you wish to obtain a non-destructive measurement)

Bell measurement



$$\sum_{x,y} \alpha_{x,y} \left| \beta_{xy} \right\rangle$$

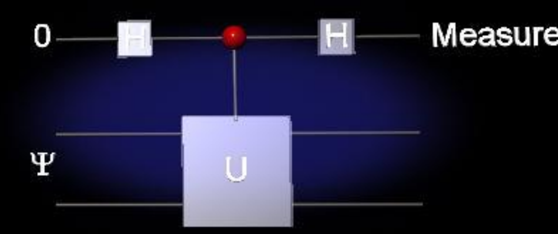
$$\left| 00 \right\rangle$$



$$\sum_{x,y} \alpha_{x,y} \left| \beta_{xy} \right\rangle \left| xy \right\rangle$$

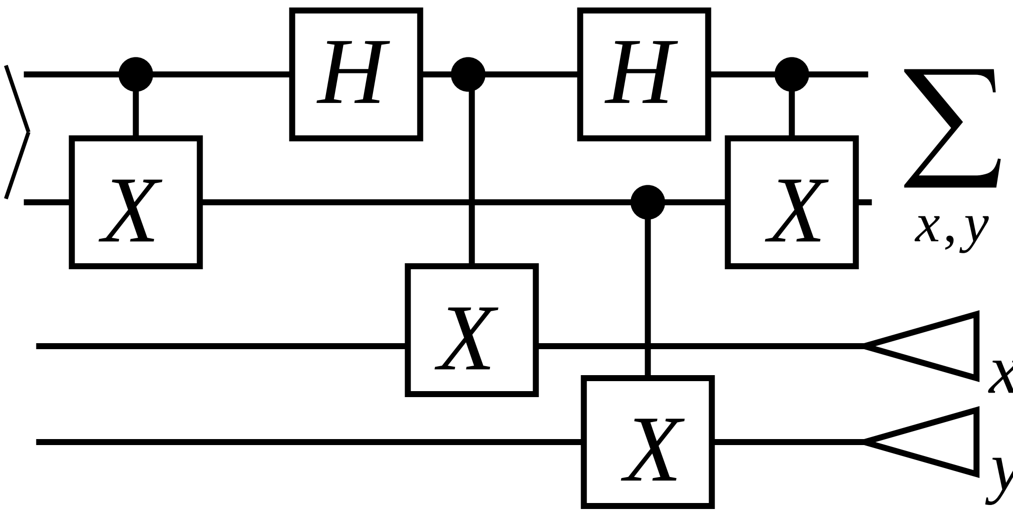
What should happen if we only measure the bottom two qubits?

Bell measurement



$$\sum_{x,y}\alpha_{x,y}\left|\beta_{xy}\right\rangle$$

$$\left|00\right\rangle$$

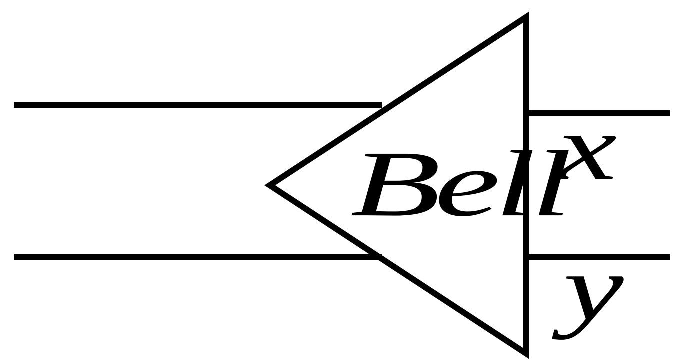


$$\sum_{x,y}\alpha_{x,y}\left|\beta_{xy}\right\rangle\left|xy\right\rangle$$

$$prob\left|\alpha_{xy}\right|^2$$

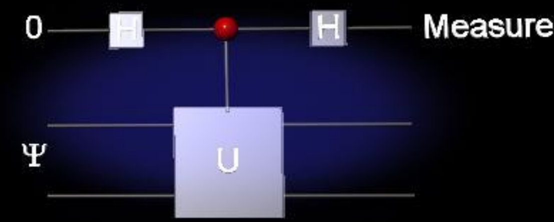
$$\equiv$$

$$\left|\psi\right\rangle=\sum_{x,y}\alpha_{x,y}\left|\beta_{xy}\right\rangle$$



$$\left|\beta_{xy}\right\rangle$$

$$prob\left|\alpha_{xy}\right|^2$$



Example 2: teleportation

Suppose Alice wishes to send a qubit $\left|\Psi\right\rangle = \alpha\left|0\right\rangle + \beta\left|1\right\rangle$ to Bob.

$\left|\Psi\right\rangle$

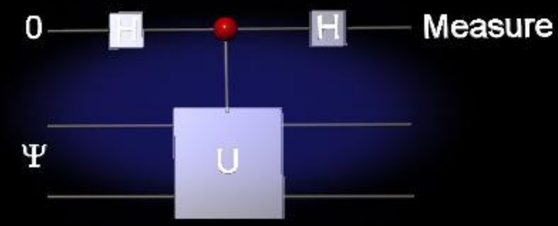
They only possess a classical communication channel.

But they also share a Bell state, e.g. $\left|\beta_{00}\right\rangle$

$\left|\beta_{00}\right\rangle$

Can they do it??

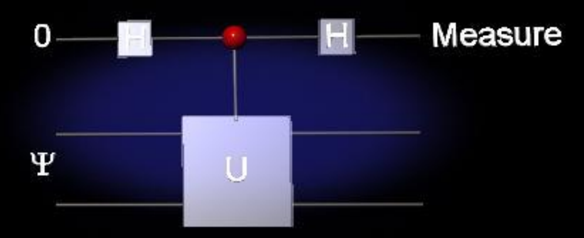
Application: teleportation



Alice wishes to send a qubit $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$ to Bob

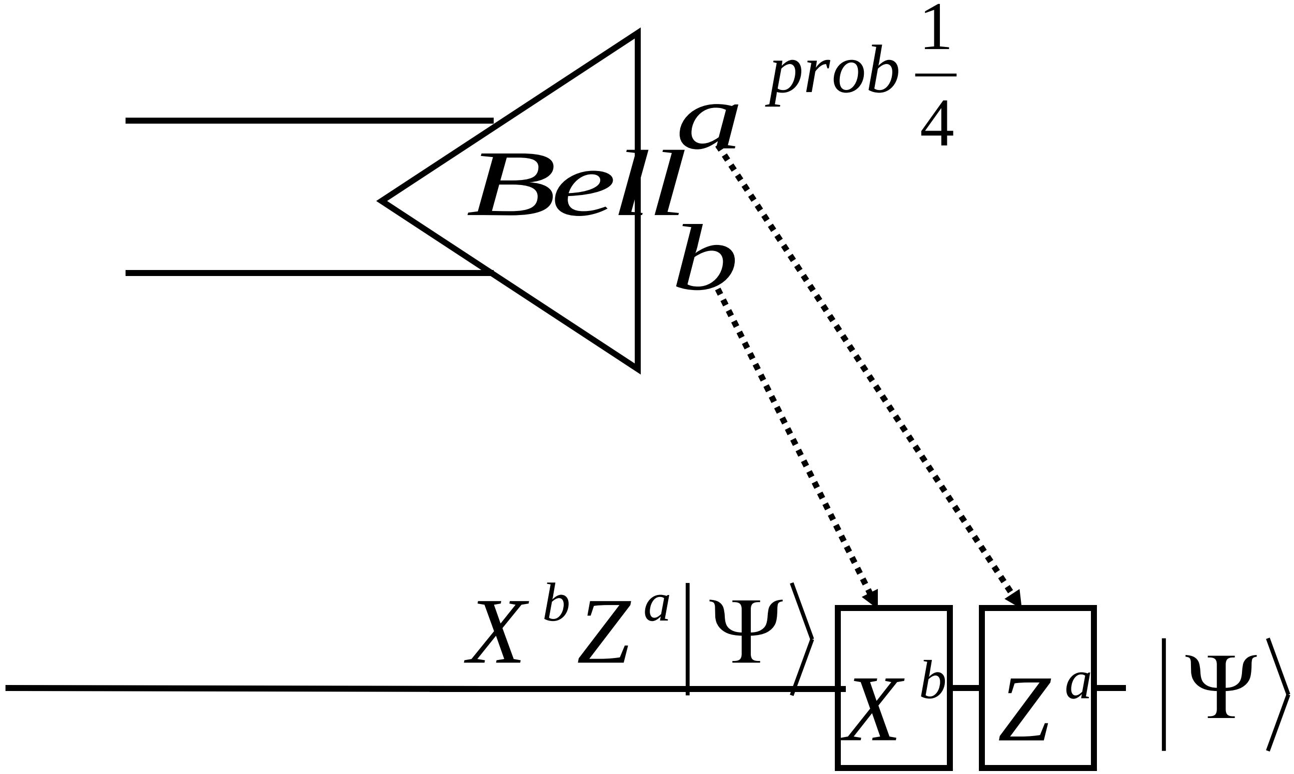
Their joint state $|\Psi\rangle|\beta_{00}\rangle$ equals

$$\begin{aligned}\alpha|0\rangle|\beta_{00}\rangle + \beta|1\rangle|\beta_{00}\rangle &= \frac{1}{2}|\beta_{00}\rangle\big(\alpha|0\rangle + \beta|1\rangle\big)\\ &+ \frac{1}{2}|\beta_{01}\rangle\big(\alpha|1\rangle + \beta|0\rangle\big)\\ &+ \frac{1}{2}|\beta_{10}\rangle\big(\alpha|0\rangle - \beta|1\rangle\big)\\ &+ \frac{1}{2}|\beta_{11}\rangle\big(\alpha|1\rangle - \beta|0\rangle\big)\end{aligned} = \sum_{a,b} \frac{1}{2}|\beta_{a,b}\rangle\big(X^b Z^a|\Psi\rangle\big)$$

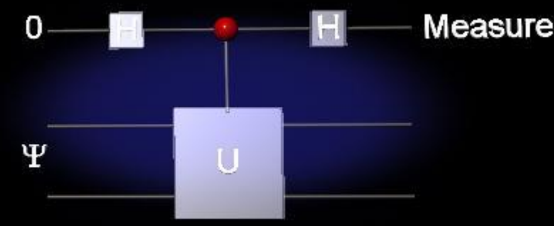


Application: teleportation

$$\frac{1}{2}|\beta_{00}\rangle(\alpha|0\rangle+\beta|1\rangle)$$
$$+\frac{1}{2}|\beta_{01}\rangle(\alpha|1\rangle+\beta|0\rangle)$$
$$+\frac{1}{2}|\beta_{10}\rangle(\alpha|0\rangle-\beta|1\rangle)$$
$$+\frac{1}{2}|\beta_{11}\rangle(\alpha|1\rangle-\beta|0\rangle)$$

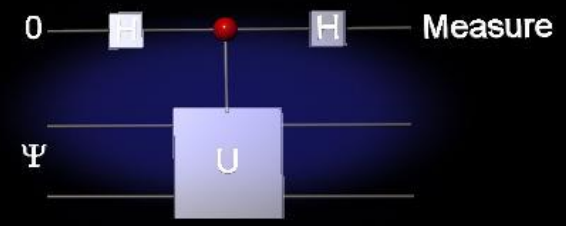


Can send one qubit with one shared Bell pair and 2 classical bits of communication!



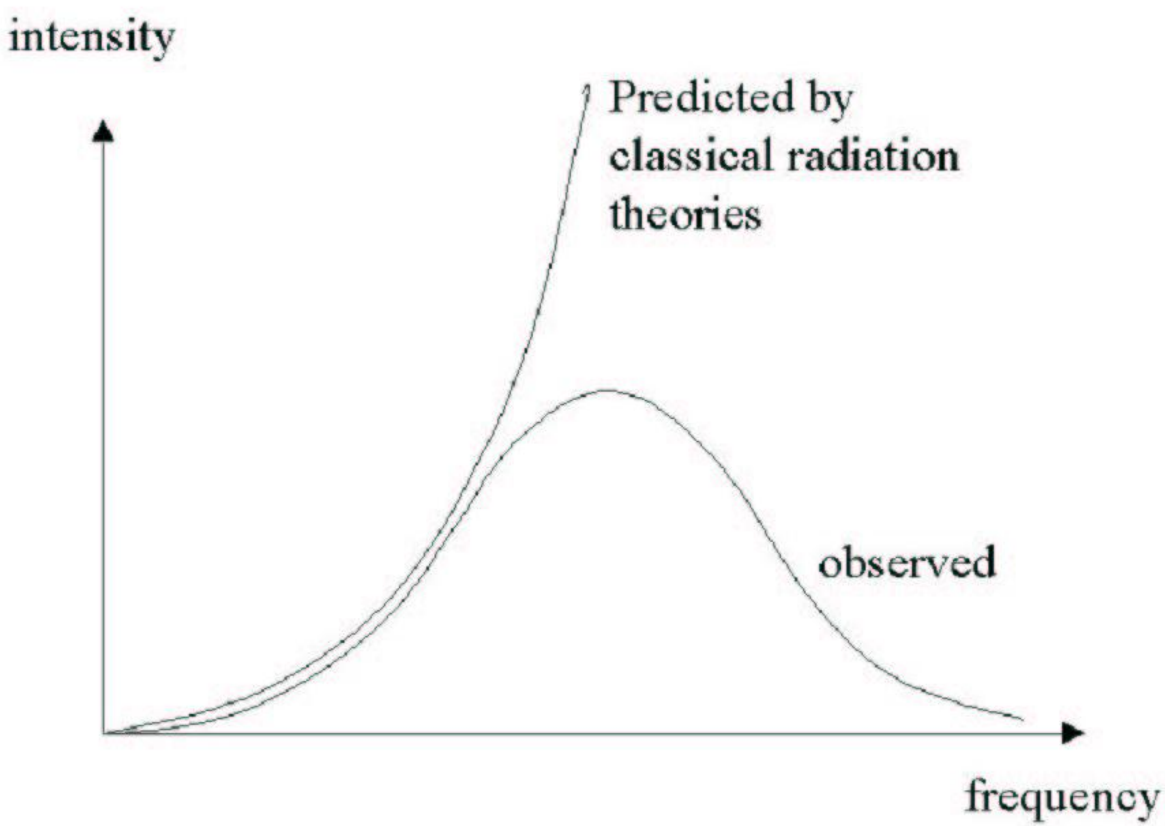
Historical motivation for quantum mechanics

Why quantum mechanics?

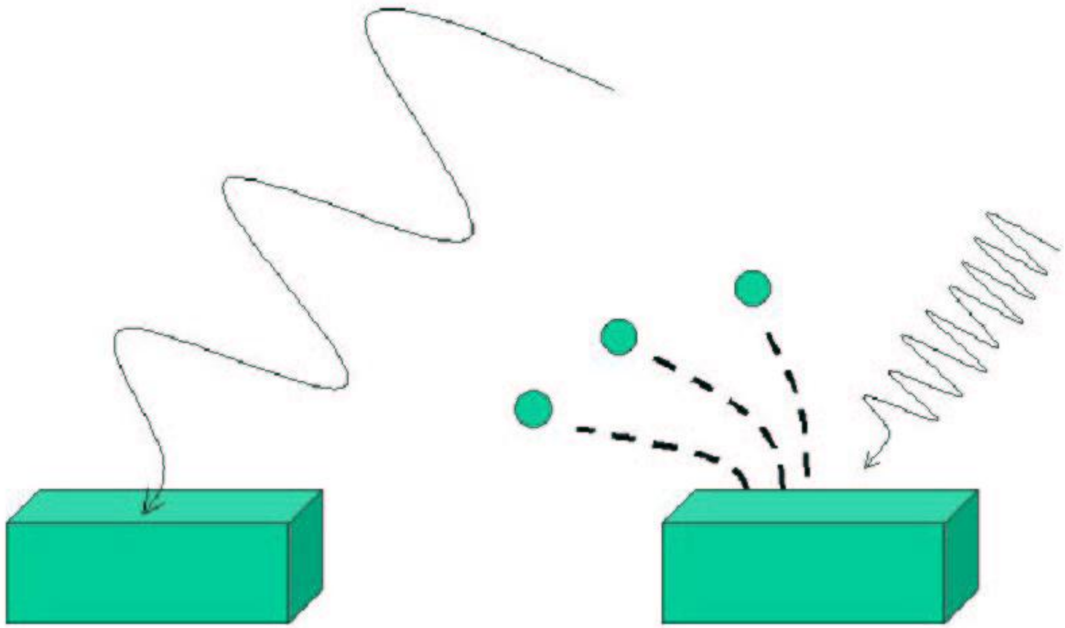


- Historically, these phenomena provided motivation for quantum mechanics
  - Equilibrium of radiation with the walls of a cavity
  - Photoelectric effect
  - Discrete spectrum of atomic radiation
  - Stability of atoms

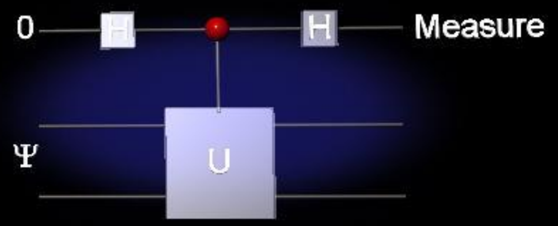
Equilibrium of radiation with the walls of a cavity



Photoelectric effect



Discrete spectrum of atomic radiation



Stability of atoms

This is what should occur according to the Maxwell equations.
But it doesn't occur.

Why?