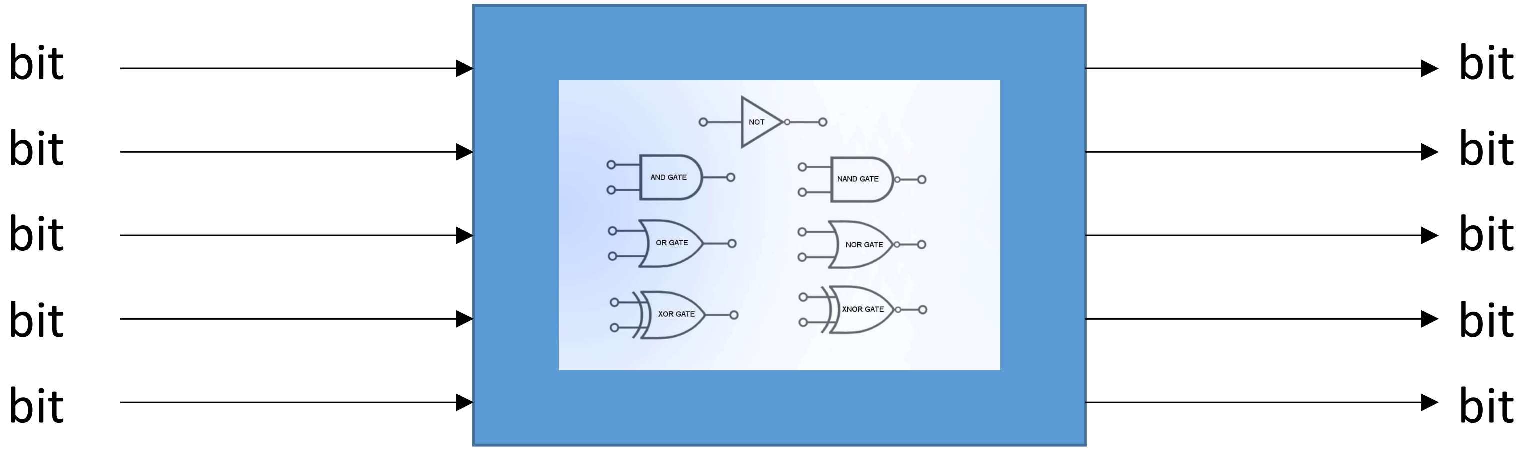
© Can Stock Photo - csp16101833

Quantum…

Computing

Lecture 4: Or how I got stuck in a time machine
And made some money

Classical computation


bit

bit

bit

bit

bit

bit

bit

bit

bit

bit

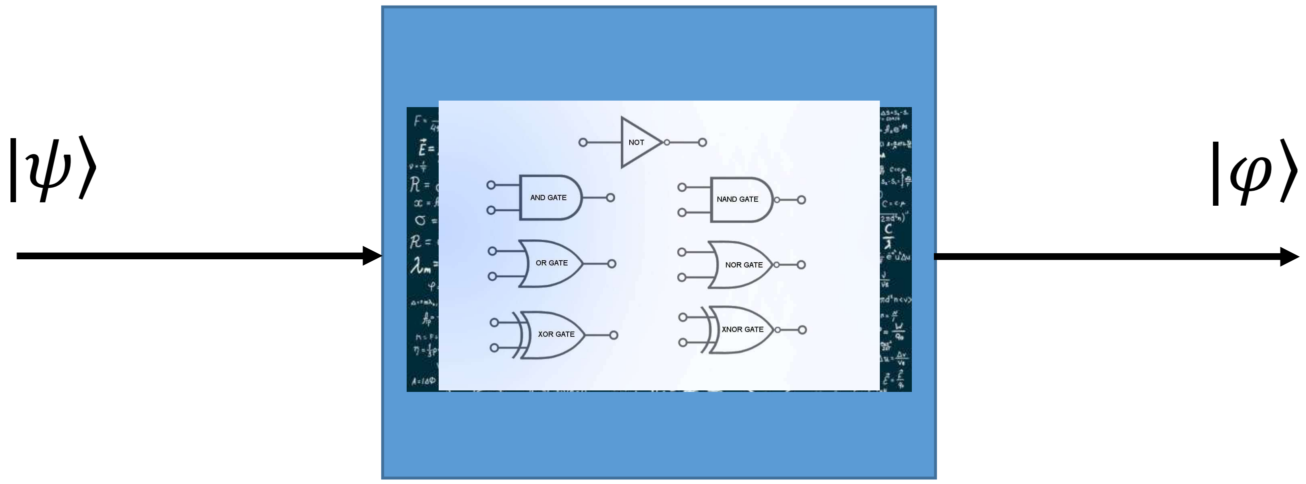
- A box that performs a computation
  - Takes in a collection of bits, outputs one or more bits
- The box is composed of gates
  - Binary gates: 2 inputs, one output
  - Large fan-in gates: many inputs one output
- Objective in design
  - **Ensure the output is always right**
  - **Minimize the number of gates**
  - **Other objectives**

Note: You can do it all using only NAND gates

(but may need an exponential number of them)

NAND is a universal gate

Quantum computation


$|\psi\rangle$ $|\varphi\rangle$

- A box that performs a computation
- The box too is composed of computations that are analogous to the Boolean operations and gates

Poll 1

- An N-bit Boolean function is built as a quantum circuit. How many inputs and outputs does the quantum circuit have.
  - ○ N qubit input , N qubit output
  - ○ 2^N qubit input, 2^N qubit output
  - ○ N qubit input, 2^N qubit output
  - ○ 2N qubit input, 1 qubit output

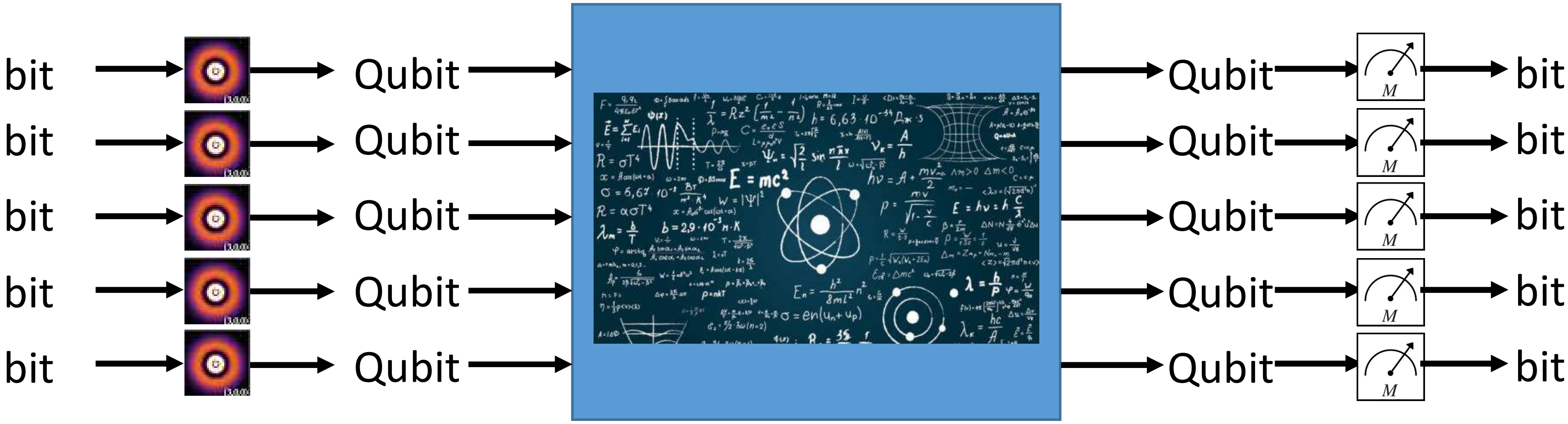
- An N-bit Boolean function is built as a quantum circuit. What is the dimensionality of the input and output of the circuit.
  - ○ N dimensional input , N dimensional output
  - ○ 2^N dimensional input, 2^N dimensional output
  - ○ N dimensional input, 2^N dimensional output
  - ○ 2N dimensional input, 1 dimensional output

Poll 1

- An N-bit Boolean function is built as a quantum circuit. How many inputs and outputs does the quantum circuit have.
  - ○ **N qubit input , N qubit output**
  - ○ 2^N qubit input, 2^N qubit output
  - ○ N qubit input, 2^N qubit output
  - ○ 2N qubit input, 1 qubit output

- An N-bit Boolean function is built as a quantum circuit. What is the dimensionality of the input and output of the circuit.
  - ○ N dimensional input , N dimensional output
  - ○ **2^N dimensional input, 2^N dimensional output**
  - ○ N dimensional input, 2^N dimensional output
  - ○ 2N dimensional input, 1 dimensional output

The secret life of a quantum computer



bit → Qubit → Qubit → bit

bit → Qubit → Qubit → bit

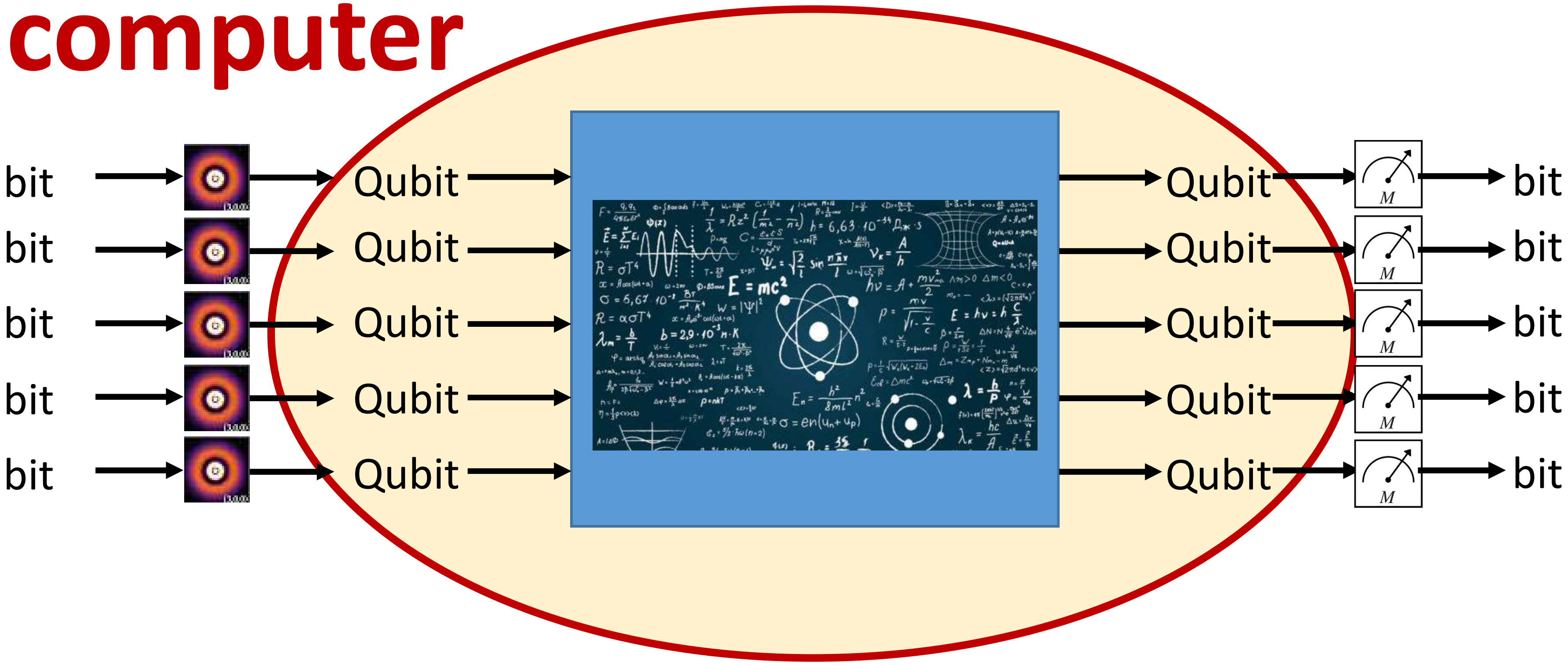
bit → Qubit → Qubit → bit

bit → Qubit → Qubit → bit

bit → Qubit → Qubit → bit

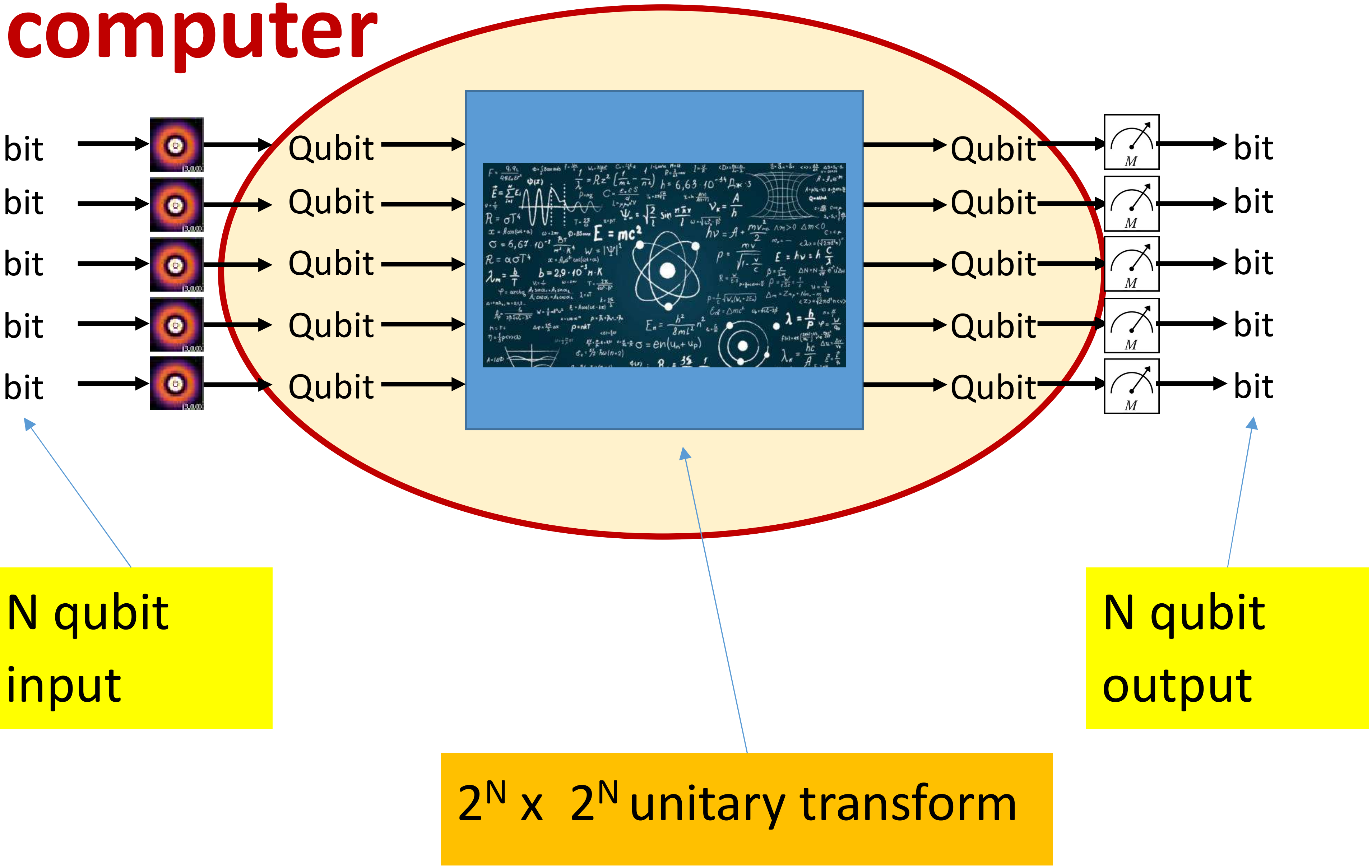
- The complete cycle

The secret life of a quantum computer



- The complete cycle
- The actual quantum computation
  - The computer may itself include measurement as in internal operation

The secret life of a quantum computer



bit → Qubit → Qubit → bit

bit → Qubit → Qubit → bit

bit → Qubit → Qubit → bit

bit → Qubit → Qubit → bit

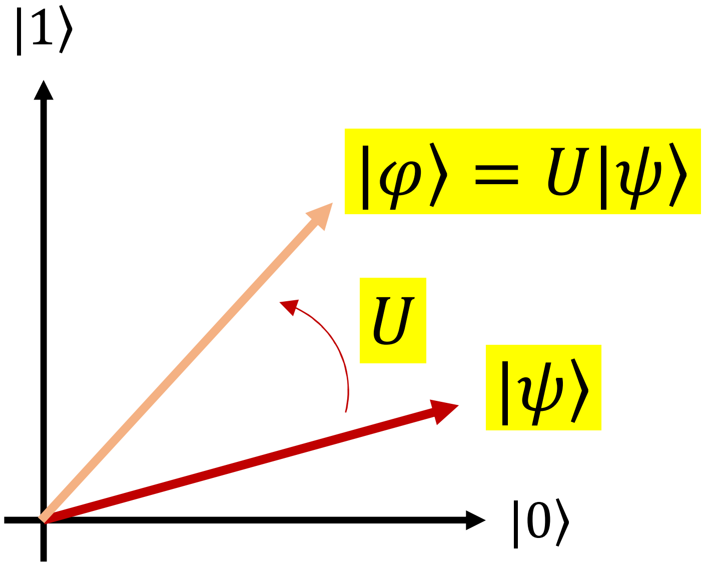
bit → Qubit → Qubit → bit

N qubit input

2^N x 2^N unitary transform

N qubit output

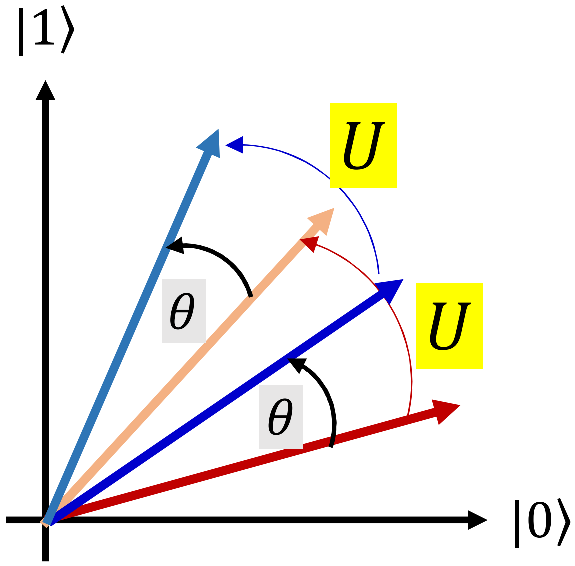
What is a Unitary Transform



$$U = \begin{bmatrix} u_1 & u_2 & \dots & u_L \end{bmatrix}$$

- A Unitary transform is a *rotation*
  - It is invertible and maintains the length of the input

Properties of a Unitary Transform



The angle between the red and blue phasors remains unchanged after each of them has been rotated by U

- If two vectors $|a\rangle$ and $|b\rangle$ are rotated by the same amount, the angle between them remains unchanged
  - *Unitary transforms retain angles*

$$\langle Ua|Ub\rangle = \langle a|b\rangle$$

$$\Rightarrow \ (Ua)^H(Ub) = a^H U^H U b = a^H b$$

$$\Rightarrow U^H U = I$$

- The Hermitian of U is its own inverse
  - The columns of U are orthogonal to one another (why)?

Poll 2

- Mark all that are true of a unitary transform matrix
  - ○ Its columns are unit-length vectors
  - ○ There is no length restriction on the length of the vectors that form the columns of the unitary matrix
  - ○ The columns of the matrix must all be orthogonal to one another
  - ○ There is no restriction on the angles between the columns
  - ○ The columns of the matrix form an orthogonal basis set
  - ○ The columns of the matrix are linearly independent, but not necessarily a complete basis set
  - ○ A unitary matrix transforms one of the bases into one of the columns of the matrix

Poll 2

- Mark all that are true of a unitary transform matrix
  - **Its columns are unit-length vectors**
  - There is no length restriction on the length of the vectors that form the columns of the unitary matrix
  - **The columns of the matrix must all be orthogonal to one another**
  - There is no restriction on the angles between the columns
  - **The columns of the matrix form an orthogonal basis set**
  - The columns of the matrix are linearly independent, but not necessarily a complete basis set
  - **A unitary matrix transforms one of the bases into one of the columns of the matrix**

Properties of a Unitary Transform

$$\begin{bmatrix} u_1 & u_2 & \dots & u_L \end{bmatrix} \begin{bmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{bmatrix} = u_2$$

$U|1\rangle = |u_2\rangle$

$$\begin{bmatrix} u_1 & u_2 & \dots & u_L \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} = u_1$$

$U|0\rangle = |u_1\rangle$

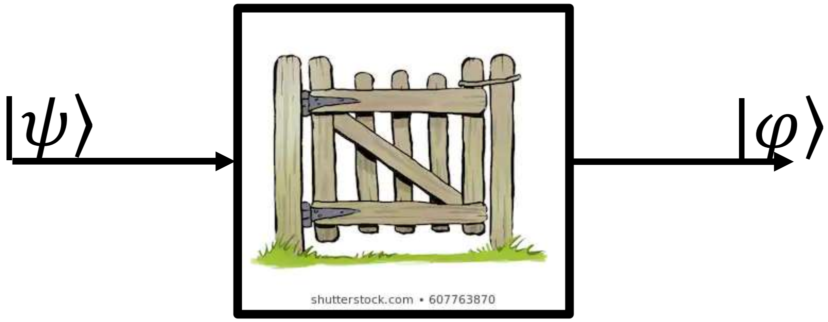
$|u_i| = ?$

$$\begin{bmatrix} u_1 & u_2 & \dots & u_L \end{bmatrix} \begin{bmatrix} a \\ b \\ 0 \\ 0 \end{bmatrix} = ?$$

$U(a|0\rangle + b|1\rangle) = ?$

- What happens when we transform a basis $| *\rangle$?
  - What is the *length* of u_i?
- Each of the original bases gets mapped onto one of the columns of U
  - The columns of U form a new bases
- What happens when we transform a superposed phasor?
- Transforming a superposed phasor results in a superposition of the columns of the matrix!

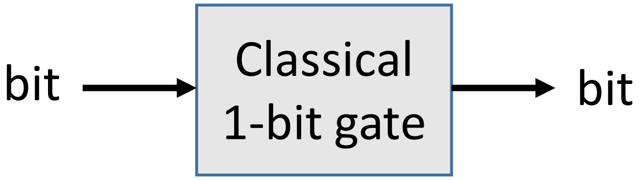
How to check if a transformation U is a valid "gate"



$|\varphi\rangle = U|\psi\rangle$

- How to check if U is a *valid* "gate" (quantum operator)
- U must be Unitary:
  - Verify that $U^H U = I$
  - Every gate must satisfy this criterion

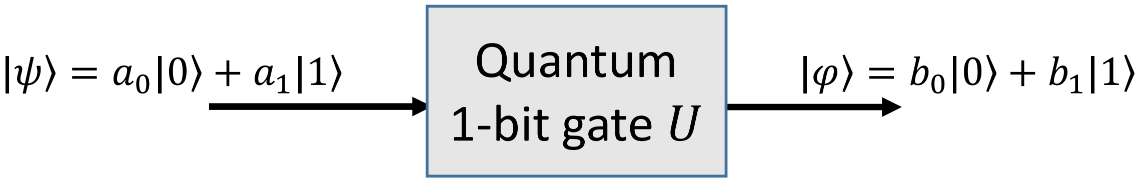
Revisiting single qubit gates



bit

Classical 1-bit gate

bit



$|\psi\rangle = a_0|0\rangle + a_1|1\rangle$

Quantum 1-bit gate U

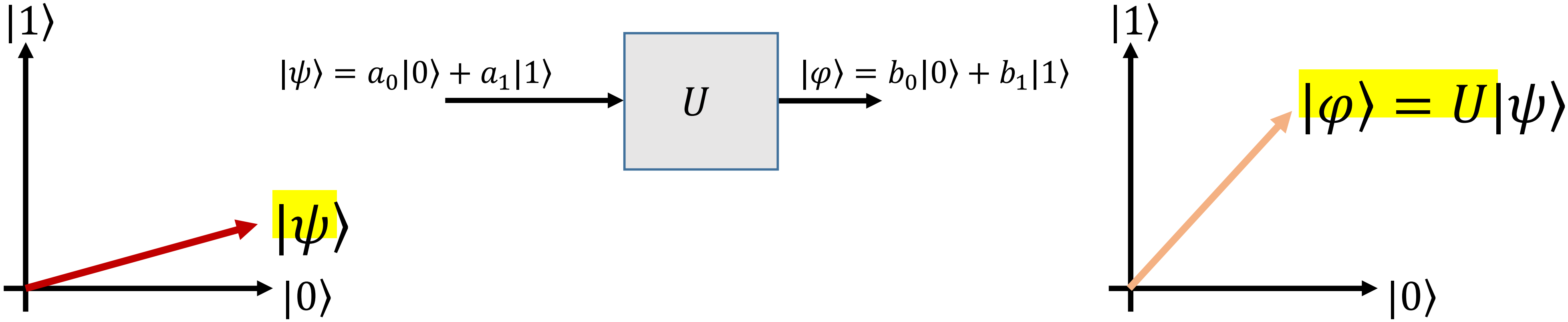
$|\varphi\rangle = b_0|0\rangle + b_1|1\rangle$

$$U = \begin{bmatrix} u_{00} & u_{01} \\ u_{10} & u_{11} \end{bmatrix}$$

$$\begin{bmatrix} b_0 \\ b_1 \end{bmatrix} = \begin{bmatrix} u_{00} & u_{01} \\ u_{10} & u_{11} \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \end{bmatrix}$$

- Classical gate: One bit goes in, one bit comes out
- Quantum gate: one qubit *encoding a 2D complex phasor* goes in, one qubit comes out
  - Note, even though its only physically one qubit, logically it represents a 2D phasor
    - This is the magic of quantum computers employing quantum phenomena

One Qubit gate



$|\psi\rangle = a_0|0\rangle + a_1|1\rangle$

$|\varphi\rangle = b_0|0\rangle + b_1|1\rangle$

$$U = \begin{bmatrix} u_{00} & u_{01} \\ u_{!0} & u_{11} \end{bmatrix}$$

$$\begin{bmatrix} b_0 \\ b_1 \end{bmatrix} = \begin{bmatrix} u_{00} & u_{01} \\ u_{!0} & u_{11} \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \end{bmatrix}$$

- 2D phasor $|\psi\rangle$ goes in, 2D phasor $|\varphi\rangle$ comes out

$$|\varphi\rangle = U|\psi\rangle$$

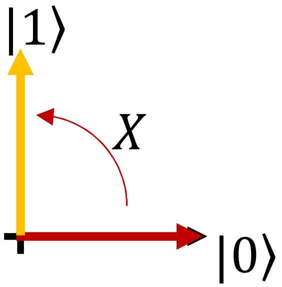
- U is a unitary transform

Single qubit gates: The bit-flip gate X

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

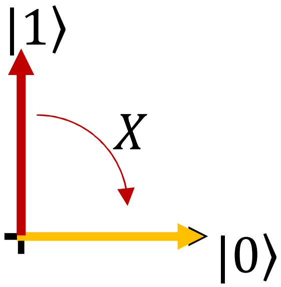
$$|0\rangle \rightarrow \boxed{X} \rightarrow |1\rangle$$

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



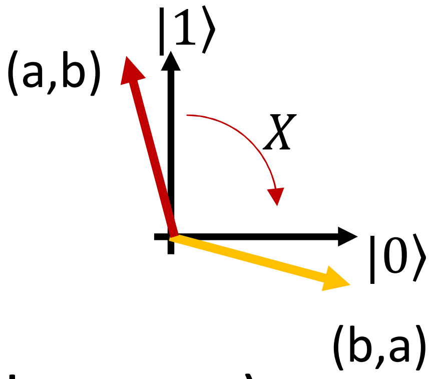
$$|1\rangle \rightarrow \boxed{X} \rightarrow |0\rangle$$

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



$$a|0\rangle + b|1\rangle \rightarrow \boxed{X} \rightarrow b|0\rangle + a|1\rangle$$

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



- First verify that X is unitary (or its not really a gate)

- Swaps the |0> and |1> bit values
  - Note – it swaps bit values in 2D
  - Can be *viewed* as flipping |0> and |1> in the phasor

The *phase* flip gate Z

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

$$|0\rangle \rightarrow \boxed{Z} \rightarrow |0\rangle$$

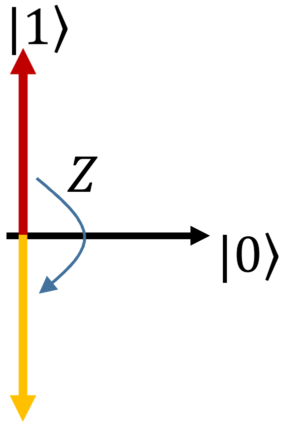
$$\begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

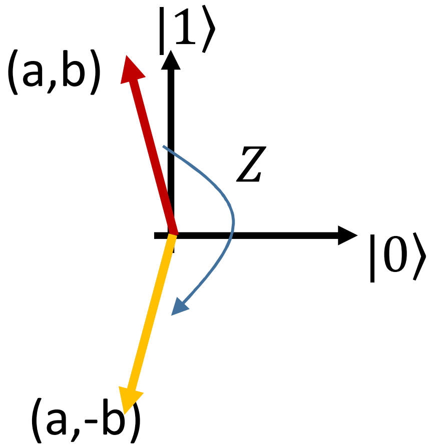
$$|1\rangle \rightarrow \boxed{Z} \rightarrow -|1\rangle$$

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

$$a|0\rangle + b|1\rangle \rightarrow \boxed{Z} \rightarrow a|0\rangle - b|1\rangle$$

$$\begin{bmatrix} a \\ -b \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix}$$





- The phase flip gate simply flips the *sign* of the |1> component
- First, verify that it’s a Unitary transform
- The phase flip gate doesn’t really change the probability of measuring |0> or |1>, so what is it doing?

The *phase* flip gate Z

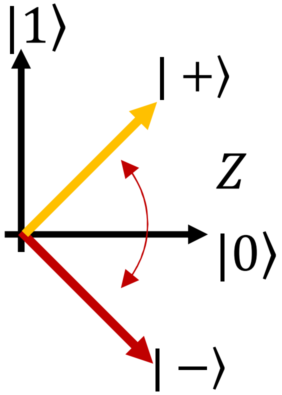
$$\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \longrightarrow \boxed{Z} \longrightarrow \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$$

$$\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle \longrightarrow \boxed{Z} \longrightarrow \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

$$|+\rangle \longrightarrow \boxed{Z} \longrightarrow |-\rangle$$

$$|-\rangle \longrightarrow \boxed{Z} \longrightarrow |+\rangle$$

$$\begin{bmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix}$$



$$\begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{bmatrix}$$

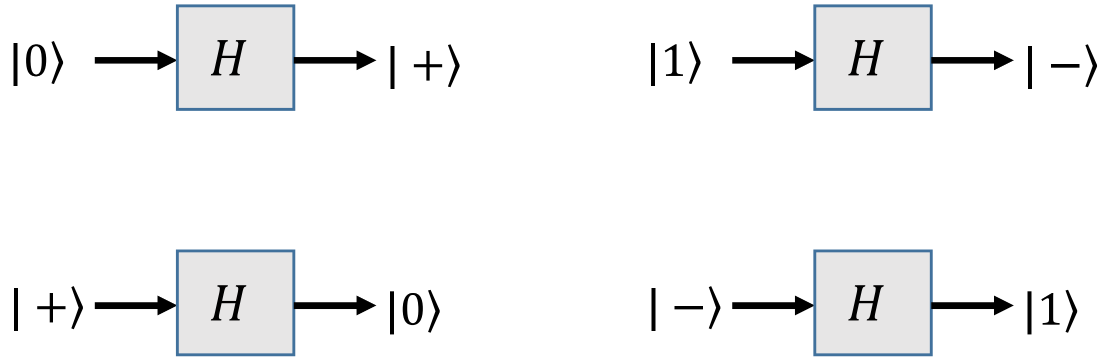
- The Phase flip gate is in fact the *sign flip* gate

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

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

The *Hadamard* gate H

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



Write this down in algebra

- First verify that it's a Unitary transform
- The Hadamard gate converts bit bases to sign bases and vice versa

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

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

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

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

A digression: How do we measure with different bases?

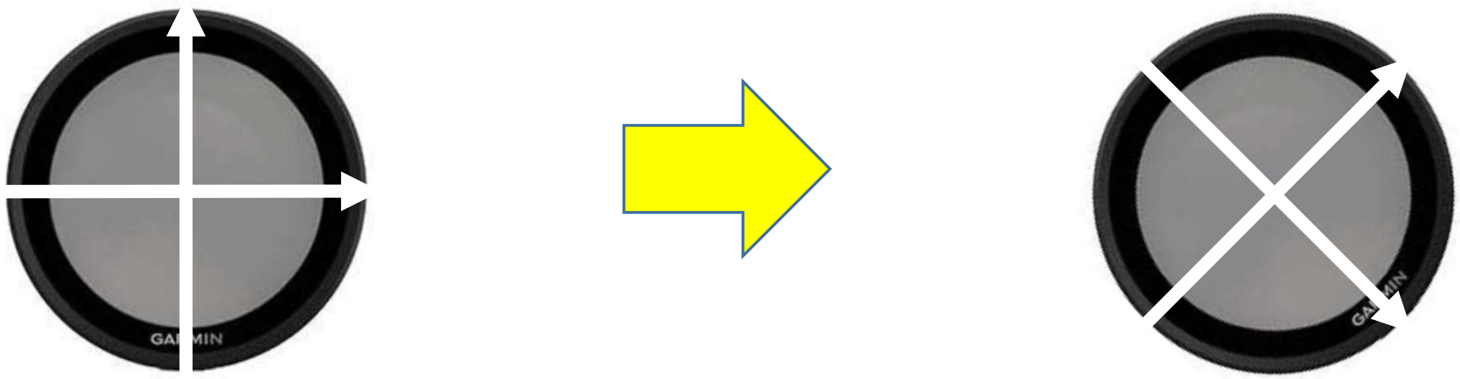
- We will specifically consider the sign bases vs the bit bases?

A digression: How do we measure with different bases?

- We will specifically consider the sign bases vs the bit bases?
  - The distinction between the two is that they are at 45 degrees to one another

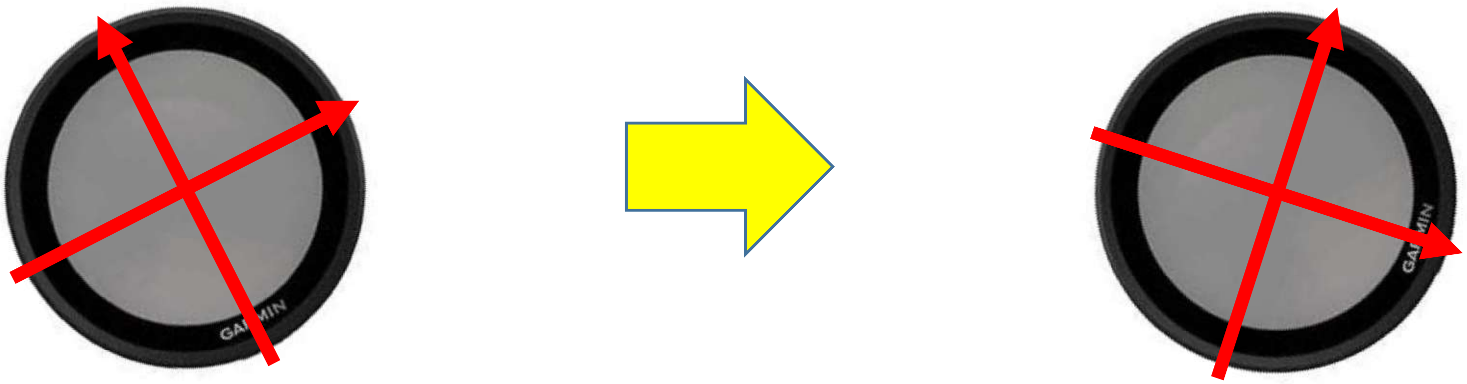
- Keep in mind that there is no “absolute” basis
  - There’s no “absolute bit basis” and no “absolute sign basis”
  - The bit and sign bases only differ from each other through their *relation* to one another
    - 45 degrees

Bit bases and Sign basis



Bit bases

Sign bases



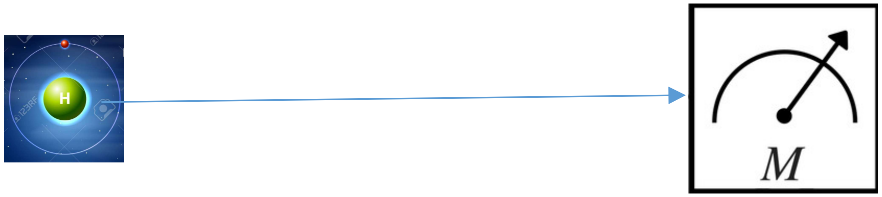
Bit bases

Sign bases

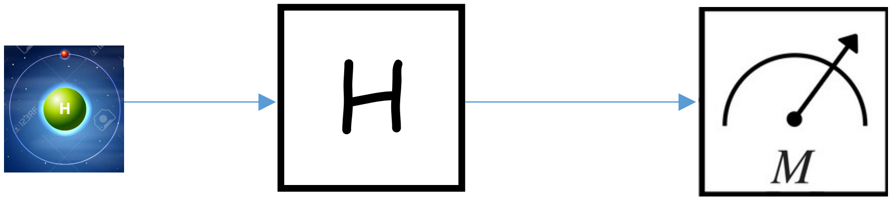
The bit bases can be oriented anyhow

The sign bases are at +-45^o to the bit bases

Measuring with bit bases vs. measuring with sign bases



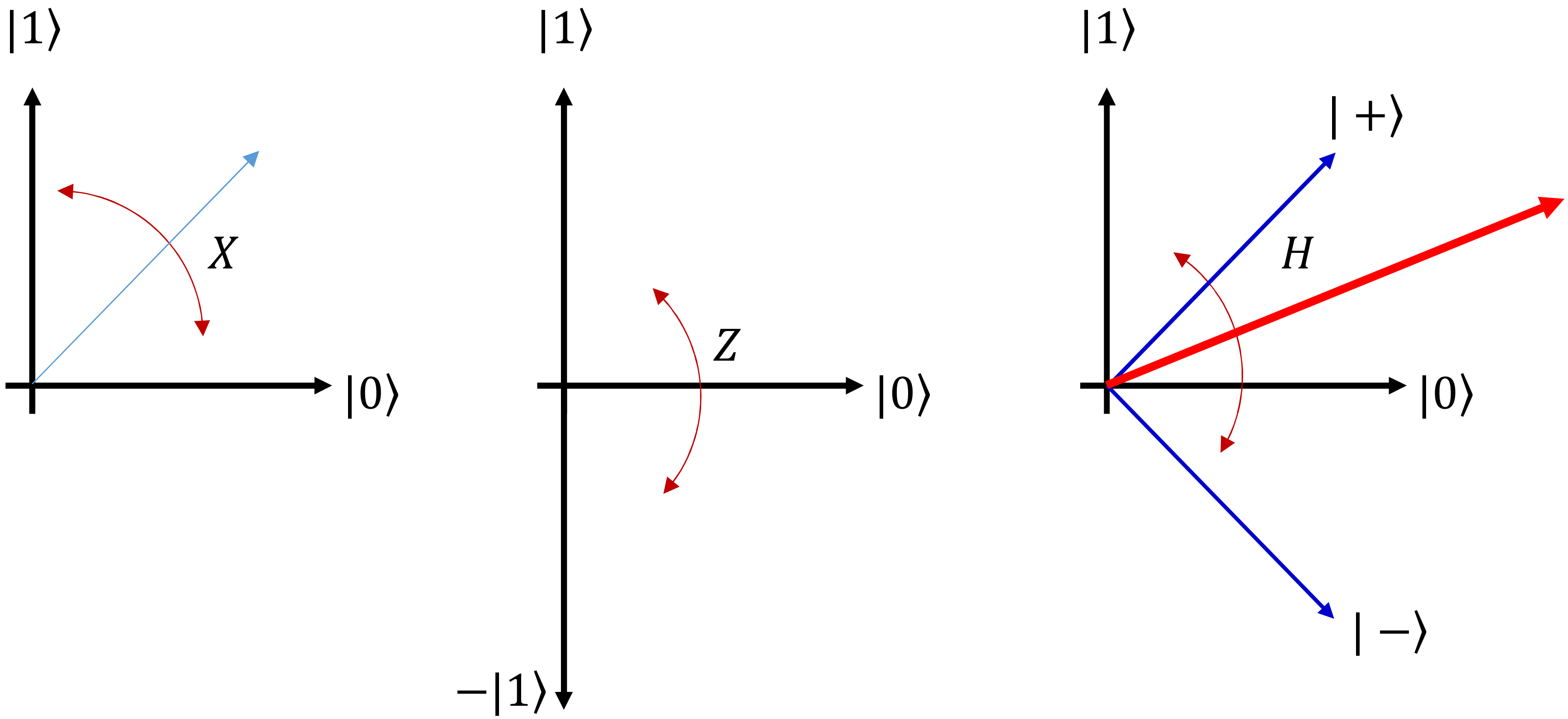
- Measuring with bit basis (above) vs.
- Measuring with sign basis (below)



Returning to our topic: Unitary transforms are *rotations*

- So what kind of rotations are
  - The bit flip gate?
  - The phase flip gate?
  - The Hadamard gate?

Unitary transforms are rotations



- Note that all of these gates are special – since their entries are all real, and they're symmetric, they are their own inverse

- Applying them twice in a row reverts to the original!!

The three 1-qubit gates: H X and Z

$$\begin{tikzcd}
|0\rangle \arrow[r, leftrightarrow, "X"] \arrow[d, leftrightarrow, "H"'] & |1\rangle \arrow[d, leftrightarrow, "H"] \\
|+\rangle \arrow[r, leftrightarrow, "Z"] & |-\rangle
\end{tikzcd}$$

- $X|0\rangle = |1\rangle$
- $Z|-\rangle = |+\rangle$
- $HZHX|a\rangle = |a\rangle$

- $H|1\rangle = |-\rangle$
- $H|+\rangle = |0\rangle$
- $HZH = X$

Single qubit gates: The phase and bit-flip gate Y

$$Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

$$|0\rangle \longrightarrow \boxed{Y} \longrightarrow i|1\rangle$$

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

$$|1\rangle \longrightarrow \boxed{Y} \longrightarrow -i|0\rangle$$

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

$$a|0\rangle + b|1\rangle \longrightarrow \boxed{Y} \longrightarrow ib|0\rangle - ia|1\rangle$$

$$\begin{bmatrix} -ib \\ ia \end{bmatrix} = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix}$$

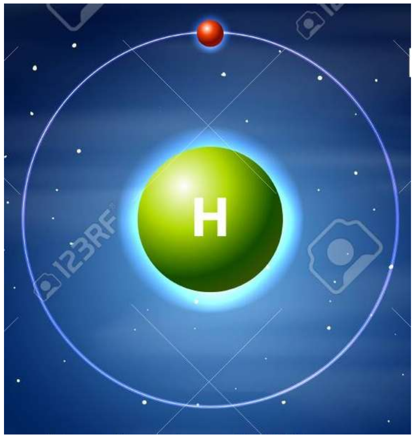
Can't really visualize

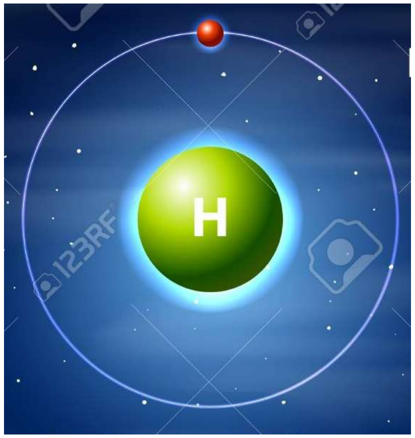
- First verify that Y is unitary (or its not really a gate)
- Swaps the |0> and |1> bit values
  - But also flips them from the real to the imaginary axis
  - Also flips the +/- bases (to where?)

Moving on…

- Not much you can do with only one bit
- Let’s add another bit..

You can’t get very far with one bit



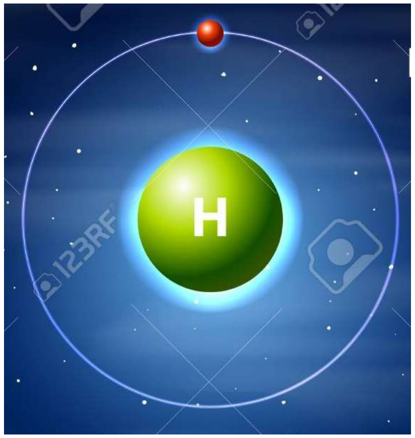


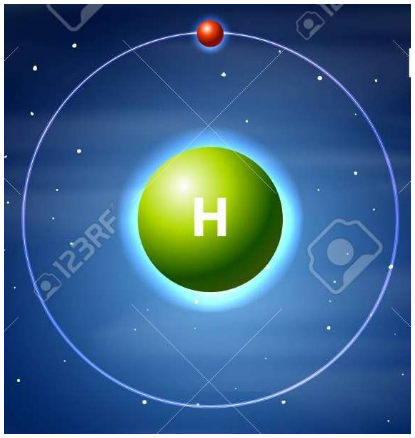
- Two qubits walk into a bar…

$$|\psi_0\rangle = \alpha_0|0> + \alpha_1|1>$$
$$|\psi_1\rangle = \beta_0|0> + \beta_1|1>$$

- How many states does the combined system have
  - How many coordinates in the new system

Representing the combined system





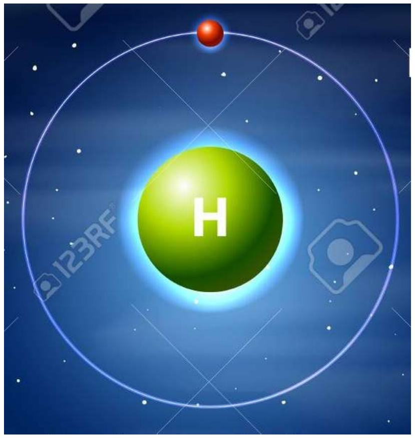
- Two qubits walk into a bar…

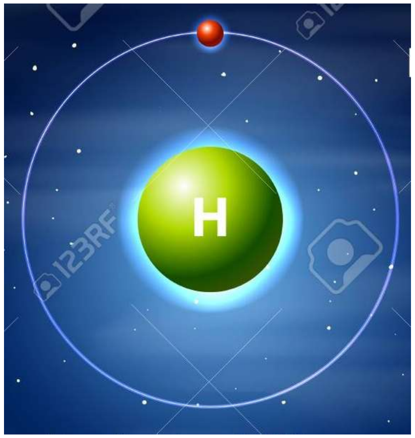
$$|\psi_0\rangle = \alpha_0|0> + \alpha_1|1>$$
$$|\psi_1\rangle = \beta_0|0> + \beta_1|1>$$

- The combined system:

$$|\psi\rangle = \gamma_{00}|00> + \gamma_{01}|01> + \gamma_{10}|10> + \gamma_{11}|11>$$

Representing the combined system





- Two qubits walk into a bar…

$$|\psi_0\rangle = \alpha_0|0> + \alpha_1|1>$$

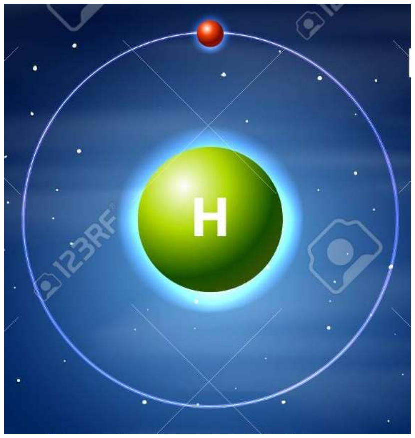
$$|\psi_1\rangle = \beta_0|0> + \beta_1|1>$$

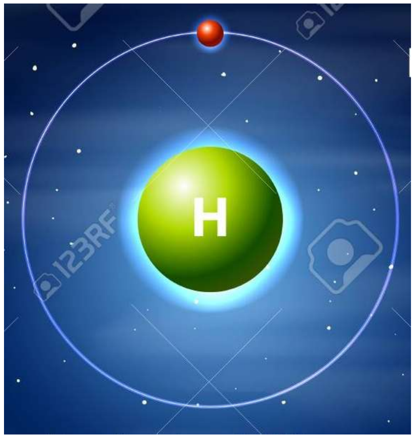
What is $|\psi\rangle$ assuming non-interacting qubits

- The combined system:

$$|\psi\rangle = \gamma_{00}|00> + \gamma_{01}|01>+ \gamma_{10}|10>+ \gamma_{11}|11>$$

Representing the combined system





- Two qubits walk into a bar…

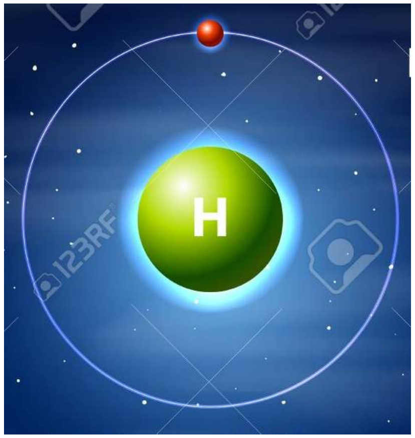
$$|\psi_0\rangle = \alpha_0|+> + \alpha_1|->$$
$$|\psi_1\rangle = \beta_0|0> + \beta_1|1>$$

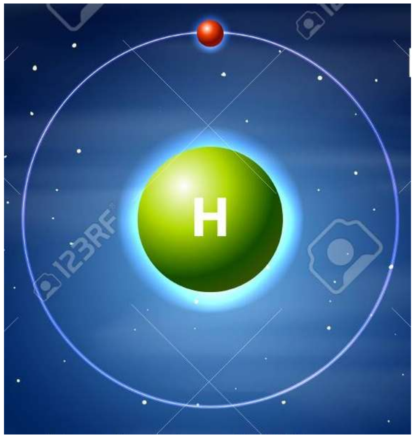
What is $|\psi\rangle$ assuming non-interacting qubits

- The combined system:

$$|\psi\rangle = \gamma_{00}|00> + \gamma_{01}|01>+ \gamma_{10}|10>+ \gamma_{11}|11>$$

Representing the combined system





- Two qubits walk into a bar…

$$|\psi_0\rangle = \alpha_0 |+> + \alpha_1 |->$$

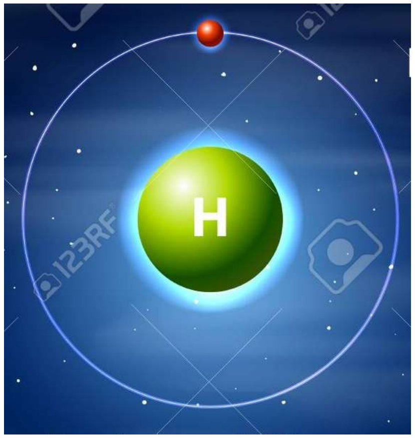
$$|\psi_1\rangle = \beta_0 |0> + \beta_1 |1>$$

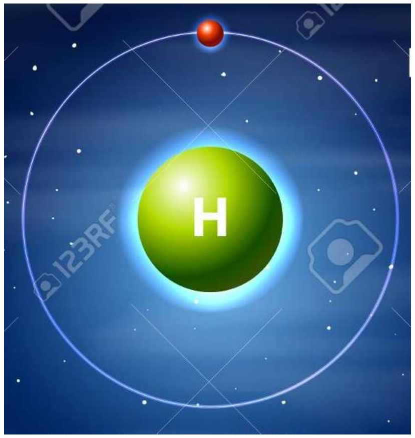
What is $|\psi\rangle$ assuming non-interacting qubits

- The combined system:

$$|\psi\rangle = \gamma_{00} |+0> + \gamma_{01} |+1> + \gamma_{10} |-0> + \gamma_{11} |-1>$$

Representing the combined system





- Two qubits walk into a bar…

$$|\psi_0\rangle = \alpha_0 |{+}{>} + \alpha_1 |{-}{>}$$

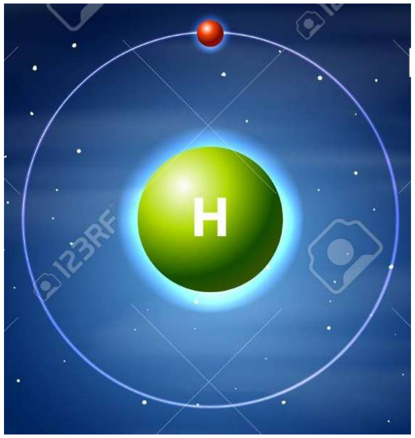
$$|\psi_1\rangle = \beta_0 |{+}{>} + \beta_1 |{-}{>}$$

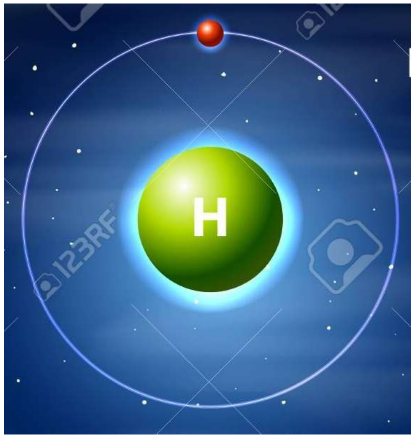
What is $|\psi\rangle$ assuming non-interacting qubits

- The combined system:

$$|\psi\rangle = \gamma_{00} |{+}{+}{>} + \gamma_{01} |{+}{-}{>} + \gamma_{10} |{-}{+}{>} + \gamma_{11} |{-}{-}{>}$$

In vector representation





- Two qubits walk into a bar…

Assuming bit bases all around

$$|\psi_0\rangle = \begin{bmatrix}\alpha_0\\ \alpha_1\end{bmatrix} \qquad |\psi_1\rangle = \begin{bmatrix}\beta_0\\ \beta_1\end{bmatrix}$$

- The combined system vector is? (Assuming non-interacting qubits)
  - What is this strange mathematical operation?

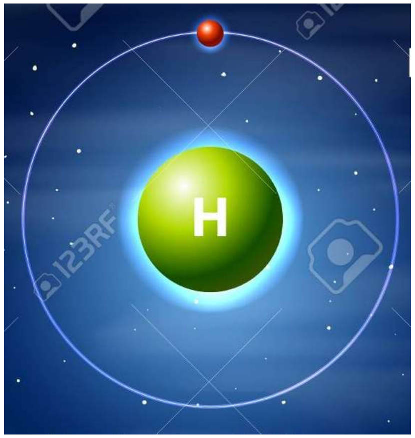
The *Kronecker* product of two vectors

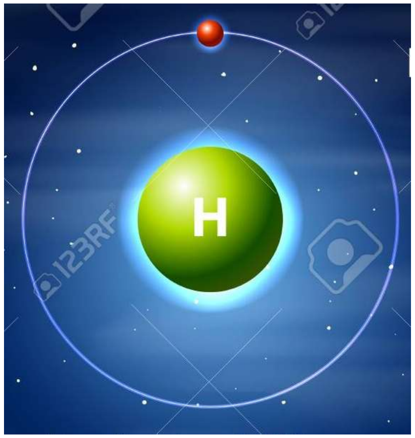
$$\begin{bmatrix}\alpha_0\\ \alpha_1\end{bmatrix} \otimes \begin{bmatrix}\beta_0\\ \beta_1\end{bmatrix} = \begin{bmatrix}\alpha_0 \begin{bmatrix}\beta_0\\ \beta_1\end{bmatrix}\\ \alpha_1 \begin{bmatrix}\beta_0\\ \beta_1\end{bmatrix}\end{bmatrix} = \begin{bmatrix}\alpha_0\beta_0\\ \alpha_0\beta_1\\ \alpha_1\beta_0\\ \alpha_1\beta_1\end{bmatrix}$$

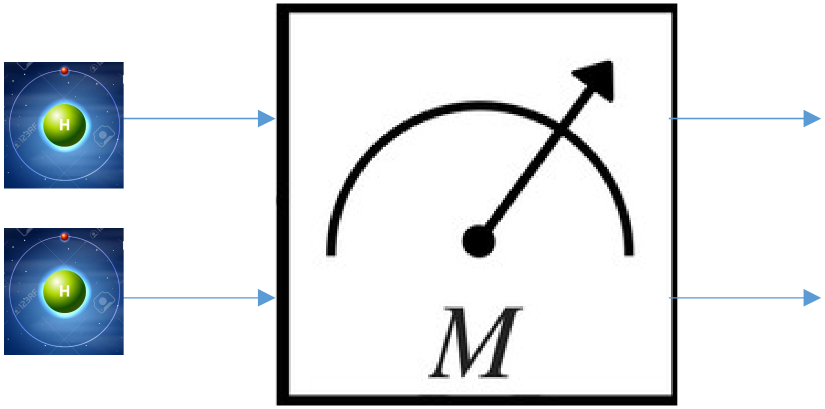
- In Ket notation

  $(\alpha_0|0> + \alpha_1|1>) \otimes (\beta_0|0> + \beta_1|1>)$
  $= \alpha_0\beta_0|00> + \alpha_0\beta_1|01> + \alpha_1\beta_0|10> + \alpha_1\beta_1|11>$

Measuring the two-cubit system



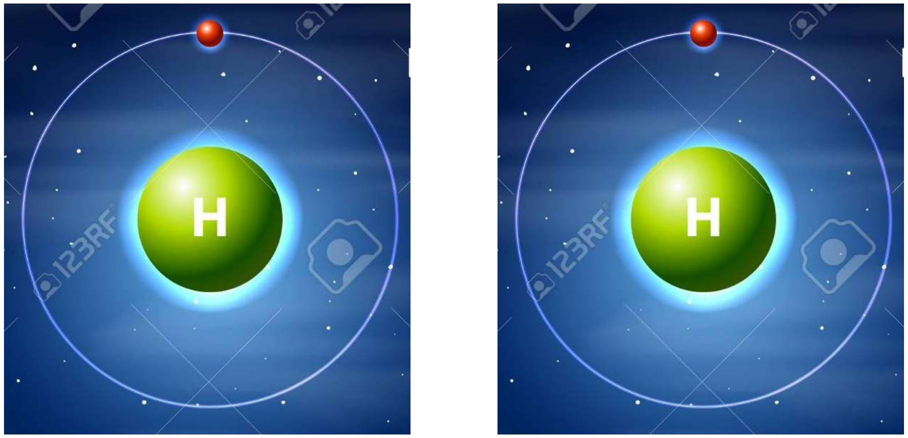


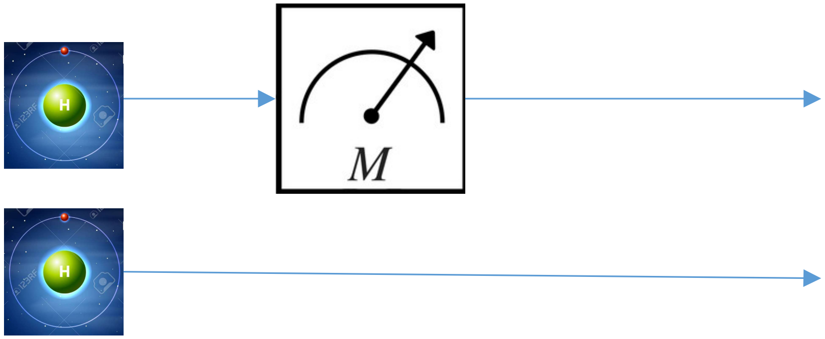


$$|\psi\rangle = \gamma_{00}|00> + \gamma_{01}|01>+ \gamma_{10}|10>+ \gamma_{11}|11>$$

- Measuring the combined system:
  - We can measure both cubits simultaneously

Measuring the two-cubit system

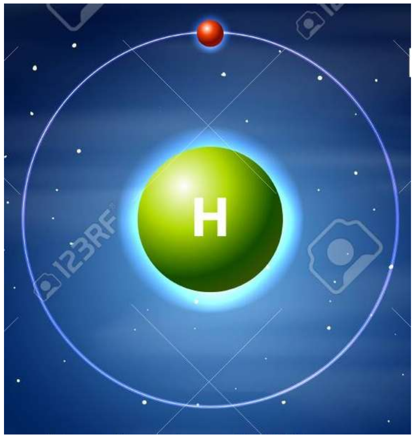


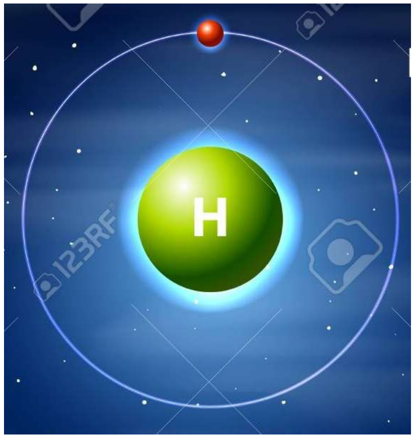


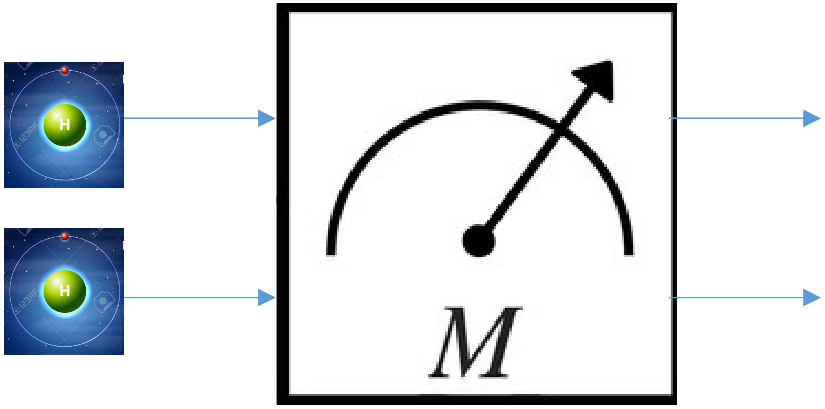
$$|\psi\rangle = \gamma_{00}|00> + \gamma_{01}|01> + \gamma_{10}|10> + \gamma_{11}|11>$$

- Measuring the combined system:
  - We can measure both cubits simultaneously
  - Or just one

Simultaneous measurement







- Two qubits walk into a bar…

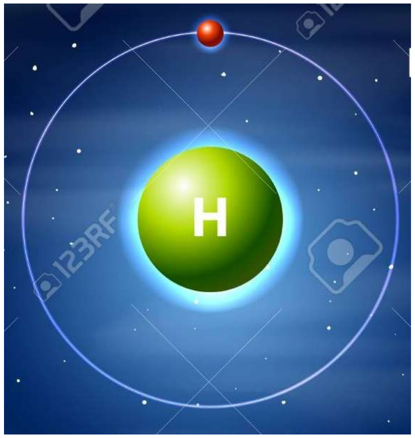
$$|\psi_0\rangle = \alpha_0|0> + \alpha_1|1>$$
$$|\psi_1\rangle = \beta_0|0> + \beta_1|1>$$

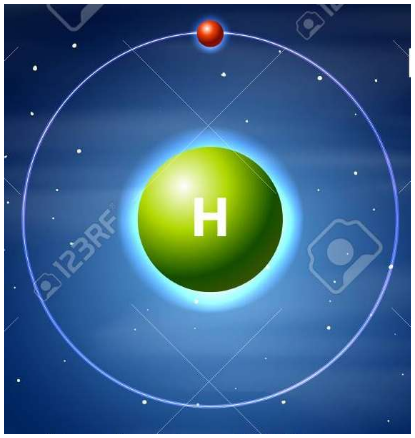
Assuming non-interacting qubits

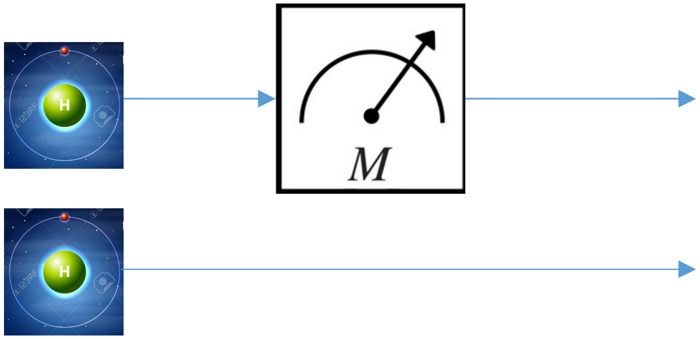
$$|\psi\rangle = \gamma_{00}|00> + \gamma_{01}|01> + \gamma_{10}|10> + \gamma_{11}|11>$$

- What will measurement give us and with what probability

Individual measurement







- Two qubits walk into a bar…

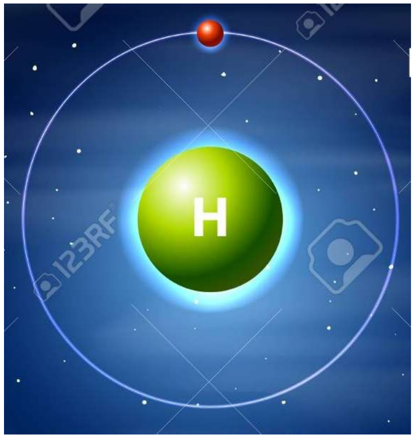
$$|\psi_0\rangle = \alpha_0|0> + \alpha_1|1>$$
$$|\psi_1\rangle = \beta_0|0> + \beta_1|1>$$

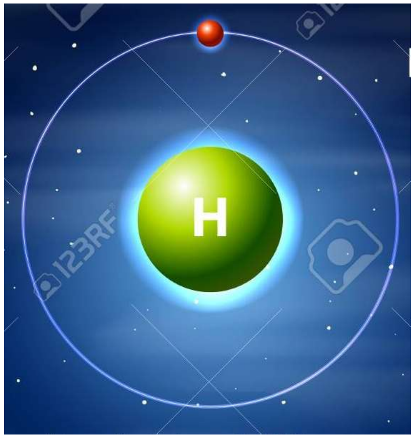
Assuming
non-interacting qubits

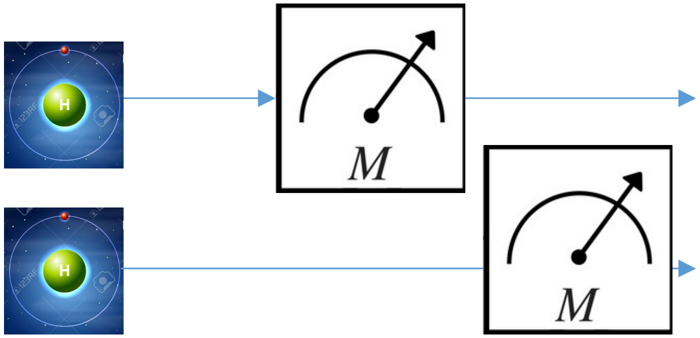
$$|\psi\rangle = \gamma_{00}|00> + \gamma_{01}|01> + \gamma_{10}|10> + \gamma_{11}|11>$$

- What will measurement give us?
  - You’re measuring bit 0
  - What are the outcomes likely to be, and with what probability?

Individual measurement







Assuming non-interacting qubits

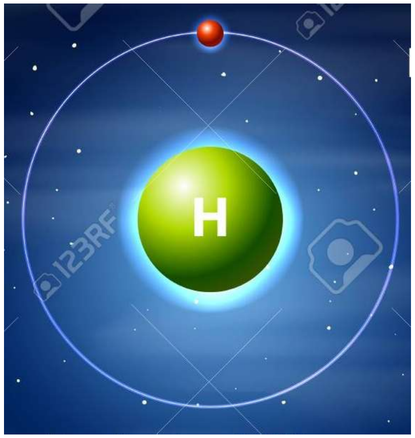
- Two qubits walk into a bar…

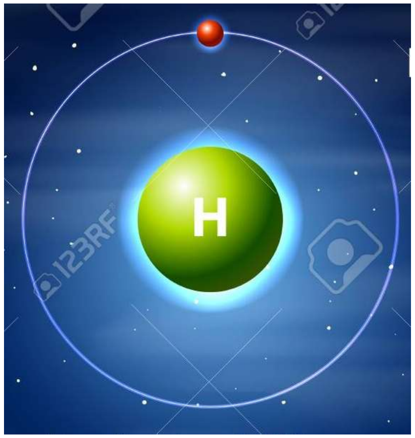
$$|\psi_0\rangle = \alpha_0 |0> + \alpha_1 |1>$$
$$|\psi_1\rangle = \beta_0 |0> + \beta_1 |1>$$

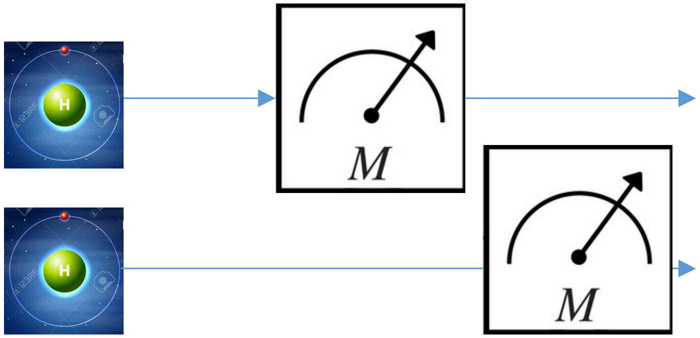
$$|\psi\rangle = \gamma_{00} |00> + \gamma_{01} |01> + \gamma_{10} |10> + \gamma_{11} |11>$$

- You measured bit 0 and got a 0.
  - Then you measure bit 1. What is the probability of getting a 0?

Individual measurement







Assuming non-interacting qubits

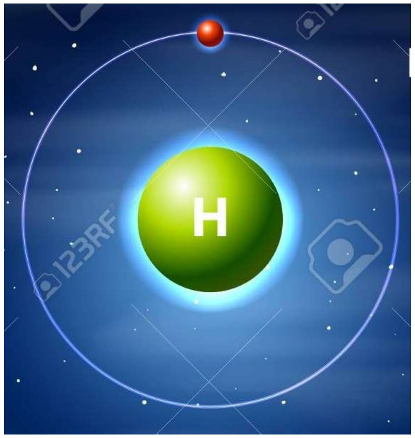
- Two qubits walk into a bar…

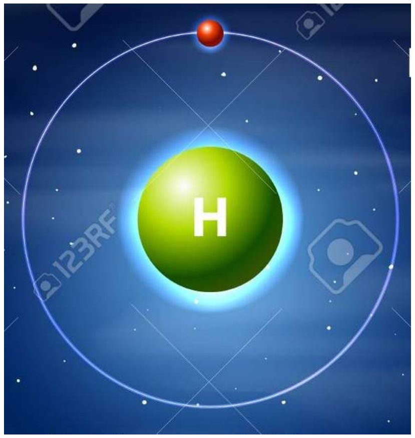
$$|\psi_0\rangle = \alpha_0|0> + \alpha_1|1>$$
$$|\psi_1\rangle = \beta_0|0> + \beta_1|1>$$

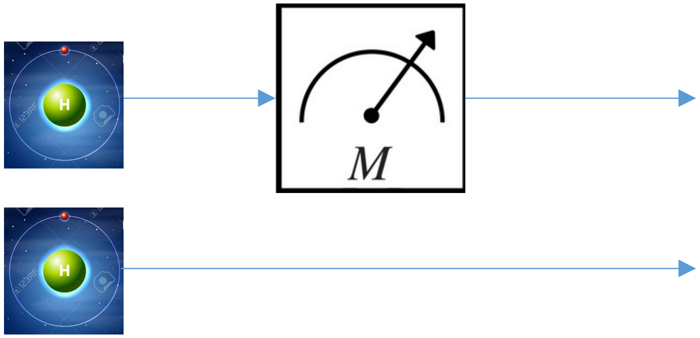
$$|\psi\rangle = \gamma_{00}|00> + \gamma_{01}|01> + \gamma_{10}|10> + \gamma_{11}|11>$$

- You measured bit 0 and got a 0.
  - Then you measure bit 1. What is the probability of getting a 0?
- You measured bit 0 and got a 1
  - Then you measure bit 1. What is the probability of getting 0?

Individual measurement



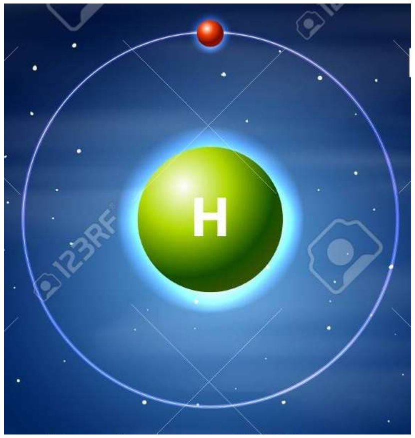


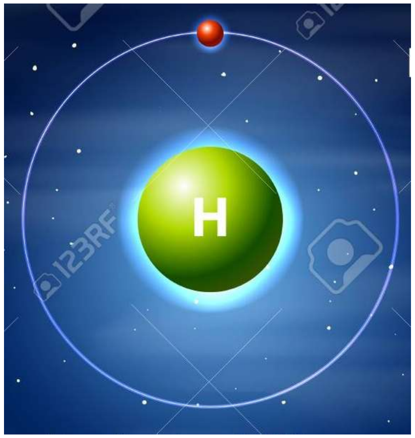


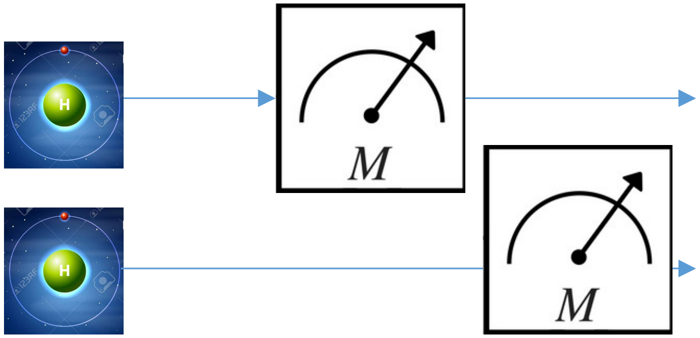
$$|\psi\rangle = \gamma_{00}|00> + \gamma_{01}|01> + \gamma_{10}|10> + \gamma_{11}|11>$$

- What will the outcomes of the measurement of bit 0 be, and with what probability?
    - What is the probability of getting 0?
    - What is the probability of getting 1?

Individual measurement



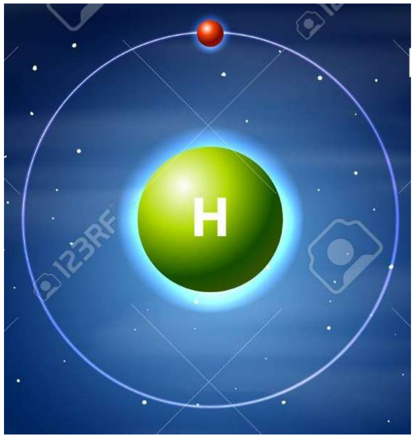


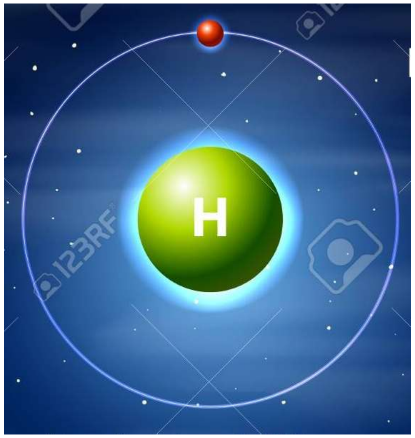


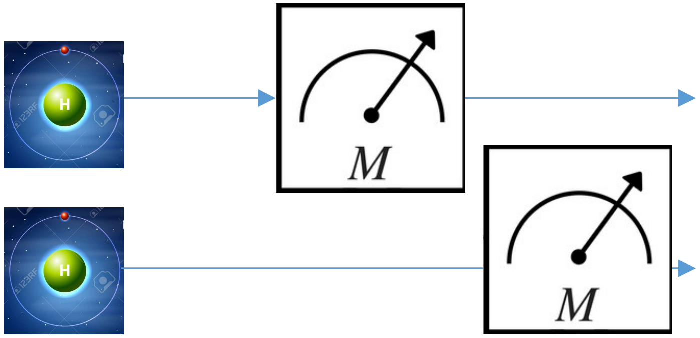
$$|\psi\rangle = \gamma_{00}|00> + \gamma_{01}|01>+ \gamma_{10}|10>+ \gamma_{11}|11>$$

- You measured bit 0 and got a 0.
  - Then you measure bit 1. What is the probability of getting a 0?
- You measured bit 0 and got a 1
  - Then you measure bit 1. What is the probability of getting 0?

Lets plug in some numbers



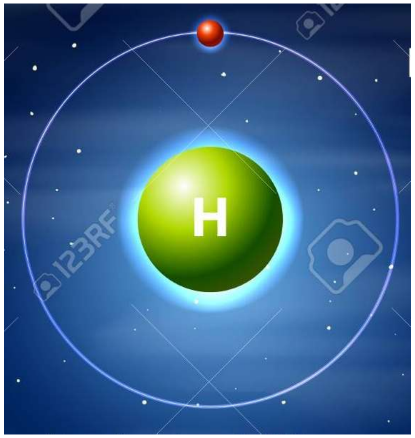


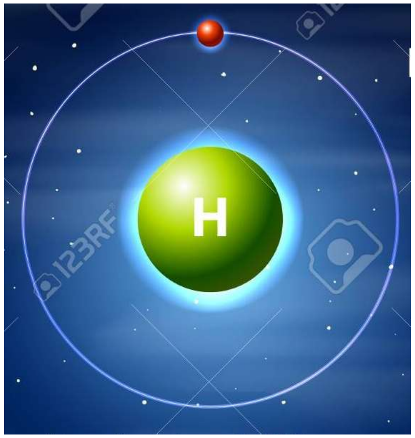


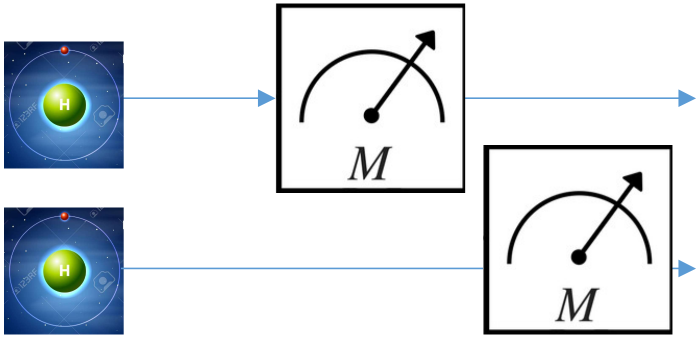
$$|\psi\rangle = \frac{1}{\sqrt{10}}|00> + \frac{\sqrt{2}}{\sqrt{10}}|01> + \frac{\sqrt{3}}{\sqrt{10}}|10> + \frac{2}{\sqrt{10}}|11>$$

- You measured bit 0 and got a 0.
  - Then you measure bit 1. What is the probability of getting a 0?
- You measured bit 0 and got a 1
  - Then you measure bit 1. What is the probability of getting 0?

Lets plug in some numbers



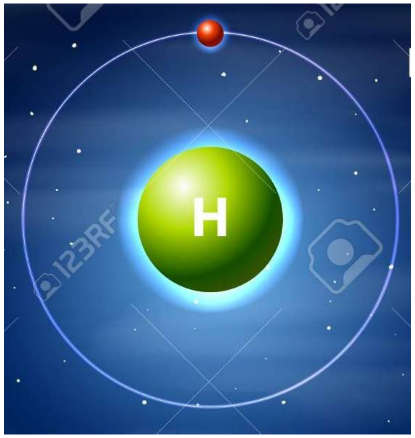


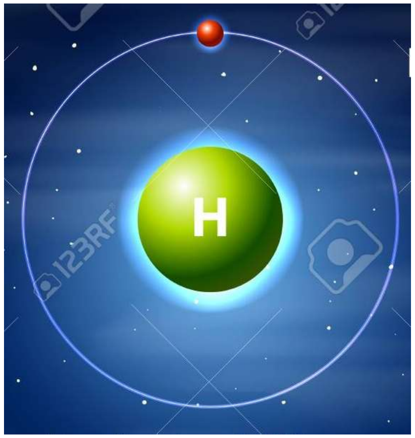


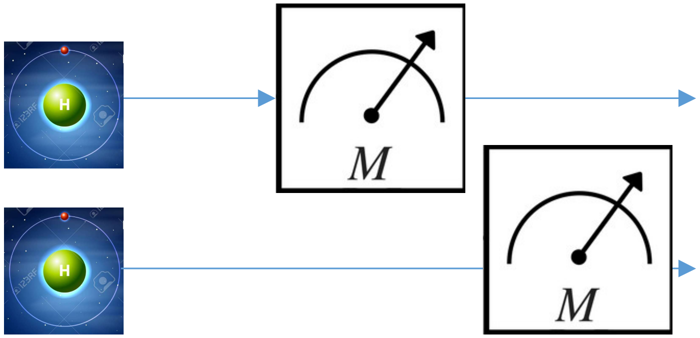
$$|\psi\rangle = \frac{1}{\sqrt{10}}|00> + \frac{\sqrt{2}}{\sqrt{10}}|01> + \frac{\sqrt{3}}{\sqrt{10}}|10> + \frac{2}{\sqrt{10}}|11>$$

- *What happened??*
  - *The value measured for bit 0 influenced the value measured for bit 1!!!*
    - The measurement probabilities for bit 1 changed if the measured value of bit 0 changed!
  - ***The bits are entangled!!!***

Lets plug in some numbers



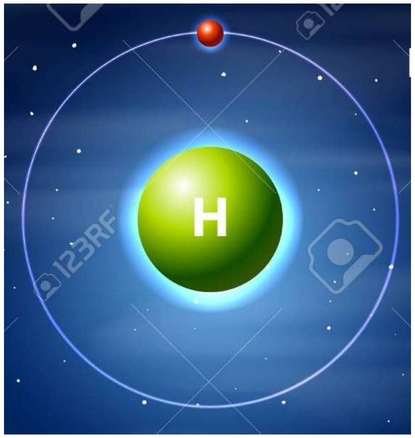


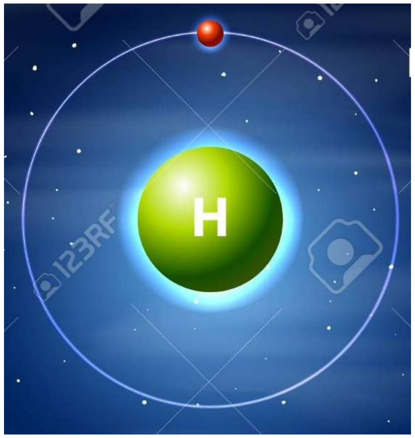


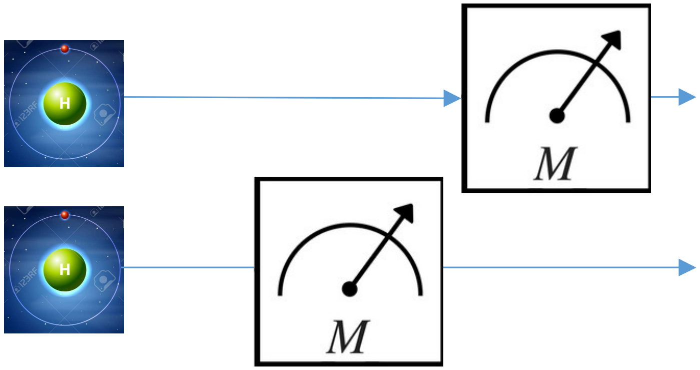
$$|\psi\rangle = \frac{1}{\sqrt{10}}|00> + \frac{\sqrt{2}}{\sqrt{10}}|01>+ \frac{\sqrt{3}}{\sqrt{10}}|10>+ \frac{2}{\sqrt{10}}|11>$$

- We measure b_0 first. What is the probability of 1?
- b_0 turned up 1, now we measure b_1.
  - What is the probability of 1?

Lets plug in some numbers



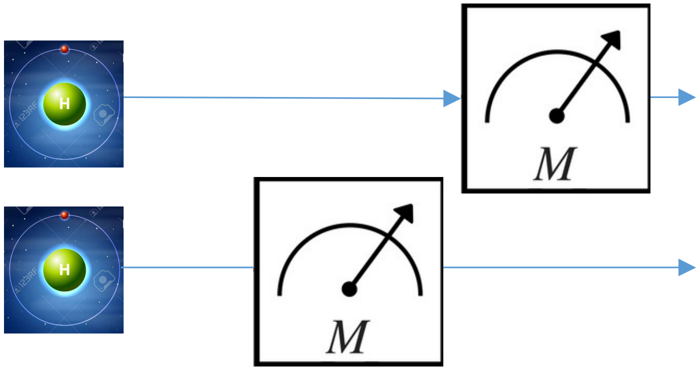


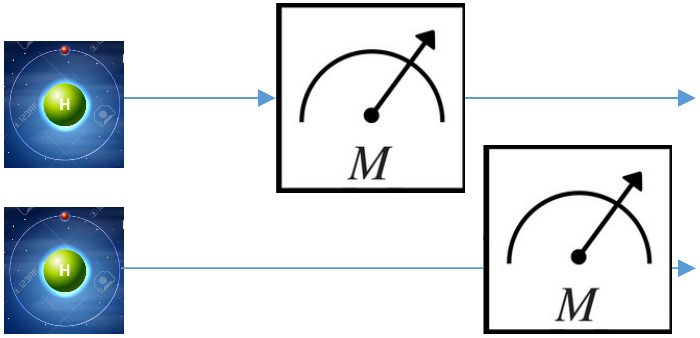


$$|\psi\rangle = \frac{1}{\sqrt{10}}\,|00> + \frac{\sqrt{2}}{\sqrt{10}}\,|01> + \frac{\sqrt{3}}{\sqrt{10}}\,|10> + \frac{2}{\sqrt{10}}\,|11>$$

- Future you measures b_0. What is the probability of 1?
- Future you found b0 = 1. Present you measures b_1 **now**.
  - What is the probability of 1?

Lets plug in some numbers





$$|\psi\rangle = \frac{1}{\sqrt{10}}|00> + \frac{\sqrt{2}}{\sqrt{10}}|01> + \frac{\sqrt{3}}{\sqrt{10}}|10> + \frac{2}{\sqrt{10}}|11>$$

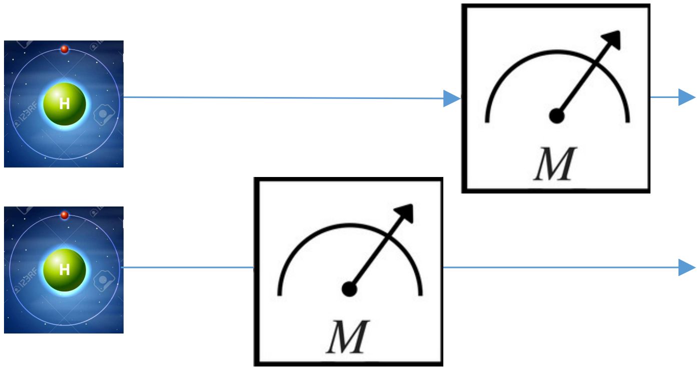
- We measure b first. What is the probability of 1?

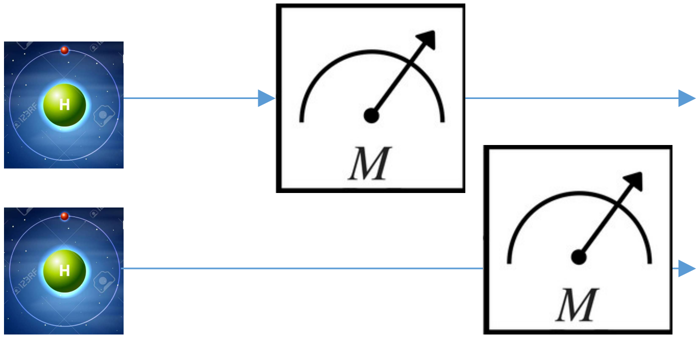
The order of measurement doesn't matter.

The only fact that matters is that the bits are entangled

  - What is the probability of 1?

Lets plug in some numbers





$$\frac{1}{\sqrt{10}} \quad \frac{\sqrt{2}}{\sqrt{10}} \quad \frac{\sqrt{3}}{\sqrt{10}} \quad \frac{2}{\sqrt{10}}$$

The system is a time machine!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

- We measure b first. What is the probability of 1?

The order of measurement doesn't matter.

The only fact that matters is that the bits are entangled

- What is the probability of 1?

A special entangled state

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

- The "Bell" state
  - Named after John Bell
  - Either both bits are 1, or both are 0
- Other Bell States

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

$$|\psi\rangle = \frac{1}{\sqrt{2}}|00> - \frac{1}{\sqrt{2}}|11>$$

$$|\psi\rangle = \frac{1}{\sqrt{2}}|01> - \frac{1}{\sqrt{2}}|10>$$

A special entangled state

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

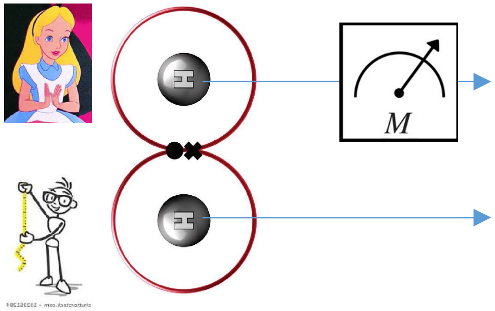
- What is the Bell state, expressed in terms of |++>, |+−>, |−+>, |−−>

The BELL state

- $|\psi\rangle = \frac{1}{\sqrt{2}}$ |00> $+ \frac{1}{\sqrt{2}}$ |11>

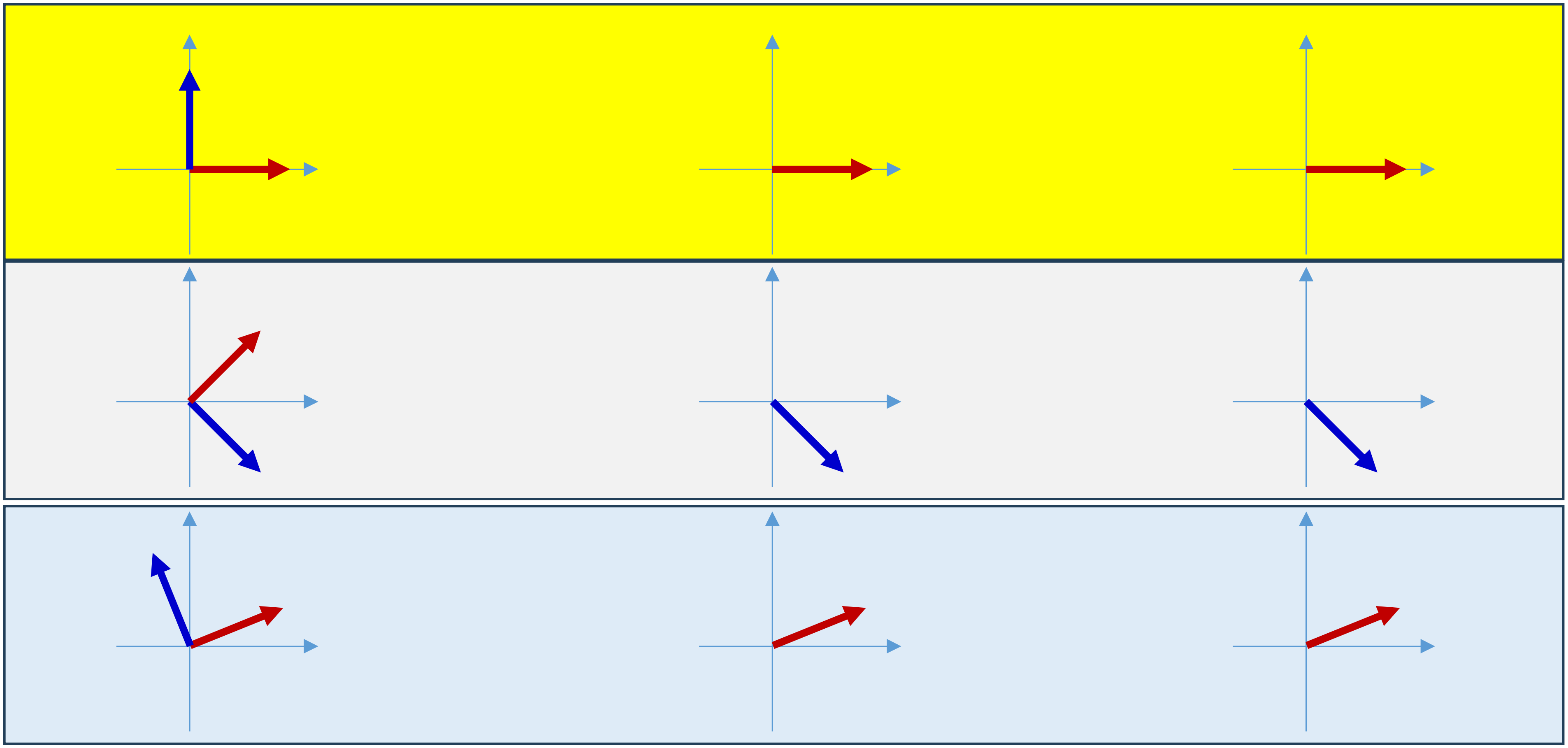
- Regardless of what bases Alice uses to measure her qubit, whatever she measures her qubit as – Bob's qubit will collapse to that same phasor!!!

The BELL state

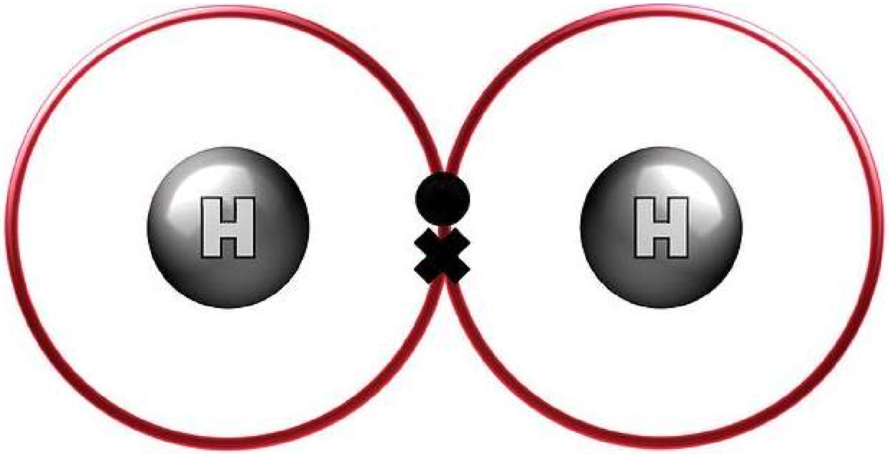


- $|\psi\rangle = \frac{1}{\sqrt{2}}|00> + \frac{1}{\sqrt{2}}|11>$

- Alice uses
- Alice measures
- Bob’s qubit



The magic of the entangled gate



- The Hydrogen molecule..
  - The two electrons will be in opposing spins
    - *Pauli's exclusion principle*
    - *Two fermions will never be in the same state*

- If you separate the two atoms, the electrons will remain in opposing spins, regardless of how far apart they're taken

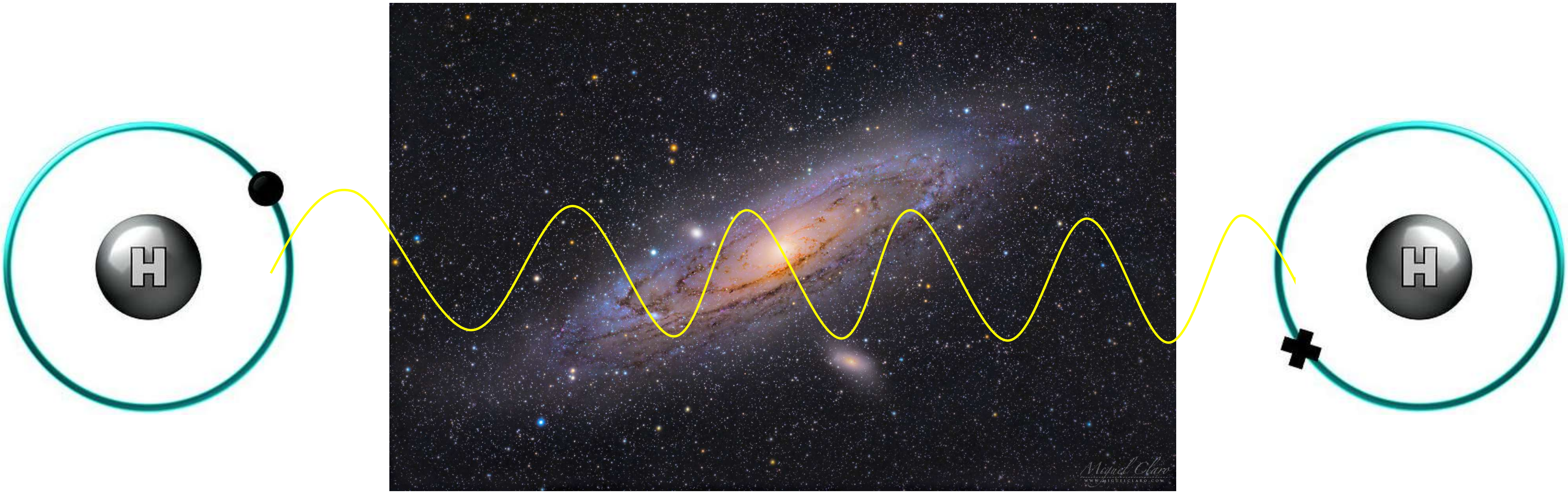
Random facts (from my friend Ramdas Menon)

“Everyone knows the great Austrian theoretical physicist Wolfgang Pauli, who won the Nobel Prize in Physics in 1945 (at the age of 45) for the eponymous Exclusion principle.

What very few people know is that there was a German physicist by name Wolfgang Paul who ALSO won the Nobel Prize in Physics in 1989 at the tender age of 76.

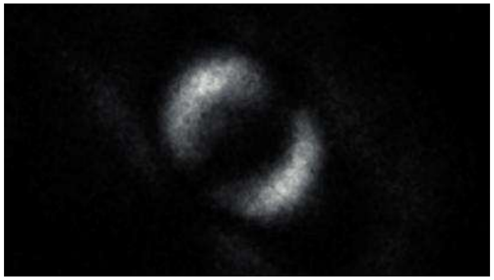
What still fewer people know is that the latter used to refer to the former as his "imaginary part"; nope, I ain't explaining this one.”

Spooky action at a distance…



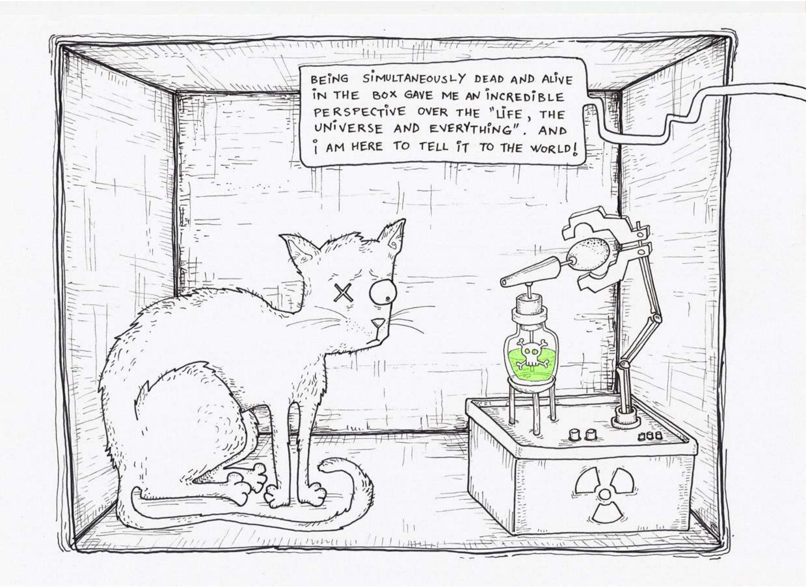
- Separate the entangled atoms by the width of the universe and they stay entangled:

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



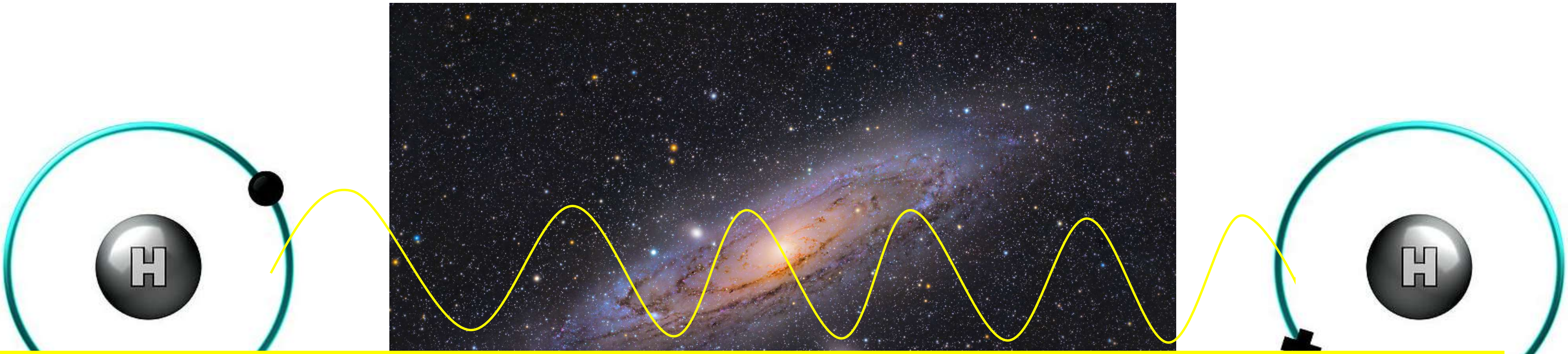
- Measure one and the other changes *instantly!*
  - *Spooky action at a distance!*

God does not play dice!


BEING SIMULTANEOUSLY DEAD AND ALIVE IN THE BOX GAVE ME AN INCREDIBLE PERSPECTIVE OVER THE "LIFE, THE UNIVERSE AND EVERYTHING". AND I AM HERE TO TELL IT TO THE WORLD!

- Einstein refused to believe in spooky action at a distance!
- So did Schrödinger
- But yeah…
  - The fact that the observer can choose their bases for measurement means that the entangled particles could not have pre-decided how they would come out
    - They would have to know a priori what bases they were going to be measured by, which they don't

Spooky action at a distance…

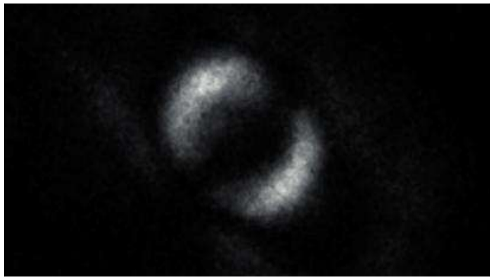


So does this mean we have found a way to communicate information instantaneously??

Faster than light!!!!!!!!!!!!!

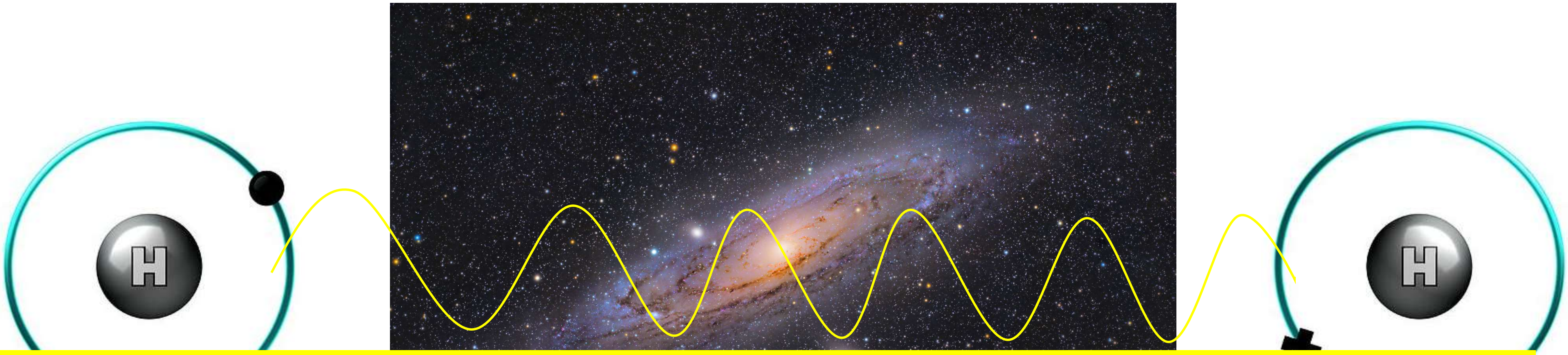
- Separate the atoms by the universe and they stay entangled:

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



- Measure one and the other changes *instantly!*
  - *Spooky action at a distance!*

Spooky action at a distance...



So does this mean we have found a way to communicate information instantaneously??
Faster than light!!!!!!!!!!!!!

If you think so, suggest how!

Can you suggest a communication protocol that uses entanglement to communicate faster than light?

- *Spooky action at a distance!*

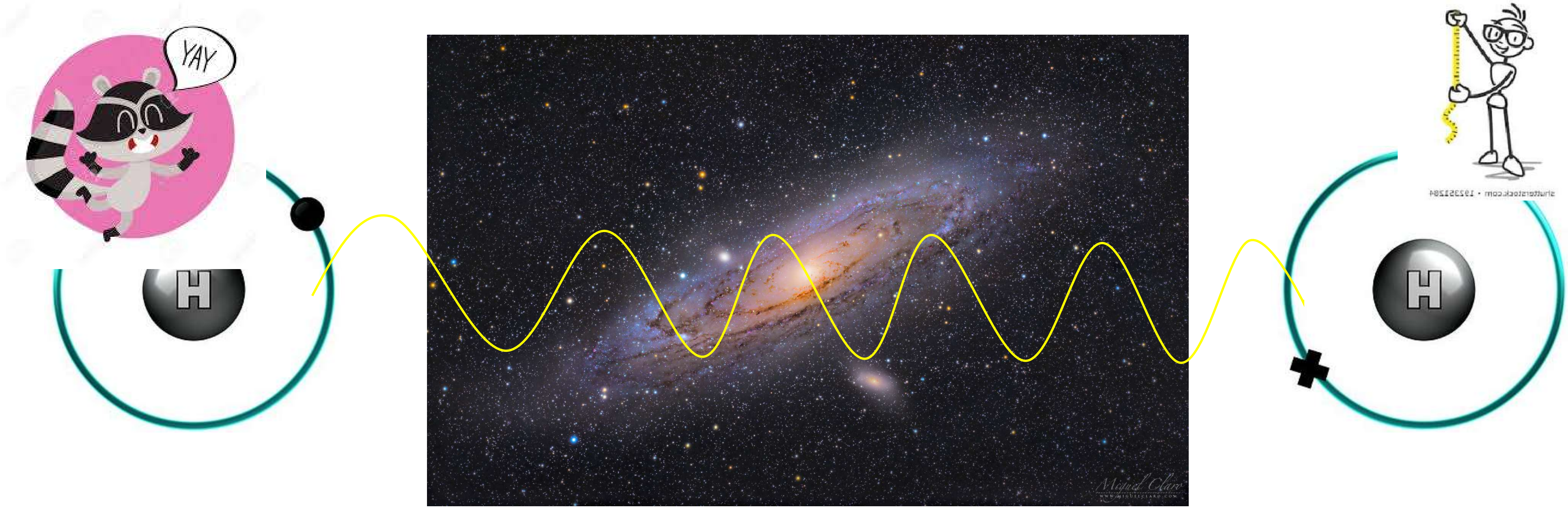
Poll 3

- Alice and Bob share a pair of entangled qubits in the Bell State. They live on opposite sides of the universe. Alice flips a coin and it turns up heads. Can she communicate this information to Bob
  - ○ No, faster-than-light communication of information is impossible
  - ○ No, not with today’s technology, but perhaps in the future we will invent a mechanism to do so using the entangled qubits
  - ○ Yes; Alice can measure her qubit and the state of her qubit will be the same as Bob’s. She can use this to communicate the information

Poll 3

- Alice and Bob share a pair of entangled qubits in the Bell State. They live on opposite sides of the universe. Alice flips a coin and it turns up heads. Can she communicate this information to Bob
  - ○ **No, faster-than-light communication of information is impossible**
  - ○ No, not with today's technology, but perhaps in the future we will invent a mechanism to do so using the entangled qubits
  - ○ Yes; Alice can measure her qubit and the state of her qubit will be the same as Bob's. She can use this to communicate the information

Information cannot travel faster than light: *No signaling theorem*

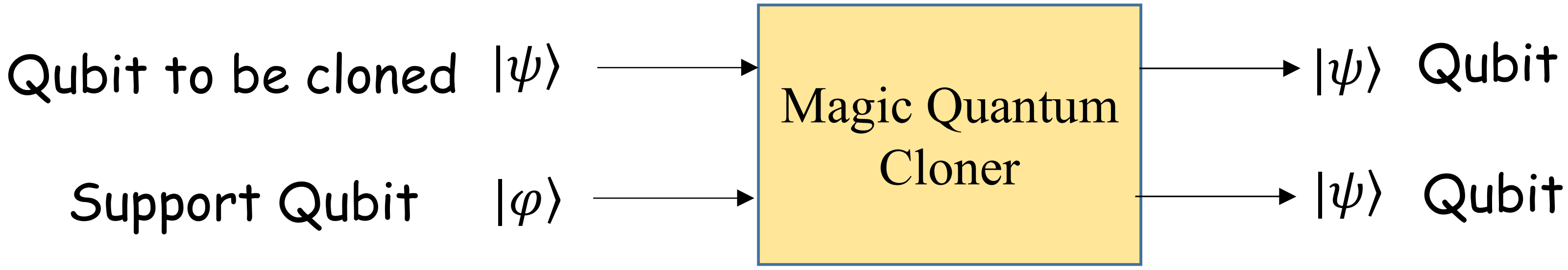


- Bob may be able to know exactly what Alice measured, Alice still cannot control what she measures
    - Its random
- So, there’s no way of letting Bob know “I have a 1”
    - But can we still use this somehow to communicate information?
        - Only it won’t be faster than light, but still…

Recap: The no cloning theorem

- You cannot clone a qubit
  - Given an *unknown* qubit, you cannot simply make 2 independent copies of it

- A) qubits aren’t just manufactured from thin air. So, to clone a qubit, you need the following system

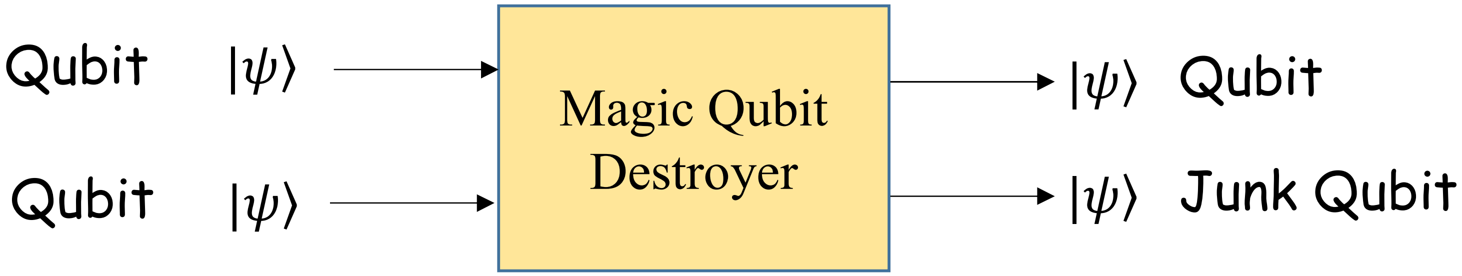

Qubit to be cloned $|\psi\rangle$
Support Qubit $|\varphi\rangle$
Magic Quantum Cloner
$|\psi\rangle$ Qubit
$|\psi\rangle$ Qubit

- Quantum systems are always invertible
  - Prove that you can’t clone a qubit

Consequence: No deleting theorem

- Given two identical qubits you cannot delete one of them
  - Deletion → destroying the information in one of them

- A system that does this:



Qubit $|\psi\rangle$

Qubit $|\psi\rangle$

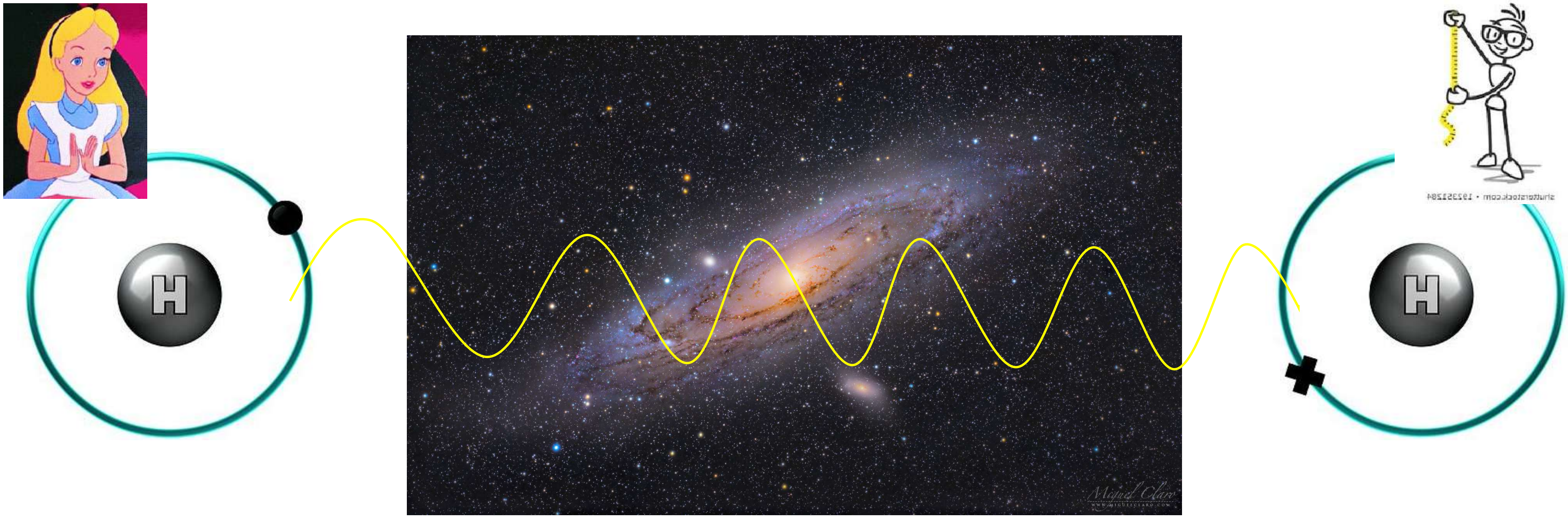
Magic Qubit Destroyer

$|\psi\rangle$ Qubit

$|\psi\rangle$ Junk Qubit

- This cannot exist
  - Prove it

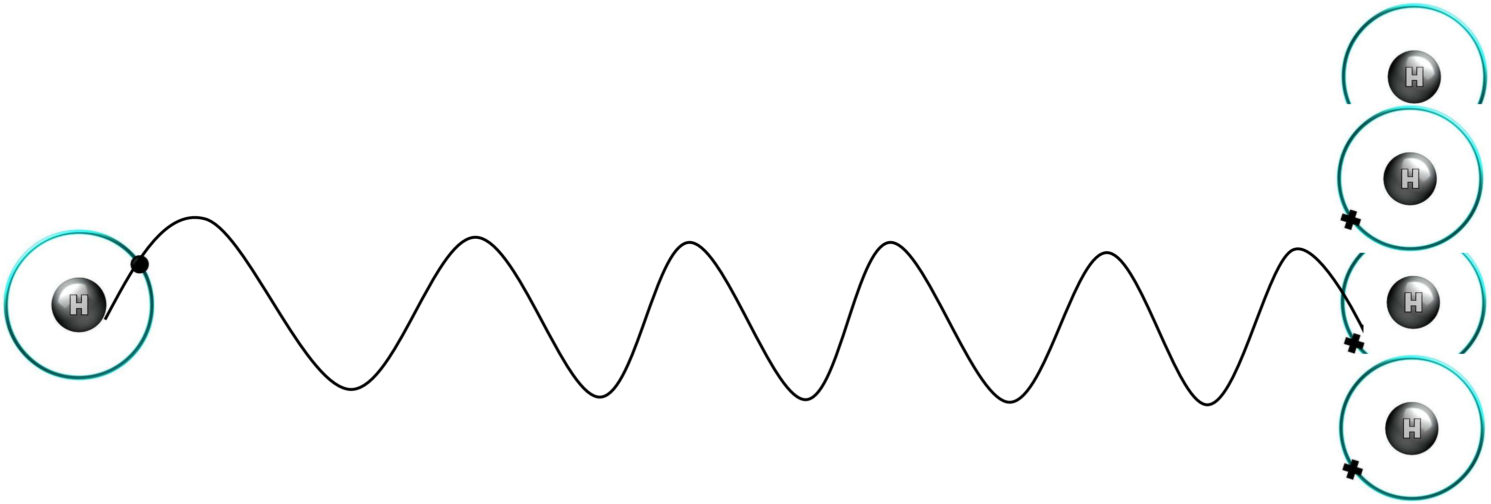
The no communication theorem



- Entangled qubits may collapse to the same state when measured, but this cannot be used to actively communicate a bit
  - The “No Communication Theorem” : You cannot use entanglement to instantly signal new information beyond the state of the qubit itself

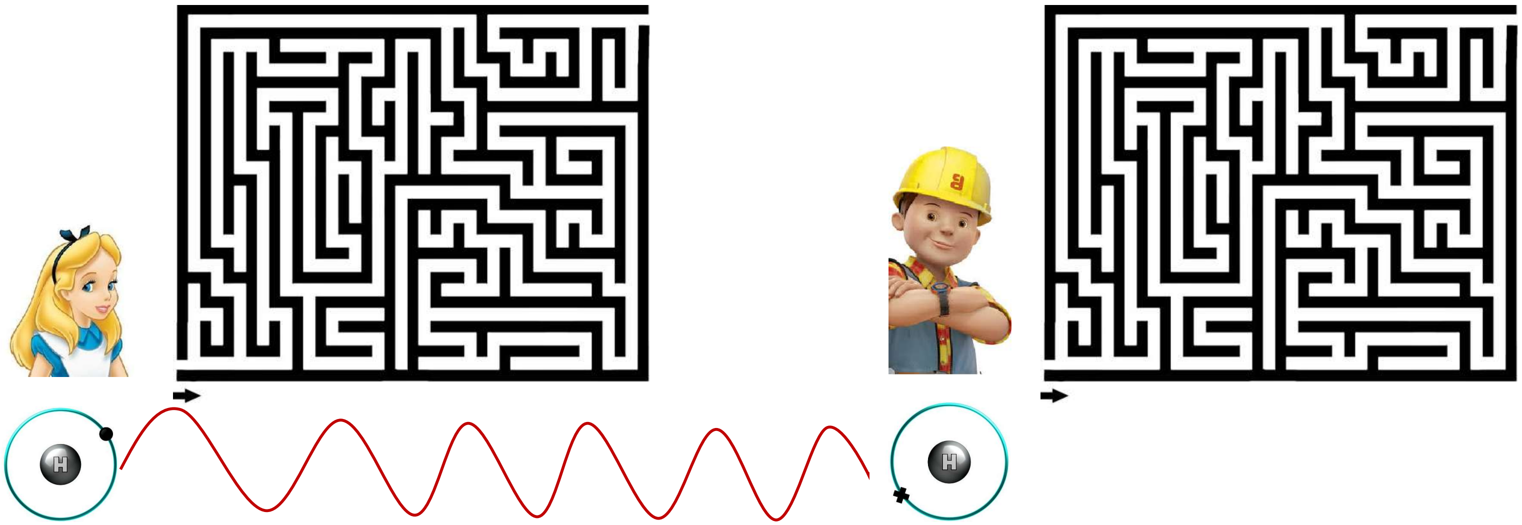
- There is *no protocol* that enables Alice to communicate *any* information to Bob

The no communication theorem



- Needs / implies the no-cloning theorem
  - Cheat protocol: To communicate her bit, Alice measures her entangled qubit if she has a 1, and doesn’t measure it if she has a 0
  - Bob clones his qubit 1million times and measures them.
  - If all are same, Alice got a 1 else she got a 0

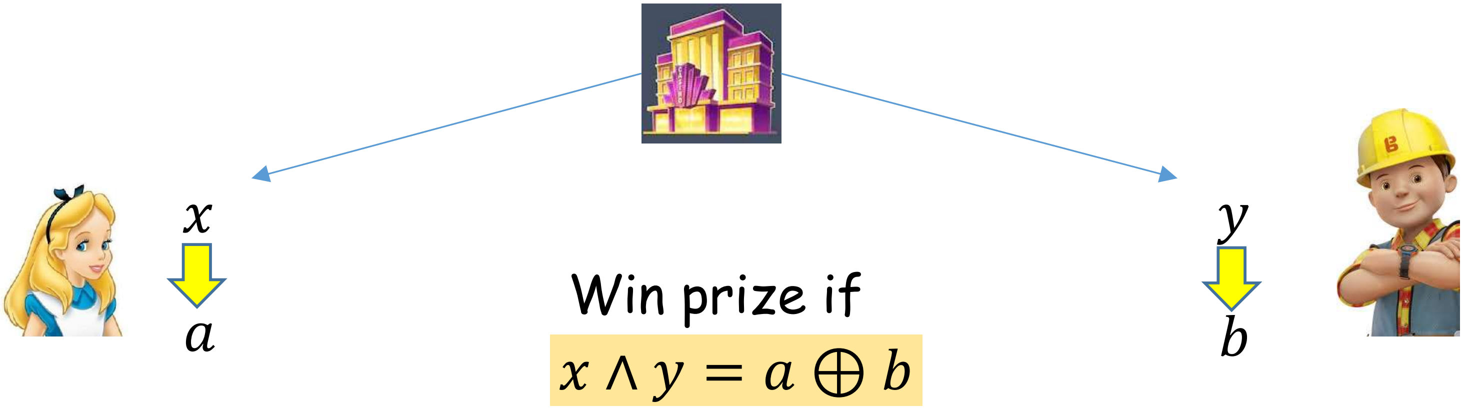
But Alice and Bob *can use entangled bits to coordinate!*



- Entanglement cannot be used for *communication,* but can be used for coordination
  - E.g. Alice and Bob have the same maze
  - They can decide: if we see a 0, go straight/right, else turn/go left
  - They can guarantee synchronized paths, but the final destination is random

- They have created *non-local* correlations
  - Without being able to predict the expected outcome
  - Can we use this somehow?

The CHSH game



x

a

Win prize if

$x \wedge y = a \oplus b$

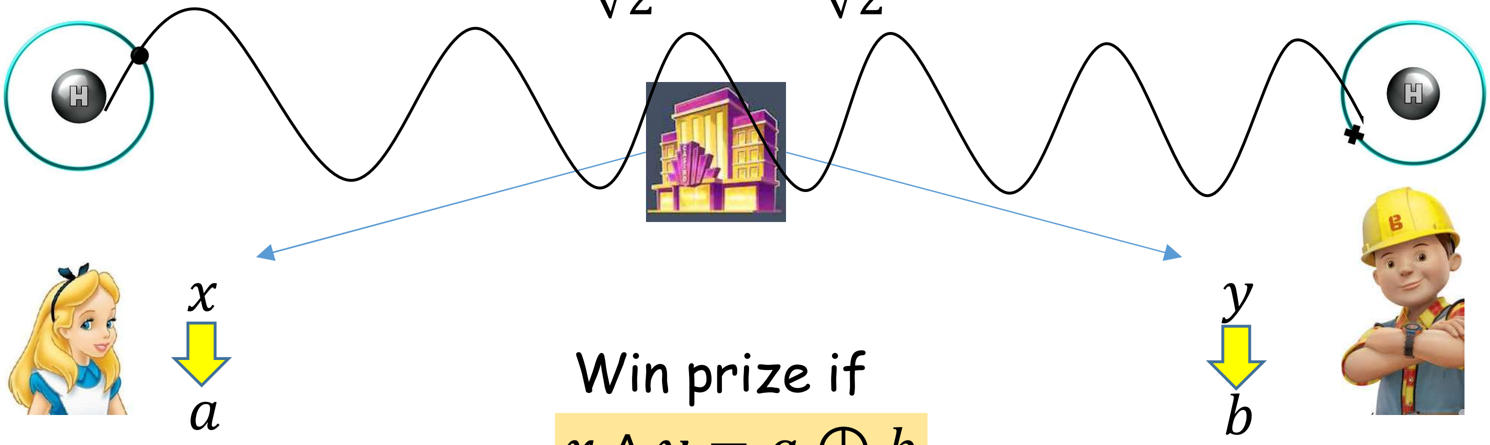
y

b

- Alice and Bob live in separate cities and may not communicate
- The casino sends each of them a random bit
  - Need not be identical
- They must inspect their bit and output a value
  - Alice outputs a, Bob outputs b
- They get a prize of $1.00 if:
  - Both got “1” from the casino and their outputs are such that $a \neq b$
  - Any other condition ([0,1], [1,0], [0,0]) they must output $a == b$
- What is the best strategy, and what is their expected earning?

The CHSH game with a qubit

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

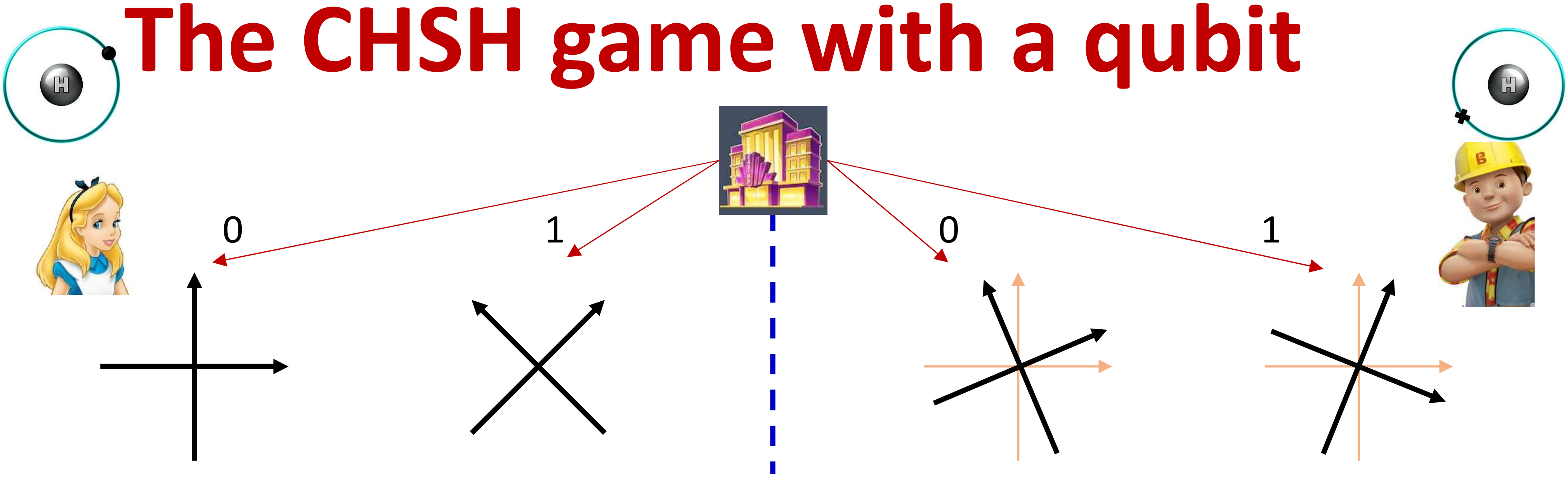


Win prize if

$x \wedge y = a \oplus b$

- Before moving to separate cities, Alice and Bob split a pair of entangled bits in the Bell State
- Now what is their best strategy?

The CHSH game with a qubit



- Alice uses two sets of bases for measurement: 0/1 and +/- (at 45°)
  - If Alice gets a 0 from the casino she measures using 0/1 and outputs the value
  - Else she measures using +/- and outputs the value
- Bob uses two sets of bases: at $\left[\frac{\pi}{8}, \frac{5\pi}{8}\right]$ and $\left[\frac{-\pi}{8}, \frac{3\pi}{8}\right]$
  - If Bob gets a 0 from the casino, he measures using $\left[\frac{\pi}{8}, \frac{5\pi}{8}\right]$ and outputs the value
  - Else he measures using the $\left[\frac{-\pi}{8}, \frac{3\pi}{8}\right]$ and outputs the value

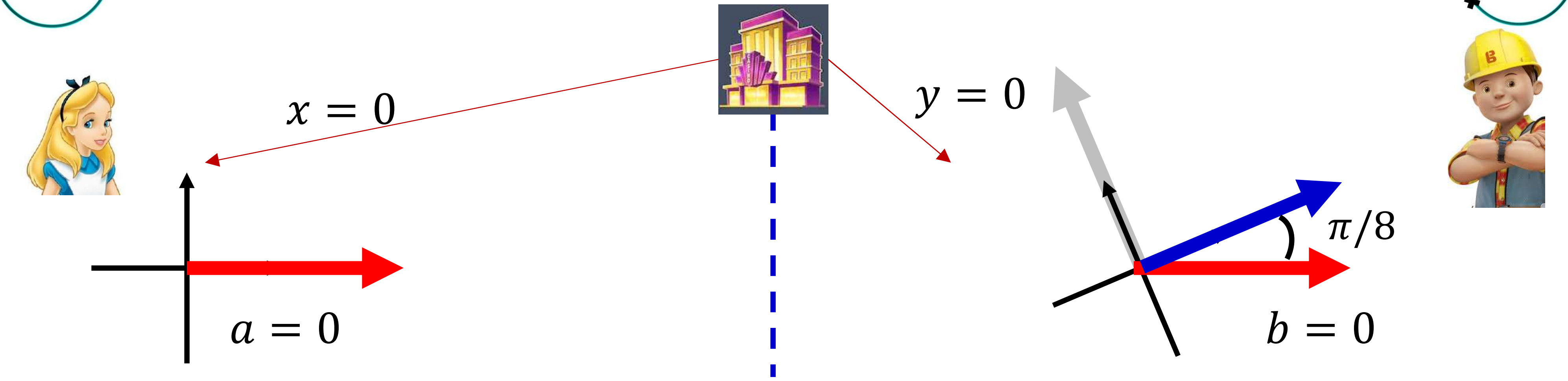
Poll 4

- Alice and Bob both get 0 from the casino. By their protocol, Alice uses bit bases to measure her qubit, while bob uses the $\left[\frac{\pi}{8}, \frac{5\pi}{8}\right]$ bases. Alice measures her qubit with bit bases and measures it as a 0. What is Bob's qubit at this point?
  - The state |0>, since it is entangled with Alice.
  - The phasor at pi/8, since Bob maps 0 to pi/8 and his qubit is entangled with Alice
  - We can't really say because they are using different bases

Poll 4

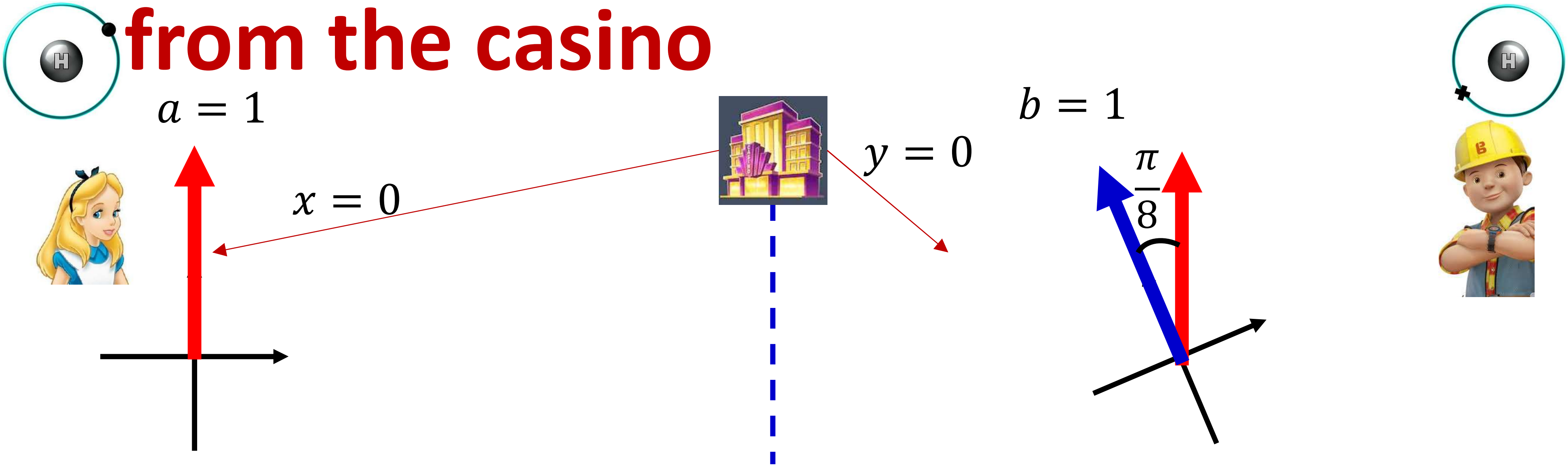
- Alice and Bob both get 0 from the casino. By their protocol, Alice uses bit bases to measure her qubit, while bob uses the $\left[\frac{\pi}{8}, \frac{5\pi}{8}\right]$ bases. Alice measures her qubit with bit bases and measures it as a 0. What is Bob's qubit at this point?
  - **The state|0>, since it is entangled with Alice.**
  - The phasor at pi/8, since Bob maps 0 to pi/8 and his qubit is entangled with Alice
  - We can't really say because they are using different bases

Case 1: Alice and Bob both get 0 from the casino



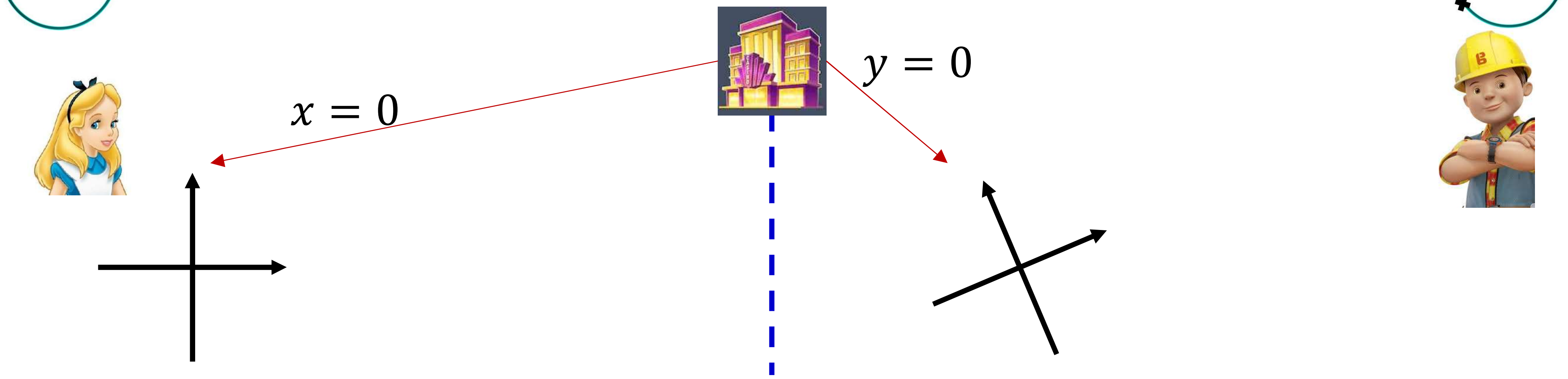
- If Alice measures first using the 0/1 bases and gets a 0
  - **Bob's qubit is also 0 due to entanglement**
  - Bob must also output a 0 to get money by the rules
- **Bob measures using the $\left[\frac{\pi}{8}, \frac{5\pi}{8}\right]$ bases**
  - He gets a 0 with probability $cos^2\frac{\pi}{8}$
  - This is $P(bob = alice|a = 0, x = 0, y = 0)$, i. e probability that Bob's output agrees with Alice, when $x = 0, y = 0$ and Alice outputs $a = 0$

Case 1: Alice and Bob both get 0 from the casino



- If Alice measures first using the 0/1 bases and gets a 1
  - **Bob’s qubit is also 1 due to entanglement**
  - Bob must also output a 1 to get money by the rules
- **Bob measures using the** $\left[\frac{\pi}{8}, \frac{5\pi}{8}\right]$ **bases**
  - He gets a 1 with probability $cos^2\frac{\pi}{8}$
  - This is $P(bob = alice|a = 1, x = 0, y = 0)$, i. e probability that Bob’s output agrees with Alice, when $x = 0, y = 0$ and Alice outputs $a = 1$

Case 1: Alice and Bob both get 0 from the casino



- Probability of agreement when $x = 0, y = 0$

$$E[x = 0, y = 0] =$$

This represents P(Alice=Bob|x=0,y=0)

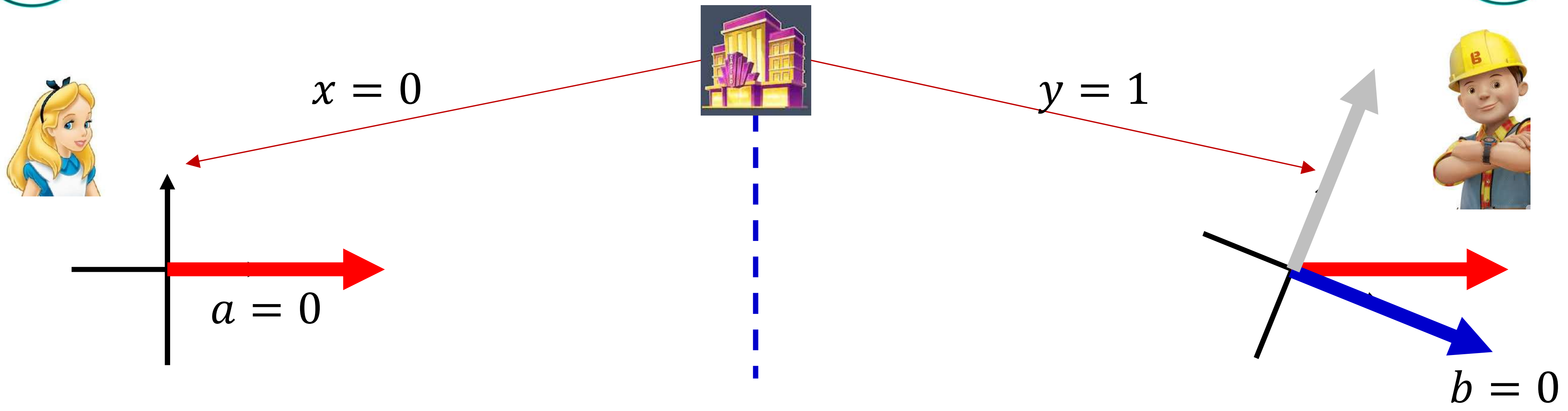
$$P(bob = alice|a = 0, x = 0, y = 0)P(a = 0|x = 0, y = 0)$$
$$+ P(bob = alice|a = 1, x = 0, y = 0)P(a = 1|x = 0, y = 0)$$
$$= P(a = 0|x = 0, y = 0)cos^2\frac{\pi}{8} + P(a = 1|x = 0, y = 0)cos^2\frac{\pi}{8}$$

i.e.

$$E[x = 0, y = 0] = cos^2\frac{\pi}{8}$$

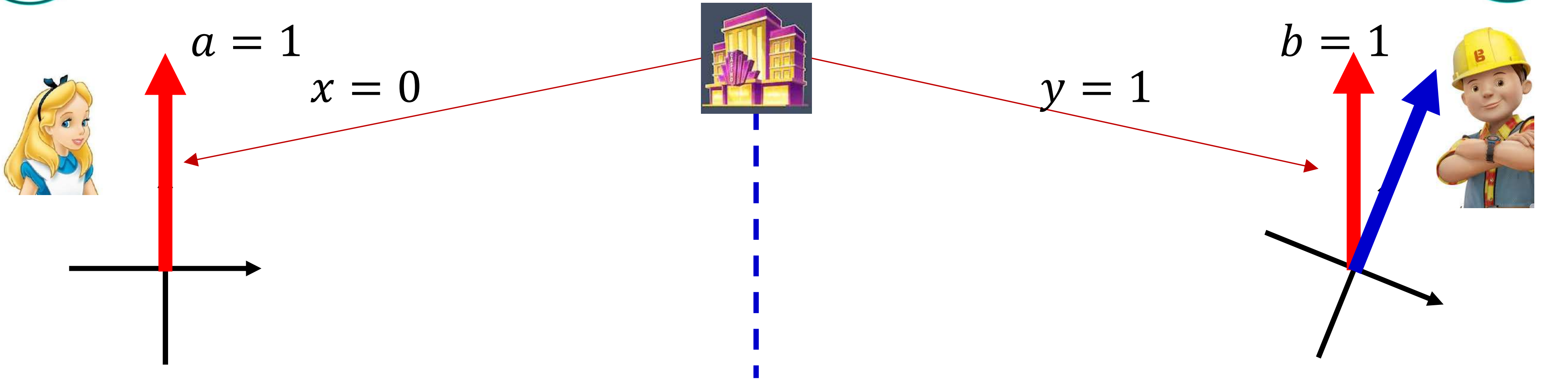
- Expected income when $x = 0, y = 0$ is $\$1 \times E[x = 0, y = 0] = cos^2\frac{\pi}{8}$

Case 2: Alice gets 0 and Bob gets 1 from the casino



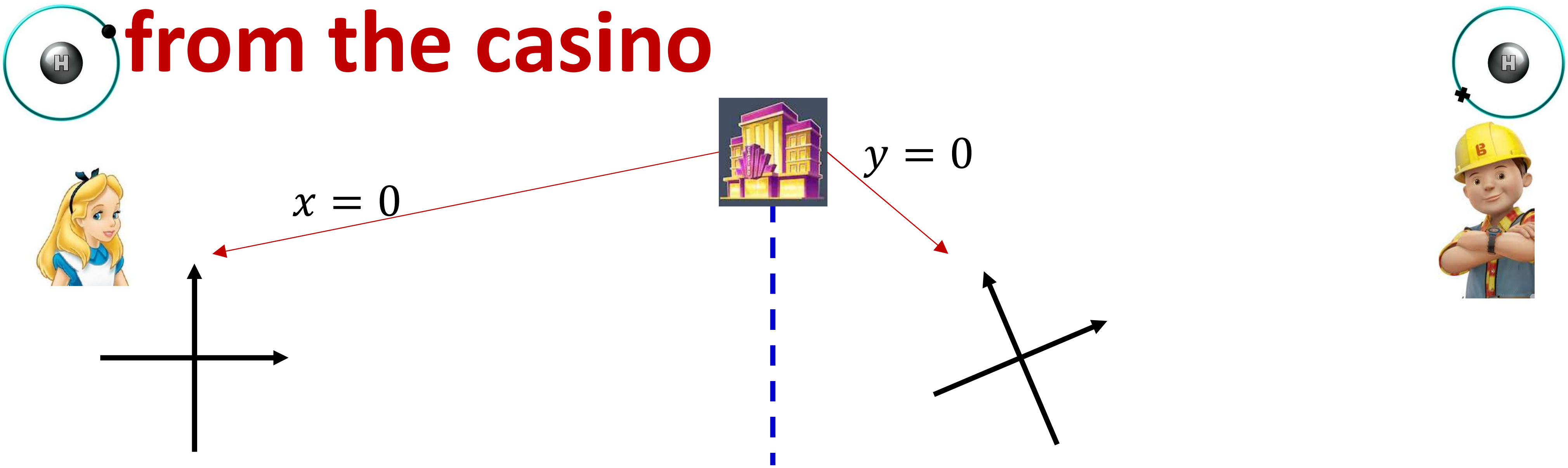
- If Alice measures first using the 0/1 bases and gets a 0
  - **Bob's qubit is also 0 due to entanglement**
  - Bob must also output a 0 to get money by the rules
- **Bob measures using the $\left[\frac{-\pi}{8}, \frac{3\pi}{8}\right]$ bases**
  - He gets a 0 with probability $cos^2 \frac{\pi}{8}$
  - This is $P(bob = alice|a = 0, x = 0, y = 1)$, i. e probability that Bob's output agrees with Alice, when $x = 0, y = 1$ and Alice outputs $a = 0$

Case 2: Alice gets 0 and Bob gets 1 from the casino



- If Alice measures first using the 0/1 bases and gets a 1
    - **Bob's qubit is also 1 due to entanglement**
    - Bob must also output a 1 to get money by the rules
- **Bob measures using the $\left[\frac{-\pi}{8}, \frac{3\pi}{8}\right]$ bases**
    - He gets a 0 with probability $cos^2 \frac{\pi}{8}$
    - This is $P(bob = alice|a = 1, x = 0, y = 1)$, i. e probability that Bob's output agrees with Alice, when $x = 0, y = 1$ and Alice outputs $a = 1$

Case 2: Alice gets 0 and Bob gets 1 from the casino



- Probability of agreement when $x = 0, y = 1$

$$E[x = 0, y = 1] =$$

This represents P(Alice=Bob|x=0,y=1)

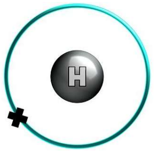
$$P(bob = alice|a = 0, x = 0, y = 1)P(a = 0|x = 0, y = 1)$$
$$+ P(bob = alice|a = 1, x = 0, y = 1)P(a = 1|x = 0, y = 1)$$
$$= P(a = 0|x = 0, y = 1)cos^2\frac{\pi}{8} + P(a = 1|x = 0, y = 1)cos^2\frac{\pi}{8}$$

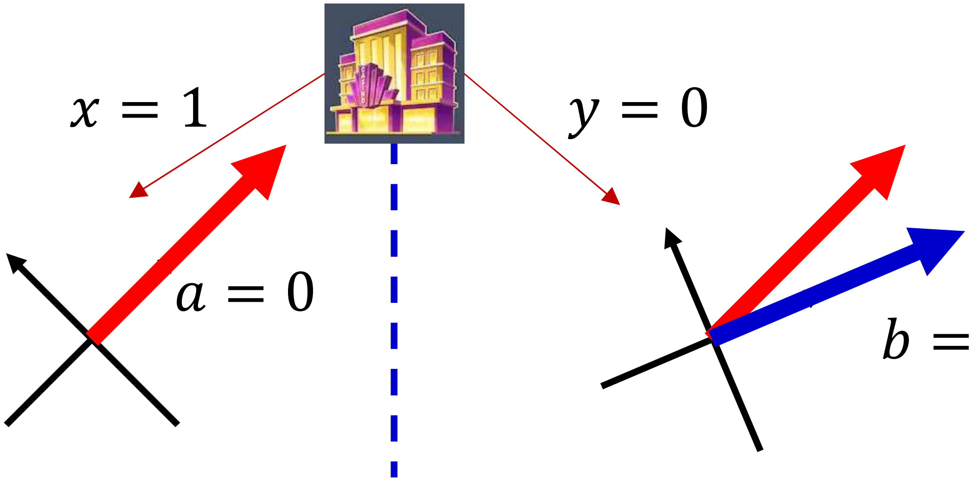
i.e.

$$E[x = 0, y = 1] = cos^2\frac{\pi}{8}$$

- Expected income when $x = 0, y = 1$ is $\$1 \times E[x = 0, y = 1] = cos^2\frac{\pi}{8}$

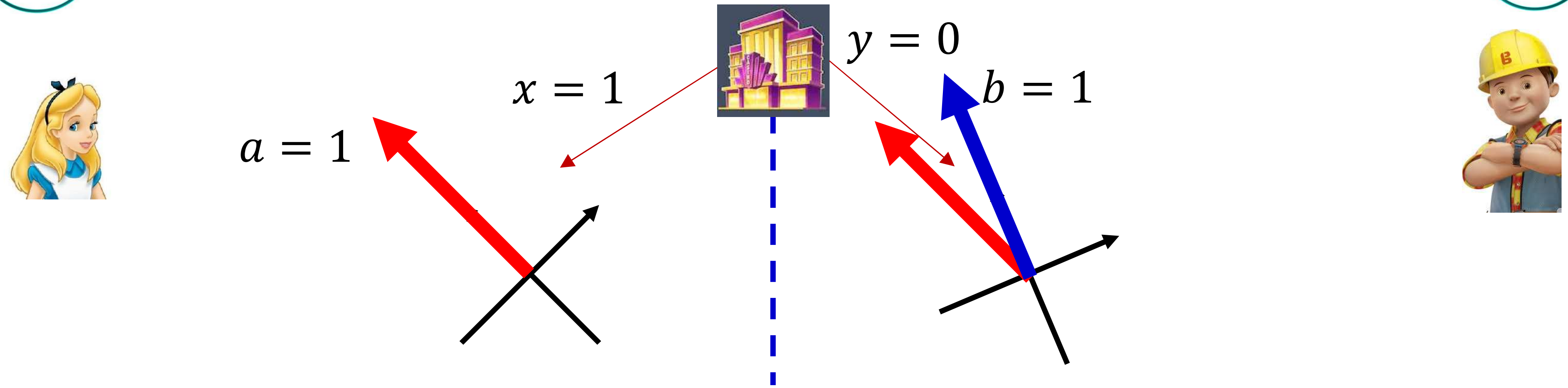
Case 3: Alice gets 1 and Bob gets 0 from the casino





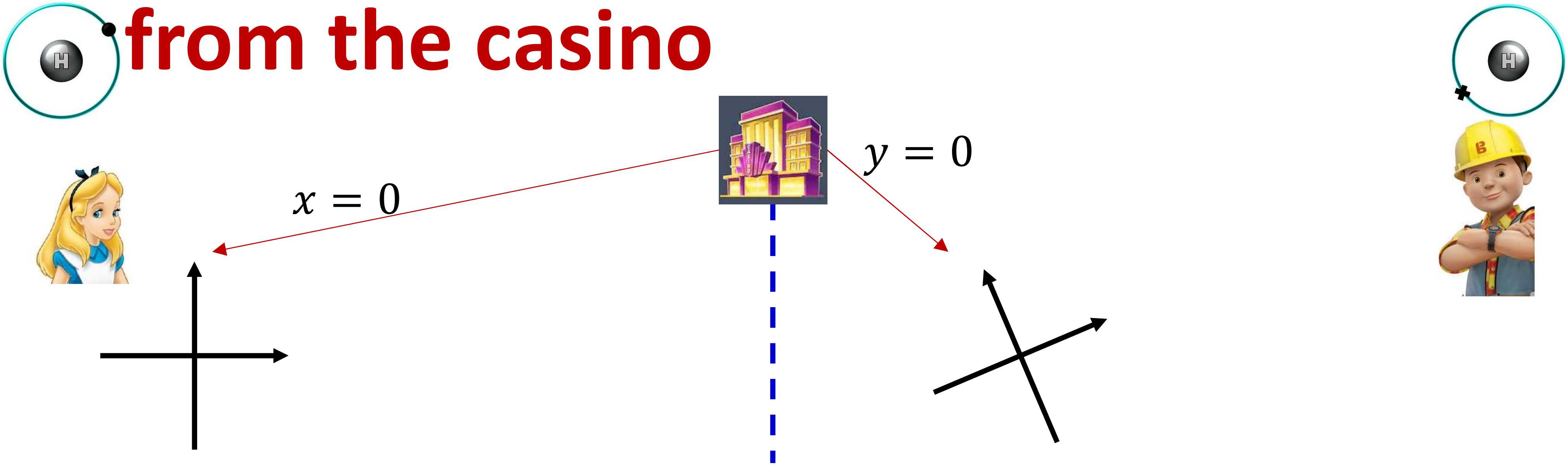
- If Alice measures first using the 0/1 bases and gets a 0
  - **Bob's qubit is also 0 due to entanglement**
  - Bob must also output a 0 to get money by the rules
- **Bob measures using the** $\left[\frac{\pi}{8}, \frac{5\pi}{8}\right]$ **bases**
  - He gets a 0 with probability $cos^2 \frac{\pi}{8}$
  - This is $P(bob = alice|a = 0, x = 1, y = 0)$, i. e probability that Bob's output agrees with Alice, when $x = 1, y = 0$ and Alice outputs $a = 1$

Case 3: Alice gets 1 and Bob gets 0 from the casino



- If Alice measures first using the 0/1 bases and gets a 1
  - **Bob's qubit is also 1 due to entanglement**
  - Bob must also output a 1 to get money by the rules
- **Bob measures using the** $\left[\frac{\pi}{8}, \frac{5\pi}{8}\right]$ **bases**
  - He gets a 1 with probability $cos^2\frac{\pi}{8}$
  - This is $P(bob = alice|a = 1, x = 1, y = 0)$, i. e probability that Bob's output agrees with Alice, when $x = 1, y = 0$ and Alice outputs $a = 1$

Case 3: Alice gets 1 and Bob gets 0 from the casino



- Probability of agreement when $x = 1, y = 0$

$$E[x = 1, y = 0] =$$

This represents P(Alice=Bob|x=1,y=0)

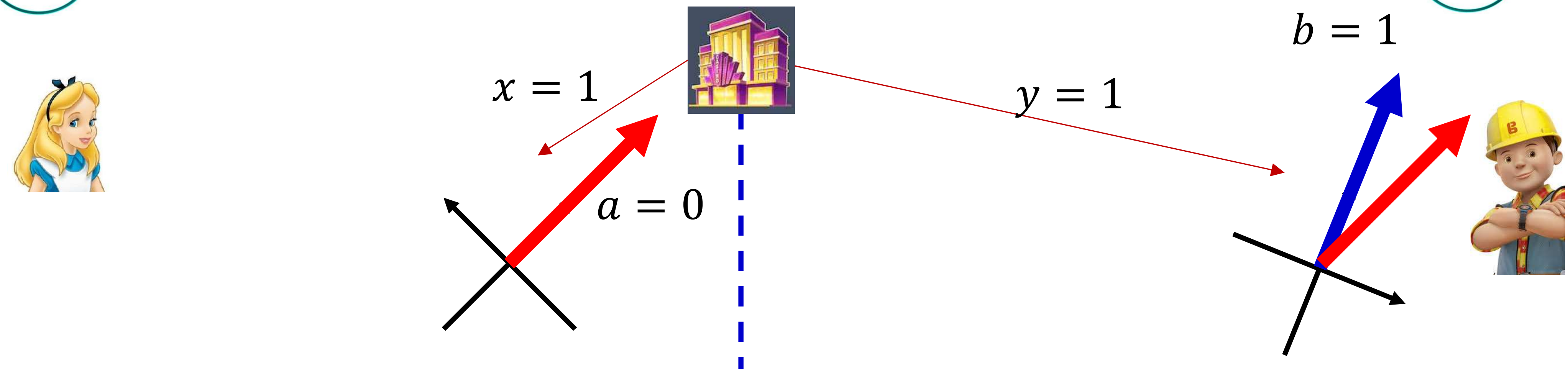
$$P(bob = alice|a = 0, x = 1, y = 0)P(a = 0|x = 1, y = 0)$$
$$+ P(bob = alice|a = 1, x = 1, y = 0)P(a = 1|x = 1, y = 0)$$
$$= P(a = 0|x = 1, y = 0)cos^2\frac{\pi}{8} + P(a = 1|x = 1, y = 0)cos^2\frac{\pi}{8}$$

i.e.

$$E[x = 1, y = 0] = cos^2\frac{\pi}{8}$$

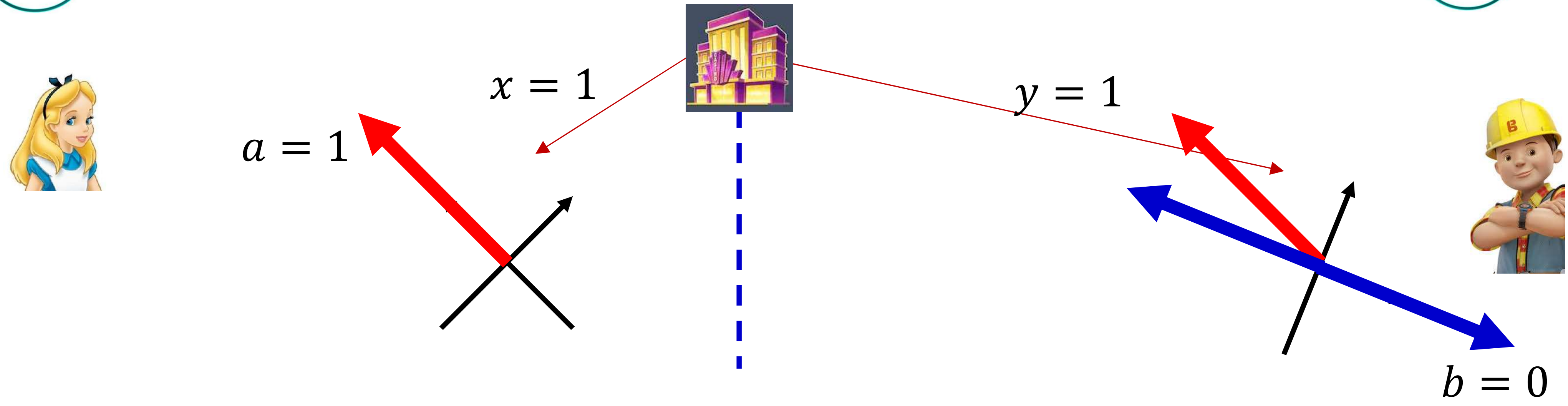
- Expected income when $x = 1, y = 0$ is $\$1 \times E[x = 1, y = 0] = cos^2\frac{\pi}{8}$

Case 4: Alice and Bob both get 1 from the casino



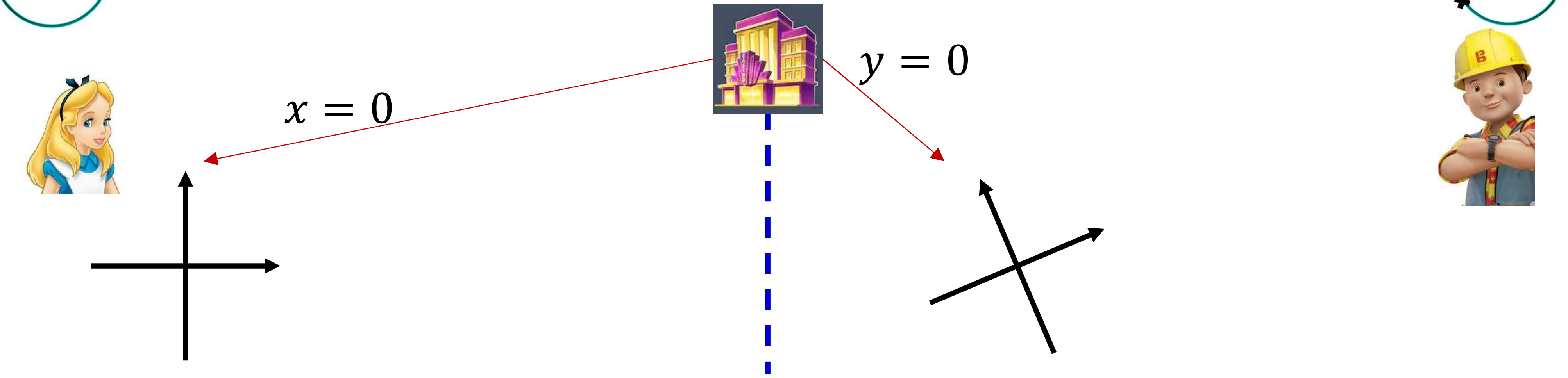
- If Alice measures first using the 0/1 bases and gets a 0
  - **Bob's qubit is also 0 due to entanglement**
  - Bob must now **output a 1** to get money by the rules
- **Bob measures using the** $\left[\frac{-\pi}{8}, \frac{3\pi}{8}\right]$ **bases**
  - He gets a 1 with probability $cos^2 \frac{\pi}{8}$
  - This is $P(bob \neq alice|a = 0, x = 1, y = 1)$, i. e probability that Bob's output ***disagrees*** with Alice, when $x = 1, y = 1$ and Alice outputs $a = 1$

Case 4: Alice and Bob both get 1 from the casino



- If Alice measures first using the 0/1 bases and gets a 1
  - **Bob's qubit is also 1 due to entanglement**
  - Bob must now **output a 0** to get money by the rules
- **Bob measures using the** $\left[\frac{-\pi}{8}, \frac{3\pi}{8}\right]$ **bases**
  - He gets a 0 with probability $cos^2\frac{\pi}{8}$
  - This is $P(bob \neq alice|a = 1, x = 1, y = 1)$, i. e probability that Bob's output ***disagrees*** with Alice, when $x = 1, y = 1$ and Alice outputs $a = 1$

Case 4: Alice and Bob both get 1 from the casino



- Probability of ***disagreement*** when $x = 1, y = 0$

$$D[x = 1, y = 0] =$$

This represents P(Alice!=Bob|x=1,y=1)

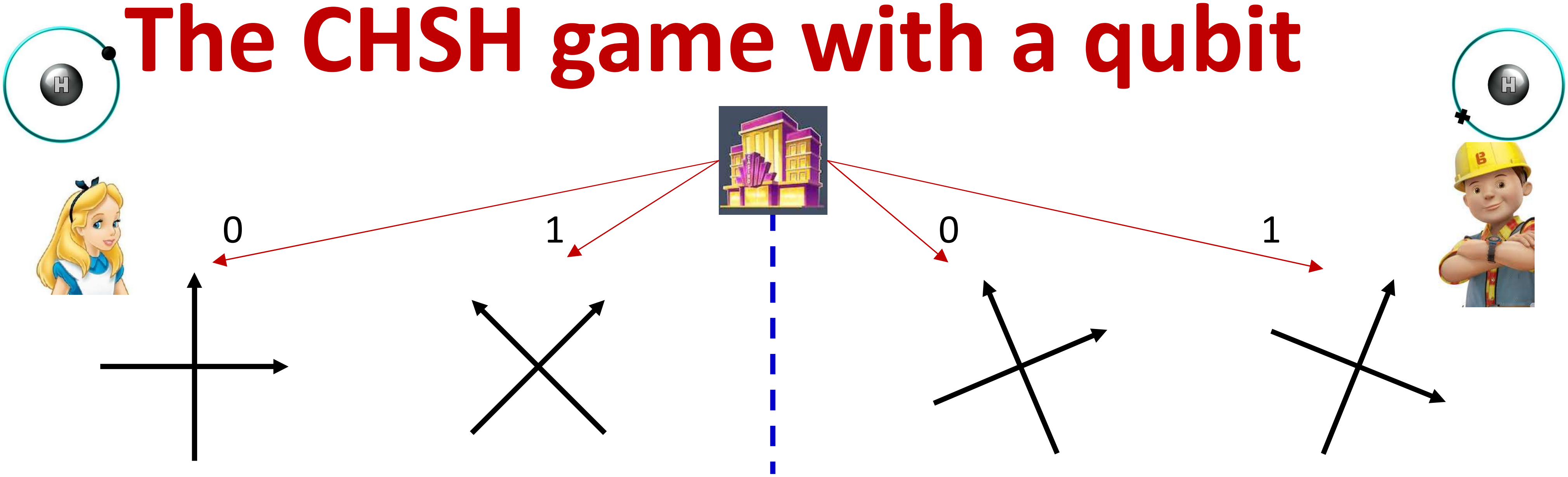
$$P(bob \neq alice | a = 0, x = 1, y = 1) P(a = 0 | x = 1, y = 1)$$
$$+ P(bob \neq alice | a = 1, x = 1, y = 1) P(a = 1 | x = 1, y = 1)$$
$$= P(a = 0 | x = 1, y = 1) cos^2 \frac{\pi}{8} + P(a = 1 | x = 1, y = 1) cos^2 \frac{\pi}{8}$$

i.e.

$$D[x = 1, y = 1] = cos^2 \frac{\pi}{8}$$

- Expected income when $x = 1, y = 1$ is $\$1 \times D[x = 1, y = 1] = cos^2 \frac{\pi}{8}$

The CHSH game with a qubit



- The overall expected gain using the strategy is

$$G = \sum_{x,y} P(x,y)G[x,y] = \sum_{x,y} P(x,y)cos^2\frac{\pi}{8} = cos^2\frac{\pi}{8}$$

- This is 0.85, which is greater than the best-case strategy with classical bits (0.75)

The CHSH game with a qubit

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

Win prize if

$$x \wedge y = a \oplus b$$

- Using entangled Qubits they got bigger returns
  - ***Without really exchanging information!***
- They created *non-local correlations,* which they exploited

The CHSH inequality

- The Clauser Horne Shimony Holt (1969):
- For classical computers

$$E[0,0] + E[0,1] + E[1,0] - E[1,1] \leq 2$$

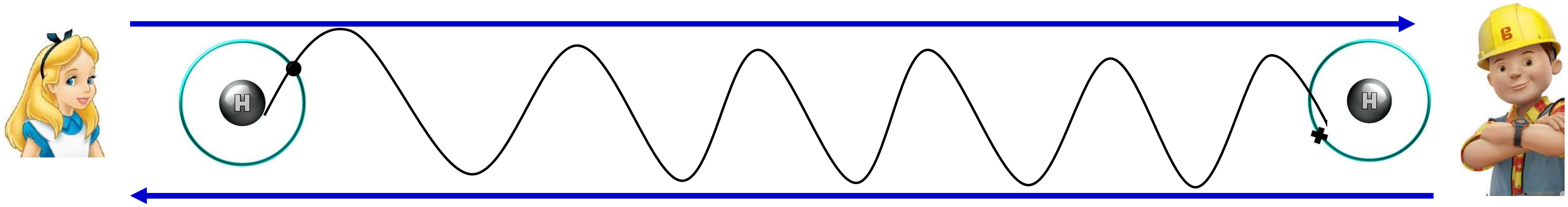
  - where $E[x, y]$ is the probability that Alice and Bob "agree" (i.e. $a = b$) when they receive x and y respectively
    - Note: The maximum possible value under perfect knowledge is 3. The closer you are to 3, the more money you make
- Using quantum entanglement

$$E[0,0] + E[0,1] + E[1,0] - E[1,1] \leq 2\sqrt{2}$$

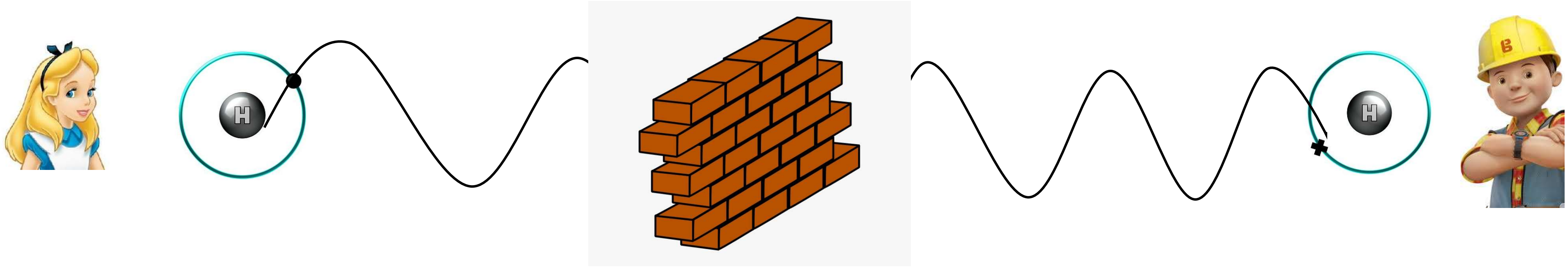
  - Regardless of the actual qubit shared
  - Over any policy / measurement strategy
  - This is 2.8, which is very close to the max possible value of 3

- Qubits, which are useless for communication, can still be used to create *correlations* which can be exploited
  - They can "enhance" asymmetries in the system

Difference between communication and correlation



- Communication : Alice and Bob send each other information over the quantum channel



- Correlation : Alice and Bob act locally upon entangled bits
  - They really have no way of knowing if the other is doing anything really
  - Nothing is being communicated

Lesson – you cannot communicate

- But you can correlate

- And correlation can be used for profit…