Quantum…

Computing

Lecture 3: Gates

© Can Stock Photo - csp16101833

Poll 1

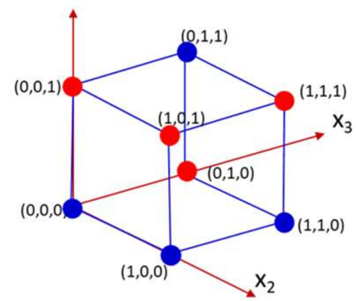
- In the old math, each bit is a coordinate direction. In the new math what are the new coordinate directions?
  - The bits
  - The qubit
  - The bit patterns

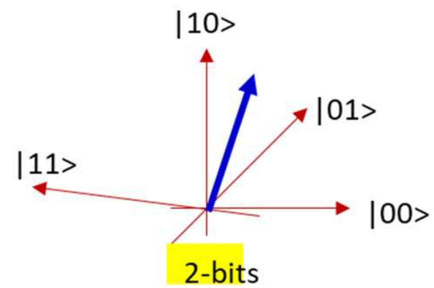
- In the new math what is true of functions (algorithms)
  - The are unrestricted
  - They must be invertible
  - They must be linear
  - They can change the length of the input

- Why does the old math work on classical computers, whereas the new math needs quantum computers
  - In classical computers a single register stores only one bit pattern
  - Storing a super position of all possible bit patterns will require an exponential number of registers on a classical computer
  - Quantum elements naturally exist in a superposition of state

Poll 1

- In the old math, each bit is a coordinate direction. In the new math what are the new coordinate directions?
  - The bits
  - The qubit
  - **The bit patterns**





- In the new math what is true of functions (algorithms)
  - The are unrestricted
  - **They must be invertible**
  - **They must be linear**
  - They can change the length of the input

- Why does the old math work on classical computers, whereas the new math needs quantum computers
  - **In classical computers a single register stores only one bit pattern**
  - **Storing a super position of all possible bit patterns will require an exponential number of registers on a classical computer**
  - **Quantum elements naturally exist in a superposition of state**

Poll 2

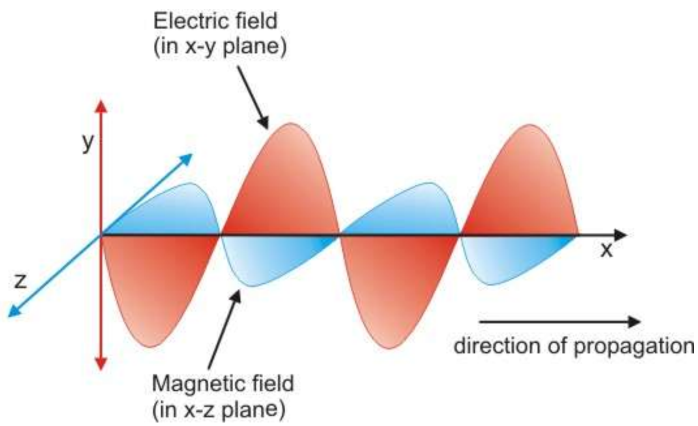
- What is this?
  - A green blob
  - One of Bhiksha's infinite states
  - Bhiksha, after an alien species briefly observed him while we were all simultaneously blinking, and we all opened our eyes again

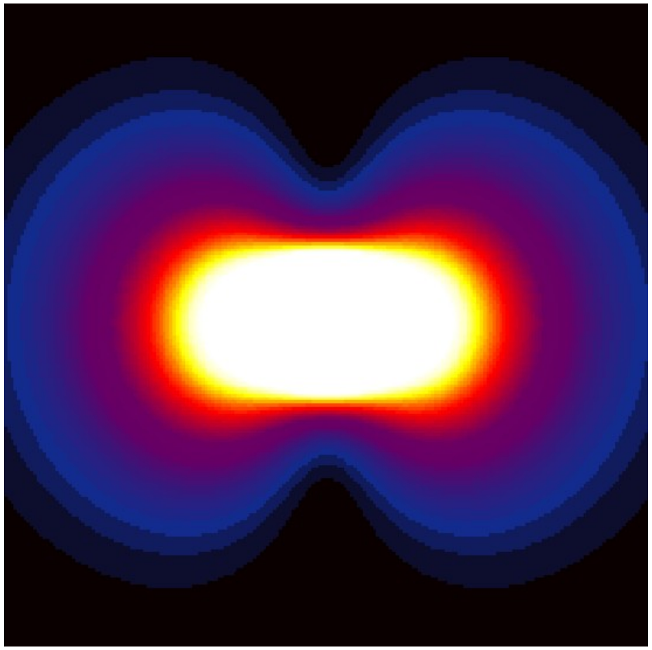
Poll 2

- What is this?
  - **A green blob**
  - **One of Bhiksha's infinite states**
  - **Bhiksha, after an alien species briefly observed him while we were all simultaneously blinking, and we all opened our eyes again**

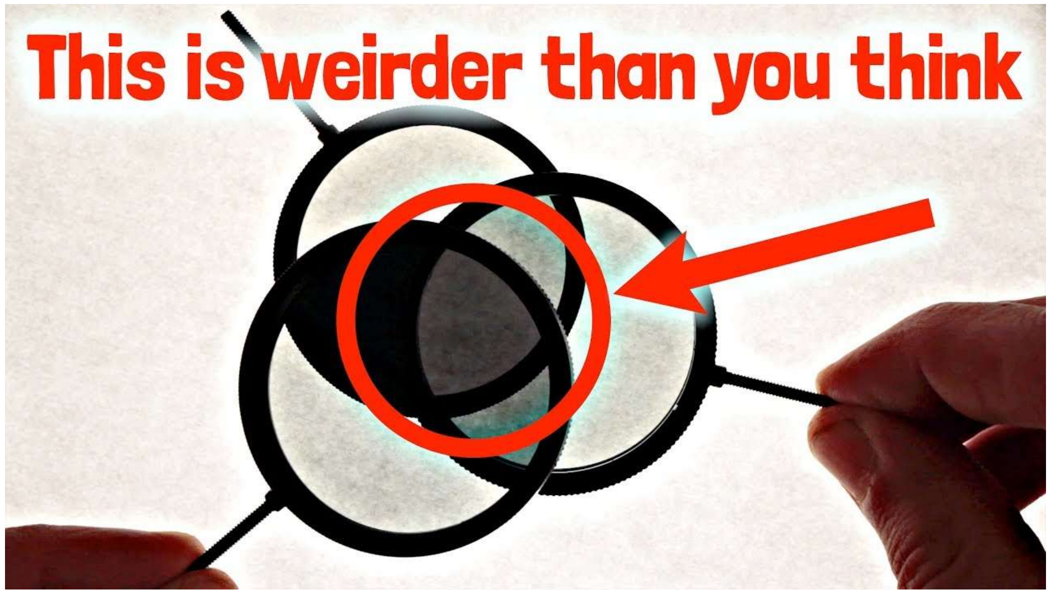
Quantum entities are in superposition?

- How do we know that these quantum entities are actually in superposition, and not probabilistically in one of the states?





The world isn't what you think it is!!!

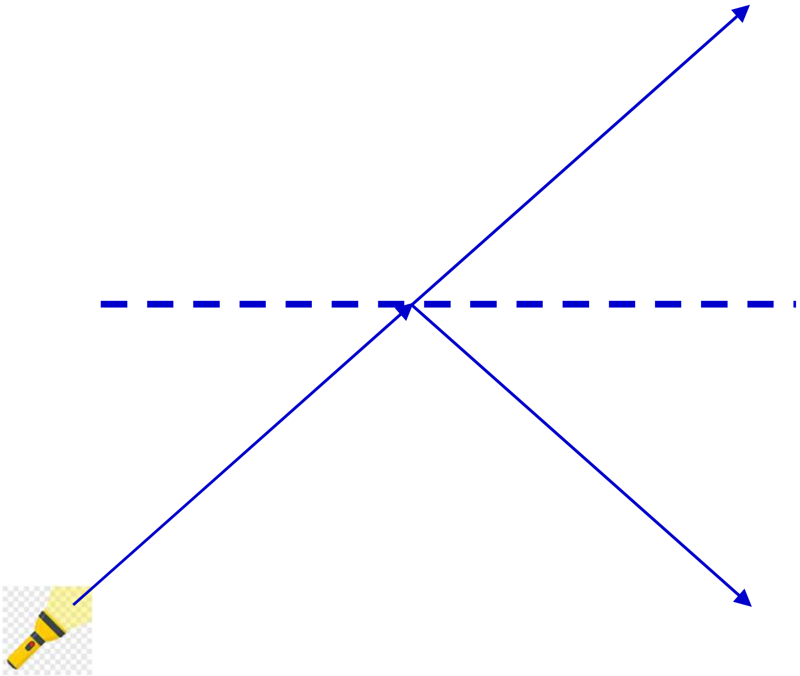


- Repeated measurements with different bases can completely alter reality!!!
  - Can you identify the horizontal and vertical polarized lenses in the picture?

Bombs and other things that go boom…

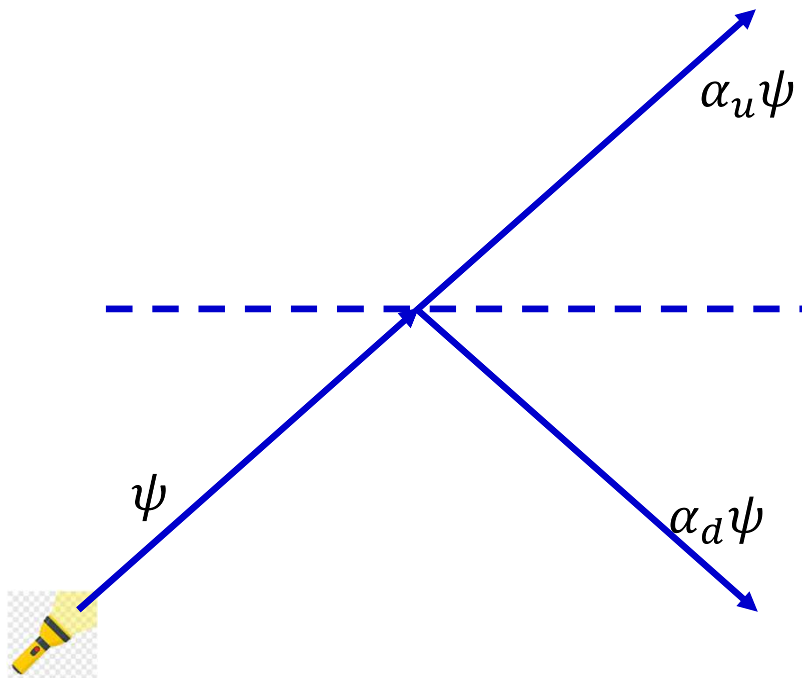
But first … beam splitters

Beam splitter



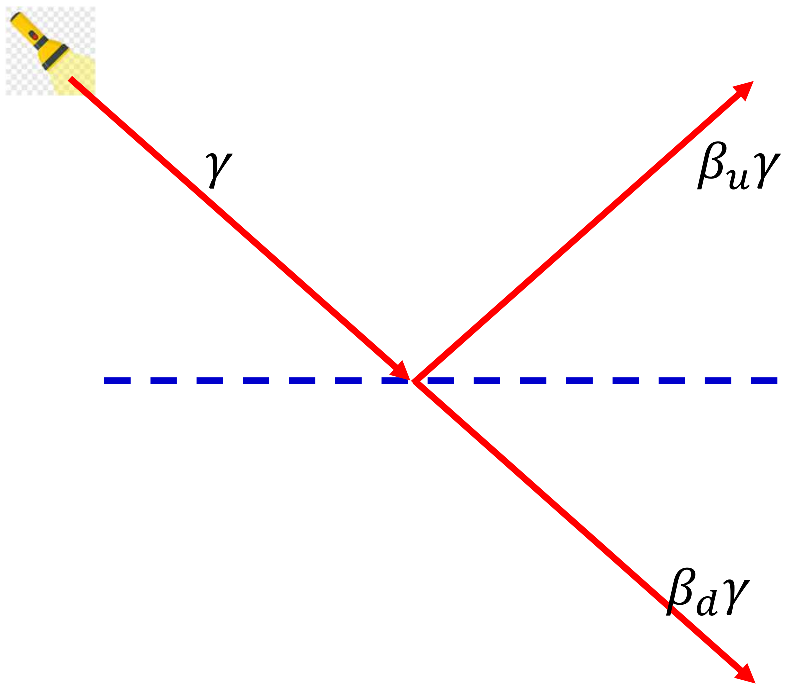
- What is a beam splitter?

Beam splitter



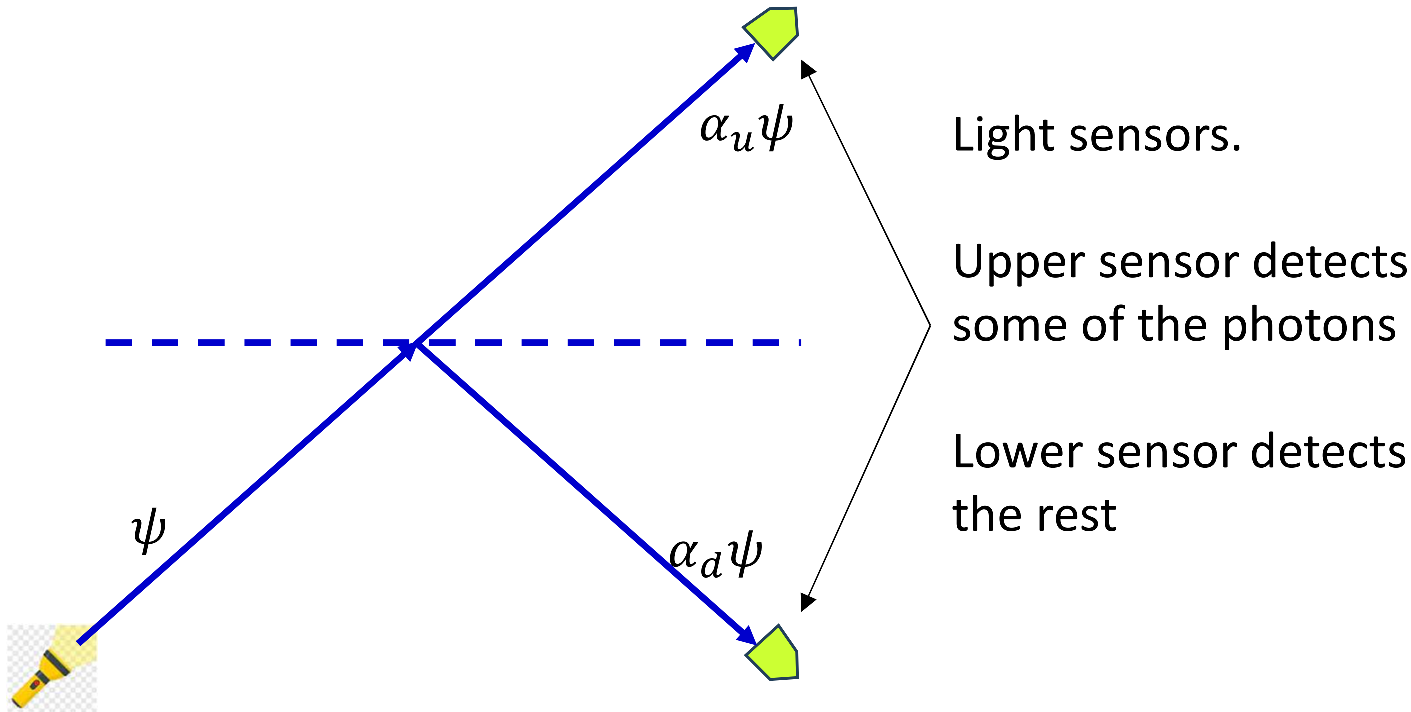
- What is a beam splitter?
  - Superposition or probabilistic distribution of photons?

Beam splitter



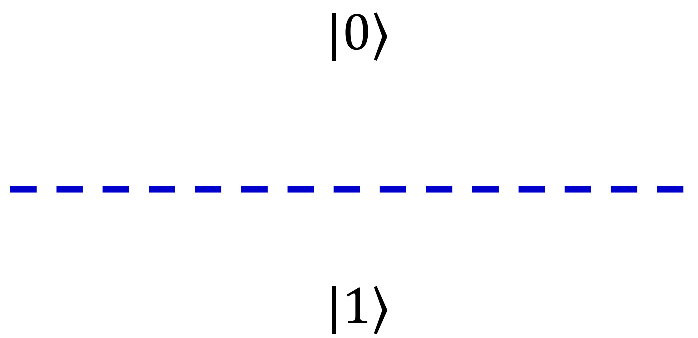
- What is a beam splitter?
  - Superposition or probabilistic distribution of photons?

Beam splitter



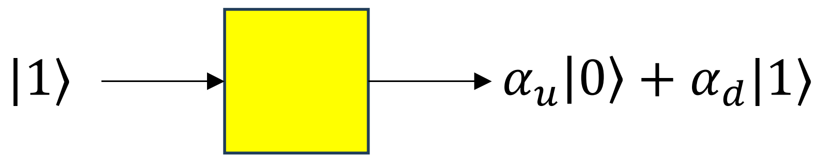
- The upper and lower beams are actually *superposed states* of the photon
  - But only a random one of the two senses the photon

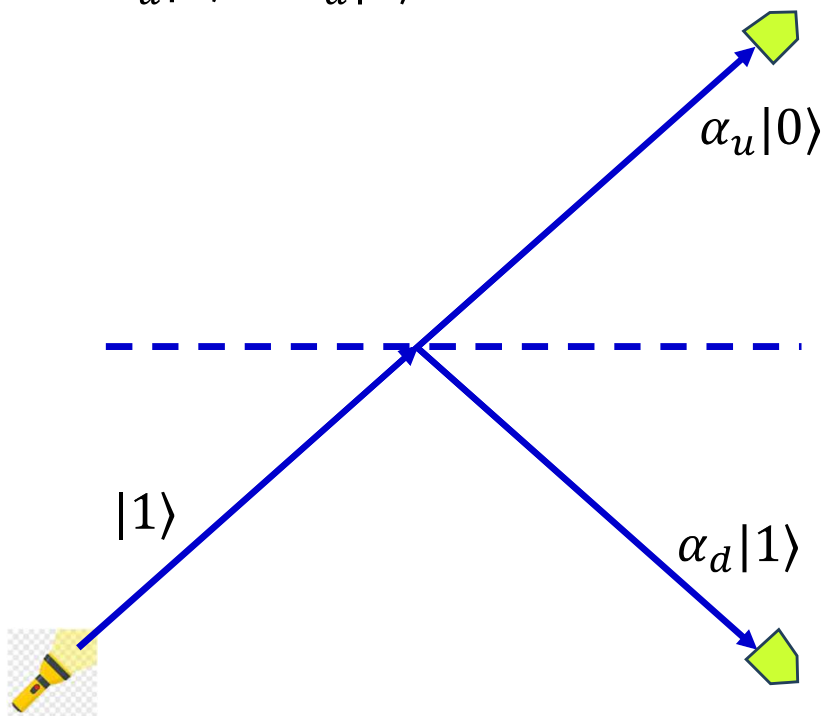
Beam splitter



- Denote everything above as $|0\rangle$ and everything below as $|1\rangle$

Beam splitter

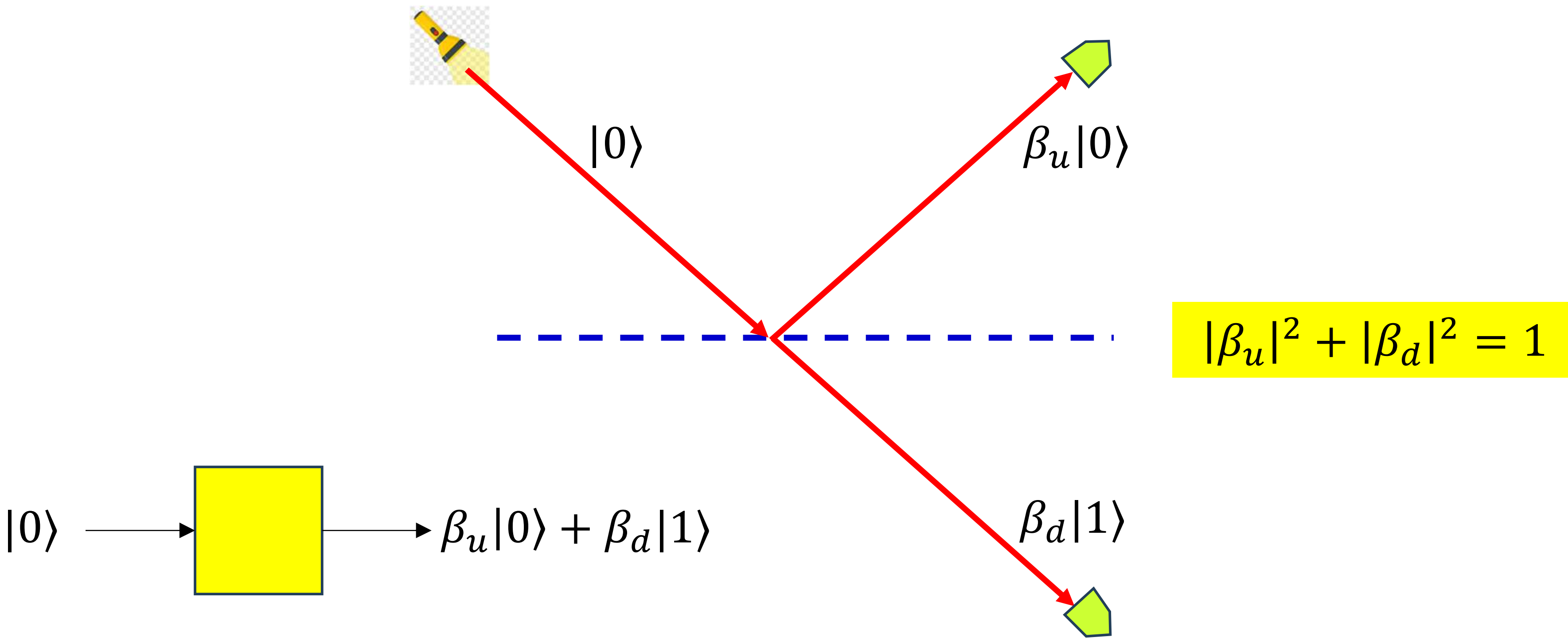




$$|\alpha_u|^2 + |\alpha_d|^2 = 1$$

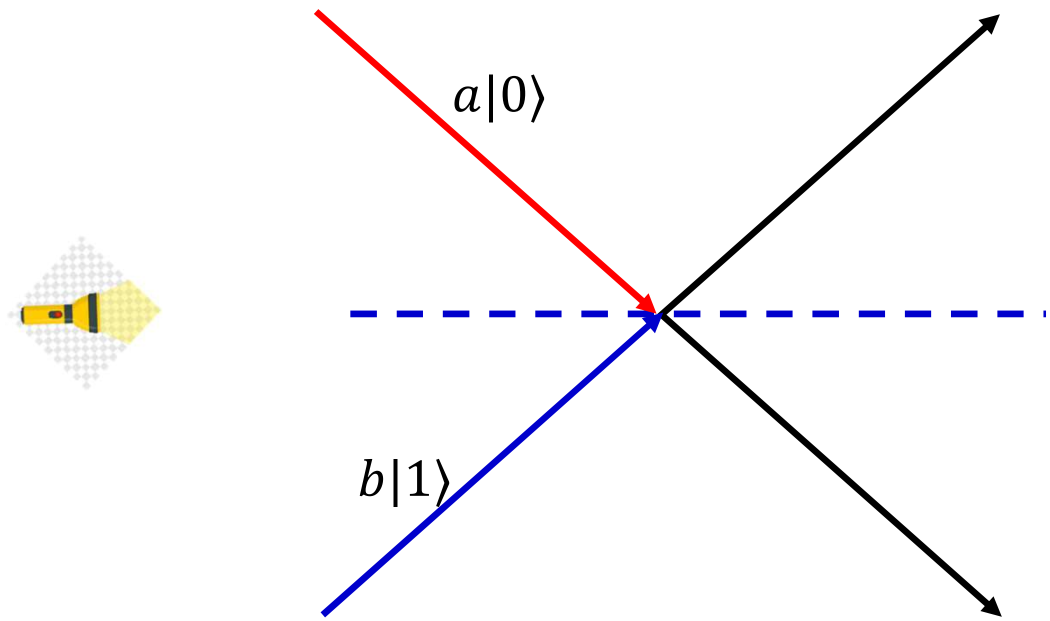
- If the input is from below
- With prob $|\alpha_u|^2$ the photon is sensed above, and with probability $|\alpha_d|^2$ it is sensed below

Beam splitter



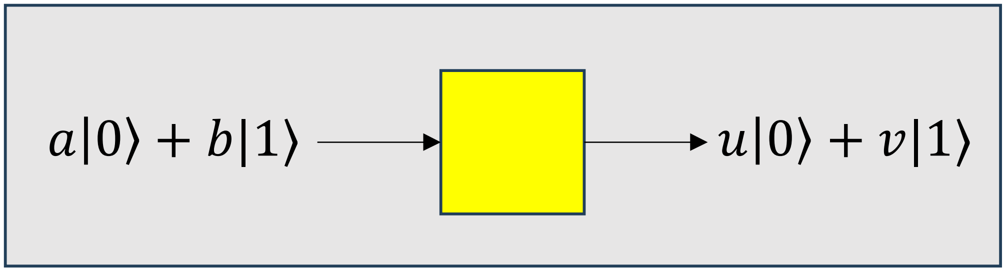
- If the input is from below
- With prob $|\beta_u|^2$ the photon is sensed above, and with probability $|\beta_d|^2$ it is sensed below

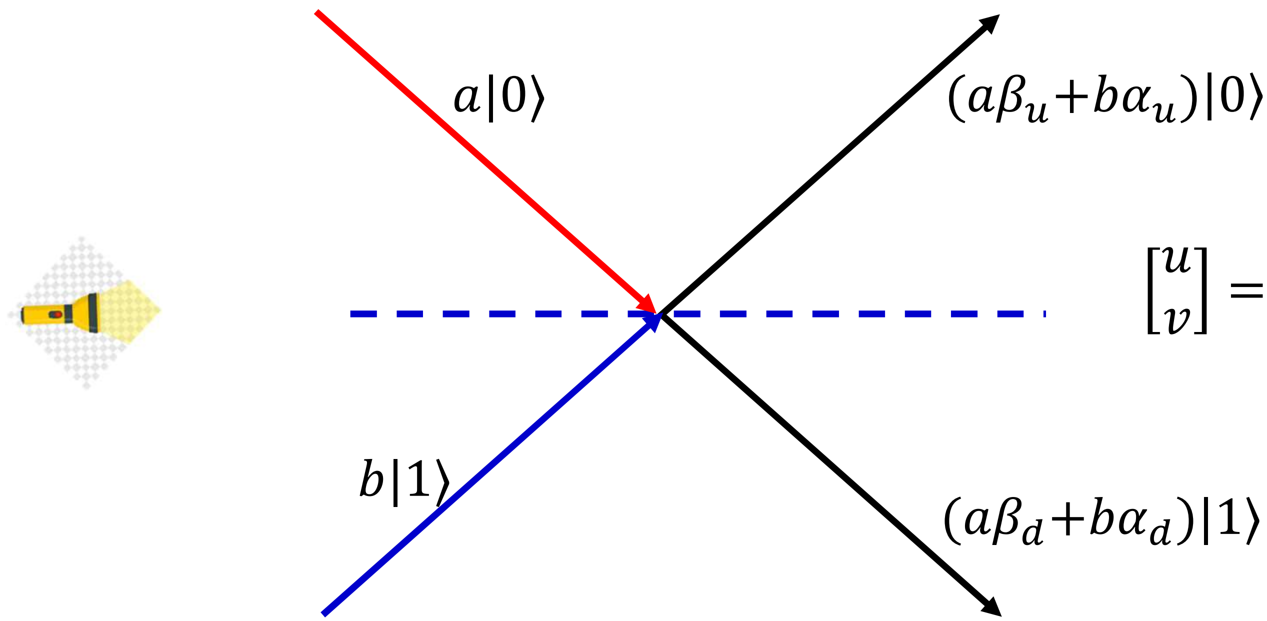
Beam splitter



- If we have a superposition of both?

Beam splitter

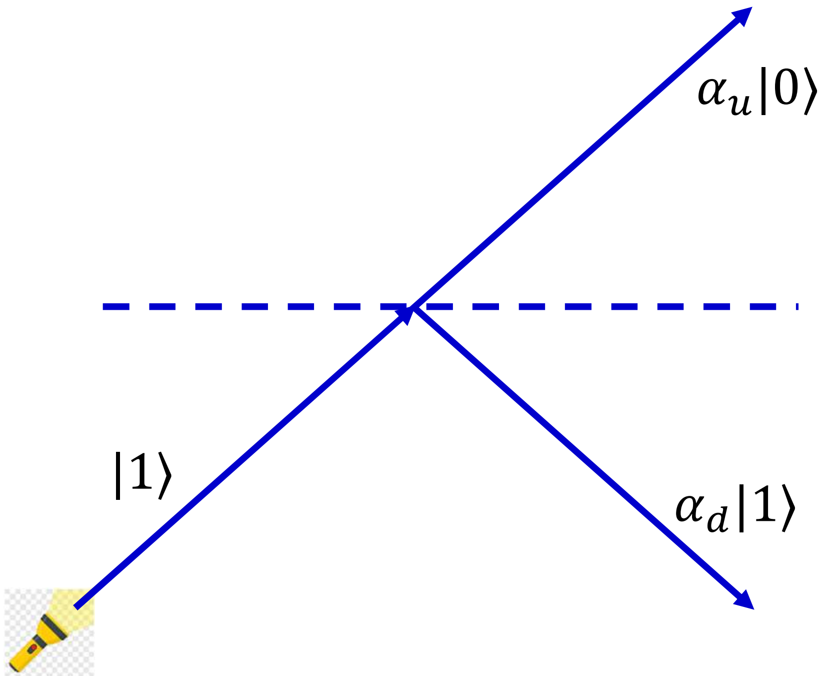




$$\begin{bmatrix} u \\ v \end{bmatrix} = \begin{bmatrix} \beta_u & \alpha_u \\ \beta_d & \alpha_d \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix}$$

- The beam splitter is a linear transform
  - Actually, a unitary transform

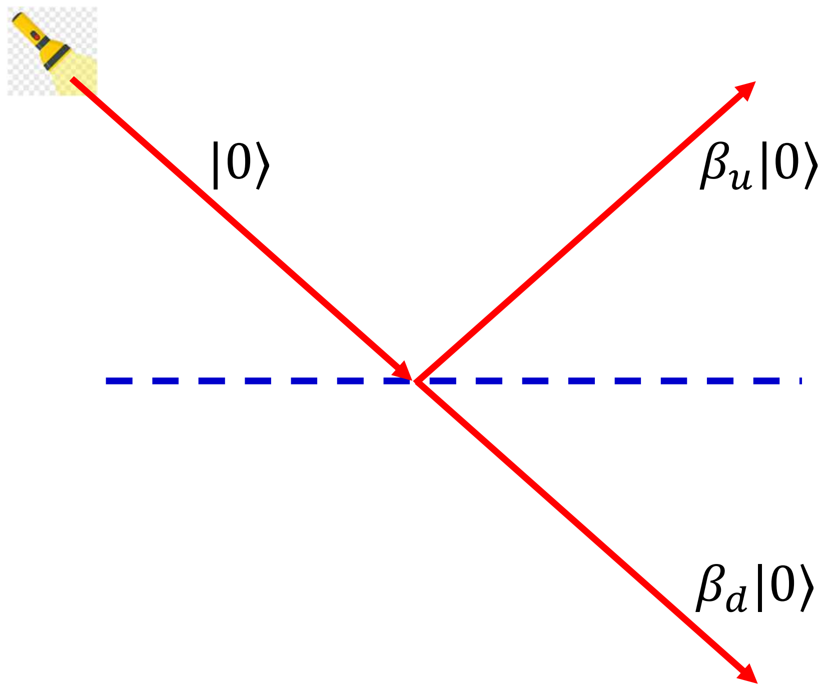
An *equal* beam splitter



$|\alpha_u| = |\alpha_v| = 1/\sqrt{2}$

- If the input below only has horizontally polarized light…

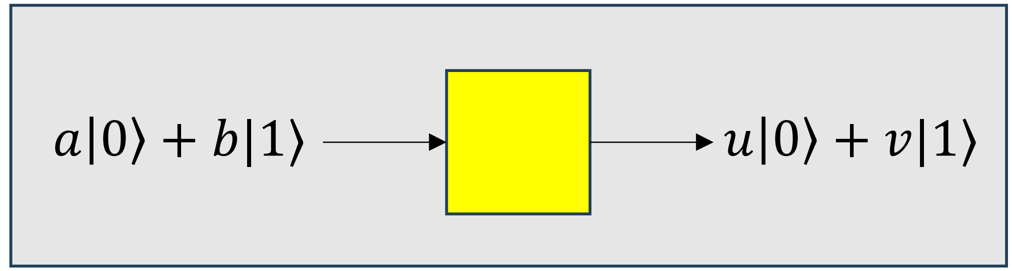
Beam splitter

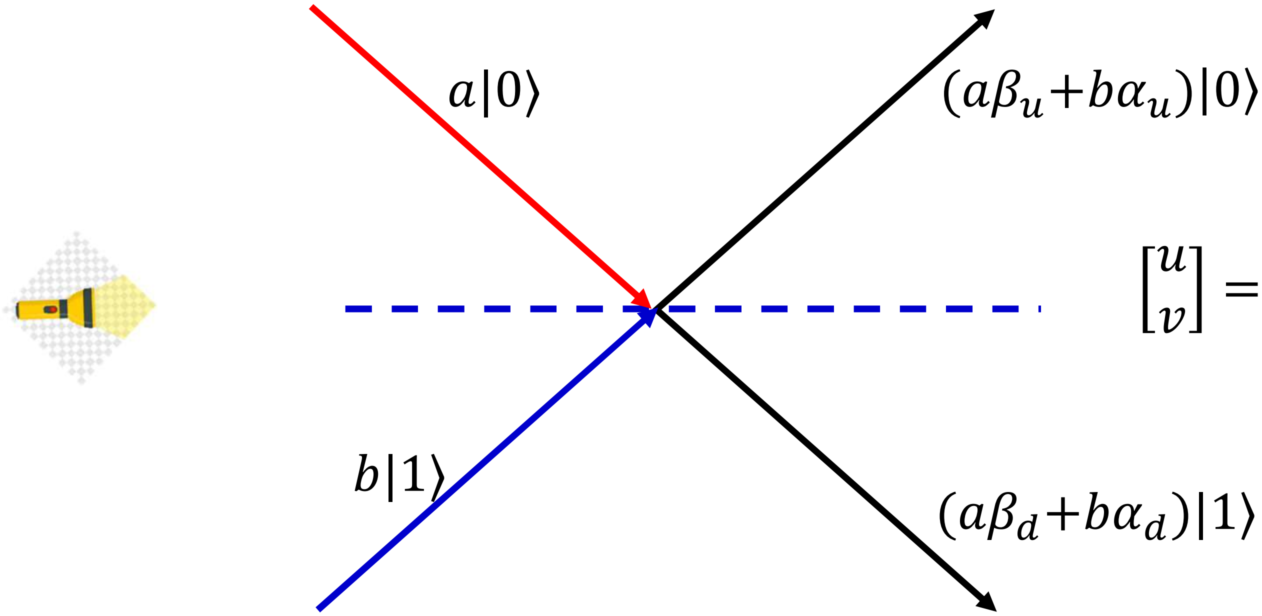


$$|\beta_u| = |\beta_v| = 1/\sqrt{2}$$

- The input above has only vertically polarized light…

Beam splitter



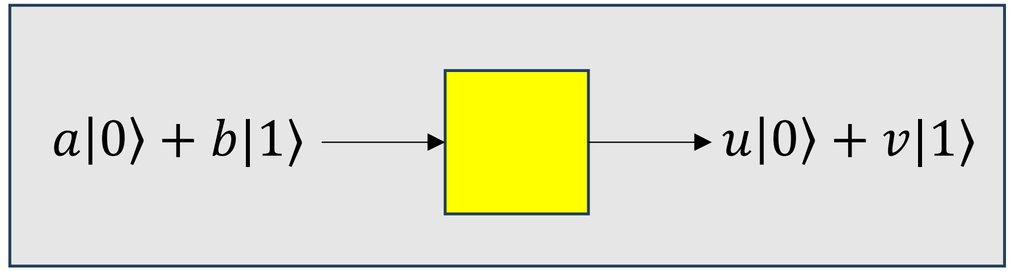


$$\begin{bmatrix} u \\ v \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix}$$

?

- What are acceptable values for α_u, α_d, β_u and β_d?
  - They all have magnitude $\frac{1}{\sqrt{2}}$
  - What are the probabilities of measuring the photon above and below?

Beam splitter

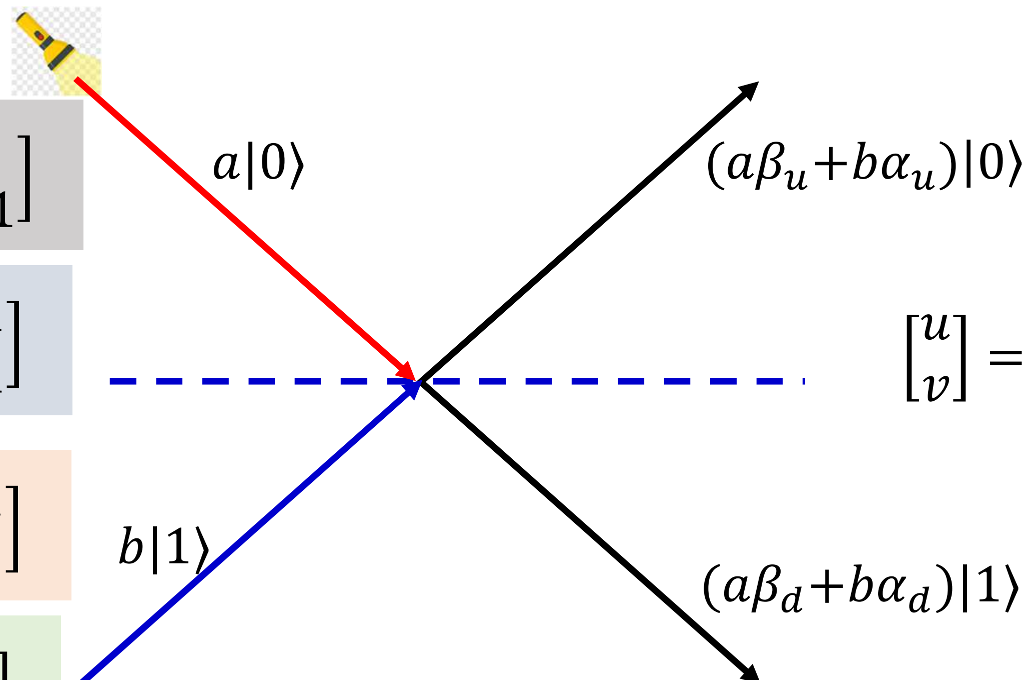


$$\begin{bmatrix} \beta_u & \alpha_u \\ \beta_d & \alpha_d \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

$$\begin{bmatrix} \beta_u & \alpha_u \\ \beta_d & \alpha_d \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} -1 & 1 \\ 1 & 1 \end{bmatrix}$$

$$\begin{bmatrix} \beta_u & \alpha_u \\ \beta_d & \alpha_d \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix}$$

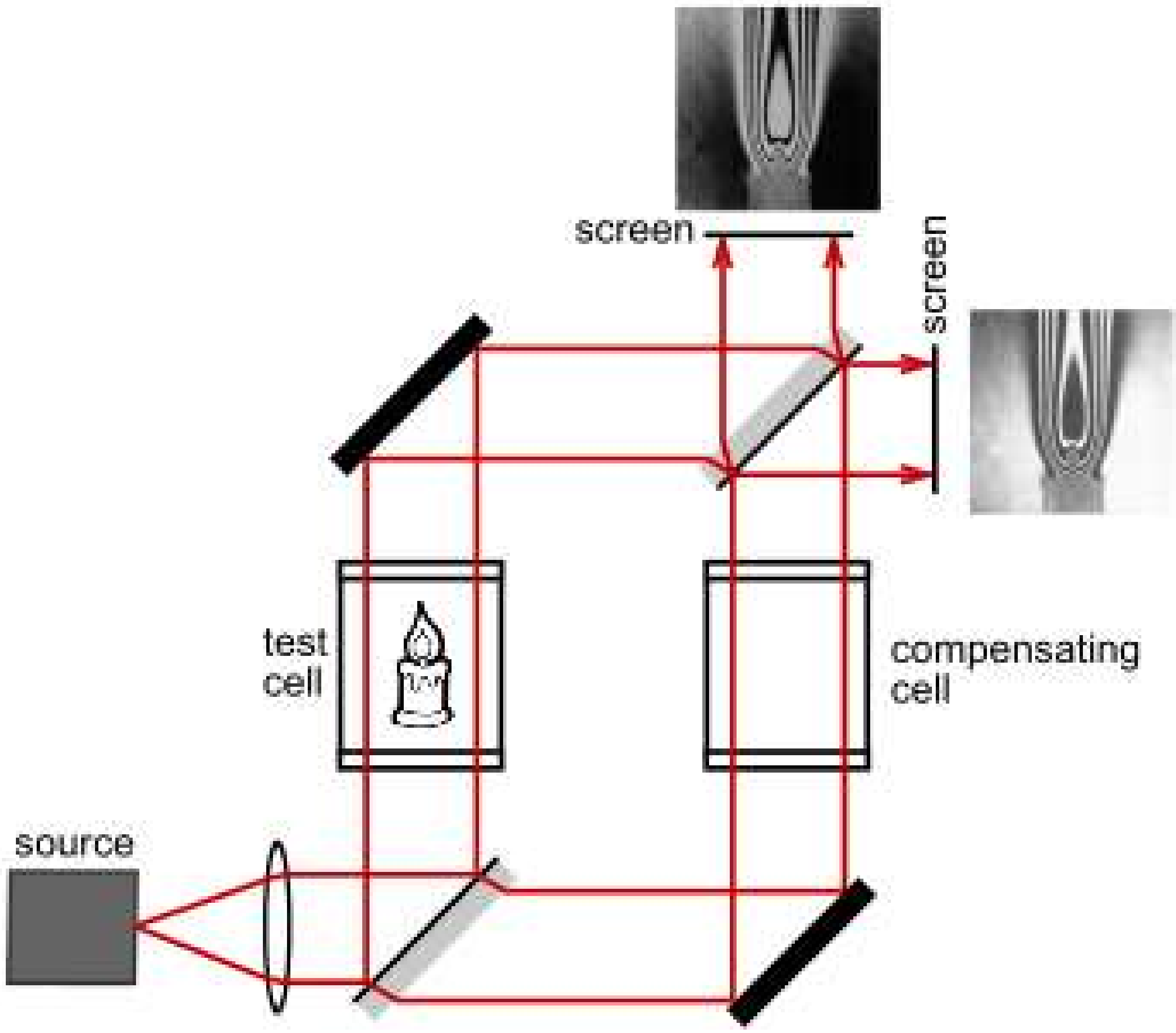
$$\begin{bmatrix} \beta_u & \alpha_u \\ \beta_d & \alpha_d \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix}$$



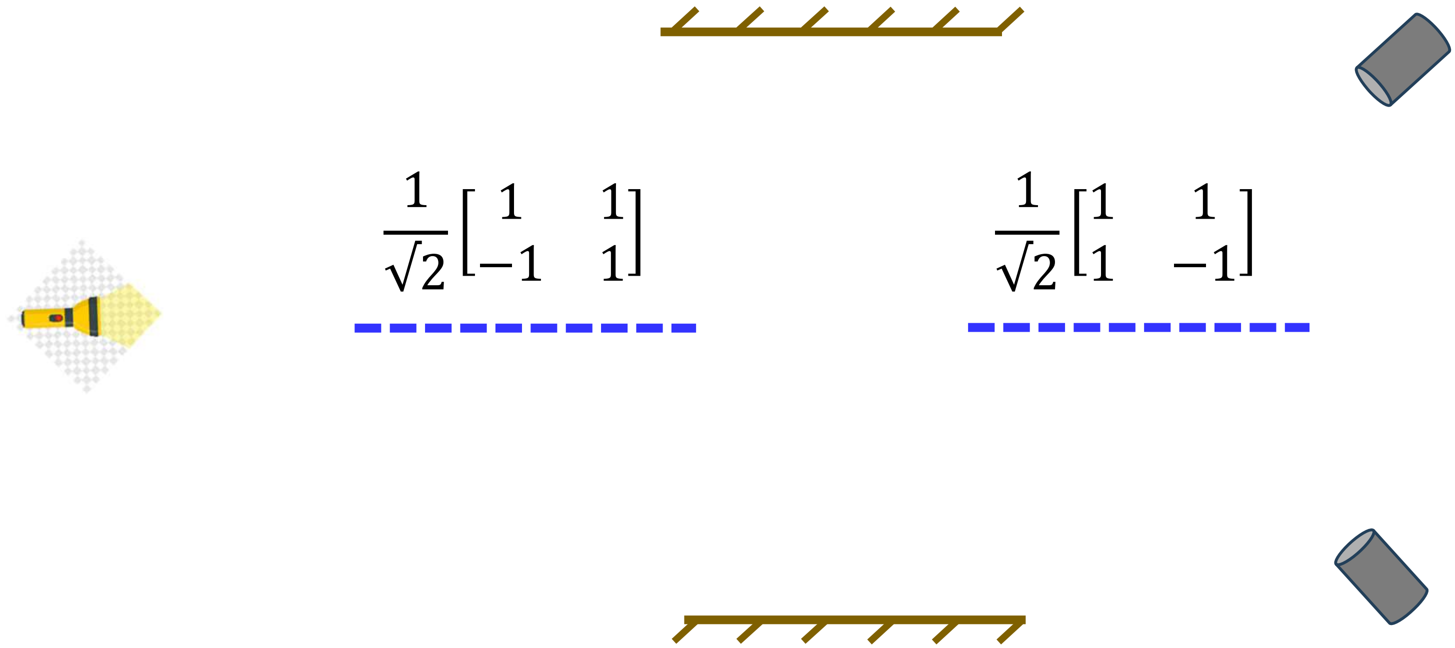
$$\begin{bmatrix} u \\ v \end{bmatrix} = \begin{bmatrix} \beta_u & \alpha_u \\ \beta_d & \alpha_d \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix}$$

- What are acceptable values for α_u, α_d, β_u and β_d?

The Mach Zehnder interferometer

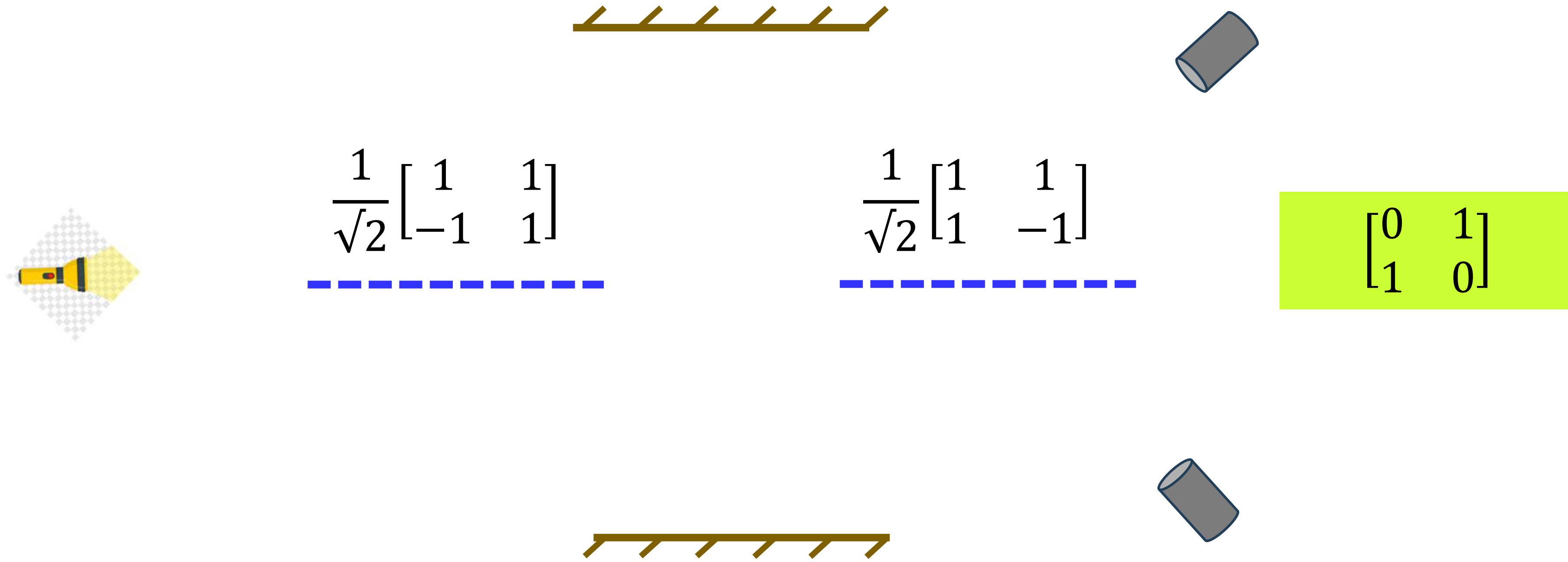


The Mach Zehnder Interferometer



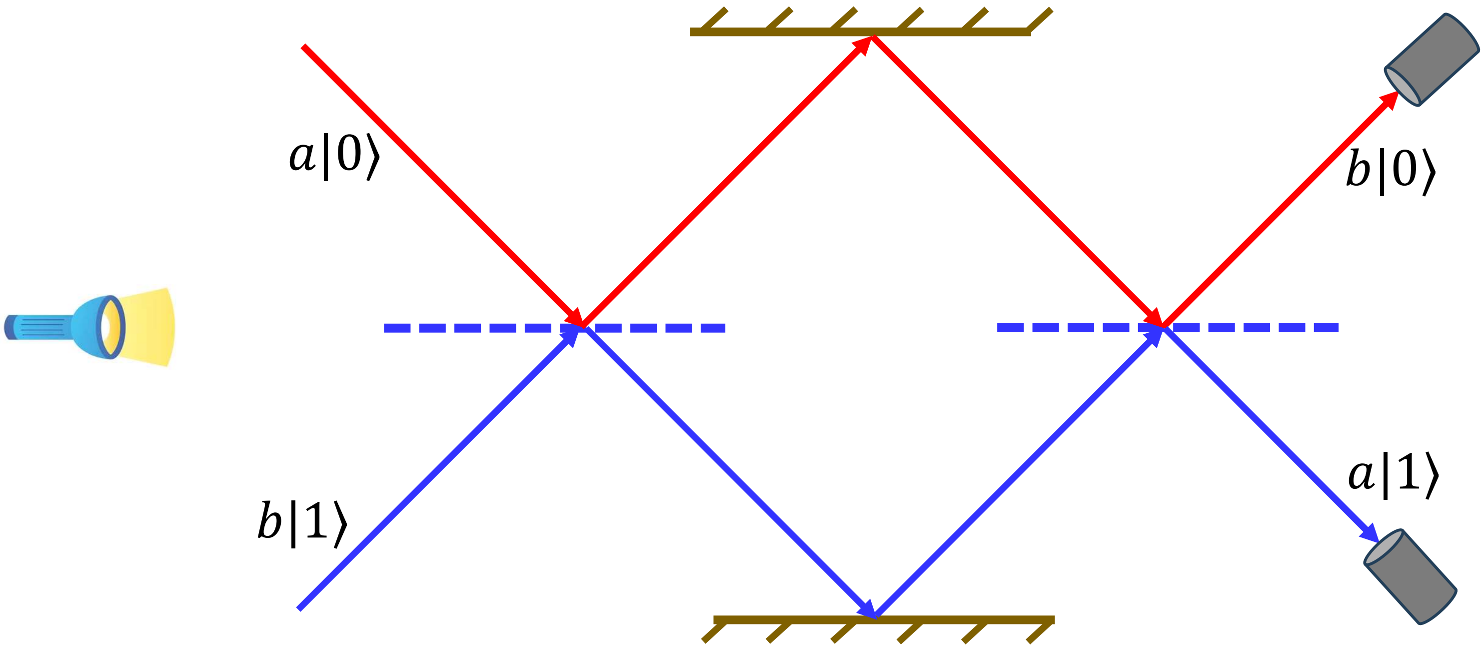
- Two beam splitters of opposite polarity
- Two mirrors $\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}$
- Two sensors
- What is the overall response of the system?

The Mach Zehnder Interferometer



- Two beam splitters of opposite polarity
- Two mirrors $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$
- Two sensors
- What is the overall response of the system?

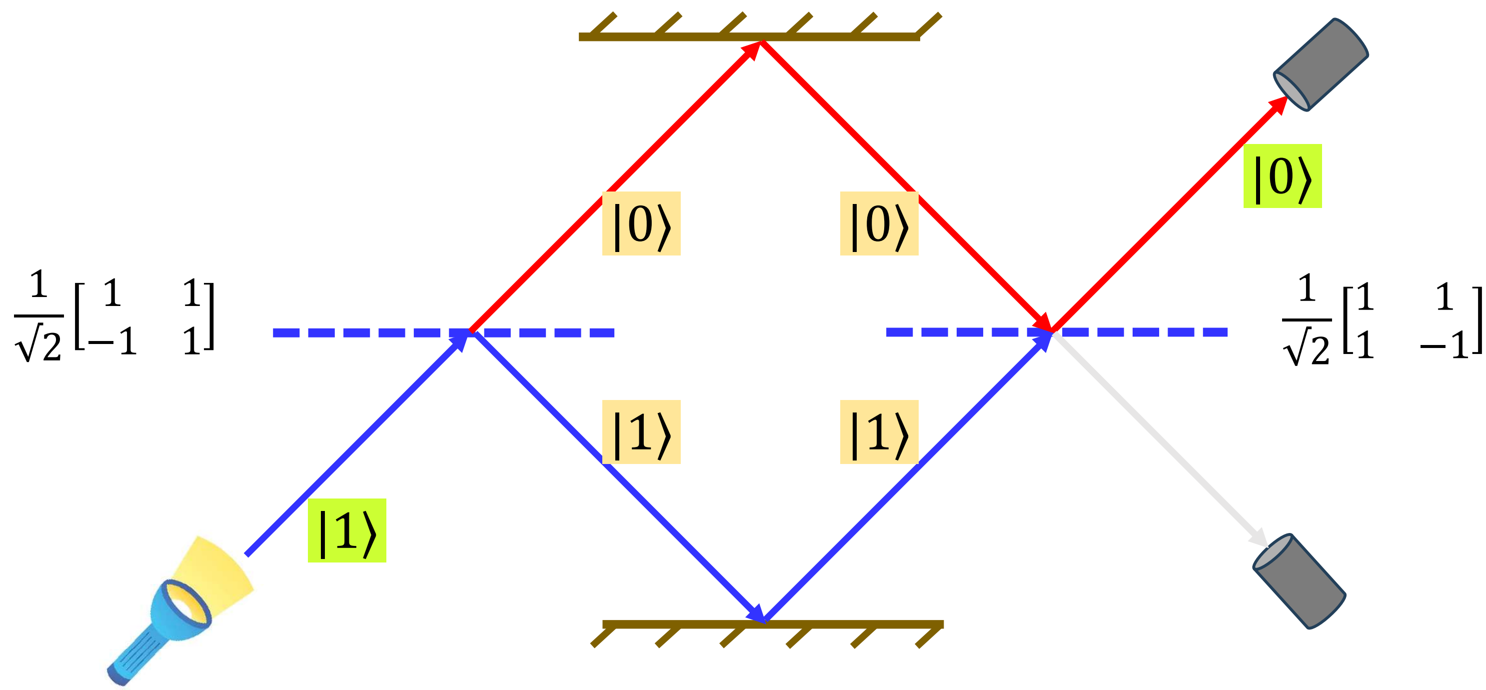
The Mach Zehnder Interferometer



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

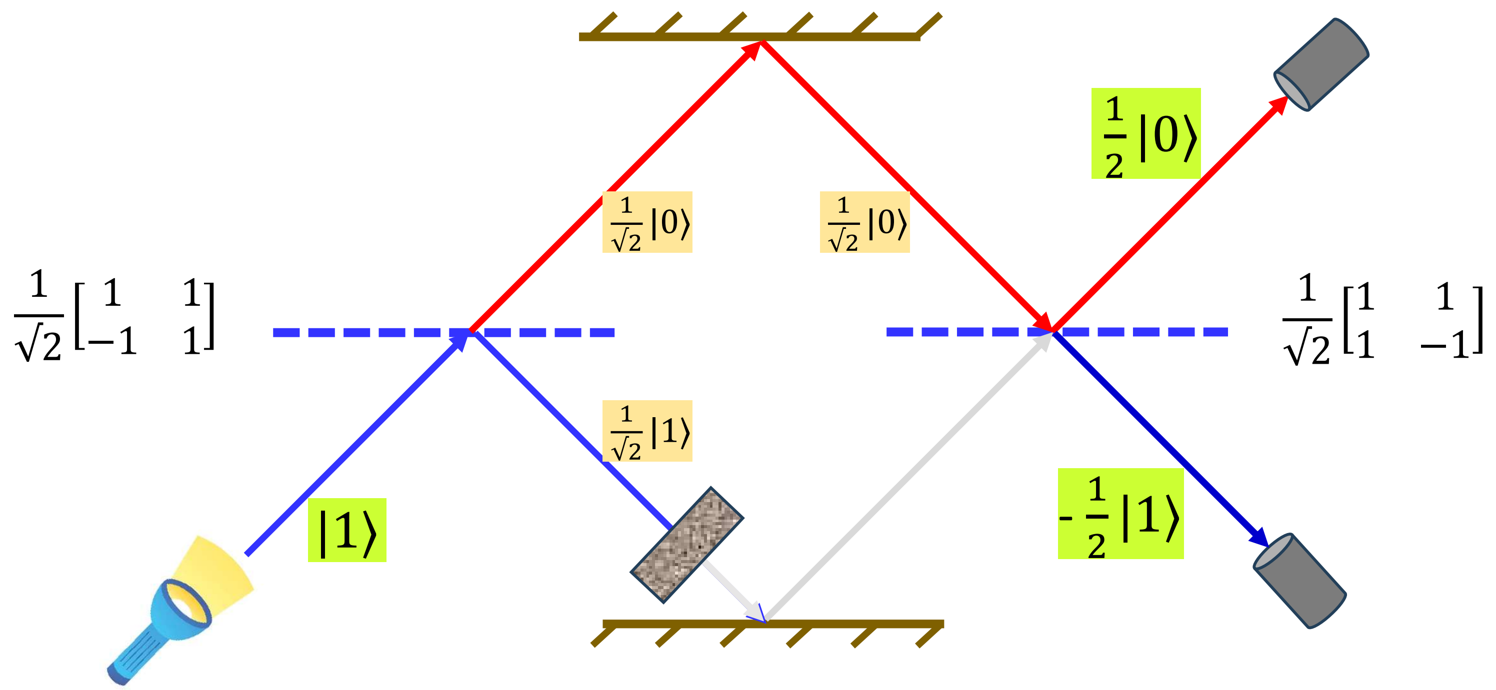
- The entire system is an inverter
  - The beam from below comes out on top
  - The beam from above goes out on bottom

The Mach Zehnder Interferometer



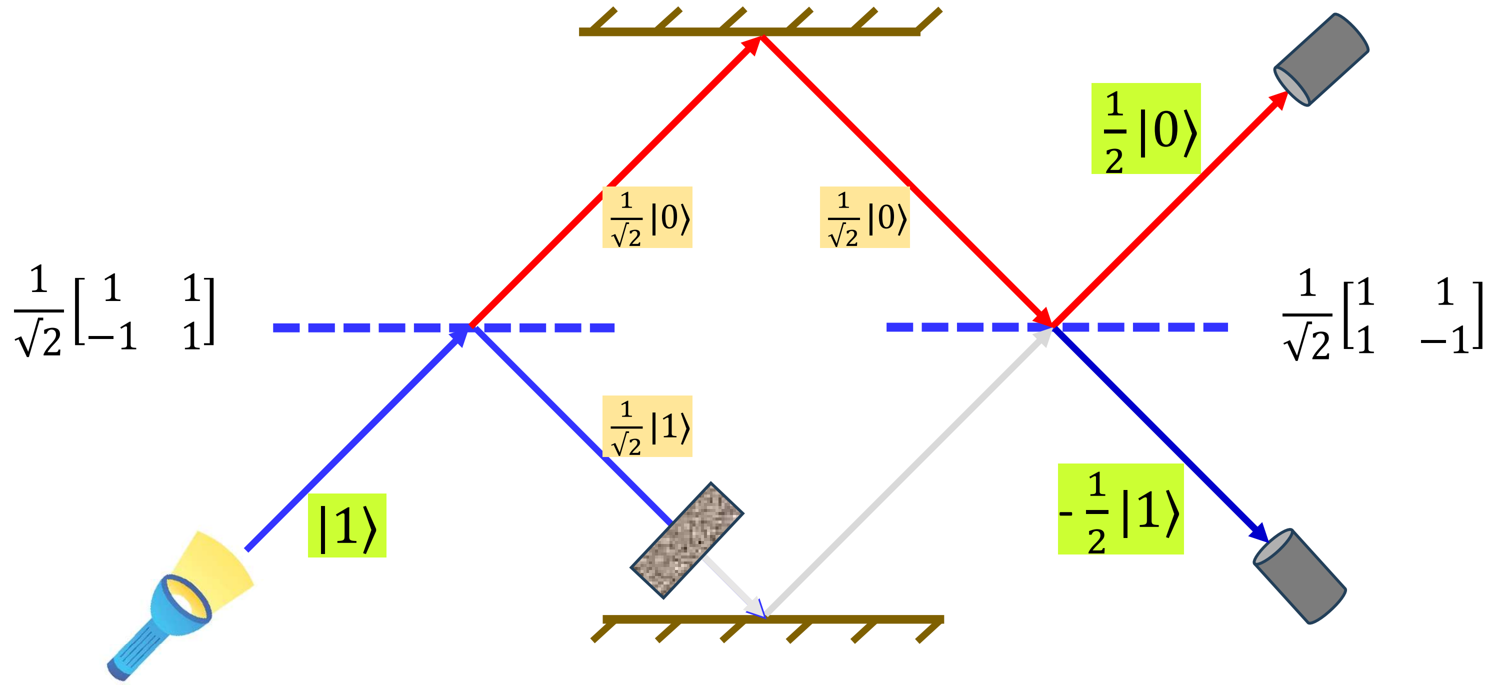
- A “pure” state from below ends up being sensed only by the upper sensor
  - On the lower sensor the two paths “interfere” and cancel out
  - The $\frac{1}{\sqrt{2}}$ factor is not shown between the splitters

The Mach Zehnder Interferometer



- Introducing a block on the lower path
  - Now the output is a superposition again
- The brick wall could "measure" the photon ½ the time
- The upper sensor could measure the photon 1/4th of the time
- The lower sensor could measure the photon 1/4th of the time

The Mach Zehnder Interferometer

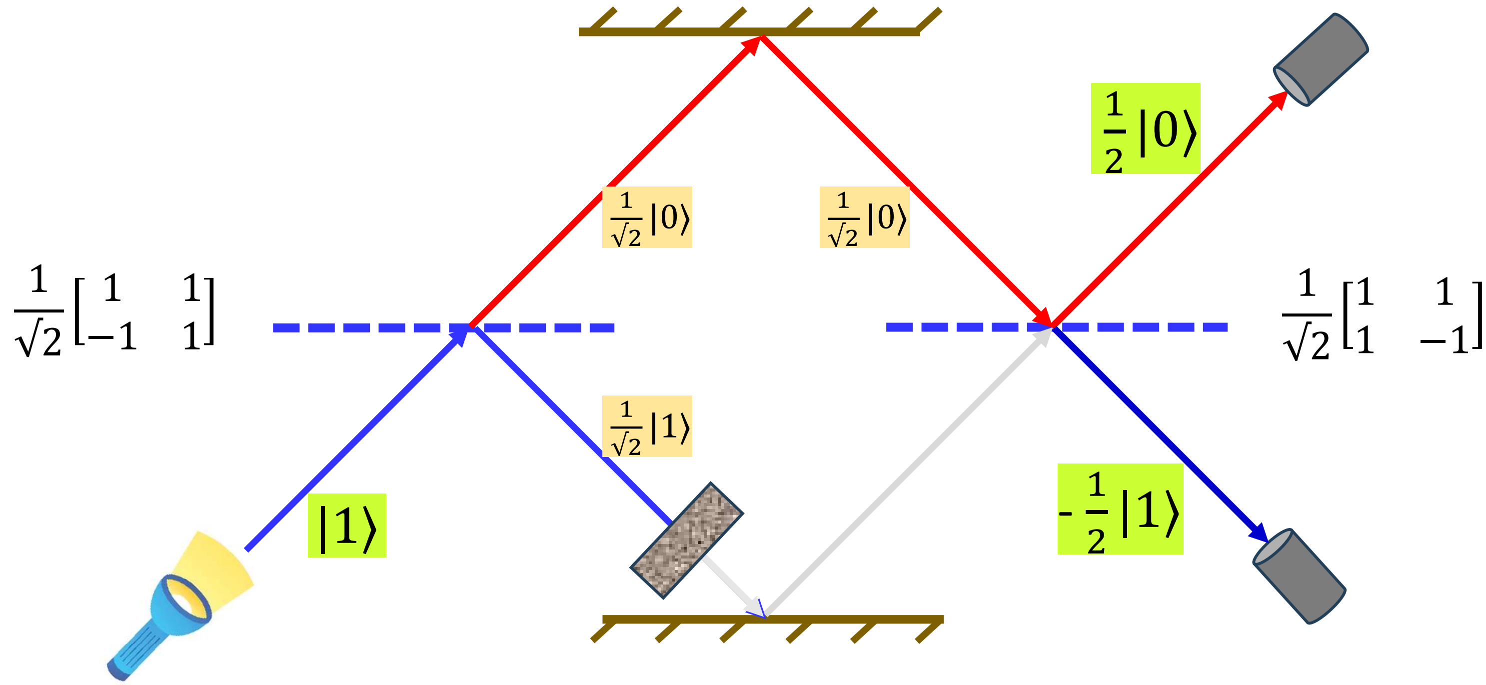


The photon is in a superposition of THREE states

BLOCKING light causes the lower sensor to *SENSE* light some of the time!

- Introducing a block on the lower path
  - Now the output is a superposition again
- The brick wall could "measure" the photon ½ the time
- The upper sensor could measure the photon 1/4th of the time
- The lower sensor could measure the photon 1/4th of the time

The Mach Zehnder Interferometer



The photon is in a superposition of THREE states

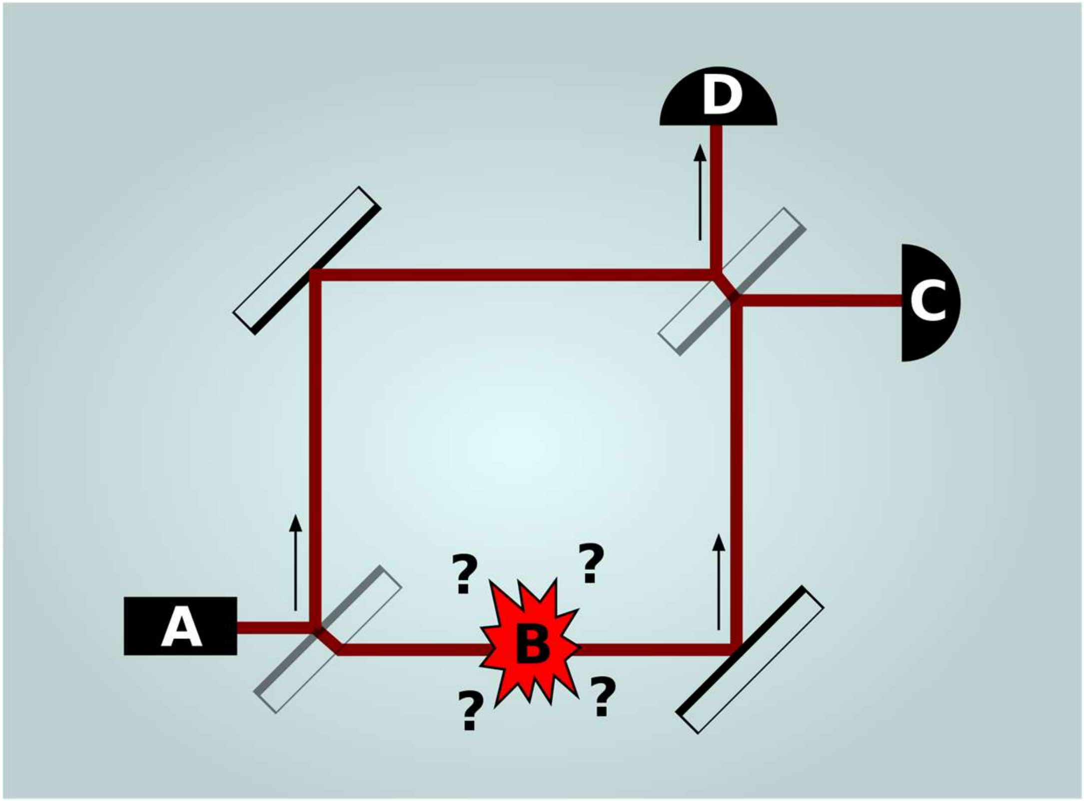
BLOCKING light causes the lower sensor to *SENSE* light some of the time!

- Introducing a block on the lower path
- e
- he time
- he time

But is this because of superposition, or simply because half the photons go one way and half the other at each splitter?

Introducing – the bomb!!!

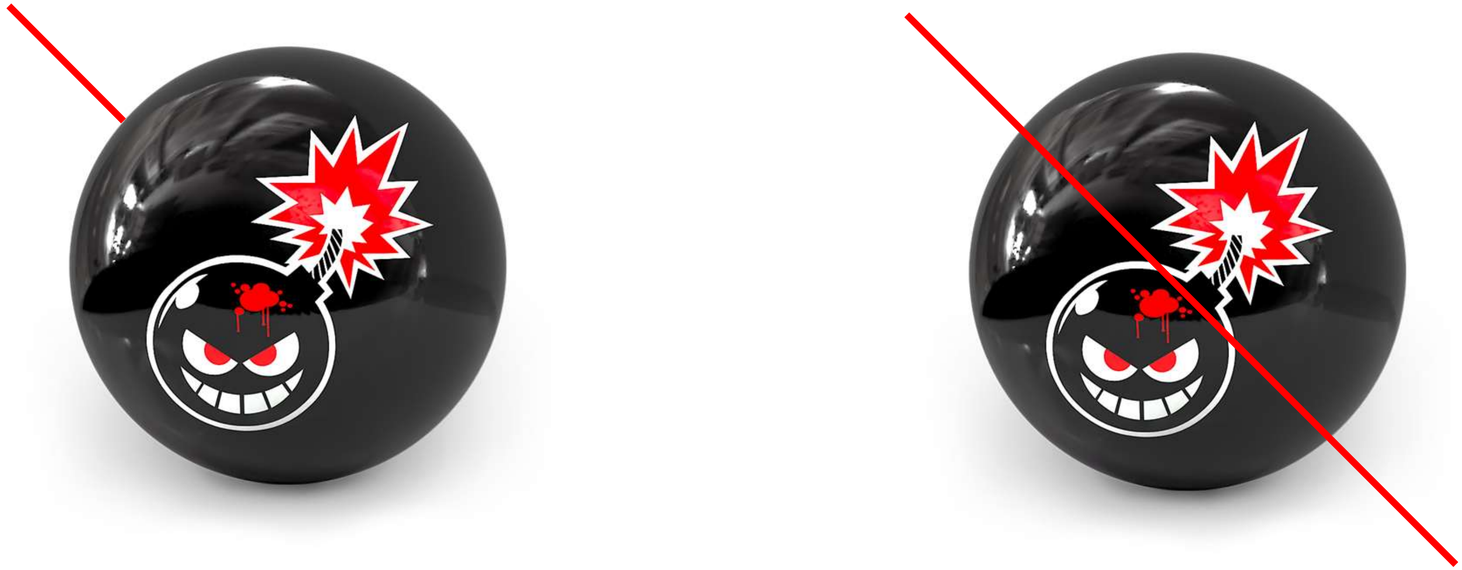
The Elitzur-Vaidman bomb tester



A special kind of bomb

- Light sensing bomb
- It goes off if a photon falls on the sensor 

A special kind of bomb

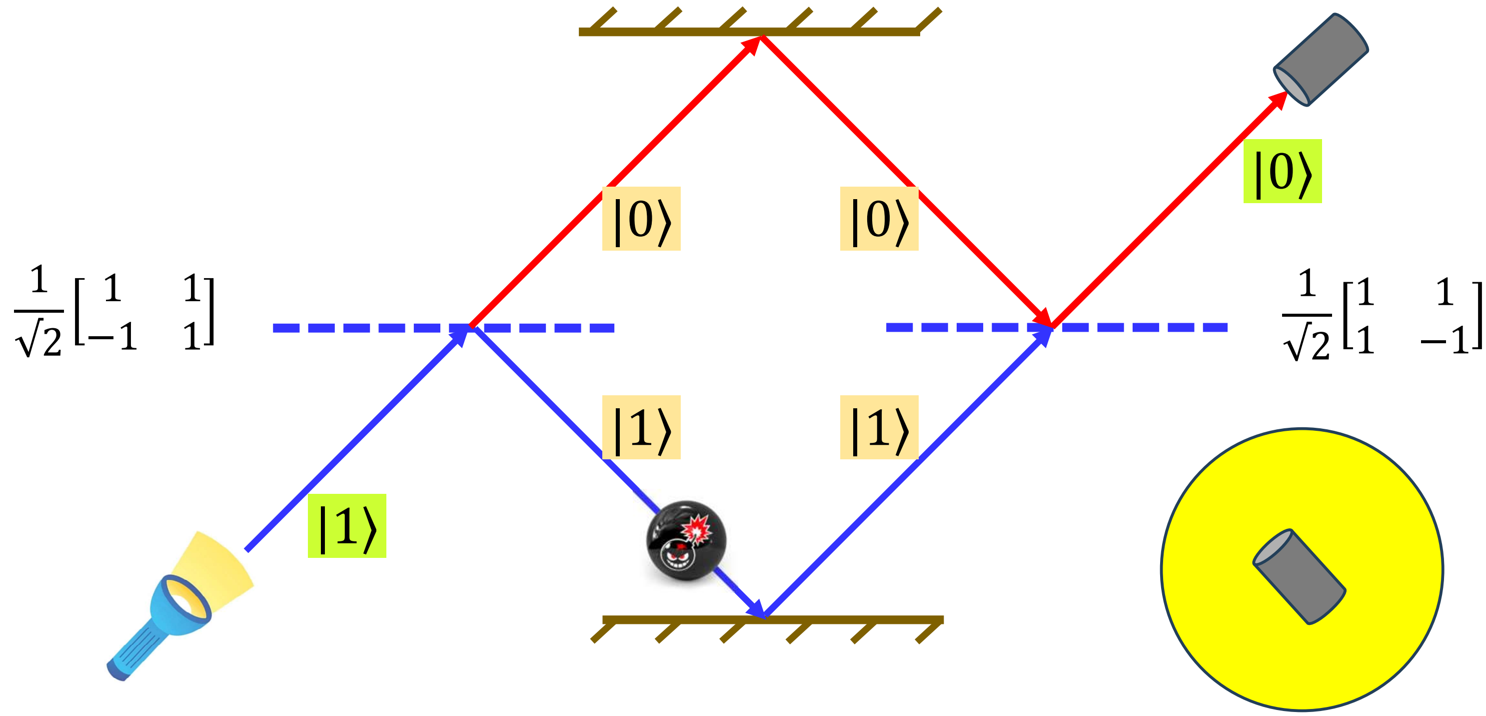


- Light sensing bomb
- It goes off if a photon falls on the sensor 
- But if the bomb is faulty, the light simply goes through without any change, and the bomb doesn’t explode 

We have a problem

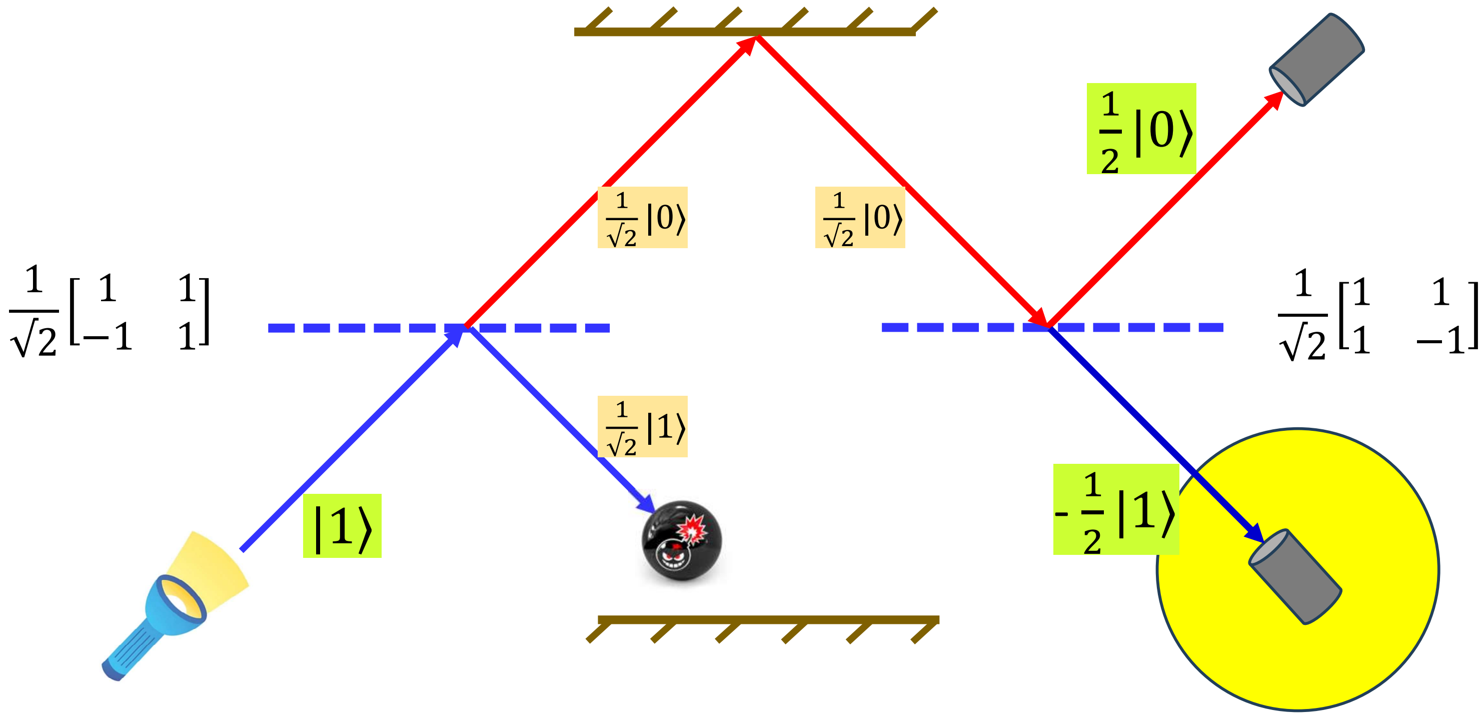
- We have a collection of bombs. Some are faulty, some are not.
- Using only a laser, how do we determine which ones are faulty without killing ourselves?

Testing the bomb



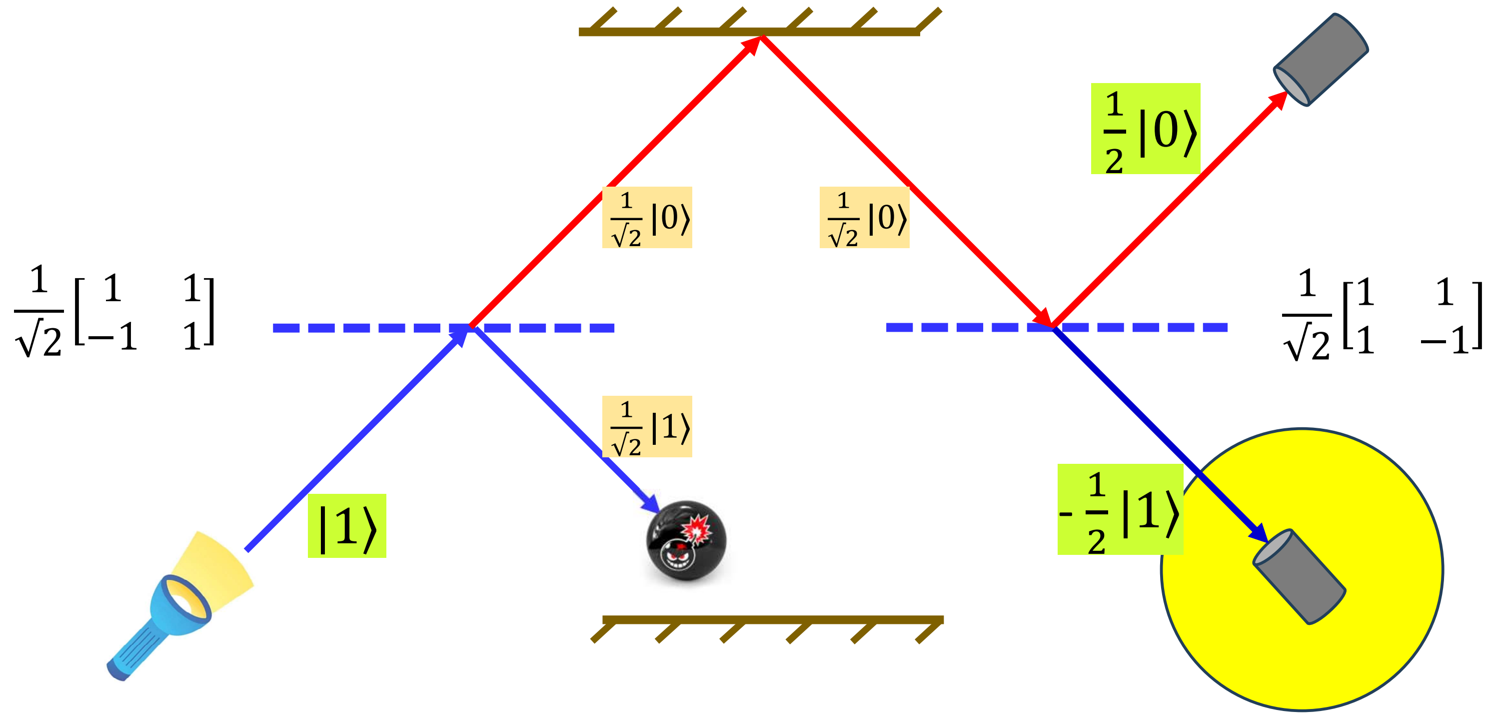
- Put the bomb in the lower path of the Mach Zehnder interferometer
- If it is faulty, the light simply goes through (as if it is not present).
  - Only the upper sensor senses light.
  - The lower sensor doesn't sense any light.
- If the lower sensor doesn't sense light, the bomb is faulty.

Elitzur-Vaidman bomb tester



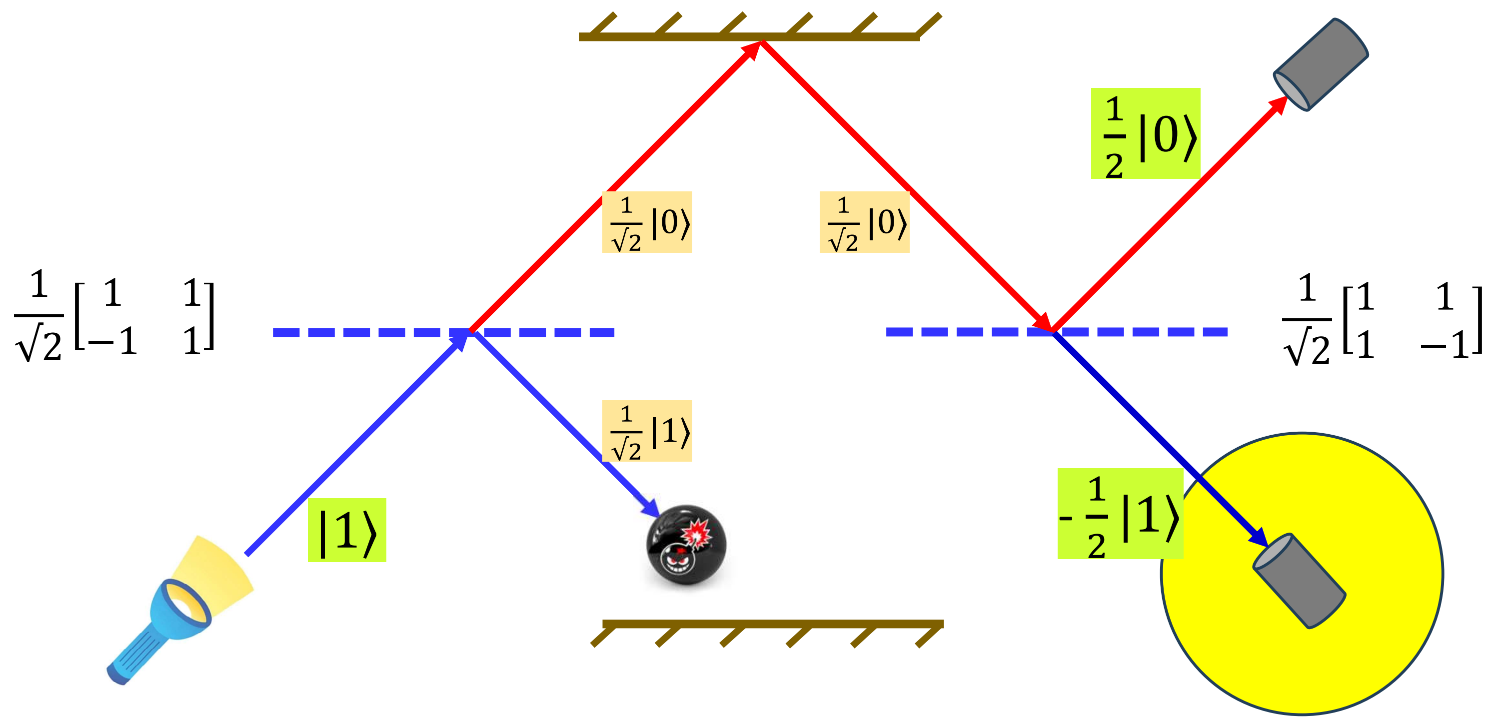
- If the bomb is not faulty (and if superposition is true), the photon is in a superposition of 3 states
- With P = ¼, it will be measured at the lower sensor
  - And yet the bomb wont go off because the photon never hit it

Elitzur-Vaidman bomb tester



- If the bomb is not faulty (and if superposition is true), the photon is in a superposition of 3 states
- With P = ¼, it will be measured at the lower sensor
  - And yet the bomb wont go off because the photon never hit it
- **If the lower sensor detects the photon, the bomb is certainly armed!**

Elitzur-Vaidman bomb tester

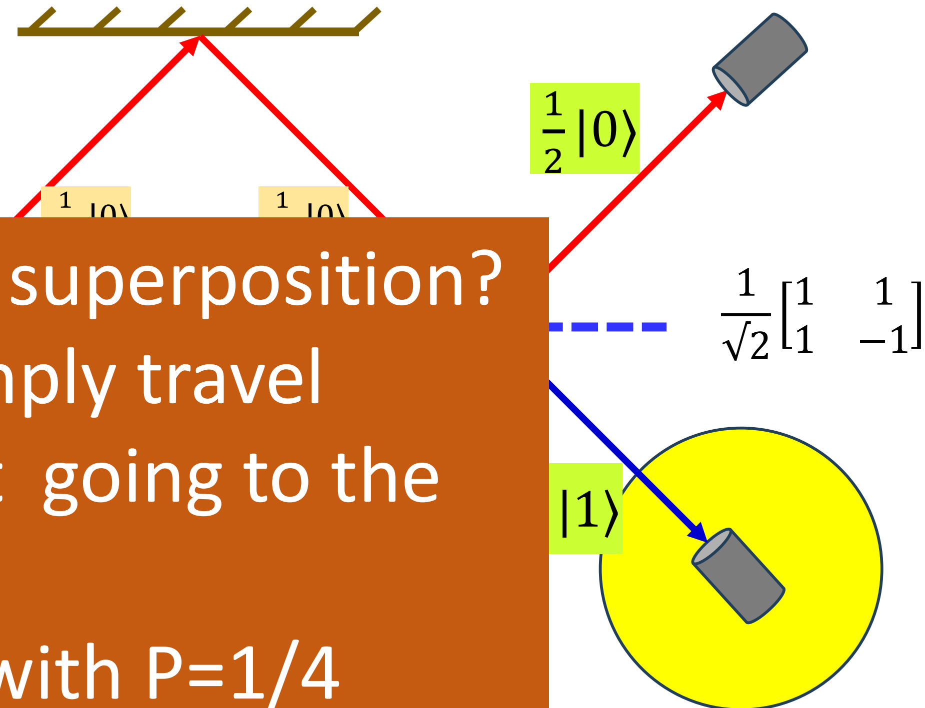


- If the bomb is not faulty (and if superpositior
  superposition of 3 states
- With P = ¼, it will be measured at the lower s
  - And yet the bomb wont go off because the photon never hit it

The lower sensor detects light for 25% of non-faulty bombs

- If the lower sensor detects the photon, the bomb is certainly armed!

Elitzur-Vaidman bomb tester



But is this because of superposition?
Or did the photon simply travel
to the sensor without going to the
bomb?
This too can happen with P=1/4

But this would happen for faulty
bombs too!!!

The lower sensor
detects light for 25%
of non-faulty bombs

- With P = ¼, it will be measured at the lower s
  - And yet the bomb wont go off because the phot

- If the lower sensor detects the photon, the bomb is certainly armed!

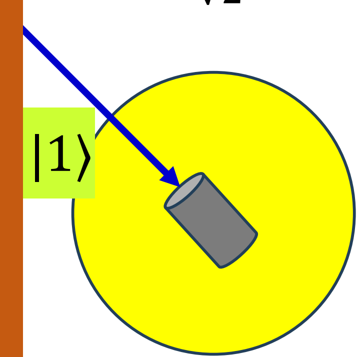
Elitzu

In every case where the lower sensor goes off, check the bomb. If the bomb is armed *every* time, the probability that this has happened randomly and not due to superposition becomes vanishingly small

But is this because of superposition? Or did the photon simply travel to the sensor without going to the bomb?
This too can happen with P=1/4

But this would happen for faulty bombs too!!!

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



The lower sensor detects light for 25% of non-faulty bombs

- With P = ¼, it will be measured at the lower s
  - And yet the bomb wont go off because the photon never hit it

- If the lower sensor detects the photon, the bomb is certainly armed!

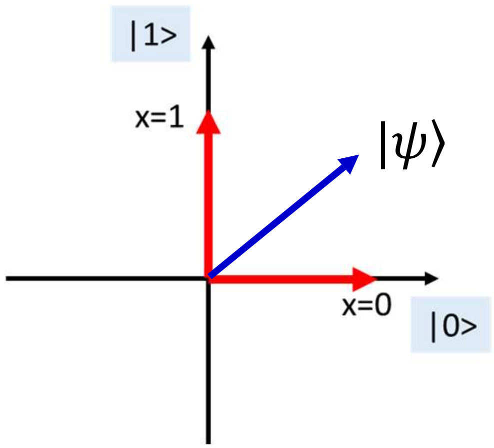
Solved!!! (Kinda)

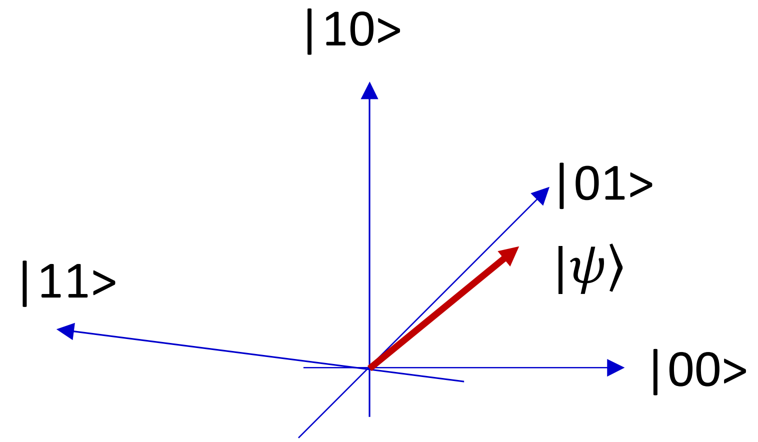
- If superposition is true: We will successfully detect 25% of good bombs
  - Please don't be in the room for the remaining 75%
- This has actually been tested in experiments
  - With the efficiency of the sensor improved all the way to 99%

Topics for the day

- The math of measurement
- How to change between measurement bases
- What is a “Boolean Gate” in this new math
- Multi-input gates
- Multi-qubits and entanglement

Recap: A new binary math

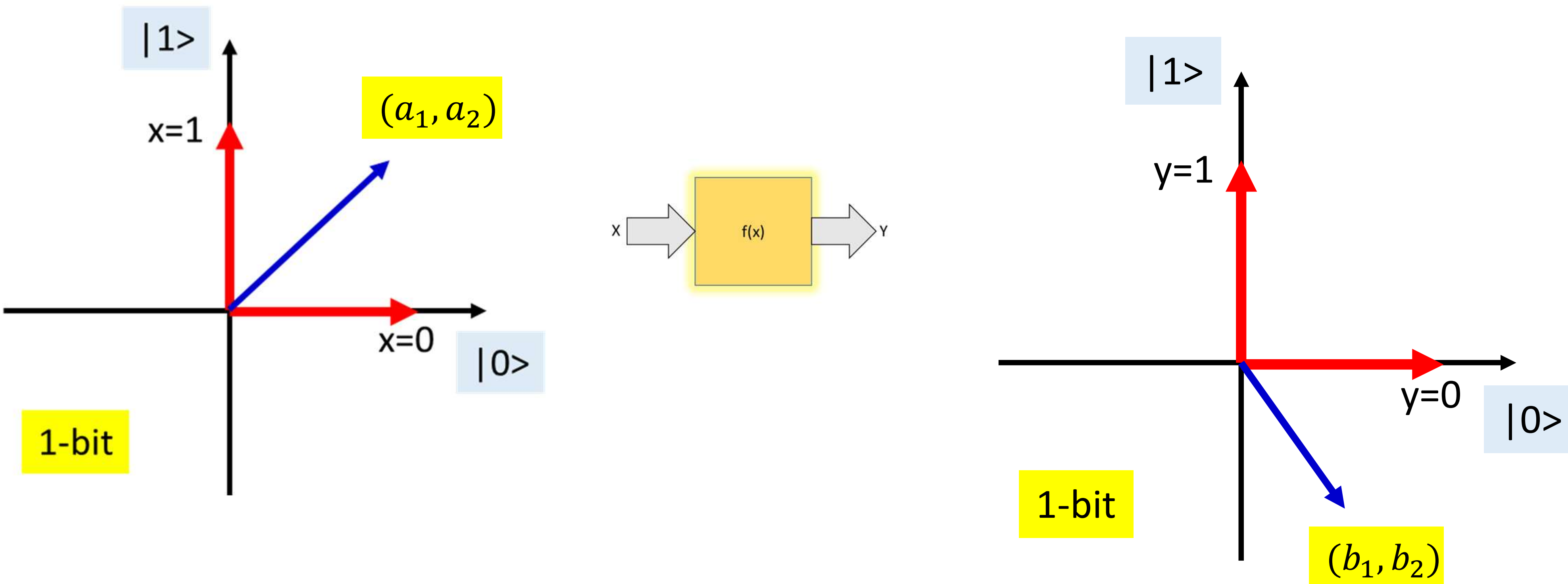




Lame attempt at visualizing 4D

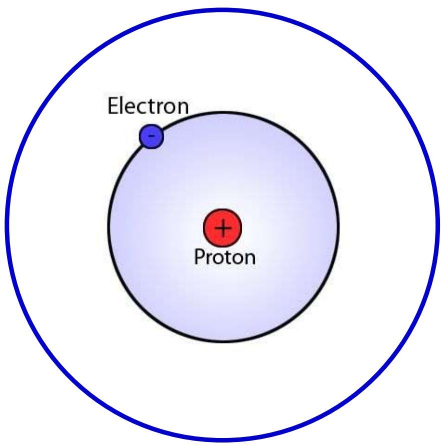
- *Bit patterns* now represent orthogonal directions
- An input is now a vector (a ***phasor***) in this new space
  - And represents a linear combination of bit patterns
  - 1 bit: $|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$
  - 2 bits: $|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$
- ***Superposition*** of all possible bit patterns

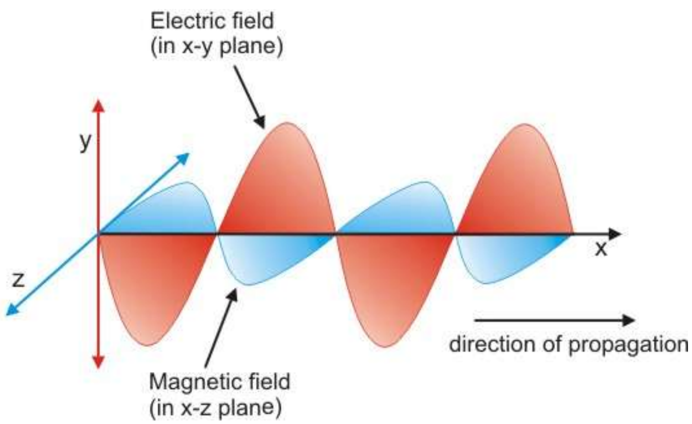
Recap: The new "quantum" math

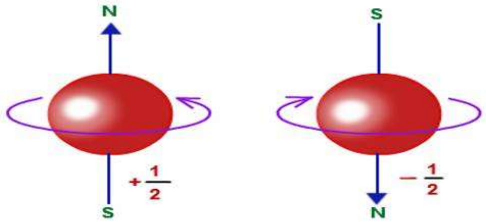


- An algorithm is now an operator that operates on the vector to produce another vector
  - Can now compute the output for *all* bit patterns in a single evaluation step
- Caveats – the operator must be:
  - Linear
  - Invertible
  - And not increase the length of the vector (i.e. it must be a rotation)
- **Additional clause**: The "Qbit" phasors must be unit length

Recap: Implementing the qubit

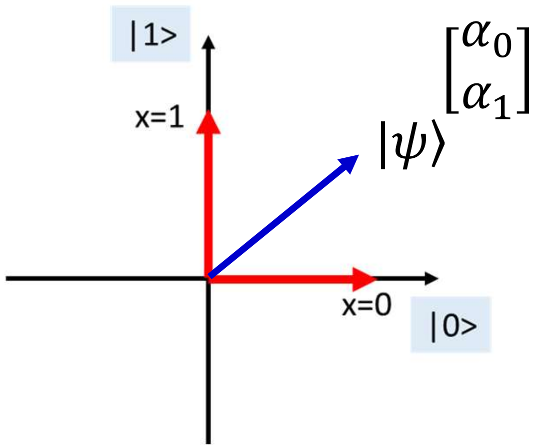


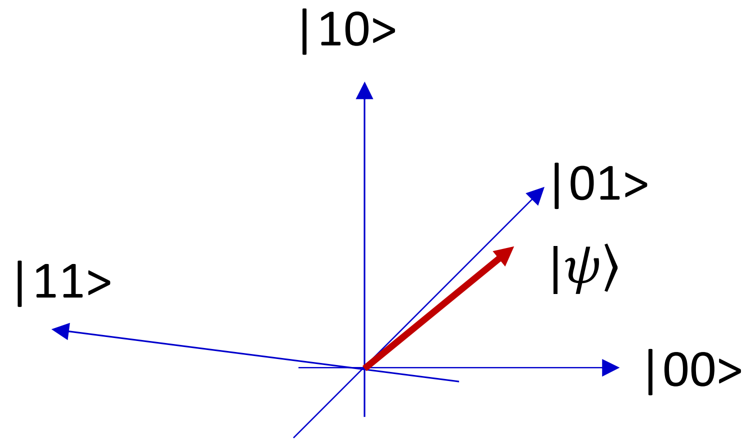




- Cannot use classical physics
  - Will require computers with exponential amounts of memory to represent even a small number of bits
- Use quantum physics
  - Derived from Schrodinger's equation: $ih\frac{d}{dt}|\psi(t)\rangle = 2\pi H|\psi(t)\rangle$
    - Every particle is a wave that exists in all states $|\psi(t,x)\rangle$ simultaneously
    - $|\psi(t,x)\rangle|^2$ = probability of finding the system in configuration x at time t when you measure it
  - Use quantum properties of quantum particles to implement the bit
  - E.g: The energy level of an electron
  - E.g: The spin of an electron
  - E.g: The polarization of a photon

Recap: A new binary math



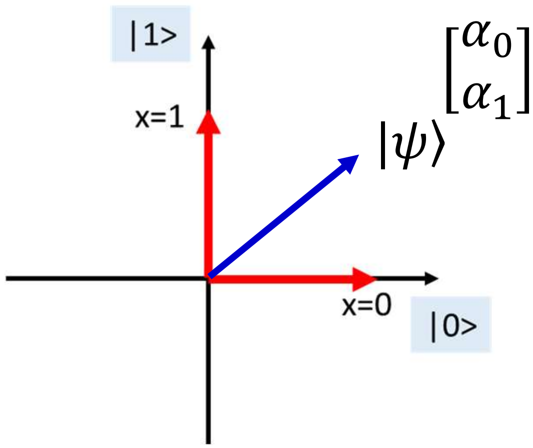


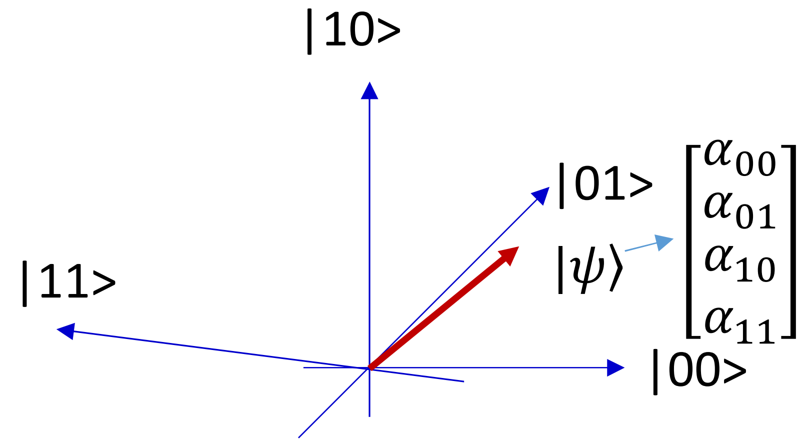
Lame attempt at visualizing 4D

- *Input "phasors" live in complex space*
  - And represent a linear combination of bit patterns
  - 1 bit: $|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$
  - 2 bits: $|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$
- ***The αs are all complex***

$\sum|\alpha_i|^2 = 1$ for any phasor

The problem of measurement





Lame attempt at visualizing 4D

- You cannot measure the phasor
  - It will collapse to one of the bases
- One qubit:

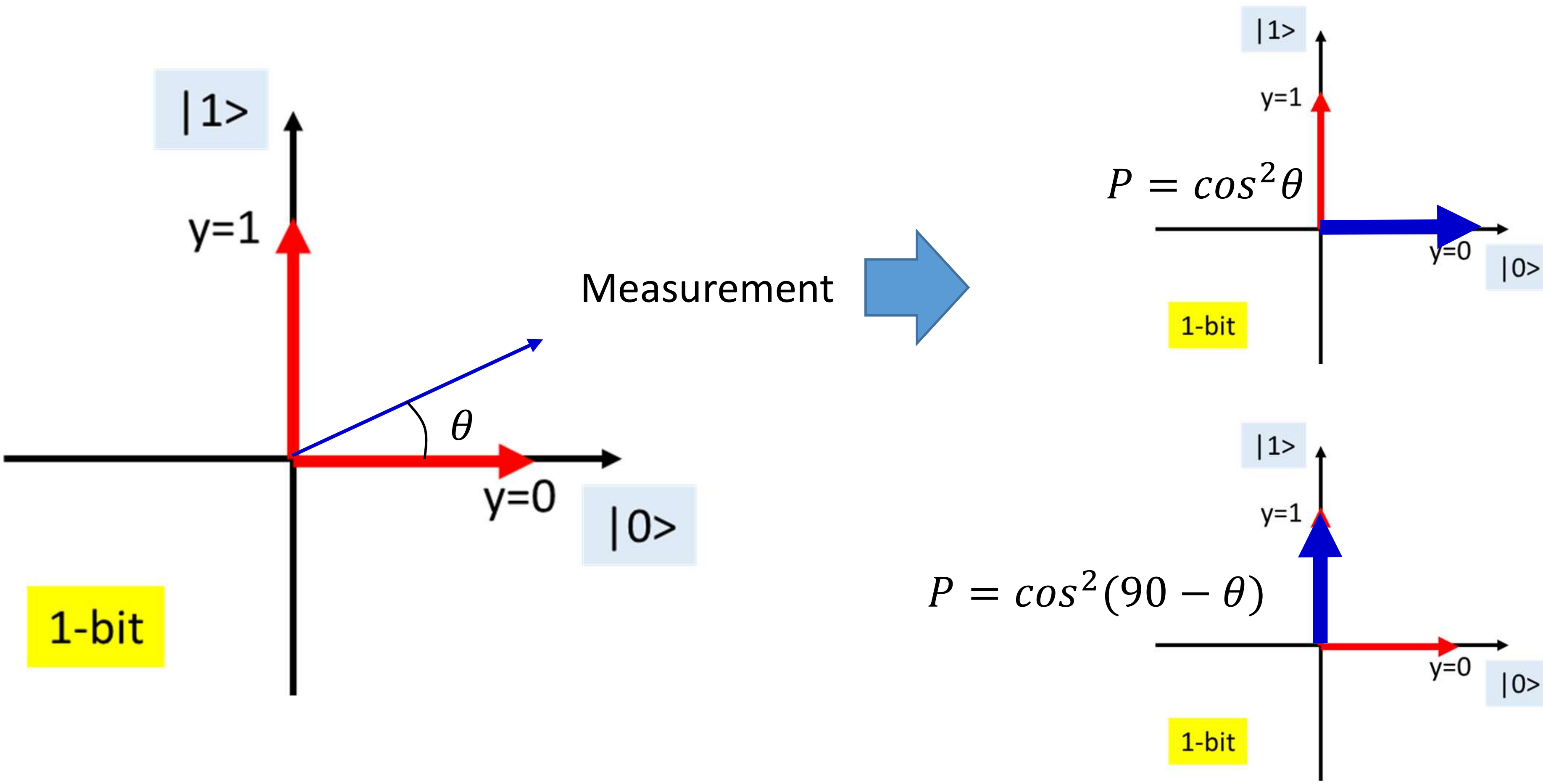
$$\alpha_0|0\rangle + \alpha_1|1\rangle \rightarrow \begin{cases}|0\rangle\ with\ probability\ |\alpha_0|^2\\ |1\rangle\ with\ probability|\alpha_1|^2\end{cases}$$

$$\sum|\alpha_i|^2 = 1$$

- Two qubits:

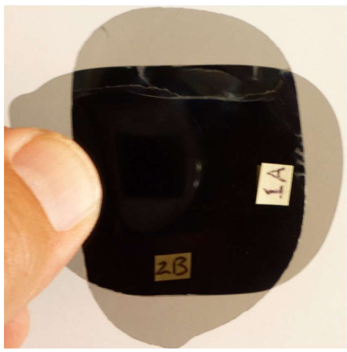
$$\alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle \rightarrow \begin{cases}|00\rangle\ with\ probability\ |\alpha_{00}|^2\\ |01\rangle\ with\ probability\ |\alpha_{01}|^2\\ |10\rangle\ with\ probability\ |\alpha_{10}|^2\\ |11\rangle\ with\ probability\ |\alpha_{11}|^2\end{cases}$$

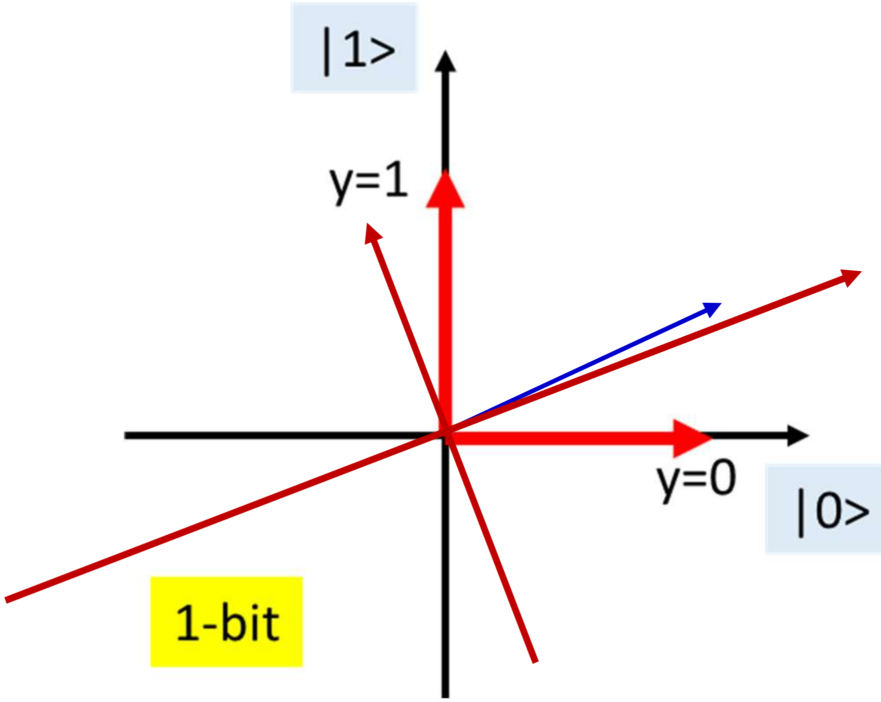
Measurement



- Measuring the output collapses the vector to one of the states
  - Bit pattern

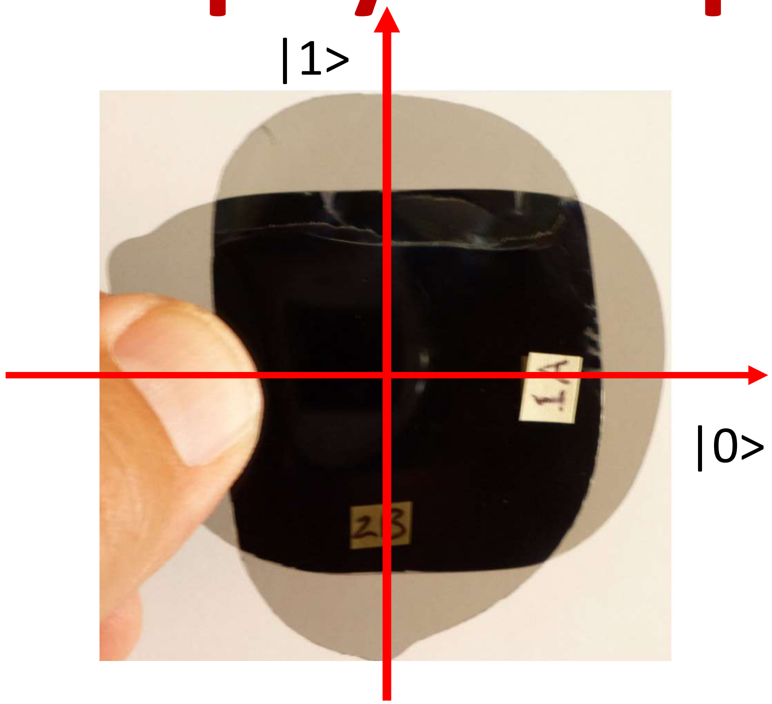
The physical Qubit

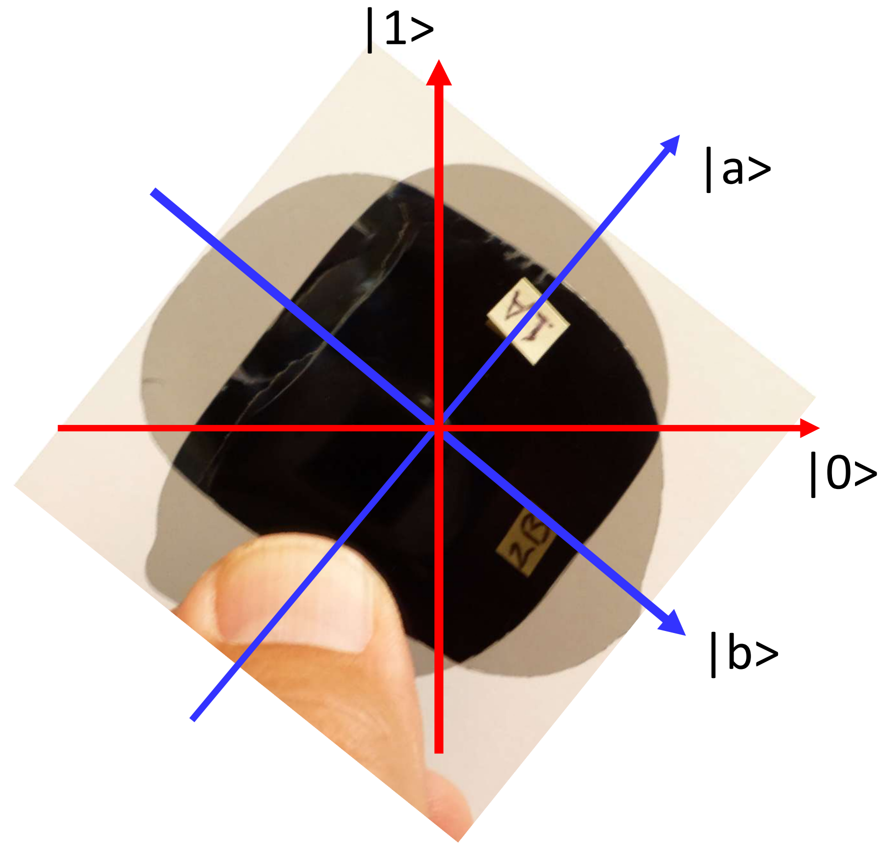




- The definition of your “bases” is a matter of convention
  - The only requirement is that they are at right angles to one another.
- The phasor (the blue arrow) is absolute though
  - And represents the state of the (qubit in the) universe

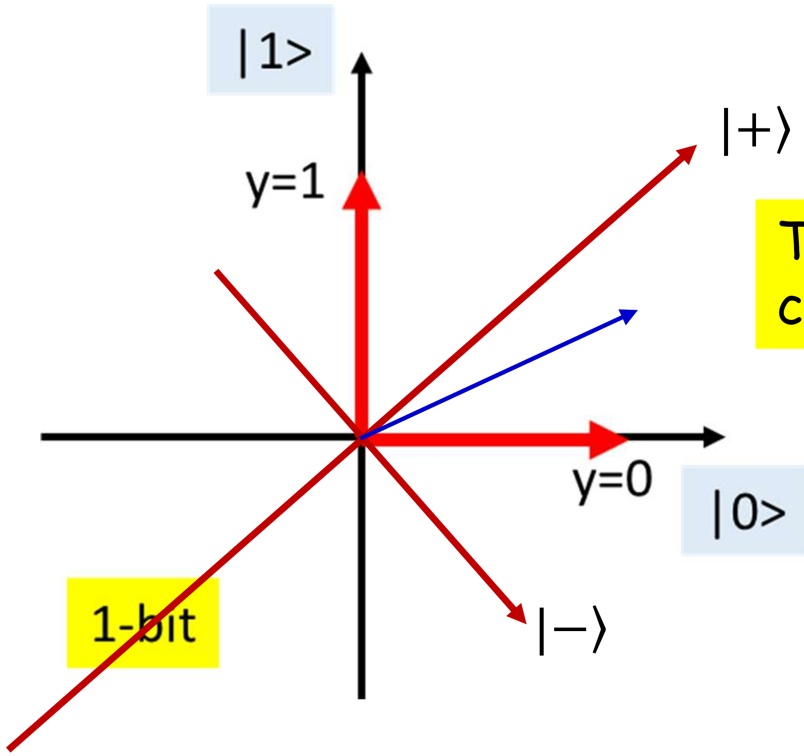
The physical qubit





- We *always* specify some (possibly arbitrarily chosen) directions as our ``canonical'' bases
  - These are typically designated as the ``bit'' bases, representing the bit values |0> and |1>
- But we can *also simultaneously* have *other* bases
  - Which can be defined in terms of our bit bases (or, alternately, our bit bases can be defined in terms of these other bases)

The physical Qubit

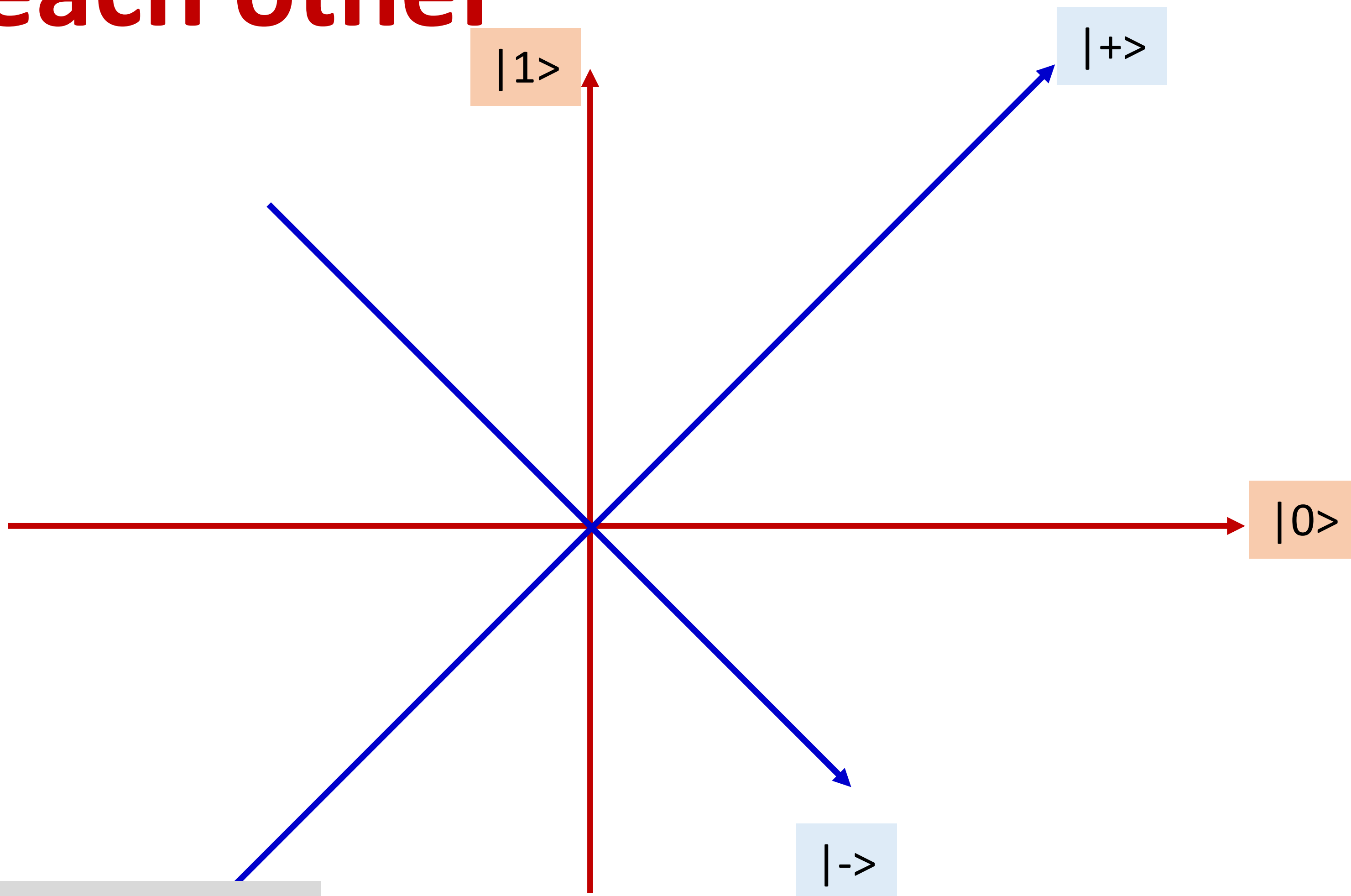


The sign bases are commonly also invoked

Note: The definition of your "bases" is a matter of convention

The phasor is absolute, though.

Bases can be expressed in terms of each other



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

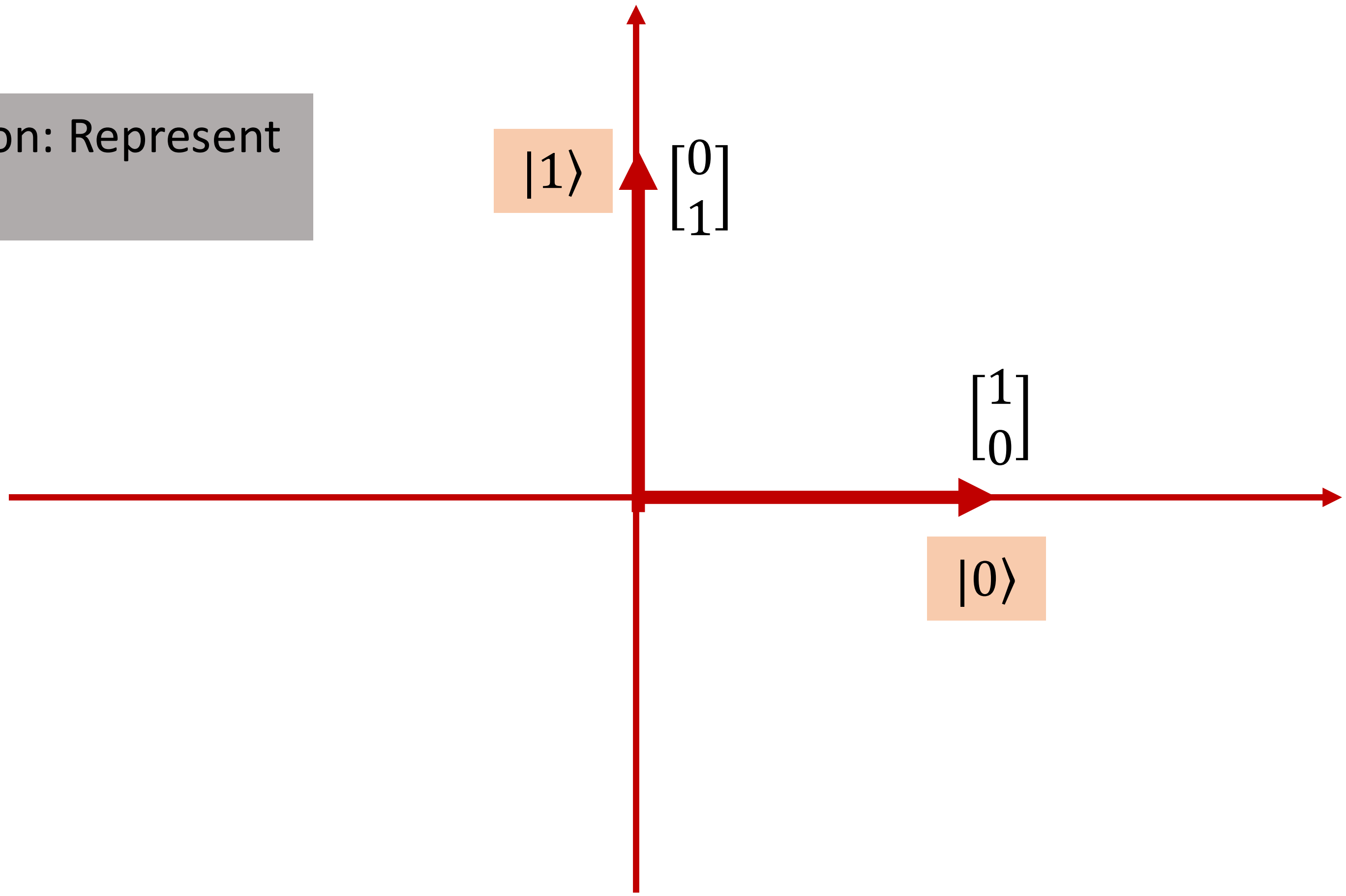
$$|-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$$

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

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

Bras, Kets, and vectors

Vector notation: Represent as vectors.



In bit bases:

$$|0\rangle = \begin{bmatrix}1\\0\end{bmatrix}$$

$$|1\rangle = \begin{bmatrix}0\\1\end{bmatrix}$$

The directions for $\begin{bmatrix}1\\0\end{bmatrix}$ and $\begin{bmatrix}0\\1\end{bmatrix}$ are implicitly the canonical bit bases

BRA – KET notation: Bases are represented using "BRA"s and "KET"s

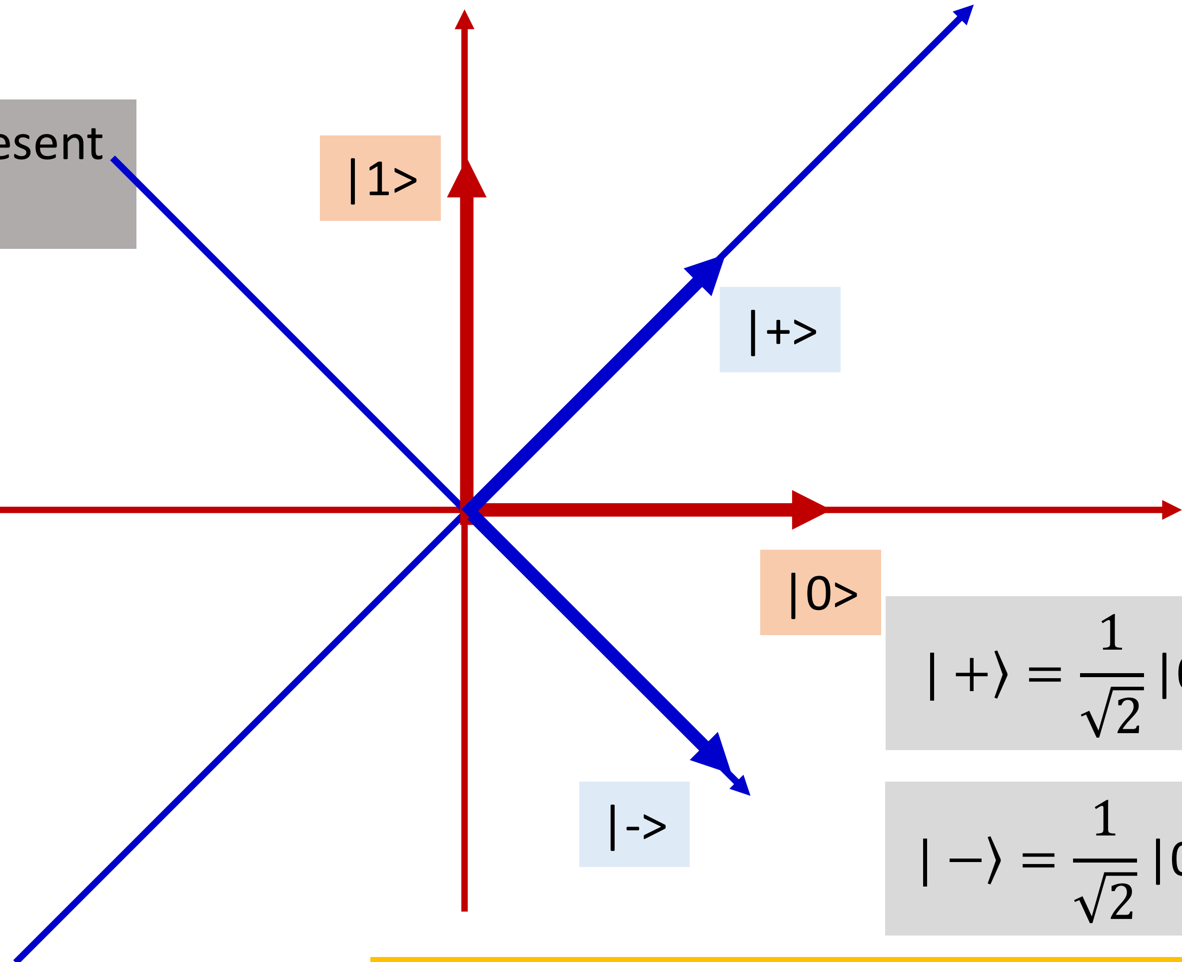
The term inside the Bra-ket is whatever we choose to notate it as, but represents a unit step in a direction

Bras, Kets, and vectors

Vector notation: Represent as vectors.

$$|+\rangle = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix}$$

$$|-\rangle = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{bmatrix}$$



In bit bases:

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

$$|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

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

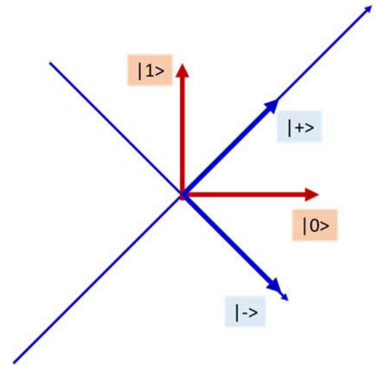
$$|-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$$

The directions for $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$ and $\begin{bmatrix} 0 \\ 1 \end{bmatrix}$ are implicitly the canonical bit bases

BRA – KET notation: Bases are represented using "BRA"s and "KET"s

The term inside the Bra-ket is whatever we choose to notate it as, but represents a unit step in a direction

Transforming bit bases to sign bases



Vector notation: Represent as vectors.

In bit bases:

$$|+\rangle = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix}$$

$$|-\rangle = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{bmatrix}$$

In bit bases:

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

$$|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

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

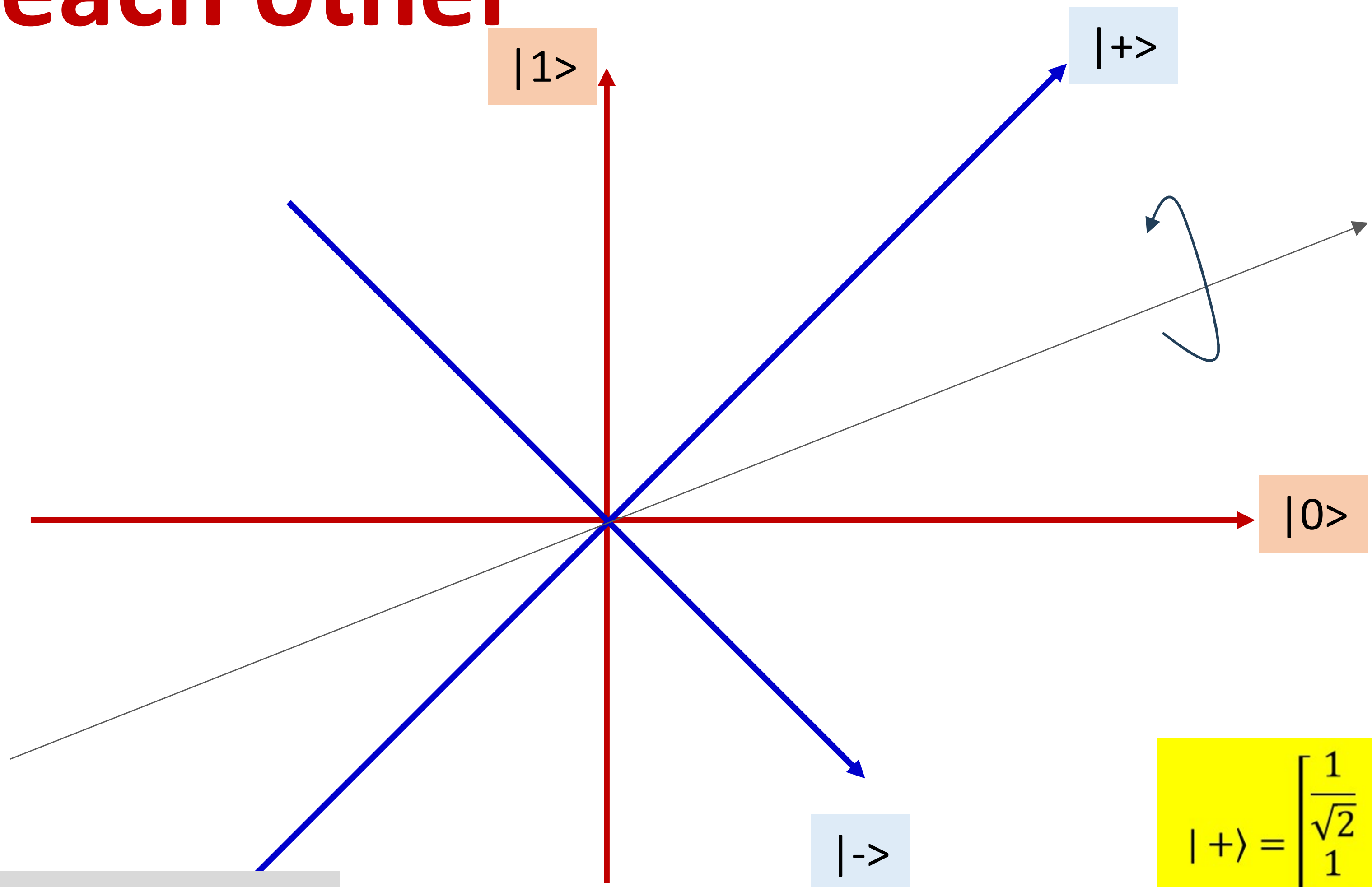
$$|-\rangle = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix} |1\rangle$$

The directions for $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$ and $\begin{bmatrix} 0 \\ 1 \end{bmatrix}$ are implicitly the canonical bit bases

We can rotate the bit bases into the sign bases

But how is this a rotation???

Bases can be expressed in terms of each other



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

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

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

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

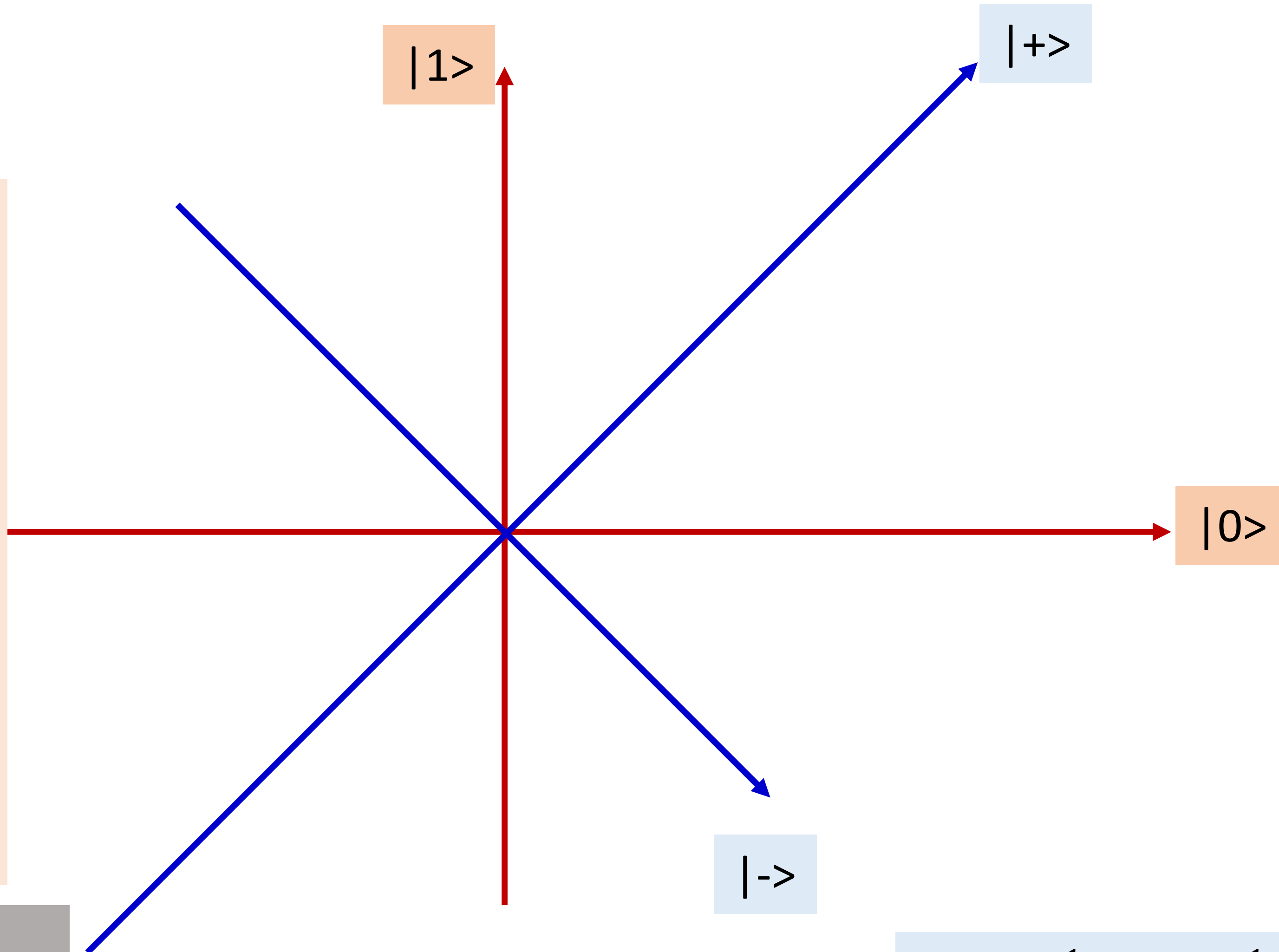
The other way…

In sign bases:

$$|1\rangle = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{bmatrix}$$

$$|0\rangle = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix}$$

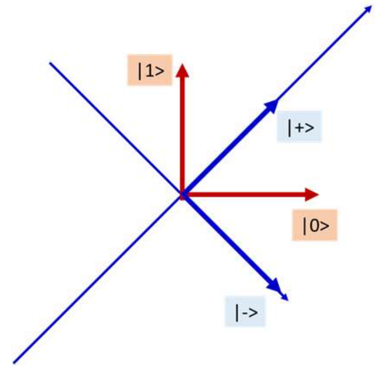
In terms of sign bases



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

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

Transforming bit bases to sign bases



Vector notation: Represent as vectors.

In sign bases:

$$|0\rangle = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix}$$

$$|1\rangle = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{bmatrix}$$

In sign bases:

$$|+\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

$$|-\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

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

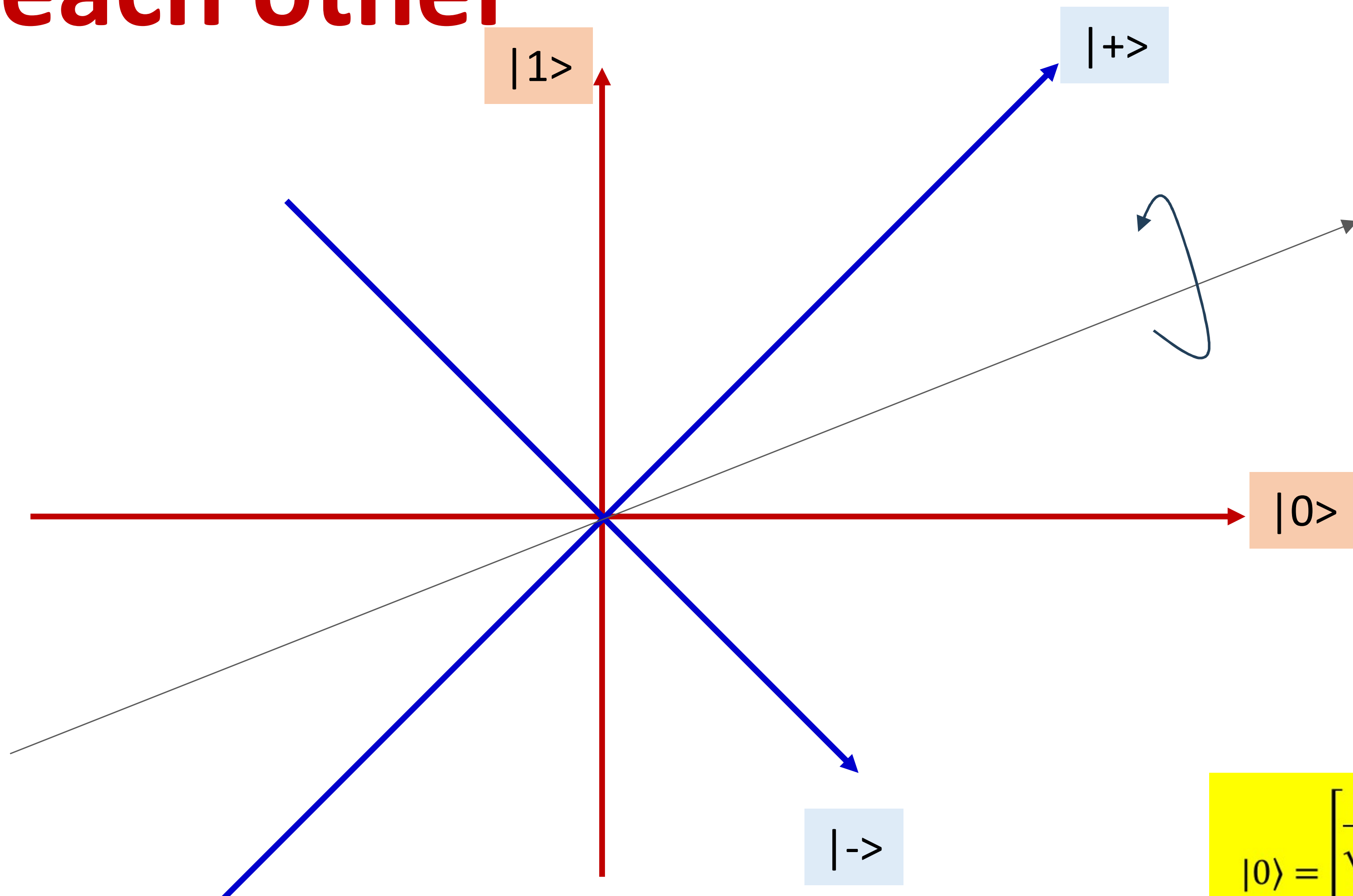
$$|1\rangle = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix} |-\rangle$$

The directions for $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$ and $\begin{bmatrix} 0 \\ 1 \end{bmatrix}$ are implicitly the canonical bit bases

We can rotate the bit bases into the sign bases

But how is this a rotation???
And how is it the *same* rotation that converted bit bases to sign bases?

Bases can be expressed in terms of each other



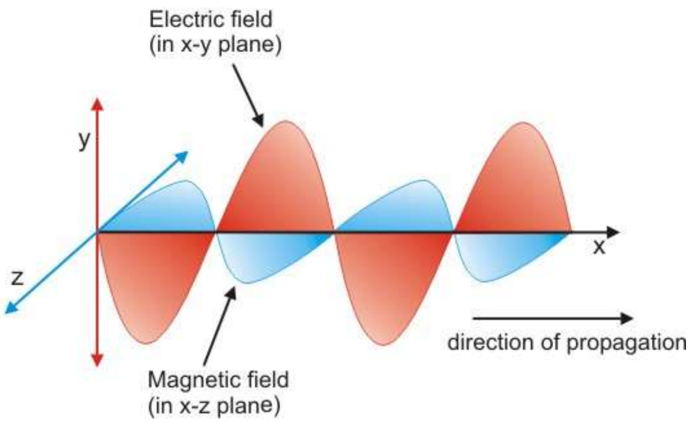
$$|0\rangle = \frac{1}{\sqrt{2}}|+\rangle + \frac{1}{\sqrt{2}}|-\rangle$$

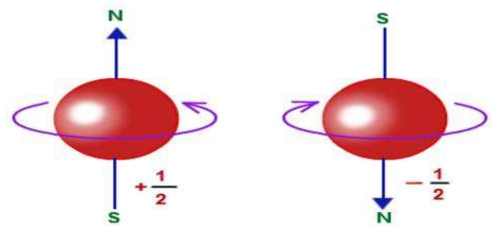
$$|1\rangle = \frac{1}{\sqrt{2}}|+\rangle - \frac{1}{\sqrt{2}}|-\rangle$$

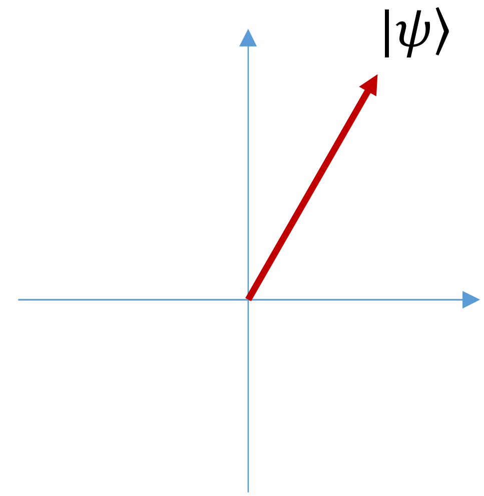
$$|0\rangle = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix} |+\rangle$$

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

The phasors are unique, but the representation is not





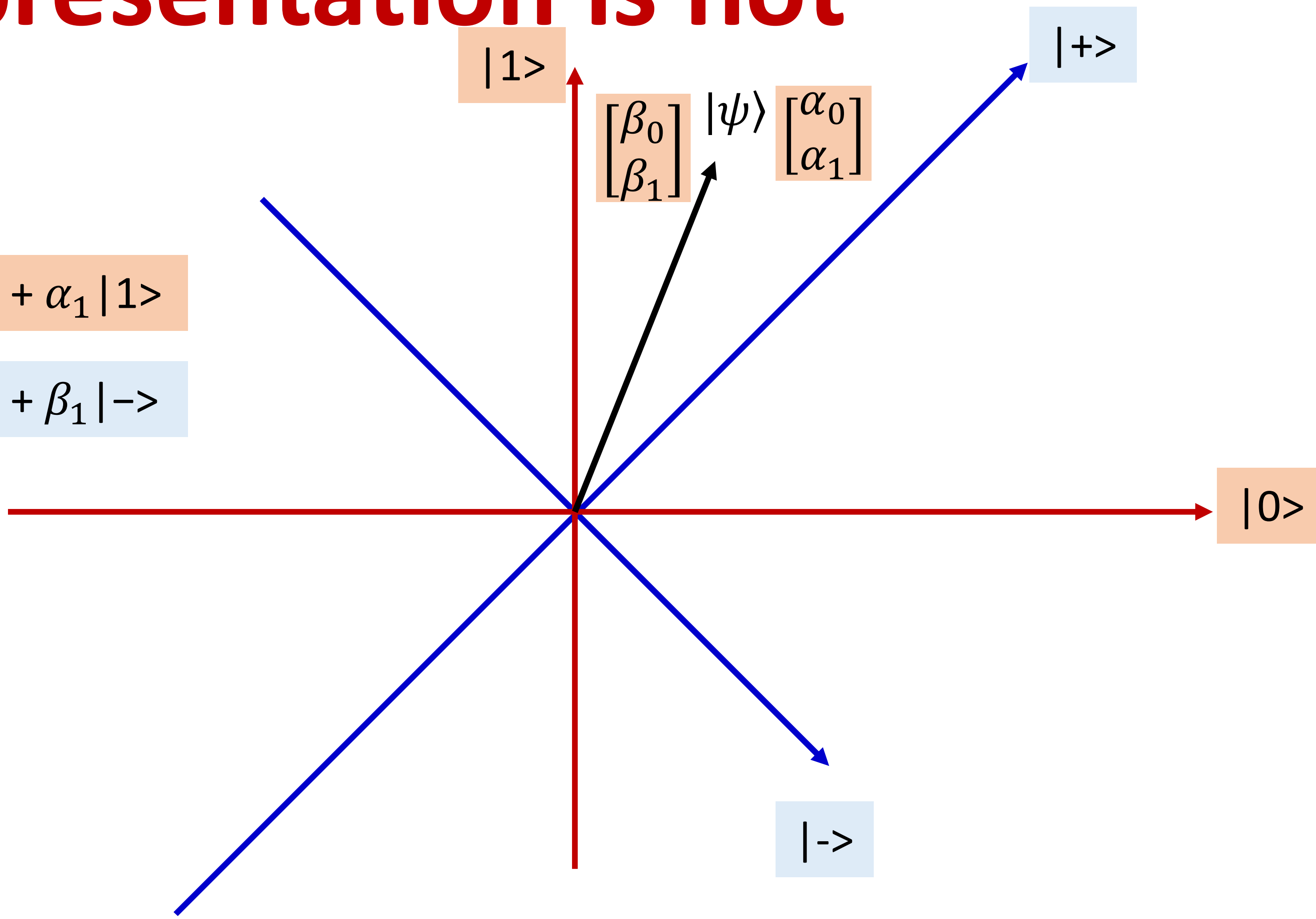


- The state of the system is absolute
  - The space is defined, and the direction of the (physical) phasor is well defined
- The actual representation depends on the bases used
  - Only restriction: the bases must be orthogonal

The phasors are unique, the representation is not

$|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$

$|\psi\rangle = \beta_0|+\rangle + \beta_1|-\rangle$



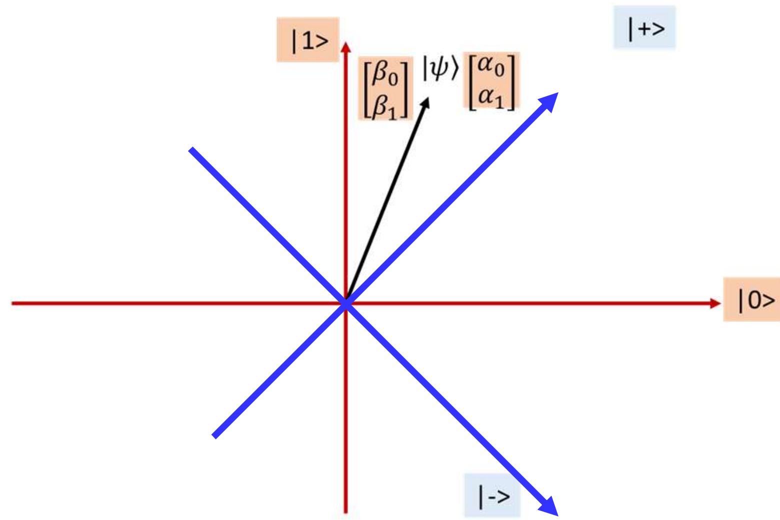
$\begin{bmatrix}\alpha_0\\ \alpha_1\end{bmatrix}$ $\begin{bmatrix}\beta_0\\ \beta_1\end{bmatrix}$

- The representation depends on the bases
    - Think orientation of your polarized glasses..
- What is the relationship twixt the two?

Changing bases

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

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

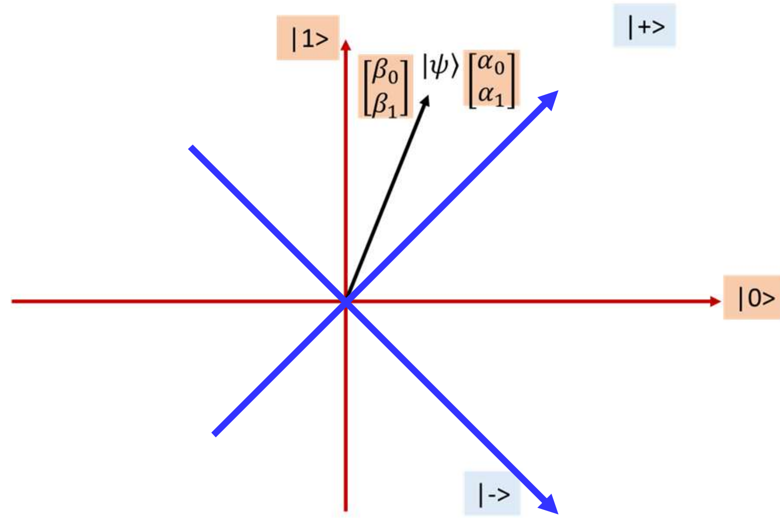


$$|\psi\rangle = \alpha_0|0> + \alpha_1|1>$$

Changing bases

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

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



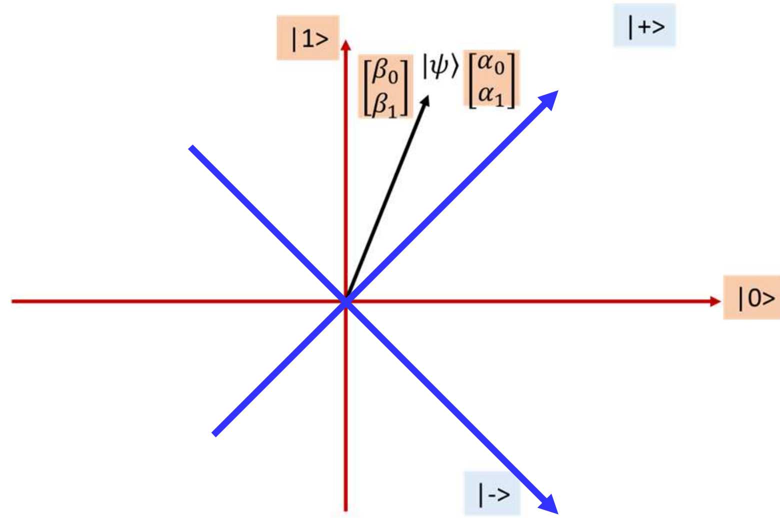
$$|\psi\rangle = \alpha_0|0> + \alpha_1|1>$$

$$= \alpha_0\left(\frac{1}{\sqrt{2}}|+> + \frac{1}{\sqrt{2}}|->\right) + \alpha_1\left(\frac{1}{\sqrt{2}}|+> - \frac{1}{\sqrt{2}}|->\right)$$

Changing bases

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

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



$$|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$$

$$= \alpha_0\left(\frac{1}{\sqrt{2}}|+\rangle + \frac{1}{\sqrt{2}}|-\rangle\right) + \alpha_1\left(\frac{1}{\sqrt{2}}|+\rangle - \frac{1}{\sqrt{2}}|-\rangle\right)$$

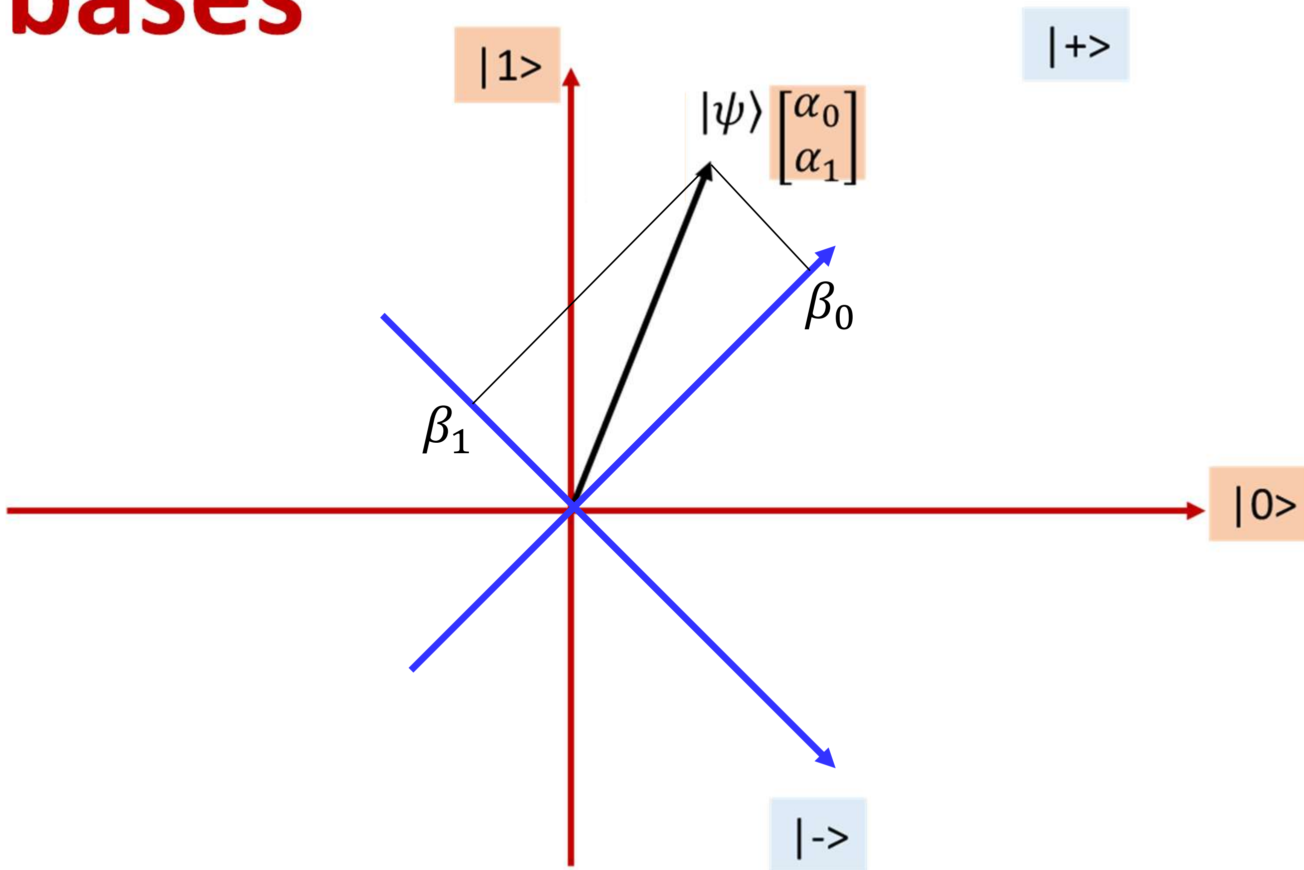
$$= \underbrace{\left(\frac{\alpha_0}{\sqrt{2}} + \frac{\alpha_1}{\sqrt{2}}\right)}_{\beta_0}|+\rangle + \underbrace{\left(\frac{\alpha_0}{\sqrt{2}} - \frac{\alpha_1}{\sqrt{2}}\right)}_{\beta_1}|-\rangle$$

Changing bases

In bit bases:

$$|+\rangle = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix}$$

$$|-\rangle = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{bmatrix}$$

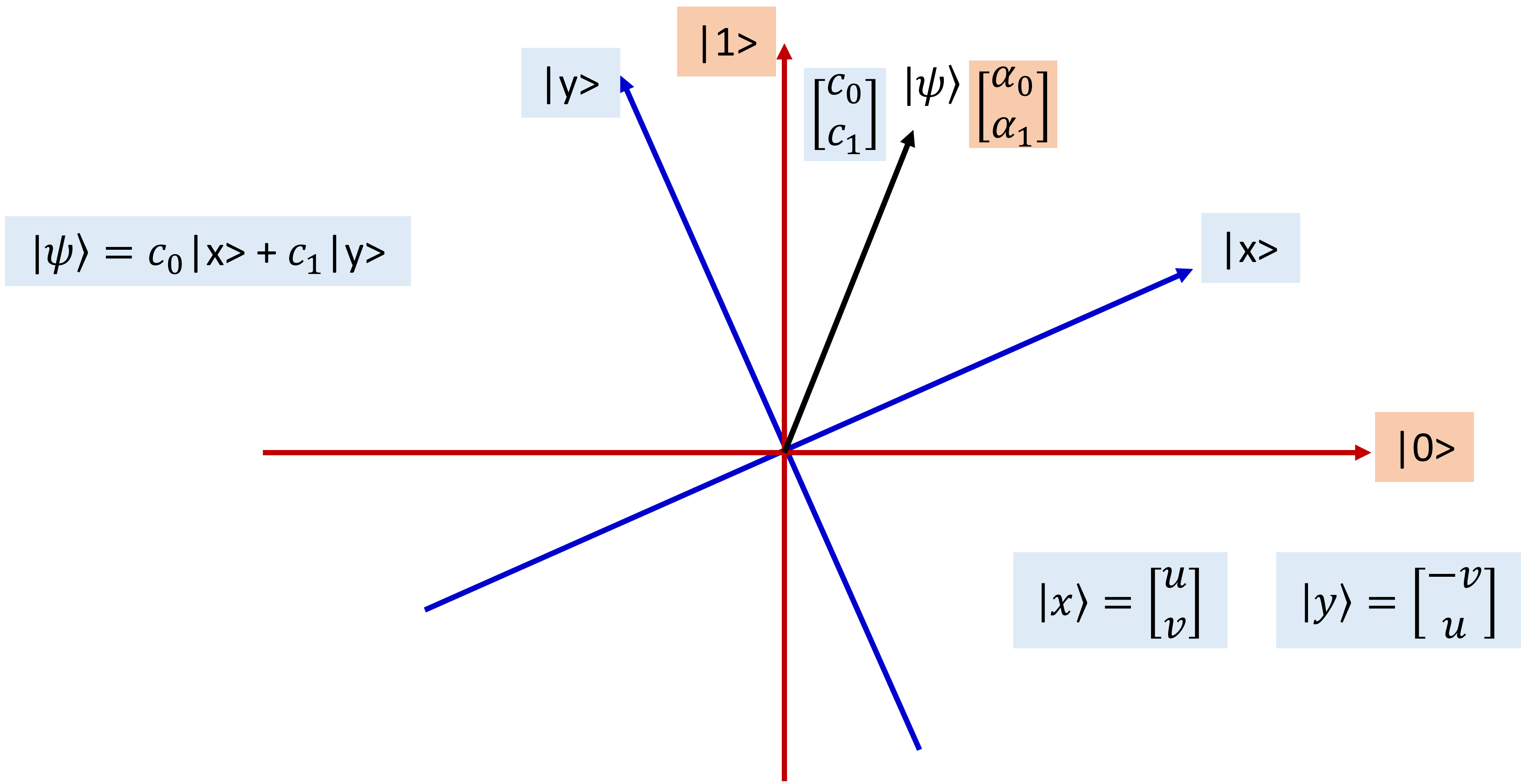


$$\beta_0 = \left(\frac{\alpha_0}{\sqrt{2}} + \frac{\alpha_1}{\sqrt{2}}\right) = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix}^H \begin{bmatrix} \alpha_0 \\ \alpha_1 \end{bmatrix}$$

$$\beta_1 = \left(\frac{\alpha_0}{\sqrt{2}} - \frac{\alpha_1}{\sqrt{2}}\right) = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{bmatrix}^H \begin{bmatrix} \alpha_0 \\ \alpha_1 \end{bmatrix}$$

The weights are simply projections on the bases

What about these bases?



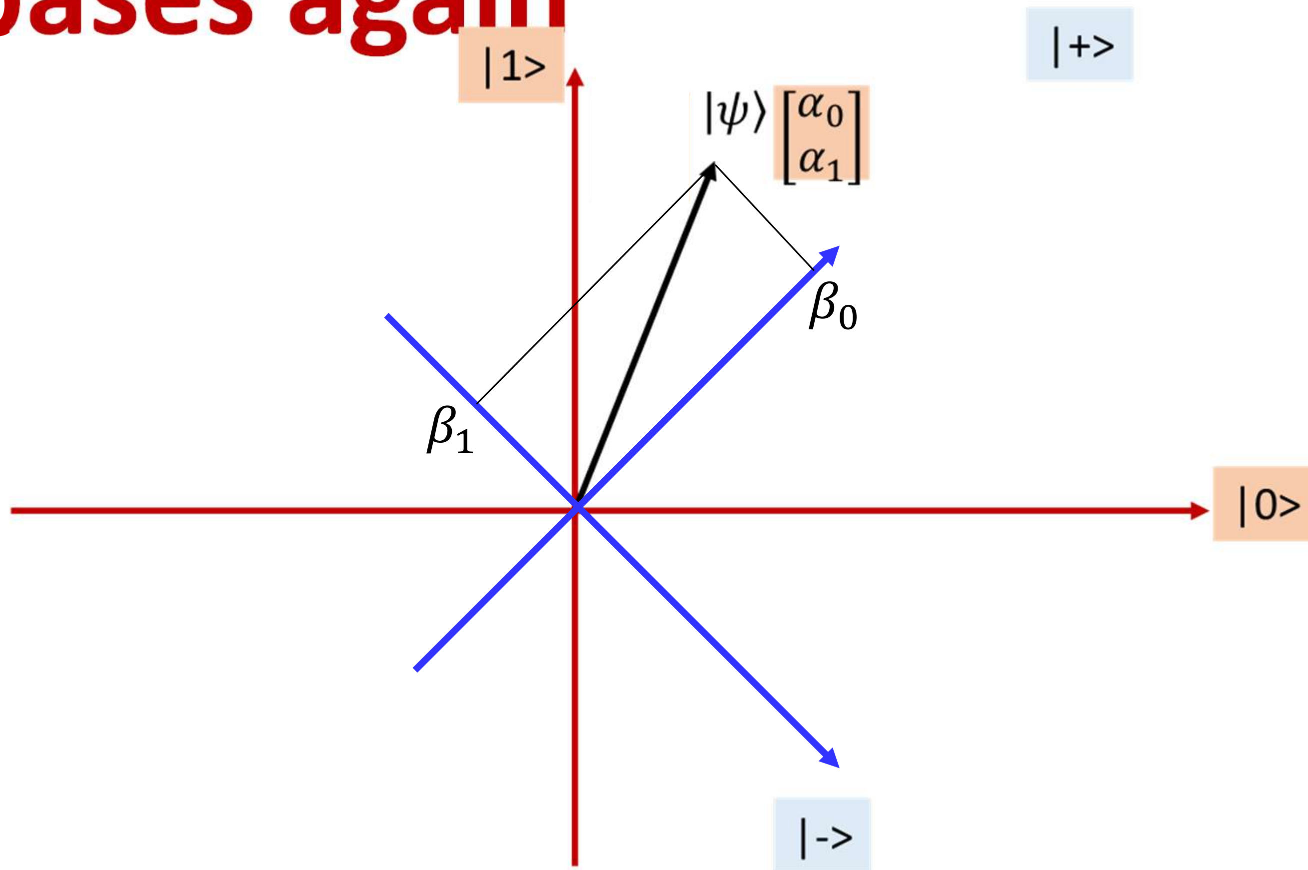
- What are c_0 and c_1?

The sign bases again

In bit bases:

$$|+\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix}$$

$$|-\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\-1\end{bmatrix}$$



$$\beta_0 = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix}^H \begin{bmatrix}\alpha_0\\\alpha_1\end{bmatrix} \qquad \beta_1 = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\-1\end{bmatrix}^H \begin{bmatrix}\alpha_0\\\alpha_1\end{bmatrix}$$

$$\begin{bmatrix}\beta_0\\\beta_1\end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\1 & -1\end{bmatrix}\begin{bmatrix}\alpha_0\\\alpha_1\end{bmatrix}$$

The transformation is a matrix
The rows of the matrix are the bases (conjugated)

Changing Bases

$$\begin{bmatrix} \beta_0 \\ \beta_1 \end{bmatrix} = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix} \begin{bmatrix} \alpha_0 \\ \alpha_1 \end{bmatrix}$$

$$\begin{bmatrix} \alpha_0 \\ \alpha_1 \end{bmatrix} = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix} \begin{bmatrix} \beta_0 \\ \beta_1 \end{bmatrix}$$

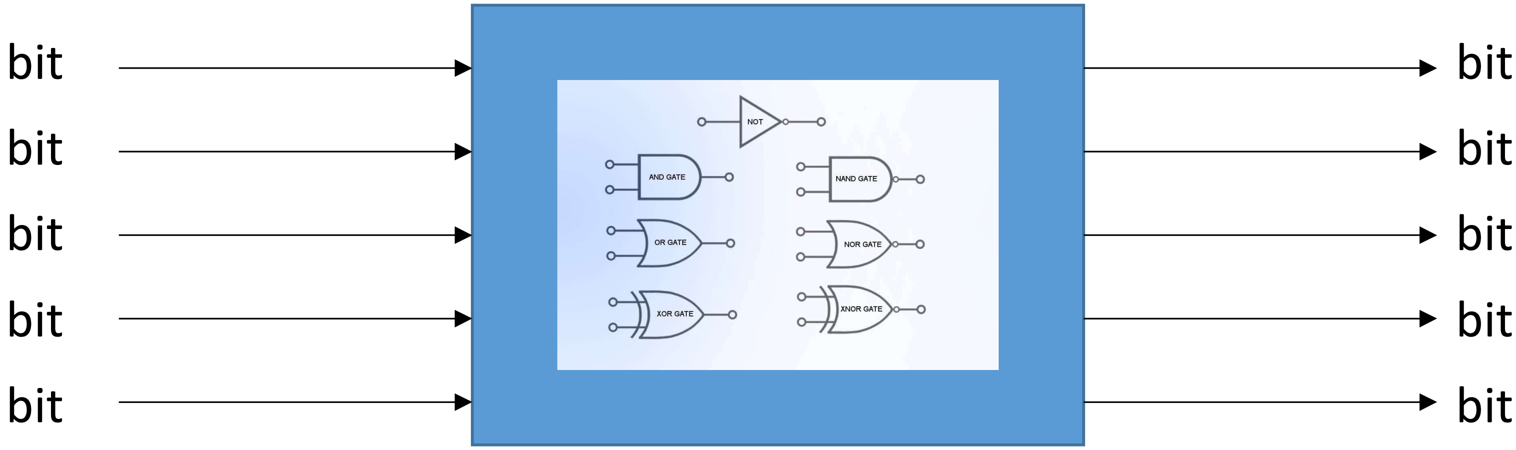
- Change of bases is a matrix transform

Moving on…

- We have a physical framework which can represent bit combinations in the new math

- Next step: We must *compute* with it

Classical computation



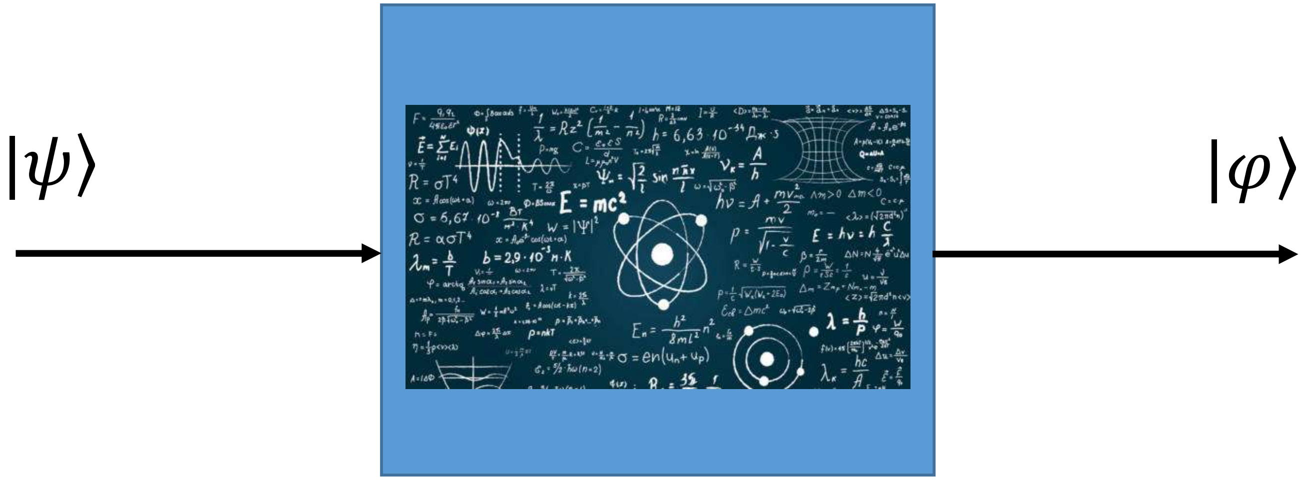
- A box that performs a computation
  - Takes in a collection of bits, outputs one or more bits
- The box is composed of gates
  - Binary gates: 2 inputs, one output
  - Large fan-in gates: many inputs one output
- Objective in design
  - **Ensure the output is always right**
  - **Minimize the number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

Note: You can do it all using only NAND gates

(but may need an exponential number of them)

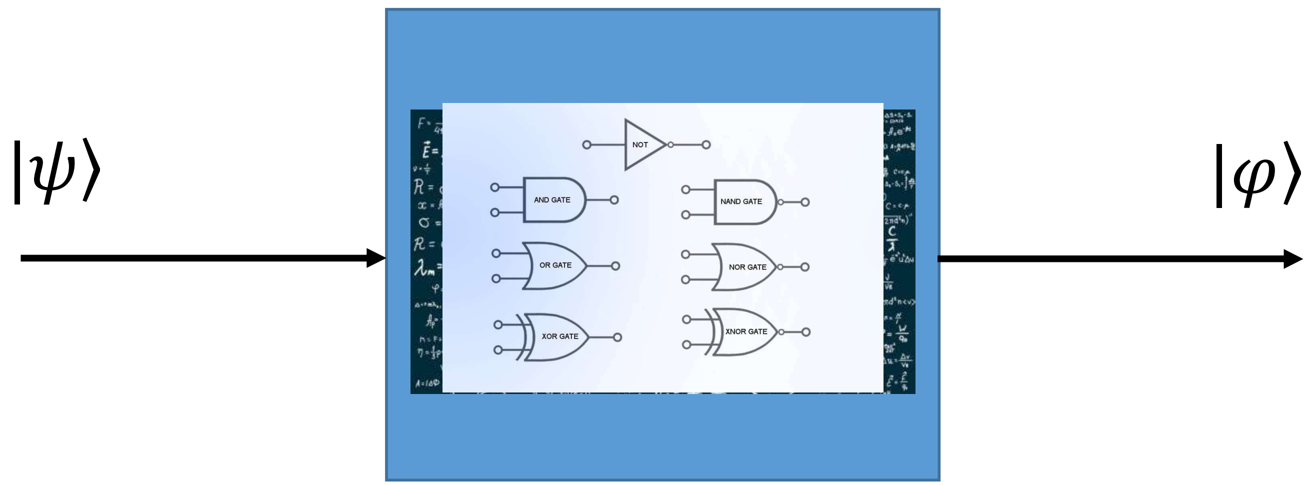
NAND is a universal gate

Quantum computation



- A box that performs a computation
  - Takes in a high-dimensional phasor
    - A phasor in a high-dimensional complex Hilbert space
  - Outputs a high-dimensional phasor
    - In the same space as the input

Quantum computation



- A box that performs a computation
  - Takes in a high-dimensional phasor
    - A phasor in a high-dimensional complex Hilbert space
  - Outputs a high-dimensional phasor
    - In the same space as the input
- The box too is composed of computations that are analogous to the Boolean operations and gates

We've learned about bits, what about Gates?

- How does one manipulate the qubits

We've learned about bits, what about gates?

- Simplest gate: The Boolean 1-bit gate
  - How many 1-bit gates can you have?

- How many of these are implementable for the quantum bit?
  - Why

- What do they look like?

Poll 3

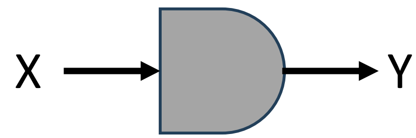
- How many different 1-bit gates exist
  - 1
  - 2
  - 3
  - 4

Poll 3

- How many different 1-bit gates exist
  - 1
  - 2
  - 3
  - **4**

One bit gate

Input	Output
0	
1	



How many different ways can we assign the output?

- A Boolean Gate is just a truth table
  - Corresponding to each Boolean value of the input is a Boolean output

One bit gate

Input	Output
0	0
1	1

Identity

Input	Output
0	1
1	0

Negation

Input	Output
0	0
1	0

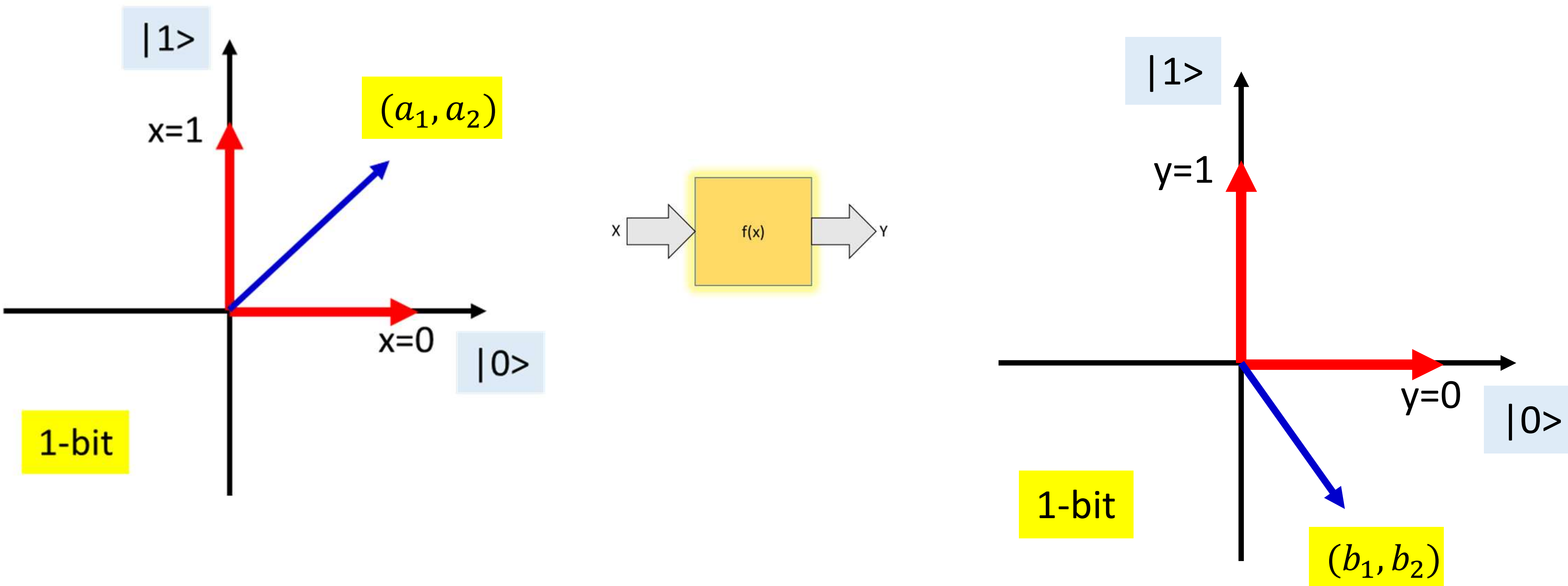
False

Input	Output
0	1
1	1

True

- A Boolean Gate is just a truth table
    - Corresponding to each Boolean value of the input is a Boolean output
- How many of these can be implemented in quantum?

Recall: The new “quantum” math



- A gate is just an operator (like any algorithm)
- Caveats – the operator must be:
  - Linear
  - Invertible
  - And not increase the length of the vector (i.e. it must be unitary)

One bit gate

Not invertible

Input	Output
0	0
1	1

Identity

Input	Output
0	1
1	0

Negation

Input	Output
0	0
1	0

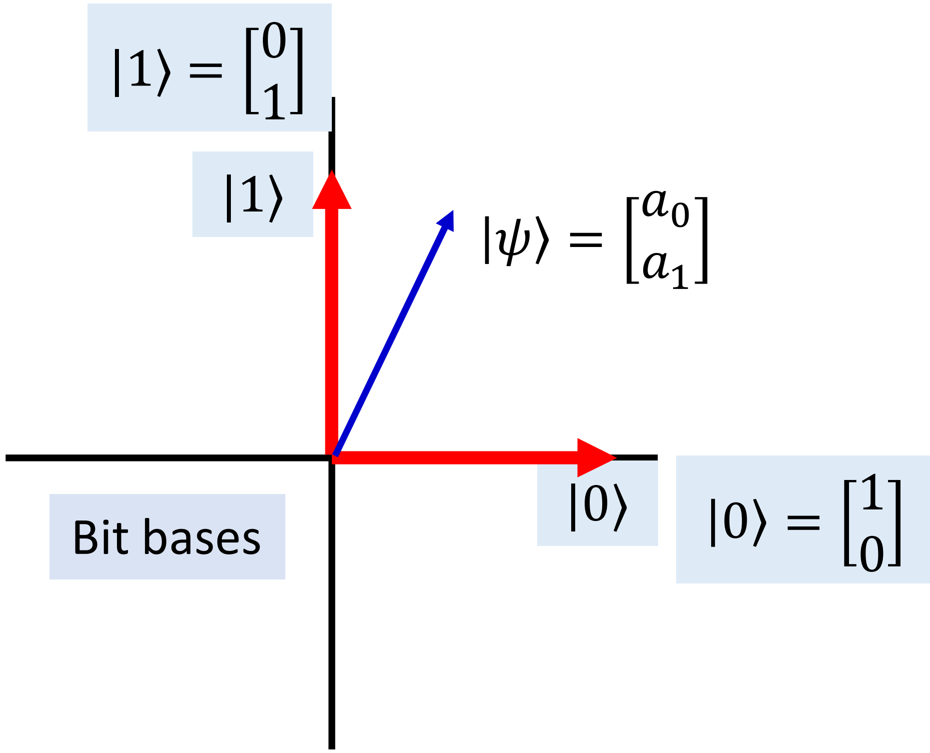
False

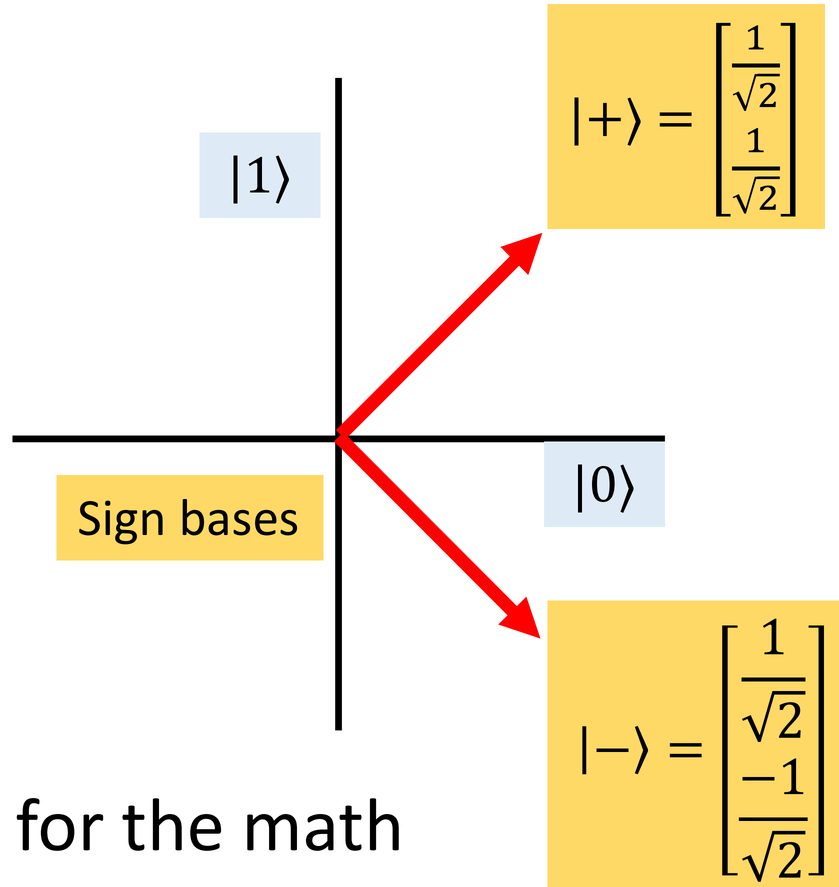
Input	Output
0	1
1	1

True

- A Boolean Gate is just a truth table
  - Corresponding to each Boolean value of the input is a Boolean output
- How many of these can be implemented in quantum?

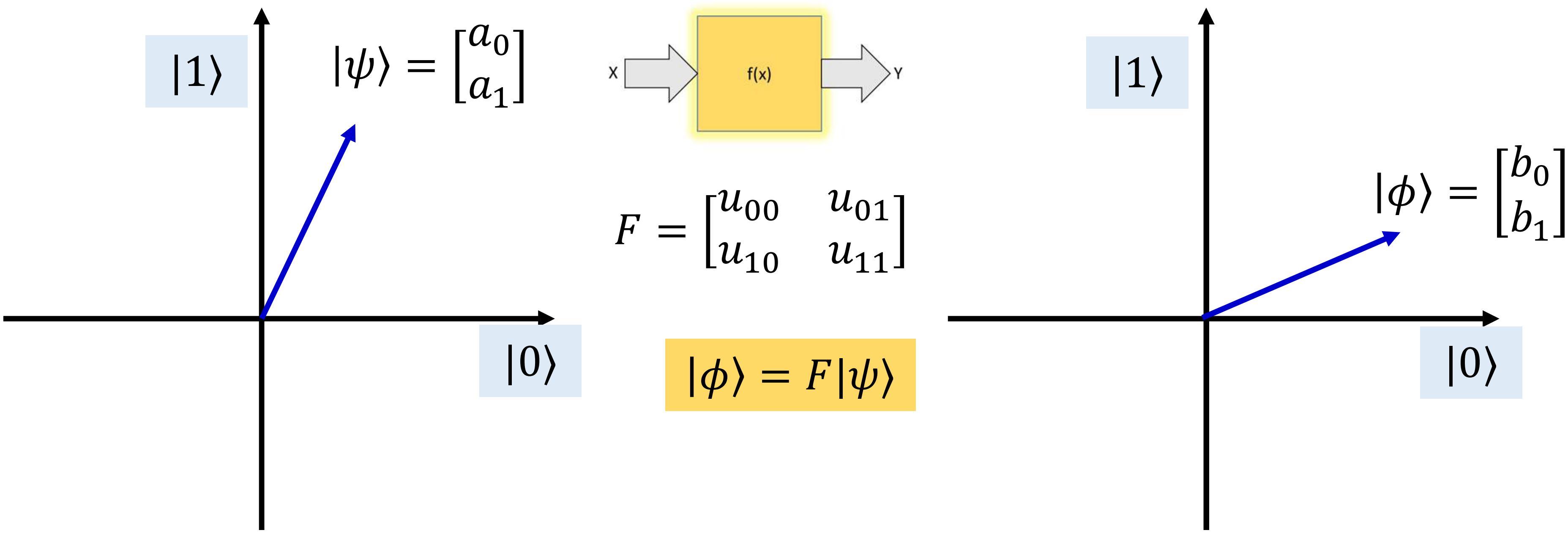
First – representing (Qu)bits





- We will use the vector notation for the math
  - Nothing sacrosanct about it; it just makes it easier to explain the operations
- Each value for the qubit is a unit vector

Gates and other operators are matrix transforms



$$|\psi\rangle = \begin{bmatrix} a_0 \\ a_1 \end{bmatrix}$$

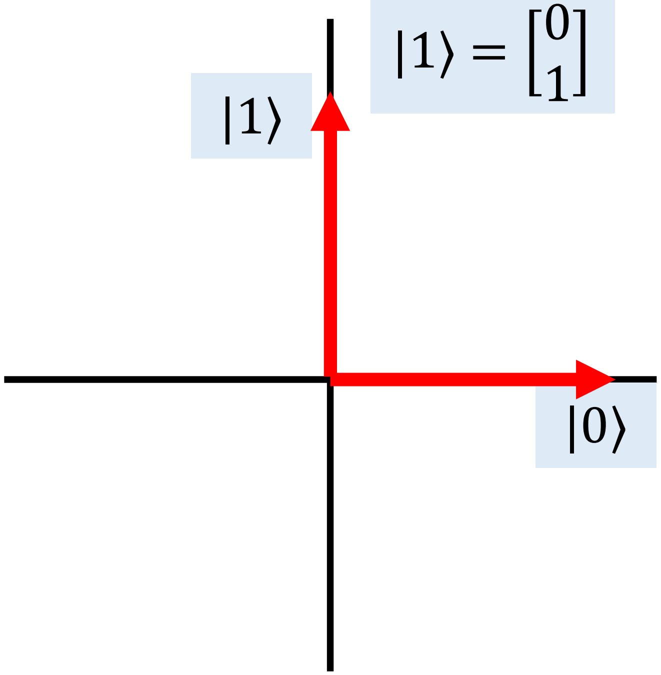
$$F = \begin{bmatrix} u_{00} & u_{01} \\ u_{10} & u_{11} \end{bmatrix}$$

$$|\phi\rangle = F|\psi\rangle$$

$$|\phi\rangle = \begin{bmatrix} b_0 \\ b_1 \end{bmatrix}$$

- Quantum circuits are operators that operate on the input phasor/vector (superposition of states) and generate the output phasor/vector
- These can be expressed as matrices that transform the input vector to the output vector
- *Gates* are just very simple circuits
  - One-qubit gates are 2x2 unitary matrices that convert the two-dimensional input phasor (representing a qubit in a superposition of 2 states) to a two-dimensional output phasor

The one-qubit identity gate



$|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$

$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$

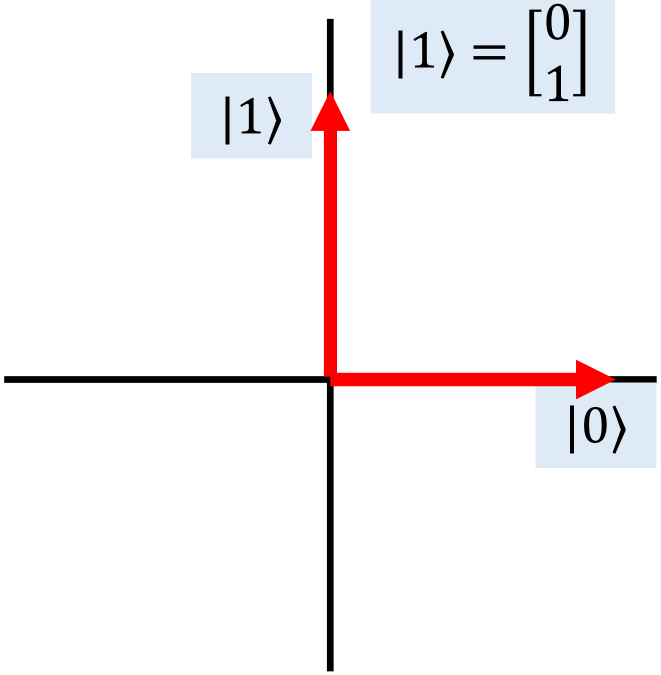
$|1\rangle \rightarrow |1\rangle \Rightarrow \begin{bmatrix} 0 \\ 1 \end{bmatrix} \rightarrow \begin{bmatrix} 0 \\ 1 \end{bmatrix}$

$|0\rangle \rightarrow |0\rangle \Rightarrow \begin{bmatrix} 1 \\ 0 \end{bmatrix} \rightarrow \begin{bmatrix} 1 \\ 0 \end{bmatrix}$

What kind of transform keeps the vector unchanged?

- The identity gate does not change the bit value

The one-qubit identity gate

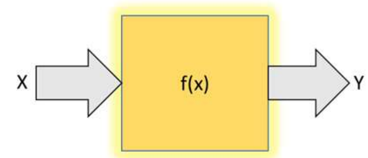


$$|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

$$|1\rangle \rightarrow |1\rangle \Rightarrow \begin{bmatrix} 0 \\ 1 \end{bmatrix} \rightarrow \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

$$|0\rangle \rightarrow |0\rangle \Rightarrow \begin{bmatrix} 1 \\ 0 \end{bmatrix} \rightarrow \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$



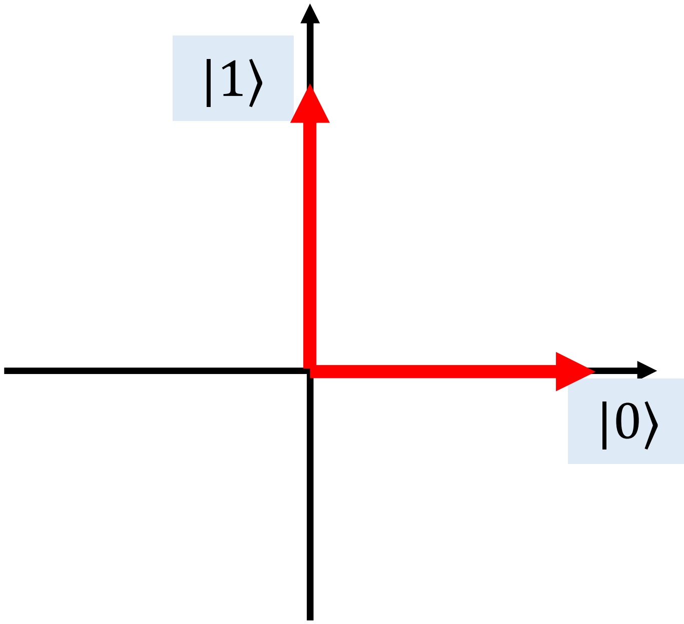
$$F = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

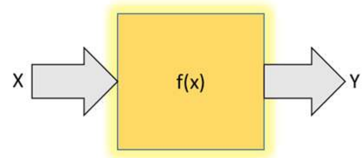
- The identity gate does not change the bit value

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

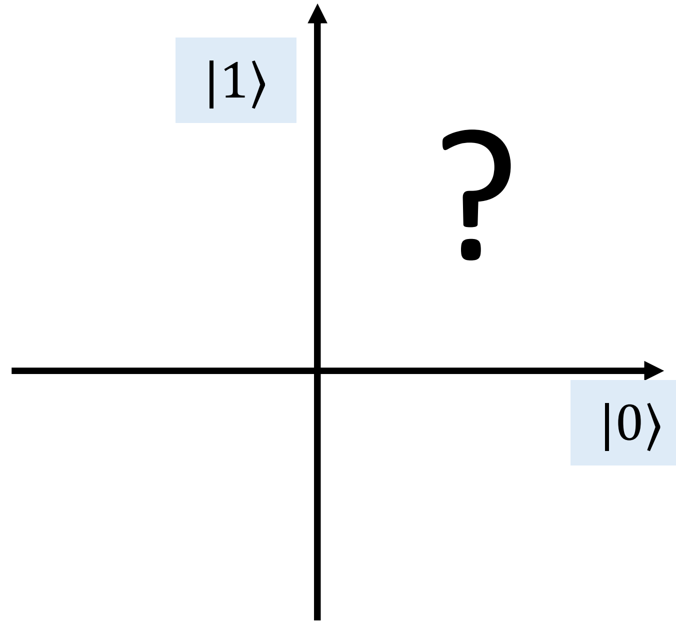
$$F \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

The one-qubit identity gate



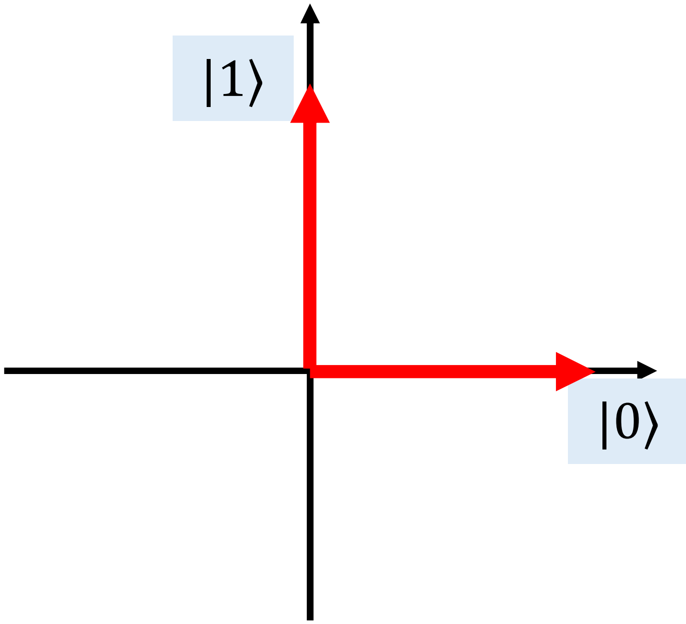


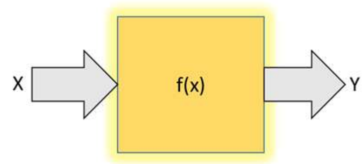
$$F = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$



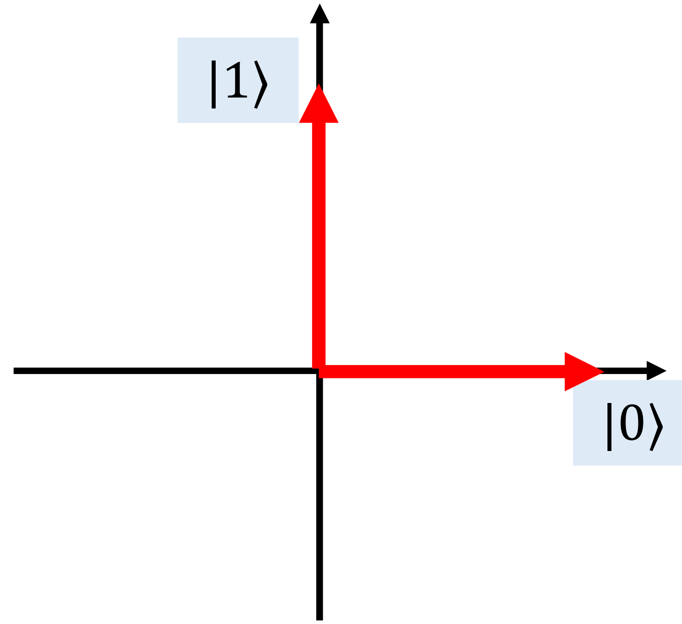
- The one-bit identity gate is an identity transform
  - How does it affect $|0\rangle$ and $|1\rangle$?

The one-qubit identity gate



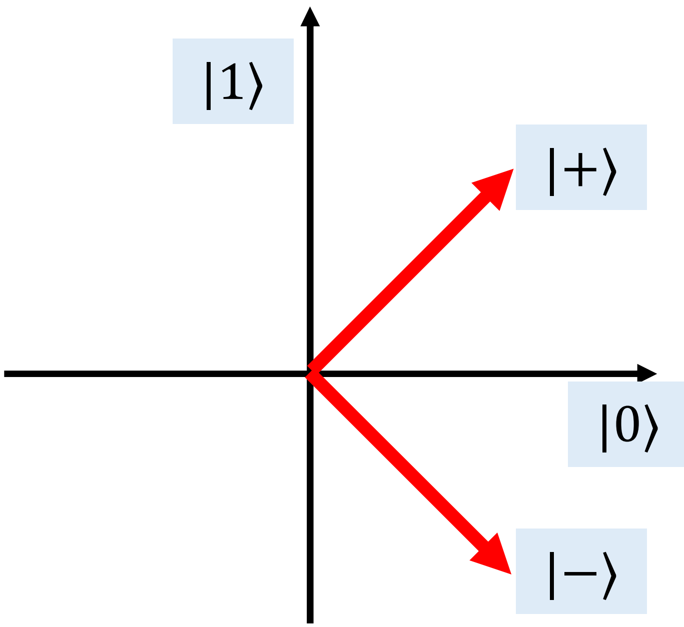


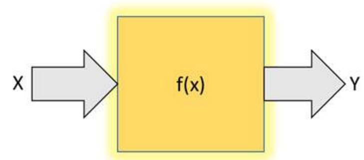
$$F = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$



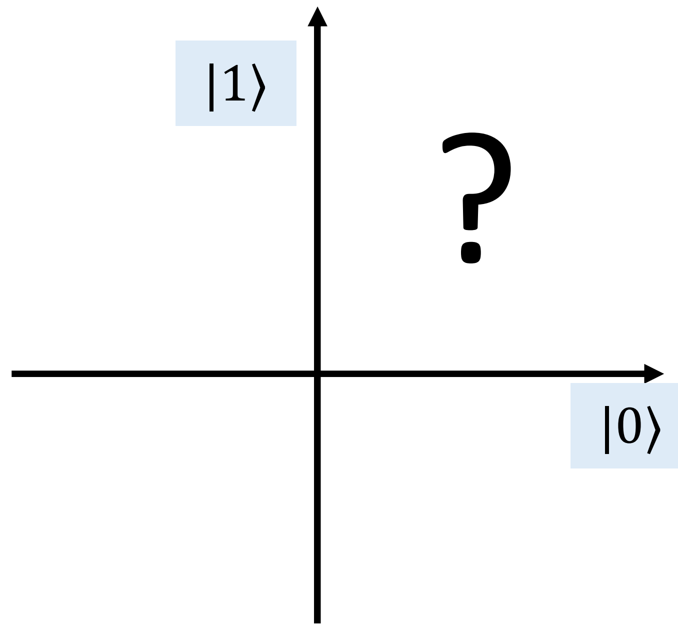
- The one-bit identity gate is an identity transform
  - How does it affect $|0\rangle$ and $|1\rangle$?

The one-qubit identity gate



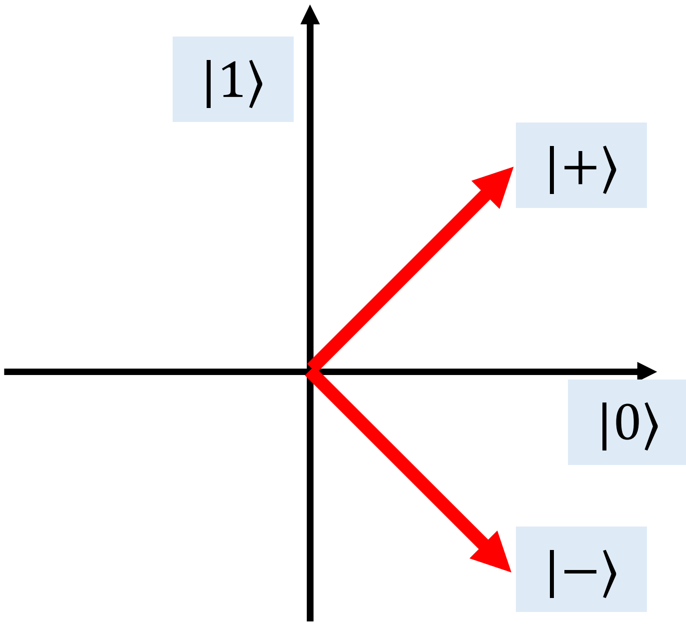


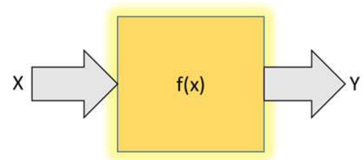
$$F = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$



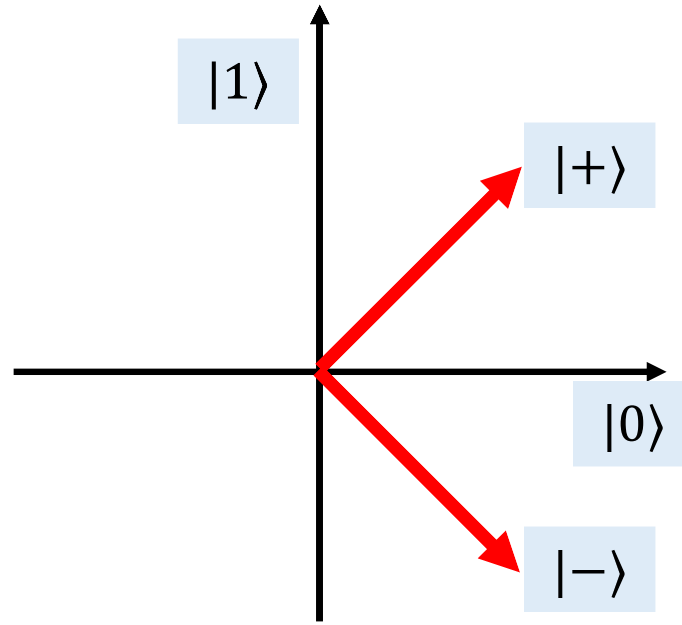
- The one-bit identity gate is an identity transform
  - How does it affect $|0\rangle$ and $|1\rangle$?
  - How does it affect $|+\rangle$ and $|-\rangle$?

The one-qubit identity gate



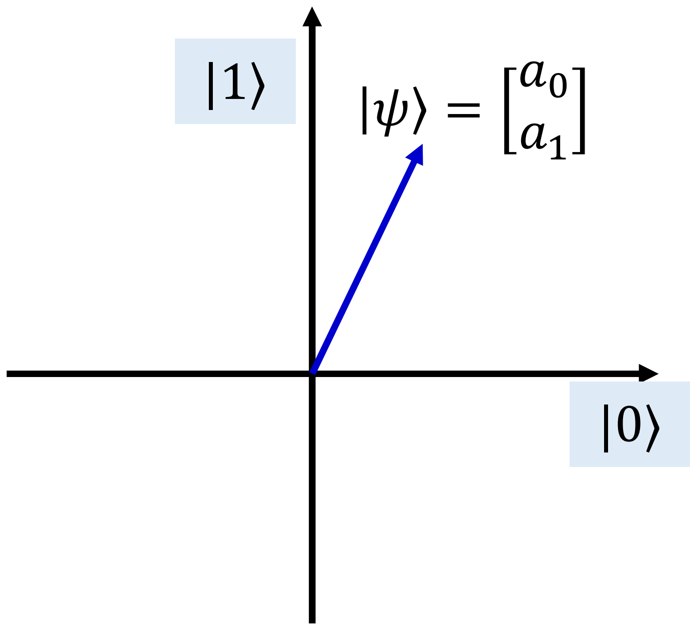


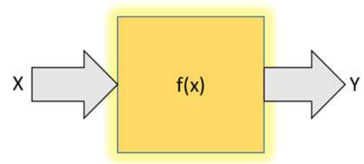
$$F = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$



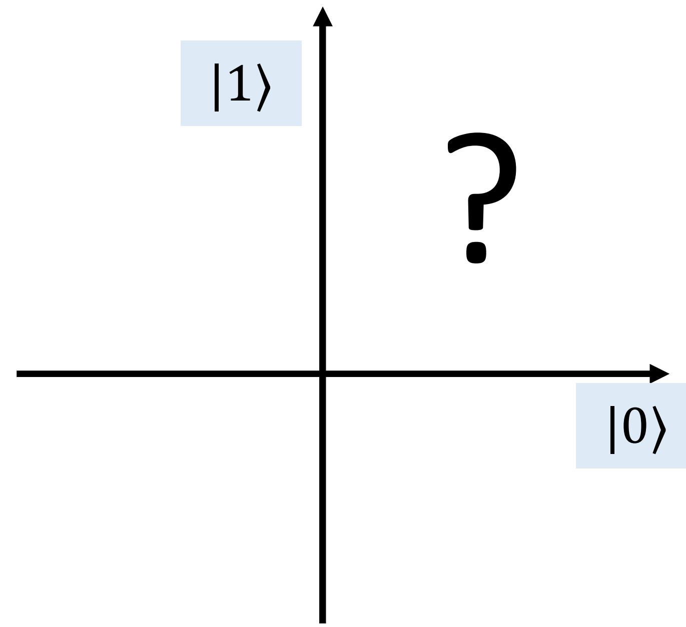
- The one-bit identity gate is an identity transform
  - How does it affect $|0\rangle$ and $|1\rangle$?
  - How does it affect $|+\rangle$ and $|-\rangle$?

The one-qubit identity gate



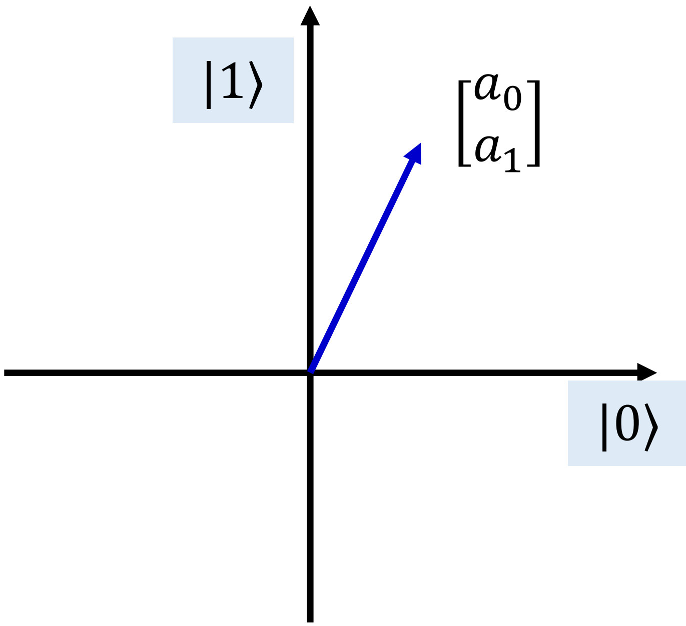


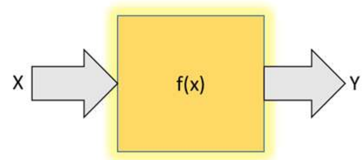
$$F = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$



- The one-bit identity gate is an identity transform
  - How does it affect $|0\rangle$ and $|1\rangle$?
  - How does it affect $|+\rangle$ and $|-\rangle$?
  - How does it affect a generic qubit in superposition: $|\psi\rangle = a_0|0\rangle + a_1|1\rangle$

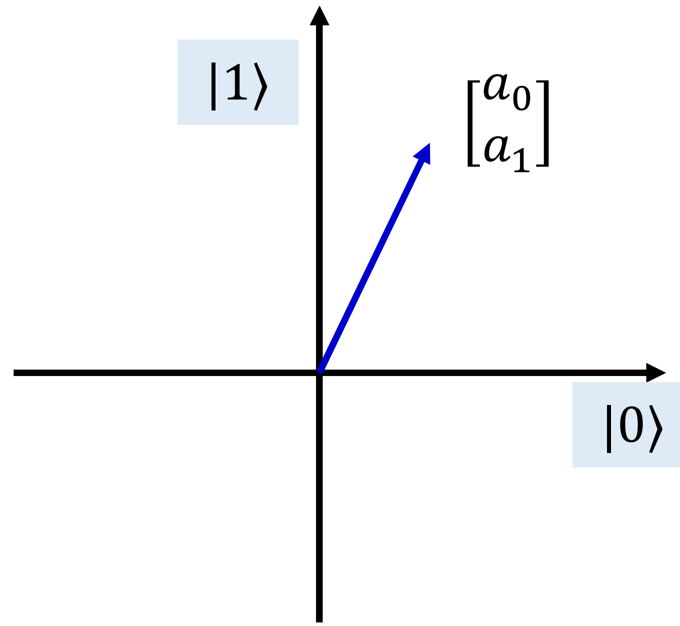
The one-qubit identity gate





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

$$F|\psi\rangle = |\psi\rangle$$



- The one-bit identity gate is an identity transform
  - How does it affect $|0\rangle$ and $|1\rangle$?
  - How does it affect $|+\rangle$ and $|-\rangle$?
  - How does it affect a generic qubit in superposition: $|\psi\rangle = a_0|0\rangle + a_1|1\rangle$

One bit inversion gate

Not invertible

Input	Output
0	0
1	1

Identity

Input	Output
0	1
1	0

Negation

Input	Output
0	0
1	0

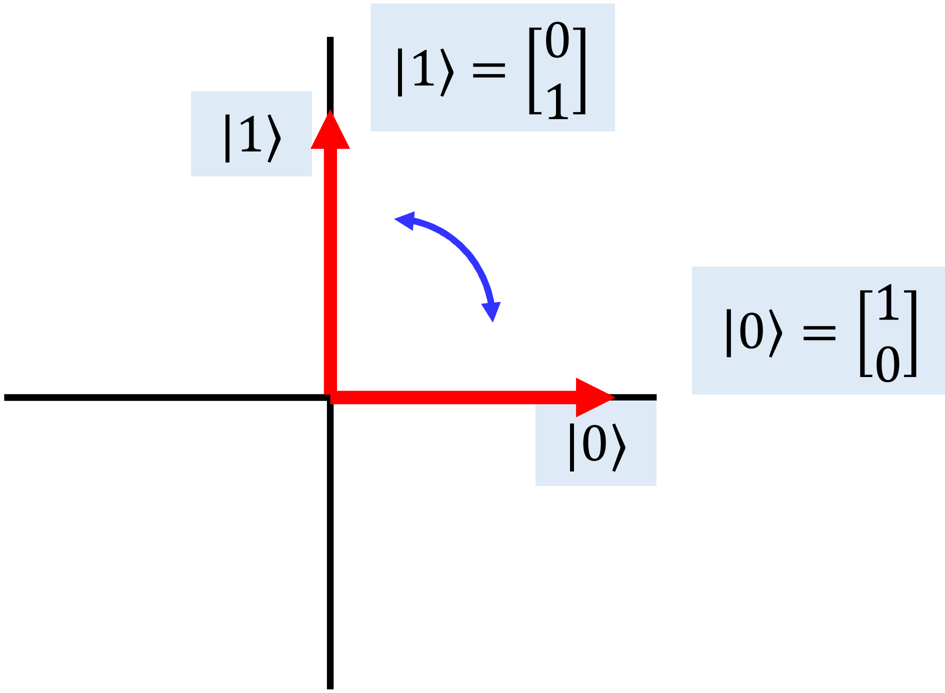
False

Input	Output
0	1
1	1

True

- The inversion/negation gate flips the bit value

The one-qubit *inversion* gate



$$|1\rangle \rightarrow |0\rangle \Rightarrow \begin{bmatrix} 0 \\ 1 \end{bmatrix} \rightarrow \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

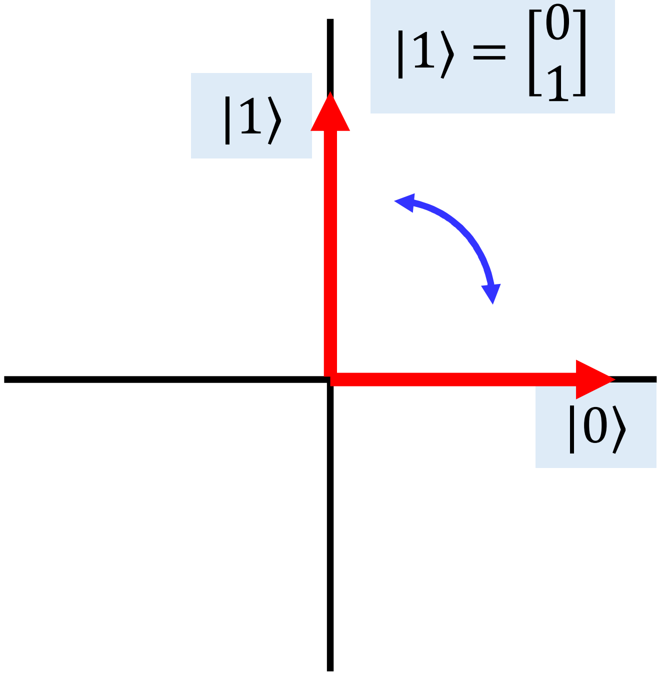
$$|0\rangle \rightarrow |1\rangle \Rightarrow \begin{bmatrix} 1 \\ 0 \end{bmatrix} \rightarrow \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

What kind of transform flips the axis vectors in this manner?

- The *bit-inversion* gate is the quantum equivalent of the Boolean NOT
- It flips a $|1\rangle$ to a $|0\rangle$ and vice versa

The one-qubit *inversion* gate

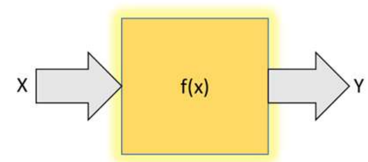
$$|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$



$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

$$|1\rangle \rightarrow |0\rangle \Rightarrow \begin{bmatrix} 0 \\ 1 \end{bmatrix} \rightarrow \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

$$|0\rangle \rightarrow |1\rangle \Rightarrow \begin{bmatrix} 1 \\ 0 \end{bmatrix} \rightarrow \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$



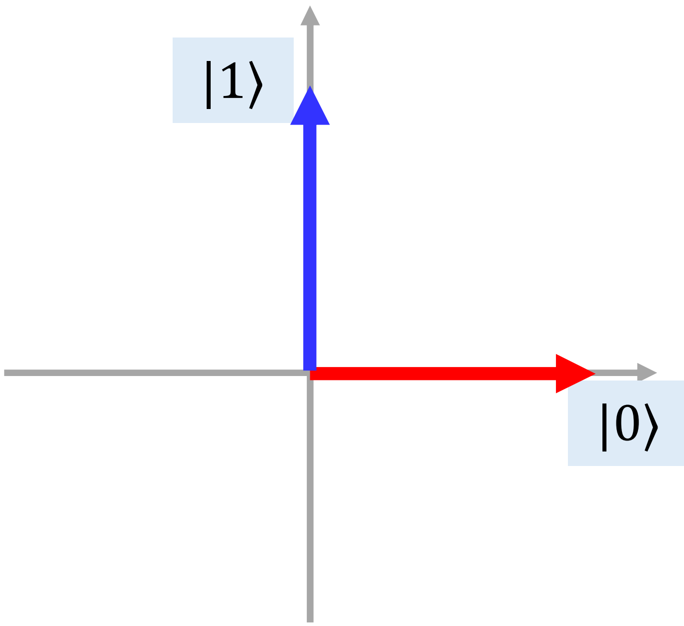
$$F = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

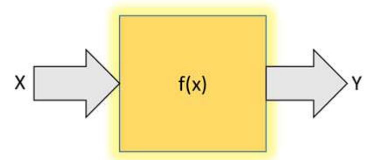
- The *bit-inversion* gate is the quantum equivalent of the Boolean NOT
- It flips a $|1\rangle$ to a $|0\rangle$ and vice versa

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

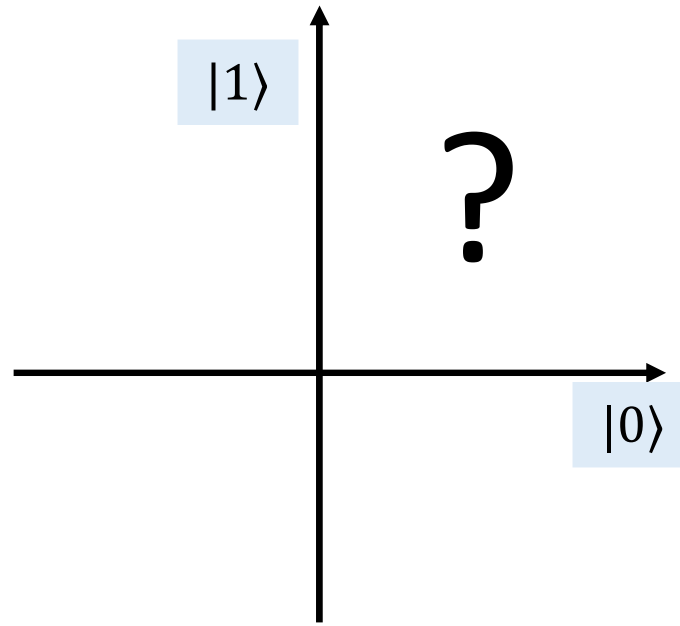
$$F \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

The one-qubit inversion gate



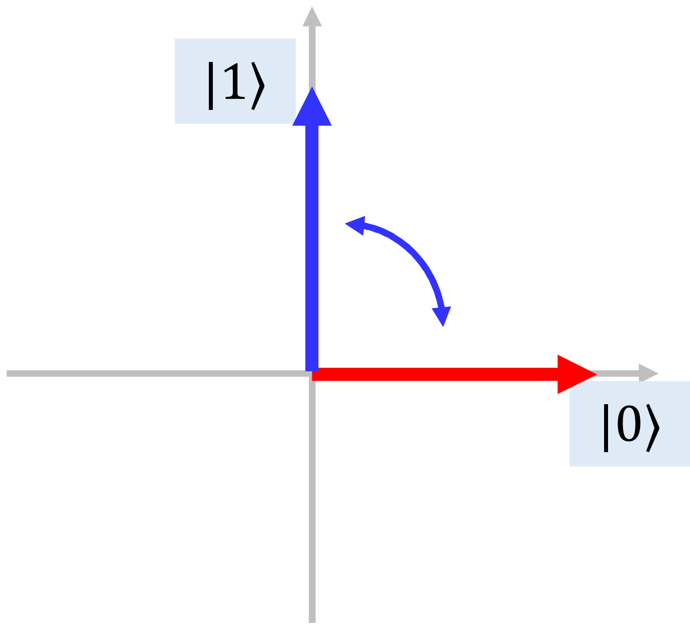


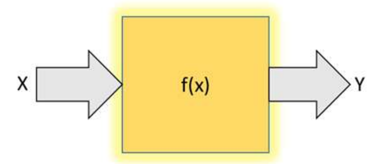
$$F = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$



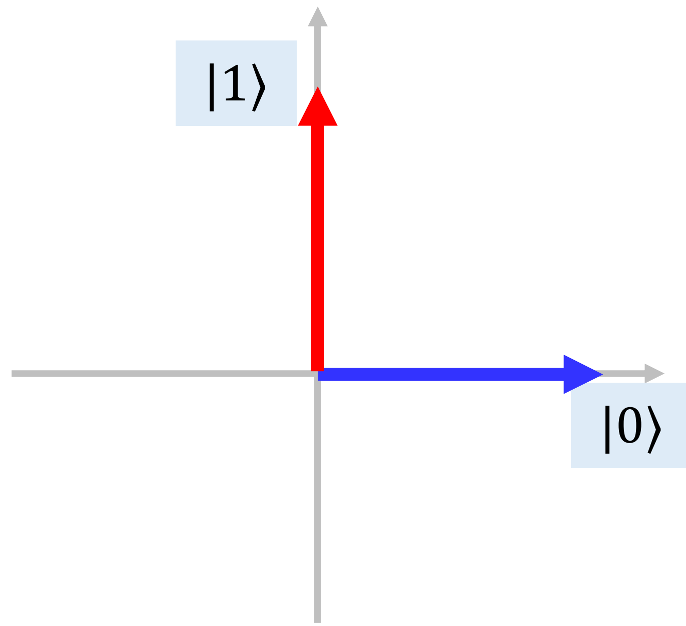
- The one-bit inversion gate flips the bits
  - How does it affect $|0\rangle$ and $|1\rangle$?

The one-qubit inversion gate





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

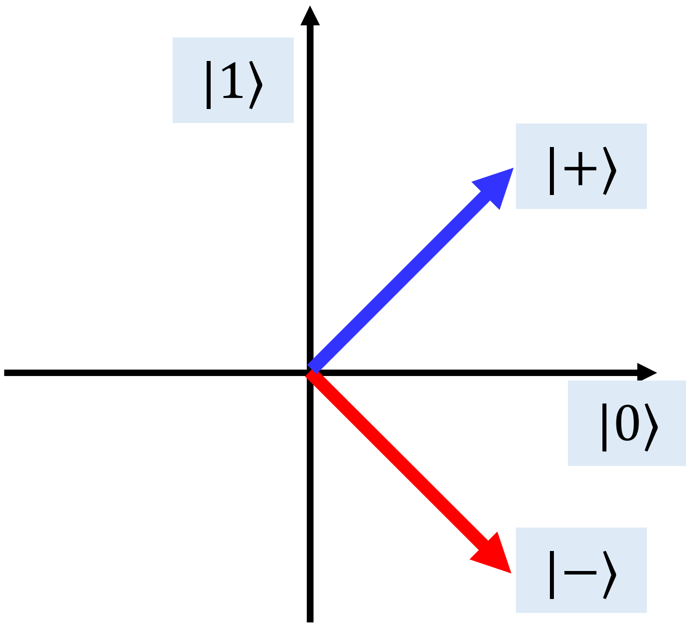


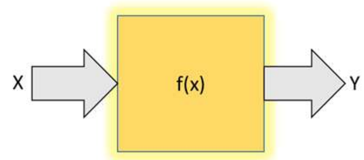
- The one-bit inversion gate flips the bits
  - How does it affect $|0\rangle$ and $|1\rangle$?

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

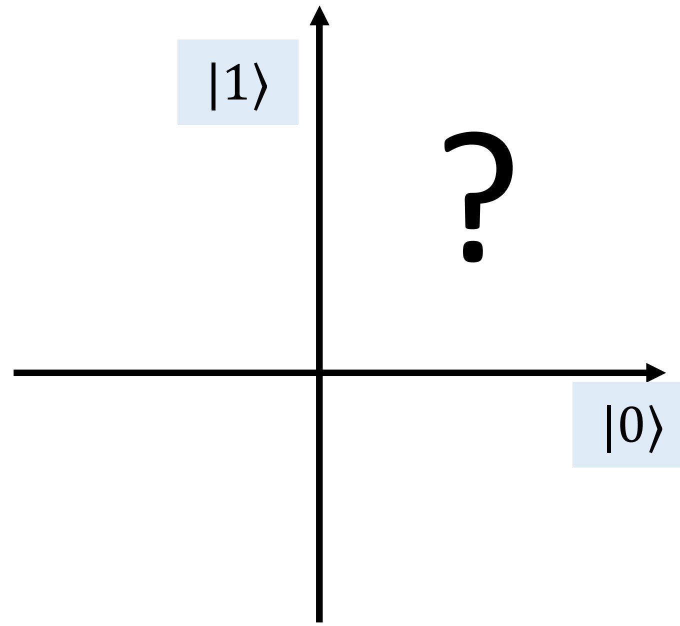
$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

The one-qubit inversion gate



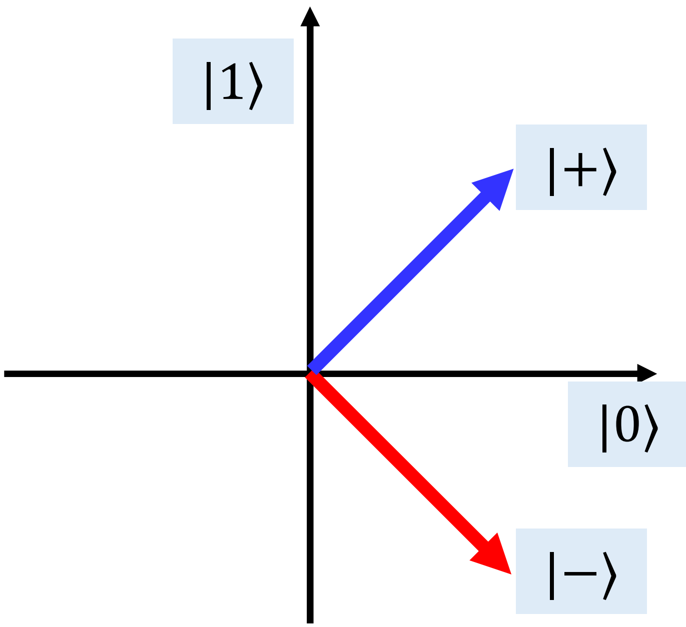


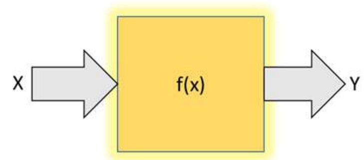
$$F = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$



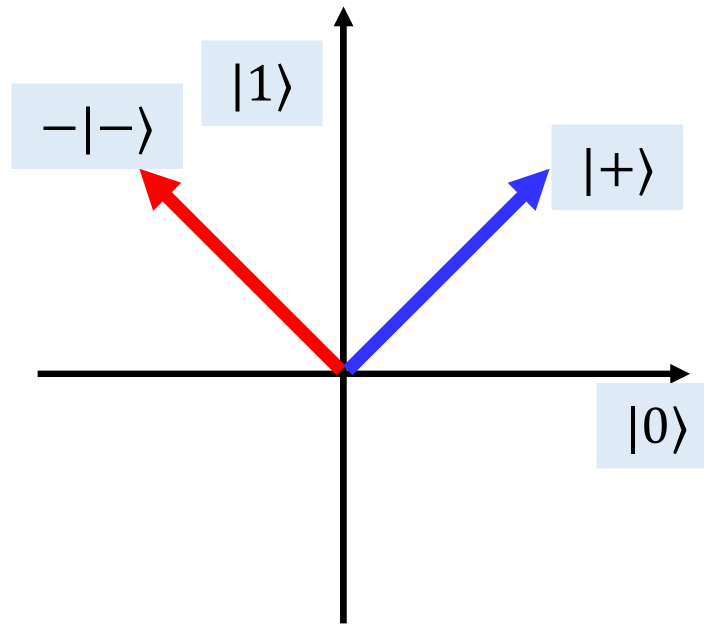
- The one-bit inversion gate flips the bits
  - How does it affect $|0\rangle$ and $|1\rangle$?
  - How does it affect $|+\rangle$ and $|-\rangle$?

The one-qubit inversion gate





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



- The one-bit inversion gate flips the bits
  - How does it affect $|0\rangle$ and $|1\rangle$?
  - How does it affect $|+\rangle$ and $|-\rangle$?

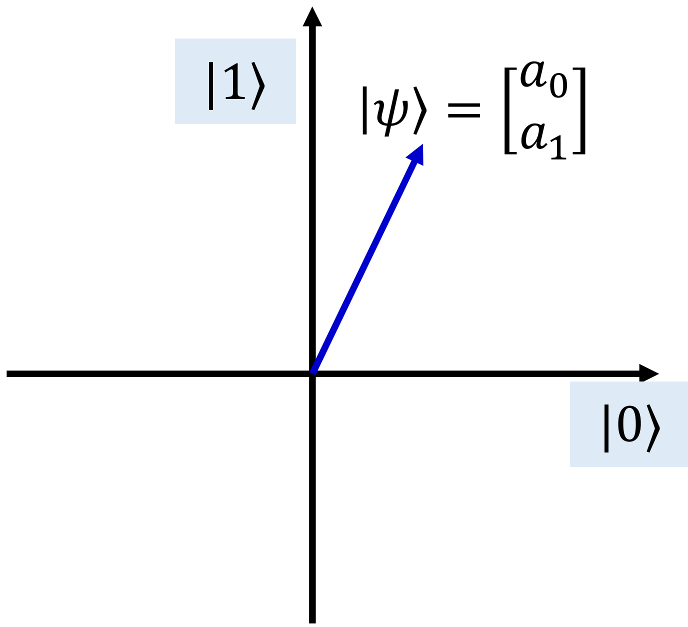
$F|+\rangle = |+\rangle$

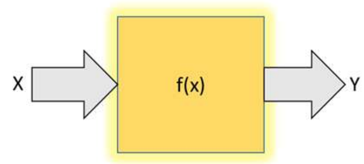
$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix} = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix}$$

$F|-\rangle = -|-\rangle$

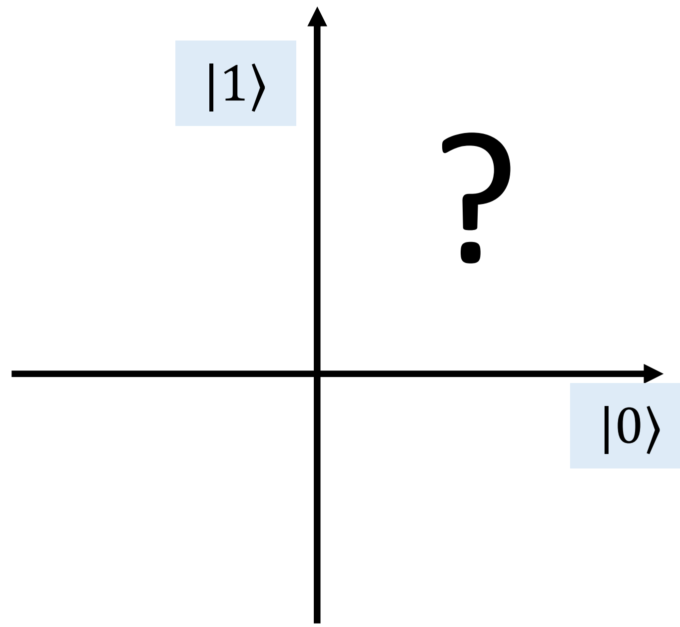
$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{-1}{\sqrt{2}} \end{bmatrix} = \begin{bmatrix} \frac{-1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix}$$

The one-qubit inversion gate



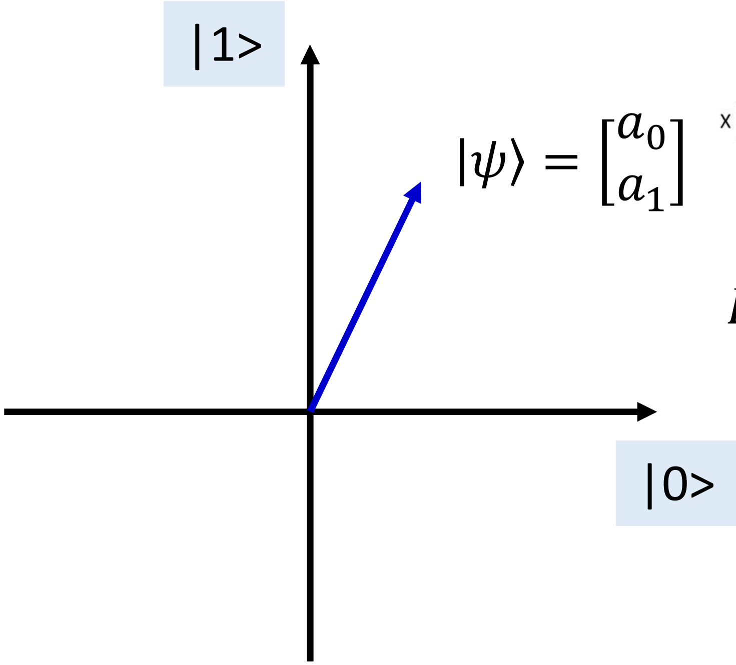


$$F = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

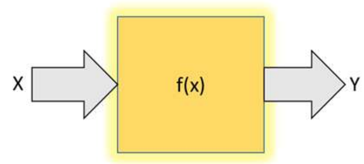


- The one-bit inversion gate flips the bits
  - How does it affect $|1\rangle$ and $|1\rangle$?
  - How does it affect $|+\rangle$ and $|-\rangle$?
  - How does it affect a generic qubit in superposition: $|\psi\rangle = a_0|0\rangle + a_1|1\rangle$

The one-bit inversion gate

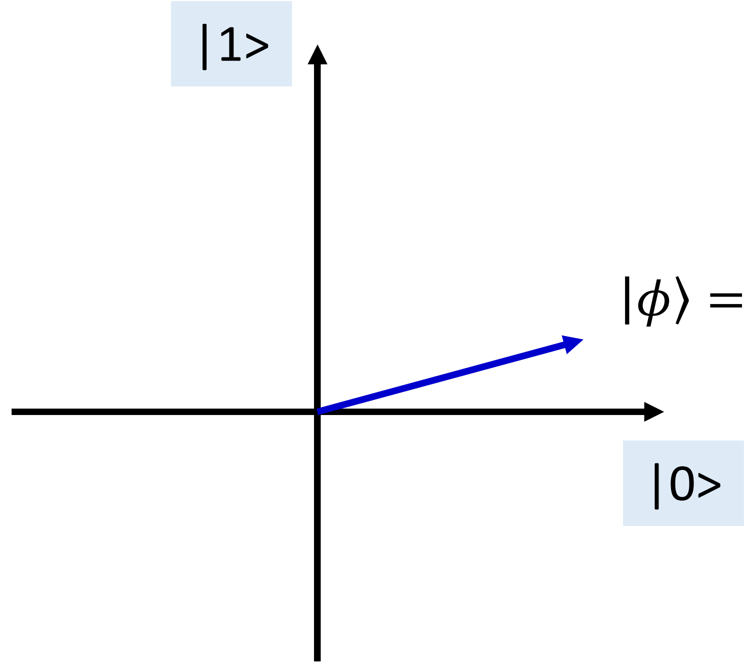


$$|\psi\rangle = \begin{bmatrix} a_0 \\ a_1 \end{bmatrix}$$



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

$$|\phi\rangle = F \cdot |\psi\rangle$$



$$|\phi\rangle = \begin{bmatrix} a_1 \\ a_0 \end{bmatrix}$$

- The one bit identity gate inversion transform
  - How does it affect |0> and |1>?
  - How does it affect |+> and |->?
- How does it affect a generic qubit in superposition:

$$|\psi\rangle = a_0|0\rangle + a_1|1\rangle \quad \Longrightarrow \quad |\phi\rangle = a_1|0\rangle + a_0|1\rangle$$

Poll 4: The sign inversion gate

- The *sign-inversion* gate flips $|+\rangle$ and $|-\rangle$. Which of the following represents the sign inversion gate? Hint: $|+\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix}$, $|-\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\-1\end{bmatrix}$
  - ○ $\begin{bmatrix}0 & 1\\1 & 0\end{bmatrix}$
  - ○ $\begin{bmatrix}\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}}\\\frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}}\end{bmatrix}$
  - ○ $\begin{bmatrix}1 & 0\\0 & -1\end{bmatrix}$
  - ○ $\begin{bmatrix}0 & 1\\-1 & 0\end{bmatrix}$

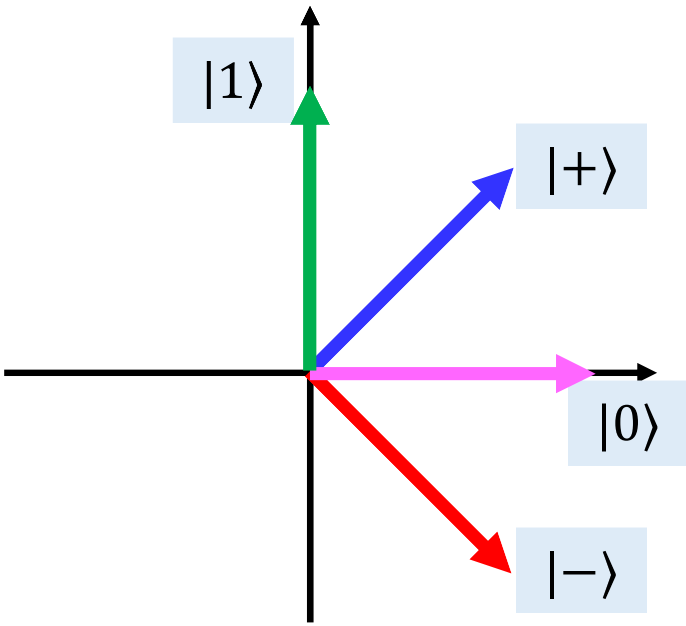
Poll 4: The sign inversion gate

- The *sign-inversion* gate flips $|+\rangle$ and $|-\rangle$. Which of the following represents the sign inversion gate? Hint: $|+\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix}, |-\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\-1\end{bmatrix}$
  - $\begin{bmatrix}0 & 1\\1 & 0\end{bmatrix}$
  - $\begin{bmatrix}\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}}\\\frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}}\end{bmatrix}$
  - $\begin{bmatrix}\mathbf{1} & \mathbf{0}\\\mathbf{0} & \mathbf{-1}\end{bmatrix}$
  - $\begin{bmatrix}0 & 1\\-1 & 0\end{bmatrix}$

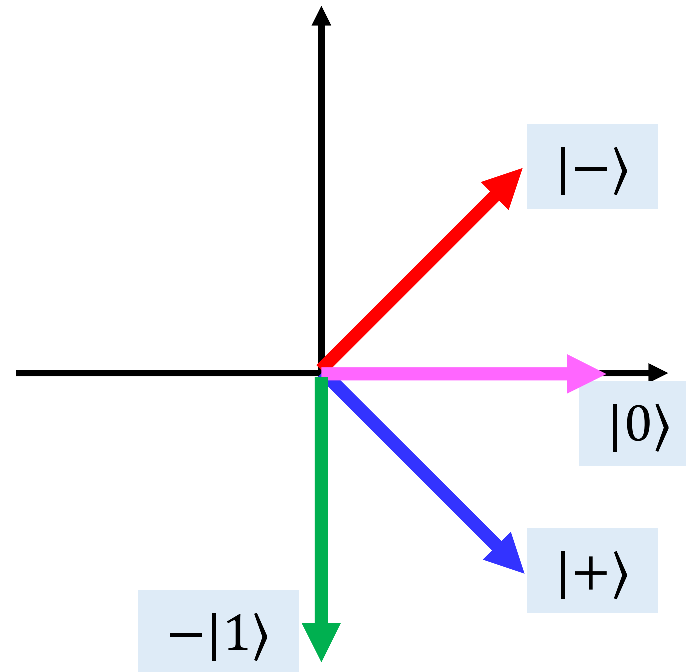
$$\begin{bmatrix}\mathbf{1} & \mathbf{0}\\\mathbf{0} & \mathbf{-1}\end{bmatrix}\left(\frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix}\right) = \left(\frac{1}{\sqrt{2}}\begin{bmatrix}1\\-1\end{bmatrix}\right)$$

$$\begin{bmatrix}\mathbf{1} & \mathbf{0}\\\mathbf{0} & \mathbf{-1}\end{bmatrix}\left(\frac{1}{\sqrt{2}}\begin{bmatrix}1\\-1\end{bmatrix}\right) = \left(\frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix}\right)$$

The sign inversion gate

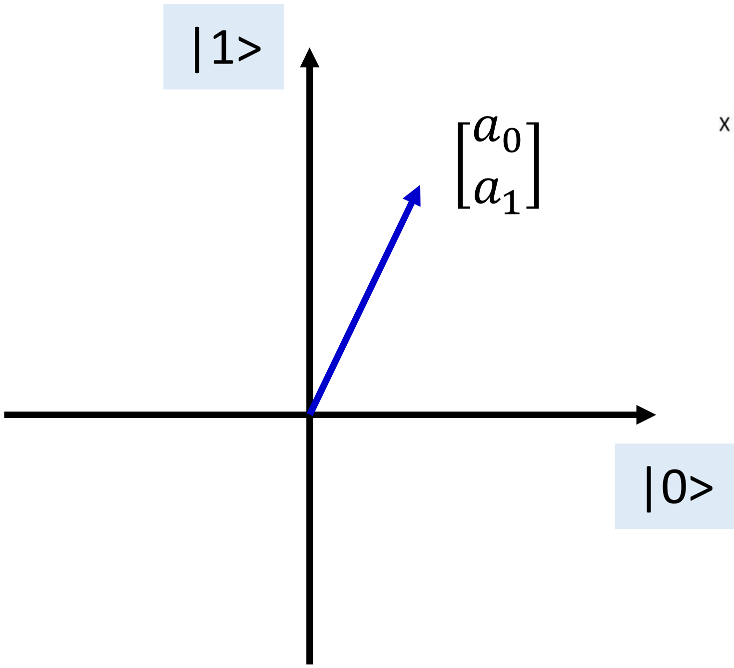


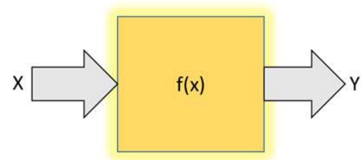
$$\begin{bmatrix} \mathbf{1} & \mathbf{0} \\ \mathbf{0} & \mathbf{-1} \end{bmatrix}$$



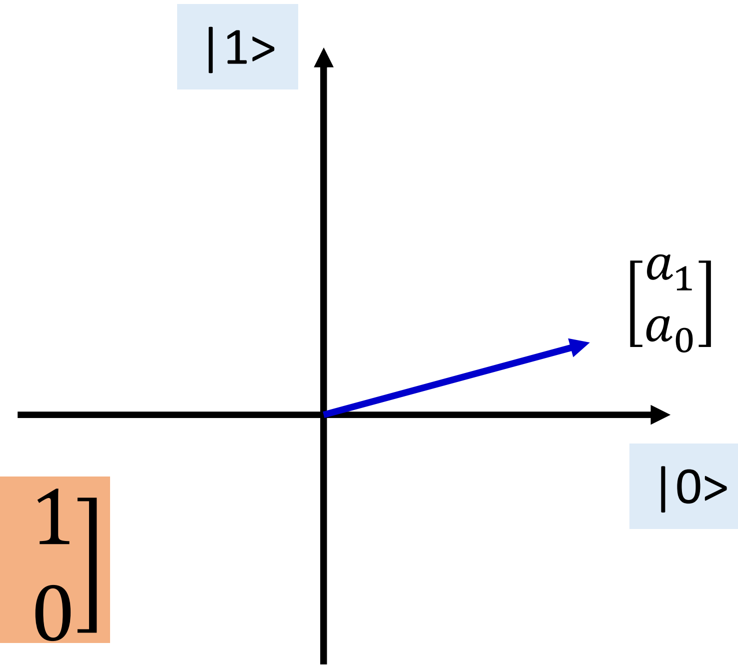
- $|-\rangle$ and $|+\rangle$ get swapped
- $|0\rangle$ remains unchanged
- $|1\rangle$ gets negated and goes to $-|1\rangle$
- This is strictly analogous to the effect of the bit inversion gate on the bit and sign bases

Returning to the bit inversion gate





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



- The bit inversion gate flips $|0\rangle$ and $|1\rangle$
- Also called a “Pauli X gate”
- What kind of other 1-bit gates identity and inversion gates can you have?
  - Keeping in mind that the phasors and matrices are actually *complex?*

The one-bit inversion gate

From wikipedia

Operator	Gate(s)		Matrix
Pauli-X (X)	X	$\oplus$	$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
Pauli-Y (Y)	Y		$\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$
Pauli-Z (Z)	Z		$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
Phase (S, P)	S		$\begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$
$\pi/8$ (T)	T		$\begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$

- Which of these are equivalent to classical identity gates?
- Which of these are equivalent to classical negation gates?

The one-bit inversion gate

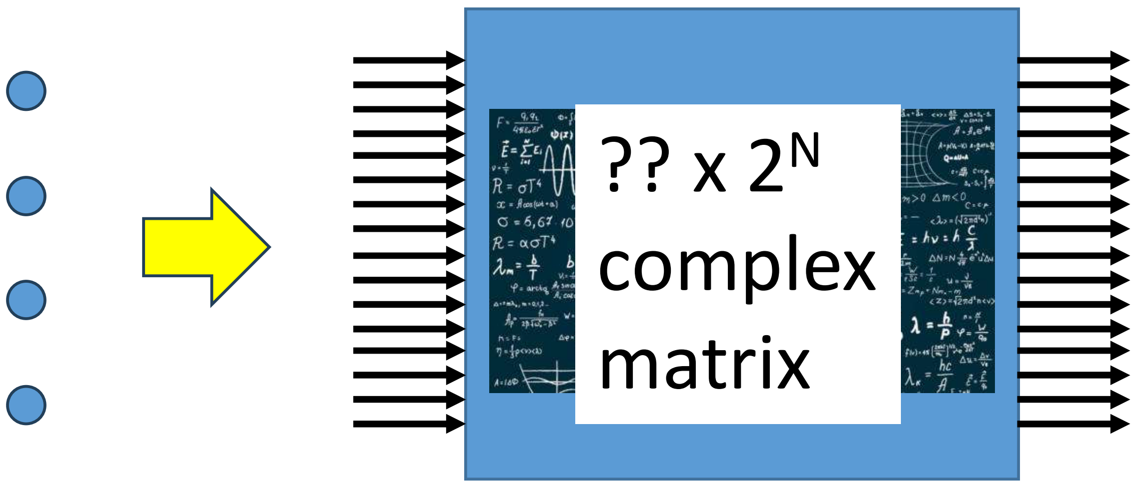
From wikipedia

Operator	Gate(s)		Matrix
Pauli-X (X)	**X**	$\oplus$	$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
Pauli-Y (Y)	**Y**		$\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$
Pauli-Z (Z)	**Z**		$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
Phase (S, P)	**S**		$\begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$
$\boldsymbol{\pi/8}$ **(T)**	**T**		$\begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$

The Pauli gates (X, Y, Z) are the three Pauli matrices $(\sigma_x, \sigma_y, \sigma_z)$ and act on a single qubit. The Pauli *X*, *Y* and *Z* equate, respectively, to a rotation around the *x*, *y* and *z* axes of the Bloch sphere by π radians.[b]

Multi-bit gates and functions

- Quantum gates that operate on N bit inputs actually operate on a 2^N-dimensional space



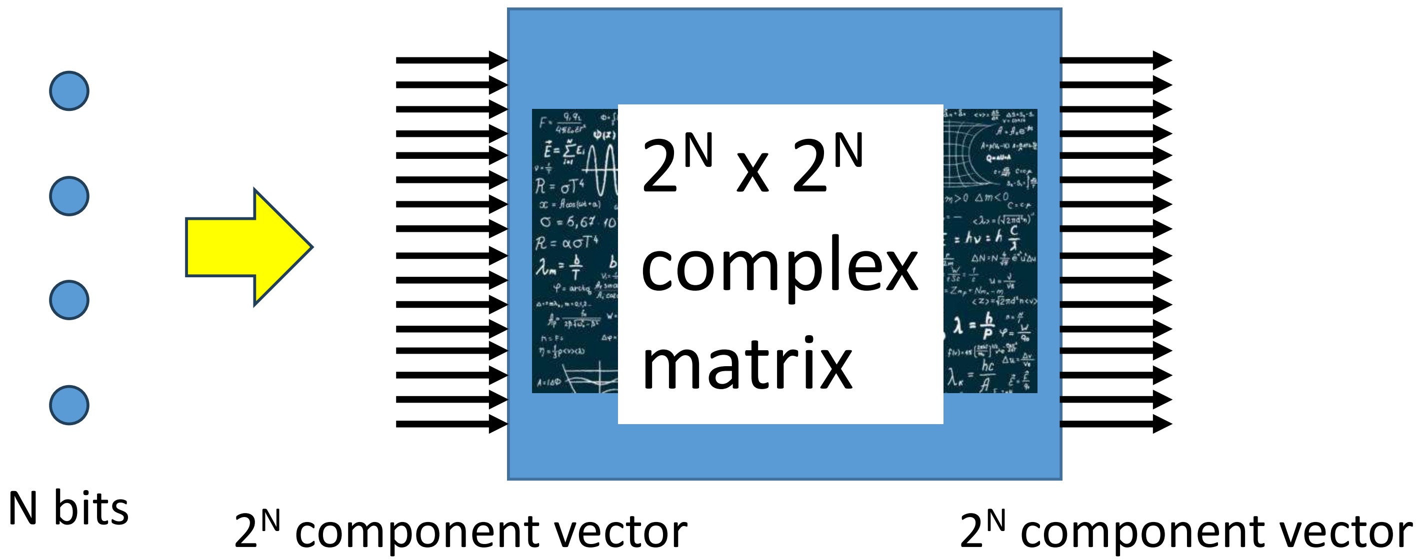
N bits

2^N component vector

How many component vector?

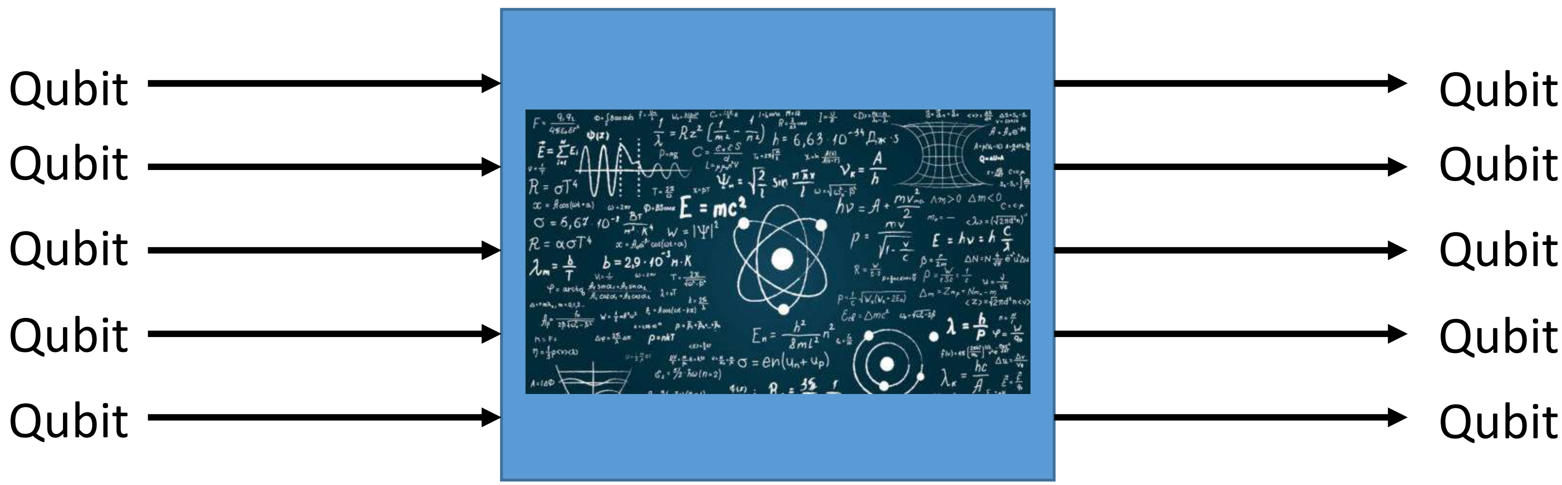
Multi-bit gates and functions

- Quantum gates that operate on N bit inputs actually operate on a 2^N-dimensional space



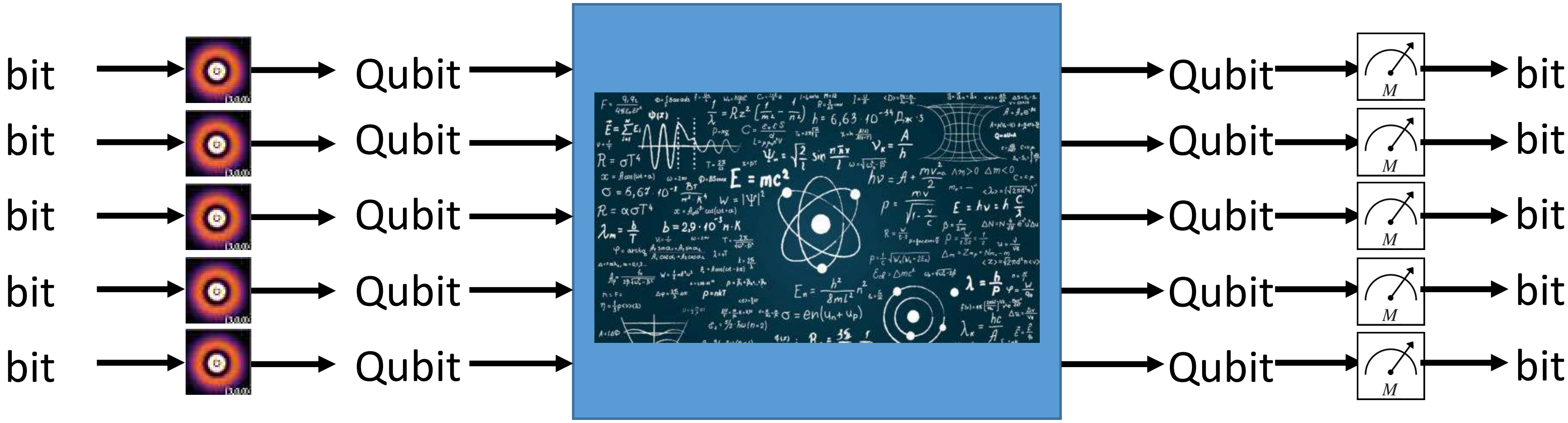
- Clearly this is infeasible if implemented directly

Quantum computation



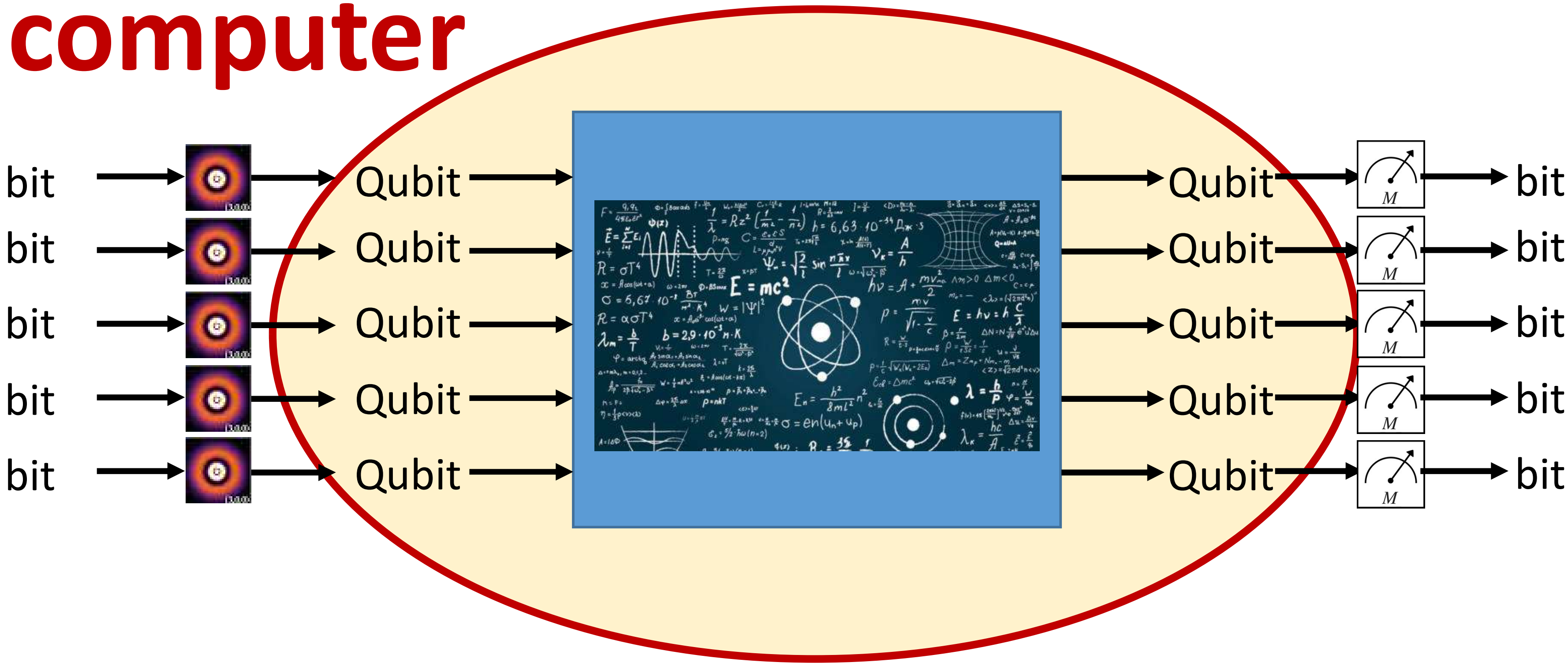
- In reality we don't work explicitly in the high-dimensional space
  - Except for simulations, which will of course blow up
- Instead, the inputs and outputs are Qubits
  - Which start (and end) life in states that represent classical bits
    - I.e. their start and end fates are classical
    - Because that's what *we* know to deal with.

The secret life of a quantum computer



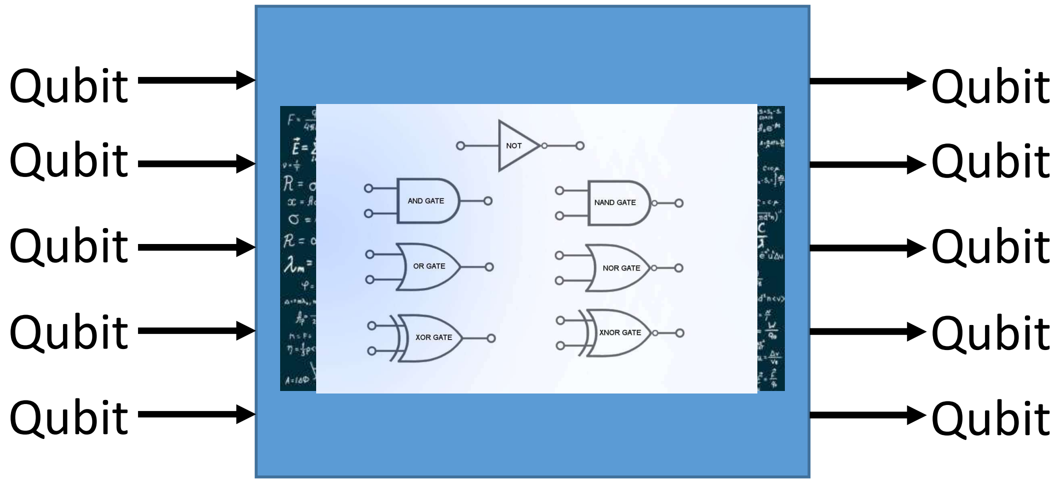
- The complete cycle

The secret life of a quantum computer



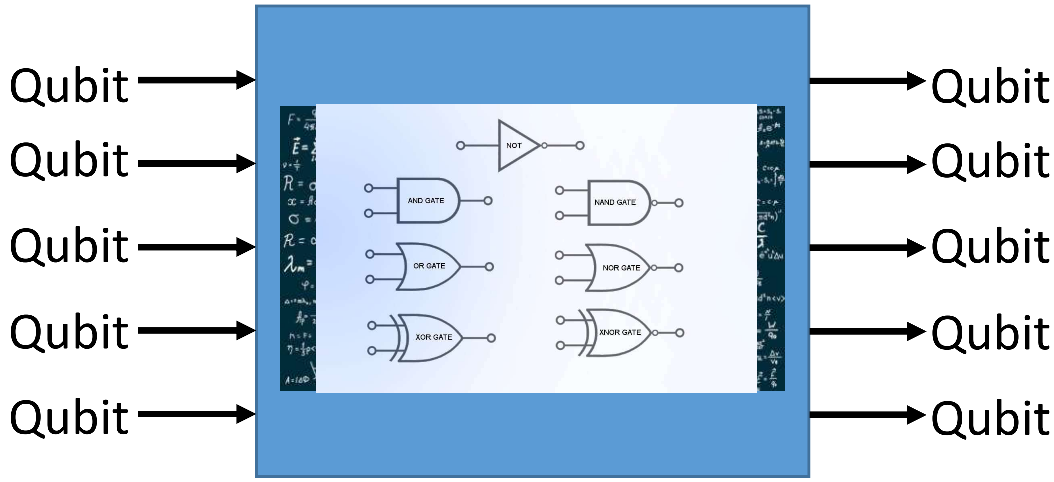
- The complete cycle
- The actual quantum computation
  - The computer may itself include measurement as in internal operation

The secret life of a quantum computer



- The internal computation is, once again, composed of a combination of smaller “Gates”
  - Operations on smaller numbers of Qubits
  - Some of which may emulate classical computation
- Challenge: Minimize the number of Gates

The secret life of a quantum computer



- The internal computat combination of smalle
  - Operations on smaller
  - Some of which may er
- Challenge: Minimize t

The quantum computer too has a Universal gate:

The TOFFOLI gate.
(The CNOT is an instance of a Toffoli gate)

Quantum gates

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

$$|\psi\rangle = \begin{bmatrix} a_0 \\ \vdots \\ a_{2^N-1} \end{bmatrix} \qquad |\varphi\rangle = \begin{bmatrix} b_0 \\ \vdots \\ b_{2^N-1} \end{bmatrix}$$

$$\begin{bmatrix} b_0 \\ \vdots \\ b_{2^N-1} \end{bmatrix} = U \begin{bmatrix} a_0 \\ \vdots \\ a_{2^N-1} \end{bmatrix}$$

- Operate on 2^N-Dimensional phasors (for N bits)
  - In a complex 2^N-D complex Hilbert space
  - The input is an 2^N-D phasor, the output too is an 2^N-D phasor
- The “gate” is itself a transform
  - **A *unitary* transform**
- So how many inputs does the gate have, and how many outputs?

Quantum gates

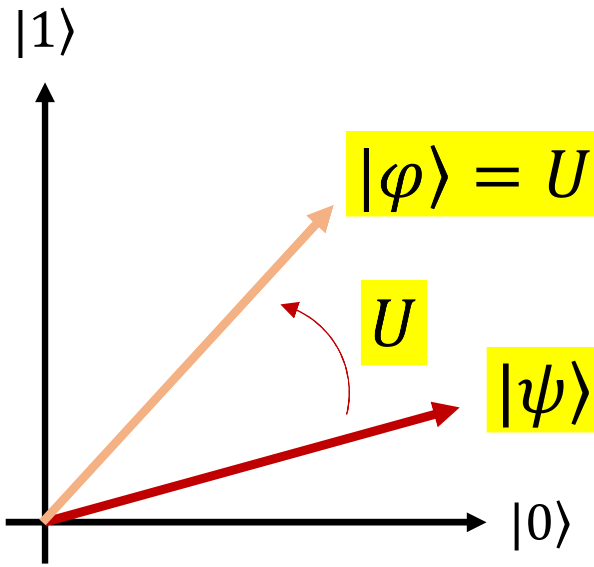
$$|\varphi\rangle = U|\psi\rangle$$

$$|\psi\rangle = \begin{bmatrix} a_0 \\ \vdots \\ a_{2^N-1} \end{bmatrix} \qquad |\varphi\rangle = \begin{bmatrix} b_0 \\ \vdots \\ b_{2^N-1} \end{bmatrix}$$

$$\begin{bmatrix} b_0 \\ \vdots \\ b_{2^N-1} \end{bmatrix} = U \begin{bmatrix} a_0 \\ \vdots \\ a_{2^N-1} \end{bmatrix}$$

- Operate on 2^N-Dimensional phasors (for N bits)
  - In a complex 2^N-D complex Hilbert space
  - The input is an 2^N-D phasor, the output too is an 2^N-D phasor
- The "gate" is itself a transform
  - **A *unitary* transform**
- So how many inputs does the gate have, and how many outputs?
  - Just the number of qubits, not the full-dimensionality of the space
  - The dimensionality of the space is implicit
  - Still, its appropriate to think of the gates as 2^N-D x 2^N-D complex *unitary* transforms

What is a Unitary Transform



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

- Simply speaking, a Unitary transform is a *rotation*
- Let's consider some properties
- Let $U = [u_1 \quad u_2 \quad \cdots \quad u_L]$ be a unitary transform, where u_i is a column vector
  - For an N qubit system, what is L
  - What is the dimension of u_i?

Properties of a Unitary Transform

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

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

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

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

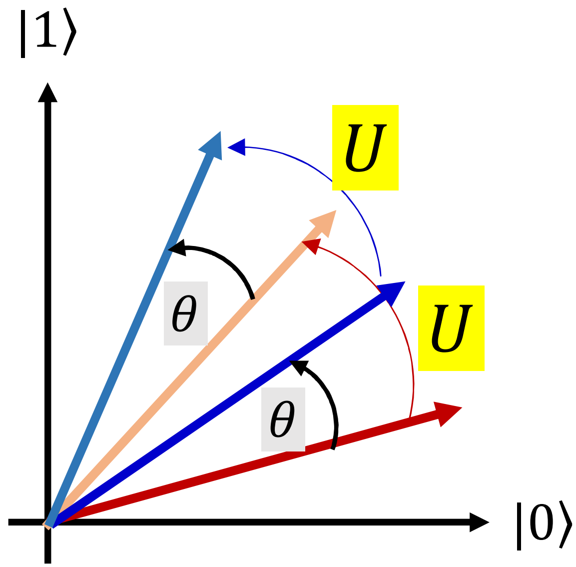
$|u_i| =?$

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

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

- 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!

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*

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

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

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

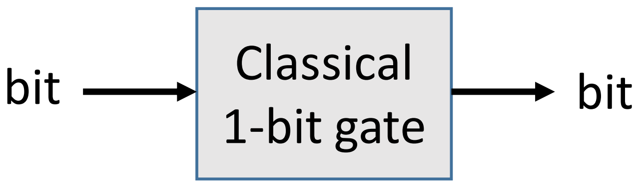
- The Hermitian of U is its own inverse
  - The columns of U are orthogonal to one another (why)?

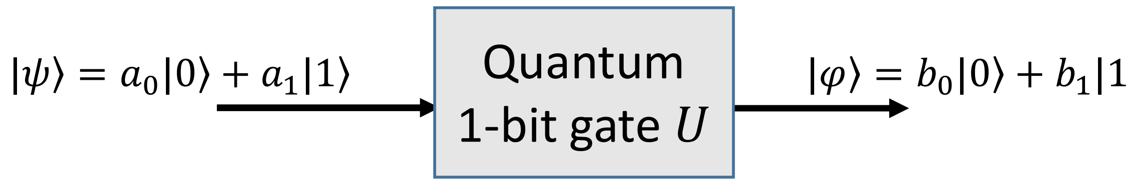
How to check if a transformation U is a valid "gate"

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

- 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



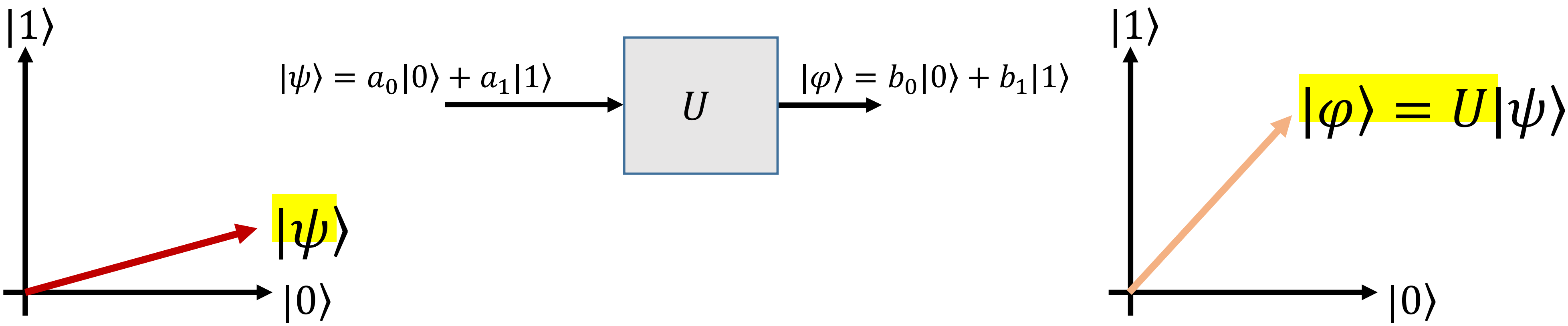


$$U = \begin{bmatrix} u_{00} & u_{01} \\ u_{10} & u_{11} \end{bmatrix}$$

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

- 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



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

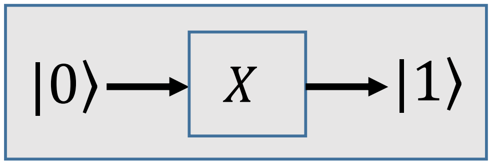
- 2D phasor $|\psi\rangle$ goes in, 2D phasor $|\varphi\rangle$ comes out

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

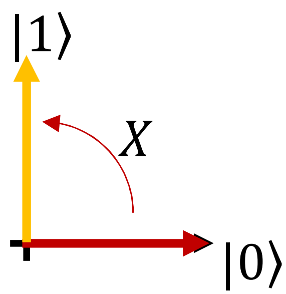
- U is a unitary transform

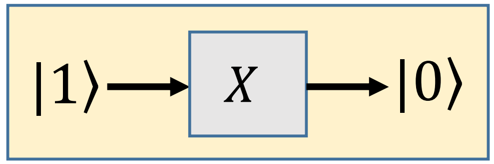
Single qubit gates: The bit-flip gate X

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

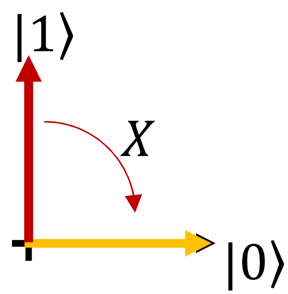


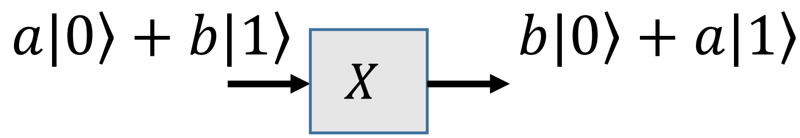
$$\begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$



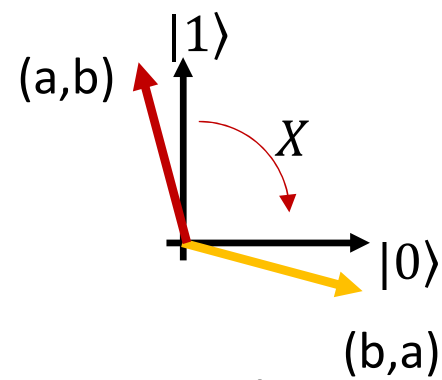


$$\begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$





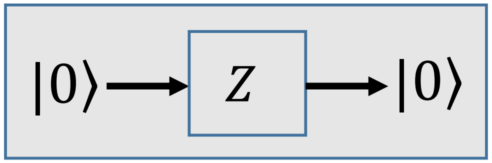
$$\begin{bmatrix} b \\ a \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix}$$



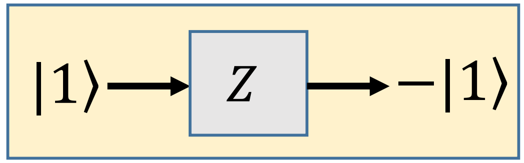
- First verify that X is unitary (or its not really a gate)
- Swaps the |0> and |1> bit values
  - Note – it swaps bit values in 2D
  - Can be *viewed* as flipping |0> and |1> in the phasor

The *phase* flip gate Z

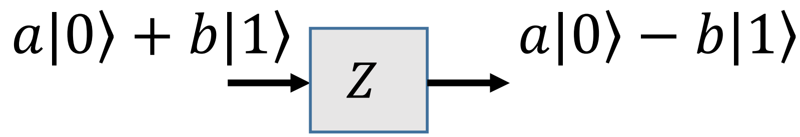
$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$



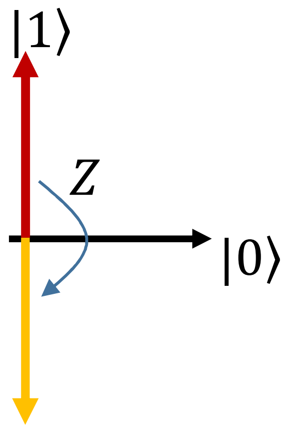
$$\begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

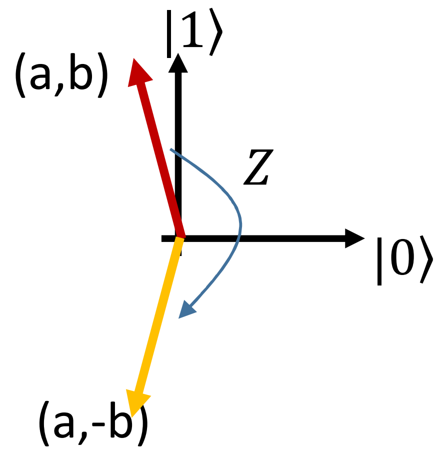


$$\begin{bmatrix} 0 \\ -1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$



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





- 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

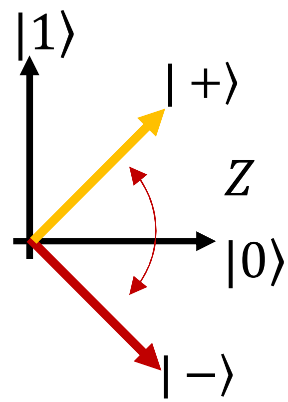
$$\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \longrightarrow \boxed{Z} \longrightarrow \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$$

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

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

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

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



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

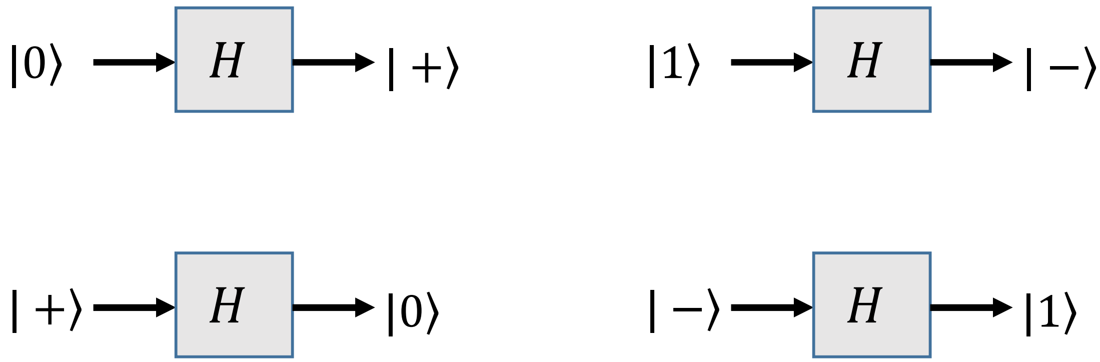
- The Phase flip gate is in fact the *sign flip* gate

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

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

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

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

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

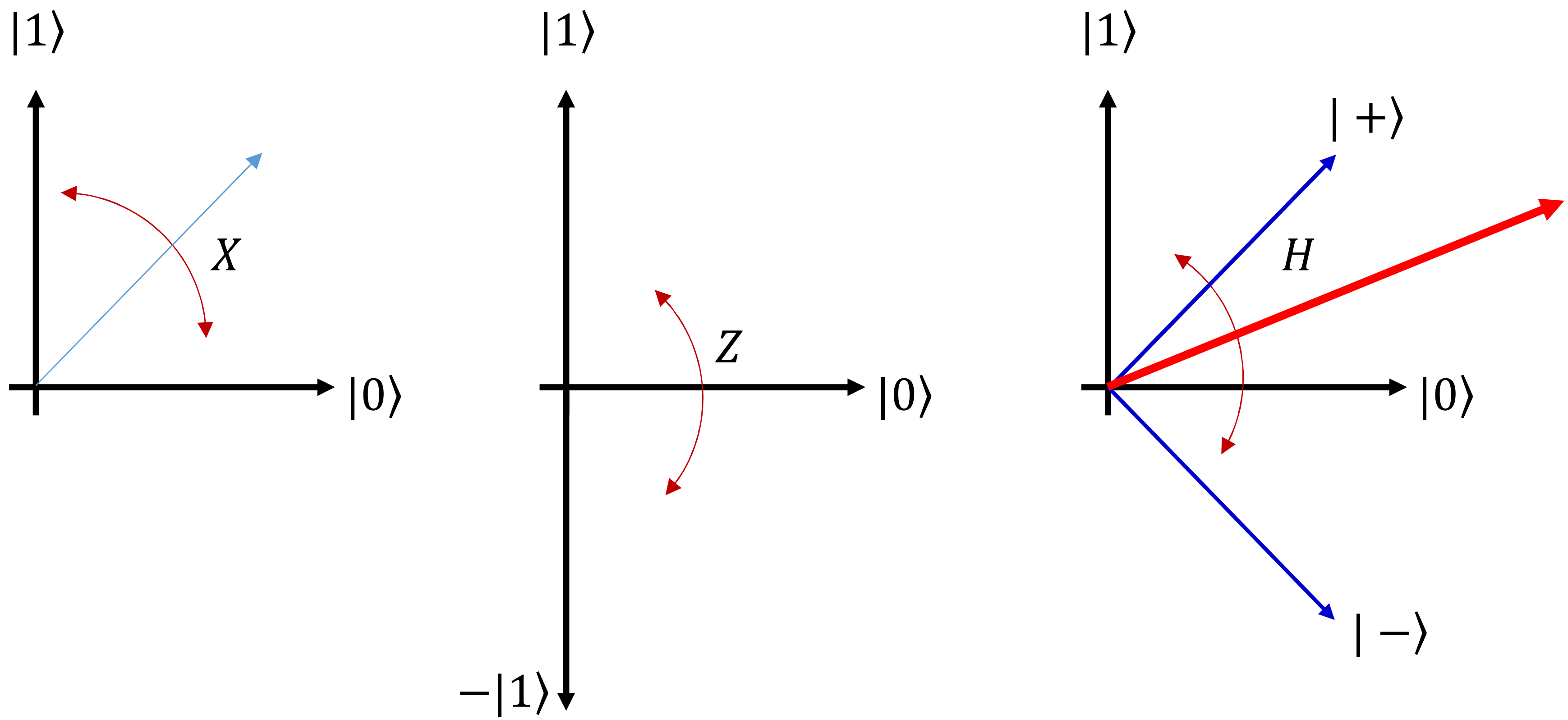
$$H\left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right) = |0\rangle \Rightarrow H|+\rangle = |0\rangle$$

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

Unitary transforms are *rotations*

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

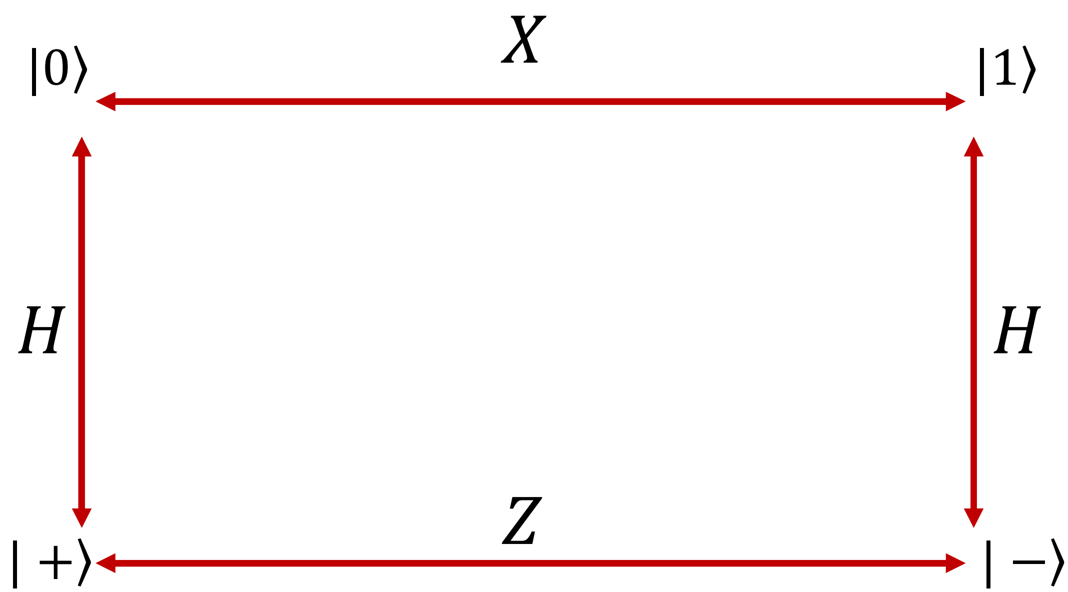
Unitary transforms are rotations



- 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



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

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

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

$|0\rangle \rightarrow [Y] \rightarrow i|1\rangle$

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

$|1\rangle \rightarrow [X] \rightarrow -i|0\rangle$

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

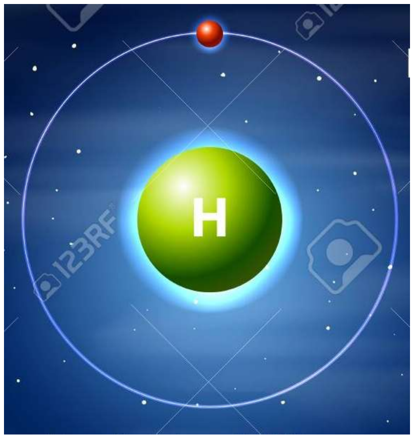
$a|0\rangle + b|1\rangle \rightarrow [X] \rightarrow ib|0\rangle - ia|1\rangle$

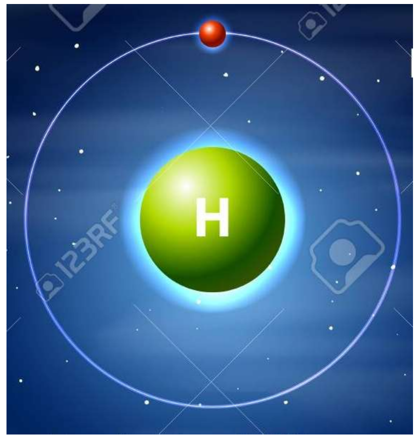
$$\begin{bmatrix} -ib \\ ia \end{bmatrix} = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}\begin{bmatrix} a \\ b \end{bmatrix}$$

Cant 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?)

You can't get very far with one bit



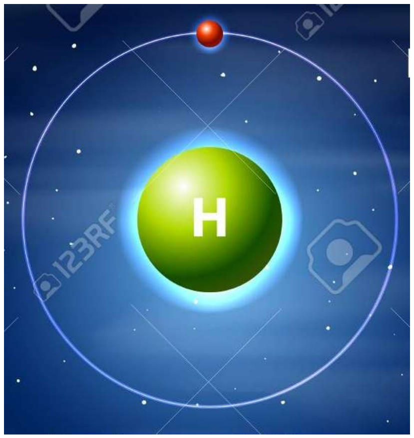


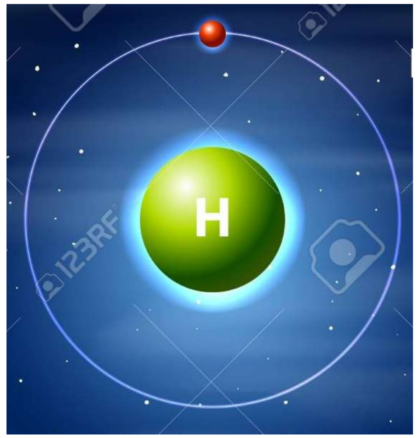
- Two qubits walk into a bar…

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

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

Representing the combined system





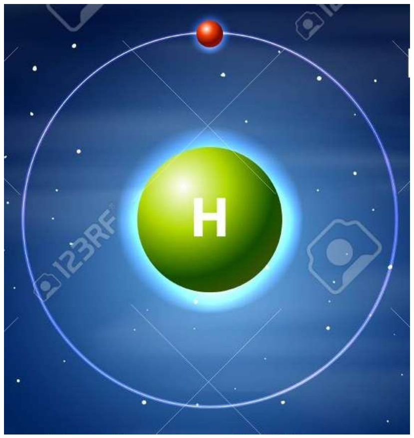
- Two qubits walk into a bar…

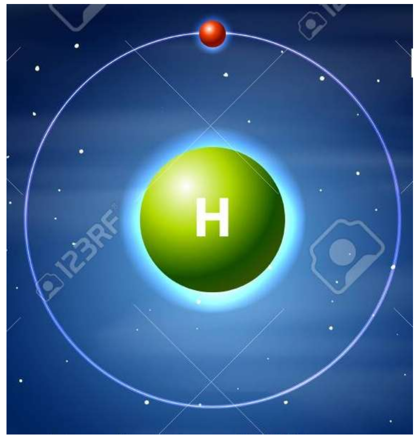
$$|\psi_0\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$$
$$|\psi_1\rangle = \beta_0|0\rangle + \beta_1|1\rangle$$

- The combined system:

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

Representing the combined system





- Two qubits walk into a bar…

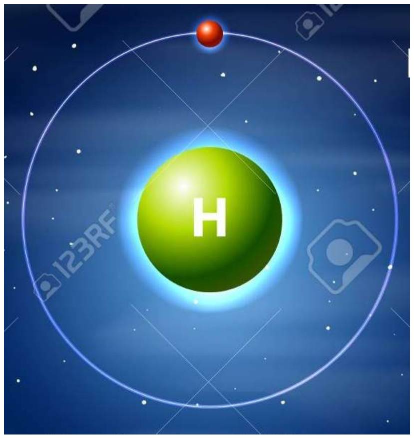
$$|\psi_0\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle$$
$$|\psi_1\rangle = \beta_0 |0\rangle + \beta_1 |1\rangle$$

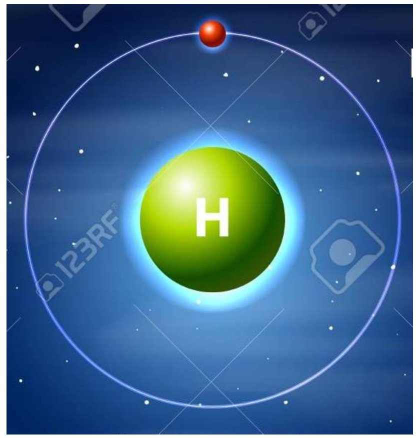
What is $|\psi\rangle$ assuming non-interacting qubits

- The combined system:

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

Representing the combined system





- Two qubits walk into a bar…

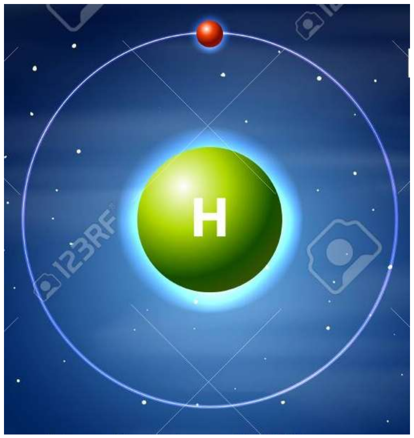
$$|\psi_0\rangle = \alpha_0|+\rangle + \alpha_1|-\rangle$$
$$|\psi_1\rangle = \beta_0|0\rangle + \beta_1|1\rangle$$

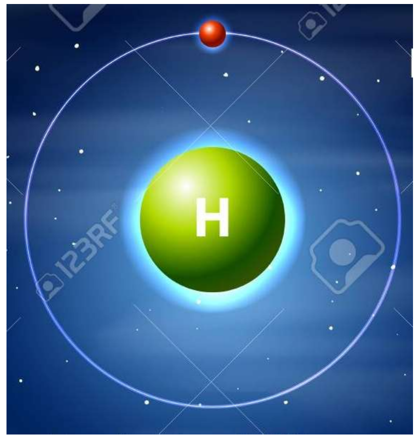
What is $|\psi\rangle$ assuming non-interacting qubits

- The combined system:

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

Representing the combined system





- Two qubits walk into a bar…

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

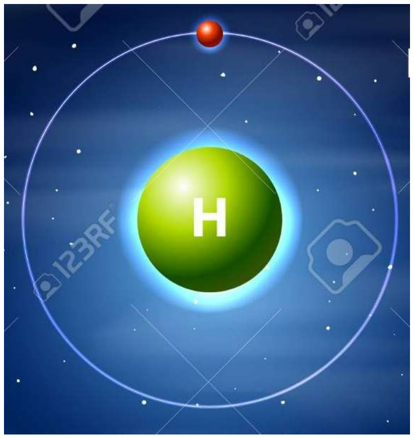
$$|\psi_1\rangle = \beta_0|0\rangle + \beta_1|1\rangle$$

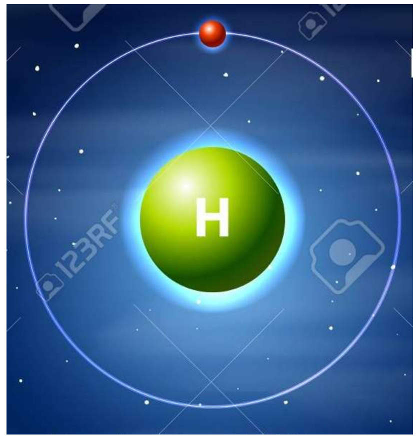
What is $|\psi\rangle$ assuming non-interacting qubits

- The combined system:

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

Representing the combined system





- Two qubits walk into a bar…

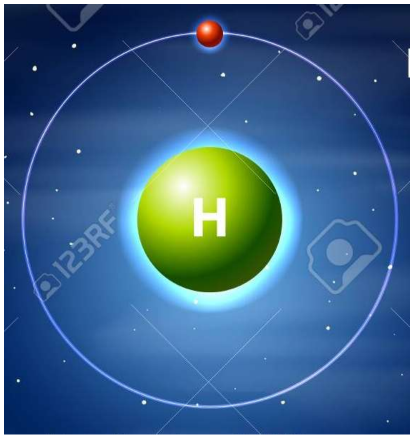
$$|\psi_0\rangle = \alpha_0|{+}\rangle + \alpha_1|{-}\rangle$$
$$|\psi_1\rangle = \beta_0|0\rangle + \beta_1|1\rangle$$

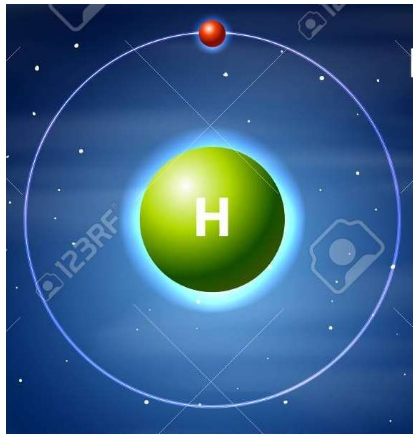
What is $|\psi\rangle$ assuming non-interacting qubits

- The combined system:

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

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

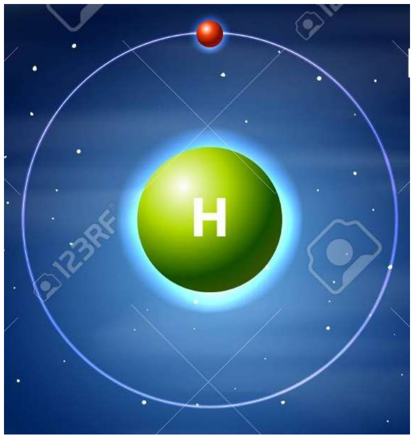
$$\begin{bmatrix}\alpha_0\\ \alpha_1\end{bmatrix} \otimes \begin{bmatrix}\beta_0\\ \beta_1\end{bmatrix} = \begin{bmatrix}\alpha_0 \begin{bmatrix}\beta_0\\ \beta_1\end{bmatrix}\\ \alpha_1 \begin{bmatrix}\beta_0\\ \beta_1\end{bmatrix}\end{bmatrix} = \begin{bmatrix}\alpha_0\beta_0\\ \alpha_0\beta_1\\ \alpha_1\beta_0\\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

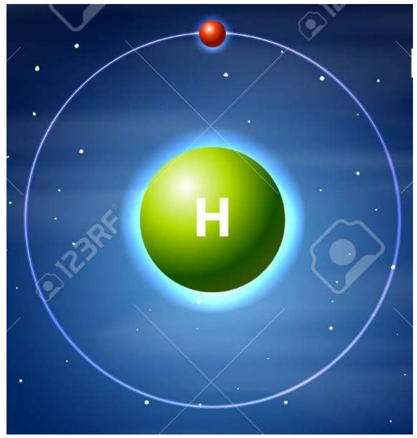
- In Ket notation

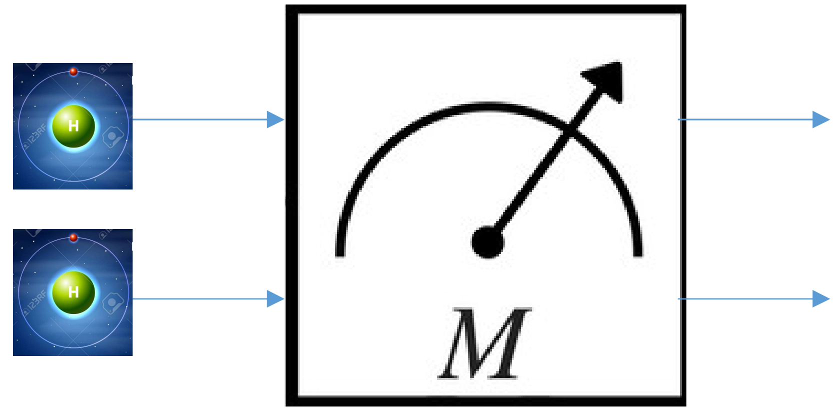
  $(\alpha_0|0> + \alpha_1|1>) \otimes (\beta_0|0> + \beta_1|1>)$

  $= \alpha_0\beta_0|00> + \alpha_0\beta_1|01> + \alpha_1\beta_0|10> + \alpha_1\beta_1|11>$

Measuring the two-cubit system



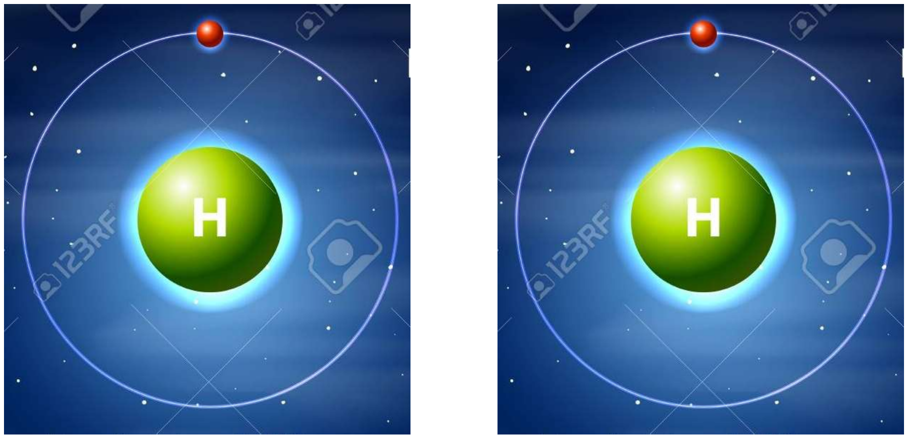


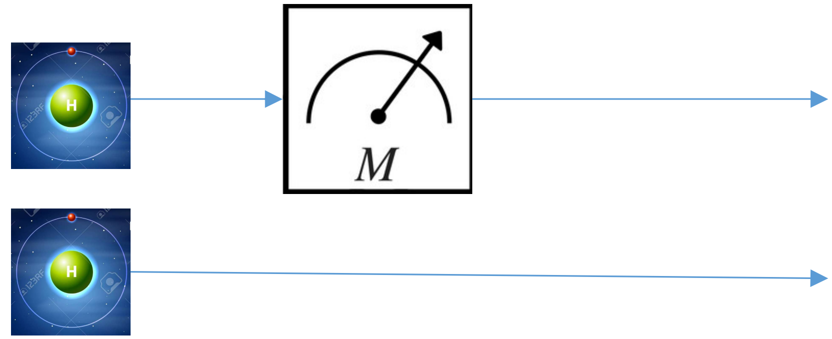


$$|\psi\rangle = \gamma_{00}|00\rangle + \gamma_{01}|01\rangle + \gamma_{10}|10\rangle + \gamma_{11}|11\rangle$$

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

Measuring the two-cubit system

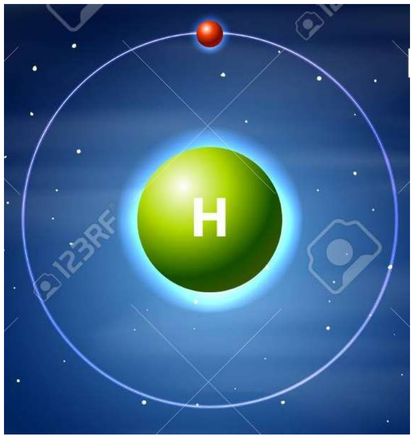


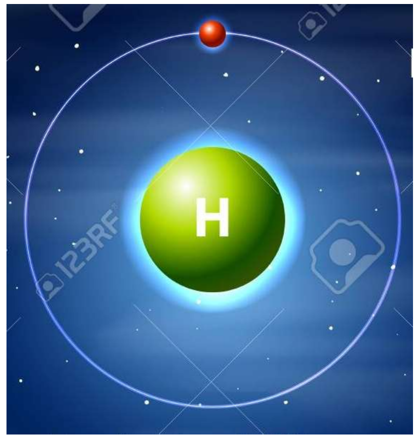


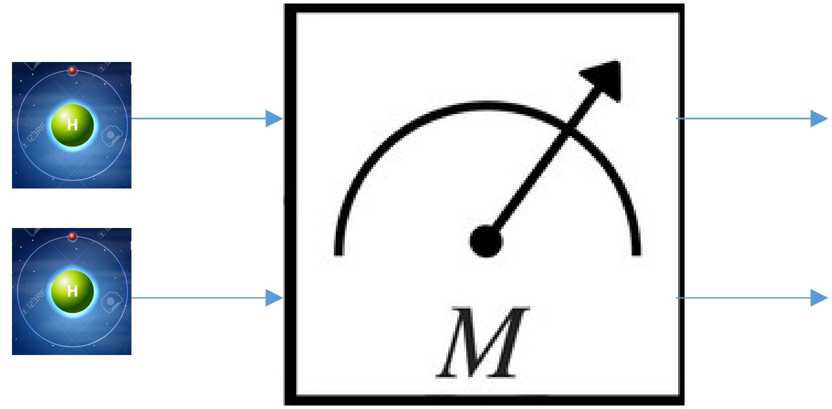
$$|\psi\rangle = \gamma_{00}|00\rangle + \gamma_{01}|01\rangle + \gamma_{10}|10\rangle + \gamma_{11}|11\rangle$$

- 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