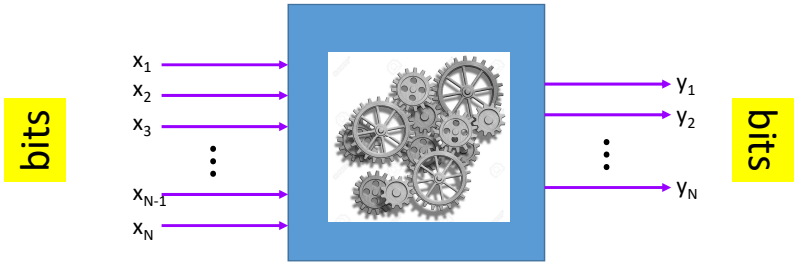
Quantum…

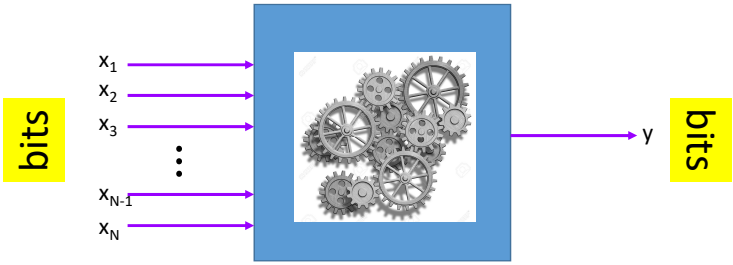
computing

A standard model for Boolean functions (aka algorithms)

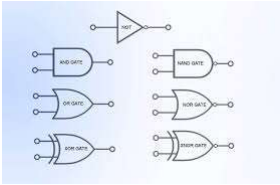


- A bunch of bits go in, and a bunch of bits come out

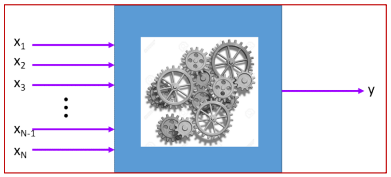
A simpler model for computation

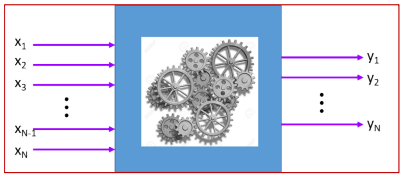


- A bunch of bits go in, and one bit comes out.
- Examples to the right



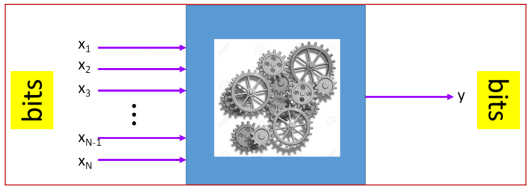
A simpler model for computation

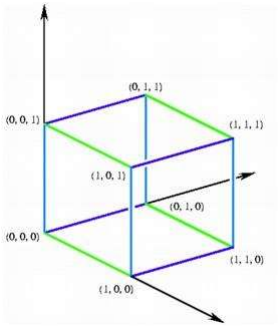




- The model to the left is in fact a generalization of the model to the right
  - How?

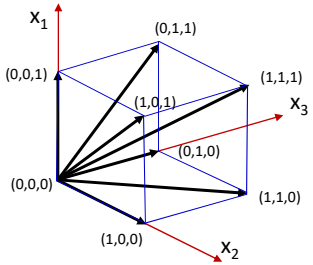
The actual model of computation





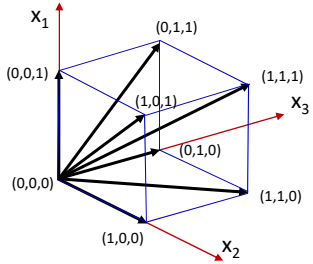
- It is a function of N bits
  - An input goes in, a unique value comes out
- The inputs lie in an N-dimensional space
  - Each input dimension can take only two values [0,1].
  - Other values are not defined
- The entire set of all possible inputs lies on the corners of an N-dimensional hypercube
  - The interior of the cube is infeasible
- The function is defined on the corners of this hypercube

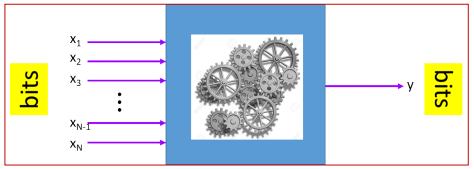
The input space representation



- For a function over N bits, the function is defined over an N-dimensional input space
  - **Each input bit represents an orthogonal direction in the space!**
- Each feasible input combination is an N-dimensional vector in this space
  - The feasible set of inputs is a countable, finite set of 2^N points.
- In order to fully represent an input, N values must be provided
  - One number for each input coordinate

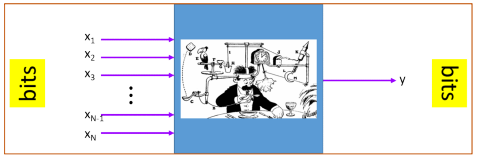
The function

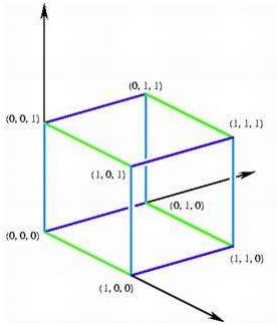




- The algorithm is simply a function that operates on this input space
  - It transforms each input vector to a Boolean value
- Note again that each input vector represents a *single* possible combination of bits
  - When operated on a vector, the function computes the output for that combination of input bits

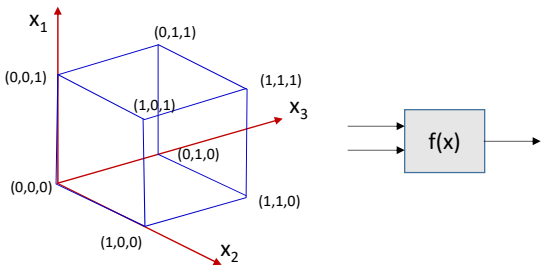
The unknown function problem





- You are given an uncharacterized function
  - N inputs
  - You know the formulae in it, but don't know what outputs it will produce for any input
- You must characterize the function fully
- How many measurements must you make?
  - "Measurement" : provide an input and note the output

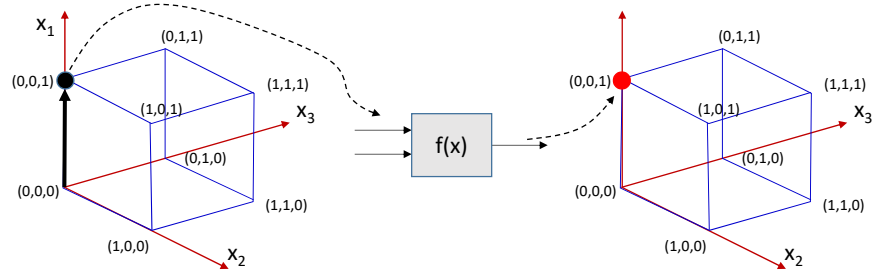
“Discovering” a 2-bit function



Determine this function fully!

- Find out how it responds to any input

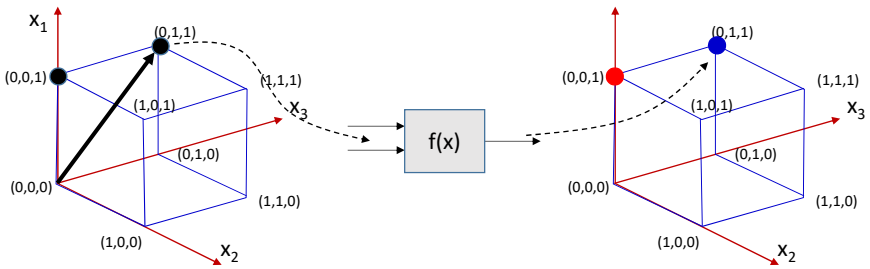
“Discovering” a 2-bit function



Determine this function fully!

- Pass each possible input vector through the function and compute its response

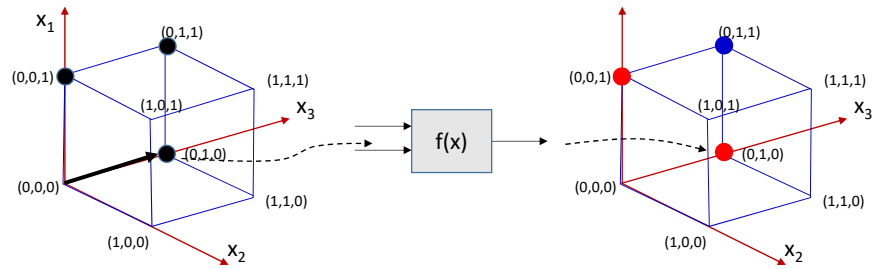
“Discovering” a 2-bit function



Determine this function fully!

- Pass each possible input vector through the function and compute its response

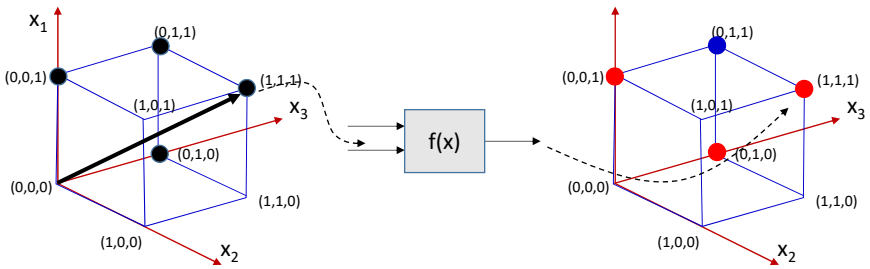
“Discovering” a 2-bit function



Determine this function fully!

- Pass each possible input vector through the function and compute its response

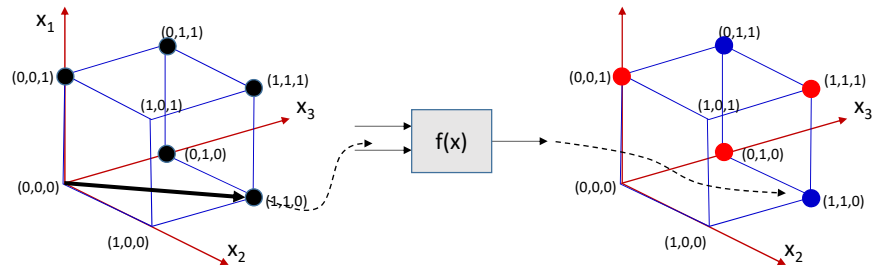
“Discovering” a 2-bit function



Determine this function fully!

- Pass each possible input vector through the function and compute its response

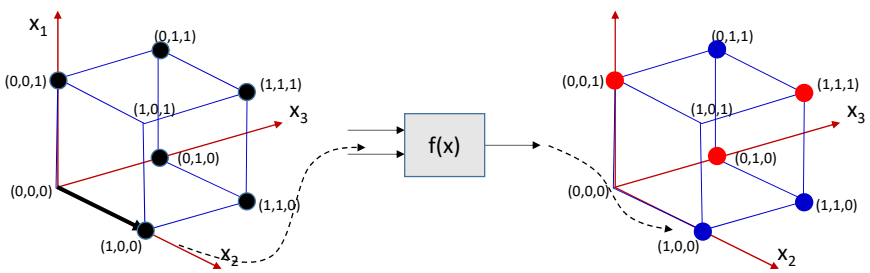
“Discovering” a 2-bit function



Determine this function fully!

- Pass each possible input vector through the function and compute its response

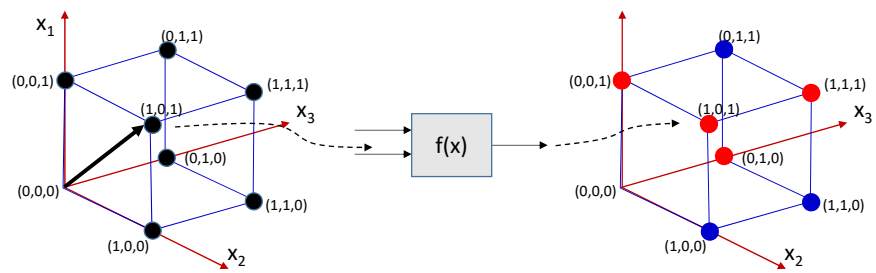
“Discovering” a 2-bit function



Determine this function fully!

- Pass each possible input vector through the function and compute its response

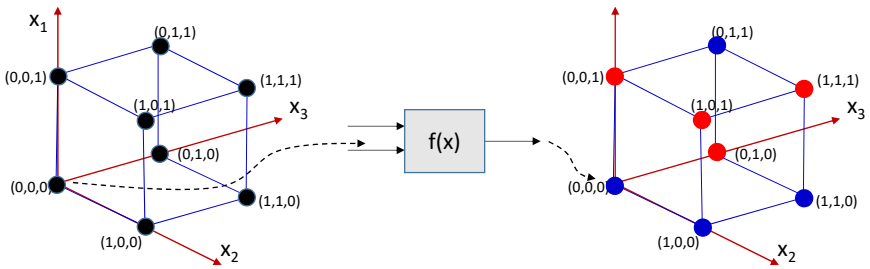
“Discovering” a 2-bit function



Determine this function fully!

- Pass each possible input vector through the function and compute its response

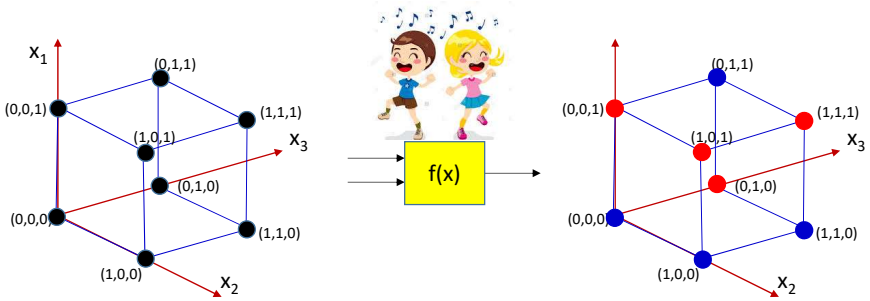
“Discovering” a 2-bit function



Determine this function fully!

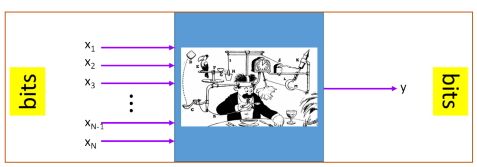
- Pass each possible input vector through the function and compute its response

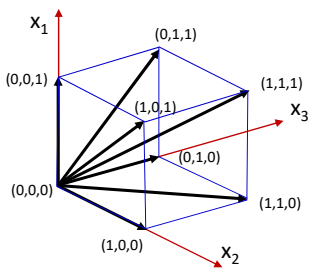
“Discovering” a 2-bit function



- Pass each possible input vector through the function and compute its response
- *And now its known*

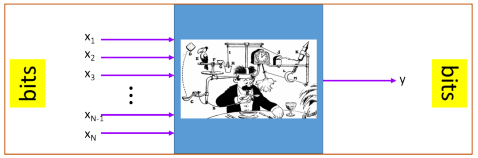
The N-bit unknown function problem

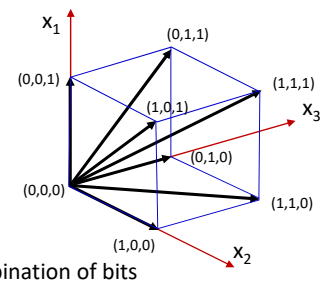




- Recall: For a function over N bits, the function is defined over an N-dimensional input space
- The feasible set of inputs is a countable, finite set of 2^N vectors.
- The function must be individually evaluated at each of these 2^N vectors to define it fully
  - Requiring 2^N evaluations
  - This cannot be reduced

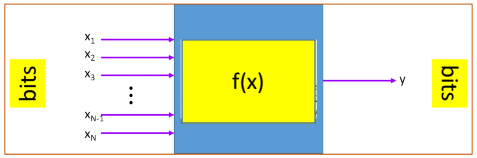
Why this limitation?

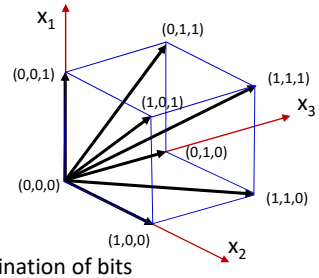




- A vector in the space represents only a *single* combination of bits
- The function operates on individual vectors. So each operation produces the output for a *single* combination of bits
- To determine the function fully, the function must be evaluated on *every* feasible vector in the input space
  - All 2^N feasible input vectors

Why this limitation?



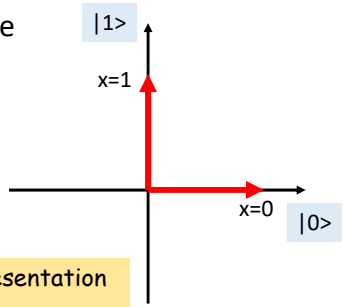


- A vector in the space represents only a *single* combination of bits
- The function operates on individual vectors. So each operation produces the output for a *single* combination of bits
- To determine the function fully, the function must be evaluated on *every* feasible vector in the input space
  - All 2^N feasible input vectors

- Can we *change* the mathematical paradigm itself to change this scenario?
  - Change the representation paradigm itself to make things more efficient, somehow
  - **E.g have a single function computation compute the outputs for multiple combinations of input bits?**

A different approach

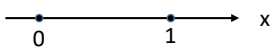
- **Modify the representation**
- Instead of each *bit* representing a (orthogonal) coordinate direction we will make each *combination of bits* represent a orthogonal coordinate direction!
- Even 1 bit is now in a 2-D input space



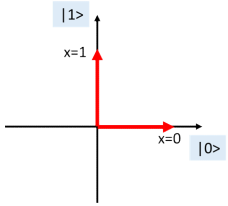
Note that this a fundamentally different representation from standard representations!

A different approach

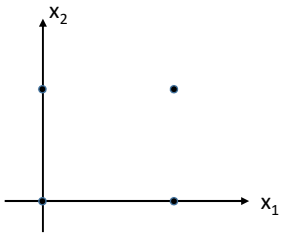
- **1 bit: Old representation**



1 bit: New representation



- **2 bits: Old representation**



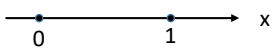
2 bits: New representation

Can't really visualize

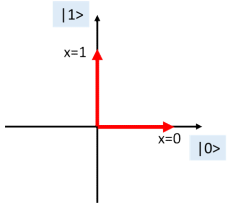
(why)?

A different approach

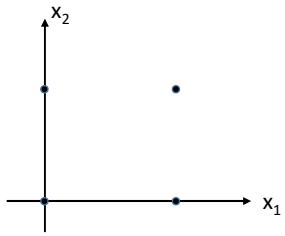
- **1 bit: Old representation**



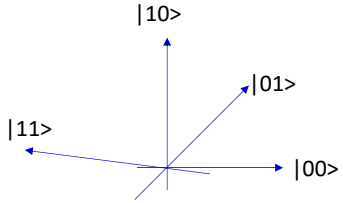
1 bit: New representation



- **2 bits: Old representation**



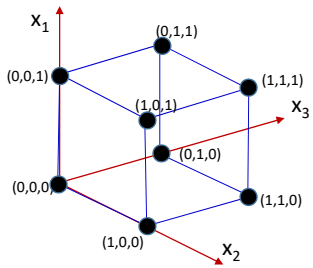
2 bits: New representation



Lame attempt at visualizing 4D

A different approach

- **3 bits: Old representation**



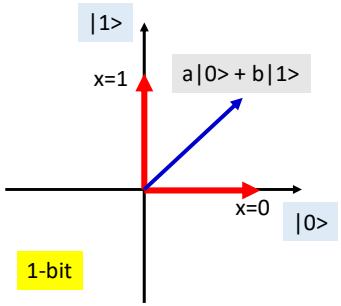
3 bits: New representation

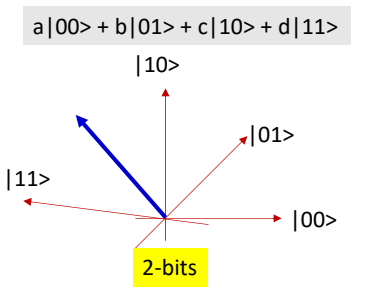
Can't really visualize

(why)?

The modified representation

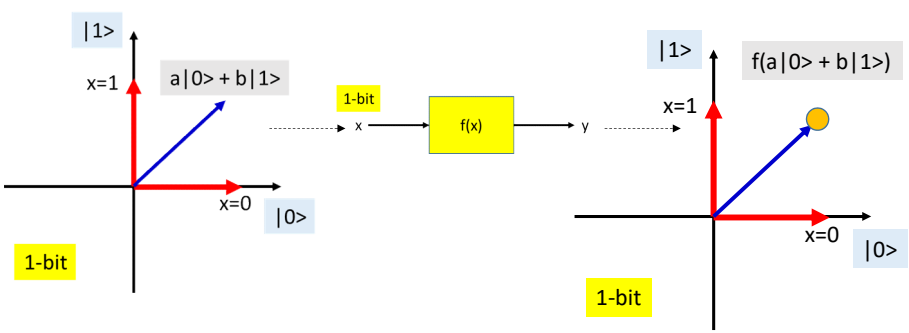
- A vector in this representation is a linear, *unambiguous* combination of *all* input bit patterns
- Unambiguous because we set each bit pattern to be an *orthogonal* direction to every other pattern





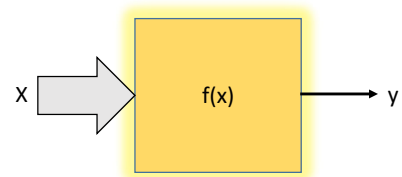
Lame attempt at visualizing 4D

Working with the modified representation



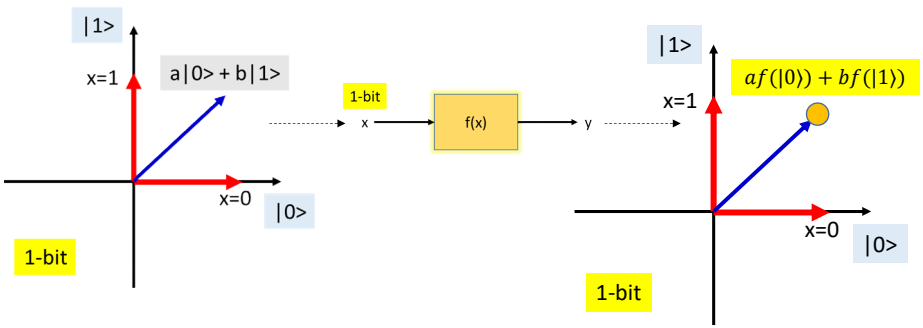
- When the function operates on a vector, it operates on a linear combination of all possible input values
  - How does this help?
  - Not directly, we need to make some assumptions

Adjustment 1: Linear functions



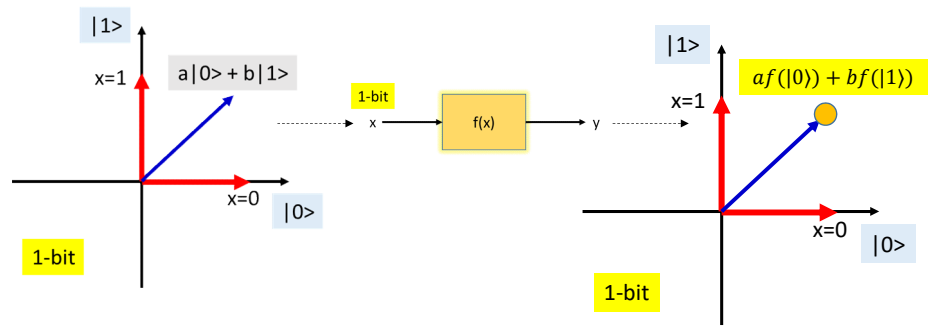
- A function $f(x)$ is *linear* if
$$f(ax + by) = af(x) + bf(y)$$
for any two scalars a and b
- We assume our function $f(x)$ to be linear
  - As it happens, Boolean functions can always be cast as linear operators

For linear f(x)



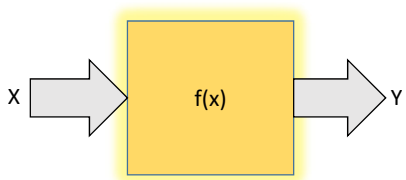
- For linear f(x), the output is a linear combination of the outputs for the individual bit patterns!
- By simply measuring the output at a *single* input vector, we obtain the combined outputs for *all* input bit patterns!
  - *One evaluation!!* (As opposed to 2^N)
- But are we done yet?

For linear f(x)



- The combined output for the individual bit patterns doesn't tell us what the output is for any *single* bit pattern
  - I.e you cant divine $f(|0\rangle)$ and $f(|1\rangle)$ from $af(|0\rangle) + bf(|1\rangle)$
- We need the output to maintain the distinction
  - The function must separately compute the output for each input combination and keep the answers distinct

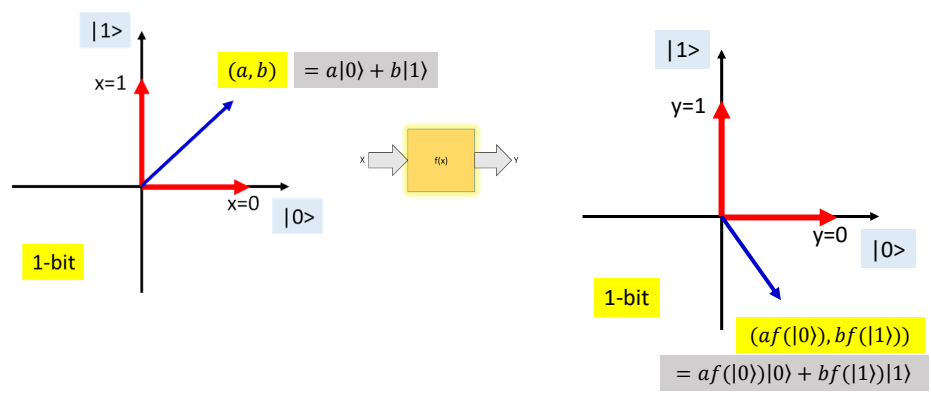
Adjustment 2: Vector functions



- The output too is a vector

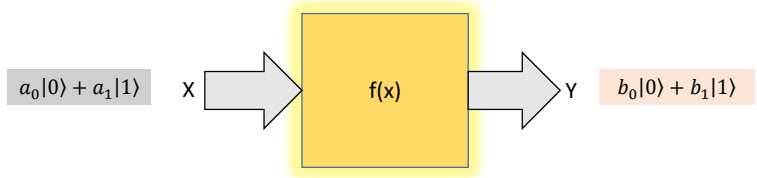
$$f(a|0\rangle + b|1\rangle) = af(|0\rangle)|0\rangle + bf(|1\rangle)|1\rangle$$

For linear f(x)



- Instead of merely computing a value at the vector, the function moves the vector to a new position, where the individual components represent the responses to individual bit patterns
  - Amazingly enough, every Boolean function can be recast in this manner

Adjustment 2: Vector functions



- $f(.)$is a linear transform

$$f \circ \begin{bmatrix} a_0 \\ a_1 \end{bmatrix} = \begin{bmatrix} b_0 \\ b_1 \end{bmatrix}$$

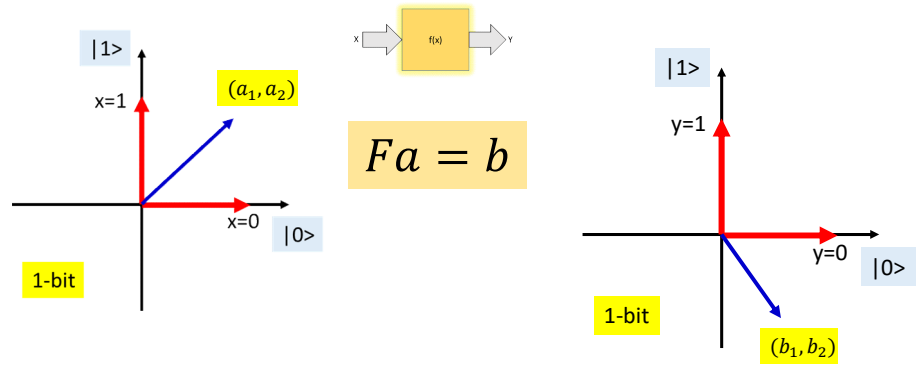
- More generally:

$$f \circ \begin{bmatrix} a_{00\ldots0} \\ a_{00\ldots1} \\ \vdots \\ a_{11\ldots1} \end{bmatrix} = \begin{bmatrix} b_{00\ldots0} \\ b_{00\ldots1} \\ \vdots \\ b_{11\ldots1} \end{bmatrix}$$

In other words $f()$ is a matrix operator.

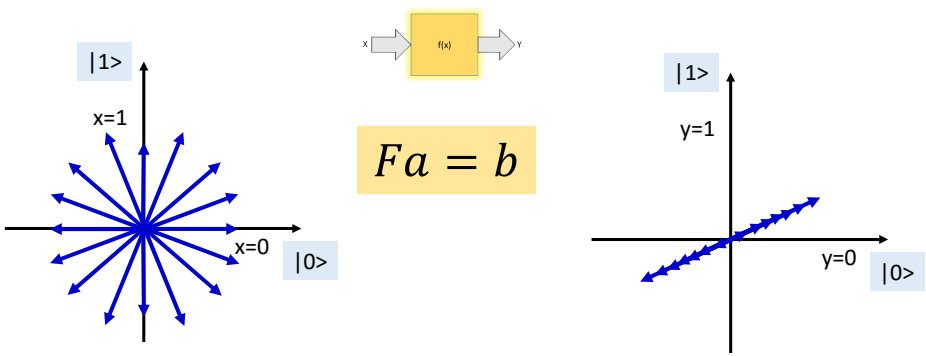
Note that this is a linear operation

For f(x) to retain information



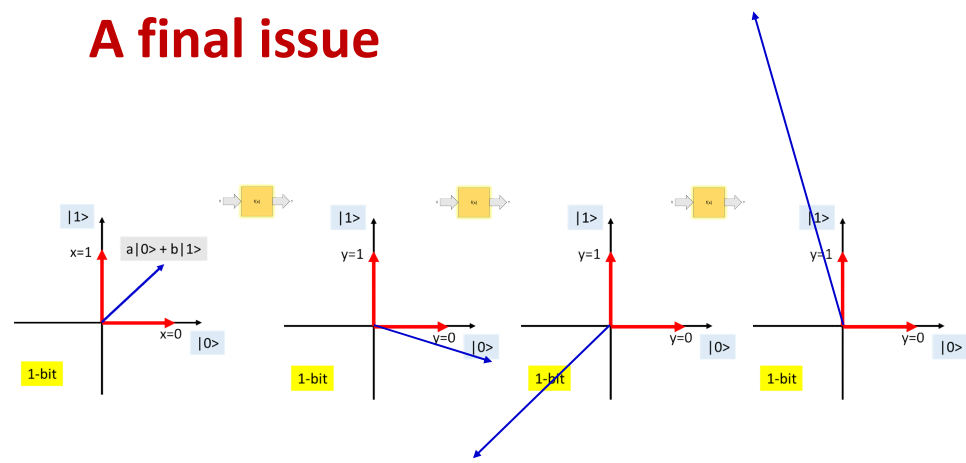
- The function is a linear transform that transforms an input vector to an output vector
  - In the process, it determines the output for *every input bit pattern* in *one step!!*
  - A single computation uncovers the entire function!
  - But there is one more requirement… (what)?

For f(x) to retain information



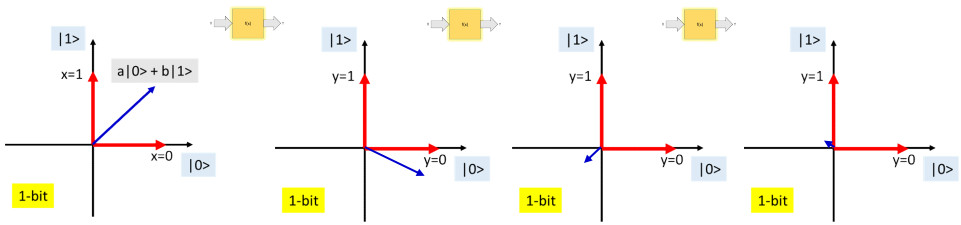
- F must be full rank
  - Otherwise we cannot recover the contribution of all components of the input vector
    - I.e. we cannot resolve the contributions of all bit patterns to the result
- In other words F must be *invertible!!*

A final issue



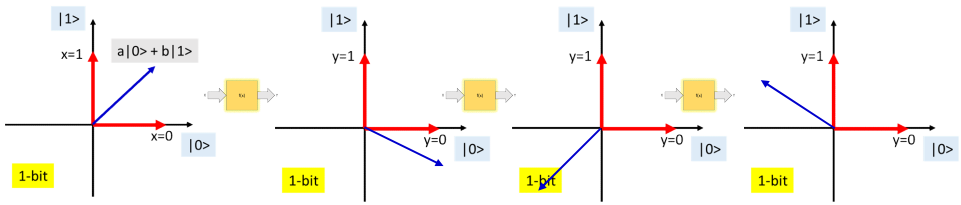
- Repeated applications of linear transforms can make a vector longer and longer and blow up…

A final issue



- Repeated applications of linear transforms can make a vector longer and longer and blow up…
- … or shrink and vanish

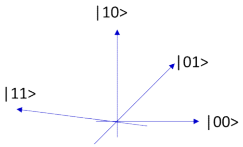
The solution



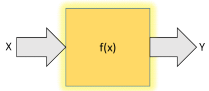
- F must not change the length of the vector
- i.e. it must be a rotation transform!

The new paradigm

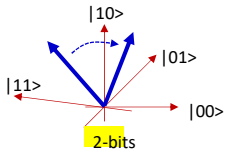
- Modified representation: Every bit *pattern* is an orthogonal direction of the input space
  - A vector in this space is a linear combination of all bit patterns



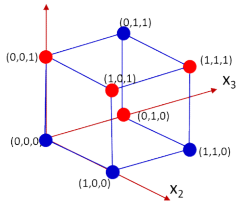
- The function being computed is representable as an invertible linear transform
  - More specifically a rotation

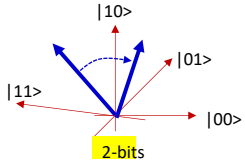


- Evaluation of the function on a single vector can compute the output for every possible bit pattern, in an identifiable way



Old vs. the new paradigm

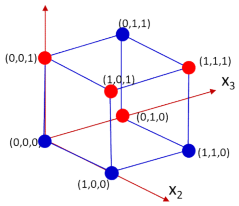


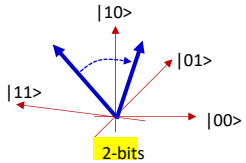


- Each bit is a coordinate dimension
- Must explicitly evaluate function for every input to fully determine it
- In reverse: Given only the output, must evaluate every input to determine which one generated it
  - 2^Ncomputations

- Each bit pattern is a coordinate dimension
- A single evaluation fully determines the function
- In reverse: Given an output, determining which input produced it is a single-step computation
  - Because computation is reversible

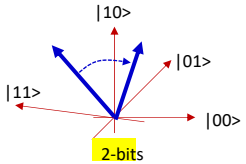
Where is this useful





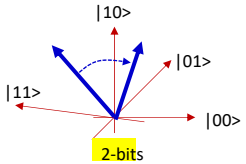
- Satisfiability problems
  - Does any bit pattern produce the output 1
- Search problems
  - Is any bit pattern in my library exactly equal to 11001010
    - Equivalent to SAT problems
- Combinatorial optimization problems
- ....
- Any problem that can be set as a SAT problem

What are the practical issues?



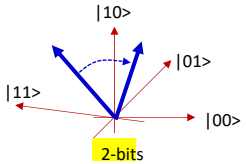
- Is this practically realizable?

What are the practical issues?



- Is this practically realizable?
- A conventional (classical) computer requires a *single* N-bit register to represent a value
  - A function takes in a single N-bit value and produces a single bit
- The new representation requires 2^N numbers to represent a single value!
  - For even N=100 bits, this requires ~1000000000000000000000000000000 numbers
  - A function take in 2^{100} values and produces 2^{100} values
    - I.e it's a 2^{200}-valued transform!
  - Which is why its not a very *useful* way of thinking about things
- Is there a *parsimonious* way of representing a 2^{100} component vector without taking up the entire universe?

What are the practical issues?



Fact that may only interest me: "Graham's number" is a number that's so large there isn't enough space in the universe to write it..

- Is this practically realizable?
- A conventional (classical) computer requires a *single* N-bit register to represent a value
  - A function takes in a single N-bit value and produces a single bit
- The new representation requires 2^N numbers to represent a single value!
  - For even N=100 bits, this requires ~1000000000000000000000000000000 numbers
  - A function take in 2^{100} values and produces 2^{100} values
    - I.e it's a 2^{200}-valued transform!
  - Which is why its not a very *useful* way of thinking about things
- Is there a *parsimonious* way of representing a 2100 component vector without taking up the entire universe?

Enter.. The cat!!

- Introducing Quantum, the cat

The world according to Schroedinger

$$ih\frac{d}{dt}|\psi(t)\rangle = 2\pi H|\psi(t)\rangle$$

- The magical formula that represents the quantum number 42

The world according to Schroedinger

$$ih\frac{d}{dt}|\psi(t)\rangle = 2\pi H|\psi(t)\rangle$$

- The magical formula that represents the quantum number 42
- The wave function!
  - For any physical system you have a wave function and a Hamiltonian
    - Which you could design

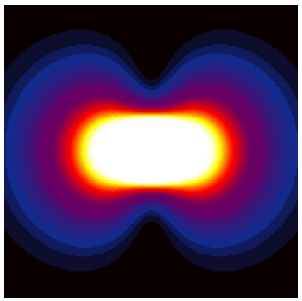
The wave function for any particle predicts its probability

$$\psi(t,x)$$

$|\psi(t,x)|^2$ is the probability that the system will be in configuration x at time t

- What does this mean

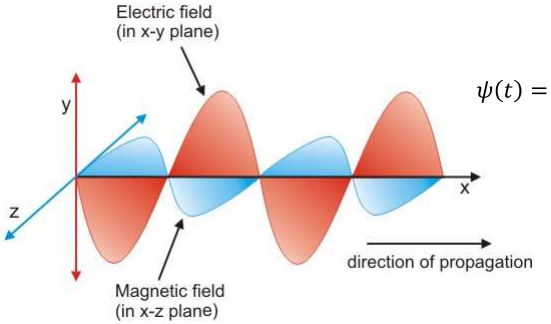
The hydrogen atom



$\psi(t) = \alpha(t)|0\rangle + \beta(t)|1\rangle$

- The probability of the electron in the hydrogen molecule

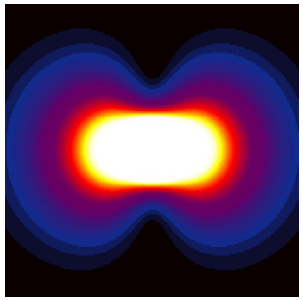
The polarization of light

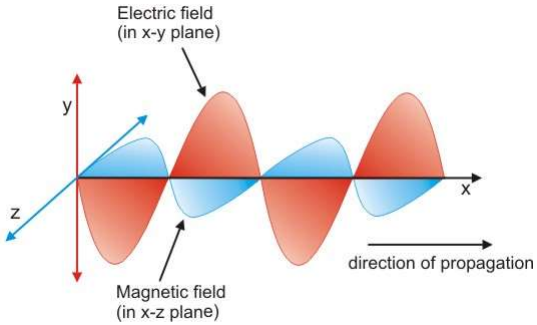


$\psi(t) = \alpha(t)|0\rangle + \beta(t)|1\rangle$

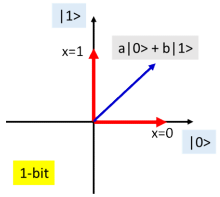
- How do polarizing glasses work?
  - Send through the component of the E/M fields that are aligned with the polarizer
- The light actually exists in both polarizations at the same time

Quantum systems



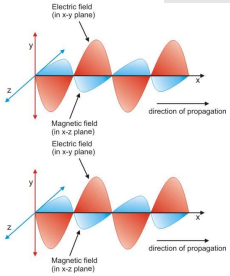


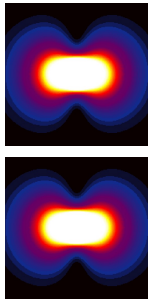
- Quantum systems naturally exist in a superposition of multiple values
  - If we assign each value to a bit value (or bit pattern), we get a quantum computing platform



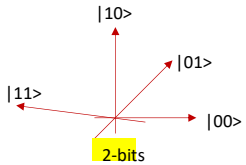
Multiple bits

a|00> + b|01> + c|10> + d|11>

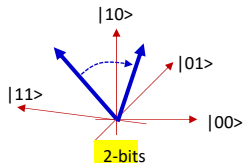




- Increasing the number of bits only takes increasing the number of basic quantum units

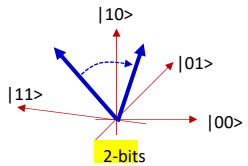


Practical implementation



- Simply use a collection of quantum bits
  - Will simultaneously represent all states
- What is missing?

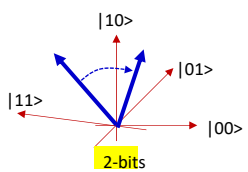
Practical implementation



- Simply use a collection of quantum bits
  - Will simultaneously represent all states
- What is missing?
  - How do you implement the functions?
    - Invertible rotations $ih\frac{d}{dt}|\psi(t)\rangle = 2\pi H|\psi(t)\rangle$

But first you must design the functions (we will see how)

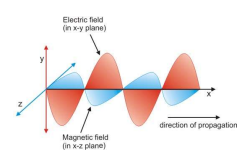
Practical implementation



- Simply use a collection of quantum bits
  - Will simultaneously represent all states
- What is missing?
  - How do you implement the functions?
    - Invertible rotations $ih\frac{d}{dt}|\psi(t)\rangle = 2\pi H|\psi(t)\rangle$
  - How do you measure the output vectors?

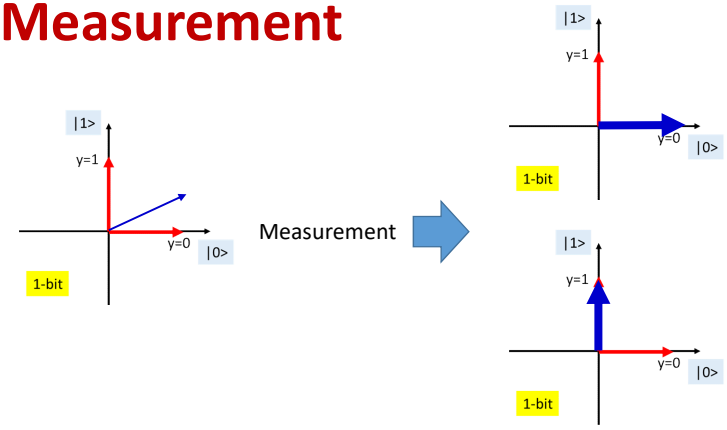
The problem with measurement

- **Reality Doesn't Exist Until We Measure It, Quantum Experiment Confirms**
- https://www.sciencealert.com/reality-doesn-t-exist-until-we-measure-it-quantum-experiment-confirms



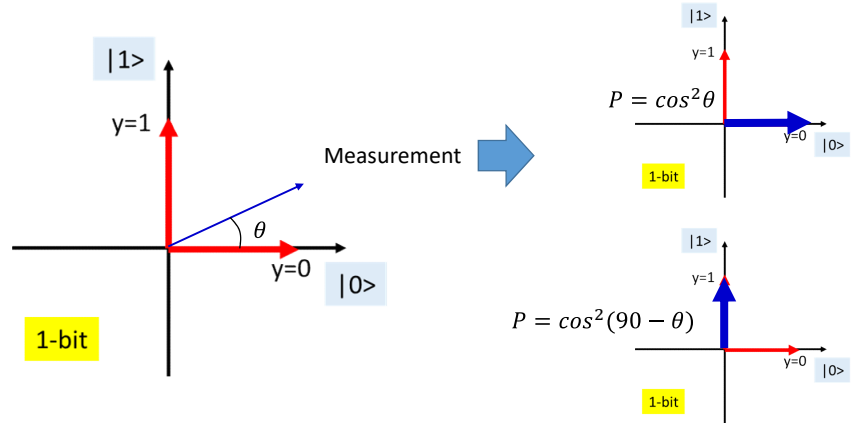
- Measuring an quantum variable "collapses" it

Measurement

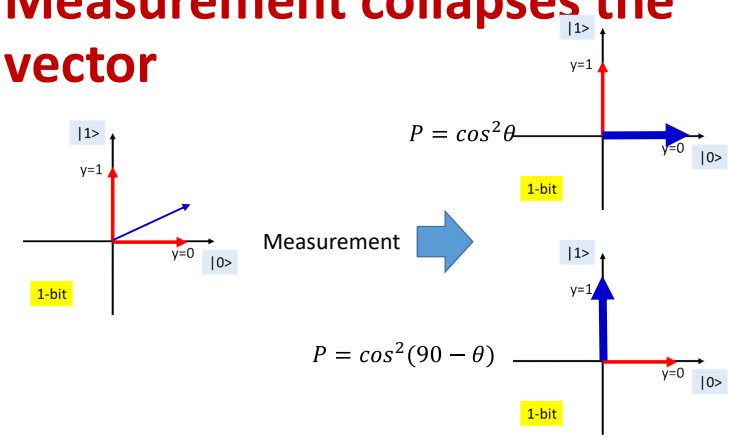


- Measuring the output collapses the vector to one of the states
  - Bit pattern
- Which one

Measurement

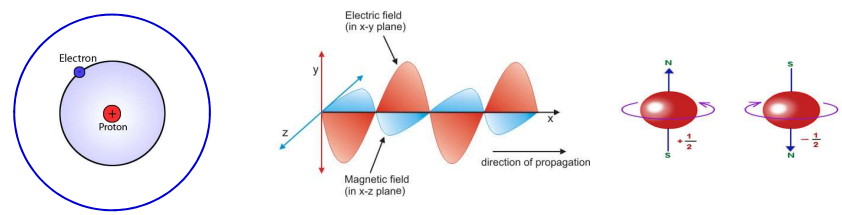


Measurement collapses the vector



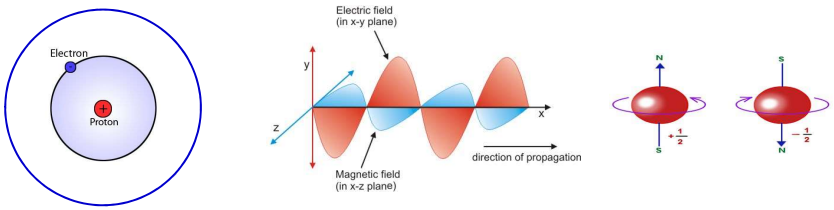
- How many measurements must you take
  - Keeping in mind that each measurement means creating and manipulation “qbits” from scratch
- How does this depend on f(x)

The physical Qubit



- Hydrogen atom electron:
  - Ground state = |0>, excited state = |1>
- Photon polarization
  - Horizontal = |0>, vertical = |1>
- Electron spin
  - NS = |0>, SN = |1>

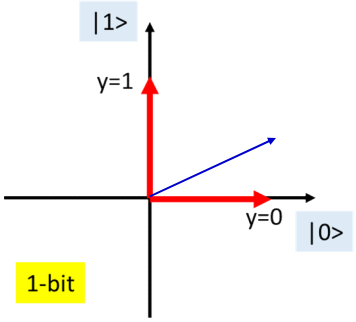
The physical Qubit



- Hydrogen atom electron:
  - Ground state = |0>, excited state = |1>
- Photon polarization
  - Horizontal = |0>, vertical = |1>
- Electron spin
  - NS = |0>, SN = |1>

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

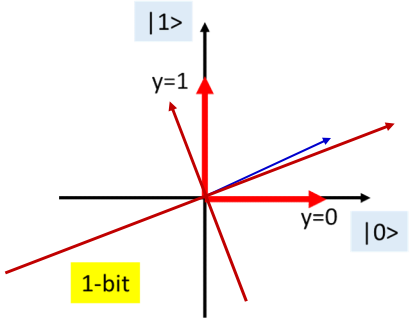
The physical Qubit



- Hydrogen atom electron:
  - Ground state = |0>, excited state = |1>
- Photon polarization
  - Horizontal = |0>, vertical = |1>
- Electron spin
  - NS = |0>, SN = |1>

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

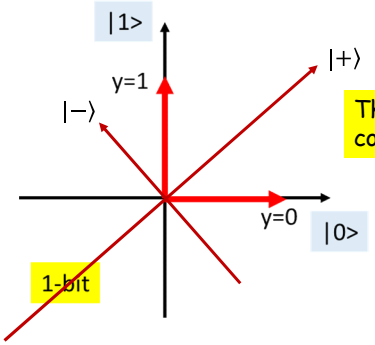
The physical Qubit



- Hydrogen atom electron:
  - Ground state = |0>, excited state = |1>
- Photon polarization
  - Horizontal = |0>, vertical = |1>
- Electron spin
  - NS = |0>, SN = |1>

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

The physical Qubit

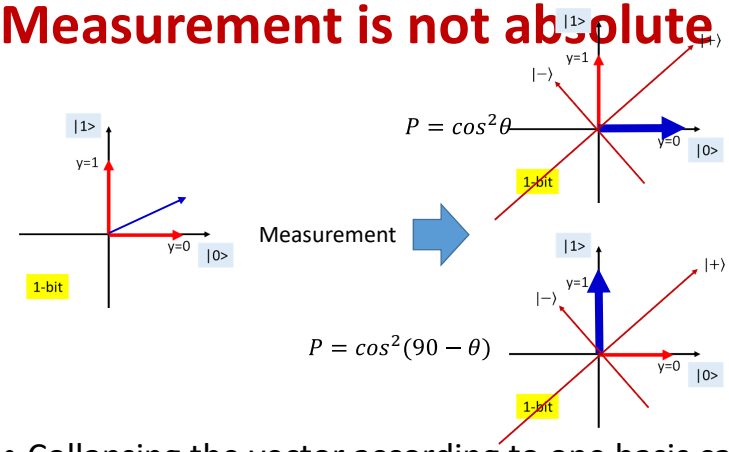


The plus/minus bases are commonly invoked

- Hydrogen atom electron:
  - Ground state = |0>, excited state = |1>
- Photon polarization
  - Horizontal = |0>, vertical = |1>
- Electron spin
  - NS = |0>, SN = |1>

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

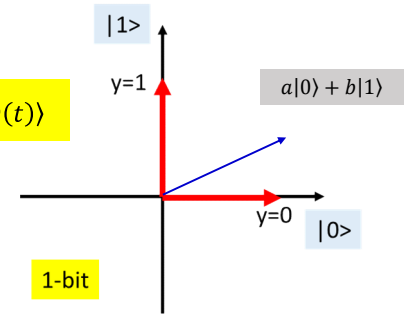
Measurement is not absolute



- Collapsing the vector according to one basis can still keep it indeterminate for other bases!
  - We will use this factor

Its all complex, but not at all complicated

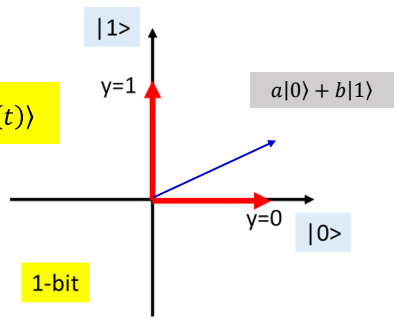
$$ih\frac{d}{dt}|\psi(t)\rangle = 2\pi H|\psi(t)\rangle$$



- The "weights" a and b are actually complex variables
  - Because Schroedinger's equation describes them as complex
- This simple visualization is *wrong*
  - Its missing two dimensions
    - The imaginary components of a and b

Visualizing a qubit

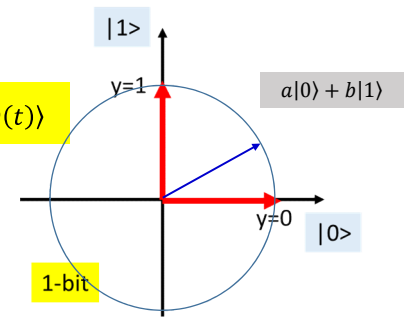
$$ih\frac{d}{dt}|\psi(t)\rangle = 2\pi H|\psi(t)\rangle$$



- The "weights" a and b are actually complex variables
  - Because Schroedinger's equation describes them as complex
- This simple visualization is *wrong*
  - Its missing two dimensions
    - The imaginary components of a and b

Restrictions on the weights

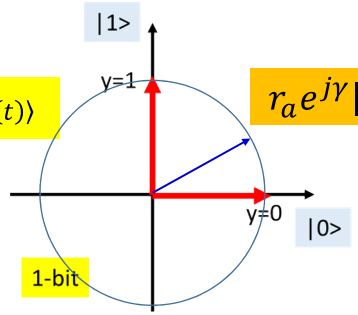
$$ih\frac{d}{dt}|\psi(t)\rangle = 2\pi H|\psi(t)\rangle$$



- $|a|^2 + |b|^2 = 1$
  - The qubits live on the surface of a hypersphere
- $P(|0\rangle) = |a|2, P(|1\rangle) = |b|2$
- $a = r_a e^{j\gamma}, b = r_b e^{j\delta}$
  - What is the relation between r_a and r_b

Restrictions on the weights

$$ih\frac{d}{dt}|\psi(t)\rangle = 2\pi H|\psi(t)\rangle$$

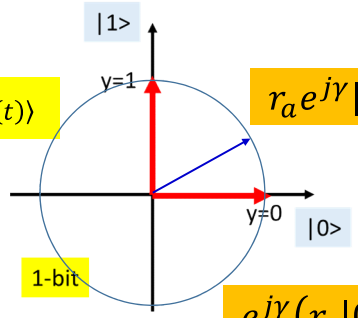


$$r_a e^{j\gamma}|0\rangle + r_b e^{j\delta}|1\rangle$$

- $|a|^2 + |b|^2 = 1$
  - The qubits live on the surface of a hypersphere
- $P(|0\rangle) = |a|2, P(|1\rangle) = |b|2$
- $a = r_a e^{j\gamma}, b = r_b e^{j\delta}$
  - What is the relation between r_a and r_b

Restrictions on the weights

$$ih\frac{d}{dt}|\psi(t)\rangle = 2\pi H|\psi(t)\rangle$$



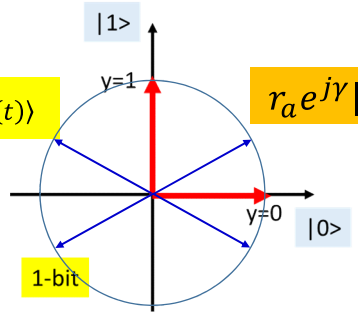
$$r_a e^{j\gamma}|0\rangle + r_b e^{j\delta}|1\rangle$$

$$e^{j\gamma}\left(r_a|0\rangle + r_b e^{j\delta-\gamma}|1\rangle\right)$$

- $|a|^2 + |b|^2 = 1$
  - The qubits live on the surface of a hypersphere
- $P(|0\rangle) = |a|2, P(|1\rangle) = |b|2$
- $a = r_a e^{j\gamma}, b = r_b e^{j\delta}$
  - What is the relation between r_a and r_b

Something odd

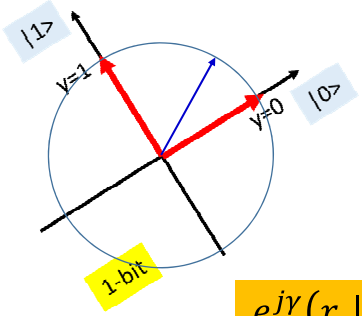
$$ih\frac{d}{dt}|\psi(t)\rangle = 2\pi H|\psi(t)\rangle$$



$$r_a e^{j\gamma}|0\rangle + r_b e^{j\delta}|1\rangle$$

- All of these vectors represent the *same* $P(|0\rangle)$ and $P(|0\rangle)$
- But they're actually different phasors
  - Something we will use all the time

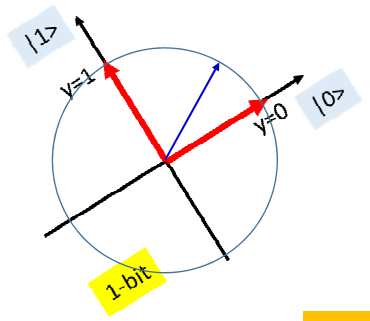
The qubit is rotation invariant



$$e^{j\gamma}\left(r_a|0\rangle + r_b e^{j(\delta-\gamma)}|1\rangle\right)$$

- Rotating the space doesn't matter

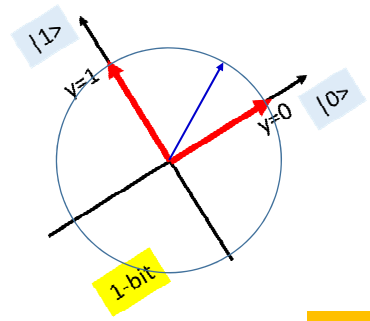
The qubit is rotation invariant



$$r_a|0\rangle + r_b e^{j(\delta-\gamma)}|1\rangle$$

- Rotating the space doesn't matter
  - What is the relation between r_a and r_b

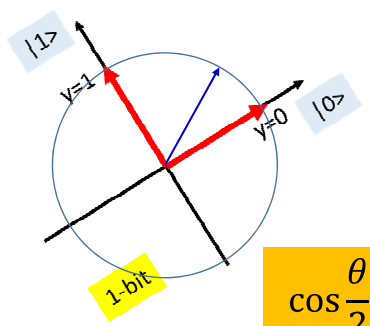
The qubit is rotation invariant



$$r_a|0\rangle + r_b e^{j\phi}|1\rangle$$

- Rotating the space doesn't matter
  - What is the relation between r_a and r_b

The qubit is rotation invariant

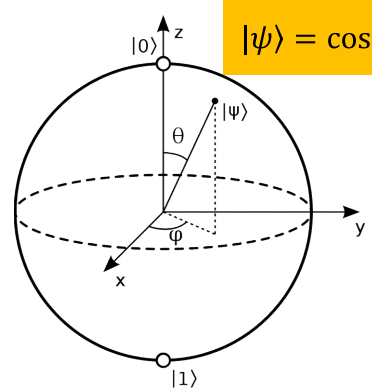


$$\cos\frac{\theta}{2}|0\rangle + \sin\frac{\theta}{2}e^{j\phi}|1\rangle$$

- Rotating the space doesn't matter
  - What is the relation between r_a and r_b
- This is now a two-variable representation of two variables!
  - Can be visualized

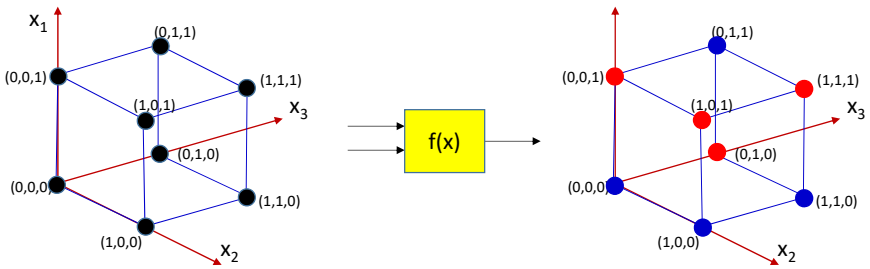
The Bloch Sphere

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + \sin\frac{\theta}{2}e^{j\phi}|1\rangle$$



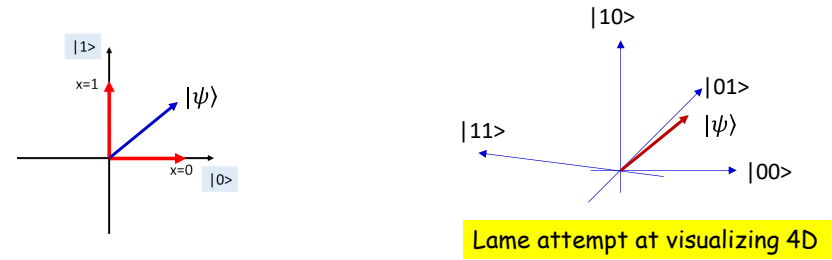
- Visualizing the qubit
  - 2 variable visualization in a 3D space

Recap: Classical math



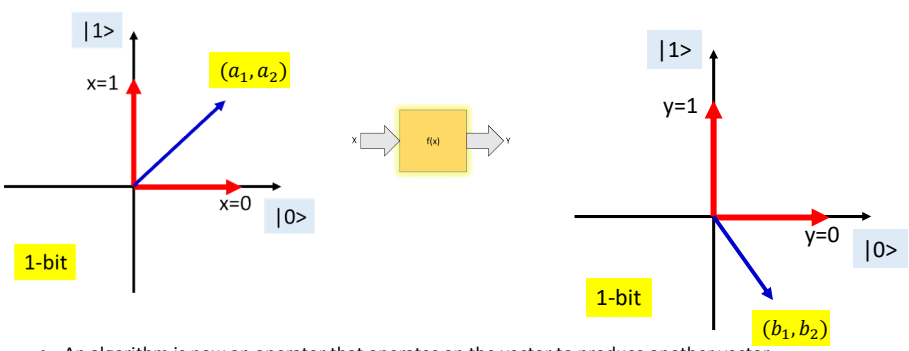
- Algorithms are just functions that operate on bit patterns and produce an output
- Classical approach: For an N-bit input, the function operates on an N-bit input space
  - Each valid bit pattern is a vector in this space
- To fully characterize a unknown glass-box algorithms we must evaluate it on all 2^N feasible inputs
  - Very expensive

Recap: A new binary math



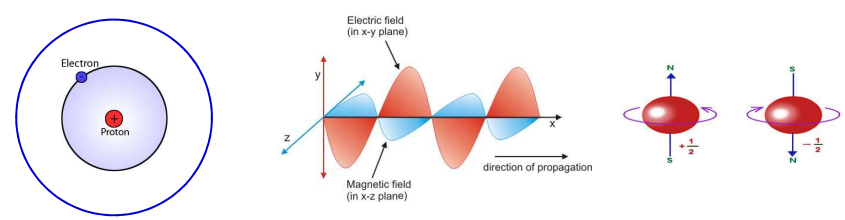
- *Bit patterns* now represent orthogonal directions
- An input is now a vector (a phasor) in this new space
  - And represents a linear combination of bit patterns
  - 1 bit: $|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$
  - 2 bits: $|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle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

Recap: The new "quantum" math



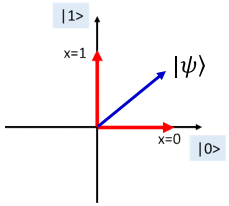
- An algorithm is now an operator that operates on the vector to produce another vector
  - Can now compute the output for *all* bit patterns in a single evaluation step
- Caveats – the operator must be:
  - Linear
  - Invertible
  - And not increase the length of the vector (i.e. it must be a rotation)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

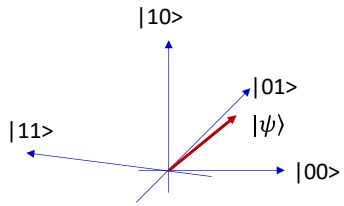
Recap: Implementing the qubit



- 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: $ih\frac{d}{dt}|\psi(t)\rangle = 2\pi H|\psi(t)\rangle$
  - 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: The physical quantum Qubit

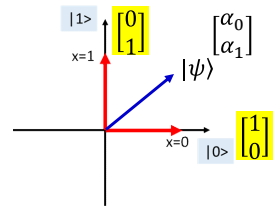


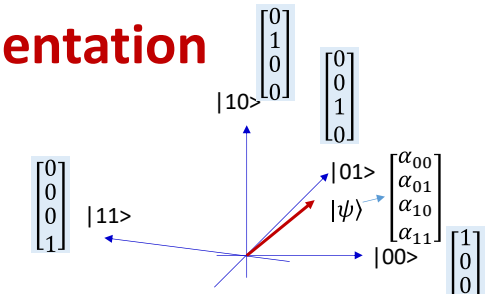


Lame attempt at visualizing 4D

- $|\psi\rangle = \alpha_{00\ldots0}|00\ldots0\rangle + \alpha_{00\ldots1}|00\ldots1\rangle + \cdots + \alpha_{11\ldots1}|11\ldots1\rangle$
- The $\alpha_{00\ldots0}$ terms are all *complex!*
  - *Thanks Heisenberg*
- Cannot even visualize a single qubit
  - One way to visualize 1 qubit: bloch sphere
  - Doesn't really scale

A vector representation





Lame attempt at visualizing 4D

- Write the phasors as a regular vector
- One-qubit phasor

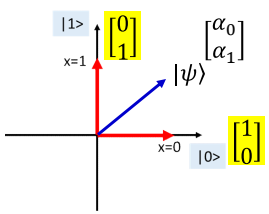
$$|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle = \begin{bmatrix}\alpha_0\\\alpha_1\end{bmatrix}$$

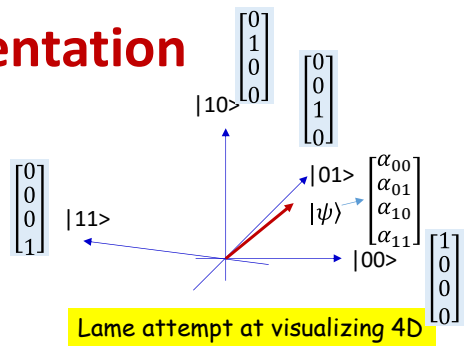
- Two qubit phasor

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle = \begin{bmatrix}\alpha_{00}\\\alpha_{01}\\\alpha_{10}\\\alpha_{11}\end{bmatrix}$$

- The α terms are all *complex!*
  - *Thanks Heisenberg*
- Note the phasors for the basis bit patterns

A vector representation





Lame attempt at visualizing 4D

- Write the phasors as a regular vector
- One-qubit phasor

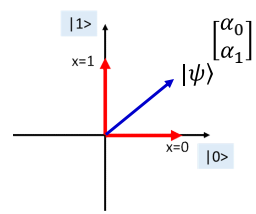
$$|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle = \begin{bmatrix}\alpha_0\\\alpha_1\end{bmatrix}$$

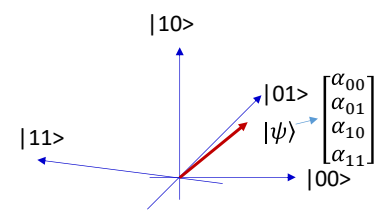
- Two qubit phasor

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle = \begin{bmatrix}\alpha_{00}\\\alpha_{01}\\\alpha_{10}\\\alpha_{11}\end{bmatrix}$$

- The α terms are all *complex!*
  - *Thanks Heisenberg*
- Note the phasors for the basis bit patterns

The problem of measurement





Lame attempt at visualizing 4D

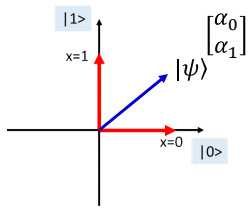
- You cannot measure the phasor
  - It will collapse to one of the bases
- One qubit:

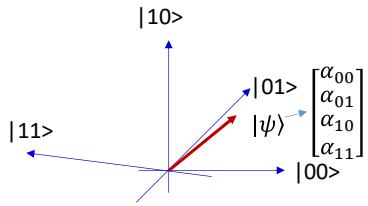
$$\alpha_0|0\rangle + \alpha_1|1\rangle \rightarrow \begin{cases}|0\rangle \; with\ probability\ |\alpha_0|^2 \\ |1\rangle \; with\ probability |\alpha_1|^2\end{cases}$$

- Two qubits:

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

The problem of measurement





Lame attempt at visualizing 4D

Clearly: $\sum|\alpha|^2 = 1$

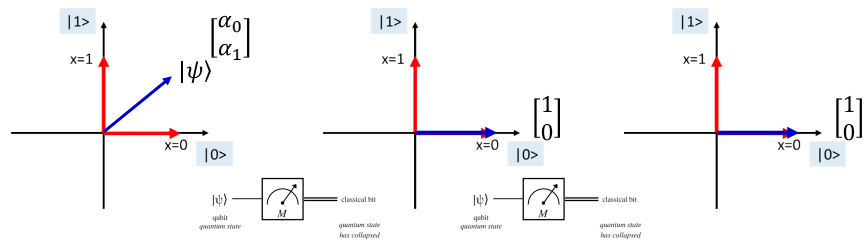
- You cannot measure the phasor
  - It will collapse to one of the bases
- One qubit:

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

- Two qubits:

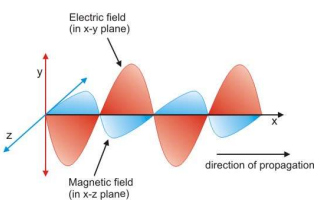
$$\alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle \rightarrow \begin{cases}|00\rangle \; with \; probability \; |\alpha_{00}|^2 \\ |01\rangle \; with \; probability \; |\alpha_{01}|^2 \\ |10\rangle \; with \; probability \; |\alpha_{10}|^2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

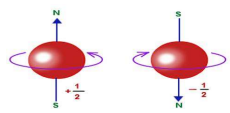
Measurement *fixes* the qubit

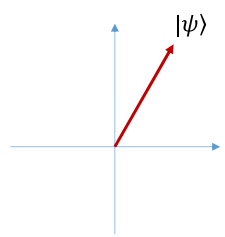


- First measurement: $|\psi\rangle$ → $|0\rangle$ with P = $|\alpha_0|^2$
- Second measurement: $|0\rangle$ → $|0\rangle$ with P = 1
- Third measurement: $|0\rangle$ → $|0\rangle$ with P = 1
- …

The phasors are unique, but the representation is not

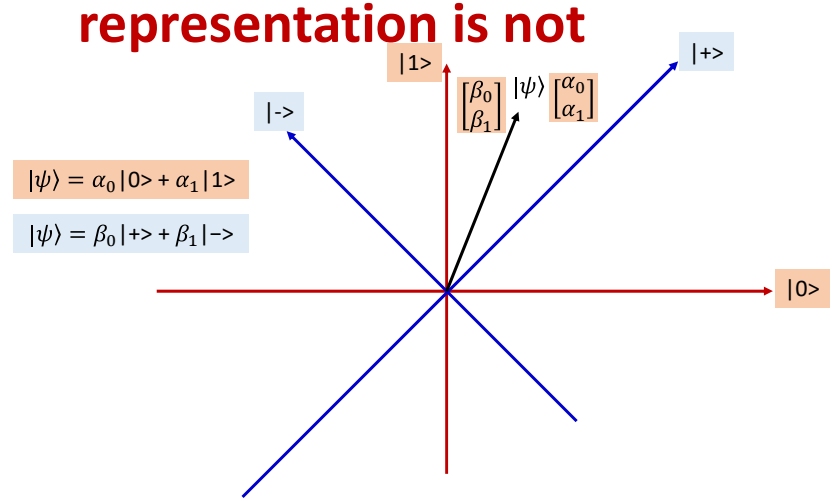






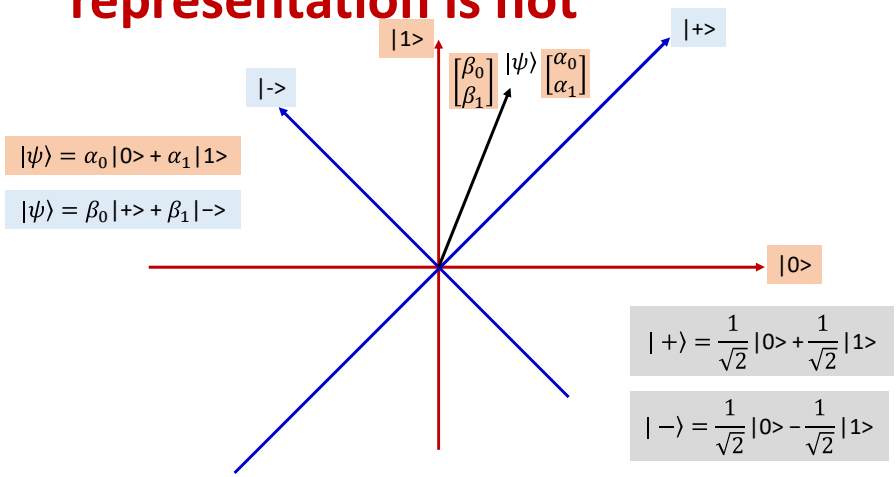
- No absolute definition of direction or sign
  - But the state of the system is well defined!
  - The space is defined, and the direction of the (physical) phasor is well defined
- The actual representation depends on the bases used
  - Only restriction: the bases must be orthogonal

The phasors are unique, the representation is not



- The representation depends on the bases
  - Think orientation of your polarized glasses..

The phasors are unique, the representation is not



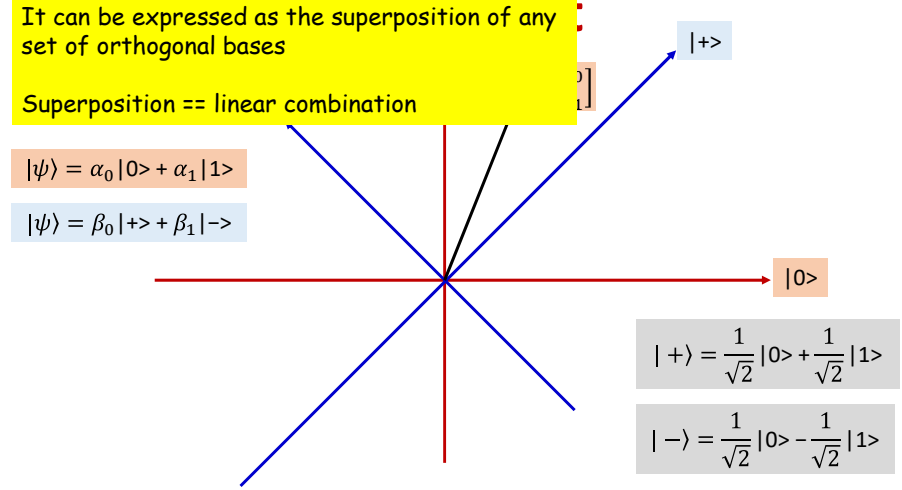
- The representation depends on the bases
  - Think orientation of your polarized glasses..

ue, the

The space of phasors is a complex Hilbert space
A cubit is a vector on a unit sphere in this space

It can be expressed as the superposition of any set of orthogonal bases

Superposition == linear combination



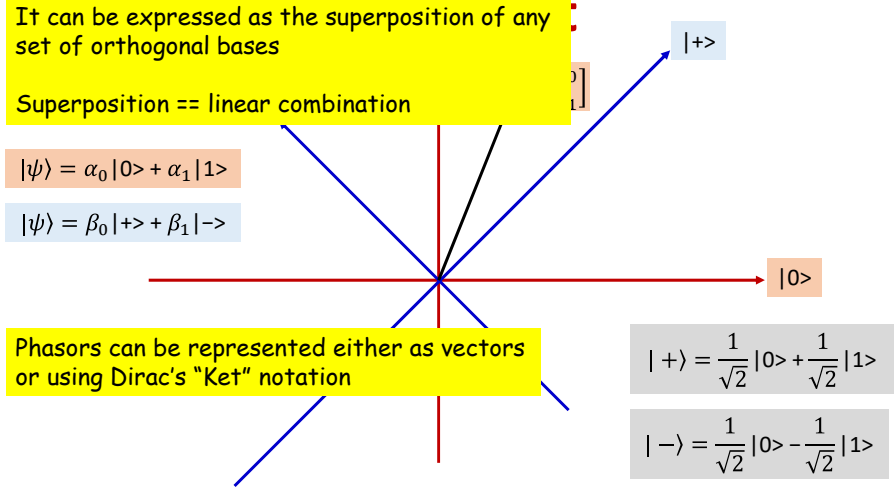
- The representation depends on the bases
  - Think orientation of your polarized glasses..

The space of phasors is a complex Hilbert space
A cubit is a vector on a unit sphere in this space

It can be expressed as the superposition of any set of orthogonal bases

Superposition == linear combination

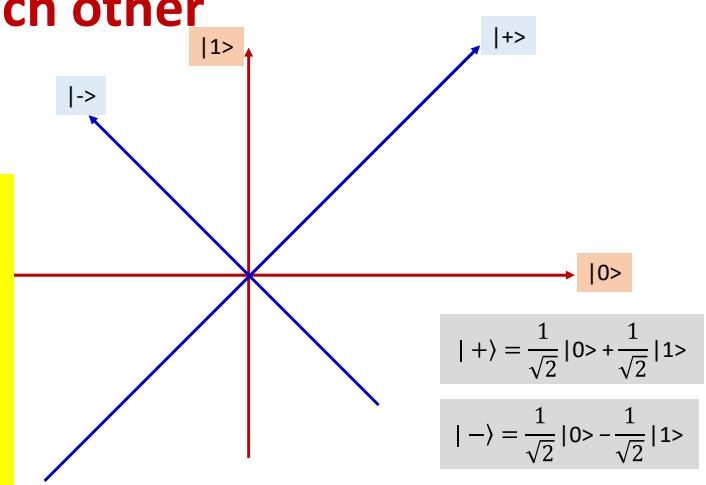
ue, the



Phasors can be represented either as vectors or using Dirac's "Ket" notation

- The representation depends on the bases
  - Think orientation of your polarized glasses..

Bases can be expressed in terms of each other

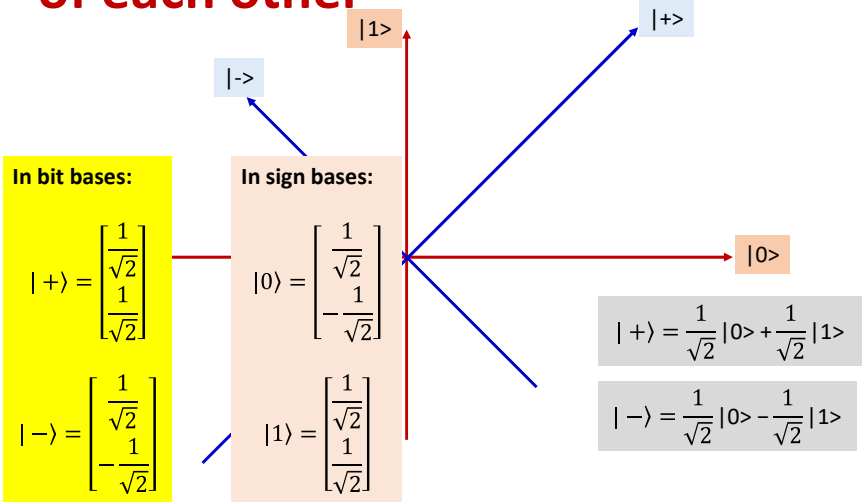


In bit bases:

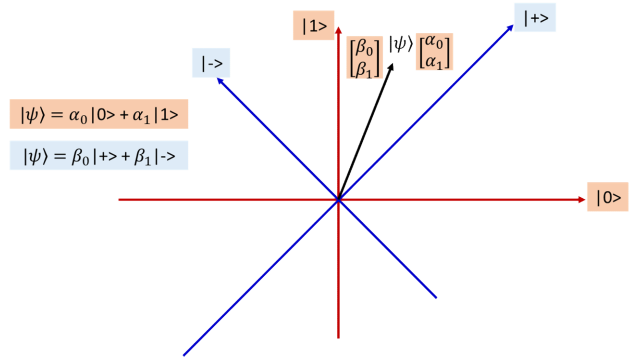
$$|+\rangle = \begin{bmatrix}\frac{1}{\sqrt{2}}\\ \frac{1}{\sqrt{2}}\end{bmatrix}$$

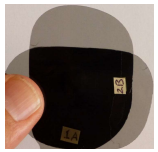
$$|-\rangle = \begin{bmatrix}\frac{1}{\sqrt{2}}\\ -\frac{1}{\sqrt{2}}\end{bmatrix}$$

Bases can be expressed in terms of each other



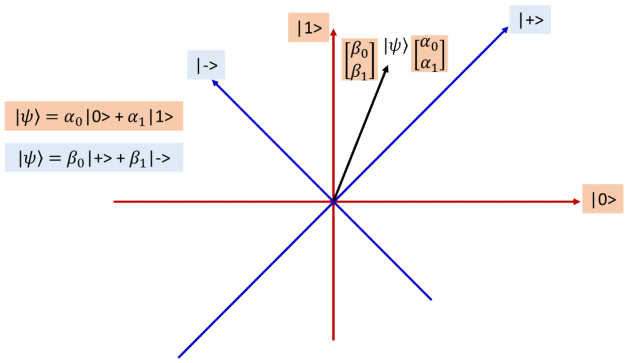
You can *measure* using either bases!!

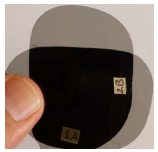


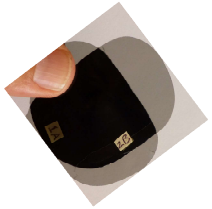


- What are P(|0>) andP(|1>)?
- What are P(|+>) andP(|−>)?

You can *measure* using either bases!!







- What are P(|0>) andP(|1>) ?
- What are P(|+>) andP(|−>) using α_0 and α_1?

So what is measurement

- Measurement *projects* the phasor on the basis with a probability that is the square of the length of the projection
  - Using bit basis representation, but measuring on sign basis:

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

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

So what is measurement

- Measurement *projects* the phasor on the basis with a probability that is the square of the length of the projection
  - Using bit basis representation, but measuring on sign basis:

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

What will be P(|+>) and P(|->) using the sign bases for representation?

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

What will be P(|0>) and P(|1>) using the sign bases for representation?

So what is measurement

- Measurement *projects* the phasor on the basis with a probability that is the square of the length of the projection
  - Using bit basis representation, but measuring on sign basis:

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

What will be P(|+>) and P(|->) using the sign bases for representation?

P(basis) is simply the square of the cosine of the angle between the phasor and the basis

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

What will be P(|0>) and P(|1>) using the sign bases for representation?

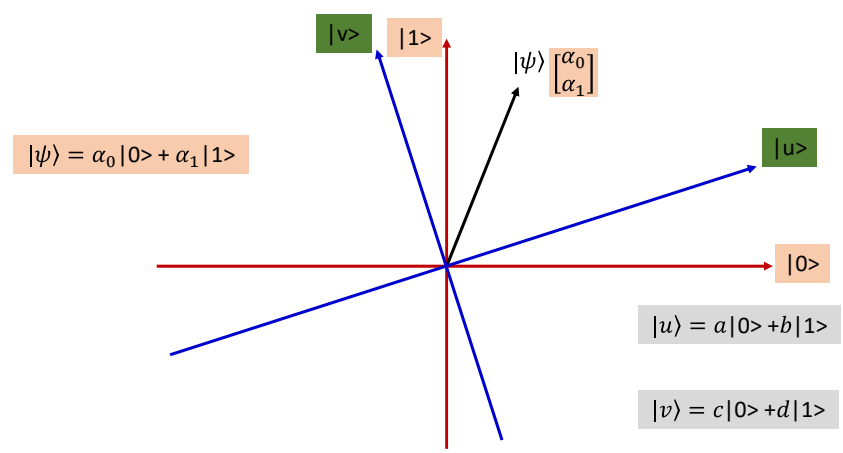
Some basic math

- The projection of a complex vector a on a complex vector b is given by

$$a^H b = \sum_i a_i^* b$$

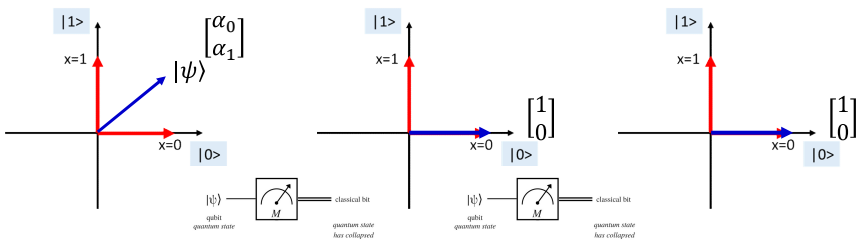
- For unit vectors it is the cosine of the angle between them
- For any basis, the probability of measuring that basis is the square of the cosine between the phasor and the basis

A different basis…



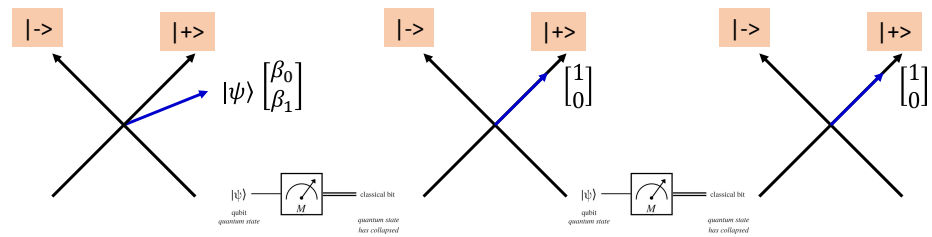
- What would P(|u>) and P(|v>) be?

Measurement *simplifies* life



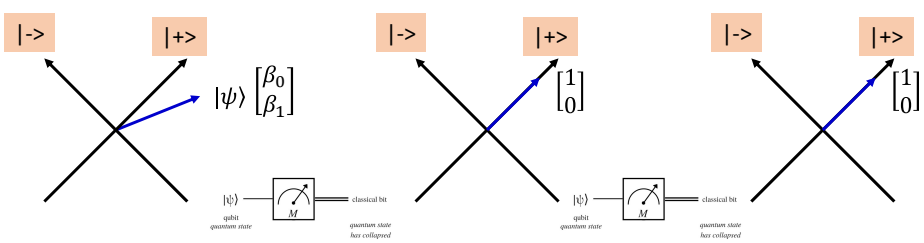
- By fixing the value

Measurement *simplifies* life



- By fixing the value

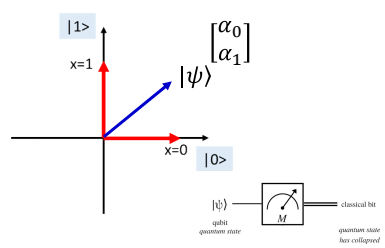
Measurement *simplifies* life



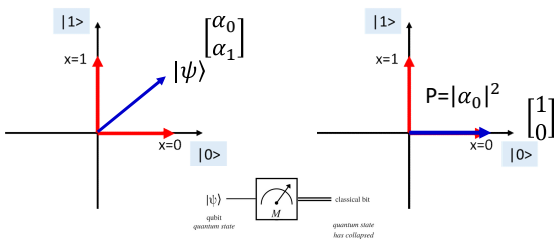
- By fixing the value

- Or does it?

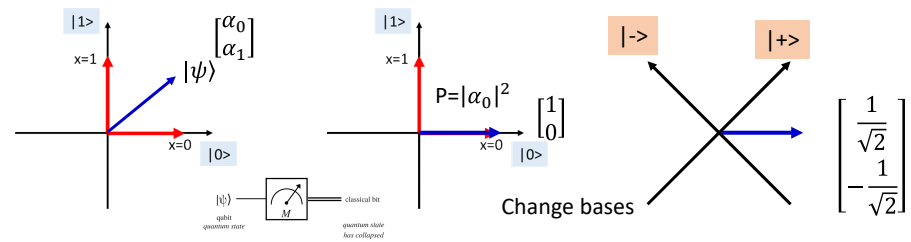
Measurement *simplifies* life



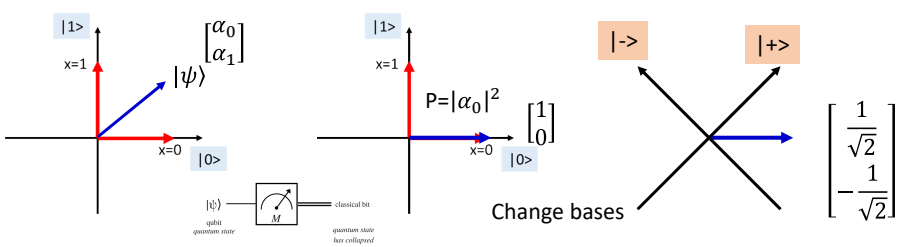
Measurement *simplifies* life

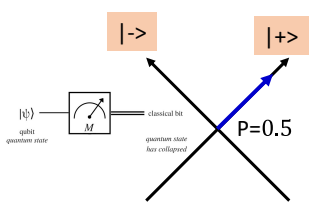


Measurement *simplifies* life

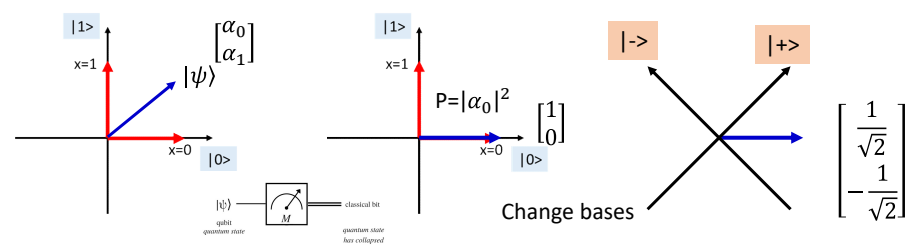


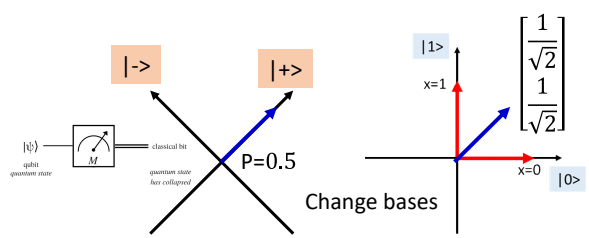
Measurement *simplifies* life



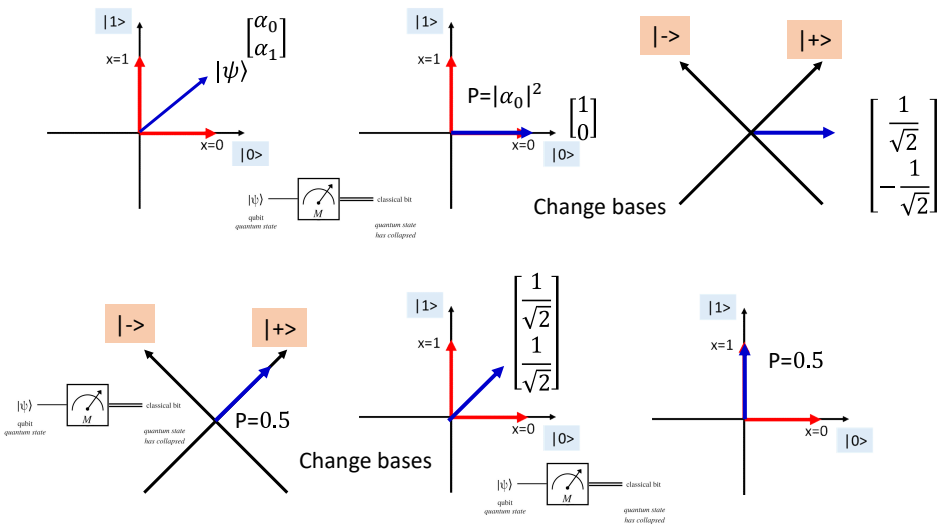


Measurement *simplifies* life

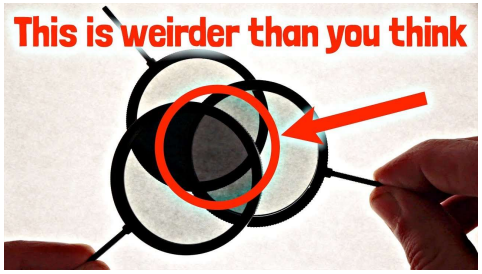




Measurement *simplifies* life

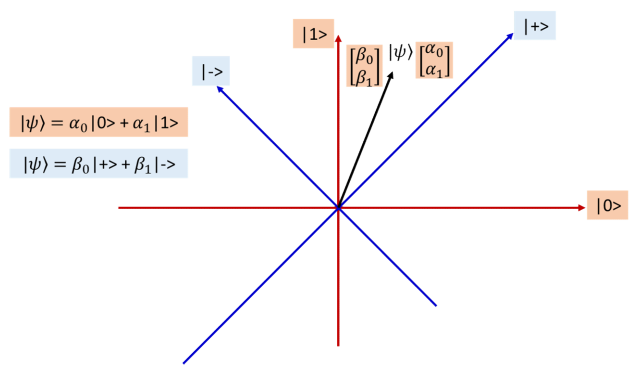


The world isn't what you think it is!!!



- Repeated measurements with different bases can completely alter reality!!!

Uncertainty Principle



- Can a qubit have perfectly unambiguous bit value *and* sign value?
  - Unambiguous bit value: $|\psi\rangle = |0\rangle$ or $|\psi\rangle = |1\rangle$
  - Unambiguous sign value: $|\psi\rangle = |+\rangle$ or $|\psi\rangle = |-\rangle$

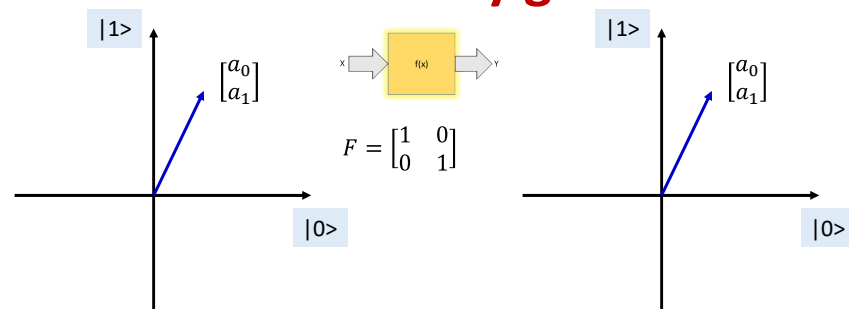
Heisenberg's uncertainty principle

- The "spread" of a phasor along the bit basis is defined as $|\alpha_0| + |\alpha_1|$
  - It is minimum when the bit is unambiguous
  - It is maximum when the phasor is at 45 degrees: $\frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}} = \sqrt{2}$
- For the sign basis, the spread is $|\beta_0| + |\beta_1|$
  - It is minimum when the phasor is aligned to one of the sign bases, i.e at 45 degrees to the bit bases
  - It is maximum when the phasor is aligned to the bit bases and equals $\sqrt{2}$
- More generally $spread(bit)spread(sign) \geq \sqrt{2}$

We've learned about bits, what about gates?

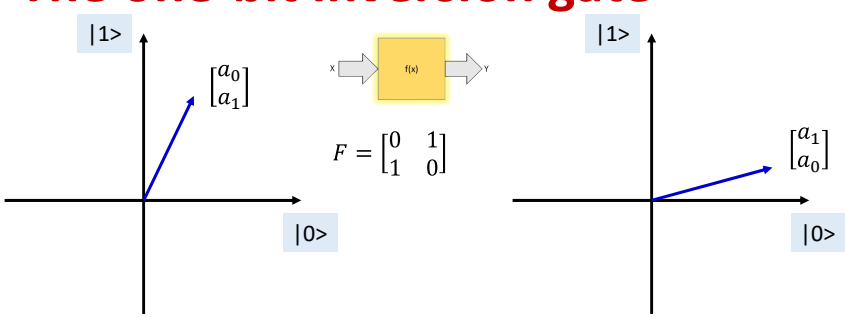
- Simplest gate: The Boolean 1-bit gate
  - How many 1-bit gates can you have?
- How many of these are implementable for the quantum bit?
  - Why
- What do they look like?

The one-bit identity gate



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

The one-bit inversion gate



- The one bit identity gate inversion transform
  - How does it affect |0> and |1>?
  - How does it affect |+> and |->?
- 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?*

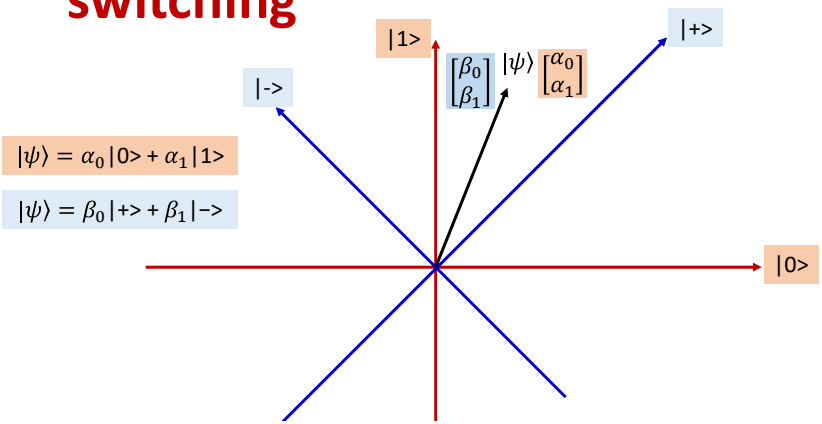
The one-bit inversion gate

From wikipedia

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

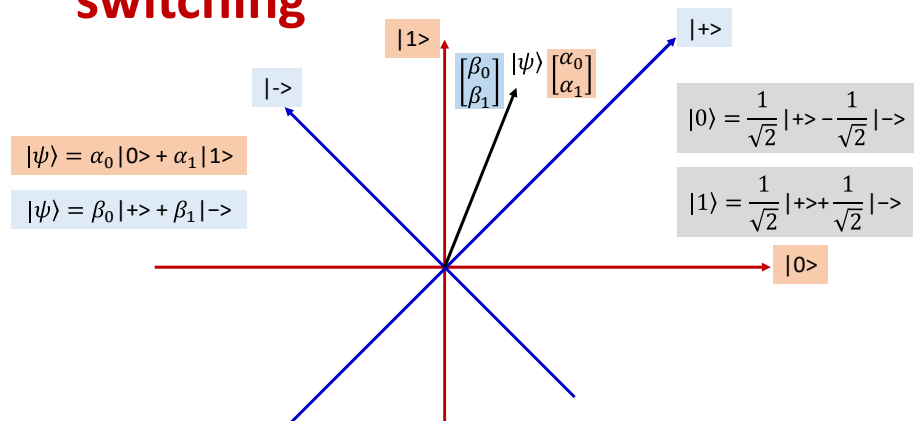
- Which of these are equivalent to classical identity gates?
- Which of these are equivalent to classical negation gates?

The Hadamard gate: Base switching



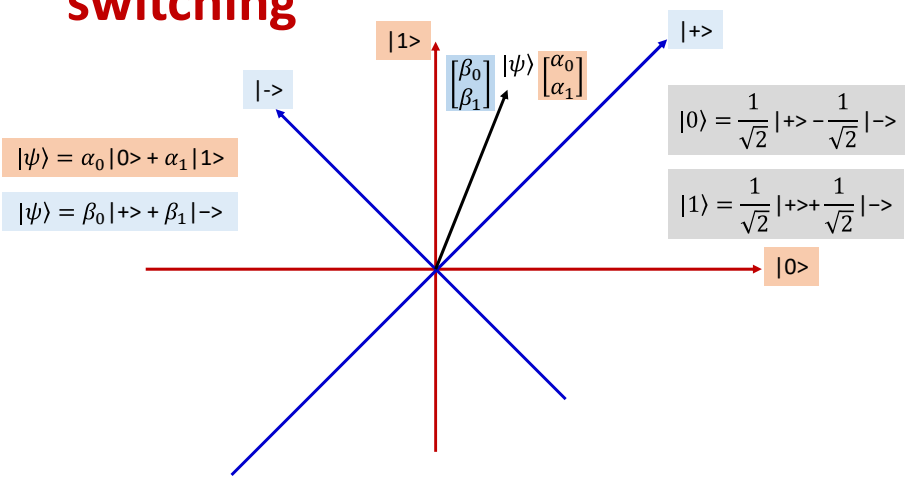
- A vector has different representations in the bit bases and the sign bases
- The Hadamard gates converts the bit-bases representation to the sign bases representation

The Hadamard gate: Base switching



- Can you derive this relation from the above info?

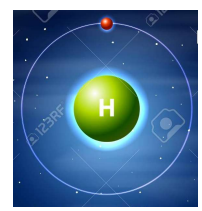
The Hadamard gate: Base switching

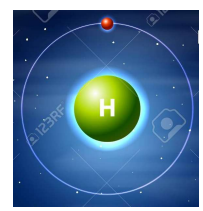


Hadamard (H) $\boxed{\mathbf{H}}$ $\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$

From wikipedia

You can't get very far with one bit



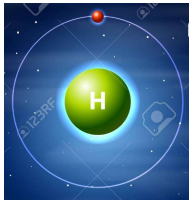


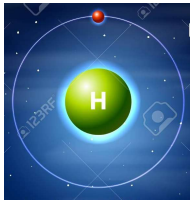
- Two qubits walk into a bar…

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

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

Representing the combined system





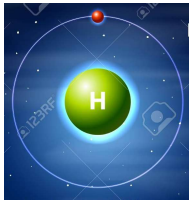
- Two qubits walk into a bar…

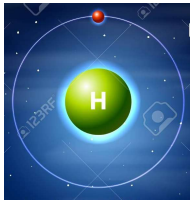
$$|\psi_0\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$$
$$|\psi_1\rangle = \beta_0|0\rangle + \beta_1|1\rangle$$

- 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…

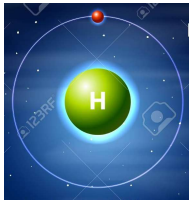
$$|\psi_0\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$$
$$|\psi_1\rangle = \beta_0|0\rangle + \beta_1|1\rangle$$

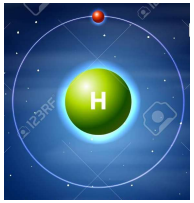
What is $|\psi\rangle$ assuming non-interacting qubits

- 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…

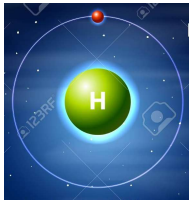
$$|\psi_0\rangle = \alpha_0|+\rangle + \alpha_1|-\rangle$$
$$|\psi_1\rangle = \beta_0|0\rangle + \beta_1|1\rangle$$

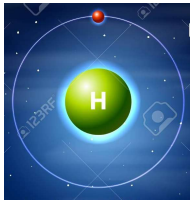
What is $|\psi\rangle$ assuming non-interacting qubits

- 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…

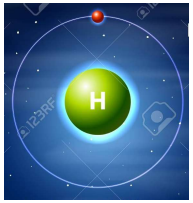
$$|\psi_0\rangle = \alpha_0|+\rangle + \alpha_1|-\rangle$$
$$|\psi_1\rangle = \beta_0|0\rangle + \beta_1|1\rangle$$

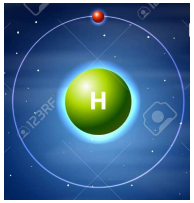
What is $|\psi\rangle$ assuming non-interacting qubits

- 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…

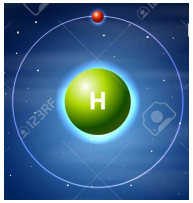
$$|\psi_0\rangle = \alpha_0|+\rangle + \alpha_1|-\rangle$$
$$|\psi_1\rangle = \beta_0|0\rangle + \beta_1|1\rangle$$

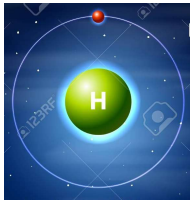
What is $|\psi\rangle$ assuming non-interacting qubits

- 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?

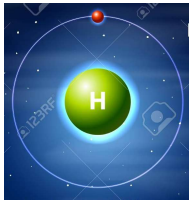
The *Kronecker* product of two vectors

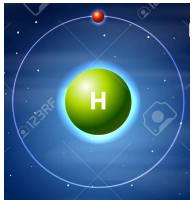
$$\begin{bmatrix}\alpha_0\\ \alpha_1\end{bmatrix} \otimes \begin{bmatrix}\beta_0\\ \beta_1\end{bmatrix} = \begin{bmatrix}\alpha_0\begin{bmatrix}\beta_0\\ \beta_1\end{bmatrix}\\ \alpha_1\begin{bmatrix}\beta_0\\ \beta_1\end{bmatrix}\end{bmatrix} = \begin{bmatrix}\alpha_0\beta_0\\ \alpha_0\beta_1\\ \alpha_1\beta_0\\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

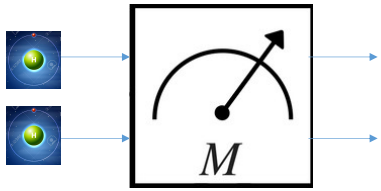
- In Ket notation

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

Measuring the two-cubit system



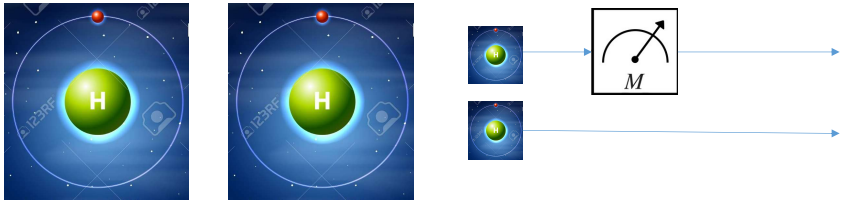




$$|\psi\rangle = \gamma_{00}|00\rangle + \gamma_{01}|01\rangle + \gamma_{10}|10\rangle + \gamma_{11}|11\rangle$$

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

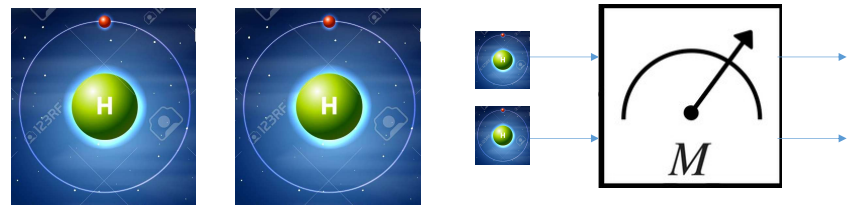
Measuring the two-cubit system



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

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

Simultaneous measurement



- Two qubits walk into a bar…

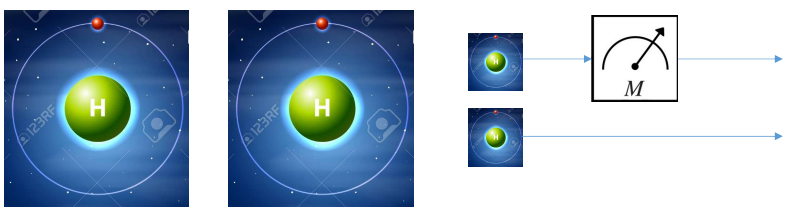
$$|\psi_0\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$$
$$|\psi_1\rangle = \beta_0|0\rangle + \beta_1|1\rangle$$

Assuming non-interacting qubits

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

- What will measurement give us and with what probability

Individual measurement



- Two qubits walk into a bar…

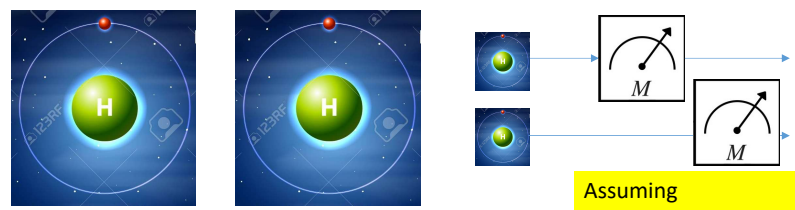
$$|\psi_0\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$$
$$|\psi_1\rangle = \beta_0|0\rangle + \beta_1|1\rangle$$

Assuming non-interacting qubits

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

- 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

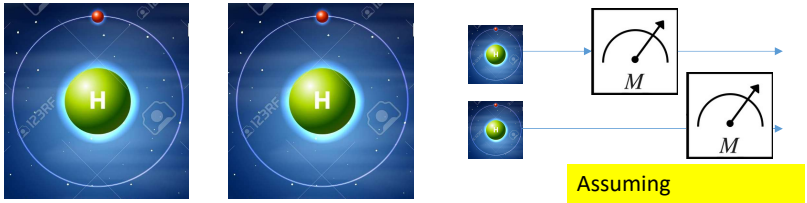
- Two qubits walk into a bar…

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

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

- 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…

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

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

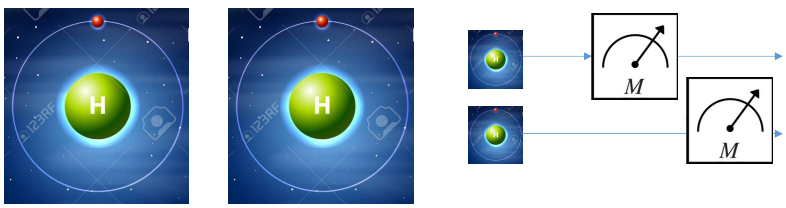
- You measured bit 0 and got a 0.
  - Then you measure bit 1. What is the probability of getting a 0?
- You measured bit 0 and got a 1
  - Then you measure bit 1. What is the probability of getting 0?

Individual measurement

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

- 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?

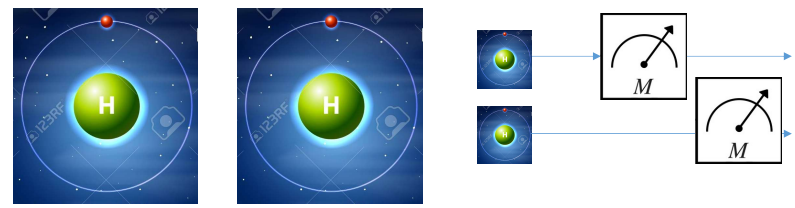
Individual measurement



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

- 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?

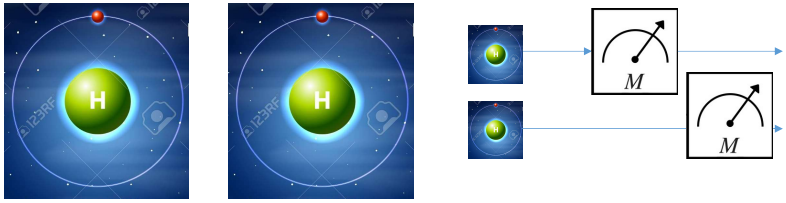
Lets plug in some numbers



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

- 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



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

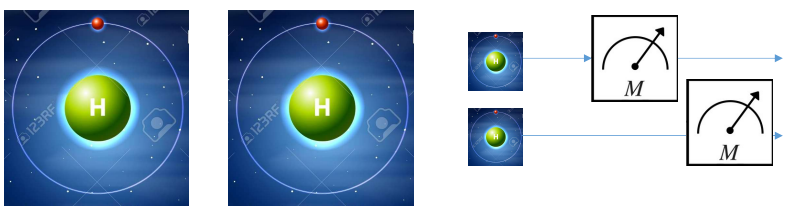
- *What happened??*
  - *The value measured for bit 0 influenced the value measured for bit 1!!!*
    - The measurement probabilities for bit 1 changed if the measured value of bit 0 changed!
  - ***The bits are entangled!!!***

Lets plug in some numbers

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

- 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



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

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

Lets plug in some numbers

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

- We measure b_1 first. What is the probability of 1?
  - What is the probability of 1?

The order of measurement doesn't matter.

The only fact that matters is that the bits are entangled

Lets plug in some numbers

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

The order of measurement doesn't matter.

The only fact that matters is that the bits are entangled

A special entangled state

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

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

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

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

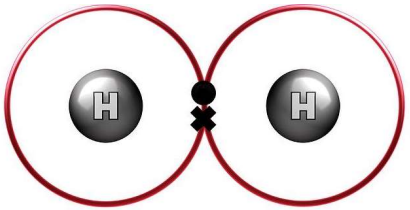
$$|\psi\rangle = \frac{1}{\sqrt{2}}|01\rangle - \frac{1}{\sqrt{2}}|10\rangle$$

A special entangled state

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

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

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

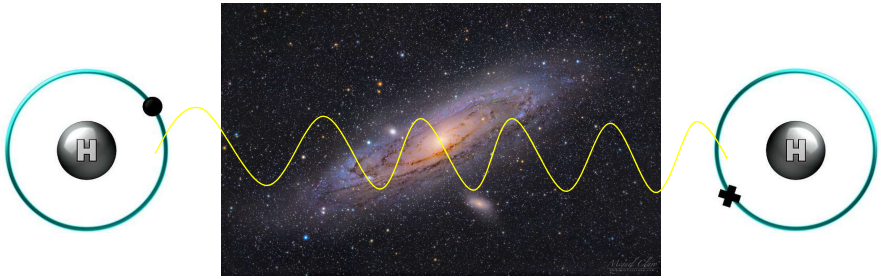
Random facts (from my friend Ramdas Menon)

"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.

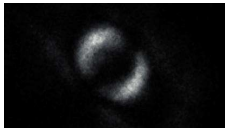
What still fewer people know is that the latter used to refer to the former as his "imaginary part"; nope, I ain't explaining this one."

Spooky action at a distance…



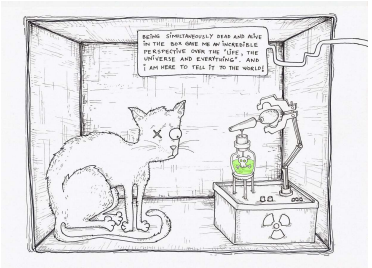
- Separate the entangled atoms by the width of the universe and they stay entangled:

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



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

God does not play dice!

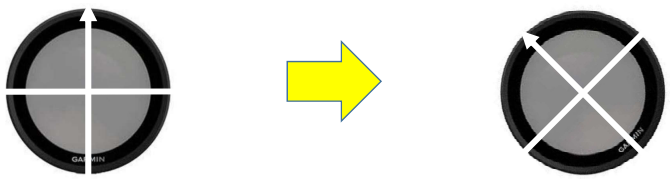


- Einstein refused to believe in spooky action at a distance!
- So did Schroedinger
- But yeah…
  - The fact that the observer can choose their bases for measurement means that the entangled particles could not have pre-decided how they would come out
    - They would have to know a priori what bases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

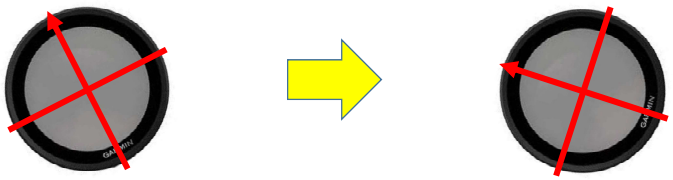
A digression: How do we measure with different bases?

- 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
- I.e. We can set the sign bases by first choosing a bit basis, and then choosing a sign basis at 45degrees
  - Or by first choosing a sign basis, and then a bit basis that's at -45 degrees to it

Bit bases and Sign basis



Bit bases Sign bases



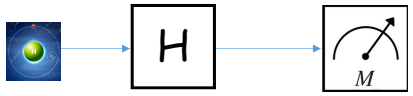
Bit bases Sign bases

The bit bases can be oriented anyhow

The sign bases are at 45º to the bit bases

Measuring with bit bases vs. measuring with sign bases

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



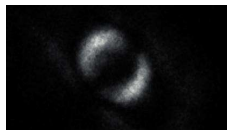
Returning from our digression…

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:

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



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

Spooky action at a distance…

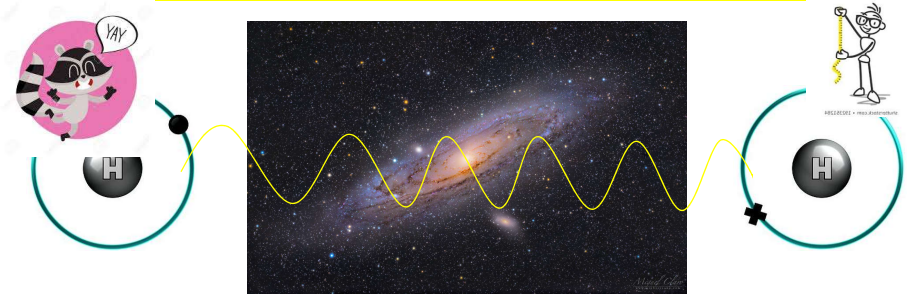
So does this mean we have found a way to communicate information instantaneously??
Faster than light!!!!!!!!!!!!

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!*

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"
  - So can we still use this somehow to communicate information
    - Only it wont be faster than light, but still…

Before we continue

Schrodinger's cat walks back in time

- Lets take a step back
- We now know a bunch of things about qubits
- How can we use that already?

So here's what we know about the qubit

- Even a single qubit exists in a superposition of states
- When you measure it, it will show up in one of the states
  - Observed reality
- Exactly how it will show up depends on the bases of measurement
  - Repeated measurements with different bases can change the observed reality

So here's what we know about the qubit

- Even a single qubit exists in a superposition of states
- When you measure it, it will show up in one of the states
  - Observed reality
- Exactly how it will show up depends on the bases of measurement
  - Repeated measurements with different bases can change the observed reality

- Pairs (or more) of qubits can get entangled
  - Measuring one "fixes" the other

So here's what we know about the qubit

- Even a single qubit exists in a superposition of states
- When you measure it, it will show up in one of the states
  - Observed reality
- Exactly how it will show up depends on the bases of measurement
  - Repeated measurements with different bases can change the observed reality

- Pairs (or more) of qubits can get entangled
  - Measuring one "fixes" the other

- **Can we build something useful with this already**

So here's what we know about the qubit

- Even a single qubit exists in a superposition of states
- When you measure it, it will show up in one of the states
  - Obs
- Exactly how it will show up depends on the bases of measurement
  - Repeated measurements with different bases can change the observed reality

- Pairs (or more) of qubits can get entangled
  - Measuring one "fixes" the other

Quantum Cryptography!!

Quantum Teleportation!!

- **Can be build something useful with this already**

So here's what we know about the qubit

- Even a single qubit exists in a superposition of states
- When you measure it, it will show up in one of the states
  - Obs
- Exactly how it will show up depends on the bases of measurement
  - Repeated measurements with different bases can change the observed reality

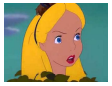
- Pairs (or more) of qubits can get entangled
  - Measuring one "fixes" the other

Quantum Cryptography!!

Quantum Teleportation!!

- **Can be build something useful with this already**

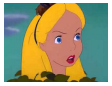
Cryptography 101: An insecure channel



My password is “Tweedledum”

- Normal communication:
  - Alice sends Bob a message
  - Bob gets the message
  - Everyone else gets the message as well
    - It’s a public channel
  - Disaster ensues

Cryptography 101: An secure channel



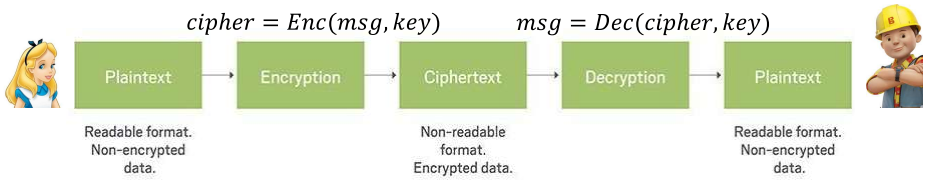
“Tweedledum”

Blarg blargity blarg

“Tweedledum”

- Encrypted communication communication:
  - Alice garbles the message using a formula that only she and Bob know
  - She sends Bob the message
    - Over the public channel – all channels are public
  - Everyone hears it, but has no idea what its saying
  - Only Bob can de-garble the message because he knows the formula

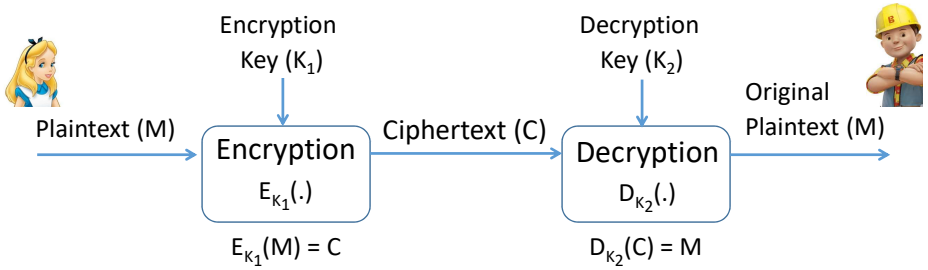
Cryptography



- Cryptography is the technique of converting messages to a form that is indecipherable to all but the intended recipient (who may even be yourself)
  - **Encrypting:** Converting the message to something that’s not decipherable
  - **Decrypting:** Recovering the message from the encrypted message
  - **Breaking an encryption:** Figuring out how to decipher the message without being told how to
    - Usually done by someone who is not the intended recipient
- Modern cryptography is done using mathematical functions that employ secret numbers called “keys” to encrypt and decrypt the message

Basics: Cryptography 101

- Messages and Encryption



Cryptographic Algorithm or **Cipher** – mathematical functions used for encryption and decryption

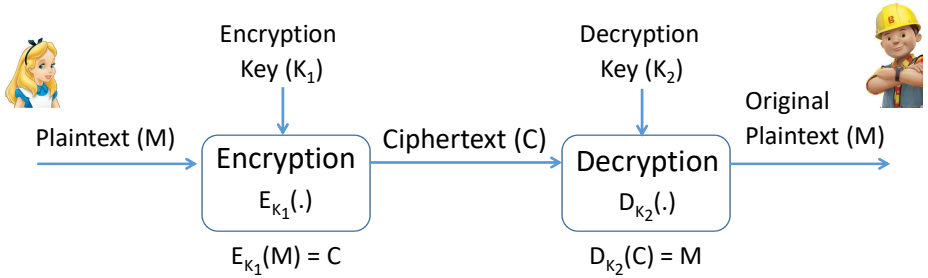
Key – Input required for the encryption (decryption) algorithm(s)

Cryptosystem – algorithms and all possible plaintexts, ciphertexts, keys

A ***Good Cryptosystem*** – all the security inherent in the knowledge of keys, and none in the knowledge of algorithms

Basics: Cryptography 101

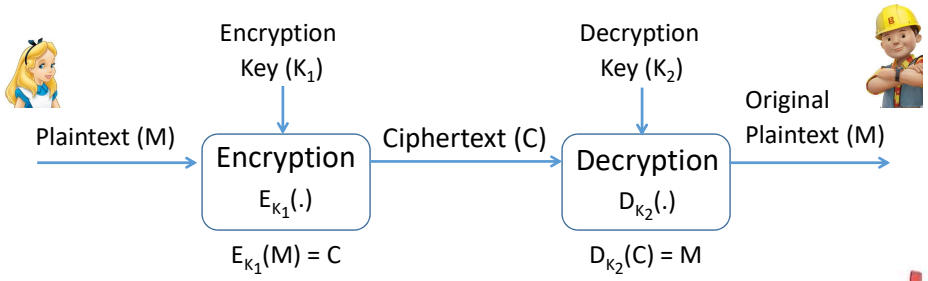
- Symmetric Cryptosystem
  - Encryption key is identical to the decryption key



Problem – Key must be distributed in secret and cannot be compromised.

Basics: Cryptography 101

- Public-key (asymmetric) Cryptosystem
  - Different keys for encryption and decryption



First described in
(Diffie and Hellman, 1976)

Quantum cryptography

- Even a single qubit exists in a superposition of states
- When you measure it, it will show up in one of the states
  - Observed reality
- Exactly how it will show up depends on the bases of measurement
  - Repeated measurements with different bases can change the observed reality

- **Can we use quantum computing to provide more secure encryption**

- Various proposals, but the most "practical" one involves not the encryption, but the *keys* …

The main challenge in Cryptography: Key exchange

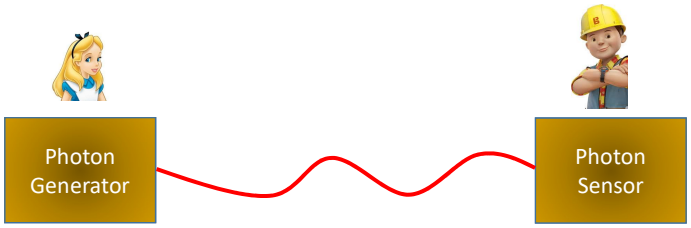
- Modern cryptographic techniques are *very* secure
  - If properly implemented
  - Will take an adversary *who doesn't have the key* many millions of years on *normal computers* to break a crypto system

- Challenge: How do you secure the key?
  - The key too must be sent to Bob over a public channel
  - How do you ensure everyone else doesn't get it?

Traditional methods for key exchange

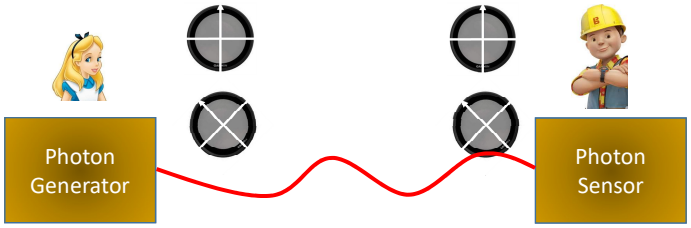
- Diffie Hellman key exchange
  - Uses the intractability of integer math to enable Bob and Alice to send partial keys to each other, such that only they can construct the entire key, but nobody else can
- Public Key cryptography
  - Alice uses Bob's public key to send the symmetric key to Bob
  - Only Bob can decrypt it and recover the real key
  - Uses the intractability of integer math to ensure that nobody without the private key can decrypt
- Problem: The relevant integer math theoretically becomes tractable with quantum computers
- Solution: Use quantum phenomena themselves to send the key
  - Obvious question: Why not use quantum phenomena to encrypt (instead of for just sending the key for classical encryption)?
  - Answer – yeah, people are working on this…

Quantum communication channels



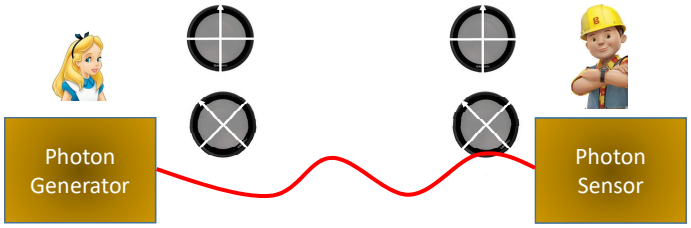
- Quantum information must be sent over "*quantum communication channels*"
  - A channel over which qubits can be communicated
    - The channel, like every other channel, is public
    - Obviously, classical bits too can be communicated
  - Measurement bases are same for sender and receiver
    - Public information
  - Example: Fibre optic channel over which photons are sent
    - In principle, anyone could tap into the fibre and also read the photons
    - **The channel is public**

Quantum communication channels



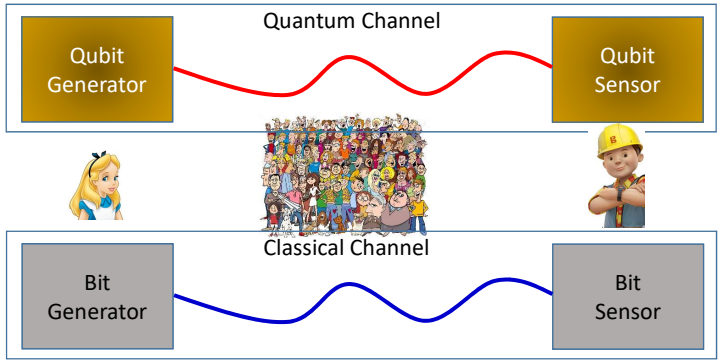
- Alice can send bits over the channel encoded in any bases
  - E.g. she could pass her photon through either a horizontal/vertical polarizer to send 1/0
  - Or she could pass it through a 45°/135° polarizer to send +/-
- Bob can measure using any bases
  - E.g. he could use a horizontally/vertically polarized lens, or a lens polarized at 45°/135°
- So long as both sides have agreed on what is "horizontal" polarization

Quantum communication channels



- Caveat:
- If Alice sends bits using the convention: horizontal = |0>, vertical = |1> using the 0/90 bases
- and Bob measures using the 45/135 bases
- Bob will not know whether he got a |0> or |1>
  - And will randomly get |+> or |->

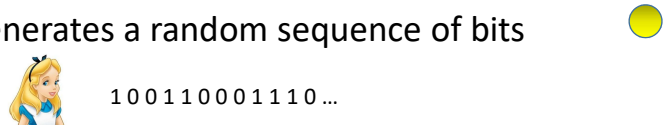
A typical setting for quantum communication



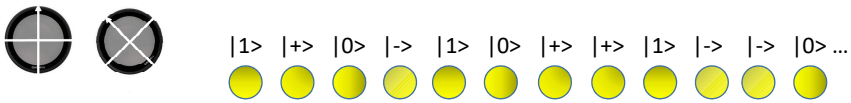
- Typical setting: Alice and Bob are connected by a quantum channel
- They are also connected by a classical channel
- They can use either (and will use both, typically, as we will see)
- All channels are public

Quantum Key Exchange : BB84

- Bennett and Brassard, 1984
- Alice generates a random sequence of bits



- She randomly encodes them using either 0/1 or +/- bases

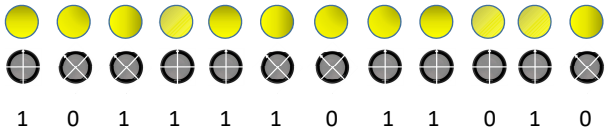


- She sends these to Bob over the quantum channel

Quantum Key Exchange : BB84

- Bob receives a series of qubits (photons) encoding bits
- He does not know which bases were used for what bits

- He randomly selects bases and measures the qubits
  - If he chose the right bases, he would get the correct bit
  - If not his measurement is random

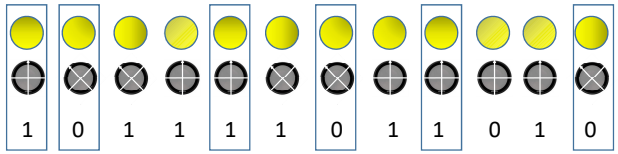


- He now has a sequence of bits some of which are right and some of which are wrong

Quantum Key Exchange : BB84

- Bob receives a series of qubits (photons) encoding bits
- He does not know which bases were used for what bits

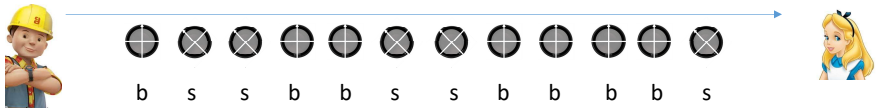
- He randomly selects bases and measures the qubits
  - If he chose the right bases, he would get the correct bit
  - If not his measurement is random



- He now has a sequence of bits some of which are right and some of which are wrong

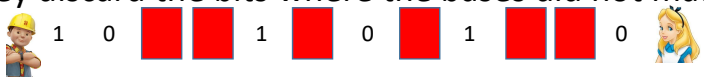
Quantum Key Exchange : BB84

- Bob uses the *classical* channel to tell Alice which bases he used for each bit



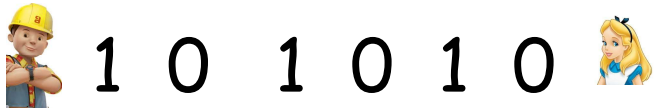
- Alice verifies for him over the same channel if he chose the right bit or not, for each bit

- They discard the bits where the bases did not match

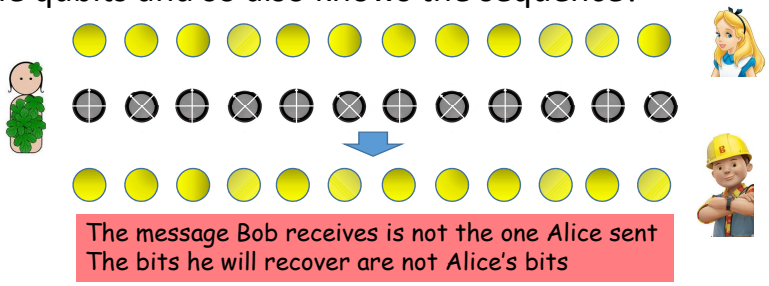


- They now a common shared bit string!!!

Outcome?

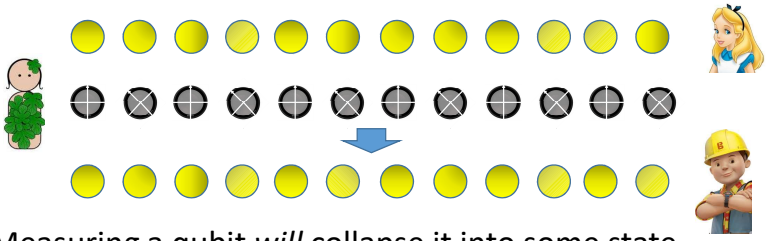


- Alice and Bob have the same sequence of bits
  - If both used the same bases, both got the same bits
- But… how do they know Eve didn't also measure all the qubits and so also knows the sequence?



No cloning theorem

- You cannot clone a qubit!!
  - If Eve measures the qubit, Bob got the qubit measured by Eve



- Measuring a qubit *will* collapse it into some state
- Eve does not know the true bases, she would have used the wrong bases half the time
- Bob remeasures the qubits using the right bases
  - But is wrong half the time anyway

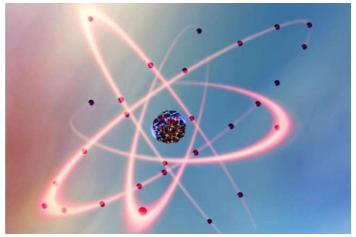
Bob and Alice verify

- Bob and Alice publicly call out some fraction of their bits
  - Which they will later throw away, so nothing lost
- If all of the bits match, they have not been messed with
- If they don't match, Eve has likely measured those bits before they got to Bob
- Alice and Bob discard the whole operation and start over!

Features and bugs

- Done entirely over public channel
- Needs no fancy math beliefs
- What are the guarantees
  - How sure can Alice and Bob be that they have the same key and Eve doesn't know it?
- What are the drawbacks?

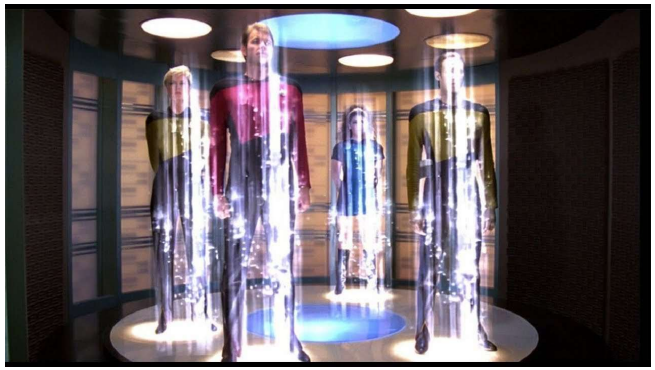
Axioms of quantum mechanics



1. Qubits always reside in a superposition of states
2. Measurement collapses them to one of the states
3. Transformations of a qubit comprise solely of unitary transforms
   - Rotations

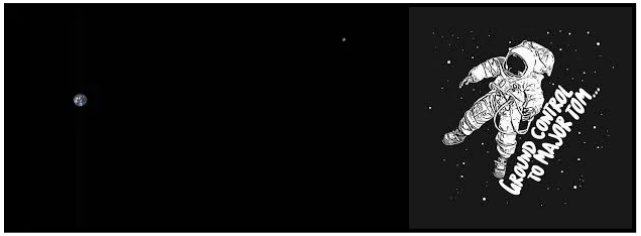
- Axioms 1 and 3 fit our new math; 2 causes challenges

Today: How to use entanglement, part 1



- To teleport a phasor, part 1

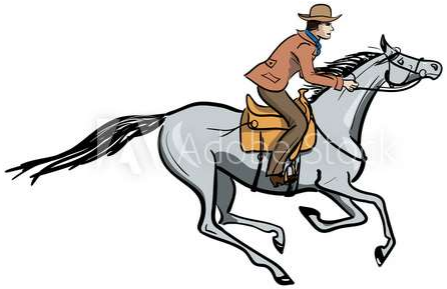
Quantum teleportation



- How do you transport an exact phasor (state) from a sender to a receiver
  - Who is not connected to you by a physical quantum communication channel?

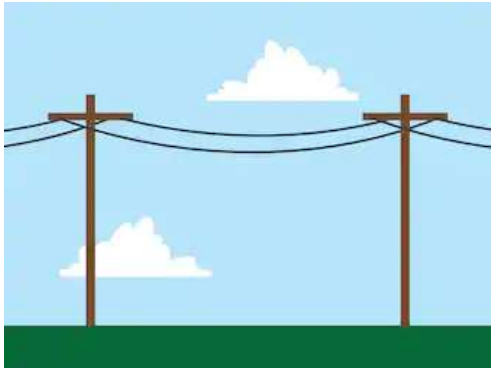
"Space Oddity" 1969

The history of communication



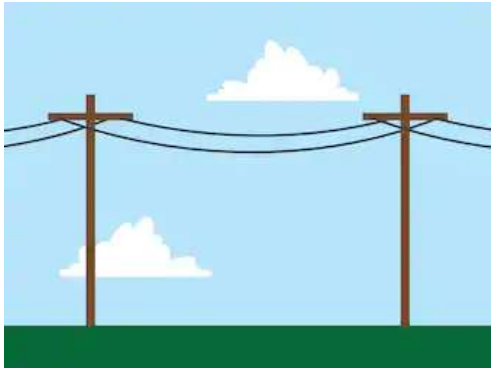
- For thousands of years messages were communicated from point A to point B via written messages on a physical medium
  - Papyrus, paper, bark, the human scalp

Then in 1816 something happened



- The first long-distance installation of telegraph by Francis Reynolds
  - What changed?

Then in 1816 something happened



- The first long-distance installation of telegraph by Francis Reynolds
  - What changed?
  - Messages could now be sent from A to B *with no transfer of medium*
  - *Not a single electron moved so much as a micrometer, yet the message got from A to B*

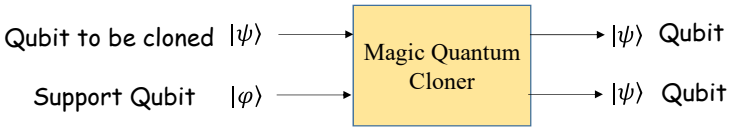
Quantum "teleportation"

- How do you transport a phasor? You don't.
  - You communicate the information about the state, so that it can be perfectly constructed on the receiving end
- How to transmit the state of a quantum system exactly to another location?
  - I.e how to transmit the coordinates of the phasor
    - They're complex, and cannot be measured!
- We will consider the simple case: how to transmit the phasor for *one* qubit exactly?

Recap: The no cloning theorem

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

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

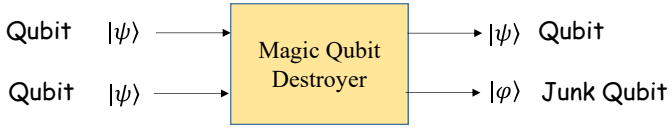


- Quantum systems are always invertible
  - Prove that you can't clone a qubit

Consequence: No deleting theorem

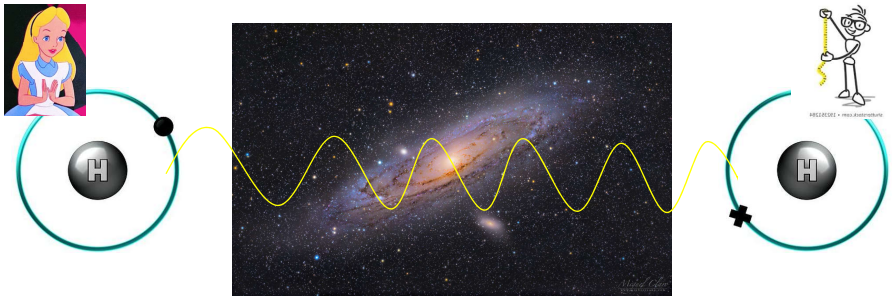
- Given two identical qubits you cannot delete wone of them
  - Deletion ➔ destroying the information in one of them

- A system that does this:



- This cannot exist
  - Prove it

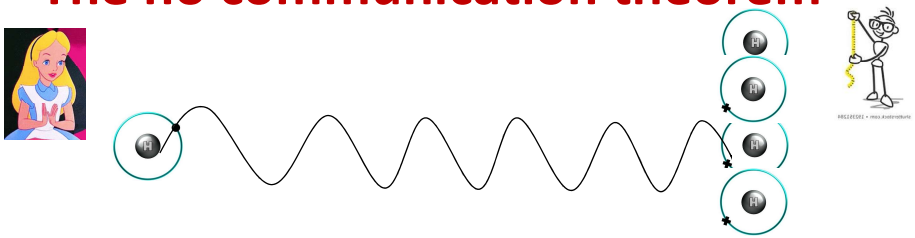
The no communication theorem



- 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

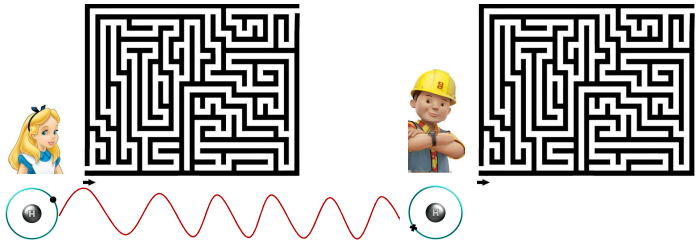
- There is *no protocol* that enables Alice to communicate *any* information to Bob

The no communication theorem



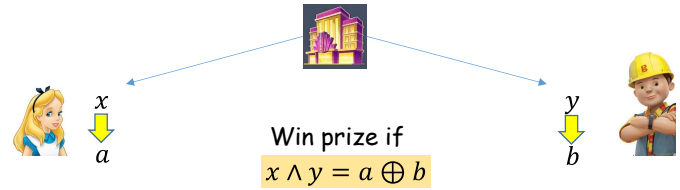
- Needs / implies the no-cloning theorem
  - Cheat protocol: To communicate her bit, Alice measures her entangled qubit if she has a 1, and doesn't measure it if she has a 0
  - Bob clones his qubit 1million times and measures them.
  - If all are same, Alice got a 1 else she got a 0

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



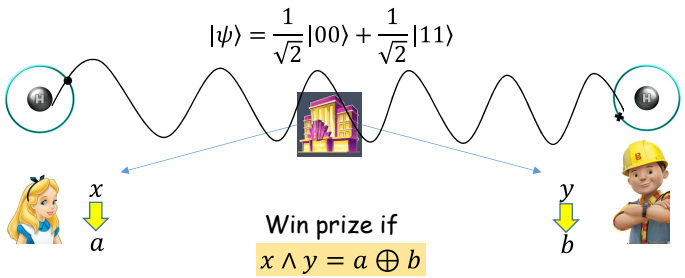
- Entanglement cannot be used for *communication,* but can be used for coordination
  - E.g. Alice and Bob have the same maze
  - They can decide: if we see a 0, go straight/right, else turn/go left
  - They can guarantee synchronized paths, but the final destination is random
- They have created *non-local* correlations
  - Without being able to predict the expected outcome
  - Can we use this somehow?

The CHSH game



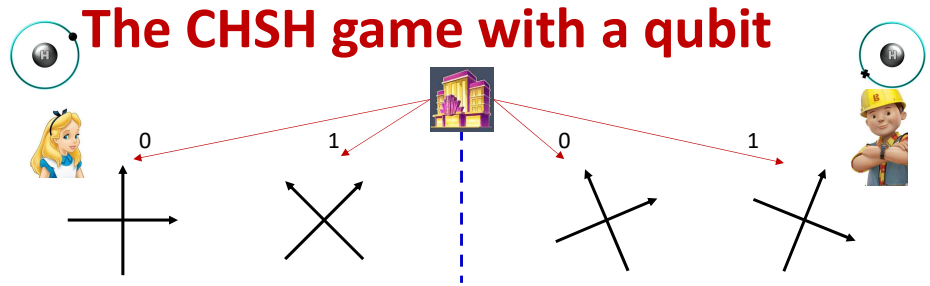
- Alice and Bob live in separate cities and may not communicate
- The casino sends each of them a random bit
  - Need not be identical
- They must inspect their bit and output a value
  - Alice outputs a, Bob outputs b
- They get a prize of $1.00 if:
  - Both got "1" from the casino and their outputs 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



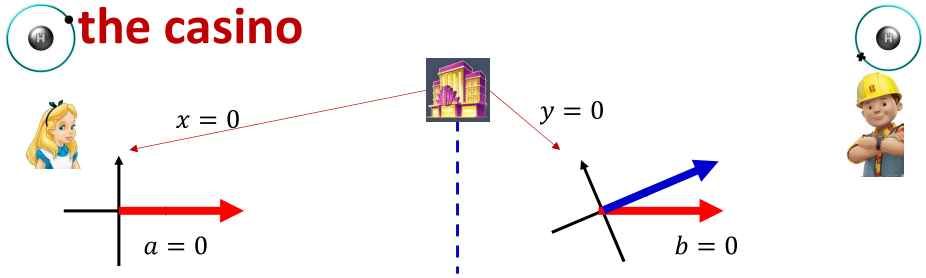
- Before moving to separate cities, Alice and Bob split a pair of entangled bits in the Bell State
- Now what is their best strategy?

The CHSH game with a qubit



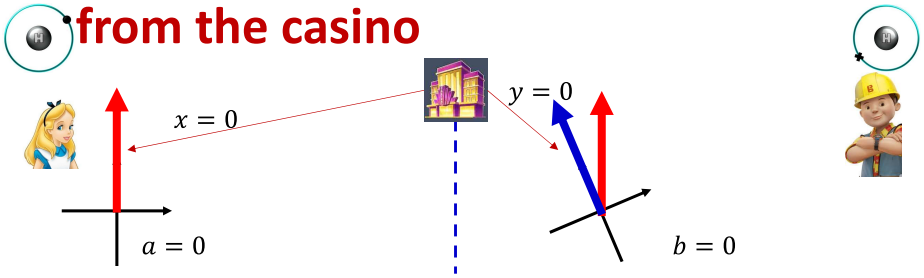
- Alice uses two sets of bases for measurement: 0/1 and +/- (at 45°)
  - If Alice gets a 0 from the casino she measures using 0/1 and outputs the value
  - Else she measures using +/- and outputs the value
- Bob uses two sets of bases: at $\left[\frac{\pi}{8}, \frac{5\pi}{8}\right]$ and $\left[\frac{-\pi}{8},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

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



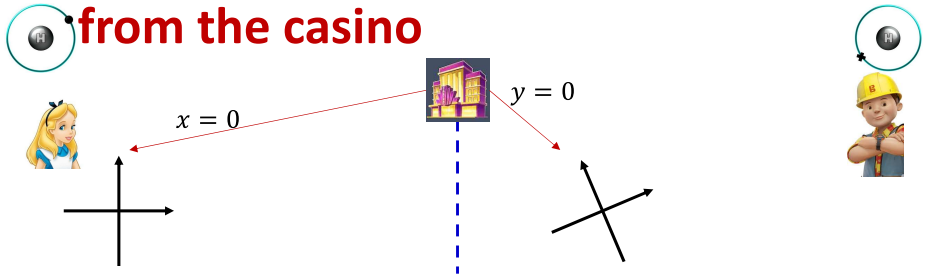
- If Alice measures first using the 0/1 bases and gets a 0
  - **Bob's qubit is also 0 due to entanglement**
  - Bob must also output a 0 to get money by the rules
- **Bob measures using the $\left[\frac{\pi}{8}, \frac{5\pi}{8}\right]$ bases**
  - He gets a 0 with probability $cos^2 \frac{\pi}{8}$
  - 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)

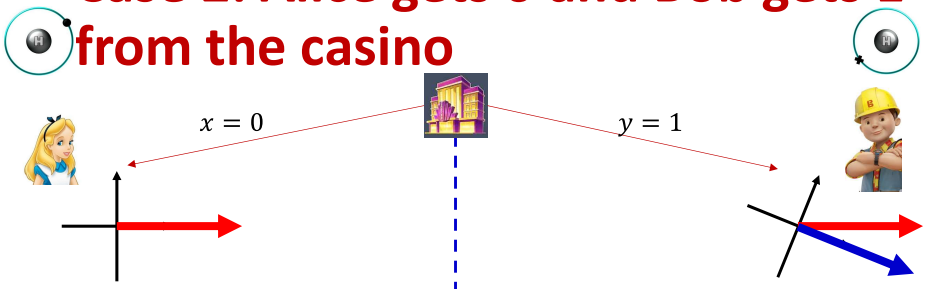
$$P(bob = alice | a = 0, x = 0, y = 0) P(a = 0 | x = 0, y = 0)$$
$$+ P(bob = alice | a = 1, x = 0, y = 0) P(a = 1 | x = 0, y = 0)$$
$$= P(a = 0 | x = 0, y = 0) cos^2 \frac{\pi}{8} + P(a = 1 | x = 0, y = 0) cos^2 \frac{\pi}{8}$$

i.e.

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

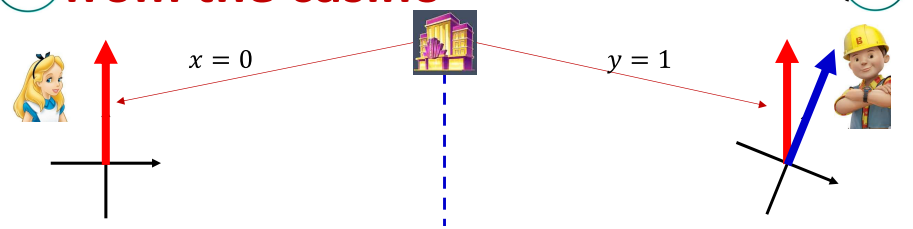
- Expected income when $x = 0, y = 0$ is $\$1 \times E[x = 0, y = 0] = cos^2 \frac{\pi}{8}$

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



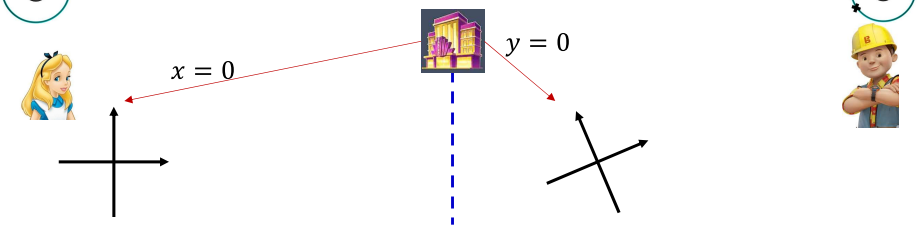
- If Alice measures first using the 0/1 bases and gets a 0
  - **Bob's qubit is also 0 due to entanglement**
  - Bob must also output a 0 to get money by the rules
- **Bob measures using the $\left[\frac{-\pi}{8}, \frac{3\pi}{8}\right]$ bases**
  - He gets a 0 with probability $cos^2 \frac{\pi}{8}$
  - 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)

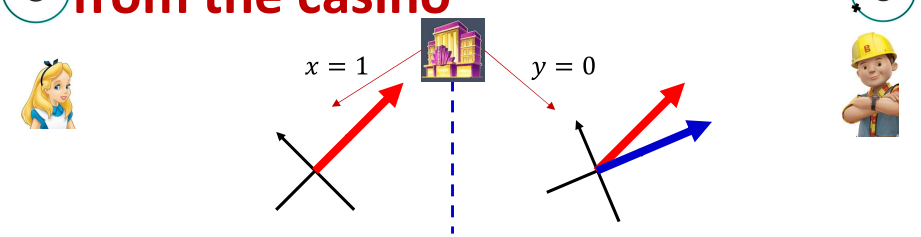
$$P(bob = alice | a = 0, x = 0, y = 1)P(a = 0 | x = 0, y = 1)$$
$$+ P(bob = alice | a = 1, x = 0, y = 1)P(a = 1 | x = 0, y = 1)$$
$$= P(a = 0 | x = 0, y = 1)cos^2\frac{\pi}{8} + P(a = 1 | x = 0, y = 1)cos^2\frac{\pi}{8}$$

i.e.

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

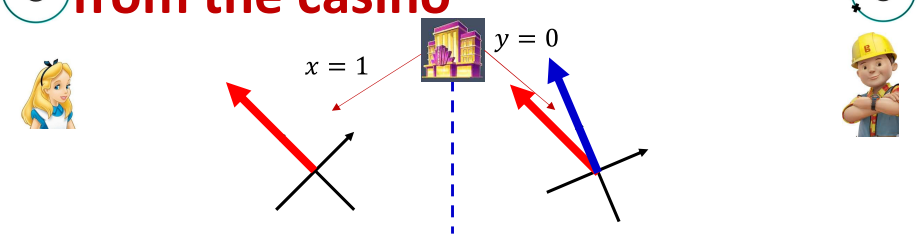
- Expected income when $x = 0, y = 1$ is $\$1 \times E[x = 0, y = 1] = cos^2\frac{\pi}{8}$

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



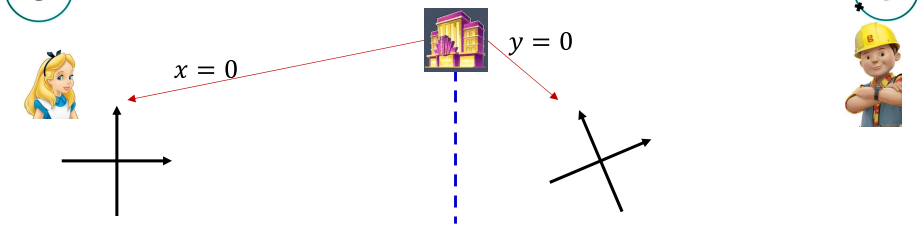
- If Alice measures first using the 0/1 bases and gets a 0
  - **Bob's qubit is also 0 due to entanglement**
  - Bob must also output a 0 to get money by the rules
- **Bob measures using the $\left[\frac{\pi}{8}, \frac{5\pi}{8}\right]$ bases**
  - He gets a 0 with probability $cos^2\frac{\pi}{8}$
  - 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)

  $P(bob = alice|a = 0, x = 1, y = 0)P(a = 0|x = 1, y = 0)$

  $+ P(bob = alice|a = 1, x = 1, y = 0)P(a = 1|x = 1, y = 0)$

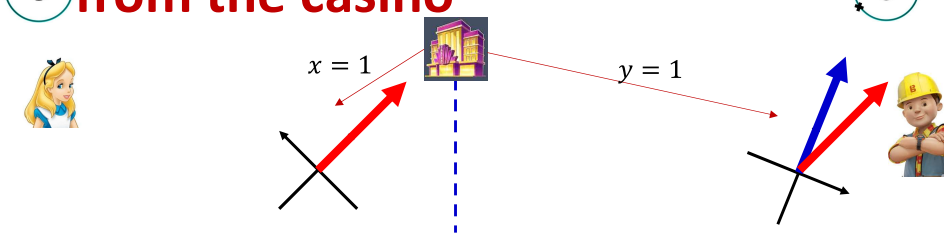
  $= P(a = 0|x = 1, y = 0)cos^2\frac{\pi}{8} + P(a = 1|x = 1, y = 0)cos^2\frac{\pi}{8}$

i.e.

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

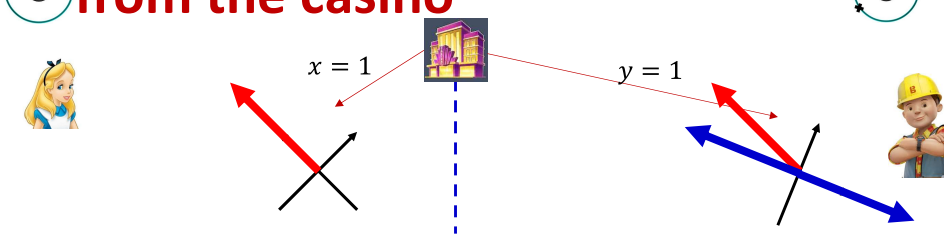
- Expected income when $x = 1, y = 0$ is $\$1 \times E[x = 1, y = 0] = cos^2\frac{\pi}{8}$

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



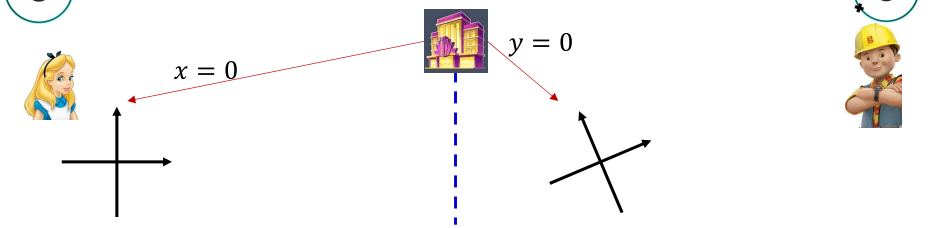
- If Alice measures first using the 0/1 bases and gets a 0
  - **Bob's qubit is also 0 due to entanglement**
  - Bob must now **output a 1** to get money by the rules
- **Bob measures using the $\left[\frac{-\pi}{8}, \frac{3\pi}{8}\right]$ bases**
  - He gets a 1 with probability $cos^2\frac{\pi}{8}$
  - 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)

  $P(bob \neq alice|a = 0, x = 1, y = 1)P(a = 0|x = 1, y = 1)$

  $+ P(bob \neq alice|a = 1, x = 1, y = 1)P(a = 1|x = 1, y = 1)$

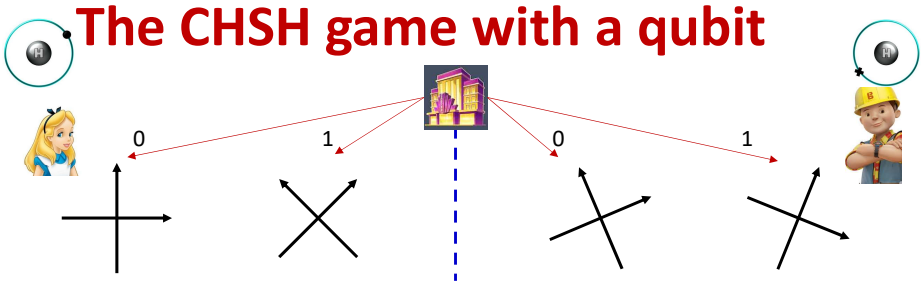
  $= P(a = 0|x = 1, y = 1)cos^2\frac{\pi}{8} + P(a = 1|x = 1, y = 1)cos^2\frac{\pi}{8}$

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

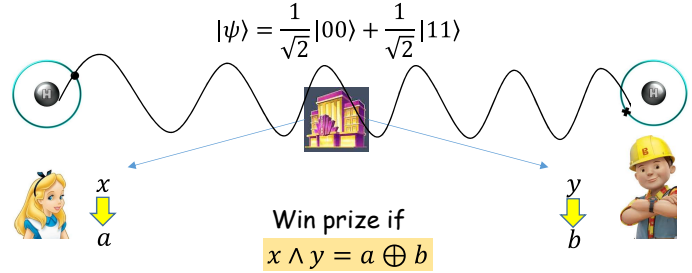


- The overall expected gain using the strategy is

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

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

The CHSH game with a qubit



- 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

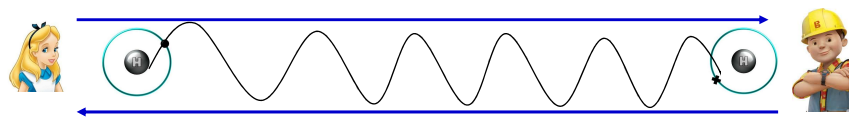
$$E[0,0] + E[0,1] + E[1,0] - E[1,1] \leq 2$$

  - 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

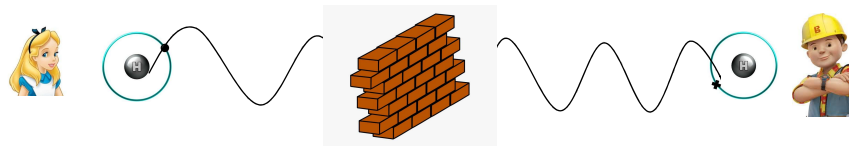
$$E[0,0] + E[0,1] + E[1,0] - E[1,1] \leq 2\sqrt{2}$$

  - 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

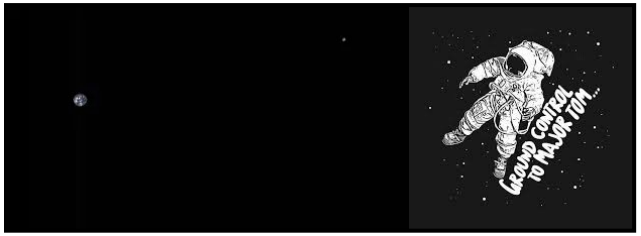


- Communication : Alice and Bob send each other information over the quantum channel



- 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

So…. Quantum teleportation

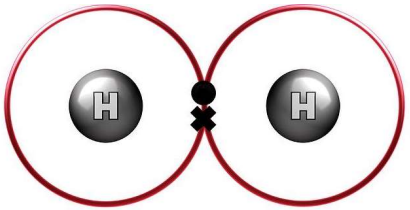


- How do you transport an exact phasor (state) from a sender to a receiver
  - Who is not connected to you by a physical quantum communication channel?
- To go further, we will need to understand Quantum operations on *pairs* of bits
- Next class…

"Space Oddity" 1969

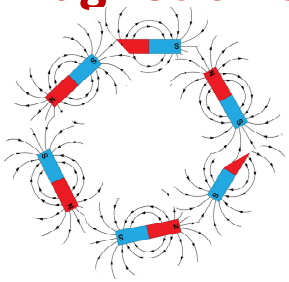
- Monday the 17th of Feb

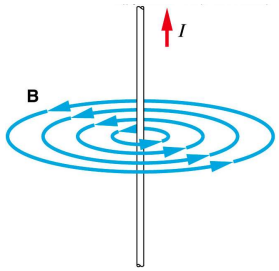
A note on spin

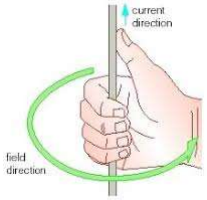


- The most common attribute of fermions (electrons) used in quantum computers is the "spin"
- What is this spin?

Moving charges and circular magnetic fields

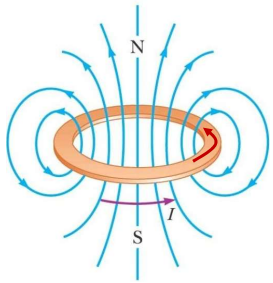


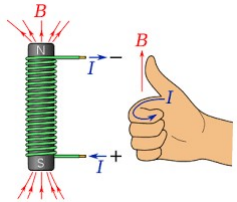




- A linearly moving charge produces a (circular) magnetic field
  - A copper wire conducting electricity consists of charged particles – electrons – travelling down the wire
  - This will cause a magnetic field
- The direction of field lines is a matter of convention – which was would a bar magnet line up if placed in the field
  - Because the "north" (up) and "south" (down) directions of the magnet are also matters of convention

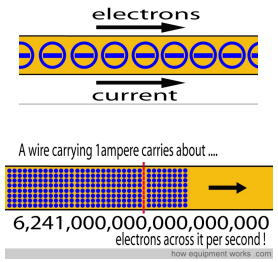
Rotating charges and magnetic fields

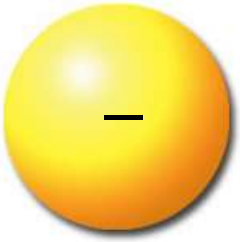




- Charges moving in a circle will cause magnetic fields
  - The direction of field lines is a matter of convention – which was would a bar magnet line up if placed in the field

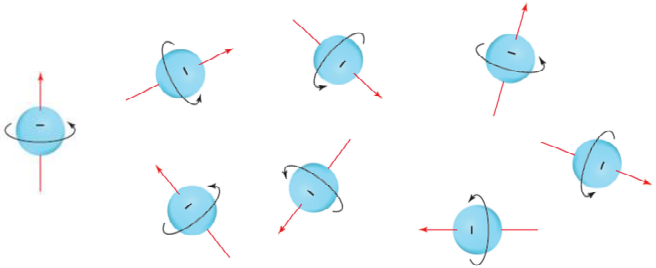
Does an electron possess a magnetic field?





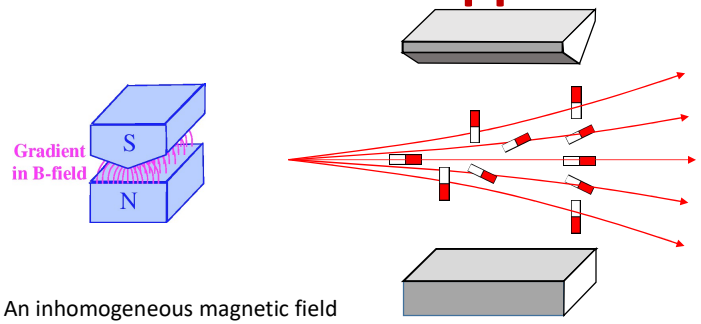
- Currents are produced through the movement of electrons (generally)
  - The charge carrying "particles"
- But, do the electrons themselves also have a magnetic field?
  - Are electrons magnets?

Hypothesis



- Electrons have an intrinsic magnetic field, just as they would if they were spinning
  - They effectively have an angular momentum
- The axis of the spin is random
  - The orientation of the random field is random

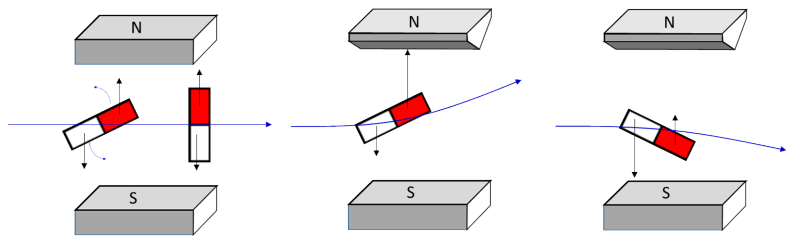
The Stern Gerlach Apparatus



- An inhomogeneous magnetic field
  - Created by two magnets, one flat, one pointy
  - The field at any point depends on it location
- Any magnet in the apparatus experiences a magnetic pull
  - Which depends on the distance between the N and S of the magnet, because the field is inhomogeneous
- A "travelling" bar magnet will be deflected by an amount that depends on its orientation
  - Which affects the N-S distance

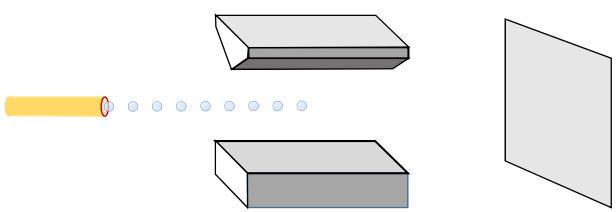
Proposed by Otto Stern in 21, implemented by Walter Gerlach in 22

Why inhomogeneous?



- If its homogeneous, the pull of the N on the S of the bar equals the pull of the S on the N of the bar and the two cancel out
  - The bar will merely rotate in place, but not be deflected
- In an inhomogeneous field, one is greater than the other and the bar moves
  - Bars oriented S/N will move up, bars oriented N/S
  - Will downward and upward deflections be equally strong?

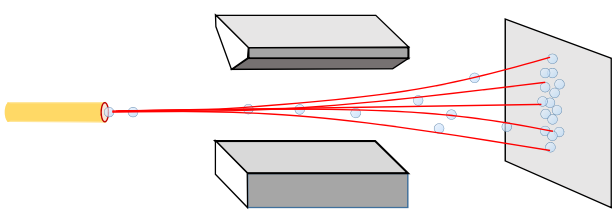
The Stern Gerlach Experiment



- Shoot a stream of electrons (actually silver atoms) through the inhomogeneous field
  - Detect the electrons on the other side with a screen, e.g. a glass slide with photoluminiscent coating

Proposed by Otto Stern in 21, implemented by Walter Gerlach in 22

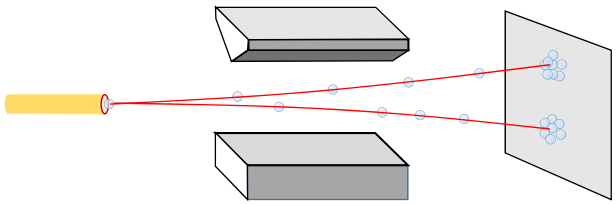
The Stern Gerlach Experiment



- Shoot a stream of electrons (actually silver atoms) through the inhomogeneous field
  - Detect the electrons on the other side with a screen, e.g. a glass slide with photoluminiscent coating
- If each electron's magnetic field is randomly oriented, the location of the arriving electrons will also be random

Proposed by Otto Stern in 21, implemented by Walter Gerlach in 22

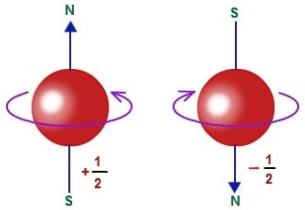
The Stern Gerlach Experiment



- Shoot a stream of electrons (actually silver atoms) through the inhomogeneous field
  - Detect the electrons on the other side with a screen, e.g. a glass slide with photoluminiscent coating
- If each electron's magnetic field is randomly oriented, the location of the arriving electrons will also be random
- In reality, the electrons were seen to be clumped, either at the top, or the bottom!

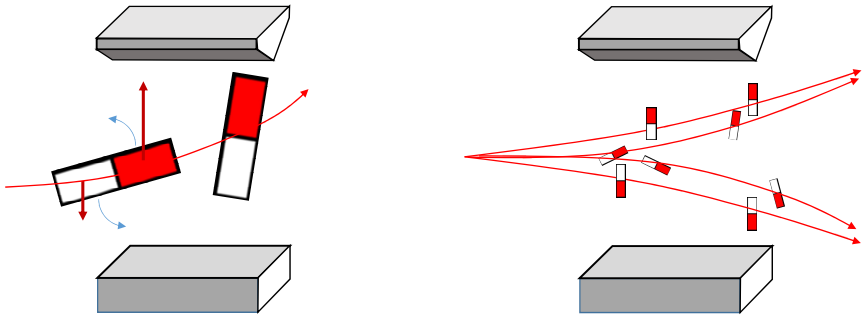
Proposed by Otto Stern in 21, implemented by Walter Gerlach in 22

So Electrons have Spin?



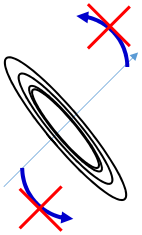
- The magnetic field of the electron is quantized!
  - I.e. the orientation of the spin is quantized.
- But is it really spin?
  - For the electron to spin fast enough to generate the magnetic moment observed, the surface must rotate faster than light
  - It can't really be spinning; it just behaves like it does
  - It *does* have *angular momentum* though (which explains the magnetic field)
- But why do we need *quantized* angular momentum?

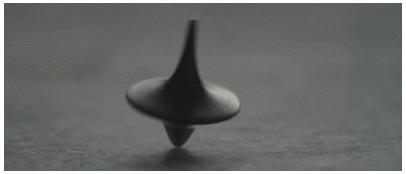
Its not so simple



- Real, non-spinning bar magnets would actually behave like the electrons
  - The inhomogeneous field would make the magnets *rotate*
    - The south would rotate towards N and vice versa
  - Eventually they'd all be vertical and clump at the screen
- If electrons were simple magnetic dipoles, they too would behave this way
  - But they aren't – they are charge particles
  - Their magnetic field is related to their angular momentum

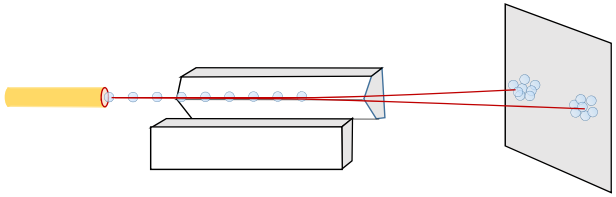
Its not so simple





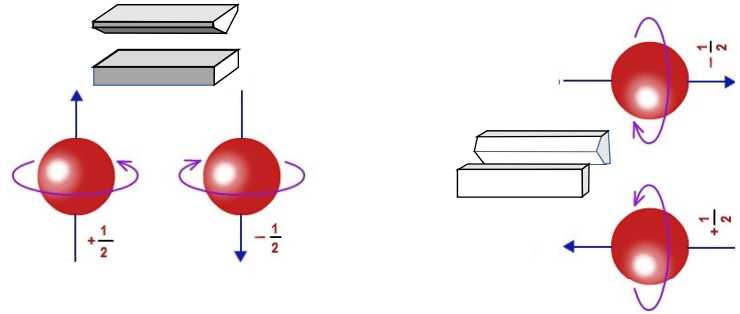
- Spin prevents the magnet from rotating
  - Gyroscopic forces, like when you cycle
  - All that happens is a precession (called Larmor precession) where the net vector still points in the same direction
  - The electron would not deflect to the ends
- I.e. the angular momentum *must* be quantized!!
  - To result in vertical up/down or down/up magnetic field
  - You cannot have random directions and magnitudes of angular momentum
- We will *call* it spin

But, you have a problem



- Is the spin North/South?
- What happens if the Stern Gerlach device is laid horizontal
  - East west?

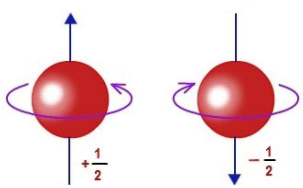
Superposition of Spin



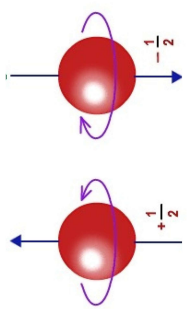
- The electron is either N/S oriented or E/W oriented
  - Depending on how you lay the apparatus
- But not both at the same time
- **The two orientations represent two different bases of measurement!**

Superposition of Spin

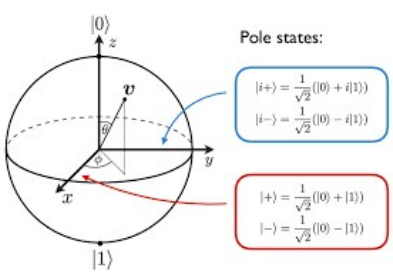
Bit Bases



Sign Bases



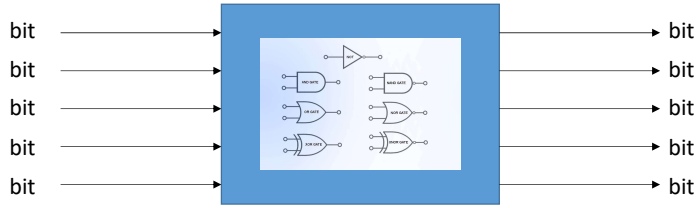
- These are, in fact, embodied exactly this way in the Bloch sphere representation of qubits



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



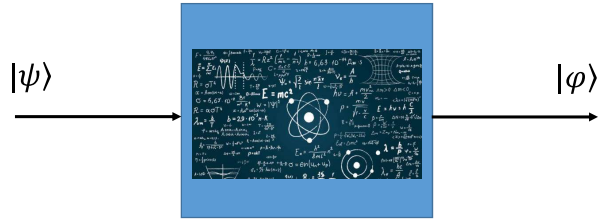
- A box that performs a computation
  - Takes in a collection of bits, outputs one or more bits
- The box is composed of gates
  - Binary gates: 2 inputs, one output
  - Large fan-in gates: many inputs one output
- Objective in design
  - **Ensure the output is always right**
  - **Minimize the number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

Note: You can do it all using only NAND gates

(but may need an exponential number of them)

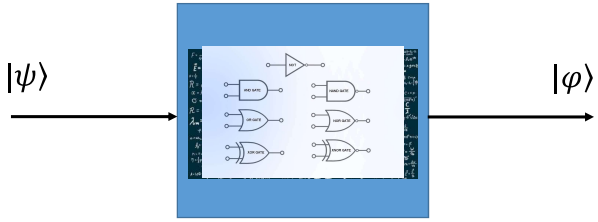
NAND is a universal gate

Quantum computation



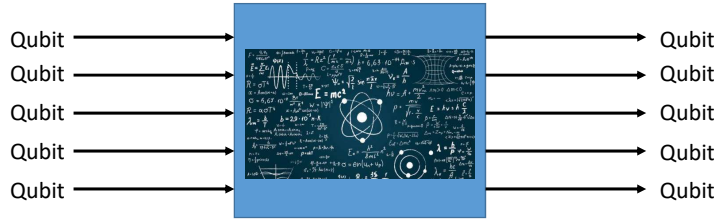
- A box that performs a computation
  - Takes in a high-dimensional phasor
    - A phasor in a high-dimensional complex Hilbert space
  - Outputs a high-dimensional phasor
    - In the same space as the input

Quantum computation



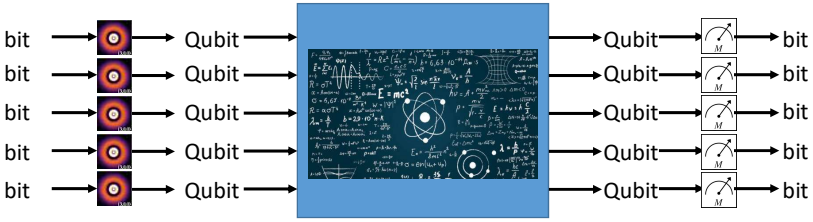
- A box that performs a computation
  - Takes in a high-dimensional phasor
    - A phasor in a high-dimensional complex Hilbert space
  - Outputs a high-dimensional phasor
    - In the same space as the input
- The box too is composed of computations that are analogous to the Boolean operations

Quantum computation



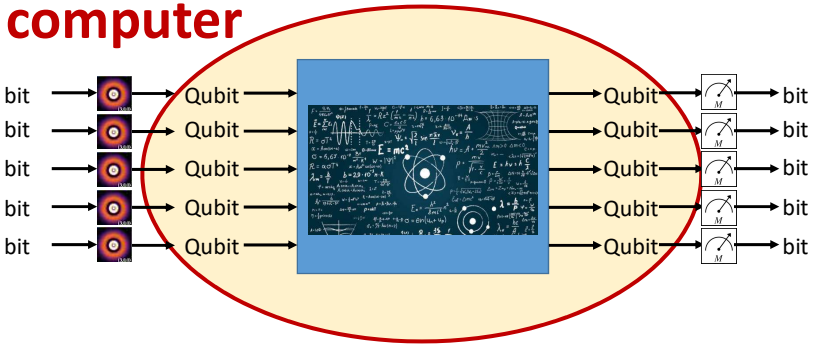
- In reality we don't work explicitly in the high-dimensional space
  - Except for simulations, which will of course blow up
- Instead the inputs and outputs are Qubits
  - Which start (and end) life in states that represent classical bits
    - I.e. they their start and end fates are classical
    -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

The secret life of a quantum computer



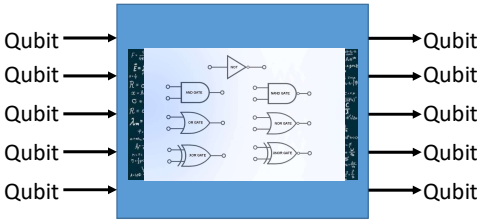
- The complete cycle

The secret life of a quantum computer



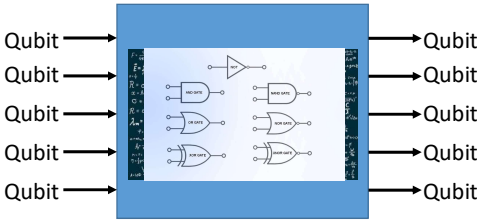
- The complete cycle
- The actual quantum computation
  - The computer may itself include measurement as in internal operation

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

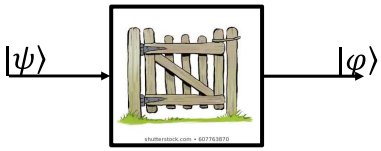


- The internal computat
  combination of smalle
  - Operations on smaller
  - Some of which may e
- Challenge: Minimize t

The quantum computer too has a Universal gate:

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

Quantum gates



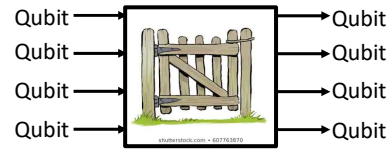
$|\varphi\rangle = U|\psi\rangle$

$$|\psi\rangle = \begin{bmatrix} a_0 \\ \vdots \\ a_N \end{bmatrix} \qquad |\varphi\rangle = \begin{bmatrix} b_0 \\ \vdots \\ b_N \end{bmatrix}$$

$$\begin{bmatrix} b_0 \\ \vdots \\ b_N \end{bmatrix} = U \begin{bmatrix} a_0 \\ \vdots \\ a_N \end{bmatrix}$$

- Operate on N-Dimensional phasors
  - In a complex N-D complex Hilbert space
  - The input is an N-D phasor, the output too is an 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



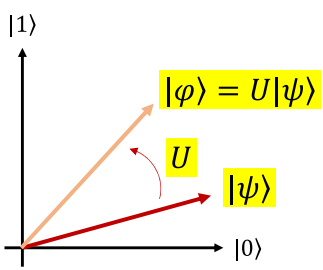
$|\varphi\rangle = U|\psi\rangle$

$$|\psi\rangle = \begin{bmatrix} a_0 \\ \vdots \\ a_N \end{bmatrix} \qquad |\varphi\rangle = \begin{bmatrix} b_0 \\ \vdots \\ b_N \end{bmatrix}$$

$$\begin{bmatrix} b_0 \\ \vdots \\ b_N \end{bmatrix} = U \begin{bmatrix} a_0 \\ \vdots \\ a_N \end{bmatrix}$$

- Operate on N-Dimensional phasors
  - In a complex N-D complex Hilbert space
  - The input is an N-D phasor, the output too is an 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 N-D x 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*
- Lets 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

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

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

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

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

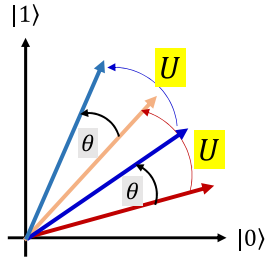
$|u_i| = ?$

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

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

- 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



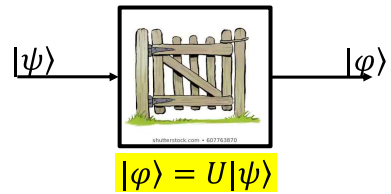
The angle between the red and blue phasors remains unchanged after each of them has been rotated by U

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

$$\langle Ua|Ub\rangle = \langle a|b\rangle$$
$$\Rightarrow\ (Ua)^H(Ub) = a^H U^H U b = a^H b$$
$$\Rightarrow U^H U = I$$

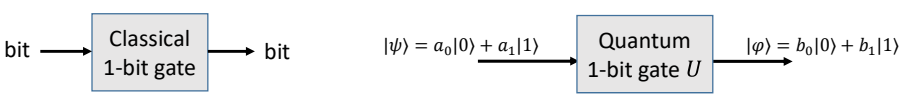
- The Hermitian of U is its own inverse
  - The columns of U are orthogonal to one another (why)?

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



- 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

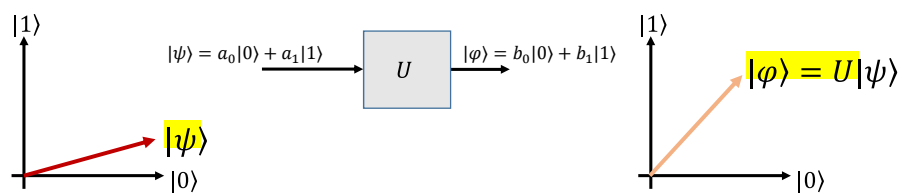
Revisiting single qubit gates



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

- 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

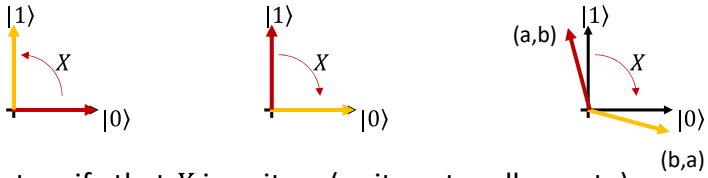
$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

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

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

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

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



- 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

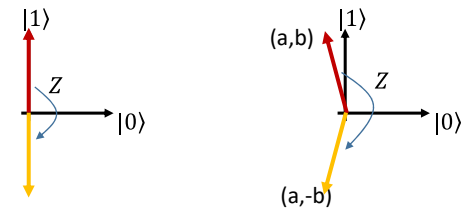
$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

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

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

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

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



- 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

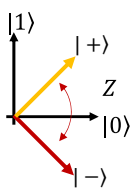
$$\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \longrightarrow \boxed{Z} \longrightarrow \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$$

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

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

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

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



- 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

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

$|0\rangle \longrightarrow \boxed{H} \longrightarrow |+\rangle$

$|1\rangle \longrightarrow \boxed{H} \longrightarrow |-\rangle$

$|+\rangle \longrightarrow \boxed{H} \longrightarrow |0\rangle$

$|-\rangle \longrightarrow \boxed{H} \longrightarrow |1\rangle$

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

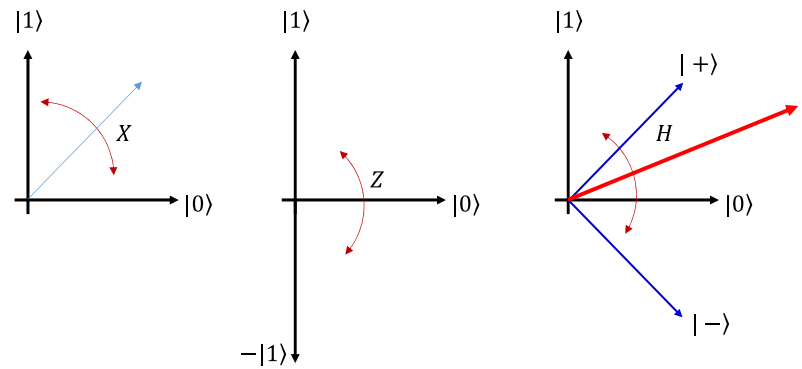
$$H|0\rangle = \left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right) \Rightarrow H|0\rangle = |+\rangle \qquad H|1\rangle = \left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\right) \Rightarrow H|1\rangle = |-\rangle$$

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

Unitary transforms are *rotations*

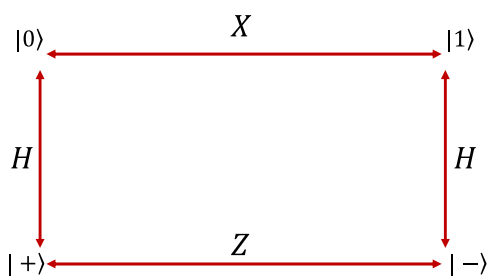
- So what kind of rotations are
- The bit flip gate?
- The phase flip gate?
- The Hadamard gate?

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

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

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

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

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

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

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

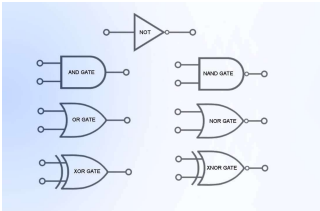
$\begin{bmatrix} -ib \\ ia \end{bmatrix} = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix}$

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?)

TWO QUBIT GATES

Classical two-bit gates



Input → Quantum 2-bit gate → Output

- Two-bit classical gates take in 2 bits, and output one or two bits
  - They operate on a two-dimensional input space
- What dimensionality of space do two-qubit quantum gates operate on

TWO QUBIT GATES

$|\psi\rangle = a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle$ → Quantum 2-bit gate → $|\varphi\rangle = b_{00}|00\rangle + b_{01}|01\rangle + b_{10}|10\rangle + b_{11}|11\rangle$

qubit → Quantum 2-bit gate → qubit
qubit → Quantum 2-bit gate → qubit

- Two-bit classical gates take in 2 bits, and output one or two bits
  - They operate on a two-dimensional input space
- What dimensionality of space do two-qubit quantum gates operate on
  - Four dimensional inputs and outputs
  - But physically still represented by two qubits (thanks quantum!)

Two-qubit gates

$|\psi\rangle = a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle$ → Quantum 2-bit gate → $|\varphi\rangle = b_{00}|00\rangle + b_{01}|01\rangle + b_{10}|10\rangle + b_{11}|11\rangle$

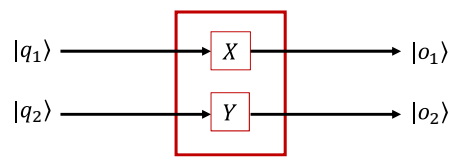
$$\begin{bmatrix} b_{00} \\ b_{01} \\ b_{10} \\ b_{11} \end{bmatrix} = \overset{U}{\begin{bmatrix} u_{00} & u_{01} & u_{02} & u_{03} \\ u_{10} & u_{11} & u_{12} & u_{13} \\ u_{20} & u_{21} & u_{22} & u_{23} \\ u_{30} & u_{31} & u_{23} & u_{33} \end{bmatrix}} \begin{bmatrix} a_{00} \\ a_{01} \\ a_{10} \\ a_{11} \end{bmatrix}$$

- A single two-qubit gate U operates on the phasor

  $a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle$ to output $b_{00}|00\rangle + b_{01}|01\rangle + b_{10}|10\rangle + b_{11}|11\rangle$

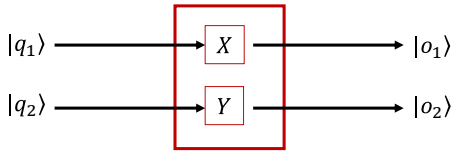
  $U(a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle) = b_{00}|00\rangle + b_{01}|01\rangle + b_{10}|10\rangle + b_{11}|11\rangle$
- U is is a 4x4 matrix.
  - It is a unitary transform
  - Its columns are orthogonal and form a new basis set
- Examples coming up

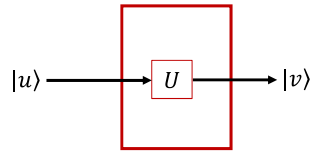
The simplest 2-qubit gate



- Each qubit is independently operated on by a one-qubit gate
  - Note: This is still a two qubit system operating on two qubits and producing two qubits
- What is the resulting 2-qubit gate?

2-qubit gate





$|q_1\rangle = a_0|0\rangle + a_1|1\rangle$ $\quad$ $|o_1\rangle = c_0|0\rangle + c_1|1\rangle$

$|q_2\rangle = b_0|0\rangle + c_1|1\rangle$ $\quad$ $|o_2\rangle = d_0|0\rangle + d_1|1\rangle$

$|u\rangle = |q_1\rangle \otimes |q_2\rangle = |q_1 q_2\rangle$

$|v\rangle = |o_1\rangle \otimes |o_2\rangle = |o_1 o_2\rangle$

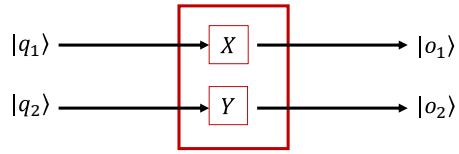
$$\begin{bmatrix} c_0 \\ c_1 \end{bmatrix} = \begin{bmatrix} x_{00} & x_{01} \\ x_{10} & x_{11} \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \end{bmatrix}$$

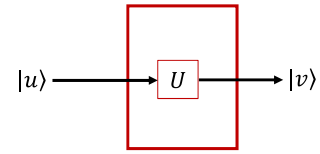
$$\begin{bmatrix} d_0 \\ d_1 \end{bmatrix} = \begin{bmatrix} y_{00} & y_{01} \\ y_{10} & y_{11} \end{bmatrix} \begin{bmatrix} d_0 \\ d_1 \end{bmatrix}$$

$$\begin{bmatrix} v_{00} \\ v_{01} \\ v_{10} \\ v_{11} \end{bmatrix} = \begin{bmatrix} u_{00} & u_{01} & u_{02} & u_{03} \\ u_{10} & u_{11} & u_{12} & u_{13} \\ u_{20} & u_{21} & u_{22} & u_{23} \\ u_{30} & u_{31} & u_{23} & u_{33} \end{bmatrix} \begin{bmatrix} u_{00} \\ u_{01} \\ u_{10} \\ u_{11} \end{bmatrix}$$

- How does U relate to X and Y

2-qubit gate





$$X = \begin{bmatrix} x_{00} & x_{01} \\ x_{10} & x_{11} \end{bmatrix}$$

$$Y = \begin{bmatrix} y_{00} & y_{01} \\ y_{10} & y_{11} \end{bmatrix}$$

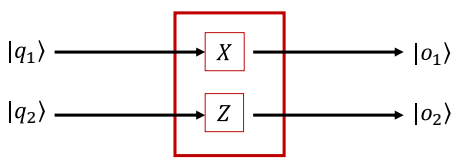
$U = X \otimes Y$

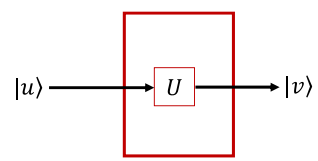
$$U = X \otimes Y = \begin{bmatrix} x_{00}\begin{bmatrix} y_{00} & y_{01} \\ y_{10} & y_{11} \end{bmatrix} & x_{01}\begin{bmatrix} y_{00} & y_{01} \\ y_{10} & y_{11} \end{bmatrix} \\ x_{10}\begin{bmatrix} y_{00} & y_{01} \\ y_{10} & y_{11} \end{bmatrix} & x_{11}\begin{bmatrix} y_{00} & y_{01} \\ y_{10} & y_{11} \end{bmatrix} \end{bmatrix}$$

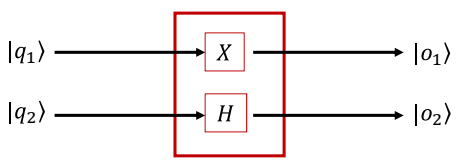
- How does U relate to X and Y *when the qubits don't interact*
  - I.e. no entanglement
  - Verify that U is unitary

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

2-qubit gate

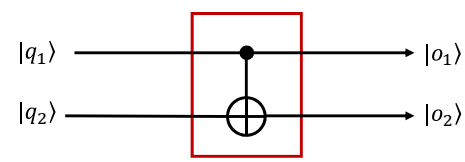






- What is U?
- What is the structure of the transform?
  - Can you generalize to more than 2 non-interacting bits?

The CNOT gate

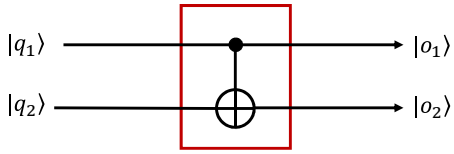


$|o_1 o_2\rangle = CNOT(|q_1 q_2\rangle)$

$o_1 = q_1 \qquad o_2 = q_1 \oplus q_2$

- $o_1 = q_1$
  - The first input is always unchanged
- $o_2 = q_2$ if $q_1 = |0\rangle$ (is 0), otherwise $o_2 = X(q_2)$
  - It bit-flips if the first input is 1
- **q_1 is the *control* bit and q_2 is the *target* bit**

The CNOT gate



$|o_1 o_2\rangle = CNOT(|q_1 q_2\rangle)$

$$\begin{bmatrix} u_{00} \\ u_{01} \\ u_{11} \\ u_{10} \end{bmatrix} = [CNOT] \begin{bmatrix} u_{00} \\ u_{01} \\ u_{10} \\ u_{11} \end{bmatrix}$$

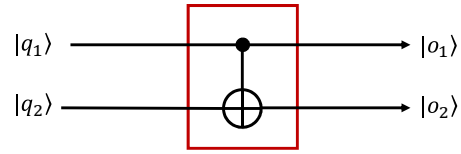
$$CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

Verify that this is unitary

$$CNOT(a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle) = a_{00}|00\rangle + a_{01}|01\rangle + a_{11}|10\rangle + a_{10}|11\rangle$$

- **Are o_1 and o_2 entangled?**

The CNOT gate



$|o_1 o_2\rangle = CNOT(|q_1 q_2\rangle)$

$$\begin{bmatrix} u_{00} \\ u_{01} \\ u_{11} \\ u_{10} \end{bmatrix} = [CNOT] \begin{bmatrix} u_{00} \\ u_{01} \\ u_{10} \\ u_{11} \end{bmatrix}$$

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

$$CNOT(a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle) = a_{00}|00\rangle + a_{01}|01\rangle + a_{11}|10\rangle + a_{10}|11\rangle$$

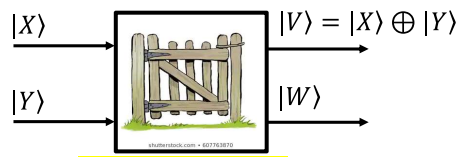
- **Are o_1 and o_2 entangled?**

CNOT IS AN ENTANGLING GATE!!

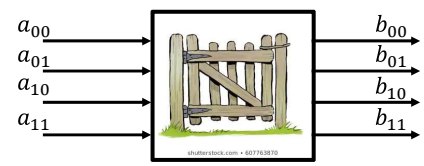
Lets try some simple gates

- So we know how to construct simple 2-qubit quantum gates
- So now, lets try to build them for the following 2-input Boolean operations
  - $X \oplus Y$
  - $X\ (AND)\ Y$

XOR



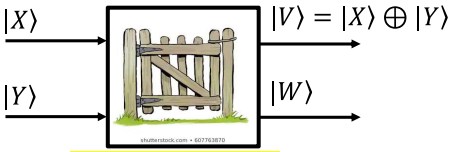
$|VW\rangle = U|XY\rangle$



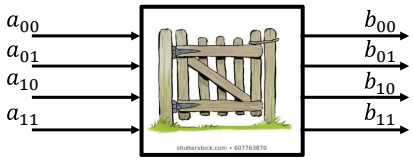
- We don't care what W is
- Create U such that the truth table to the right is produced

X	Y	V	W
0	0	0	
0	1	1	
1	0	1	
1	1	0	

XOR



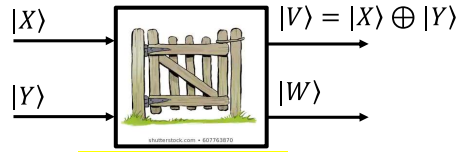
$|VW\rangle = U|XY\rangle$



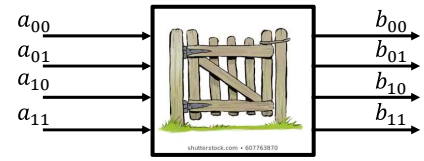
- $U|00\rangle = |0*\rangle$
- How do we select W to construct a U for this?

X	Y	V	W
0	0	0	
0	1	1	
1	0	1	
1	1	0	

XOR



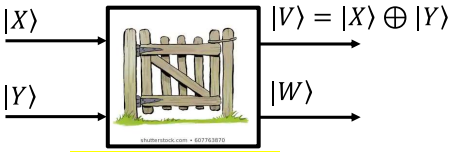
$|VW\rangle = U|XY\rangle$



- $U|00\rangle = |0*\rangle$
- How do we select W to construct a U for this?
- Invertibility: Every orange row must be unique (or the function is not invertible)
  - Create W for this
- Design a U for the chosen W

X	Y	V	W
0	0	0	0
0	1	1	0
1	0	1	1
1	1	0	1

XOR



$|VW\rangle = U|XY\rangle$

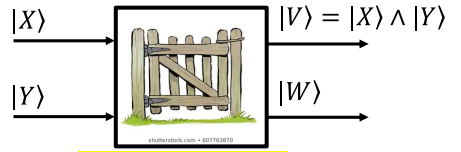
X	Y	V	W
0	0	0	0
0	1	1	0
1	0	1	1
1	1	0	1

- $U|00\rangle = |00\rangle, U|01\rangle = |10\rangle, U|10\rangle = |11\rangle, U|11\rangle = |01\rangle$

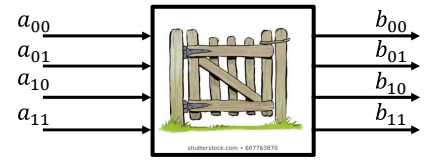
$$\begin{bmatrix}1\\0\\0\\0\end{bmatrix} = \begin{bmatrix}u_{00} & u_{01} & u_{02} & u_{03}\\ u_{10} & u_{11} & u_{12} & u_{13}\\ u_{20} & u_{21} & u_{22} & u_{23}\\ u_{30} & u_{31} & u_{23} & u_{33}\end{bmatrix}\begin{bmatrix}1\\0\\0\\0\end{bmatrix} \qquad \begin{bmatrix}0\\0\\1\\0\end{bmatrix} = \begin{bmatrix}u_{00} & u_{01} & u_{02} & u_{03}\\ u_{10} & u_{11} & u_{12} & u_{13}\\ u_{20} & u_{21} & u_{22} & u_{23}\\ u_{30} & u_{31} & u_{23} & u_{33}\end{bmatrix}\begin{bmatrix}0\\1\\0\\0\end{bmatrix}$$

$$\begin{bmatrix}0\\0\\0\\1\end{bmatrix} = \begin{bmatrix}u_{00} & u_{01} & u_{02} & u_{03}\\ u_{10} & u_{11} & u_{12} & u_{13}\\ u_{20} & u_{21} & u_{22} & u_{23}\\ u_{30} & u_{31} & u_{23} & u_{33}\end{bmatrix}\begin{bmatrix}0\\0\\1\\0\end{bmatrix} \qquad \begin{bmatrix}0\\1\\0\\0\end{bmatrix} = \begin{bmatrix}u_{00} & u_{01} & u_{02} & u_{03}\\ u_{10} & u_{11} & u_{12} & u_{13}\\ u_{20} & u_{21} & u_{22} & u_{23}\\ u_{30} & u_{31} & u_{23} & u_{33}\end{bmatrix}\begin{bmatrix}0\\0\\0\\1\end{bmatrix}$$

AND



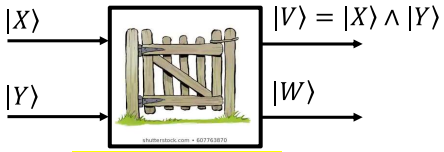
$|VW\rangle = U|XY\rangle$



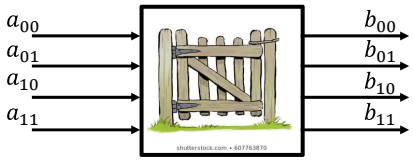
- How do we select W to be able to construct a U for this table?

X	Y	V	W
0	0	0	*
0	1	0	*
1	0	0	*
1	1	1	*

AND



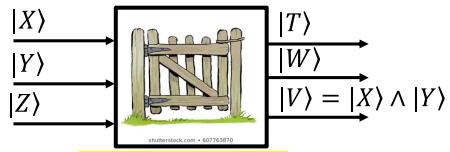
$|VW\rangle = U|XY\rangle$



X	Y	V	W
0	0	0	*
0	1	0	*
1	0	0	*
1	1	1	*

- How do we select W to be able to construct a U for this table?
- You cannot!!!
  - Which other gates are similarly impossible to model?

So how do you do an AND

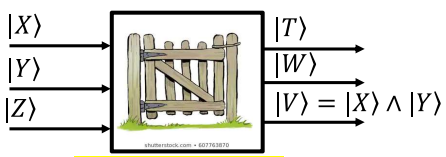


$|VW\rangle = U|XY\rangle$

X	Y	Z	T	W	V
0	0	0	*	*	*
0	0	1	*	*	*
0	1	0	*	*	*
0	1	1	*	*	*
1	0	0	*	*	*
1	0	1	*	*	*
1	1	0	*	*	*
1	1	1	*	*	*

- You add an *output qubit*
  - The fact is, the output is not manufactured from thin air
  - Its actually an entire qubit
- Does this help?

So how do you do an AND

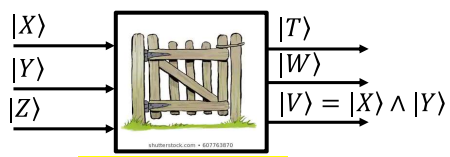


$|VW\rangle = U|XY\rangle$

X	Y	Z	T	W	V
0	0	0	*	*	0
0	0	1	*	*	0
0	1	0	*	*	0
0	1	1	*	*	0
1	0	0	*	*	0
1	0	1	*	*	0
1	1	0	*	*	1
1	1	1	*	*	1

- You can't in general
  - If you want V to give you the right input regardless of Z

So how do you do an AND

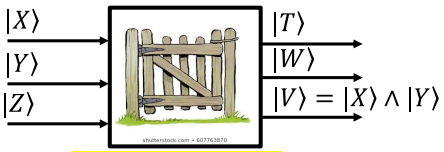


$|VW\rangle = U|XY\rangle$

X	Y	Z	T	W	V
0	0	0	*	*	0
0	0	1	*	*	*
0	1	0	*	*	0
0	1	1	*	*	*
1	0	0	*	*	0
1	0	1	*	*	*
1	1	0	*	*	1
1	1	1	*	*	*

- You can't in general
  - If you want V to give you the right input regardless of Z
- But it only has to work for *one value of Z*
  - This gives you a lot more freedom to "design" your transform

So how do you do an AND

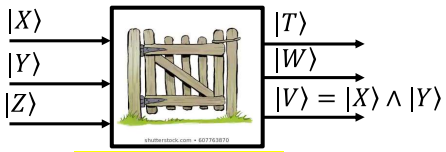


$|VW\rangle = U|XY\rangle$

X	Y	Z	T	W	V
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	1	0
1	1	0	1	0	1
1	1	1	1	1	1

- You can't in general
  - If you want V to give you the right input regardless of Z
- But it only has to work for *one value of Z*
  - This gives you a lot more freedom to "design" your transform

The CSWAP (or FREDKIN) Gate

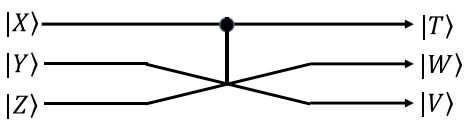


$|VW\rangle = U|XY\rangle$

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

X	Y	Z	T	W	V
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	1	0
1	1	0	1	0	1
1	1	1	1	1	1

The CSWAP gate

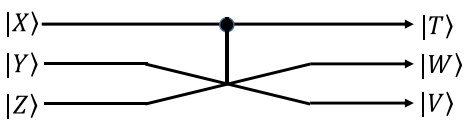


- The controlled swap gate
  - If the "control" X is 0, Y and Z go through in the same order
  - If X is 1, Y and Z swap
- Verify that when Z = 0, V = X AND Y
- What other Boolean functions can you get by varying Z?
  - And at what output variable?
- What would the output be for *superposed* states?

The CSWAP gate

Note: The CSWAP, combined with a NOT is a universal gate!!

Why??



- The controlled swap gate
  - If the "control" X is 0, Y and Z go through in the same order
  - If X is 1, Y and Z swap
- Verify that when Z = 0, V = X AND Y
- What other Boolean functions can you get by varying Z?
  - And at what output variable?
- What would the output be for *superposed* states?

Lesson for the day

- You cannot simply emulate N-bit classical gates with an N-bit quantum circuit
- You will have to add extra qubits to hold the output
- And still more qubits to hold other necessary variables
  - AKA “junk”
- More on this next week…