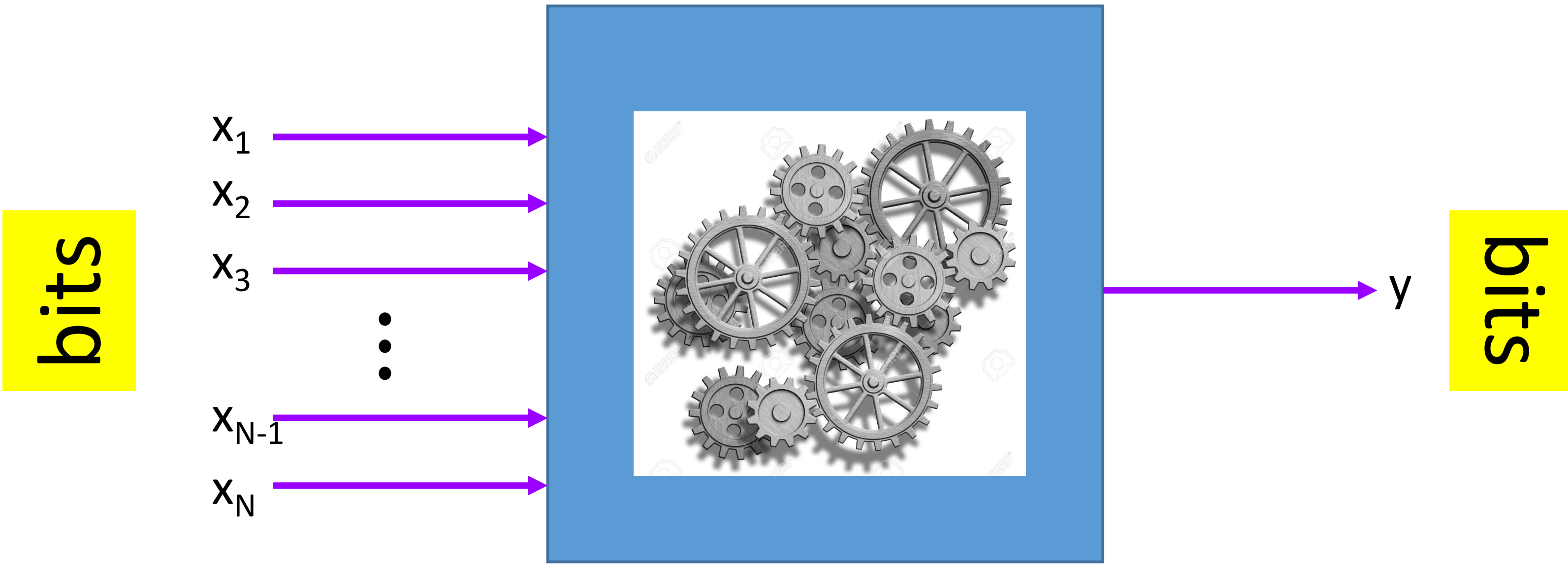
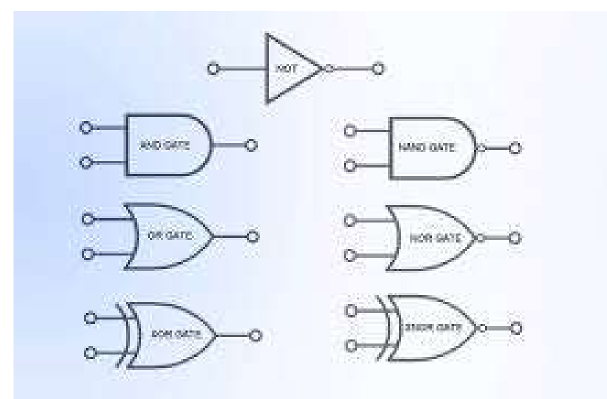
Quantum…

computing

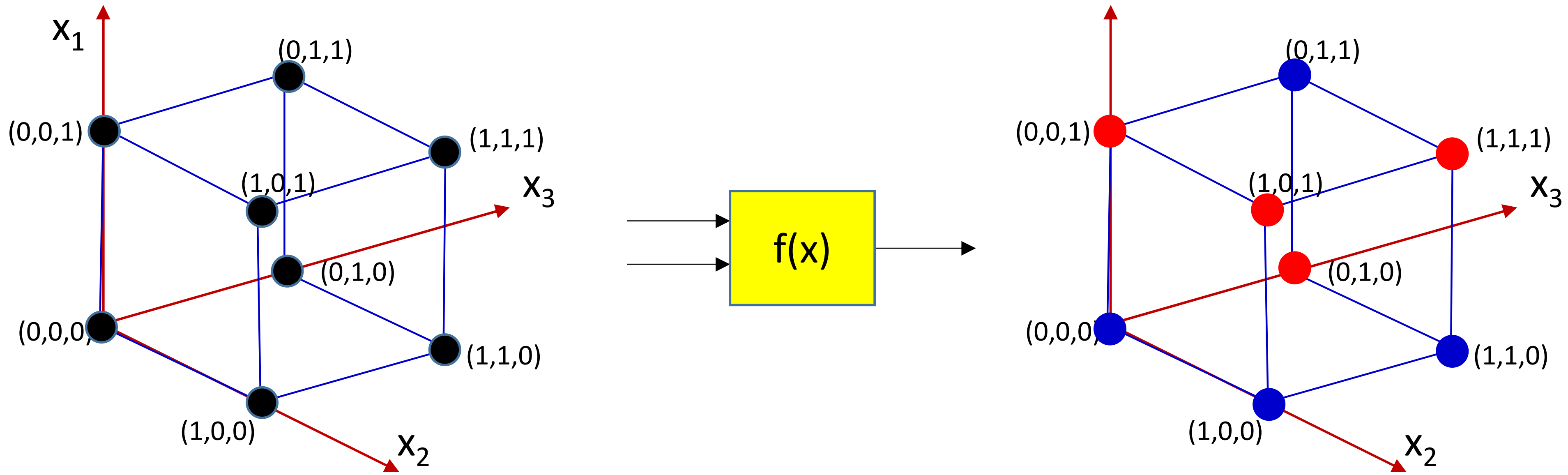
Recap: A model for computation



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

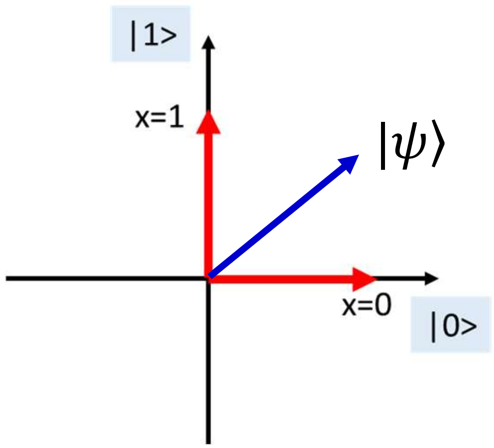


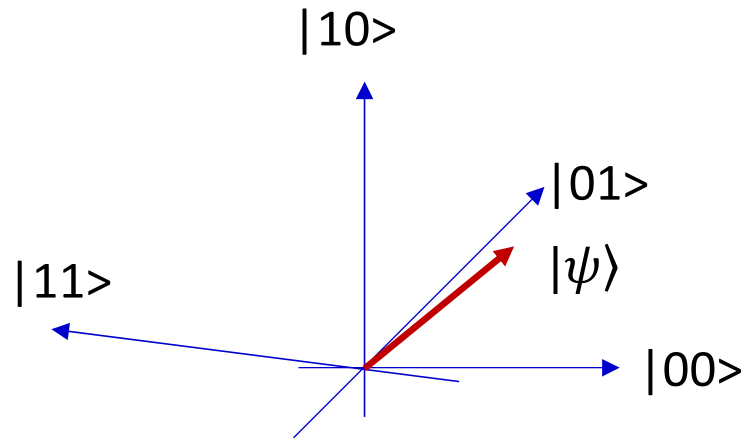
Recap: Classical math



- 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

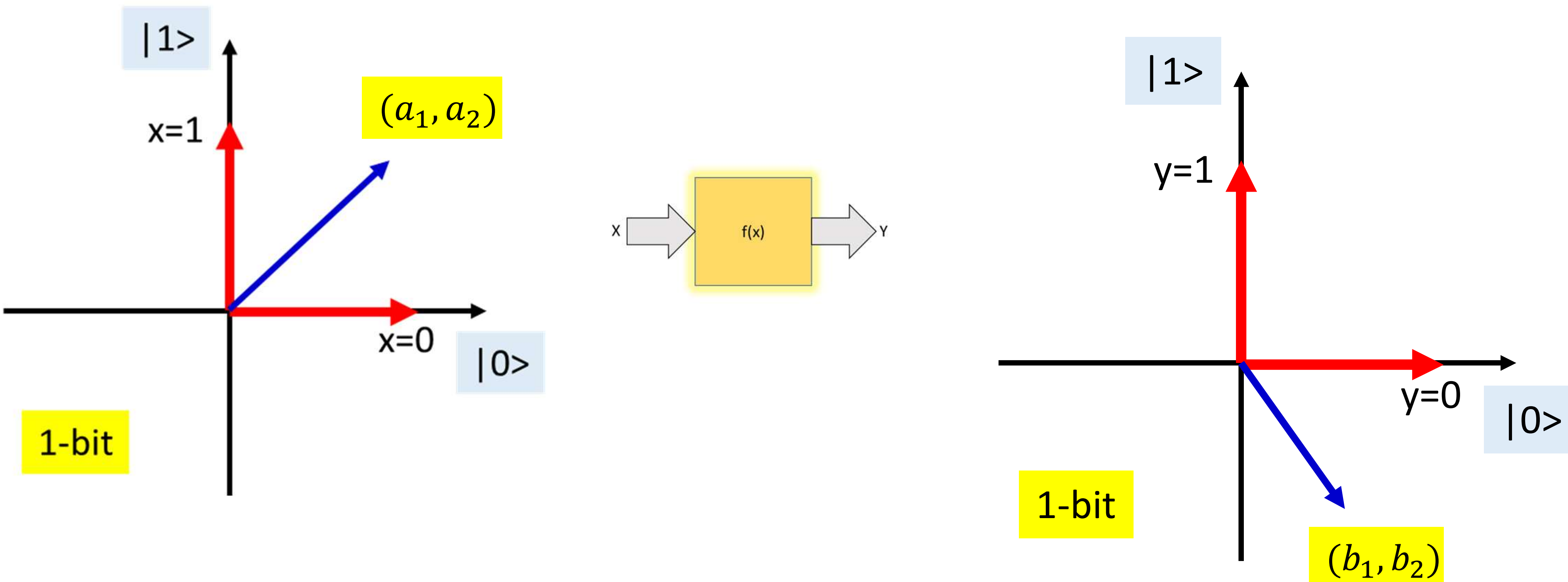




Lame attempt at visualizing 4D

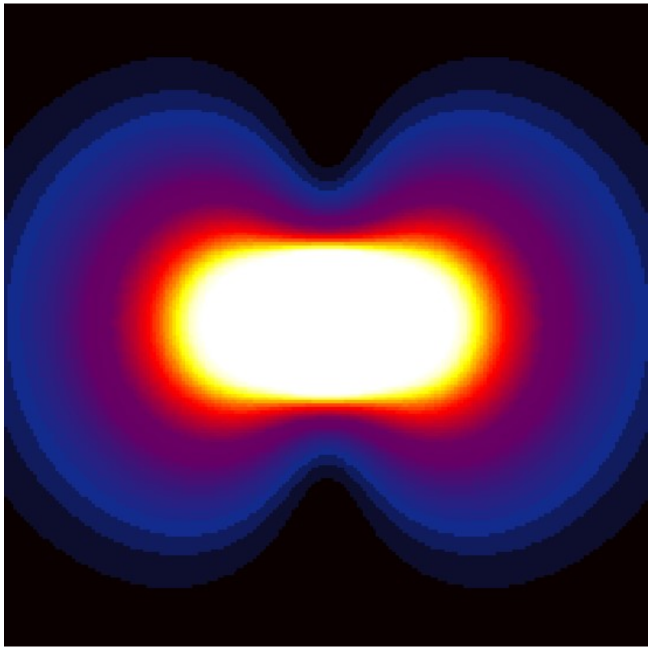
- *Bit patterns* now represent orthogonal directions
- An input is now a vector (a phasor) in this new space
  - And represents a linear combination of bit patterns
  - 1 bit: $|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$
  - 2 bits: $|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle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

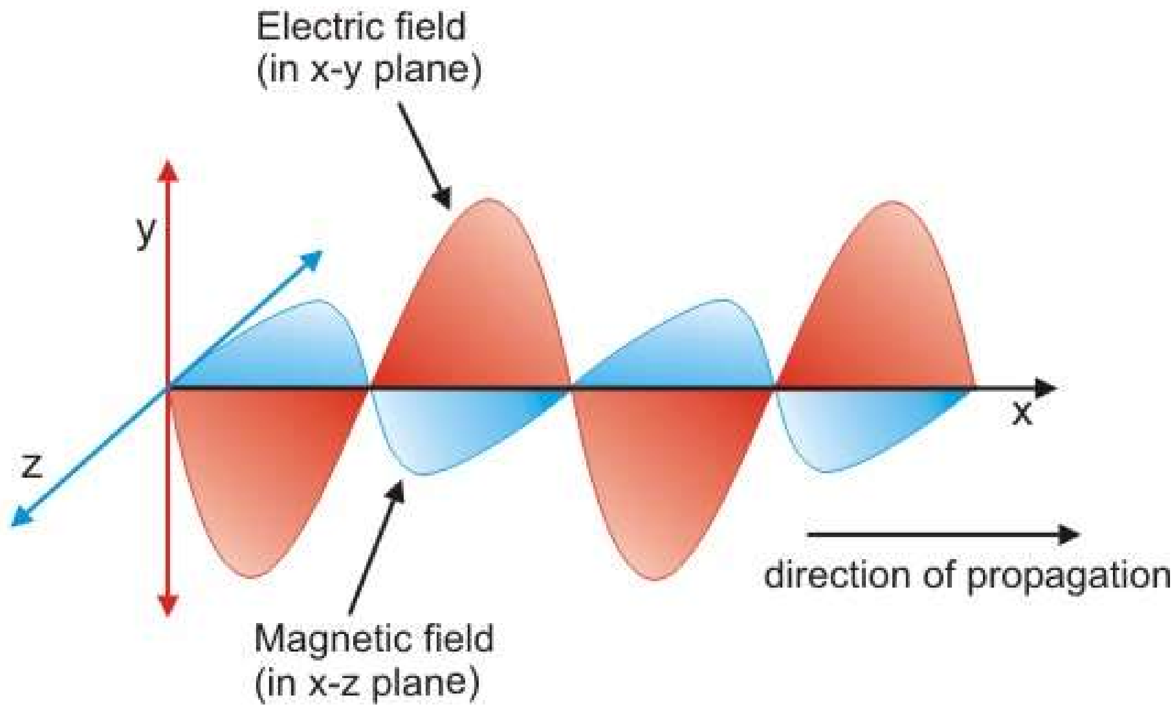
Recap: The new "quantum" math



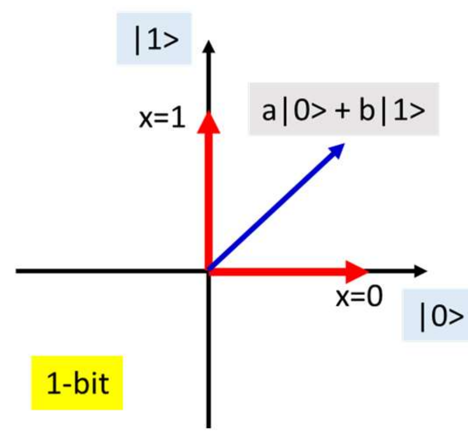
- An algorithm is now an operator that operates on the vector to produce another vector
  - Can now compute the output for *all* bit patterns in a single evaluation step
- Caveats – the operator must be:
  - Linear
  - Invertible
  - And not increase the length of the vector (i.e. it must be a rotation)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

Quantum systems

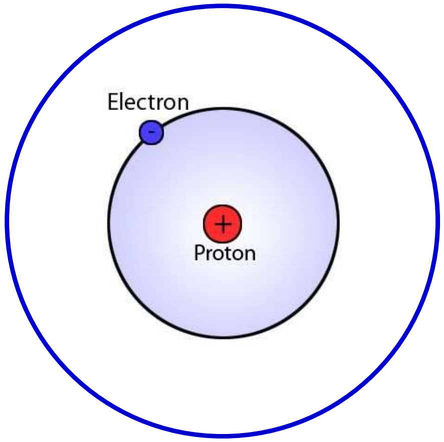


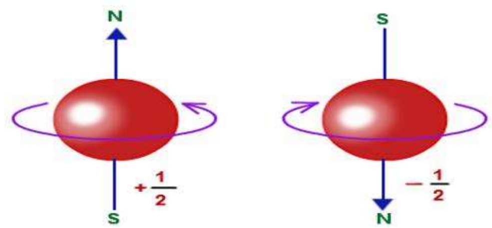


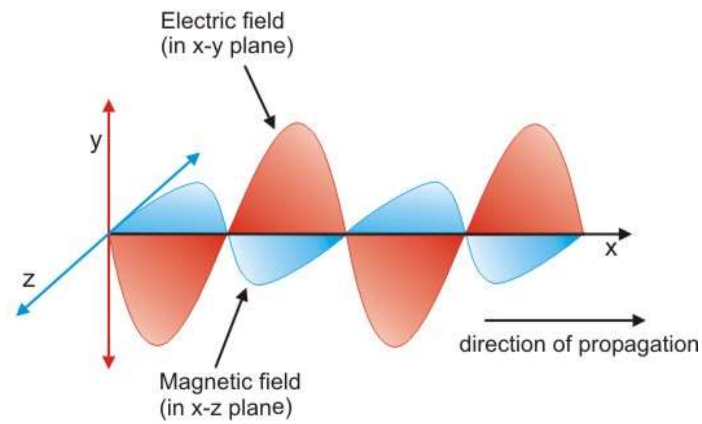
- Cannot use classical physics
  - Will require computers with exponential amounts of memory to represent even a small number of bits
- Quantum systems naturally exist in a superposition of multiple values
  - If we assign each value to a bit value (or bit pattern), we get a quantum computing platform



Recap: Implementing the qubit

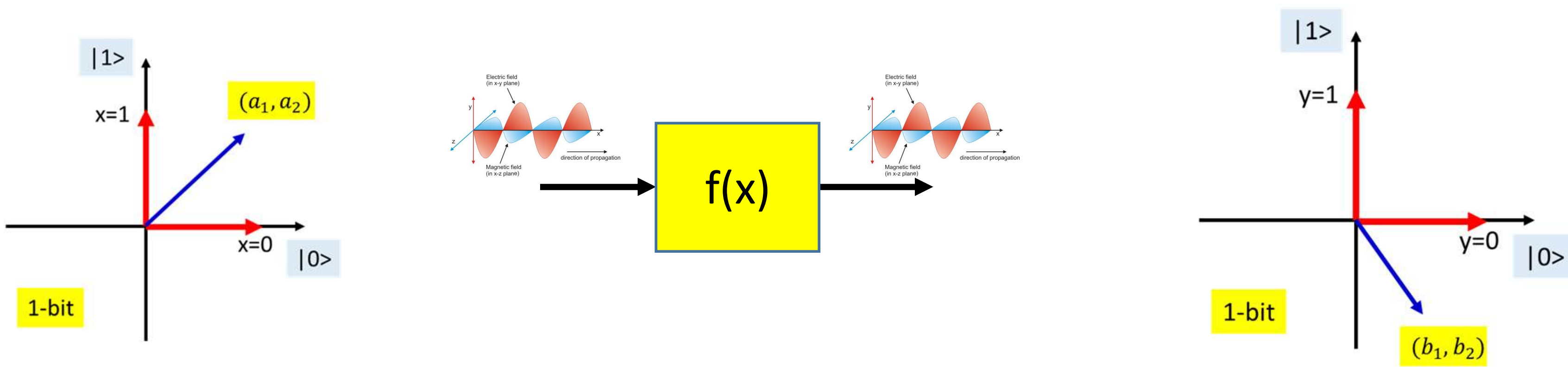






- Use quantum physics
  - Derived from Schrodinger's equation: $ih\frac{d}{dt}|\psi(t)\rangle = 2\pi H|\psi(t)\rangle$
    - Every particle is a wave that exists in all states $|\psi(t,x)\rangle$ simultaneously
    - $|\psi(t,x)\rangle|^2$ = probability of finding the system in configuration x at time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

The 1-qubit quantum system



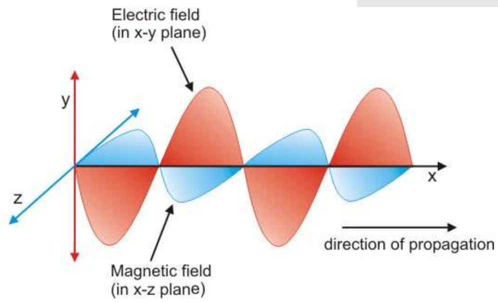
- The one-qubit system utilizes a single quantum entity to represent a bit in the new math
  - As input and output

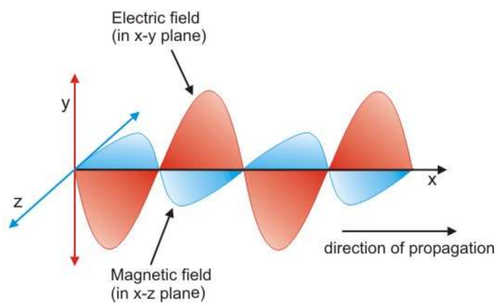
- I.e. the input is a single qubit, and the output too is a single qubit

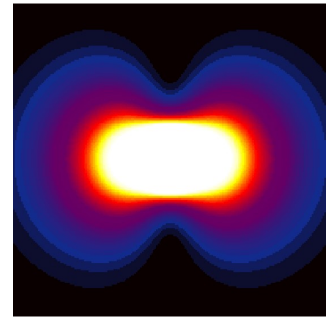
- The input is actually a 2-dimensional vector, and so is the output
  - It is just that a single “qubit” can fully encode this 2-dimensional vector
    - Thank you Shroedinger

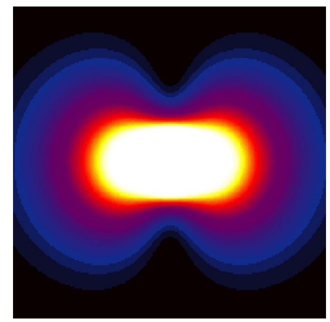
Multiple bits

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

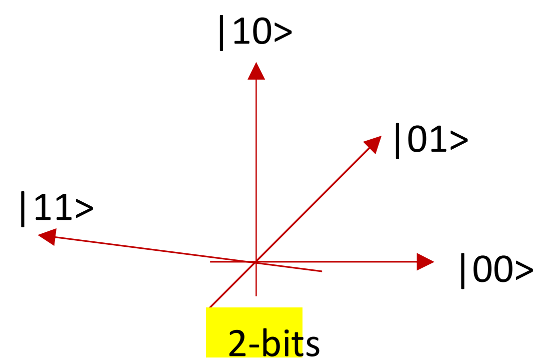




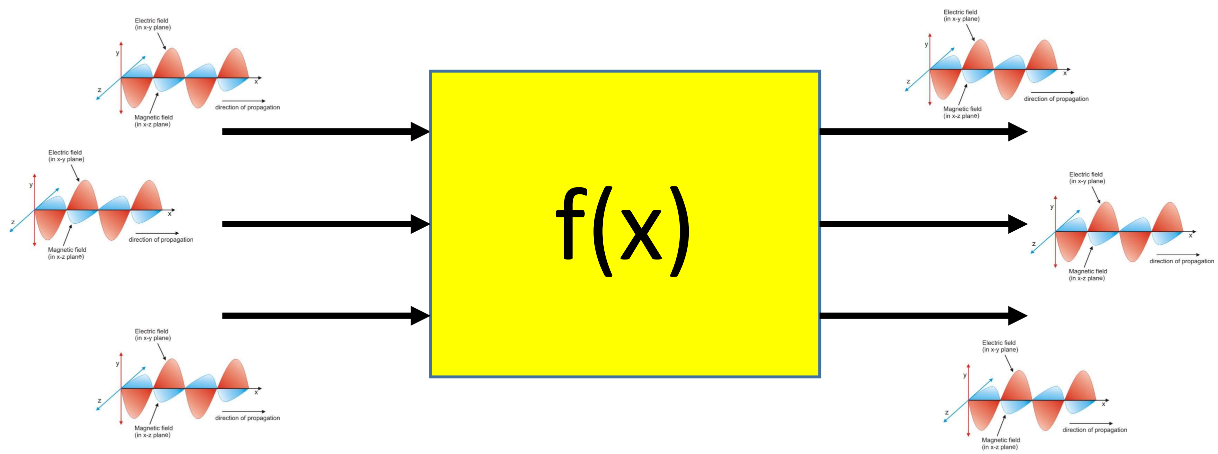




- Increasing the number of bits only takes increasing the number of basic quantum units



The multi-qubit quantum system



- N qubits go in and N qubits come out
- The input is actually a 2^N-dimensional vector, and so is the output
  - It is just that a single "qubit" can fully encode this 2-dimensional vector
  - N qubits can encode a 2^N dimensional space
    - Thank you Shroedinger

Poll 1

- Which of the following are instances of representation in the new math
  - 000
  - $a_0|00\rangle + a_1|01\rangle + a_2|10\rangle + a_3|11\rangle$
  - 00 + 01
  - $a_0|0\rangle + a_1|1\rangle + a_2|2\rangle + a_3|3\rangle + a_4|4\rangle + a_5|5\rangle + a_6|6\rangle + a_7|7\rangle$

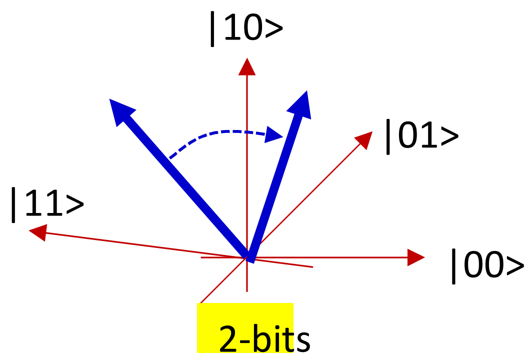
- Which of the following are potential practical platforms for the new math
  - Silicon transistors
  - Photons
  - Electrons
  - Magnetic moments of atoms

Poll 1

- Which of the following are instances of representation in the new math
  - 000
  - $\boldsymbol{a_0|00\rangle + a_1|01\rangle + a_2|10\rangle + a_3|11\rangle}$
  - 00 + 01
  - $\boldsymbol{a_0|0\rangle + a_1|1\rangle + a_2|2\rangle + a_3|3\rangle + a_4|4\rangle + a_5|5\rangle + a_6|6\rangle + a_7|7\rangle}$

- Which of the following are potential practical platforms for the new math
  - Silicon transistors
  - **Photons**
  - **Electrons**
  - **Magnetic moments of atoms**

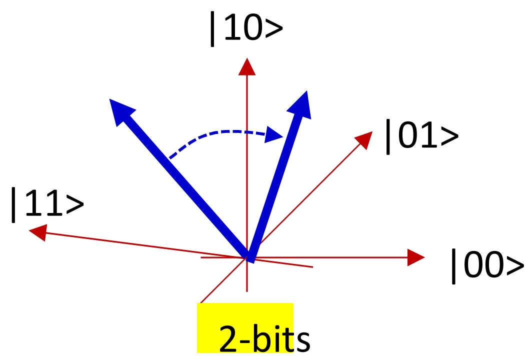
Practical implementation



- Simply use a collection of quantum bits
  - Will simultaneously represent all states

- What is missing?

Practical implementation

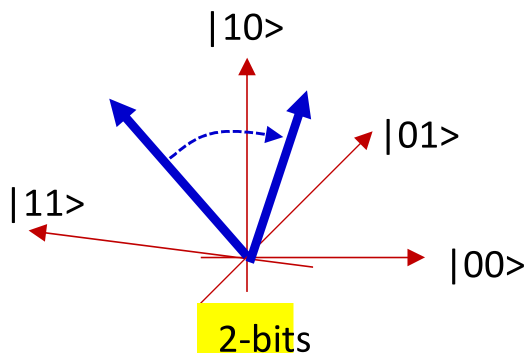


- Simply use a collection of quantum bits
  - Will simultaneously represent all states

- What is missing?
  - How do you implement the functions?
    - Invertible rotations $i h \frac{d}{dt} |\psi(t)\rangle = 2\pi H |\psi(t)\rangle$

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

Practical implementation

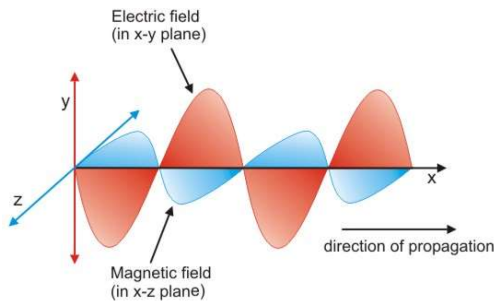


- Simply use a collection of quantum bits
  - Will simultaneously represent all states

- 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?**

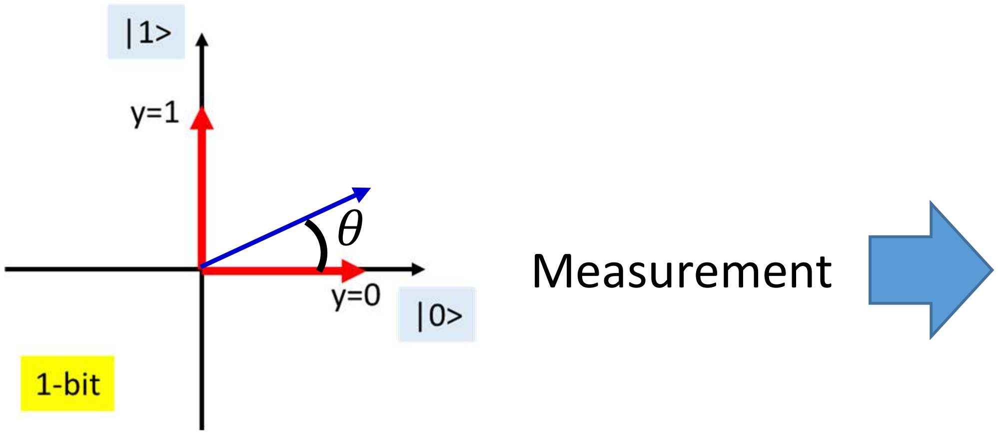
The problem with measurement

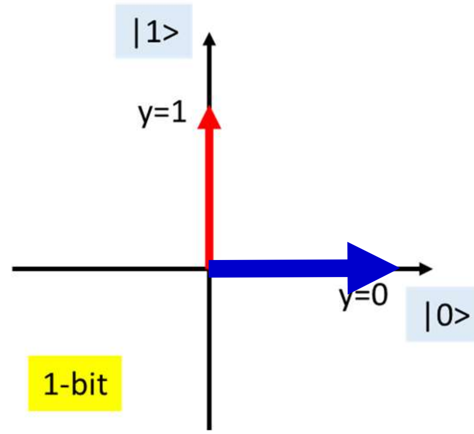
- **Reality Doesn't Exist Until We Measure It, Quantum Experiment Confirms**
- https://www.sciencealert.com/reality-doesn-t-exist-until-we-measure-it-quantum-experiment-confirms

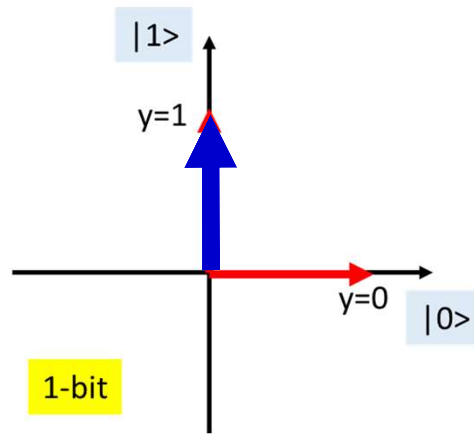


- Measuring a quantum variable "collapses" it

Measurement

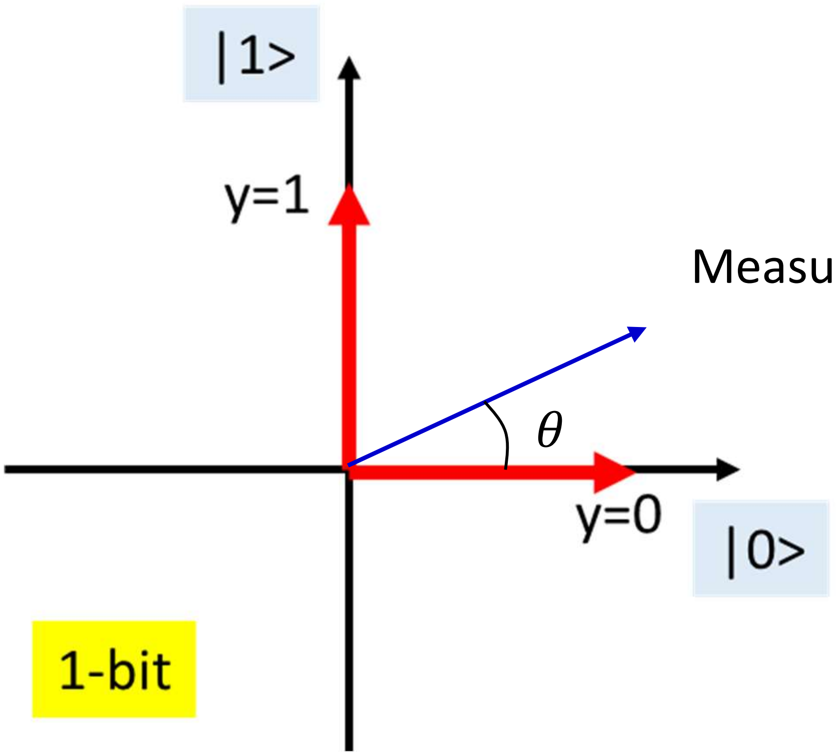




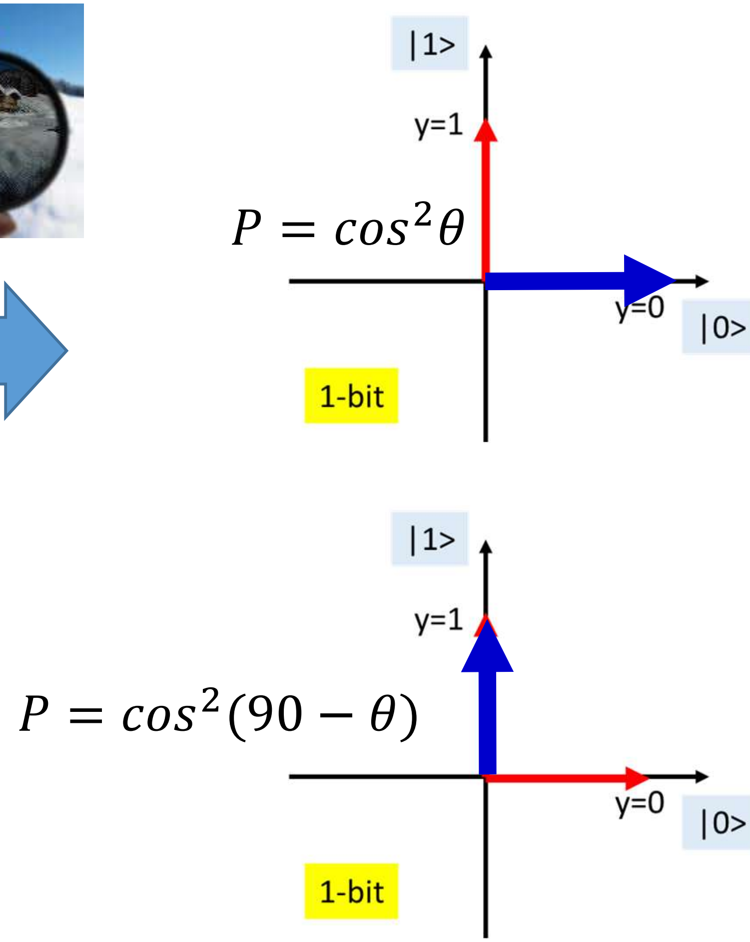


- Measuring the output collapses the vector to one of the states
  - Bit pattern
- Which one

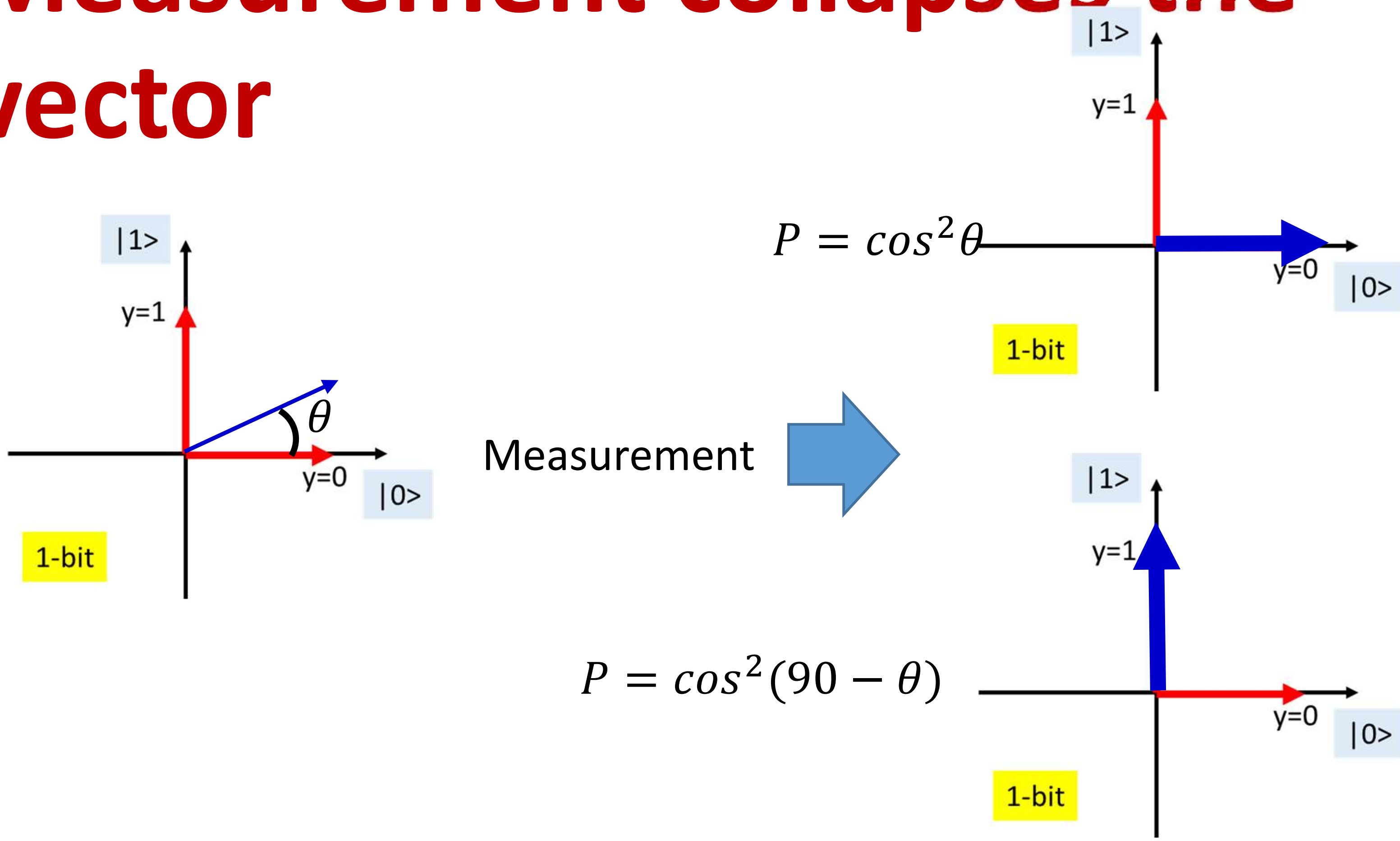
Measurement



Measurement



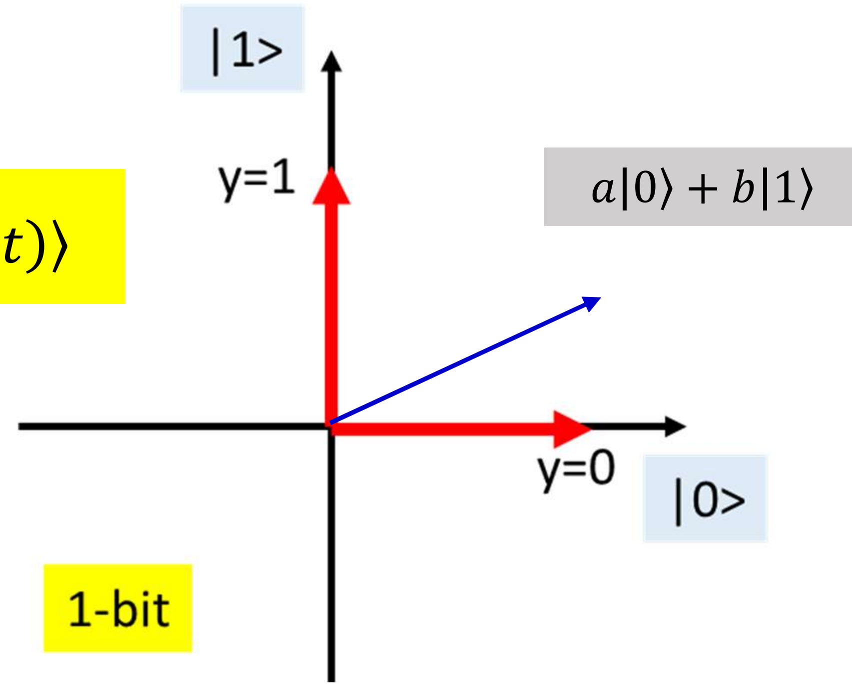
Measurement collapses the vector



- How many measurements must you take to recover the full vector?
  - *Keeping in mind that each measurement means creating and manipulation "qbits" from scratch*
  - Can you even recover it fully?

It's complex, but not complicated

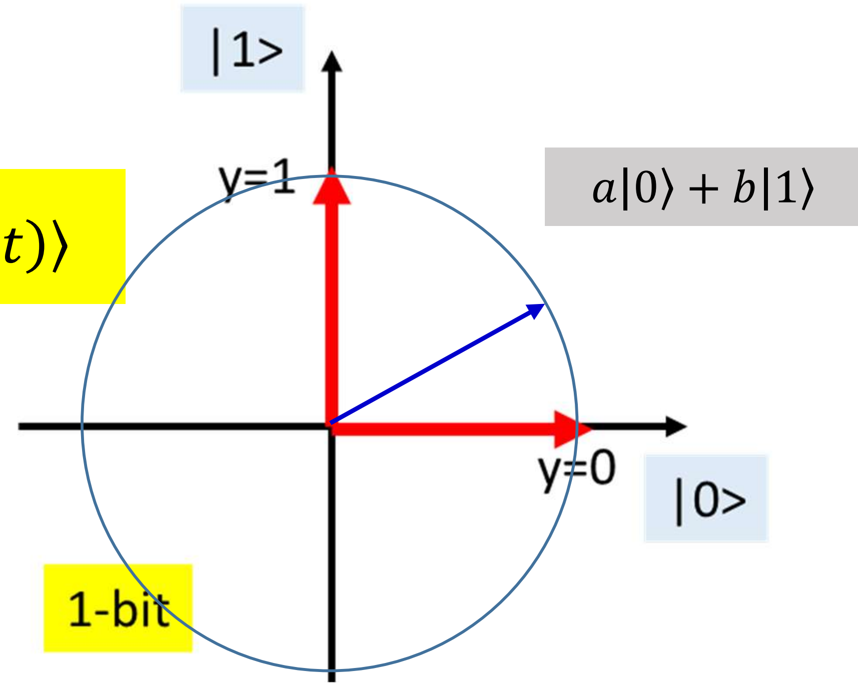
$$ih\frac{d}{dt}|\psi(t)\rangle = 2\pi H|\psi(t)\rangle$$



- 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

Restrictions on the weights

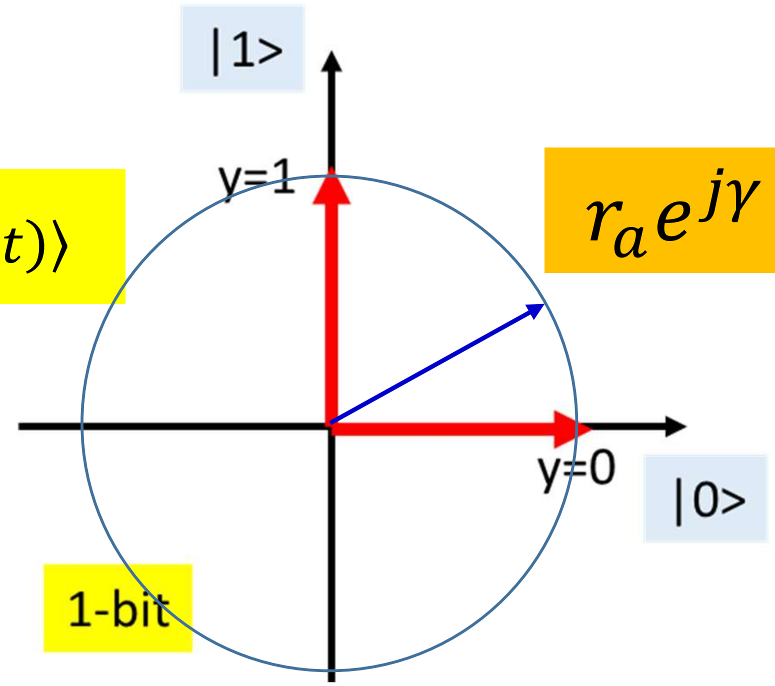
$$ih\frac{d}{dt}|\psi(t)\rangle = 2\pi H|\psi(t)\rangle$$



- $|a|^2 + |b|^2 = 1$
  - The qubits live on the surface of a hypersphere
- $P(|0\rangle) = |a|^2,\ \ P(|1\rangle) = |b|^2$
- $\boldsymbol{a = r_a e^{j\gamma}, b = r_b e^{j\delta}}$
  - ${r_a}^2 + {r_b}^2 = 1$
  - The vector is actually a *complex* vector, where each component has a magnitude and a phase
- The *length of the vector is always 1* (because the probabilities of 0 and 1 must sum to 1.0)
  - Repeated measurement can recover the *magnitude* r_a and r_b of the components, but not the phase

Visualizing the qubit

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

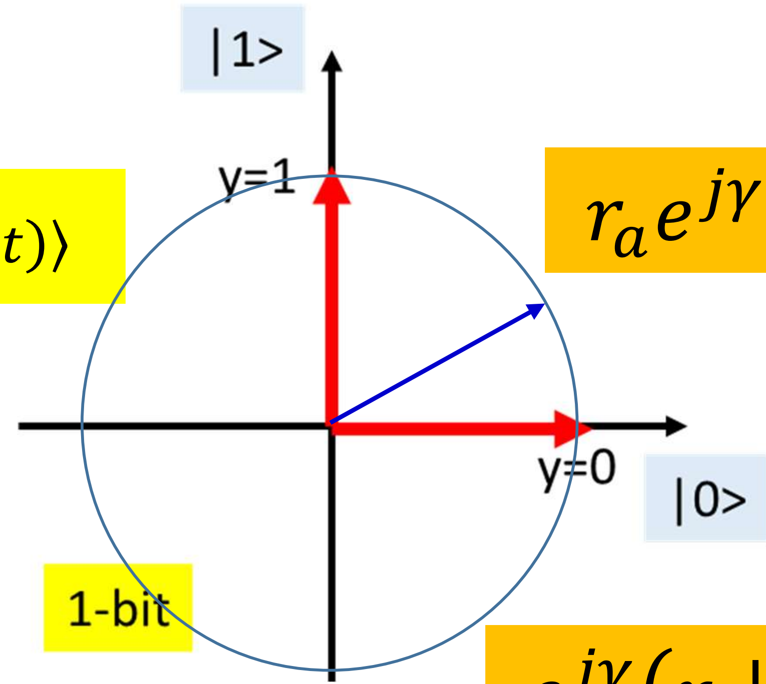


$$r_a e^{j\gamma}|0\rangle + r_b e^{j\delta}|1\rangle$$

- $a = r_a e^{j\gamma}, b = r_b e^{j\delta}$

Visualizing the qubit

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



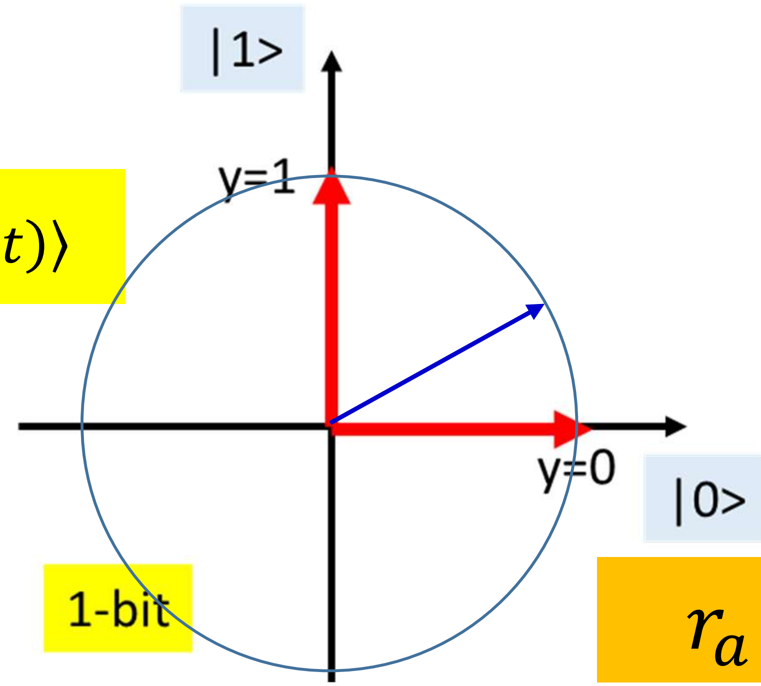
$$r_a e^{j\gamma}|0\rangle + r_b e^{j\delta}|1\rangle$$

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

- $a = r_a e^{j\gamma}, b = r_b e^{j\delta}$
- The common phase γ represents the angle of the viewpoint and can be ignored

Visualizing the qubit

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

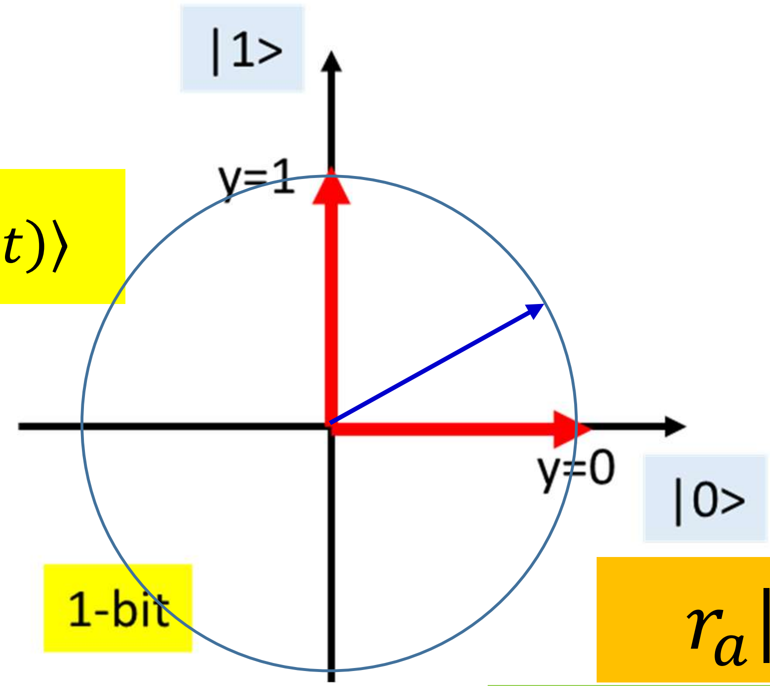


$$r_a|0\rangle + r_b e^{j\phi}|1\rangle$$

- $|r_a|^2 + |r_b|^2 = 1$
- Have the form $r_a = \cos\frac{\theta}{2}, r_b = \sin\frac{\theta}{2}$

Visualizing the qubit

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



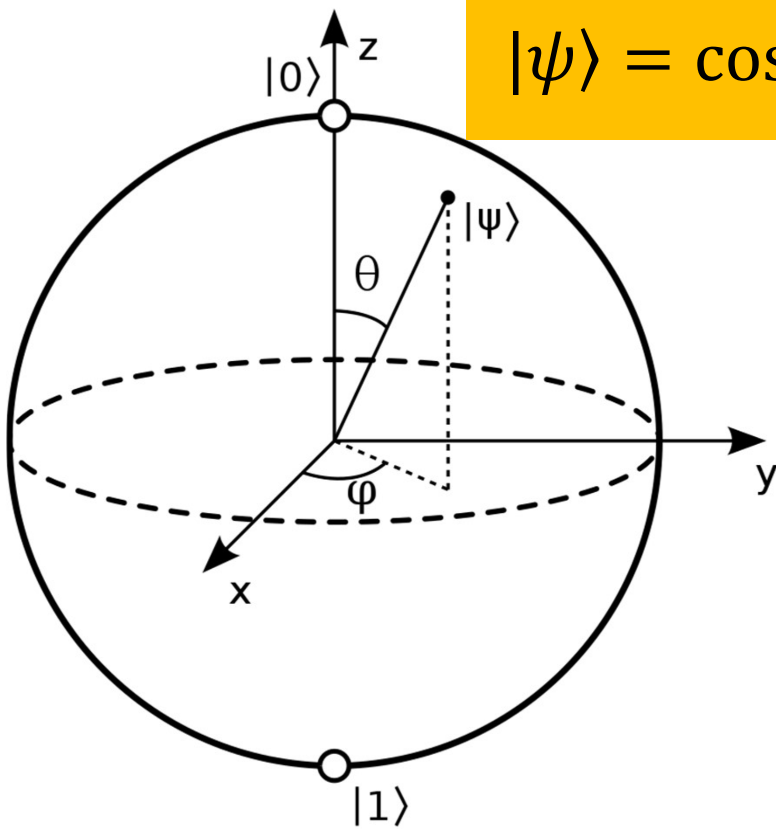
$$r_a|0\rangle + r_b e^{j\phi}|1\rangle$$

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

- $|r_a|^2 + |r_b|^2 = 1$
- Have the form $r_a = \cos\frac{\theta}{2}, r_b = \sin\frac{\theta}{2}$

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

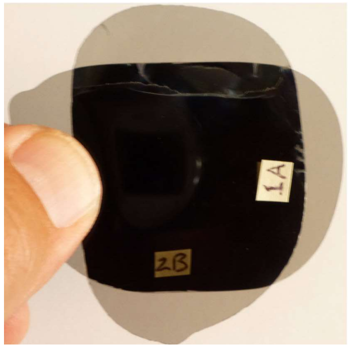
Poll 2

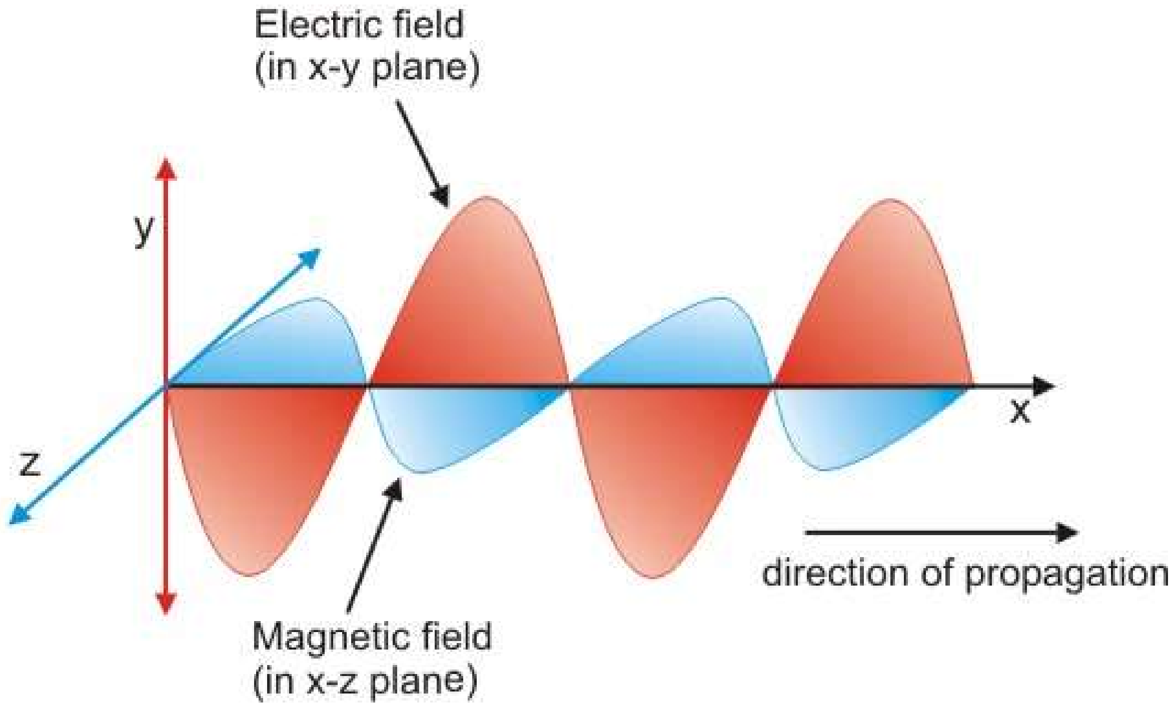
- Mark all true statements
  - Although it is currently not possible to recover the value of a qubit fully (because measurement always collapses it to one of the states), we can expect that eventually physics will catch up and this will become possible
  - We can recover the approximate value of a qubit by repeated measurement, which will give us estimates of the P(|0>) and P(|1>) for the qubit
  - We can never recover the true, or even approximate value of a qubit, and can never hope to do so in the current universe with its laws of physics
  - We should stop worrying about metaphysics and just go to the beach…

Poll 2

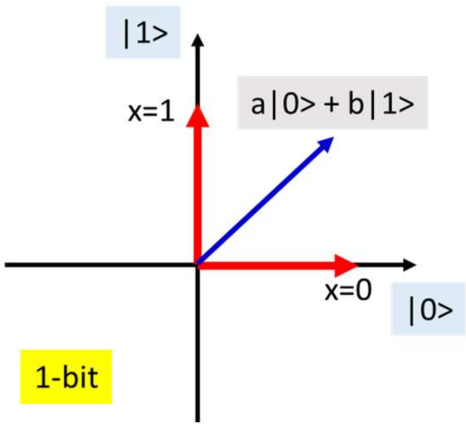
- Mark all true statements
  - Although it is currently not possible to recover the value of a qubit fully (because measurement always collapses it to one of the states), we can expect that eventually physics will catch up and this will become possible
  - We can recover the approximate value of a qubit by repeated measurement, which will give us estimates of the P(|0>) and P(|1>) for the qubit
  - **We can never recover the true, or even approximate value of a qubit, and can never hope to do so in the current universe with its laws of physics**
  - **We should stop worrying about metaphysics and just go to the beach…**

Returning to measurement

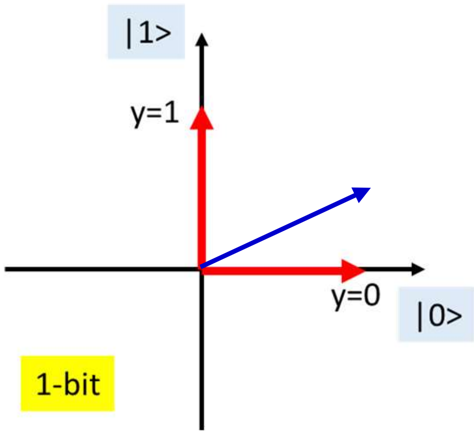


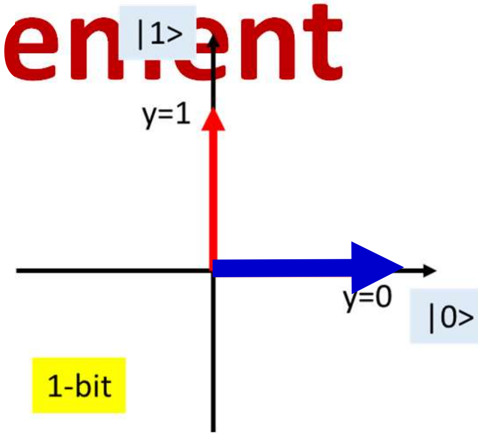


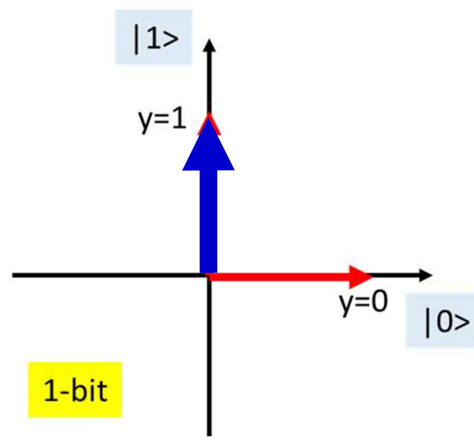
- The system lives in a superposition of states
  - A "phasor" in the quantum space
  - But what are these "states"?
- To 'read' it, we need a measuring device
- The measuring device basically represents a set of "bases", or coordinate axes, with respect to which we attempt to assign coordinate values to the phasor
  - The bases represent the set of orthogonal "states"



Returning to Measurement

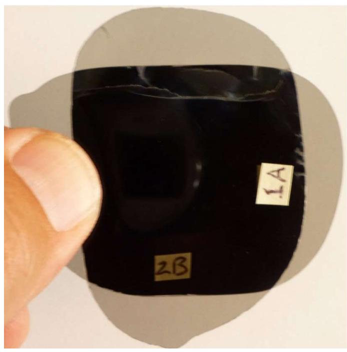


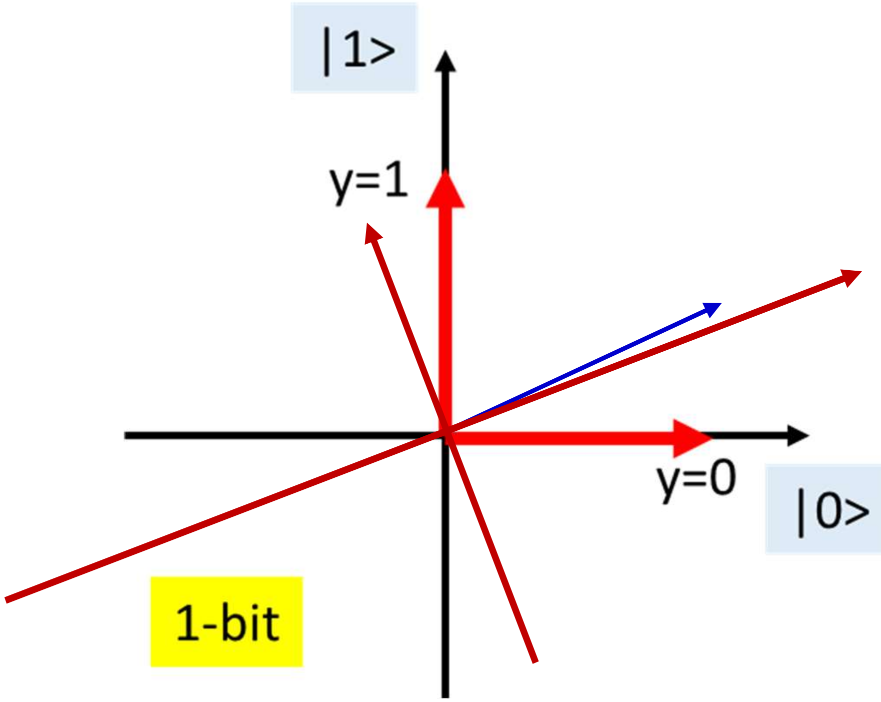




- Measuring the output collapses the vector to one of the states
- **The states represent *bases***
  - **And are associated with bit patterns only by fiat**
- **Measurement collapses the vector to one of the bases**

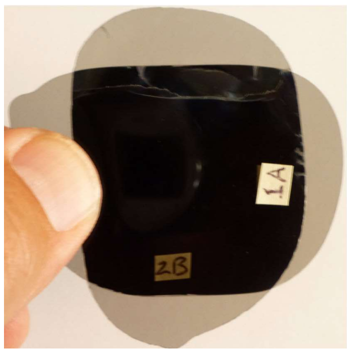
The physical Qubit

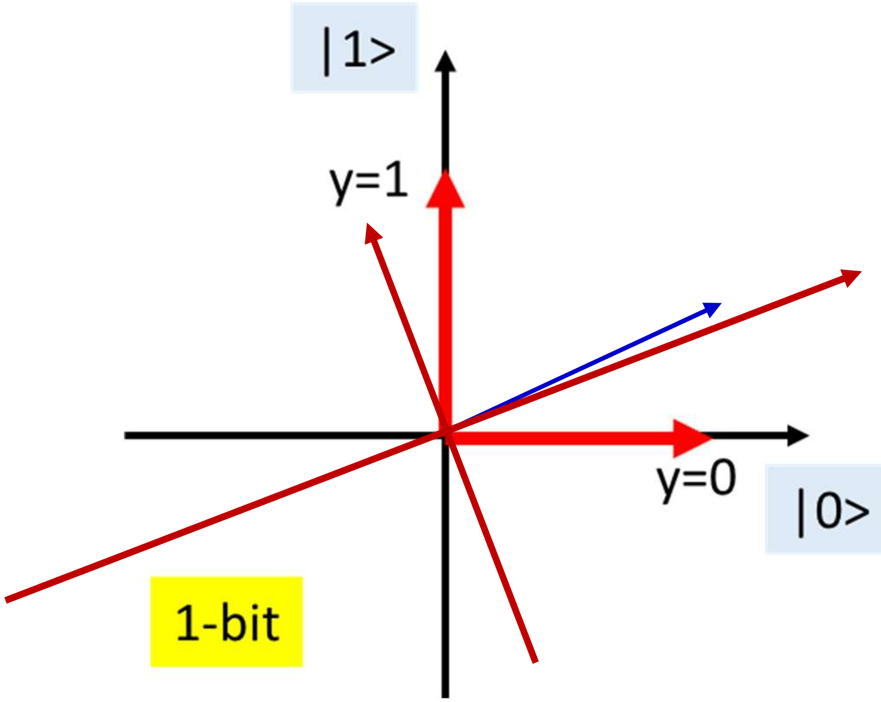




- The definition of your “bases” is a matter of convention
- The only requirement is that they are at right angles to one another.
- The representation of the vector will, obviously, depend on the bases

The physical Qubit



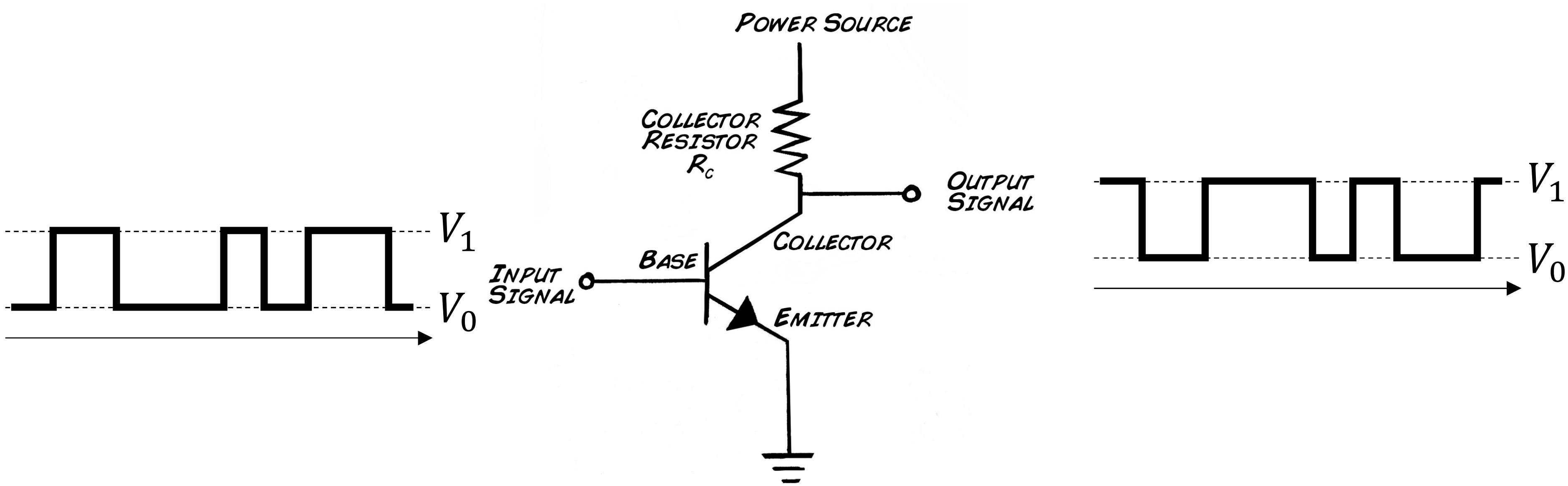


- The definition of your “bases” is a matter of convention

But how do these “bases” relate to our new math?

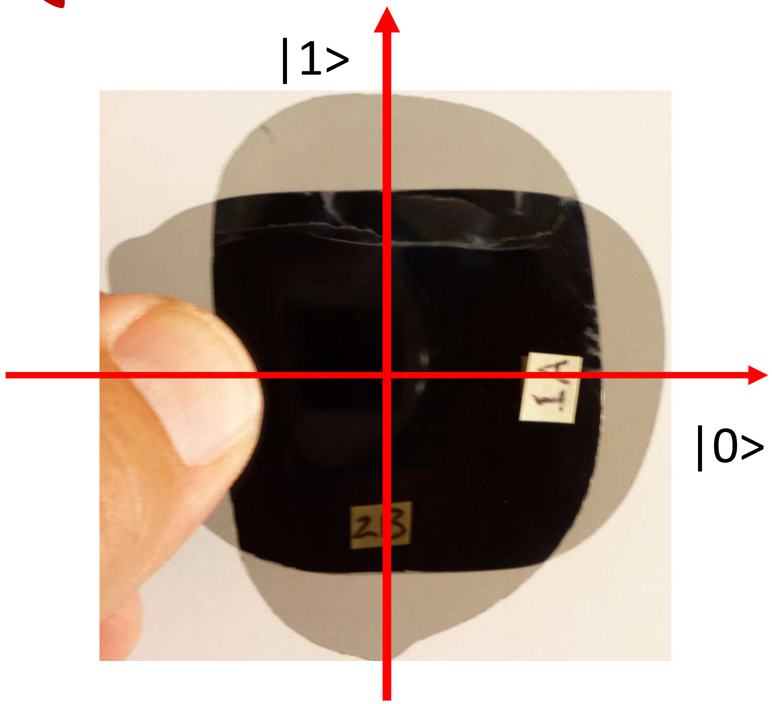
Revisiting classical computation

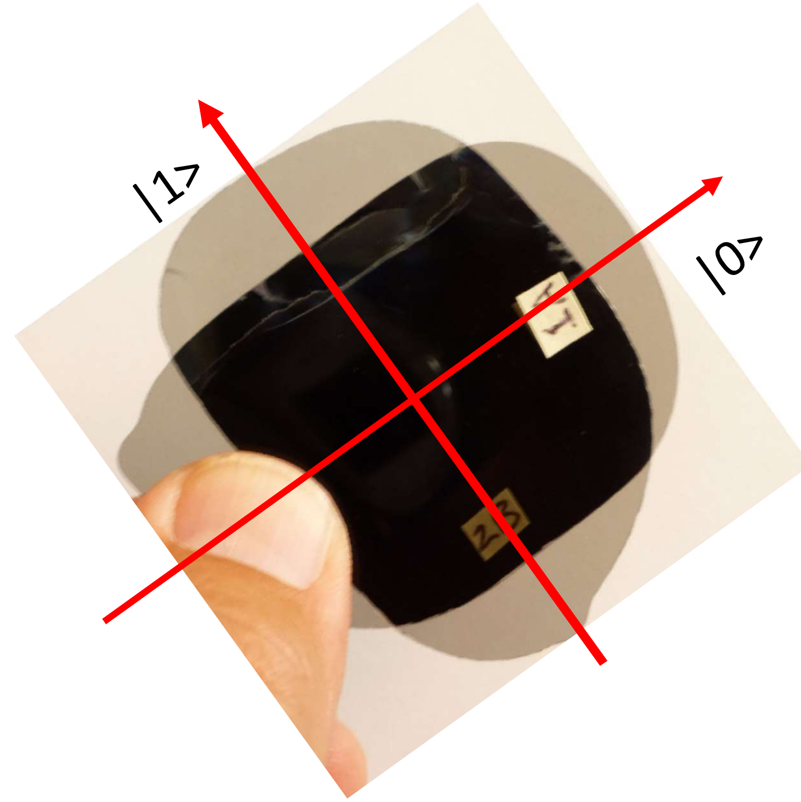
|1>



- Note: In classical computation, the symbols 0 or 1 are just designations
  - The circuits don't *actually* produce a number 0 or a number 1
- Typically designate some voltage level (or voltage pattern) V_0 and "0" and V_1 as "1"
  - The key is that there are only two levels, so there is one unique Boolean representation derived from it

Quantum bases

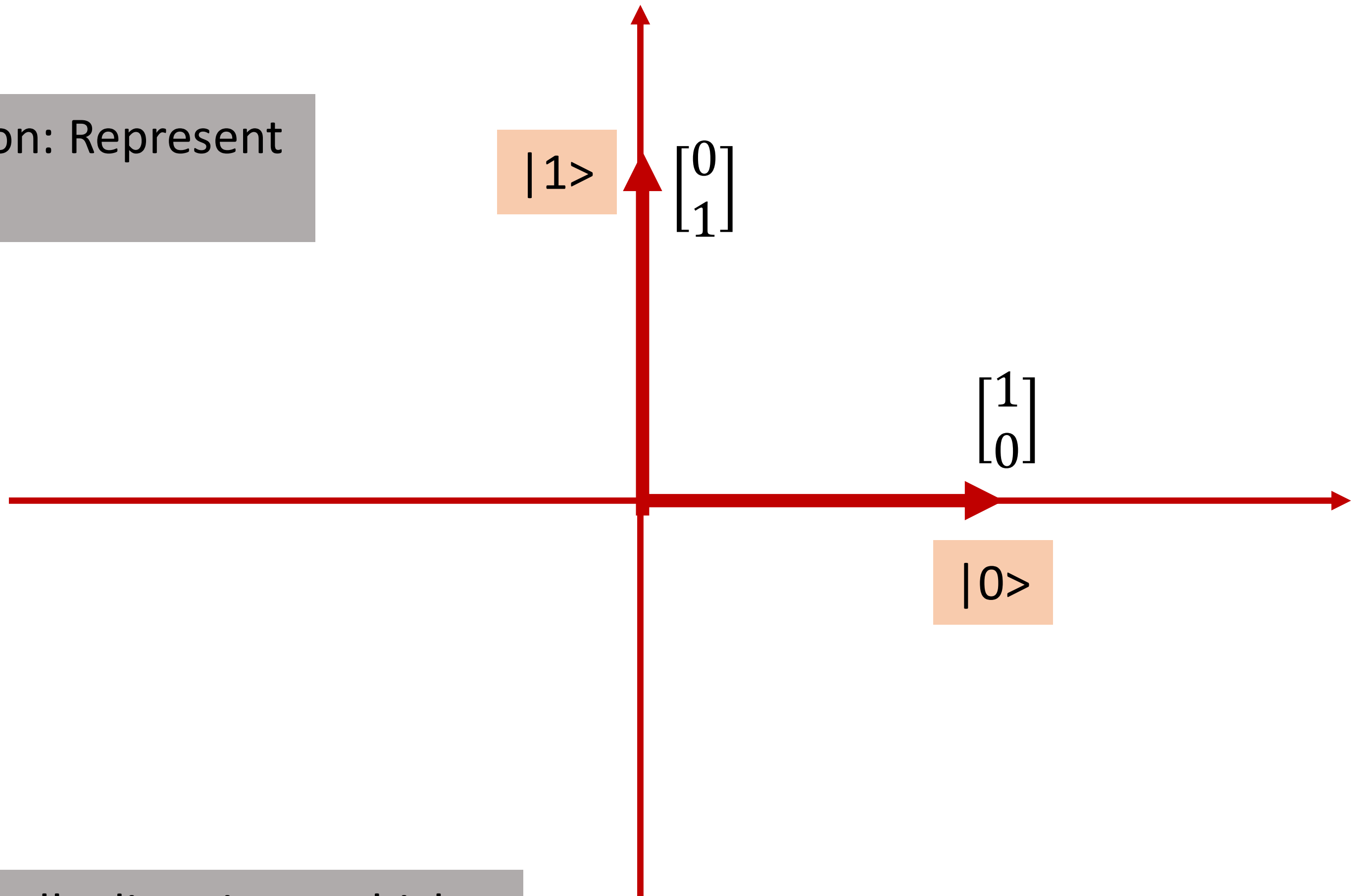




- In quantum computing too, values are just arbitrary designations
- We now have *bases* instead of voltage levels. These must be designated
  - E.g. the horizontal bit basis is designated as bit value 0 and the vertical basis is designated as bit value 1
  - To distinguish between the *value* 0 and the direction of the *basis* that represents 0, we will designate it using a special notation: the “BRA-KET” notation
    - Bit value 0 → |0>
    - Bit value 1 → |1>

Bras, Kets, and vectors

Vector notation: Represent as vectors.



In bit bases:

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

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

Bases are actually directions, which can be represented as vectors .

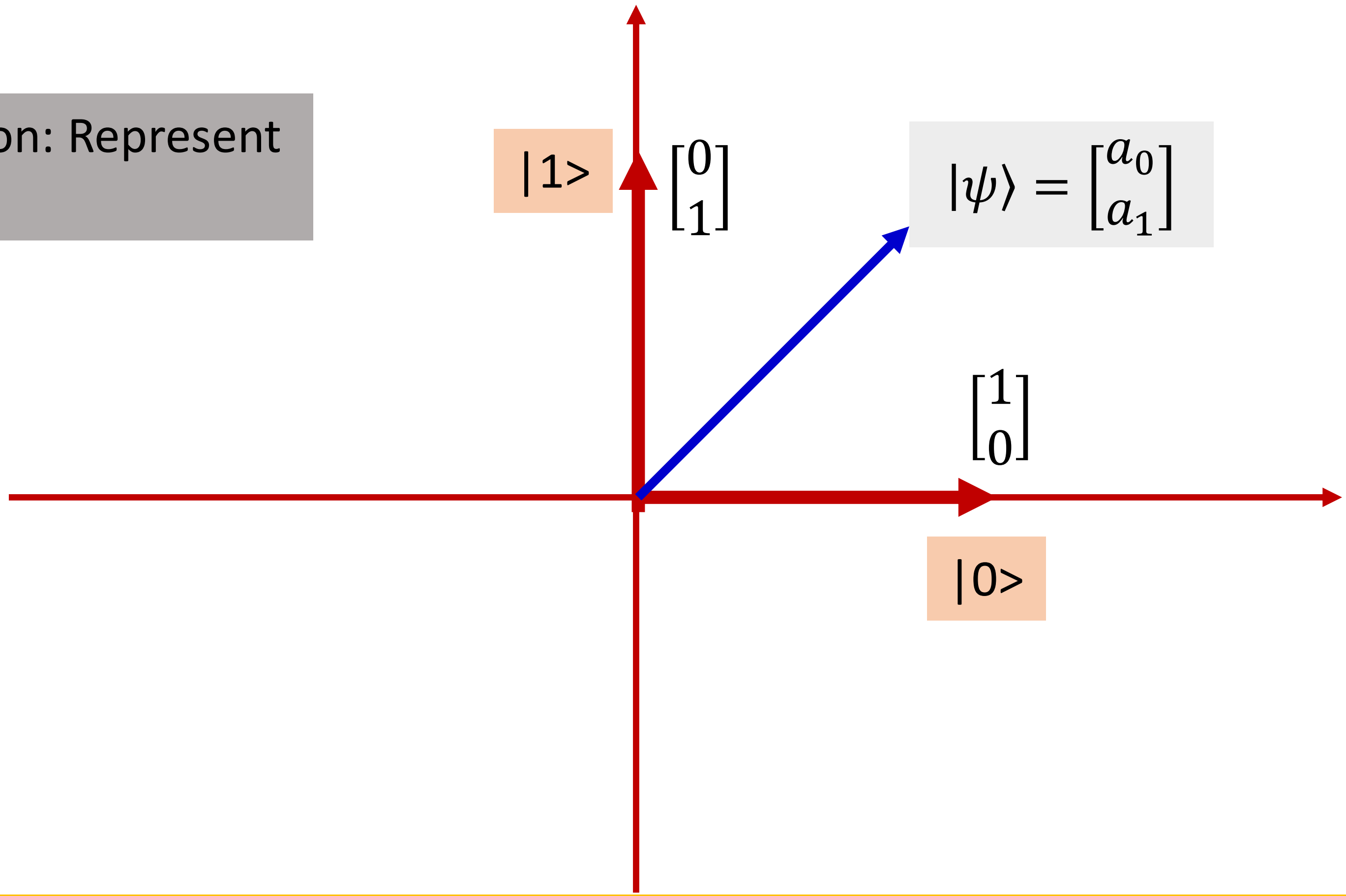
The directions for $\begin{bmatrix}1\\0\end{bmatrix}$and $\begin{bmatrix}0\\1\end{bmatrix}$ are implicitly the canonical bit bases

BRA – KET notation: Bases are represented using “BRA”s and “KET”s

The symbol inside the Bra-ket can be anything, but it represents a unit step in a direction

Bras, Kets, and vectors

Vector notation: Represent as vectors.



In bit bases:

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

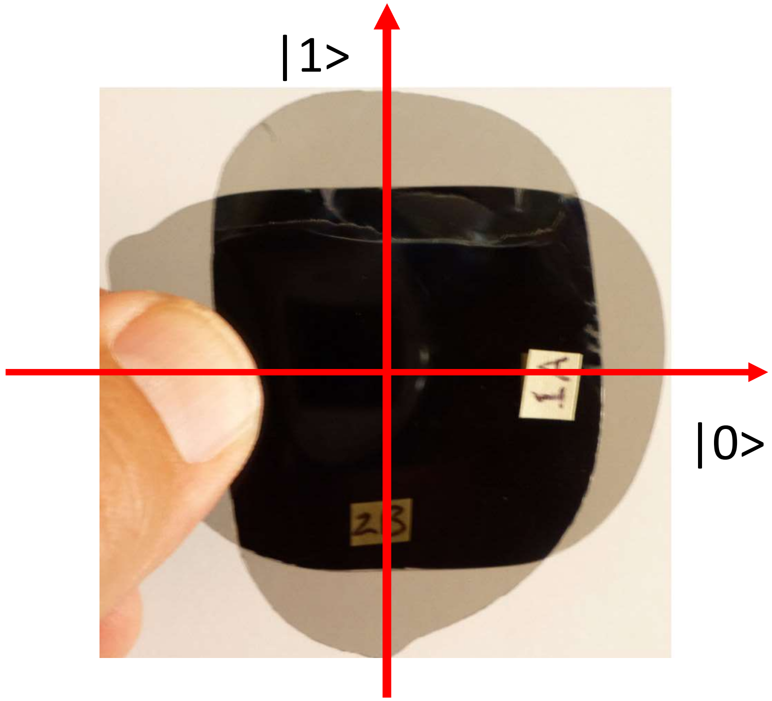
$$|1\rangle = \begin{bmatrix}0\\1\end{bmatrix}$$

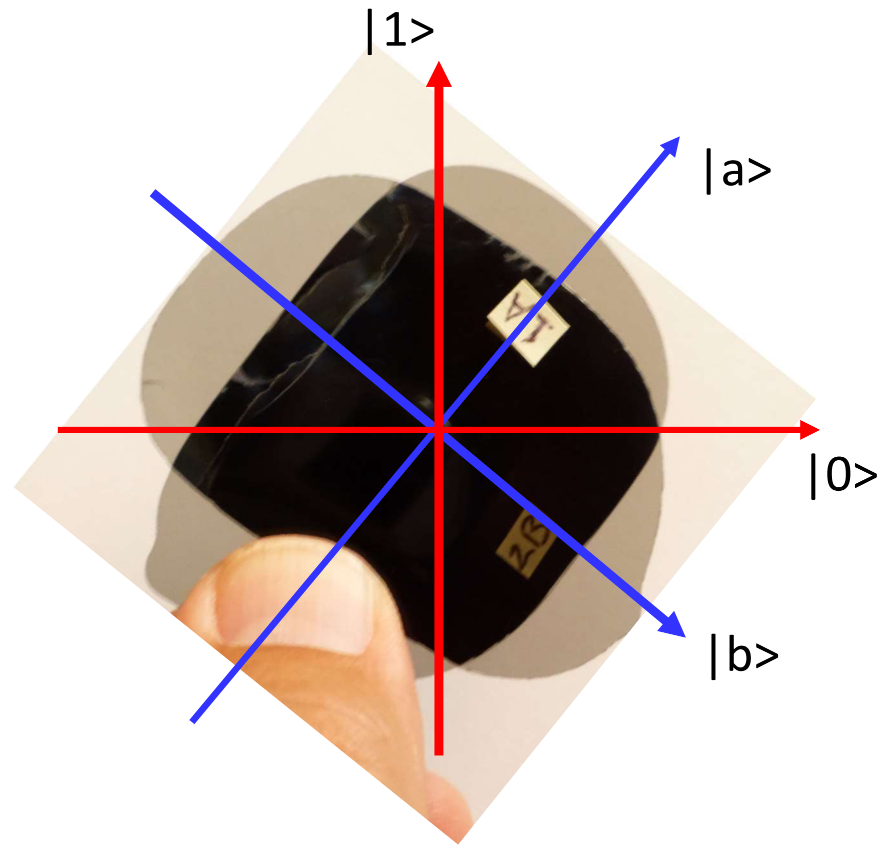
All phasors are also often represented using the Bra-Ket notation
But the phase is also a vector, which is a location in the space

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

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

Back to Bases…

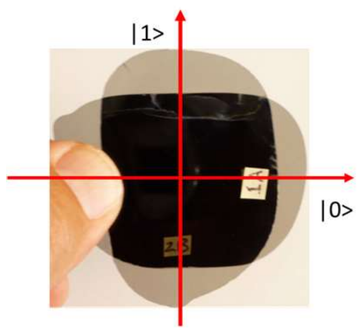


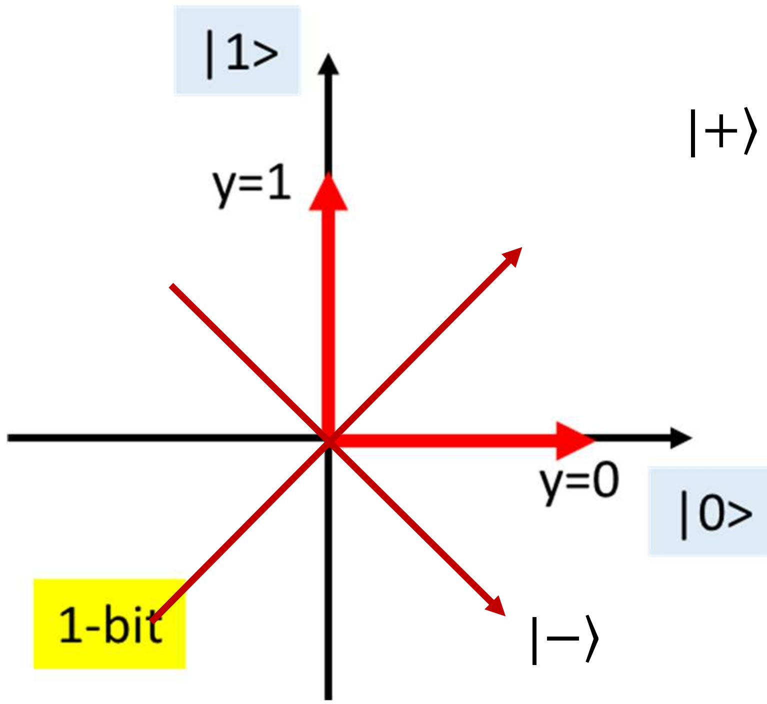


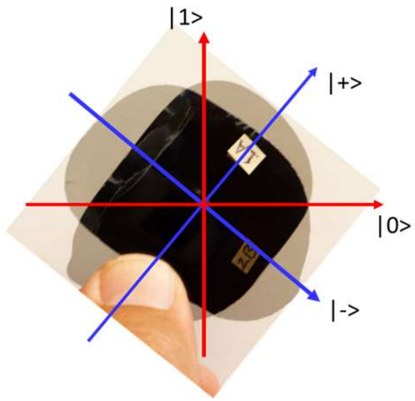
- We *always* specify some (possibly arbitrarily chosen) directions as our ``canonical'' bases
  - These are typically designated as the ``bit'' bases, representing the boolean values 0 and 1, represented as |0> and |1>

- But we can *also* have *other* bases
  - Which will have their own bra-ket symbols
  - The alternate bases can be defined in terms of our bit bases (or, alternately, our bit bases can be defined in terms of these other bases)

Alternate bases: The “sign” bases

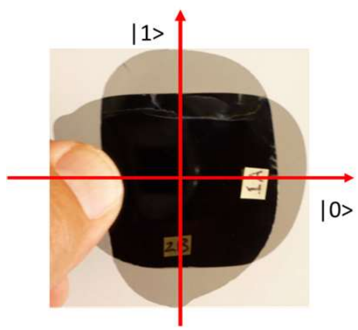


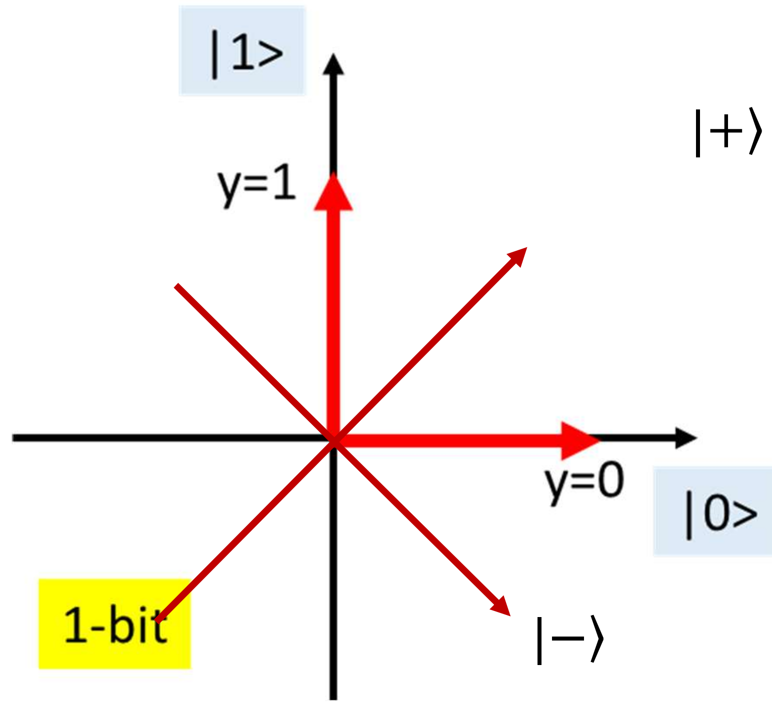


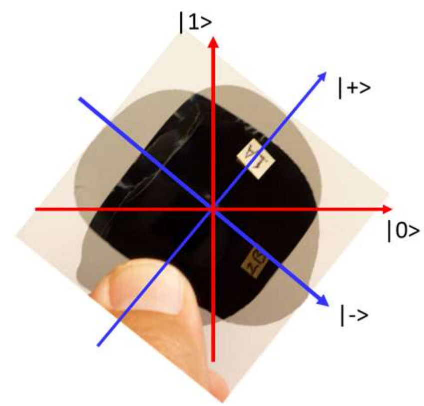


- A very popular set of alternate bases are the “sign” bases
  - Designated as $|+\rangle$ and $|-\rangle$ respectively
  - These are at +45 and -45 degrees to the bit bases, respectively
- Flipping between bit-based representations and sign-based representations is an often-encountered operation

Alternate bases: The "sign" bases







- Defining the sign bases in terms of the bit bases

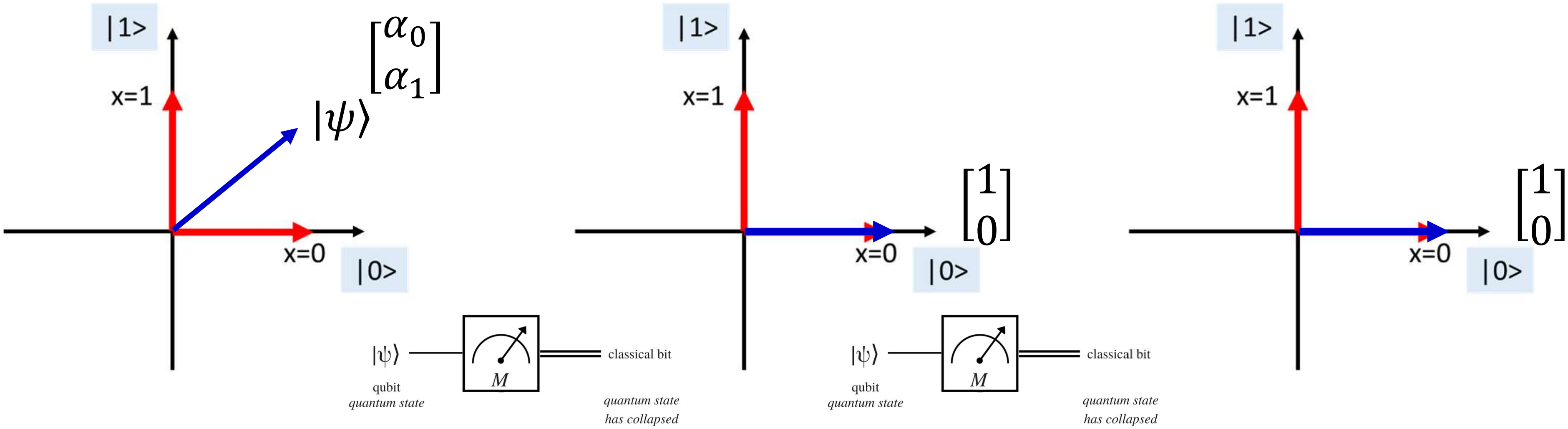
$$|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

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

Note: By definition, bases are always unit length

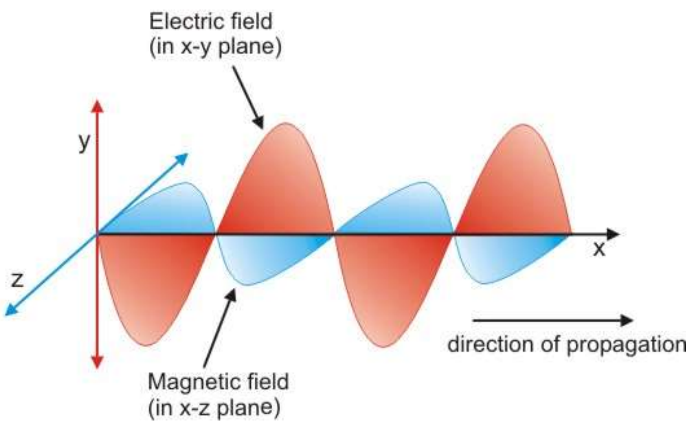
What would the bit bases be in terms of the sign bases?

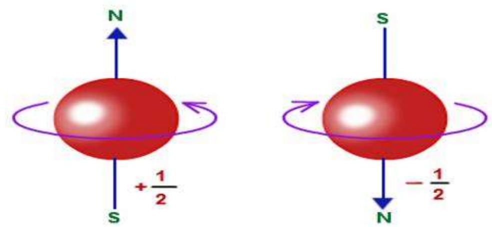
Measurement *fixes* the qubit

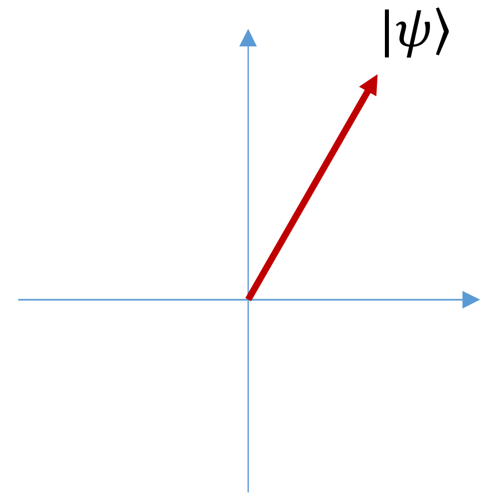


- First measurement: $|\psi\rangle \rightarrow |0\rangle$ with P = $|\alpha_0|^2$
- Second measurement: $|0\rangle \rightarrow |0\rangle$ with P = 1
- Third measurement: $|0\rangle \rightarrow |0\rangle$ with P = 1
- …

The phasors are unique, but the representation is not





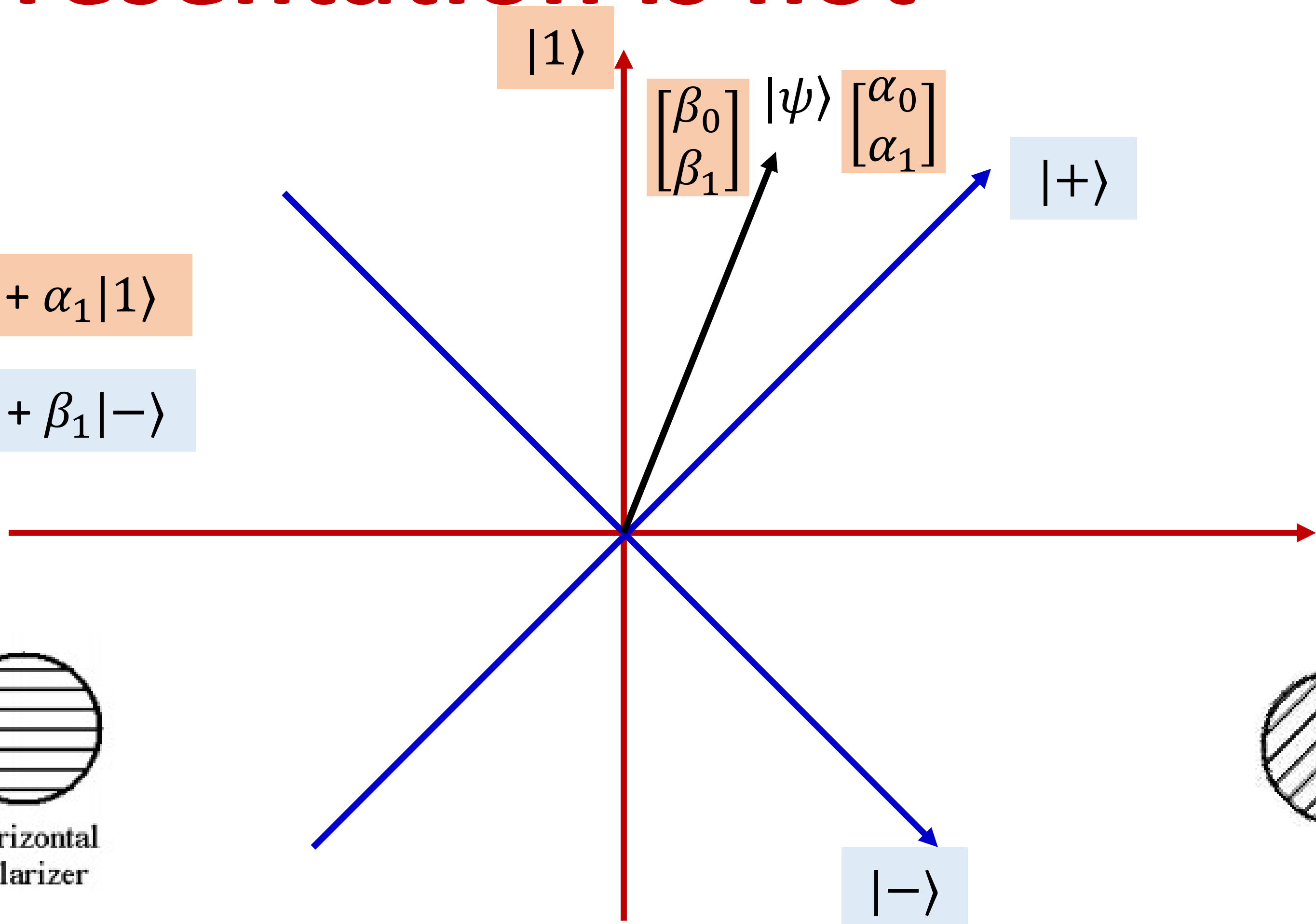


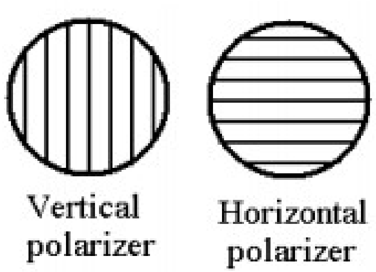
- No absolute definition of direction or sign
  - But the state of the system is well defined!
  - The space is defined, and the direction of the (physical) phasor is well defined
- The actual representation depends on the bases used
  - Only restriction: the bases must be orthogonal

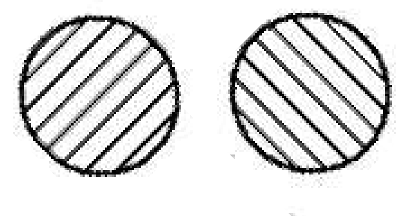
The phasors are unique, the representation is not

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

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





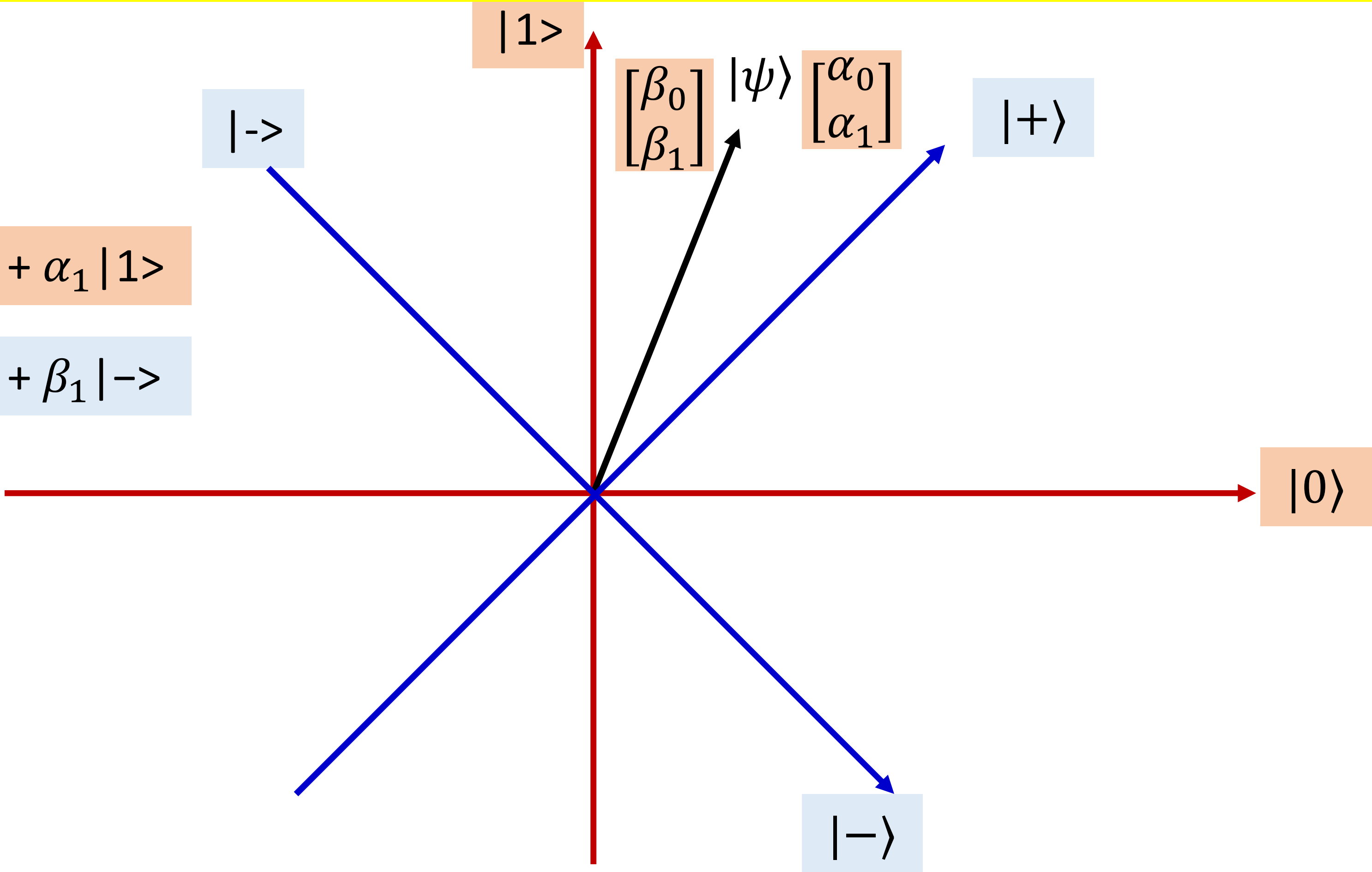


- The representation depends on the bases
  - Think orientation of your polarized glasses..

The space of phasors is a complex Hilbert space. A qubit 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

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

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



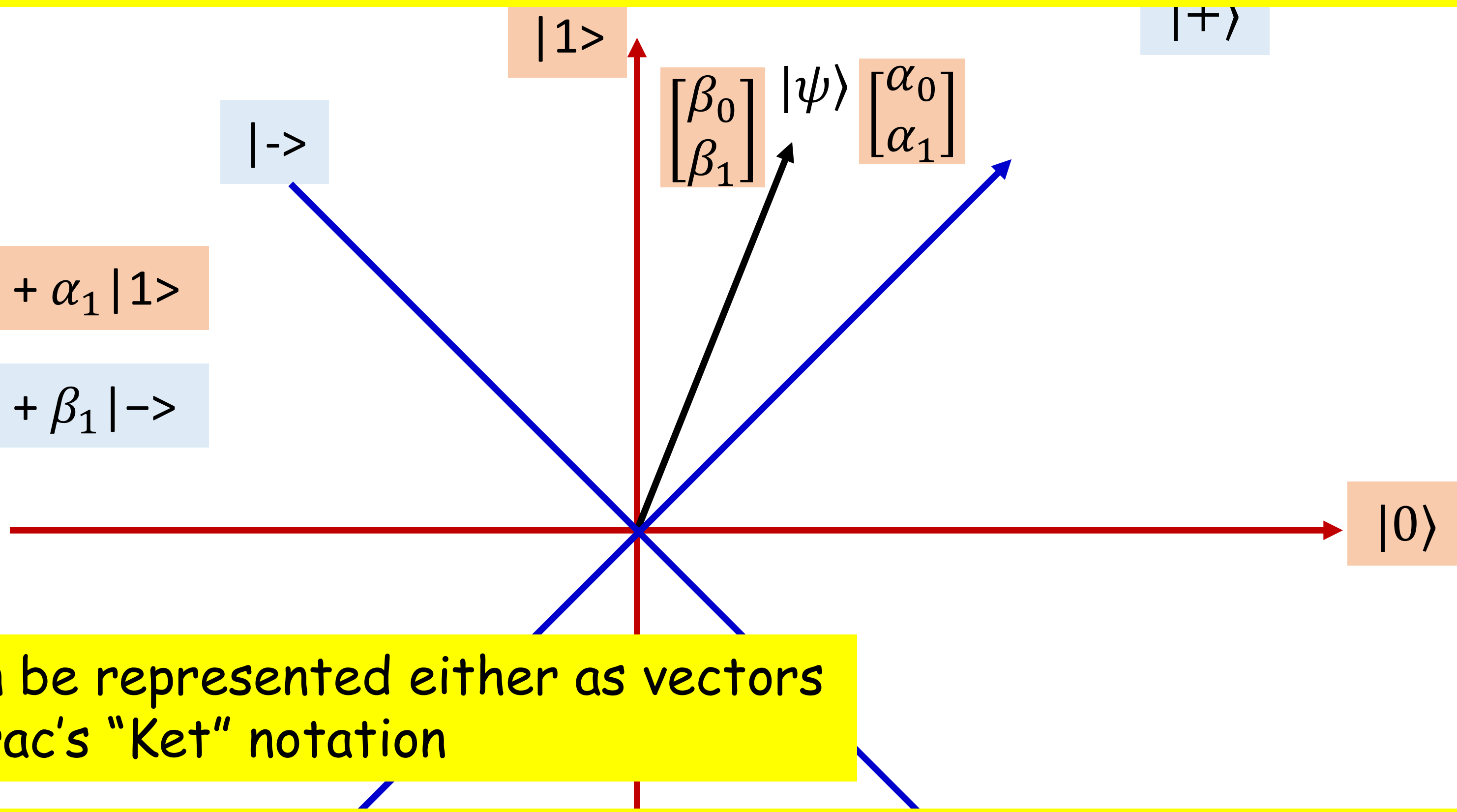
- The representation depends on the bases
  - Think orientation of your polarized glasses..

The space of phasors is a complex Hilbert space. A qubit 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

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

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



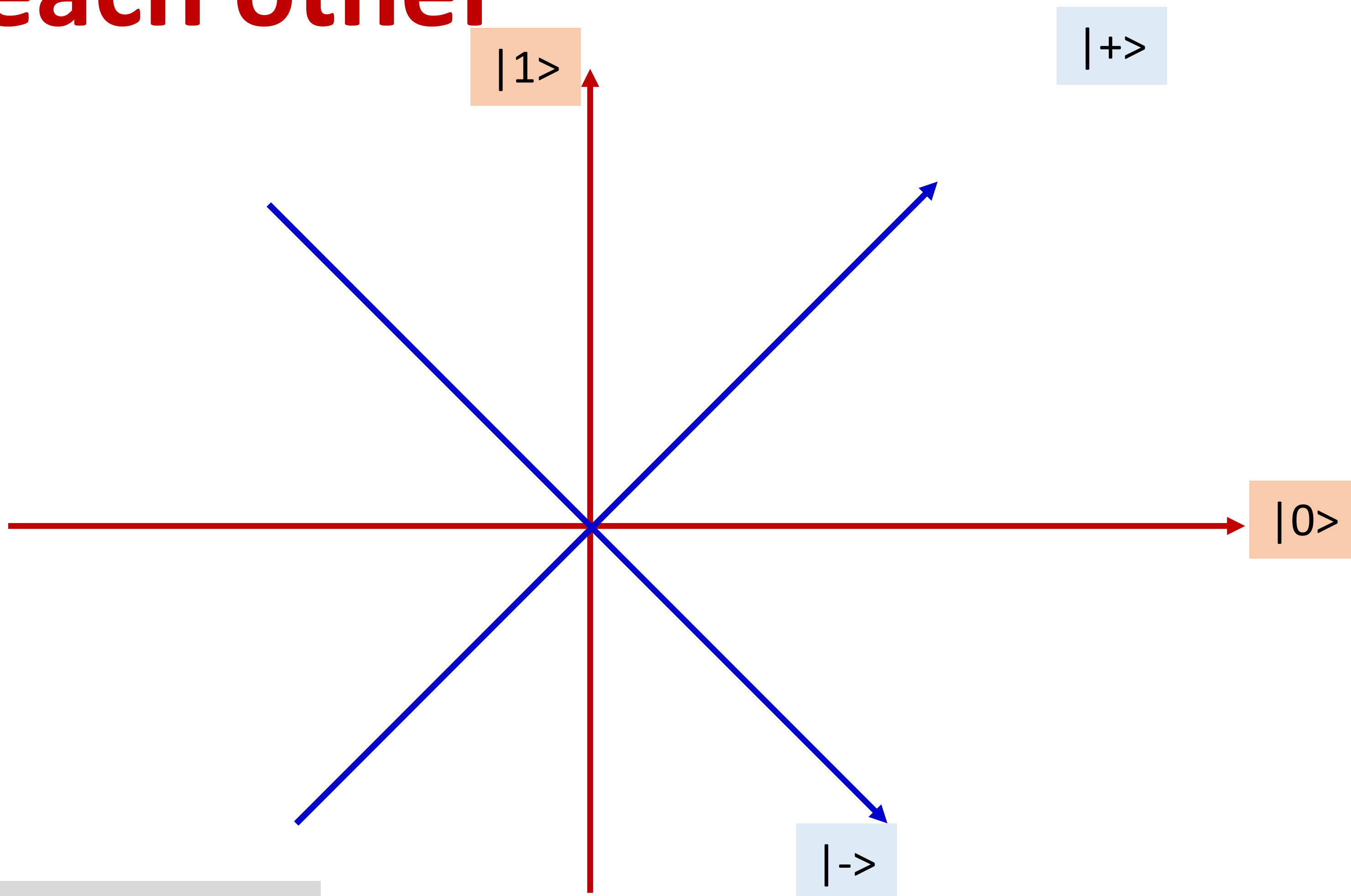
Phasors can be represented either as vectors or using Dirac's "Ket" notation

A Ket representation represents the underlying reality and is independent of bases

The *vector* representation depends on the bases

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

Bases can be expressed in terms of each other



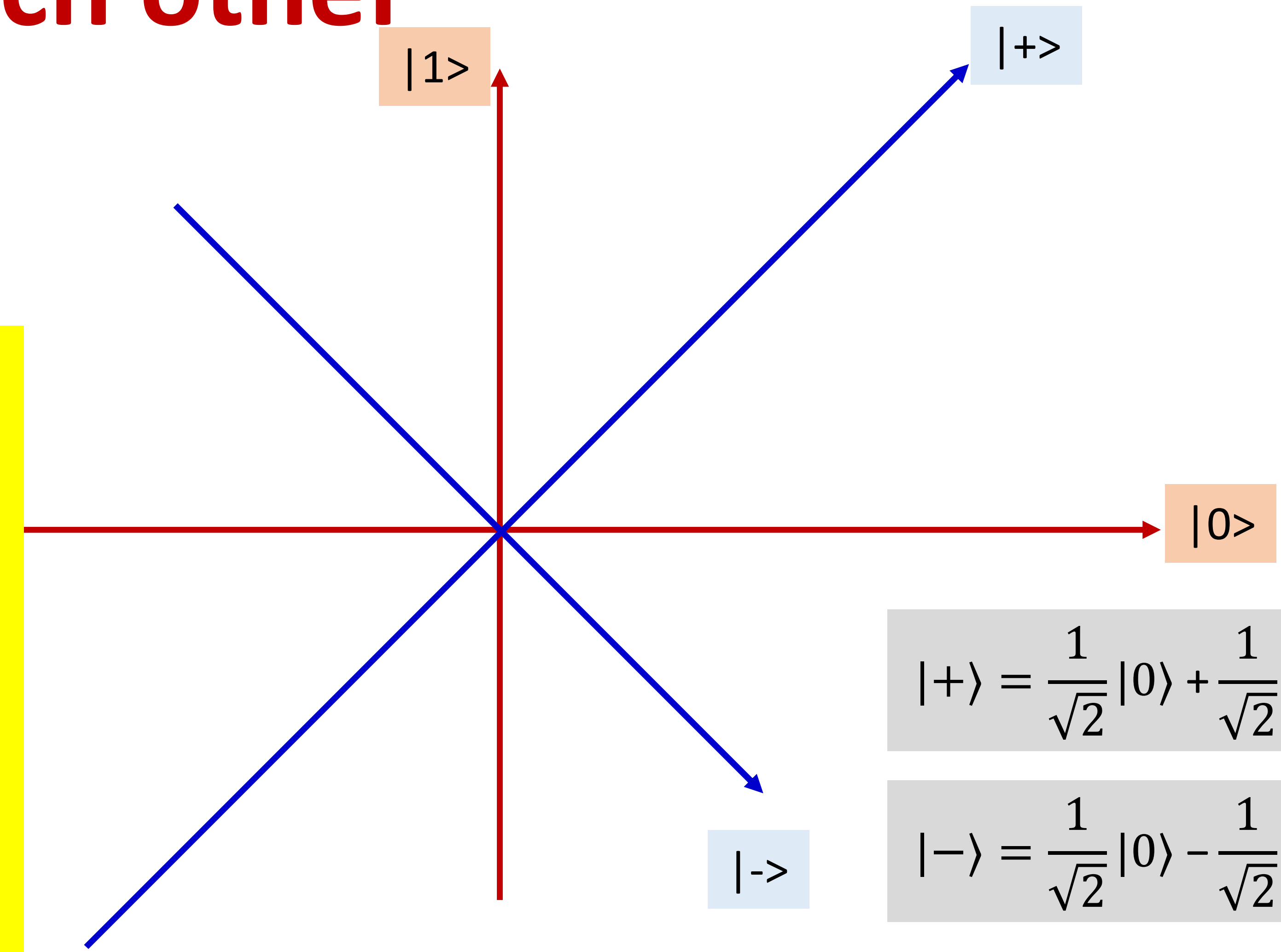
$$|+\rangle = \frac{1}{\sqrt{2}}|0> + \frac{1}{\sqrt{2}}|1>$$

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

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

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

Bases can be expressed in terms of each other



In bit bases:

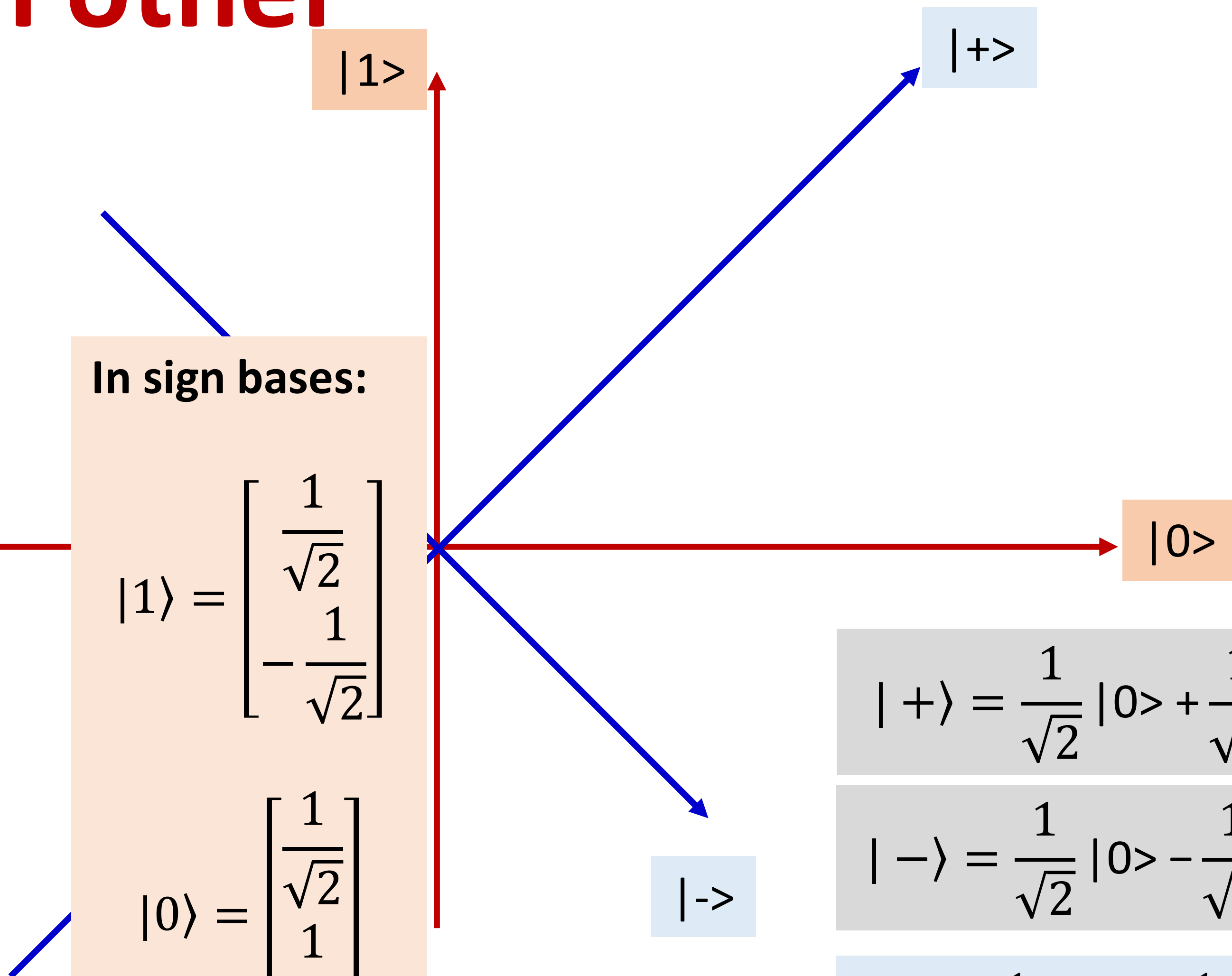
$$|+\rangle = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix}$$

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

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

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

Bases can be expressed in terms of each other



In bit bases:

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

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

In sign bases:

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

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

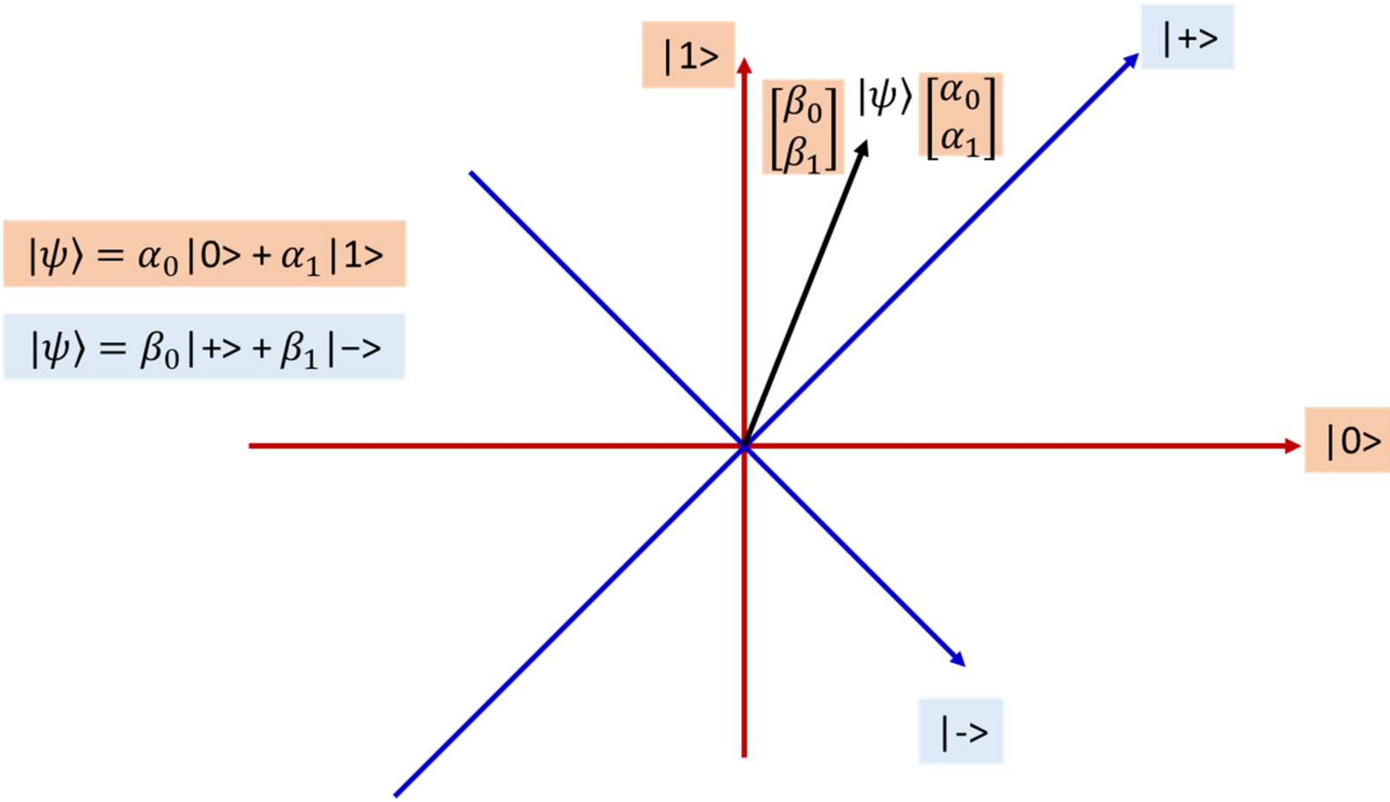
$$|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

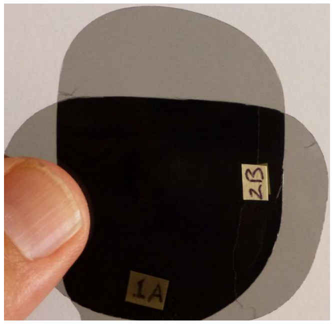
$$|-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$$

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

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

You can *measure* using either bases!!



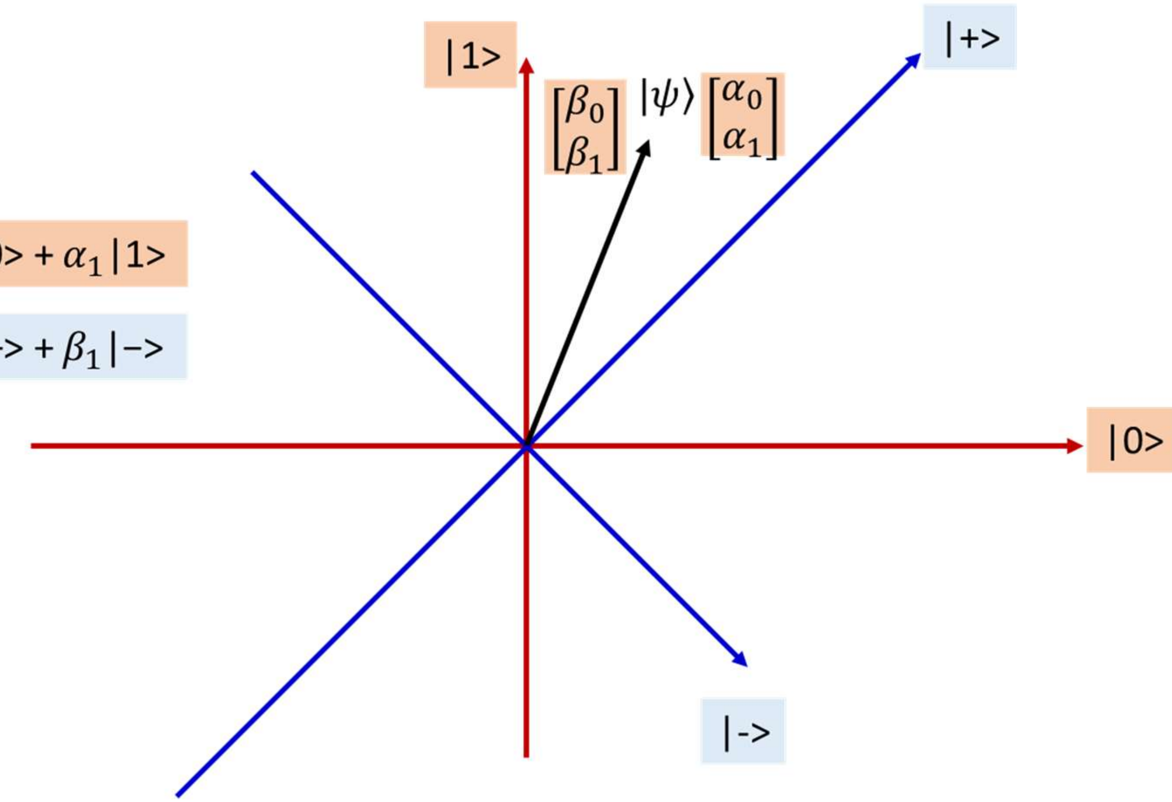


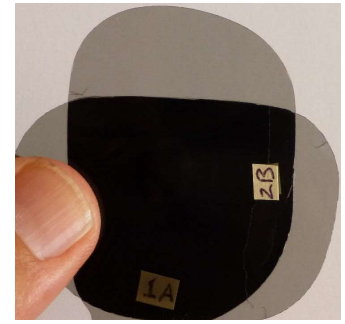
- What are P(|0>) andP(|1>)?
- What are P(|+>) andP(|−>)?

You can *measure* using either bases!!

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

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





- 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?

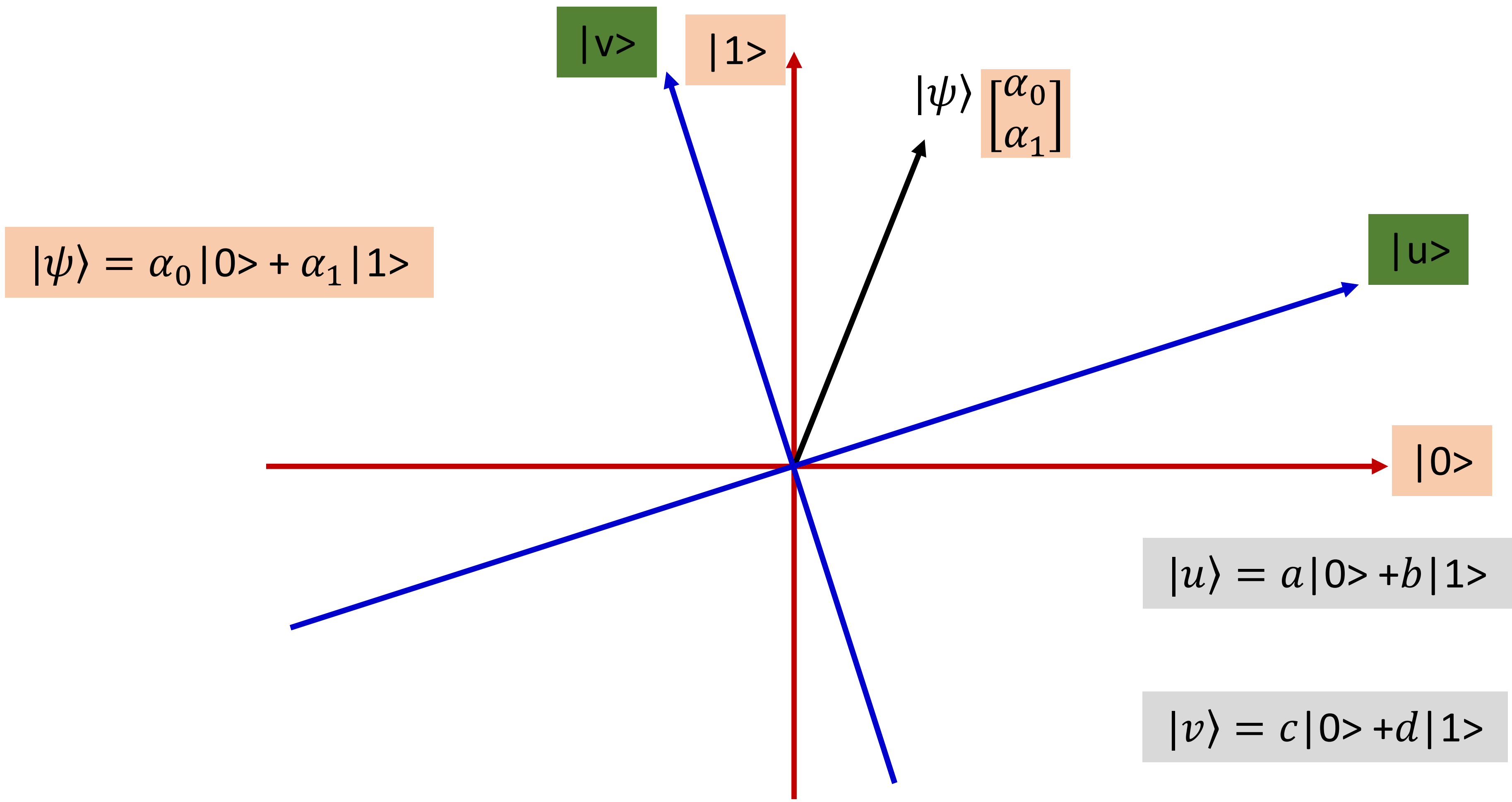
Some basic math

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

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

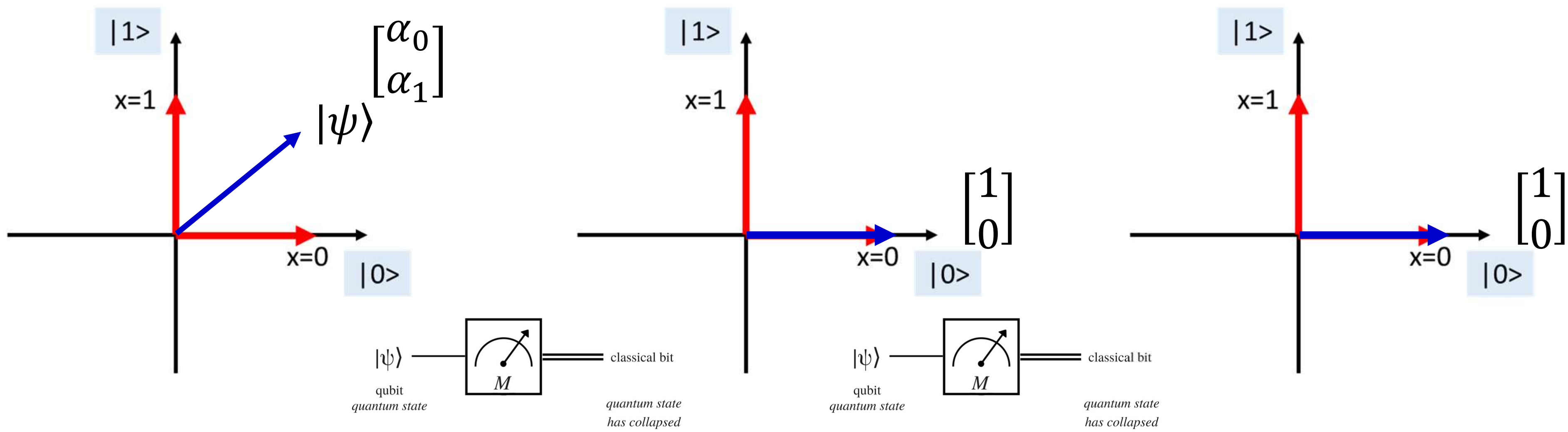
- For unit vectors it is the cosine of the angle between them
- For any basis, the probability of measuring that basis is the square of the cosine between the phasor and the basis

A different basis…



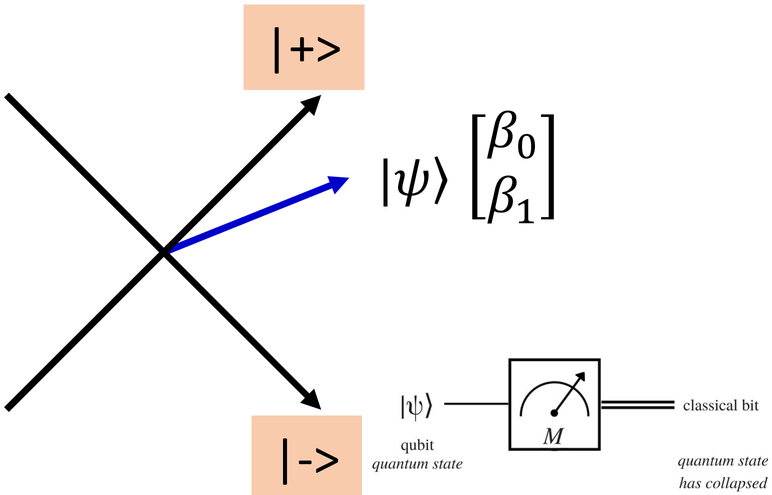
- What would P(|u>) and P(|v>) be?

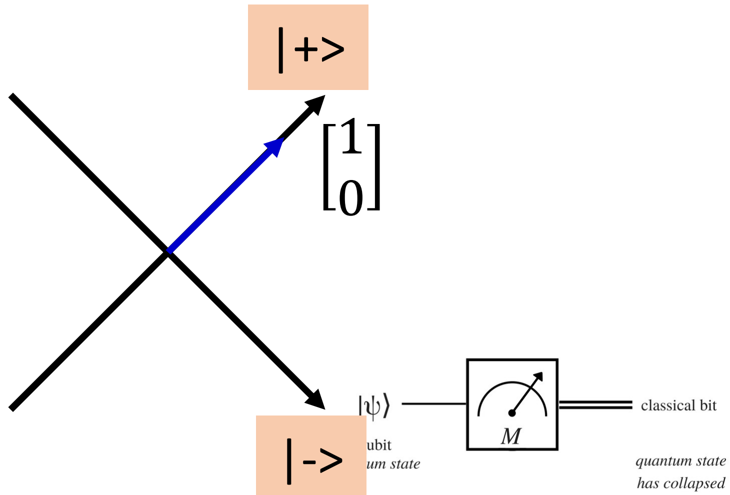
Measurement *simplifies* life

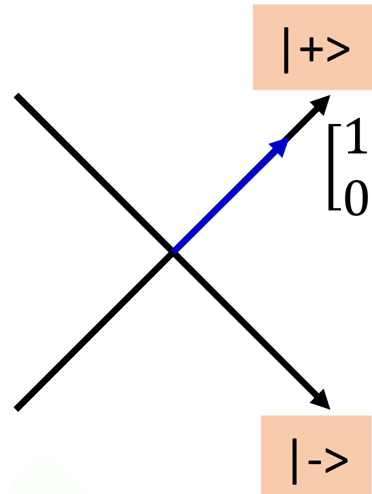


- By fixing the value

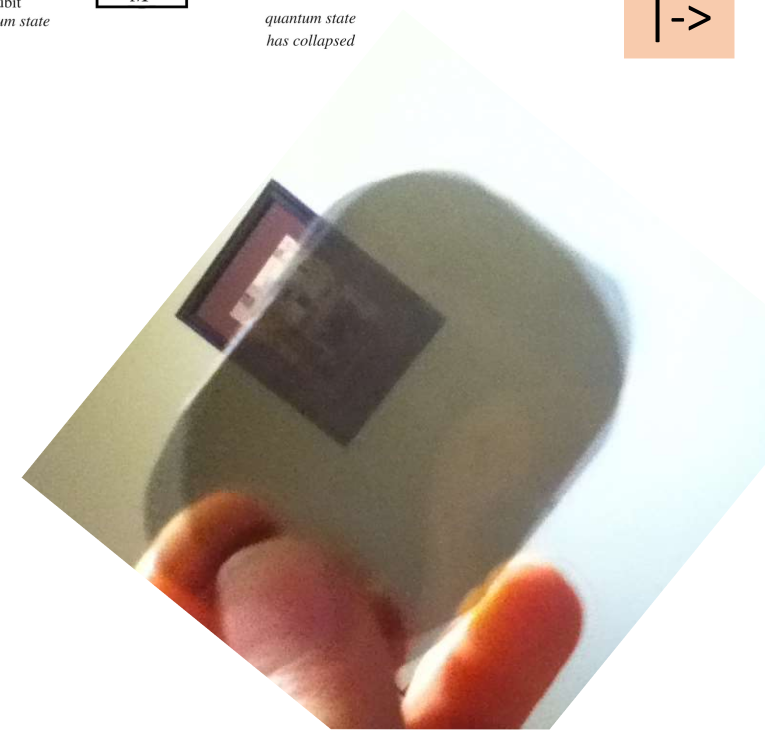
Measurement *simplifies* life



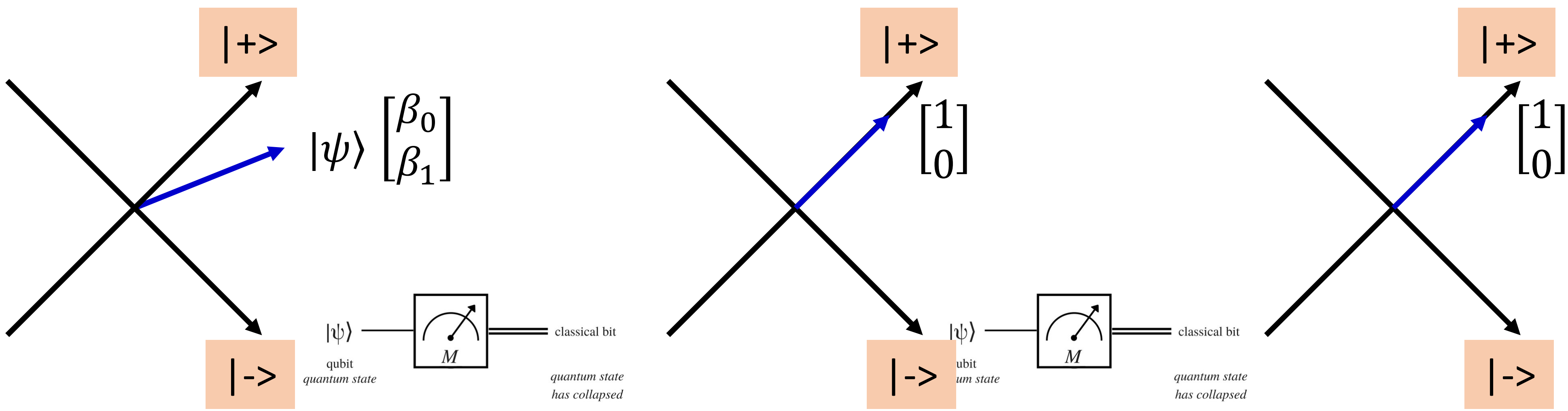




- By fixing the value



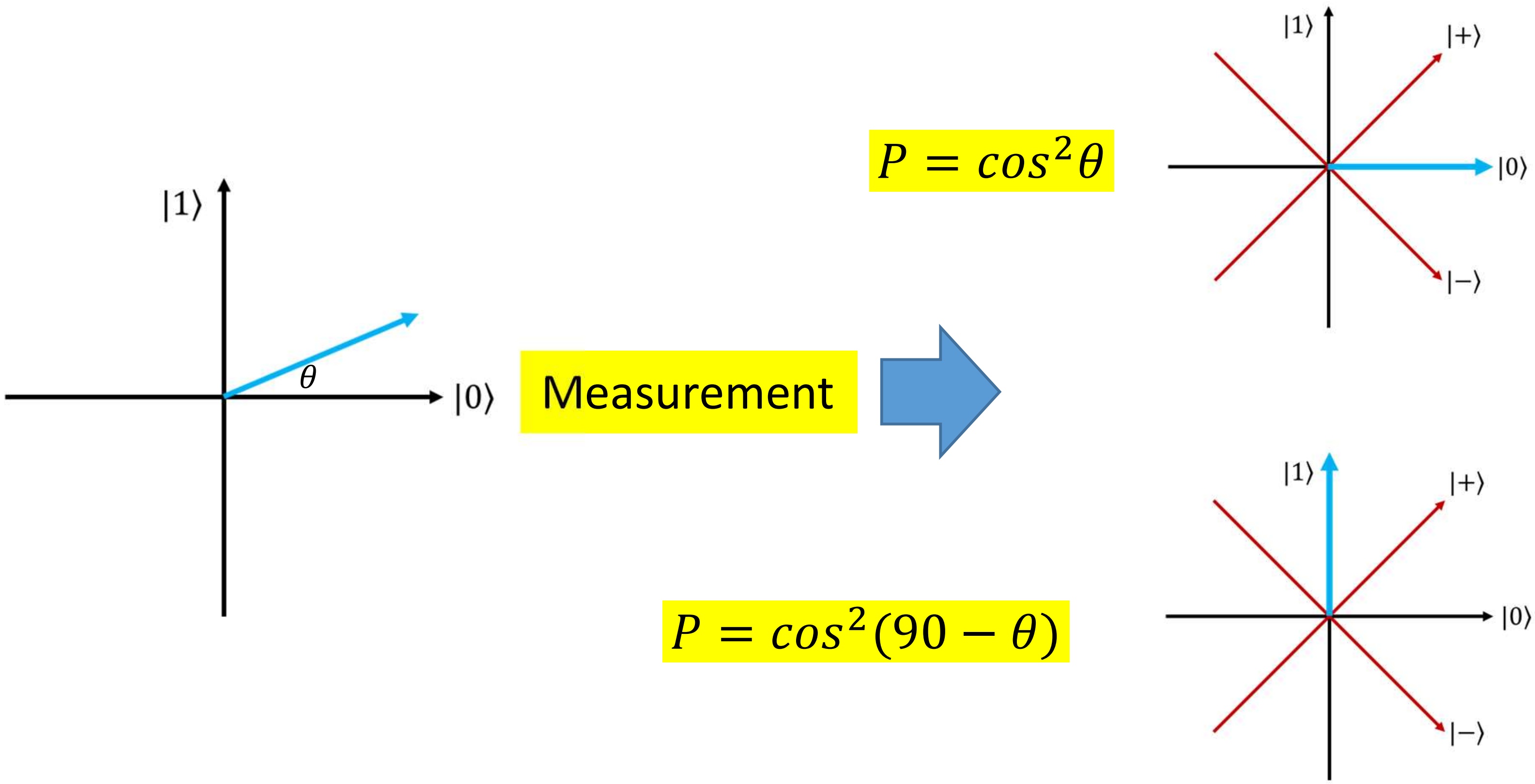
Measurement *simplifies* life



- By fixing the value

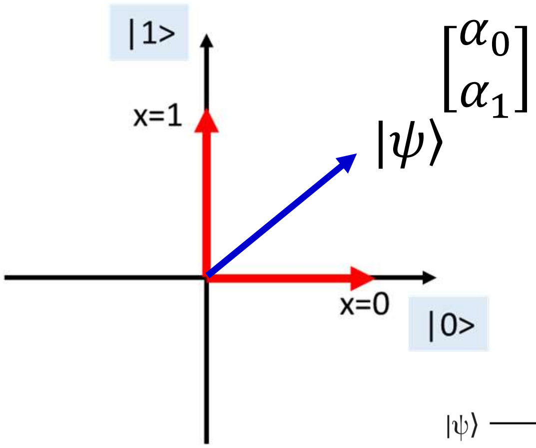
- Or does it?

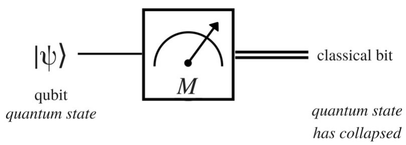
Measurement is not absolute



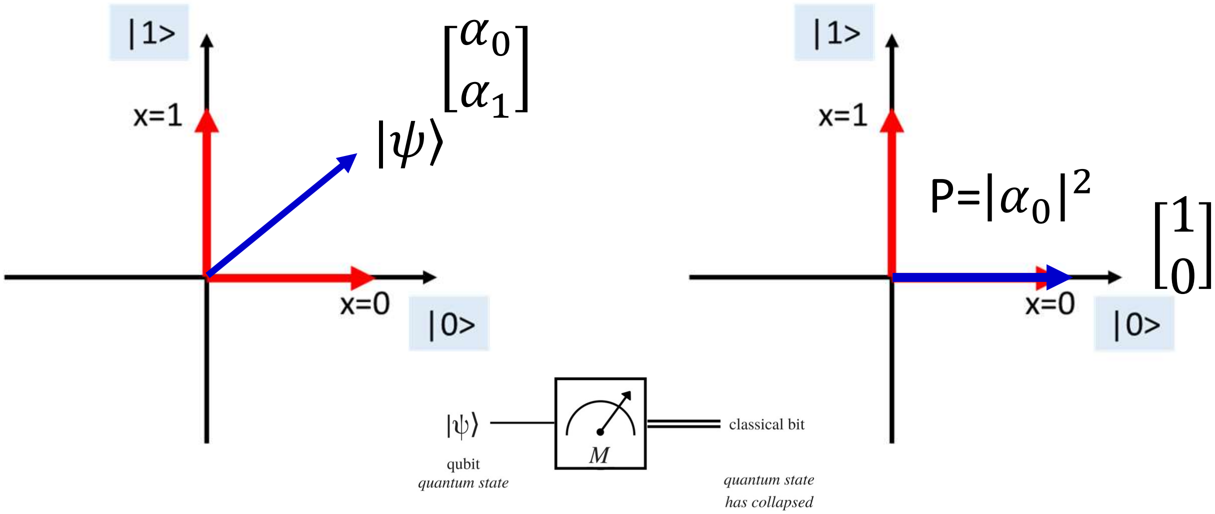
- Collapsing the vector according to one basis can still keep it indeterminate for other bases!
  - We will use this feature

Measurement *simplifies* life

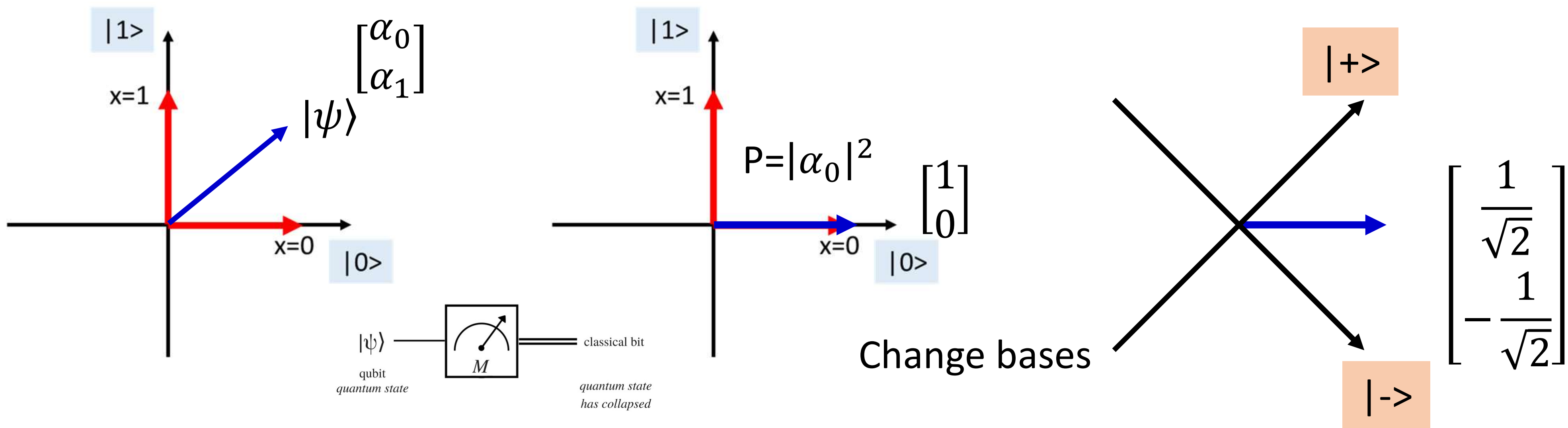




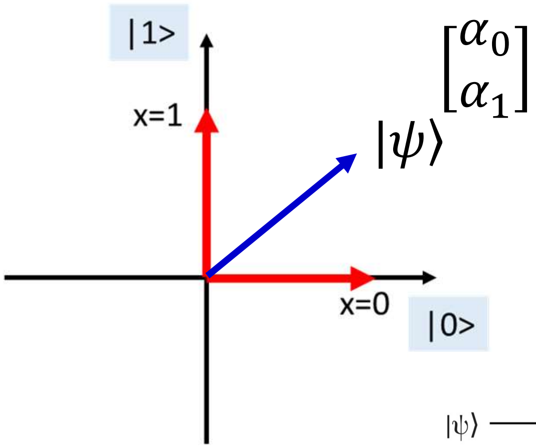
Measurement *simplifies* life

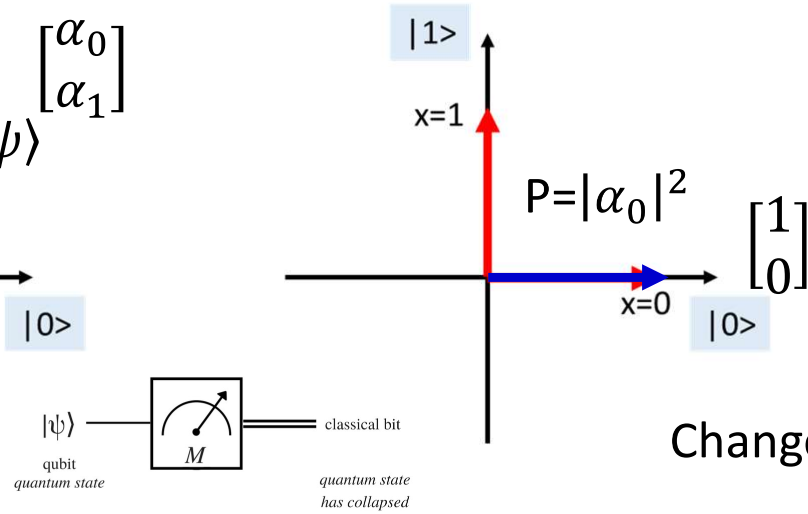


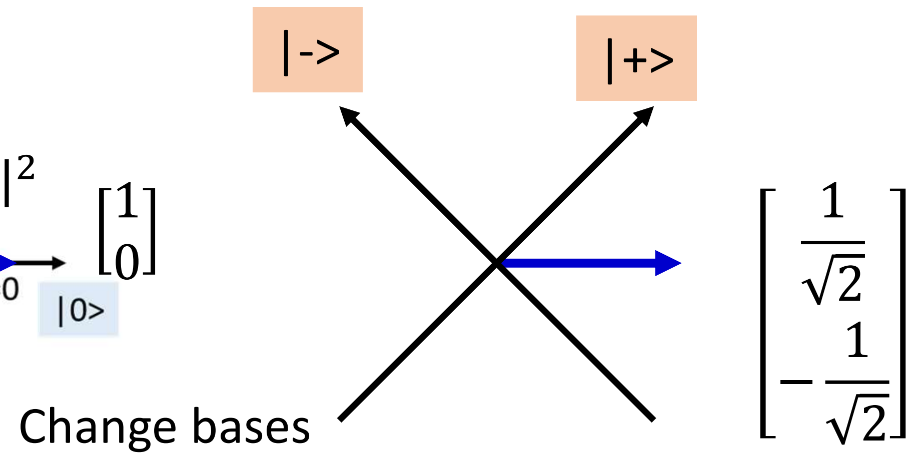
Measurement *simplifies* life

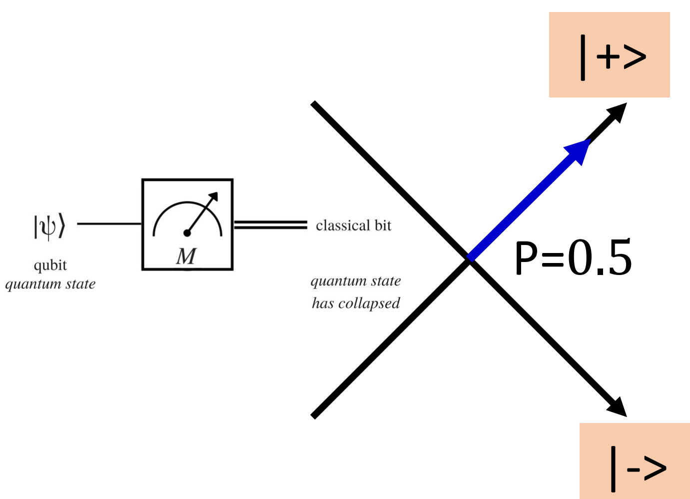


Measurement *simplifies* life

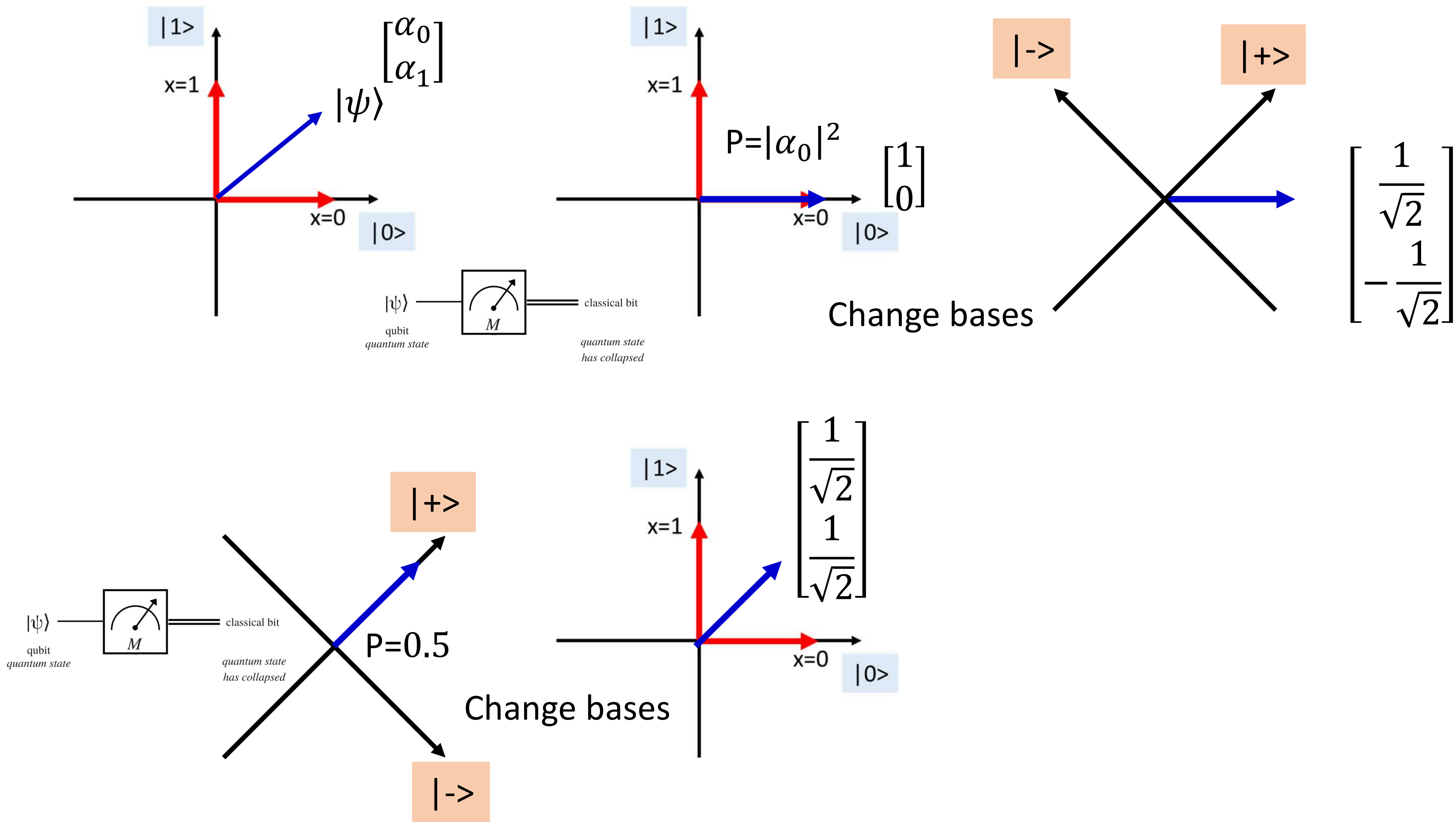




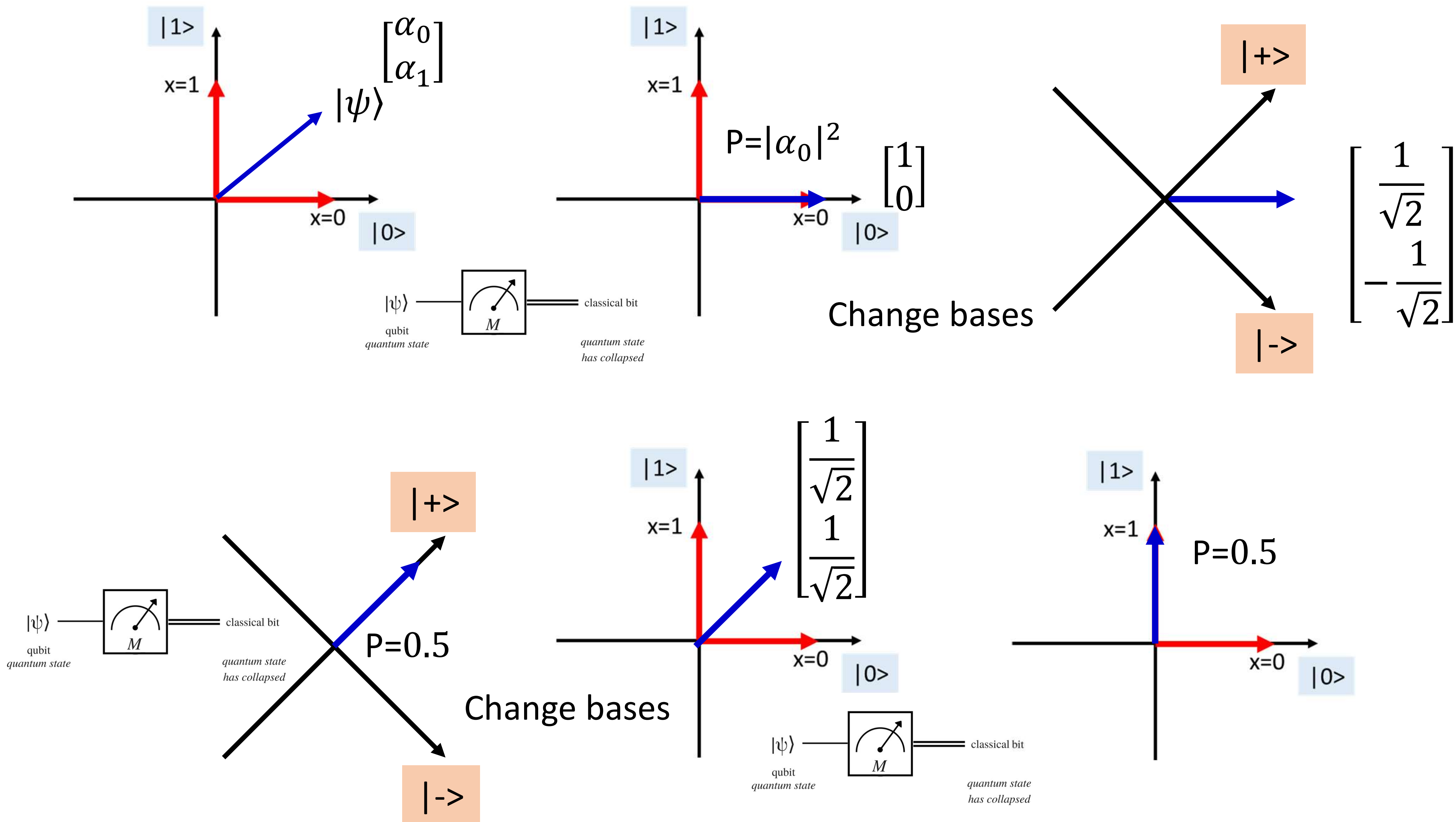




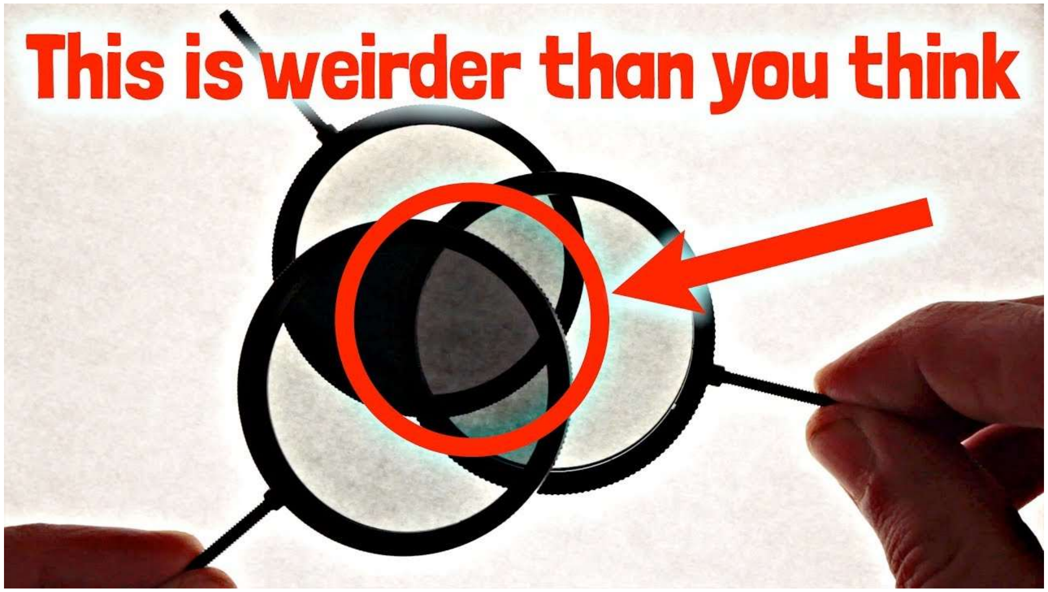
Measurement *simplifies* life



Measurement *simplifies* life

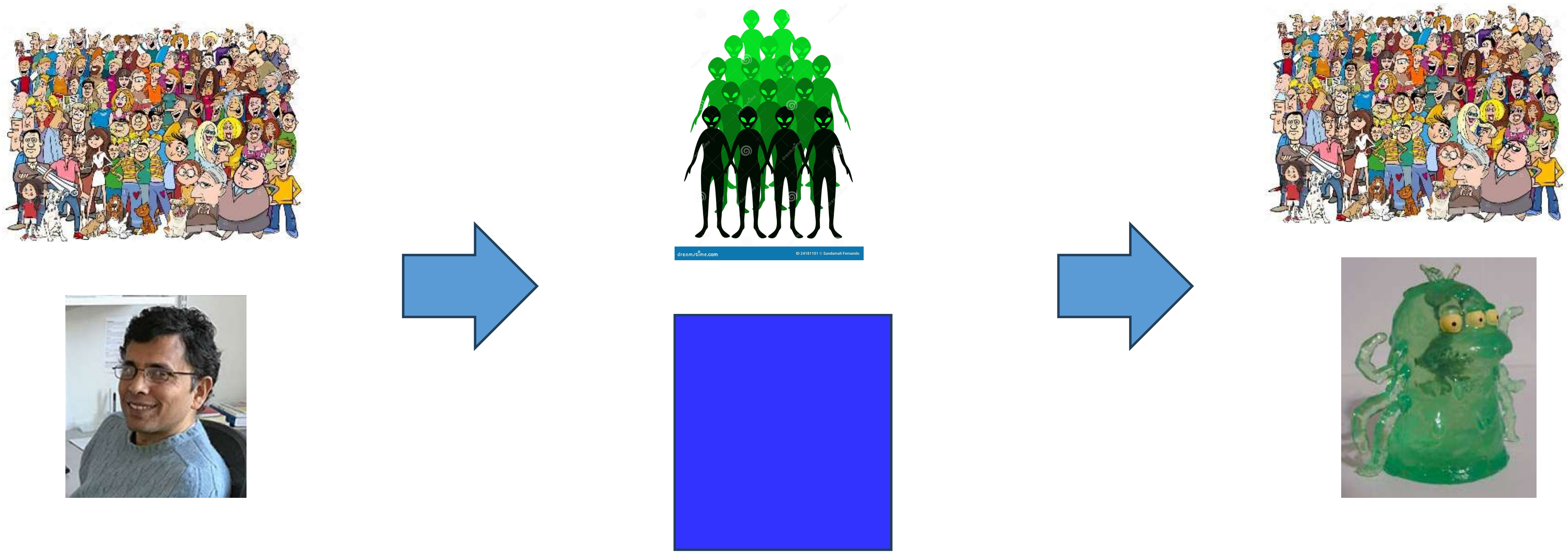


The world isn't what you think it is!!!



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

And so…



Quiz 3

- A qubit |0> is measured using the sign bases. What is the probability that the measured value is |+>?

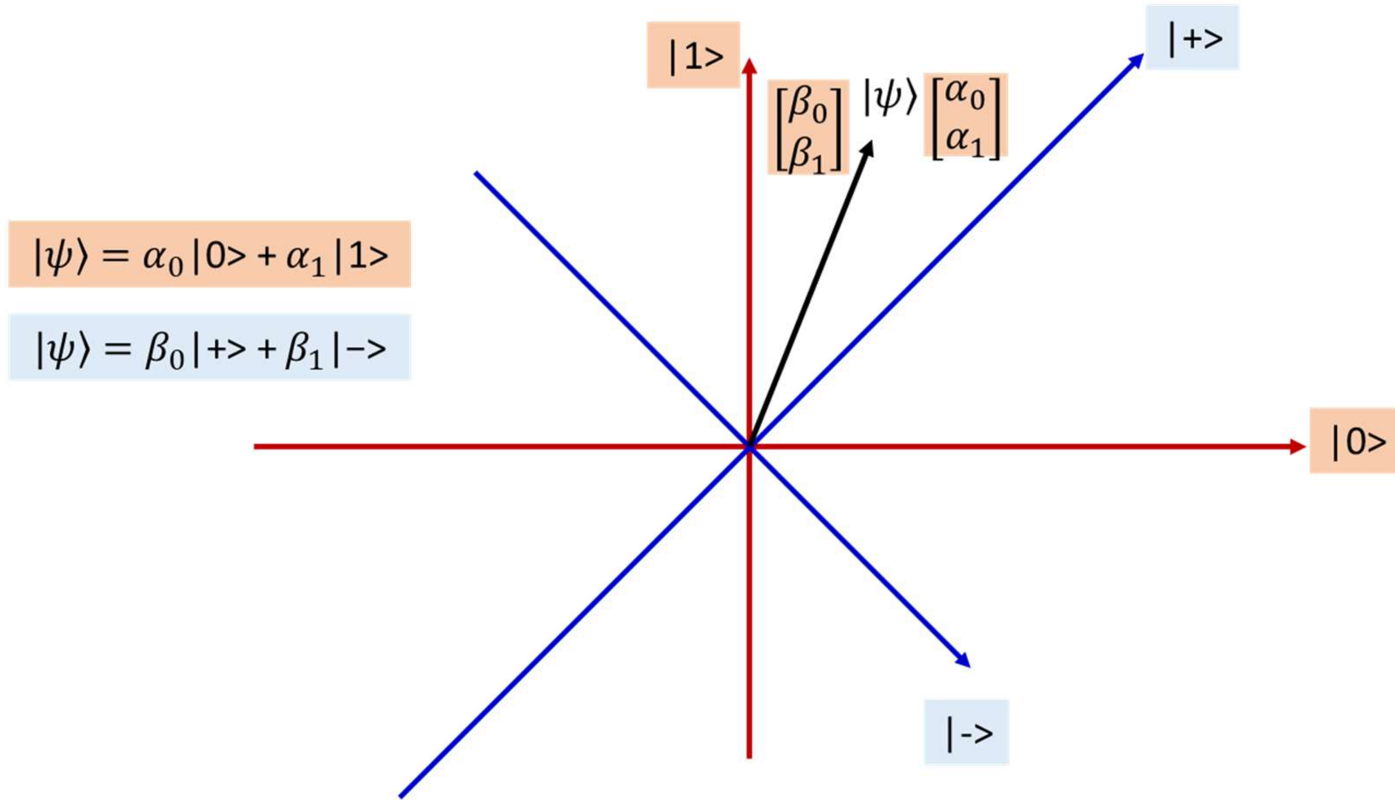
- The measured output is remeasured using the bit bases. What is the probability that the measured value is |0>?

Quiz 3

- A qubit |0> is measured using the sign bases. What is the probability that the measured value is |+>?
  - **0.5**

- The measured output is remeasured using the bit bases. What is the probability that the measured value is |0>?
  - **0.5**

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 $|\psi\rangle = |-\rangle$

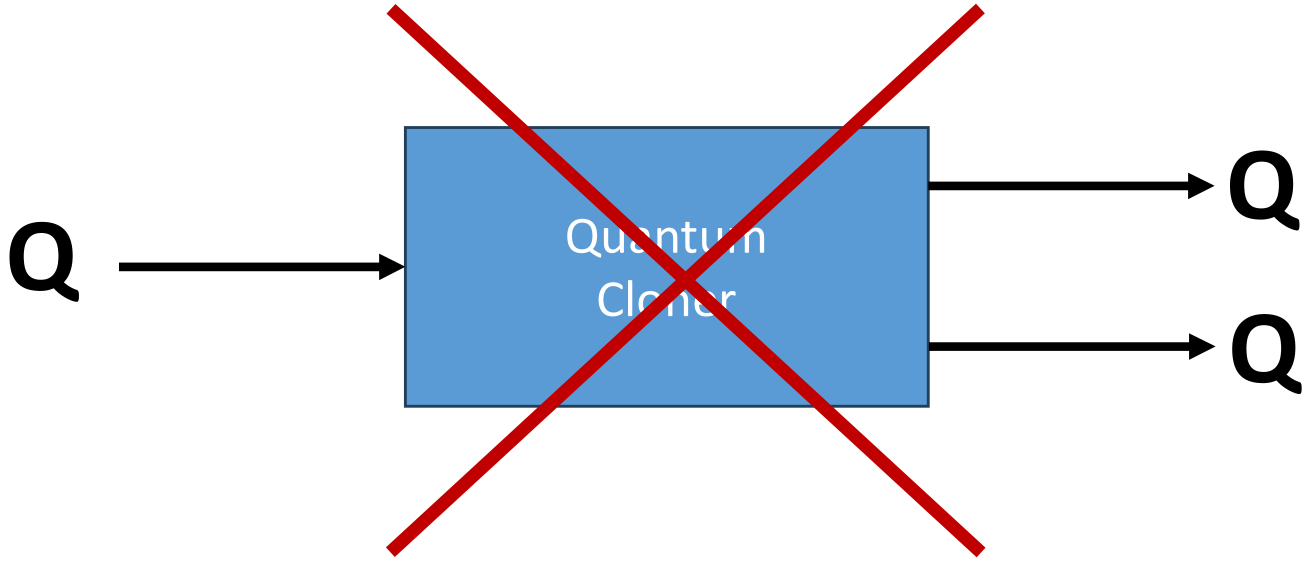
Heisenberg's uncertainty principle

- 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 $\sqrt{2}$

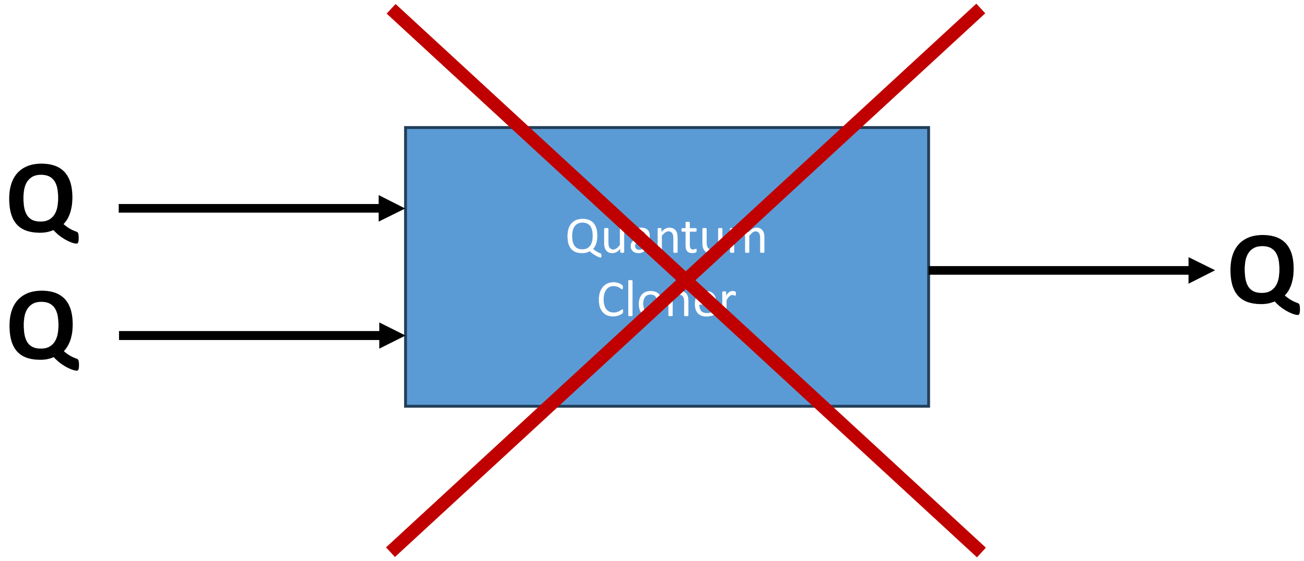
- More generally $spread(bit)spread(sign) \geq \sqrt{2}$

No Cloning Theorem



- A Qubit can never be cloned!
  - A system cannot take in one qubit and output two copies of the same qubit
  - Why?

No Destruction Theorem



- A Qubit can never be destroyed!
  - A system cannot take in N qubits and output N-1 qubits
  - Why?

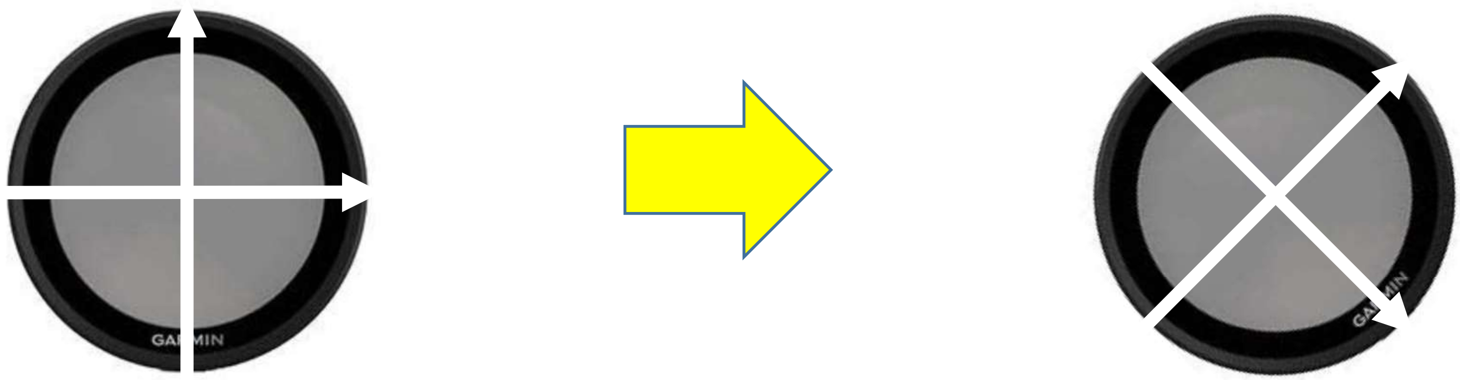
A digression: How do we measure with different bases?

- 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

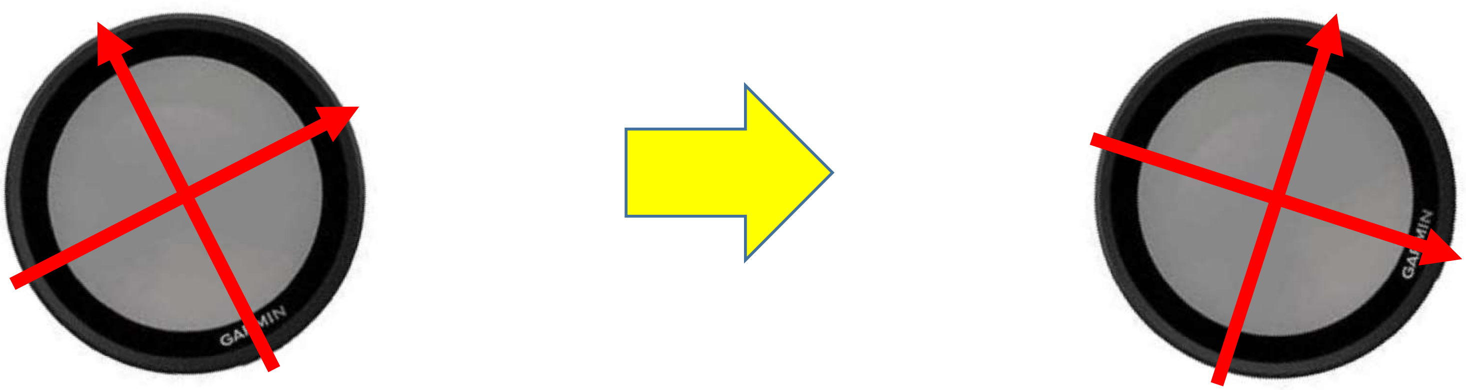
- Keep in mind that there is no “absolute” basis
  - There’s no “absolute bit basis” and no “absolute sign basis”
  - The bit and sign bases only differ from each other through their *relation* to one another
    - 45 degrees

- I.e. We can set the sign bases by first choosing a bit basis, and then choosing a sign basis at 45/-135 degrees
  - Or by first choosing a sign basis, and then a bit basis that’s at -45/135 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 45^{o} to the bit bases

So here's what we know about the qubit

- A 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 build something useful with this already**

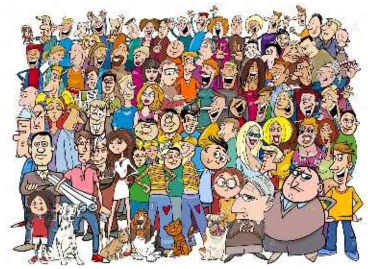
So here's what we know about the qubit

- A 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

Quantum Cryptography!!

- **Can we 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

Blarg blargity blarg

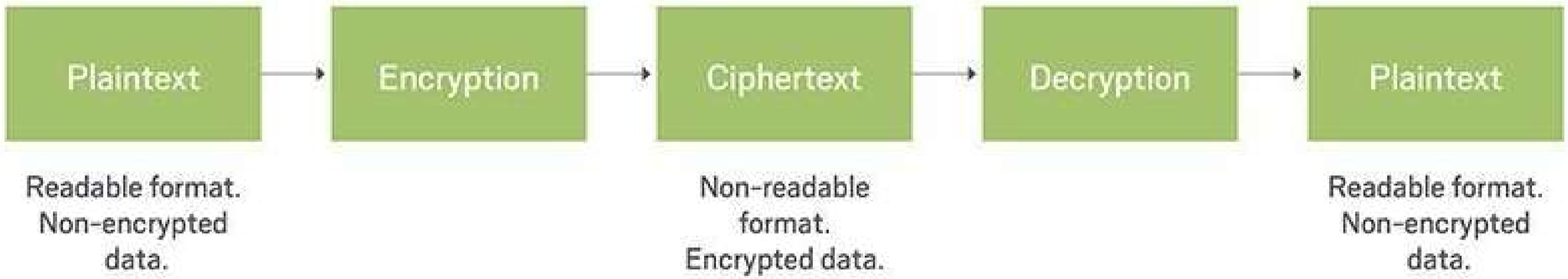
“Tweedledum”

“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 it’s saying
  - Only Bob can de-garble the message because he knows the formula

Cryptography

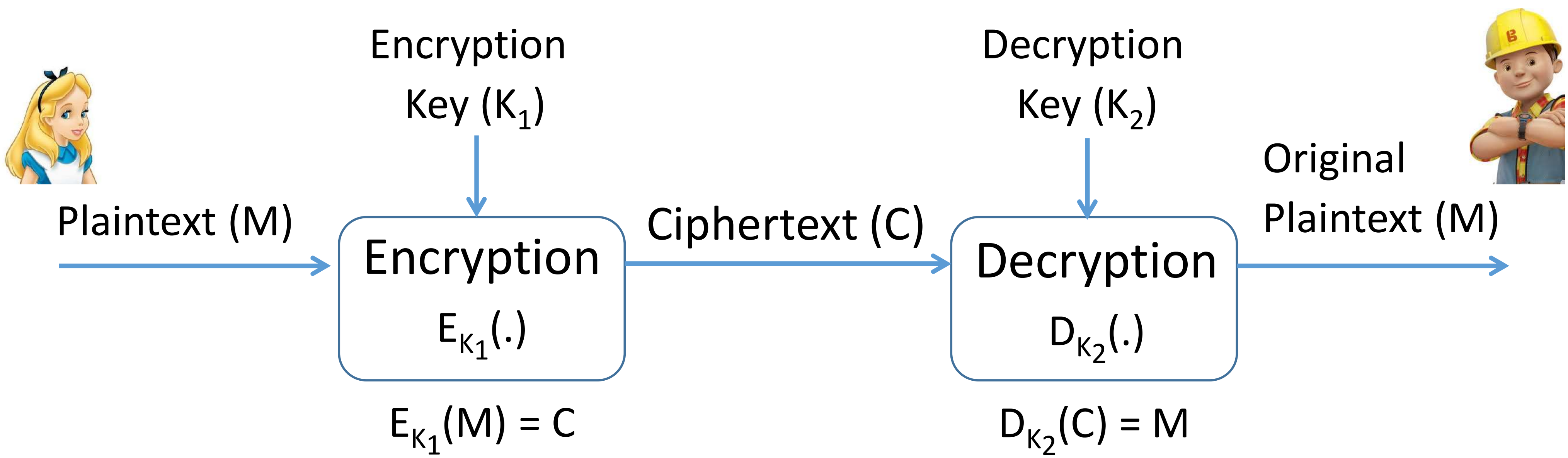
$$cipher = Enc(msg, key) \qquad msg = Dec(cipher, key)$$



- 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

Encryption Key (K_1)

Decryption Key (K_2)

Plaintext (M) → Encryption $E_{K_1}(.)$ → Ciphertext (C) → Decryption $D_{K_2}(.)$ → Original Plaintext (M)

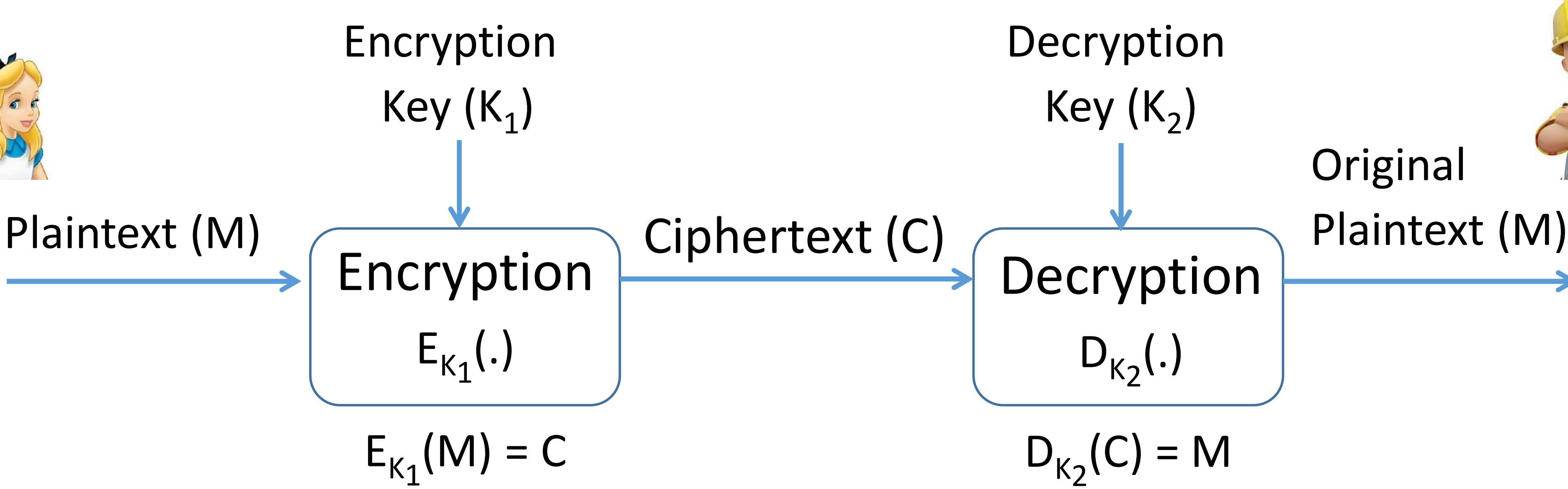
$E_{K_1}(M) = C$

$D_{K_2}(C) = M$

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* …