Thurs Jan 26

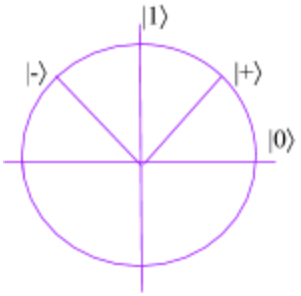
We call the matrix $R_{\pi/4} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$ the $\sqrt{NOT}$ gate, as $R_{\pi/4}^2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ aka the NOT Gate.

The **Hadamard Gate** is $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

It's useful because it represents a mapping between the $|0\rangle,|1\rangle$ basis to the $|+\rangle,|-\rangle$ basis.

$H|0\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \sqrt{2} \\ \sqrt{2} \end{pmatrix} = |+\rangle$ Similarly $H|+\rangle = |0\rangle$, $H|1\rangle = |-\rangle$, and $H|-\rangle = |1\rangle$

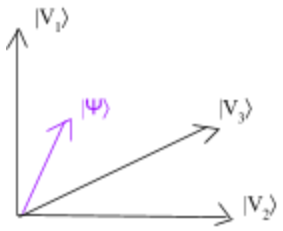
Note that we've got two orthogonal (complementary) basis: being maximally certain in the $|+\rangle,|-\rangle$ basis means that you're maximally uncertain in the $|0\rangle,|1\rangle$ basis and vice versa.



Why would we want to use 2 different bases?

We like to think of vectors existing abstractly in vector space, but to use it meaningfully, we've got to get it to a basis. We're not really going to get a satisfactory answer until we start talking about quantum protocols.

Side note, when talking about the Born Rule, we've been using a special case for one particular basis for simplicity.



We can think about measurement more generally. Measuring in the orthonormal basis $\{|V_1\rangle,...,|V_N\rangle\}$, you'll get the outcome $|V_i\rangle$ with probability $|\langle V_i|\Psi\rangle|^2$.

So the probability of the outcome $|V_3\rangle$ is the projection onto the basis vector.

$|\langle V_i|\Psi\rangle|^2 = |\alpha_1|^2$

We use bases $|0\rangle$ and $|1\rangle$ arbitrarily as a nice convention.

To do operations in a different basis use unitary transformations to convert.

So for $\{|V_1\rangle,...,|V_N\rangle\}$ use $U|V_1\rangle = |1\rangle,...,U|V_N\rangle = |N\rangle$ to use the basis $\{|1\rangle,...,|N\rangle\}$

There's an extreme point of view in quantum mechanics that unitary transformations are the only thing that really exist, and measurements don't really exist. And the converse also exists: the view that measurements are the only thing that really exist, and that unitary transformations don't.

Unitary Transformations are :

- *Invertible*. This should be clear, since preserving the two norm means that $U^\dagger U = 1$ which means $U^\dagger = U^{-1}$.
    - Reversible. The transformation $|\Psi\rangle \rightarrow U|\Psi\rangle$ can be reversed with $U^{-1}U|\Psi\rangle = |\Psi\rangle$.

Interestingly this implies that unitary evolution can never destroy information, which should

imply that the universe is reversible. We've known that the microscopic laws of physics are reversible since galileo times (i.e. observing a falling object backwards follows gravity backwards). So for example burning a book shouldn't necessarily destroy the information within, as physics says that you can get all the information from the smoke and ash left over.

- *Deterministic*
- *Continuous*
  i.e. you can always apply them in a time-continuous way. That's why it's important that unitary matrices are complex. If the transformation $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ took place in 1 sec. $\begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$ took place over the first half of the second.

By the way, there is a 3x3 matrix that squares to $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$.

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & 0 \end{pmatrix}^2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$$

Which means that you could apply $\begin{pmatrix} \alpha \\ \beta \end{pmatrix}$ on $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ by using $\begin{pmatrix} \alpha \\ 0 \end{pmatrix}$ on it. without ever needing complex numbers! That's because using complex numbers works in the same way as adding a new dimension to your vector. Just like you could reflect your three-dimensional self by rotating yourself in the fourth dimension.

Important: Never eat anything in the fourth-dimension. It'll mess with the chirality of your molecules.

Measurements break all three rules of unitary transformations. They are:

- *Irreversible*
  - Whatever information about qubit you didn't capture is now lost.
- *Probabilistic*
  - Everything in quantum mechanics is deterministic *until* measurement (or information leaves the system).
- *Discontinuous*

So how can we reconcile these two sets of rules?

That's the **Measurement Problem**. We'll talk about points of view on it later.

Despite the philosophical conflict, unitary transformations and measurement sync up well because:

unitary transformations preserve the 2-norm and

Measurement gives probabilities given by the 2-norm

- We used to think everything was based on the 1-norm, until we found that quantum mechanics was based on the 2-norm. This got researchers looking for things based on the 3-norm, 4-norm, etc. They didn't really find anything though (the extra credit problem on the homework on norm preserving linear transformations sheds light on why).
  - Making quantum mechanics a bit of "an island in theory space". If you try to adjust anything about it in any way you get gunk. You could alternatively say that there's "nothing nice near quantum mechanics".

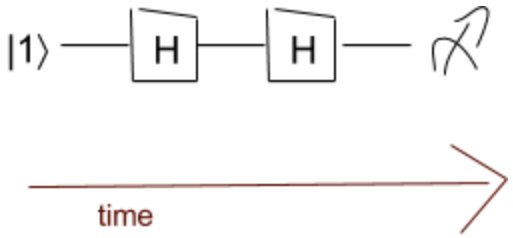
- There are many reasons why complex numbers work better than the reals or quaternions.

One more example of a linear transformation.

$\sum|\alpha_i|^4$

$$\text{for } \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ i & -i \end{pmatrix} \quad \text{maps } |0\rangle \to |i\rangle \quad \frac{|0\rangle + i|1\rangle}{\sqrt{2}}$$
$$\text{and } |1\rangle \to |-i\rangle \quad \frac{|0\rangle - i|1\rangle}{\sqrt{2}}$$

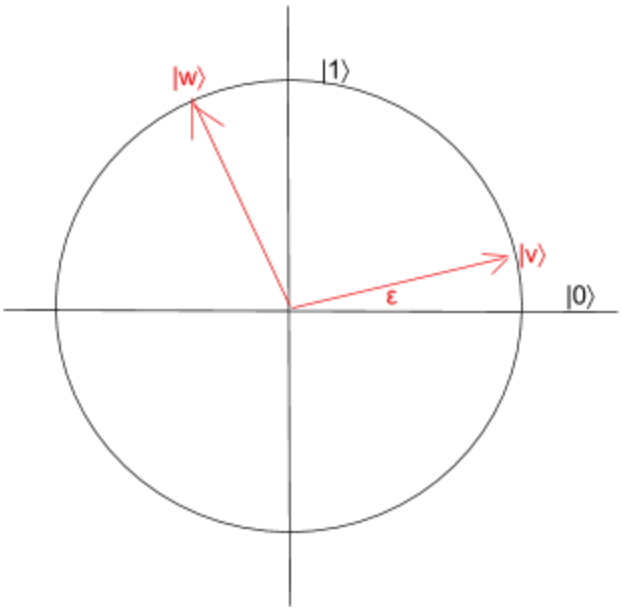
Quantum Circuit Notation keeps track of what qubits we have and the linear transformations we apply.



So to the left we start with $|1\rangle$, apply a Hadamard Gate, apply a Hadamard Gate, then measure (implied to be in the $|0\rangle$,$|1\rangle$ basis)

We'll never brach in a quantum circuits, since that can't correspond to a unitary transformation. To enlarge a system we can use a new $|0\rangle$ qubit, an **ancilla** qubit.

There are several interesting phenomena that already happen in the quantum mechanics of one qubit.



Suppose you have a qubit in the $|0\rangle$ state. We can know this because it's staying 0 over and over in measurements. Let's say we want to put it in the $|1\rangle$ state without using any unitary transformations.

For some small ε, we can measure the qubit on the ε basis. The probability of getting the qubit to move to ε increases as ε decreases.

$\text{Prob}(|v\rangle) = \text{KO}||v\rangle|^2 = \cos^2\varepsilon$

$|v\rangle = \cos\varepsilon|0\rangle + \sin\varepsilon|1\rangle$

Over ε measurements we could inch the qubit from $|0\rangle$ to $|1\rangle$.

$\text{Prob}(|w\rangle) = \sin^2\varepsilon \sim \varepsilon^2$

What's the likelihood that we'd get a measurement that *isn't* the one we want?

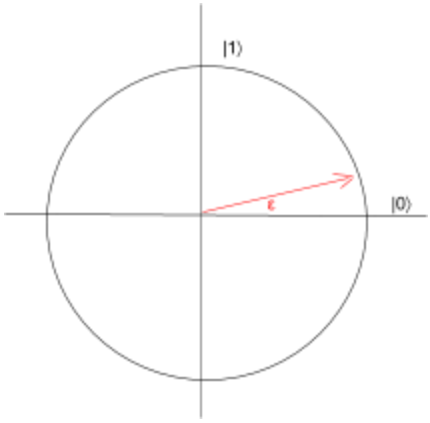
By union bound $1/\varepsilon * \varepsilon^2 = \varepsilon$

This is called **The Quantum Zeno Effect**

It was discovered by Alan Turing.

Perhaps a real world analog would be asking a stranger to marry you, getting coffee and then asking them to marry you, etc. You could refer to this situation as moving between bases for the 'yes'/'no' measurement.

Another interesting variant of the same kind of effect is as follows:

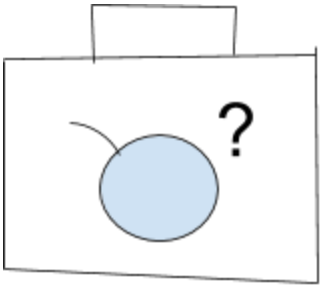


Say we want to keep a qubit at $|0\rangle$ but it keeps rotating towards $|1\rangle$ (it's *drifting*).

If we keep measuring it on the $|0\rangle$,$|1\rangle$ basis the odds of it rotating to $|1\rangle$ is ε^2.

This is called **The Watched Pot Effect.**

Another interesting phenomenon is the **Elitzur-Vaidman Bomb**.
A quantum effect discovered in the 1990's.



Say we're at a quantum airport and there's a piece of unattended luggage which could be a bomb, but opening the suitcase would trigger it.

How do we disarm the bomb without opening the suitcase?

We could make a query with a classical bit:

$b \in$ {0 (don't make query), 1 (make query)}

But we only either find nothing or blow up the bomb. Not good!

Instead, we can upgrade to a qubit:

$|b\rangle = \alpha|0\rangle + \beta|1\rangle$

Now: If there's no bomb $|b\rangle$ gets returned to you.
If there is a bomb [$|0\rangle$ returns $|0\rangle$] and [$|1\rangle$ explodes it].

$$\begin{pmatrix} \cos\varepsilon & -\sin\varepsilon \\ \sin\varepsilon & \cos\varepsilon \end{pmatrix}$$

What we can do is apply the rotation R_ε = (sinε cosε). Giving us:

$\cos\varepsilon|0\rangle + \sin\varepsilon|1\rangle$

If there's a bomb, the probability it explodes is $\sin^2\varepsilon \sim \varepsilon^2$, otherwise you get $|0\rangle$

If there's no bomb, $\cos\varepsilon|0\rangle + \sin\varepsilon|1\rangle$

So repeating about $\pi/2$ times makes the probability of setting off the bomb as $1/\varepsilon * \varepsilon^2 = \varepsilon$