Lecture 4: Thurs Jan 26: Quantum Gates and Circuits, Zeno Effect, Elitzur-Vaidman Bomb

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

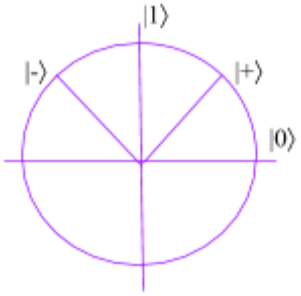
The **Hadamard Gate** is $H = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$

Hadamard is ubiquitous in quantum information because it maps the $|0\rangle,|1\rangle$ basis to the $|+\rangle,|-\rangle$ basis.

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

Similarly $H|+\rangle = |0\rangle$, $H|1\rangle = |-\rangle$, and $H|-\rangle = |1\rangle$

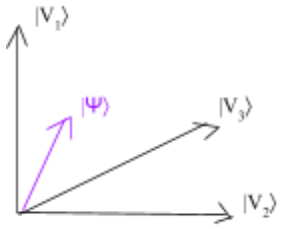
Note that we've got two orthogonal (complementary) bases: being maximally certain in the $|+\rangle,|-\rangle$ basis means that you're maximally uncertain in the $|0\rangle,|1\rangle$ basis and vice versa.



Why would we want to use 2 different bases?

We like to think of vectors existing abstractly in vector space, but to use one meaningfully, we often need to pick a basis. When we see some actual quantum algorithms and protocols, we'll see the power that comes from switching between bases.

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



We can think about measurement more generally. Measuring the state $|\psi\rangle$ in the orthonormal basis $\{|V_1\rangle,\ldots,|V_N\rangle\}$, 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 pick bases like $\{|0\rangle,|1\rangle\}$ arbitrarily as a nice convention.

To do operations in a different basis, we can use unitary transformations to convert between bases.

So for $\{|V_1\rangle,\ldots,|V_N\rangle\}$ use $|V_1\rangle = |1\rangle,\ldots,U|V_N\rangle = |N\rangle$ if you want the $\{|1\rangle,\ldots,|N\rangle\}$ basis

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. More when we talk about interpretations!

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. Physics has treated the microscopic laws as reversible since Galileo's time (i.e. a time-reserved video of a swinging pendulum still shows it obeying the laws of physics). So for example burning a book shouldn't destroy the information within, as physics says that in principle you can get all the information from the smoke and ash left over.

- *Deterministic*
- *Continuous*

  i.e. you can apply them in a time-continuous way.

That's why it's important that unitary matrices are complex.

If the transformation $\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ took place in 1 second, then over the first half of the second, perhaps $\begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$ took place—or some other square root of the transformation.

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

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

But to take a square root of this transformation, *either* you need complex numbers, or else you need to add a third dimension. The latter is analogous to reflecting your three-dimensional self by rotating yourself in a fourth dimension--as in some science fiction stories!

Important: If you come back reflected after a trip into the fourth dimension, don't eat anything without first consulting medical professionals. Normal food will have molecules of the wrong chirality for you to digest them.

Measurements break all three rules of unitary transformations! Measurements are:

- *Irreversible*
    - Whatever information about the system you didn't capture is now lost.
- *Probabilistic*
    - Everything in quantum mechanics is deterministic *until* measurement (or information leaves the system), but measurement outcomes are in general random.
- *Discontinuous*
    - The "collapse of the amplitude vector" is treated as instantaneous in textbooks.

So how can we reconcile these two sets of rules?

That's the **Measurement Problem**. We'll talk about various 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 governed by the 2-norm

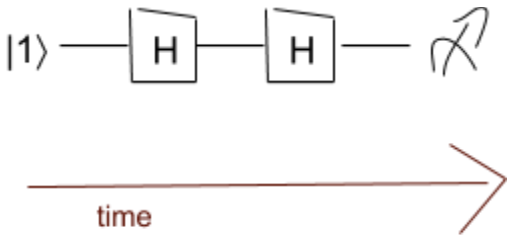
Classical probability is based on the 1-norm, while quantum mechanics is based on the 2-norm. So it's natural to wonder: what about theories based on the 3-norm, 4-norm, etc.? Actually, there don't seem to be any interesting theories there (the extra credit problem on the homework on norm preserving 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 typically get gunk! You could alternatively say that there seems to be "nothing near quantum mechanics, that's nearly as nice as quantum mechanics itself." As another example of this, there are many technical reasons why complex numbers work better than the reals or quaternions as amplitudes.

One more example of a linear transformation.

The matrix $\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ i & -i\end{bmatrix}$ maps $|0\rangle \rightarrow |i\rangle$ $\quad \frac{|0\rangle+i|1\rangle}{\sqrt{2}}$

and $|1\rangle \rightarrow |-i\rangle$ $\quad \frac{|0\rangle-i|1\rangle}{\sqrt{2}}$

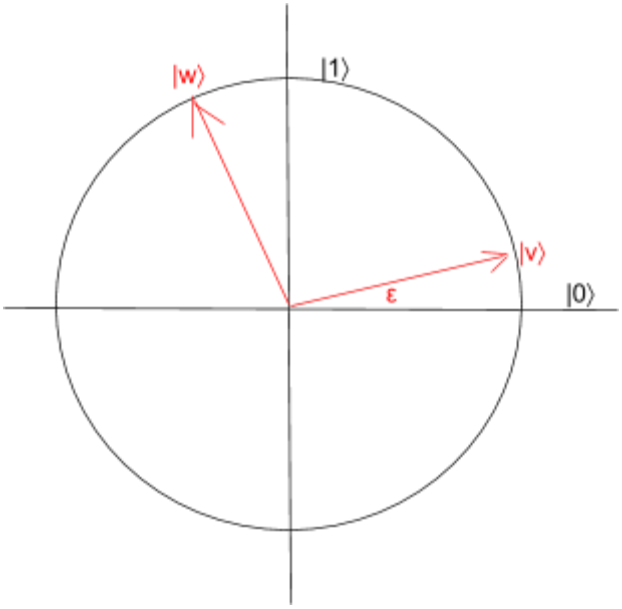
Quantum Circuit Notation helps us keep track of what qubits we have and what operations we apply to them.



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

We'll never branch a qubit line into multiple qubit lines, since that doesn'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 state $|0\rangle$. 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 in a basis that's rotated from $\{|0\rangle, |1\rangle\}$ by an angle ε. The probability of getting the qubit to move by ε increases as ε decreases.

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

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

where

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

So over $\approx \frac{1}{\varepsilon}$ such measurements, we could slowly drag the qubit from $|0\rangle$ to $|1\rangle$.

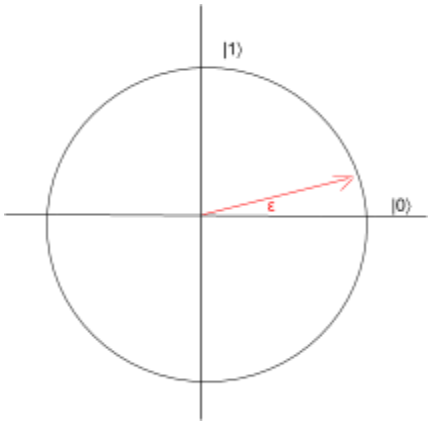
What's the likelihood that we'd ever get a measurement outcome that *wasn't* the one we wanted?

By union bound, it's of order $\frac{1}{\varepsilon} \times \varepsilon^2 = \varepsilon$, so can be made arbitrarily small.

This is called **The Quantum Zeno Effect**
One of its discoverers was Alan Turing.

Perhaps an everyday-life analog would be asking a stranger to have coffee with you, then to go dancing, etc.—there's a higher probability of success than if you just immediately ask them to marry you!

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

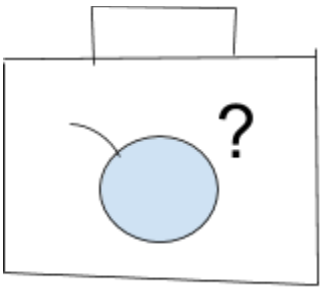


Say we want to keep a qubit at $|0\rangle$, but it keeps rotating towards $|1\rangle$ (it's *drifting*).

If we keep measuring it on the $|0\rangle, |1\rangle$ basis the odds of it jumping to $|1\rangle$ at any given measurement is only ε^2. So if we repeat $\approx \frac{1}{\varepsilon}$ times, then the probability it ending up at $|1\rangle$ is only $\approx \varepsilon$, even though it would have drifted to $|1\rangle$ with certainty had we not measured.

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

Another interesting phenomenon is the **Elitzur-Vaidman Bomb**.
A quantum effect discovered in the early 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 check if there's a bomb there without triggering it?

We could make a query with a classical bit:

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

But then we either learn find nothing, *or* we set off the bomb if there's indeed a bomb there. Not good!

Instead, we can upgrade to a qubit:

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

Now assume: If there's no bomb the state $|b\rangle$ gets returned to you.

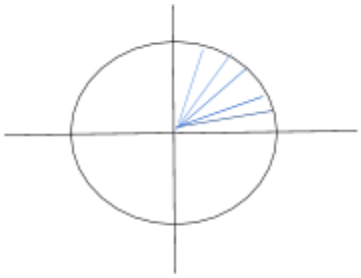
If there is a bomb, the bomb measures in the $\{|0\rangle, |1\rangle\}$ basis. If the outcome is $|0\rangle$, then $|0\rangle$ is returned to you, while if the outcome is $|1\rangle$, the bomb explodes.

What we can do is apply the rotation $R_\varepsilon = \begin{bmatrix} cos\,\varepsilon & -sin\,\varepsilon \\ sin\,\varepsilon & cos\,\varepsilon \end{bmatrix}$. Giving us:

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

If there's a bomb, the probability it explodes is $sin^2\varepsilon \approx \varepsilon^2$, otherwise we get back $|0\rangle$.

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



So repeating about π/(2ε) times makes the probability of setting off the bomb only $\approx \frac{1}{\varepsilon} \times \varepsilon^2 = \varepsilon$. Yet by measuring our $|b\rangle$ qubit to see whether it's $|0\rangle$ or $|1\rangle$, we still learn whether or not a bomb was there.

Of course, the catch is that this requires not merely a qubit on our end, but also a bomb that can be "quantumly interrogated"!