Limitations on quantum information

Despite sharing a common underlying mathematical structure, quantum and classical information have key differences. As a result, there are many examples of tasks that quantum information allows but classical information does not.

Before exploring some of these examples, however, we'll take note of some important limitations on quantum information. Understanding things quantum information can't do helps us identify the things it can do.

Irrelevance of global phases

The first limitation we'll cover — which is really more of a slight degeneracy in the way that quantum states are represented by quantum state vectors, as opposed to an actual limitation — concerns the notion of a *global phase*.

What we mean by a global phase is this. Let $|\psi\rangle$ and $|\phi\rangle$ be unit vectors representing quantum states of some system, and suppose that there exists a complex number α on the unit circle, meaning that $|\alpha| = 1$, or alternatively $\alpha = e^{i\theta}$ for some real number θ, such that

$$|\phi\rangle = \alpha|\psi\rangle.$$

The vectors $|\psi\rangle$ and $|\phi\rangle$ are then said to *differ by a global phase*. We also sometimes refer to α as a *global phase*, although this is context-dependent; any number on the unit circle can be thought of as a global phase when multiplied to a unit vector.

Consider what happens when a system is in one of the two quantum states $|\psi\rangle$ and $|\phi\rangle$, and the system undergoes a standard basis measurement. In the first case, in which the system is in the state $|\psi\rangle$, the probability of measuring any given classical state a is

$$\big|\langle a|\psi\rangle\big|^2.$$

In the second case, in which the system is in the state $|\phi\rangle$, the probability of measuring any classical state a is

$$\big|\langle a|\phi\rangle\big|^2 = \big|\alpha\langle a|\psi\rangle\big|^2 = |\alpha|^2\big|\langle a|\psi\rangle\big|^2 = \big|\langle a|\psi\rangle\big|^2,$$

because $|\alpha| = 1$. That is, the probability of an outcome appearing is the same for both states.

Now consider what happens when we apply an arbitrary unitary operation U to both states. In the first case, in which the initial state is $|\psi\rangle$, the state becomes

$$U|\psi\rangle,$$

and in the second case, in which the initial state is $|\phi\rangle$, it becomes

$$U|\phi\rangle = \alpha U|\psi\rangle.$$

That is, the two resulting states still differ by the same global phase α.

Consequently, two quantum states $|\psi\rangle$ and $|\phi\rangle$ that differ by a global phase are completely indistinguishable; no matter what operation, or sequence of operations, we apply to the two states, they will always differ by a global phase, and performing a standard basis measurement will produce outcomes with precisely the same probabilities as the other. For this reason, two quantum state vectors that differ by a global phase are considered to be equivalent, and are effectively viewed as being the same state.

For example, the quantum states

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

differ by a global phase (which is -1 in this example), and are therefore considered to be the same state.

On the other hand, the quantum states

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

do not differ by a global phase. Although the only difference between the two states is that a plus sign turns into a minus sign, this is not a *global* phase difference, it is a *relative* phase difference because it does not affect every vector entry, but only a proper subset of the entries. This is

consistent with what we have already observed previously, which is that the states $|+\rangle$ and $|-\rangle$ can be discriminated perfectly. In particular, performing a Hadamard operation and then measuring yields outcome probabilities as follows:

$$\begin{aligned} \bigl|\langle 0|H|+\rangle\bigr|^2 &= 1 \qquad & \bigl|\langle 0|H|-\rangle\bigr|^2 &= 0 \\ \bigl|\langle 1|H|+\rangle\bigr|^2 &= 0 \qquad & \bigl|\langle 1|H|-\rangle\bigr|^2 &= 1. \end{aligned}$$

No-cloning theorem

The *no-cloning theorem* shows it is impossible to create a perfect copy of an unknown quantum state.

> **Theorem (No-cloning theorem).** Let Σ be a classical state set having at least two elements, and let X and Y be systems sharing the same classical state set Σ. There does not exist a quantum state $|\phi\rangle$ of Y and a unitary operation U on the pair (X, Y) such that
>
> $$U\bigl(|\psi\rangle \otimes |\phi\rangle\bigr) = |\psi\rangle \otimes |\psi\rangle$$
>
> for every state $|\psi\rangle$ of X.

That is, there is no way to initialize the system Y (to any state $|\phi\rangle$ whatsoever) and perform a unitary operation U on the joint system (X, Y) so that the effect is for the state $|\psi\rangle$ of X to be *cloned*—resulting in (X, Y) being in the state $|\psi\rangle \otimes |\psi\rangle$.

The proof of this theorem is actually quite simple: it boils down to the observation that the mapping

$$|\psi\rangle \otimes |\phi\rangle \mapsto |\psi\rangle \otimes |\psi\rangle$$

is not linear in $|\psi\rangle$.

In particular, because Σ has at least two elements, we may choose $a, b \in \Sigma$ with $a \neq b$. If there did exist a quantum state $|\phi\rangle$ of Y and a unitary operation U on the pair (X, Y) for which $U\bigl(|\psi\rangle \otimes |\phi\rangle\bigr) = |\psi\rangle \otimes |\psi\rangle$ for every quantum state $|\psi\rangle$ of X, then it would be the case that

$$U\bigl(|a\rangle \otimes |\phi\rangle\bigr) = |a\rangle \otimes |a\rangle \quad \text{and} \quad U\bigl(|b\rangle \otimes |\phi\rangle\bigr) = |b\rangle \otimes |b\rangle.$$

By linearity, meaning specifically the linearity of the tensor product in the first argument and the linearity of matrix-vector multiplication in the second (vector) argument, we must therefore have

$$U\left(\left(\frac{1}{\sqrt{2}}|a\rangle + \frac{1}{\sqrt{2}}|b\rangle\right) \otimes |\phi\rangle\right) = \frac{1}{\sqrt{2}}|a\rangle \otimes |a\rangle + \frac{1}{\sqrt{2}}|b\rangle \otimes |b\rangle.$$

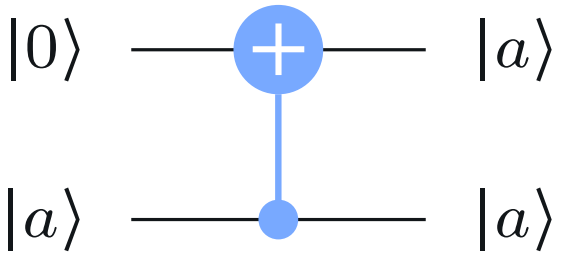
However, the requirement that $U\big(|\psi\rangle \otimes |\phi\rangle\big) = |\psi\rangle \otimes |\psi\rangle$ for every quantum state $|\psi\rangle$ demands that

$$\begin{aligned}
&U\left(\left(\frac{1}{\sqrt{2}}|a\rangle + \frac{1}{\sqrt{2}}|b\rangle\right) \otimes |\phi\rangle\right) \\
&\quad = \left(\frac{1}{\sqrt{2}}|a\rangle + \frac{1}{\sqrt{2}}|b\rangle\right) \otimes \left(\frac{1}{\sqrt{2}}|a\rangle + \frac{1}{\sqrt{2}}|b\rangle\right) \\
&\quad = \frac{1}{2}|a\rangle \otimes |a\rangle + \frac{1}{2}|a\rangle \otimes |b\rangle + \frac{1}{2}|b\rangle \otimes |a\rangle + \frac{1}{2}|b\rangle \otimes |b\rangle \\
&\quad \neq \frac{1}{\sqrt{2}}|a\rangle \otimes |a\rangle + \frac{1}{\sqrt{2}}|b\rangle \otimes |b\rangle
\end{aligned}$$

Therefore there cannot exist a state $|\phi\rangle$ and a unitary operation U for which $U\big(|\psi\rangle \otimes |\phi\rangle\big) = |\psi\rangle \otimes |\psi\rangle$ for every quantum state vector $|\psi\rangle$.

A few remarks concerning the no-cloning theorem are in order. The first one is that the statement of the no-cloning theorem above is absolute, in the sense that it states that *perfect* cloning is impossible — but it does not say anything about possibly cloning with limited accuracy, where we might succeed in producing an approximate clone (with respect to some way of measuring how similar two different quantum states might be). There are, in fact, statements of the no-cloning theorem that place limitations on approximate cloning, as well as methods to achieve approximate cloning with limited accuracy.

The second remark is that the no-cloning theorem is a statement about the impossibility of cloning an *arbitrary* state $|\psi\rangle$. In contrast, we can easily create a clone of any standard basis state, for instance. For example, we can clone a qubit standard basis state using a controlled-NOT operation:



While there is no difficulty in creating a clone of a standard basis state, this does not contradict the no-cloning theorem. This approach of using a controlled-NOT gate would not succeed in creating a clone of the state $|+\rangle$, for instance.

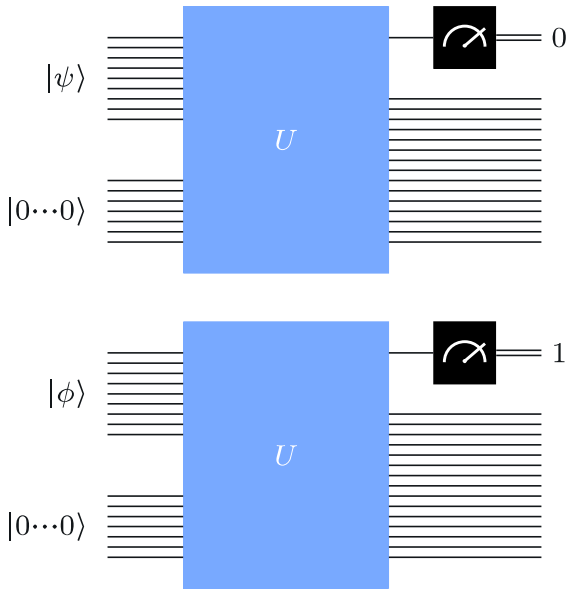
One final remark about the no-cloning theorem is that it really isn't unique to quantum information — it's also impossible to clone an arbitrary probabilistic state using a classical (deterministic or probabilistic) process. Imagine someone hands you a system in some probabilistic state, but you're not sure what that probabilistic state is. For example, maybe they randomly generated a number between 1 and 10, but they didn't tell you how they generated that number. There's certainly no physical process through which you can obtain two *independent* copies of that same probabilistic state: all you have in your hands is a number between 1 and 10, and there just isn't enough information present for you to somehow reconstruct the probabilities for all of the other outcomes to appear.

Mathematically speaking, a version of the no-cloning theorem for probabilistic states can be proved in exactly the same way as the regular no-cloning theorem (for quantum states). That is, cloning an arbitrary probabilistic state is a non-linear process, so it cannot possibly be represented by a stochastic matrix.

Non-orthogonal states cannot be perfectly discriminated

For the final limitation to be covered in this lesson, we'll show that if we have two quantum states $|\psi\rangle$ and $|\phi\rangle$ that are not orthogonal, which means that $\langle\phi|\psi\rangle \neq 0$, then it's impossible to discriminate them (or, in other words, to tell them apart) perfectly. In fact, we'll show something logically equivalent: if we do have a way to discriminate two states perfectly, without any error, then they must be orthogonal.

We'll restrict our attention to quantum circuits that consist of any number of unitary gates, followed by a single standard basis measurement of the top qubit. What we require of a quantum circuit, to say that it perfectly discriminates the states $|\psi\rangle$ and $|\phi\rangle$, is that the measurement always yields the value 0 for one of the two states and always yields 1 for the other state. To be precise, we shall assume that we have a quantum circuit that operates as the following diagrams suggest:



The box labeled U denotes the unitary operation representing the combined action of all of the unitary gates in our circuit, but not including the final measurement. There is no loss of generality in assuming that the measurement outputs 0 for $|\psi\rangle$ and 1 for $|\phi\rangle$; the analysis would not differ fundamentally if these output values were reversed.

Notice that, in addition to the qubits that initially store either $|\psi\rangle$ or $|\phi\rangle$, the circuit is free to make use of any number of additional *workspace* qubits. These qubits are initially each set to the $|0\rangle$ state — so their combined state is denoted $|0\cdots0\rangle$ in the figures — and these qubits can be used by the circuit in any way that might be beneficial. It is very common to make use of workspace qubits in quantum circuits like this.

Now, consider what happens when we run our circuit on the state $|\psi\rangle$ (along with the initialized workspace qubits). The resulting state, immediately prior to the measurement being performed, can be written as

$$U\big(|0\cdots0\rangle|\psi\rangle\big) = |\gamma_0\rangle|0\rangle + |\gamma_1\rangle|1\rangle$$

for two vectors $|\gamma_0\rangle$ and $|\gamma_1\rangle$ that correspond to all of the qubits except the top qubit. In general, for such a state the probabilities that a measurement of the top qubit yields the outcomes 0 and 1 are as follows:

$$\text{Pr}(\text{outcome is } 0) = \big\||\gamma_0\rangle\big\|^2 \qquad \text{and} \qquad \text{Pr}(\text{outcome is } 1) = \big\||\gamma$$

Because our circuit always outputs 0 for the state $|\psi\rangle$, it must be that $|\gamma_1\rangle = 0$, and so

$$U\big(|0\cdots 0\rangle|\psi\rangle\big) = |\gamma_0\rangle|0\rangle.$$

Multiplying both sides of this equation by $U^\dagger$ yields this equation:

$$|0\cdots 0\rangle|\psi\rangle = U^\dagger\big(|\gamma_0\rangle|0\rangle\big). \tag{1}$$

Reasoning similarly for $|\phi\rangle$ in place of $|\psi\rangle$, we conclude that

$$U\big(|0\cdots 0\rangle|\phi\rangle\big) = |\delta_1\rangle|1\rangle$$

for some vector $|\delta_1\rangle$, and therefore

$$|0\cdots 0\rangle|\phi\rangle = U^\dagger\big(|\delta_1\rangle|1\rangle\big). \tag{2}$$

Now let us take the inner product of the vectors represented by the equations (1) and (2), starting with the representations on the right-hand side of each equation. We have

$$\big(U^\dagger\big(|\gamma_0\rangle|0\rangle\big)\big)^\dagger = \big(\langle\gamma_0|\langle 0|\big)U,$$

so the inner product of the vector (1) with the vector (2) is

$$\big(\langle\gamma_0|\langle 0|\big)UU^\dagger\big(|\delta_1\rangle|1\rangle\big) = \big(\langle\gamma_0|\langle 0|\big)\big(|\delta_1\rangle|1\rangle\big) = \langle\gamma_0|\delta_1\rangle\langle 0|1\rangle = 0.$$

Here we have used the fact that $UU^\dagger = \mathbb{I}$, as well as the fact that the inner product of tensor products is the product of the inner products:

$$\langle u\otimes v|w\otimes x\rangle = \langle u|w\rangle\langle v|x\rangle$$

for any choices of these vectors (assuming $|u\rangle$ and $|w\rangle$ have the same number of entries and $|v\rangle$ and $|x\rangle$ have the same number of entries, so that it makes sense to form the inner products $\langle u|w\rangle$ and $\langle v|x\rangle$). Notice that the value of the inner product $\langle\gamma_0|\delta_1\rangle$ is irrelevant because it is multiplied by $\langle 0|1\rangle = 0$.

Finally, taking the inner product of the vectors on the left-hand sides of the equations (1) and (2) must result in the same zero value that we've already calculated, so

$$0 = \big(|0\cdots 0\rangle|\psi\rangle\big)^\dagger\big(|0\cdots 0\rangle|\phi\rangle\big) = \langle 0\cdots 0|0\cdots 0\rangle\langle\psi|\phi\rangle = \langle\psi|\phi\rangle.$$

We have therefore concluded what we wanted, which is that $|\psi\rangle$ and $|\phi\rangle$ are orthogonal: $\langle\psi|\phi\rangle = 0$.

It is possible, by the way, to perfectly discriminate any two states that are orthogonal, which is the converse to the statement we just proved. Suppose that the two states to be discriminated are $|\phi\rangle$ and $|\psi\rangle$, where $\langle\phi|\psi\rangle = 0$. We can then perfectly discriminate these states by

performing the projective measurement described by these matrices, for instance:

$$\big\{|\phi\rangle\langle\phi|,\, \mathbb{I} - |\phi\rangle\langle\phi|\big\}.$$

For the state $|\phi\rangle$, the first outcome is always obtained:

$$\big\||\phi\rangle\langle\phi|\phi\rangle\big\|^2 = \big\||\phi\rangle\langle\phi|\phi\rangle\big\|^2 = \big\||\phi\rangle\big\|^2 = 1,$$
$$\big\|(\mathbb{I} - |\phi\rangle\langle\phi|)|\phi\rangle\big\|^2 = \big\||\phi\rangle - |\phi\rangle\langle\phi|\phi\rangle\big\|^2 = \big\||\phi\rangle - |\phi\rangle\big\|^2 = 0.$$

And, for the state $|\psi\rangle$, the second outcome is always obtained:

$$\big\||\phi\rangle\langle\phi|\psi\rangle\big\|^2 = \big\||\phi\rangle\langle\phi|\psi\rangle\big\|^2 = \big\|0\big\|^2 = 0,$$
$$\big\|(\mathbb{I} - |\phi\rangle\langle\phi|)|\psi\rangle\big\|^2 = \big\||\psi\rangle - |\phi\rangle\langle\phi|\psi\rangle\big\|^2 = \big\||\psi\rangle\big\|^2 = 1.$$

Was this page helpful?

Yes No

Report a bug or request content on GitHub ↗.

Previous page

Start the next lesson