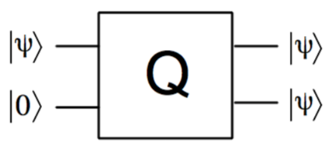
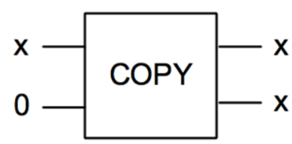
The No-Cloning Theorem

It is easy to make a copy of a classical bit using the *COPY* gate. What about for qubits? Can we find a quantum gate that will make a copy of a qubit in an arbitrary superposition state? In other words, is it possible to *clone* an arbitrary qubit? Such a gate would have to be unitary, so it would need two inputs and two outputs. Suppose that a 2-qubit linear operator $Q : \mathbb{V} \otimes \mathbb{V} \to \mathbb{V} \otimes \mathbb{V}$ takes as inputs a qubit in an arbitrary superposition state $|\psi\rangle$ and a qubit in state $|0\rangle$, and produces two exact copies of $|\psi\rangle$ as outputs. That is, $Q(|\psi\rangle \otimes |0\rangle) = |\psi\rangle \otimes |\psi\rangle$. For comparison, we could imagine adding a "dummy" input bit of 0 to the *COPY* gate, which shows that the Q gate is just a generalization of *COPY*:





Q should operate on the basis states $|0\rangle$ and $|1\rangle$ like this:

- $Q(|0\rangle \otimes |0\rangle) \longrightarrow |0\rangle \otimes |0\rangle$
- $Q(|1\rangle \otimes |0\rangle) \longrightarrow |1\rangle \otimes |1\rangle$

Q should operate on an arbitrary superposition state $\alpha|0\rangle + \beta|1\rangle$, where $\alpha, \beta \in \mathbb{C}$, like this:

- $Q((\alpha|0\rangle + \beta|1\rangle) \otimes |0\rangle) \longrightarrow (\alpha|0\rangle + \beta|1\rangle) \otimes (\alpha|0\rangle + \beta|1\rangle)$

In the latter case, the output is of the form $(A + B) \otimes (A + B)$, where $A = \alpha|0\rangle$ and $B = \beta|1\rangle$. We can rewrite this using the rules for tensor products:

$$(A + B) \otimes (A + B)$$

$$= A \otimes (A + B) + B \otimes (A + B)$$

$$= A \otimes A + A \otimes B + B \otimes A + B \otimes B$$

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

$$= \alpha^2(|0\rangle \otimes |0\rangle) + \alpha\beta(|0\rangle \otimes |1\rangle) + \beta\alpha(|1\rangle \otimes |0\rangle) + \beta^2(|1\rangle \otimes |1\rangle)$$

$$= \alpha^2|00\rangle + \alpha\beta|01\rangle + \beta\alpha|10\rangle + \beta^2|11\rangle$$

This is the output that we *should* get if Q copies the state $\alpha|0\rangle + \beta|1\rangle$ correctly.

But we can also directly work out the result of applying Q to the input $(\alpha|0\rangle + \beta|1\rangle) \otimes |0\rangle$, since we know that Q is a linear operator (all quantum gates are), and that $Q(|0\rangle \otimes |0\rangle) = |0\rangle \otimes |0\rangle$ and $Q(|1\rangle \otimes |0\rangle) = |1\rangle \otimes |1\rangle$. Let's see what we get:

$$
\begin{aligned}
& Q\big((\alpha|0\rangle + \beta|1\rangle) \otimes |0\rangle\big) & \\
= \;& Q\big(\alpha|0\rangle \otimes |0\rangle + \beta|1\rangle \otimes |0\rangle\big) & \text{since } (A+B)\otimes C \text{ is equivalent to } A\otimes C + B\otimes C \\
= \;& Q\big(\alpha|0\rangle \otimes |0\rangle\big) + Q\big(\beta|1\rangle \otimes |0\rangle\big) & \text{since } Q \text{ is linear: } Q(A+B) = Q(A) + Q(B) \\
= \;& Q\big(\alpha(|0\rangle \otimes |0\rangle)\big) + Q\big(\beta(|1\rangle \otimes |0\rangle)\big) & \text{since } cA\otimes B \text{ is equivalent to } c(A\otimes B) \\
= \;& \alpha Q\big(|0\rangle \otimes |0\rangle\big) + \beta Q\big(|1\rangle \otimes |0\rangle\big) & \text{since } Q \text{ is linear: } Q(cA) = cQ(A) \\
= \;& \alpha(|0\rangle \otimes |0\rangle) + \beta(|1\rangle \otimes |1\rangle) & \text{since } Q(|0\rangle\otimes|0\rangle) = |0\rangle\otimes|0\rangle \text{ and } Q(|1\rangle\otimes|0\rangle) = |1\rangle\otimes|1\rangle \\
= \;& \alpha|00\rangle + \beta|11\rangle & \text{since } |00\rangle \text{ and } |11\rangle \text{ are shorthand for } |0\rangle\otimes|0\rangle \text{ and } |1\rangle\otimes|1\rangle
\end{aligned}
$$

The only way in which $\alpha|00\rangle + \beta|11\rangle$ can equal $\alpha^2|00\rangle + \alpha\beta|01\rangle + \beta\alpha|10\rangle + \beta^2|11\rangle$ is if $\alpha = 1$ and $\beta = 0$, or if $\alpha = 0$ and $\beta = 1$. In other words, the only superposition states $\alpha|0\rangle + \beta|1\rangle$ on which Q works correctly are the basis states $|0\rangle = 1|0\rangle + 0|1\rangle$ and $|1\rangle = 0|0\rangle + 1|1\rangle$. This means that only classical bits can be cloned, not arbitrary qubits!

An example

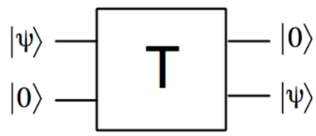
To be more concrete, suppose that $|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$. Cloning $|\psi\rangle$ should give $Q(|\psi\rangle \otimes |0\rangle) = |\psi\rangle \otimes |\psi\rangle = (\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle) \otimes (\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle)$, which, following the above analysis with $\alpha = \beta = \frac{1}{\sqrt{2}}$, equals $\frac{1}{2}|00\rangle + \frac{1}{2}|01\rangle + \frac{1}{2}|10\rangle + \frac{1}{2}|11\rangle$. This means that, after cloning, we would expect both qubits to be in "equally balanced" superpositions of $|0\rangle$ and $|1\rangle$, independent of each other. However, because Q is a linear operator, applying Q to $(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle) \otimes |0\rangle$ must give:

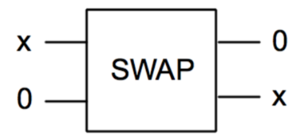
$$
\begin{aligned}
& Q\left((\tfrac{1}{\sqrt{2}}|0\rangle + \tfrac{1}{\sqrt{2}}|1\rangle) \otimes |0\rangle\right) \\
&= Q\left(\tfrac{1}{\sqrt{2}}|0\rangle \otimes |0\rangle + \tfrac{1}{\sqrt{2}}|1\rangle \otimes |0\rangle\right) \\
&= Q\left(\tfrac{1}{\sqrt{2}}|0\rangle \otimes |0\rangle\right) + Q\left(\tfrac{1}{\sqrt{2}}|1\rangle \otimes |0\rangle\right) \\
&= \tfrac{1}{\sqrt{2}}\, Q\Big(|0\rangle \otimes |0\rangle\Big) + \tfrac{1}{\sqrt{2}}\, Q\Big(|1\rangle \otimes |0\rangle\Big) \\
&= \tfrac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle) + \tfrac{1}{\sqrt{2}}(|1\rangle \otimes |1\rangle) \\
&= \tfrac{1}{\sqrt{2}}|00\rangle + \tfrac{1}{\sqrt{2}}|11\rangle \\
&\neq \tfrac{1}{2}|00\rangle + \tfrac{1}{2}|01\rangle + \tfrac{1}{2}|10\rangle + \tfrac{1}{2}|11\rangle
\end{aligned}
$$

which means that the qubits in fact become *entangled* as a result of the "cloning" operation, instead of producing two independent copies of the qubit. Thus Q does not work as it should on the superposition state $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$.

Transporting a qubit

On the other hand, unlike cloning, there is no problem in *transporting* an arbitrary qubit state from one place to another. A 2-qubit transport operator $T : \mathbb{V} \otimes \mathbb{V} \to \mathbb{V} \otimes \mathbb{V}$ would work as follows: $T(|\psi\rangle \otimes |0\rangle) = |0\rangle \otimes |\psi\rangle$. In transporting the state of the first qubit to the second, the first qubit gets reset to $|0\rangle$. This is essentially a quantum version of the $SWAP$ operation:





T should operate on the basis states $|0\rangle$ and $|1\rangle$ like this:

- $T(|0\rangle \otimes |0\rangle) \longrightarrow |0\rangle \otimes |0\rangle$
- $T(|1\rangle \otimes |0\rangle) \longrightarrow |0\rangle \otimes |1\rangle$

T should operate on an arbitrary superposition state $\alpha|0\rangle + \beta|1\rangle$ like this:

- $$\begin{aligned} T((\alpha|0\rangle + \beta|1\rangle) \otimes |0\rangle) &\longrightarrow |0\rangle \otimes (\alpha|0\rangle + \beta|1\rangle) \\ &= |0\rangle \otimes \alpha|0\rangle + |0\rangle \otimes \beta|1\rangle \\ &= \alpha(|0\rangle \otimes |0\rangle) + \beta(|0\rangle \otimes |1\rangle) \\ &= \alpha|00\rangle + \beta|01\rangle \end{aligned}$$

This is the output that we *should* get if T transports the state $\alpha|0\rangle + \beta|1\rangle$ correctly.

Directly working out the actual result gives:

$$\begin{aligned} & T\big((\alpha|0\rangle + \beta|1\rangle) \otimes |0\rangle\big) & \\ = \;& T\big(\alpha|0\rangle \otimes |0\rangle + \beta|1\rangle \otimes |0\rangle\big) & \text{since } (A+B) \otimes C \text{ is equivalent to } A \otimes C + B \otimes C \\ = \;& T\big(\alpha|0\rangle \otimes |0\rangle\big) + T\big(\beta|1\rangle \otimes |0\rangle\big) & \text{since } T \text{ is linear: } T(A+B) = T(A) + T(B) \\ = \;& \alpha\, T\big(|0\rangle \otimes |0\rangle\big) + \beta\, T\big(|1\rangle \otimes |0\rangle\big) & \text{since } T \text{ is linear: } T(cA) = cT(A) \\ = \;& \alpha(|0\rangle \otimes |0\rangle) + \beta(|0\rangle \otimes |1\rangle) & \text{since } T(|0\rangle \otimes |0\rangle) = |0\rangle \otimes |0\rangle \text{ and } T(|1\rangle \otimes |0\rangle) = |0\rangle \otimes |1\rangle \\ = \;& \alpha|00\rangle + \beta|01\rangle & \text{since } |00\rangle \text{ and } |01\rangle \text{ are shorthand for } |0\rangle \otimes |0\rangle \text{ and } |0\rangle \otimes |1\rangle \end{aligned}$$

which is exactly the behavior we expect when applying T to $\alpha|0\rangle + \beta|1\rangle$.

The 2-qubit output state $\alpha|00\rangle + \beta|01\rangle$ is equivalent to $|0\rangle \otimes (\alpha|0\rangle + \beta|1\rangle)$, meaning that the state of the first qubit is $|0\rangle$ and the state of the second is $\alpha|0\rangle + \beta|1\rangle$. Measuring the first qubit would yield $|0\rangle$ with certainty, but would give us no information about the state of the second. Thus the two output qubits are independent rather than entangled.