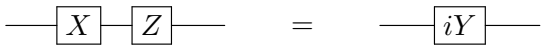
PHY 4105: Quantum Information Theory
Lecture 22

Anil Shaji
School of Physics, IISER Thiruvananthapuram
(Dated: October 29, 2013)

Circuit Identities

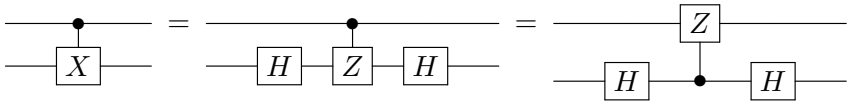
It is useful to see how some standard operator identities look in the circuit model because that helps us in simplifying combinations of gates into simpler ones. We start with a few simple identities whose operator version is well known.

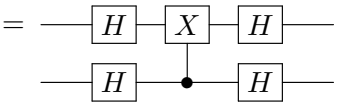
1. Order



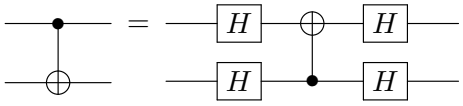
2. The Hadamard swaps the standard basis and the X basis $(|0\rangle \pm |1\rangle)/\sqrt{2}$. This gives us,

3. Following from the above we have the bit more complicated two qubit gate identity:





This means that

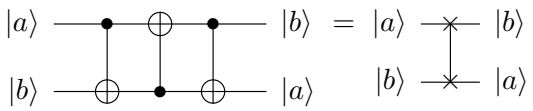


This follows from

$$P_0 \otimes \mathbb{1} + P_1 \mathbb{1} X = P_0 \otimes (P_x + P_{-x}) + P_1 \otimes (P_x - P_{-x}) = \mathbb{1} \otimes P_x + Z \otimes P_{-x}.$$

In other words one can exchange the control and the target in the case of the controlled not by using Hadamards.

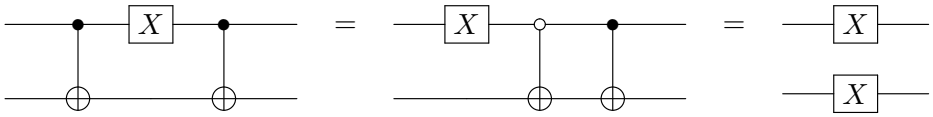
4. Swap



In the circuit on the left, the transformations that are happening are

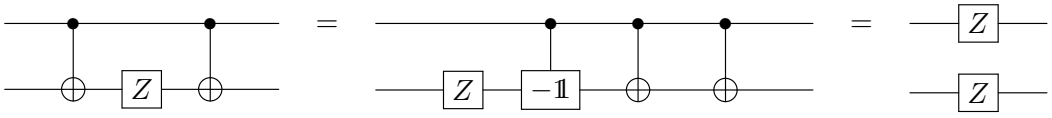
$$|a,b\rangle \;\rightarrow\; |a,a\oplus b\rangle \;\rightarrow\; |a\oplus(a\oplus b),a\oplus b\rangle = |b,a\oplus b\rangle \;\rightarrow\; |b,(b\oplus a)\oplus b\rangle = |b,a\rangle.$$

5. Sometimes combinations of two qubit gates reduce to one qubit operations

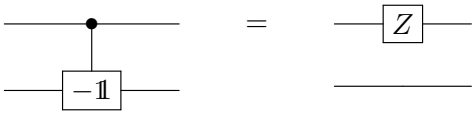


The empty control denotes a control on $|0\rangle$ rather on $|1\rangle$.

6. Similarly

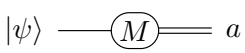


where we have used

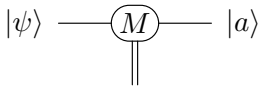


1. Measurements

We denote a measurement in the standard basis as

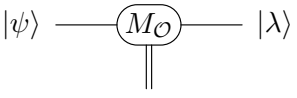


Here a denotes the result of the measurement and the double wire stands for a classical wire. If we are interested in the post measurement state also, then the circuit is drawn as



$$a,\ p_a = |\langle a|\psi\rangle|^2$$

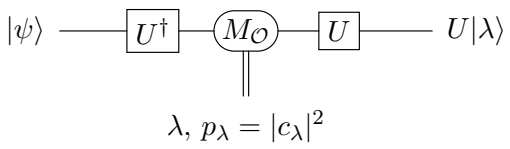
A measurement in a different basis is denoted as



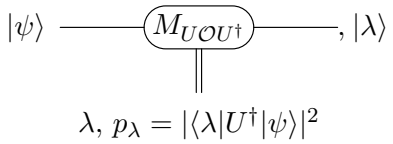
$$\lambda,\ p_\lambda = |\langle \lambda|\psi\rangle|^2$$

with $\mathcal{O} = \sum_\lambda \lambda|\lambda\rangle\langle\lambda|$.

Now consider



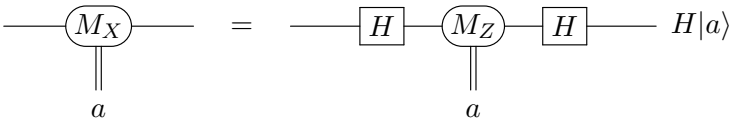
After the first unitary we have $|\psi\rangle = \sum_\lambda c_\lambda U|\lambda\rangle \to U|\psi\rangle = \sum_\lambda c_\lambda|\lambda\rangle$. Now the measurement on to the $|\lambda\rangle$ basis gives a result λ with probability $|c_\lambda|^2$. The corresponding post measurement state is the basis vector $|\lambda\rangle$ as expected. The last U brings this post measurement state back to the original (computational) basis. This process can equivalently be described as a measurement in the basis $U|\lambda\rangle$ as



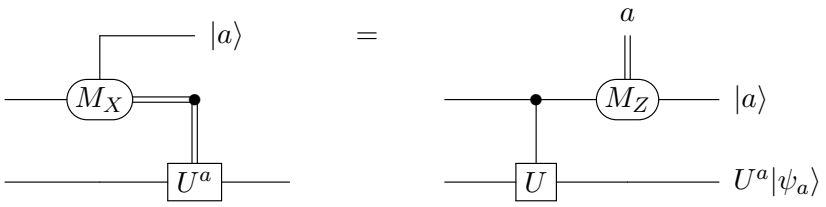
where

$$U\mathcal{O}U^\dagger = \sum_\lambda \lambda U|\lambda\rangle\langle\lambda|U^\dagger.$$

As an example



Using the circuit identities we have seen, it is possible to move a measurement that happens in the middle of a quantum protocol to the end of the circuit so that the protocol itself remains reversible. This is called the *principle of deferred measurement*. For instance, if a control is based on a the result of a measurement, we can do the control first and then do an appropriate measurement which "post-selects" the correct final state:



In the first circuit, for the input state on the left side, we can do a relative state decomposition as

$$\sqrt{p_0}|0\rangle \otimes |\psi_1\rangle + \sqrt{p_1}|1\rangle \otimes |\psi_1\rangle.$$

The action of the measurement is to pick out one of the terms of the superposition and if the result of the measurement is $|1\rangle$ for the top qubit, then U is applied to the relative state of the

second. So after the unitary controlled on the classical result of the measurement we have the state $|a\rangle \otimes U^a|\psi_a\rangle$ for the whole system. In the second circuit, the state after the controlled U is

$$\sqrt{p_0}|0\rangle \otimes |\psi_1\rangle + \sqrt{p_1}|1\rangle \otimes U|\psi_1\rangle.$$

So again, after the measurement, one of the two pieces of the superposition is picked out and the final state is again $|a\rangle \otimes U^a|\psi_a\rangle$.