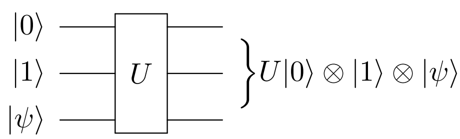
PHY 4105: Quantum Information Theory
Lecture 21

Anil Shaji
School of Physics, IISER Thiruvananthapuram

(Dated: October 22, 2013)

The circuit model

The quantum circuit model provides an alternate, equivalent and pictorial way of representing the states, dynamics and other steps involved in a quantum information processing protocol that also sheds more light on possible physical realizations of the same. In this way of looking at things, quantum states propagate along “wires” through “gates”:



The quantum circuits clearly display the temporal and spatial relations that are usually difficult to convey and not very apparent in the algebraic descriptions.

Taking a cue from classical computing and information processing, we do not focus on arbitrary transformations or gates U but rather look for a specific universal set of gates/transformations using which all other transformations can be built. The following table summarizes the typical classical gates and indicates whether analogues of these gates are possible in a quantum circuit:

Classical Gates		**Quantum version**	**Remarks**
Identity	$a \to a$	✓	
Not	$a \to \bar{a} = 1 \oplus a$	✓	
Fanout	$a \to a,\, a,\, a$	$\times$	No Cloning
Swap	$a,\, b \to b,\, a$	✓	
And	$a,\, b \to ab$	$\times$	Irreversible
Or	$a,\, b \to \overline{\bar{a}\bar{b}} = a \oplus b \oplus ab$	$\times$	Irreversible
Xor	$a,\, b \to a \oplus b$	$\times$	Irreversible
Nand	$a,\, b \to \overline{ab} = 1 \oplus ab$	$\times$	Irreversible
Nor	$a,\, b \to \bar{a}\bar{b} = (1+a) \oplus (1+b)$	$\times$	Irreversible

The classical gates can be characterized with truth tables of the form:

Xor

a	b	$a \oplus b$
0	0	0
0	1	1
1	0	1
1	1	0

	AND	
a	b	$a \oplus b$
0	0	0
0	1	0
1	0	0
1	1	1

With reversible quantum (closed) dynamics we cannot implement irreversible gates. So we have to find reversible analogues of irreversible universal classical gates like XOR, NAND etc.

We start with some important quantum gates that we have seen before

$$ie^{-iX\pi/2} = X \leftrightarrow \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \begin{matrix} |0\rangle \to |1\rangle \\ |1\rangle \to |0\rangle \end{matrix} \quad |a\rangle \to |\bar{a}\rangle = |1 \oplus a\rangle \qquad \text{NOT.}$$

$$ie^{-iZ\pi/2} = Z \leftrightarrow \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad \begin{matrix} |0\rangle \to |0\rangle \\ |1\rangle \to -|1\rangle \end{matrix} \quad |a\rangle \to (-1)^a |a\rangle \qquad \text{SIGN.}$$

$$-e^{-iY\pi/2} = iY = ZX \leftrightarrow \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad \begin{matrix} |0\rangle \to -|1\rangle \\ |1\rangle \to |0\rangle \end{matrix} \quad |a\rangle \to (-1)^{\bar{a}} |\bar{a}\rangle = -(-1)^a |1 \oplus a\rangle.$$

$$ie^{-i\frac{1}{\sqrt{2}}(X+Y)\pi/2} = \frac{1}{\sqrt{2}}(X+Z) \equiv H \leftrightarrow \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad \begin{matrix} |0\rangle \to \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ |1\rangle \to \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \end{matrix}.$$

This is the HADAMARD gate or Hadamard transformation.

$$H \quad \leftrightarrow \quad |a\rangle \frac{1}{\sqrt{2}}(|0\rangle + (-1)^a |1\rangle).$$

All of the above gates are chosen to be 180 degree rotations about some axis so that the gates themselves are Hermitian (not just unitary) and they all square to 1.

$$H = H^\dagger \Rightarrow H^2 = \mathbb{1}.$$

We also have

$$HXH = Z, \qquad HZH = X, \qquad HYH = Y.$$

It is instructive to compare the Hadamard gate with the almost similar gate which rotates 90 degrees about the Y axis:

$$U = e^{-iY\pi/4} = \frac{1}{\sqrt{2}}(\mathbb{1} - iY) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}.$$

We have

$$UXU^\dagger = -Z \qquad UZU^\dagger = X, \qquad UYU^\dagger = Y.$$

Another couple of single qubit gates which are not Hermitian and do not square to one but are of interest to us later are:

$$e^{i\pi/4}e^{-iZ\pi/4} \equiv S \leftrightarrow \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \qquad \begin{matrix} |0\rangle \to |0\rangle \\ |1\rangle \to i|1\rangle \end{matrix} \qquad |a\rangle \to i^a|a\rangle \qquad \text{PHASE.}$$

This is, apart from a phase, a $pi/2$ rotation about the Z axis. On the Pauli basis,

$$SXS^\dagger = -Y \qquad SYS^\dagger = -X, \qquad SZS^\dagger = Z.$$

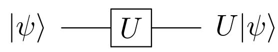
Finally we have

$$e^{i\pi/8}e^{-iZ\pi/4} \equiv T \leftrightarrow \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix} \qquad \begin{matrix} |0\rangle \to |0\rangle \\ |1\rangle \to e^{i\pi/4}|1\rangle \end{matrix} \qquad |a\rangle \to e^{ia\pi/4}|a\rangle \qquad \text{T.}$$

This is, apart from a phase, a $pi/4$ rotation about the Z axis. On the Pauli basis,

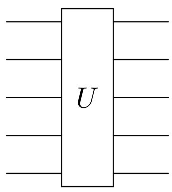
$$TXT^\dagger = \frac{1}{\sqrt{2}}(X+Y) \qquad TYT^\dagger = \frac{1}{\sqrt{2}}(-X+Y), \qquad TZT^\dagger = Z.$$

Single qubit gates in the circuit model look like:

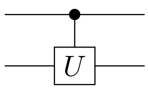


A. Multiple qubit gates

We are not particularly interested in arbitrary multiqubit gates that act on any number of qubits since we are again looking for simple universal operations from which to build more complex unitaries. So we are not going to look at gates of the form:



We restrict ourselves to two qubit gates from which multi qubit gates can be built. These two qubit gates are typically controlled unitaries:



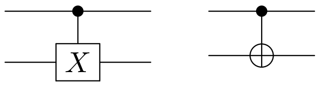
$$P_0 \otimes \mathbb{1} + P_1 \otimes U \quad \leftrightarrow \quad \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & u_{11} & u_{12} \\ 0 & 0 & u_{21} & u_{22} \end{pmatrix}$$

The truth table of U can be written in equation form as

$$|00\rangle \to |00\rangle, \quad |01\rangle \to |01\rangle, \quad |10\rangle \to |1\rangle \otimes U|0\rangle, \quad |11\rangle \to |1\rangle \otimes U|1\rangle.$$

Specific useful examples of two qubit gates include

CNOT



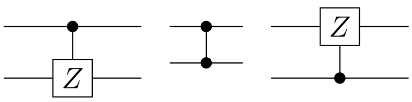
$$P_0 \otimes \mathbb{1} + P_1 \otimes X \quad \leftrightarrow \quad \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

$$(\mathrm{CNOT})^\dagger = \mathrm{CNOT}, \qquad \Rightarrow \qquad (\mathrm{CNOT})^2 = \mathbb{1}.$$

$$|00\rangle \to |00\rangle, \quad |01\rangle \to |01\rangle, \quad |10\rangle \to |11\rangle, \quad |11\rangle \to |10\rangle, \qquad |a, b\rangle \to |a, a \oplus b\rangle.$$

The cnot has an essentially classical truth table. The XOR or the inputs is placed in the second qubit.

CSIGN, also called CPHASE



$$P_0 \otimes \mathbb{1} + P_1 \otimes Z \quad \leftrightarrow \quad \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}.$$

$$(\mathrm{CSIGN})^\dagger = \mathrm{CSIGN}, \qquad \Rightarrow \qquad (\mathrm{CSIGN})^2 = \mathbb{1}.$$

$$|00\rangle \to |00\rangle, \quad |01\rangle \to |01\rangle, \quad |10\rangle \to |10\rangle, \quad |11\rangle \to -|11\rangle, \qquad |a, b\rangle \to (-1)^{ab}|a, b\rangle.$$

The csign also has an essentially classical truth table. The AND or the inputs is placed in the phase bit.