1 Readings

Benenti, Casati, and Strini:

Quantum Gates Ch. 3.2-3.4

Universality Ch. 3.5-3.6

2 Quantum Gates

Continuing from last time, we will conside two-qubit and n-qubit gates.

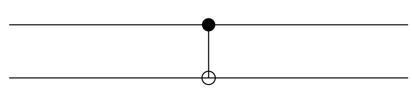
2.1 Two-qubit gates:

- Any one-qubit gate can be tensored with itself or another gate to make a two-qubit gate, as done above for $H \otimes H$. Such tensor products of one-qubit gates have no ability to generate entanglement and are referred to as 'local' gates.
- Controlled Not ($CNOT$).

$$\text{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

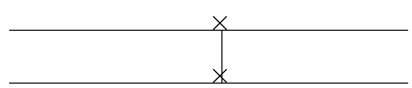
The first bit of a $CNOT$ gate is the "control bit;" the second is the "target bit." The control bit never changes, while the target bit flips if and only if the control bit is 1.

The $CNOT$ gate is usually drawn as follows, with the control bit on top and the target bit on the bottom:



Note that $(CNOT)^2 = 1$, i.e., $CNOT^{-1} = CNOT$.

- SWAP

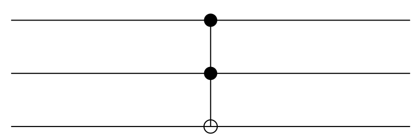


$$\text{SWAP} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

2.2 n-qubit gates:

- local n-qubit gates formed as tensor products of one-qubit gates, e.g., $H^{\otimes n}$
- Toffoli gate

  This is a 3-qubit generalization of the CNOT gate. The third, target, qubit is flipped iff both the first and second qubits are in state 1. $TOFF^2 = 1$.

  The Toffoli gate can be decomposed into a combination of one-qubit and two-qubit gates. See Figures 3 and 4.

2.3 Useful gate equivalences

- *SWAP* equals 3 x *CNOT*

  See Figure 5.

  Suppose we have two qubits in state $|y_2, y_1\rangle$:

  $$\begin{bmatrix} a \\ b \end{bmatrix} \otimes \begin{bmatrix} c \\ d \end{bmatrix}$$
  $$= ac|00\rangle + ad|01\rangle + bc|10\rangle + bd|11\rangle$$

  Apply the first $CNOT$:

  $$ac|00\rangle + ad|01\rangle + bd|10\rangle + bc|11\rangle$$

  Apply the second $CNOT$:

  $$ac|00\rangle + bc|01\rangle + bd|10\rangle + ad|11\rangle$$

  Apply the third $CNot$:

  $$ac|00\rangle + bc|01\rangle + ad|10\rangle + bd|11\rangle$$
  $$= ca|00\rangle + cb|01\rangle + da|10\rangle + db|11\rangle$$
  $$= \begin{bmatrix} c \\ d \end{bmatrix} \otimes \begin{bmatrix} a \\ b \end{bmatrix}$$

  The resulting state is $|y_1, y_2\rangle$, i.e., the states of the two qubits have been swapped.

- Control and target of *CNOT* can be swapped by conjugating both qubits with H

  See Figure 6.

  Proof: see homework 2.

3 Universality of Gate Sets

3.1 Classical

The *NAND* gate is universal for classical computation. The *NAND* gate is the result of applying *NOT* to $aANDb = a \wedge b = a \uparrow b$. See Figure 7.

For any boolean function $\{0,1\}^n \longrightarrow \{0,1\}$, there is a circuit built of *NAND* gates (possibly with *FANOUT*= copy) for that function. Note that neither of these gates are reversible.

In general, the circuit may require an exponential number 2^n of gates. Functions which can be efficiently evaluated require only a polynomial number n^c gates. Complexity theory categorizes the scaling of the resources, esp. the number of gates, with the number of bits n. Provided the gate set is universal, the distinction between functions which require exponentially large circuits and those which can be computed with polynomial-size circuits does not depend on the chosen set of gates.

3.2 Quantum

A set G of quantum gates is called universal if for any $\varepsilon > 0$ and any unitary matrix U on n qubits, there is a sequence of gates $g_1, \ldots, g_l$ from G such that $\|U - U_{g_l} \cdots U_{g_2} U_{g_1}\| \leq \varepsilon$.

Here U_g is $V \otimes I$, where V is the unitary transformation on k qubits operated on by the quantum gate g, and I is the identity acting on the remaining $n-k$ qubits. The operator norm is defined by $\|U - U'\| = \max_{|v\rangle \text{unit vector}} \|(U - U')|v\rangle\|$. (Recall that for a vector w, $\|w\| = \sqrt{\langle w|w\rangle}$.)

Examples of universal gate sets include

- *CNOT* and all single qubit gates (continuous gates)
- *CNOT*, Hadamard, and suitable phase flips (continuous gates)
- *CNOT*, Hadamard, X and T $(\pi/8)$ (discrete gates)
- Toffoli and Hadamard (discrete gates)

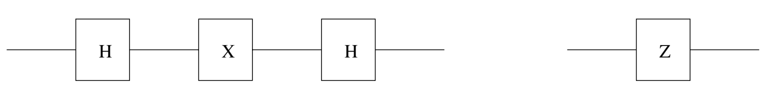


Figure 1: An X gate conjugated by H gates is a Z gate.

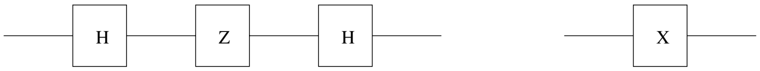


Figure 2: A Z gate conjugated by H gates is an X gate.

Inputs			Outputs		
a	b	c	a'	b'	c'
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0

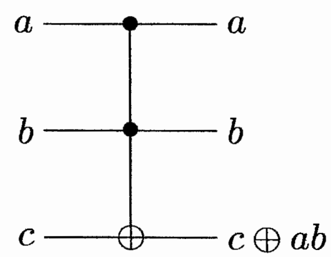


Figure 3: Toffoli gate, a 3-qubit double controlled NOT gate (bit c is flipped iff both a and b are 1.

4 Approximating Unitary Operators

Last time we defined a universal set of quantum gates. Now we consider the question of just how many gates are needed to effect an arbitrary quantum operation, or circuit?

An n-qubit gate U (a $2^n \times 2^n$ unitary matrix) has exponentially many parameters. So typically in general we need $\exp(n)$ many gates to even approximate U.

The Solovay-Kitaev theorem says that, as a function of ε, the complexity of an approximation is only $\log^2 \frac{1}{\varepsilon}$. This is rather efficient – the complexity as a function of n is the problem.

Quantum computation may be regarded as the study of those unitary transformations on n qubits that can be described by a sequence of polynomial in n quantum gates from a universal family of gates. U is "easy" (implementable) if $U \approx U_{g_k} \cdots U_{g_1}$ for $k = O(\text{poly}(n))$. This definition doesn't depend on our choice of a (finite) universal gate family, since any particular gate in one gate family can be well-approximated with a constant number of gates from another universal gate family. The constant factor does not affect the distinction between polynomial- and exponential-size circuits.

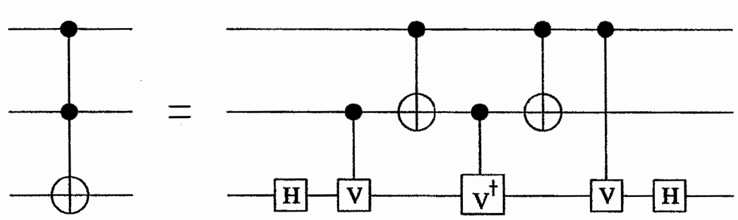


Figure 4: A Toffoli gate can be decomposed into a circuit of 1- and 2-qubit gates. Here $V = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} = R_z(\pi/2)$.

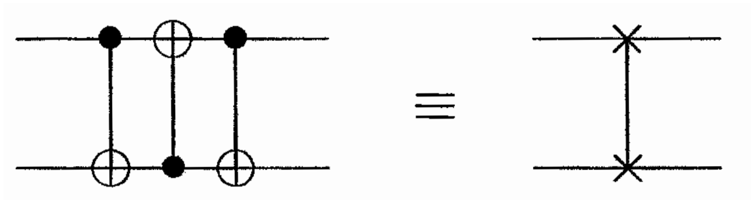


Figure 5: A *SWAP* gate is three back to back *CNOT* gates with control and target qubits alternating.

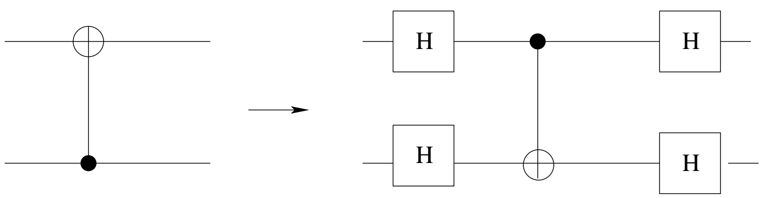


Figure 6: Control and target qubits of *CNOT* can be exchanged by conjugating with H on both qubits.

a	b	$a \uparrow b$
0	0	1
0	1	1
1	0	1
1	1	0

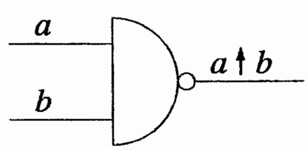


Figure 7: Classical NAND gate and its truth table.