Chapter 4: Quantum Circuits

John Martinez
john.r.martinez14@gmail.com

1 Quantum Circuits

1.1 Quantum Algorithms

What is a quantum computer good for? The promise of quantum computers is to enable new algorithms which render feasible problems requiring exorbiant resources for their solution on a classical computer.

1.2 Single Qubit Operations

Useful gates not mentioned yet:

$$T = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}; \quad S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$$

A few useful algebraic facts to keep in mind are that $H = \frac{(X+Z)}{\sqrt{2}}$ and $S = T^2$

The Pauli matrices give rise to three useful classes of unitary matrices when they are exponentiated, the *rotation operators* about the $\hat{x}$, $\hat{y}$, and $\hat{z}$ axes, defined by the equations:

$$R_x(\theta) \equiv e^{-i\theta X/2} = \begin{bmatrix} \cos\frac{\theta}{2} & -i\sin\frac{\theta}{2} \\ -i\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{bmatrix}$$

$$R_y(\theta) \equiv e^{-i\theta Y/2} = \begin{bmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{bmatrix}$$

$$R_z(\theta) \equiv e^{-i\theta Z/2} = \begin{bmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{bmatrix}$$

Theorem 4.1:

Suppose U is a unitary operation on a single qubit. Then $\exists \alpha, \beta, \gamma, \delta \in \mathbb{R}$ such that

$$U = e^{i\alpha} R_z(\beta) R_y(\gamma) R_z(\delta).$$

Proof

Since U is unitary, the rows and columns of U are orthonomal, from which it follow that $\exists \alpha, \beta, \gamma, \delta \in \mathbb{R}$ such that

$$U = \begin{bmatrix} e^{i(\alpha-\beta/2-\delta/2)}\cos(\gamma/2) & -e^{i(\alpha-\beta/2+\delta/2)}\sin(\gamma/2) \\ e^{i(\alpha+\beta/2-\delta/2)}\sin(\gamma/2) & e^{i(\alpha+\beta/2+\delta/2)}\cos(\gamma/2) \end{bmatrix}$$

The above equation follows immediately from the definition of the rotational matrices.

■

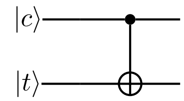
Preprint. Under review.

1.3 Controlled Operations

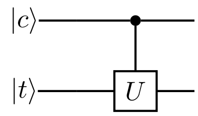
"If A is true, then do B". This is an example of a *controlled operation*.

A prototypical controlled operation is the controlled-NOT. The action of the $CNOT$ is given by $|c\rangle\,|t\rangle \rightarrow |c\rangle\,|t \oplus c\rangle$. The matrix representation of $CNOT$ is

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

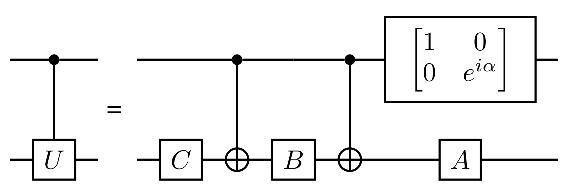


Suppose U is an arbitrary single qubit unitary operation. A *controlled-U* operation is a two qubit operation. That is, $|c\rangle\,|t\rangle \rightarrow |c\rangle\,U^c\,|t\rangle$

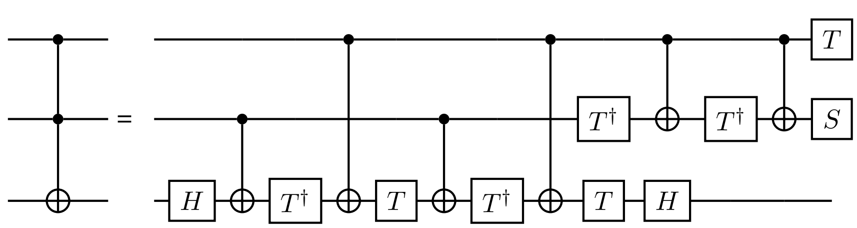


Our immediate goal is to understand how to implement the controlled-*U* operation for arbitrary single qubit U, using only single qubit operations and the *CNOT* gate. Our strategy is a two-part procedure based upon the decomposition $U = e^{i\alpha}AXBXC$ given in Corollary 4.2 on page 176.

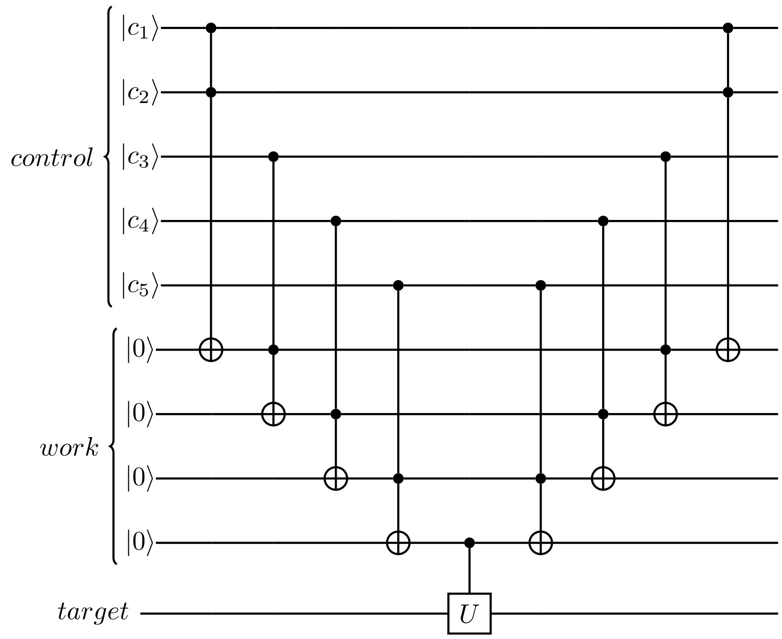
Corollary 4.2: Suppose U is a unitary gate on a single qubit. The there exists unitary operators, A, B, C on a single qubit such that $ABC = I$ and $U = e^{i\alpha}AXBXC$, where α is some overall phase factor.



Toffoli Gate



Network implementation of the $C^n(U)$ operation for the case $n = 5$.

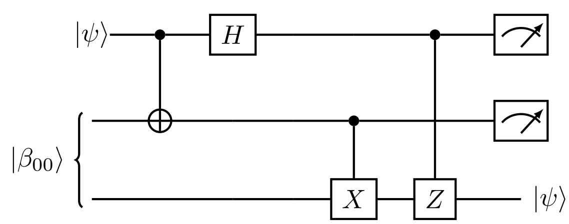


1.4 Measurement

There are two important principles that it is worth bearing in mind about quantum circuits.

Principle of deferred measurement: Measurements can always be moved from an intermediate stage of a quantum circuit to the end of the circuit; if the measurement results are used at any stage of the circuit, then the classically controlled operations can be replaced by conditional quantum operations.

Quantum Teleportation circuit



Principle of implicit measurement: Without loss of generality, any unterminated quantum wires (quibits which are not measured) at the end of a quantum circuit may be assumed to be measured.

1.5 Universal Quantum Gates

1.5.1 Two-Level Unitary Gates are Universal

Consider a Unitary matrix U which acts on a d-dimensional Hilbert space. U may be decomposed into a product of *two-level unitary matrices*. Suppose U has the form

$$U = \begin{bmatrix} a & d & g \\ b & e & h \\ c & f & j \end{bmatrix}$$

We will find two-level unitary matrices $U_1, \ldots, U_3$ such that

$$U_3 U_2 U_1 U = I.$$

It follows that

$$U = U_1^\dagger U_2^\dagger U_3^\dagger.$$

U_1, U_2, and U_3 are all two-level unitary matrices, and it is easy to see that their inverses, $U_1^\dagger$, $U_2^\dagger$, and $U_3^\dagger$ are also two-level unitary matrices.

1.5.2 Single Qubit and $CNOT$ Gates are Universal