Chapter 4

Quantum circuits

4.1 Single q-bit gates

A single q-bit in matrix notations is given by

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \alpha \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \beta \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \tag{4.1}$$

And the single q-bit gates are given by unitary 2x2 matrices such as

$$\begin{aligned}
\text{Pauli } X\text{matrix: } X &\equiv \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\
\text{Pauli } Y\text{matrix: } Y &\equiv \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \\
\text{Pauli } Z\text{matrix: } Z &\equiv \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \\
\text{Hadamard gate: } H &\equiv \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \\
\text{Phase gate: } S &\equiv \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} = e^{i\pi/4} \begin{pmatrix} e^{-i\pi/4} & 0 \\ 0 & e^{i\pi/4} \end{pmatrix} \\
\pi/8 \text{ gate : } T &\equiv \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix} = e^{i\pi/8} \begin{pmatrix} e^{-i\pi/8} & 0 \\ 0 & e^{i\pi/8} \end{pmatrix}
\end{aligned} \tag{4.2}$$

4.2 Bloch sphere

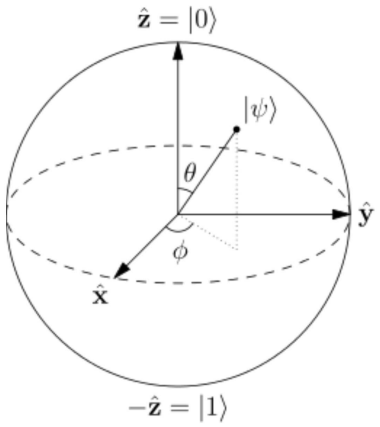
Consider the following parametrization of the state of a single q-bit

$$|\psi\rangle = e^{i\gamma} \left(\cos\frac{\theta}{2}|0\rangle + e^{i\varphi} \sin\frac{\theta}{2}|1\rangle \right) \tag{4.3}$$

with $\gamma \in [0, 2\pi), \varphi \in [0, 2\pi)$ and $\theta \in (0, \pi]$, where WLOG we can set $\gamma = 0$ since the overall phase in unobservable

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle. \tag{4.4}$$

Then the states of the q-bit are described by longitudinal φ and azimuthal θ angles on the so called Bloch sphere.



The Bloch sphere is S^2 which can be embedded in $\mathbb{R}^3$ using the following

map

$$f : (\phi, \theta) \to (\cos\phi \sin\theta, \sin\varphi \sin\theta, \cos\theta). \tag{4.5}$$

Then rotations of vectors on the Bloch sphere can be generated by Pauli matrices

$$R_x(\theta) \equiv e^{-i\theta X/2} = \cos\frac{\theta}{2} I - i \sin\frac{\theta}{2} X = \begin{pmatrix} \cos\frac{\theta}{2} & -i\sin\frac{\theta}{2} \\ -i\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix} \tag{4.6}$$

$$R_y(\theta) \equiv e^{-i\theta Y/2} = \cos\frac{\theta}{2} I - i \sin\frac{\theta}{2} Y = \begin{pmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix} \tag{4.7}$$

$$R_z(\theta) \equiv e^{-i\theta Z/2} = \cos\frac{\theta}{2} I - i \sin\frac{\theta}{2} Z = \begin{pmatrix} \exp\left(-i\frac{\theta}{2}\right) & 0 \\ 0 & \exp\left(i\frac{\theta}{2}\right) \end{pmatrix} \tag{4.8}$$

4.3 Decomposition of q-bit.

An arbitrary unitary operation on a single q-bit can be expressed as

$$U = e^{i\alpha} R_z(\beta) R_y(\gamma) R_z(\delta) \tag{4.9}$$

If we denote

$$A \equiv R_z(\beta) R_y(\gamma/2) \tag{4.10}$$

$$B \equiv R_y(-\gamma/2) R_z(-(\delta+\beta)/2) \tag{4.11}$$

$$C \equiv R_z((\delta-\beta)/2) \tag{4.12}$$

then

$$ABC = R_z(\beta) R_y(\gamma/2) R_y(-\gamma/2) R_z(-(\delta+\beta)/2) R_z((\delta-\beta)/2) = I \tag{4.13}$$

But since

$$X^2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I \tag{4.14}$$

$$XYX = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix} = -Y \tag{4.15}$$

$$XZX = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} = Z \tag{4.16}$$

we have

$$\begin{aligned} XBX &= XR_y(-\gamma/2) R_z(-(\delta+\beta)/2) X \\ &= XR_y(-\gamma/2) XX R_z(-(\delta+\beta)/2) X \\ &= XR_y(-\gamma/2) XX R_z(-(\delta+\beta)/2) X \\ &= R_y(\gamma/2) R_z((\delta+\beta)/2) \end{aligned} \tag{4.17}$$

and thus

$$\begin{aligned} AXBXC &= R_z(\beta)R_y(\gamma/2)R_y(\gamma/2)R_z((\delta+\beta)/2)R_z((\delta-\beta)/2) \\ &= R_z(\beta)R_y(\gamma)R_z(\delta) \end{aligned} \tag{4.18}$$

or from (4.9)

$$U = e^{i\alpha}AXBXC \tag{4.19}$$

where $ABC = I$.

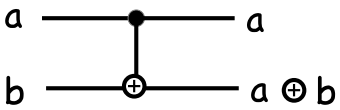
4.4 Controlled operations with a single bit

The controlled NOT gate (or CNOT gate) is given by

$$U_{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \tag{4.20}$$

such that

$$|a, b\rangle \rightarrow |a, a \oplus b\rangle \tag{4.21}$$



where $\oplus$ is sum module two. We can now generalize the CNOT to controlled U gate for arbitrary single q-bit unitary gate U using the decomposition of eq. (4.19). First let us define the Phase Shift gate (which generalizes $\pi/8$ (or T) and Phase (or S) gates)

$$\begin{pmatrix} 1 & 0 \\ 0 & e^{i\alpha} \end{pmatrix}$$

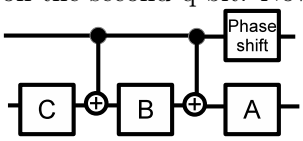
whose action on the first (or controlled) bit is given by

$$\begin{aligned} |00\rangle &\rightarrow |00\rangle \\ |01\rangle &\rightarrow |01\rangle \\ |10\rangle &\rightarrow e^{i\alpha}|10\rangle \\ |11\rangle &\rightarrow e^{i\alpha}|11\rangle. \end{aligned}$$

But this is equivalent to the controlled operation of gate

$$\begin{pmatrix} e^{i\alpha} & 0 \\ 0 & e^{i\alpha} \end{pmatrix}$$

on the second q-bit. Now it is easy to check that the following circuit



has the following action on the second bit

$$I = ABC \text{ if the first bit is 0}$$

or

$$U = e^{i\alpha} AXBXC \text{ if the first bit is 1.}$$

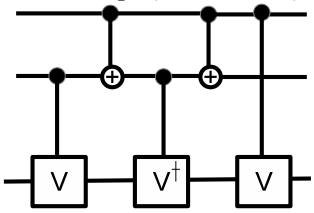
Note that the state of controlled bit was taken to be $|1\rangle$ when the unitary operation is preformed on the second q-bit, but (more generally) one may take the controlled state to be $|0\rangle$ or any other state of the first q-bit.

4.5 Controlled operations with multiple bits

More generically one could imagine controlled operations with multiple bits,

$$C^n(U)|x_1x_2x_3...x_n\rangle|\psi\rangle = |x_1x_2...x_n\rangle U^{x_1 \cdot x_2 \cdot x_3 \cdots x_n}|\psi\rangle.$$

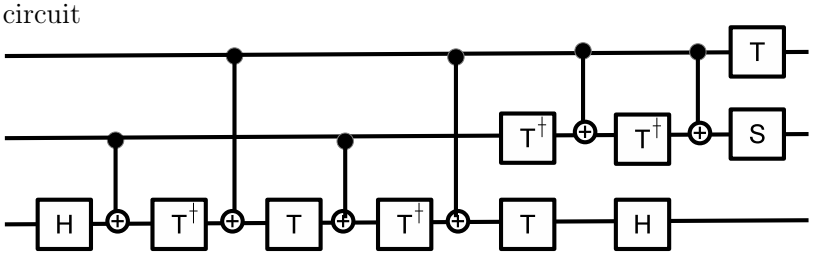
For example, if $V^2 = U$, then the following circuit is equivalent to $C^2(U)$



In a special case $C^2(U) = C^2(X)$, $V = (1+i)(I+iX)/2$ so that

$$V^2 = \frac{(1-i)^2 (I+iX)^2}{4} = \frac{(1-2i-1)(I+2iX-I)}{4} = X.$$

It turns out that arbitrary unitary operation to an arbitrary good approximation can composed of only Hadamard (H), phase (S), controlled-NOT and $\pi/8$ (T) gates. For example the Toffoli gate is given by the following circuit

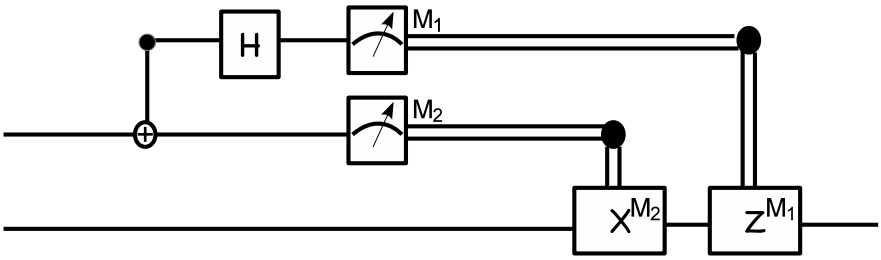


and using the Toffoli gate one can employ the so-called work bits to condition the unitary operation on an arbitrary number of control bits. How?

4.6 Measurement Principles

There are two important (but trivial) measurement principles which apply to any quantum circuit:

1. *Principle of deferred measurement. Measurement 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.*
   For example in the quantum teleportation circuit the measurement may be delayed until the very end. This would not change the overall action of the circuit on the q-bits, although the interpretation of teleportation would get lost.



   (a) *Principle of implicit measurement. Without loss of generality, any unterminated quantum wires (q-bits which are not measures) at the end of a quantum circuit may be assumed to be measured.*
   This is just a statement of the fact that the reduced density matrix (of any subset of q-bits) is insensitive to whether any other q-bits (which are not in the subset) were measured.

4.7 Universal Quantum Gates

One can show that an arbitrary unitary matrix U on a d- dimensional Hilbert space can be decomposed into a product of d two-level matrices (i.e. matrices acting non-trivially on only two or fewer components),

$$U = U_1 U_2 U_3 ... U_d.$$

Moreover any two-level unitary matrix acting on a space of n q-bits can be implemented using only single q-bit gates and $CNOT$ gates. These two results imply that single q-bit gates and $CNOT$ gates form a universal set of gates which can be used to compute arbitrary transformation.
Due to the continuum infinity of single-bit gates this universal set is still pretty large,

$$\{\text{All singe qbit gates }, CNOT\}$$

and one might wonder whether it is possible to approximate and arbitrary unitary transformation with only a finite set of gates such as

$$\{\text{Hadamard}, \text{Phase}, \pi/8, CNOT\}.$$

It is in fact possible to approximate and arbitrary unitary transformation with only these gates and the overhead is only polynomial (compared to the circuit from with arbitrary q-bit gates), but does depend on the desired precision. Of course the main problem is that the circuit representing a unitary transformation in a system of n q-bits generically requires an exponential number of gates. Why?