1 Basics of Quantum Computation (Week 1)

1.1 Quantum Bits

We start by defining the central mathematical object, *qubit* (quantum bit), analogous to classical bit. Just as classical bit has state 0 and 1, a qubit also has states $|0\rangle$ and $|1\rangle$. The difference between bits and qubits is that it is also possible to form linear combinations of states, called *superpositions*:

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$$

for $\alpha, \beta \in \mathbb{C}$ and $|\alpha|^2 + |\beta|^2 = 1$. We will often forgo that qubits are physical objects, and think of state of a qubit as a vector in $\mathbb{C}^2$ with $|0\rangle$ and $|1\rangle$ forming an orthonormal basis, also known as *computational basis states*

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \quad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}.$$

And the general state

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle = \begin{bmatrix} \alpha \\ 0 \end{bmatrix} + \begin{bmatrix} 0 \\ \beta \end{bmatrix} = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$$

An example of a single qubit state, that we will see often in the class, is $|+\rangle$ and $|-\rangle$ state.

$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \quad |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

A crucial difference between classical bit and quantum bit is in their measurements. We can examine a classical bit to determine whether it is in state 0 or 1. However, we can not examine a qubit to determine its quantum state , i.e. the values of α and β. When we measure a qubit, we get either the result 0 with probability $|\alpha|^2$, or results 1 with probability $|\beta|^2$. This is also referred to as Born rule.

1.2 Multiple Qubits

Suppose we have two qubits. Then, similar to classical bits, we will have 4 computational basis states $|00\rangle$, $|01\rangle$, $|10\rangle$ and $|11\rangle$. As an example, if we have two qubits: $|x\rangle = \alpha_0\,|0\rangle + \alpha_1\,|1\rangle$ and $|y\rangle = \beta_0\,|0\rangle + \beta_1\,|1\rangle$. Then, their joint state is given by their tensor product:

$$\begin{aligned} |x\rangle \otimes |y\rangle &= (\alpha_0\,|0\rangle + \alpha_1\,|1\rangle) \otimes (\beta_0\,|0\rangle + \beta_1\,|1\rangle) \\ &= \alpha_0\beta_0\,|0\rangle \otimes |0\rangle + \alpha_0\beta_1\,|0\rangle \otimes |1\rangle + \alpha_1\beta_0\,|1\rangle \otimes |0\rangle + \alpha_1\beta_1\,|1\rangle \otimes |1\rangle \end{aligned}$$

where we regard $|0\rangle \otimes |0\rangle$ as the computational state $|00\rangle$, etc.

$$|00\rangle = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} \quad |01\rangle = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} \quad |10\rangle = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} \quad |11\rangle = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}.$$

Couple of remarks are in order.

1. First, notice that tensor product is *not commutative*: for example $|0\rangle \otimes |1\rangle \neq |1\rangle \otimes |0\rangle$.

2. Another thing to keep in mind is that not all states in the multiple-qubit system are of tensor product form, namely product states. An important example of such a state is the Bell state or EPR pair,
$$\frac{|00\rangle + |11\rangle}{\sqrt{2}}.$$
Such states which can not be written in terms of a tensor product are called the *entangled states*. Later we will see many interesting properties associated to product and entangled states.

3. For n qubit system, a typical state is specified by 2^n amplitudes. For $n = 500$, 2^n is bigger than # of atoms in the universe. We can not even store these numbers in a classical computer, however, in principle, Nature manipulates such data, even for systems containing few hundred atoms.

1.3 Single Qubit Quantum Gates

Changes occurring to a quantum state can be described using the language of quantum computation. Analogous to classical computer, a quantum computer is built from quantum gates.

We start with examining single qubit gates. For a classical bit, the only non trivial single bit gate is NOT gate. The analogous quantum NOT gate (also called X-gate) is a *linear map* which maps state $|0\rangle$ to state $|1\rangle$, and state $|1\rangle$ to state $|0\rangle$.

Definition 1.1 (X gate)**.** *X gate acts on the computational basis as*
$$\begin{aligned} |0\rangle &\to |1\rangle \\ |1\rangle &\to |0\rangle \end{aligned}$$

A convenient way to represent the X-gate is by its matrix form:
$$X \stackrel{\mathsf{def}}{=} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

Using this, we can write action of X-gate on an arbitrary single qubit state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ as
$$|\psi\rangle \to X|\psi\rangle = \alpha|1\rangle + \beta|0\rangle$$

In a circuit diagram, this looks like
$$|\psi\rangle \;\; -\!\boxed{X}\!- \quad X|\psi\rangle$$

More generally, what properties does a linear map $U : \mathbb{C}^2 \to \mathbb{C}^2$ need to satisfy to be a valid quantum gate? The only restriction on U is that it must map quantum states to quantum states i.e. for $\langle\psi|\psi\rangle = 1$, U should satisfy

$$(U|\psi\rangle)^\dagger U|\psi\rangle = \langle\psi| U^\dagger U |\psi\rangle = 1$$

This enforces U to be unitary i.e. $U^\dagger U = I$, which is the only constraint!

So, unlike classical case (where only trivial gate is NOT gate), there are many non-trivial single qubit gates.

Definition 1.2 (Phase gate)**.** *Z gate acts on the computational basis as*

$$\begin{aligned} |0\rangle &\to |0\rangle \\ |1\rangle &\to -|1\rangle \end{aligned}$$

Observation 1.3 (Pauli Matrices)**.** *The matrices X, Z and $Y = -iZX$ together are known as Pauli Matrices. These matrices are observables:= i.e matrices O which are Hermitian and square to identity i.e. $O^2 = I$.*

Another important gate, Hadamard, transforms from X-basis to Z-basis.

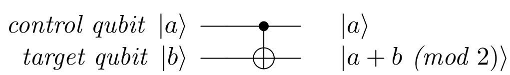
Definition 1.4 (Hadamard gate)**.** *H gate acts on the computational basis as*

$$\begin{aligned} |0\rangle &\to |+\rangle \\ |1\rangle &\to |-\rangle \end{aligned}$$

1.4 Multiple Qubit Quantum Gates

Unlike classical gates, unitary quantum gates are always invertible. For example, if we consider XOR gate: (for input A and B, outputs $A \oplus B$), we can not recover the inputs A and B, given its output: there is a loss of information. A typical 2-qubit gate is a CNOT gate, a generalization of the XOR gate.

Definition 1.5 (CNOT gate)**.** *CNOT gate is described as*



which acts on the computational basis as

$$\begin{aligned} |00\rangle &\to |00\rangle \\ |01\rangle &\to |01\rangle \\ |10\rangle &\to |11\rangle \\ |11\rangle &\to |10\rangle \end{aligned}$$

1.5 Quantum Measurement

We now describe what happens when an experimentalist and their equipment performs a measurement on the system. We first define quantum measurements.

Quantum measurements are described by a collection $\{M_m\}$ of measurement operators where the index m refers to the measurement outcomes. If the state of the quantum state is $|\psi\rangle$ immediately before the measurement, then the probability that result m occurs is given by

$$p(m) = \langle\psi| M_m^\dagger M_m |\psi\rangle \ ,$$

and the state of the system after the measurement is

$$\frac{M_m |\psi\rangle}{\sqrt{p(m)}} \, .$$

The measurement operators should satisfy the completeness equation

$$\sum_m M_m^\dagger M_m = I$$

which ensures that the outcome probabilities sum to 1

$$\sum_m p(m) = \sum_m \langle\psi| M_m^\dagger M_m |\psi\rangle = 1 \, .$$

Observation 1.6. *The following can be verified:*

1. *In general, M_m need not be Hermitian.*
2. *Non-orthogonal states can not reliably distinguished.*
3. *We can simulate measurement of a qubit in computational basis using*

$$M_0 = |0\rangle\langle 0| \, , \quad M_1 = |1\rangle\langle 1|$$

A subclass of measurements, namely projective measurements will be useful in measuring parity/syndromes for codewords.

Definition 1.7 (Projective measurements)**.** *Projective (or von Neumann) measurement is described by an observable, M, a Hermitian operator on the state space. The operator has a spectral decomposition:*

$$M = \sum_m m P_m$$

where P_m is the projector onto the eigenspace of M with eigenvalue m. Again, index m refers to the measurement outcome with probability $p(m) = \langle\psi| P_m |\psi\rangle$, and the state after outcome m is given by

$$\frac{P_m |\psi\rangle}{\sqrt{p(m)}}$$

Example 1.8 (Measurement of observable Z)**.** *Z has eigenvalue +1 and -1 with eigenvectors $|0\rangle$ and $|1\rangle$:*

$$P_{+1} = |0\rangle\langle 0| \, , P_{-1} = |1\rangle\langle 1| \, .$$