1 What is Quantum Computing

An Exciting Avenue

Almost 200 years ago an English mathematician Charles Babbage envisaged a general purpose computer, the technology required to implement the design was not available at the time, it took more than a 100 years to develope the technology and the astronomical development of classical computers does not need any explanation. It must be said that Quantum computing is at similar stage. However development is on a tremendous speed. The development of Quantum computers is going to transform into a practical and operational technology.

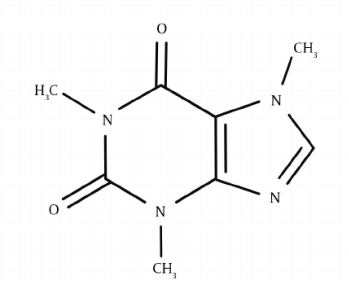
Classical Bits	Quantum Bits
Can be into two distinct states 0/1	Can be in state $\|0\rangle$ or $\|1\rangle$ or any linear combination of the two.
Can be measured	Can be measured partially
not changed by measurement	changed by measurements
can be copied	can not be copied
can be erased	can not be erased

In classical computer any n-bit number represents only one possible state out $2^n - 1$ possible states. However owing to super-position and entanglement any n-qubit system can represent all 2^n states at the same time. This implies that adding more qubit increases the number of possible states exponentially.

To double the power of a digital computer 32 bits $\rightarrow$ 64 bits, however to double the power of a quantum computer 32 qubits $\rightarrow$ 33 qubits.

64-bit computer can perform manipulation on 64-bit binary number at a time. However, a single 64-qubit quantum computer operates in a space of 2^{64} dimensions, or roughly $16,000,000,000,000,000,000$ i.e. (16×10^{18}) number of states of the quantum system. This makes it much easier to solve complex problem using quantum computers.

A single caffeine molecule is made up of 24 atoms and it can have 10^{48} quantum states (there are only 10^{50} atoms that make up our beloved planet Earth). Modeling caffeine precisely is simply not possible with with even the most powerful (classical) super computers. However this molecule may be simulated with the help of a quantum computer having as many as 160 qubits.



A Quantum Computer is a device that leverages specific properties described by quantum mechanics to perform computation.

Every classical (that is non-quantum) computer can be described by quantum mechanics since quantum mechanics is the basis of the physical universe. However, a classical computer does not take advantage of the physical properties and states that quantum mechanics affords us in doing calculation.

We will be using Dirac notation, linear algebra and other tool extensively.

A qubit is quantum bit. A qubit is similar to a classical bit in that it can take on 0 or 1 as states, but it differs from a bit in that it can also take on a continuous. In Quantum Mechanics (QM) we represent states as vectors and operators as matrices, use Dirac notation instead of traditional linear algebra symbols to represent vectors.

We can represent a qubit as a two dimensional complex Hilbert space $\mathbb{C}^2$. The state of the qubit at any given time can be represented by a vector in this complex Hilbert Space.

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad\qquad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

In short-hand notation $|0\rangle$ is called *ket zero* and $|1\rangle$ is called *ket one*. similarly, expressing the vector in row notation

$$\langle 0| = \begin{pmatrix} 1 & 0 \end{pmatrix} \qquad\qquad \langle 1| = \begin{pmatrix} 0 & 1 \end{pmatrix}$$

In short-hand notation $\langle 0|$ is called *bra zero* and $\langle 1|$ is called *bra one*. This Dirac notation is common known as *bra-ket* notation. A set of mathematical operations

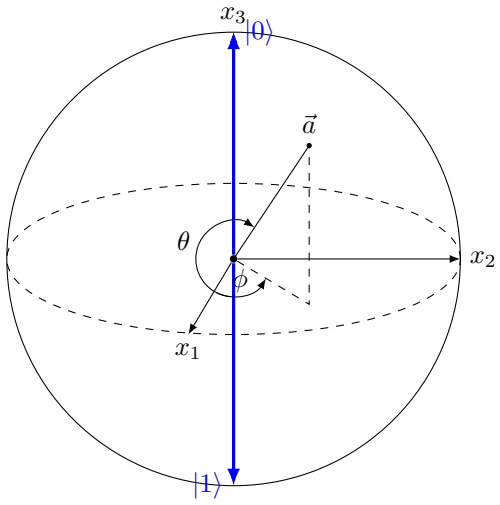
$$|0\rangle\langle 1| = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$
$$|1\rangle\langle 0| = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$$
$$|1\rangle\langle 1| = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$
$$|0\rangle\langle 1| + |1\rangle\langle 0| = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

2 Superposition of State

generally speaking

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

where α and $\beta \in \mathbb{C}$, with scaling factor of α and β the condition is fixed $\alpha^2 + \beta^2 = 1$.



We represent a superposition of the states as a linear combination of the computational bases of the state space. Each term in the superposition has a

complex coefficient or amplitude.

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$
$$|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

These two states differ by a minus sign on the $|1\rangle$ state.

3 Quantum Circuits

We use circuits to depict the quantum circuits. We construct and read these diagrams from left to right. A quantum circuit which specifies operators which we apply to which qubit or qubits in which order. We begin the construction of a quantum circuit diagrams with circuit wire which is represented as Initial

prepared state of the circuit is labels on the left

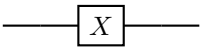
4 Quantum Operators

In this section we discuss the set of commonly used quantum operators. A quantum operator could be unary, binary or ternary operator.

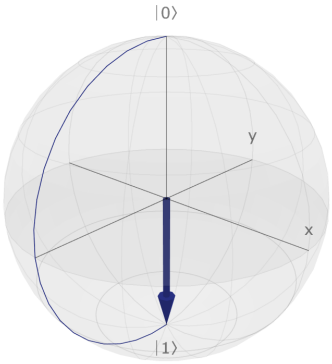
In the first section we cover the set of one-bit or unary quantum operators. The first three operators are known as Pauli's operators. These three matrices along with the identity matrix and all of their ± 1 and $\pm i$ multiples constitute what is known as Pauli group.

4.1 Pauli-X

This is the NOT operator (also known as bit flip operator).



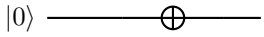
$$X := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$



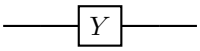
if we apply X to $|0\rangle$ then we have

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle$$

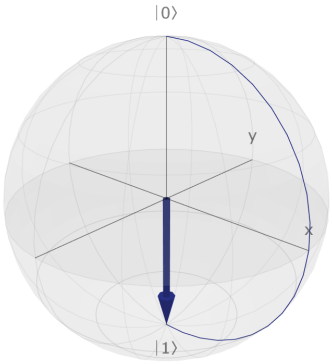
$$X := |0\rangle\langle 1| + |1\rangle\langle 0|$$



Next we have the Y operator, which rotates the state vector about y-axis The diagram for the Y operator is



$$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$



so that if we apply it to the $|1\rangle$ state we have

$$\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} -i \\ 0 \end{pmatrix} = -i|0\rangle$$

And the Z operator, which rotates the state vector about the $z-$axis (also called the phase flip operator since it flips it by π-radians or 180° degrees)

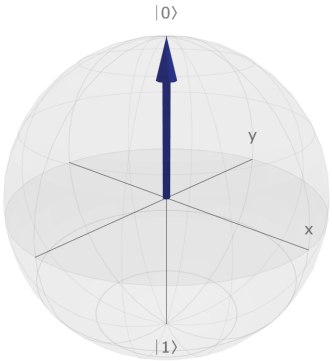
The diagram for the Z operator

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

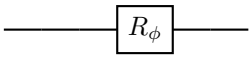
If we apply Z to the computational basis state we have

$$Z|j\rangle = (-1)^j|j\rangle$$

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ -1 \end{pmatrix} = -|1\rangle$$



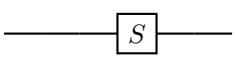
Note that we can multiply the bit-flip operator X by the phase-flip operator Z to yield the Y operator with global phase shift of i. i.e. $Y = iXZ$.
Pauli Z operator is just a special case of R_ϕ where $\phi = \pi$. Let's recall that $e^{i\pi} = -1$ by Euler's identity so we can replace $e^{i\pi}$ with -1 in the Z matrix. The circuit diagram for the R operator is



Two additional phase shift operator that are special cases of R_ϕ matrix. First, the S operator, where $\phi = \pi/2$

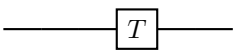
$$S := \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$$

The S operator thus rotates the state about the $z-$axis by $90°$. The circuit diagram for the S operator is



The T operator rotates the state about the $z-$axis by $45°$. If we give ϕ the value of $\pi/4$ then

$$T := \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{pmatrix}$$



4.2 Hadamard Operator

The operator is crucial is quantum computing since it enables us to take a qubit from a definite computational basis state into a superposition of two states. The Hadamard matrix

$$H := \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

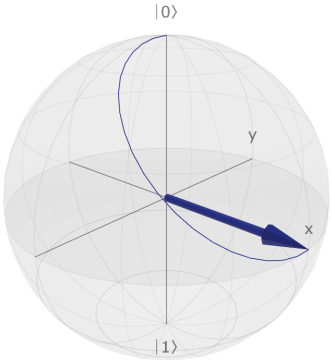
If we apply Hadamard to state $|0\rangle$ we obtain

$$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

and to state $|1\rangle$ we have

$$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

The diagram for the H operator is



The identity operator is simply the matrix which maintains the current state of qubits. So for one qubit we can use

$$I := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Having covered the set of unary opertors, we can show the following identities:

$$HXH = Z$$
$$HZH = X$$
$$HYH = -Y$$
$$H^\dagger = H$$
$$H^2 = I$$

5 Binary Operator

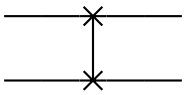
Consider two qubits, or binary operators. In a two-qubit systems, by convention, we use the following computational basis states:

$$|00\rangle = \begin{pmatrix}0\\0\\0\\0\end{pmatrix} |01\rangle = \begin{pmatrix}0\\1\\0\\0\end{pmatrix} \qquad |10\rangle = \begin{pmatrix}0\\0\\1\\0\end{pmatrix} |11\rangle = \begin{pmatrix}0\\0\\0\\1\end{pmatrix} \tag{1}$$

The swap operator takes the state $|01\rangle$ to $|10\rangle$ and of course $|10\rangle$ to $|01\rangle$. We can represent this operator with the following matrix.

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

When this operator is applied to one of the two-qubit computational basis vectors will have the desired results. For the circuit diagram of the SWAP operator



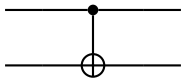
The most critical operator for quantum computing is the controlled Not Gate (CNOT) gate. The first qubit is identified as control bit and the second bit is identified as target qubit. If control qubit is in $|0\rangle$ state we do nothing to the target qubit. However, the control qubit is in state $|1\rangle$ we apply NOT gate operator (X) to the target qubit. We use CNOT gate to to entangle two qubits in QC. In matrix notation CNOT Gate is represented as

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

computation of CNOT on $|10\rangle$ would lead to $|11\rangle$

$$\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix} \begin{pmatrix}0\\0\\1\\0\end{pmatrix} = \begin{pmatrix}0\\0\\0\\1\end{pmatrix} = |11\rangle$$

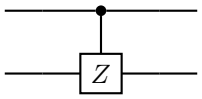
The circuit diagram for CNOT gate is illustrated as



The SWAP and CNOT gates are related as illustrated below

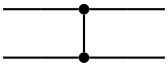
$$\text{SWAP} = \text{CNOT}_{ij}\text{CNOT}_{ji}\text{CNOT}_{ij}$$

CZ gate has a control bit and target bit just as CNOT, However, here if control bit is one we apply Z operator to the target bit



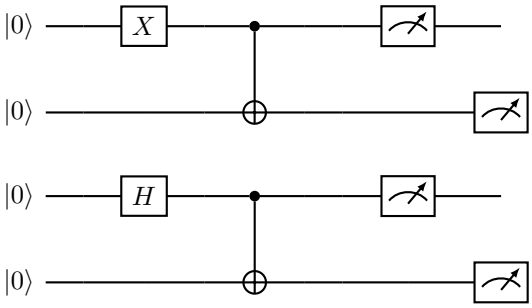
$$\text{CNOT} := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

The CZ operator is also illustrated as



Unlike CNOT operator, the CZ gate is symmetric, w can choose either qubit as the control or the target and end up with same result. That's why CZ gate has dots on both circuit wires.

5.1 Examples



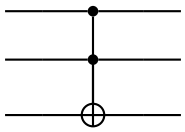
5.2 Ternary Operator

First Ternary or 3-qubit operator is the Toffoli operator commonly known as CCNOT gate. Just as with CNOT gate, we have control and target qubits. the

first two bits are control qubits and the third qubit is the target bit. When both control bits are in state $|1\rangle$ the target qubit is modified. This gates is similar to Boolean AND function

$$(x, y, z) \rightarrow (x, y, (z \oplus) xy)$$

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



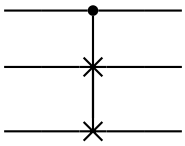
The Fredkin gate, also known as CSWAP gate has a control and two other target gates. If first qubit is in state $|0\rangle$ we do nothing and it is in state $|1\rangle$ we SWAP the other two qubits with each other. The matrix representation of this operation is

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

e.g. Fredkin gate applied to $|110\rangle$ gives

$$\text{CSWAP} := \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = |101\rangle$$

The Fredkin gate is illustrated as



6 Comparison with Classical Gates

In classical computing commonly used gates AND, NOT, OR, NAND, XOR, FANOUT etc. We can construct any complex logic with the combination of these gates. A classical computer that can run these gates is called Turing Complete or Universal. It can be shown that NAND gate alone is enough to construct all other classical gates (so is NOR gate). Neither AND, OR, XOR, NAND and FANOUT gates can be used in Quantum Computing. These gates are non-reversible. The Fan-out gate would not be allowed in quantum computing since it involves duplication or cloning of a state;

6.1 Universality of Quantum Operators

If NAND is universal for classical computing, there are several combination of unary and binary operators that lead to universality. Not set of unary and binary operators on their own can lead to universal QC. The two sets of gates that yield to universality are:

1. The Toffoli gate is universal for QC when paired with basis-changing unary operator with real coefficients (such as H).

2. Another set of gates which is universal is {CNOT, T and H}.

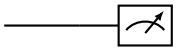
7 Measurement

Measurement in classical physics is seemingly straightforward process. The act of measurement is assumed to have no effect on the item that we are measuring. Furthermore, we have the ability to measure one property and be confident that the first property measured still retains its observed value. Not so in Quantum mechanics; in this regime, the act of measurement has a profound effect on the observation.
Building on the principles of quantum mechanics, we can state the measurement postulate as

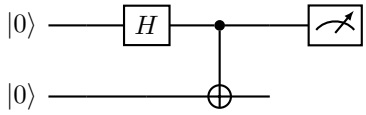
7.1 Measurement Postulate

Every measurable physical quantity o is described my corresponding Hermitian operator O, acting on the state Ψ. According to this postulate there exist an Hermitian operator, which we can call an observable $\hat{x}$ is associated with the position of a particle. We recall that a Hermitian operator is equal to its adjoint. If O is Hermitian then we can state that $O = O^{\dagger}$.
Hermitian operators have the desirable property that their eigenvalues are gauranteed to be real numbers. When measuring a physical system for properties outcome of the measurement.

The measurement in quantum circuit is represented as



A basic quantum circuit



Let we have two qubits $q0$ and $q1$, each prepare in state $|0\rangle$. Applying Hadamard operator to $q0$ which puts it into superposition states

$$|q0\rangle = \frac{1}{\sqrt{2}}|0\rangle + |1\rangle$$

As we apply CNOT across $q0$ and $q1$. This entangles the two qubits so we have the combined non separable state of the two qubits

$$\frac{1}{\sqrt{2}}|00\rangle + |11\rangle$$

This is called the Bell state or EPR pair. Wet then measure $q0$ with a 50/50 chance of finding a 0 or a 1 value for the real- valued output.