I

Quantum Computing Basics

Bra–Ket Notation

At fist we introduce some notations for quantum computing, this starts with notation for spin up and spin down here:

$$|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \quad \text{(spin up)}, \qquad |0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \quad \text{(spin down)}.$$

Each of these represents one qubit. Using $|1\rangle$ and $|0\rangle$ we can define single qubit superposition as:

$$\begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \end{bmatrix} + \frac{1}{\sqrt{2}} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}} \big(|0\rangle + |1\rangle \big).$$

Based on the same logic we can define higher dimensions for example, the computational basis for two qubits is:

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

which is equivalent to:

$$|00\rangle = |0\rangle{\otimes}|0\rangle\,, \quad |01\rangle = |0\rangle{\otimes}|1\rangle\,, \quad |10\rangle = |1\rangle{\otimes}|0\rangle\,, \quad |11\rangle = |1\rangle{\otimes}|1\rangle\,.$$

The above notion is a tensor product notion. One example of tensor product is:

$$|0\rangle \otimes |1\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} = |01\rangle\,.$$

This means we have two qubits: the first is in $|0\rangle$ and the second is in $|1\rangle$.

Similarly, we can have entanglement:

$$\begin{bmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ \frac{1}{\sqrt{2}} \end{bmatrix} = \frac{1}{\sqrt{2}}\big(|00\rangle + |11\rangle\big), \qquad \text{(superposition + entanglement).}$$

Classical Logic Gates (Truth Tables)

To better understand the Quantum gates, we start from the classical logic gates. Hence, we introduce the classical logic gates:

Buffer Buffer gate passes the same bit as is (this is a classical bit so the out put (Q) can be either 0 or 1. Depending on the input (A) for the Buffer gate, we get the same bit with no change:

A	Q
0	0
1	1

NOT NOT gate changes flips the 0 to 1, and 1 to 0:

A	Q
0	1
1	0

AND Gate AND is based on two inputs and one classical bit for output:

A	B	Q
0	0	0
0	1	0
1	0	0
1	1	1

OR Gate OR is also based on two inputs and one output:

A	B	Q
0	0	0
0	1	1
1	0	1
1	1	1

NAND Gate NAND is the flipped output of gate AND:

A	B	Q
0	0	1
0	1	1
1	0	1
1	1	0

Quantum Gates

Now, we focus our attention into the quantum gates,

Pauli-X (NOT): The Pauli matrix: $X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$, in practice performs the same logical flip as the classical NOT gate.

$$X\left|1\right\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \left|0\right\rangle, \tag{I.1}$$

$$X\left|0\right\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \left|1\right\rangle. \tag{I.2}$$

Pauli-Y

$$Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}. \tag{I.3}$$

Pauli-Z

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}. \tag{I.4}$$

Hadamard Hadamard is one the most important gates in quantum computing:

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}. \tag{I.5}$$

Hadamard makes superposition! For example, when it is applied into $\left|0\right\rangle$, the output becomes a superposition of $\left|0\right\rangle$ and $\left|1\right\rangle$:

$$H\left|0\right\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}} \left(\left|0\right\rangle + \left|1\right\rangle\right), \tag{I.6}$$

$$H\left|1\right\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix} = \frac{1}{\sqrt{2}} \left(\left|0\right\rangle - \left|1\right\rangle\right). \tag{I.7}$$

Conditional NOT (CNOT) Operates on two qubits, its matrix form is:

$$\text{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}. \tag{I.8}$$

Here is the operation of CNOT on $|01\rangle$:

$$\text{CNOT}\,|01\rangle = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} = |01\rangle\,. \tag{I.9}$$

Hence we have:

$$\text{CNOT}\,|00\rangle = |00\rangle\,, \qquad \text{CNOT}\,|01\rangle = |01\rangle\,, \tag{I.10}$$

$$\text{CNOT}\,|10\rangle = |11\rangle\,, \qquad \text{CNOT}\,|11\rangle = |10\rangle\,. \tag{I.11}$$

With out going through the computation also we can use the control logic which is, if the control (first bit) is 0, the target (second bit) remains unchanged, and if the control is 1, then the target will flip.

From Superposition to Entanglement (Hadamard + CNOT)

To demonstrate demonstrate how entanglement arises, we will build our first two-qubit entangled state: a Bell state. We begin by introducing a few basic circuit conventions. In Fig. I.1, the horizontal wires represent qubit lines in the circuit, and we initialize both qubits in the state $|0\rangle$.

Starting from the two-qubit state $|00\rangle$, we apply a Hadamard gate to the first qubit q_1. This creates the superposition state $|+\rangle$:

$$H\,|0\rangle = |+\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle + |1\rangle\big). \tag{I.12}$$

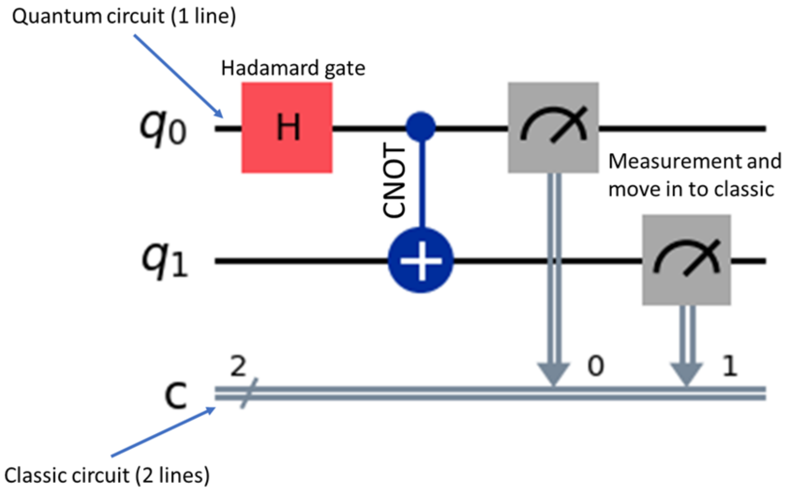

Figura I.1: Schematics of a quantum circuit that prepares a Bell state.

Including the second qubit (still in $|0\rangle$), the joint state becomes

$$\begin{aligned} |+\rangle \otimes |0\rangle &= \frac{1}{\sqrt{2}}\big(|0\rangle \otimes |0\rangle + |1\rangle \otimes |0\rangle\big) \\ &= \frac{1}{\sqrt{2}}\big(|00\rangle + |10\rangle\big). \end{aligned} \tag{I.13}$$

Next, we apply a CNOT gate with the first qubit as the control and the second as the target:

$$\mathrm{CNOT}\left[\frac{1}{\sqrt{2}}\big(|00\rangle + |10\rangle\big)\right] = \frac{1}{\sqrt{2}}\big(|00\rangle + |11\rangle\big). \tag{I.14}$$

Because CNOT flips the target qubit only when the control qubit is $|1\rangle$, the two basis states become correlated. The resulting state

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

is a maximally entangled Bell state: $|00\rangle$ and $|11\rangle$ occur with equal probability upon measurement. Once a measurement is performed (the measurement symbol is indicated in Fig. I.1), the quantum state collapses to one of these classical outcomes.

II
Quantum Phase Kickback and the Bernstein–Vazirani Algorithm

II.1 Phase Kickback Trick

The oracle acts as:

$$U_f \left|x\right\rangle \left|y\right\rangle = \left|x\right\rangle \otimes \left|y \oplus f(x)\right\rangle$$

We use the special state:

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

Applying the oracle:

$$\begin{aligned} U_f \left|x\right\rangle \left|-\right\rangle &= U_f \left(\left|x\right\rangle \otimes \frac{1}{\sqrt{2}} \left(\left|0\right\rangle - \left|1\right\rangle\right)\right) \\ &= \frac{1}{\sqrt{2}} \left(U_f \left|x\right\rangle \left|0\right\rangle - U_f \left|x\right\rangle \left|1\right\rangle\right) \end{aligned}$$

Now use:

$$U_f |x\rangle |0\rangle = |x\rangle |f(x)\rangle$$
$$U_f |x\rangle |1\rangle = |x\rangle |1 \oplus f(x)\rangle = |x\rangle |\overline{f(x)}\rangle$$

So:

$$\begin{aligned} U_f |x\rangle |-\rangle &= \frac{1}{\sqrt{2}} \Big(|x\rangle |f(x)\rangle - |x\rangle |\overline{f(x)}\rangle \Big) \\ &= |x\rangle \otimes \frac{1}{\sqrt{2}} \Big(|f(x)\rangle - |\overline{f(x)}\rangle \Big) \end{aligned}$$

Consider two cases:

- If $f(x) = 0$, then

$$U_f |x\rangle |-\rangle = |x\rangle |-\rangle$$

- If $f(x) = 1$, then

$$U_f |x\rangle |-\rangle = -|x\rangle |-\rangle$$

Conclusion:

$$U_f |x\rangle |-\rangle = (-1)^{f(x)} |x\rangle |-\rangle$$

—

II.2 Hadamard Operator

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

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

For a general qubit:

$$H|x\rangle = \frac{1}{\sqrt{2}} \sum_{y \in \{0,1\}} (-1)^{x \cdot y} |y\rangle$$

So:

$$H = \frac{1}{\sqrt{2}} \sum_{x,y \in \{0,1\}} (-1)^{x \cdot y} |y\rangle \langle x|$$

Tensor product form:

$$H^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{x,y \in \{0,1\}^n} (-1)^{x \cdot y} |y\rangle \langle x|$$

Example:

$$H^{\otimes n} |0\rangle = \frac{1}{\sqrt{2^n}} \sum_{z \in \{0,1\}^n} |z\rangle$$

Applying $H^{\otimes n}$ again:

$$H^{\otimes n} \left(\frac{1}{\sqrt{2^n}} \sum_{z} |z\rangle \right) = |0\rangle$$

$$H^{\otimes n} H^{\otimes n} = I \quad \Rightarrow \quad \text{Applying twice returns original state.}$$

—

II.3 Bernstein–Vazirani Algorithm

Let:

$$f(x) = s \cdot x \quad \text{where } s \in \{0,1\}^n$$

The oracle is:

$$U_f = \sum_{x,y} |x\rangle \langle x| \otimes |y \oplus f(x)\rangle \langle y|$$

Apply it to:

$$U_f\left(|x\rangle \otimes |-\rangle\right) = (-1)^{f(x)} |x\rangle |-\rangle$$

After phase kickback, we get:

$$|\psi_s\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (-1)^{x\cdot s} |x\rangle$$

Apply Hadamard:

$$H^{\otimes n} |\psi_s\rangle = |s\rangle$$

—

II.4 Why Is This Correct?

Start with:

$$H^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{x,y} (-1)^{x\cdot y} |y\rangle \langle x|$$

And:

$$|\psi_s\rangle = \frac{1}{\sqrt{2^n}} \sum_{x} (-1)^{x\cdot s} |x\rangle$$

Apply $H^{\otimes n}$:

$$H^{\otimes n} |\psi_s\rangle = \frac{1}{2^n} \sum_{y} \left(\sum_{x} (-1)^{x\cdot(y\oplus s)} \right) |y\rangle$$

Inner sum:

$$\sum_{x} (-1)^{x\cdot(y\oplus s)} = \begin{cases} 2^n & \text{if } y = s \\ 0 & \text{otherwise} \end{cases}$$

Final result:

$$H^{\otimes n} |\psi_s\rangle = |s\rangle$$

Hence, the complete secret string s is revealed.

III
Quantum Phase Estimation

To understand Quantum Phase Estimation (QPE), we begin by recalling the Quantum Fourier Transform (QFT), defined as:

$$|x\rangle \to \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} \omega_N^{-xy} |y\rangle \quad \text{with } \omega_N = e^{2\pi i/N}$$

Its inverse transformation can be written as:

$$\frac{1}{\sqrt{N}} \sum_{y} \omega_N^{xy} |y\rangle \to |x\rangle$$

QFT generalizes the idea of phase kickback. Unlike classical Boolean logic where operations may flip a sign (e.g., ± 1), QFT introduces more nuanced phase rotations—complex roots of unity:

$$e^{2\pi ik/N}$$

These values represent points on the unit circle in the complex plane. This enables fine-grained phase encoding, which is central to QPE.

If a unitary operator U has an eigenvector $|\psi\rangle$ with eigenvalue $e^{2\pi i\phi}$, then QPE enables the estimation of ϕ.

Although we cannot measure the phase directly, we can induce a phase kickback using controlled applications of powers of U and then apply QFT to extract ϕ into measurable qubits.

Suppose we can prepare an eigenstate $|\psi\rangle$ of a unitary U and apply controlled-U^{2^j} gates. If

$$U|\psi\rangle = e^{2\pi i\phi}|\psi\rangle \quad \Rightarrow \quad U^{2^j}|\psi\rangle = e^{2\pi i\cdot 2^j\phi}|\psi\rangle$$

then controlled unitaries act as:

$$CU(|0\rangle \otimes |\psi\rangle) = |0\rangle \otimes |\psi\rangle, \quad CU(|1\rangle \otimes |\psi\rangle) = |1\rangle \otimes U|\psi\rangle$$

Starting with the superposition state:

$$|\text{init}\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |\psi\rangle$$

After applying the controlled-U:

$$\frac{1}{\sqrt{2}}\left(|0\rangle \otimes |\psi\rangle + |1\rangle \otimes e^{2\pi i\phi}|\psi\rangle\right) = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i\phi}|1\rangle\right) \otimes |\psi\rangle$$

Extending to n control qubits, the combined state becomes:

$$\frac{1}{\sqrt{2^n}}\bigotimes_{j=0}^{n-1}\left(|0\rangle + e^{2\pi i\cdot 2^{n-1-j}\phi}|1\rangle\right) \tag{III.1}$$

This encodes the binary representation of ϕ through relative phases of the qubit states.

Recall the binary expansion:

$$\phi = 0.\phi_1\phi_2\ldots\phi_n = \frac{\phi_1}{2} + \frac{\phi_2}{4} + \cdots + \frac{\phi_n}{2^n}$$

Each control qubit accumulates phase based on the significance of its bit: the highest qubit collects the most significant part of ϕ.

If ϕ has an exact n-bit binary representation, then applying the inverse QFT yields:

$$|\Psi\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} e^{2\pi i \phi x} |x\rangle \quad \xrightarrow{\text{QFT}^{-1}} \quad |y\rangle \quad \text{where } y = 2^n \cdot \phi$$

Applying inverse QFT explicitly:

$$\text{QFT}^{-1} \left(\sum_{x=0}^{2^n-1} e^{2\pi i \phi x} |x\rangle \right) = \sum_{x=0}^{2^n-1} e^{2\pi i \phi x} \cdot \text{QFT}^{-1} |x\rangle$$

$$\text{QFT}^{-1} |x\rangle = \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} e^{-2\pi i x y / 2^n} |y\rangle$$

$$\Rightarrow \text{QFT}^{-1} |\Psi\rangle = \frac{1}{2^n} \sum_{y=0}^{2^n-1} \left(\sum_{x=0}^{2^n-1} e^{2\pi i x (\phi - y/2^n)} \right) |y\rangle$$

Thus, the amplitude for outcome y is:

$$A(y) = \frac{1}{2^n} \sum_{x=0}^{2^n-1} e^{2\pi i x (\phi - y/2^n)} \quad \Rightarrow \quad P(y) = |A(y)|^2$$

This means that $P(y)$ is maximized when $\frac{y}{2^n}$ is close to ϕ.

Define the phase error as:

$$\delta = \phi - \frac{y}{2^n} \quad \text{so that} \quad r = e^{2\pi i \delta}$$

We use the geometric series identity:

$$\sum_{x=0}^{2^n-1} r^x = \frac{1 - r^{2^n}}{1 - r} \quad \Rightarrow \quad P(y) = \left| \frac{1 - r^{2^n}}{2^n (1 - r)} \right|^2$$

When $\phi = \frac{y}{2^n}$ exactly, then $r = 1$ and $P(y) = 1$.
If not exact but close, we can show:

$$P(y) \geq \frac{4}{\pi^2} \approx 0.405$$

This guarantees a minimum of 40%.