Quantum Computation and Quantum Information by Michael A. Nielsen and Isaac L. Chuang

Chris Doble

May 2024

Contents

Part I

Fundamental concepts

1 Introduction and overview

1.2 Quantum bits

- The special states $|0\rangle$ and $|1\rangle$ form an orthonormal basis and are known as **computational basis states**.
- A quantum bit (**qubit**) is a linear combination of the computational basis states

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

  where α and β are complex numbers.
- When we measure a qubit we either get $|0\rangle$ with probability $|\alpha|^2$ or $|1\rangle$ with probability $|\beta|^2$. Thus, $|\alpha|^2 + |\beta|^2 = 1$ and a qubit can be thought of as a unit vector in a two-dimensional complex vector space.

- If a qubit is in the state

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

there's a 50/50 chance of measuring $|0\rangle$ or $|1\rangle$.

- If we let

$$\alpha = e^{i\gamma} \cos\frac{\theta}{2}$$

and

$$\beta = e^{i\gamma} e^{i\varphi} \sin\frac{\theta}{2}$$

then

$$\begin{aligned} |\alpha|^2 + |\beta|^2 &= \alpha^* \alpha + \beta^* \beta \\ &= \cos^2\frac{\theta}{2} + \sin^2\frac{\theta}{2} \\ &= 1 \end{aligned}$$

so the qubit is still normalised and it can be written

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

It turns out that $e^{i\gamma}$ has no observable effects and we can effectively write

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

This defines a point on a three-dimensional sphere known as the **Bloch sphere** where θ and φ take on their usual roles in a spherical coordinate system.

- Before measurement a qubit is in a linear combination of $|0\rangle$ and $|1\rangle$ but when measured you get one or the other and the state of the system changes to match the measured result.

1.2.1 Multiple Bits

- A two qubit system has four computational basis state $|00\rangle$, $|01\rangle$, $|10\rangle$, and $|11\rangle$ so the general expression for the state of such a system is

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle.$$

- If you were to measure the first qubit, you would get $|0\rangle$ with probability $|\alpha_{00}|^2 + |\alpha_{01}|^2$ and the system would be left in the state

$$|\psi\rangle = \frac{\alpha_{00}|00\rangle + \alpha_{01}|01\rangle}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}},$$

i.e. it is renormalised such that the normalisation condition still holds.

1.3 Quantum Computation

1.3.1 Single Qubit Gates

- The quantum NOT changes $|0\rangle$ to $|1\rangle$ and $|1\rangle$ to $|0\rangle$. It acts linearly on superpositions of those states, i.e. it turns $\alpha\,|0\rangle + \beta\,|1\rangle$ into $\beta\,|0\rangle + \alpha\,|1\rangle$. If a quantum state $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ is written in vector notation as

  $$|\psi\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$$

  then the quantum NOT gate can be expressed in matrix form as

  $$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

- In order to preserve the normalisation condition, matrix representations of quantum gates must be unitary, i.e. $M^\dagger M = I$ where I is the identity matrix.

- An arbitrary unitary 2x2 matrix can be decomposed into a finite set of other 2x2 matrices. This means an arbitrary single qubit gate can be generated by a finite set of other gates.