Quantum Computing and Quantum Information

Pradipta Parag Bora

April 2020

Contents

1 Introduction

Through this Summer of Science report, I attempt to summarise everything I covered related to Quantum Computing and Quantum Information Theory. We will mainly follow the book **Quantum Computation and Quantum Information** by **Nielsen and Chuang**. We will begin by going through the mathematical preliminaries, including an introduction to the linear algebraic treatment of Quantum Mechanics through which we will explore Quantum Computation. Then we will move onto qubits, their representation and on the way we will study and go through various fascinating Quantum algorithms and their uses. Hopefully through this report one will be able to gain a decent understanding of Quantum Computation.

2 Mathematical Preliminaries

We assume that the reader is familiar with basic linear algebra that is covered during the first year. As our treatment of Quantum Computation heavily uses this, we will summarise some key theorems and notations that we will be using.

2.1 Vectors and Vector Spaces

The most important structure in linear algebra is a vector which we will represent as $|\psi\rangle$. This vector resides in a vector space that satisfies some axioms that give this structure it's core defining properties. This is famously known as the *bra-ket* notation and the $|.\rangle$ is used to represent a vector. The same vector in the vector space $\mathbf{C}^n$ is conveniently represented as a column vector.

We will be generally working in the vector space $\mathbf{C}^n$ over the field $\mathbf{C}$. A set of vectors $|\psi_1\rangle, |\psi_2\rangle \cdots |\psi_n\rangle$ is said to be *linearly-independent* if for any set of coefficients a_i,

$$\sum_{i=1}^{n} a_i |\psi_i\rangle = 0 \implies a_i = 0 \forall 1 \leq i \leq n$$

A set of vectors $|\psi_i\rangle$ is said to be a spanning set of a vector space $\mathbf{W}$ if any vector in $\mathbf{W}$ can be represented as a linear combination of that set. Note that such a set may be non-finite however we will be dealing with finite dimensional vector spaces only. If this set is linearly independent then this set is called a *basis* of that vector space. It is left as an exercise to show that the cardinality of all bases are same and this value is termed as the *dimension* of that vector space.

2.2 Linear Operators and Matrices

A linear operator A from vector space $\mathbf{V}$ to $\mathbf{W}$ is a function mapping vectors from $\mathbf{V}$ to $\mathbf{W}$ satisfying linearity, that is:

$$A(\sum_i a_i \,|\psi_i\rangle) = \sum_i a_i A \,|\psi_i\rangle$$

We can then define compositions of operators, BA as function that first operates A and then operates B.

It is easy to see that matrix multiplication is a linear operator. Conversely any linear operator has a matrix representation. To see this, let $A : V -> W$ be a linear operator. Let $|v_i\rangle$ be an ordered basis (basis formed by fixing order of it's elements, in this case by enforcing an order restriction on $|v_i\rangle$.) of V and $|w_j\rangle$ be an ordered basis of W.

Then there exists complex numbers $A_{i,j}$ such that:

$$A \,|v_i\rangle = \sum_j A_{i,j} \,|w_j\rangle$$

. If we represent any vector in V by it's coordinate vector representation, that is form a column vector whose elements with respect to an ordered basis are the scalar coefficients along the basis elements and multiply it by the matrix formed by $A_{i,j}$ we get the coordinate vector representation of the output vector in the ordered basis $|w_j\rangle$.

2.3 Inner Products

An inner product of a vector space $\mathbf{V}$ is defined as a function from $\mathbf{V} \times \mathbf{V}$ to $\mathbf{C}$. We will denote the inner product of $|v\rangle$ and $|w\rangle$ as $(|v\rangle , |w\rangle)$ or as $\langle v|w\rangle$. The inner product satisfies the following properties:

1. $\langle v|w\rangle = (\langle w|v\rangle)^*$

2. $\left\langle v \Big| \sum_j a_j w_j \right\rangle = \sum_j a_j \langle v|w_j\rangle$

3. $\langle v|v\rangle \geq 0$ with equality *iff* $v = 0$

We can now define the *length* or *norm* of a vector $\||v\rangle\| = \sqrt{\langle v|v\rangle}$. Two vectors are said to be orthogonal if their inner product is 0. We now define an *orthonormal* basis as a basis $|v_i\rangle$ whose elements have unit norm and they are pairwise orthogonal, that is for $i \neq j$ $\langle v_i|v_j\rangle = 0$. It can be proven that every finite dimensional vector space has an orthonormal basis. This is left as an exercise. The procedure for determining this orthonormal set from any basis is termed as the *Gram-Schmidt* orthogonalisation process.