Notes on An Introduction to Quantum Computing

Adith Tom Alex

January 28, 2025

1 Citation

Phillip Kaye, Raymond Laflamme, Michele Mosca. 2007. *An Introduction to Quantum Computing.*

2 Keywords

Quantum Computing; Computer Architecture; Circuit Design

3 Goals

- Learn the basics of quantum computers

- Learn the basic mathematical background of quantum mechanics

- Learn how to simulate and put together qubits and circuits

1 Introduction and Background

Two measures of complexity of a computation: time and space.

The Church–Turing Thesis says that a computing problem can be solved on any computer that we could hope to build, if and only if it can be solved on a very simple 'machine', named a Turing machine. The Turing machine is a mathematical abstraction. The very term *computable* corresponds to what can be computed by a Turing machine.

A probabilistic Turing machine is one capable of making a random binary choice at each step, where the state transition rules are expanded to account for these random bits. There are some important problems that we know how to solve efficiently using a probabilistic Turing machine, but do not know how to solve efficiently using a conventional Turing machine.

(Classical) Strong Church–Turing Thesis: *A probabilistic Turing machine can efficiently simulate any realistic model of computation.*

Quantum Strong Church–Turing Thesis: *A quantum Turing machine can efficiently simulate any realistic model of computation.*

Another useful model of computation is that of a uniform families of reversible circuits. A family of circuits is a set of circuits $\{C_n \mid n \in \mathbb{Z}^+\}$, one circuit for each input size n.

Def 1. *A set of gates is universal for classical computation if, for any positive integers n, m, and function $f : \{0,1\}^n \rightarrow \{0,1\}^m$, a circuit can be constructed for computing f using only gates from that set.*

Three measures of complexity of a computation can be used for the circuit model.
- Depth: The total number of time slices in circuit C_n.
- Width: The total number of bits or adjacent wires (analogous to space).
- Total number of gates.

1.1 Linear Algebraic Formulation of the Circuit Model

We can summarize the information in a bit by a 2-dimensional vector of probabilities such that it is in state 0 with probability p_0 and in state 1 with probability p_1. This description can also be used for deterministic circuits. A wire in a deterministic circuit whose state is 0 could be specified by the probabilities $p_0 = 1$ and $p_1 = 0$.

Similarly, we would be able to represent gates in the circuit by operators that take the form of matrices.

$$\text{NOT} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \quad \text{NOT} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \tag{1}$$

This implies that we can represent the *NOT* operator as

$$\text{NOT} \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \text{NOT} \begin{pmatrix} p_0 \\ p_1 \end{pmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{pmatrix} p_1 \\ p_0 \end{pmatrix} \tag{2}$$

To describe the state associated with a given point in a probabilistic circuit having two wires we can use a 4-dimensional vector of probabilities. The four possibilities for the combined state of both wires at the given point are 00,01,10,11 (where the binary string ij indicates that the first wire is in state i and the second wire in state j). The probabilities of each of these four states can be obtained by multiplying the corresponding probabilities: $\text{prob}(ij) = p_i q_j$ and the 4D vector will be:

$$\begin{pmatrix} p_0 q_0 \\ p_0 q_1 \\ p_1 q_0 \\ p_1 q_1 \end{pmatrix} \tag{3}$$

This is the tensor product of the 2D state vectors of the first and second wires separately.

We can also represent gates acting on more than one wire. For example, the controlled-not gate, denoted CNOT. The reversible CNOT gate flips the value of the target bit t if and only if the control bit c has value 1. The CNOT gate can be represented by the matrix:

$$\text{CNOT} \equiv \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \tag{4}$$

1.2 Reversible Computation

A computation is reversible if it is always possible to uniquely recover the input, given the output. Each gate in a finite family of gates can be made reversible by adding some additional input and output wires if necessary.

Note that the reversible AND gate is a generalization of the CNOT gate (the CNOT gate is reversible), where there are two bits controlling whether the not is applied to the third bit.

In general, given an implementation (not necessarily reversible) of a function f, we can easily describe a reversible implementation of the form:

$$(x, c) \mapsto (x, c \oplus f(x)) \tag{5}$$

1.3 A Preview of Quantum Physics

The quantum mechanical behaviour of microscopic particles be illustrated by a simple experiment.

Simple Beam Splitter: Photon source, beam splitter, two photon detectors. Here the beam splitter acts like a fair coin flipper and the photon arrives at each photon detector 50% of the time.

Modified Experiment (Two Beam Splitters): Added two mirrors and an additional beam splitter as per figure. Contradictory to classical intuition, the photons arrive at one detector 100% of the time.
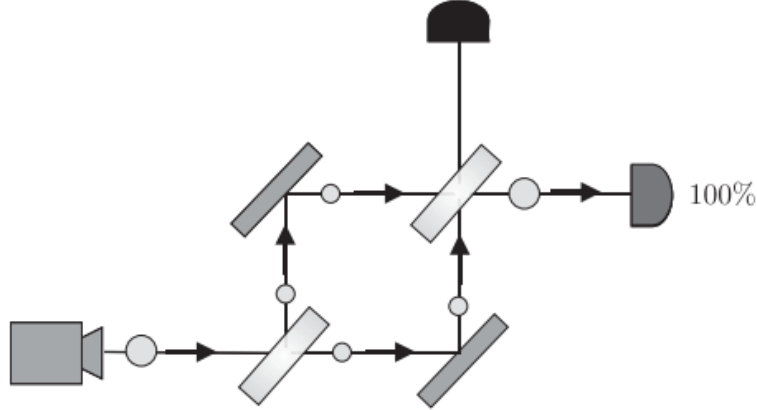

Figure 1: Two beam splitter experiment

To understand this, we will consider the photon in this apparatus as a two state system. These states are represented by the paths they follow in the figures 2 and 3.
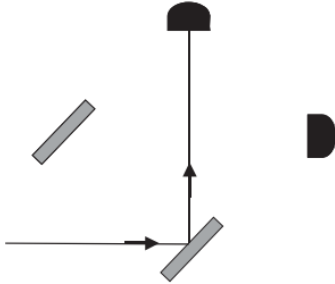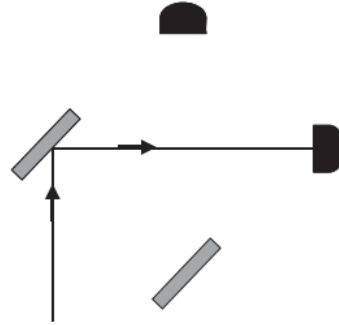

Figure 2: Path 0

Figure 3: Path 1

According to the quantum mechanical description, the first beam splitter causes the photon to go into a superposition of taking both the '0' and '1' paths. Mathematically, we describe such a superposition by taking a linear combination of the state vectors for the '0' and '1' paths, so the general path state will be described by the vector:

$$\alpha_0 \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \alpha_1 \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix} \tag{6}$$

If we were to physically measure the photon to see which path it is in, we will find it in path '0' with probability $|\alpha_0|^2$, and in path '1' with probability $|\alpha_1|^2$. Since we should find the photon in exactly one path, we must have $\alpha_0|^2 + |\alpha_1|^2 = 1$.

When the photon passes through the beam splitter, we multiply its **state vector** by the matrix:

$$\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & i \\ i & 1 \end{bmatrix} \tag{7}$$

So for the photon starting out in path '0', after passing through the first beam splitter it comes out in state:

$$\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & i \\ i & 1 \end{bmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ i \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \frac{i}{\sqrt{2}} \begin{pmatrix} 0 \\ 1 \end{pmatrix} \tag{8}$$

If we measure the photon after passing through the first splitter, we find to the path 0 to have a probability of

$$\left| \frac{1}{\sqrt{2}} \right|^2 = \frac{1}{2},$$

and path '1' with probability:

$$\left| \frac{i}{\sqrt{2}} \right|^2 = \frac{1}{2}.$$

However, if we do not take the measurement, the photon remains in a state of superposition represented as:

$$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ i \end{pmatrix} \tag{9}$$

Now if the photon is allowed to pass through the second beam splitter (before making any measurement of the photon's path), its new state vector is

$$\left(\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & i \\ i & 1 \end{bmatrix} \right) \left(\frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ i \end{bmatrix} \right) = \begin{bmatrix} 0 \\ i \end{bmatrix} \tag{10}$$

Now if we measure the probabilities along paths 0 and 1, which is what the detector is doing, the probability along path 0 will be 0 and the probability along path 1 will be $|i|^2 = 1$. In the language of quantum mechanics, the second beam splitter has caused the two paths (in superposition) to interfere, resulting in cancellation of the '0' path.

2 Linear Algebra and The Dirac Notation

2.1 The Dirac Notation and Hilbert Spaces

In the Dirac notation, the symbol identifying a vector is written inside a 'ket', and looks like $|a\rangle$. We denote the dual vector for a (defined later) with a 'bra', written as $\langle a|$. Then inner products will be written as 'bra-kets' (e.g., $\langle a|b\rangle$).

Hilbert spaces are finite-dimensional and over complex numbers denoted by $\mathcal{H}$. Since $\mathcal{H}$ is finite-dimensional, we can choose a basis and alternatively represent vectors (kets) in this basis as finite column vectors, and represent operators with finite matrices.

The Hilbert spaces of interest for quantum computing will typically have dimension 2^n. The standard way to associate column vectors corresponding to these basis vectors is as follows:

$$|00\ldots00\rangle \iff \left.\begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}\right\}2^n, \quad |00\ldots01\rangle \iff \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \quad \ldots$$

$$\ldots, \quad |11\ldots10\rangle \iff \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 1 \\ 0 \end{pmatrix}, \quad |11\ldots11\rangle \iff \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix} \quad (11)$$

An arbitrary vector in can be written either as a weighted sum of the basis vectors in the Dirac notation, or as a single column matrix.

3   Further Reading

List papers cited by "Paper"

4   Bibliography

List papers not cited by "Paper" that inform your understanding of the work.