Quantum Computing

Pietro Garofalo
Jasmine Amani Murphy

August 31, 2023

Todo list

Contents

Introduction

Hi everyone, this work is a simple collection of notes taken during the Womanium Global Quantum program, our goal is to try to share as much as possible what we learned during the course and not only : the document is open-source so anyone can participate in the writing or just correct any mistakes, the repository can be found here.

Chapter 1

Single Qbit and superposition principle

When we are talking about a qbit we are referring to a quantum state and in order to describe it mathematically we need a vector space called Hilbert space.
In the simplest case of a single qbit we define our " computational basis " as follows using the Dirac notation:

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

As the classical case our qbit can be in either the state $|0\rangle$ or the $|1\rangle$, the difference is a fundamental principle of quantum mechanics called *Quantum superposition*: in classical mechanics things are well defined however in quantum mechanics the state of a particle (our qbit) can be write as the linear combination of other states, in other words a sum of two or more states gives as result another valid state

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

1.1 Quantum logic gates

In quantum circuits we can perform operations to the qbits through what are called *Quantum logical gates* represented as unitary matrices.
In order to understand their effects to a qbit is easier to give some examples of the most important ones.

1.1.1 The NOT gate X

Chapter 2

Multistate qbit

Chapter 3

Quantum Algorithms

For many students, practice is the best way to learn so in this chapter we study some quantum algorithms.

3.1 Deutsch-Jozsa Algorithm

The problem is : given a function $f : \{0,1\}^n \to \{0,1\}$ whose definition in unknown, determine whether that function is constant or balanced, knowing for certain that f will be either constant or balanced.
What does it mean? Well f is just a machine that "eats" a string of length n composed by 0 and 1, and spits out either a 0 or a 1, lets do and example with just 2 bits :

$\{0,1\}^2$	f
00	1
01	1
10	0
11	0

$\{0,1\}^2$	f
00	1
01	1
10	1
11	1

In the example above each row of the tables represent a " question " asked to the oracle, we have 2 bits so $\{0,1\}^2$ is a string of length 2, the whole set is in general of dimension 2^n so in our case we can create four different combinations.
We can notice that the table on the left represents a balanced function in fact as output it gives the exact same number of 0 and 1, the table on the right represents a constant function.
It is easy to see that in order to be sure about the nature of our function, if we have n bits,we have to ask a number of questions equal to half plus one of the size of our set : $2^{n-1}+1$, in contrast in the quantum case we will see how we need only ask one question.
We start by implementing the algorithm for 2 qbits and then we can generalize for n qbit.

3.1.1 Implementation for two qbits

By making mistakes we learn, we will implement the Deutsch algorithm by trial and error. As we can see in figure **??** we start with two bits both at state $|0\rangle$, since the oracle calculates f on the first qbit, in order to maximize the potential of qbits we apply the Hadamard gate to the first qbit so that we have a state in superposition.

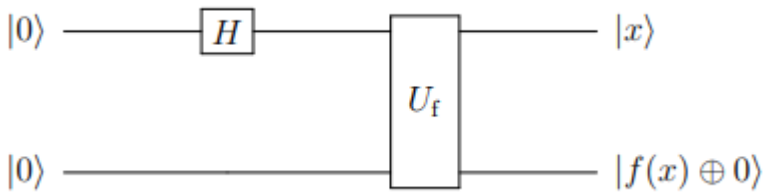


Figure 3.1:

We denote the state after the i-th operation $|\psi_i\rangle$.
So we have the initial state :

$$|\psi_1\rangle = |00\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

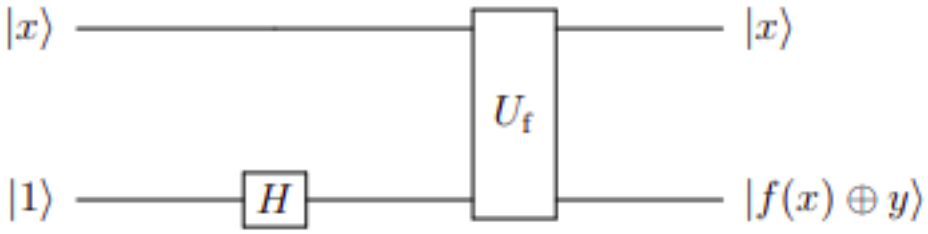
After applying the hadamard gate to the first qbit we have :

$$\begin{aligned} |\psi_2\rangle &= H|0\rangle \otimes \mathbb{I}|0\rangle \\ &= \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)|0\rangle \\ &= \frac{|00\rangle + |10\rangle}{\sqrt{2}} \end{aligned}$$

At the end of our circuit we have :

$$\begin{aligned} |\psi_3\rangle &= \frac{|0, f(0) \oplus 0\rangle + |1, f(1) \oplus 0\rangle}{\sqrt{2}} \\ &= \frac{|0, f(0)\rangle + |1, f(1)\rangle}{\sqrt{2}} \end{aligned}$$

Effectively our circuit calculates what we need, the problem is that the final state is kept in superposition so measuring it we would have a 50% chance of having *f(0)* and 50% chance of having *f(1)*.
Let's try another approach, we set the second qbit to 1 and apply hadamard gate to it, to be as general as possible the first is set to any state



$$|\psi_2\rangle = |x\rangle \otimes H\,|1\rangle$$

$$= \frac{|x,0\rangle - |x,1\rangle}{\sqrt{2}}$$

Chapter 4

Qbit Hardware

In the previous chapter we saw several examples of the kinds of algorithms that can become possible by leveraging quantum technologies with information processing. To take these algorithms from theory to actualization will require a physical quantum computer capable of performing various calculations on a system of stable qbits. An active area of research in quantum computing is deciding what physical system is best able to model the quantum nature of a qbit, particularly based on the Di Vincenzo's criteria.

In this chapter we'll go over several of the leading hardware solutions to building a universal gate quantum computer, and at the end compare their pros and cons as it relates to the Di Vincenzo criteria.

4.1 Quantum Annealers

Before we get into creating quantum computers, Let's discuss anther device that has come a long way in recent decades - the quantum annealer. A quantum annealer is a device designed for optimizing solutions to a single type of problem by quickly searching over a space and finding a solution.

4.2 Neutral-Atom Quantum Computers

4.3 Superconducting Quantum Computers

4.4 Photonic Quantum Computers

4.5 Silicon-based Quantum Computers

4.6 Trapped-Ion Quantum Computers

4.7 Summary

Chapter 5

Quantum Key Distribution

When Peter Shor introduced his now famous Shor's algorithm in the 1990s, it spelled the end of RSA and other factorization-based encryption methods. It was an unofficial call to kick the quantum computing race into high gear - although not all for the same reasons. Suddenly there was an awareness that this technology could devastate the security of various important sectors by rendering their encryption methods useless. With this issue becoming very apparent over time, In light of the capabilities of a fully realized quantum computer, there are certain security concerns that become realized