1. Introduction

Welcome to the journey of quantum computation! As a first step, let us review some general concepts related to this subject.

1.1 Theory of computation

First of all, we need to clarify what we mean by computation. A computation is defined as a mathematical calculation which involves a pre-defined sequence of steps. The first computation models used to solve certain mathematical problems, like the solution of quadratic equations, can actually be traced back to the time of the ancient Babylonians. To facilitate the process of computing, machines capable of helping to go through a computation were invented soon after. For example, one can think of the abacus, which was used for calculating many arithmetic operations. The fundamental idea behind the use of machines for computation is the one-to-one correspondence between the states of the machine and the computational states at each step of the computation.

Turing Machine

Computational machines can be designed following many different models. Among all, the most examined one is the Turing machine, which was formulated by Alan Turing [1]. Such a machine is made of three main parts: the memory, the input/output module and the instruction set. The memory is in the form of an infinitely long tape which is divided into cells; the input/output module is a "head", which moves along the tape and reads/writes symbols in each cell on the tape; the instruction set is a user-defined table of instructions specifying which action the head will do next. The machine executes a computation in the following way: each time the head reads in a symbol from the tape, then it gives an output based on the symbol read and the instruction set; the process either continues as the head moves forward or backwards, or it halts.

Circuit model of computation

Another model for a computational machine is the circuit model of computation. This model enjoys an easier implementation in practice and is the one that has been adopted by modern digital computers. In the circuit model, the basic unit for computation is a gate. Gates implement specific elementary operations. When several gates are assembled together into a circuit, it becomes possible to calculate more complicated mathematical expressions. In this model, a computation is done by feeding the input values to a circuit and retrieving the output at the end of the circuit. In the case of digital computers, gates compute Boolean logic operations (NOT, AND, OR, ...). Circuits can be designed to calculate Boolean expressions equivalent to all known arithmetic operations.

One important characteristic of the gates in the circuit model is their reversibility/irreversibility. A reversible gate allows you to carry out the computation backwards and retrieve the inputs, given the output. In contrast, an irreversible gate does not allow to reconstruct the input from the output. This detail will be of importance in quantum computations, which must be done in a reversible manner.

Reversible circuits

A reversible circuit is a circuit that allows to retrieve the input values of the computation given its output values. A reversible circuit must involve a series of reversible gates. An example of a reversible logic gate is the NOT gate. For such a logic gate, it is always possible to reconstruct the input given the output.

Irreversible circuits

On the contrary, irreversible circuits can only work in one direction and it is impossible to reconstruct the input values of the computation from the outputs. Given any circuit, a single irreversible gate is enough to make the entire circuit irreversible. An example of an irreversible logic gate is the AND gate. The AND gate has four possible input combinations and generates two possible outputs. Therefore, for a given output there is no way to uniquely identify the input values. In general, it is possible to turn an irreversible logic gate into a reversible one by including the input in the output. An example of this procedure is the Toffoli gate. It takes three inputs: the two values used in the AND operation, and the third value which is simply zero. The output of the Toffoli gate also consists of three values: the copy of two inputs which are used in the computation and the result itself. Naturally, irreversible circuits lose information during the computation. According to Landauer's principle, there is a minimum entropy cost associated with the erasure of information. Therefore, irreversible computation dissipate energy in the form of heat.

1.2 Quantum mechanics

Quantum mechanics is the theory of physics which provides a universal framework for the description of all natural phenomena. Its name, "quantum", has to do with the fact that the theory was developed for the description of atomic and subatomic particles, whose energy levels were found to be quantized in certain circumstances. But do not be mistaken, quantum mechanics is a completely general theory which can be used to make any predictions about the physical world. When dealing with macroscopic objects, however, the quantum mechanical description coincides with the classical one. Therefore, it is simpler to use classical theories for their description. Quantum mechanics is in-famously known for the counter-intuitive features which arise because of the mathematical structure of the theory. The superposition principle and quantum entanglement are two examples of such quantum features which are of extreme importance in quantum computation. Although their existence is directly contained in the mathematics of the theory, an interpretation in terms of physical phenomena can be extremely difficult. These, and more, issues related to the interpretation of the mathematical characteristics of the theory in terms of the corresponding properties of the physical world are still today's subjects of much debate and thus will not be discussed in this lecture notes.

1.3 Quantum computation

In the discussion of the theory of computation given above, we assumed that the machines implementing the computation behaved according to the classical laws of physics. This is true for most macroscopic objects operating in conditions familiar to us. Since the beginning of the century, however, our ability to arrange the extreme conditions in order to observe quantum mechanical effects has increased dramatically. To the point that we are now able to manipulate quantum mechanical objects in a predictable manner. This allows us to implement computations on machines which behave according to the principles of quantum mechanics. As mentioned earlier, quantum objects possess some very interesting and counter-intuitive features. Because of these features, like superposition and entanglement, machines built with quantum mechanical elements can do computation differently. Therefore, a computation which might take a long time to run on a Turing machine (and thus a digital computer), can take much less time on, say, a quantum Turing machine, a Turing machine improved to exploit the features of quantum mechanics. It is important to emphasize that not all mathematical problems can be solved faster on a quantum Turing machine. As of today, only a few quantum algorithms have been found which can speed-up the computation of the solution to certain mathematical problems, like factoring numbers.

Similarly, to classical computation, quantum computation is implemented in actual machine following the circuit model of computation. Because of the reversibility inherent in the laws of quantum mechanics, quantum circuits must be made of reversible gates. To carry out a quantum computation, a certain quantum state (a vector of complex values) is given as input to the quantum circuit. Then a sequence of quantum gates executes unitary operations (roughly speaking, equivalent to multiply by complex valued matrices) on the input state. The quantum state at the end of the circuit is measured to obtain the result of the computation.

In the rest of the lecture notes, we will focus on the introduction of quantum mechanics, quantum computation and the first applications.

In the next chapters...

These lecture notes provide an introduction to quantum computation for beginning undergraduate students. In the first part of the notes, corresponding to chapters 2,3 and 4, we introduce the fundamentals of quantum mechanics and quantum computation. Chapter 2 is devoted to the mathematics of quantum mechanics, linear algebra. In chapter 3, the fundamental ideas of quantum mechanics are introduced in an axiomatic way. The relation between the mathematical tools and their physical interpretation is made clearer. The basic elements of quantum computation are explained in chapter 4.

The second part of the lecture notes delves more deeply into quantum computation and its applications. Starting from chapter 5, programming with QISKit is introduced. A template for writing quantum programs with QISKit is given and several examples are worked out. Chapter 6 provides the first examples of quantum algorithm which promise an advantage over their classical counterparts. The Deutsch, Bernstein-

Vazirani and Simon algorithm are thoroughly reviewed. In chapter 7, other interesting applications of quantum computation are explored. Here the details of quantum teleportation, the possibility of transferring an unknown quantum state, and superdense coding, the communication of 2 classical bits through the transmission of a single entangled qubit, are given. The most famous quantum algorithm, Shor's, is explained in chapter 8. A useful protocol which exploits quantum features to improve the security of communication is shown in chapter 9. At the last stop of our journey, in chapter 10 we introduce quantum error correction.

References

[1] A. M. Turing, Proceedings of the London Mathematical Society. Series 2, 442 230 (1937).

[2] D. Deutsch Proceedings of the Royal Society of London. Series A, Mathematical and Physical Sciences Vol. 400, No. 1818 (Jul. 8, 1985), pp. 97-117