Quantum computing

Elisa Pettinà
telegram: @ElisaPettina
Github: QuantumComputing

March 12, 2022

Contents

Chapter 1

Introduction: from classical to quantum

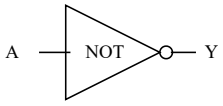
1.1 Classical computing

Classical computers are made by

- Elementary units: **bits**, that can take values $0, 1$;
- Elementary operations carried out by **logical gates**.

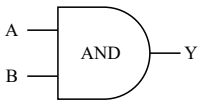
Examples of the usage of these two elements are the

- The NOT gate



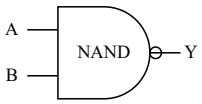
Truth table	
A	Y
0	1
1	0

- The AND gate



Truth table		
A	B	Y
0	0	0
0	1	0
1	0	0
1	1	1

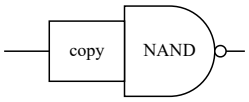
- The NAND gate



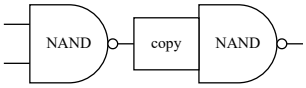
Truth table		
A	B	Y
0	0	1
0	1	1
1	0	1
1	1	0

1.1.0.1 Universality and Turing machine

The concept of universality yields a set of elementary objects that can do all sort of comptutation inside a classical computer. The NAND gate with the copy procedue are togheter universal gates, since all gates can be cosntructed from these two.
In the pictures below the construction of the NOT and AND gate are depicted, using ongli the copy and the NAND.

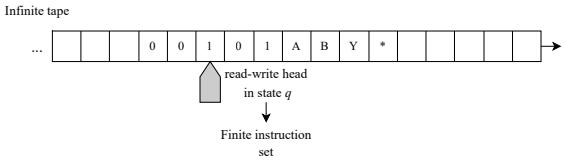


Input	Copy	NAND
0	00	1
1	11	0



Input	NAND	Copy	NAND
00	1	11	0
01	1	11	0
10	1	11	0
11	0	00	1

Since the NAND and copy operations can be used to describe all sort of (classical) computations, they also provide for the costruction of the Turing machine.
A Turing machine is a mathematical model of computation that defines an abstract machine that manipulates symbols on a strip of tape according to a table of rules.Despite the model's simplicity, given any computer algorithm, a Turing machine capable of implementing that algorithm's logic can be constructed[1].



The machine operates on an infinite memory tape divided into discrete "cells". The machine positions its "head" over a cell and reads the symbol there. The read/write head is now in state q. Given the state q and the symbol, the machine proceeds with the given finite instruction set: modifies the symbol, the head moves and q is adapted. Based on the observed symbol and the machine's own state, either proceeds to another instruction or halts computation.

[1] wikipedia/Turing_Machine

However, the very same definition of the turing machine proves the existance of its fundamental limits. For example, it cannot solve for problems that are not deducidable. The *halting problem* is a well known case: it states that it does not exist an algorithm f that cand etermine for any other agorithm g if g will eventually terminate or run forever. Algorithm shows as an absurd an algorithm f that checks wether g terminates:

```
: f(algorithm g)
if f(g) = terminate then
    while true do
        end
else
    return
```

Not only that, but also finite resources is another restriction. For example, factorizing prime number is extremely hard (as we'll see later, it is in fact NP) and for this this reason many cryptographic protocols are based on the difficulty of factoring large composite integers or a related problem—for example, the RSA problem.
However, Shor's (quantum) algorithm can find the prime factors of an integer in polynomial time. Subsequently, a quantum computer with sufficient number of qbits (and the ability not to succumb any dechorence phenomena) could break RSA and other cryptographic schemes.

1.2 Quantum computing

As classical computers have bits as fundamental units, quantum ones have **quantum bits**, or **qbits** as the basic unit of quantum information. The quantum version of the classical bit is physically realized with a two-state device.

1.2.1 Qbits

There are two possible outcomes for the measurement of a qubit—usually taken to have the value "0" and "1", like a bit or binary digit. However, whereas the state of a bit can only be either 0 or 1, the general state of a qubit according to quantum mechanics can be a coherent superposition of both. Moreover, whereas a measurement of a classical bit would not disturb its state, a measurement of a qubit would destroy its coherence and irrevocably disturb the superposition state. It is possible to fully encode one bit in one qubit[2].

1.2.1.1 Qbit states

In quantum mechanics, the general quantum state of a qubit can be represented by a linear superposition of its two orthonormal basis states (or basis vectors). These vectors are usually denoted as

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \quad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \tag{1.1}$$

[2] Wikipedia/Qubit