Introduction to Quantum Information Processing

Gilles Brassard (brassard@iro.umontreal.ca)
Université de Montréal
Département d'informatique et de recherche opérationnelle
C.P. 6128, Succ. Centre-ville
Montréal, Québec
H3C 3J7, Canada

Abstract.

Classical *information theory* was invented by Claude Shannon more than 50 years ago. It has grown into one of the most beautiful and fruitful branches of mathematics. Today, it is indispensable in many aspects of our data-driven society whenever information has to be stored, transmitted, processed or protected. Despite its undeniable successes, classical information theory is firmly rooted in classical physics, which is at best an approximation of the quantum world in which we live. This has prevented us from tapping the full potential of physical reality for information processing purposes.

Quantum mechanics is one of the most successful theories of last century. Although in principle valid at all scales, its main purpose is to explain the behaviour of elementary particles such as photons, electrons and atoms. According to quantum mechanics, things do not behave at this scale the way we are used to in our macroscopic experience. For example, quantum objects can be in several places or states at the same time. Two apparently separated objects can be *entangled*, which means that they *appear* to react instantaneously to each other's experiences no matter how distant they are. Quantum mechanics has been amply corroborated by experiments: its predictions have never been observed to be wrong, no matter how strange.

Quantum information theory is the new and exciting field that studies the implication of quantum mechanics for information processing purposes. The key to understanding the foundations of this field is the dichotomy that exists between the everyday notion of classical information and its less intuitive quantum counterpart. Classical information can be read, copied and transcribed into any medium; it can be transmitted and broadcast. In contrast, quantum information cannot be read without disturbance, it cannot be copied or broadcast at all, but it can exist in superposition of classical states. This makes it possible to design unbreakable cryptographic codes and it provides such a high level of parallelism in computation that a classical computer the size of the universe would be left behind. Some of these concepts are still theoretical, but others have been realized experimentally.

In classical information theory, a bit can take either value 0 or 1. According to quantum mechanics, a quantum bit, or *qubit*, can be in *superposition* of the two classical states. Best visualized as points on the surface of a unit sphere whose North and South poles correspond to the classical values, qubits are entirely different from classical *analogue signals*, which take their values *between* 0 and 1. A quantum *register* composed of n qubits can be in an arbitrary superposition of all 2^n different classical states on n bits. Quantum computers exploit this phenomenon so that exponentially many computations are performed simultaneously in a single piece of hardware, a phenomenon known as quantum *parallelism*. What makes this so powerfuland mysteriousis the exploitation of constructive and destructive *interference*, which allows for the reinforcement of the probability of obtaining desired

results while at the same time the probability of spurious results is reduced or even annihilated.

In my lectures, I shall set the stage for an in-depth exploration of this fascinating new field. After a brief introduction to quantum mechanics, with emphasis on the notion of *entanglement*, I shall explain the concept of quantum bits and quantum registers. I shall explain how quantum information can be manipulated: through measurements and unitary operations. After a digression on classical reversible computing, our first example of a quantum circuit will demonstrate the notion of *quantum teleportation*. We shall then see how quantum *parallelism* and quantum *interference* can be harnessed for the purpose of computing more efficiently than would be possible in a sad classical world. In these introductory lectures, we shall cover only the simplest of quantum algorithms, such as the Deutschs algorithm, which makes it possible to decide whether or not $f(0) = f(1)$ after a single computation of function f.