Lectures on Quantum Information Science

Artur Ekert

2020-11-14

Contents

Overview

Chapter 1

Quantum interference

> About complex numbers, called probability amplitudes, that, unlike probabilities, can cancel each other out, leading to quantum interference and qualitatively new ways of processing information.

The classical theory of computation does not usually refer to physics. Pioneers such as Alan Turing, Alonzo Church, Emil Post and Kurt Gödel managed to capture the correct classical theory by intuition alone and, as a result, it is often falsely assumed that its foundations are self-evident and purely abstract. They are not![1]

The concepts of information and computation can be properly formulated only in the context of a physical theory — information is stored, transmitted and processed always by *physical* means. Computers are physical objects and computation is a physical process. Indeed, any computation, classical or quantum, can be viewed in terms of physical experiments, which produce **outputs** that depend on initial preparations called **inputs**. Once we abandon the classical view of computation as a purely logical notion independent of the laws of physics it becomes clear that whenever we improve our knowledge about physical reality, we may also gain new means of computation. Thus, from this perspective, it is not very surprising that the discovery of quantum mechanics in particular has changed our understanding of the nature of computation. In order to explain what makes quantum computers so different from their classical counterparts, we begin with the rudiments of quantum theory.

1.1 Two basic rules

Quantum theory, at least at some instrumental level, can be viewed as a modification of probability theory. We replace positive numbers (probabilities) with

[1] Computation is a physical process. Computation is a physical process. Computation is …

complex numbers z (called **probability amplitudes**) such that the squares of their absolute values, $|z|^2$, are interpreted as probabilities.

Definition 1.1. The correspondence between probability amplitude z and probability $p = |z|^2$ is known as **Born's Rule**.

The rules for combining amplitudes are very reminiscent of the rules for combining probabilities:

1. Whenever something can happen in a sequence of independent steps, we multiply the amplitudes of each step.
2. Whenever something can happen in several alternative ways, we add the amplitudes for each separate way.

That's it! These two rules are basically all you need to manipulate amplitudes in any physical process, no matter how complicated.[2] They are universal and apply to any physical system, from elementary particles through atoms and molecules to white dwarfs stars. They also apply to information, since, as we have already emphasised, information is physical. The two rules look deceptively simple but, as you will see in a moment, their consequences are anything but trivial.

[2]We will, however, amend the two rules later on when we touch upon particle statistics.

1.2 Quantum interference (the failure of probability theory)

1.3 Superpositions

1.4 Interferometers

1.5 Qubits, gates, and circuits

1.6 Quantum decoherence

1.7 Computation: deterministic, probabilistic, and quantum

1.8 Computational complexity

1.9 Outlook

1.10 Notes and Exercises

1.11 Supplement: Physics against logic, via beamsplitters

1.12 Supplement: Quantum interference revisited (still about beamsplitters)

Chapter 2

Qubits

Chapter 3

Measurements

Chapter 4

Quantum entanglement

Chapter 5

Quantum algorithms

Chapter 6

Bell's theorem

Chapter 7

Decoherence, and elements of quantum error correction

Chapter 8

Density matrices

Chapter 9

Quantum channels (or CP maps)

Chapter 10

Quantum error correction and fault tolerance