Ew Applied Maths

January 17, 2020

1 Introduction

What is information?

We get information when we acquire knowledge. In classical information, the fundamental unit of information is a bit - a Boolean unit, which takes values of either 0 or 1. If we have a question with 2^n possible different, answers, then we can label each answer with a string of n bits.

What is computation?

Computation can be defined as the processing of information - updating a bit string using a prescribed sequence of steps, which we might call a program. Each of these steps can be the actions of a Boolean gate, such as NOT, AND, OR.

What is a bit physically?

Physically a bit is given by any 2 *different* physical states of a system that can be reliably distinguished by some physical measurement. For instance, I can write 0 or 1 in this document, which is stored as data on GitHub or your hard drive, and you can conduct the physical measurement of loading this document and reading the following number: 1. This concept is summed up in the saying "There is no information without representation". We see that any computation is then the manipulation of a physical system, and so computers must obey the laws of physics. Modern computers obey classical physics (at least for now - please email me / hololens call me if this is not the case for you), but as Feynmann once said: "Nature isn't classical dammit".

On the atomic and subatomic (and even now molecular) scales, particles are governed by Quantum Mechanics. This has some novel features over classical mechanics, such as the ideas of quantum superposition, entanglement, and quantum measurement. Throughout this course, we will be exploiting these features. They will make things more complicated, but at the same time will give us some advantages in information storage, communication, computation, as well as security/cryptography.

Most of the work for this course was done during the 1980's and 1990's, although the Russian mathematician Alexander Holevo was already working on the ideas of quantum information in the 1970's.

In what ways is QIC better than its classical counterpart?

A quantum computer cannot compute any computational task which isn't already computable *in principle* by a classical computer. However, some things will require many times the age of the universe to compute even on the fastest of classical supercomputers.

1.1 Computational Complexity Theory

We want to have some idea of the "difficulty" of a computational task. We measure this by the amount required of the two computational resources of time and space. For instance, consider the problem of factoring a number with n digits. Then the input size for the computation is n, and we can look at how the time/space grow as functions of n.

If the time grows polynomially in n, we call this a poly-time algorithm. These are computable in practice. If it grows faster than any polynomial, we call it an exponential-time algorithm, which are, whilst theoretically computable, uncomputable in practice for large inputs.

Currently, there is no known poly-time factoring algorithm for a classical computer, but in 1994 Peter Shor came up with a poly-time quantum algorithm for integer factorisation.

1.2 Communication & Security Issues

If we use quantum particles as information carriers, we end up with communication possibilities which were the stuff of science fiction previously, such as quantum teleportation, or implement mathematically provably secure communication.

1.3 Technological Issue

Moore's law states that, since 1965, devices will miniaturise by a factor of 4 every 3.5 years. Eventually (and this is already happening), we will get close to quantum scales. For instance, modern CPUs are built by manufacturing machines with a resolution of around 10nm, or 100 atoms across. At these scales, quantum mechanics will start to cause problems for classical computation, so why not embrace this new feature? In reality, the technological barrier to actually using quantum bits (qubits) is huge, and the most advanced current quantum computers have about 53 qubits. Moreover, Google has claimed ***quantum supremacy*** in demonstrating a task, known as the "random sampling algorithm", which their quantum computer can complete faster than a classical computer.

1.4 Quantum Mechanics

We have 4 key postulates of quantum mechanics:

(QM1) Describes the quantum state of a physical system, S

(QM2) Describes the joint state of two composite systems, S_1S_2

(QM3) Describes how quantum states evolve throughout time. Here we will be interested in discrete time steps.

(QM4) Describes how quantum states respond to measurement.

The idea behind the mathematics of quantum mechanics, which we'll get to properly in the next section, is that we want to associate to every quantum-mechanical system S a ***complex inner product vector space*** $\mathcal{V}$, or ***Hilbert space***. We will be using ***Dirac's bra-ket notation***.

A ***ket*** is a vector $|\psi\rangle \in \mathcal{V}$. For quantum computation, we will use $\mathcal{V} = \mathbb{C}^2$. Then we will represent the ***qubit*** $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, and $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$. Then for $\alpha, \beta \in \mathbb{C}$, we can represent a valid quantum state by $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. If $|\alpha|^2 + |\beta|^2 = 1$, then this is a ***qubit***, and when we measure it we get 0 with probability $|\alpha|^2$ and 1 with probability $|\beta|^2$.