Notes:
Quantum Computation and Quantum Information: 10th Anniversary Edition

Daniel Saunders

August 21, 2018

Notes

1. Some *emphasis* is from the book, some is added.

2. Abbreviations such as QC may interchangeably refer to *quantum computation* and *quantum computer*.

Part I
Fundamental concepts

1 Introduction and Overview

"Information is physical" - Rolf Landauer.

Purpose of chapter: Answer questions "What are the fundamental concepts of quantum computation and quantum information?", "How can they be used?", "How will they be presented in the book?".

1.1 Global perspectives

Quantum computation (QC) and quantum information (QI) (together, QCI): study of info. processing tasks that can be done using quantum mechanical (QM) systems.

Which fields contributed ideas to QCI? QM, computer science (CS), information theory (IT), and cryptography (crypto).

1.1.1 History of quantum computation and quantum information

At the turn of the 20th century, *classical physics* was predicting absurdities (such as the "ultraviolet catastrophe"). These were at first resolved using additional *ad hoc* hypotheses to classical physics, but became more convoluted as better understanding of atoms and radiation were obtained. In the 1920s, this crisis resulted in the creation of *quantum mechanics*.

QM is a mathematical framework / set of rules for the construction of physical theories; e.g., *quantum electrodynamics* (QED), which accurately describes the interaction of atoms and light.

The rules of QM are simple yet counterintuitive. One of the goals of QCI is the develop ways to sharpen our intuition about QM and make its predictions more transparent.

1980s: Is it possible to use QM effects to signal faster than light (violating Einstein's theory of relativity)? Resolution depends on whether it's possible to *clone* an unknown quantum state; i.e., construct a copy of it. If cloning were possible, then it would be possible signal faster than light.

However, cloning is not possible *in general* in QM, due to one of the earliest results of QCI (the *no-cloning theorem*). Tools now exist to understand how well an imperfect quantum cloning device might work.

1970s: Interest in obtaining *complete control over single quantum systems*. QM applications pre-1970s typically involved coarse-grained control over a large sample with an enormous number of QM systems, none of which were directly accessible; e.g., superconductivity. Such experiments allow for the probing of only a few aspects of QM systems, with individual system states remaining inaccessible.

Since then, several techniques for controlling single quantum states have been developed; e.g., the "atom trap" and the scanning tunneling microscope.

The ability to control single QM systems is essential in order to harness QM for QCI applications.

Efforts to build quantum information processing (QIP) systems have resulted in modest success. Small quantum computers (QCs) capable of dozens of operations on a few *qubits* are the state of the art (SOTA). Experimental prototypes for *quantum cryptography* have also been demonstrated.

Turning to computer science:

Alan Turing developed the notion of the programmable computer, a model of computation known as the *Turing machine* (TM). He showed there is a *Universal Turing machine* (UTM) capable of simulating any other TM. He claimed the UTM *completely captures* what it means to perform an algorithmic task; i.e., if an algorithm can be performed on any hardware, there is an equivalent algorithm which does the same thing on a UTM. This is known as the *Church-Turing thesis* (CT thesis) (after Alan Turing and Alonzo Church).

John von Neumann developed a theoretical model for how to assemble a digital computer as capable as a UTM. *Moore's law* refers to the tendency of computer power to roughly double for constant cost every two years, coined by Gordon Moore in 1965.

Moore's law has held approximately since its inception, but this is expected to end since conventional approaches to microchip fabrication are starting to run up against fundamental size difficulties; i.e., quantum effects are interfering in the functioning of electronic devices as they're made increasingly smaller.

One solution to this problem: move to a different computing paradigm, one of which is provided by QC. Although classical computers (CCs) can simulate QC, it appears impossible to do so *efficiently*, resulting in a QC speed advantage over DC. Researchers believe that *no* amount of progress in CC is enough to overcome this advantage.

Key notions of "efficiency" in computer algorithms is made mathematically precise by *computational complexity*; roughly, efficient algorithms run in polynomial time in the size of the problem solved, whereas inefficient algorithms require super-polynomial time. In the 1960s-70s, it seemed that the TM model of computation (MoC) was at least as powerful as any other MoC, in that any problem efficiently solved by another MoC could be efficiently solved by the TM model by using the TM to simulate the other MoC. This results in the *strong CT* thesis: *Any algorithmic process can be simulated efficiently using a Turing machine.*

Researchers in the field of *analog computation* (AC) noticed that certain type of ACs can efficiently solve problems without known efficient TM solutions. However, when realistic assumptions about presence of noise in ACs is used, their power disappars: they can't efficiently solve problems than TMs can't. The development of *quantum error-correcting codes* and *fault-tolerant quantum computation* solved this problem for QCI. Unlike AC, QC can tolerate a finite amount of noise and still retain a computational advantage.

First major challenge to strong CT thesis (1970s): Solovay and Strassesn showed that it's possible to test for primality using a *randomized algorithm*. It could determine that a number was *probably* prime or otherwise composite *with certainty*. The test could be repeated to improve confidence in the results of the probabilistic test. It seemed that computers with a random number generator (RNG) could efficiently solve problems with no efficient solution on deterministic TMs.

Randomized algorithms pose a challenge to the strong CT thesis, resulting in another modification of the strong CT thesis: *Any algorithmic process can be simulated efficiently using a probabilistic*

Turing machine.

1985: David Deutsch asked whether the laws of physics could be used to derive a stronger CT thesis, instead of using *ad hoc* hypothesis. He attempted to device a version of a TM that would be capable simulating an *arbitrary* physical system, and, since the laws of physics are quantum mechanical, was led to consider computing devices based on QM principles.

It's not clear wther the quantum TM (QTM) is sufficient to efficiently simulate an arbitrary physical system. It's possible that some effect of more complicated physical theories may be required to enable still more powerful computation.

The QTM posed another challenge to the strong, probabilistic CT thesis. Deutsch constructed an example suggesting that QCs might have computational power exceeding those of CCs; i.e., that QCs can efficiently solve problems which have no efficient solution on classical computers.

This first step was improved in the next decade, culminating with Peter Shor's algorithm(s) for the efficient QC solution of the prime factorization and "discrete logarithm" problems (1994). These problems are still believed not to have efficient solutions on CCs. Lev Grover demonstrated a QC speedup on search in unstructured search spaces (1995).

1982: Richard Feynman pointed out the seemingly essential difficulties in simulating QM systems with CCs, and suggeseting QCs would avoid these. 1990s: A team of researchers showed it is indeed possible to efficiently simulate QM systems with no known efficient simulation on CCs. Likely major application of QCs: perfoming simulations of such QM systems.

Designing quantum algorithms (QAs) seems to be hard, perhaps because designers face two problems not faced in algorithm design for CCs:

1. Human intuition is apparently rooted in the "classical world". To design good QAs, one must ignore classical intuition for at least part of the design process and use quantum effects to achieve the algorithmic goal.

2. The QA much be better than any existing classical algorithm. Although a QA may make use of aspects of QM, it may not be of interest as a classical algorithm (CA) with similar performance characteristics may exist.

What is is that makes QCs more powerful than CCs? What class of problems can be solved efficiently on QCs, and how does that compare to the same class of problems for CCs?

Turning to information theory:

1948: Claude Shannon published a pair of papers on the foundations of the theory of information and communication. Key step: *mathematically defining hte concept of information.* Two key questions relation to communication of information over a channel:

1. What resources are needed to send information over a channel?

2. Can information be transmitted such that it's protected against noise in the channel?

Shannon answered these questions with two fundamental IT theorems:

1. The *noiseless channel coding theorem* quantifies the physical resources needed to store the output from an information source.

2. The *noisy channel coding theorem* quantifies how much information it's possible to reliably transmit through a noisy channel. To get reliable transmission in the presence of noise, *error-correcting codes* (ECCs) could be used to protect the information being sent. This theorem gives an upper limit on the protection afforded by ECCs.

A sophisticated theory of ECCs now exists.

Quantum information theory (QIT) follows a similar developments. 1995: Ben Schumacher provided an another of the noiseless channel coding theorem and defined the *quantum bit*, or *qubit*, as

the tangible physical resource. No analogue to the noisy channel coding theorem is known for QIT. A theory of quantum EC (QEC) has been developed, allowing QCs to compute effectively in the presence of noise, and allows reliable communcation over noisy quantum channels.

1992: Charles Bennett and Stephen Wiesner showed how to transmit two classical bits of information while only transmitting one quantum bit; called *superdense coding*.

Distributed quantum computation: exponentially less communication is sometimes required to solve problems with networked QCs than with networked CCs.

Networked information theory: The study of networks of multiple communications channels.

Study of networked QIT is in its infancy; no unifying theory of networked IT exists for QCs.

Turning to cryptography:

Cryptography is the problem of doing communication or computation with two or more parties who many not trust each other. Secret communication can be accomplished using a *cryptographic protocol*, distinguishing between *private key* and *public key cryptosystems*.

Quantum cryptography or *quantum key distribution* allows for private crypto key distribution such that Alice and Bob's security cannot be compromised. Basic idea: exploit QM principle that observations disturbs QM systems. Eavesdroppers can be detected as a disturbance of the communication channel Alice and Bob use to establish a private key. 1984: Charles Bennet and Gilles Brassard proposed a QM protocol to distribute keys between Alice and Bob without possibility of compromise.

Public key cryptosystems: Bob publishes a "public key" which Alice uses to encrypt a message to Bob, which is extremely difficult to decrypt without the private key known only to Bob. Such cryptosystems solve the key distribution problem by making it unnecessary to share private keys before communication.

Presumed security of the *RSA cryptosystem* relies on the belief that factoring is hard to solve using CCs. Shor's algorithm for factoring on QCs could break RSA!

Quantum entanglement: uniquely QM *resource* that plays a role in many interesting applications of QCI; not well understood.

1.1.2 Future directions

QCI has taught us to *think physically about computation*; any physical theory may be used as the basis for a theory of information processing and communication. On the other hand, we may also *think computationally about physics*. Physics has traditionally focused on understanding elementary objects and simple systems; computation and algorithms provide means for constructing and understanding complex systems.

1.2 Quantum bits

QCI are built on a concept analogous the to classical *bit*, the *qubit* or *quantum bit*. They have a physical realization, but will be described as *mathematical objects* with certain properties, since treating them as abstract entities gives the freedom to construct a general theory of QCI which doesn't depend on a specific physical system for realization.

A qubit has a *state*, just like a bit. Two possible states are $|0\rangle$ and $|1\rangle$, corresponding to the 0 and 1 states for classical bits. This is called the *Dirac notation*. It's possible to form *linear combinations* of states, often called *superpositions*:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle. \tag{1.1}$$

The numbers α and β are complex numbers, and the state of a qubit is a vector in a two-dimensional complex vector space. The special states $|0\rangle$ and $|1\rangle$ are called *computational basis states* and form an orthonormal basis for the vector space.

We can't examine a qubit to determine its quantum state (the values of α and β). We can acquire more restricted information by measuring a qubit a obtaining a 0 with probability $|\alpha|^2$ or a 1 with probability $|\beta|^2$. Thus, a qubit's state is a unit vector in a two-dimensional complex vector space.
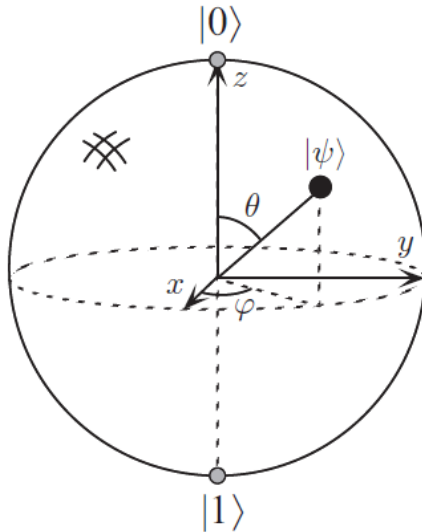
4

Figure 1: Bloch sphere representation of a qubit.

There is an indirect correspondence between qubit states and their consequences, and they can be manipulated and transformed in ways that lead to measurement outcomes that depend on their properties.

Classical bits are like coins: they can exist either in a heads up (1) or tails up (1) state. Qubits, OTOH, can exist in a *continuum* of states between $|0\rangle$ and $|1\rangle$, but only ever gives "0" or "1' (probabilistic) outcomes when measured. A qubit can be in the state (denoted $|+\rangle$)

$$\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle, \tag{1.2}$$

which gives 0 or 1 each with probability $\frac{1}{2}$.

Because $|\alpha|^2 + |\beta|^2 = 1$, we can rewrite Equation 1.1 as

$$|\psi\rangle = e^{i\gamma}\left(\cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle\right) \tag{1.3}$$

where $\theta, \varphi, \gamma \in \mathbb{R}$. We will later see that we can *ignore* the factor in front because it has *no observable effects* and effectively write

$$|\phi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle \tag{1.4}$$

The numbers θ and φ define a point on the unit 3D sphere, called the *Bloch sphere*, useful for visualizing state of a single qubit (Figure 1.2).

How much information is represented by a qubit? There are an infinite number of points on the unit sphere, so one can in principle store infinite θ. However, qubits only yield 0 or 1 when observed, and measurement *changes* the state of a qubit, collapsing it from its superposition to a specific measurement state. For example, if the measurement of $|+\rangle$ gives 0, then the post-measurement state of the qubit is $|0\rangle$. No one knows why this collapse occurs; this behavior is one of the *fundamental postulates* of QM. A single measurement gives only a single bit of information about the state of the qubit. Only if there were infinitely many identically prepared qubits to measure would we be able to determine the values of α and β of a qubit's superposition state.

How much information is represented by a qubit *if we don't measure it*? Nature evolves a closed quantum system of qubits with performing "measurements", but apparently tracking the continuous

variables describing their states, in a sense concealing "hidden information". The potential amount of this extra information grows exponentially with the number of qubits.

1.2.1 Multiple qubits

"Hilbert space is a big place" - Carlton Caves.

A two qubit system has four *computational basis states*: $|00\rangle, |01\rangle, |10\rangle, |11\rangle$, and can exist in a superposition of these four states; the quantum state of two qubits involves associating complex coefficients (*amplitudes* with each computational basis state:

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle. \tag{1.5}$$

The condition that probabilities sum to one is expressed by the *normalization condition* that $\sum_{x\in\{0,1\}^2} |\alpha_x|^2 = 1$. Measuring the first qubit alone gives 0 with probability $|\alpha_{00}|^2 + |\alpha_{01}|^2$, leaving the post-measurement state as:

$$|\phi'\rangle = \frac{\alpha_{00}|00\rangle + \alpha_{01}|01\rangle}{\sqrt{(|\alpha_{00}|^2 + |\alpha_{01}|^2)}}. \tag{1.6}$$

The post-measurement state is *re-normalized* by the factor $\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}$ so that it still satisfies the normalization condition.

An important two qubit state is the *Bell state* or *EPR pair*:

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}}. \tag{1.7}$$

It is key to quantum teleportation and super-dense coding, and the prototype for many other interesting quantum states. It has the property that upon measuring the first qubit, one obtains either 0 with probability $\frac{1}{2}$ (giving post-measurement state $|\phi'\rangle = |00\rangle$), and 1 with probability $\frac{1}{2}$ (giving $|\phi'\rangle = |11\rangle$). A measurement of the second qubit always gives the same result as the measurement of the first qubit; the measurement outcomes are *correlated*. Other types of measurements can be performed on the Bell state by first applying some operations to the first or second qubit, and interesting correlations still exist between the result of a measurement of the two. John Bell: the measurement correlations in the Bell state are *stronger than could ever exist between classical systems*.

We may consider a system of n qubits with computational basis states of the form $|x_1 x_2 ... x_n\rangle$, with quantum states specified by 2^n amplitudes. For moderate n, storing and computing over all these complex numbers is not possible on classical computers; however, Nature manipulates such quantities of data, even for systems containing only a few hundred atoms. This potential computational power is something we'd like to harness. But how to think to QM as computation?

1.3 Quantum computation

Changes occurring to a quantum state can be described using *quantum computation*. QCs are built from *quantum circuits* with wires and *quantum gates* to carry / manipulate quantum information.

1.3.1 Single qubit gates

Quantum `NOT` gate acts *linearly*: takes the state

$$\alpha|0\rangle + \beta|1\rangle \tag{1.8}$$

to the corresponding state where the roles of $|0\rangle$ and $|1\rangle$ are interchanged:
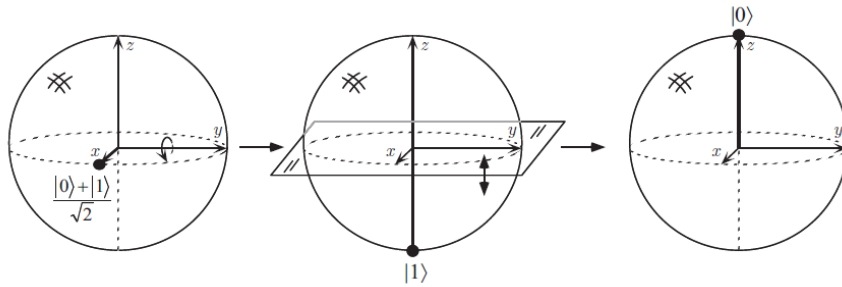
$$\alpha|1\rangle + \beta|0\rangle. \tag{1.9}$$

Figure 2: Visualization of the Hadamard gate on the Bloch sphere acting on the input state $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$.

Linear behavior is a general property of QM, and well-motivated empirically; nonlinear behavior can lead to apparent paradoxes such as time travel, faster-than-light communication, and violations of the second law of thermodynamics.

A matrix X can be used to represent the quantum `NOT` gate, following from the linearity of quantum gates (QGs):

$$X \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \tag{1.10}$$

QGs on single qubits can be described by two by two matrices. The appropriate condition on matrices representing QGs is that matrices U describing single qubit gates be *unitary*: $U^\dagger U = I$, where $U^\dagger$ is the *adjoint* of U.

This *unitarity* condition is the only constraint on QGs. Any unitary matrix specifies a valid QG. There are many non-trivial single qubit gates; e.g., the Z gate:

$$Z \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \tag{1.11}$$

and the *Hadamard gate*:

$$H \equiv \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}. \tag{1.12}$$

In the Bloch sphere picture, it turns out that single QGs correspond to rotations and reflections of the sphere.