Mid-Term Report

Quantum Computing, Information and Quantum Technologies

Sravan K Suresh
22B3936

Mentor:

Aniket Zambare

Abstract

This mid-term report aims to highlight the basics of Quantum Computing, Information and Quantum Technology. My learning so far is based on the following resources:

- Quantum Computation and Quantum Information, by *Nielsen* and *Chuang*
- *John Preskill's* notes
- PH-534 Lecture Series

We start with an overview to the world of Quantum technologies by going through its global perspectives, then understanding what Quantum bits are. These base-level concepts help us dive deep into the quantum computation, its algorithms, and the experimental quantum information processing.

With particular interest and passion in the Quantum computation, we go ahead to explore what makes up the Quantum physics, i.e.: Quantum Circuits. After studying the Quantum Algorithms that are likely to be involved, we understand the various single Qubit operations, followed by how are can their controlled operations be performed. At the heart of Quantum physics, 'measurement' brings about some counter-intuitive changes in the systems which are crucial in understanding the subject. After sound knowledge of the universal Quantum gates, we get to completely realize the Quantum circuit model of computation, which is helps us finally reach the simulations of Quantum systems.

Salient points:

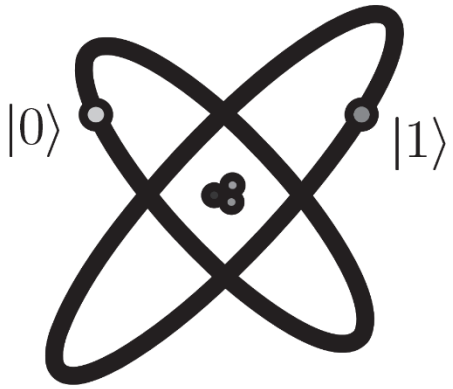
- Quantum mechanics is a mathematical framework or set of rules for the construction of physical theories.
- In 1995, Ben Schumacher provided an analogue to Shannon's noiseless coding theorem, and in the process defined the 'quantum bit' or 'qubit' as a tangible physical resource. However, no analogue to Shannon's noisy channel coding theorem is yet known for quantum information.
- By building upon the basic ideas of classical linear coding theory, the discoveries of CSS codes (an important class of Quantum codes) greatly facilitated a rapid understanding of quantum error-correcting codes.
- The theory of quantum error-correcting codes was developed to protect quantum states against noise.
- Quantum computers can require exponentially less communication to solve certain problems than would be required if the networked computers were classical!
- A major challenge for the future of quantum computation and quantum information is to find problems of real-world importance for which distributed quantum computation offers a substantial advantage over distributed classical computation.
- The basic idea in **Quantum Cryptography** to exploit the quantum mechanical principle that observation in general disturbs the system being observed. Thus, if there is an eavesdropper listening in as Alice and Bob attempt to transmit their key, the presence of the eavesdropper will be visible as a disturbance of the communications channel Alice and Bob are using to establish the key. Alice and Bob can then throw out the key bits established while the eavesdropper was listening in, and start over.

- Public key cryptosystems solve the key distribution problem by making it unnecessary for Alice and Bob to share a private key before communicating. The key to the security of public key cryptosystems is that it should be difficult to invert the encryption stage if only the public key is available.
- Quantum Entanglement is a uniquely quantum mechanical resource that plays a key role in many of the most interesting applications of quantum computation and quantum information; entanglement is iron to the classical world's bronze age.
- Quantum computation and quantum information has taught us to think physically about computation, and we have discovered that this approach yields many new and exciting capabilities for information processing and communication. Quantum computation and quantum information certainly offer challenges aplenty to physicists, but it is perhaps a little subtle what quantum computation and quantum information offers to physics in the long term.
- One of the messages of quantum computation and information is that new tools are available for traversing the gulf between the small and the relatively complex: computation and algorithms provide systematic means for constructing and understanding such systems. Applying ideas from these fields is already beginning to yield new insights into physics.
- The bit is the fundamental concept of classical computation and classical information. Quantum computation and quantum information are built upon an analogous concept, the quantum bit, or 'qubit' for short.
- Two possible states for a qubit are the states $|\mathbf{0}\rangle$ and $|\mathbf{1}\rangle$, which as one might guess correspond to the states 0 and 1 for a classical bit. The difference between bits and qubits is that a qubit can be in a state other than $|\mathbf{0}\rangle$ or $|\mathbf{1}\rangle$ .It is also possible to form linear combinations of states, often called superpositions:

$$|\psi\rangle = \alpha\,|\mathbf{0}\rangle + \beta\,|\mathbf{1}\rangle.$$

The numbers α and β are complex numbers, although for many purposes not much is lost by thinking of them as real numbers. Put another way, **the state of a qubit is a vector in a two-dimensional complex vector space.** The special states $|0\rangle$ and $|1\rangle$ are known as **computational basis states**, and form an orthonormal basis for this vector space.

- we cannot examine a qubit to determine its quantum state, that is, the values of α and β. Instead, quantum mechanics tells us that we can only acquire much more restricted information about the quantum state. When we measure a qubit we get either the result 0, with probability $|\alpha|^2$, or the result 1, with probability $|\beta|^2$. Naturally, $|\alpha|^2 + |\beta|^2 = 1$, since the probabilities must sum to one. Geometrically, we can interpret this as the condition that the **qubit's state be normalized to length 1**. Thus, **in general a qubit's state is a unit vector in a two-dimensional complex vector space**.
- A classical bit is like a coin: either heads or tails up. For imperfect coins, there may be intermediate states like having it balanced on an edge, but those can be disregarded in the ideal case. By contrast, a qubit can exist in a continuum of states between $|0\rangle$ and $|1\rangle$ – until it is observed!
- By shining light on the atom, with appropriate energy and for an appropriate length of time, it is possible to move the electron from the $|0\rangle$ state to the $|1\rangle$ state and vice versa. But more interestingly, by reducing the time we shine the light, an electron initially in the state $|0\rangle$ can be moved 'halfway' between $|0\rangle$ and $|1\rangle$, into the $|+\rangle$ state.

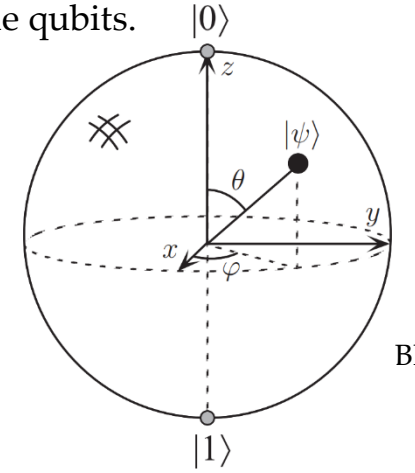


Qubit represented by two electronic levels in an atom

- Many of the operations on single qubits are neatly described within the Bloch sphere picture. However, it must be kept in mind that this intuition is limited because there is no simple generalization of the Bloch sphere known for multiple qubits.

Hilbert space is a big place.

– *Carlton Caves*



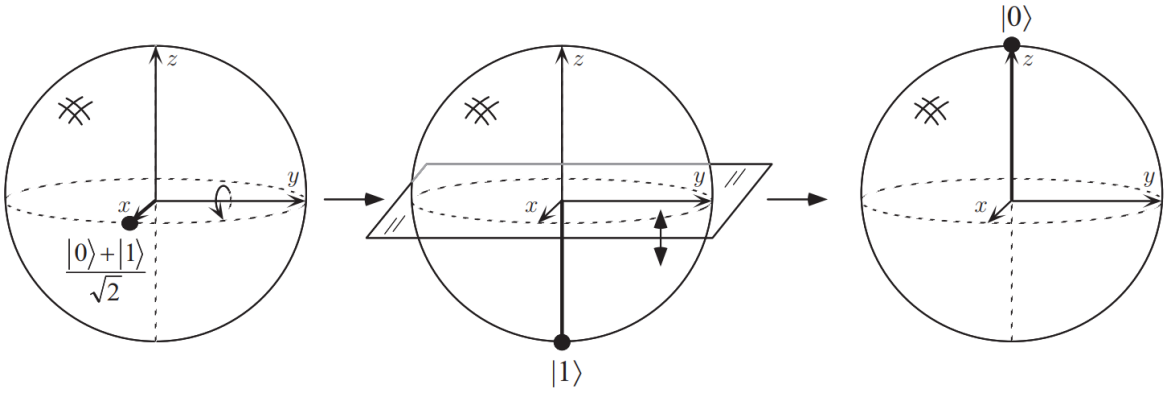
Bloch sphere representation of a qubit.

- Measurement changes the state of a qubit, collapsing it from its superposition of $|0\rangle$ and $|1\rangle$ to the specific state consistent with the measurement result. For example, if measurement of $|+\rangle$ gives 0, then the post-measurement state of the qubit will be $|0\rangle$.
- when Nature evolves a closed quantum system of qubits, not performing any 'measurements', she apparently does keep track of all the continuous variables describing the state, like α and β. In a sense, in the state of a qubit, Nature conceals a great deal of **'hidden information'**. The potential amount of this extra 'information' grows exponentially with the number of qubits.
- An important two qubit state is the **Bell state** or **EPR pair**.

$$\frac{|00\rangle + |01\rangle}{\sqrt{2}}$$

This innocuous-looking state is responsible for many surprises in quantum computation and quantum information. It is the key ingredient in quantum teleportation and super-dense coding!

- More generally, we may consider a system of n qubits. The computational basis states of this system are of the form $|x_1\, x_2 \ldots x_n\rangle$, and so a quantum state of such a system is specified by 2^n amplitudes. Trying to store all these complex numbers would not be possible on any conceivable classical computer. Hilbert space is indeed a big place. In principle, however, Nature manipulates such enormous quantities of data, even for systems containing only a few hundred atoms. It is as if Nature were keeping 2500 hidden pieces of scratch paper on the side, on which she performs her calculations as the system evolves. This enormous potential computational power is something we would very much like to take advantage of!
- Quantum Computation: Analogous to the way a classical computer is built from an electrical circuit containing wires and logic gates, a quantum computer is built from a quantum circuit containing wires and elementary quantum gates to carry around and manipulate the quantum information.
- Single qubit gates: Classical computer circuits consist of wires and logic gates. The wires are used to carry information around the circuit, while the logic gates perform manipulations of the information, converting it from one form to another.
- The appropriate condition on the matrix representing the gate is that the matrix U describing the single qubit gate be unitary, that is $U^\dagger U = I$, where $U^\dagger$ is the adjoint of U. This unitarity constraint is the only constraint on quantum gates. Any unitary matrix specifies a valid quantum gate!



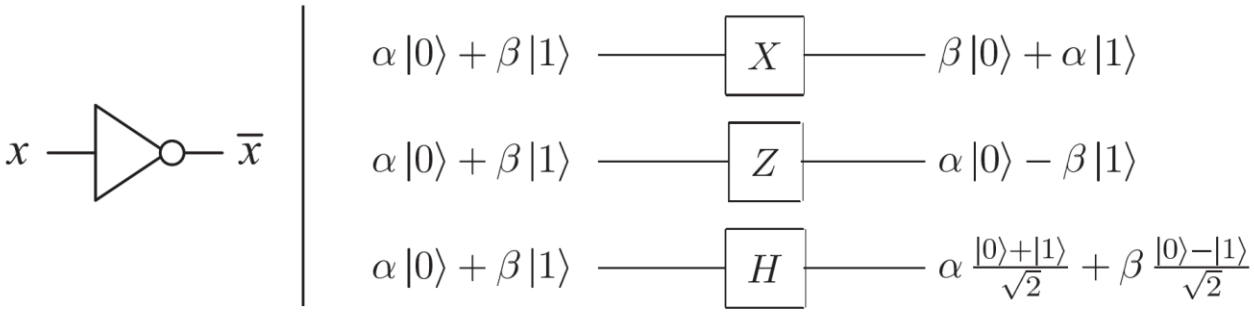


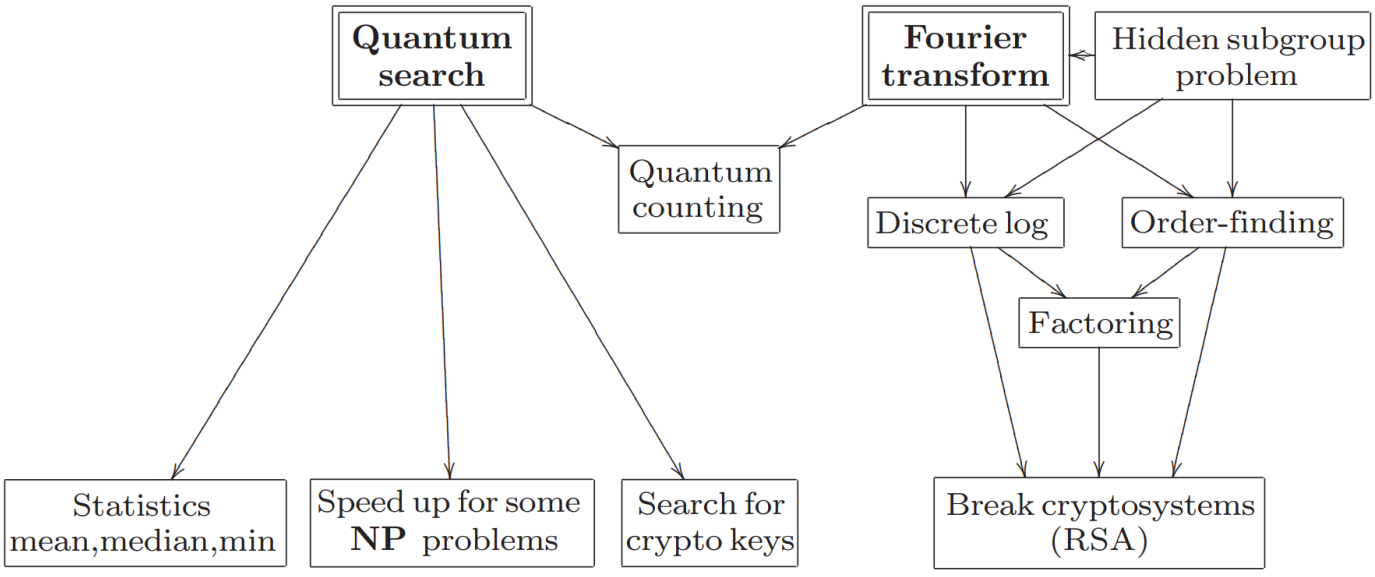
Figure 1.5. Single bit (left) and qubit (right) logic gates.

Box 1.1: Decomposing single qubit operations

In Section 4.2 starting on page 174 we prove that an arbitrary 2×2 unitary matrix may be decomposed as

$$U = e^{i\alpha} \begin{bmatrix} e^{-i\beta/2} & 0 \\ 0 & e^{i\beta/2} \end{bmatrix} \begin{bmatrix} \cos\frac{\gamma}{2} & -\sin\frac{\gamma}{2} \\ \sin\frac{\gamma}{2} & \cos\frac{\gamma}{2} \end{bmatrix} \begin{bmatrix} e^{-i\delta/2} & 0 \\ 0 & e^{i\delta/2} \end{bmatrix}, \quad (1.17)$$

where α, β, γ, and δ are real-valued. Notice that the second matrix is just an ordinary rotation. It turns out that the first and last matrices can also be understood as rotations in a different plane. This decomposition can be used to give an exact prescription for performing an *arbitrary* single qubit quantum logic gate.



Status with respect to my PoA:

Currently I have completed the contents planned uptil week-5, therefore I am in-line with the initial plan of action.