FINAL REPORT

27^{th} July, 2023

Summer Of Science (SoS)

Quantum Computing, Information and Quantum Technologies

Mentee: Sravan K Suresh

Roll no: 22B3936

Mentor: Aniket Zambare

Indian Institute of Technology Bombay

Sumário

1 ABSTRACT

This FINAL report encompasses my learning in Quantum Computing, Information and Quantum Technologies, a course under the initiative 'Summer Of Science (SoS)' by the `MnP club` at IIT Bombay.

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 very likely to be involved, we understand the various single Qubit operations, followed by how 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. Now, having a sound knowledge of the universal Quantum gates, we get to completely realize the Quantum circuit model of computation, which finally helps us reach the simulations of Quantum systems.

Further, in the section of Quantum computation, we study the quantum Fourier transform and its applications like order-finding, period-finding, factoring etc. The Fourier transform is the key to a general procedure known as Phase estimation, which in turn is the key for many quantum algorithms. This section also covers the same, along with its performance and requirements.

Building upon the groundwork laid in the previous chapters, we explore the pivotal quantum algorithms. The iconic algorithm of Shor for factoring large numbers is introduced, along with Grover's algorithm for quantum search. These algorithms exemplify the exponential speedup that quantum computation can offer over classical counterparts. Moving ahead, in the segment 'Quantum compexity theory', the focus shifts to

investigating the inherent difficulty of solving problems on quantum computers. We encounter the concept of quantum NP-completeness and explore the implications of quantum oracle machines.

Now, as quantum computers are inherently prone to errors, quantum error correction becomes crucial. This section explores stabilizer codes, quantum error-correction codes, and introduces fault-tolerant quantum computation. Understanding error correction is vital for scalable quantum computation.

Quantum information is not limited to computation but also includes quantum communication. In this part, we discover quantum key distribution protocols like BB84, quantum teleportation, and superdense coding, which allow secure and efficient transmission of information. This takes us to one of the most interesting sub-topic, Quantum cryptography!

Incorporating quantum communication principles, the sub-section 'Quantum Cryptography' explains the quantum key distribution protocols, their security features, and the fascinating phenomenon of quantum entanglement as a resource for secure communication.

Finally, Entanglement is a quintessential feature of quantum mechanics, and the chapter 'Quantum Entanglement and Quantum Information Theory' explores its properties and applications in detail. It also introduces quantum information theory, including *Von Neumann* entropy, relative entropy, and quantum mutual information.

2 Salient Points

2.1 Overview

- 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 $|0\rangle$ and $|1\rangle$, 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 $|0\rangle$ or $|1\rangle$. It is also possible to form linear combinations of states, often called superpositions:

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$$

- 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.

- 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.

- 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.

- 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:

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

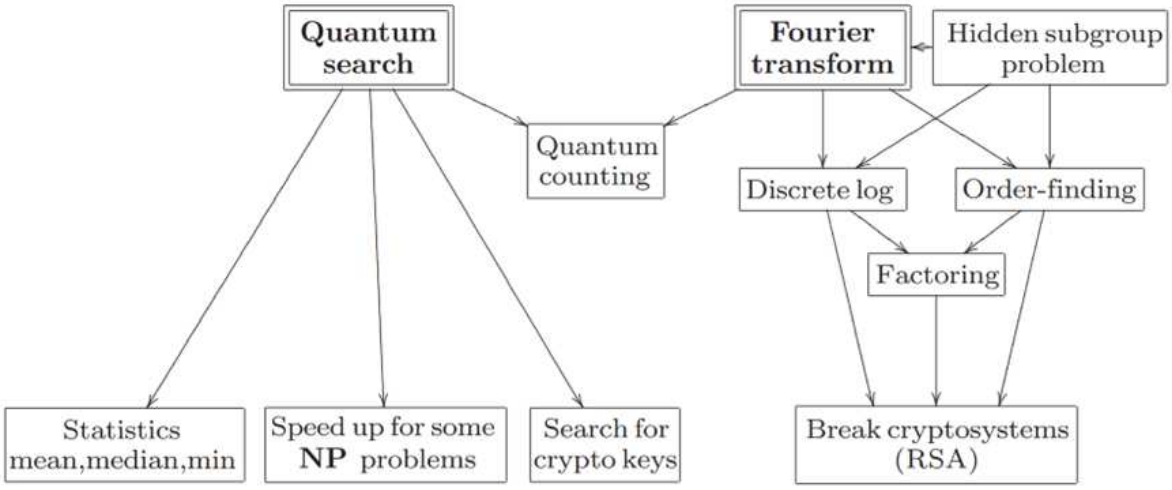
  This innocuous-looking state is responsible for many surprises in quantum computation and quantum information. It is the key ingredient in quantum teleportation and super-dense coding!

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.



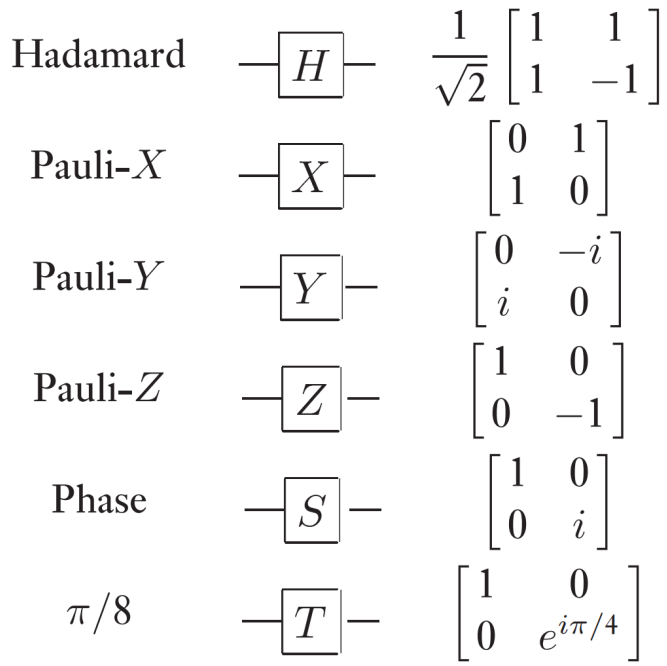
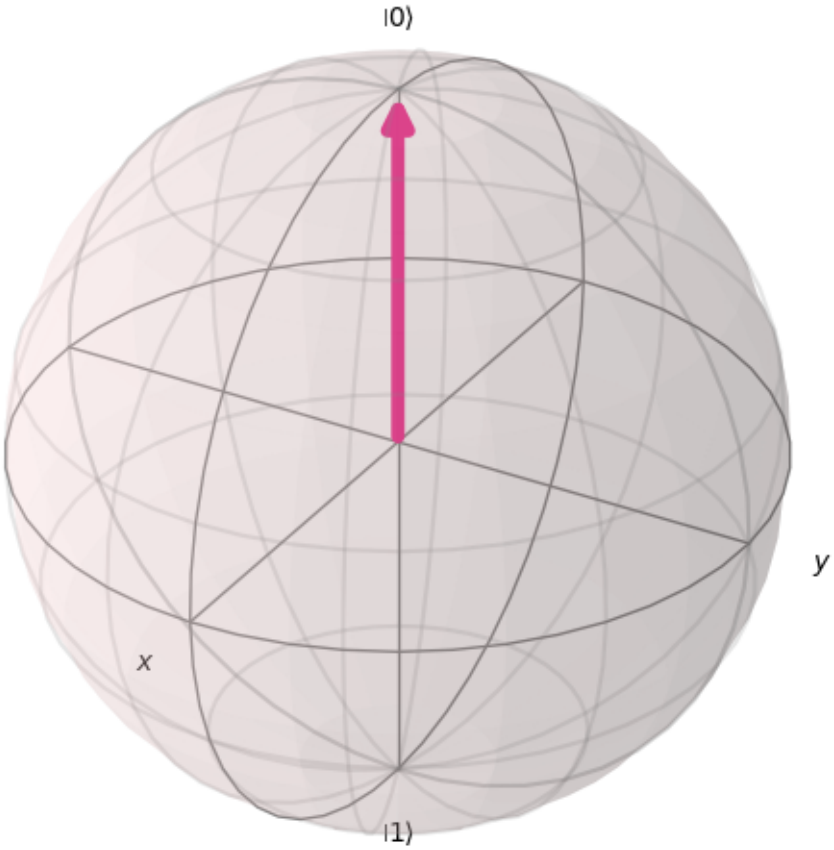


Figure 4.2. Names, symbols, and unitary matrices for the common single qubit gates.

[6]:
```
from math import pi
from qiskit_textbook.widgets import plot_bloch_vector_spherical
```

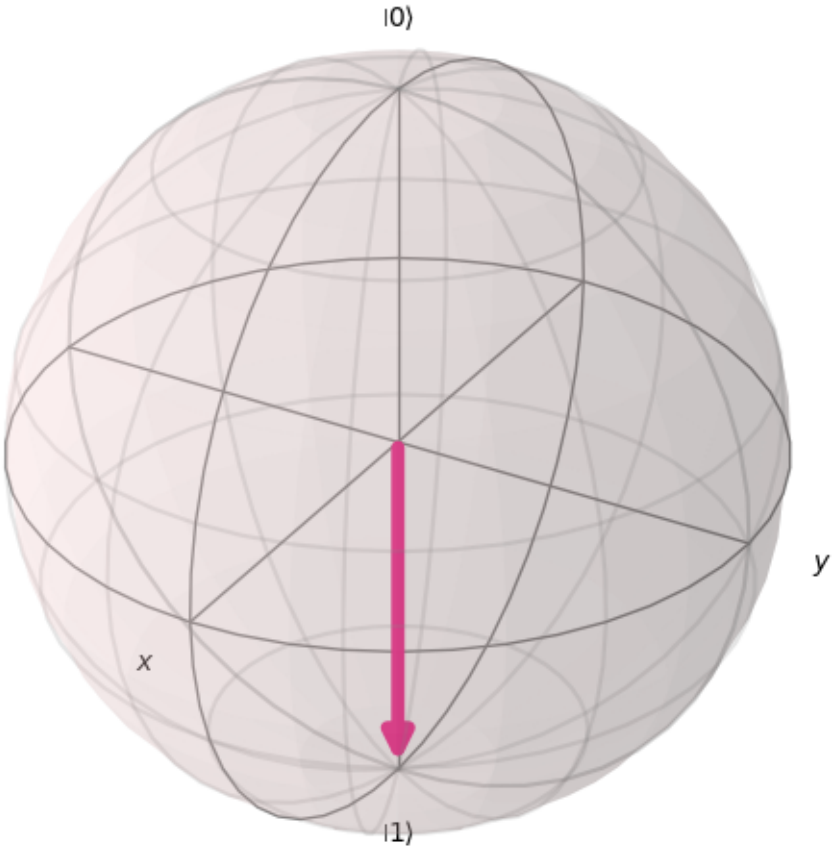
[7]:
```
coords = [0,0,1] # [Theta, Phi, Radius]
plot_bloch_vector_spherical(coords)
```

[7]:



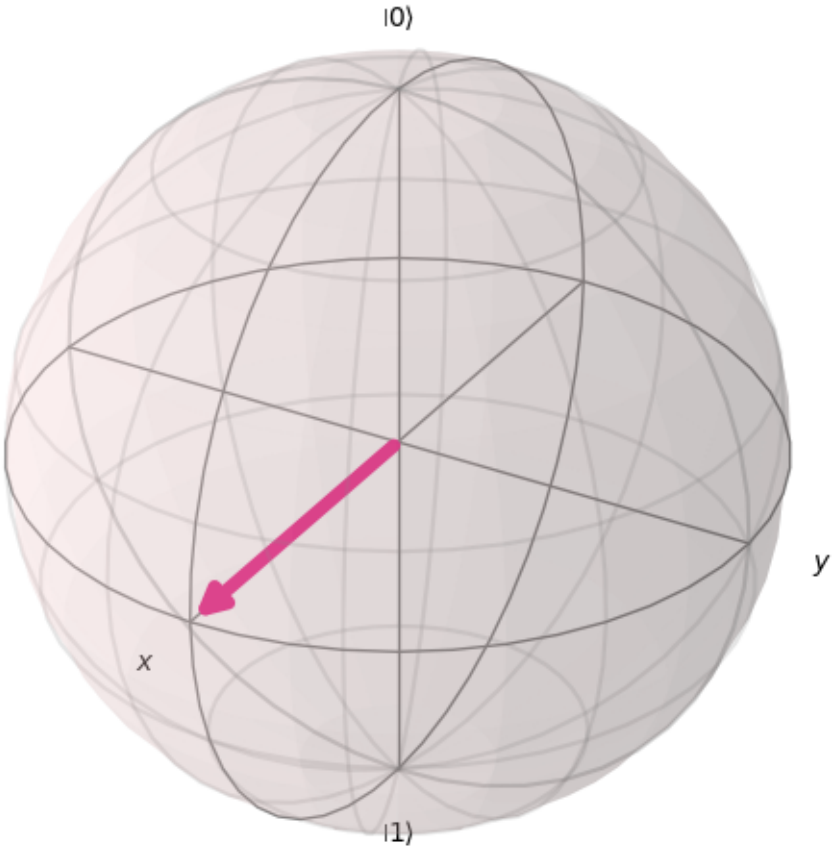
[8]:
```
coords = [pi,0,1] # [Theta, Phi, Radius]
plot_bloch_vector_spherical(coords)
```

[8]:



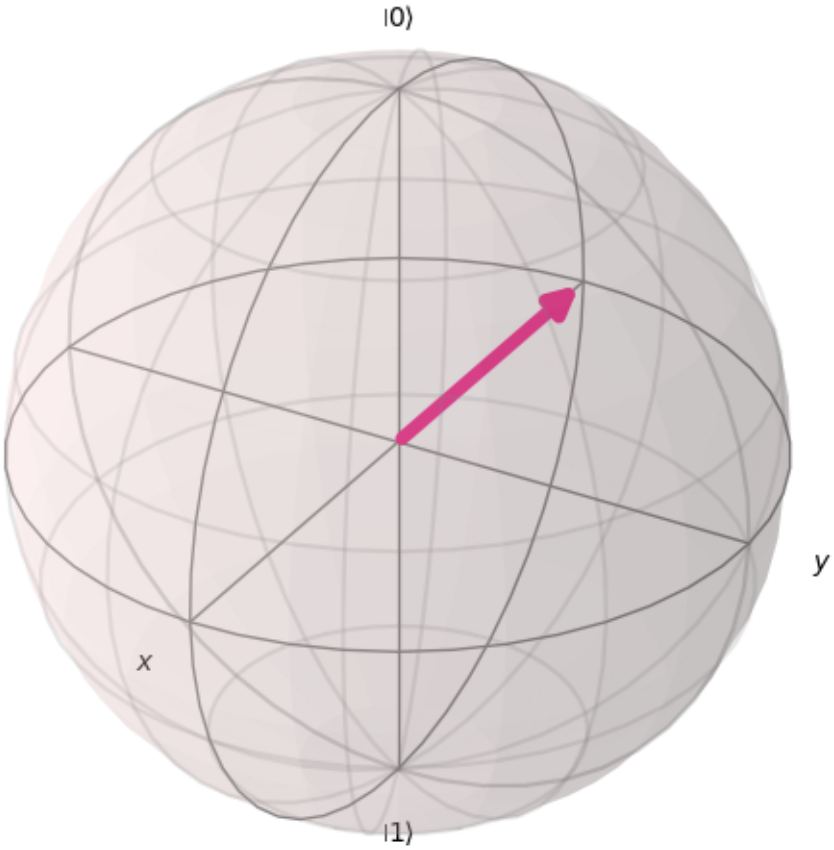
[9]:
```
coords = [pi/2,0,1] # [Theta, Phi, Radius]
plot_bloch_vector_spherical(coords)
```

[9]:



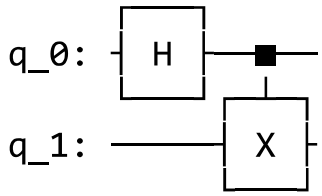
[10]:
```
coords = [pi/2,pi,1] # [Theta, Phi, Radius]
plot_bloch_vector_spherical(coords)
```

[10]:


|0⟩
y
x
|1⟩

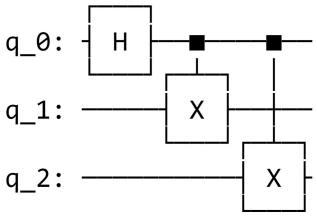
[1]:
```
import qiskit
```

[12]:
```
# For preparing Bell state \beta_{00} using |00⟩
from qiskit import QuantumCircuit, transpile, assemble, Aer, execute
from math import sqrt

# Create a quantum circuit with 2 qubits
circuit = QuantumCircuit(2)

# Apply Hadamard gate (H) to the first qubit
circuit.h(0)

# Apply CNOT gate (CX) between the first qubit and the second qubit
circuit.cx(0, 1)

# Visualize the circuit
print(circuit)

# Simulate the circuit
simulator = Aer.get_backend('statevector_simulator')
job = execute(circuit, simulator)
result = job.result()
statevector = result.get_statevector()

# Print the resulting statevector
print("Resulting Statevector:")
print(statevector)
```




```
Resulting Statevector:
Statevector([0.70710678+0.j, 0.        +0.j, 0.        +0.j,
             0.70710678+0.j],
            dims=(2, 2))
```

[13]:
```
# Create a quantum circuit with 3 qubits
circuit = QuantumCircuit(3)

# Apply Hadamard gate (H) to the first qubit
circuit.h(0)

# Apply CNOT gate (CX) between the first qubit and the second qubit
circuit.cx(0, 1)

# Apply CNOT gate (CX) between the first qubit and the third qubit
circuit.cx(0, 2)

# Visualize the circuit
print(circuit)

# Simulate the circuit
simulator = Aer.get_backend('statevector_simulator')
job = execute(circuit, simulator)
result = job.result()
statevector = result.get_statevector()

# Print the resulting statevector
print("Resulting Statevector:")
print(statevector)
```




```
Resulting Statevector:
Statevector([0.70710678+0.j, 0.        +0.j, 0.        +0.j,
             0.        +0.j, 0.        +0.j, 0.        +0.j,
             0.        +0.j, 0.70710678+0.j],
            dims=(2, 2, 2))
```

3 CONCLUSION

"Quantum Computation and Quantum Information"presents a well-structured sequence of topics that gradually immerse readers into the profound and transformative field of quantum computation and information theory. Through this journey, readers gain the knowledge and tools to appreciate the potential impact of quantum technologies on computing, communication, and cryptography, setting the stage for future advancements in this exciting and rapidly evolving field.