Chapter 1
Fundamentals of Quantum Computation and Basic Quantum Gates

Swathi Mummadi
National Institute of Technology Karnataka, India

Bhawana Rudra
National Institute of Technology Karnataka, India

ABSTRACT

Quantum computing plays a major role in modern computation. It can perform operations exponentially faster when compared to classical computation. It has applications in various areas like Secure communication, Drug design, Artificial Intelligence, Cyber security, etc. Thus the researchers and students are showing interest to perform experiments in quantum computing to design novel architectures. But to learn/understand quantum computing, one should have strong knowledge of its basics. Because quantum computing performs operations at the atomic level, so the learners need to understand basic concepts like Qubits, Superposition, Quantum gates, etc. Therefore this chapter gives a clear idea about the basic concepts of quantum computing like Qubits, Superposition, Entanglement, Teleportation, and Quantum gates.

INTRODUCTION

Quantum computing and Quantum communications are exciting frontiers in computing and communications. It has many advantages over classical computing. Quantum computing was first introduced by Paul Benioff in the early 1980s (Gill et al., 2020). He developed a Turing machine by applying quantum mechanical principles. Richard Feynman proved that quantum computers are exponentially powerful compared to classical computers (Feynman, 1986). This experiment was a big breakthrough and motivated many researchers to enact quantum technology in various fields like secure communication, Finance, Drug design, simulations, chemistry, smart city transportation, agriculture and many more. In the year 1994,

DOI: 10.4018/978-1-6684-6697-1.ch001

Peter Shor introduced an algorithm named Shor's algorithm for integer factorization (Shor, 1995). With this algorithm, it has been proved that the RSA algorithm can easily breakable by a quantum computer where as a worlds powerful super computer will take millions of years to break this algorithm. Most of the current security systems are implemented based on the RSA algorithm (Bernstein et al., 2017; Zhou & Tang, 2011). Due to this, the research in quantum computing has increased to develop quantum safe security systems. Various companies are working on the development of full-fledged Quantum computers to overcome the issues of classical computers and to solve complex problems in various fields. Initially, all the quantum experiments were performed either mathematically or theoretically. With the existence of a quantum computer, it is possible to perform experiments on a real quantum computer and can observe how the quantum particles are reacting to the various operations. The major problem with current quantum systems is noise. In quantum system, the quantum states are generated from the photon particles. Due to the inbuilt property of photon particles, whenever the operations are performed with these particles it leads to the noise. Because of this the currently available quantum systems are in Noisy Intermediate Scale Quantum (NISQ) level (Ippoliti et al., 2021; Tannu & Qureshi, 2019).

Classical computers deal with binary information, i.e., 0 and 1, but Quantum computers perform operations on atomic and subatomic particles. An atom performs operations based on principles of Physics. Hence in Quantum computing, the information is represented in the form of qubits. It can store an infinite range of values between 0 and 1 in multiple states so that Quantum computers can perform multiple operations simultaneously (Benioff, 1982). Due to this, one can say that quantum computers are highly efficient than the world's best Supercomputers. Efficient quantum algorithms like Shor's and Grover's algorithms (Jingle et al., 2022; Long, 2001; Paler & Basmadjian, 2022; Rossi et al., 2022; Saha et al., 2022) solve classical security and searching problems in very little time. The multiple advantages of quantum computing are attracting researchers to work in this area. But the information regarding this technology is very less, so it is difficult for the people to understand the basic concepts of quantum computing. Especially to work in quantum technology, one should have a strong knowledge on quantum basics. Hence this chapter gives a clear idea about the basic concepts of Quantum computing.

MOTIVATION AND OBJECTIVE

Quantum computing has many advantages in various fields like Chemistry, Mechanics, Security, Communication, Machine learning and many more. Due to this the research in this area has been increased. Even in many universities and college, Quantum Computing has been introduced as a subject. But the major problem for the students and researchers who are willing to work in this field are lack of basic knowledge in Quantum Computing. In Quantum, operations are performed based on the reversible computation. Even all the quantum gates are developed based on the reversible concept only. So for a new comer it is very important to understand reversible computation and quantum gates in order to develop Quantum circuits or algorithms. Hence it motivated us to write a chapter on Basic principles of Quantum computing, Reversible computation and Quantum gates. The major contributions of this chapter are as follows:

Detailed discussion on basic principles of quantum computing like Superposition, Entanglement, etc.
Detailed discussion on single and multi qubit quantum gates with block diagram and truth tables.