Chapter 3

ALGORITHMS

INTRODUCTION

Quantum algorithms make use of several specific features of the quantum world, for example quantum superposition, to get from classical inputs, through entangled states, to classical outputs more efficiently than classical algorithms. A variety of quantum algorithms are presented in this chapter. They range from pioneering algorithms, simple but powerful, for several promise problems, through seminal Shor's algorithms and a variety of algorithms for various search problems and their modifications, due to Grover and others.

Design of faster-than-classical quantum algorithms for important algorithmic problems has been an interesting intellectual adventure and achievement. Their existence keeps being one of the key stimuli to those trying to overcome enormous technology problems to build (powerful) quantum computers.

Methods to design quantum algorithms and to show limitations of quantum power have also been developed gradually and will be presented and illustrated in this chapter.

LEARNING OBJECTIVES

The aim of the chapter is to learn:

1. the power of quantum superpositions, parallelism and entanglement;
2. the efficient quantum algorithms for several basic promise problems;
3. the quantum Fourier transform and its properties and implementation;
4. Shor's quantum algorithms for integer factorization and discrete logarithm computation;
5. the hidden subgroup problems and their role in quantum computing;
6. a variety of search algorithms due to Grover and others;
7. methods to design efficient quantum algorithms;
8. methods to show lower bounds and limitations of quantum computing.