

Chapter 4

Quantum circuit

Quantum circuit model $\rightarrow$ universal quantum gates

4.1 Quantum algorithms

problems of classical computation $\rightarrow$ requirement of astronomical resources.

new algorithms of quantum computation

- Shor's *quantum Fourier transformation*
- Grover's algorithm for performing *quantum searching*

The quantum search algorithm has many potential applications,

- can be used to extract statistics from an unordered data set
- can be used to speed up algorithms for some problems in **NP**
- can be used to speed up the search for keys to cryptosystems such as DES

The quantum Fourier transform also has many interesting applications

- to solve the discrete logarithm and factoring problems.

- finding hidden subgroup (a generation of finding the period of a periodic function)

This chapter will provide an efficient and powerful language for describing quantum algorithms, the language of quantum circuits – assemblies of discrete sets of components which describe computational procedures.