Chapter 121 Quantum Computing and Quantum Communication

Göran Pulkkis
Arcada University of Applied Sciences, Finland

Kaj J. Grahn
Arcada University of Applied Sciences, Finland

ABSTRACT

This chapter presents state-of-the-art and future perspectives of quantum computing and communication. Timeline of relevant findings in quantum informatics, such as quantum algorithms, quantum cryptography protocols, and quantum computing models, is summarized. Mathematics of information representation with quantum states is presented. The quantum circuit and adiabatic models of quantum computation are outlined. The functionality, limitations, and security of the quantum key distribution (QKD) protocol is presented. Current implementations of quantum computers and principles of quantum programming are shortly described.

INTRODUCTION

Quantum computing and quantum communication are based on quantum physics. Information is represented by quantum states defined by energy levels of molecules, atoms, and photons. Quantum information technology includes quantum computers, other quantum information processing devices, quantum programming methodologies, and quantum communication applications such as quantum key distribution systems and quantum signatures. Error correction is a necessary quantum information technology property because of high error vulnerability caused by quantum physics characteristics. This article presents state-of-the-art and future perspectives of quantum computing and communication.

BACKGROUND

Feynman's (1982) observation, that a classical computer cannot efficiently simulate the stochastic parallelism of quantum states, started research on using quantum mechanical effects for efficient information processing. Operating principles and implementation possibilities of quantum computing were outlined in Oxford University (Deutsch, 1985).

DOI: 10.4018/978-1-5225-7598-6.ch121

Bennett and Brassard (1984) proposed a quantum protocol, BB84, for perfectly secret information transfer. Efficient quantum algorithms, for example integer factorization (Shor, 1994) and unsorted search (Grover, 1996), were proposed. BB84 has been used for distribution of symmetric encryption/decryption keys (Quantum Key Distribution, QKD) in research networks (Elliot, Pearson, & Troxel, 2004; Quellette, 2004; Poppe, Momtchil, & Maurhart, 2008). Commercial QKD technology has been available over 10 years. Quantum digital signatures have been proposed and experimentally verified (Gottesman & Chuang, 2001; Lu & Feng, 2005; Clarke et al., 2012).

Small scale quantum circuit based computers have been built and successfully tested in research laboratories (Vandersypen et al., 2001; Monz et al., 2011). Since 2011 large scale commercial adiabatic quantum computers (Das & Chakrabarti, 2008) are available.

Achievements in quantum computing and quantum communication from 1970 till October 2015 are listed in (Timeline, 2015). Universities engaged in research and education on this topic are for example (qis.mit.edu, 2013; …from Quantum, 2011; mathQI, 2015; Quantum, 2015a; Quantum, 2015b)

INFORMATION REPRESENTATION WITH QUANTUM STATES

Two quantum states, for which a state transition exists, can represent a bit called a quantum bit or qubit, if the energy level of both states is measurable. However, quantum states are probabilistic. A measured energy level is one of several possibilities. Each possible outcome has a probability. The sum of all possible outcome probabilities is of course 1.

The *No Cloning* qubit property is the impossibility to clone an unknown quantum state. However, *Teleportation*, which changes the original qubit state, can transfer also an unknown quantum state.

Mathematical Treatment of Qubits

A qubit representation is a 2-dimensional vector. The orthogonal base vectors $(1,0)^T,(0,1)^T$ in *Dirac notation* $|0>,|1>$ represent binary values 0,1.

A qubit is a concurrent superposition of $|0>,|1>$. A measurement outcome is $|0>$ or $|1>$. In a qubit

$$|\psi>=a\cdot|0>+b\cdot|1>. \qquad (1)$$

a,b are complex numbers and

$$<\psi||\psi>=(a^*,b^*)\cdot(a,b)^T=a^*\cdot a+b^*\cdot b=|a|^2+|b|^2=1. \qquad (2)$$

$\{a^*,b^*\}$ are complex conjugates of $\{a,b\}$. $\{|a|^2,|b|^2\}$ are measurement probabilities of $|0>,|1>$.

Multiple Qubits

A *2 qubit* quantum state is a 2^2 component column vector. For

$$|\psi_1>=a\cdot|0>+b\cdot|1>,\ |\psi_2>=c\cdot|0>+d\cdot|1> \qquad (3)$$