Artificial Intelligence 174 (2010) 162–176

Contents lists available at ScienceDirect

Artificial Intelligence

www.elsevier.com/locate/artint

Quantum computation, quantum theory and AI ☆

Mingsheng Ying [a,b,*]

[a] Center of Quantum Computation and Intelligent Systems, Faculty of Engineering and Information Technology, University of Technology, Sydney, Australia
[b] State Key Laboratory of Intelligent Technology and Systems, Tsinghua National Laboratory for Information Science and Technology, Department of Computer Science and Technology, Tsinghua University, China

A R T I C L E I N F O

Article history:
Received 30 July 2009
Received in revised form 8 September 2009
Accepted 19 September 2009
Available online 18 November 2009

Keywords:
Quantum computation
Quantum theory
Search
Learning
Discrimination and recognition
Bayesian network
Semantic analysis
Communication

A B S T R A C T

The main purpose of this paper is to examine some (potential) applications of quantum computation in AI and to review the interplay between quantum theory and AI. For the readers who are not familiar with quantum computation, a brief introduction to it is provided, and a famous but simple quantum algorithm is introduced so that they can appreciate the power of quantum computation. Also, a (quite personal) survey of quantum computation is presented in order to give the readers a (unbalanced) panorama of the field. The author hopes that this paper will be a useful map for AI researchers who are going to explore further and deeper connections between AI and quantum computation as well as quantum theory although some parts of the map are very rough and other parts are empty, and waiting for the readers to fill in.

1. Introduction

Quantum theory is without any doubt one of the greatest scientific achievements of the 20th century. It provides a uniform framework for the construction of various modern physical theories. After more than 50 years from its inception, quantum theory married with computer science, another great intellectual triumph of the 20th century and the new subject of quantum computation was born.

Quantum computers were first envisaged by Nobel Laureate physicist Feynman [47] in 1982. He conceived that no classical computer could simulate certain quantum phenomena without an exponential slowdown, and so realized that quantum mechanical effects should offer something genuinely new to computation. In 1985, Feynman's ideas were elaborated and formalized by Deutsch in a seminal paper [30] where a quantum Turing machine was described. In particular, Deutsch introduced the technique of quantum parallelism based on the superposition principle in quantum mechanics by which a quantum Turing machine can encode many inputs on the same tape and perform a calculation on all the inputs simultaneously. Furthermore, he proposed that quantum computers might be able to perform certain types of computation that classical computers can only perform very inefficiently.

One of the most striking advances was made by Shor [91] in 1994. By exploring the power of quantum parallelism, he discovered a polynomial-time algorithm on quantum computers for prime factorization of which the best known algorithm

☆ This work was partly supported by the National Natural Science Foundation of China (Grant Nos. 60736011, 60621062) and the National Key Project for Fundamental Research of China (Grant No. 2007CB807901).

* Address for correspondence: Center of Quantum Computation and Intelligent Systems, Faculty of Engineering and Information Technology, University of Technology, Sydney, Australia.

E-mail address: mying@it.uts.edu.au.

0004-3702/$ – see front matter
doi:10.1016/j.artint.2009.11.009

on classical computers is exponential. In 1996, Grover [52] offered another killer application of quantum computation, and he found a quantum algorithm for searching a single item in an unsorted database in square root of the time it would take on a classical computer. Since database search and prime factorization are central problems in computer science and cryptography, respectively, and the quantum algorithms for them are much faster than the classical ones, Shor and Grover's works stimulated an intensive investigation in quantum computation. Since then, quantum computation has been an extremely exciting and rapidly growing field of research.

Since it revolutionized the very notion of computation, quantum computation forces us to reexamine various branches of computer science, and AI is not an exception. Roughly speaking, AI has two overall goals: (1) engineering goal – to develop intelligent machines; and (2) scientific goal – to understand intelligent behaviors of humans, animals and machines [75]. AI researchers mainly employ computing techniques to achieve both the engineering and scientific goals. Indeed, recently, McCarthy [8] even pointed out that "computational intelligence" is a more suitable name of the subject of AI to highlight the key role played by computers in AI. Naturally, the rapid development of quantum computation leads us to ask the question: how can this new computing technique help us in achieving the goals of AI. It seems obvious that quantum computation will largely contribute to the engineering goal of AI by applying it in various AI systems to speedup the computational process, but it is indeed very difficult to design quantum algorithms for solving certain AI problems that are more efficient than the existing classical algorithms for the same purpose. At this moment, it is also not clear how quantum computation can be used in achieving the scientific goal of AI, and to the best of my knowledge there are no serious research pursuing this problem. Instead, it is surprising that quite a large amount of literature is devoted to applications of quantum theory in AI and vice versa, not through quantum computation. It can be observed from the existing works that due to its inherent probabilistic nature, quantum theory can be connected to numerical AI in a more spontaneous way than to logical AI.

The aim of this paper is two-fold: (1) to give AI researchers a brief introduction and a glimpse of the panorama of quantum computation; and (2) to examine connections between quantum computation, quantum theory and AI. The remainder of the paper is organized as follows: Section 2 is a tutorial of quantum computation for readers who are not familiar with quantum computation and quantum theory. Section 3 surveys some areas of quantum computation which the author is familiar with. Some potential applications of quantum computation in AI are considered in Section 4, and the interplay between quantum theory and AI is discussed in Section 5. A brief conclusion is drawn in Section 6.

2. A tutorial of quantum computation

For convenience of the readers, I will give a very brief introduction to quantum computation in this section. The fundamental principles of quantum theory are embodied very well in the basic apparatus of quantum computation. To illustrate the power of quantum computation, I will present the Deutsch–Jozsa algorithm which I believe to be one of the best examples that a newcomer can appreciate. For more details, we refer to the excellent textbook [74].

2.1. Qubits and quantum registers

The basic data unit in a quantum computer is a qubit, which can be physically realized by a two-level quantum-mechanical system, e.g. the horizontal and vertical polarizations of a photon, or the up and down spins of a single electron. Mathematically, a qubit is represented by a unit vector in the two-dimensional complex Hilbert space, and it can be written in the Dirac notation as follows:

$$|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle, \tag{1}$$

where $|0\rangle$ and $|1\rangle$ are two basis states, and α_0 and α_1 are complex numbers with $|\alpha_0|^2 + |\alpha_1|^2 = 1$. The states $|0\rangle$ and $|1\rangle$ are called computational basis states of qubits. Obviously, they correspond to the two states 0 and 1 of classical bits. The number α_0 and α_1 are called probability amplitudes of the state $|\psi\rangle$. A striking difference between classical bits and qubits is that the latter can be in a superposition of $|0\rangle$ and $|1\rangle$ in the form of Eq. (1). An example state of qubit is: $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$.

A quantum register is formed by putting multiple qubits together. A state of a quantum register consisting of n qubits is described in the following way:

$$|\psi\rangle = \sum_{t\in\{0,1\}^n} \alpha_t|t\rangle = \sum_{t_1,t_2,\dots,t_n\in\{0,1\}} \alpha_{t_1t_2\dots t_n}|t_1t_2\dots t_n\rangle, \tag{2}$$

where the complex numbers $\alpha_{t_1t_2\dots t_n}$ are required to satisfy the normalization condition:

$$\sum_{t\in\{0,1\}^n} |\alpha_t|^2 = \sum_{t_1,t_2,\dots,t_n\in\{0,1\}} |\alpha_{t_1t_2\dots t_n}|^2 = 1.$$

The state $|\psi\rangle$ in Eq. (2) is a superposition of the computational basis states $|t_1t_2\dots t_n\rangle$ $(t_1,t_2,\dots,t_n = 0,1)$ of the quantum registers. The numbers $\alpha_{t_1t_2\dots t_n}$'s are the probability amplitudes of $|\psi\rangle$. We can also write:

$$|\psi\rangle = \sum_{t=0}^{2^n-1} \alpha_t|t\rangle$$