International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2020 IJSRCSEIT | Volume 6 | Issue 3 | ISSN : 2456-3307
DOI : https://doi.org/10.32628/CSEIT206321

The Road to Quantum Computational Supremacy

Rahul Kumar, Shivraj Patil
B. Tech Scholar, Department of Computer Science and Engineering, Amity University Jharkhand, India

ABSTRACT

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.

Keywords : Quantum Computation, Quantum Theory

I. 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 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. First and foremost, quantum computing cannot compute all partial functions a universal Turing machine can calculate because only total functions can be computed by quantum circuits . Consequently, quantum computing potential advantages could come only from faster than classical computations.

While Shor's algorithm, Deutsch-Jozsa algorithm and various others in the "black-box" paradigm are believed to provide an exponential speedup over classical computers, this is far from the case in general. We said "believed" because the superiority of Shor's quantum algorithm over classical ones is still an open problem and various techniques allowing efficient classical simulation of quantum algorithms have been successfully developed even for some "black-box" quantum ones. In fact, since the introduction of Shor's and Grover's algorithms some twenty years ago, the development within the field of quantum algorithmics has been rather slow for a global picture—and many of them are novel Where access to a quantum black-box or "oracle" with certain structural properties is assumed.

The second reason is that there really might be relatively few problems for which quantum computers can offer a substantial speed-up over classical computers, and we may have already discovered many or all of the important techniques for constructing quantum algorithms.

What is quantum computational supremacy?

The quantum computational advantage for simulating quantum systems was first stated by Feynman in 1982, in one of the pioneering papers in quantum computing . According to the data processing inequality (classical) post-processing cannot increase information. This suggests that to run an accurate classical simulation of a quantum system one must know a lot about the system before the simulation is started . The postulate of quantum computation: Computational devices based on quantum mechanics will be computationally superior compared to digital computers.

A spectacular support for this postulate came from Shor's 1994 polynomial factoring quantum algorithm in spite of the fact that the problem whether factoring is in P was, and still is, open. The belief that factoring integers is computationally hard is essential for much of modern cryptography and computing security.

Criteria for quantum computational supremacy

1. a well-defined computational problem,
2. a quantum algorithm solving the problem which can run on a near-term hardware capable of dealing with noise
1. and imperfections,
2. an amount of computational resources (time/space) allowed to any classical competitor,
3. a small number of well-justified complexity-theoretic assumptions,
4. a verification method that can efficiently distinguish between the performances of the quantum algorithm from any classical competitor using the allowed resources.

Is the quest for quantum computational supremacy worthwhile?

Let us examine closer the foundational gain. A successful quantum supremacy experiment could be a complement to

Bell experiment: the latter refuted local hidden models of quantum mechanics, while the former seems to invalidate the Extended Church-Turing Thesis . The paper discusses the advantages of a successful quantum supremacy experiment, even one that barely surpasses any classical competitor, illustrated with hard-to-simulate classical systems like protein folding or fluid dynamics.

The Extended Church-Turing Thesis—which incidentally has nothing to do with either Church nor Turing—is a foundational principle of classical complexity theory which ensures that the polynomial time class P is well defined. The Thesis places strong constraints, one of them being that the model of computation is digital.

At first glance quantum computers (and, more generally, quantum systems) appear to be analog devices, since a quantum gate is described by a unitary transformation, specified by complex numbers; a more in-depth analysis is still required. This amounts to prove that any computation performed by any quantum computer can be simulated by a classical machine in polynomial time

Models of quantum computation

Quantum Turing machine and quantum automata

The models of quantum computation have their ancestors from the studies of connections between physics and computation. In 1973, to understand the thermodynamics of classical computation Bennet noted that a logically reversible operation does not need to dissipate any energy and found that a logically reversible Turing machine is a theoretical possibility.

Quantum circuits

Quantum circuits has become the most popular model of quantum computation in which most of the existing quantum algorithms are expressed.Synthesis of quantum circuits is crucial for quantum computation due to the fact that in current technologies it is very difficult to implement quantum gates acting on three or more qubits. As early as in 1995, it was shown that any quantum gate can be (approximately) decomposed to a circuit consisting only of the CNOT gates and a small set of single qubit gates.

Adiabatic quantum computation

Quantum Turing machine, quantum automata and quantum circuits are quantum generalizations of their classical counterparts.

In adiabatic quantum computation, the evolution of the quantum register is governed by a Hamiltonian that varies slowly. The state of the system is prepared at the beginning in the ground state of the initial Hamiltonian. The solution of a computational problem is then encoded in the ground state of the final Hamiltonian. The quantum adiabatic theorem guarantees that the final state of the system will differ from the ground state of the final Hamiltonian by a negligible amount provided. The adiabatic model provides a new way of designing quantum algorithms; for example, the Grover's algorithm has been recast in the adiabatic model.

Measurement-based quantum computation

Another model of quantum computation without a classical counterpart is measurement-based computation. In the quantum Turing machine and quantum circuits, measurements are mainly used at the end to extract computational outcomes from quantum states.

Distributed quantum computation

A natural idea is to use the physical resources of two or more small capacity quantum computers to simulate a large capacity quantum computer; for example, a distributed implementation of Shor's quantum factoring algorithm is presented in . Another major motivation comes from the studies of quantum communication. By employing quantum mechanical principles, some provably secure communication protocols have been proposed, and quantum communication systems using these protocols are already commercially available.

Logical foundations of quantum computation

Categorical quantum logic

Currently, quantum algorithms and communication protocols are expressed mainly at the very low level of quantum circuits. We learned in classical computation that high-level description is very useful for design and analysis of algorithms and protocols because it enables us to think about a problem that we intend to solve in a conceptual way, rather than the details of implementation. However, high-level description techniques are still lacking in quantum computation.

Quantum lambda calculus

The lambda calculus is a formalism of high-order functions and it is a logical basis of some important classical functional programming languages such as

LISP, Scheme, ML and Haskell. A quantum generalization of λ-calculus was first introduced by Tonder The no-cloning property of quantum data makes quantum lambda calculus closely related to linear lambda calculus developed by the linear logic community. In a series of papers Selinger and Valiron systematically develop quantum lambda calculus. In particular, quantum lambda calculus was used by them to provide a fully abstract model.

Quantum computational logic

Propositions in quantum logic are interpreted as closed subspaces of the state space (a Hilbert space) of a quantum system, or their algebraic abstraction, elements of an orthomodular lattice, and logical connectives are then naturally interpreted as the operations in the orthomodular lattice.

Quantum algorithms

Research on quantum algorithms has been the driving force of the whole field of quantum computation because some quantum algorithms indicate that quantum computation may provide considerable speedup over classical computation.

Quantum computer architectures

Progress in the techniques of quantum devices has made people widely believe that large-scalable and functional quantum computers will eventually be built. Architecture design will become more and more important as the size of quantum computers grows. Quantum computer architecture is another area that I am not familiar with. What I know is merely that research in quantum computer architectures is still in its infancy and there are only few papers devoted to this topic.

Quantum programming

Our experiences with classical computation suggest that when quantum computers become available in the future, quantumsoftwares will play a key role in exploiting their power. Unfortunately, today's software development methodologies and techniques are not suited to quantum computers due to essential differences between the nature of the classical world and that of the quantum world. To lay a solid foundation for tomorrow's quantum software development techniques, it is critically essential to pursue systematic research into quantum programming.

The earliest proposal for a quantum programming language was made by Knill . The first real quantum programming language, QCL, was proposed by Omer he also implemented a simulator for this language. A quantum programming language in the style of Dijkstra's guarded-command language, qGCL, was designed by Sanders and Zuliani . A quantum extension of C++ was proposed by Bettelli et al. and implemented in the form of a C++ library.

The essential difference between quantum loops and classical loops comes from quantum measurements in the loop guards. In a fixed finite-dimensional state space, a necessary and sufficient condition under which a quantum loop program terminates on a given input was found by employing Jordan normal form of complex matrices. In particular, it was proved that a small disturbance either on the unitary transformation in the loop body or on the measurement in the loop guard can make any quantum loop (almost) terminate, provided that some obvious dimension restriction is satisfied.

Google quantum computational supremacy

Google sparked controversy in the scientific community by claiming that it has achieved the anticipated milestone known as quantum supremacy.

Interplay between quantum theory and AI

Research arising from the interplay between quantum theory and AI can be roughly classified into two categories: Using some ideas from quantum theory to solve certain problems in AI; and Conversely, applying some ideas developed in AI to quantum theory. We first see how ideas from quantum theory be used in AI by considering two typical examples.

Semantic analysis

Some similarities between the mathematical structure used by the AI community in semantic analysis of natural language and those employed in quantum mechanics were observed in But these similarities exposed in seems very superficial, and they do not convince me to believe that a certain intrinsic connection exists between semantic analysis and quantum mechanics because it is not surprising that the same mathematical tools can be applied in unrelated domains, and indeed universal effectiveness is exactly one of the most important advantages of mathematics. On the other hand, however, observation of these similarities is still useful since by analogy it may provide hints as to how one can borrow some ideas from the well-established subject of quantum mechanics in semantic analysis or even more broadly in AI.

Quantum Bayesian networks

Statistical inference is at the heart of quantum theory due to the essential probabilistic nature of quantum systems. Bayesian methods have been widely used in statistical inference in the classical world. Recently, several versions of quantum Bayes rule have been derived in the physics literature Bayesian networks are graph models for representing and reasoning about probability information and widely used in AI. It is hoped that this kind of graph model can be adopted in reasoning about the behaviors of large systems in the quantum world.

Recognition and discrimination of quantum states and quantum operations

Pattern recognition is an important area of AI, and discrimination of objects can be seen as a special case of pattern recognition. However, only recognition and discrimination of classical objects have been considered by AI researchers. In the last 20 years, a large amount of work on discrimination and recognition of quantum states and quantum operations has

been conducted by physicists without knowing much about existing AI work.

Conclusion

This paper identifies three classes of opportunities for AI researchers at the intersection of quantum computation, quantumtheory and AI:

- Design quantum algorithms to solve problems in AI more efficiently;
- Develop more effective methods for formalizing problems in AI by borrowing ideas from quantum theory;
- Develop new AI techniques to deal with problems in the quantum world.

The first class of research is still in the initial stage of development, and not much progress has been made listed some reasons to explain why quantum algorithms are so hard to discover. Unfortunately, these reasons are valid for the problems in AI too.

In particular, more experimental research is required to test the effectiveness. It appears that research in the third class is making steady progress. My main concern is whether the AI techniques developed in this class of research will be useful in quantum physics and will be appreciated by physicists. Certainly, collaboration between AI researchers and physicists will highly benefit the development of this area. Perhaps, experience from bioinformatics can be used for reference where close collaboration between computer scientists and biologists frequently happens and leads to high impact research.

II. REFERENCES

[1]. S. Abramsky, High-level methods for quantum computation and information, in: Proceedings of the 19th Annual IEEE Symposium on Logic in Computer Science, pp. 410–414.

[2]. S. Abramsky, B. Coecke, A categorical semantics of quantum protocols, in: Proceedings of the 19th Annual IEEE Symposium on Logic in Computer Science, pp.

[3]. S. Abramsky, R. Duncan, A categorical quantum logic, Mathematical Structures in Computer Science 16 (2006) 469–489.

[4]. A. Acin, Statistical distinguishability between unitary operations, Physical Review Letters 87 (2001), art. no. 177901.

Cite this article as :

Rahul Kumar, Shivraj Patil, "The Road to Quantum Computational Supremacy", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 6, Issue 3, pp.146-151, May-June-2020. Available at
doi : https://doi.org/10.32628/CSEIT206321
Journal URL : http://ijsrcseit.com/CSEIT206321