数理解析研究所講究録
1166 巻 2000 年 76-85

QUANTUM MODELS AND MODES OF COMPUTATION AND COMMUNICATION

Jozef Gruska[1], Roland Vollmar[2]
[1] Faculty of Informatics, Masaryk University
Botanická 68a, 602 00 Brno, Czech Republik
[2]Fakultät für Informatik, Universität Karlsruhe
Am Fasanengarten 5, 76128 Germany

Abstract

The paper deals with the main approaches to quantum computing and communication models and modes. In addition, it discusses briefly various specific issues connected with quantum models of computation and communication – their importance and impacts.

1 Introduction

There are several reasons why it is important to explore various models and modes of quantum computation and communication.

- An understanding has emerged that foundations of computing and communication should be based on the quantum physics laws and limitations and not on the classical physics.
- An understanding has emerged that quantum processors can be of large importance for simulation of quantum phenomena and, hopefully, also for computation, and therefore we need to explore models of quantum computation and communication.[2]
- An understanding has emerged that quantum resources are not cheap and therefore there is a big need for a more detailed investigation of the power of the models and modes of quantum computation with limited or imperfect quantum resources.
- An understanding is emerging that outcomes of quantum information processing and communication (QIPC) research, and byproducts of the experimental attempts to massage some of the most advanced current technologies to perform rudimentary computations, can have important and broad impacts also outside of QIPC.

There are also three new features to deal and cope with when considering new quantum models and modes of computation: new (quantum) elements, new (quantum) resources and new (quantum) limitations. Let us discuss briefly all of them.

[1]Paper has been written mainly during the first author stay at the University of Karlsruhe, Department of Informatics, in summer 2000. Support of the grants GAČR 201/98/0369, CEZ:J07/98:143300001 and VEGA 1/7654/20 is to be acknowledged.

[2]Several technical results are behind. At first the proof by Bernstein and Vazirani (1993) that there exist efficient universal Turing machines. Secondly, the result of Simon (1994) that quantum computers seem to be exponentially more powerful than the classical ones. Thirdly, the result by Shor (1994) that quantum computers could solve much more efficiently some important practical problems than the best known classical algorithms. Fourthly, the result due to Lloyd (1996), that there are efficient universal quantum simulators. Finally, the result by Bennett at al. (1993) that quantum teleportation works.

The research in the area of models and modes of quantum computation and communication has the following main goals.

- To get insights into the power of different quantum computing models and modes using automata-theoretic methods and concepts.
- To get insights (and some qualitative and quantitative understanding) into the power of various quantum resources (superposition, parallelism, entanglement, measurement).
- To explore the potential of the most simple models of quantum computing (the very basic quantum processors are expected to perform quantum actions on the classical inputs).
- To explore, using at first the simplest models of quantum computation, how much of quantumness is needed and how pure it has to be in order to have automata (machines or algorithms) more powerful than the classical ones.
- To develop design and optimization methodologies at first for very simple models of quantum computation.
- To develop lower bound techniques for showing limitations first for the simplest models of quantum processors.

For a detailed presentation of quantum computing see the book by Gruska (1999) and its web extensions. For a more concise introduction and overview see Gruska (2000a).

Quantum elements. New basic elements are pure and mixed quantum states, unitary operations and superoperators; quantum bits, registers and parallelism; quantum gates, circuits and quantum measurements (projection measurements, POVM, non-demolition measurements, interaction-free measurements, ...) for quantum computation and quantum ebits[3], channels and teleportation for quantum communication.

Quantum resources. The most basic resources are quantum superpositions, quantum parallelism, quantum entanglement and quantum measurements (of various types). Each of them has very specific features:

- The power of quantum superposition is due to the fact that it is in principle possible, in one "step", using only a linear number of simple gates, to create an exponentially large superposition of basis states; for example, using the Hadamard transformation on an n qubit register to the basis state $|0^n\rangle$ we can obtain the exponentially large, equally weighted, superposition

$$\frac{1}{\sqrt{n}} \sum_{i=0}^{2^n-1} |i\rangle,$$

of all basis states in the Hilbert space of dimension 2^n (that is the state on which some of the main quantum algorithms work). It is also possible to reduce exponentially large superpositions to a single basis state, in a single computational "step".

[3] we say that the entangled state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ carries one ebit of entanglement.

- Quantum entanglement brings non-locality features into quantum communication and allows "instantaneous" communication between two parties that are far away from each other.

- Quantum measurement allows, indirectly, in some cases, to solve, in some way and in a single "step", a complicated system of constraints.

Quantum limitations. The most fundamental one is the *Heisenberg uncertainty principle* that says that measuring the value of one observable more accurately makes the value of another, noncommutative, observable less certain. In addition, there is a certain intrinsic uncertainty with which values of two observables can be measured, and once a way of measurement is fixed, this uncertainty, in general, increases.

As consequences we have two important limitations for quantum computation:

- *No cloning theorem.* An unknown quantum state cannot be cloned. Namely, there is no unitary transformation U, such that for any one-qubit state $|\psi\rangle$,

$$U(|\psi, 0\rangle) = |\psi, \psi\rangle.$$

  The no cloning theorem seems to be a bad news. For example, it was to a large extent due to this theorem that quantum error-correcting codes seemed to be impossible. One can also hardly imagine how to perform more complex information processing without having a possibility to copy information. However, no cloning theorem is also a good news. Due to the impossibility to copy quantum information safely we have quantum key generation systems that are provably unconditionally secure.

- *Holevo theorem* says that into an n-qubit register state we can encode and later decode safely only n bits.

One additional limitation one gets from the Schrödinger equation.

- *Reversibility of evolutions.* Quantum evolution has to be reversible. This implies that quantum automata have to be reversible. In other words each configuration should uniquely determine the previous one. On the level of Turing machines, this is not an essential limitations as already demonstrated by Bennett (1973), who has shown that any function that can be computed by a one-tape Turing machine can be computed, with constant time overhead only, by a three-tape reversible Turing machine. However, on the level of less powerful computation models reversibility requirement can be a very significant restriction.

2 Quantum computation models and modes

A variety of the models of quantum computing has already been introduced and investigated. Their computational power can be stronger or weaker than that of the corresponding classical models. Their descriptional power can also be (provably) exponentially stronger or weaker than that of their classical counterparts.

From the deterministic through nondeterministic and probabilistic models to quantum models of computation. There are two paths on the way from the deterministic to quantum computations. The first path is through nondeterministic computation models and their natural generalization — probabilistic models. From this point of view

basic quantum models of automata are modifications of the probabilistic models at which probabilities of transitions are replaced by probability amplitudes. However, and this is an important and far from easy to deal with modification, the probability amplitudes have to be assigned in such a way to transitions that the evolution of the corresponding models is unitary. Second path to quantum models of computation is through reversible classical models of computation. Unfortunately it is non easy to combine probabilistic behaviour of automata with quite restrictive requirement on their reversibility and this makes the explorations of quantum models of computation so non easy.

For example, the language 0^*1^* cannot be recognized by any one-way finite reversible classical automaton, but it can be recognized by a one-way quantum automaton with the probability 0.68 and by a classical two-way reversible (and therefore also quantum) automaton with probability 1 (see Gruska (2000) for references).

Main models of quantum automata. From a variety of models of quantum automata three deserves a special attention.

1. *Quantum finite automata* (QFA) QFA are considered to be the simplest model of quantum processors, with "finite" quantum memory, that models well the basic mode of quantum computing — quantum actions are performed on classical inputs.

2. *Quantum Turing machines* (QTM). QTM are used to explore, at the most general level of sequential computation, the potential and limitations of quantum computing. Using this model the main computational complexity classes have been defined. QTM are a main "quantum abstraction of the human computational processes".

3. *Quantum cellular automata* (QCA). QCA are used to model and to explore, on a very general and basic level of parallel computation, the potential and limitations of quantum computing. QCA are a very basic abstraction of the quantum computation processes performed by Nature.

Classical automata models with quantum memory. It is nowadays clear that quantum bits are expensive and therefore a very important task of QIPC research is to find out how much of quantumness is already enough to have models of computation that are already more powerful than classical ones.

For example, it has first been estimated that in order to implement Shor's factorization algorithm to factorize m bit integers one needs $5m$ qubits. A more detailed analysis due to Zalka (1998) shows that $3m$ qubits are sufficient. However, this does not exclude the possibility that there is a different algorithm to factorize integers that is still polynomial in quantum time, but requires much less qubits. Moreover, it has been recently shown, by Parker and Plenio (2000), that to have an efficient factorization, only one pure qubit is needed, the rest of quantum register can be in a mixed state.

An interesting and important outcome of the research in this direction are two-way quantum/classical finite automata (2QCFA) introduced by Ambainis and Watrous (2000). They are ordinary two-way classical automata augmented with a quantum register that can be in a quantum state. The transition function of such an automaton determines, for a given state and a symbol scanned either a classical operation of the automaton (a new state and a movement of the head), and, in addition, a unitary operation to be performed on the quantum memory, or it determines a measurement to be performed on the current quantum state — and the next classical action of the automaton is then determined by the result of the measurement. It has been shown that such automata can accept languages that cannot be accepted by probabilistic two-way finite automata. More exactly, it has

been shown that the language $\{0^i 1^i \mid i \geq 0\}$ can be recognized by a 2QCFA in polynomial time, but this language can be recognized by a two-way classical probabilistic automaton only in exponential time. Moreover, the language of palindromes can be recognized by a 2QCFA, but not by a classical probabilistic two-way finite automaton.

Well-formedness conditions. The basic formal way to develop a quantum version of a classical automata model is to replace in its probabilistic version probabilities of transitions, between configurations, by probability amplitudes for transitions. The main problem is to do this replacement in such a way that a to-be-quantum automaton is really quantum, that is that its evolution is unitary.

A way to deal with this problem is to determine the so called well-formedness conditions (that are easy to verify, if such well-formedness conditions exist), for the transition function of a to-be-quantum automata such that these conditions are satisfied if and only if the evolution of the corresponding automaton is unitary. As one can expect, for quantum universal models of computation there is no effective way to decide whether a particular to-be-quantum automaton satisfies the corresponding well-formedness conditions. This is of course a very essential problem concerning quantum automata that has to be dealt with, especially for the case of quantum cellular automata.

Measurement modes. Various modes of computation depend on what kind of measurements are performed, and when, during the computation process.

In order to investigate potentials of quantum Turing machines and higher level quantum computation complexity classes, it is believed that only simple qubit projection measurements are needed and that the measurement process can be postponed to the very end of the computation.

A different situation is in the case of finite quantum automata. For these models so far only the projection measurements have been used. They project the current state into the set of the accepting configurations, or into the set of rejecting configurations, or into the remaining set of nonterminating configurations. Two basic modes of measurement are then the following ones:

- *Measurement-once (MO) mode*: The measurement is performed only once, at the very end of computation.
- *Measurement-many (MM) mode*: Measurement is performed after each evolution step.

In the case of one-way quantum automata those with MM-mode of computation are more powerful than those with MO-mode of computation, but the later, more exactly the corresponding family of languages, have nicer characterizations and richer closure properties.

In general, the question of the measurement: how often and what types of measurement to perform, is still open and requires further investigations.

Acceptance modes. If quantum automata are considered as acceptors, then they accept, similarly as in the case of probabilistic automata, a given input and a given language with a certain probability. The most basic modes of acceptance are variations of those used in randomized computing: Monte Carlo and Las Vegas acceptance as well as the bounded-error acceptance and the unbounded-error acceptance.

Quantum finite automata with unbounded-error acceptance can be essentially more powerful than those with bounded-error acceptance mode, even though the first type of acceptance is not considered as realistic.

In the case of quantum Turing machine computations, the main computational complexity class is the class **BQP**, a quantum version of the classical complexity class **BPP** —the class of languages accepted in polynomial time with bounded-error and with the cut-point greater than $\frac{1}{2}$. Interesting and important enough, a polynomial time computational equivalence between quantum Turing machines and uniform families of quantum circuits has been shown only for bounded-error computation. It is an important open problem whether the same holds true (what seems to be unlikely) also for Las Vegas computations.

Probability amplitudes. In principle, probability amplitudes for transitions at the quantum models of automata can be arbitrary complex numbers the absolute values of which are not larger than one and such that the *local probability condition* for transitions is satisfied.

However, once computational power of quantum automata is considered, then the problem what types of amplitudes to allow is a nontrivial and important one. Let us list some of the problems and outcomes.

- In order to study (low) computational complexity we need to assume that probability amplitudes are (easily) computable.
- In the case of Turing machines, one can show that a restriction to real amplitudes can increase computational complexity only by a small constant factor comparing to the case no restriction on amplitudes is made.
- There is a universal Turing machine that uses only a very small set of amplitudes; namely the amplitudes from the set $\{0, \pm\frac{3}{5}, \pm\frac{4}{5}, 1\}$ (Adleman et al., 1997).
- For basic quantum complexity classes, in some cases there is no essential difference if only rational or only algebraic amplitudes are allowed, but not in all cases is this question resolved yet.

It is an open problem how much can a restriction to amplitudes of certain type influence the computational power of finite automata.

Uncomputing trick and its applications. How to get rid of the "garbage" is an important problem of quantum computation. If a computation creates "garbage", that is auxiliary results that are finally not needed for other purposes than to make computation reversible, then it is often important, especially if some partial computations are performed, to remove garbage as soon as possible, because "garbage states " can get entangled with the environment what can cause disruption of otherwise very sensitive superpositions.

The basic trick for removing garbage goes back to Bennett (1973). Let us assume that for a function f a reversible classical computation $\mathcal{C}$ maps $a \to (a, g(a), f(a))$, where $g(a)$ is a "garbage". By making a copy of the output we get $(a, g(a), f(a), f(a))$ and then an "uncomputing" process, $(a, g(a), f(a)) \to a$, gets rid of the garbage and provides $(a, f(a))$.

One of the cases when the uncomputing trick can be used is that of multiple terminations. In the case of classical Turing machines, we can easily say that one accepting configuration is sufficient. We can do that because we can make a Turing machine, each time it wants to stop, first to clean its work tapes, then to move the head to left and to

enter the unique accepting configuration. This we cannot do with quantum machines due to the reversibility requirement. However, the above garbage removal trick can be used.

The second case is that of the handling of subroutines. Again, by using the "uncomputation trick", we can achieve that a quantum subroutine can finish its computation without leaving behind a garbage. This is necessary, for example to show robustness of such complexity classes as **BQP** (that is to show that $\mathbf{BQP}^{\mathbf{BQP}} = \mathbf{BQP}$).

Computational power of entanglement Communicational power of entanglement is clear. It can be shown that in some cases entanglement can decrease communicational complexity exponentially, as discussed below. An extent of the computational power of entanglement is less clear. Shor's algorithm makes (essential?) use of it. On the other hand, quantum entanglement does not seem to contribute much to the power of such quantum computational complexity classes as **BQP**. In addition, basic models of quantum automata, at least quantum versions of probabilistic automata, do not work with entangled states.

A surprising use of entanglement, as a catalyst, has been discovered by Jonathan and Plenio (1999). Namely, that the mere presence of a (borrowed) entangled state can be an essential advantage when the task is to transform one quantum state into another with local quantum operations and classical communication (LQCC).

They have shown that there are pairs of pure states $(|\phi_1\rangle, |\phi_2\rangle)$ such that using LQCC one cannot transform $|\phi_1\rangle$ into $|\phi_2\rangle$, but with the assistance of an appropriate entangled state $|\psi\rangle$ one can transfer $|\phi_1\rangle$ into $|\phi_2\rangle$ using LQCC in such a way that the state $|\psi\rangle$ is not changed in the process (and can be "returned back" after the process). In such a case $|\psi\rangle$ serves as a "catalyst" for otherwise impossible transformation (reaction).

Computational and descriptional power of quantum automata. In order to present basic results on the power of quantum automata it is useful to deal with three main types of automata models separately.

On the level of quantum Turing machines, the most fundamental result is due to Bernstein and Vazirani (1993). Namely that there exist efficient universal Turing machines. Concerning the power of quantum Turing machines the strongest evidence, but not proof, that quantum Turing machine could be, for some tasks, exponentially more powerful, is due to Simon (1994). Of course, the most basic problems concerning the relation of such fundamental complexity classes of quantum computation as the classes **QP**, **QBP**, to the classical complexity classes are, as one could expect, very open. It is also not known whether the class **BQP** contains some **NP**-complete problems.

Even worser is the situiation with quantum cellular automata. It is an open problem whether quantum Turing machines and quantum cellular automata can mutually efficiently simulate each other.

Some models of quantum finite automata are known to be weaker than classical automata, for example one-way quantum automata. On the other hand, quantum two-way finite automata are known to be more powerful than classical two-way finite automata and quantum one-counter automata are known to be more powerful than probabilistic counter automata (see Gruska (1999) for a survey and Bonner et al. (2000).

Concerning the descriptional power, the relation between classical and quantum automata has been explored in details (see Gruska (2000) for a survey for one-way automata). For example, for any prime p the language $L_p = \{a^i \mid i \text{ is divisible by } p\}$ can be recognized by a one-way quantum automaton with $\mathcal{O}(\lg p)$ states, but each deterministic finite automaton recognizing this language needs to have $\mathcal{O}(p)$ states. On the other hand, for any

integer n, the language $L_n = \{w0 \mid w \in \{0,1\}^*, |w| \leq n\}$ can be recognized by a deterministic finite automaton with $\mathcal{O}(n)$ states, but each one-way quantum finite automaton recognizing this language has to have $2^{\Omega(n)}$ states.

Counterfactual computations. One of the most controversial issues in quantum mechanics are conterfactual reasonings and the corresponding puzzling phenomena. The term counterfactuality refers to the phenomenon that the fact that an event might have happened allows to obtain some information about the event even if the event did not happen.

One of such puzzles is the possibility of *counterfactual computations*. They are processes by which one can learn the results of the computation without actually performing the computation — provided the possibility to perform that computation is available, even though computation itself is not performed. Such counterfactual computations are investigated in details by Mitchinson and Jozsa (1999).

3 Quantum communications

There are two subareas of QIPC where quantum communication problems are investigated in depth from different points of view. The first one is quantum information theory (especially the theory of quantum channels), and quantum communication complexity.

Quantum information theory. The importance of quantum information theory follows from the observation that if we want to be able to utilize fully the information processing potential available in Nature, then the concepts of classical information theory need to be generalized to accumulate quantum information carriers.

Main problems of quantum information theory can be seen as follows:

1. The development of the basic concepts of the quantum information theory that parallels and generalizes those of the classical information theory.

2. A study of the data compression methods and limitations.

3. An understanding of quantum channels, their capacities and ways they can be used to transmit effectively classical and quantum information.

4. Quantitative and qualitative characterization of quantum (multipartite) entanglement.

Quantum channels. A basic understanding of quantum channels and their capacity to transfer classical and quantum information has been developed.

In order to communicate through quantum channels three communication primitives can be used: **bit, qubit** and **ebit**

A variety of the concepts of quantum channel capacities have been identified and investigated.

In the case quantum states are transmitted through a quantum channel and in order to do that both way classical communication between the sender and the receiver is possible, then we speak about **assisted quantum capacity**, Q_2.

In the case quantum states are transmitted, but no classical communication is allowed, we speak about **quantum capacity**, Q.

Finally, in the case classical information is transmitted we speak about **classical capacity**, C. In the last case there are still four special cases to consider depending on whether encoders and decoders are classical or quantum.

In the case classical information is transmitted, but "borrowed" entanglement can be used, we speak about **entanglement assissted classical capacity** C_E.

All these capacities can be different for some channels.

Quantum teleportation. One of the most quantum communication resources is quantum teleportation. It allows a "teleportation" of an unknown quantum state from one particle to another one. The original version of quantum teleportation deals with teleportation of qubits and with the use of Bell states as quantum channels. Currently, the subject of teleportation, both from the theoretical and experimental point of view, is one of the most studied area of QIPC.

Quantum communication complexity. The goal of communication complexity is to determine how many bits two parties need to exchange in order to perform some computational task provided each party possess only some part of the input data.

For example, one party possess a string $x \in \{0,1\}^n$ and the other party a string $y \in \{0,1\}^n$ and they want to determine whether $x = y$. In the case they have to use a deterministic protocol for communication, they need to communicate n bits. If a randomized protocol can be used $\mathcal{O}(\lg n)$ bits are sufficient. Finally, in the case they share a random n bit string, then there is a protocol with which they need to exchange only one bit and if $x = y$ then the protocol always gives the right answer, but if $x \neq y$, then the protocol is correct only with probability $\frac{1}{2}$.

It has been shown that for some communication problems quantum protocols at which one can send qubits instead of bits can be much more efficient.

The strongest result so far is due to Raz (1999). He showed an exponential gap between the classical and quantum complexity for the following *promise problem.*

One party holds $x \in \mathbf{R}^n$ and two orthogonal subspaces S_0 and S_1 of $\mathbf{R}^n$. The second party holds a unitary transformation U on $\mathbf{R}^n$. The promise is that Ux is either close to S_0 or to S_1. The output has to be such an i that Ux is close to S_i. x, S_0, S_1 are expected to be described using poly(n) bits with a sufficient accuracy.

4 Challenges

In spite of many successes there are several important challenges to deal with in order to see more clearly power of quantum computation.

- So far we have basically only two techniques to design quantum algorithms that are asymptotically more efficient than the classical ones. The task is to find more such techniques (or to show that they do not exist, in a reasonable sense).
- The task is to determine whether one can solve in quantum polynomial time the Hidden subgroup problem for non-Abelian groups? (A positive answer to this problem would imply that we could have a quantum polynomial algorithm also for the graph isomorphism problem.)
- How many quantum states we need to have quantum algorithms and automata more powerful than the classical ones? How pure this quantumness has to be?
- How much, in terms of physical resources, quantum measurements really cost?

- Are quantum cellular automata more powerful than quantum Turing machines?

References

[1] Leonard M. Adleman, Jonathan DeMarrais, and Ming-Deh A. Huang Quantum computability. *SIAM Journal of Computing*, 26(5):1524–1540, 1997.

[2] Andris Ambainis and John Watrous. Two-way finite automata with quantum and classical states. Technical report, quant-ph/9911009, 1999.

[3] Charles H. Bennett, Gilles Brassard, Sandu Popescu, Benjamin W. Schumacher, John A. Smolin, and William K. Wootters Purification of noisy entaglement and faithful teleportation via noisy channels. *Physical Review Letters*, 76(5):722–725, 1996b.

[4] Ethan Bernstein and Umesh Vazirani. Quantum complexity theory. *SIAM Journal of Computing*, 26(5):1411–1473, 1997.

[5] Richard Bonner, Rusins Freivalds, and Maxim Kravtsev. Quantum versus probabilistic one-way finite automata with counter. In *Proceedings of the International Workshop on Quantum Computing and Learning, Sundbyholms Slott, Sweden, May 2000*, pages 80–88, 2000a.

[6] Jozef Gruska. *Quantum computing.* McGraw-Hill, 1999. See also additions and updatings of the book on http://www.mcgraw-hill.co.uk/gruska.

[7] Jozef Gruska. Descriptional complexity issues in quantum computing. *Journal of Automata, Languages and Combinatorics*, 5:191–218, 2000.

[8] Jozef Gruska. *Mathematics unlimited, 2001 and beyond*, chapter Quantum computing challenges, pages ?–?+37. Springer, 2000.

[9] I. D. Jonathan and Martin B.Plenio. Entanglement-assisted local manipulation of pure quantum states. Technical report, quant-ph/9905071, 1999. See also Phys. Rev. Lett., 83, 3566, 1999.

[10] Seth Lloyd. Universal quantum simulators. *Science*, 273:1073–1078, 1996.

[11] Graeme Mitchison and Richard Jozsa. Counterfactual computation. Technical report, quant-ph/9906026, 1999.

[12] S. Parker and M. B. Plenio. Efficient factorization with a single pure qubit. Technical report, quant-ph/0001066, 2000.

[13] Ran Raz. Exponential separation of quantum and classical communication complexity. In *Proceedings of 31st ACM STOC*, pages 358–367, 1999.

[14] Peter W. Shor Polynomial time algorithms for prime factorization and discrete logarithms on quantum computer. *SIAM Journal on Computing*, 26(5):1484–1509, 1997.

[15] Daniel R. Simon On the power of quantum computation. In *Proceedings of 35th IEEE FOCS*, pages 116–123, 1994. See also SIAM Journal of Computing, V26, N5, 1474-1483, 1997.

[16] Christof Zalka. Fast version of Shor's quantum factoring algorithm. Technical report, quant-ph/9806084, 1998.