Classically-controlled Quantum Computation

Simon Perdrix [1]   Philippe Jorrand[2]

Leibniz Laboratory
IMAG-INPG
Grenoble, France

Abstract

It is reasonable to assume that quantum computations take place under the control of the classical world. For modelling this standard situation, we introduce a Classically-controlled Quantum Turing Machine (CQTM) which is a Turing machine with a quantum tape for acting on quantum data, and a classical transition function for a formalized classical control. In CQTM, unitary transformations and quantum measurements are allowed. We show that any classical Turing machine is simulated by a CQTM without loss of efficiency. Furthermore, we show that any k-tape CQTM is simulated by a 2-tape CQTM with a quadratic loss of efficiency. The gap between classical and quantum computations which was already pointed out in the framework of measurement-based quantum computation (see [14]) is confirmed in the general case of classically-controlled quantum computation. In order to appreciate the similarity between programming classical Turing machines and programming CQTM, some examples of CQTM will be given in the full version of the paper. Proofs of lemmas and theorems are omitted in this extended abstract.

Keywords: Classically-Controlled Quantum Computation, Quantum Turing Machine

1   Introduction

Quantum computations operate in the quantum world. For their results to be useful in any way, by means of measurements for example, they operate under the control of the classical world. Quantum teleportation [1] illustrates the importance of classical control: the correcting Pauli operation applied at the end is classically controlled by the outcome of a previous measurement. Another example of the importance of classical control is measurement-based quantum

---

[1]   Email: simon.perdrix@imag.fr
[2]   Email: philippe.jorrand@imag.fr

computation [10,12,15,14,16,5], where classical conditional structures are required for controlling the computation. This classical control may be described as follows: *"if the classical outcome of measurement number i is λ, then measurement number $i + 1$ is on qubit q_a according to observable O_a, otherwise measurement number $i + 1$ is on qubit q_b according to observable O_b".* A particularly elegant formalization of measurement-based quantum computation is the measurement calculus [5].

The necessity of integrating the classical control in the description of quantum computations is a now well understood requirement in the design of high level languages for quantum programming [7,17]. There are also some propositions of lower level models of computation integrating classical control, like the quantum random access machines (QRAM[9,2]). However there exist no formal and abstract model of quantum computation integrating classical control explicitly. This paper aims at defining such an abstract model of classically-controlled quantum computation.

One of the main existing abstract models of quantum computation is the Quantum Turing Machine (QTM) introduced by Deutsch [4], which is an analogue of the classical Turing machine (TM). It has been extensively studied by Bernstein and Vazirani [3]: a quantum Turing machine is an abstract model of quantum computers, which expands the classical model of a Turing machine by allowing a *quantum* transition function. In a QTM, superpositions and interferences of configurations are allowed, but the classical control of computation is not formalized and inputs and outputs of the machine are still classical. This second point means that the model of QTM explores the computational power of quantum mechanics for solving classical problems, without considering *quantum* problems, i.e. quantum input/output.

While models dealing with quantum states like quantum circuits [8,19] and QRAM, are mainly used for describing specific algorithms, the development of complexity classes, like QMA [18], which deal with quantum states, points out the necessity of theoretical models of quantum computation acting on quantum data.

The recently introduced model of Linear Quantum Turing Machine (LQTM) by S. Iriyama, M. Ohya, and I. Volovich [6] is a generalization of QTM dealing with mixed states and allowing irreversible transition functions which allow the representation of quantum measurements without classical outcomes. As a consequence of this lack of classical outcome, the classical control is not formalized in LQTM, and, among others, schemes like teleportation cannot be expressed. Moreover, like QTM, LQTM deals with classical input/output only.

We introduce here a Classically-controlled Quantum Turing Machine (CQTM)

which is a TM with a quantum tape for acting on quantum data, and a classical transition function for a formalized classical control. In CQTM, unitary transformations and quantum measurements are allowed. Notice that the model of CQTM restricted to projective measurements is equivalent to the model of measurement-based quantum Turing machines (MQTM) introduced in [14]. *Theorem 2.1* shows that any TM is simulated by a CQTM without loss of efficiency. In section 3, CQTM with multiple tapes is introduced. *Theorem 3.1* shows that any k-tape CQTM is simulated by a 2-tape CQTM with a quadratic loss of efficiency. Moreover, the gap between classical and quantum computations which was already pointed out in the framework of measurement-based quantum computation (see [14]) is confirmed in the general case of classically-controlled quantum computation. A perspective is to make the CQTM not only a well defined theoretical model but also a bridge to practical models of quantum computations like QRAM, by relying on the fact that natural models of quantum computations are classically controlled.

2 Classically-controlled Quantum Turing Machines

2.1 *Quantum states and admissible transformations*

The quantum memory of a CQTM is composed of quantum cells. A quantum cell is a d-level quantum system [11], its state is a normalized vector in a d-dimensional Hilbert space. A basis of this Hilbert space is described by a finite alphabet of symbols Σ_Q such that $|\Sigma_Q| = d$. The state $|\phi\rangle \in \mathcal{H}_{\Sigma_Q}$ of a quantum cell is

$$|\phi\rangle = \sum_{\tau \in \Sigma_Q} \alpha_\tau |\tau\rangle \,,$$

with $\sum_{\tau \in \Sigma_Q} |\alpha_\tau|^2 = 1$.

General quantum measurements operate according to the corresponding postulate of quantum mechanics: quantum measurements are described by a collection $\{M_{\tau_1}, \ldots, M_{\tau_k}\}$ of measurement operators acting on the state space of the system being measured. The index τ refers to the measurement outcomes that may occur in the experiment. If the state of the quantum system is $|\psi\rangle$ immediately before the measurement then the probability that the classical result τ occurs is given by

$$p(\tau) = \langle\psi| M_\tau^\dagger M_\tau |\psi\rangle \,,$$

and the state of the system after the measurement is

$$\frac{M_\tau |\psi\rangle}{\sqrt{p(\tau)}}.$$

The measurement operators satisfy the completness equation,

$$\sum_{\tau} M_\tau^\dagger M_\tau = I.$$

General quantum measurements are also called *admissible transformations*. Notice that admissible transformations which are composed of only one operator M_τ are nothing but unitary transformations since $p(\tau) = 1$, the state after the transformation is $M_\tau |\psi\rangle$ and the completeness equation reduces to $M_\tau^\dagger M_\tau = I$. Conversely, any unitary transformation A is an admissible transformation.

For a given Hilbert space $\mathcal{H}_{\Sigma_Q}$, we exhibit some admissible transformations with classical results belonging to a finite set $\Sigma_C = \Sigma_Q \cup \overline{\Sigma_Q} \cup \{\lambda\}$, where $\overline{\Sigma_Q} = \{\overline{\tau} : \tau \in \Sigma_Q\}$ and $\lambda \notin \Sigma_Q$:

- $Std = \{M_\tau\}_{\tau \in \Sigma_Q}$ is a projective measurement in the standard basis: $\forall \tau \in \Sigma_Q, M_\tau = |\tau\rangle \langle \tau|$,
- $\mathcal{T}_\tau = \{M_\tau, M_{\overline{\tau}}\}$ is a test for the symbol τ: $M_\tau = |\tau\rangle \langle \tau|$ and $M_{\overline{\tau}} = I - |\tau\rangle \langle \tau|$,
- $\mathcal{P}_{[\tau_a, \tau_b]} = \{M_\lambda\}$ is a unitary transformation with outcome λ, and $M_\lambda = (\sum_{\tau \in \Sigma_Q - \{\tau_a, \tau_b\}} |\tau\rangle \langle \tau|) + |\tau_a\rangle \langle \tau_b| + |\tau_b\rangle \langle \tau_a|$ is a permutation of the symbols τ_a and τ_b.
- $\mathcal{U}_V = \{M_\lambda\}$ is the unitary transformation $M_\lambda = V$, with classical outcome λ.
- $\mathcal{O}_O = \{P_k\}_k$, is a projective measurement according to the observable $O = \Sigma_k P_k$.

2.2   Defining a CQTM

For completeness, definition 2.1 is the definition of a deterministic TM [13]. A classically-controlled quantum Turing machine (definition 2.2) is composed of a quantum tape of quantum cells, a set of classical internal states and a head for applying admissible transformations to cells on the tape. The role of the head is crucial because it implements the interaction across the boundary between the quantum and the classical parts of the machine.

Definition 2.1 A deterministic (classical) Turing Machine is defined by a triplet $M = (K, \Sigma, \delta)$, where K is a finite set of states with an identified initial state s, Σ is a finite alphabet with an identified "blank" symbol $\#$, and δ is a deterministic transition:

$$\delta : K \times \Sigma \to (K \cup \{\text{"yes"}, \text{"no"}, h\}) \times \Sigma \times \{\leftarrow, \to, -\}.$$

We assume that h (the halting state), "*yes*" (the accepting state) and "*no*" (the rejecting state) are not in K.

Definition 2.2 A Classically-controlled Quantum Turing Machine is a quin-tuple $M = (K, \Sigma_C, \Sigma_Q, \mathcal{A}, \delta)$. Here K is a finite set of classical states with an identified initial state s, Σ_Q is a finite alphabet which denotes basis states of quantum cells, Σ_C is a finite alphabet of classical outcomes, $\mathcal{A}$ is a set of one-quantum cell admissible transformations, and δ is a classical transition function:

$$\delta : K \times \Sigma_C \to (K \cup \{\text{"}yes\text{"}, \text{"}no\text{"}, h\}) \times \{\leftarrow, \rightarrow, -\} \times \mathcal{A}.$$

We assume that h (the halting state), "*yes*" (the accepting state) and "*no*" (the rejecting state) are not in K, and that all possible classical outcomes of each measurement of $\mathcal{A}$ are in Σ_C. Moreover we assume that Σ_Q always contains a "blank" symbol $\#$, Σ_C always contains a "blank" symbol $\#$ and a "non-blank" symbol $\overline{\#}$, and $\mathcal{A}$ always contains the admissible "blank test" transformation $\mathcal{T}_{\#}$.

The function δ is a formalization of the classical control of the quantum computation and can also be viewed as the "program" of the machine. It specifies, for each combination of current state $q \in K$ and last obtained classical outcome $\tau \in \Sigma_C$, a triplet $\delta(q, \tau) = (p, D, A)$, where p is the next classical state, $D \in \{\leftarrow, \rightarrow, -\}$ is the direction in which the head will move, and $A \in \mathcal{A}$ is the admissible transformation to be performed next. The *blank test* admissible transformation $\{M_{\#}, M_{\overline{\#}}\}$ establishes a correspondence between the quantum blank symbol ($\#$) and the classical blank ($\#$) and non-blank ($\overline{\#}$) symbols: if the state $|\phi\rangle$ of the measured quantum cell is $|\#\rangle$, the outcome of the measurement is $\#$ whereas if $|\phi\rangle$ is orthogonal to $|\#\rangle$ ($\langle\phi\,|\#\rangle = 0$) then the outcome is $\overline{\#}$.

How does the program start? The quantum input of the computation $|\phi\rangle = \sum_{\tau \in (\Sigma_Q - \{\#\})^n} \alpha_\tau |\tau\rangle$, which is in general unknown, is placed on n adjacent cells of the tape, while the state of all other quantum cells of the tape is $|\#\rangle$. The head is pointing at the blank cell immediately located on the left of the input. Initially, the classical state of the machine is s and $\#$ is considered as the last classical outcome, thus the first transition is always $\delta(s, \#)$.

How does the program halt? The transition function δ is total on $K \times \Sigma_C$ (irrelevant transitions will be omitted from its description). There is only one reason why the machine cannot continue: one of the three halting states h, "*yes*", and "*no*" has been reached. If a machine M halts on input $|\phi_{in}\rangle$, the output $M(|\phi_{in}\rangle)$ of the machine M on $|\phi_{in}\rangle$ is defined. If states "*yes*" or "*no*" are reached, then $M(|\phi_{in}\rangle) = $ "*yes*" or "*no*" respectively. Otherwise, if halting

state h is reached then the output is the state $|\phi_{out}\rangle$ of the tape of M at the time of halting. Since the computation has gone on for finitely many steps, only a finite number of cells are not in the state $|\#\rangle$. The output state $|\phi_{out}\rangle$ is the state of the finite register composed of the quantum cells from the leftmost cell in a state which is not $|\#\rangle$ to the rightmost cell in a state which is not $|\#\rangle$. Naturally, it is possible that M never halts on input $|\phi_{in}\rangle$. If this is the case we write $M(|\phi_{in}\rangle) = \nearrow$.

A *configuration* of a CQTM M is intuitively a complete description of the current state of the computation. Formally, a configuration is a triplet $(q, \tau, |\psi\rangle)$, where $q \in K \cup \{h, \text{``yes''}, \text{``no''}\}$ is the internal state of M, $\tau \in \Sigma_C$ is the last obtained outcome, and $|\psi\rangle \in \mathcal{H}_{\Sigma'_Q}$ represents the state of the tape and the position of the head. Here $\Sigma'_Q = \Sigma_Q \cup \underline{\Sigma}_Q$, where $\underline{\Sigma}_Q = \{\underline{\tau} : \tau \in \Sigma_Q\}$ is a set of *pointed* versions of the symbols in Σ_Q. From a state $|\phi\rangle \in \mathcal{H}_{\Sigma_Q}$ of the tape, the state $|\psi\rangle \in \mathcal{H}_{\Sigma'_Q}$ is obtained by replacing the symbol of Σ_Q by the corresponding symbol of $\underline{\Sigma}_Q$ for the quantum cell pointed at by the head. For instance, if $K = \{q_1, q_2\}$, $\Sigma_C = \{\#, \overline{\#}, t, u, v\}$ and $\Sigma_Q = \{\#, a, b\}$, the configuration

$$\left(q_1, u, \frac{1}{\sqrt{2}}(|a\#\underline{b}b\rangle + |b\#\underline{a}b\rangle)\right)$$

means that the internal state of the machine is q_1, the last outcome is u, the state of the tape is $\frac{1}{\sqrt{2}}(|a\#bb\rangle + |b\#ab\rangle)$, and the head is pointing at the third cell from the right.

3   CQTM and TM

The following theorem shows that any TM is simulated by a CQTM without loss of efficiency.

Theorem 3.1 *Given any TM M_C operating in time $f(n)$, where n is the input size, there exists a CQTM M_Q operating in time $O(f(n))$ and such that for any input x, $M_C(x) = M_Q(|x\rangle)$*

Since any TM is simulated by a CQTM without loss of efficiency, the model of CQTM is classically universal (see [14] for definitions of classical and quantum universalities), but, as will be shown in *Lemma 4.4*, CQTM with one tape are not quantum universal, because only one-cell admissible transformations are allowed. In order to allow transformations on more than one cell, we introduce multiple tapes CQTMs. Intuitively, with k heads, k-cell admissible transformations can be performed.

4 CQTM with multiple tapes

We introduce a generalization of the CQTM, the classically-controlled Turing machine with multiple tapes. We show that any k-tape CQTM is simulated by a 2-tape CQTM with an inconsequential loss of efficiency. Moreover, by showing that 1- and 2-tape CQTM are not equivalent, we point out a *gap* between classical and quantum computations.

Definition 4.1 A k-tape Classically-controlled Quantum Turing Machine where $k > 0$, is a quintuple $M = (K, \Sigma_C, \Sigma_Q, \mathcal{A}, \delta)$, where K is a finite set of classical states with an identified initial state s, Σ_Q is a finite alphabet which denotes basis states of each quantum cell. $\mathcal{A}$ is a set of k-cell admissible transformations, Σ_C is a finite alphabet of classical outcomes of k-cell admissible transformations and δ is a classical transition function

$$\delta : K \times \Sigma_C \to (K \cup \{ \text{``yes''}, \text{``no''}, h \}) \times (\{\leftarrow, \rightarrow, -\})^k \times \mathcal{A}.$$

We assume that all possible classical outcomes of each measurement of $\mathcal{A}$ are in Σ_C and that $\mathcal{A}$ always contains the k admissible "blank test" transformations, one for each tape of the machine.

Intuitively, $\delta(q, \tau) = (q', (D_1, \ldots D_k), A)$ means that, if M is in state q and the last classical outcome is τ, then the next state will be q', the k heads of the machine will move according to $D_1, \ldots, D_k$ and the next k-quantum cell admissible transformation will be A. This admissible transformation will be performed on the k quantum cells pointed at by the heads of the machine after they have moved. A k-cell admissible transformation A can be defined directly, for instance by use of a k-cell unitary transformation V ($A = \mathcal{U}_V$). A can also be defined as a composition of two admissible transformations A_1, A_2 respectively on j and l cells such that $j + l = k$, then $A = [A_1, A_2]$ means that the first j heads apply A_1 and, simultaneously, the last l heads apply A_2. The classical outcome is the concatenation of the outcomes of A_1 and A_2, where λ is the unit element of the concatenation (i.e. $\tau.\lambda = \tau$).

A k-tape CQTM starts with an input state $|\phi\rangle$ on a specified tape T_1, and if the halting state h is reached, the machine halts and the output is the state of the specified tape T_1.

Theorem 4.2 *Given any k-tape CQTM M operating in time $f(n)$, where n is the input size, there exists a 2-tape CQTM M' operating in time $O(f(n)^2)$ and such that for any input $|\psi\rangle$, $M(|\psi\rangle) = M'(|\psi\rangle)$.*

Theorem 4.1 is a strong evidence of the power and stability of CQTMs: adding a bounded number of tapes to a 2-tape CQTM does not increase

their computational capabilities, and impacts their efficiency polynomially only. This stability makes 2-tape CQTMs a good candidate for quantum universality, i.e. the ability to simulate any quantum computation. This ability is proved with the following two lemmas:

Lemma 4.3 *Any pattern of the measurement calculus [5] can be simulated in a time polynomial in the size of the pattern by a 2-tape CQTM.*

Lemma 4.4 *Any quantum circuit can be simulated by a 2-tape CQTM in polynomial time.*

The following lemma shows that some 2-tape CQTMs cannot be simulated by 1-tape CQTMs:

Lemma 4.5 *There exists a 2-tape CQTM M such that no 1-tape CQTM simulates M.*

To sum up, two tapes are enough for quantum computation (*Lemma 4.3*), whereas one tape is enough for classical computation (*Theorem 3.1*) but not for quantum computation (*Lemma 4.4*). Thus a *gap* between classical and quantum computations appears. Notice that this result does not contradict the equivalence, in terms of decidability, between classical and quantum computations: the gap appears iff quantum data are considered.

One may wonder why 1-tape CQTMs are not quantum universal whereas Briegel and Raussendorf have proved, with their One-way quantum computer, that one-qubit measurements are universal [16]. The proof by Briegel and Raussendorf is given with a strong assumption which is that there exists a grid of auxiliary qubits which have been initially prepared, by some unspecified external device, in a globally entangled state (the cluster state), whereas *creation* of entanglement is a crucial point in the proof of *Lemma 4.4*. Moreover, another strong assumption of one-way quantum computation is that the input state $|\varphi\rangle$ has to be classically known (i.e. a mathematical description of $|\varphi\rangle$ is needed), whereas the manipulation of unknown states (i.e. manipulation of qubits in an unknown state) is usual in quantum computation (e.g. teleportation [1]). Since none of these assumptions are verified by 1-tape CQTM, the previous results do not contradict the results of Briegel and Raussendorf.

5   Conclusion

This paper introduces a new abstract model for quantum computations, the model of classically-controlled quantum Turing machines (CQTM). This model allows a rigorous formalization of the inherent interactions between the quantum world and the classical world during a quantum computation. Any clas-

sical Turing machine is simulated by a CQTM without loss of efficiency, moreover any k-tape CQTM is simulated by a 2-tape CQTM affecting the execution time only polynomially.

Moreover the gap between classical and quantum computations which was already pointed out in the framework of measurement-based quantum computation (see [14]) is confirmed in the general case of classically-controlled quantum computation.

The classically-controlled quantum Turing machine is a good candidate for establishing a bridge between, on one side, theoretical models like QTM, CQTM, MQTM [14] and on the other side practical models of quantum computation like quantum random access machines.

References

[1] C. Bennett et al. *Teleporting an unknown quantum state via dual classical and EPR channels*, Phys Rev Lett, 1895-1899, 1993.

[2] S. Bettelli, L. Serafini, and T. Calarco. *Toward an architecture for quantum programming*, http://arXiv.org/cs.PL/0103009, 2001.

[3] E. Bernstein and U. Vazirani, *Quantum complexity theory*, SIAM J. Compt. 26, 1411-1473, 1997.

[4] D. Deutsch. *Quantum theory, the Church-Turing principle and the universal quantum computer*, Proceedings of the Royal Society of London A 400, 97-117, 1985.

[5] V. Danos, E. Kashefi, P. Panangaden *The Measurement Calculus* , e-print http://arXiv.org/quant-ph/0412135.

[6] S. Iriyama, M. Ohya, I. Volovich. *Generalized Quantum Turing Machine and its Application to the SAT Chaos Algorithm*, http://arXiv.org/quant-ph/0405191, 2004.

[7] Ph. Jorrand and M. Lalire. *Toward a Quantum Process Algebra*, Proceedings of the first conference on computing frontiers, 111-119, 2004, e-print http://arXiv.org/quant-ph/0312067.

[8] A. Y. Kitaev, A. H. Shen and M. N. Vyalyi. *Classical and Quantum Computation*, American Mathematical Society, 2002.

[9] E. H. Knill. *Conventions for Quantum Pseudocode*, unpublished, LANL report LAUR-96-2724

[10] D. W. Leung. *Quantum computation by measurements*, arXiv, quant-ph/0310189, 2003.

[11] A. Muthukrishnan and C. R. Stroud. *Multi-valued logic gates for quantum computation*, arXiv, quant-ph/0002033, 2000.

[12] M. A. Nielsen. *Universal quantum computation using only projective measurement, quantum memory, and preparation of the 0 state*, http://arXiv.org/quant-ph/0108020, 2001.

[13] C. M. Papadimitriou. *Computational Complexity*, Addisson-Wesley Publishing Compagny, 1994.

[14] S. Perdrix and Ph. Jorrand. *Measurement-Based Quantum Turing Machines and their Universality*, arXiv, quant-ph/0404146, 2004.

[15] S. Perdrix. *State Transfer instead of Teleportation in Measurement-based Quantum Computation*, arXiv, quant-ph/0402204, 2004.

[16] R. Raussendorf, D. E. Browne and H. J. Briegel. *Measurement-based quantum computation with cluster states*, http://arXiv.org/quant-ph/0301052, 2003.

[17] P. Selinger. *Towards a quantum programming language.* To appear in Mathematical Structures in Computer Science, 2003.

[18] J. Watrous, *Succinct quantum proofs for properties of finite groups*, Proc. 41st Annual Symposium on Foundation of Computer Science, pp. 537-546, 2000.

[19] A. C. Yao, *Quantum circuit complexity*, Proc. 34th IEEE Symposium on Foundation of Computer Science, pp. 352-361, 1993.