Partial Observation of Quantum Turing Machine and Weaker Well-Formedness Condition

Simon Perdrix

Oxford University Computing Laboratory

Abstract. The quantum Turing machine (QTM) has been introduced by Deutsch as an abstract model of quantum computation. The transition function of a QTM is linear, and has to be unitary to be a well-formed QTM. This well-formedness condition ensures that the evolution of the machine does not violate the postulates of quantum mechanics. However, we claim in this paper that the well-formedness condition is too strong and we introduce a weaker condition, leading to a larger class of Turing machines called Observable Quantum Turing Machines (OQTMs). We prove that the evolution of such OQTM does not violate the postulates of quantum mechanics while offering a more general abstract model for quantum computing. This novel abstract model unifies classical and quantum computations, since every well-formed QTM and every deterministic TM are OQTMs, whereas a deterministic TM has to be reversible to be a well-formed QTM. In this paper we introduce the fundamentals of OQTM like a well-observed lemma and a completion lemma. The introduction of such an abstract machine allowing classical and quantum computations is motivated by the emergence of models of quantum computation like the one-way model. More generally, the OQTM aims to be an abstract framework for the pragmatic paradigm of quantum computing: 'quantum data, classical control'. Furthermore, this model allows a formal and rigorous treatment of problems requiring classical interactions, like the halting of QTM. Finally, it opens new perspectives for the construction of a universal QTM.

1 Introduction

How to make a quantum version of the deterministic Turing machine (DTM)? While a probabilistic Turing machine (PTM) is obtained from a DTM by allowing probability distributions over machine configurations, a pre-quantum Turing machine (pQTM) is defined from a DTM by allowing superpositions of machine configurations. In addition, a PTM has to satisfy a well formedness condition ensuring that the probabilities are positive numbers and sum to one. In the same way, a reversible Turing machine (RTM) is an instance of DTM which satisfies a well formedness condition ensuring its reversibility. In a similar vein, Deutsch had introduced the Quantum Turing machines (QTM) as a class of pQTMs which satisfy a well formedness condition. This well formedness condition ensures that QTMs do not violate the postulate of quantum mechanics and implies reversibility as well. As a consequence, a QTM is a quantum version of a RTM. However, recent developments of models of quantum computation like the one-way quantum computer, point out that a quantum computation may be irreversible. Thus, the well-formedness condition is too restrictive.

The main contribution of this paper consists in introducing a weaker well formedness condition to capture the postulates of quantum mechanics, independently of the question of reversability. This weaker condition leads to a class of quantum versions of DTMs, called Observable Quantum Turing machines (OQTM).

After a brief introduction to quantum basics (see [9] for a complete introduction), we introduce in section 4, such a less restrictive class of quantum Turing machines, the *observable quantum Turing machines* (OQTM), where partial observations can be performed at each transition. Fondamentals of OQTM are given: evolution operator (which is not a unitary transformation any more, but a trace-preserving completely-positive map, like in the linear quantum Turing machines [6]) a well-observation condition (which is the generalisation of the well-formedness condition.) Essential tools for programming OQTMs are introduced: a well-observation lemma (i.e. the conditions the transition function has to satisfy to make the machine a well-observed pQTM); and a completion lemma (if a partial transition function satisfies the conditions of the well-obseravtion lemma, it can be extended to a total function of a well-observed pQTM.) In section 5.1, we prove that any QTM can be simulated by an OQTM in which a partial measurement is performed at each transition in order to know whether the computation is halted or not.

In section 5.2, we prove that any QTM and any deterministic Turing machine are well-observed. Thus, OQTM expands the classical model of deterministic Turing machine, including non-reversible machines. Moreover, well-observation can be seen as a weaker well-formedness condition allowing non-reversible computations.

In section 6, we prove that the computational power of OQTM is equivalent to the one of QTM, since any OQTM can be simulated by a QTM within a quadratic slowdown.

2 Quantum Computing Basics

The basic carrier of information in quantum computing is a 2-level quantum system (*qubit*), or more generally a d-level quantum system (*qudit*). The state of a single qudit is a normalized vector of a Hilbert space $\mathbb{C}^A$, where A is a finite alphabet of symbols. An orthonormal basis (o.n.b.) of this Hilbert space is described as: $\{|\tau\rangle, \tau \in A\}$. So the general state $|\varphi\rangle \in \mathbb{C}^A$ of a single qudit can be written as:

$$\sum_{\tau \in A} \alpha_\tau |\tau\rangle,$$

with $\sum_{\tau \in A} |\alpha_\tau|^2 = 1$. Vectors, inner and outer products are expressed in the notation introduced by Dirac. Vectors are denoted $|\varphi\rangle$; the inner product of two vectors $|\varphi\rangle$, $|\psi\rangle$ is denoted by $\langle\varphi|\psi\rangle$. If $|\varphi\rangle = \sum_{\tau \in A} \alpha_\tau |\tau\rangle$ and $|\psi\rangle = \sum_{\tau \in A} \beta_\tau |\tau\rangle$, then $\langle\varphi|\psi\rangle = \sum_{\tau \in A} \alpha_\tau^* \beta_\tau$ (where α^* stands for the complex conjugate). The left hand side $\langle\varphi|$ of the inner product is a *bra-vector*, and the right hand side $|\psi\rangle$ is a *ket-vector*. A bra-vector is defined as the adjoint of the corresponding ket-vector: if $|\varphi\rangle = \sum_{\tau \in A} \alpha_\tau |\tau\rangle$, then $\langle\varphi| = |\varphi\rangle^\dagger = \sum_{\tau \in A} \alpha_\tau^* \langle\tau|$. The bra-ket notation can also be used to describe outer products: $|\varphi\rangle\langle\psi|$ is a linear operator, $(|\varphi\rangle\langle\psi|)|\epsilon\rangle = \langle\psi|\epsilon\rangle\, |\varphi\rangle$. The state of a system composed of 2 qudits in state $|\varphi\rangle \in \mathbb{C}^A$ and $|\psi\rangle \in \mathbb{C}^B$ respectively, is the normalized vector $|\varphi\rangle \otimes |\psi\rangle \in \mathbb{C}^A \otimes \mathbb{C}^B \cong \mathbb{C}^{A \times B}$, where $\otimes$ is the tensor product. For any $\tau \in A, \gamma \in B$, $|\tau, \gamma\rangle$ denotes $|\tau\rangle \otimes |\gamma\rangle$.

Probability distribution of quantum states of $\mathbb{C}^A$ can be represented by a density matrix $\rho \in \mathcal{D}(\mathbb{C}^A) \subseteq \mathbb{C}^{A \times A}$, i.e. a self adjoint[1] positive-semidefinite[2] complex matrix of trace[3] one.

According to the second postulate of quantum mechanics, an isolated system evolves according to a unitary transformation[4] $U \in \mathbb{C}^{A \times A}$, transforming a state $\rho \in \mathcal{D}(\mathbb{C}^A)$ into

[1] M is self adjoint (or Hermitian) if and only if $M^\dagger = M$

[2] M is positive-semidefinite if all the eignenvalues of M are non-negative.

[3] The trace of M ($tr(M)$) is the sum of the diagonal elements of M

[4] U is unitary if and only if $U^\dagger U = UU^\dagger = \mathbb{I}$.

$U\rho U^\dagger$. More generally, whether the system is isolated or not, the state evolves according to a trace-preserving completely-positive (tpcp) map F, transforming ρ into $F(\rho)$. According to the Kraus representation theorem [2], for any tpcp map F, there exists a collection of matrices $M_i \in \mathbb{C}^{A\times A}$, that satisfies a completeness condition $\sum_i M_i^\dagger M_i = \mathbb{I}$, such that $F(\rho) = \sum_i M_i \rho M_i^\dagger$. A special instance of tpcp-map is a projective measurement described by a collection of projectors P_i. A projective measurement transforms ρ into $\sum_i P_i \rho P_i$. A projective measurement produces a classical outcome i_0 with probability $p_{i_0}(\rho) = Tr(P_{i_0}\rho P_{i_0}) = Tr(P_{i_0}\rho)$. [5] For instance, a projection onto a given state $|\varphi\rangle$ is $P_0 = |\varphi\rangle\langle\varphi|$, thus the probability to obtain the classical outcome associated with this projector is $|\varphi\rangle$ is $Tr(|\varphi\rangle\langle\varphi|\rho) = Tr(\langle\varphi|\rho|\varphi\rangle)$.

3 Quantum Turing Machine

For completeness, the definition of deterministic Turing machines is given. See [12] for fondamentals on (classical) Turing machines.

Definition 1 (Deterministic Turing Machine (DTM)). *A deterministic Turing machine is defined by a triplet (Σ, Q, δ) where: Σ is a finite alphabet with an identified blank symbol $\#$, Q is a finite set of states with an identified initial state q_0 and final state $q_f \neq q_0$, and δ, the deterministic transition function*[6]*, is a function*

$$\delta : Q \times \Sigma \to \Sigma \times Q \times \{-1, 0, 1\}$$

Deutsch in [4] introduced a quantum version of the Turing machine, extensively studied by Bernstein and Vazirani [1]:

Definition 2 (Pre-Quantum Turing Machine (pQTM)). *A pre-quantum Turing machine* (pQTM) *is defined by a triplet (Σ, Q, δ) where: Σ is a finite alphabet with an identified blank symbol $\#$, Q is a finite set of states with an identified initial state q_0 and final state $q_f \neq q_0$, and δ, the quantum transition function, is a function*

$$\begin{aligned} \delta : Q \times \Sigma &\to \mathbb{C}^{\Sigma\times Q\times\{-1,0,1\}} \\ (p,\tau) &\mapsto \textstyle\sum_{q\in Q,\sigma\in\Sigma,d\in\{-1,0,1\}} \alpha_{p,\tau,q,\sigma,d}|\sigma,q,d\rangle \end{aligned}$$

For convenience, the expression $\delta(p,\tau,q,\sigma,d)$ is used to denote $\alpha_{p,\tau,q,\sigma,d} \in \mathbb{C}$, i.e. the amplitude in $\delta(p,\tau)$ of $|\sigma,q,d\rangle$. The evolution of a pQTM M is given by the linear operator U_M defined on $\mathbb{C}^{Q\times\Sigma^*\times\mathbb{Z}}$ (called the state space of configurations):

$$U_M = \sum_{p,q\in Q,\sigma\in\Sigma,d\in\{-1,0,1\},T\in\Sigma^*,x\in\mathbb{Z}} \delta(p,T_x,q,\sigma,d)|q,T_x^\sigma,x+d\rangle\langle p,T,x|$$

where $T_x^\sigma \in \Sigma^*$ is T where the symbol in position x is replaced by σ.

A quantum Turing machine (QTM) is a *well-formed* pre-quantum Turing machine:

Definition 3 (Well-formedness condition). *A* pQTM M *is well-formed if and only if U_M is an isometry, i.e. $U_M^\dagger U_M = \mathbb{I}$.*

[5] since $Tr(MN) = Tr(NM)$ and for any projector P, $P^2 = P$.
[6] The transition function of deterministic Turing machine is supposed to be total in this paper.

Lemma 1 (Well-formedness lemma [11]). *For a given* pQTM $M = (\Sigma, Q, \delta)$*,* M *is well-formed if and only if:*
(a) $\forall(\tau, p) \in \Sigma \times Q$*,*

$$\delta(p, \tau)^\dagger \delta(p, \tau) = 1$$

(b) $\forall(\tau, p), (\tau', p') \in \Sigma \times Q$ *with* $(p, \tau) \neq (p', \tau')$*,*

$$\delta(p, \tau)^\dagger \delta(p', \tau') = 0$$

(c) $\forall(\tau, p, \sigma), (\tau', p', \sigma') \in Q \times \Sigma \times \Sigma$*,*

$$\sum_{d \in \{0,1\}, q \in Q} \delta(p, \tau, q, \sigma, d-1)^* \delta(p', \tau', q, \sigma', d) = 0$$

(d) $\forall(\tau, p, \sigma), (\tau', p', \sigma') \in Q \times \Sigma \times \Sigma$*,*

$$\sum_{q \in Q} \delta(p, \tau, q, \sigma, -1)^* \delta(p', \tau', q, \sigma', 1) = 0$$

A triple $M = (\Sigma, Q, \delta)$ is called a partial pQTM if δ is a partial quantum transition function. If such a δ satisfies the four conditions of the well-formedness lemma 1, then M is called a partially well-formed pQTM.

Lemma 2 (Completion lemma [11]). *For every partially well-formed pQTM* M *with a partial quantum transition* δ*, there exists a* QTM M' *with the same alphabet, the same set of states, and a transition function* δ' *which is equal to* δ *on the domain of* δ*.*

A QTM *M* evolves according to U_M: if the initial configuration of M is $|c\rangle \in \mathbb{C}^{Q \times \Sigma^* \times \mathbb{Z}}$, then after n transitions, the configuration of the machine is $(U_M)^n |c\rangle$. Configurations may also be represented by density matrices $\rho \in \mathcal{D}(\mathbb{C}^{Q \times \Sigma^* \times \mathbb{Z}})$ (see [6]). Density matrices allows representation of probabilistic distributions over quantum states. The evolution operator is then the tpcp map:

$$F_M : \mathcal{D}(\mathbb{C}^{Q \times \Sigma^* \times \mathbb{Z}}) \to \mathcal{D}(\mathbb{C}^{Q \times \Sigma^* \times \mathbb{Z}})$$
$$\rho \mapsto U_M \rho U_M^\dagger$$

4 Observable Quantum Turing Machine

Since a QTM has a unitary evolution, no measurement can be applied until the machine halts. It turns out that it may be useful to observe the machine during the evolution, for instance to know whether the machine is already halted or not. This problem has been solved [10] by proving that one can add a halt qubit that can be measured after each transition, and which switches from 0 to 1 when the machine halts. We introduce a formal and more general framework to describe a partial observation of the machine before and after each transition:

Definition 4 (Observed pre-quantum Turing machine). *For a given* pQTM $M = (\Sigma, Q, \delta)$*, and a partition* $K = \{K_\lambda, \lambda \in \Lambda\}$ *of* $\Sigma \times Q$*,* $[M]_K$ *is an* observed pre-quantum Turing machine*. The evolution of* $[M]_K$ *is given by* $F_{[M]_K}$*:*

$$F_{[M]_K} : \mathcal{D}(\mathbb{C}^{Q \times \Sigma^* \times \mathbb{Z}}) \to \mathcal{D}(\mathbb{C}^{Q \times \Sigma^* \times \mathbb{Z}})$$
$$\rho \mapsto \sum_{\lambda, \mu \in \Lambda} \chi_{\lambda,\mu} \rho \chi_{\lambda,\mu}^\dagger$$

where $\chi_{\lambda,\mu}$ is a linear operator defined as follows:

$$\chi_{\lambda,\mu} = \sum_{(\tau,p)\in K_\lambda,(\sigma,q)\in K_\mu,d\in\{-1,0,1\},x\in\mathbb{Z},T\in\Sigma^*,\text{ s.t. } T_x=\tau} \delta(p,T_x,q,\sigma,d)|q,T_x^\sigma,x+d\rangle\langle p,T,x|$$

Remark 1. Notice that $\chi_{\lambda,\mu} = P_\mu U_M P_\lambda$, where P_ν is a projector defined for any $\nu \in \Lambda$ as follows:

$$P_\nu = \sum_{p\in Q,x\in\mathbb{Z},T\in\Sigma^* \text{ s.t. } (T_x,p)\in K_\nu} |p,T,x\rangle\langle p,T,x|$$

As a consequence, the evolution of $[M]_K$ can be decomposed into a projective measurement of the internal states and the cell pointed out by the head according to the observable $\mathcal{O}_\Lambda = \sum_{\lambda\in\Lambda}\lambda P_\lambda$, then a linear transition U_M – which is the same as the evolution of M – and finally a second projective measurement according to $\mathcal{O}_\Lambda$.

Thus, before and after each transition, a *property* of the machine is measured. The measured property is described by a partition $\{K_\lambda, \lambda \in \Lambda\}$, composed of $|\Lambda|$ regions, of the internal states and the symbols of the cell pointed out by the head. The measurement consists in projecting the internal state of the machine and the state pointed out by the head into one of these regions. This measurement, which produces a classical outcome $\lambda \in \Lambda$, is a *partial* observation, since after the measurement the configuration can be in a superposition of the elements of the region K_λ.

From a physical point of view, $[M]_K$ is realizable if $F_{[M]_K}$ is a trace-preserving completely-positive (tpcp) map.

Definition 5 (Well-observation condition). *An observed* pQTM $[M]_K$ *is well-observed if and only if $F_{[M]_K}$ is a tpcp map, i.e.:*

$$\sum_{\lambda,\mu\in\Lambda} \chi^\dagger_{\lambda,\mu}\chi_{\lambda,\mu} = \mathbb{I}$$

Such a well-observed pre-quantum Turing machine is an observable quantum Turing machine:

Definition 6 (Observable quantum Turing machine). *An* observable quantum Turing machine *(*OQTM *) is a well-observed* pQTM $[M]_K$.

Well-formedness lemma and completion lemma are essential tools for programming QTMs. We introduce analogues for OQTM, i.e., a well-observation lemma and a completion lemma:

Lemma 3 (Well-observation lemma). *For a given* pQTM $M = (\Sigma, Q, \delta)$ *and a given* $K = \{K_\lambda, \lambda \in \Lambda\} \subseteq \Sigma \times Q$, $[M]_K$ *is well-observed if and only if:*
(a) $\forall (\tau, p) \in \Sigma \times Q$,

$$\delta(p,\tau)^\dagger \delta(p,\tau) = 1$$

(b) $\forall \lambda \in \Lambda, \forall (\tau,p),(\tau',p') \in K_\lambda$ *with* $(p,\tau) \neq (p',\tau')$,

$$\delta(p,\tau)^\dagger\delta(p',\tau') = 0$$

(c) $\forall \lambda \in \Lambda, \forall (\tau,p,\sigma),(\tau',p',\sigma') \in K_\lambda \times \Sigma$,

$$\sum_{d\in\{0,1\},q\in Q} \delta(p,\tau,q,\sigma,d-1)^*\delta(p',\tau',q,\sigma',d) = 0$$

(d) $\forall \lambda \in \Lambda, \forall (\tau, p, \sigma), (\tau', p', \sigma') \in K_\lambda \times \Sigma$,

$$\sum_{q \in Q} \delta(p, \tau, q, \sigma, -1)^* \delta(p', \tau', q, \sigma', 1) = 0$$

Proof. According to remark 1, $\chi_{\lambda,\mu} = P_\mu U_M P_\lambda$ so $\sum_{\lambda,\mu \in \Lambda} \chi^\dagger_{\lambda,\mu} \chi_{\lambda,\mu} = \sum_{\lambda \in \Lambda} P_\lambda U_M^\dagger U_M P_\lambda$ since $\sum_{\mu \in \Lambda} P_\mu = \mathbb{I}$. Thus, $[M]_K$ is well-observed if and only if for any basis configurations $|p, T, x\rangle, |p', T', x'\rangle$, $\sum_{\lambda \in \Lambda} \langle p, T, x | P_\lambda U_M^\dagger U_M P_\lambda | p', T', x'\rangle = \langle p, T, x | p', T', x'\rangle$. Since $P_\lambda |p, T, x\rangle = |p, T, x\rangle$ if $(T_x, p) \in K_\lambda$ and 0 otherwise, the well-observation equation is obviously satisfied if (T_x, p) and $(T'_{x'}, p')$ are not in a same block K_λ. If they are in the same block then the well-observation condition is $\langle p, T, x | U_M^\dagger U_M | p', T', x'\rangle = \langle p, T, x | p', T', x'\rangle$. Thus, $[M]_K$ is well-observed iff for each $\lambda \in \Lambda$, the restriction of U_M to $\mathbb{C}^{\{(p,T,x),\ s.t.\ (T_x,p) \in K_\lambda\}}$ is an isometry. For each of these restrictions of U_M, one can apply the well-formedness conditions (see lemma 1) leading to equations (a) to (d). □

Comparing with the well-formedness lemma for QTM (see [11]), the well-observation lemma points out that the well-observation is a weaker condition than the well-formedness condition: equation (a) has to be satisfied by both well-formed and well-observed machines, whereas equations (b) to (d) are weaker for well-observation, since only the pairs of elements in a *same* block have to satisfy the equations.

For a given a partial pQTM $M = (Q, \Sigma, \delta)$ and a given partition K of $\Sigma \times Q$, if δ satisfies the four conditions of the well-observation lemma 3, then $[M]_K$ is called a partially well-observed pQTM.

Lemma 4 (Completion lemma). *For every partially well-observed pQTM $[M]_K$ with a partial quantum transition δ, there exists an* OQTM $[M']_K$ *with the same alphabet, the same set of states, and a transition function δ' which is equal to δ on the domain of δ.*

Proof. The proof consists in applying the QTM completion lemma on each block of the partition K. If $K = \{K_\lambda, \lambda \in \Lambda\}$, then let $M_\lambda = (\Sigma, Q, \delta_\lambda)$, where δ_λ is the restriction of δ to K_λ. According to lemmas 1 and 3, M_λ is a well-formed partial *QTM* , thus M_λ can be expanded to a well-formed *QTM* M'_λ. Let $\delta^{(k)}$ be the transition function of M'_k. Finally, let δ' be such that for any (p, τ), $\delta'(p, \tau) = \delta^{(\lambda)}(p, \tau)$ if $(\tau, p) \in K_\lambda$. Since each $\delta^{(k)}$ satisfies the conditions of lemma 1, δ' satisfies the conditions of lemma 3. Moreover, δ' extends δ. □

5 Examples of Observable Quantum Turing Machines

5.1 Quantum Turing machine

The formalism of observable quantum Turing machines expands the formalism of quantum Turing machines: any QTM is an OQTM where a non-informative partial measurement is performed. Indeed:

Proposition 1. *For any pQTM $M = (\Sigma, Q, \delta)$, M is well-formed if and only if $[M]_{\{\Sigma \times Q\}}$ is well-observed. Moreover, M and $[M]_{\{\Sigma \times Q\}}$ have the same evolution: $F_{[M]_{\{\Sigma \times Q\}}} = F_M$.*

More generally, for any QTM M and any partition K of its internal states, $[M]_K$ is well-observed. However, the evolution of the machine depends on the partition K, so the language recognized by the machine and the execution time depend on the partition K. Proposition 1 states that if K is composed of a unique block, then the evolution of a QTM M and the OQTM $[M]_K$ are the same. Another example where K is a bipartition is given in lemma 5. In that example, for a given QTM M, M and $[M]_K$ do not have the same evolution, however in this particular example the computational power of M and $[M]_K$ are the same.

Halting of quantum Turing machines is symptomatic of the lack of a coherent integration of the notion of observation. The unitary evolution of a QTM implies that the machine, seen as the physical system, does not interact with its environment. As a consequence, it is impossible to know whether the machine halts without measuring it. Moreover, if this measurement reveals that the computation was actually not finished, the machine has to be re-initialised. In order to solve this problem, an ad hoc mechanism, consists in adding a halting qubit to the machine. This qubit can be measured at any time in order to know whether the computation is halted. Such a machine is no more a QTM since its evolution is not unitary, however if some halting condition are satisfied then the computational power of the ad hoc machine is equivalent to the one of the corresponding QTM. One of the aims of the model of observable quantum Turing machines is to describe such a mechanism in a coherent formalism (since observation can be represented in this formalism) and then gives a deeper understanding of the halting of quantum process in general. Thus, following the work of Ozawa [10] on halting of QTM, we show that any QTM M satisfying the halting condition have the same computational power as $[M]_K$ where at each transition the internal state of the machine is measured in order to know when the machine halts.

Lemma 5. *Let $M = (Q, \Sigma, \delta)$ be a* QTM *, then $[M]_H$ is well-observed, where $H = \{\Sigma \times (Q \setminus \{q_f\}), \Sigma \times \{q_f\}\}$. Moreover, if M satisfies the halting condition (i.e., $\forall T \in \Sigma^*, \forall c \in Q \times \Sigma^* \times \mathbb{Z}, \forall t \geq 0, U_M P U_M^t |c\rangle = P U_M P U_M^t |c\rangle$, where $P = \sum_{x \in \mathbb{Z}} |q_f, T, x\rangle\langle q_f, T, x|$), the computational powers of M and $[M]_H$ are equivalent:*
$\forall n \in \mathbb{N}, \forall \rho \in \mathcal{D}(\mathbb{C}^{Q \times \Sigma^* \times \mathbb{Z}}), \forall T \in \Sigma^*$,

$$p_{halt,T}\left(F_M^n(\rho)\right) = p_{halt,T}\left(F_{[M]_H}^n(\rho)\right)$$

where $p_{halt,T}(\rho)$ denotes the probability that the machine halts (i.e. the internal state is q_f) and that the outcome of the tape measurement is T if the configuration of the machine is ρ.

Proof. The proof is based on the result presented in [10].

5.2 Classical Turing machines

In this section, we prove that $[M]_K$ may be well-observed for some K, even if the pQTM M is not well-formed. As a consequence, the well-observation condition is weaker than the well-formedness condition. In lemma 2 a separation between well-formed and well-observed machines is pointed out, by considering deterministic Turing machines.

One can describe a deterministic Turing machines $M = (Q, \Sigma, \delta)$ by means of the pre-quantum Turing machine $\tilde{M} = (Q, \Sigma, \tilde{\delta})$, where $\tilde{\delta}(p, \tau) = |\delta(p, \tau)\rangle$. It is well-known that $\tilde{M}$ is well-formed if and only if M is a reversible deterministic Turing machine. However, we prove for any deterministic Turing machine M, that the OQTM $[\tilde{M}]_{\{\{c\}, c \in \Sigma \times Q\}}$, where a total measurement of the internal states and the cell pointed out by the head is performed, is well-observed:

Proposition 2. *For any* DTM $M = (Q, \Sigma, \delta)$, $[\tilde{M}]_{\{\{c\}, c \in \Sigma \times Q\}}$ *is well-observed, where* $\tilde{M} = (Q, \Sigma, \tilde{\delta})$ *is a* pQTM *such that* $\forall (p, \tau) \in Q \times \Sigma, \tilde{\delta}(p, \tau) = |\delta(p, \tau)\rangle$. *Moreover,* M *and* $[\tilde{M}]_{\{\{c\}, c \in \Sigma \times Q\}}$ *have the same evolution: for any* $c \in Q \times \Sigma^* \times \mathbb{Z}$, $F_{[\tilde{M}]_{\{\{c\}, c \in \Sigma \times Q\}}}(|c\rangle\langle c|) = |M(c)\rangle\langle M(c)|$.

Probabilistic Turing machines are also special instances of OQTMs. A probabilistic Turing machine is a triple $M = (Q, \Sigma, \delta)$, with $\delta : Q \times \Sigma \times Q \times \Sigma \times \{-1, 0, 1\} \to \mathbb{R}^+$, such that for any $(p, \tau) \in Q \times \Sigma$, $\sum_{q \in Q, \sigma \in \Sigma, d \in \{-1,0,1\}} \delta(p, \tau, q, \sigma, d) = 1$. A configuration is a probabilistic distribution described by a valuation function $\nu : Q \times \Sigma^* \times \mathbb{Z} \to \mathbb{R}^+$. The evolution operator F_M of a PTM M is such that for any configuration ν, $F_M(\nu) = (q, T, y) \mapsto \sum_{(p,\tau) \in Q \times \Sigma, d \in \{-1,0,1\}} \delta(p, \tau, q, T_{y-d}, d) \nu(p, T^\tau_{y-d}, y - d)$.

Proposition 3. *For any probabilistic Turing machine* $M = (\Sigma, Q, \delta)$, $[M']_{\{\{c\}, c \in \Sigma \times Q \times \{-1,0,1\}\}}$ *is well observed, and has the same evolution*[7] *as* M, *where* $M' = (\Sigma, Q \times \{-1, 0, 1\}, \delta')$ *is a pQTM with* $\delta' = (p, \tau, q, (\sigma, e), d) \mapsto \begin{cases} \sqrt{\delta(p, \tau, q, \sigma, d)} & \text{if } e = d \\ 0 & \text{otherwise} \end{cases}$.

Proof. In order to satisfy conditions (c) and (d) of the well-observation lemma, a copy of the head move is added to the internal states of the machine, such that the total measurements of the internal states of M' avoid any superposition of the positions of the head, making the observable quantum Turing machine a probabilistic machine without superposition. □

As a consequence, the model of observed quantum Turing machines is not only a formalisation of partial observation of properties during the evolution, but also a unifying model since quantum Turing machines and deterministic Turing machines are observable quantum Turing machines. In the next section, the computational power of observable quantum Turing machines is studied.

6 Computational Power of Observable Quantum Turing Machine

In this section, we mainly show that any observable quantum Turing machine can be simulated within a polynomial slowdown by a quantum Turing machine. In other words, even if the model of observable quantum Turing machines is more expressive than the model of quantum Turing machines, they have the same computational power.

Theorem 1. *For any* OQTM $[M]_K$, *there exists a* QTM M' *which simulates* $[M]_K$ *within a quadratic slowdown.*

The rest of this section is dedicated to the proof of this theorem. In order to simulate the OQTM $[M]_K$ a two-tape QTM $\tilde{M}$ is used. Multi-tape quantum Turing machines have been introduced in [16]. One of the tapes of $\tilde{M}$ is used to simulate the tape of M, whereas the second tape is an history, where the superposition of the possible outcomes of an hypothetical observation according to K of the current internal state is stored. At the end of the computation, this auxillary tape is measured, simulating the observable quantum Turing machine. First, a

[7] Notice that the configuration of an OQTM $[M]_K$ is a density matrix where as a configuration of a probabilistic Turing machine M' is a probabilistic distribution that can be represented as a valuation function $\nu : Q \times \Sigma^* \times \mathbb{Z} \to \mathbb{R}^+$. As a consequence, we say that the evolutions of $[M]_K$ and M' are the same if $\Phi \circ F_{[M]_K} \circ \Psi = F_{M'}$, where $\Psi(\nu) = \sum_{c \in Q \times \Sigma^* \times \mathbb{Z}} \nu(c) \, |c\rangle\langle c|$ and $\Phi(\rho) = c \mapsto \langle c|\rho|c\rangle$.

such two-tape quantum Turing machine is defined and we prove the well-fornedness of this machine, then we prove the simulation of the original observable quantum Turing machine with a linear slowdown. Finally, this two-tape quantum Turing machine can be simulated by a one-tape quantum Turing machine within a quadratic slowdown.

For a given pQTM $M = (Q, \Sigma, \delta)$ and a partition $K = \{K_\lambda, \lambda \in \Lambda\}$ of $\Sigma \times Q$, let $\tilde{M} = (Q, \Sigma \times \Lambda^2 \cup \{\#\}, \tilde{\delta})$ be a 2-tape quantum Turing machine. The alphabet of the first tape is Σ, the alphabet of the second tape is $\Lambda^2 \cup \{\#\}$. The transition function $\tilde{\delta}$ of $\tilde{M}$ is defined as follows: $\forall p \in Q, \forall \tau \in \Sigma$,

$$\tilde{\delta}(p, \tau, \#) = \sum_{\mu \in \Lambda, (\sigma, q) \in K_\mu, d \in \{-1,0,1\}} \delta(p, \tau, q, \sigma, d)|q, \sigma, d, ([\tau, p], \mu), 1\rangle$$

where $[\tau, p] \in \Lambda$ is such that $(\tau, p) \in K_{[\tau,p]}$.

Notice that the second head always moves right, revealing necessary a blank symbol. That is why the transition function is partially defined. One can prove that $\tilde{\delta}$ verifies the well formedness conditions of *unity, orthogonality, and separability* – see theorem 5.2.2 in [1] for the well-formedness lemma for 1-tape QTM and lemma 1 in [16] for multi-tape QTM. Thus according to the completion lemma – lemma 2 in [16] – $\tilde{\delta}$ can be extended such that the corresponding pQTM is well-formed.

The evolution $U_{\tilde{M}}$ of $\tilde{M}$ is such that for any $p \in Q, x \in \mathbb{Z}, n \in \mathbb{N}^*, T \in \Sigma^*, w \in (\Lambda^2)^{n-1}$,

$$U_{\tilde{M}}|p, T, x, w, n\rangle = \sum_{q \in Q, \sigma \in \Sigma, \lambda, \mu \in \Lambda, d \in \{-1,0,1\}} \tilde{\delta}(p, T_x, \#, q, \sigma, d, (\lambda, \mu), 1)|q, T_x^\sigma, x + d, w(\lambda, \mu), n + 1\rangle$$

Thus,

$$U_{\tilde{M}}|p, T, x, w, n\rangle = \sum_{\mu \in \Lambda, (\sigma, q) \in K_\mu, d \in \{-1,0,1\}} \delta(p, T_x, q, \sigma, d)|q, T_x^\sigma, x + d, w([\tau, p], \mu), n + 1\rangle$$

The simulation of M by the 2-tape quantum Turing machine $\tilde{M}$ works as follows: for any initial configuration $\rho \in \mathcal{D}(\mathbb{C}^{Q \times \Sigma \times \mathbb{Z}})$ of M, the initial configuration of $\tilde{M}$ is $\rho \otimes |\#\rangle\langle\#| \otimes |0\rangle\langle 0|$. It means that the internal state and the state of the first tape are the same as M, whereas the second tape is empty and the head of the second tape points out the cell indexed by 0. After n transitions, the configuration of $\tilde{M}$ is $U^n_{\tilde{M}}(\rho \otimes |\#\rangle\langle\#| \otimes |0\rangle\langle 0|)U^{\dagger n}_{\tilde{M}}$. At that time, the second head points out the cell indexed by n, and all the cells of the second tape have a blank symbol except the cells between 0 and $n-1$. These non-blank cells of the second tape are then measured, leading to the configuration $\sum_{w \in (\Lambda^2)^n} \langle w|U^n_{\tilde{M}}(\rho \otimes |\#\rangle\langle\#| \otimes |0\rangle\langle 0|)U^{\dagger n}_{\tilde{M}}|w\rangle$. We prove, by induction on n, that this resulting configuration is equal to $F^n_{[M]_K}(\rho) \otimes |\#\rangle\langle\#| \otimes |n\rangle\langle n|$. In order to initialize the induction, notice that the property is true after $n = 0$ transition. For any $n > 0$, the configuration of $\tilde{M}$, after $n + 1$ transitions and the measurement of the second tape is

$$\begin{aligned}\rho' &= \sum_{w \in (\Lambda^2)^{n+1}} \langle w|U^{n+1}_{\tilde{M}}(\rho \otimes |\#\rangle\langle\#| \otimes |0\rangle\langle 0|)U^{\dagger n+1}_{\tilde{M}}|w\rangle \\ &= \sum_{\lambda, \mu \in \Lambda, w \in (\Lambda^2)^n} \langle w|\langle(\lambda, \mu)|_{n+1} U^{n+1}_{\tilde{M}}(\rho \otimes |\#\rangle\langle\#| \otimes |0\rangle\langle 0|)U^{\dagger n+1}_{\tilde{M}}|w\rangle|(\lambda, \mu)\rangle_{n+1}\end{aligned}$$

where $\langle(\lambda, \mu)|_n$ means that $\langle(\lambda, \mu)|$ is applied on the cell indexed by n on the second tape.

Since the second head always moves right, the transition number $n+1$ does not act on the cells indexed between 0 and $n-1$ of the second tape, and thus commutes with any operation acting on these cells:

$$\rho' = \sum_{\lambda,\mu\in\Lambda, w\in(\Lambda^2)^n} \langle(\lambda,\mu)|_n U_{\tilde{M}} \langle w|U_{\tilde{M}}^n(\rho\otimes|\#\rangle\langle\#|\otimes|0\rangle\langle 0|)U_{\tilde{M}}^{\dagger n+1}|w\rangle U_{\tilde{M}}^{\dagger}|(\lambda,\mu)\rangle_n$$

By induction,

$$\rho' = \sum_{\lambda,\mu\in\Lambda} \langle(\lambda,\mu)|_n U_{\tilde{M}}(F_{[M]_K}^n(\rho)\otimes|\#\rangle\langle\#|\otimes|n\rangle\langle n|)U_{\tilde{M}}^{\dagger}|(\lambda,\mu)\rangle_n$$

For any $p,p'\in Q$, any $T,T'\in\Sigma^*$, and any $x,x'\in\mathbb{Z}$,

$$\begin{aligned}
&\sum_{\lambda,\mu\in\Lambda}\langle(\lambda,\mu)|_n U_{\tilde{M}}|p,T,x,\#,n\rangle\langle p',T',x,\#,n|U_{\tilde{M}}^{\dagger}|(\lambda,\mu)\rangle_n\\
&=\sum_{\lambda,\mu\in\Lambda}\langle(\lambda,\mu)|_n \sum_{\mu_0,\mu_0'\in\Lambda,(\sigma,q)\in K_{\mu_0},(\sigma',q')\in K_{\mu_0'},d,d'\in\{-1,0,1\}} \delta(p,T_x,q,\sigma,d)\delta^{\dagger}(p',T'_{x'},q',\sigma',d')|q,T_x^{\sigma},x+d,([T_x,p],\mu_0),n+1\rangle\\
&\qquad\qquad\langle q',T'^{\sigma'}_{x'},x'+d',([T'_{x'},p'],\mu_0'),n+1||(\lambda,\mu)\rangle_n\\
&=\sum_{\lambda,\mu\in\Lambda}\langle\lambda|[T_x,p]\rangle\langle[T'_{x'},p']|\lambda\rangle\sum_{(\sigma,q)\in K_\mu,d,d'\in\{-1,0,1\}}\delta(p,T_x,q,\sigma,d)\delta^{\dagger}(p',T'_{x'},q',\sigma',d')|q,T_x^{\sigma},x+d,\#,n+1\rangle\\
&\qquad\qquad\langle q',T'^{\sigma'}_{x'},x'+d',\#,n+1|\\
&=\sum_{\lambda,\mu\in\Lambda}\chi_{\lambda,\mu}|p,T,x\rangle\langle p',T',x'|\chi_{\lambda,\mu}^{\dagger}\otimes|\#\rangle\langle\#|\otimes|n+1\rangle\langle n+1|\\
&=F_{[M]_K}(|p,T,x\rangle\langle p',T',x'|)\otimes|\#\rangle\langle\#|\otimes|n+1\rangle\langle n+1|
\end{aligned}$$

Thus,

$$\rho' = F_{[M]_K}^{n+1}(\rho)\otimes|\#\rangle\langle\#|\otimes|n+1\rangle\langle n+1|$$

Thus $\tilde{M}$ simulates M within a linear slowdown. Since any two-tape quantum Turing machine can be simulated by a one-tape QTM within a quadratic slowdown [16], M is simulated by a one-tape QTM within a quadratic slowdown. □

7 Conclusion and perspectives

This paper has introduced observable quantum Turing machines (OQTM) as a generalisation of quantum Turing machines (QTM) allowing partial observation of the machine during the computation. OQTM provides a formal model to deal with applications where partial observations of the machine are necessary, like the halting problem where observations are used to know whether the computation is halted or not. OQTM turns out to be a unifying model of Turing machines, since any QTM but also any deterministic TM are special instances of OQTM, whereas it is well-known that non reversible deterministic TM cannot be expressed into the formalism of QTM. However, the computational power of OQTM is equivalent to the power of QTM. Thus, the well-observation condition (condition verified by OQTM) is weaker than the well-formedness condition (condition verified by QTM) and is a good candidate to meet the necessary and sufficient conditions for a Turing machine to be a valid quantum device. Since observations are formalized in OQTM, a perspective is to investigate the connections between OQTM and recent models of quantum computation based on measurements (Teleportation-based model [8, 13], One-way model [15, 3]) and the formal framework of classically-controlled quantum Turing machines [14].

Indeed, the structure of the OQTM is inspired from the paradigm *quantum data, classical control*: quantum data are stored on the tape of the machine, while the control, thanks to the partial observation of the internal states and the cell pointed out by the cell, is hybrid. A perspective is to characterize the amount of quantum control needed to have an efficient quantum device: what is the minimal k for which any OQTM $[M]_K$ can be efficiently simulated with an OQTM $[M']_{K'}$ where all the blocks of K' have a size less than k ?

Another open question is the existence of a universal OQTM. Recent developments in the quest of a universal QTM [5, 7] point out that existence of a classical control could be helpful for the design of a universal machine.

References

1. E. Bernstein and U. Vazirani. Quantum complexity theory. *SIAM J. Comput.*, 26:1411–1478, 1997.
2. M.-D. Choi. Completely positive linear maps on complex matrices. *Linear Algebra Appl.*, 10:285, 1975.
3. V. Danos, E. Kashefi, and P. Panangaden. The measurement calculus. arXiv:quant-ph/0412135, 2004.
4. D. Deutsch. Quantum theory, the Church-Turing principle and the universal quantum computer. *Proc. R. Soc. Lond. A*, 400:97–117, 1985.
5. Willem Fouché, Johannes Heidema, Glyn Jones, and Petrus H. Potgieter. Universality and programmability of quantum computers. arXiv.org:0710.3329, 2007.
6. S. Iriyama, M. Ohya, and I. Volovich. Generalized quantum Turing machine and its application to the sat chaos algorithm. In *Proceedings of the Symposium on Information Theory and Its Applications*, pages 779–781, 2006.
7. M. Müller. Strongly universal quantum turing machines and invariance of kolmogorov complexity. *IEEE Transactions on Information Theory,*, 54(2), 2008.
8. M. A. Nielsen. Universal quantum computation using only projective measurement, quantum memory, and preparation of the 0 state. *Phys. Rev. A*, 308:96–100, 2003.
9. M. A. Nielsen and I. L. Chuang. *Quantum computation and quantum information*. Cambridge University Press, New York, NY, USA, 2000.
10. M. Ozawa. Halting of quantum Turing machines. In *UMC*, pages 58–65, 2002.
11. Masanao Ozawa and Harumichi Nishimura. Local transition functions of quantum turing machines. *Theoretical Informatics and Applications*, 34:379, 2000.
12. C. M. Papadimitriou. *Computational complexity*. Addison-Wesley, 1994.
13. S. Perdrix. State transfer instead of teleportation in measurement-based quantum computation. *International Journal of Quantum Information*, 3(1):219–223, 2005.
14. S. Perdrix and Ph. Jorrand. Classically-controlled quantum computation. *Math. Struct. in Comp. Science*, 16:601–620, 2006.
15. R. Raussendorf, D. E. Browne, and H. J. Briegel. The one-way quantum computer - a non-network model of quantum computation. *Journal of Modern Optics*, 49:1299, 2002.
16. T. Yamakami. A foundation of programming a multi-tape quantum Turing machine. In *MFCS '99: Proceedings of the 24th International Symposium on Mathematical Foundations of Computer Science*, pages 430–441, London, UK, 1999. Springer-Verlag.