Int. Journ. of Unconventional Computing, Vol. 7, pp. 291–311
Reprints available directly from the publisher
Photocopying permitted by license only

Towards Observable Quantum Turing Machines: Fundamentals, Computational Power, and Universality

SIMON PERDRIX

CNRS, LIG, Grenoble University, France
E-mail: Simon.Perdrix@imag.fr

Received: September, 2009. Accepted: February, 2010

We study the observation of quantum Turing machines by allowing interactions between a quantum machine and its environment during the computation, whereas a quantum Turing machine —original model introduced by Deutsch— remains isolated.

We show that the introduction of observations leads to a weakening of the well formedness conditions of quantum Turing machines such that any (reversible or not) classical Turing machine is a special instance of a quantum machine. Moreover, observation of quantum Turing machines provides a formal solution to the halting process problem: the impossibility to know whether a given quantum Turing machine has actually reached its halting state. It also provides a more realistic abstract architecture of a quantum computer while most of the physical proposals of quantum computers are based on an hybrid classical-quantum architecture.

However, we show that a natural formalisation of an observable quantum Turing machines leads to an over-powerful model solving undecidable problems. As a consequence, we introduce a restricted version of observable quantum Turing machines and we show that, under this restriction, any observable quantum Turing machine can be efficiently simulated by a quantum Turing machine. Finally, we discuss the potential application of the observable quantum Turing machine in the quest of a universal quantum Turing machine while recent papers have pointed out that a classical control is a key feature of a universal quantum machine.

Keywords: Quantum Computing, Turing machine

1 INTRODUCTION

The quantum Turing machine (QTM) has been introduced by Deutsch [4] as the very first model of quantum computation. Roughly speaking, a quantum Turing machine can be seen as a generalisation of a probabilistic Turing machine where the probabilities which are associated with any transition are replaced by *amplitudes* i.e., complex numbers. The use of complex numbers leads to model fundamental phenomena of quantum mechanics like interferences and entanglement.

A probabilistic Turing machine has to satisfy well-formedness conditions ensuring that for any configuration, the probabilities of all the possible evolutions sum to one (or at most one). A quantum Turing machine has to satisfy similar well-formedness conditions. These well-formedness conditions ensure that the evolution of a quantum Turing machine (i) does not violate the law of quantum mechanics; (ii) is reversible. This latter condition can be rephrased in more physical terms as an isolation of the quantum Turing machine from its environment during the computation.

The reversibility assumption of quantum Turing machines is questionable for several reasons, including the emergence of quantum computing models based on non reversible evolutions, like the one-way model [2, 3, 17] or more generally the measurement-based quantum computations [9, 15], which point out that a quantum computation is not necessary reversible. Moreover, the isolation assumption leads to technical issues like the impossibility to know whether a running computation is terminated or not i.e., whether the halting state is reached or not. Finally, due to the isolation assumption, quantum Turing machines are the natural quantum versions of reversible Turing machines, but the natural embedding of any reversible Turing machine into a quantum Turing machine cannot be extended to non-reversible and probabilistic Turing machines.

We study a weakening of the well-formedness condition of QTM leading to Observable Quantum Turing Machines (OQTM). No more isolated, an OQTM can be seen as a QTM which is able to interact with its environment. Modelling environment behaviour is a key issue. Indeed, we point out that some naive modelling of environment increases drastically the computational power of the machine. Finally, we show that the environment can be modelled in such way that QTM and OQTM have the same computational power.

In section 2, we present the mathematical background on Hilbert spaces for describing quantum states and evolutions. Section 3 is dedicated to quantum Turing machines and their basic properties. In section 5, observable quantum Turing machines are introduced: the action of the environment is modelled as a measurement of the configuration of the machine. This measurement occurs between every transition of the machine and is characterised by a partition of the classical configurations of the machine. In section 6, examples of OQTMs are given: all deterministic, probabilistic and quantum Turing machines are

special instances of OQTM, making this model a general model of quantum computing. A formal solution to the halting process of quantum machines is also presented. In section 7, we prove that the undecidable halting problem can be solved in constant time and high probability with an OQTM, proving that this model is over-powerful. A restricted version is introduced, where the environment can act on the internal state of the machine and the cell pointed out by the head only. We show that any such restricted machine can be efficiently simulated by a quantum Turing machine. Moreover fundamental lemmas (well-observation and completion lemmas) are introduced for restricted OQTM. Finally, in section 8, the role of the OQTM in the quest of a universal Turing machine is discussed.

2 QUANTUM COMPUTING BASICS

We briefly recall the basic definitions of quantum computing; please refer to Nielsen and Chuang [10] for a complete introduction to the subject.

For any countable set A, we denote by $\mathbb{C}^A$ the ℓ^2 space $\{\varphi : A \to \mathbb{C} \mid \sum_{a\in A} |\varphi(a)|^2 < \infty\}$. For any $a \in A$, let $|a\rangle = x \mapsto \delta_{x,a} \in \mathbb{C}^A$ be a *ket* vector where $\delta_{x,y} = 1$ if $x = y$ and 0 otherwise. $\{|a\rangle\}_{a\in A}$ is a basis of $\mathbb{C}^A$.

For any $a \in A$, let $\langle a| : \mathbb{C}^A \to \mathbb{C} :: \varphi \mapsto \varphi(a)$ be a *bra* vector[1]. For any $\varphi \in \mathbb{C}^A$, let $\varphi^\dagger : \mathbb{C}^A \to \mathbb{C} :: \sum_{a\in A} \varphi(a)^* \langle a|$ be the adjoint of φ, where x^* is the complex conjugate of x. Moreover, for any φ in the dual space $\mathbb{C}^A \to \mathbb{C}$, let $\varphi^\dagger \in \mathbb{C}^A$ be $\sum_{a\in A} \varphi(|a\rangle)^* |a\rangle$. Notice that for any $\varphi \in \mathbb{C}^A$, $\varphi^{\dagger\dagger} = \varphi$. The adjoint of a linear map $U : \mathbb{C}^A \to \mathbb{C}^B$ is $U^\dagger : \mathbb{C}^B \to \mathbb{C}^A :: \varphi \mapsto (\varphi^\dagger \circ U)^\dagger$.

For any $\varphi \in \mathbb{C}^A$ and $\psi \in \mathbb{C}^B$ let $\varphi \otimes \psi = (a, b) \mapsto \varphi(a).\psi(b) \in \mathbb{C}^{A\times B}$. The tensor product is defined on linear maps as follows on basis states: for any $U : \mathbb{C}^A \to \mathbb{C}^C$ and $V : \mathbb{C}^B \to \mathbb{C}^D$, $U \otimes V : \mathbb{C}^{A\times B} \to \mathbb{C}^{C\times D} :: |a\rangle \otimes |b\rangle \mapsto (U|a\rangle) \otimes (V|b\rangle)$.

$\mathbb{C}^A$ together with the inner product $\langle . | . \rangle : \mathbb{C}^A \times \mathbb{C}^A \to \mathbb{C} = (\varphi, \psi) \mapsto \varphi^\dagger \psi$ is a Hilbert space.

Definition 1. *Let $\mathcal{D}(A)$ be the set of density matrices[2] on $\mathbb{C}^A$ i.e., the self-adjoint positive-semidefinite linear maps of trace one:*

$$\mathcal{D}(A) = \{\rho : \mathbb{C}^A \to \mathbb{C}^A \mid \rho = \rho^\dagger, \rho \geq 0 \text{ and } Tr(\rho) = 1\}$$

where $\rho \geq 0$ means that all eignevalues of ρ are non negative, and $Tr(\rho) = 1$ means that the eigenvalues of ρ sum to one.

A density matrix represents the state of a quantum system. For any $a \in A$, $|a\rangle\langle a| \in \mathcal{D}(A)$ is interpreted as a classical state a. A diagonal density matrix

[1] $\langle a|$ is a vector of the dual space $\mathbb{C}^A \to \mathbb{C}$

[2] We use the term density 'matrix', instead of 'map', even if A is infinite

$\rho = \sum_{a\in A} p_a |a\rangle\langle a|$ is interpreted as a probability distribution where a occurs with probability p_a.

Definition 2. *A quantum evolution is a trace-preserving completely-positive (tpcp) map $F : \mathcal{D}(A) \to \mathcal{D}(B)$ i.e., $\forall \rho \in \mathcal{D}(A), Tr(F(\rho)) = Tr(\rho)$ and for any finite set C, and any $\rho \in \mathcal{D}(A \times C)$, $\rho \geq 0$ implies $(F \otimes I)(\rho) \geq 0$ where $I : \mathcal{D}(C) \to \mathcal{D}(C)$ is the identity.*

A Kraus representation of a tpcp map $F : \mathcal{D}(A) \to \mathcal{D}(B)$ is a countable family of linear maps $\{M_x : \mathbb{C}^A \to \mathbb{C}^B\}_{x\in X}$ satisfying the completeness condition $\sum_{x\in X} M_x^\dagger M_x = I$ such that for any $\rho \in \mathcal{D}(A)$, $F(\rho) = \sum_{x\in X} M_x \rho M_x^\dagger$. Two important subfamilies of tpcp maps are the *isometries* and the *projective measurements*:

- A tpcp map $F : \mathcal{D}(A) \to \mathcal{D}(A)$ is an *isometry* if it has a Kraus representation composed of a unique map U such that $U^\dagger U = I$. Such a tpcp map $F : \rho \mapsto U\rho U^\dagger$ represents the evolution of an isolated quantum system.
- A tpcp map $F : \mathcal{D}(A) \to \mathcal{D}(A)$ is an *projective measurement* if it has a Kraus representation $\{P_x\}_{x\in X}$ composed of orthogonal projectors ($P_x P_y = \delta_{x,y} P_x$.) Such a tpcp map $F : \rho \mapsto \sum_{x\in X} P_x \rho P_x$ represents the observation of a quantum system.

3 QUANTUM TURING MACHINE

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

Definition 3. *Let $\tilde{\mathbb{R}}$ be the set of computable real numbers: a real number $x \in \mathbb{R}$ is computable if and only if it exists a deterministic Turing machine which on input 1^n computes a binary representation of an integer $m \in \mathbb{Z}$ such that $\left|\frac{m}{2^n} - x\right| \leq \frac{1}{2^n}$.*

Computable complex numbers are defined as follows: $z = x + iy \in \tilde{\mathbb{C}}$ if and only if $x, y \in \tilde{\mathbb{R}}$. Moreover, a vector $\varphi \in \mathbb{C}^A$ is a computable vector ($\tilde{\mathbb{C}}^A$) if and only if for any $a \in A$, $\varphi(a) \in \tilde{\mathbb{C}}$.

Definition 4. (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*

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

such that $\forall \tau \in \Sigma, \delta(q_f, \tau) = |q_f, \tau, 0\rangle$.

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

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

$T_x^\sigma \in \Sigma^*$ 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 5. (Well-formedness condition) *A* pQTM M *is well-formed if and only if* F_M *is an isometry, i.e.* $U_M^\dagger U_M = I$.

Lemma 1 (Well-formedness lemma [12]). *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) $\forall (\tau, p, \sigma), (\tau', p', \sigma') \in \Sigma \times Q \times \Sigma$,

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

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

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

A triple $M = (\Sigma, Q, \delta)$ is called a partial pQTM if δ is a partial quantum transition function, i.e. δ is not defined on all inputs. 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 [12]). *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 $\rho_0 = |c\rangle\langle c| \in \mathcal{D}(Q \times \Sigma^* \times \mathbb{Z})$ (we assume that the initial configuration is a classical configuration), then after n transitions, the configuration of the machine is $\rho_n = U_M^n \rho_0 (U_M^\dagger)^n$.

In order to know the outcome of the computation, a final projective measurement $\{P_c = |c\rangle\langle c|\}_{c \in \{q_f\} \times \Sigma^* \times \mathbb{Z}} \cup \{P_\perp = \sum_{c \in (Q \setminus \{q_f\}) \times \Sigma^* \times \mathbb{Z}} |c\rangle\langle c|\}$ is performed. The classical outcome $\perp$ represents the case where the halting state is not reached thus the computation made is useless. Notice that no transition is applied after this final measurement.

4 COMPUTABILITY AND UNIVERSALITY OF QUANTUM TURING MACHINES

Quantum computational models are expected to be more powerful than the classical Turing machines in terms of complexity but not in terms of computability. In the particular case of the QTMs, the restriction to computable complex numbers guarantees that any QTM can be simulated by a TM.

The existence of a universal quantum Turing machine is still an open question. Bernstein and Vazirani [1] showed the existence of a universal machine for a subclass of QTM, namely the stationary and normal form quantum Turing machines (SNQTM). This universal machine U simulates any SNQTM M with accuracy ϵ within a slowdown polynomial in $1/\epsilon$ and T where T is the execution time of M and is part of the input of U.

5 OBSERVABLE QUANTUM TURING MACHINE

Since the evolution of a QTM is an isometry, 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 [11] 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 6. (Observable pre-quantum Turing machine) *Given a* pQTM $M = (\Sigma, Q, \delta)$*, and a partition* $K = \{K_\lambda, \lambda \in \Lambda\}$ *of* $Q \times \Sigma^* \times \mathbb{Z}$*,* $[M]_K$ *is an* observable pre-quantum Turing machine*. The evolution of* $[M]_K$ *is given by* $F_{[M]_K}$*:*

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

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

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

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:*

$$P_\nu = \sum_{(p,T,x)\in K_\nu} |p,T,x\rangle\langle p,T,x|$$

As a consequence, the evolution of $[M]_K$ can be decomposed into a projective measurement of the configuration according to the projective measurement $\{P_\lambda\}_{\lambda\in\Lambda}$ induced by the partition K, then a linear transition U_M – which is the same as the evolution of M – and finally a second projective measurement according to $\{P_\lambda\}_{\lambda\in\Lambda}$. Indeed,

$$F_{[M]_K} = Meas_K \circ F_M \circ Meas_K$$

where $Meas_{\{K_\lambda,\lambda\in\Lambda\}} = \rho \mapsto \sum_{\lambda\in\Lambda} P_\lambda \rho P_\lambda$

Thus, before and after every transition, a *property* of the machine is observed. The measured property is described by a partition $\{K_\lambda, \lambda \in \Lambda\}$ of the configurations of the machine. The measurement consists in projecting the configuration of the machine 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.

$[M]_K$ has a valid evolution if $F_{[M]_K}$ is a trace-preserving completely-positive (tpcp) map leading to the following condition called *well-observation*:

Definition 7. (Well-observation condition) *An observable* pQTM $[M]_K$ *is well-observed if and only if $F_{[M]_K}$ is a tpcp map, i.e.:*

$$\sum_{\lambda,\mu\in\Lambda} \chi_{\lambda,\mu}^\dagger \chi_{\lambda,\mu} = I$$

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

Definition 8. (Observable quantum Turing machine) *An* observable quantum Turing machine *(*OQTM *) is a well-observed* pQTM $[M]_K$.

6 EXAMPLES OF OBSERVABLE QUANTUM TURING MACHINES

6.1 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:

Lemma 3. *For any* pQTM $M = (\Sigma, Q, \delta)$, *M is well-formed if and only if $[M]_K$ is well-observed for any partition K. Moreover, M and $[M]_{\{Q\times\Sigma\times\mathbb{Z}\}}$ have the same evolution: $F_{[M]_{\{Q\times\Sigma\times\mathbb{Z}\}}} = F_M$.*

Proof. If M is well-formed, then for any partition K, $[M]_K$ is well observed since

$$\begin{aligned}\sum_{\lambda,\mu\in\Lambda} \chi^\dagger_{\lambda,\mu}\chi_{\lambda,\mu} &= \sum_{\lambda,\mu\in\Lambda} P^\dagger_\lambda U^\dagger_M P^\dagger_\mu P_\mu U_M P_\lambda \\ &= \sum_{\lambda\in\Lambda} P^\dagger_\lambda U^\dagger_M \left(\sum_{\mu\in\Lambda} P_\mu\right) U_M P_\lambda \\ &= \sum_{\lambda\in\Lambda} P^\dagger_\lambda U^\dagger_M U_M P_\lambda \\ &= \sum_{\lambda\in\Lambda} P_\lambda \\ &= I\end{aligned}$$

Moreover, let $K = \{Q \times \Sigma \times \mathbb{Z}\}$ be the trivial partition composed of a unique region $K_0 = Q \times \Sigma \times \mathbb{Z}$, the corresponding projector $P_0 = I$. Thus, if $[M]_{\{Q\times\Sigma\times\mathbb{Z}\}}$ is well-observed, then M is well-formed and $F_{[M]_{\{Q\times\Sigma\times\mathbb{Z}\}}} = F_M$. □

According to lemma 3, any QTM M and any partition K of its configurations, $[M]_K$ 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. Lemma 3 states that if K is composed of a unique block, then the evolutions 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.

Lemma 3 shows that if M is a well-formed QTM, then for any partition K of the configurations, $[M]_K$ is well-observed. Conversely, if $[M]_K$ is a well-observed OQTM, $[M]_K$ can be decomposed into a collection of partially well-formed QTM, each of these acting on one region defined by the partition K:

Lemma 4. *An observed* pQTM *$[M]_{\{K_\lambda,\lambda\in\Lambda\}}$ is well-observed iff for any $\lambda \in \Lambda$, $M^\lambda = (Q, \Sigma, \delta^\lambda)$ is partially well-formed, where δ^λ is the restriction of δ to S_λ and $S_\lambda = \{(\tau, p) \in \Sigma \times Q \mid \exists (T, x) \in \Sigma^* \times \mathbb{Z}$ s.t. $Tx = \tau$ and $(p, T_x, x) \in K_\lambda\}$.*

Proof. Notice that M_λ is well-formed iff $U_{M^\lambda} : \mathbb{C}^{K_\lambda} \to \mathbb{C}^{Q\times\Sigma^*\times\mathbb{Z}}$ is an isometry. Moreover, for any $\lambda \in \Lambda$, and any $\varphi \in \mathbb{C}^{K_\lambda}$, $U_{M^\lambda}\varphi = U_M\varphi = U_M P_\lambda \varphi$.

Thus, $\forall\lambda \in \Lambda$, M^λ is well-formed $\iff$ $\forall\lambda \in \Lambda, U^\dagger_{M^\lambda} U_{M^\lambda} = I_{K_\lambda}$ $\iff$ $\bigoplus_{\lambda\in\Lambda} U^\dagger_{M^\lambda} U_{M^\lambda} = I_{Q\times\Sigma^*\times\mathbb{Z}}$ $\iff$ $\sum_{\lambda\in\Lambda} P_\lambda U^\dagger U_M P_\lambda = I$ $\iff$ $\sum_{\lambda,\mu\in\Lambda} P_\lambda U^\dagger P_\mu P_\mu U_M P_\lambda = I$ □

6.2 Halting of quantum Turing machines

Halting of quantum Turing machines is symptomatic of the lack of a coherent integration of the notion of observation in the model of quantum Turing machines. The isometric 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 [11]. This qubit can be measured at any time in order to know whether the computation is halted or not. Such a machine is no more a QTM since its evolution is not unitary, however if some halting conditions 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 [11] on halting of QTM, we show that any QTM M satisfying the halting condition has the same computational power as $[M]_K$ where at each transition the internal state of the machine is measured in order to know whether the halting state of the machine is reached or not.

Definition 9 (Halting condition). *A pQTM $M = (Q, \Sigma, \delta)$ satisfies the halting condition if $\forall T \in \Sigma^*, \forall c \in Q \times \Sigma^* \times \mathbb{Z}, \forall t \geq 0$,*

$$U_M P U_M^t |c\rangle = P U_M P U_M^t |c\rangle$$

where $P = \sum_{x\in\mathbb{Z}} |q_f, T, x\rangle\langle q_f, T, x|$.

Lemma 5. *Let $M = (Q, \Sigma, \delta)$ be a* QTM *, then $[M]_H$ is well-observed, where $H = \{(Q \setminus \{q_f\}) \times \Sigma^* \times \mathbb{Z}, \Sigma \times \{q_f\} \times \Sigma^* \times \mathbb{Z}\}$ and $q_f \in Q$ is the halting state of M. Moreover, if M satisfies the halting condition, then M and $[M]_H$ are equivalent:*
$\forall n \in \mathbb{N}, \forall \rho \in \mathcal{D}(Q \times \Sigma^* \times \mathbb{Z}), \forall T \in \Sigma^*$,

$$p_{halt,T}\left(F^n_M(\rho)\right) = p_{halt,T}\left(F^n_{[M]_H}(\rho)\right)$$

where $p_{halt,T}(\rho) = \sum_{x\in\mathbb{Z}} \langle q_f, T, x|\rho|q_f, T, x\rangle$ *denotes the probability that the machine halts (i.e. the internal state is* q_f*) and that the state of the tape is* T *if the configuration of the machine is* ρ.

Proof. The proof is based on the result presented in [11]. Let $K_f = \Sigma \times \{q_f\}$ and $K_{\bar{f}} = \Sigma \times (Q \setminus \{q_f\})$ then $H = \{K_f, K_{\bar{f}}\}$. Let P_f and $P_{\bar{f}}$ be defined as in remark 1 and $\chi_{\lambda,\mu} = P_\mu U_M P_\lambda$, with $\lambda, \mu \in \{f, \bar{f}\}$ as in definition 8.

First, since q_f is the final internal state, for any $\tau \in \Sigma$, $\delta(q_f, \tau) = |q_f, \tau, 0\rangle$, so $\chi_{f,f} = P_f U_M P_f = P_f$ and $\chi_{f,\bar{f}} = 0$. Thus, $F_{[M]_H}(\rho) = \chi_{f,f}\rho\chi_{f,f}^\dagger + \chi_{\bar{f},f}\rho\chi_{\bar{f},f}^\dagger + \chi_{\bar{f},\bar{f}}\rho\chi_{\bar{f},\bar{f}}^\dagger$.

Moreover, $\chi_{f,f}\chi_{f,f} = \chi_{f,f}$, $\chi_{f,f}\chi_{\bar{f},f} = \chi_{\bar{f},f}$ and $\chi_{f,f}\chi_{\bar{f},\bar{f}} = \chi_{\bar{f},f}\chi_{f,f} = \chi_{\bar{f},f}\chi_{\bar{f},f} = \chi_{\bar{f},\bar{f}}\chi_{f,f} = \chi_{\bar{f},\bar{f}}\chi_{\bar{f},f} = 0$. It comes, for any $n \in \mathbb{N}$,

$$F^n_{[M]_H}(\rho) = \chi_{f,f}\rho\chi_{f,f}^\dagger + \sum_{k=0}^{n-1} \chi_{\bar{f},f}\chi^k_{\bar{f},\bar{f}}\rho\chi^{\dagger k}_{\bar{f},\bar{f}}\chi^\dagger_{\bar{f},f} + \chi^n_{\bar{f},\bar{f}}\rho\chi^{\dagger n}_{\bar{f},\bar{f}}$$

By definition, $p_{halt,T}(\rho) = \sum_{x\in\mathbb{Z}} \langle q_f, T, x|\rho|q_f, T, x\rangle = Tr(\langle T|P_f\rho P_f|T\rangle)$. As a consequence,

$$p_{halt,T}\left(F^n_M(\rho)\right) \quad = \quad Tr(\langle T|P_f U^n_M \rho U^{\dagger n}_M P_f|T\rangle)$$

and

$$\begin{aligned}
&p_{halt,T}\left(F^n_{[M]_H}(\rho)\right) = \\
&Tr(\langle T|P_f F^n_{[M]_H}(\rho)P_f|T\rangle) = \\
&Tr(\langle T|P_f(\chi_{f,f}\rho\chi^\dagger_{f,f} + \textstyle\sum_{k=0}^{n-1} \chi_{\bar{f},f}\chi^k_{\bar{f},\bar{f}}\rho\chi^{\dagger k}_{\bar{f},\bar{f}}\chi^\dagger_{\bar{f},f} + \chi^n_{\bar{f},\bar{f}}\rho\chi^{\dagger n}_{\bar{f},\bar{f}})P_f|T\rangle) = \\
&Tr(\langle T|P_f\rho P_f|T\rangle) + \textstyle\sum_{k=0}^{n-1} Tr\left(\langle T|\chi_{\bar{f},f}\chi^k_{\bar{f},\bar{f}}\rho\chi^{\dagger k}_{\bar{f},\bar{f}}\chi^\dagger_{\bar{f},f}|T\rangle\right)
\end{aligned}$$

Ozawa has proved in [11], that for any $\varphi \in \mathbb{C}^{Q\times\Sigma^*\times\mathbb{Z}}$, any $T \in \Sigma^*$, and any $n \in \mathbb{N}$,

$$||\langle T|P_f U^n_M\varphi||^2 = \sum_{k=0}^{n} ||\langle T|P_f(U_M P_{\bar{f}})^k\varphi||^2$$

where $||\varphi|| = \sqrt{\varphi^\dagger\varphi}$

Thus, for any $\varphi \in \mathbb{C}^{Q\times\Sigma^*\times\mathbb{Z}}$,

$$\begin{aligned}
p_{halt,T}\left(F^n_M(\varphi\varphi^\dagger)\right) &= Tr(\langle T|P_f U^n_M \varphi\varphi^\dagger U^{\dagger n}_M P_f|T\rangle)\\
&= ||\langle T|P_f U^n_M \varphi||^2\\
&= \textstyle\sum_{k=0}^n ||\langle T|P_f (U_M P_{\bar f})^k \varphi||^2\\
&= ||\langle T|P_f\varphi||^2 +\\
&\quad \textstyle\sum_{k=0}^n ||\langle T|P_f U_M P_{\bar f}(P_{\bar f} U_M P_{\bar f})^k\varphi||^2\\
&= ||\langle T|P_f\varphi||^2 + \textstyle\sum_{k=0}^n ||\langle T|\chi_{\bar f,f}(\chi_{\bar f,\bar f})^k\varphi||^2\\
&= Tr(\langle T|P_f\varphi\varphi^\dagger P_f|T\rangle)+\\
&\quad \textstyle\sum_{k=0}^{n-1} Tr\left(\langle T|\chi_{\bar f,f}\chi^k_{\bar f,\bar f}\varphi\varphi^\dagger \chi^{\dagger k}_{\bar f,\bar f}\chi^\dagger_{\bar f,f}|T\rangle\right)\\
&= p_{halt,T}\left(F^n_{[M]_H}(\varphi\varphi^\dagger)\right)
\end{aligned}$$

Finally, for any $\rho \in \mathcal{D}(Q\times\Sigma^*\times\mathbb{Z})$, there exist a collection of $a_i > 0$ and a collection of $\varphi_i \in \mathbb{C}^{Q\times\Sigma^*\times\mathbb{Z}}$ such that $\rho = \sum_i a_i\varphi_i\varphi_i^\dagger$. So, by linearity, $p_{halt,T}\left(F^n_M(\rho)\right) = p_{halt,T}\left(F^n_{[M]_H}(\rho)\right)$. Thus, M and $[M]_H$ are equivalent. □

6.3 Classical Turing machines

In this section, we show 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 6 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 $[\tilde M]_K$, where a total measurement of the internal states and the cell pointed out by the head is performed, is well-observed:

Lemma 6. *For any* DTM $M = (Q,\Sigma,\delta)$, $[\tilde M]_{\{K_{\tau,p}\}_{(\tau,p)\in\Sigma\times Q}}$ *is well-observed, where* $\tilde M = (Q,\Sigma,\tilde\delta)$ *is a* pQTM *such that* $\forall(p,\tau)\in Q\times\Sigma, \tilde\delta(p,\tau) = |\delta(p,\tau)\rangle$ *and* $K_{\tau,p} = \{(p,T,x)\in Q\times\Sigma^*\times\mathbb{Z}$ *s.t.* $T_x = \tau\}$ *. Moreover,* M *and* $[\tilde M]_{\{\{a\},a\in\Sigma\times Q\}}$ *have the same evolution: for any* $c\in Q\times\Sigma^*\times\mathbb{Z}$*,*

$$F_{[\tilde M]_{\{K_{\tau,p}\}_{(\tau,p)\in\Sigma\times Q}}}(\,|c\rangle\langle c|\,) = |M(c)\rangle\langle M(c)|$$

Proof. For any $(\tau,p),(\sigma,q)\in\Sigma\times Q$, if there is no $d\in\{-1,0,1\}$ such that $\delta(p,\tau) = (\sigma,q,d)$, then $\chi_{(\tau,p),(\sigma,q)} = 0$. Otherwise $\chi_{(\tau,p),(\sigma,q)} = \sum_{x\in\mathbb{Z},T\in\Sigma^*\text{ s.t. }T_x=\tau} |q,T^\sigma_x,x+d\rangle\,\langle p,T,x|$ and,

$$\chi^{\dagger}_{(\tau,p),(\sigma,q)}\chi_{(\tau,p),(\sigma,q)} =$$
$$\sum_{x,x'\in\mathbb{Z},T,T'\in\Sigma^* \text{ s.t. } T'_{x'}=T_x=\tau} |p,T',x'\rangle\langle q,T'^{\tau}_{x'},x'+d||q,T^{\tau}_{x},x+d\rangle\langle p,T,x| =$$
$$\sum_{x\in\mathbb{Z},T,T'\in\Sigma^* \text{ s.t. } T'_{x}=T_x=\tau} |p,T',x\rangle\langle q,T'^{\tau}_{x},x+d||q,T^{\tau}_{x},x+d\rangle\langle p,T,x| =$$
$$\sum_{x\in\mathbb{Z},T\in\Sigma^* \text{ s.t. } T_x=\tau} |p,T,x\rangle\langle p,T,x|$$

Thus,

$$\begin{aligned}\sum_{(\tau,p),(\sigma,q)\in\Sigma\times Q}\chi^{\dagger}_{(\tau,p),(\sigma,q)}\chi_{(\tau,p),(\sigma,q)} &= \sum_{(\tau,p)\in\Sigma\times Q,x\in\mathbb{Z},T\in\Sigma^* \text{ s.t. } T_x=\tau}|p,T,x\rangle\langle p,T,x| \\ &= \sum_{p\in Q,x\in\mathbb{Z},T\in\Sigma^*}|p,T,x\rangle\langle p,T,x| \\ &= I\end{aligned}$$

Moreover, for any $(p,T,x)\in Q\times\Sigma^*\times\mathbb{Z}$,

$$\begin{aligned} & F_{[\tilde{M}]_{\{K_\tau,p\}}(\tau,p)\in\Sigma\times Q}(\,|p,T,x\rangle\langle p,T,x|\,) \\ = \;& \textstyle\sum_{(\sigma,q)\in\Sigma\times Q}\chi_{(p,T_x),(\sigma,q)}\,|p,T,x\rangle\langle p,T,x|\,\chi^{\dagger}_{(p,T_x),(\sigma,q)} \\ = \;& |q,T^{\sigma},x+d\rangle\langle q,T^{\sigma},x+d| \qquad \text{where } \delta(p,\tau)=(\sigma,q,d) \\ = \;& |M(p,T,x)\rangle\langle M(p,T,x)|\end{aligned}$$

□

Probabilistic Turing machines are also special instances of OQTMs. A probabilistic Turing machine is a triple $M=(Q,\Sigma,\delta)$, with $\delta: Q\times\Sigma\times Q\times\Sigma\times\{-1,0,1\}\to\tilde{\mathbb{R}}^{+}$, 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 ν in the ℓ^2 space $\mathbb{R}^{+Q\times\Sigma^*\times\mathbb{Z}}$. The evolution operator F_M of a PTM M is such that for any configuration ν,

$$F_M(\nu)=(q,T,y)\mapsto \sum_{(p,\tau)\in Q\times\Sigma,d\in\{-1,0,1\}}\delta(p,\tau,q,T_{y-d},d)\nu(p,T^{\tau}_{y-d},y-d)$$

Lemma 7. *For any probabilistic Turing machine $M=(\Sigma,Q,\delta)$, the OQTM $[M']_{\{\{c\}\}_{c\in Q\times\Sigma\times\mathbb{Z}}}$ is well observed, and has the same evolution as M, where $M'=(\Sigma,Q,\sqrt{\delta})$.*

Proof. For any $(p,T,x)\in Q\times\Sigma^*\times\mathbb{Z}$, let $M^{(p,T,x)}=(Q,\Sigma,\delta^{(p,T,x)}=(T_x,p)\mapsto\sqrt{\delta(T_x,p)})$ be a pQTM such that its partial transition function

is defined on a unique point (T_x, p). For any $c \in Q \times \Sigma^* \times \mathbb{Z}$, M^c is a partially well formed QTM, thus according to lemma 2, $[M]_{\{\{c\}\}_{c\in Q\times\Sigma^*\times\mathbb{Z}}}$ is well observed.

Moreover, $F_M = \Phi \circ F_{[M']_{\{\{c\}\}_{c\in Q\times\Sigma^*\times\mathbb{Z}}}} \circ \Psi$, where Φ and Ψ are two maps transforming a probability distribution represented by a valuation into its density matrix representation and vice-versa : $\Psi : (\nu)\mathbb{R}^{+A} \to \mathcal{D}(A) :: \nu \mapsto \sum_{c\in A} \nu(c)\,|c\rangle\langle c|$ and $\Phi : \mathcal{D}(A) \to \mathbb{R}^{+A} :: \rho \mapsto (c \mapsto \langle c|\rho|c\rangle)$. □

As a consequence, the model of observable 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.

7 COMPUTATIONAL POWER OF OBSERVABLE QUANTUM TURING MACHINES

7.1 Solving undecidable problems

In this section we show that the model of observed QTM, as defined in definition 8 is over powerful since it allows to solve with high probability and in constant time the halting problem.

The halting problem consists in deciding whether a given deterministic Turing machine M accepts a given input u. More formaly, the input of the problem is composed of two words, one is the encoding w_M of a deterministic Turing machine M and the second is an input u. The ouput of the problem is *yes* if and only if $M(u)$ is halting.

The halting problem is known to be undecidable, however we show that there is an OQTM for deciding this problem:

Theorem 1. *There is a well-observed OQTM $[M_h]_K$ for deciding (with high probability), for any DTM M and any input u, whether M halts on input u.*

The proof is based on a bipartition K of the machines depending whether they are halting or not.

Proof. For a given finite alphabet Σ, let $M_h = (\{q_0, q_1, q_2, q_h, q_{\bar{h}}\}, \Sigma, \delta_h)$ be a QTM, s.t. q_h and $q_{\bar{h}}$ are the halting states and for any $\sigma \in \Sigma$

$$\begin{aligned}
\delta_h(q_0, \sigma, q_1, \sigma, 0) &= 1/\sqrt{2} \\
\delta_h(q_0, \sigma, q_2, \sigma, 0) &= 1/\sqrt{2} \\
\delta_h(q_1, \sigma, q_h, \sigma, 0) &= 1/\sqrt{2} \\
\delta_h(q_1, \sigma, q_{\bar{h}}, \sigma, 0) &= 1/\sqrt{2} \\
\delta_h(q_2, \sigma, q_h, \sigma, 0) &= 1/\sqrt{2} \\
\delta_h(q_2, \sigma, q_{\bar{h}}, \sigma, 0) &= -1/\sqrt{2}
\end{aligned}$$

M_h is well-formed and for any $(T, x) \in \Sigma^* \times \mathbb{Z}$. Since the head does not move during the computation, the position of the head is omitted in the description of the configuration of the machine. If the initial configuration is (q_0, T), after one transition the configuration is:

$$\begin{aligned} F_{M_h}(\,|q_0,T\rangle\langle q_0,T|\,) &= \tfrac{1}{2}(\,|q_1,T\rangle\langle q_1,T| + |q_1,T\rangle\langle q_2,T| \\ &\quad + |q_2,T\rangle\langle q_1,T| + |q_2,T\rangle\langle q_2,T|\,) \end{aligned}$$

After two steps, the configuration is $F^2_{M_h}(\,|q_0,T\rangle\langle q_0,T|\,) = |q_h,T\rangle\langle q_h,T|$ which is a halting state. Thus M_h is halting after two steps if the initial configuration is $|q_0,T\rangle\langle q_0,T|$.

Given an encoding of deterministic Turing machine, such that the encoding of a DTM M together with its input u is denoted $w_{M,u} \in \Sigma^*$, let $K_{\bar{h}} = \{(q_1, w_{M,u}) \in Q \times \Sigma^* \text{ s.t. } M \text{ does not halt on } u\} \cup \{(q_{\bar{h}}, T) \mid T \in \Sigma^*\}$ and $K_h = (Q \times \Sigma^*) \setminus K_{\bar{h}}$.

Since M_h is well-formed, $[M_h]_{\{K_h,K_{\bar{h}}\}}$ is well-observed.

- If $M(u)$ halts then for any $q \in Q$, $(q, w_{M,u}) \in K_h$, thus $[M_h]_{\{K_h,K_{\bar{h}}\}}$ has the same evolution as M_h since the intermediate configurations of the machine are all in the eigenspace of the projector associated with K_h, thus the halting state $\left|q_h, w_{M,u}\right\rangle\left\langle q_h, w_{M,u}\right|$ is reached within two steps, meaning that $[M_h]_{\{K_h,K_{\bar{h}}\}}$ answers *M(u) halts'* with probability 1.
- If $M(u)$ does not halt then the intermediate measurements break the superposition state of the configuration, and the final configuration reached by $[M_h]_{\{K_h,K_{\bar{h}}\}}$ after two transitions is $\frac{1}{2}\left|q_h, w_{M,u}\right\rangle\left\langle q_h, w_{M,u}\right| + \frac{1}{2}\left|q_{\bar{h}}, w_{M,u}\right\rangle\left\langle q_{\bar{h}}, w_{M,u}\right|$, meaning that $[M_h]_{\{K_h,K_{\bar{h}}\}}$ answers *'M(u) halts'* with probability $1/2$ and *'M(u) does not halt'* with probability $1/2$.

By repeating n times the application of $[M_h]_{\{K_h,K_{\bar{h}}\}}$ on $(q_0, w_{M,u})$, it leads to a one-side error algorithm for deciding whether M accepts u which fails with probability $1/2^n$. □

The model of OQTM is over-powerful. This extra power comes from the environment which is able to perform unrealistic measurement like in the proof of theorem 1. In order to turn the OQTM model into a realistic model some restrictions on the power of the environment have to be made.

For instance, instead of acting on all the configurations of the machine, we can constrain the environment to perform measurements on the control part, i.e. the internal state and the position of the head. This assumption correspond to the well developed paradigm in quantum computing: *quantum data, classical control*, which is used in most of the quantum programming languages [6, 18] for instance, and which is also the basis of the measurement based quantum computation.

However, we prove in the following theorem that even if the environment is constrained to perform measurements on the control part of the machine ($Q \times \mathbb{Z}$) only then the machine is still over-powerful:

Theorem 2. *There is a well-observed OQTM* $[M_h]_{K \times \Sigma^*}$*, where K is a partition of* $Q \times \mathbb{Z}$*, for deciding (with high probability), for any DTM M and any input u, whether M halts on input u.*

Proof. The proof is similar to the proof of theorem 1, but based on a unary encoding of Turing machines, such that if the head is on the last cell of the encoded machine, the position of the head characterised the machine encoded on the tape. More precisely, we consider the QTM $M_h = (\{q_0, q_1, q_2, q_h, q_{\bar{h}}\}, \{0,1\}, \delta_h)$ such that:

$$\begin{array}{rcl}
\delta_h(q_0,1,q_0,1,1) & = & 1 \\
\delta_h(q_0,0,q_1,0,0) & = & 1/\sqrt{2} \\
\delta_h(q_0,0,q_2,0,0) & = & 1/\sqrt{2} \\
\delta_h(q_1,\sigma,q_h,\sigma,0) & = & 1/\sqrt{2} \\
\delta_h(q_1,\sigma,q_{\bar{h}},\sigma,0) & = & 1/\sqrt{2} \\
\delta_h(q_2,\sigma,q_h,\sigma,0) & = & 1/\sqrt{2} \\
\delta_h(q_2,\sigma,q_{\bar{h}},\sigma,0) & = & -1/\sqrt{2}
\end{array}$$

M_h is a well-formed QTM. Moreover, let $w_{M,u} \in \{1\}^*$ be a unary encoding of a DTM M and its input u. Let $K_{\bar{h}} = \{(q_1, x) \in Q \times \mathbb{Z} \text{ s.t. } |w_{M,u}| = x \text{ and } M \text{ does not accept } u\} \cup \{(q_{\bar{h}}, x) \mid x \in \mathbb{Z}\}$ and $K_h = (Q \times \mathbb{Z}) \setminus K_{\bar{h}}$.

Let $(q_0, w_{M,u}0, 0)$ be the initial configuration. If M accepts u then the final configuration is $\left|q_h, w_{M,u}0, |w_{M,u}|\right\rangle\left\langle q_h, w_{M,u}0, |w_{M,u}|\right|$ whereas if M does not accept u then the final configuration is $\frac{1}{2}|q_h, w_{M,u}0, |w_{M,u}|\rangle\langle q_h, w_{M,u}0, |w_{M,u}|| + \frac{1}{2}\left|q_{\bar{h}}, w_{M,u}0, |w_{M,u}|\right\rangle\left\langle q_{\bar{h}}, w_{M,u}0, |w_{M,u}|\right|$, leading to a one-side error algorithm for deciding with high probability whether M is halting on u. □

7.2 Towards observable quantum Turing machines

In order to avoid the extra power of the environment in the OQTM model, we restrict the environment to perform observation of the classical control (excluding the position of the head) only i.e., the internal state of the machine and the symbol of the cell pointed out by the head. As a consequence, we consider only partitions K of $Q \times \Sigma^* \times \mathbb{Z}$ such that for any region $K_\lambda \in K$, $\exists(\tau, p) \in \Sigma \times Q$ s.t. $K_\lambda \supseteq \{(p, T, x) \mid T_x = \tau\}$. In the following, such partition are equivalently represented as partitions of $\Sigma \times Q$.

Definition 10. $[M]_K$ *is a restricted* OQTM *(*OQTM_r*) if* $M = (Q, \Sigma, \delta)$ *is a* pQTM *and K is a partition of* $\Sigma \times Q$*. The evolution of* $[M]_K$ *is the same*

as the evolution of the OQTM $[M]_{K'}$, *where* $K' = \{(p, T, x) \in Q \times \Sigma^* \times \mathbb{Z} \mid (T_x, p) \in K\}$.

Notice that OQTM_r can be seen as subclass of generalized quantum Turing machines defined in [7].

In this section, we mainly show that any such restriction of observable quantum Turing machine can be simulated within a polynomial slowdown by a quantum Turing machine.

Theorem 3. *For any* $\mathrm{OQTM}_r [M]_K$, *there exists a* QTM M' *which simulates* $[M]_K$ *within a quadratic slowdown.*

Proof. In order to simulate the *OQTM*$_r$ $[M]_K$ a two-tape QTM $\tilde{M}$ is used. Multi-tape quantum Turing machines have been introduced in [20]. 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. The proof proceeds as follows: first, a such two-tape quantum Turing machine is defined and we prove the well-formedness 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 is 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 $\Sigma' = \Lambda^2 \cup \{\#\}$. The transition function $\tilde{\delta} : Q \times \Sigma \times \Sigma' \to \tilde{\mathbb{C}}^{Q \times \Sigma \times \{-1,0,1\} \times \Sigma' \times \{-1,0,1\}}$ of $\tilde{M}$ is partially 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 to the right, revealing necessary a blank symbol #. That is why the transition function is partially defined. $\tilde{\delta}$ verifies the well formedness conditions (see lemma 1 in [20] for multi-tape QTM well-formedness.) Thus according to the completion lemma (lemma 2 in [20]) $\tilde{\delta}$ can be extended such that the corresponding pQTM is well-formed.

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

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

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 $\rho \in \mathcal{D}(Q\times\Sigma\times\mathbb{Z})$ 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 $U_{\tilde{M}}^n(\rho\otimes|\#\rangle\langle\#|\otimes|0\rangle\langle 0|)U_{\tilde{M}}^{\dagger n}$. 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 $n-1$. If the computation is terminated, these non-blank cells of the second tape are then measured, leading to the configuration $\sum_{w\in(\Lambda^2)^n} P_w U_{\tilde{M}}^n(\rho\otimes|\#\rangle\langle\#|\otimes|0\rangle\langle 0|)U_{\tilde{M}}^{\dagger n}P_w$ where $P_w = |w\rangle\langle w|$. We prove, by induction on n, that this resulting configuration is equal to $F_{[M]_K}^n(\rho)\otimes|\#\rangle\langle\#|\otimes|n\rangle\langle n|$. 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

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

where $P_{\lambda,\mu}^{(n)}$ means that $P_{\lambda,\mu}$ is applied on the cell indexed by n on the second tape.

Since the second head always moves to the 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:

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

By induction,

$$\rho' = \sum_{\lambda,\mu\in\Lambda} P_{\lambda,\mu}^{(n+1)}U_{\tilde{M}}(F_{[M]_K}^n(\rho)\otimes|\#\rangle\langle\#|\otimes|n\rangle\langle n|)U_{\tilde{M}}^\dagger P_{\lambda,\mu}^{(n+1)}$$

Moreover, for any $p\in Q$, any $T\in\Sigma^*$, and any $x\in\mathbb{Z}$,

$$P_{\lambda,\mu}^{(n+1)}U_{\tilde{M}}^{n+1}|p,T,x,\#,n\rangle = (\chi_{\lambda,\mu}|p,T,x\rangle)\otimes|\#,n+1\rangle$$

Thus,

$$\rho' = F^{n+1}_{[M]_K}(\rho) \otimes \hat{\mathrm{E}}|\#\rangle\langle\#| \otimes |n+1\rangle\langle n+1|$$

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 [20], M is simulated by a one-tape QTM within a quadratic slowdown. □

7.3 Well-observation and completion lemmas for OQTM$_r$

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

Lemma 8 (Well-observation lemma). *For a given* pQTM $M = (\Sigma, Q, \delta)$ *and a given* $K = \{K_\lambda, \lambda \in \Lambda\}$ *a partition of* $\Sigma \times Q$, $[M]_K$ *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 lemma 4, $[M]_K$ is well-observed iff for every $\lambda \in \Lambda$, $M^\lambda = (Q, \Sigma, \delta^\lambda)$ is partially well formed, where δ^λ is restriction of δ to $S_\lambda = K_\lambda$. For each $\lambda \in \Lambda$, 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 lemma 1), 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 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 8, then $[M]_K$ is called a partially well-observed pQTM.

Lemma 9 (Completion lemma). *Given a partially well-observed pQTM* $[M]_K$ *with a partial quantum transition* δ*, there exists an* OQTM_r $[\tilde{M}]_K$ *with the same alphabet, the same set of states, and a transition function* $\tilde{\delta}$ *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 8, M^λ is a well-formed partial QTM, thus M^λ can be expanded to a well-formed QTM $\tilde{M}^\lambda$. Let $\tilde{\delta}^\lambda$ be the transition function of $\tilde{M}^\lambda$. Finally, let $\tilde{\delta}$ be such that for any $(p, \tau) \in Q \times \Sigma$, $\tilde{\delta}(p, \tau) = \tilde{\delta}^\lambda(p, \tau)$ if $(\tau, p) \in K_\lambda$. Since each $\tilde{\delta}^\lambda$ satisfies the conditions of lemma 1, $\tilde{\delta}$ satisfies the conditions of lemma 8. Moreover, $\tilde{\delta}$ extends δ, so $\tilde{M} = (Q, \Sigma, \tilde{\delta})$ is an OQTM_r.

□

8 UNIVERSALITY

The existence of a universal quantum Turing machine is one of the main open questions in quantum computing. So far, only approximated universal machines have been introduced for subclasses of quantum Turing machines which satisfy specific halting conditions [1, 8]. The usual approach to tackle this problem is to consider subclasses of QTM and find a universal model for this subfamily. Observable quantum Turing machines offer a new perspective in the quest of finding a universal quantum machine, by extending the model instead. This extension allows the representation of the classical control which has been pointed out as the potential missing capability for a QTM to be universal [5, 8]. The existence of a universal observable quantum Turing machine is an open question and we leave this question to further investigations. But some remarks can already be made on the existence of a universal observable quantum Turing machine:

- The existence of a universal observable quantum Turing machine $[M]_K$ without restriction on the environment power (i.e., K can be any partition of the configurations) is an open question, but the fact that this model is over-powerful implies that even if such a universal machine exists for this class of machines, this machine is not what is expected for a universal quantum machine.

- Since any restricted OQTM can be efficiently simulated by a QTM, the existence of a universal restricted OQTM implies the existence of a universal QTM and vice-versa.
- A third way can be explored, which consists in a subclass – if it exists – of OQTM where the allowed measurements are more general than the restricted version, but sufficiently constrained to guaranty that no undecidable problems can be solved. The existence of a universal machine for such a class can be expected, as well as the ability to *approximate* any machine in this class by a QTM.

9 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 or probabilistic TM are special instances of OQTM.

We have shown that the OQTMs are over-powerful, solving the undecidable halting problem. But a restricted version of OQTM, where observations are limited to the control of the machine (internal state and cell pointed out by the head) has the same computational power as the QTMs. 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 [9, 13, 15], One-way model [17, 2, 3]) and the formal framework of classically-controlled quantum Turing machines [16].

Indeed, the structure of an 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 head, 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 by 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, 8] 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. (1997). Quantum complexity theory. *SIAM J. Comput.*, 26:1411–1478.

[2] V. Danos, E. Kashefi, and P. Panangaden. (2007). The measurement calculus. *J. ACM*, 54(2).

[3] V. Danos, E. Kashefi, P. Panangaden, and S. Perdrix. (2010). Extended measurement calculus. *Chapter of Semantic Techniques in Quantum Computation*, Cambridge University Press.

[4] D. Deutsch. (1985). Quantum theory, the Church-Turing principle and the universal quantum computer. *Proc. R. Soc. Lond. A*, 400:97–117.

[5] W. Fouché, J. Heidema, G. Jones, and P. Potgieter. (2008). Universality and programmability of quantum computers. *Theor. Comput. Sci.*, 403(1):121–129.

[6] S. J. Gay. (2006). Quantum programming languages: Survey and bibliography. *Mathematical Structures in Computer Science*, 16(4).

[7] S. Iriyama, M. Ohya, and I. Volovich, (2004). Generalized quantum Turing machine and its application to the sat chaos algorithm. arXiv quant-ph/0405191.

[8] M. Mueller. (2008). Strongly universal quantum Turing machines and invariance of kolmogorov complexity. *IEEE Transactions on Information Theory*, 54(2):763–780.

[9] M. A. Nielsen. (2003). Universal quantum computation using only projective measurement, quantum memory, and preparation of the 0 state. *Phys. Rev. A*, 308:96–100.

[10] M. A. Nielsen and I. L. Chuang. (2000). *Quantum computation and quantum information*. Cambridge University Press, New York, NY, USA.

[11] M. Ozawa. (2002). Halting of quantum Turing machines. In *UMC*, pages 58–65.

[12] M. Ozawa and H. Nishimura. (2000). Local transition functions of quantum Turing machines. *Theoretical Informatics and Applications*, 34(5):379–402.

[13] S. Perdrix. (2005). State transfer instead of teleportation in measurement-based quantum computation. *International Journal of Quantum Information*, 3(1):219–223.

[14] S. Perdrix. (2006). Formal models of quantum computing: resources, abstract machines and measurement-based quantum computing. *PhD Thesis, INPG, University of Grenoble.*

[15] S. Perdrix. (2007). Towards minimal resources of measurement-based quantum computation. *New J. Phys.*, 9 206.

[16] S. Perdrix and Ph. Jorrand. (2006). Classically-controlled quantum computation. *Math. Struct. in Comp. Science*, 16:601–620.

[17] R. Raussendorf, D. E. Browne, and H. J. Briegel. (2002). The one-way quantum computer - a non-network model of quantum computation. *Journal of Modern Optics*, 49:1299.

[18] P. Selinger. (2004). A brief survey of quantum programming languages. In *Proceedings of the 7th International Symposium on Functional and Logic Programming*, volume 2998 of *Lecture Notes in Computer Science*, pages 1–6. Springer.

[19] A. Turing. (1936). On computable numbers with an application to the entscheidungsproblem. In *Proceedings of the London Mathematical Society*, volume 42.

[20] T. Yamakami. (1999). 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. Springer-Verlag.