Temporal logics for reasoning about quantum systems

P. Mateus, J. Ramos, A. Sernadas, and C. Sernadas

SQIG-Instituto de Telecomunicações, IST - TULisbon,
Av. Rovisco Pais, 1049-001, Lisbon, Portugal

January 6, 2009

Abstract

Reasoning about quantum systems has gained prominence due to a big potential in applications such as information processing, security, distributed systems and randomized algorithms. This fact has attracted research in formal reasoning about quantum states, programs and processes. On the other hand, temporal logics have proved to be successful in the verification of classical distributed systems and security protocols. In this chapter we extend Exogenous Quantum Propositional Logic with temporal modalities, considering both linear and branching time. We provide a weakly complete Hilbert calculi for the proposed quantum temporal logics and study their SAT and model-checking problems.

Contents

1 Introduction

Reasoning about quantum systems has gained prominence due to their potential applications in information processing, security, distributed systems and randomized algorithms. This has attracted research in formal reasoning about quantum states [28, 27, 20, 12, 8] and quantum programs [19, 24, 1, 16, 2, 25, 3, 5, 11, 10, 4]. On the other hand, formal methods have proved to be successful in design and verification of classical distributed systems and security protocols, e.g, [14, 22]. Herein, we present branching and linear temporal logics for reasoning about evolution of quantum systems composed of a fixed finite set of qubits.

Our starting point is the logic dEQPL for reasoning about quantum states presented in [20, 12]. The logic dEQPL is an exogenous logic [21] and designed around the first two postulates of quantum mechanics. The first postulate says that a quantum state is a unit vector in a complex Hilbert space and the second one says that the quantum state composed of two independent quantum states is the tensor product of the composing states. Herein, we consider just a restricted sub-logic of dEQPL based on the first postulate. The models of this logic are basically the quantum states of the finite qubit system. This simplification was initially proposed in [4].

We present a sound and complete axiomatization of this state logic. The completeness proof, which is inspired by [12, 17], suggests a decision procedure for the SAT problem and we compute the complexity of the decision procedure assuming that all basic integer operations (addition, subtraction, multiplication and comparison) take unit time. Furthermore, assuming a floating point representation of complex numbers and assuming that basic floating point operations take unit time, we compute the complexity of the model-checking algorithm.

Next, we present quantum computational tree logic QCTL by replacing the state formulas in the standard computational tree logic CTL [13] by dEQPL formulas. The standard CTL is interpreted over classical states and transition relations amongst these states. QCTL is interpreted over quantum states and transition relations. We give a sound and complete axiomatization of QCTL capitalizing on the complete axiomatization of dEQPL and CTL. The proof of completeness follows the techniques introduced in [9, 6]. We combine the standard CTL SAT and model-checking algorithm with those from dEQPL to obtain a SAT and a model-checking algorithm for QCTL. Some of the results in this section where presented in [4].

Finally, we replicate the effort of obtaining a complete proof system, a SAT and a model-checking algorithm to quantum linear temporal logic (QLTL).

2 Exogenous Quantum Propositional Logic

We discuss here briefly the restricted state logic, dEQPLas introduced in [4]. The logic is designed around the first postulate of quantum mechanics which states that each quantum system is a unit vector in a complex Hilbert space. For our purposes, we shall only deal with a finite-dimensional Hilbert space composed of a finite set of qubits. We shall thus assume a fixed finite set of qubit symbols, qB, which will represent these qubits.

A quantum state $|\psi\rangle$ therefore is a unit vector in $\mathcal{H}_{\mathsf{qB}} = \mathcal{H}(2^{\mathsf{qB}})$, the Hilbert space generated by the set of valuations 2^{qB}. Please note that these valuations constitute what is commonly called the standard computational basis. Assuming that qB has n elements, the vector $|\psi\rangle$ is then specified by 2^n complex numbers $\{\langle v|\psi\rangle \mid v \subseteq \mathsf{qB}\}$. The complex number $\langle v|\psi\rangle$ gives the projection of the unit vector $|\psi\rangle$ on the basis vectors $|v\rangle$. We shall have terms in our language representing the real and complex parts of these 2^n complex numbers. Furthermore, please also note that there is a natural bijection between the subsets of qB and the set of valuations over qB: a set A corresponds to a valuation v_A which valuates to true if $\mathsf{qb} \in A$ and valuates to false if $\mathsf{qb} \notin A$.

We shall also have terms in our logic that will represent the probability of outcomes if all the qubits in qB were to be measured in the standard computational basis. We are now ready to discuss the syntax and semantics of dEQPL.

2.1 Language and semantics

Syntax. The terms in dEQPL denote elements from $\mathbb{R}$, the set of real numbers. The formulas of dEQPL henceforth called *quantum formulas*, are constructed from *comparison formulas* (formulas that compare terms) using propositional connectives. We present language of dEQPL in Table 1 using an abstract version of BNF notation [23] for a compact presentation of inductive definitions and discuss the language in detail below.

The first syntactic category is that of *classical formulas.* Please recall that we fixed a finite set of qubit symbols qB. Classical formulas are built from qubit symbols in qB using the classical disjunctive connectives, falsum $\perp$ and implication $\Rightarrow$. As usual, other classical connectives like $\neg, \wedge, \vee, \Leftrightarrow$ and $\top$ are introduced as abbreviations.

For the term language, we pick a denumerable sets of variables $X = \{x_k : k \in \mathbb{N}\}$ interpreted over reals. We also have a copy of integers in the set of terms. The terms $\mathrm{Re}(|\top\rangle_A)$ and $\mathrm{Im}(|\top\rangle_A)$ denote the real and complex parts of the logical amplitude $\langle v_A|\psi\rangle$, where ψ is a quantum state over qB and v_A is

Table 1: Language dEQPL

Classical formulas

$$\alpha \quad := \quad \bot \;[\!]\; \mathsf{qb} \;[\!]\; (\alpha \Rightarrow \alpha)$$

Term language (with the proviso $m \in \mathbb{Z}$ and $A \subseteq \mathsf{qB}$)

$$t \quad := \quad x \;[\!]\; m \;[\!]\; (t + t) \;[\!]\; (t\,t) \;[\!]\; \mathrm{Re}(|\top\rangle_A) \;[\!]\; \mathrm{Im}(|\top\rangle_A) \;[\!]\; (\textstyle\int \alpha)$$

Quantum formulas

$$\gamma \quad := \quad (t \leq t) \;[\!]\; \perp\!\!\!\perp \;[\!]\, (\gamma \sqsupset \gamma)$$

the (unique) valuation corresponding to the set A. The *probability term* $(\int \alpha)$ denotes the probability that the classical formula α holds for an outcome of measuring all the qubits (in qB) in the standard basis.

As usual, we may define the notion of occurrence of a term t_1 in a term t, and the notion of replacing zero or more occurrences of terms t_1 in t by t_2. If $\vec{x}$ and $\vec{t}$ are sequences of variables and terms respectively, we will write $t\{\!|\vec{x}/\vec{t}|\!\}$ to mean the real term obtained by substituting *all* occurrences of x_i by t_i.

The quantum formulas are built from *comparison formulas* $(t \leq t)$ using the connectives $\perp\!\!\!\perp$ and $\sqsupset$. The set of comparison formulas shall henceforth be called qAtom and we shall use δ, δ' to range over this set. Please note that quantum bottom $\perp\!\!\!\perp$ and quantum implication $\sqsupset$ should not be confused with their classical counterparts. For clarity sake, we shall often drop parenthesis in formulas and terms if it does not lead to ambiguity.

Semantics. The language is interpreted over a unit vector $|\psi\rangle$ on the Hilbert space $\mathcal{H}_{\mathsf{qB}}$ spanned by all valuations over qB. For interpreting the variables, we also need the concept of an assignment. An *assignment* ρ is a map from X, the set of variables, to the real numbers $\mathbb{R}$. Given a classical formula α and a valuation v over qB, we shall also assume the definition of satisfaction of α by v; and write $v \Vdash_c \alpha$ if v satisfies α. For interpreting the probability terms $(\int \alpha)$, we shall use the *probability map* $\mu_{|\psi\rangle} : \wp(\mathsf{qB}) \to \mathbb{R}$ defined as:

$$\mu_{|\psi\rangle}(U) = \sum_{v \in U} \; ||\langle v|\psi\rangle||^2 \,.$$

For the probability terms, we shall also need the *extent* of classical formulas defined as:

$$|\alpha| = \{v \in \wp(\mathsf{qB}) : v \Vdash_c \alpha\}.$$

The terms $\mathrm{Re}(|\top\rangle_A)$ and $\mathrm{Im}(|\top\rangle_A)$ are interpreted as the real and complex parts of the logical amplitude $\langle v_A|\psi\rangle$ where v_A is the valuation corresponding to the set A. Given a quantum state ψ and an assignment ρ, the *denotation of terms*

Table 2: Semantics of dEQPL

Denotation of terms

$$\begin{array}{lcl}
[\![x]\!]_{|\psi\rangle\rho} & = & \rho(x) \\
[\![(\int\alpha)]\!]_{|\psi\rangle\rho} & = & \mu_{|\psi\rangle}(|\alpha|) \\
[\![\mathrm{Re}(|\top\rangle_A)]\!]_{|\psi\rangle\rho} & = & \mathrm{Re}(\langle v_A|\psi\rangle) \\
[\![\mathrm{Im}(|\top\rangle_A)]\!]_{|\psi\rangle\rho} & = & \mathrm{Im}(\langle v_A|\psi\rangle)
\end{array}$$

Satisfaction of quantum formulas

$$\begin{array}{lcl}
|\psi\rangle\rho \Vdash_{\mathsf{dEQPL}} (t_1 \leq t_2) & \text{iff} & [\![t_1]\!]_{|\psi\rangle\rho} \leq [\![t_2]\!]_{|\psi\rangle\rho} \\
|\psi\rangle\rho \nVdash_{\mathsf{dEQPL}} \perp\!\!\!\perp & & \\
|\psi\rangle\rho \Vdash_{\mathsf{dEQPL}} (\gamma_1 \sqsupset \gamma_2) & \text{iff} & |\psi\rangle\rho \nVdash_{\mathsf{dEQPL}} \gamma_1 \text{ or } |\psi\rangle\rho \Vdash_{\mathsf{dEQPL}} \gamma_2
\end{array}$$

and *satisfaction of quantum formulas* at $|\psi\rangle$ and ρ is inductively defined in Table 2 (omitting the obvious ones).

Please note that the assignment ρ is sufficient to interpret a useful sub-language of our quantum formulas defined as:

$$\begin{array}{lcl}
a & := & x \,[\!]\, m \,[\!]\, (a + a) \,[\!]\, (a\,a) \\
\kappa & := & (a \leq a) \,[\!]\, (\perp\!\!\!\perp) \,[\!]\, (\kappa \sqsupset \kappa)
\end{array}$$

Henceforth, the terms of this sub-language will be called *analytical terms* and the formulas will be called *analytical formulas.*

Abbreviations. As anticipated, the proposed quantum language with the semantics above is rich enough to express interesting properties of quantum systems. To this end, it is quite useful to introduce other operations, connectives and modalities through abbreviations. We start with some additional quantum connectives:

- quantum negation: $(\boxminus\gamma)$ for $(\gamma\sqsupset \perp\!\!\!\perp)$;
- quantum disjunction: $(\gamma_1 \sqcup \gamma_2)$ for $((\boxminus\gamma_1) \sqsupset \gamma_2)$;
- quantum conjunction: $(\gamma_1 \sqcap \gamma_2)$ for $(\boxminus((\boxminus\gamma_1) \sqcup (\boxminus\gamma_2)))$;
- quantum equivalence: $(\gamma_1 \equiv \gamma_2)$ for $((\gamma_1 \sqsupset \gamma_2) \sqcap (\gamma_2 \sqsupset \gamma_1))$.

It is also useful to introduce some additional comparison formulas:

- $(t_1 < t_2)$ for $((t_1 \leq t_2) \sqcap (\boxminus(t_2 \leq t_1)))$;
- $(t_1 = t_2)$ for $((t_1 \leq t_2) \sqcap (t_2 \leq t_1))$.

Given $A \subseteq \mathsf{qB}$, the following abbreviation will also be useful:

- $(\wedge A)$ for $((\wedge_{\mathsf{qb}_k \in A}\mathsf{qb}_k) \wedge (\wedge_{\mathsf{qb}_k \notin A}(\neg\,\mathsf{qb}_k)))$.

The above formula represents the valuation v_A in the language. The following abbreviation denotes the square of the absolute value of $\langle v_A|\psi\rangle$:

- $||\top\rangle_A|^2$ for $((\mathrm{Re}(|\top\rangle_A))^2 + (\mathrm{Im}(|\top\rangle_A))^2)$;

The following abbreviation is also useful:

- $(\Box\alpha)$ for $(\int\alpha) = 1$.

Intuitively, the formula $(\Box\alpha)$ means that the probability α being true of the outcome of measuring all the qubits in the standard computational basis is 1.

2.2 Axiomatization

We need two new concepts for the axiomatization, one of quantum tautology and a second of valid analytical formulas.

Consider propositional formulas built from a countable set of propositional symbols Q using the classical connectives $\Rightarrow$ and $\bot$. A quantum formula γ is said to be a *quantum tautology* if there is a propositional tautology β over Q and a map σ from Q to the set of quantum formulas such that β_σ coincides with γ where β_σ is the quantum formula obtained from β by replacing all occurrences of $\bot$ by $\perp\!\!\!\perp$, $\Rightarrow$ by $\sqsupset$ and $q \in Q$ by $\sigma(q)$. For instance, the expected formula $((y_1 \sqsupset y_2) \sqsupset (y_1 \sqsupset y_2))$ is tautological (obtained, for example, from the propositional tautology $q \Rightarrow q$).

Please recall that an assignment is enough to interpret analytical formulas. We say that an analytical formula κ is *a valid analytical formula* if it holds for any assignment. It is a well-known fact from the theory of real closed fields [7] that the set of valid analytical formulas so defined is decidable. However, we shall not go into details of this result and will focus our attention on reasoning about quantum aspects only.

The axioms and inference rules of dEQPL are listed in Table 3. The only inference rule is modus ponens for quantum implication **QMP**.

The axiom **QTaut** says that a quantum tautology is an axiom. Since the set of quantum tautologies is recursive, there is no need for spelling out details of tautological reasoning. The axiom **RCF** says that if κ is a valid analytical formula, then any formula obtained by replacing variables with the terms of dEQPL is a tautology. Since the set of valid analytical formulas is recursive, we refrain from spelling out the details. The axiom **Unit** says that a quantum state is a unit vector.

The axioms **CTaut**, **Meas**$\boldsymbol{\emptyset}$, **FAdd** and **Mon** reason about probability terms $(\int\alpha)$. These axioms are basically the axioms (or minor variations of) the axioms of the probability logics in literature [17]. Hence, the probability logics in [17] can be seen as a sub-logic of dEQPL.

Finally, the axiom **Prob** relates probabilities and amplitudes. This axiom says that for any $A \subseteq \mathsf{qB}$, the probability of observing the valuation v_A when all qubits are measured is the square of the amplitude $|\top\rangle_A$.

Table 3: Axioms for dEQPL

Axioms		
[**QTaut**]	$\vdash_{\mathsf{dEQPL}}$	γ for each quantum tautology γ
[**RCF**]	$\vdash_{\mathsf{dEQPL}}$	$\kappa\{\!\!\{\vec{x}/\vec{t}\}\!\!\}$ where κ is a valid analytical formula, $\vec{x}$ and $\vec{t}$ are sequences of variables and terms
[**Unit**]	$\vdash_{\mathsf{dEQPL}}$	$((\sum_{A\subseteq\mathsf{qB}} \lvert\lvert\top\rangle_A\rvert^2) = 1)$
[**CTaut**]	$\vdash_{\mathsf{dEQPL}}$	$(\Box\alpha)$ for each classical tautology α
[**Mes$\emptyset$**]	$\vdash_{\mathsf{dEQPL}}$	$((\int\bot) = 0)$
[**FAdd**]	$\vdash_{\mathsf{dEQPL}}$	$(((\int(\alpha_1\wedge\alpha_2)) = 0)\sqsupset$ $((\int\alpha_1\vee\alpha_2) = (\int\alpha_1) + (\int\alpha_2)))$
[**Mon**]	$\vdash_{\mathsf{dEQPL}}$	$((\Box(\int(\alpha_1\Rightarrow\alpha_2)))\sqsupset((\int\alpha_1)\leq(\int\alpha_2)))$
[**Prob**]	$\vdash_{\mathsf{dEQPL}}$	$((\int\wedge A) = \lvert\lvert\top\rangle_A\rvert^2)$
Inference rules		
[**QMP**]	$\gamma_1, (\gamma_1\sqsupset\gamma_2)\vdash_{\mathsf{dEQPL}}\gamma_2$	

The axiomatization presented above is sound and weakly complete. The proof of weak completeness presented below follows the lines of the proof in [17, 12]. The proof of completeness also suggests an algorithm for deciding whether a formula is theorem of dEQPL or not. The central result in the completeness proof is the Model Existence Lemma, namely, if γ is *consistent* then there is a quantum state ψ and an assignment ρ such that $|\psi\rangle\rho\Vdash_{\mathsf{dEQPL}}\gamma$. A quantum formula γ is said to be consistent if $\nvdash_{\mathsf{dEQPL}} (\boxminus\gamma)$. A quantum formula γ is a theorem if and only if $(\boxminus\gamma)$ is inconsistent.

Theorem 2.1 (Model Existence Theorem) If the quantum formula γ is consistent then there is a unit vector $|\psi\rangle$ and a ρ such that $|\psi\rangle\rho\Vdash_{\mathsf{dEQPL}}\gamma$.

Proof: Given a classical state formula α, we can show using the axioms **CTaut**, **Meas$\emptyset$**, **FAdd** and **Mon** that $\vdash_{\mathsf{dEQPL}} ((\int\alpha) = \sum_{\{A\subseteq\mathsf{qB}\,|\,v_A\Vdash_c\alpha\}}(\int\wedge A))$. The axiom **Prob** then gives us that $(\int\alpha) = \sum_{\{A\subseteq\mathsf{qB}\,|\,v_A\Vdash_c\alpha\}}\lvert\lvert\top\rangle_A\rvert^2$. Hence, given a quantum formula γ, we can find an equivalent quantum formula that does not contain any probability terms.

Given a formula γ free of probability terms, consider the formula $\gamma^\dagger \overset{def}{=} (\gamma\sqcap(\sum_{A\subseteq\mathsf{qB}}\lvert\lvert\top\rangle_A\rvert^2 = 1))$. Please note that γ is consistent iff $\gamma^\dagger$ is consistent. Now, for each $A\subseteq\mathsf{qB}$, pick two fresh variables x_A and y_A. Consider the formula $\gamma^{\dagger\dagger}$ obtained from $\gamma^\dagger$ by replacing each term $\mathrm{Re}(|\top\rangle_A)$ by x_A and $\mathrm{Im}(|\top\rangle_A)$ by y_A. Now, by axiom **RCF**, $\gamma^\dagger$ is consistent if and only if $\gamma^{\dagger\dagger}$ is consistent over the reals. Observe that $\gamma^{\dagger\dagger}$ is a purely analytical formula. Therefore there is an assignment, say ρ', that satisfies $\gamma^{\dagger\dagger}$ or otherwise $\vdash_{\mathsf{dEQPL}} \boxminus \gamma^{\dagger\dagger}$ by **RCF**, and $\gamma^{\dagger\dagger}$ would not be consistent and neither would $\gamma^{\dagger}$, which is a contradiction. We conclude that there is such an assignment ρ', and from this assignment we can construct $|\psi\rangle$ and ρ that satisfies γ as required. $\diamond$

2.3 SAT problem

As there is an algorithm for deciding the consistency of analytical formulas [7], the proof of the Model Existence Lemma suggests an algorithm for deciding the consistency of quantum formulas. We shall now compute the complexity of one such algorithm. We shall need a few definitions for this.

A term t of the dEQPL is said to be a *polynomial* in variables $x_1, \ldots, x_k$ if t is of the form $(\sum m_{n_1,\ldots,n_k} x_1^{n_1} \ldots x_k^{n_k})$. The *degree* of a polynomial term is defined as expected. We will also assume for the rest of the paper that each polynomial is in a normal form: for any two summands $x_1^{n_1} \ldots x_k^{n_k}$ and $x_1^{n'_1} \ldots x_k^{n'_k}$ there is some j such that $n_j \neq n'_j$. Now, given a set of classical formulas $\mathcal{A} = \{\alpha_1, \ldots, \alpha_m\}$, a set of variables $\mathcal{V} = \{x_1, \ldots x_k, z_\alpha, \ldots, z_{\alpha_m}\}$ and a set of polynomials $\mathcal{P} = \{p_1, \ldots, p_s\}$ with variables in the set $\mathcal{V}$, we say that a comparison formula $(t \leq t')$ is an $(\mathcal{A}, \mathcal{V}, \mathcal{P})$-*atom* if t' is 0 and there is some polynomial term $p \in \mathcal{P}$ such that replacing *all* occurrences of the variables z_{α_i} by $(\int \alpha_i)$ for each $(1 \leq i \leq m)$ yields t. A dEQPL formula γ is said to be a $(\mathcal{A}, \mathcal{V}, \mathcal{P})$-*formula* if each comparison formula occurring in γ is an $(\mathcal{A}, \mathcal{V}, \mathcal{P})$-atom. We have:

Theorem 2.2 Let the set qB have n elements. Let $\mathcal{A} = \{\alpha_1, \ldots, \alpha_m\}$ be a set of classical formulas, $\mathcal{V} = \{x_1, \ldots x_k, z_\alpha, \ldots, z_{\alpha_m}\}$ be a set of variables and $\mathcal{P} = \{p_1, \ldots, p_s\}$ be a set of polynomials with variables in $\mathcal{V}$. Let the degree of each polynomial in $\mathcal{P}$ be bounded by d and let $r = 2^{n+1} + k + m$. Then, assuming that all basic integer operations take unit time, there is an $\mathsf{O}(|\gamma|(s + m + 1)^r (\max(d, 2))^{\mathsf{O}(r)})$ algorithm to decide whether an $(\mathcal{A}, \mathcal{V}, \mathcal{P})$-formula γ is a theorem or not.

Proof: For each $\alpha_i \in \mathcal{V}$ compute the set $\mathcal{B}_i = \{A \subseteq \mathsf{qB} \; | v_A \Vdash_{\mathsf{dEQPL}} \alpha_i\}$. Computation of each $\mathcal{B}_i$ takes at most $\mathsf{O}(2^n |\alpha_i|)$ steps, where $|\alpha_i|$ is the length of α_i. Since the sum $(\sum_{1 \leq im} |\alpha_i|)$ is less than $|\gamma|$, this whole computation takes at most $\mathsf{O}(2^n |\gamma|)$ steps. Please note that $(2^n |\gamma|)$ is bounded by $|\gamma|(s + m + 1)^r (\max(d, 2))^{\mathsf{O}(r)}$.

Given a $(\mathcal{A}, \mathcal{V}, \mathcal{P})$-formula γ, let γ_1 be the formula obtained from γ by replacing all probability terms $(\int \alpha_i)$ by z_{α_i}. Now, for each $A \subseteq \mathsf{qB}$, pick two fresh variables x_A and y_A and consider the formula

$$\gamma^{\dagger} = \gamma_1 \sqcap (\textstyle\prod_{1 \leq i \leq m} (z_{\alpha_i}^2 - \sum_{A \in B_i} (x_A^2 + y_A^2) = 0)) \sqcap ((\sum_{A \subseteq \mathsf{qB}} x_A^2 + y_A^2) - 1 = 0).$$

We make a few observations here:

- γ is consistent iff and only if $\gamma^{\dagger}$ is.

- $\gamma^\dagger$ is purely analytical.
- $\gamma^\dagger$ is built from comparison formulas of the form $(p \leq 0)$ or $(p = 0)$ where each p is a polynomial in the set

  $\mathcal{P}' = \mathcal{P} \cup \{(z^2_{\alpha_i} - \sum_{A \in B_i}(x^2_A + y^2_A)) | 1 \leq i \leq m\} \cup \{(\sum_{A \subseteq \mathsf{qB}} x^2_A + y^2_A) - 1\}$.
- $\mathcal{P}'$ has $(s+m+1)$ polynomials. The degree of each polynomial is bounded by $\max(d, 2)$ and is built from $r = 2^{n+1} + k + m$ variables.
- The length of $\gamma^\dagger$ is $\mathrm{O}(|\gamma| + m(\max(d, 2)^{\mathsf{O}(r)}))$.

Assuming that integer operations take unit time, the results of [7] give an $\mathsf{O}(|\gamma|(s + m + 1)^r(\max(d, 2))^{\mathsf{O}(r)})$ algorithm to decide consistency of $\gamma^\dagger$ which concludes the proof of the corollary . $\diamond$

2.4 Model-checking problem

For the model-checking procedure, we only consider closed formulas, *i.e.*, formulas without variables. We assume that a quantum state $|\psi\rangle$ over qB is modeled by a 2^n-array of pairs of real numbers, with $n = |\mathsf{qB}|$. We also assume that the basic arithmetical operations take $O(1)$ time.

We also assume the definition of the *length* of a classical formula α or a quantum formula γ as the number of symbols required to write the formula. The length of a formula ξ (classical or quantum) is represented by $|\xi|$.

Given a quantum state $|\psi\rangle$ and a quantum formula γ, the first step is to evaluate all the terms occurring in γ. For the probability terms $\int \alpha$, the evaluation takes $2^n|\alpha|$ steps as we have to compute the set of valuations $\wp(\mathsf{qB})$ that satisfy α. Once the terms are evaluated, the model checking algorithm is straightforward.

Theorem 2.3 Assuming that all basic arithmetical operations take unit time, there is an algorithm $O(|\gamma|.2^n)$ to decide if a quantum state $|\psi\rangle$ over qB satisfies γ with $|\mathsf{qB}| = n$.

Proof: First notice that the terms that consume more time to evaluate are those of the type $(\int \alpha)$ (both the terms $\mathrm{Re}(|\top\rangle_A)$ and $\mathrm{Im}(|\top\rangle_B)$ can be accessed in $O(1)$ time, since they are elements of the array). The number of terms of type $(\int \alpha)$ is bounded by $|\gamma|$. To evaluate one of these terms we require $O(2^n)$ time corresponding to traveling throughout all the valuations satisfying α, computing the square of the real and imaginary part, and summing all these values. So, computing all $(\int \alpha)$ terms takes $O(|\gamma|.2^n)$ time.

After these values are obtained, the remaining computation (comparing terms, negating a boolean value, and making implications between boolean values) takes at most $O(|\gamma|)$ time. Hence, the total time to decide if a quantum state $|\psi\rangle$ satisfies γ is $O(|\gamma|.2^n + |\gamma|) = O(|\gamma|.2^n)$. $\diamond$

3 Quantum Computational Tree Logic

We now introduce a temporal version of dEQPL by adopting the temporal modalities of computational tree logic (CTL) [13]. The logic is interpreted over a transition system in which the states are quantum states and the transitions are unitary operators. We also provide a sound and complete proof system by enriching the usual CTL proof system with the axioms of the quantum state logic. We start by briefly recalling the syntax, semantics and proof system of CTL.

3.1 Computational Tree Logic

Syntax. We shall assume that there is a countable set of propositional symbols Ξ. Assuming the set Ξ, the formulas of a CTL are given in BNF notation as

$$\theta := \perp\!\!\!\perp \talloblong p \talloblong (\theta \sqsupset \theta) \talloblong \mathsf{EX}\theta \talloblong \mathsf{AF}\theta \talloblong \mathsf{E}[\theta \mathsf{U} \theta]$$

where $p \in \Xi$.

Semantics. The semantics of the temporal logic CTL is given using a Kripke structure

Definition 3.1 (Kripke Structure) A *Kripke structure* over a set of propositions Ξ is a tuple $\mathcal{K} = (\mathsf{S}, \mathsf{R}, \mathsf{L})$ where:

- S is a set, elements of which are called *states.*
- $\mathsf{R} \subseteq S \times S$ is a said to be the *accessibility relation* and it is assumed that for every $s \in \mathsf{S}$ there exists $s' \in \mathsf{S}$ such that $(s, s') \in \mathsf{R}'$.
- $\mathsf{L} : \mathsf{S} \to \wp(\Xi)$ is said to be a *labeling function.*

Given a Kripke structure, $\mathcal{K} = (\mathsf{S}, \mathsf{R}, \mathsf{L})$, an infinite sequence of states $s_1 s_2 \ldots$ is said to be a *computation path* if $(s_i, s_{i+1}) \in \mathsf{R}$ for all $i \geq 1$. The semantics of CTL is defined in terms of a Kripke structure $\mathcal{K}$ and a state s of the Kripke structure. Intuitively, the modalities are composed by two symbols where the first one is chosen between E or A and the second one amongst X, F, G and the bi-modality U. The second symbol is used for temporal reasoning: X stands for ne**x**t; F for sometime in the **f**uture; G for always in the future; and U for **u**ntil. The first symbol quantifies over computation paths: an existential (E - for there **e**xists) path or a universal (A - for **a**ll) paths. The combination of the two symbols can be easily guessed. For example, the formula $\mathsf{EX}\theta$ holds in a state s if there **e**xists a ne**x**t state s' (that is, $(s, s') \in \mathsf{R}$) that satisfies θ. Given a Kripke structure $\mathcal{K}$, a state s of the Kripke structure, and a CTL formula θ, the formal semantics is defined inductively in terms of a relation $\mathcal{K}, s \Vdash_{\mathsf{CTL}} \theta$ and is given in Table 4.

Table 4: Semantics of CTL

$\mathcal{K}, s \nVdash_{\mathsf{CTL}} \perp\!\!\!\perp$;		
$\mathcal{K}, s \Vdash_{\mathsf{CTL}} p$	iff	$p \in \mathsf{L}(s)$;
$\mathcal{K}, s \Vdash_{\mathsf{CTL}} (\theta_1 \sqsupset \theta_2)$	iff	$\mathcal{K}, s \nVdash_{\mathsf{CTL}} \theta_1$ or $\mathcal{K}, s \Vdash_{\mathsf{CTL}} \theta_2$
$\mathcal{K}, s \Vdash_{\mathsf{CTL}} \mathsf{EX}\theta$	iff	$\mathcal{K}, s' \Vdash_{\mathsf{CTL}} \theta$ for some $(s, s') \in \mathsf{R}$;
$\mathcal{K}, s \Vdash_{\mathsf{CTL}} \mathsf{AF}\theta$	iff	for all paths $s_1 s_2 \ldots$ with $s = s_1$ there is some $i \geq 1$ such that $\mathcal{K}, s_i \Vdash_{\mathsf{CTL}} \theta$;
$\mathcal{K}, s \Vdash_{\mathsf{CTL}} \mathsf{E}[\theta_1 \mathsf{U} \theta_2]$	iff	there is a path $s_1 s_2 \ldots$ with $s = s_1$ such that for some $i \geq 1$ $\mathcal{K}, s_1 \Vdash_{\mathsf{CTL}} \theta_2$ and $\mathcal{K}, s_j \Vdash_{\mathsf{CTL}} \theta_1$ for $1 \leq j < i$.

Axiomatization. The temporal logic CTL enjoys a sound and complete axiomatization [15]. In order to give the axiomatization, we need to introduce some useful abbreviations

- $(\mathsf{AX}\theta)$ for $\boxminus \mathsf{EX}(\boxminus \theta)$;
- $(\mathsf{EF}\theta)$ for $\boxminus(\mathsf{E}[(\boxminus \perp\!\!\!\perp)\mathsf{U}\theta])$;
- $(\mathsf{AG}\theta)$ for $\boxminus(\mathsf{EF}(\boxminus \theta))$;
- $(\mathsf{EG}\theta)$ for $\boxminus(\mathsf{AF}(\boxminus \theta))$;
- $\mathsf{A}[\theta_1 \mathsf{U} \theta_2]$ for $\boxminus(\mathsf{E}[(\boxminus \theta_2)\mathsf{U}(\boxminus \theta_1 \sqcap \boxminus \theta_2)]) \sqcap (\boxminus(\mathsf{EG}(\boxminus \theta_2)))$.

The proof system HC_{CTL} of CTL is given in Table 5. The following result is proved in [15].

Theorem 3.2 *The proof system HC_{CTL} is sound and weakly complete with respect to Kripke structures.*

3.2 QCTL: Syntax and semantics

Syntax. Please recall that given the state logic dEQPL (see Section 2) describes quantum states over a finite set of qubits qB and is interpreted over unit vectors in the Hilbert space $\mathcal{H}_{\mathsf{qB}}$ and assignments $\rho : \mathbf{X} \to \mathbb{R}$ where $\mathbf{X}$ is a countable set of variables.

Table 5: HC_{CTL} : complete calculus for CTL

Axioms

[**Taut**]		All propositional tautologies with propositional symbols substituted by CTL formulas;
[**EX**]	$\vdash_{\mathsf{CTL}}$	$\mathsf{EX}(\theta_1 \sqcup \theta_2) \equiv \mathsf{EX}\theta_1 \sqcup \mathsf{EX}\theta_2$
[**X**]	$\vdash_{\mathsf{CTL}}$	$\mathsf{AX}(\boxminus \perp\!\!\!\perp) \sqcap \mathsf{EX}(\boxminus \perp\!\!\!\perp)$
[**EU**]	$\vdash_{\mathsf{CTL}}$	$\mathsf{E}[\theta_1 \mathsf{U} \theta_2] \equiv \theta_2 \sqcup (\theta_1 \sqcap \mathsf{EX}(\mathsf{E}[\theta_1 \mathsf{U} \theta_2]))$
[**AU**]	$\vdash_{\mathsf{CTL}}$	$\mathsf{A}[\theta_1 \mathsf{U} \theta_2] \equiv \theta_2 \sqcup (\theta_1 \sqcap \mathsf{AX}(\mathsf{A}[\theta_1 \mathsf{U} \theta_2]))$
[**AG1**]	$\vdash_{\mathsf{CTL}}$	$\mathsf{AG}(\theta_3 \sqsupset ((\boxminus \theta_2) \sqcap \mathsf{EX}\theta_3)) \sqsupset (\theta_3 \sqsupset (\boxminus \mathsf{A}[\theta_1 \mathsf{U} \theta_2]))$
[**AG2**]	$\vdash_{\mathsf{CTL}}$	$\mathsf{AG}(\theta_3 \sqsupset ((\boxminus \theta_2) \sqcap (\theta_1 \sqsupset \mathsf{AX}\theta_3))) \sqsupset (\theta_3 \sqsupset (\boxminus \mathsf{E}[\theta_1 \mathsf{U} \theta_2]))$
[**AG3**]	$\vdash_{\mathsf{CTL}}$	$\mathsf{AG}(\theta_1 \sqsupset \theta_2) \sqsupset (\mathsf{EX}\theta_1 \sqsupset \mathsf{EX}\theta_2)$

Inference rules

[**MP**]	$\theta_1, (\theta_1 \sqsupset \theta_2) \vdash_{\mathsf{CTL}} \theta_2$
[**AGen**]	$\theta_1 \vdash_{\mathsf{CTL}} \mathsf{AG}\theta_1$

Table 6: Language of QCTL

QCTL formulas

$$\theta \quad := \quad \gamma \talloblong (\theta \sqsupset \theta) \talloblong \mathsf{EX}\theta \talloblong \mathsf{AF}\theta \talloblong \mathsf{E}[\theta \mathsf{U} \theta] \text{ where } \gamma \text{ is a } \mathsf{dEQPL} \text{ formula.}$$

The formulas of Quantum Computation Tree Logic (QCTL) are obtained by enriching the quantum formulas with CTL modalities and are depicted in Table 6.

As in the case of CTL formulas, other temporal modalities $\mathsf{AX}\theta$, $\mathsf{EF}\theta$, $\mathsf{AG}\theta$, $\mathsf{EG}\theta$ and $\mathsf{A}[\theta_1 \mathsf{U} \theta_2]$ are introduced as abbreviations. The intuitive semantics of the temporal modalities is similar to those in classical CTL.

Semantics. In order to provide semantics to the logic, we introduce a very simple notion of quantum Kripke structure.

Definition 3.3 (Quantum Kripke structure) A *finite quantum Kripke structure* over the set of qubits qB and variables $\mathbf{X}$ is a pair $\mathcal{T} = (S, R)$ where:

- $S \subset \mathcal{H}_{\mathsf{qB}} \times \mathbb{R}^{\mathbf{X}}$ is a set of pairs $(|\psi\rangle, \rho)$ such that $|\psi\rangle$ is a unit vector in $\mathcal{H}_{\mathsf{qB}}$ and ρ is an assignment; and

- $R \subseteq S \times S$ is a relation such that for any $(|\psi\rangle, \rho) \in S$, there is an $(|\psi'\rangle, \rho') \in S$ such that $((|\psi\rangle, \rho), (|\psi'\rangle, \rho')) \in R$.

If S is finite then $\mathcal{T}$ is said to be *finite* and $|S|$, the number of elements of S, is said to be the *size* of $\mathcal{T}$.

For the sake of brevity, we shall often write the pair $(|\psi\rangle, \rho)$ as $|\psi\rangle\rho$. As usual, a computation path is a infinite sequence $|\psi_1\rangle\rho_1|\psi_2\rangle\rho_2 \ldots$ such that for any $i \geq 1$, we have $(|\psi_1\rangle\rho_1, |\psi_2\rangle\rho_2) \in R$. Given a quantum Kripke structure $\mathcal{T} = (S, R)$, a pair $(|\psi\rangle, \rho) \in S$ and a QCTL formula θ, the semantics of QCTL is defined in terms of a relation $\mathcal{T}, |\psi\rangle\rho \Vdash_{\mathsf{QCTL}} \gamma$ given in Table 7.

Table 7: Semantics of QCTL

$\mathcal{T}, \lvert\psi\rangle\rho \Vdash_{\mathsf{QCTL}} \gamma$	iff	$\lvert\psi\rangle\rho \Vdash_{\mathsf{dEQPL}} \gamma$;
$\mathcal{T}, \lvert\psi\rangle\rho \Vdash_{\mathsf{QCTL}} (\theta_1 \sqsupset \theta_2)$	iff	$\mathcal{T}, \lvert\psi\rangle\rho \nVdash_{\mathsf{QCTL}} \theta_1$ or $\mathcal{T}, \lvert\psi\rangle\rho \Vdash_{\mathsf{QCTL}} \theta_2$
$\mathcal{T}, \lvert\psi\rangle\rho \Vdash_{\mathsf{QCTL}} \mathsf{EX}\theta$	iff	$\mathcal{T}, \lvert\psi'\rangle\rho' \Vdash_{\mathsf{QCTL}} \theta$ for some $\lvert\psi'\rangle\rho' \in S$ such that $(\lvert\psi\rangle\rho, \lvert\psi'\rangle\rho') \in R$;
$\mathcal{T}, \lvert\psi\rangle\rho \Vdash_{\mathsf{QCTL}} \mathsf{AF}\theta$	iff	for all paths $\lvert\psi_1\rangle\rho_1\lvert\psi_2\rangle\rho_2 \ldots$ with $\lvert\psi_1\rangle = \lvert\psi\rangle, \rho_1 = \rho$ there is a $i \geq 1$ such that $\mathcal{T}, \lvert\psi_i\rangle\rho_i \Vdash_{\mathsf{QCTL}} \theta$;
$\mathcal{T}, \lvert\psi\rangle\rho \Vdash_{\mathsf{QCTL}} \mathsf{E}[\theta_1 \mathsf{U} \theta_2]$	iff	there is a path $\lvert\psi_1\rangle\rho_1\lvert\psi_2\rangle\rho_2 \ldots$ with $\psi_1 = \psi, \rho_1 = \rho$ such that for some $i \geq 1$ $\mathcal{T}, \lvert\psi_i\rangle\rho_i \Vdash_{\mathsf{QCTL}} \theta_2$ and$\mathcal{T}, \lvert\psi_j\rangle\rho_j \Vdash_{\mathsf{QCTL}} \theta_1$ for $1 \leq j < i$.

It is easy to see that for closed formulas *i.e.*, formulas without variables, we can drop the assignment in the interpretation side of the satisfaction relation. A quantum Kripke structure $\mathcal{T}$ is said to satisfy a temporal formula θ, which we denote by $\mathcal{T} \Vdash_{\mathsf{QCTL}} \theta$, if $\mathcal{T}, |\psi\rangle\rho \Vdash_{\mathsf{QCTL}} \theta$ for all $|\psi\rangle\rho \in S$. Please note that we are not considering generalized measurements. However, we will be able to reason about protocols where measurements in the standard computational basis are performed at the end of the protocol, thanks to the probability terms $\int \alpha$ in the state logic. Moreover, it is possible to rewrite any protocol in such a way that at the end we only need to make measurements in the computational basis. Similarly, classical states (bits) can be simulated by quantum states (qubits) that remain in the computational basis throughout the transitions.

3.3 Axiomatization

A weakly complete axiomatization of QCTL capitalizing on the complete CTL calculus HC_{CTL} is given in Table 8. Please note that although the completeness of the calculus may look trivial the proof of completeness is subtle. This is because the connectives $\perp\!\!\!\perp$ and $\sqsupset$ are shared between dEQPL and CTL logics which may create new theorems that will not be obtained by just adding the dEQPL axioms to CTL axioms.

Table 8: HC_{QCTL} calculus for QCTL

Axioms

[**QTeo**]	All dEQPL theorems;
[**CTLTaut**]	All CTL tautologies with propositional symbols substituted by QCTL formulas;

Inference rules

[**QMP**]	$\theta_1, (\theta_1 \sqsupset \theta_2) \vdash_{\mathsf{QCTL}} \theta_2$
[**AGen**]	$\theta_1 \vdash_{\mathsf{QCTL}} \mathsf{AG}\theta_1$

It is straightforward to check the soundness of the calculus, for this reason we omit here the lengthy exercise of verifying that all axioms and inference rules are sound.

Theorem 3.4 (Soundness) *The axiomatization HC_{QCTL} is sound.*

The completeness of the calculus is established by following a technique introduced in [9, 6]. Towards this end, it will be useful to translate QCTL formulas and models to the CTL framework. Consider first the subset of atomic dEQPL formulas qAtom (*i.e.*, the set constituted by comparison formulas $(t_1 \leq t_2)$). Let Ξ be the countable set of propositional symbols used to write CTL formulas. Given a fixed bijective map $\lambda : \mathsf{qAtom} \to \Xi$ (that translates each global atom to a CTL propositional symbol) we can translate each dEQPL formula θ to a CTL formula $\lambda(\theta)$ by extending inductively λ on the structure of the formula θ (and preserving all connectives). For simplicity, we denote $\lambda(\theta)$ just by $\widetilde{\theta}$. The map λ can also be used to translate a quantum Kripke structure $\mathcal{T} = (S, R)$ to the CTL model $\widetilde{\mathcal{T}} = (S, R, L)$, where $p \in \mathsf{L}(|\psi\rangle\rho)$ if $|\psi\rangle\rho \Vdash_{\mathsf{dEQPL}} \lambda^{-1}(p)$.

Lemma 3.5 *Let $\mathcal{T}$ be an quantum Kripke structure. Then,*

$$\mathcal{T}, |\psi\rangle\rho \Vdash_{\mathsf{QCTL}} \theta \qquad \textit{iff} \qquad \widetilde{\mathcal{T}}, |\psi\rangle\rho \Vdash_{\mathsf{CTL}} \widetilde{\theta}.$$

Proof: The proof follows by straightforward induction on the structure of θ.

- Base: If θ is $\perp\!\!\!\perp$ or $(t_1 \leq t_2)$ then $\mathcal{T}, |\psi\rangle\rho \Vdash_{\mathsf{QCTL}} \theta$ iff $\widetilde{\mathcal{T}}, |\psi\rangle\rho \Vdash_{\mathsf{CTL}} \widetilde{\theta}$ by definition.
- Step: For the sake of simplicity, we just consider the case when θ is $\mathsf{EX}\theta_1$. The other cases can be similarly handled.

  Now, if $\mathcal{T}, |\psi\rangle\rho \Vdash_{\mathsf{QCTL}} \mathsf{EX}\theta_1$ then there is a $|\psi'\rangle\rho'$ such that $(|\psi\rangle\rho, |\psi'\rangle\rho') \in R$ and $\mathcal{T}, |\psi'\rangle\rho' \Vdash_{\mathsf{QCTL}} \mathsf{EX}\theta_1$. By induction, $\mathcal{T}, |\psi'\rangle\rho' \Vdash_{\mathsf{CTL}} \mathsf{EX}\theta_1$ iff $\widetilde{\mathcal{T}}, |\psi'\rangle\rho' \Vdash_{\mathsf{CTL}} \widetilde{\theta}_1$. Thus, by definition $\widetilde{\mathcal{T}}, |\psi\rangle\rho \Vdash_{\mathsf{CTL}} \widetilde{\theta}$. The other direction can be similarly proved.

$\diamond$

QCTL incorporates both CTL and dEQPL reasoning.

Lemma 3.6 *For any QCTL formula θ*

- $\vdash_{\mathsf{CTL}} \widetilde{\theta}$ *then* $\vdash_{\mathsf{QCTL}} \theta$*;*
- $\vdash_{\mathsf{dEQPL}} \gamma$ *then* $\vdash_{\mathsf{QCTL}} \gamma$ *if* γ *is a* dEQPL *formula.*

Proof: Follows directly from axioms **CTLTaut** and **QTeo**. $\diamond$

Indeed, if one restricts just to dEQPL formulas, QCTL reasoning coincides with that of dEQPL.

Lemma 3.7 (Conservative Extension) *Let γ be an dEQPL formula. Then*

$$\vdash_{\mathsf{QCTL}} \gamma \qquad \textit{iff} \qquad \vdash_{\mathsf{dEQPL}} \gamma.$$

Proof: In light of Lemma 3.6, it suffices to show that if $\vdash_{\mathsf{QCTL}} \gamma$ then $\vdash_{\mathsf{dEQPL}} \gamma$. Suppose $\vdash_{\mathsf{QCTL}} \gamma$. Then $\Vdash_{\mathsf{QCTL}} \gamma$ by soundness of QCTL. Let $|\psi\rangle$ be an arbitrary unit vector in $\mathcal{H}_{\mathsf{qB}}$ and ρ an arbitrary assignment. Consider the the quantum Kripke structure $\mathcal{T} = (\{|\psi\rangle\rho\}, \{(|\psi\rangle\rho, |\psi\rangle\rho)\})$. We have that $\mathcal{T}, |\psi\rangle\rho \Vdash_{\mathsf{QCTL}} \gamma$. By definition, we get $|\psi\rangle\rho \Vdash_{\mathsf{dEQPL}} \gamma$. Since ψ and ρ are arbitrary, we get $\Vdash_{\mathsf{dEQPL}} \gamma$. By completeness of dEQPL, we get $\vdash_{\mathsf{dEQPL}} \gamma$. $\diamond$

The following Lemma is crucial to the proof of completeness.

Lemma 3.8 *Let θ be an QCTL formula such that $\Vdash_{\mathsf{QCTL}} \theta$. Then there is a dEQPL formula γ_θ such that*

$$\vdash_{\mathsf{QCTL}} \gamma_\theta \ \textit{and} \ \Vdash_{\mathsf{CTL}} (\mathsf{AG}\widetilde{\gamma}_\theta \sqsupset \widetilde{\theta}).$$

Proof: Let $at = \{\gamma_1, \ldots, \gamma_k\}$ be the set of atomic dEQPL formulas that are atoms of θ. Now for each k-vector $i \in \{0,1\}^k$, consider the dEQPL formula

$$\delta_i = \bigsqcap_{j=1}^{k} \varphi_j \qquad \text{where} \qquad \varphi_j = \left\{ \begin{array}{cl} \gamma_j & \text{if } j\text{-th bit of } i \text{ is } 1 \\ (\boxminus \gamma_j) & \text{otherwise} \end{array} \right.$$

Let $K \subseteq \{0,1\}^k$ be such that δ_i is a dEQPL consistent formula and let $\gamma_\theta = \bigsqcup_{i \in K} \delta_i$. Clearly, $\vdash_{\mathsf{dEQPL}} \gamma_\theta$ and therefore by Lemma 3.7, $\vdash_{\mathsf{QCTL}} \gamma_\theta$. Also please note for any quantum state $|\psi\rangle$ and assignment ρ, $|\psi\rangle\rho \Vdash \delta_i$ for exactly one $i \in K$.

We shall prove $\Vdash_{\mathsf{CTL}} (\mathsf{AG}\widetilde{\gamma}_\theta \sqsupset \widetilde{\theta})$ by contradiction. Suppose that $\mathcal{K} = (\mathsf{S}, \mathsf{R}, \mathsf{L})$ is a CTL model such that $\mathcal{K}, s \nVdash_{\mathsf{CTL}} (\mathsf{AG}\widetilde{\gamma}_\theta \sqsupset \widetilde{\theta})$ for some $s \in \mathsf{S}$. Then $\mathcal{K}, s \Vdash_{\mathsf{CTL}} \mathsf{AG}\widetilde{\gamma}_\theta$. and $\mathcal{K}, s \nVdash_{\mathsf{CTL}} \widetilde{\theta}$. Let $\mathsf{S}' = \{s' \in \mathsf{S} : s' \text{ is reachable from } s\}$ (by reachable we mean reachable using the accessibility relation R).

Pick $s' \in \mathsf{S}'$ and fix it. Since $\mathcal{K}, s' \Vdash_{\mathsf{CTL}} \mathsf{AG}\widetilde{\gamma}_\theta$, we get that $\mathcal{K}, s' \Vdash_{\mathsf{CTL}} \widetilde{\gamma}_\theta$. Hence, there is some $i_{s'} \in K$ such that $\mathcal{K}, s' \Vdash_{\mathsf{CTL}} \widetilde{\delta_{i_{s'}}}$. Since $\delta_{i_{s'}}$ is consistent dEQPL formula, there is a unit vector $|\psi_{s'}\rangle$ and an assignment $\rho_{s'}$ such that $|\psi_{s'}\rangle\rho_{s'} \Vdash_{\mathsf{dEQPL}} \delta_{i_{s'}}$. For each s' fix on such $|\psi_{s'}\rangle$ and $\rho_{s'}$ ensuring that $\rho_{s_1} \neq \rho_{s_2}$ (this can be ensured by modifying the assignments on real variables not occurring in θ). Consider the set $S_\theta = \{(|\psi_{s'}\rangle, \rho_{s'}) : s' \in \mathsf{S}'\}$ and the QCTL model $\mathcal{T} = (S_\theta, R_\theta)$, where $(|\psi_{s'}\rangle\rho_{s'}, |\psi_{s''}\rangle\rho_{s''}) \in R_\theta$ iff $(s', s'') \in R$. Using the fact that $\mathcal{K}, s \nVdash \widetilde{\theta}$, it follows from Lemma 3.5 $\mathcal{T}, |\psi_s\rangle\rho_s \nVdash \theta$ which contradicts $\vdash_{\mathsf{QCTL}} \gamma_\theta$ ◇

We are now able to show the completeness of HC_{QCTL}.

Theorem 3.9 *The axiomatization HC_{QCTL} is weakly complete.*

Proof: Let $\Vdash_{\mathsf{QCTL}} \theta$ be a valid QCTL formula. Let γ_θ be as in Lemma 3.8, then, $\Vdash_{\mathsf{CTL}} (\mathsf{AG}\widetilde{\gamma}_\theta \sqsupset \widetilde{\theta})$. Using CTL completeness we have $\vdash_{\mathsf{CTL}} (\mathsf{AG}\widetilde{\gamma}_\theta \sqsupset \widetilde{\theta})$. Now, from Lemma 3.6 we get $\vdash_{\mathsf{QCTL}} (\mathsf{AG}\gamma_\theta \sqsupset \theta)$.

Hence, we are able do the following derivation in QCTL:

1)	$\vdash_{\mathsf{QCTL}} \gamma_\theta$	Tautology
2)	$\vdash_{\mathsf{QCTL}} (\mathsf{AG}\gamma_\theta)$	Rule **AGen**
3)	$\vdash_{\mathsf{QCTL}} (\mathsf{AG}\gamma_\theta \sqsupset \theta)$	Lemma 3.8,Lemma 3.6
4)	$\vdash_{\mathsf{QCTL}} \theta$	Modus Ponens $2, 3$

Therefore, HC_{QCTL} is complete. ◇

3.4 SAT problem

The completeness proof suggests a SAT algorithm for QCTL. Let θ be the QCTL formula that we want to test for satisfiability and $at = \{\gamma_1, \ldots, \gamma_k\}$ be the set of atomic dEQPL formulas that are atoms of θ. Now for each k-vector $i \in \{0,1\}^k$, consider the dEQPL formula

$$\delta_i = \prod_{j=1}^{k} \varphi_j \qquad \text{where} \qquad \varphi_j = \begin{cases} \gamma_j & \text{if } j\text{-th bit of } i \text{ is } 1 \\ (\boxminus \gamma_j) & \text{otherwise} \end{cases}$$

Let $K \subseteq \{0,1\}^k$ be such that δ_i is a dEQPL consistent formula and let $\gamma_\theta = \bigsqcup_{i\in K} \delta_i$. Observe that $\Vdash_{\mathsf{dEQPL}} \gamma_\theta$ and that for each $|\psi\rangle, \rho$ there exists a unique $i \in K$ such that $|\psi\rangle, \rho \Vdash_{\mathsf{dEQPL}} \delta_i$. Given a CTL model $\mathcal{K} = (S, R, L)$ of $(\mathsf{AG}(\widetilde{\gamma}_\theta) \sqcap \widetilde{\theta})$ and a state $s \in S$ we denote by $(|\psi_s\rangle, \rho_s)$ a dEQPL model that satisfies δ_i whenever $\mathcal{K}, s \Vdash_{\mathsf{CTL}} \widetilde{\delta}_i$. Moreover, choose $(|\psi_s\rangle, \rho_s) \neq (|\psi_{s'}\rangle, \rho_{s'})$ whenever $s \neq s'$ (this can be done just by changing the assignments of variables not occurring in θ). Finally, we denote by $\mathcal{T}_\mathcal{K}$ the quantum Kripke structure (S_K, R_K) where $\{(|\psi_s\rangle, \rho_s) : s \in S\}$ and $((|\psi_s\rangle, \rho_s), (|\psi_{s'}\rangle, \rho_{s'})) \in R_K$ iff $(s, s') \in R$.

The following theorem is crucial to obtain the QCTL SAT algorithm.

Theorem 3.10 *Let θ be a QCTL formula. Then, $(\mathsf{AG}(\widetilde{\gamma}_\theta) \sqcap \widetilde{\theta})$ is CTL-satisfiable iff θ is QCTL-satisfiable. Moreover, $\mathcal{K}, s \Vdash_{\mathsf{CTL}} (\mathsf{AG}(\widetilde{\gamma}_\theta) \sqcap \widetilde{\theta})$ iff $\mathcal{T}_\mathcal{K}, |\psi_s\rangle\rho_s \Vdash_{\mathsf{QCTL}} \theta$.*

Proof: $\Leftarrow$) Follows directly from Lemma 3.5 and from the fact that $\Vdash_{\mathsf{dEQPL}} \gamma_\theta$. Concerning the second assertion, it follows by noticing that $\widetilde{\mathcal{T}_\mathcal{K}}$ is equal to $\mathcal{K}$ up to relabeling of states.

$\Rightarrow$) For this direction, it is sufficient to show the second assertion. Since $\widetilde{\mathcal{T}_\mathcal{K}}$ is equal to $\mathcal{K}$ up to relabeling of states, by Lemma 3.5 we have that $\mathcal{T}_\mathcal{K}, |\psi_s\rangle\rho_s \Vdash_{\mathsf{QCTL}} \mathsf{AG}(\gamma_\theta) \sqcap \theta$ and therefore $\mathcal{T}_\mathcal{K}, |\psi_s\rangle\rho_s \Vdash_{\mathsf{QCTL}} \theta$. ◇

The SAT algorithm is now easily obtained from the CTL SAT algorithm.

Table 9: Algorithm to determine $Sat(\theta)$

1) Generate δ_i for all $i \in 2^k$ where k is number of atomic dEQPL formulas that are atoms of θ.

2) Using the SAT algorithm for dEQPL compute the set of indexes K such that $i \in K$ iff δ_i is a consistent dEQPL formula,
in this case store the dEQPL model output by the SAT algorithm
and call it $(|\psi_i\rangle, \rho_i)$.

3) Find a model $\mathcal{K}$ for $(\mathsf{AG}(\widetilde{\gamma}_\theta) \sqcap \widetilde{\theta})$ using the CTL SAT algorithm.

4) Construct $\mathcal{T}_\mathcal{K}$ from the models stored in 2).

3.5 Model-checking problem

We now address the problem of model-checking a closed temporal formula. Following the usual model-checking technique for CTL, the goal is to compute the set

$$Sat_{\mathcal{T}}(\theta) := \{|\psi\rangle \in S : \mathcal{T}, |\psi\rangle \Vdash_{\mathsf{QCTL}} \theta\}$$

for a given finite quantum Kripke structure $\mathcal{T} = (S, R)$ and closed formula θ (please note that assignments play no part the entailment relation for closed formulas). This is called the global model-checking problem. The (global) model-checking algorithm is given in Table 10.

Table 10: Algorithm to determine $Sat_{\mathcal{T}}(\theta)$

$$\begin{aligned}
&(1)\ Sat_{\mathcal{T}}(\gamma) &&= \{|\psi\rangle \in S : |\psi\rangle \Vdash_{\mathsf{dEQPL}} \gamma\};\\
&(2)\ Sat_{\mathcal{T}}(\theta_1 \sqsupset \theta_2) &&= (S \setminus Sat_{\mathcal{T}}(\theta_1)) \cup Sat_{\mathcal{T}}(\theta_2)\\
&(3)\ Sat_{\mathcal{T}}\mathsf{EX}\theta &&= \{|\psi\rangle \in S : R(|\psi\rangle) \cap Sat_{\mathcal{T}}(\theta) \neq \emptyset\};\\
&(4)\ Sat_{\mathcal{T}}\mathsf{AF}\theta &&= \mathbf{FixedPoint}[\lambda X.\{R^{-1}X\} \bigcup X, Sat_{\mathcal{T}}(\theta)];\\
&(5)\ Sat_{\mathcal{T}}(\mathsf{E}[\theta_1 \mathsf{U} \theta_2]) &&= \mathbf{FixedPoint}[\lambda X.\{R^{-1}X \bigcap Sat_{\mathcal{T}}(\theta_1)\}, Sat_{\mathcal{T}}(\theta_2)];
\end{aligned}$$

where $R^{-1}X = \{\psi \in S \mid \exists \psi' \in X, \rho, \rho' \text{ s.t. } (|\psi\rangle\rho, |\psi'\rangle\rho') \in R\}$.

Clearly, quantum Kripke structures require, in general, exponential space (over the number of qubits) to simulate with classical computers due to the exponential number of possible state superpositions. For this reason, the model checking algorithm takes exponential time on the number of qubits, but it is polynomial on the size of the transition system and the complexity of the formula.

Theorem 3.11 Assuming that all basic arithmetical operations take unit time, the algorithm in Table 10 takes $O(|\theta|^2.|S_{\mathcal{T}}|^2.2^n)$ time.

Proof: The propositional CTL model-checking algorithm takes $O(|\theta|.|S_{\mathcal{T}}|^2)$ (see [13] for a detailed analysis). So, if we consider each quantum atom to be a propositional symbol, the time complexity of the algorithm would be $O(|\theta|.|S_{\mathcal{T}}|^2)$. Finally, since checking if a quantum atom is satisfied by a quantum state takes $O(|\theta|.2^n)$ (c.f. Theorem 2.3) we derive the desired upper bound. Recall that we consider all arithmetic computations to be $O(1)$ by using floating point representation for the real numbers. $\diamond$

4 Quantum Linear Time Logic

4.1 Linear Time Logic

Syntax. Like in the case of CTL, we assume that there is a countable set of propositional symbols Ξ. Assuming the set Ξ, the formulas of Linear Time Logic (LTL) are given in BNF notation as

$$\theta := \perp\!\!\!\perp \talloblong p \talloblong (\theta \sqsupset \theta) \talloblong \mathsf{X}\theta \talloblong \theta \mathsf{U} \theta$$

where $p \in \Xi$.

Semantics. The semantics of the temporal logic LTL is also given using a Kripke structure. The semantics of LTL is defined in terms of a Kripke structure $\mathcal{K}$ and a computation path $\pi = s_1, s_2 \ldots$ Given that the computation path is fixed, the LTL modalities contain only the symbols for temporal reasoning: X stands for ne**x**t; and U for **u**ntil. The remaining temporal modalities, F and G, are easily obtained by abbreviation: $(\mathsf{F}p)$ for $((\boxminus \perp\!\!\!\perp)\mathsf{U}p)$; and $(\mathsf{G}p)$ for $(\boxminus \mathsf{F}(\boxminus p))$.

In terms of expressiveness, LTL and CTL are incomparable. For instance, the LTL formula $\mathsf{FG}p$ has no CTL translation. Likewise, the CTL formula $\mathsf{AGEF}p$ has no LTL counterpart. LTL has the advantage that it is able to express fairness constrains, which are important in reasoning about distributed/parallel systems. On the other hand, the complexity of model-checking LTL formulas is PSPACE-complete [26], whereas CTL formulas can be checked in polynomial time [13].

Given a Kripke structure $\mathcal{K}$, a computation path $\pi = s_1 \ldots$ of the Kripke structure, and a LTL formula θ, the formal semantics is defined inductively in terms of a relation $\mathcal{K}, \pi \Vdash \theta$ and is given in Table 11. We denote by π^i the i-th suffix of π, that is, the path $s_i, s_{i+1} \ldots$

Table 11: Semantics of LTL

$\mathcal{K}, \pi \nVdash_{\mathsf{LTL}} \perp\!\!\!\perp$;		
$\mathcal{K}, \pi \Vdash_{\mathsf{LTL}} p$	iff	$p \in \mathsf{L}(s_1)$ with $\pi = s_1, \ldots$;
$\mathcal{K}, \pi \Vdash_{\mathsf{LTL}} (\theta_1 \sqsupset \theta_2)$	iff	$\mathcal{K}, \pi \nVdash_{\mathsf{LTL}} \theta_1$ or $\mathcal{K}, \pi \Vdash_{\mathsf{LTL}} \theta_2$;
$\mathcal{K}, \pi \Vdash_{\mathsf{LTL}} \mathsf{X}\theta$	iff	$\mathcal{K}, \pi^2 \Vdash_{\mathsf{LTL}} \theta$;
$\mathcal{K}, s \Vdash_{\mathsf{LTL}} (\theta_1 \mathsf{U} \theta_2)$	iff	there is some $i \geq 1$ such that $\mathcal{K}, \pi^i \Vdash_{\mathsf{LTL}} \theta_2$ and $\mathcal{K}, \pi^j \Vdash_{\mathsf{LTL}} \theta_1$ for $1 \leq j < i$.

Axiomatization. The temporal logic LTL enjoys a sound and complete axiomatization. The proof system HC_{LTL} of LTL is given in Table 12. The following result is proved in [18].

Theorem 4.1 *The proof system HC_{LTL} is sound and weakly complete with respect to Kripke structures.*

Table 12: HC_{LTL} : complete calculus for LTL

Axioms

[**Taut**]		All propositional tautologies with propositional symbols substituted by LTL formulas;
[**X1**]	$\vdash_{\mathsf{LTL}}$	$(\boxminus \mathsf{X}\theta_1) \equiv (\mathsf{X} \boxminus \theta_1)$
[**X2**]	$\vdash_{\mathsf{LTL}}$	$(\mathsf{X}(\theta_1 \sqsupset \theta_2)) \sqsupset (\mathsf{X}\theta_1 \sqsupset \mathsf{X}\theta_2)$
[**G**]	$\vdash_{\mathsf{LTL}}$	$(\mathsf{G}\theta_1) \sqsupset (\theta_1 \sqcap (\mathsf{X}\mathsf{G}\theta_1))$
[**U1**]	$\vdash_{\mathsf{LTL}}$	$(\theta_1 \mathsf{U} \theta_2) \sqsupset (\mathsf{F}\theta_2)$
[**U2**]	$\vdash_{\mathsf{LTL}}$	$(\theta_1 \mathsf{U} \theta_2) \equiv (\theta_2 \sqcup (\theta_1 \sqcap \mathsf{X}(\theta_1 \mathsf{U} \theta_2)))$

Inference rules

[**MP**]	$\theta_1, (\theta_1 \sqsupset \theta_2) \vdash_{\mathsf{LTL}} \theta_2$
[**XGen**]	$\theta_1 \vdash_{\mathsf{LTL}} (\mathsf{X}\theta_1)$
[**Ind**]	$(\theta_1 \sqsupset \theta_2), (\theta_1 \sqsupset (\mathsf{X}\theta_1)) \vdash_{\mathsf{LTL}} (\theta_1 \sqsupset (\mathsf{G}\theta_2))$

4.2 QLTL: Syntax and Semantics

Syntax. Similarly to QCTL, the formulas of Quantum Linear Time Logic (QLTL) are obtained by enriching the quantum formulas with LTL modalities and are depicted in Table 13.

Table 13: Language of QLTL

QLTL formulas

$$\theta \quad := \quad \gamma \;[\!]\; (\theta \sqsupset \theta) \;[\!]\; (\mathsf{X}\theta) \;[\!]\; (\theta \mathsf{U} \theta) \text{ where } \gamma \text{ is a } \mathsf{dEQPL} \text{ formula.}$$

The temporal modalities $\mathsf{F}\theta$ and $\mathsf{G}\theta$ are introduced as abbreviations.

Semantics. We now provide a semantics for QLTL based on quantum Kripke structures. A computation path is a infinite sequence $\pi = |\psi_1\rangle\rho_1, |\psi_2\rangle\rho_2 \dots$ such that for any $i \geq 1$, we have $(|\psi_i\rangle\rho_i, |\psi_{i+1}\rangle\rho_2) \in R$. Given a quantum Kripke structure $\mathcal{T} = (S, R)$, a computational path π in $\mathcal{T}$ and a QLTL formula θ, the semantics of QLTL is defined in terms of a relation $\mathcal{T}, \pi \Vdash_{\mathsf{QLTL}} \gamma$ given in Table 14.

Table 14: Semantics of QLTL

$\mathcal{T}, \pi \Vdash_{\mathsf{QLTL}} \gamma$	iff	$|\psi_1\rangle\rho_1 \Vdash_{\mathsf{dEQPL}} \gamma$;
$\mathcal{T}, \pi \Vdash_{\mathsf{QLTL}} (\theta_1 \sqsupset \theta_2)$	iff	$\mathcal{T}, \pi \nVdash_{\mathsf{QLTL}} \theta_1$ or $\mathcal{T}, \pi \Vdash_{\mathsf{QLTL}} \theta_2$;
$\mathcal{T}, \pi \Vdash_{\mathsf{QLTL}} (\mathsf{X}\theta)$	iff	$\mathcal{T}, \pi^2 \Vdash_{\mathsf{QLTL}} \theta$;
$\mathcal{T}, \pi \Vdash_{\mathsf{QLTL}} (\theta_1 \mathsf{U} \theta_2)$	iff	there is some $i \geq 1$ such that $\mathcal{T}, \pi^i \Vdash_{\mathsf{QLTL}} \theta_2$ and $\mathcal{T}, \pi^j \Vdash_{\mathsf{QLTL}} \theta_1$ for $1 \leq j < i$.

A quantum Kripke structure $\mathcal{T}$ is said to satisfy a QLTL formula θ, which we denote by $\mathcal{T} \Vdash_{\mathsf{QLTL}} \theta$, if $\mathcal{T}, \pi \Vdash_{\mathsf{QLTL}} \theta$ for all computational paths π in $\mathcal{T}$.

4.3 Axiomatization

Like for the case of QCTL, we are able to provide a weakly complete axiomatization of QLTL capitalizing on the complete LTL calculus HC_{CTL} is given in Table15.

Table 15: HC_{QLTL} calculus for QLTL

Axioms	
[QTeo]	All dEQPL theorems;
[LTLTaut]	All LTL tautologies with propositional symbols substituted by QLTL formulas;
Inference rules	
[QMP]	$\theta_1, (\theta_1 \sqsupset \theta_2) \vdash_{\mathsf{QCTL}} \theta_2$
[Gen]	$\theta_1 \vdash_{\mathsf{LTL}} \mathsf{G}\theta_1$

It is straightforward to check the soundness of the calculus, for this reason we omit here the lengthy exercise of verifying that all axioms and inference rules are sound.

Theorem 4.2 (Soundness) *The axiomatization HC_{QLTL} is sound.*

The completeness of the calculus is established by the same technique of QCTL, that is, by translating quantum atoms into propositional symbols. Consider the subset of atomic dEQPL formulas qAtom (*i.e.*, the set constituted by comparison formulas $(t_1 \leq t_2)$). Let Ξ be the countable set of propositional symbols used to write LTL formulas. Given a fixed bijective map $\lambda : \mathsf{qAtom} \to \Xi$ (that translates each global atom to a LTL propositional symbol) we can translate each dEQPL formula θ to a LTL formula $\lambda(\theta)$ by extending inductively λ on the structure of the formula θ (and preserving all connectives). For simplicity, we denote $\lambda(\theta)$ just by $\widetilde{\theta}$. The map λ can also be used to translate a quantum Kripke structure $\mathcal{T} = (S, R)$ to the LTL model $\widetilde{\mathcal{T}} = (S, R, L)$, where $p \in \mathsf{L}(|\psi\rangle\rho)$ if $|\psi\rangle\rho \Vdash_{\mathsf{dEQPL}} \lambda^{-1}(p)$.

Lemma 4.3 *Let $\mathcal{T}$ be an quantum Kripke structure. Then,*

$$\mathcal{T}, \pi \Vdash_{\mathsf{QLTL}} \theta \qquad \textit{iff} \qquad \widetilde{\mathcal{T}}, \pi \Vdash_{\mathsf{LTL}} \widetilde{\theta}.$$

Proof: The proof follows by straightforward induction on the structure of θ.

- Base: If θ is $\perp\!\!\!\perp$ or $(t_1 \leq t_2)$ then $\mathcal{T}, \pi \Vdash_{\mathsf{QLTL}} \theta$ iff $|\psi_1\rangle\rho_1 \Vdash_{\mathsf{dEQPL}} \theta$ iff $\widetilde{\mathcal{T}}, \pi \Vdash_{\mathsf{LTL}} \widetilde{\theta}$ by definition.
- Step: For the sake of simplicity, we just consider the case when θ is $\mathsf{X}\theta_1$. The other cases can be similarly handled.

  Now, $\mathcal{T}, \pi \Vdash_{\mathsf{QLTL}} \mathsf{X}\theta_1$ iff $\mathcal{T}, \pi^2 \Vdash_{\mathsf{QLTL}} \theta_1$ iff, by induction, $\widetilde{\mathcal{T}}, \pi^2 \Vdash_{\mathsf{LTL}} \widetilde{\theta}_1$ iff $\widetilde{\mathcal{T}}, \pi \Vdash_{\mathsf{LTL}} \mathsf{X}\widetilde{\theta}_1$ iff, by definition, $\widetilde{\mathcal{T}}, \pi \Vdash_{\mathsf{LTL}} \widetilde{\theta}$.

$\diamond$

QLTL incorporates both LTL and dEQPL reasoning.

Lemma 4.4 *For any QLTL formula θ*

- $\vdash_{\mathsf{LTL}} \widetilde{\theta}$ *then* $\vdash_{\mathsf{QLTL}} \theta$;
- $\vdash_{\mathsf{dEQPL}} \gamma$ *then* $\vdash_{\mathsf{QLTL}} \gamma$ *if* γ *is a dEQPL formula.*

Proof: Follows directly from axioms **LTLTaut** and **QTeo**. $\diamond$

If one restricts just to dEQPL formulas, QLTL reasoning coincides with that of dEQPL.

Lemma 4.5 (Conservative Extension) *Let γ be an dEQPL formula. Then*

$$\vdash_{\mathsf{QLTL}} \gamma \qquad \textit{iff} \qquad \vdash_{\mathsf{dEQPL}} \gamma.$$

Proof: Thanks to Lemma 4.4 it suffices to show that if $\vdash_{\mathsf{QLTL}} \gamma$ then $\vdash_{\mathsf{dEQPL}} \gamma$. Suppose $\vdash_{\mathsf{QLTL}} \gamma$. Then $\Vdash_{\mathsf{QLTL}} \gamma$ by soundness of QLTL. Let $|\psi\rangle$ be an arbitrary unit vector in $\mathcal{H}_{\mathsf{qB}}$ and ρ an arbitrary assignment. Consider the quantum Kripke structure $\mathcal{T} = (\{|\psi\rangle\rho\}, \{(|\psi\rangle\rho, |\psi\rangle\rho)\})$ and π its unique path. We have that $\mathcal{T}, \pi \Vdash_{\mathsf{QLTL}} \gamma$. By definition, we get $|\psi\rangle\rho \Vdash_{\mathsf{dEQPL}} \gamma$. Since ψ and ρ are arbitrary, we get $\Vdash_{\mathsf{dEQPL}} \gamma$. By completeness of dEQPL, we get $\vdash_{\mathsf{dEQPL}} \gamma$. $\diamond$

The following lemma is crucial to the proof of completeness.

Lemma 4.6 *Let θ be an QLTL formula such that $\Vdash_{\mathsf{QLTL}} \theta$. Then there is a dEQPL formula γ_θ such that*

$$\vdash_{\mathsf{QLTL}} \gamma_\theta \ \textit{and} \ \Vdash_{\mathsf{LTL}} (\mathsf{G}\widetilde{\gamma_\theta} \sqsupset \widetilde{\theta}).$$

Proof: Let $at = \{\gamma_1, \dots, \gamma_k\}$ be the set of atomic dEQPL formulas that are atoms of θ. Now for each k-vector $i \in \{0,1\}^k$, consider the dEQPL formula

$$\delta_i = \prod_{j=1}^{k} \varphi_j \qquad \text{where} \qquad \varphi_j = \begin{cases} \quad \gamma_j & \text{if } j\text{-th bit of } i \text{ is } 1 \\ (\boxminus \gamma_j) & \text{otherwise} \end{cases}$$

Let $K \subseteq \{0,1\}^k$ be such that δ_i is a dEQPL consistent formula and let $\gamma_\theta = \bigsqcup_{i \in K} \delta_i$. Clearly, $\vdash_{\mathsf{dEQPL}} \gamma_\theta$ and therefore by Lemma 4.5, $\vdash_{\mathsf{QLTL}} \gamma_\theta$. Also please note for any quantum state $|\psi\rangle$ and assignment ρ, $|\psi\rangle\rho \Vdash \delta_i$ for exactly one $i \in K$.

We shall prove $\Vdash_{\mathsf{LTL}} (\mathsf{G}\widetilde{\gamma_\theta} \sqsupset \widetilde{\theta})$ by contradiction. Suppose that $\mathcal{K} = (\mathsf{S}, \mathsf{R}, \mathsf{L})$ is a CTL model such that $\mathcal{K}, \pi \nVdash_{\mathsf{LTL}} (\mathsf{G}\widetilde{\gamma_\theta} \sqsupset \widetilde{\theta})$ for some $s \in \mathsf{S}$. Then $\mathcal{K}, \pi \Vdash_{\mathsf{LTL}} \mathsf{G}\widetilde{\gamma_\theta}$ and $\mathcal{K}, \pi \nVdash_{\mathsf{LTL}} \widetilde{\theta}$. Let $\mathsf{S}' = \{s' \in \mathsf{S} : s' \text{ occurs in } \pi\}$.

Since $\mathcal{K}, \pi \Vdash_{\mathsf{LTL}} \mathsf{G}\widetilde{\gamma_\theta}$, we get that $\mathcal{K}, \pi \Vdash_{\mathsf{LTL}} \widetilde{\gamma_\theta}$. Hence, there is some $i_{s_1} \in K$ such that $\mathcal{K}, \pi \Vdash_{\mathsf{LTL}} \widetilde{\delta_{i_{s_1}}}$. Since $\delta_{i_{s_1}}$ is consistent dEQPL formula, there is a unit vector $|\psi_{s_1}\rangle$ and an assignment ρ_{s_1} such that $|\psi_{s_1}\rangle\rho_{s_1} \Vdash_{\mathsf{dEQPL}} \delta_{i_{s_1}}$. For each s_j fix on such $|\psi_{s_j}\rangle$ and ρ_{s_j} ensuring that $\rho_{s_j} \neq \rho_{s_k}$ whenever $j \neq k$ (this can be ensured by modifying the assignments on real variables not occurring in θ). Consider the set $S_\theta = \{(|\psi_{s'}\rangle, \rho_{s'}) : s' \in \mathsf{S}'\}$ and the QLTL model $\mathcal{T} = (S_\theta, R_\theta)$, where $(|\psi_{s'}\rangle\rho_{s'}, |\psi_{s''}\rangle\rho_{s''}) \in R_\theta$ iff $(s', s'') \in R$. Denote by π' the path $|\psi_{s_1}\rangle\rho_{s_1}, |\psi_{s_2}\rangle\rho_{s_2} \dots$ Using the fact that $\mathcal{K}, \pi \nVdash \widetilde{\theta}$, it follows from Lemma 4.3 $\mathcal{T}, \pi' \nVdash \theta$ which contradicts $\vdash_{\mathsf{QLTL}} \gamma_\theta$. $\diamond$

We are now able to show the completeness of HC_{QLTL}.

Theorem 4.7 *The axiomatization HC_{QLTL} is weakly complete.*

Proof: Let $\Vdash_{\mathsf{QLTL}} \theta$ be a valid QLTL formula. With γ_θ as in Lemma 4.6 we have that $\Vdash_{\mathsf{LTL}} \ (\mathsf{G}\widetilde{\gamma}_\theta \ \sqsupset \ \widetilde{\theta})$. Using LTL completeness we have $\vdash_{\mathsf{LTL}} (\mathsf{G}\widetilde{\gamma}_\theta \sqsupset \widetilde{\theta})$. Now, from Lemma 4.4 we get $\vdash_{\mathsf{QLTL}} (\mathsf{G}\gamma_\theta \sqsupset \theta)$.

Hence, we are able do the following derivation in QLTL:

1)	$\vdash_{\mathsf{QLTL}} \gamma_\theta$	Tautology
2)	$\vdash_{\mathsf{QLTL}} (\mathsf{G}\gamma_\theta)$	Rule **Gen**
3)	$\vdash_{\mathsf{QLTL}} (\mathsf{G}\gamma_\theta \sqsupset \theta)$	Lemma 4.6,Lemma 4.4
4)	$\vdash_{\mathsf{QLTL}} \theta$	Modus Ponens $2, 3$

Therefore, HC_{QLTL} is complete. ◇

4.4 SAT problem

The SAT algorithm for QLTL is obtained similarly to the QCTL SAT algorithm. For the sake of completeness we will present the details herein. Let θ be the QLTL formula that we want to test for satisfiability and $at = \{\gamma_1, \ldots, \gamma_k\}$ be the set of atomic dEQPL formulas that are atoms of θ. Now for each k-vector $i \in \{0,1\}^k$, consider the dEQPL formula

$$\delta_i = \bigsqcap_{j=1}^{k} \varphi_j \qquad \text{where} \qquad \varphi_j = \begin{cases} \gamma_j & \text{if } j\text{-th bit of } i \text{ is } 1 \\ (\boxminus \gamma_j) & \text{otherwise} \end{cases}$$

Let $K \subseteq \{0,1\}^k$ be such that δ_i is a dEQPL consistent formula and let $\gamma_\theta = \bigsqcup_{i \in K} \delta_i$. Observe that $\Vdash_{\mathsf{dEQPL}} \gamma_\theta$ and that for each $|\psi\rangle, \rho$ there exists a unique $i \in K$ such that $|\psi\rangle, \rho \Vdash_{\mathsf{dEQPL}} \delta_i$. Given a LTL model $\mathcal{K} = (S, R, L)$ of $(\mathsf{G}(\widetilde{\gamma}_\theta) \sqcap \widetilde{\theta})$ and a path π starting at $s \in S$ we denote by $(|\psi_s\rangle, \rho_s)$ a dEQPL model that satisfies δ_i whenever $\mathcal{K}, \pi \Vdash_{\mathsf{CTL}} \widetilde{\delta}_i$. Moreover, choose $(|\psi_s\rangle, \rho_s) \neq (|\psi_{s'}\rangle, \rho_{s'})$ whenever $s \neq s'$ (this can be done just by changing the assignments of variables not occurring in θ). We denote by $\mathcal{T}_{\mathcal{K}}$ the quantum Kripke structure $(S_{\mathcal{K}}, R_{\mathcal{K}})$ where $S_{\mathcal{K}} = \{(|\psi_s\rangle, \rho_s) : s \in S\}$ and $((|\psi_s\rangle, \rho_s), (|\psi_{s'}\rangle, \rho_{s'})) \in R_{\mathcal{K}}$ iff $(s, s') \in R$. Finally, given a computation path $\pi = s_1, \ldots$ in $\mathcal{K}$ we denote by π_K the computation path $(|\psi_{s_1}\rangle, \rho_{s_1}), \ldots$ in $\mathcal{T}_{\mathcal{K}}$.

The following theorem is the kernel of the QLTL SAT algorithm.

Theorem 4.8 *Let θ be a QLTL formula. Then, $(\mathsf{G}(\widetilde{\gamma}_\theta) \sqcap \widetilde{\theta})$ is LTL-satisfiable iff θ is QLTL-satisfiable. Moreover, $\mathcal{K}, \pi \Vdash_{\mathsf{CTL}} (\mathsf{G}(\widetilde{\gamma}_\theta) \sqcap \widetilde{\theta})$ iff $\mathcal{T}_{\mathcal{K}}, \pi_{\mathcal{K}} \Vdash_{\mathsf{QLTL}} \theta$.*

Proof: $\Leftarrow$) Follows directly from Lemma 4.3 and from the fact that $\Vdash_{\mathsf{dEQPL}} \gamma_\theta$. Concerning the second assertion, it follows by noticing that $\widetilde{\mathcal{T}_{\mathcal{K}}}$ is equal to $\mathcal{K}$ up to relabeling of states.

$\Rightarrow$) For this direction, it is sufficient to show the second assertion. Since $\widetilde{\mathcal{T}_{\mathcal{K}}}$ is equal to $\mathcal{K}$ up to relabeling of states, by Lemma 4.3 we have that $\mathcal{T}_{\mathcal{K}}, \pi_{\mathcal{K}} \Vdash_{\mathsf{QLTL}} \mathsf{G}(\gamma_\theta) \sqcap \theta$ and therefore $\mathcal{T}_{\mathcal{K}}, \pi_{\mathcal{K}} \Vdash_{\mathsf{QLTL}} \theta$. ◇

We are now able to show the SAT algorithm for QLTL.

Table 16: Algorithm to determine $Sat(\theta)$

1) Generate δ_i for all $i \in 2^k$ where k is number of atomic dEQPL formulas that are atoms of θ.

2) Using the SAT algorithm for dEQPL compute the set of indexes K
such that $i \in K$ iff δ_i is a consistent dEQPL formula,
in this case store the dEQPL model output by the SAT algorithm
and call it $(|\psi_i\rangle, \rho_i)$.

3) Find a model $\mathcal{K}$ for $(\mathsf{G}(\widetilde{\gamma}_\theta) \sqcap \widetilde{\theta})$ using the LTL SAT algorithm.

4) Construct $\mathcal{T}_{\mathcal{K}}$ from the models stored in 2).

4.5 Model-checking problem

In contrast to the case of QCTL, we will give a model-checking algorithm for QLTL that uses directly the PSPACE model-checking algorithm for LTL. This make the problem more or less trivial thanks to Lemma 4.3. Given the QLTL formula θ and a quantum Kripke structure $\mathcal{T}$, we start by transforming $\mathcal{T}$ into a classical Kripke structure $\widetilde{\mathcal{T}}$ by checking whether the quantum states in $\mathcal{T}$ satisfy or not the quantum atoms in θ. Then, it remains to model check $\widetilde{\mathcal{T}}$ against $\widetilde{\theta}$. Clearly, the model-checking procedure is still in PSPACE, since the translation of $\mathcal{T}$ into $\widetilde{\mathcal{T}}$ can be done in polynomial space. We formalize the algorithm in Table 17.

Table 17: Algorithm to determine $Sat_{\mathcal{T}}(\theta)$

1) Construct $\widetilde{\mathcal{T}}$ by checking whether the quantum states in $\mathcal{T}$
satisfy or not the quantum atoms in θ.

2) Model-check $\widetilde{\mathcal{T}}$ against $\widetilde{\theta}$ using a LTL model-checker.

5 Conclusions

We presented temporal quantum logics combining the quantum state logic given in [12] with the computational tree logic CTL and linear temporal logic LTL. We were able to obtain a complete calculus, and provide a SAT and model-checking algorithm.

The main idea behind the temporalization of dEQPL was to replace the propositional symbols of the temporal logics by the atomic formulas of dEQPL. This approach is expressive enough to reason about quantum protocols (see for instance [5]) and has the great advantage that is endowed with a complete Hilbert calculus.

On the other hand, the SAT algorithms of the temporal quantum logics have prohibitive complexity. For the case of QCTL, we need to apply the CTL Exptime SAT algorithm to a CTL formula that has grown exponentially, obtaining therefore a double-exponential time upper-bound. In the case of LTL, from the PSPACE SAT algorithm of LTL, we obtain a EXPSPACE upper-bound. Moreover, in both cases we also need to apply an exponential number of times the SAT algorithm for EPPL, for which we gave an double-exponential time upper-bound over the number of qubits. For all these reasons, the SAT results presented here have more a theoretical value than a practical one. It is possible to find better upper-bounds for the algorithms by exploring the particularities of quantum Kripke structures, but the authors believe that the improved algorithms, alone, would never be usable in practice.

Concerning model checking, the results are more positive. Actually, if one considers floating-point representation, the complexity upper-bounds obtained for QCTL and QLTL are precisely the same of those for CTL and LTL, respectively. Thus, the model-checking algorithms can be used in practice.

There is still much work to be done along this research line. From the state logic point of view, an interesting improvement would be to consider density operators instead of unit vectors, thus giving a global phase independent semantics. In what concerns temporalization, it would be interesting to have a quantum version of the full branching time logic CTL^* and of the μ-calculus. Finally, and from the semantics point of view, it would be interesting to have a more refined notion of quantum Kripke structure, one that would mimic closer the evolution of a quantum system.

Acknowledgments

This work was partially supported by FCT and EU FEDER, namely via CLC POCTI (Research Unit 1-601), QuantLog project POCI/MAT/55796/2004, SQIG - IT, QSEC project PTDC/EIA/67661/2006 and KLOG project PTDC/MAT/-68723/2006.

References

[1] S. Abramsky and B. Coecke. A categorical semantics of quantum protocols. In *Proceedings of the 19th Annual IEEE Symposium on Logic in Computer Science (LICS 2004)*, pages 415–425. IEEE Computer Science Press, 2004.

[2] T. Altenkirch and J. Grattage. A functional quantum programming language. In *Proceedings of the 20th Annual IEEE Symposium on Logic in Computer Science (LICS)*, pages 249–258. IEEE Computer Society, 2005.

[3] A. Baltag and S. Smets. LQP: The dynamic logic of quantum information. *Mathematical Structures in Computer Science*, 2006. To appear.

[4] P. Baltazar, R. Chadha, and P. Mateus. Quantum computation tree logic – model checking and complete calculus. *International Journal of Quantum Information*, 6(2):281–302, 2008.

[5] P. Baltazar, R. Chadha, P. Mateus, and A. Sernadas. Towards model-checking quantum security protocols. In P. Dini et al, editor, *Proceedings of the First Workshop on Quantum Security: QSec'07*, page 0014. IEEE Press, 2007. Joint e-proceedings with Quantum, Nano, and Micro Technologies: ICQNM '07. 6 pages.

[6] P. Baltazar and P. Mateus. Temporalization of probabilistic propositional logic. In *Logic Foundations of Computer Science 2009*, Lecture Notes in Computer Science. Springer, In print.

[7] S. Basu, R. Pollack, and R. Marie-Françoise. *Algorithms in Real Algebraic Geometry.* Springer, 2003.

[8] C. Caleiro, P. Mateus, A. Sernadas, and C. Sernadas. Quantum institutions. In K. Futatsugi, J.-P. Jouannaud, and J. Meseguer, editors, *Algebra, Meaning, and Computation – Essays Dedicated to Joseph A. Goguen on the Occasion of His 65th Birthday*, volume 4060 of *Lecture Notes in Computer Science*, pages 50–64. Springer-Verlag, 2006.

[9] C. Caleiro, C. Sernadas, and A. Sernadas. Parameterisation of logics. In J. Fiadeiro, editor, *Recent Trends in Algebraic Development Techniques - Selected Papers*, volume 1589 of *Lecture Notes in Computer Science*, pages 48–62. Springer-Verlag, 1999.

[10] R. Chadha, L. Cruz-Filipe, P. Mateus, and A. Sernadas. Reasoning about probabilistic sequential programs. *Theoretical Computer Science*, 379(1-2):142–165, 2007.

[11] R. Chadha, P. Mateus, and A. Sernadas. Reasoning about quantum imperative programs. *Electronic Notes in Theoretical Computer Science*, 158:19–40, 2006. Invited talk at the Twenty-second Conference on the Mathematical Foundations of Programming Semantics.

[12] R. Chadha, P. Mateus, A. Sernadas, and C. Sernadas. Extending classical logic for reasoning about quantum systems. In D. Gabbay K. Engesser and D. Lehmann, editors, *Handbook of Quantum Logic and Quantum Structures: Quantum Logic*, pages 325–372. Elsevier, 2009.

[13] E. M. Clarke and E. A. Emerson. Design and synthesis of synchronization skeletons using branching time temporal logics. In *Proceeding of the Workshop on Logics of Programs*, volume 131 of *LNCS*. Springer-Verlag, 1981.

[14] E. M. Clarke and J. M. Wing. Formal methods: state of the art and future directions. *ACM Comput. Surv.*, 28(4):626–643, 1996.

[15] Edmund M. Clarke and Bernd-Holger Schlingloff. Model checking. In *Handbook of Automated Reasoning*, pages 1635–1790. 2001.

[16] E. D'Hondt and P. Panangaden. Quantum weakest preconditions. In Peter Selinger, editor, *Proceedings of the 2nd International Workshop on Quantum Programming Languages*, number 33 in TUCS General Publications, pages 75–90. Turku Centre for Computer Science, 2004.

[17] R. Fagin, J. Y. Halpern, and N. Megiddo. A logic for reasoning about probabilities. *Information and Computation*, 87(1-2):78–128, 1990.

[18] D. Gabbay, A. Pnueli, S. Shelah, and J. Stavi. The temporal analysis of fairness. In *Proceedings 7th Symp. on Principles of Programming Languages, POPL'80*, pages 163–173. ACM, 1980.

[19] E. Knill. Conventions for quantum pseudocode. Technical Report LAUR-96-2724, Los Alamos National Laboratory, 1996.

[20] P. Mateus and A. Sernadas. Weakly complete axiomatization of exogenous quantum propositional logic. *Information and Computation*, 204(5):771–794, 2006.

[21] P. Mateus, A. Sernadas, and C. Sernadas. Exogenous semantics approach to enriching logics. In G. Sica, editor, *Essays on the Foundations of Mathematics and Logic*, volume 1 of *Advanced Studies in Mathematics and Logic*, pages 165–194. Polimetrica, 2005.

[22] C. Meadows. Formal methods for cryptographic protocol analysis: emerging issues and trends. *IEEE Journal on Selected Areas in Communications*, 21(1):44– 54, 2003.

[23] P. Naur. Revised report on the algorithmic language Algol 60. *The Computer Journal*, 5:349–367, 1963.

[24] J. W. Sanders and P. Zuliani. Quantum programming. In *Mathematics of Program Construction*, volume 1837 of *Lecture Notes in Computer Science*, pages 80–99. Springer, 2000.

[25] P. Selinger and B. Valiron. A lambda calculus for quantum computation with classical control. In *Proceedings of the 7th International Conference on Typed Lambda Calculi and Applications (TLCA)*, volume 3461 of *Lecture Notes in Computer Science*, pages 354–368. Springer, 2005.

[26] A. P. Sistla and E. M. Clarke. The complexity of propositional linear temporal logics. *Journal of ACM*, 32(3):733–749, 1985.

[27] R. van der Meyden and M. Patra. Knowledge in quantum systems. In M. Tennenholtz, editor, *Theoretical Aspects of Rationality and Knowledge*, pages 104–117. ACM, 2003.

[28] R. van der Meyden and M. Patra. A logic for probability in quantum systems. In M. Baaz and J. A. Makowsky, editors, *Computer Science Logic*, volume 2803 of *Lecture Notes in Computer Science*, pages 427–440. Springer-Verlag, 2003.