Extending classical logic for reasoning about quantum systems

R. Chadha* P. Mateus A. Sernadas C. Sernadas
Department of Mathematics, IST, TU Lisbon
SQIG, Instituto de Telecomunicações
{rchadha,pmat,acs,css}@math.ist.utl.pt

February 26, 2008

Abstract

A decidable logic extending classical reasoning and supporting quantum reasoning is presented. The quantum logic is obtained by applying the exogenous semantics approach to propositional logic. The design is guided by the postulates of quantum mechanics and inspired by applications in quantum computation and information. The models of the quantum logic are superpositions of classical valuations. In order to achieve decidability, the superpositions are taken in inner product spaces over algebraic closures of arbitrary real closed fields.

1 Introduction

A new logic EQPL (exogenous quantum propositional logic) was proposed in [26, 27, 28] for modeling and reasoning about quantum systems, embodying all that is stated in the relevant Postulates of quantum physics (as presented, for instance, in [15, 31]). The logic was designed from the semantics upwards, starting with the key idea of adopting superpositions of classical models as the models of the proposed quantum logic.

This novel approach to quantum reasoning is different from the mainstream approach [19, 14]. The latter, as initially proposed by Birkhoff and von Neumann [8], focuses on the lattice of closed subspaces of a Hilbert space and replaces the classical connectives by new connectives representing the lattice-theoretic operations. The former adopts superpositions of classical models as the models of the quantum logic, leading to a natural extension of the classical language containing the classical connectives (just as modal languages are extensions of the classical language). Furthermore, EQPL allows quantitative reasoning about amplitudes and probabilities, being in this respect much closer to the possible worlds logics for probability reasoning than to the mainstream quantum logics. Finally, EQPL is designed to reason about finite collections of qubits and, therefore, it is suitable for applications in quantum computation

*Now at University of Illinois at Urbana-Champaign.

and information. The models of EQPL are superpositions of classical valuations that correspond to unit vectors expressed in the computational basis of the Hilbert space resulting from the tensor product of the independent qubit systems.

Therefore, in EQPL we can express a wide range of properties of states of such a finite collection of qubits. For example, we can impose that some qubits are independent of (that is, not entangled with) other qubits; we can prescribe the amplitudes of a specific quantum state; we can assert the probability of a classical outcome after a projective measurement over the computational basis; and, we can also impose classical constraints on the admissible quantum states.

Herein, we concentrate on presenting a decidable fragment of EQPL by suitably relaxing the semantic structures of EQPL. Instead of considering Hilbert spaces we work with inner product spaces over an arbitrary real closed field and its algebraic closure. The decidability results from the fact that the first order theory of such fields is decidable [24, 6]. This technique was inspired by related work on probabilistic logic [1]. Furthermore, the decidable fragment of EQPL so established turns out to be strongly complete although we concentrate on weak completeness. The price we have to pay for decidability is a weak arithmetic language – we loose the analytic aspects of complex numbers.

The exogenous approach to extending a given logic is discussed and illustrated in Section 2. Section 3 presents dEQPL step by step: design options, models, language and its interpretation, sound axiomatization, and some useful metatheorems. In Section 4 we show that dEQPL is weakly complete and decidable. The proof of weak completeness can easily be adapted to a proof of strong completeness but we refrained to do so since our primary interest is in applications involving finitely presented theories. We illustrate the use of dEQPL with two worked examples in Section 5. First we reason about a Bell state. Afterwards, we reason about the quantum teleportation protocol proposed in [7]. Finally, in Section 6 we assess what was achieved and provide an outlook of further developments of the proposed approach to quantum reasoning.

2 Exogenous approach

The exogenous semantics approach to enriching a given logic roughly consists of taking as models of the new logic sets of models of the original logic, possibly together with some additional structure. This general mechanism for building new logics is described in detail in [29, 9]. The first example of the approach appeared in the context of probabilistic logics [32, 33], although by then not yet recognized as a general construction.

The adjective "exogenous" is used as a counterpoint to "endogenous". For instance, in order to enrich some given logic with probabilistic reasoning it may be convenient to tinker with the models of the original logic. This endogenous approach has been used extensively. For example, the domains of first-order structures are endowed with probability measures in [21]. Other examples include labeling the accessibility pairs with probabilities in the case of Kripke structures [22] for reasoning about probabilistic transition systems.

By not tinkering with the original models and only adding some additional structure on collections of those models as they are, the exogenous approach has the potential for providing general mechanisms for enriching a given logic with some additional reasoning dimension. As we shall see, in our case the exogenous approach has the advantage of closely guiding the design of the language around the underlying concepts of quantum physics while keeping the classical connectives.

The exogenous approach of collecting the original models as proposed in [26, 27] is inspired by the possible worlds semantics of modal logic [25]. It is also akin to the society semantics for many-valued logic [12] and to the possible translations semantics for paraconsistent logic [11]. The possible worlds approach also plays a role in probabilistic logic [32, 33, 5, 4, 18, 1, 13].

As an introductory example of the exogenous approach, we briefly explain how a probabilistic logic can be obtained from classical propositional logic, following closely [29]. Since quantum reasoning subsumes probabilistic reasoning, this example will also be useful for our purposes. However, before we proceed to explain the probabilistic logic, we first concentrate on a fragment of the probabilistic logic called *global propositional logic*. Global logic is also a fragment of the quantum logic proposed in this paper.

We start by taking a set Π of propositional symbols. From a semantic point of view, the models of global logic are sets of valuations over Π. The language of global logic consists of:

- Classical propositional formulas constructed from Π using the classical connectives $\bot$ and $\Rightarrow$.
- Global formulas constructed from the classical propositional formulas by the global connectives $\perp\!\!\!\perp$ and $\sqsupset$. The global connectives mimic the classical connectives in a sense which we will make precise shortly.

The satisfaction relation between the semantic models and the formulas is as follows. A model V (V is some set of "classical" valuations) of the global logic satisfies a classical propositional formula α if every classical valuation $v \in V$ satisfies α. Therefore, any classical tautology is a global tautology.

Analogous to the case of classical logic, a global valuation V satisfies the global formula $\gamma_1 \sqsupset \gamma_2$ if either V satisfies γ_2 or V does not satisfy γ_1. The global connective $\perp\!\!\!\perp$ is never satisfied. Clearly this is a copy of the classical propositional logic and indeed, if we replace the classical connectives in a classical tautology by their global counterparts we will get a global tautology.

As we just saw, there are two copies of the classical propositional logic in the global logic. A natural question to ask is whether the two copies are necessarily distinct. The answer is yes and while the connectives $\bot$ and $\perp\!\!\!\perp$ collapse, it is not the case with the two implications. However, there is a relation between those two and if V satisfies $\alpha_1 \Rightarrow \alpha_2$ then V also satisfies $\alpha_1 \sqsupset \alpha_2$. The reverse does not hold in general.

There is a sound and strongly complete axiomatization for global logic which contains five axiom schemas and an inference rule. One axiom schema says that every classical tautology is a global tautology while the other says that replacing

classical connectives by their global counterparts results in a global tautology. One axiom identifies $\bot$ and $\between$, a second one axiomatizes the relation between the two implications that we mentioned above, and the last one says that the classical and global conjunctions (global conjunction is introduced as usual) collapse. The inference rule is the global counterpart of modus ponens.

Global logic is the first step towards creating the exogenous probabilistic logic. The probabilistic logic is obtained "exogenously" by assigning probabilities to each of the classical valuations in a global valuation V. This allows us to reason about the probability that a classical propositional formula is true in V: the probability of φ is the sum of the probabilities of the valuations that satisfy φ. Given a set Π of propositional symbols, the language of the probabilistic logic consists of:

- Classical propositional formulas constructed from Π using the classical connectives $\bot$ and $\Rightarrow$.
- A set of terms that include:
  - real-valued variables and real computable numbers;
  - probability terms denoting probabilities of classical formulas; and
  - sum and product of terms.
- Comparison formulas of the form $t_1 \leq t_2$ where t_1 and t_2 are terms.
- Formulas constructed from classical propositional formulas and comparison formulas using the global connectives $\between$ and $\sqsupset$.

A model for the probabilistic logic, that is a *probabilistic valuation*, contains a global valuation along with a probability measure which assigns to each classical valuation a real value between 0 and 1. As explained, this gives us an interpretation of the probability terms in the language. The satisfaction of classical formulas is the same as in the global logic. Observe that if V satisfies a classical formula α then the probability of α being true is 1 regardless of the probability measure on V. Hence, the probability of a classical tautology in any model is always 1.

In order to interpret the variables, the model also contains an assignment of variables to real numbers. This helps to interpret the terms and the comparison formulas in the natural way. The interpretation of the global connectives is the same as before.

An axiomatization of probabilistic logic is obtained by extending the axiomatization for global logic as follows. The connection between the classical connectives and probability terms is obtained by three axioms:

1. The probability of any classical tautology is 1.
2. If the probability of the classical formula $\alpha_1 \wedge \alpha_2$ is 0 then the probability of $\alpha_1 \vee \alpha_2$ is the sum of the probabilities of α_1 and α_2. This is the finite additivity of probability measures.

3. If the probability of the classical formula $\alpha_1 \Rightarrow \alpha_2$ is 1 then the probability of α_1 is less than the probability of α_2. This is the monotonicity property of probability measures.

For the comparison formulas, an oracle is used which gives the valid comparison formulas. The axiomatization is sound and *weakly* complete modulo the oracle. However, even with the oracle strong completeness fails as the logic is not compact.

The development of the exogenous quantum logic herein follows the same lines as the development of the probabilistic one. Instead of assigning probabilities, we assign amplitudes to the classical valuations in a global valuation. The classical valuations themselves represent the computational basis of the qubits in a quantum system. In fact, we are only interested in quantum systems composed of a finite number of qubits since applications in quantum computation and information only deal with such systems. A superposition of these classical valuations will then give the state of the quantum system. We will explicitly have terms in the language to interpret these amplitudes and they will be at the core of the design of our language. We postpone the detailed discussion of the language and the logic to Section 3. The resulting quantum logic is a decidable fragment of the logic in [28].

These quantum logics obtained using the exogenous approach are philosophically closer to some probabilistic logics (like [18, 1]) than to the mainstream quantum logics in the tradition of Birkhoff and von Neumann [8, 19, 14]. Both types of quantum logic are motivated by semantic considerations, albeit very different ones. The mainstream quantum logics are based on the idea of replacing the Boolean algebras of truth values by the more relaxed notion of orthomodular lattices. Thus, they end up with non classical connectives reflecting the properties of meets and joins of those lattices. The exogenous quantum logics are based on the idea of replacing classical valuations by superpositions of classical valuations while preserving the classical connectives. On the other hand, in both types of quantum logic a formula and a propositional symbol in particular denotes a subspace of the Hilbert space at hand. However, in the exogenous quantum logics a quantum system is assumed to be composed of n qubits and, hence, the underlying Hilbert space has dimension 2^n.

Our semantics of quantum logic, although inspired by modal logic, is also completely different from the alternative Kripke semantics given to mainstream quantum logics (as first proposed in [16]). That Kripke semantics is based on orthomodular lattices.

The quantum logic proposed in [36, 35, 34] is also inspired by probabilistic logics [18] and capitalizes on some techniques first proposed for those logics, but it has aspects of both mainstream quantum logics and exogenous quantum logics. In short, it is a classical logic of probabilistic measurements over a quantum system where quantum formulas denote projectors, quantum negation stands for orthogonal complement and quantum conjunction stands for composition. Note also that no amplitude terms appear in [36, 35] contrarily to exogenous quantum logics where amplitudes replace probabilities as the central concept.

The tensor product plays a key role in the exogenous quantum logics as it

does in the categorical semantics proposed in [2, 3]. However, in our logics we still use the concrete characterization of tensor product of qubits (represented in our language by the propositional symbols).

3 Decidable fragment of EQPL

We start by discussing design issues, and then proceed to introduce the logic.

3.1 Design issues

In this section, we shall discuss how the Postulates of quantum mechanics [15] guided the design of the proposed logic, and give a brief introduction to the relevant concepts and results. The first Postulate of quantum mechanics states:

Postulate 1: *Every isolated quantum system is described by a Hilbert space. The states of the quantum system are the unit vectors of the corresponding Hilbert space.*

Please recall that a Hilbert space is a complete inner product space over $\mathbb{C}$ (the field of complex numbers). In quantum computation and information the quantum systems are composed of qubits. For example, the states of an isolated qubit are vectors of the form $z_0|0\rangle + z_1|1\rangle$ where $z_0, z_1 \in \mathbb{C}$ and $|z_0|^2 + |z_1|^2 = 1$. In other words, they are unit vectors in the (unique up to isomorphism) Hilbert space of dimension two. As pointed out in the introduction, instead of working with a Hilbert space we shall consider a "generalized" inner product space over the algebraic closure of an arbitrary *real closed field*. This design decision has the advantage that the resulting logic is decidable. It is possible to work with Hilbert spaces and still get a weakly-complete calculus as was the case in EQPL [28], a previous version of the logic developed herein. Indeed, the logic defined here identifies a decidable fragment of EQPL, and hence we shall call it dEQPL. In addition to being decidable, dEQPL turns out to be strongly complete and, therefore, compact. In fact, the source of the non compactness of EQPL mentioned in [28] was in its arithmetic component.

We shall now briefly review some definitions and results concerning real closed fields and their algebraic closures.

Definition 3.1 (Real closed fields) An ordered field $\mathcal{K} = (K, +, ., 1, 0, \leq)$ is said to be a real closed field if the following hold:

- Every non-negative element of the K has a square root in K.
- Any polynomial of odd degree with coefficients in K has at least one solution in K.

We shall use $\mathcal{K}_1, \mathcal{K}_2, \ldots$ to range over real closed fields and $k_1, k_2, \ldots$ to range over the elements of a real closed field. The set of real numbers with the usual multiplication, addition and order constitute a real closed field. The set

of computable real numbers with the same operations is another example of a real closed field.

The *algebraic closure* of a real closed field $\mathcal{K} = (K, +, \times, 1, 0, \leq)$ is obtained by adjoining an element δ to $\mathcal{K}$ such $\delta^2 + 1 = 0$. The algebraic closure, denoted by $\mathcal{K}(\delta)$, is a two-dimensional vector space over $\mathcal{K}$. Each element in $\mathcal{K}(\delta)$ is of the form $k_1 + k_2\delta$ where $k_1, k_2 \in K$. The addition and multiplication are defined as:

$$\begin{array}{lcl} (k_1 + k_2\ \delta) + (k_1' + k_2'\ \delta) & = & (k_1 + k_1'\ \delta) + (k_2 + k_2'\ \delta) \\ (k_1 + k_2\ \delta).(k_1' + k_2'\ \delta) & = & (k_1.k_1' - k_2.k_2') + (k_1.k_2' + k_1'.k_2\delta) \\ & & \text{where } -k_2.k_2' \text{ is the additive inverse of } k_2.k_2' \end{array}$$

We shall use $c_1, c_2, \ldots$ to range over the elements of $\mathcal{K}(\delta)$. For example, the field of complex numbers is the algebraic closure of the set of real numbers with $\delta = i$. The standard notion of conjugation, absolute value and real and imaginary parts from complex numbers can be generalized to $\mathcal{K}(\delta)$ as follows:

$$\begin{array}{lcl} Re(k_1 + k_2\ \delta) & = & k_1 \\ Im(k_1 + k_2\ \delta) & = & k_2 \\ |k_1 + k_2\ \delta| & = & k_1^2 + k_2^2 \\ \overline{k_1 + k_2\delta} & = & k_1 + (-k_2)\delta \text{ where } -k_2 \text{ is the additive inverse of } k_2 \end{array}$$

The conjugation allows us to generalize the notion of inner product and normed vector space over $\mathbb{C}$ to an arbitrary $\mathcal{K}(\delta)$ as follows:

Definition 3.2 ($\mathcal{K}(\delta)$-inner product space) A $\mathcal{K}(\delta)$-*inner product space* is a vector space W over the field $\mathcal{K}(\delta)$ together with a map

$$\langle \cdot, \cdot \rangle : W \times W \to \mathcal{K}(\delta)$$

such that for all $w, w_1, w_2 \in V$ and $k \in \mathcal{K}(\delta)$, the following hold:

1. $\langle w, w_1 + w_2 \rangle = \langle w, w_1 \rangle + \langle w, w_2 \rangle$.
2. $\langle w, w \rangle \in \mathcal{K}$ and $\langle w, w \rangle \geq 0$.
3. $\langle w, w \rangle = 0$ if and only if $w = 0$.
4. $\langle w_1, w_2 \rangle = \overline{\langle w_2, w_1 \rangle}$.
5. $\langle w_1, cw_2 \rangle = c\langle w_1, w_2 \rangle$.

Definition 3.3 ($\mathcal{K}(\delta)$-normed vector space) A $\mathcal{K}(\delta)$-*normed space* is a vector space W over the field $\mathcal{K}(\delta)$ together with a map

$$||.|| : W \times W \to \mathcal{K}$$

such that for all $w, w_1, w_2 \in V$ and $k \in \mathcal{K}$, the following hold

1. $||w|| \geq 0$.

2. $||w|| = 0$ if and only if $w = 0$.

3. $||cw|| = |c|||w||$ where $|c|$ is the absolute value of c.

4. $||w_1 + w_2|| \leq ||w_1|| + ||w_2||$.

We shall say that a vector w is a *unit vector* if $||w|| = 1$.

As in the case of inner product spaces over complex numbers, a $\mathcal{K}(\delta)-$inner product space $(W, \langle \cdot, \cdot \rangle)$ gives rise to a norm by letting:

$$||w|| = \sqrt{\langle w, w \rangle}.$$

For example, the field $\mathcal{K}(\delta)$ together with the map: $\langle c_1, c_2 \rangle = c_1.\overline{c_2}$ is itself a $\mathcal{K}(\delta)-$inner product space. In this case, the resulting norm ($||c|| = \sqrt{c.\overline{c}}$) is the absolute value function.

Any Hilbert space is a C-inner product space. However, we shall model quantum systems as $\mathcal{K}(\delta)-$inner product spaces instead of Hilbert spaces, and the field $\mathcal{K}(\delta)$ will be a part of our semantic structure. Therefore, any theorem we prove in the logic would remain valid if we had just used Hilbert spaces.

It is also worthwhile to point out that, unlike Hilbert spaces, $\mathcal{K}(\delta)-$inner product spaces in general may not have an analytical structure. So, we will not be able to express properties that necessarily depend upon the analytical structure[1].

Moreover, as the logic is intended to be applied for quantum computation and information, we shall work only with a special kind of $\mathcal{K}(\delta)-$inner product spaces that are defined by free construction from finite sets:

Definition 3.4 (Free $\mathcal{K}(\delta)$-inner product space) Given an arbitrary finite set $\mathcal{B}$, we can construct the free $\mathcal{K}(\delta)$-inner product space $\mathcal{H}_{\mathcal{K}(\delta)}(\mathcal{B})$ as:

- Each element of $\mathcal{H}_{\mathcal{K}(\delta)}(\mathcal{B})$ is a map $|\psi\rangle : \mathcal{B} \to \mathcal{K}(\delta)$.
- $|\psi_1\rangle + |\psi_2\rangle$ is pointwise addition, *i.e.*,

$$(|\psi_1\rangle + |\psi_2\rangle)(b) = |\psi_1\rangle(b) + |\psi_2\rangle(b).$$

- $c|\psi\rangle$ is pointwise scalar multiplication, *i.e.*,

$$(c|\psi\rangle)(b) = c\,(|\psi\rangle(b)).$$

- The inner product is given by[2]

$$\langle \psi_1 | \psi_2 \rangle = \sum_{b \in \mathcal{B}} \overline{|\psi_1\rangle(b)}\, |\psi_2\rangle(b).$$

[1] For example, we cannot define the exponential function on an arbitrary $\mathcal{K}(\delta)$.

[2] We adopt here the Dirac notation, given its widespread use by the community of quantum physics and computation.

The dimension of the vector space $\mathcal{H}_{\mathcal{K}(\delta)}(\mathcal{B})$ is the cardinality of the set $\mathcal{B}$. Given $b \in \mathcal{B}$, let $|b\rangle \in \mathcal{H}_{\mathcal{K}(\delta)}(\mathcal{B})$ be the vector defined as

$$|b\rangle(b) = 1 \text{ and } |b\rangle(b_1) = 0 \text{ for every } b_1 \neq b.$$

It can be easily checked that the set $\{|b\rangle : b \in \mathcal{B}\}$ forms a basis of the vector space $\mathcal{H}_{\mathcal{K}(\delta)}(\mathcal{B})$. Furthermore, it is the case that $\langle b|b\rangle = 1$ and $\langle b|b_1\rangle = 0$ for every $b \neq b_1$. For obvious reasons, we say that $\{|b\rangle : b \in \mathcal{B}\}$ is an *orthonormal basis* of $\mathcal{H}_{\mathcal{K}(\delta)}(\mathcal{B})$. This basis plays an important role in the semantics of dEQPL and for this reason we will henceforth refer to it as being the *canonical basis* of $\mathcal{H}_{\mathcal{K}(\delta)}$.

A natural question that arises in this context is how do we choose $\mathcal{B}$. The answer lies in our interest in quantum systems composed of qubits. As mentioned before, the states of an isolated qubit are vectors of the form $z_0|0\rangle + z_1|1\rangle$ where $z_0, z_1 \in \mathbb{C}$ and $|z_0|^2 + |z_1|^2 = 1$. The set of states can be identified with (upto isomorphism) the unit vectors in the free $\mathbb{C}$-inner product $\mathcal{H}_{\mathbb{C}}(\mathcal{B})$ where $\mathcal{B}$ is an set of 2 elements. Keeping this is mind, it is natural to represent a qubit by a propositional symbol (henceforth called a qubit symbol) and take $\mathcal{B}$ in this case to be the set of two possible classical valuations of the qubit symbol: 0 that assigns false to the qubit symbol and 1 that assigns true to it.

Similarly, the states of a isolated *pair* of qubits are of the form $z_{00}|00\rangle + z_{01}|01\rangle + z_{10}|10\rangle + z_{11}|11\rangle$, where $z_{00}, z_{10}, z_{01}, z_{11} \in \mathbb{C}$ and $|z_{00}|^2 + |z_{01}|^2 + |z_{10}|^2 + |z_{11}|^2 = 1$. The set of states in this case can be identified with the unit vectors in the free $\mathbb{C}$-inner product $\mathcal{H}_{\mathbb{C}}(\mathcal{B})$ where $\mathcal{B}$ is the set of the four classical valuations over the pair of qubit symbols representing the two qubits at hand.

The pattern becomes clear, and in general, we will fix a *finite* set of qubit symbols [3]:

$$\mathsf{qB} = \{\mathsf{qb}_k : 0 < k \leq n\}.$$

These will represent the n qubits in our system. As we need to work with the algebraic closure of arbitrary real closed fields, the states in our systems will be unit vectors in the free $\mathcal{K}(\delta)$-inner product space $\mathcal{H}_{\mathcal{K}(\delta)}(2^{\mathsf{qB}})$, where 2^{qB} is the set of 2^n possible *classical valuations* of the n qubit symbols. We shall call these unit vectors $\mathcal{K}(\delta)$-*quantum valuations* over the set qB.

Another characteristic of quantum systems that we are likely to encounter in applications in computation and information is that they will be built from independent sub-systems. We shall model the sub-systems by partitioning the set qB, and a semantic structure will contain this partition. Each member of the partition, henceforth called a *component*, will then model the qubits of an independent sub-system.

If $A \subseteq \mathsf{qB}$ is a component, then the states of the A sub-system will be quantum valuations over A, *i.e.*, unit vectors in $\mathcal{H}_{\mathcal{K}(\delta)}(2^A)$. If S is the partition, then the semantic structure also includes a collection $\{|\varphi\rangle_A : A \in S\}$, where $|\varphi\rangle_A$ is a quantum valuation over A. These represent the states of the sub-systems.

[3] In [28], the set of qubits was infinite. However, the set was restricted when judgments were considered.

In addition to reasoning about component sub-systems, we also need to reason about bigger sub-systems. The sets of qubits of bigger sub-systems are given by union of qubits of the component sub-systems. Therefore, given a partition S of qB, we define Alg(S) $= \{\cup_i A_i : A_i \in S\}$. A member $F \in$ Alg(S) models the qubits of the component systems. It is easy to see that Alg(S) satisfies the following properties[4]:

1. $\emptyset,\ \mathsf{qB} \in S$.
2. $G \in S$ implies that $\mathsf{qB} \setminus G \in S$.
3. $G_1, G_2 \in S$ implies that $G_1 \cup G_2 \in S$

We also need a way to construct the states of sub-systems from smaller ones. For this, we take recourse to the second Postulate of quantum mechanics:

Postulate 2: *The Hilbert space of a quantum system composed of a finite number of independent components is the tensor product of the component Hilbert spaces.*

Therefore, for instance, the state of a sub-system composed of two independent sub-systems is the "tensor product" of the states of the sub-system. Of course, we remember that we are not working with Hilbert spaces. Therefore, we need a definition of a $\mathcal{K}(\delta)$-tensor product. For this, we will assume that the reader is familiar with tensor products of vector spaces. Given two vector $(K)(\delta)$ vector spaces W_1 and W_2, we shall denote the tensor product by $W_1 \otimes W_2$. Please recall that the vector space $W_1 \otimes W_2$ is generated by vectors of form $w_1 \otimes w_2$ where $w_1 \in W_1$ and $w_2 \in W_2$. We are ready to define $\mathcal{K}(\delta)$-tensor products:

Definition 3.5 ($\mathcal{K}(\delta)$-tensor product) The tensor product of two $\mathcal{K}(\delta)$-inner product spaces $(W_1, \langle\cdot,\cdot\rangle_1)$ and $(W_2, \langle\cdot,\cdot\rangle_2)$, is the pair $(W_1 \otimes W_2, \langle\cdot,\cdot\rangle)$, where $\langle\cdot,\cdot\rangle$ is defined as:

$$\langle \sum_i a_i\, v_i \otimes w_i\ ,\ \sum_j b_j\, v'_j \otimes w'_j \rangle\ =\ \sum_{i,j} a_i \overline{b_j}\, \langle v_i, v'_j\rangle \langle w_i, w'_j\rangle$$

Observe also that given $w \in W_1 \otimes W_2$ it is not always possible to find $w_1 \in W_1$ and $w_2 \in W_2$ such that $w = w_1 \otimes w_2$. Furthermore, when that factorization is possible it is not necessarily unique.

Please also observe that in our case, the $\mathcal{K}$-vector spaces over the set of qubits A are generated by vectors $|v\rangle$ where v is a classical valuation over A. Therefore, if S is the partition of qB in our model and $A_1, A_2 \in S$ then the sub-system composed of A_1 and A_2 will be generated by vectors of the form $|v_1\rangle \otimes |v_2\rangle$ where $v_i \in \mathcal{H}(2^{A_i})$. We will identify $|v_1\rangle \otimes |v_2\rangle$ with the vector $|v_1 v_2\rangle \in \mathcal{H}(2^{A_1 \cup A_2})$ where $v_1 v_2$ is the unique valuation that extends v_1 and v_2. Furthermore, the state of sub-system composed of A_1 and A_2 is the tensor

[4]These properties define a structure often called an algebra in probability theory.

product $\psi_{A_1} \otimes \psi_{A_2}$. (Please note that the tensor product of two unit vectors is again a unit vector.)

When given a quantum state $|\psi\rangle \in \mathcal{H}_{\mathcal{K}(\delta)}(2^{\mathsf{qB}})$ and non empty $G \subsetneq \mathsf{qB}$, we say that the qubits in G are *not entangled* with the other qubits if there are $|\psi_1\rangle \in \mathcal{H}_{\mathcal{K}(\delta)}(2^G)$ and $|\psi_2\rangle \in \mathcal{H}_{\mathcal{K}(\delta)}(2^{\mathsf{qB}\setminus G})$ such that $|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$.

Therefore, given any $G \in \mathrm{Alg(S)}$, the qubits in G are not entangled with the other qubits, thanks to the way we build the whole state of the system from the states of the components. Hence, qubits taken from any two independent components of the system are not entangled in every possible quantum state.

Please note also that (contrarily to what was adopted in [28]) we do not require that each component state be non factorisable. This relaxation of the notion of quantum structure had no impact on the entailment relation.

Another key concept in the design of our logic is the concept of logical amplitudes. Given a $\mathcal{K}(\delta)$-quantum valuation $|\psi\rangle$ and a classical valuation v, the inner product $\langle v|\psi\rangle$ is said to be the *logic amplitude* of $|\psi\rangle$ for v. As we shall see, these logical amplitudes are at the core of dEQPL. These amplitudes appear in two ways in the structure which we discuss below.

It is also sometimes convenient to work with $V \subsetneq 2^{\mathsf{qb}}$, as we may want to impose classical constraints on the quantum valuations. For example, we may want to impose $(\mathsf{qb}_1 \vee \mathsf{qb}_2)$ requiring states to have (logical) amplitude zero for every classical valuation not satisfying this classical formula. In our semantics structures, we shall therefore explicitly have a set $V \subseteq 2^{\mathsf{qB}}$ and we shall call V the *set of admissible classical valuations*. Furthermore, for any $v \notin V$, we will require that the amplitude $\langle v|\psi\rangle = 0$ where ψ is the quantum state of the full system.

Note also that every subset A of qB can be identified with a classical valuation v over qB: v assigns true to qb if and only if $\mathsf{qb} \in A$. This, of course, can be generalized. Any set $A \subset G \subset \mathsf{qB}$ can be identified with a classical valuation v_A^G over G: v_A^G assigns true to all elements of A and false to all elements of $G \setminus A$.

Finally, we also have a collection of $\mathcal{K}(\delta)$ values $\nu = \{\nu_{GA}\}_{G\subseteq\mathsf{qB},\, A\subseteq G}$ in the semantic structure. We impose that if $G \subset \mathrm{Alg(S)}$ then $\nu_{GA} = \langle v_A^G|\psi\rangle_G$ where $|\psi\rangle_G$ is the state of the sub-system composed of qubits modeled by G. In other words, they are logic amplitudes when the qubits in G constitute an independent sub-system.

It should be stressed that these values are not always physically meaningful. A term ν_{GA} is meaningful only if $G \in Alg(S)$. The others are nevertheless useful for our purposes and help to avoid partial denotation maps. We are now ready to assemble the different pieces of our semantic structure:

Definition 3.6 (Quantum structure) A *quantum structure over* qB is a tuple

$$\mathbf{w} = (\mathcal{K}, \delta, V, \mathcal{S}, |\psi\rangle, \nu)$$

where:

- $\mathcal{K}$ is a real closed field and $\mathcal{K}(\delta)$ is its algebraic closure;
- V is a nonempty subset of 2^{qB};

- $\mathcal{S}$ is a partition of qB;
- $|\psi\rangle = \{|\psi\rangle_S\}_{S\in\mathcal{S}}$ where each $|\psi\rangle_S$ is a unit vector of $\mathcal{H}_\mathcal{S}$. We extend $|\psi\rangle$ to $\mathrm{Alg}(\mathcal{S})$ as follows:
  1. $|\psi\rangle_\emptyset = 1$;
  2. $|\psi\rangle_{S_1\cup\cdots\cup S_n} = |\psi\rangle_{S_1} \otimes \cdots \otimes |\psi\rangle_{S_n}$;
- $\langle v|\psi\rangle_\mathsf{qB} = 0$ if $v \notin V$;
- $\nu : \{\nu_{GA}\}_{G\subseteq\mathsf{qB},A\subseteq G}$ where $\nu_{GA} = \langle v^G_A|\psi\rangle_G$ if $G \in \mathrm{Alg}(\mathcal{S})$. In particular, $\nu_{\emptyset\emptyset} = 1$.

The proposed quantum logic will be interpreted over these quantum structures. Obviously, we have some redundancy in the notion of quantum structure, namely, $|\psi\rangle$ can be reconstructed from ν. However, this redundancy pays off in ease of use and in clarifying the connection to quantum physics.

The first two Postulates were sufficient to guide us in the task of setting up the notion of quantum structures over which we shall be able to define the semantics of dEQPL. Now, we turn our attention to the Postulates concerning measurements of physical quantities.

Postulate 3: *Every measurable physical quantity of an isolated quantum system is described by an observable acting on its Hilbert space.*

Please recall that an observable is a Hermitian operator such that the direct sum of its eigensubspaces coincides with the underlying Hilbert space. Also recall that the *s*pectrum Ω of a Hermitian operator (set of its eigenvalues) is a subset of the set of real numbers, $\mathbb{R}$. For each $e \in \Omega$, we denote the corresponding eigensubspace by H_e, and the projector onto the subspace E_e by P_e.

It might seem at first that we need to extend the definition of Hermitian operators to an arbitrary $\mathcal{K}(\delta)$ as Hermitian operators are usually defined over Hilbert spaces. However, as we shall see shortly, fortunately that is not required. This is because we do not have constructs in the language for denoting such measurement operators. In order to use Postulate 3, we need to consider Postulate 4.

Postulate 4: *The possible outcomes of the measurement of a physical quantity are the eigenvalues of the corresponding observable. When the physical quantity is measured using observable A on a system in a state $|\psi\rangle$, the resulting outcomes are ruled by the probability space $\mathcal{P}^A_{|\psi\rangle} = (\Omega, \mathcal{E}|_\Omega, \mu^A_{|\psi\rangle})$ where (in the case A has a countable spectrum)*

- *Ω is the spectrum of the observable A,*
- *$\mathcal{E}|_\Omega$ is $\wp\Omega$ the power-set of Ω , and*

- $\mu^A_{|\psi\rangle} : \mathcal{E}|_\Omega \to \mathbb{R}$ *is the probability measure defined as*

$$\mu^A_{|\psi\rangle}(E) = \sum_{e \in E} ||P_e|\psi\rangle||^2 .$$

For the applications in quantum computation and information that we have in mind, only *logic projective measurements* are relevant. Given a quantum system with the set of qubits qB and a set of classical valuations V, these are measurements A such that:

- The spectrum of A is *equipotent*[5] to V, *i.e.*, there is a bijection between the spectrum of A and V.
- If we identify V with the spectrum of A then for each $v \in V$, the corresponding eigenspace H_v is generated by the vector $|v\rangle$. The projector P_v is the operator $|v\rangle\langle v|$, *i.e.*, $P_v|\psi\rangle = \langle v, \psi\rangle\ |v\rangle$ for each vector $\psi \in \mathcal{H}_{\mathbb{C}}(2^{\mathsf{qB}})$.

Postulate 4 then tells us that the stochastic result of making a logic projective measurement A given a quantum structure $\mathbf{w} = (\mathcal{K}, \delta, V, \mathcal{S}, |\psi\rangle, \nu)$ is described by the finite probability space $\mathcal{P}_{\mathbf{w}} = (V, \wp V, \mu_{\mathbf{w}})$ where for each $U \subseteq V$:

$$\mu_{\mathbf{w}}(U) = \sum_{v \in U} |\langle v|\psi\rangle|^2 . \tag{1}$$

For example, if the quantum system is in the particular state

$$\alpha_{00\omega_1}|00\omega_1\rangle + \alpha_{01\omega_2}|01\omega_2\rangle + \alpha_{01\omega_3}|01\omega_3\rangle + \alpha_{10\omega_4}|10\omega_4\rangle$$

then the probability of observing the first two qubits $\mathsf{qb}_0, \mathsf{qb}_1$ in the classical valuation 01 (here we take V as $\{00\omega_1, 00\omega_2, 00\omega_3, 00\omega_4\}$) is given by $|\alpha_{01\omega_2}|^2 + |\alpha_{01\omega_3}|^2$.

We have probability terms in the language of the proposed logic and Equation 1 is all that we need from Postulates 3 and 4 for interpreting them as we shall see in Section 3.2.

Once again, we recall that we are working with an arbitrary real closed field. Given a quantum structure $\mathbf{w} = (\mathcal{K}, \delta, V, \mathcal{S}, |\psi\rangle, \nu)$, we define the *probability map* $\mu_{\mathbf{w}} : \wp(V) \to \mathcal{K}$ as:

$$\mu_{\mathbf{w}}(U) = \sum_{v \in U} |\langle v|\psi\rangle|^2 . \tag{2}$$

The essential difference between Equation 1 and 2 is that summands in the former are real numbers while the summands of the latter one are elements of a real closed field given by the quantum structure. It is easy to check that μ_V defined in Equation 2 satisfies the "usual" finite probability axioms:

[5]The chosen bijection depends on how the qubits are physically implemented. For example, when implementing a qubit using the spin of an electron, we may impose that spin $+\frac{1}{2}$ corresponds to true and spin $-\frac{1}{2}$ corresponds to false. But, as we shall see, the semantics of EQPL does not depend on the choice of the bijection, as long as one exists. The same happens in the case of classical logic – its semantics does not depend on how bits are implemented. The details of which voltages correspond to which truth values are irrelevant.

1. $\mu_V(\emptyset) = 0$ and $\mu_V(V) = 1$, and

2. $\mu_V(U_1 \cup U_2) = \mu_V(U_1) + \mu_V(U_2)$ if U_1 and U_2 are disjoint sets.

Therefore, given a quantum structure $\mathbf{w}$, we have the means for interpreting dEQPL terms of the form $(\int \alpha)$ that denote probabilities.

Finally, although irrelevant to the design of dEQPL, we mention *en passant* Postulate 5 that rules how quantum systems evolve beyond measurements:

Postulate 5 : *Excluding measurements, the evolution of a quantum system is described by unitary transformations.*

This last Postulate becomes relevant only when designing a dynamical extension of the logic (see for instance [27]).

3.2 Language and semantics

There are two kinds of terms in dEQPL, one denoting elements of real closed field in the quantum structure and the other denoting elements in its algebraic closure. The formulas of dEQPL, henceforth called *quantum formulas*, are constructed from classical propositional formulas, formulas denoting sub-systems and comparison formulas (comparing terms denoting elements of real closed fields) using global connectives introduced in Section 2. We present language of dEQPL in Table 1 using an abstract version of BNF notation [30] for a compact presentation of inductive definitions. We discuss the language in detail below.

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

Term language (with the proviso $A \subseteq G \subseteq \mathsf{qB}$)
$t \quad := \quad x \,[\!]\, 0 \,[\!]\, 1 \,[\!]\, (t + t) \,[\!]\, (t\, t) \,[\!]\, \mathrm{Re}(u) \,[\!]\, \mathrm{Im}(u) \,[\!]\, |u| \,[\!]\, (\int \alpha)$
$u \quad := \quad z \,[\!]\, |\top\rangle_{GA} \,[\!]\, t + it \,[\!]\, \overline{u} \,[\!]\, (u + u) \,[\!]\, (u\, u) \,[\!]\, (\alpha \rhd u;\, u)$

Quantum formulas (with the proviso $F \subseteq \mathsf{qB}$):
$\gamma \quad := \quad \alpha \,[\!]\, (t \leq t) \,[\!]\, [F] [\!]\, \perp\!\!\!\perp \,[\!] (\gamma \sqsupset \gamma)$

Table 1: Language of dEQPL

The first syntactic category is 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 $\bot$ and implication $\Rightarrow$. As usual, other classical connectives like $\neg, \wedge, \vee, \Leftrightarrow$ and $\top$ are introduced as abbreviations. We denote the set of qubit symbols occurring in α by $\mathsf{qB}(\alpha)$, and say that a classical formula α is over a set S of qubit symbols if $\mathsf{qB}(\alpha) \subseteq S$.

For the term language, we pick two disjoint denumerable sets of variables. The first set of variables $X = \{x_k : k \in \mathbb{N}\}$ is interpreted in the real closed field of the quantum structure, and the second set $Z = \{z_k : k \in \mathbb{N}\}$ is interpreted in the closure of the real closed fields. As we shall see in Section 5, variables are often useful for applications that we have in mind. There are two syntactic categories t and u for terms, which are mutually defined. The syntactic category t denotes the elements of a real closed field and u denotes the elements of its closure respectively. We will often abuse the notation by saying that t is a real term and u is a complex term.

Most of the term constructs are self-explanatory and already motivated in the previous section. The term $|\top\rangle_{GA}$ denotes the logical amplitude ν_{GA} in the quantum structure, and henceforth will be called an *amplitude term*. The term $(\int \alpha)$ denotes the probability that classical formula α holds for an outcome of a logical projective measurement, and will be called a *probability term*. The denotation of the *alternative term* $(\alpha \rhd u_1; u_2)$ will be the value denoted by u_1 if α is true, and the value denoted by u_2 otherwise.

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 $\vec{x}$, $\vec{t}$, $\vec{z}$ and $\vec{u}$ are sequences of real variables, real terms, complex variables and complex terms respectively, we will write $t\{\!|\vec{x}/\vec{t}, \vec{z}/\vec{u}|\!\}$ to mean the real term obtained by substituting <u>all</u> occurrences of x_i by t_i and all occurrences of z_j by u_j. The complex term $u\{\!|\vec{x}/\vec{t}, \vec{z}/\vec{u}|\!\}$ is similarly defined.

The quantum formulas are built from classical formulas α, *sub-system formulas* $[F]$ and *comparison formulas* $(t \leq t)$ using the connectives $\perp\!\!\!\perp$ and $\sqsupset$. The formulas consisting of just the classical formulas, sub-system and comparison formulas are called *quantum atoms*, and the set of quantum atoms shall henceforth be called qAtom. We shall use δ, δ' to range over elements of qAtom. Please note that quantum bottom $\perp\!\!\!\perp$ and quantum implication $\sqsupset$ are global connectives and should not be confused with their classical (local) counterparts.

The notion of occurrence of a term t in a quantum formula γ can be easily defined. However, we have to be careful while defining the notion of occurrence of a quantum formula γ in the quantum formula γ_1. This is because we want γ to occur as a *quantum sub-formula* of γ_1 and rule out situations where γ occurs as classical sub-formula. More precisely, we define γ_1 *q-occurs* in γ inductively as:

- if γ is a classical formula, a comparison formula, a sub-system formula, or $\perp\!\!\!\perp$, then γ_1 q-occurs in γ if and only if γ_1 is γ and;
- if γ is $\gamma' \sqsupset \gamma''$ then γ_1 q-occurs in γ if and only if one of the following holds:
  - γ_1 is γ, or
  - γ_1 q-occurs in γ', or
  - γ_1 q-occurs in γ''.

The notion of replacing zero or more q-occurrences of a quantum formula γ_1 in γ by γ' can now be suitably defined.

For example, the classical formula qb q-occurs in $(\mathsf{qb} \sqsupset \mathsf{qb}_1)$ and replacing one q-occurrence of qb by qb_2 will yield the quantum formula $(\mathsf{qb}_2 \sqsupset \mathsf{qb}_1)$. On the other hand qb does not q-occur in $(\mathsf{qb} \Rightarrow \mathsf{qb}_1)$ (qb is a classical sub-formula and not quantum sub-formula). The replacement qb by qb_2 in $(\mathsf{qb} \Rightarrow \mathsf{qb}_1)$ has no effect. Similarly, qb does not q-occur in $[\{\mathsf{qb}\}]$.

For clarity sake, we shall often drop parenthesis in formulas and terms if it does not lead to ambiguity. As expected, other quantum connectives will be introduced as abbreviations. However, before introducing a whole set of useful abbreviations, we present the semantics of the language.

The language is interpreted in a quantum structure as defined in Section 3.1. Given a quantum structure $\mathbf{w} = (\mathcal{K}, \delta, V, \mathcal{S}, |\psi\rangle, \nu)$, recall that $\mathcal{K}$ is a real closed field with $\mathcal{K}(\delta)$ as its algebraic closure, V is a set of valuations over qB, $\mathcal{S}$ is a partition of qB, $|\psi\rangle$ is a collection of $\mathcal{K}(\delta)$-quantum states, and ν is a collection of amplitude terms. We shall assume the semantics of classical propositional logic, and say that $v \Vdash_c \alpha$ if the classical valuation v satisfies the classical formula α.

For interpreting the probability terms, we shall use the *probability map* $\mu_{\mathbf{w}} : \wp(V) \to \mathcal{K}$ defined in Section 3.1 as:

$$\mu_{\mathbf{w}}(U) = \sum_{v \in U} \left|\left|\langle v|\psi\rangle\right|\right|^2.$$

For the probability terms, we shall also need the *extent* at a set V of classical formulas over S defined as:

$$|\alpha|_V = \{v \in V : v \Vdash_c \alpha\}.$$

For interpreting the variables, we need the concept of an assignment. Given a real closed field $\mathcal{K}$, a $\mathcal{K}$*-assignment* ρ is a map such that $\rho(x) \in \mathcal{K}$ for each $x \in X$ and $\rho(z) \in \mathcal{K}(\delta)$ for each $z \in Z$. Please note that when $\mathcal{K}$ is clear from the context, we shall drop $\mathcal{K}$.

Given a quantum structure $\mathbf{w} = (\mathcal{K}, \delta, V, \mathcal{S}, |\psi\rangle, \nu)$ and a $\mathcal{K}$-assignment ρ. The *denotation of terms* and *satisfaction of quantum formulas* at $\mathbf{w}$ and ρ and is inductively defined in Table 2 (omitting the obvious ones).

Please observe that the set V is sufficient to interpret the classical formulas, and the partition $\mathcal{S}$ is sufficient to interpret the sub-system formulas. The $\mathcal{K}$-assignment ρ is sufficient to interpret a useful sub-language of the formulas defined as:

$$\begin{array}{lcl} \kappa & := & (a \leq a)[\!] \perp\!\!\!\perp [\!](\kappa \sqsupset \kappa) \\ a & := & x [\!] 0 [\!] 1 [\!] (a + a) [\!] (a\,a) [\!] \mathrm{Re}(b) [\!] \mathrm{Im}(b) [\!] |b| \\ b & := & z [\!] a + ia [\!] \overline{b} [\!] (b + b) [\!] (b\,b) \end{array}$$

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

We may use the satisfaction relation to define *entailment* as expected: we say that a set of quantum formulas Γ entails a quantum formula η, written $\Gamma \vDash \eta$, if $\mathbf{w}\rho \Vdash \eta$ for every $\mathbf{w}$ and ρ satisfying every element of Γ. We say a quantum formula η is valid when it is entailed by the empty set of quantum

Denotation of terms

$$
\begin{array}{lcl}
[\![x]\!]_{\mathbf{w}\rho} & = & \rho(x) \\
[\![t_1 + it_2]\!]_{\mathbf{w}\rho} & = & [\![t_1]\!]_{\mathbf{w}\rho} + \delta[\![t_2]\!]_{\mathbf{w}\rho} \\
[\![(\int \alpha)]\!]_{\mathbf{w}\rho} & = & \mu_{\mathbf{w}}(|\alpha|_V) \\
[\![z]\!]_{\mathbf{w}\rho} & = & \rho(z) \\
[\![|\top\rangle_{GA}]\!]_{\mathbf{w}\rho} & = & \nu_{GA} \\
[\![(\alpha \rhd u_1;\, u_2)]\!]_{\mathbf{w}\rho} & = & \begin{cases} [\![u_1]\!]_{\mathbf{w}\rho} & \text{if } |\alpha|_V = V \\ [\![u_2]\!]_{\mathbf{w}\rho} & \text{otherwise} \end{cases}
\end{array}
$$

Satisfaction of quantum formulas

$$
\begin{array}{lll}
\mathbf{w}\rho \Vdash \alpha & \text{iff} & |\alpha|_V = V \\
\mathbf{w}\rho \Vdash (t_1 \leq t_2) & \text{iff} & [\![t_1]\!]^{\mathbf{w}}_{\rho} \leq [\![t_2]\!]^{\mathbf{w}}_{\rho} \\
\mathbf{w}\rho \Vdash [A] & \text{iff} & A \in \mathrm{Alg}(\mathcal{S}) \\
\mathbf{w}\rho \nVdash \perp\!\!\!\perp & & \\
\mathbf{w}\rho \Vdash (\gamma_1 \sqsupset \gamma_2) & \text{iff} & \mathbf{w}\rho \nVdash \gamma_1 \text{ or } \mathbf{w}\rho \Vdash \gamma_2
\end{array}
$$

Table 2: Semantics of dEQPL

formulas. Please note also that the metatheorem of entailment holds: $\Gamma, \eta_1 \vDash \eta_2$ iff $\Gamma \vDash (\eta_1 \sqsupset \eta_2)$. That is, quantum implication internalizes the notion of quantum entailment. The following are some examples of entailment:

$$
\begin{array}{rcl}
 & \vDash & (\neg\, \alpha) \sqsupset (\boxminus\, \alpha) \\
 & \vDash & (\alpha_1 \wedge \alpha_2) \equiv (\alpha_1 \sqcap \alpha_2) \\
[G_1],\ [G_2] & \vDash & [G_1 \cap G_2] \\
\alpha & \vDash & ((\int \alpha) = 1) \\
[G] & \vDash & ((\sum_{A \subseteq G} ||\top\rangle_{GA}|^2) = 1)
\end{array}
$$

We shall now present some useful abbreviations, and give some small examples.

3.3 Abbreviations and examples

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 $((t_1 \leq t_2) \sqcap (t_2 \leq t_1))$;
- $(u_1 = u_2)$ for $((\mathrm{Re}(u_1) = \mathrm{Re}(u_2)) \sqcap (\mathrm{Im}(u_1) = \mathrm{Im}(u_2)))$

Please note that the only constants in our term language are 0 and 1. As every real closed field $\mathcal{K}$ has characteristic 0, we can embed a copy of rationals in $\mathcal{K}$. It is also possible to take square roots of positive numbers. Hence, it will be useful to use the following abbreviations (with the proviso $n > 0$):

- $(t = n)$ for $t = \underbrace{((1 + (1 + \ldots ...)))}_{n \text{ times}}$;
- $(t = \frac{m}{n})$ for $((m.t) = n)$;
- $(t_1 = \sqrt{t_2})$ for $((t_2 \geq 0) \sqcap ({t_1}^2 = t_2))$.

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

- $(\wedge_G A)$ is $((\wedge_{\mathsf{qb}_k \in A} \mathsf{qb}_k) \wedge (\wedge_{\mathsf{qb}_k \in G \setminus A} (\neg\, \mathsf{qb}_k))$.

The classical formula $(\wedge_G A)$ specifies the unique classical valuation that satisfies all the qubit symbols in A and does not satisfy the qubit symbols in $G \setminus A$. We will often need this classical formula in the case the set G is the full set of qubit symbols qB. Therefore, we will often use the following abbreviation

- $(\wedge A)$ for $(\wedge_{\mathsf{qB}} A)$.

The logical amplitude terms, $|\top\rangle_{GA}$, are easily extendible to any classical formula as (with the provisos $\mathsf{qB}(\alpha) \subseteq G$ and $A \subseteq G \subseteq \mathsf{qB}$):

- $|\alpha\rangle_{GA}$ for $(((\wedge_G A) \Rightarrow \alpha) \rhd |\top\rangle_{GA}; 0)$.

Intuitively, the amplitude term $|\alpha\rangle_{GA}$ coincides with $|\top\rangle_{GA}$ when the valuation $\wedge_G A$ satisfies with α and is 0 otherwise. We will often use this term in the case G is the full set of qubit symbols qB. Therefore, the following abbreviation will also be useful:

- $|\alpha\rangle_A$ for $|\alpha\rangle_{\mathsf{qB}A}$.

We introduce a couple of probability modalities as abbreviations:

- $(\Diamond\alpha)$ for $(0 < (\int \alpha))$;
- $(\Box\alpha)$ for $(1 = (\int \alpha))$.

Finally, we can also define a quantum modality as an abbreviation:

- $([G]\Diamond\ \alpha : u)$ for $([G] \sqcap (|u| > 0) \sqcap (\sqcup_{A \subseteq G} (|\alpha\rangle_{GA} = u)))$.

Intuitively $([G]\Diamond\, \alpha : u)$ is true iff G is a sub-system, there is a subset A of G such that the classical valuation $\wedge_G A$ satisfies α and the logical amplitude $|\top\rangle_{GA}$ takes the non-zero value u.

We discuss a small example where we demonstrate the usefulness of dEQPL to specify properties of a quantum system. We postpone the discussion of more involved examples to Section 5. Consider the following variant of Schrödinger's cat. The attributes of the cat that we consider are: being inside or outside the box, alive or dead, and moving or still. We choose three qubit symbols $\mathsf{qb}_0, \mathsf{qb}_1, \mathsf{qb}_2$ to represent these attributes. For the sake of readability, we use **cat-in-box**, **cat-alive** and **cat-moving** instead of the symbols $\mathsf{qb}_0, \mathsf{qb}_1$ and qb_2 respectively. The following dEQPL formulas constrain the state of the cat at different levels of detail:

1. $[\mathbf{cat\text{-}in\text{-}box}, \mathbf{cat\text{-}alive}, \mathbf{cat\text{-}moving}]$;
2. $(\mathbf{cat\text{-}moving} \Rightarrow \mathbf{cat\text{-}alive})$;
3. $((\Diamond\, \mathbf{cat\text{-}alive}) \sqcap (\Diamond\, (\neg\, \mathbf{cat\text{-}alive})))$;
4. $(\boxminus[\mathbf{cat\text{-}alive}])$;
5. $((\int \mathbf{cat\text{-}alive}) = \frac{1}{3})$;
6. $([\mathbf{cat\text{-}alive}, \mathbf{cat\text{-}moving}] \sqcap ((\int \mathbf{cat\text{-}alive} \wedge \mathbf{cat\text{-}moving}) = \frac{1}{6})$
   $\sqcap ((\int \mathbf{cat\text{-}alive} \wedge (\neg\, \mathbf{cat\text{-}moving})) = \frac{1}{6})$
   $\sqcap ((\int (\neg\, \mathbf{cat\text{-}alive}) \wedge (\neg\, \mathbf{cat\text{-}moving})) = \frac{2}{3}))$.

Please observe that all the above assertions are consistent with each other. Intuitively, the first assertion states that the qubits **cat-in-box**, **cat-alive** and **cat-moving** form a sub-system and therefore, are not entangled with the other qubits of the cat system. The second is a classical constraint on the set of admissible valuations: if the cat is moving then it is alive. The third assertion is a consequence of the famous paradox: the cat can be in a state where it is possible that the cat is alive and it is possible that the cat is dead. The fourth assertion states that the qubit **cat-alive** is necessarily entangled with other qubits. The fifth assertion states that the cat is in a state where the probability of observing it alive (after collapsing the wave function) is $\frac{1}{3}$. Finally, the sixth assertion states that the qubits **cat-alive**, **cat-moving** are not entangled with other qubits, and that the cat is in quantum state where: the probability of observing it alive and moving is $\frac{1}{6}$, the probability of observing it alive and not moving is $\frac{1}{6}$, and the probability of observing it dead (and, thus also not moving by second assertion)is $\frac{2}{3}$.

3.4 The axiomatization

We shall present a Hilbert-style axiomatization of the dEQPL. We need two new concepts for the axiomatization, one of quantum tautology and the second of a valid arithmetical formula.

Let P be a countable set of propositional symbols disjoint from qB. Given a classical formula β over P, let β_q be the syntactic entity obtained by replacing all occurrences of $\bot$ by $\perp\!\!\!\perp$ and $\Rightarrow$ by $\sqsupset$. A quantum formula σ is said to be a *quantum tautology* if there is a classical tautology β over P and a map $\sigma : \mathrm{P} \to \mathsf{qAtom}$ such that σ coincides with $\beta_q\sigma$ where $\beta_q\sigma$ is the quantum formula obtained from β_q by replacing each $p \in \mathrm{P}$ by $\sigma(p)$. For instance, the quantum formula $((x_1 \leq x_2) \sqsupset (x_1 \leq x_2))$ is tautological (obtained, for example, from the classical tautology $p \Rightarrow p$).

Please recall that an arithmetical formula in the dEQPL is any formula that does not have probability terms, amplitude terms, alternative terms, classical formulas and sub-system formulas. As noted in Section 3.2, given an quantum structure with $\mathcal{K}_0$ as the underlying real closed field, a $\mathcal{K}_0$-assignment is enough to interpret all arithmetical formulas. We say that an arithmetical formula κ is a *valid arithmetical formula* if it holds for any assignment that maps variables into an arbitrary real closed field $\mathcal{K}$. Clearly, a valid arithmetical formula holds for all semantic structures of dEQPL. It is a well-known fact from the theory of quantifier elimination [24, 6] that the set of valid arithmetical formulas so defined is decidable[6]. However, we shall not go into details of this result as we want to focus our attention on reasoning about quantum aspects only.

The axioms and inference rules of dEQPL are listed in Table 3. In total, we have two inference rules and sixteen axioms. The two inference rules are modus ponens for classical implication **CMP** and *modus ponens* for quantum implication **CMP**[7]. The axioms are better understood in the following groups.

We have as axioms the classical tautologies and the quantum tautologies (**CTaut** and **QTaut**, respectively). Since the set of classical tautologies and the set of quantum tautologies are both recursive, there is no need to spell out the details of tautological reasoning.

The axioms **Lift**$\Rightarrow$, **Eqv**$\bot$ and **Ref**$\sqcap$ are sufficient to relate (local) classical reasoning and (global) quantum tautological reasoning. These are exactly the axioms that relate classical connectives and global connectives in global logic (see Section 2). We refer to [29] for more details.

The axioms **Sub**, **Sub**$\cup$, and **Sub**$\setminus$ are enough to reason about sub-systems. Together, they impose that sub-systems are closed under set-theoretic operations (closure under intersection and set difference appear as theorems).

The axiom **RCF** says that if κ is a valid arithmetical formula, then any formula obtained by replacing variables with the terms of dEQPL is a tautology. Since the set of valid arithmetical formulas is recursive, we refrain from spelling out the details.

The axioms **If**$\top$ and **If**$\bot$ are self-explanatory, and will be used in the completeness proof to remove alternative terms.

The axioms **Empty**, **NAdm**, **Unit** and **Mul** rule logical amplitudes. Each of them closely reflects a property of our semantic structures. The axiom empty says that the logical amplitude $|\top\rangle_{\emptyset\emptyset}$ is always 1. The axiom **Unit** says that

[6]For the arithmetical sub-language, we may treat the global connectives as classical connectives

[7]Actually, **CMP** can be derived from **QMP** and **Lift**$\Rightarrow$.

Axioms

[CTaut]	$\vdash$	α for each classical tautology α
[QTaut]	$\vdash$	γ for each quantum tautology γ
[Lift$\Rightarrow$]	$\vdash$	$((\alpha_1 \Rightarrow \alpha_2) \sqsupset (\alpha_1 \sqsupset \alpha_2))$
[Eqv$\bot$]	$\vdash$	$(\bot \equiv \perp\!\!\!\perp)$
[Ref$\sqcap$]	$\vdash$	$((\alpha_1 \sqcap \alpha_2) \sqsupset (\alpha_1 \wedge \alpha_2))$
[Sub$\emptyset$]	$\vdash$	$[\emptyset]$
[Sub$\cup$]	$\vdash$	$([G_1] \sqsupset ([G_2] \sqsupset [G_1 \cup G_2]))$
[Sub$\setminus$]	$\vdash$	$([G] \equiv [\mathsf{qB} \setminus G])$
[RCF]	$\vdash$	$\kappa\{\!\{\vec{x}/\vec{t},\ \vec{z}/\vec{u}\}\!\}$ where κ is a valid arithmetical formula, $\vec{x}$, $\vec{z}$, $\vec{t}$ and $\vec{u}$ are sequences of real variables, complex variables, real terms and complex terms respectively
[If$\top$]	$\vdash$	$(\alpha \sqsupset ((\alpha \rhd u_1; u_2) = u_1))$
[If$\bot$]	$\vdash$	$((\boxminus \alpha) \sqsupset ((\alpha \rhd u_1; u_2) = u_2))$
[Empty]	$\vdash$	$(\lvert\top\rangle_{\emptyset\emptyset} = 1)$
[NAdm]	$\vdash$	$((\neg(\wedge A)) \sqsupset (\lvert\top\rangle_{\mathsf{qB}A} = 0))$
[Unit]	$\vdash$	$([G] \sqsupset ((\sum_{A \subseteq G} \lvert\lvert\top\rangle_{GA}\rvert^2) = 1))$
[Mul]	$\vdash$	$(([G_1] \sqcap [G_2]) \sqsupset (\lvert\top\rangle_{G_1 \cup G_2 A_1 \cup A_2} = \lvert\top\rangle_{G_1 A_1} \lvert\top\rangle_{G_2 A_2}))$ where $G_1 \cap G_2 = \emptyset$, $A_1 \subseteq G_1$ and $A_2 \subseteq G_2$
[Prob]	$\vdash$	$((\int \alpha) = (\sum_A \lvert\lvert\alpha\rangle_A\rvert^2))$

Inference rules

[CMP]	$\alpha_1, (\alpha_1 \Rightarrow \alpha_2) \vdash \alpha_2$
[QMP]	$\gamma_1, (\gamma_1 \sqsupset \gamma_2) \vdash \gamma_2$

Table 3: Axioms for dEQPL

the state of each sub-system is a unit vector. The axiom **NAdm** says that the amplitude of a non-admissible classical valuation is 0. The axiom **Mul** says that the state of a system composed of two subs-systems is a tensor product of the two sub-systems.

Finally, the axiom **Prob** relates probabilities and amplitudes, closely following Postulate 4 of quantum mechanics.

As expected, we say that a formula γ is a *theorem*, written $\vdash \gamma$, if we can build a derivation of γ from the axioms using the inference rules. We say that a (possibly infinite) set of formulas Γ *derives* γ, written $\Gamma \vdash \gamma$, if we can build

a derivation of γ from axioms and the inference rules using formulas in Γ as hypothesis. As an illustration of the axiomatization, we establish the following theorems:

Proposition 3.7 For any classical formulas α_1, α_2, we have

$$\begin{array}{ll} [\textbf{Lift}\wedge] & \vdash (\alpha_1 \wedge \alpha_2) \sqsupset (\alpha_1 \sqcap \alpha_2). \\ [\textbf{PUnit}] & \vdash ((\int \top) = 1). \end{array}$$

Proof: Derivation of [**Lift**$\wedge$]:

1	$(\alpha_1 \wedge \alpha_2) \Rightarrow \alpha_1$	**CTaut**
2	$((\alpha_1 \wedge \alpha_2) \Rightarrow \alpha_1) \sqsupset ((\alpha_1 \wedge \alpha_2) \sqsupset \alpha_1)$	**Lift**$\Rightarrow$
3	$(\alpha_1 \wedge \alpha_2) \sqsupset \alpha_1$	**QMP**:1,2
4	$(\alpha_1 \wedge \alpha_2) \Rightarrow \alpha_2$	**CTaut**
5	$((\alpha_1 \wedge \alpha_2) \Rightarrow \alpha_2) \sqsupset ((\alpha_1 \wedge \alpha_2) \sqsupset \alpha_2)$	**Lift**$\Rightarrow$
6	$(\alpha_1 \wedge \alpha_2) \sqsupset \alpha_2$	**QMP**:4,5
7	$((\alpha_1 \wedge \alpha_2) \sqsupset \alpha_1) \sqsupset (((\alpha_1 \wedge \alpha_2) \sqsupset \alpha_2) \sqsupset ((\alpha_1 \wedge \alpha_2) \sqsupset (\alpha_1 \sqcap \alpha_2)))$	**Qtaut**
8	$((\alpha_1 \wedge \alpha_2) \sqsupset \alpha_2) \sqsupset ((\alpha_1 \wedge \alpha_2) \sqsupset (\alpha_1 \sqcap \alpha_2))$	**QMP**:3,8
9	$(\alpha_1 \wedge \alpha_2) \sqsupset (\alpha_1 \sqcap \alpha_2)$	**QMP**:6,8

Derivation of [**PUnit**]

1	$[\emptyset]$	**Sub**$\emptyset$
2	$[\emptyset] \sqsupset [\mathsf{qB}]$	**Sub**$\setminus$
3	$[\mathsf{qB}]$	**QMP**:1,2
4	$([\mathsf{qB}] \sqsupset ((\sum_{A \subseteq \mathsf{qB}} \|\|\top\rangle_{\mathsf{qB}A}\|^2) = 1))$	**Unit**
5	$((\sum_{A \subseteq \mathsf{qB}} \|\|\top\rangle_{\mathsf{qB}A}\|^2) = 1)$	**QMP**:3,4
6	$((\int \top) = (\sum_{A \subseteq \mathsf{qB}} \|\|\top\rangle_{\mathsf{qB}A}\|^2))$	**Prob**
7	$(((\int \top) = (\sum_{A \subseteq \mathsf{qB}} \|\|\top\rangle_{\mathsf{qB}A}\|^2)) \sqsupset (((\sum_{A \subseteq \mathsf{qB}} \|\|\top\rangle_{\mathsf{qB}A}\|^2) = 1) \sqsupset ((\int \top) = 1)))$	**RCF**
8	$(((\sum_{A \subseteq \mathsf{qB}} \|\|\top\rangle_{\mathsf{qB}A}\|^2) = 1) \sqsupset ((\int \top) = 1))$	**QMP**:6,7
9	$((\int \top) = 1)$	**QMP**:5,8

$\diamond$

We finish this section with a list of interesting theorems. The first three shall be proved in Section 3.6 using the metatheorems of the logic. The first two relate local equivalence and negation with their global counterparts, while the third one says sub-systems are closed under set intersection and the fourth one says that sub-systems are closed under set difference.

$$
\begin{array}{ll}
[\mathbf{Lift}\Leftrightarrow] & \vdash (\alpha_1 \Leftrightarrow \alpha_2) \sqsupset (\alpha_1 \equiv \alpha_2). \\
[\mathbf{Lift}\neg] & \vdash \neg\,\alpha \sqsupset \boxminus\,\alpha. \\
[\mathbf{Sub}\cap] & \vdash_F ([G_1] \sqsupset ([G_2] \sqsupset [G_1 \cap G_2])). \\
[\mathbf{SubDiff}] & \vdash_F ([G_1] \sqsupset ([G_2] \sqsupset [G_1 \setminus G_2])).
\end{array}
$$

The following theorems give some insight on the major properties of logical amplitudes.

$$
\begin{array}{ll}
[\mathbf{AAdd}] & \vdash ((|(\alpha_1 \vee \alpha_2)\rangle_G + |(\alpha_1 \wedge \alpha_2)\rangle_G) = (|\alpha_1\rangle_G + |\alpha_2\rangle_G)). \\
[\mathbf{AMon}] & \vdash ((\alpha_1 \Rightarrow \alpha_2) \sqsupset (||\alpha_1\rangle_G| \leq ||\alpha_2\rangle_G|)). \\
[\mathbf{ASoE}] & \vdash ((\alpha_1 \Leftrightarrow \alpha_2) \sqsupset (|\alpha_1\rangle_G = |\alpha_2\rangle_G)). \\
[\mathbf{ANec}] & \vdash (\alpha \sqsupset (|\alpha\rangle_G = |\top\rangle_G)). \\
[\mathbf{AMExc}] & \vdash ((|\alpha\rangle_G + |(\neg\,\alpha)\rangle_G) = |\top\rangle_G)\ .
\end{array}
$$

The first of the following theorems about probability after measurements just states finite additivity. The second relates logical reasoning with probability reasoning (monotonicity). These two theorems and the theorem **PUnit** illustrated in Proposition 3.7 are axioms in the exogenous probabilistic logic discussed in Section 2.

$$
\begin{array}{ll}
[\mathbf{PAdd}] & \vdash (((\int(\alpha_1 \vee \alpha_2)) + (\int(\alpha_1 \wedge \alpha_2))) = ((\int\alpha_1) + (\int\alpha_2))). \\
[\mathbf{PMon}] & \vdash ((\alpha_1 \Rightarrow \alpha_2) \sqsupset ((\int\alpha_1) \leq (\int\alpha_2))).
\end{array}
$$

The following theorems show that probability modalities behave as normal modalities.

$$
\begin{array}{ll}
[\mathbf{PNec}] & \vdash (\alpha \sqsupset (\Box\alpha)). \\
[\mathbf{PNorm}] & \vdash ((\Box(\alpha \Rightarrow \alpha')) \sqsupset ((\Box\alpha) \sqsupset (\Box\alpha'))).
\end{array}
$$

The quantum modalities also behave as normal modalities.

$$
\begin{array}{ll}
[\mathbf{QNorm}] & \vdash (([G]\Diamond\ (\alpha \vee \alpha') : u) \equiv (([G]\Diamond\ \alpha : u) \sqcup ([G]\Diamond\ \alpha' : u)))\ . \\
[\mathbf{QMon}] & \vdash ((\alpha \Rightarrow \alpha') \sqsupset (([G]\Diamond\ \alpha : u) \sqsupset ([G]\Diamond\ \alpha' : u))). \\
[\mathbf{QCong}] & \vdash ((u = u') \sqsupset (([G]\Diamond\ \alpha : u) \sqsupset ([G]\Diamond\ \alpha : u')))\ .
\end{array}
$$

3.5 Soundness

We now show that the calculus is strongly sound, *i.e.*, if $\Gamma \vdash \gamma$ then $\Gamma \vDash \gamma$. It suffices to show that each of the axioms is valid, *i.e.*, if $\vdash \gamma_1$ is an axiom, then every semantic structure satisfies γ_1.

Lemma 3.8 The axiom **QTaut** is valid.

Proof: Assume that β is a classical tautology over the set of propositional symbols P and let $\sigma : \mathrm{P} \to \mathsf{qAtom}$ be a map from P into quantum atoms. We show that $\beta_q\sigma$ is valid in all models of dEQPL.

Take an arbitrary quantum structure $\mathbf{w} = (K, \delta, V, \mathcal{S}, |\psi\rangle, \nu)$, and consider the classical valuation v' over P such that

$$v'(p) = \begin{cases} 1 & \text{if } \mathbf{w}\rho \Vdash \sigma(p) \\ 0 & \text{otherwise} \end{cases} .$$

We show that for any classical formula β' over P

$$v' \Vdash \beta' \text{ iff } \mathbf{w}\rho \Vdash \beta'_q\sigma$$

by induction on the structure of β' as follows.

If β' is a propositional symbol then it follows from the definition of v'. The case where β' is the connective $\bot$ is immediate.

If β' is $(\beta_1 \Rightarrow \beta_2)$, then v' satisfies β_2 or v' does not satisfy β_1. If v' satisfies β_2 then by induction hypothesis $\mathbf{w}\rho \Vdash (\beta_2)_q$. If v' does not satisfy β_1, then by induction hypothesis once again, $v' \nVdash (\beta_1)_q$. Therefore, in either case, $\mathbf{w}\rho \Vdash (\beta_1)_q \sqsupset (\beta_2)_q$. Now, note that β'_q is $(\beta_1)_q \sqsupset (\beta_2)_q$.

The lemma now follows by observing that $v' \Vdash \beta$. $\diamond$

Lemma 3.9 The axioms are valid.

Proof: The axioms **CTaut**, **Eqv**$\bot$, **RCF**, **If**$\top$, **If**$\bot$, **Empty**, **Sub**$\emptyset$, **Sub**$\cup$ and **Sub**$\setminus$ are easy to show. For the rest, let $\mathbf{w} = (K, \delta, V, \mathcal{S}, |\psi\rangle, \nu)$ be a quantum structure and ρ a $\mathcal{K}$-assignment. We consider the other axioms one by one:

- **Lift**$\Rightarrow$. Assume that $\mathbf{w}\rho \Vdash (\alpha_1 \Rightarrow \alpha_2)$. Then, by definition, all classical valuations in V must satisfy $(\alpha_1 \Rightarrow \alpha_2)$. Therefore, if all classical valuations in V satisfy α_1 they must satisfy α_2 also. Hence, either $|\alpha_1|_V \neq V$ or $|\alpha_2|_V = V$. We conclude, by definition, $\mathbf{w} \Vdash \alpha_1 \sqsupset \alpha_2$.

- **Ref**$\sqcap$. Similar to the axiom **Lift**$\Rightarrow$.

- **NAdm**. Assume that $\mathbf{w}\rho \Vdash (\neg(\wedge A))$. This means that the classical valuation v_A^{qB} that assigns 1 to the qubit symbols in A and 0 to all other qubits is not an element of V. Therefore, $\nu_{\mathsf{qB}A} = \langle v_A^{\mathsf{qB}} | \psi \rangle_{\mathsf{qB}} = 0$ and hence $\mathbf{w}\rho \Vdash |\top\rangle_{\mathsf{qB}A} = 0$.

- **Prob**. Using the definition $[\![(\int \alpha)]\!]_{\mathbf{w}\rho} = \mu_{\mathbf{w}}(|\alpha|_V) = \sum_{v \in |\alpha|_V} |\langle v|\psi\rangle_{\mathsf{qB}}|^2$, it suffices to show that

$$\sum_{v \in |\alpha|_V} |\langle v|\psi\rangle_{\mathsf{qB}}|^2 = [\![\sum_A ||\alpha\rangle_A|^2]\!]_{\mathbf{w}\rho}.$$

  Please note that $[\![|\alpha\rangle_A]\!]_{\mathbf{w}\rho} = \begin{cases} \nu_{\mathsf{qB}A} & \text{if } v_A^{\mathsf{qB}} \in |\alpha|_V \\ 0 & \text{otherwise} \end{cases}$.

  Also, by definition, $\nu_{\mathsf{qB}A} = \langle v_A^{\mathsf{qB}} | \psi \rangle_{\mathsf{qB}}$. Therefore,

$$[\![\sum_A ||\alpha\rangle_A|^2]\!]_{\mathbf{w}\rho} = \sum_{v_A^{\mathsf{qB}} \in |\alpha|_V} |\langle v_A^{\mathsf{qB}}|\psi\rangle_{\mathsf{qB}}|^2$$

  We conclude by observing that every v is a v_A^{qB} for some unique $A \subseteq \mathsf{qB}$.

- **Unit**. Assume that $\mathbf{w}\rho \Vdash [G]$. Then $G \in \mathrm{Alg}(\mathcal{S})$. Please note that $\{|v_A^G\rangle : A \subseteq G\}$ forms an orthonormal basis of $H(2^G)$. Hence,

$$|\psi\rangle_G = \sum_{A \subseteq G} \langle v_A^G | \psi \rangle_G \ |v_A^G\rangle.$$

Again, by definition, $\langle v_A^G | \psi \rangle_G = \nu_{GA}$ and so

$$|\psi\rangle_G = \sum_{A \subseteq G} \nu_{GA} \ |v_A^G\rangle.$$

Since $|\psi\rangle_G$ is a unit vector, we get

$$\sum_{A \subseteq G} |\nu_{GA}|^2 = 1.$$

We conclude by noting that $[\![|\top\rangle_{GA}]\!]_{\mathbf{w}\rho} = \nu_{GA}$ by definition.

- **Mul.** Assume that $\mathbf{w}\rho \Vdash [G_1] \sqcap [G_2]$ where $G_1 \cap G_2 = \emptyset$. Then $G_1, G_2 \in \mathrm{Alg}(\mathcal{S})$. The definition of quantum structure says that $|\psi\rangle_{G_1 \cup G_2} = |\psi\rangle_{G_1} \otimes |\psi\rangle_{G_2}$.

The definition of tensor product says that $|v_{A_1 \cup A_2}^{G_1 \cup G_2}\rangle = |v_{A_1}^{G_1}\rangle \otimes |v_{A_2}^{G_2}\rangle$.

The definition of quantum structure gives

$$\nu_{G_1 \cup G_2 A_1 \cup A_2} = \langle v_{A_1 \cup A_2}^{G_1 \cup G_2} \ |\psi\rangle_{G_1 \cup G_2}.$$

The definition of tensor product then gives,

$$\nu_{G_1 \cup G_2 A_1 \cup A_2} = \langle v_{A_1}^{G_1} \otimes v_{A_2}^{G_2} \mid \psi_{G_1} \otimes \psi_{G_2} \rangle_{G_1 \cup G_2} = \langle v_{A_1}^{G_1} | \psi \rangle_{G_1} \langle v_{A_2}^{G_2} | \psi \rangle_{G_2}.$$

We conclude by observing that $\nu_{G_1 A_1}$ is $\langle v_{A_1}^{G_1} | \psi \rangle_{G_1}$ and $\nu_{G_2 A_2}$ is $\langle v_{A_2}^{G_2} | \psi \rangle_{G_2}$.

$\diamond$

Theorem 3.10 (Soundness) The proof system of dEQPL is sound.

Proof: The proof now follows by induction on the number of steps in the derivation. $\diamond$

3.6 Metatheorems

We now prove some useful metatheorems for dEQPL. We start by showing that the inference rule Hypothetical Syllogism holds for dEQPL.

Lemma 3.11 (Hypothetical Syllogism) Let $\gamma_1, \gamma_2, \gamma_3$ be quantum formulas. Then,

$$[\mathbf{HypSyl}] \ \Gamma \vdash \gamma_1 \sqsupset \gamma_2 \text{ and } \Gamma \vdash \gamma_2 \sqsupset \gamma_3 \text{ imply } \Gamma \vdash \gamma_1 \sqsupset \gamma_3.$$

Proof: Observe that by **QTaut**,

$$\vdash (\gamma_1 \sqsupset \gamma_2) \sqsupset ((\gamma_2 \sqsupset \gamma_3) \sqsupset (\gamma_1 \sqsupset \gamma_3)).$$

The proposition follows by using two instances of **QMP**. ◇

The inference rule **HypSyl** is a useful rule as illustrated in the derivation of the theorem **Lift**$\neg$ below:

Proposition 3.12 For any classical formula α, we have

$$[\mathbf{Lift}\neg] \quad \vdash \neg\alpha \sqsupset \boxminus\alpha.$$

Proof:

1	$((\bot\sqsupset \perp\!\!\!\perp) \sqcap (\perp\!\!\!\perp \sqsupset\bot))$	**Eqv**$\bot$
2	$((\bot\sqsupset \perp\!\!\!\perp) \sqcap (\perp\!\!\!\perp \sqsupset\bot)) \sqsupset (\bot\sqsupset \perp\!\!\!\perp)$	**QTaut**
3	$(\bot\sqsupset \perp\!\!\!\perp)$	**QMP**: 1,2
4	$(\bot\sqsupset \perp\!\!\!\perp) \sqsupset ((\alpha \sqsupset \bot) \sqsupset (\alpha\sqsupset \perp\!\!\!\perp))$	**QTaut**
5	$(\alpha \sqsupset \bot) \sqsupset (\alpha\sqsupset \perp\!\!\!\perp)$	**QMP**: 3,4
6	$(\alpha \Rightarrow \bot) \sqsupset (\alpha \sqsupset \bot)$	**Lift**$\Rightarrow$
7	$(\alpha \Rightarrow \bot) \sqsupset (\alpha\sqsupset \perp\!\!\!\perp)$	**HypSyl**: 5,6

◇

The axiomatization also enjoys the metatheorem of deduction :

Theorem 3.13 (Metatheorem of deduction) Let Γ be a set of quantum formulas and γ_1, γ_2 be quantum formulas. Then,

$$\Gamma \cup \{\gamma_1\} \vdash \gamma_2 \text{ iff } \Gamma \vdash \gamma_1 \sqsupset \gamma_2.$$

Proof: ($\leftarrow$) Assume that $\Gamma \vdash \gamma_1 \sqsupset \gamma_2$. Let Π be a proof of the derivation $\Gamma \vdash \gamma_1 \sqsupset \gamma_2$ and assume that the length of Π is n. We can extend Π to obtain $\Gamma \cup \{\gamma_1\} \vdash \gamma_2$ as follows:

n	$\gamma_1 \sqsupset \gamma_2$	Π
n+1	γ_1	**Hyp**
n+2	γ_2	**QMP**: n,n+1

($\rightarrow$) Assume that $\Gamma \cup \{\gamma_1\} \vdash \gamma_2$. We will prove $\Gamma \vdash \gamma_1 \sqsupset \gamma_2$ by induction on n, the length of proof of $\Gamma \cup \{\gamma_1\} \vdash \gamma_2$. The base step $n = 1$ will be subsumed by the inductive step. In the inductive step, we consider the last rule applied. There are three cases:

- γ_2 is either an hypothesis or an axiom. In this case:

1	γ_2	axiom or hypothesis
2	$\gamma_2 \sqsupset (\gamma_1 \sqsupset \gamma_2)$	**QTaut**
3	$\gamma_1 \sqsupset \gamma_2$	**QMP**: 1,2

- γ_2 is obtained from γ and $\gamma \sqsupset \gamma_2$ by **QMP** where γ and $\gamma \sqsupset \gamma_2$ are also derived from $\Gamma \cup \{\gamma_1\}$. Then, by the induction hypothesis,

  - $\Gamma \vdash \gamma_1 \sqsupset \gamma$;
  - $\Gamma \vdash \gamma_1 \sqsupset (\gamma \sqsupset \gamma_2)$

  Let Π_1 and Π_2 be the proofs of $\Gamma \vdash \gamma_1 \sqsupset \gamma$ and $\Gamma \vdash \gamma_1 \sqsupset (\gamma \sqsupset \gamma_2)$ of lengths m_1 and m_2, respectively. Let m_3 be $m_1 + m_2$. The proof of $\Gamma \vdash \gamma_1 \sqsupset \gamma_2$ is as follows:

$m_1.$	$\gamma_1 \sqsupset \gamma$	Π_1
$m_3.$	$\gamma_1 \sqsupset (\gamma \sqsupset \gamma_2)$	Π_2
$m_3 + 1.$	$(\gamma_1 \sqsupset (\gamma \sqsupset \gamma_2)) \sqsupset ((\gamma_1 \sqsupset \gamma) \sqsupset (\gamma_1 \sqsupset \gamma_2))$	**QTaut**
$m_3 + 2.$	$(\gamma_1 \sqsupset \gamma) \sqsupset (\gamma_1 \sqsupset \gamma_2)$	**QMP**: m_3,$m_3 + 1$
$m_3 + 3.$	$\gamma_1 \sqsupset \gamma_2$	**QMP**: m_1,$m_3 + 2$

- γ_2 is obtained from γ and $\gamma \Rightarrow \gamma_2$ by **CMP** where γ and $\gamma \Rightarrow \gamma_2$ are also derived from $\Gamma \cup \{\gamma_1\}$. Then, by the induction hypothesis,

  - $\Gamma \vdash \gamma_1 \sqsupset \gamma$;
  - $\Gamma \vdash \gamma_1 \sqsupset (\gamma \Rightarrow \gamma_2)$.

  By the axiom **Lift**$\Rightarrow$ we also have $\Gamma \vdash (\gamma \Rightarrow \gamma_2) \sqsupset (\gamma \sqsupset \gamma_2)$.

By hypothetical syllogism (Lemma 3.11) we also have $\Gamma \vdash \gamma_1 \sqsupset (\gamma \sqsupset \gamma_2)$. The proof now proceeds as in the previous case. $\diamond$

We get as a corollary:

Corollary 3.14 (Metatheorem of reductio ad absurdum) Let Γ be a set of quantum formulas and γ be a quantum formula. Then,

$$\text{If } \Gamma \cup \{\gamma\} \vdash \perp\!\!\!\perp \text{ then } \Gamma \vdash \boxminus \gamma.$$

We use the metatheorem of equivalence to derive the following theorems:

Proposition 3.15 For every classical formulas α_1 and α_2 and subsets $G_1, G_2 \in \mathsf{qB}$, we have

$$\begin{array}{ll} [\textbf{Lift}\equiv] & \vdash (\alpha_1 \Leftrightarrow \alpha_2) \sqsupset (\alpha_1 \equiv \alpha_2). \\ [\textbf{Sub}\cap] & \vdash_F ([G_1] \sqsupset ([G_2] \sqsupset [G_1 \cap G_2])). \end{array}$$

Proof: We shall use metatheorem of deduction to show each of the theorems:

Lift$\equiv$**.** It suffices to show that $(\alpha_1 \Leftrightarrow \alpha_2) \vdash (\alpha_1 \equiv \alpha_2)$

1	$(\alpha_1 \Rightarrow \alpha_2) \wedge (\alpha_2 \Rightarrow \alpha_1)$	Hyp
2	$((\alpha_1 \Rightarrow \alpha_2) \wedge (\alpha_2 \Rightarrow \alpha_1)) \Rightarrow (\alpha_1 \Rightarrow \alpha_2)$	**CTaut**
3	$(\alpha_1 \Rightarrow \alpha_2)$	**CMP**: 1,2
4	$(\alpha_1 \Rightarrow \alpha_2) \sqsupset (\alpha_1 \sqsupset \alpha_2)$	**Lift**$\Rightarrow$
5	$(\alpha_1 \sqsupset \alpha_2)$	**QMP**: 3, 4
6	$((\alpha_1 \Rightarrow \alpha_2) \wedge (\alpha_2 \Rightarrow \alpha_1)) \Rightarrow (\alpha_2 \Rightarrow \alpha_1)$	**CTaut**
7	$(\alpha_2 \Rightarrow \alpha_1)$	**CMP**: 1,2
8	$(\alpha_2 \Rightarrow \alpha_1) \sqsupset (\alpha_2 \sqsupset \alpha_1)$	**Lift**$\Rightarrow$
9	$(\alpha_2 \sqsupset \alpha_1)$	**QMP**: 7, 8
10	$(\alpha_1 \sqsupset \alpha_2) \sqsupset ((\alpha_2 \sqsupset \alpha_1) \sqsupset (\alpha_1 \equiv \alpha_2))$	**QTaut**
11	$(\alpha_2 \sqsupset \alpha_1) \sqsupset (\alpha_1 \equiv \alpha_2)$	**QMP**: 5,10
12	$(\alpha_1 \equiv \alpha_2)$	**QMP**: 9,11

Sub$\cap$. It suffices to show that $[G_1], [G_2] \vdash [G_1 \cap G_2]$

1	$[G_1]$	Hyp
2	$[G_1] \sqsupset [\mathsf{qB} \setminus G_1]$	**Sub**$\setminus$
3	$[\mathsf{qB} \setminus G_1]$	**QMP**: 1,2
4	$[G_2]$	Hyp
5	$[G_2] \sqsupset [\mathsf{qB} \setminus G_2]$	**Sub**$\setminus$
6	$[\mathsf{qB} \setminus G_2]$	**QMP**: 4,5
7	$[\mathsf{qB} \setminus G_1] \sqsupset ([\mathsf{qB} \setminus G_2] \sqsupset [\mathsf{qb} \setminus (G_1 \cap G_2)])$	**Sub**$\cup$
8	$[\mathsf{qB} \setminus G_2] \sqsupset [\mathsf{qb} \setminus (G_1 \cap G_2)]$	**QMP**: 3,7
9	$[\mathsf{qb} \setminus (G_1 \cap G_2)]$	**QMP**: 6,8
10	$[\mathsf{qb} \setminus (G_1 \cap G_2)] \sqsupset [G_1 \cap G_2])$	**Sub**$\setminus$
11	$[G_1 \cap G_2]$	**QMP**: 9,10

$\diamond$

We also have the principles of substitution of equal terms and equivalent formulas.

Theorem 3.16 (Principle of substitution of equal terms) Given a quantum formula γ, two real terms t_1 and t_2, let γ' be a quantum formula obtained from γ by replacing zero or more occurrences of t_1 in γ_1 by t_2. Then,

$$\vdash t_1 = t_2 \sqsupset (\gamma \equiv \gamma').$$

Proof: The proof is by a straightforward induction on the structure of γ. We note that in the case where γ is $t \leq t'$, we use the axiom **RCF**. The other cases are immediate. $\diamond$

Substitution of equivalent terms preserves quantum equivalence:

Theorem 3.17 (Principle of substitution of equivalent formulas) Given three quantum formulas γ, γ_1 and γ_2, let γ' be obtained from γ by replacing zero or more q-occurrences of γ_1 in γ by γ_2. Then,

$$\vdash (\gamma_1 \equiv \gamma_2) \sqsupset (\gamma \equiv \gamma').$$

Proof: The case γ_1 does not q-occur in γ is trivial. We just consider the case in which γ_1 has at least one q-occurrence in γ and γ' is obtained by replacement of at least one such q-occurrence. The proof is carried out by induction on the structure of γ. There are two cases:

1. γ is a quantum atom or $\perp\!\!\!\perp$. Then γ_1 is γ, γ_1 q-occurs in γ exactly once, and replacement of q-occurrence of γ_1 in γ by γ_2 yields γ_2. Hence, in that case γ' is γ_2. So the theorem holds trivially by the following assertion (justified by the axiom **QTaut**):

$$\vdash (\gamma_1 \equiv \gamma_2) \sqsupset (\gamma_1 \equiv \gamma_2).$$

2. γ is $\gamma_a \sqsupset \gamma_b$. Then there are two cases.

   - γ_1 is γ. Then the theorem follows as in the previous case.
   - γ_1 q-occurs in γ_a or γ_b (it may occur in both). Let γ' be $\gamma'_a \sqsupset \gamma'_b$ where γ'_a and γ'_b are obtained by replacing zero or more occurrences of γ_a and γ_b respectively. Then, by the induction hypothesis we have

     $$(\gamma_1 \equiv \gamma_2) \vdash (\gamma_a \equiv \gamma'_a)$$

     and

     $$(\gamma_1 \equiv \gamma_2) \vdash (\gamma_b \equiv \gamma'_b).$$

     We show that

     $$(\gamma_1 \equiv \gamma_2), \gamma \vdash \gamma'$$

     as follows.

1	$\gamma_1 \equiv \gamma_2$	Hyp
2	$\gamma_a \sqsupset \gamma_b$	Hyp
3	$\gamma_b \sqsupset \gamma'_b$	1, Induction Hypothesis
4	$\gamma_a \sqsupset \gamma'_b$	2, 3, **HypSyl**
5	$\gamma'_a \sqsupset \gamma_a$	1, Induction Hypothesis
6	$\gamma'_a \sqsupset \gamma'_b$	4,5, **HypSyl**

     We can show similarly that

     $$(\gamma_1 \equiv \gamma_2), \gamma' \vdash \gamma.$$

     The theorem now follows from metatheorem of deduction.

$\diamond$

We get as a corollary that substitution of classically equivalent formulas preserves quantum equivalence:

Corollary 3.18 Given a quantum formula γ, two classical formulas α_1, α_2, let γ' be obtained from γ by replacing zero or more q-occurrences of α_1 in γ by α_2. Then

$$\vdash (\alpha_1 \Leftrightarrow \alpha_2) \sqsupset (\gamma \equiv \gamma').$$

Proof: We observe that by **Lift**$\Leftrightarrow$, we have $\vdash (\alpha_1 \Leftrightarrow \alpha_2) \sqsupset (\alpha_1 \equiv \alpha_2)$. The result then follows from principle of substitution of equivalent formulas and hypothetical syllogism. $\diamond$

Please note that we are only concerned with occurrence of classical formulas only as quantum sub-formulas and not as classical formulas. Indeed, replacement of a classical formula by a quantum formula may not always yield valid a quantum formula. Even in the case it yields a valid quantum formula, the principle of substitution does not hold. For example, let α_1 be qb_1, α_2 be qb_2 and γ be qb_3. Now, consider the quantum formula:

$$(\mathsf{qb}_1 \equiv \mathsf{qb}_2) \sqsupset ((\mathsf{qb}_1 \Rightarrow \mathsf{qb}_3) \equiv (\mathsf{qb}_2 \Rightarrow \mathsf{qb}_3)).$$

Let V be the set of two valuations v_1, v_2 such that:

- $v_1(\mathsf{qb}_1) = v_1(\mathsf{qb}_3) = 0$, $v_1(\mathsf{qb}_2) = 1$;
- $v_2(\mathsf{qb}_1) = v_2(\mathsf{qb}_3) = 1$, $v_2(\mathsf{qb}_2) = 0$.

Any quantum structure with V as the set of valuations would then invalidate the above quantum formula.

4 Completeness and decidability

We shall prove weak completeness of dEQPL – if Γ is a finite set of quantum formulas, then $\Gamma \vDash \gamma$ implies that $\Gamma \vdash \gamma$. As our proof system enjoys principle of deduction, it suffices to demonstrate weak completeness when the set Γ is empty. The proof of weak completeness will go hand-in-hand with the proof of decidability, and can be adapted to a proof of strong completeness as we will sketch later.

The proof of weak completeness essentially follows the proof in [28], which in turn was inspired by the Fagin-Megiddo-Halpern technique for probabilistic logic [18]. The main difference is in the way the sub-system formulas are treated here. The other difference is that the proof is carried out in a manner so as to facilitate the proof of decidability.

The central result in the proof is the Model Existence Lemma, namely, if γ is consistent then there is a quantum structure $\mathbf{w}$ and an assignment ρ such that $\mathbf{w}\rho \Vdash \gamma$. A quantum formula γ is said to be *consistent* if $\nvdash (\boxminus \gamma)$. It

will suffice to show that the model existence lemma holds for specials kinds of quantum formula, namely *quantum molecular formulas*. A quantum molecular formula is a quantum disjunction of *quantum literals* (a quantum literal is either a quantum atom or the quantum negation of a quantum atom). Please recall that quantum atoms are classical formulas, comparison terms and sub-system assertions.

The first steps in the proof of the Model Existence Lemma are to remove the probability and alternative terms using the axioms **Prob**, **If**$\top$ and **If**$\bot$. Next, we use the weak completeness of classical propositional logic to construct the set of valuations V in the envisaged quantum structure. The partition S is constructed by considering the sub-system literals in the quantum molecule, and the construction is guided by the fact that sub-systems are closed under set operations (axioms **Sub**$\emptyset$, **Sub**$\cup$ and **Sub**$\setminus$). The logical amplitudes ν_{GA} are constructed by first adding all consistent equations using the axioms **NAdm**, **Unit**, **Empty** and **Mul**, and then "solving" for the (in)equations in the quantum molecule using **RCF**.

Before proceeding with carrying out the above outline, we start with a few abbreviations and notations. We introduce the following abbreviation where $Q \subset \mathsf{qAtom}$ and $D \subseteq Q$:

- $(\bigsqcap_Q D)$ for $((\bigsqcap_{\mu \in D}\ \mu) \sqcap (\bigsqcap_{\mu \in (Q \setminus D)} (\boxminus \mu)))$.

We shall say that D is the positive part of the quantum molecule $(\bigsqcap_Q D)$ and that $Q \setminus D$ is its negative part. Given a molecule η, we denote by η^+ and η^- the positive and negative parts respectively. We denote by η_c the conjunction of the classical literals in η. In a similar way we define $\eta_\leq$ and η_s.

As is the case with classical propositional logic, every dEQPL formula has a *quantum disjunctive normal form*. A quantum formula is said to be in quantum disjunctive normal form if it is a disjunction of quantum molecules.

Proposition 4.1 Every quantum formula is equivalent to a quantum disjunctive normal form. Furthermore, there is an algorithm that computes the quantum disjunctive normal form.

Proof: It is easier to prove a stronger result. That is, we show that any quantum formula η has both a quantum disjunctive normal form and a quantum conjunctive normal form. We say that η is in quantum conjunctive normal form if it is a quantum conjunction of quantum disjunctions of literals. The proof is constructive and follows by induction on the structure of the quantum formula as in the case of classical logic. The construction also gives the algorithm for computing the normal forms. $\diamond$

From now on we will assume that every quantum formula is in quantum disjunctive normal form. The following proposition will ensure that to decide consistency of a quantum formula we only need to check if one of its molecules is consistent.

Proposition 4.2 A quantum formula is consistent iff one of its molecules is consistent.

Proof: ($\Rightarrow$) It suffices to show that the quantum disjunction of two inconsistent quantum formulas γ_1 and γ_2 is inconsistent. If γ_1 and γ_2 are inconsistent then $\vdash (\boxminus \gamma_1)$ and $\vdash (\boxminus \gamma_2)$. We can easily show that in this case $\vdash \boxminus(\gamma_1 \sqcup \gamma_2)$ as follows:

1	$\vdash (\boxminus \gamma_1) \sqsupset ((\boxminus \gamma_2) \sqsupset \boxminus(\gamma_1 \sqcup \gamma_2))$	**QTaut**
2	$\vdash (\boxminus \gamma_1)$	Hyp
3	$\vdash (\boxminus \gamma_2)$	Hyp
4	$(\boxminus \gamma_2) \sqsupset \boxminus(\gamma_1 \sqcup \gamma_2)$	**QMP**: 1,2
5	$\boxminus(\gamma_1 \sqcup \gamma_2)$	**QMP**: 3,4

Hence the formula, $(\gamma_1 \sqcup \gamma_2)$ is inconsistent.

($\Leftarrow$) Assume that η is inconsistent. Then $\vdash (\boxminus \eta)$. Let η be $\eta_1 \sqcup \ldots \sqcup \eta_n$. By **QTaut**, $\vdash (\boxminus \eta) \equiv (\boxminus \eta_1 \sqcap \ldots \sqcap \boxminus \eta_n)$. Using **QMP** and **QTaut** we can easily show that η_i is inconsistent for $i = 1, \ldots, n$. $\diamond$

The first step in the proof is to remove the probability terms.

Proposition 4.3 Given a quantum molecule η, there is a η' such that η' has no probability terms and $\vdash \eta \equiv \eta'$. Furthermore, there is an algorithm that computes η'.

Proof: Let η be a molecule. For every probability term of the form $(\int \alpha)$ replace it by $(\sum_A |\langle \alpha \rangle_A|^2))$. Then by axiom **Prob** and the principle of substitution of equal terms, the resulting formula is equivalent to η. $\diamond$

The following proposition allows us to remove alternative terms in quantum molecules.

Proposition 4.4 A quantum molecule η is consistent iff there is a consistent quantum molecule η' such that η' has no alternative terms and $\vdash (\eta' \sqsupset \eta)$. Moreover, if there is an algorithm for deciding the consistency of quantum molecules without alternative terms then there is an algorithm for deciding the consistency of quantum molecules.

Proof: The existence of a consistent η' such that $\vdash (\eta' \sqsupset \eta)$ clearly implies the consistency of η. For the other direction, consider an ordering $\alpha_0, \ldots, \alpha_m$ of the guards of alternative terms occurring in η. Let α_i^0 be α_i and α_i^1 be $\boxminus \alpha_i$ for $i = 0, \ldots, m$.

Given $b_0 \ldots b_m \in \{0,1\}^m$, let

$$\eta_{b_0 \ldots b_m} := \eta \sqcap \alpha_0^{b_0} \sqcap \ldots \sqcap \alpha_m^{b_m}.$$

Using **QTaut** we get,

$$\vdash \eta \equiv \bigsqcup_{b_0 \ldots b_m \in \{0,1\}^m} \eta_{b_0 \ldots b_m}.$$

Observe that, using the axioms **If**$\top$ and **If**$\bot$ and the principle of substitution of equal terms, each $\eta_{b_0 \ldots b_m}$ is equivalent to a formula in which the alternative $(\alpha_i \rhd u_i^0; u_i^1)$ is replaced by $u_i^{b_i}$. Let $\overline{\eta}_{b_0 \ldots b_m}$ be the resulting formula. Therefore,

$$\vdash \eta \equiv \bigsqcup_{b_0 \ldots b_m \in \{0,1\}^m} \overline{\eta}_{b_0 \ldots b_m}.$$

With a reasoning similar to the one in Proposition 4.2, we conclude that η is consistent iff $\overline{\eta}_{b_0 \ldots b_m}$ is consistent for some $b_0 \ldots b_m \in \{0,1\}^m$. Please note that $\vdash \overline{\eta}_{b_0 \ldots b_m} \sqsupset \eta$ for each $b_0 \ldots b_m \in \{0,1\}^m$.

Finally, as the construction of each $\overline{\eta}_{b_0 \ldots b_m}$ can be defined by an algorithm, we get the proposition. $\diamond$

We shall now build the set of classical valuations V. Given a classical formula α and a non-empty set of valuations V, we write $V \Vdash_c \alpha$ if every element of V classically satisfies α. We say that $V \Vdash_c \eta$ if $V \Vdash_c \alpha$ for every $\alpha \in \eta_c^+$ and $V \nVdash_c \beta$ for every $\beta \in \eta_c^-$.

We will consider only a special kind of molecular formulas which will allow us to deal with the restrictions imposed by the axiom **NAdm**. Please recall that given $A \subseteq \mathsf{qB}$, v_A is the valuation that assigns true to qubit symbols in A and false to qubit symbols in $\mathsf{qb} \setminus A$. A molecular formula η is said to be *maximal with respect to admissible classical valuations* if for every subset A of qB and set of valuations V such that $V \Vdash_c \eta$, we have:

$$v_A \notin V \text{ iff } (\neg(\wedge A)) \in \eta_c^+.$$

The following proposition ensures that it suffices to consider molecular formulas maximally consistent with classical valuations.

Proposition 4.5 A molecule η is consistent iff there is a consistent molecule η' such that η' is maximal with respect to admissible classical valuations and $\vdash \eta' \sqsupset \eta$. Moreover, if there is an algorithm for deciding the consistency of quantum molecules maximal with respect to admissible valuations then there is an algorithm for deciding consistency of quantum molecules.

Proof: Let $A_1, \ldots, A_m$ be an ordering of the subsets of qB. Let A_i^0 be $(\neg(\wedge A_i))$ and A_i^1 be $\boxminus(\neg(\wedge A_i))$ for $i = 0, \ldots, m$. Given $b_0 \ldots b_m \in \{0,1\}^m$, let

$$\eta_{b_0 \ldots b_m} := \eta \sqcap A_0^{b_0} \sqcap \ldots \sqcap A_m^{b_m}.$$

Using **QTaut**,

$$\vdash \eta \equiv \bigsqcup_{b_0 \ldots b_m \in \{0,1\}^m} \eta_{b_0 \ldots b_m}.$$

With a reasoning similar to the one in Proposition 4.2, we can conclude that η is consistent iff $\eta_{b_0 \ldots b_m}$ is consistent for some $b_0 \ldots b_m \in \{0,1\}^m$. Please note that $\vdash \eta_{b_0 \ldots b_m} \sqsupset \eta$ for each $b_0 \ldots b_m \in \{0,1\}^m$. We claim that each $\eta_{b_0 \ldots b_m}$ is maximal with respect to admissible valuations. Fix one $\eta_{b_0 \ldots b_m}$.

Let V be a set of valuations such that $V \Vdash_c \eta_{b_0 \ldots b_m}$. We will show that

$$v_{A_i} \notin V \text{ iff } (\neg(\wedge A_i)) \in (\eta_{b_0 \ldots b_m})_c^+.$$

Clearly if $(\neg(\wedge A_i)) \in (\eta_{b_0 \ldots b_m})_c^+$ then $v_{A_i} \notin V$.

For the other part, if $v_{A_i} \notin V$ it suffices to show that $b_i = 0$. Suppose that $b_i = 1$. Then $V \nVdash_c (\neg(\wedge A_i))$. That means there is $v \in V$ such that $v \nVdash_c (\neg(\wedge A_i))$. This means that $v \Vdash_c \wedge A_i$ which in turn implies that v is equal to v_{A_i}. Therefore $v_{A_i} \in V$ contradicting the assumption $b_i = 1$.

As the construction of $\eta_{b_0 \ldots b_m}$ can be defined by an algorithm, we get the proposition. $\diamond$

We will say that η is *g-satisfiable* if there is a set of valuations V such that $V \Vdash_c \eta$. Given a consistent molecule η, we now construct V such that $V \Vdash_c \eta$ as follows.

Lemma 4.6 (g-satisfiability) If η is consistent then η is g-satisfiable. Furthermore, there is an algorithm to decide if η is g-satisfiable.

Proof: Let V be the set of valuations v such that $v \Vdash_c \alpha$ for every $\alpha \in \eta_c^+$. This set can be computed since the set of qubit symbols is finite.

If V is empty then η is not g-satisfiable. If V is not empty, then η is g-satisfiable iff $V \nVdash_c \beta$ for every $\beta \in \eta_c^-$. As V and η_c^- are finite sets, this gives us an algorithm to check if η is g-satisfiable.

Assume that η is a consistent formula. Please note that using the theorem **Lift**$\wedge$ and the principle of substitution, it is easy to show that if η is consistent then $(\wedge_{\alpha \in \eta_c^+} \alpha)$ is consistent as a classical propositional formula.

We show that η is g-satisfiable. As $(\wedge_{\alpha \in \eta_c^+} \alpha)$ is consistent (in propositional logic), there is a classical valuation v that satisfies every α. As above, let V be the set of valuations v such that $v \Vdash_c \alpha$ for every $\alpha \in \eta_c^+$. It suffices to show that $V \nVdash_c \beta$ for every $\beta \in \eta_c^-$.

We proceed by contradiction. Assume that there is $\beta \in \eta_c^-$ such that $V \Vdash_c \beta$. Fix one such β say β_0. Therefore, by construction of V, we get:

$$\Vdash_c \left(\left(\bigwedge_{\alpha \in \eta_c^+} \alpha \right) \Rightarrow \beta_0 \right).$$

So, by **CTaut** we get:

$$\vdash \left(\left(\bigwedge_{\alpha \in \eta_c^+} \alpha \right) \Rightarrow \beta_0 \right).$$

Thus, by **Lift**$\Rightarrow$, we obtain

$$\vdash \left(\left(\bigwedge_{\alpha \in \eta_c^+} \alpha \right) \sqsupset \beta_0 \right).$$

Thus, by **Ref**$\sqcap$ and **QTaut** (transitivity of $\sqsupset$) we get

$$\vdash \left(\left(\bigsqcap_{\alpha \in \eta_c^+} \alpha \right) \sqsupset \beta_0 \right).$$

Therefore, by **QTaut** (right weakening of $\sqsupset$)

$$\vdash \left(\left(\bigsqcap_{\alpha \in \eta_c^+} \alpha \right) \sqsupset \left(\bigsqcup_{\beta \in \eta_c^-} \beta \right) \right)$$

leading to

$$\vdash \left(\boxminus \left(\left(\bigsqcap_{\alpha \in \eta_c^+} \alpha \right) \sqcap \left(\bigsqcap_{\beta \in \eta_c^-} (\boxminus \beta) \right) \right) \right)$$

by several obvious tautological steps. That is, we have $\vdash (\boxminus \eta)$, contradicting the consistency of η. $\diamond$

Please observe that if η has neither probability nor alternative terms then η' as constructed in the above proof also does not have probability and alternative terms.

Given a sub-system formula $[G]$ and a partition $\mathcal{S}$ of the set of qubits, we write $\mathcal{S} \Vdash_s [G]$ if $G \in \mathrm{Alg}(\mathcal{S})$. We say that $\mathcal{S} \Vdash_s \eta$ if $\mathcal{S} \Vdash_s [G]$ for every $[G] \in \eta_s^+$ and $\mathcal{S} \nVdash_s [G]$ for every $[G] \in \eta_s^-$. We will say that η is *s-satisfiable* if there is a partition $\mathcal{S}$ such that $\mathcal{S} \Vdash_s \eta$. We construct the partition S in the proof of Model Existence Lemma as follows.

Lemma 4.7 (*s*-satisfiability) If η is consistent then η is s-satisfiable. There is an algorithm to decide if η is s-satisfiable.

Proof:

Assume that η is consistent. We will show that η is s-satisfiable. Please recall that an algebra of sets on a domain X is a non-empty collection of subsets of X closed under complements and unions. Let $\mathrm{Alg}(\eta_s^+)$ be the smallest algebra on qB containing η_s^+.

Find the minimal elements for $\mathrm{Alg}(\eta_s^+)$: a set $G \in \mathrm{Alg}(\eta_s^+)$ is minimal if $G' \subseteq G$ and $G \in \mathrm{Alg}(\eta_s^+)$ implies that G' is either the empty set or G itself. Take $\mathcal{S}$ to be the set of minimal elements of $\mathrm{Alg}(\eta_s^+)$ (it can be easily shown that they form a partition). Therefore, by construction, $\mathcal{S} \Vdash_s [G]$ for every $[G] \in \eta_s^+$.

If $[H] \in \eta_s^-$ then we need to show $[H] \notin \mathrm{Alg}(\eta_s^+)$. We proceed by contradiction and assume $H \in \mathrm{Alg}(\eta_s^+)$. Then $H = H_1 \cup \ldots \cup H_m$, where either $H_i \in \eta_s^+$ or $\mathsf{qB} \setminus H_i \in \eta_s^+$ for each $1 \leq i \leq m$. Using the axioms **QTaut**, **Sub**$\setminus$ and **Sub**$\cup$, we can show that

$$\vdash \eta \equiv \eta \sqcap [H].$$

Now as $[H] \in \eta_s^-$, we get

$$\vdash \eta \equiv \eta \sqcap [H] \equiv \eta \sqcap [H] \sqcap \boxminus [H].$$

Now, by **QTaut**,

$$\vdash (\eta \sqcap [H] \sqcap \boxminus[H]) \sqsupset \perp\!\!\!\perp .$$

Then, by principle of substitution of equivalent formulas, we get

$$\vdash (\boxminus \eta).$$

This contradicts the consistency of η.

The algorithm for checking the s-consistency is as follows. Take η_s^+ and generate the algebra $\mathrm{Alg}(\eta_s^+)$ with them. This algebra can be computed since the set of qubit symbols is finite. The formula η is s-satisfiable iff $G \notin \mathrm{Alg}(\eta_s^+)$ for every $[G] \in \eta_s^-$. This can be checked by an algorithm again as the set of qubits is finite. $\diamond$

We are now ready to construct the model (the amplitudes ν_{GA} will be constructed in the proof). We need some auxiliary definitions. Recall that assignments are enough to interpret the arithmetical formulas. Let κ be a quantum conjunction of comparison literals. Let $\mathcal{K}$ be a real closed field with algebraic closure $\mathcal{K}(\delta)$ and ρ be a $\mathcal{K}$-assignment. We say that $\mathcal{K}(\delta)$, $\rho \Vdash_i \kappa$ if

- $[\![s]\!]_\rho \leq [\![t]\!]_\rho$ if $s \leq t \in \kappa^+$;
- $[\![s]\!]_\rho \not\leq [\![t]\!]_\rho$ if $s \leq t \in \kappa^-$.

We say that ρ is a *solution* of κ in $\mathcal{K}(\delta)$. We say that κ is $\leq$-*consistent* if there is a real closed field $\mathcal{K}$ with algebraic closure $\mathcal{K}(\delta)$, and a $\mathcal{K}$-assignment ρ such that $\mathcal{K}(\delta)$, $\rho \Vdash_i \kappa$. Please note that the theory of elimination of quantifiers ensures that there is an algorithm to decide the $\leq$-consistency [24, 6].

Theorem 4.8 (Model Existence Theorem) If the molecule η is consistent then there is a quantum structure $\mathbf{w} = (\mathcal{K}, \delta, V, \mathcal{S}, |\psi\rangle, \nu)$ and a $\mathcal{K}$-assignment ρ such that $\mathbf{w}\rho \Vdash \eta$.

Proof: As a result of Propositions 4.3 and 4.4, we can assume that η does not have any probability and alternative terms and is maximally consistent with respect to admissible valuations.

Using Lemma 4.6 and Lemma 4.7, we find V and $\mathcal{S}$ such that $V \Vdash_c \eta$ and $\mathcal{S} \Vdash_s \eta$. We can show that $\vdash \eta \equiv (\eta \sqcap \bigsqcap_{[G] \in \mathrm{Alg}(\mathcal{S})} [G])$ using axioms **Sub**$\emptyset$, **Sub**$\cup$ and **Sub**$\setminus$.

Please observe that the axiom **Unit** allows us to establish for every $[G] \in \mathrm{Alg}(\mathcal{S})$:

$$\vdash \eta \sqsupset (\sum_{A \subseteq G} |\langle \top \rangle_{GA}|^2 = 1).$$

Let η_1 be the formula

$$\eta \sqcap \bigsqcap_{G \in \mathrm{Alg}(\mathcal{S})} (\sum_{A \subseteq G} |\langle \top \rangle_{GA}|^2 = 1).$$

As a result we get that $\vdash (\eta_1 \equiv \eta)$.

We also get as a result of the axiom **NAdm**, for every $(\neg(\wedge A))$ occurring in η:

$$\vdash \eta_1 \sqsupset (|\top\rangle_{\mathsf{qB}A} = 0).$$

Let η_2 be the formula

$$\eta_1 \sqcap \bigsqcap_{(\neg(\wedge A)) \text{ in } \eta_c^+} (|\top\rangle_{\mathsf{qB}A} = 0).$$

As a result of axiom **Mul**, for every G_1, G_2, A_1, A_2 such that $G_1, G_2 \in \mathrm{Alg}(\mathcal{S})$, $A_1 \subseteq G_1$ and $A_2 \subseteq G_2$, we get

$$\vdash \eta_2 \sqsupset (|\top\rangle_{G_1 \cup G_2 A_1 \cup A_2} = |\top\rangle_{G_1 A_1} |\top\rangle_{G_2 A_2}).$$

Let η_3 be the formula

$$\eta_2 \sqcap \bigsqcap_{\substack{G_1, G_2 \in \mathrm{Alg}(\mathcal{S}) \\ A_1 \subseteq G_1, A_2 \subseteq G_2}} (|\top\rangle_{G_1 \cup G_2 A_1 \cup A_2} = |\top\rangle_{G_1 A_1} |\top\rangle_{G_2 A_2}).$$

The axiom **Empty** gives us

$$\vdash \eta_3 \sqsupset (|\top\rangle_{\emptyset\emptyset} = 1).$$

Let $\eta^\bullet$ be the formula

$$\eta_3 \sqcap (|\top\rangle_{\emptyset\emptyset} = 1).$$

Observe that we can show:

$$\vdash (\eta \equiv \eta^\bullet).$$

Please recall that $\eta^\bullet{}_{\leq}$ is the conjunction of the (in)equations in $\eta^\bullet$. Let η_R be the formula obtained from $\eta^\bullet$ by replacing each term of the form $|\top\rangle_{GA}$ by a fresh variable $z_{|\top\rangle_{GA}}$. Please observe that $\eta^\bullet$ is $\eta_R\{\!\{z_{|\top\rangle_{GA}} / \ |\top\rangle_{GA}\}\!\}$.

Now, either there is a real closed field $\mathcal{K}$ with $\mathcal{K}(\delta)$ as its algebraic closure, and a $\mathcal{K}$-assignment ρ such that $K(\delta)$, $\rho \Vdash_i (\eta_R)_{\leq}$ or not. If there is no such $\mathcal{K}$ and ρ then it must be the case that $\boxminus(\eta_R)_{\leq}$ is a valid arithmetic formula. So, by axiom **RCF**,

$$\vdash (\boxminus(\eta_R)_{\leq})\{\!\{z_{|\top\rangle_{GA}} / \ |\top\rangle_{GA}\}\!\}.$$

However, the formula $(\boxminus(\eta_R)_{\leq})\{\!\{z_{|\top\rangle_{GA}} / \ |\top\rangle_{GA}\}\!\}$ is $(\boxminus \eta_{\leq})$ and this will imply that η is inconsistent.

Therefore there are $\mathcal{K}(\delta)$ and ρ such that $\mathcal{K}(\delta)$, $\rho \Vdash_i (\eta_R)_{\leq}$. We fix such a $\mathcal{K}$, $\mathcal{K}(\delta)$ and ρ.

We now construct $|\psi\rangle = \{|\psi\rangle_S\}_{S \in \mathcal{S}}$ as follows:

- $|\psi\rangle_{[\emptyset]} = 1$;
- Let $\nu_{SA} = \rho(z_{|\top\rangle_{SA}})$ for every $S \in \mathcal{S}$ and $A \subseteq S$. Then,

$$|\psi\rangle_{[S]} = \sum_{A \subseteq S} \nu_{SA} |v_A^S\rangle.$$

We construct $\nu = \{\nu_{GA}\}_{G \subset \mathsf{qB}, A \subseteq G}$ as follows:

$$\nu_{GA} = \begin{cases} \rho(z_{|\top\rangle_{GA}}) & \text{if } z_{|\top\rangle_{GA}} \text{ is a variable in } \eta_R \\ 0 & \text{otherwise} \end{cases} .$$

Please note that, by construction $\nu_{GA} = \langle v_A^G | \psi \rangle_{[G]}$ if $G \in \mathrm{Alg}(\mathcal{S})$. Let $\mathbf{w}$ be $(\mathcal{K}, \delta, V, \mathcal{S}, |\psi\rangle, \nu)$. We can easily show that $\mathbf{w}$ is a quantum structure and $\mathbf{w}\rho \Vdash \eta$. $\diamond$

The decidability of consistency of molecular formulas follows as a corollary to the proof of the Model Existence Lemma.

Corollary 4.9 There is an algorithm to decide if a quantum molecule η is consistent.

Proof: As a result of Propositions 4.3 and 4.4, we can assume that η does not have any probability and alternative terms and is maximally consistent with respect to admissible valuations. Now as a result of the model existence lemma, all we need to do is to check if there is a quantum structure $\mathbf{w}$ such that $\mathbf{w} \Vdash \eta$. We refer to the proof of model existence lemma.

We first check if η is g-satisfiable and s-satisfiable which is algorithmic by Lemmas 4.6 and 4.7. If not then η is not consistent. Otherwise, let V and $\mathcal{S}$ be as in the proof of the model existence lemma.

Now, we construct η_R as in the same proof. Note that the construction is algorithmic. We check if $(\eta_R)_{\leq}$ is $\leq$-consistent or not. If it is not the case then η is not consistent. If $(\eta_R)_{\leq}$ is $\leq$-consistent then we can construct $\mathbf{w}$ as in that proof such that $\mathbf{w} \Vdash \eta$. Therefore η will be consistent if $(\eta_R)_{\leq}$ is $\leq$-consistent. $\diamond$

Please note any formula γ is equivalent to a disjunction of quantum molecular formulas. Furthermore, if γ is consistent, so is one of its molecules, say η. Theorem 4.8 gives a quantum structure $\mathbf{w}$ and an assignment ρ such that $\mathbf{w}\rho \models \eta$. As η is a quantum molecule of Γ we get easily $\mathbf{w}\rho \models \gamma$. Hence, if any quantum formula γ is consistent then γ has a model. We can now deduce the weak completeness of dEQPL in the standard way.

Theorem 4.10 (Completeness) The proof system of dEQPL is weakly complete, *i.e.*, $\models \gamma$ implies $\vdash \gamma$.

Proof:

We prove completeness by contradiction. Assume that $\nvdash \gamma$. So by **Qtaut** and **QMP**, we have $\nvdash (\boxminus(\boxminus \gamma))$. Therefore, $\boxminus \gamma$ is consistent, and hence there is a quantum structure $\mathbf{w}$ and an assignment ρ such that $\mathbf{w}\rho \models \boxminus \gamma$. Therefore, $\mathbf{w}\rho \not\models \gamma$. $\diamond$

Finally, we get the decidability of dEQPL.

Theorem 4.11 (Decidability) The set of theorems is decidable.

Proof: As a result of soundness and completeness we have, $\vdash \eta$ iff $\boxminus \eta$ is inconsistent. We can decide consistency of a formula by Corollary 4.9, Proposition 4.1 and Proposition 4.2. $\diamond$

We finish this section by observing two things. The first observation is that the proof of weak completeness can be adapted to a proof of strong completeness as follows. The key in the proof is again the Model Existence Lemma. Given a possibly infinite consistent set of quantum formulas Γ, we construct a maximally consistent set (the usual Henkin-Lindenbaum construction). Next, by looking at the classical formulas in Γ, we construct V using the strong completeness of propositional logic. The construction of the partition S is by considering the sub-system literals in Γ and is similar to the one in the above proof. Finally, just as in the proof above, we replace the amplitude terms in comparison-literals by fresh variables and "solve" the resulting equations using the strong completeness of first-order logic (note that as Γ is maximal all the maximally consistent information about logical amplitudes is already in Γ).

The second observation is that in our semantic structures, if G is the set of qubits of a sub-system then the qubits in G are necessarily not entangled with the rest. That is, the following is a theorem in dEQPL:

$$\vdash [G] \sqsupset \bigsqcap_{A_1 \subseteq G\,,\, A_2 \subseteq \mathsf{qB} \setminus G} (|\top\rangle_{\mathsf{qB}(A_1 \cup A_2)} = |\top\rangle_{GA_1} |\top\rangle_{(\mathsf{qB}\setminus G)A_2}).$$

In EQPL [28], the reverse implication was also true. That is in [28], it was the case that G is a sub-system if and only if the qubits in G are not entangled with the rest. We can extend our results to such semantic structures by considering the (finite) set of formulas $\Gamma = \{\gamma_G \,|\, G \subseteq \mathsf{qB}\}$ where

$$\gamma_G := ([G] \equiv (\bigsqcap_{A_1 \subseteq G\,,\, A_2 \subseteq \mathsf{qB} \setminus G} (|\top\rangle_{\mathsf{qB}(A_1 \cup A_2)} = |\top\rangle_{GA_1} |\top\rangle_{(\mathsf{qB}\setminus G)A_2}))).$$

Clearly $\Gamma \vDash \gamma$ if and only γ holds in all the semantic structures where every set of qubits not entangled with the rest forms a sub-system. If were to augment our axiom system with elements of Γ, then γ is a theorem in the augmented axiomatization if and only if $\Gamma \vdash \gamma$. The weak completeness and decidability in the augmented system then follow from the results of this section.

5 Application examples

As it is, dEQPL is appropriate for reasoning about quantum states only. For reasoning about the evolution of quantum systems through the application of measurements and unitary transformations we will need to extend it towards a dynamic logic, as already sketched in [26, 27].

Herein, we first illustrate how dEQPL can be used to reason about a Bell state. Afterwards, we turn our attention to quantum teleportation and outline there some of the relevant constructs of the envisaged dynamic logic. In the following examples, we write $|F\rangle$ as an abbreviation for the vector $(|\top\rangle_{FA})_{A \subseteq F}$ assuming the lexicographic ordering of the subsets of F. We may also abbreviate $\{\mathsf{qb}_{k_1}, \ldots, \mathsf{qb}_{k_m}\}$ by $\mathsf{qb}_{k_1,\ldots,k_m}$ in amplitude terms.

5.1 Reasoning about Bell states

Bell states were first discussed by Einstein, Podolsky and Rosen [17] and have been very useful in designing quantum protocols. An independent sub-system composed of a pair of qubits is said to be in a Bell state if they are maximally entangled. For instance,

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|10\rangle - |01\rangle)$$

is a Bell state.

In order to represent this pair in our logic, we choose two qubit symbols, say qb_0 and qb_1. The fact that these qubits are independent from other qubits can be written as

$$\gamma_{\text{ind}} := [\mathsf{qb}_0, \mathsf{qb}_1].$$

We can express the state as the following formula

$$\gamma_{\text{EPR}} := (|\mathsf{qb}_{01}\rangle = \frac{1}{\sqrt{2}}(0, -1, 1, 0)).$$

We can use our logic to derive that these qubits are necessarily entangled, that is, neither qb_0 nor qb_1 form an independent sub-system. In other words we will show that

$$\gamma_{\text{ind}}, \gamma_{\text{EPR}} \vdash \boxminus[\mathsf{qb}_0] \sqcap \boxminus[\mathsf{qb}_1].$$

The proof will follow by applying the metatheorem theorem of deduction. In particular, we show

$$\gamma_{\text{ind}}, \gamma_{\text{EPR}}, [\mathsf{qb}_0] \vdash \perp\!\!\!\perp,$$

as follows:

1	$[\mathsf{qb}_0, \mathsf{qb}_1]$	Hyp
2	$[\mathsf{qb}_0]$	Hyp
3	$([\mathsf{qb}_0, \mathsf{qb}_1] \sqsupset ([\mathsf{qb}_0] \sqsupset [\mathsf{qb}_1]))$	**SubDiff**
4	$([\mathsf{qb}_0] \sqsupset [\mathsf{qb}_1]))$	**QMP**: 1,3
5	$[\mathsf{qb}_1]$	**QMP** :2,4
6	$(\|\top\rangle_{\mathsf{qb}_{01}\emptyset} = 0) \sqcap ((\|\top\rangle_{\mathsf{qb}_{01}\mathsf{qb}_0} = -\frac{1}{\sqrt{2}}) \sqcap (\|\top\rangle_{\mathsf{qb}_{01}\mathsf{qb}_1} = \frac{1}{\sqrt{2}}) \sqcap (\|\top\rangle_{\mathsf{qb}_{01}\mathsf{qb}_{01}} = 0))$	Hyp
7	$(\gamma_1 \sqcap \gamma_2) \sqsupset \gamma_2$	**QTaut**
8	$(\|\top\rangle_{\mathsf{qb}_{01}\mathsf{qb}_0} = -\frac{1}{\sqrt{2}}) \sqcap (\|\top\rangle_{\mathsf{qb}_{01}\mathsf{qb}_1} = \frac{1}{\sqrt{2}}) \sqcap (\|\top\rangle_{\mathsf{qb}_{01}\mathsf{qb}_{01}} = 0)$	**QMP**: 6,7
9	$\|\top\rangle_{\mathsf{qb}_{01}\mathsf{qb}_0} = \|\top\rangle_{\mathsf{qb}_0\mathsf{qb}_0}\|\top\rangle_{\mathsf{qb}_1\emptyset}$	**Mul**: 2,5
10	$\|\top\rangle_{\mathsf{qb}_{01}\mathsf{qb}_1} = \|\top\rangle_{\mathsf{qb}_0\emptyset}\|\top\rangle_{\mathsf{qb}_1\mathsf{qb}_1}$	**Mul**: 2,5
11	$\|\top\rangle_{\mathsf{qb}_{01}\mathsf{qb}_1} = \|\top\rangle_{\mathsf{qb}_0\mathsf{qb}_0}\|\top\rangle_{\mathsf{qb}_1\mathsf{qb}_1}$	**Mul**: 2,5
12	$\perp$	**RCF**: 8–11
13	$\perp\!\!\!\perp$	**Eqv**$\perp$: 12

Therefore, by metatheorem of deduction, we get

$$\gamma_{\text{ind}}, \gamma_{\text{EPR}} \vdash \boxminus[\mathsf{qb}_0].$$

In a similar way, we can derive

$$\gamma_{\text{ind}}, \gamma_{\text{EPR}} \vdash \boxminus[\mathsf{qb}_1],$$

and consequently, we get

$$\gamma_{\text{ind}}, \gamma_{\text{EPR}} \vdash \boxminus[\mathsf{qb}_0] \sqcap \boxminus[\mathsf{qb}_1].$$

In the next section, we consider a protocol which uses this Bell state to achieve teleportation.

5.2 Reasoning about quantum teleportation

A protocol for quantum teleportation was first proposed in [7]. The idea is to move a qubit from one agent to another who share an entangled pair of qubits while exchanging only classical information.

Before describing and verifying the protocol we need to extend dEQPL with some features from dynamic logic. Namely, we shall use formulas, called *Hoare triples* for historical reasons [23], of the form

$$\{\gamma_1\}\, P\, \{\gamma_2\}$$

where γ_1 and γ_2 are dEQPL formulas and P is a quantum program denoting some composition of unitary transformations and measurements. It is often useful to reserve some qubits that are always in a classical state. Let us call them classical bits and use the symbols $\mathsf{cb}_1, \ldots, \mathsf{cb}_m$ to range over them. We shall avoid going into the details of the quantum program language and semantics, better left to a specific paper on a dynamic extension of dEQPL. However, we shall provide the needed intuitions. Namely, The Hoare triple above means that if the system is in a quantum state satisfying γ_1 then after running P it reaches a state satisfying γ_2.

The protocol in [7] uses three qubits, say qb_0, qb_1 and qb_2 plus two classical bits cb_0 and cb_2. The purpose is to transfer the quantum state of qb_0 to qb_1, using qb_2 and the classical bits as auxiliary variables. Initially, qb_1 and qb_2 will be prepared in a Bell state not entangled with qb_0. Afterwards, a measurement of qb_0 and qb_2 is made (by Alice). Note that this measurement will also affect qubit 1 because it is entangled with qubit 2. The classical bits are used to store the result of measuring the corresponding qubits. The classical information to be exchanged is precisely the contents of the classical bits after the measurement. Finally, this information is used (by Bob) to decide which unitary transformation to apply on qb_1 in order to achieve the required state.

In short, the protocol QTP is as follows:

$$
\begin{array}{l}
M_{\mathsf{qb}_{02}};\\
IF\\
\qquad\begin{array}{lcl}
|\mathsf{cb}_{02}\rangle = (1,0,0,0) & \rightarrow & -I_{\mathsf{qb}_1}\\
|\mathsf{cb}_{02}\rangle = (0,1,0,0) & \rightarrow & -Z_{\mathsf{qb}_1}\\
|\mathsf{cb}_{02}\rangle = (0,0,1,0) & \rightarrow & X_{\mathsf{qb}_1}\\
|\mathsf{cb}_{02}\rangle = (0,0,0,1) & \rightarrow & -X_{\mathsf{qb}_1} Z_{\mathsf{qb}_1}
\end{array}\\
FI
\end{array}
$$

where I is the identity operator and X and Z are the standard Pauli operators (not and phase flip, respectively).

The initial state of the system (after preparing the qubits 1 and 2) is assumed to comply with:

$$\gamma_{\text{init}} := [\mathsf{qb}_0] \sqcap (|\mathsf{qb}_{12}\rangle = \frac{1}{\sqrt{2}}(0,1,-1,0)) \sqcap (|\mathsf{qb}_0\rangle = (z_0, z_1)) \ .$$

Observe that we are not constraining the state of qubit 0. We just need to refer to it which we achieve by using the (rigid) variables z_0 and z_1. Note also that in such a state the qubits 1 and 2 are entangled. Actually, they are in a Bell state as discussed in the previous example.

We want the final state of the system (after running the protocol) to comply with:

$$\gamma_{\text{fin}} := [\mathsf{qb}_1] \sqcap (|\mathsf{qb}_1\rangle = (z_0, z_1)) \ .$$

In other words, we want to establish:

$$\text{Spec} := \{\gamma_{\text{init}}\}\ \text{QTP}\ \{\gamma_{\text{fin}}\} \ .$$

To this end, it is enough to assume that the measurement operator $M_{\mathsf{qb}_{02}}$ complies with the following non probabilistic specification:

$$\{\gamma_{\text{init}}\}\ M_{\mathsf{qb}_{02}}\ \{\sqcup_{k=1}^{4} \gamma_k\}$$

where

$$
\begin{array}{l}
\gamma_1 := (|\mathsf{cb}_{02}\rangle = (1,0,0,0)) \ \sqcap\ (|\mathsf{qb}_{02}\rangle = \frac{1}{\sqrt{2}}(1,0,0,1)) \ \sqcap\ (|\mathsf{qb}_1\rangle = -(z_0, z_1));\\
\gamma_2 := (|\mathsf{cb}_{02}\rangle = (0,1,0,0)) \ \sqcap\ (|\mathsf{qb}_{02}\rangle = \frac{1}{\sqrt{2}}(-1,0,0,1)) \ \sqcap\ (|\mathsf{qb}_1\rangle = (-z_0, z_1));\\
\gamma_3 := (|\mathsf{cb}_{02}\rangle = (0,0,1,0)) \ \sqcap\ (|\mathsf{qb}_{02}\rangle = \frac{1}{\sqrt{2}}(0,1,1,0)) \ \sqcap\ (|\mathsf{qb}_1\rangle = (z_1, z_0));\\
\gamma_4 := (|\mathsf{cb}_{02}\rangle = (0,0,0,1)) \ \sqcap\ (|\mathsf{qb}_{02}\rangle = \frac{1}{\sqrt{2}}(0,-1,1,0)) \ \sqcap\ (|\mathsf{qb}_1\rangle = (z_1, -z_0)).
\end{array}
$$

Observe that the IF part of the protocol QTP complies with:

$$\{\gamma_k\}\ \text{IF}\ \{\gamma_{\text{fin}}\}$$

for $k = 1, \ldots, 4$. Therefore, we can derive Spec using the traditional composition rules of dynamic logic.

6 Concluding remarks

A decidable quantum logic allowing us to reason about amplitudes of quantum states and probabilities of classical outcomes was obtained as a fragment of EQPL. Decidability was achieved by relaxing the semantics, replacing Hilbert spaces by inner product spaces over arbitrary real closed fields and their algebraic closures. The proof of decidability was carried out hand in hand with the proof of weak completeness and follows the Fagin-Halpern-Megiddo technique (originally proposed for probabilistic logics [18, 1]).

We envision to use this decidable quantum logic in the specification and verification of quantum procedures and protocols, either via model checking or theorem proving. To this end, the hardness of the proposed decision algorithm needs to be analyzed. We also intend to enrich this decidable quantum logic with Hoare triples as outlined in Section 5 and in [26, 27]. Temporal extensions of dEQPL should also be explored to reason about liveness and progress properties of quantum computations. Another interesting line of research would be to develop a first-order quantum logic based on the exogenous semantics approach.

Both EQPL and dEQPL allow us to express amplitudes of pure quantum states of collections of qubits. Therefore, these logics are not insensitive to the global phase of the quantum state. One may argue that it should be insensitive since no physical measurement will ever be able to distinguish two quantum states that are equivalent up to global phase. We decided to leave dEQPL as it is (that is, sensitive to global phase) for two reasons. In practice, physicists and quantum computer scientists need to work with both levels of abstraction. Sometimes they want to work with states as unit vectors and other times they want to abstract away the global phase. Therefore, a calculus supporting the former level of abstraction is also useful. The second reason is a consequence of the fact that forgetting global phase requires a major semantic shift. Indeed, it is better solved by identifying a quantum state with a density operator working on the underlying inner product space, that is, working with probabilistic ensembles or mixed quantum states in general.

Such a shift toward a semantics based on density operators will lead to a quite different quantum logic (but still extending classical logic by applying the exogenous approach) that will also be useful for reasoning about quantum systems evolving under partial tracing, besides unitary transformations and measurements. Clearly, this is yet another line of research that will deserve attention.

The relationship between the exogenous quantum logics and the more traditional quantum logics (based on the original Birkhoff and von Neumann proposal) should be further explored. At the preliminary stage of work in this direction, it seems that most of the qualitative assertions possible in the latter can be made in the former and that the latter can be easily extended with quantitative aspects of the former. In other words, it seems feasible to combine the two quantum logics into a single logic by using fibring techniques [20, 10].

Acknowledgments

The authors wish to express their gratitude to the regular participants in the QCI Seminar at SQIG-IT (formerly at CLC), and also to Dave Marker and Anand Pillay for their help on real closed fields and their algebraic completion. This work was partially supported by FCT and FEDER through POCTI, namely via the QuantLog POCTI/MAT/55796/2004 (Quantum Logic), KLog PTDC/MAT/68723/2006 (Kleistic Logic) and QSec PTDC/EIA/67661/2006 (Quantum Security) projects.

References

[1] M. Abadi and J. Y. Halpern. Decidability and expressiveness for first-order logics of probability. *Information and Computation*, 112(1):1–36, 1994.

[2] 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. Extended version at arXiv:quant-ph/0402130).

[3] S. Abramsky and R. Duncan. A categorical quantum logic. *Mathematical Structures in Computer Science*, 16(3):469–489, 2006.

[4] F. Bacchus. On probability distributions over possible worlds. In *Uncertainty in Artificial Intelligence, 4*, volume 9 of *Machine Intelligence and Pattern Recognition*, pages 217–226. North-Holland, 1990.

[5] F. Bacchus. *Representing and Reasoning with Probabilistic Knowledge*. MIT Press Series in Artificial Intelligence. MIT Press, 1990.

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

[7] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters. Teleporting an unkown quantum state via dual classical and einstein-podolsky-rosen channels. *Physical Review Letters*, 70(13):1895–1899, 1993.

[8] G. Birkhoff and J. von Neumann. The logic of quantum mechanics. *Annals of Mathematics*, 37(4):823–843, 1936.

[9] 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.

[10] C. Caleiro, A. Sernadas, and C. Sernadas. Fibring logics: Past, present and future. In S. Artemov, H. Barringer, A. S. d'Avila Garcez, L. C. Lamb, and J. Woods, editors, *We Will Show Them: Essays in Honour of Dov Gabbay, Volume One*, pages 363–388. College Publications, 2005.

[11] W. A. Carnielli. Possible-translations semantics for paraconsistent logics. In *Frontiers of Paraconsistent Logic (Ghent, 1997)*, volume 8 of *Studies in Logic and Computation*, pages 149–163. Research Studies Press, 2000.

[12] W. A. Carnielli and M. Lima-Marques. Society semantics and multiple-valued logics. In *Advances in Contemporary Logic and Computer Science (Salvador, 1996)*, volume 235 of *Contemporary Mathematics*, pages 33–52. AMS, 1999.

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

[14] M. L. D. Chiara, R. Giuntini, and R. Greechie. *Reasoning in Quantum Theory*. Kluwer Academic Publishers, 2004.

[15] C. Cohen-Tannoudji, B. Diu, and F. Laloë. *Quantum Mechanics*. John Wiley, 1977.

[16] H. Dishkant. Semantics of the minimal logic of quantum mechanics. *Studia Logica*, 30:23–32, 1972.

[17] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Physical Review*, 47:777–780, 1935.

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

[19] D. J. Foulis. A half-century of quantum logic. What have we learned? In *Quantum Structures and the Nature of Reality*, volume 7 of *Einstein Meets Magritte*, pages 1–36. Kluwer Acad. Publ., 1999.

[20] D. M. Gabbay. Fibred semantics and the weaving of logics: Part 1. *Journal of Symbolic Logic*, 61(4):1057–1120, 1996.

[21] J. Y. Halpern. An analysis of first-order logics of probability. *Artificial Intelligence*, 46:311–350, 1990.

[22] H. Hansson and B. Jonsson. A logic for reasoning about time and reliability. *Formal Aspects of Computing*, 6:512–535, 1995.

[23] C. Hoare. An axiomatic basis for computer programming. *Communications of the ACM*, 12:576–583, 1969.

[24] W. Hodges. *Model Theory*. Cambridge University Press, 1993.

[25] S. A. Kripke. Semantical analysis of modal logic. I. Normal modal propositional calculi. *Zeitschrift für Mathematische Logik und Grundlagen der Mathematik*, 9:67–96, 1963.

[26] P. Mateus and A. Sernadas. Exogenous quantum logic. In W. A. Carnielli, F. M. Dionísio, and P. Mateus, editors, *Proceedings of CombLog'04, Workshop on Combination of Logics: Theory and Applications*, pages 141–149, 1049-001 Lisboa, Portugal, 2004. Departamento de Matemática, Instituto Superior Técnico. Extended abstract.

[27] P. Mateus and A. Sernadas. Reasoning about quantum systems. In J. Alferes and J. Leite, editors, *Logics in Artificial Intelligence, Ninth European Conference, JELIA'04*, volume 3229 of *Lecture Notes in Artificial Intelligence*, pages 239–251. Springer-Verlag, 2004.

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

[29] 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.

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

[31] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

[32] N. J. Nilsson. Probabilistic logic. *Artificial Intelligence*, 28(1):71–87, 1986.

[33] N. J. Nilsson. Probabilistic logic revisited. *Artificial Intelligence*, 59(1-2):39–42, 1993.

[34] M. Patra. A logic for quantum computation and classical simulation of quantum algorithms. *International Journal of Quantum Information*, 6(2), 2008. In print.

[35] 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.

[36] 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.

Index