The Logic of Quantum Programs

Alexandru Baltag[1] and Sonja Smets[2]

Abstract

We present a logical calculus for reasoning about information flow in quantum programs. In particular we introduce a dynamic logic that is capable of dealing with quantum measurements, unitary evolutions and entanglements in compound quantum systems. We give a syntax and a relational semantics in which we abstract away from phases and probabilities. We present a sound proof system for this logic, and we show how to characterize by logical means various forms of entanglement (e.g. the Bell states) and various linear operators. As an example we sketch an analysis of the teleportation protocol.

1 Introduction

In this paper we elaborate on the ideas presented in [2, 3, 9] and give a full-fledged *dynamic Logic for Quantum Programs* LQP. It is well-known that PDL (Propositional Dynamic Logic) and its fragment the Hoare Logic are among the main logical formalisms used in *program verification* for classical programs, i.e. in checking that a given (classical) program meets the required specification. It is natural to ask for a *quantum* version of PDL, to be used in the verification of quantum programs. In our past work [3], we presented several such logical systems, starting with a *logic of quantum measurements* LQM for single quantum systems, and later extending this system into a dynamic logic LQA of *quantum actions* (i.e. compositions of measurements and unitary evolutions). In this paper, we extend LQA into a logic for *compound* quantum systems. We present a self-contained version of LQP such that no knowledge of LQA or LQM is necessary to understand the basic concepts. Note the difference between our logic and the approach with a similar name in [4]: our dynamic logic goes much further in capturing essential properties of quantum systems and quantum programs, as well as in recovering the ideas of traditional quantum logic [6, 7].

2 Quantum Frames

In this section we introduce quantum frames for single quantum systems and quantum frames for compound quantum systems; in the later case we restrict our attention to n compound qubits.

[1]Oxford University Computing Laboratory, baltag@comlab.ox.ac.uk

[2]Vrije Universiteit Brussel, Flanders' Fund for Scientific Research Post-Doc, sonsmets@vub.ac.be

2.1 Single System Quantum Frames

A *modal frame* is a set of *states*, together with a family of *binary relations* between states. A (generalized) *PDL frame* is a modal frame $(\Sigma, \{\overset{S?}{\rightarrow}\}_{S\in\mathcal{L}}, \{\overset{a}{\rightarrow}\}_{a\in\mathcal{A}})$, in which the relations on the set of states Σ are of two types: the first, called *tests* and denoted by $S?$, are labelled with subsets S of Σ, coming from a given family $\mathcal{L} \subseteq \mathcal{P}(\Sigma)$ of sets, called *testable properties*; the others, called *actions*, are labelled with action labels a from a given set $\mathcal{A}$. Given a PDL frame, there exists a standard way to give a semantics to the usual language of *propositional dynamic logic*. Classical PDL can be considered as a special case of such a logic, in which tests are given by *classical tests*: $s \overset{S?}{\rightarrow} t$ if and only if $s = t \in S$. Observe that *classical tests, if executable, do not change the current state*.

In the context of quantum systems, a natural idea is to replace classical tests by "quantum tests", given by *quantum measurements* of a given property. Such tests will obviously change the state of the system. To model them, we introduce a special kind of PDL frames: *quantum frames*. The "tests" are essentially given by *projectors* in a Hilbert space. In [3], we considered PDL with the above-mentioned standard semantics, having the same clauses in the classical case, but interpreted in quantum frames. What we obtained is a *quantum PDL*, whose negation-free part with dynamic modalities for quantum tests is equivalent to what is traditionally called "(orthomodular) quantum logic" [6, 7]. In this paper, we extend the syntax of this logic to deal with unitary evolutions, entanglements and some quantum protocols.

Definition 1. *(Quantum Frame)*
Given a Hilbert space $\mathcal{H}$, the following steps construct a *Quantum (PDL) Frame*

$$\Sigma(\mathcal{H}) := (\Sigma, \{\overset{S?}{\rightarrow}\}_{S\in\mathcal{L}}, \{\overset{U}{\rightarrow}\}_{U\in\mathcal{U}})$$

1. Let Σ be the set of *one dimensional subspaces* of $\mathcal{H}$, called the set of *states*. We denote a state $s = \overline{x}$ of $\mathcal{H}$ using any of the non-zero vectors $x \in \mathcal{H}$ that generate them. Note that any two vectors that differ only in *phase* (i.e. $x = \lambda y$, with $\lambda \in C$ with $|\lambda| = 1$) will generate the same state $\overline{x} = \overline{y} \in \Sigma$.

2. Call two states s and t in Σ *orthogonal* and write $s \perp t$, if and only if $\forall x \in s$ and $\forall y \in t$: x is orthogonal to y, i.e. if $\langle x \mid y\rangle = 0$. Or, equivalently we can state that $s \perp t$ if and only if $\exists x \in s, y \in t$ with $x \neq 0$, $y \neq 0$ and $\langle x \mid y\rangle = 0$. We put $S^{\perp} := \{t \in \Sigma \mid t \perp s \text{ for all } s \in S\}$; and we denote by $\overline{S} = S^{\perp\perp} := (S^{\perp})^{\perp}$ the biorthogonal closure of S. In particular, for a singleton $\{x\}$, we just write $\overline{x}$ for $\overline{\{x\}}$, which agrees with the notation $\overline{x}$ used above to denote the state generated by x.

3. A set of states $S \subseteq \Sigma$ is called a *(quantum) testable property* iff it is *biorthogonally closed*, i.e. if if $\overline{S} = S$. (Note that $S \subseteq \overline{S}$ is always the case.) We denote by $\mathcal{L} \subseteq P(\Sigma)$ the family of all quantum testable properties. All the *other* sets $S \in P(\Sigma) \setminus \mathcal{L}$ are called *non-testable properties*.

4. There is a natural bijective correspondence between the family $\mathcal{L}$ of all testable properties and the family $\mathcal{W}$ of all *closed linear subspaces* W of $\mathcal{H}$, bijection given by $S \mapsto W_S =: \bigcup S$. Observe that, under this correspondence, the image of the biorthogonal closure $\overline{S}$ of any arbitrary set $S \subseteq \Sigma$ is the closed linear subspace $\overline{\bigcup S} \subseteq \mathcal{H}$ generated by the union $\bigcup S$ of all states in S.

5. For each testable property $S \in \mathcal{L}$, there exists a partial map $S?$ on Σ, called a *quantum test*. If $W = W_S = \bigcup S$ is the corresponding subspace of $\mathcal{H}$, then the quantum test is the map induced on states by the *projector* P_W onto the subspace W. In other words, it's given by:

$$\begin{aligned} S?(\overline{x}) &:= \overline{P_W(x)} \in \Sigma\,, \text{ if } \overline{x} \notin S^{\perp} \text{ (i.e. if } P_W(x) \neq 0) \\ S?(\overline{x}) &:= \text{ undefined }, \text{ otherwise .} \end{aligned}$$

   We denote by $\overset{S?}{\rightarrow} \subseteq \Sigma \times \Sigma$ the binary relation corresponding to the partial map $S?$, i.e. given by: $s \overset{S?}{\rightarrow} t$ if and only if $S?(s) = t$. So we have *a family of binary relations indexed by the testable properties* $S \in \mathcal{L}$.

6. For each unitary transformation U on $\mathcal{H}$, consider the corresponding binary relation $\overset{U}{\rightarrow} \subseteq \Sigma \times \Sigma$, given by: $s \overset{U}{\rightarrow} t$ if and only if $U(x) = y$ for some non-zero vectors $x \in s, y \in t$. So we obtain *a family of binary relations indexed by the unitary transformations* $U \in \mathcal{U}$ (where $\mathcal{U}$ is the set of unitary transformations on $\mathcal{H}$).

So a quantum frame is just a PDL frame built on top of a given Hilbert space $\mathcal{H}$, using projectors as "tests" and unitary evolutions as "actions". Our notion of "state" in this paper is closely connected to the way quantum logicians approach quantum systems; i.e., contrary to identifying states with unitary vectors (as customary in quantum computation), we took them to be *one dimensional subspaces* generated by these vectors. This imposes some limits to our approach, mainly that we will not be able to express *phase*-related properties. While it is possible to build up a quantum frame starting from unitary vectors as the states, the resulting logical system will be much more complex[3], and so we do not elaborate on it in this paper.

[3]It would require the introduction of a propositional *tensor* operator.

Operators on states, adjoints and generalized tests. To generalize our notations introduced earlier, observe that every *linear operator* $F : \mathcal{H} \to \mathcal{H}$ induces a partial map $F : \Sigma \to \Sigma$ on states (i.e. subspaces), given by $F(\overline{x}) = \overline{F(x)}$, if $F(x) \neq 0$ (and undefined, in rest). (Note that *linearity* ensures that this map on states is well-defined.) In particular, every map $F : \Sigma \to \Sigma$ obtained in this way has an *adjoint* $F^\dagger : \Sigma \to \Sigma$, defined as the map on states induced by the adjoint ("Hermitian conjugate") of the linear operator F on $\mathcal{H}$. Observe that, for unitary transformations U, the adjoint is the inverse:$U^\dagger = U^{-1}$ Also, one can naturally generalize *quantum tests* to arbitrary, possibly *non-testable properties*, $S \subseteq \Sigma$, by putting: $S? := \overline{S}?$. So we identify a test of a "non-testable" property S with the quantum test of its biorthogonal closure. Observe that $S?^\dagger = S?$ (since projectors are self-adjoint).

Definition 2. *(Non-orthogonality, or Measurement, Relation)* For all $s, t \in \Sigma$, let $s \to t$ if and only if $s \stackrel{S?}{\to} t$ for some property $S \in \mathcal{L}$. In other words, $s \to t$ means that one can reach state t by doing *some measurement* on state s.

An important observation is that *the measurement relation is the same as non-orthogonality*: $s \to t$ iff $s \not\perp t$. The non-orthogonality relation has indeed been used to introduce an accessibility relation in the orthoframe semantics within quantum logic [7].

Definition 3. *(Dynamic Modalities and Measurement Modalities)* For any property $T \subseteq \Sigma$ and any partial map $F : \Sigma \to \Sigma$ induced on states by a linear operator F, let $[F]T := F^{-1}(T) = \{s \in \Sigma : F(s) \in T, \text{if defined}\}$ and $\langle F\rangle T := \Sigma\backslash([F](\Sigma\backslash T))$. Similarly, put $\Box T := \{s \in \Sigma : \forall t(s \to t \Rightarrow t \in T)\}$ and $\Diamond T := \Sigma\backslash(\Box(\Sigma\backslash T))$.

Observe that $[F]T$ expresses the *weakest precondition* for the "program" F and post-condition T. In particular, $[S?]T$ expresses the weakest precondition ensuring the satisfaction of property T in any state after the system passes a quantum test of property S. Similarly, $\langle S?\rangle T$ means that one can perform a quantum test of property S on the current state, ending up in a state having property T. $\Box T$ means that property T will hold after *any* measurement (quantum test) performed on the current state. Finally, $\Diamond T$ means that property T is *potentially satisfied*, in the sense that one can do some quantum test to reach a state with property T.

Lemma 1. *For every property $S \subseteq \Sigma$, we have $S^\perp = [S?]\emptyset = \Sigma \setminus \Diamond S$ and $\overline{S} = \Box\Diamond S$.*

Proposition 1. *For every property $S \subseteq \Sigma$, if $T \in \mathcal{L}$ (i.e. is testable), then $\Box S, S^{\perp}, [S?]T \in \mathcal{L}$ (are testable), and more generally $[F]T \in \mathcal{L}$, for every (map on states induced by a) linear operator F.*

Proposition 2. *(Testable Properties) A property $S \subseteq \Sigma$ is testable if and only if any of the following conditions hold: (1) $S = \overline{S}$; (2) $S = \Box\Diamond S$; (3) $\exists T \in \Sigma$ such that $S = T^{\perp}$; (4) $\exists T \in \Sigma$ such that $S = \Box T$. The family $\mathcal{L}$ of testable properties is a complete lattice with respect to inclusion, having as its meet set-intersection $S \cap T$, and as its join the biorthogonal closure of set-union $S \sqcup T := \overline{S \cup T}$, called the quantum join of S and T. For every state $s \in \Sigma$, the singleton $\{s\} \in \mathcal{L}$ is testable. For any arbitrary property $S \subseteq \Sigma$, we have $\overline{S} = \bigsqcup\{\{s\} : s \in S\} = \bigcap\{T \in \mathcal{L} : S \subseteq T\}$, so the biorthogonal closure of S is the strongest testable property implied by (the property) S.*

Theorem 1. *In every quantum frame $\Sigma(\mathcal{H})$ the following properties for quantum tests are provable:*

1. *Partial functionality: If $s \xrightarrow{S?} t$ and $s \xrightarrow{S?} v$ then $t = v$.*
2. *Trivial tests: $\xrightarrow{\emptyset?} = \emptyset$ and $\xrightarrow{\Sigma?} = \Delta_{\Sigma}$, where $\Delta_{\Sigma} = \{(s, s) : s \in \Sigma\}$ is the identity relation on $\Sigma \times \Sigma$.*
3. *Adequacy: If $s \in S$ then $s \xrightarrow{S?} s$*
4. *Repeatability: If $S \in \mathcal{L}$ is testable and $s \xrightarrow{S?} t$, then $t \in S$*
5. *Compatibility: If $S, T \in \mathcal{L}$ are testable and $S?;T? = T?;S?$ then $S?;T? = (S \cap T)?$.*
6. *Self-Adjointness: If $s \xrightarrow{S?} w \xrightarrow{T?} t$ then $t \xrightarrow{S?} v \xrightarrow{W?} s$, for some $v \in \Sigma$ and $W \in \mathcal{L}$. In other words: if $s \xrightarrow{S?} w \rightarrow t$ then $t \xrightarrow{S?} v \rightarrow s$, for some $v \in \Sigma$.*
7. *Universal Accessibility: For all $s, t \in \Sigma$, there exists a state $w \in \Sigma$ such that $s \rightarrow w \rightarrow t$*

Proofs: *Partial functionality* follows from the fact that projectors correspond to partially defined maps in $\mathcal{H}$. *Trivial tests* follows from the fact that projecting on the empty space yields the empty space and that projecting on the total space doesn't change anything. *Adequacy* follows from the fact that for every $x \in W$ we have that $P_W(x) = x$. *Repeatability* follows from the fact that $P_W(x) \in W$ for every $x \in \mathcal{H}$. *Compatibility* follows from the fact that if two projectors commute,

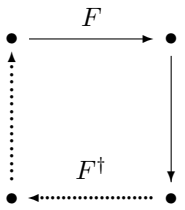
i.e. $P_W \circ P_V = P_V \circ P_W$, then $P_W \circ P_V = P_{W \cap V}$. *Self-Adjointness* follows from the more general Adjointness theorem stated below, together with the fact $S?^{\dagger} = S?$. *Universal Accessibility* can be proved by cases: If $s \not\perp t$, i.e. let $s \to t$, then $w = s \Rightarrow s \to s \to t$. If $s \perp t$, i.e. let $s \not\to t$ then let $s = \overline{x}, t = \overline{y}$ with $x, y \in \mathcal{H}$. Take the superposition $x + y \in \mathcal{H}$ of x and y and note that $x + y \neq 0$ (since from $x + y = 0 \Rightarrow x = -y \Rightarrow s = t$ which contradicts $s \not\perp t$). Next observe that $x \not\perp (x+y)$ (Indeed, suppose $x \perp (x+y)$ then $\langle x \mid x+y \rangle = 0$ and then $\langle x \mid x \rangle + \langle x \mid y \rangle = 0$; but $x \perp y$ implies $\langle x \mid x \rangle = 0$. So from $\langle x \mid x \rangle = 0$ follows that $x = 0$, which yields a contradiction). Similarly, we get $y \not\perp (x + y)$. Taking now $w = \overline{x + y}$, we can see that $w \in \Sigma$, $s \to w$ and $w \to t$.

Theorem 2. *In every quantum frame $\Sigma(\mathcal{H})$ the following properties for unitary transformations (stated for all $U, U^{\dagger} \in \mathcal{U}$) are provable:*

1. *Functionality: For every state $s \in \Sigma$ we have $\exists! t : s \xrightarrow{U} t$*
2. *Inverse-adjoint (bijectivity): $s \xrightarrow{U} t \xrightarrow{U^{\dagger}} w$ implies $s = w$. Similarly, $s \xrightarrow{U^{\dagger}} t \xrightarrow{U} w$ implies $s = w$*

Proofs: *Functionality* follows from the fact that unitary transformations are well-defined on all states, i.e. the kernell of the linear map encoding the transformation is $\emptyset$. *Inverse-adjoint* follows from the fact that unitary operators on a Hilbert space have the property that $U^{\dagger} = U^{-1}$.

Theorem 3. *(Adjointness) Let F be a linear transformation and let $s, w, t \in \Sigma$ be states: If $s \xrightarrow{F} w \to t$ then there exists some state $v \in \Sigma$ such that $t \xrightarrow{F^{\dagger}} v \to s$.*



Proof: To prove this theorem we use the definition of adjointness in a Hilbert space: $\langle Fx \mid y \rangle = \langle x \mid F^{\dagger} y \rangle$. From this, we get the equivalence: $\langle Fx \mid y \rangle = 0$ iff $\langle x, F^{\dagger} y \rangle = 0$; or, otherwise stated, $Fx \perp y$ iff $x \perp F^{\dagger} y$. Taking the negation of both sides and using the fact that the measurement relation $s \to t$ is the same as non-orthogonality $s \not\perp t$, we obtain the equivalence: $\exists w(\overline{x} \xrightarrow{F} \overline{w} \to \overline{y})$ iff $\exists v(\overline{y} \xrightarrow{F^{\dagger}} \overline{v} \to \overline{x})$. This proves the adjointness property.

As a consequence:

Corollary 1. *For every property $P \subseteq \Sigma$ and every linear map F we have:*

$$P \subseteq [F]\Box\langle F^{\dagger}\rangle\Diamond P$$

2.2 Compound System Quantum Frames

In this subsection we like to extend the quantum frame presented above for single systems into a quantum frame for compound systems. Let H be a Hilbert space of dimension 2 with basis $\{\mid 0\rangle, \mid 1\rangle\}$. We fix a natural number $n \geq 2$ (although later we will restrict to the case $n \geq 4$), and we put $N = \{1, 2, \ldots, n\}$. A *compound-system quantum frame* will be the quantum frame $\Sigma(\mathcal{H}_n)$ build on a Hilbert space $\mathcal{H}_n = H^{\otimes n} = H \otimes H \otimes ... \otimes H$ (n times) .

Notation. In fact, we consider all the n copies of H as distinct (although isomorphic) and denote by $H^{(i)}$ the i-th component of the tensor $H^{\otimes n}$. Also, for any set of indices $I \subseteq N$, we put $\mathcal{H}_I = H^{\bigotimes I} = \bigotimes_{i\in I} H^{(i)}$. (So, in particular, $\mathcal{H}_N = \mathcal{H}_n = \mathcal{H}$.) We denote by $\epsilon_i : H \to H^{(i)}$ the canonical isomorphism between $\mathcal{H}$ and $\mathcal{H}^{(i)}$. This notation can be extended to sets $I \subseteq N$ of indices of length $|I| = k$, by putting $\epsilon_I : H^{\otimes k} \to \mathcal{H}_I$ to be the canonical isomorphism between these spaces. Similarly, for each set $I \subseteq N$, we denote by $\mu_I : \mathcal{H}_I \otimes \mathcal{H}_{N\setminus I} \to \mathcal{H}$ the canonical isomorphism between these two spaces. For any vector $\mid x\rangle \in H$, we denote by $\mid x\rangle^{\bigotimes I} = \bigotimes_{i\in I} \mid x\rangle$ the corresponding vector in $\mathcal{H}_I$ (obtained by tensoring $|I|$ copies of $\mid x\rangle$). Given a set $I \subseteq N$, we say that a state $s \in \Sigma(\mathcal{H})$ *has its I-qubits in state* $s' in \Sigma(\mathcal{H}_I)$, and write $s_I = s'$, if there exist vectors $\psi \in s$, $\psi' \in \mathcal{H}_I$ and $\psi'' \in \mathcal{H}_{N\setminus I}$ such that $\psi = \mu_I(\psi' \otimes \psi'')$. Note that the state s_I, *if it exists, then it is unique* (having the above property). In particular, when $I = \{i\}$, we say that state s *has as its i-th coordinate* the state $s_i \in \mathcal{H}_{\{i\}} = H^{(i)}$.

We will further denote the vector $\mid 0\rangle + \mid 1\rangle$ by $\mid +\rangle$, and similarly denote $\mid 0\rangle - \mid 1\rangle$ by $\mid -\rangle$. For the states generated by the vectors in a two dimensional Hilbert space we introduce the following abbreviations: $+ := \overline{\mid +\rangle}$, $- := \overline{\mid -\rangle}$, $0 := \overline{\mid 0\rangle}$, $1 := \overline{\mid 1\rangle}$. In order to refer to the state corresponding to a pair of qubits, we similarly delete the Dirac notation, e.g. $00 := \overline{\mid 00\rangle} = \overline{\mid 0\rangle \otimes \mid 0\rangle}$.

The Bell states will be abbreviated as follows: $\beta_{00} := \overline{\mid 00\rangle + \mid 11\rangle}$, $\beta_{01} := \overline{\mid 01\rangle + \mid 10\rangle}$, $\beta_{10} := \overline{\mid 00\rangle - \mid 11\rangle}$, $\beta_{11} = \mid 01\rangle - \mid 10\rangle$ and $\gamma := \overline{\mid 00\rangle + \mid 01\rangle + \mid 11\rangle + \mid 10\rangle}$.

The following two results are well-known:

Proposition 3. *Let $H^{(i)}$ and $H^{(j)}$ be two Hilbert spaces. There exists a bijective correspondence ψ between the linear maps $F : H^{(i)} \to H^{(j)}$ and the states of $H^{(i)} \otimes H^{(j)}$. Given the bases $\{\epsilon_\alpha^{(i)}\}_\alpha$ and $\{\epsilon_\beta^{(j)}\}_\beta$ of these spaces, the correspondence ψ is given by the mapping $F = \Sigma_{\alpha\beta}\, m_{\alpha\beta}\, \langle \epsilon_\alpha^{(i)} \mid -\rangle . \epsilon_\beta^{(j)}$ into the state $\psi(F) = \Sigma_{\alpha\beta}\, m_{\alpha\beta}\, . \epsilon_\alpha^{(i)} \otimes \epsilon_\beta^{(j)}$.*

Proposition 4. *Let $\mathcal{H} = H^{\otimes n}$ and let $W = \{x \otimes \mid 0\rangle^{\otimes(n-1)} : x \in H\}$ be given. Any linear map $F : \mathcal{H} \to \mathcal{H}$ induces a linear map $F_{(1)} : H \to H$ in a canonical manner: it is defined as the unique map on H satisfying $F_{(1)}(x) = P_W \circ F(x \otimes \mid 0\rangle^{\otimes(n-1)})$. Conversely, any linear map $G : H \to H$ can be represented as $G = F_{(1)}$ for some linear map $F : \mathcal{H} \to \mathcal{H}$.*

Notation. The above results allow us to specify a compound state in $H^{(i)} \otimes H^{(j)}$ via some linear map F on $\mathcal{H}$. Indeed, if $F : \mathcal{H} \to \mathcal{H}$ is any such linear map, let $F_{(1)} : H \to H$ be the map in the above proposition; this induces a corresponding map $F_{(1)}^{(ij)} : H^{(i)} \to H^{(j)}$, by putting $F_{(1)}^{(ij)} := \epsilon_j \circ F_{(1)} \circ \epsilon_i^{-1}$, where ϵ_i is the canonical isomorphism introduced above (between H and the i-th component $H^{(i)}$ of $H^{\otimes n}$). Then we denote by $\overline{F}_{(ij)}$ the state

$$\overline{F}_{(ij)} := \overline{\psi(F_{(1)}^{(ij)})}$$

given by the above mentioned bijective correspondence ψ between $H^{(i)} \to H^{(j)}$ and $H^{(i)} \otimes H^{(j)}$. The following result is also known from the literature:

Proposition 5. *Let $F : \mathcal{H} \to \mathcal{H}$ be a linear map. Then the state $\overline{F}_{(ij)}$ is "entangled according to $F_{(1)}$"; i.e. if $F_{(1)}(\mid x\rangle) = \mid y\rangle$ and if the state of a 2-qubit system is $\overline{F}_{(ij)} \in H^{(i)} \otimes H^{(j)}$, then any measurement of qubit i resulting in a state x_i collapses the qubit j to state y_j.*

Notation. The notation $\overline{F}_{(ij)}$ can be further extended to define a property (set of states) $\overline{F}_{ij} \subseteq \Sigma = \Sigma(\mathcal{H})$, by defining it as *the set of all states having the $\{i, j\}$-qubits in the state $\overline{F}_{(ij)}$* :

$$\begin{aligned} \overline{F}_{ij} &= \{s \in \Sigma : s_{\{i,j\}} = \overline{F}_{(ij)}\} \\ &= \{\overline{\mu_{\{i,j\}}(\psi \otimes \psi')} : \psi \in \overline{F}_{(ij)}, \psi' \in \mathcal{H}_{N\setminus\{i,j\}}\} \subseteq \Sigma \end{aligned}$$

where $\mu_{\{i,j\}}$ is as above the canonical isomorphism between $\mathcal{H}_{\{i,j\}} \otimes \mathcal{H}_{N\setminus\{i,j\}}$. In other words, $\overline{F}_{ij}$ is simply the property of an n-qubit compound state of having its i-th and j-th qubits (separated from the others, and) in a state that is "entangled according to $F_{(1)}$" .

Local properties. Given a set $I \subseteq N$, a property $S \subseteq \Sigma$ is *local in* I if it corresponds to a property of the subsystem formed by the qubits in I; in other words, if there exists some property $S' \subseteq \Sigma(\mathcal{H}_I)$ such that:

$$S' = \{s \in \Sigma : s_I \in S'\}$$

or, more explicitly:

$$S' = \{\overline{\mu_I(\psi \otimes \psi')} : \overline{\psi} \in S', \psi' \in \mathcal{H}_{N\setminus I}\}$$

An *example* is the property $\overline{F}_{ij}$, which is $\{i,j\}$-local. The family of local properties is closed under union, intersection but *not under complementation*.

Local transformations. Given $I \subseteq N$, a linear map $F : \mathcal{H} \to \mathcal{H}$ is I-local if it "affects only the qubits in I"; in other words, if there exists a map $G : \mathcal{H}_I \to \mathcal{H}_I$ such that:

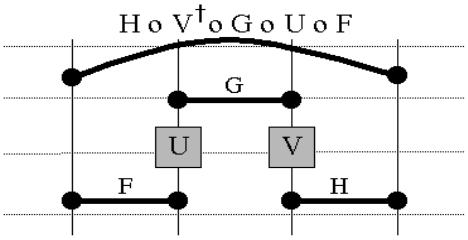
$$F \circ \mu_I(\psi \otimes \psi') = \mu_I(G(\psi) \otimes \psi')$$

A map $F : \Sigma \to \Sigma$ is *I-local* if it is the map induced on Σ by an I-local linear map on $\mathcal{H}$. *Examples* are: all the tests $S_I?$ of I-local properties; logic gates that affect only the qubits in I, i.e. (maps on Σ induced by) unitary transformations $U_I : \mathcal{H} \to \mathcal{H}$ such that for all $\psi, \psi' \in \mathcal{H}_I$, we have $U_I \circ \mu_I(\psi \otimes \psi') = \mu_I(U(\psi) \otimes \psi')$, for some $U : \mathcal{H}_I \to \mathcal{H}_I$. The family of local maps is closed under composition.

Lemma 2. *The main lemma in [5] states (in our notation) that, given a quadruple of distinct indices i, j, k, l, let $F, G, H, U, V : H \to H$ be single-qubit linear maps, then we have:*

$$G_{jk} \circ V_k \circ U_j [\overline{F}_{ij} \cap \overline{H}_{kl}] \subseteq \overline{(H \circ U^\dagger \circ G \circ V \circ F)}_{il}$$

Using the formalism of *entanglement specification networks* introduced in [5], this can be encoded in the following diagrammatic representation:



[5] and [1] use this as the main tool in explaining teleportation, quantum gate teleportation and many other quantum protocols. We will use this work in our logical treatment of such protocols, by taking this lemma as one of our main axioms.

Observe that in the above Lemma, the order in which the operations U_j and V_k are applied is in fact *irrelevant*. This is a consequence of the following important property of local transformations:

Proposition 6. *(Compatibility of local transformations affecting different sets of qubits) If $I \cap J = \emptyset$, F_I is an I-local map and G_J is a J-local map, then we have:*

$$F_I \circ G_J = G_J \circ F_I$$

Another important property of local maps (on *states*) is:

Proposition 7. *("Agreement Property") Let $F_I, G_I : \Sigma \to \Sigma$ be two I-local maps on states, having the same domain[4] : $dom(F) = dom(G)$. Then their output-states agree on all non-I qubits, i.e.:*

$$F(s)_J = G(s)_J$$

for all $s \in \Sigma$ and all J such that $I \cap J = \emptyset$. (We take this equality to imply in particular that the right-hand is defined iff the left-hand is also defined.)

Dynamic Characterizations of Main Unitary Transformations.

It is well-known that a linear operator on a vector space in a given Hilbert space is *uniquely determined* by the values it takes on the vectors of an (orthonormal) basis. An important observation is that this fact is no longer "literally true" when we move to "states" as one-dimensional subspaces instead of vectors. The reason is that "phase"-aspects (or, in particular, the signs "$+$" and "$-$") are not "state"

[4]The domain of a map is defined by $dom(F) = \{s \in \Sigma : F(s) \text{ is defined }\}$. If F' is the corresponding linear map on $\mathcal{H}$, this means that $dom(F) = \{\overline{\psi} : F'(\psi) \neq 0\}$.

properties in our setting. In other words, two vectors that differ only in phase, i.e $x = \lambda y$ where λ is a complex number with $\mid \lambda \mid = 1$, belong to the same subspaces, so they correspond to the same state $\overline{x} = \overline{y}$.

Example 1. *(Counterexample)* Consider a 2 dimensional Hilbert space in which we denote the basis vectors by $\mid 0\rangle$ and $\mid 1\rangle$, a transformation I is given by $I(\alpha\mid 0\rangle + \beta\mid 1\rangle) = \alpha \mid 0\rangle + \beta \mid 1\rangle$; and a transformation J is given by $J(\alpha\mid 0\rangle + \beta\mid 1\rangle) = \alpha \mid 0\rangle - \beta \mid 1\rangle$. Although I and J induce different operators on states , these operators map the basis states to the same images:
$I(0) = \overline{I(\mid 0\rangle)} = 0 = \overline{J(\mid 0\rangle)} = J(0)$, $I(1) = \overline{I(\mid 1\rangle)} = 1 = \overline{- \mid 1\rangle} = \overline{J(\mid 1\rangle)} = J(1)$. But of course we do distinguish the subspaces generated by different superpositions: $I(+) = \overline{\mid 0\rangle + \mid 1\rangle} = + \neq - = \overline{\mid 0\rangle - \mid 1\rangle} = J(+)$.

Proposition 8. *A linear operator on the state space $\Sigma(\mathcal{H}_1)$ of a 2 dimensional Hilbert space is uniquely determined by its images on the states: $\overline{\mid 0\rangle}, \overline{\mid 1\rangle}, \overline{\mid +\rangle}$.*

Corollary 2. *A linear operator on the state space $\Sigma(\mathcal{H}_n)$ of the space $\mathcal{H}_n$ is uniquely determined by its images on the states:*

$$\{\overline{\mid x\rangle_1 \otimes ... \otimes \mid x\rangle_n} : \mid x\rangle_i \in \{\mid 1\rangle_i, \mid 0\rangle_i, \mid +\rangle_i\}\}$$

In the definition of a quantum frame given above, we introduced the set $\mathcal{U}$ as the set of unitary transformations for single systems. For compound systems the set $\mathcal{U}$ will be extended with the kind of operators that are active on compound systems. Following the quantum computation literature, we take $\mathcal{U} = \{X, Z, H, CNOT, ...\}$ where X, Z and H are defined by the following table:

	0	1	+
X	1	0	+
Z	0	1	-
H	+	-	0

The transformation $CNOT$ is given by the table:

	00	01	0+	11	10	1+	+0	+1	++
$CNOT$	00	01	0+	11	10	1+	β_{00}	β_{01}	γ

3 Syntax of LQP

The Basic Language of LQP:

To build up the language of LQP, we are given a natural number n, and we put $N = \{1, 2, \ldots, n\}$. We start from a set $\mathcal{Q}$ of *propositional variables*, together with an *arity map*, i.e. every $p \in \mathcal{Q}$ has an arity $k \leq n$; a set $\mathcal{C} = \{+, 1, ...\}$ of *propositional constants*; and a set $\mathcal{U} = \{CNOT_2, X_1, H_1, Z_1, ...\}$ of constants, denoting *basic programs*, to be interpreted as *unitary transformations*; each such program comes also with an arity $k \leq n$. The syntax of LQP is an extension of the classical syntax for PDL, with a set of propositional *formulas* and a set of *programs*, defined by mutual induction:

$$\begin{array}{lllllllllllll} \varphi & ::= & p_I & | & c_i & | & \overline{\pi}_{i,j} & | & \neg\varphi & | & \varphi \wedge \varphi & | & [\pi]\varphi \\ \pi & ::= & \top & | & \varphi? & | & U_I & | & \pi^\dagger & | & \pi \cup \pi & | & \pi;\pi \quad | \quad \pi^* \end{array}$$

Here, we take I to denote sequents of distinct indices in $N = \{1, 2, \ldots, n\}$. In the above syntax, p_I and U_I are well-formed terms iff the arity k of p, or of U, matches the length of the sequence, i.e. $k = |I|$. In the semantics we will interpret p to be a physical property of a system of $|I|$ qubits, and the sentence p_I as saying that the qubits with indices in I have the property p consisting of $k =\mid I \mid$ relevant basic states which are specifically the ones labeled corresponding to the numbers in the subset I. Similarly, in the semantics it will become clear that every member of $\mathcal{U}$ encodes a specific quantum logical gate and the subscript I in U_I will then indicate on which qubits the gate is active. When the arity of a variable p is n, then we skip the subscript, and simply write p instead of p_n.

For a given propositional constant $c \in \mathcal{C}$, we interpret the sentence c_i as saying that "the i-th-qubit is in the state $\mid c\rangle$". Note that 1 as a logical constant (characterizing the qubit $\mid 1\rangle$) is different from the propositional formula $\top$ (*verum*) which we formally introduce later in this section, to denote the "top" element of the lattice of properties. This, in its turn, is also different from the *program* $\top$, introduced in the syntax above, which will simply denote the trivial program, relating any two states.

Extending the Basic Language of LQP:

We extend our language by defining the operations for a *classical disjunction* and a *classical implication* in the usual way, i.e. $\varphi \vee \psi := \neg(\neg\varphi \wedge \neg\psi)$, $\varphi \rightarrow \psi := \neg\varphi \vee \psi$. We introduce constants *verum* $\top := 1_1 \vee \neg 1_1$, and *falsum* $\bot := 1_1 \wedge \neg 1_1$. We define the *classical dual* of $[\pi]\varphi$ in the usual way as $\langle\pi\rangle\varphi := \neg[\pi]\neg\varphi$; the *measurement modalities* $\Box$ and $\Diamond$ that are known in the quantum logic literature can be defined in LQP by putting $\Diamond\varphi := \langle\varphi?\rangle\top$ and $\Box\varphi := \neg\Diamond\neg\varphi$. The *orthocomplement* is defined as $\sim \varphi := \Box\neg\varphi$, or equivalently as $\sim \varphi := [\varphi?]\bot$. By

means of the orthocomplement we define new propositional constants $0_i :=\sim 1_i$ and $-_i :=\sim +_i$, and a binary operation for *quantum join* $\varphi \sqcup \psi :=\sim (\sim \varphi \wedge \sim \psi)$. This expresses *superpositions*: $\varphi \sqcup \psi$ is true at any state which is a superposition of states satisfying φ or ψ. We can also define the *quantum dual* of a modality $[\pi]\psi$ as $\langle \pi^{\sim} \rangle \psi :=\sim [\pi] \sim \psi$. Finally, we put $\langle \pi \rangle^{-1} \psi := \langle (\pi^{\dagger})^{\sim} \rangle \psi$. As we'll see, this captures the *strongest post-condition* ensured by applying program π on a state satisfying (a precondition) ψ.

Testable formulas. We call a program π *deterministic* if π is constructed without the use of choice $\cup$ or iteration $*$. Next we define the set of *testable formulas* φ_t of LQP to be a subset of the above given language, constructed by induction in the following way:

$$\varphi_t \quad ::= \quad \bot \quad | \quad c_i \quad | \quad \overline{\pi}_{i,j} \quad | \quad \varphi_t \wedge \varphi_t \quad | \quad [\pi]\varphi_t$$

where π is any *deterministic program*. Observe that the construction of π might involve non-testable formulas. In particular, for an arbitrary (not necessarily testable) formula φ, remark that $[\varphi?]\psi_t$ is a testable formula.

Proposition 9. *For any formula φ in LQP, $\sim \varphi$ and $\Box\varphi$ are testable formulas.*

Local formulas and local programs. We would like to isolate *local* formulas and programs, i.e. the ones that "affect only the qubits in a given set $I \subseteq N$". These formulas will express local properties (in the sense defined above). When we want to stress that a formula or program is local, we denote them with φ_I or π_I. The definition is:

$$\begin{array}{lllllllllll} \varphi_I & ::= & p_J & | & c_i & | & \overline{\pi}_{ij} & | & \varphi_I \vee \varphi_I & | & \varphi_I \wedge \neg\varphi_I \quad | \quad \varphi_I \wedge [\pi_I]\varphi_I \\ \pi_I & ::= & \varphi_I? & | & U_J & | & \pi_I ; \pi_I & | & \pi_I \cup \pi_I & | & \pi_I^* \end{array}$$

with $i, j \in I$, $J \subseteq I$. Observe that local formulas are not closed under negation: this is because the complement of a local property is not necessarily a local property. But instead they are closed under set-theoretic difference, disjunction, and also conjunction: this is because $\varphi \wedge \psi$ is equivalent to $\varphi \wedge \neg(\varphi \wedge \neg\psi)$.

Relabeling local formulas and programs. When we label a local formula φ_I or a local program π_I with a sequence of indices I, we can of course take any other sequence J of indices, with $|J| = |I|$, and substitute all the I indices in our formula (program) with the corresponding J indices; we denote by φ_J, and respectively π_J, the corresponding formula, or program.

Notation. *The unary map induced by a program:* We want to capture in our syntax the construction $F_{(1)}$, by which a linear map F on $H^{\otimes n}$ was used to describe a

unary map $F_{(1)}$ on H. For this, we put: $0_i! := 0_i? \cup (1_i?; X_i)$, and $0_I! := 0_{i_1}!; 0_{i_2}!; \cdots; 0_{i_k}!$, where $I = (i_1, i_2, \ldots, i_k)$. This maps any qubit in I to 0. Similarly, we put; $0_I? := (0_{i_1} \wedge 0_{i_2} \wedge \cdots \wedge 0_{i_k})?$. Finally we define:

$$\pi_{(i)} := 0_{N\setminus\{i\}}!; \pi; 0_{N\setminus\{i\}}?$$

This is the map we need (which encodes a single qubit transformation). In fact, we shall only use $\pi_{(1)}$ in the rest of this paper.

4 Semantics of LQP

An LQP-*model* is a *quantum frame equipped with a valuation function*, mapping each propositional variable p of arity k into a set $|| \ p \ ||\subseteq \Sigma(H^{\otimes k})$ of k-qubit states. Given a sequence I of length i of indices, let ϵ be the canonical isomorphism between $H^{\otimes k}$ and $H^{\otimes I}$.
We will use the valuation map to give an interpretation $|| \ \varphi \ ||\subseteq \Sigma$ to all our formulas, in terms of properties of our n qubit system, i.e. sets of states in $\Sigma = \Sigma(\mathcal{H})$. In the same time, we give an interpretation $|| \ \pi \ ||\subseteq \Sigma \times \Sigma$ to all our programs, in terms of binary relations between states. The two interpretations are defined by *mutual recursion*.

Interpretation of the Programs: The basic programs U_I, with $|I| = k$, come from a list of corresponding k-bit unitary transformations $U : H^{\otimes k} \to H^{\otimes k}$. We take $|| \ U_I \ ||$ to be the (map on states induced by the) unique linear map on $\mathcal{H}$ such that:

$$|| \ U_I \ || \circ \mu_I \ (\psi \otimes \psi')) := \mu_I(\epsilon_I \circ U \circ \epsilon_i^{-1}(\psi) \otimes \psi')$$

for every $\psi \in \mathcal{H}_I$, $\psi' \in \mathcal{H}_{N\setminus I}$. Here, recall that ϵ_I is the canonical isomorphism between $H^{\otimes k}$ and $\mathcal{H}_I$, and μ_I is the canonical isomorphism between $\mathcal{H}_I \otimes \mathcal{H}_{N\setminus I}$ and $\mathcal{H}$.
As for the others:

$$\begin{array}{llllll}
|| \top || & := & \Sigma \times \Sigma & , & || \varphi? || & := & || \varphi ||? \\
|| \pi_1 \cup \pi_2 || & := & || \pi_1 || \cup || \pi_2 || & , & || \pi^* || & := & || \pi ||^* \\
|| \pi_1; \pi_2 || & := & || \pi_2 || \circ || \pi_1 || & , & || U_I^\dagger || & := & || U_I ||^{-1} \\
|| (\pi^\dagger)^\dagger || & := & || \pi || & , & || (\pi_1; \pi_2)^\dagger || & := & || \pi_2^\dagger; \pi_1^\dagger || \\
|| (\pi_1 \cup \pi_2)^\dagger || & := & || (\pi_1)^\dagger \cup (\pi_2)^\dagger || & , & || (\pi^*)^\dagger || & := & || (\pi^\dagger)^* ||
\end{array}$$

where R^* is the reflexive-transitive closure of relation R. Note that *deterministic programs* π have as interpretations $|| \ \pi \ ||$ (maps on states which are induced by) *linear maps* on $\mathcal{H}$.

The interpretation $|| \pi ||$ allows us to extend the notation $\stackrel{\pi}{\rightarrow}$ to all programs, by putting: $s \stackrel{\pi}{\rightarrow} t$ iff $(s,t) \in || \pi ||$.

Interpretation of the Formulas: We give the interpretation here first for all except propositional variables p_i and entangled state formulas $\overline{\pi}_{ij}$:

$$\begin{array}{lcllcl} || \varphi \wedge \psi || & = & || \varphi || \cap || \psi || & ; & || \neg\varphi || & = & \Sigma \backslash || \varphi || \\ || 1_i || & = & 1_i & ; & || +_i || & = & +_i \end{array}$$

and finally $|| [\pi]\varphi || = \{s \in \Sigma \mid \forall t : s \stackrel{\pi}{\rightarrow} t \Rightarrow t \in || \varphi ||\}$.
The last clause obviously defines *the weakest precondition* $[\pi]\varphi$ ensuring that (postcondition) φ will be satisfied after executing program π. As for the propositional variables, we put:

$$\begin{array}{rcl} || p_I || & = & \{s \in \mathcal{H} : s_I \in \epsilon_I(|| p ||)\} \\ & = & \{\overline{\mu_I(\epsilon_I(\psi) \otimes \psi')} : \overline{\psi} \in || p ||, \psi' \in \mathcal{H}_{N \backslash I}\} \end{array}$$

where ϵ_I and μ_I are the above-mentioned canonical isomorphisms, and s_I is (as defined above) the state of the qubits in I. So the meaning of p_I is that the system of qubits with indices in I is separated from (i.e. non-entangled with) the rest of the system, and that moreover this system has the property expressed by p.

The interpretation of $\overline{\pi}_{ij}$, for *deterministic programs* π, is given by the construction $\overline{F}_{ij}$ above. Since the interpretation $|| \pi ||$ of a deterministic program is a linear map on $\mathcal{H}$, we know, by the results mentioned above, that the map $F_{(1)}$ can be used to specify a set of compound states $\overline{F}_{ij} \subseteq \mathcal{H}$. This is our intended interpretation for $\overline{\pi}_{ij}$:

$$|| \overline{\pi}_{ij} ||:= \overline{|| \pi ||}_{ij}$$

For the program $\top$, we put: $|| \overline{\top} ||:= \{s \in \Sigma : s_{\{i,j\}} \text{ is defined}\} = \{\overline{\mu_{\{i,j\}}(\psi \otimes \psi')} : \psi \in \mathcal{H}_{\{i\,j\}}, \psi' \in \mathcal{H}_{N \backslash \{i,j\}}\}$, i.e. the property of having the $\{i,j\}$-qubits in a separated state from the others. This can be extended to other programs in the natural way, by putting e.g. $|| \overline{\pi \cup \pi'}_{ij} ||:=|| \overline{\pi}_{ij} \cup \overline{\pi'}_{ij} ||$ etc.

Proposition 10. *The interpretation of any testable formula is a testable property. The interpretation of an I-local formula (or deterministic program) is an I-local formula (or linear map on states).*

Lemma 3. $||\sim \varphi ||=|| \varphi ||^{\perp}$, $|| [\varphi?]\psi ||= [|| \varphi ||?] || \psi ||$, $|| \Box\varphi ||= \Box || \varphi ||$, $\overline{|| \varphi ||} =|| \Box\Diamond\varphi ||$

Proposition 11. *The following are equivalent, for every formula φ:*

1. $||\ \varphi\ ||$ *is testable*
2. φ *is semantically equivalent to* $\Box\Diamond\varphi$
3. φ *is semantically equivalent to some formula* $\Box\psi$
4. φ *is equivalent to some formula* $\sim\psi$

5 Axioms for LQP

First, we admit *all the axioms and rules* of **classical** PDL, except for the one concerning tests $\varphi?$. In particular, we have a basic axiom and rule for sentences involving *modalities* $[\pi]$, stated for elementary sentences and basic programs:

Kripke Axiom. $\vdash [\pi](p \to q) \to ([\pi]p \to [\pi]q)$
Necessitation Rule. if $\vdash p$ then $\vdash [\pi]p$

Considering $\Box p$, we introduce the following axioms:
Test Generalization Rule. if $p \to [q?]r$ for all q , then $\vdash p \to \Box r$
Testability Axiom. $\vdash \Box p \to [q?]p$

Testability can be stated in its dual form by means of $\langle q?\rangle p \to \Diamond p$ or equivalently as $\langle q?\rangle p \to \langle p?\rangle\top$. This dual formulation of Testability allows us to give a straightforward interpretation: if the property associated to p can be actualized by a measurement (yielding an output state satisfying p), then we can directly test the property p (by doing a measurement for p). The Test Generalization Rule encodes the fact that $\Box$ is a universal quantifier over all possible measurements.

Other LQP-axioms are:

Partial Functionality.	$\vdash$	$\neg[p?]q \to [p?]\neg q$
Adequacy.	$\vdash$	$p \wedge q \to \langle p?\rangle q$
Repeatability.	$\vdash$	$[\phi_t?]\phi_t$ for all *testable* formulas ϕ_t
Universal Accessibility.	$\vdash$	$\langle\pi\rangle\Box\Box p \to [\pi']p$
Unitary Functionality.	$\vdash$	$\neg[U]q \leftrightarrow [U]\neg q$
Unitary Bijectivity 1.	$\vdash$	$p \leftrightarrow [U; U^\dagger]p$
Unitary Bijectivity 2.	$\vdash$	$p \leftrightarrow [U^\dagger; U]p$
Adjointness.	$\vdash$	$p \to [\pi]\Box\langle\pi^\dagger\rangle\Diamond p$

Substitution Rule. From $\vdash \Theta$ infer $\vdash \Theta[p_I/\varphi_I]$

Compatibility Rule. For all *testable* formulas ψ, φ and every variable $p \notin \varphi, \psi$:

$$\text{From} \quad \vdash \langle\varphi?;\psi?\rangle p \to \langle\psi?;\varphi?\rangle p \ \text{ infer } \ \vdash \langle\varphi?;\psi?\rangle p \to \langle(\varphi \wedge \psi)?\rangle p$$

Proposition 12. *(Quantum Logic, Weak Modularity or Quantum Modus Ponens) All the axioms and rules of traditional Quantum Logic are satisfied by our testable*

formulas. In particular, from our axioms one can prove "Quantum Modus Ponens"[5] $\varphi \wedge [\varphi?]\psi \vdash \psi$. *In its turn, this rule is equivalent to the condition known in quantum logic as Weak Modularity, stated as follows:* $\varphi \wedge (\sim \varphi \sqcup (\varphi \wedge \psi)) \vdash \psi$.

Theorem 4. *(Soundness, Expressivity, Completeness of the above axioms with respect to PDL frames) In the presence of (axioms of classical logic, plus) Kripke's Axiom, Necessitation, Test Generalization, Testability and Substitution Rule, all the other axioms above are sound and expressive with respect to the corresponding semantic conditions mentioned in the Section 2 above. More precisely: any of these axioms is valid on a PDL frame iff the corresponding semantic condition is satisfied by the frame. Moreover, the system given by the above axioms is complete for the class of PDL frames satisfying all the corresponding semantic conditions.*

Proposition 13. *The formula* $< \pi >^{-1} \varphi$ *expresses the strongest testable post-condition ensured by executing program* π *on any state satisfying (precondition)* φ. *In other words: for every testable* ψ, *the following are equivalent:*

1. $\vdash < \pi >^{-1} \varphi \rightarrow \psi$
2. $\vdash \varphi \rightarrow [\pi]\psi$

Moreover, in the context of the other axioms, this equivalence is itself equivalent to the Adjointness Axiom.

Basic Axioms for constants ($0, 1, +, -$**).**
The first axiom says that c_i's are "states" in the i-th part of the system, i.e. they are atomic properties, which determine completely whether any other property is jointly satisfied. We state in a *weak*, as well as in *stronger* version:
Atomicity (weak version). For all $c \in \{0, 1, +, -\}$: $\vdash c_i \wedge p_i \rightarrow \Box\Box(c_i \rightarrow p_i)$
Atomicity (strong version). For all $c \in \{0, 1, +, -\}$:
$\vdash \bigwedge_{i \in I} c_i \wedge p_I \rightarrow \Box\Box(\bigwedge_{i \in I} c_i \rightarrow p_I)$
The following axioms state that $+_i$ and $-_i$ are proper superpositions of 0_i and 1_i:
Proper Superposition Axioms: $\vdash +_i \rightarrow \Diamond 0_i \wedge \Diamond 1_i$ and $\vdash -_i \rightarrow \Diamond 0_i \wedge \Diamond 1_i$.
Next two axioms assert that 1 and $+$ are *testable* properties:
Constants are testable. $\vdash \Box\Diamond 1_i \rightarrow 1_i$ and $\vdash \Box\Diamond +_i \rightarrow +_i$.
Determinacy Axiom of Deterministic Programs. For deterministic programs π, π':

[5] This explains why the weakest precondition $[\varphi?]\psi$ has been taken as the basic implicational connective in traditional Quantum Logic, under the name of "Sasaki hook", denoted by $\varphi \xrightarrow{S} \psi$.

$\vdash \Big(\Box\Box \bigwedge_{(c^{(1)},\ldots,c^{(n)})\in\{0,1,+\}^n} (\langle\pi\rangle^{-1}(c_1^{(1)} \wedge \ldots \wedge c_n^{(n)}) \leftrightarrow \langle\pi'\rangle^{-1}(c_1^{(1)} \wedge \ldots \wedge c_n^{(n)}))\Big)$
$\rightarrow\ (\langle\pi\rangle p \leftrightarrow \langle\pi'\rangle p)$

This expresses the above-mentioned property of linear operators on $\mathcal{H}$ of being uniquely determined by their values on all the states $\mid x\rangle_1 \otimes \cdots \mid x\rangle_n$, with $\mid x\rangle_i \in \{\mid 0\rangle_i, \mid 1\rangle_i, \mid +\rangle_i\}$.

Agreement Axiom. If two I-local programs π, π' have the same domain, then their output states agree on all non-I qubits: i.e. if $I \cap J = \emptyset$ then
$\Box\Box(\langle\pi_I\rangle\top \leftrightarrow \langle\pi'_I\rangle\top) \rightarrow (\langle\pi_I\rangle p_J \leftrightarrow \langle\pi'_I\rangle p_J)$

Compatibility of programs affecting different sets of qubits. If $I \cap J = \emptyset$ then
$\vdash [\pi_I;\pi_J]p \leftrightarrow [\pi_J;\pi_I]p$

Entanglement Rule. From $\vdash p_1 \rightarrow [\pi_{(1)}]q_1$ infer $\vdash \overline{\pi_{ij}} \rightarrow [p_i?]q_j$

Entanglement Composition Axiom. For distinct indices i, j, k, l, programs π, π', π'' and local $\{1\}$-programs σ_1, ρ_1 we have:
$\vdash \overline{\pi}_{ij} \wedge \overline{\pi'}_{kl} \rightarrow [\sigma_j;\rho_k;\overline{\pi''}_{jk}?]\overline{(\pi;\sigma_1;\pi'';\rho_1^\dagger;\pi')}_{il}$

Trivial Entanglement. $\vdash p_{i,j} \rightarrow \overline{\top}_{ij}$ This says that separation of the i,j-qubits implies their trivial entanglement.

Theorem 5. *(Teleportation Property). If φ_1 is a 1-local testable property and if $\vdash \varphi_1 \rightarrow [\pi_{(1)};\sigma_{(1)}]q_1$, then $\vdash \varphi_1 \wedge \overline{\sigma}_{23} \rightarrow [\overline{\pi}_{12}?]q_3$.*

Proof: We apply the Entanglement Composition Axiom, taking $i = 4, j = 1, k = 2, l = 3$, and substituting the programs $\top$ for π, σ for π', π for π'', $\varphi_1?$ for σ_1, and $id_1 = X_1; X_1$ for ρ_1. We obtain: $\vdash \overline{\top}_{41} \wedge \overline{\sigma}_{23} \rightarrow [\varphi_1?;id_2;\overline{\pi}_{12}?]\overline{(\top;p_1?;\pi;id_1^\dagger;\sigma)}_{43}$. On the other hand, we have: $\vdash \varphi_1 \wedge \overline{\sigma}_{23} \rightarrow [0_4!](p_1 \wedge \overline{\top}_{41} \wedge \overline{\sigma}_{23})$ (since $0_4!$ is 4-local and has the same domain as id_4, so by Agreement Axiom it agrees with id_4 on non-4 qubits, thus preserving φ_1 and $\overline{\sigma}_{23}$; but also $\vdash [0_4!]0_4$ and using the Trivial Entanglement Axiom, we get the conclusion). From these two together, we obtain: $\vdash \varphi_1 \wedge \overline{\sigma}_{23} \rightarrow [0_4!][\overline{\pi}_{12}?]\overline{(\top;\varphi_1?;\pi;id_1^\dagger;\sigma)}_{43}$. But on the other hand, we have $\vdash \overline{(\top;\varphi_1?;\pi;id_1^\dagger;\sigma)}_{43} \rightarrow [0_4?]q_3$. (This is because we assumed $\vdash \varphi_1 \rightarrow [\pi_{(1)};\sigma_{(1)}]q_1$, from which it follows that $\vdash 0_1 \rightarrow [\top;\varphi_1?;\pi_{(1)};id_1^\dagger;\sigma_{(1)}]q_1$, using the fact that $id^\dagger = id$ and $\vdash [\varphi_1?]\varphi_1$, by Repeatability axiom and the testability of φ_1. Apply now Entanglement Rule, obtaining the above conclusion.) From these two, we get that: $\vdash \varphi_1 \wedge \overline{\sigma}_{23} \rightarrow [0_4!;\overline{\pi}_{12}?;0_4?]q_3$. The desired conclusion follows from the Agreement Axiom and the fact that $0_4!;\overline{\pi}_{12}?;0_4?$ and $\overline{\pi}_{12}?$ are $\{1,2,4\}$-local programs with the same domain.

Characteristic Formulas. In order to formulate our next axioms (dealing with special logic gates), we give some characteristic formulas for binary states, considering two qubits indexed by i and j:

States	Characteristic Formulas
$\overline{\mid 00\rangle_{ij}} = \overline{\mid 0\rangle_i \otimes \mid 0\rangle_j}$	$\langle 0_i ?\rangle 0_j \wedge [1_i ?] \perp$
Bell states: $\beta_{xy}^{i,j} = \overline{\mid 0\rangle_i \otimes \mid y\rangle_j + (-1)^x \mid 1\rangle_i \otimes \tilde{y}\rangle_j}$ with $\tilde{0} = 1$ and $\tilde{1} = 0$, $x, y \in \{0, 1\}$	$\langle 0_i ?\rangle y_j \wedge \langle 1_i ?\rangle \tilde{y}_j \wedge \langle +_i ?\rangle (-)_j^x$ where $(-)^x = -$ if $x = 1$ and $(-)^x = +$ if $x = 0$
$\gamma^{i,j} = \beta_{00}^{i,j} + \beta_{01}^{i,j} =$ $\overline{\mid 00\rangle_{ij} + \mid 01\rangle_{ij} + \mid 10\rangle_{ij} + \mid 11\rangle_{ij}}$	$\langle 0_i ?\rangle +_j \wedge \langle 1_i ?\rangle +_j \wedge \langle +_i ?\rangle +_j$

Characteristic Axioms for Quantum Gates X and Z.

In general, for all unitary transformations $U \in \mathcal{U}$, we have as a *consequence* of the previous axioms that: $\vdash p_K \rightarrow [U_I] p_K$, for $I \cap K = \emptyset$.
In addition to this, we require for X, Z, H:

$$\begin{array}{lllllllll}
\vdash & 0_i \rightarrow [X_i] 1_i & ; & \vdash & 1_i \rightarrow [X_i] 0_i & ; & \vdash & +_i \rightarrow [X_i] +_i \\
\vdash & 0_i \rightarrow [Z_i] 0_i & ; & \vdash & 1_i \rightarrow [Z_i] 1_i & ; & \vdash & +_i \rightarrow [Z_i] -_i \\
\vdash & 0_i \rightarrow [H_i] +_i & ; & \vdash & 1_i \rightarrow [H_i] -_i & ; & \vdash & +_i \rightarrow [H_i] 0_i
\end{array}$$

Notation. For $x, y \in \{0, 1\}$ and distinct indices $i, j \in N$, we make the following abbreviations for "Bell formulas": $\beta_{xy}^{ij} := \overline{(Z_1^x ; X_1^y)}_{ij}$.

Proposition 14. *The Bell states $\beta_{xy}^{i,j}$ are characterized by the logic Bell formulas β_{xy}^{ij}. In other words, a state satisfies one of these formulas iff it coincides with the corresponding Bell state.*

Proof: It is enough to check that the formulas β_{xy}^{ij} imply the corresponding characteristic formulas in the above table. For this, we use the Entanglement Axiom and the following (easily checked) theorems: $\vdash 0_1 \leftrightarrow < Z_1^x ; X_1^y > y_1$, $\vdash 1_1 \leftrightarrow < Z_1^x ; X_1^y > \tilde{y}_1$, $\vdash +_1 \rightarrow < Z_1^x ; X_1^y > (-)_1^x$.

Characteristic Axioms for $CNOT$. With the above notations, we put:

$$\begin{array}{llllll}
\vdash & 0_i \wedge c_j \rightarrow [CNOT_{ij}] c_j & ; & \vdash & 1_i \wedge 0_j \rightarrow [CNOT_{ij}] 1_j \\
\vdash & 1_i \wedge 1_j \rightarrow [CNOT_{ij}] 0_j & ; & \vdash & 1_i \wedge +_j \rightarrow [CNOT_{ij}] +_j \\
\vdash & +_i \wedge 0_j \rightarrow [CNOT_{ij}] \beta_{00}^{ij} & ; & \vdash & +_i \wedge 1_j \rightarrow [CNOT_{ij}] \beta_{01}^{ij} \\
\vdash & +_i \wedge +_j \rightarrow [CNOT_{ij}] \gamma^{ij} & where & \gamma^{ij} & = \langle 0_i ?\rangle +_j \wedge \langle 1_i ?\rangle +_j \wedge \langle +_i ?\rangle +_j
\end{array}$$

Proposition 15. *For all* $x, y \in \{0,1\}$*:* $\vdash (x_i \wedge y_j) \rightarrow [H_i; CNOT_{i,j}]\beta^{ij}_{xy}$

Corollary. If i, j, k are all distinct then
$\vdash \langle CNOT_{ij}; H_j; (x_i \wedge y_j)?\rangle p_k \leftrightarrow \langle \beta^{i,j}_{xy}?\rangle p_k$. *Proof*: From the above and $H^\dagger = H$, $CNOT^\dagger = CNOT$, we get $\vdash \beta^{ij}_{xy} \rightarrow [CNOT_{i,j}; H_i](x_i \wedge y_i)$, and so $\vdash \langle CNOT_{ij}; H_j; (x_i \wedge y_j)?\rangle \top \leftrightarrow \langle \beta^{ij}_{xy}?\rangle \top$. The conclusion follows from this, together with the Agreement Axiom.

6 Correctness of the Teleportation Protocol

Following [8], quantum teleportation is the name of a technique that makes it possible to teleport the state of a quantum system without using a channel that allows for quantum communication, but with a channel that allows for classical communication. We are working in $H \otimes H \otimes H$, with H being the two-dimensional (qubit) space, and so $n = 3$. We assume two agents, Alice and Bob who are separated in space and each has one qubit of an entangled EPR pair that is represented by $\beta^{2,3}_{00} \in H^{(2)} \otimes H^{(3)}$. Alice holds in addition to her part of the EPR pair also a qubit $q_1 \in H^{(1)}$ in an unknown state φ_1. Alice "teleports" this state to Bob, i.e. she performs a program that will output a state satisfying φ_3. To do this, she first entangles q_1 with her part q_2 of the EPR pair (i.e. she performs a $CNOT_{1,2}$ gate on the two qubits and then a Hadamard transformation H_1 on the first component). Bob's qubit has suffered during the actions of Alice and when Alice will measure her qubits she will destroy the entanglement of the EPR pair that she shares with Bob. The initial state of Bob's qubit is known and we can calculate which changes it has gone through when we know the result that Alice obtains from the two measurements. Moreover, the result that Alice obtains from the two measurements indicate the actions that Bob has to perform in order to transfer his qubit into q_3 into the state q_1 was before the protocol. It is enough for Alice to send Bob two classical bits encoding the result x_1 of the first measurement and the result y_2 of the second measurement. This means that Bob will have to apply y times the X-gate followed by x times the Z gate, if he wants to force his qubit q_3 into the state φ_3.
In our syntax, the quantum program described here is:

$$\pi = \bigcup_{x,y \in \{0,1\}} CNOT_{12}; H_1; (x_1 \wedge y_2)?; X_3^y; Z_3^x$$

and the validity expressing the correctness of teleportation is

$$\vdash \varphi_1 \wedge \beta^{2,3}_{00} \rightarrow [\pi]\varphi_3$$

for all testable 1-local formulas φ_1. To show this, observe that by applying the above Corollary (at the end of the last section) in which we take $i = 1, j = 2, k = 3$ and then substitute p_3 with $[X_3^y; Z_3^x]\varphi_3$, we obtain that the validity above (to be proved) is equivalent to: $\vdash \varphi_1 \wedge \beta_{00}^{2,3} \rightarrow [\beta_{xy}^{1,2}?][X_3^y; Z_3^x]\varphi_3$.
Replacing the logical Bell formulas with their definitions $\beta_{xy}^{ij} := \overline{(Z_1^x; X_1^y)}_{ij}$, we obtain the following equivalent validity: $\vdash \varphi_1 \wedge \overline{id}_{23} \rightarrow [\overline{(Z_1^x; X_1^y)}_{1,2}?][X_3^y; Z_3^x]\varphi_3$, where $id = Z_1^0; X_1^0$ is the identity. This last validity follows from applying the Teleportation Property and the validity $\vdash \varphi_1 \rightarrow [Z_1^x; X_1^y; X_1^y; Z_1^x]\varphi_1$ (due to $X^{-1} = X, Z^{-1} = Z$).
Note. This proof of correctness can be easily adapted to cover logic-gate teleportation. Moreover, the whole range of quantum programs covered by the "entanglement networks" in [5] can be similarly treated using our logic.

References

[1] S. Abramsky and B. Coecke, "A Categorical Semantics of Quantum Protocols.", in the proceedings of LICS'04. Available at arXiv:quant-ph/0402130.

[2] A. Baltag, "Dynamic and Epistemic Logics for Quantum Measurements", Presented at PML'04, Brussels 2004.

[3] A. Baltag and S. Smets, "The Logic of Quantum Actions", preprint. Abstract at http://emmy.nmsu.edu/IQSA/ has been accepted for presentation at *Quantum Structures '04* (IQSA), Denver 2004.

[4] O. Brunet and P. Jorrand, "Dynamic Quantum Logic for Quantum Programs", Grenoble 2003. Available at arXiv:quantph/0311143

[5] B. Coecke, "The Logic of Entanglement", March 2004, arXiv: quant-ph/0402014.

[6] M.L. Dalla Chiara and R. Giuntini, "Quantum Logics", in D.M. Gabbay and F. Guenthner (eds.) *Handbook of Philosophical Logic*, Second Edition, vol. 6, Kluwer Ac. Pub., Dordrecht, 129-228, 2002.

[7] R.I. Goldblatt, "Semantic Analysis of Orthologic", *Journal of Philosophical Logic*, **3**, 19-35, 1974.

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

[9] S. Smets, "On Quantum Propositional Dynamic Logic", Presented at PML'04, Brussels 2004.