

# LQP: The Dynamic Logic of Quantum Information

Alexandru Baltag\* and Sonja Smets†

## Abstract

We present a dynamic logic for reasoning about information flow in quantum programs. In particular, we give a finitary syntax and a relational semantics for a *Logic of Quantum Programs (LQP)*, that is capable of dealing with quantum measurements, unitary evolutions and entanglements in compound quantum systems. 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 quantum gates. As an example of application, we use our logic to give a formal proof for the correctness of the Teleportation protocol (proof which can be easily adapted to check Logic-Gate Teleportation).

## 1 Introduction

As a natural extension of Hoare Logic, Propositional Dynamic Logic (*PDL*) is an important tool for the logical study of programs, especially by providing a basis for *program verification*. In the context of recent advances in quantum programming, it is natural to look for a *quantum* version of *PDL*, which could play the same role in proving correctness for quantum programs that classical *PDL* (and Hoare logic) played for classical programs.

The search for such a “quantum dynamic logic” has been one of our main objectives, in the process of investigating the logic of quantum information flow in a series of presentations [4, 34] and papers [6, 5, 7]. Several logical systems have been proposed: in [6] we focused on single quantum systems and presented two equivalent *complete axiomatizations* for a Logic of Quantum Actions (*LQA*,

---

\*Oxford University Computing Laboratory, baltag@comlab.ox.ac.uk

†Vrije Universiteit Brussel, Flanders’ Fund for Scientific Research Post-Doc, sonsmets@vub.ac.be

allowing actions such as measurements and unitary evolutions, but no entanglements). The completeness result was obtained with respect to infinite-dimensional classical Hilbert spaces, as models for *single quantum systems*. The challenge of providing a similar axiomatization for *compound systems* was taken up in [5], where a first proposal for a *logic of multi-partite quantum systems* was sketched.

In this paper we elaborate further, simplify and improve on the work outlined in [5], developing a full-fledged *Logic of Quantum Programs LQP*.<sup>1</sup> This includes: (1) a simple *finitary syntax* for a *modal language*, based on a minor variation of classical *PDL*, with dynamic modalities corresponding to (weakest preconditions of) quantum programs; (2) a *relational semantics* for this logic, in terms of *quantum states and quantum actions over a finite-dimensional Hilbert space*; (3) a *sound proof system*, which includes axioms to handle *separation, locality and entanglement*; (4) *formal proofs (in our proof system LQP) of non-trivial computational properties of compound quantum systems*; (5) *an analysis (with a formal correctness proof) of the Teleportation Protocol*.

The first fundamental idea underlying our logic is one that was first presented in [4, 34] and developed in [6], but whose deep “ideological” roots come from a long tradition of previous work on dynamic interpretations of quantum logic (in [18, 19, 20, 3, 10, 14, 11, 13, 12, 35]): this is the idea of having a *quantum reinterpretation* of the language of classical *PDL*, in which the “test” actions  $\varphi?$  of *PDL* (used to capture conditional programs in dynamic logic) are to be read as “*successful measurements*” of a *quantum property*  $\varphi$  (i.e. projectors in a Hilbert space over the subspace generated by the set of states satisfying  $\varphi$ ), while the other basic actions of *PDL* are taken to be *quantum gates* (i.e. unitary operators on a Hilbert space). As shown in [4, 34, 6], this immediately allows us to re-capture in our (Boolean) logic all the power of traditional (non-Boolean) Quantum Logic: the “quantum disjunction” (expressing superpositions), the “quantum negation” (the so-called “orthocomplement”  $\sim \varphi$ , expressing necessary failure of a measurement) and the “quantum implication” (the so-called “Sasaki hook”  $\phi \xrightarrow{S} \psi$ , capturing causality in quantum measurements) are all expressible using quantum-dynamic modalities  $[\varphi?]\psi$  (which capture *weakest preconditions*<sup>2</sup> of *quantum measurements*).<sup>3</sup> In other words: in our logic (unlike other logi-

<sup>1</sup>But note the difference between our logic *LQP* and the approach with a similar name in [9]: 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 (see e.g. [16, 17, 22]).

<sup>2</sup>See e.g. [25] for an introduction to dynamic modalities  $[\pi]\psi$  describing weakest preconditions ensuring (the satisfaction of some given post-condition)  $\psi$  after the execution of an action  $\pi$ .

<sup>3</sup>Indeed, it turns out that a quantum implication  $\phi \xrightarrow{S} \psi$  is simply equivalent to the weakest pre-

cal approaches to quantum systems), *all the non-classical “quantum” effects are captured using a non-classical “logical dynamics”, while keeping the classical, Boolean structure of the underlying propositional logic of “static” properties.*

The second fundamental idea of our approach is the one first outlined in [5]: adding *spatial features* to dynamic logic, in order to capture relevant properties of *multi-partite (i.e. compound) quantum systems* (e.g. separation, locality, entanglement). For this, we use a finite set  $N$  of *indices* to denote the most basic “parts” (qubits) of the system, and use *sets of indices*  $I \subseteq N$  to denote all the (possibly compound) subsystems; we have special propositional constants  $1, 0, +$  etc. to express the fact that qubits are in the state  $|1\rangle, |0\rangle$  or  $|+\rangle$  etc; we use a basic propositional formula  $\top_I$  to express “*separation*”<sup>4</sup> (the fact that qubits in the subsystem  $I$  are separated from the rest); and we have a basic program  $\top_I$ , denoting a *non-determined (i.e. randomly chosen) local transformation* (affecting only the qubits in the subsystem  $I$ ). These ingredients are enough to define all the relevant spatial features we need, and in particular to define the notion of (*local*) *component*  $\varphi_I$  of a (*global*) *property*  $\varphi$ , the notion of (*I*-)local *property*  $I(\varphi)$  (i.e.  $\varphi$  is a property of the separated  $I$ -subsystem) and the notion of (*I*-)local *program*  $I(\pi)$  (i.e.  $\pi$  is a program affecting only the  $I$ -subsystem).

The third fundamental idea that underlies our approach comes from [14] and [15] (and was further elaborated in a category-theoretical setting in [1]): this is a *computational understanding of entanglement, in which an entangled state is seen as a “static” encoding of a program.* Mathematically, this comes from the simple observation that a tensor product  $H_i \otimes H_j$  of two Hilbert spaces is canonically isomorphic to the space  $H_i \rightarrow H_j$  of all linear maps between the two spaces. But, as noted in [14, 15], this isomorphism has a *physical meaning*: the entangled state  $\overline{\pi_{ij}}$ , that “*encodes*” (via the above isomorphism) the linear map  $\pi : H_i \rightarrow H_j$ , has the property that *any successful measurement of its  $i$ -th qubit (resulting in some local output-state  $q_i$ ) induces a correlative collapse of the  $j$ -th qubit, whose local output-state (after the collapse) is computed by the map  $\pi$  (i.e. it is given by  $\pi(q)_j$ ).* So *the above isomorphism captures the correlations between possible results of potential local measurements* (on the two qubits). We use this idea to define formulas  $\overline{\pi_{ij}}$  that characterize such specifically entangled states (by using weakest preconditions to express potential behavior under possible measurements). The fundamental correlation given by the above isomorphism is then stated as our “*Entanglement Axiom*”, which plays a central role in our system.

---

condition  $[\varphi?]\psi$ . In quantum logic, this dynamic view can be traced back to the analysis of the Sasaki hook as a Stalnaker conditional presented in [23, 24] and is reflected upon in e.g. [8, 33].

<sup>4</sup>This can be compared with the *exogenous quantum logic approach* in [30], that makes use of general modal operators to separate subsystems.

This *combination of quantum-dynamic and spatial logic* is what allows us to give a *logical characterization of Bell states* and of *various quantum gates*, and to *prove from our axioms highly non-trivial properties of quantum information flow* (such as the “Teleportation Property”, the “Agreement Property”, the “Entanglement Preparation” and “Entanglement Composition” lemmas etc.).

It is well-known that *PDL*, and its fragment the Hoare Logic, are among the main logical formalisms used in *program verification* of classical programs, i.e. in checking that a given (classical) program is *correct* (in the sense of meeting the required specifications). It is thus natural to expect our quantum dynamic logic to play a significant role in the formal *verification of quantum programs*. In this paper, we partially fulfil this expectation by giving a *fully axiomatic correctness proof for the Teleportation protocol*; the proof can be easily adapted to verify *Logic-Gate Teleportation* and many other quantum programs.

Finally, we mention here some of the *limitations of our approach*, which arise from our *purely qualitative, logic-based* view of quantum information. The quantitative aspects are thus neglected: in our presentation, we follow the *operational quantum logic* tradition (for which see e.g. [26, 27]) in abstracting away from complex numbers, “phases” and probabilities. As customary in quantum logic, we identify the “states” of a physical system with “rays” in a Hilbert space (i.e. one-dimensional closed linear subspaces), rather than with unitary vectors, and consequently, our programs will be “*phase-free*”. This is a serious limitation, as phase aspects are important in quantum computation; there are ways to re-introduce (relative) phases in our approach, but this gives rise to a much more complicated logic, and so we leave this development for future work. Similarly, although our dynamic logic *cannot express probabilities, but only “possibilities”* (via the dynamic modalities, which capture the system’s potential behavior under possible actions), *there exist natural extensions of this setting to a probabilistic modal logic*. One of our projects is to work out the full details of this setting, developing a proof system for probabilistic *LQP*.

## 2 Preliminaries: Quantum Frames

In this section we organize Hilbert spaces as relational structures, called *quantum frames* (also called *quantum transition systems* in [6]). We first study the quantum frames of a *single quantum system*, then consider systems composed of *parts* (sub-systems): these are called *compound* (or *multi-partite*) *quantum systems*. In this later case we restrict our attention to systems composed of finitely many “qubits”.

## 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  $\Sigma$  are of two types: the first, called *tests* and denoted by  $S?$ , are labelled with subsets  $S$  of  $\Sigma$ , 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 [6], 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 was a *quantum PDL*, whose negation-free part with dynamic modalities for quantum tests was equivalent to what is traditionally called “(orthomodular) quantum logic” (see e.g. [16, 17, 22]). In this paper, we extend the syntax of this logic to deal with unitary evolutions, entanglements and some quantum protocols.

Recall that a *Hilbert space*  $\mathcal{H}$  is a complex vector space with an inner product  $\langle - | - \rangle$ , which is complete in the induced metric. The *adjoint* (or *Hermitian conjugate*) of a linear map  $F : \mathcal{H} \rightarrow \mathcal{H}$  is the unique linear map  $F^\dagger : \mathcal{H} \rightarrow \mathcal{H}$  s.t.  $\langle x | F(y) \rangle = \langle F^\dagger(x) | y \rangle$ , for all  $x, y \in \mathcal{H}$ . For any closed linear subspace  $W \subseteq \mathcal{H}$ , the *projector*  $P_W : \mathcal{H} \rightarrow \mathcal{H}$  onto  $W$  is given by:  $P_W(u + v) = u$ , for all  $u \in W, v \in W^\perp$ . Projectors are linear, idempotent ( $P \circ P = P$ ) and self-adjoint ( $P^\dagger = P$ ). A *unitary transformation* is a linear map  $U$  on  $\mathcal{H}$  s.t.  $U \circ U^\dagger = U^\dagger \circ U = id$ , where  $id$  is the identity on  $\mathcal{H}$ . Unitary operators preserve inner products.

In Quantum Mechanics, projectors are used to represent (*successful*) *measurements*. A measurement is in fact a *set* of projectors (over mutually orthogonal subspaces); but, whenever a measurement is successfully performed, *only one* of the projectors is “actualized”: the outcome is given by that particular projector. In Quantum Mechanics, unitary transformations represent *reversible evolutions* of a system. In Quantum Computation, they correspond to *quantum-logical gates*.

**Quantum Frames.** 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  $\Sigma$  be the set of *one dimensional subspaces* of  $\mathcal{H}$ , called the set of *states*. We denote a state  $s = \bar{x}$  of  $\mathcal{H}$  using any of the non-zero vectors  $x \in \mathcal{H}$  that generate it, as a subspace. Note that any two vectors that differ only in *phase* (i.e.  $x = \lambda y$ , with  $\lambda \in \mathbb{C}$  with  $|\lambda| = 1$ ) will generate the same state  $\bar{x} = \bar{y} \in \Sigma$ .
2. Call two states  $s$  and  $t$  in  $\Sigma$  *orthogonal*, and write  $s \perp t$ , if every two vectors  $x \in s, y \in t$  are orthogonal, i.e. if  $\forall x \in s \forall y \in t \langle x | y \rangle = 0$ . Equivalently, we can state that  $s \perp t$  iff  $\exists x \in s, y \in t$  with  $x \neq 0, y \neq 0$  and  $\langle x | y \rangle = 0$ . We put  $S^\perp := \{t \in \Sigma \mid t \perp s \text{ for all } s \in S\}$ ; and we denote by  $\bar{S} = S^{\perp\perp} := (S^\perp)^\perp$  the *biorthogonal closure* of  $S$ . In particular, for a singleton  $\{x\}$ , we just write  $\bar{x}$  for  $\{\bar{x}\}$ , which agrees with the notation  $\bar{x}$  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  $\bar{S} = S$ . (Note that  $S \subseteq \bar{S}$  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  $\bar{S}$  of any arbitrary set  $S \subseteq \Sigma$  is the closed linear subspace  $\bigcup \bar{S} \subseteq \mathcal{H}$  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  $\Sigma$ , 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:

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

We denote by  $\overset{S?}{\subseteq} \subseteq \Sigma \times \Sigma$  the binary relation corresponding to the partial map  $S?$ , i.e. given by:  $s \overset{S?}{\subseteq} t$  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  $\xrightarrow{U} \subseteq \Sigma \times \Sigma$ , given by:  $s \xrightarrow{U} t$  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  $\mathcal{H}$ , by taking one-dimensional subspaces as “states”, 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. As mentioned in the Introduction, this imposes some limits to our approach, mainly that we will not be able to express *phase*-related properties.

**Operators on states, adjoints and generalized tests.** To generalize our notations introduced earlier, observe that every *linear operator*  $F : \mathcal{H} \rightarrow \mathcal{H}$  induces a partial map  $F : \Sigma \rightarrow \Sigma$  on states (i.e. subspaces), given by  $F(\bar{x}) = \overline{F(x)}$ , 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  $F : \Sigma \rightarrow \Sigma$  obtained in this way has an *adjoint*  $F^\dagger : \Sigma \rightarrow \Sigma$ , defined as the map on states induced by the adjoint 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:  $S^\dagger := \overline{S}$ . So we identify a test of a “non-testable” property  $S$  with the quantum test of its biorthogonal closure. Observe that  $S^{\dagger\dagger} = S$  (since projectors are self-adjoint).

**Measurement (Non-orthogonality) Relation.** For all  $s, t \in \Sigma$ , let  $s \rightarrow t$  if and only if  $s \xrightarrow{S^\dagger} t$  for some property  $S \in \mathcal{L}$ . In other words,  $s \rightarrow t$  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*<sup>5</sup>:  $s \rightarrow t$  iff  $s \not\perp t$ .

**Quantum Actions.** A *quantum action* is any relation  $R \subseteq \Sigma \times \Sigma$  which can be written as an arbitrary<sup>6</sup> union  $R = \bigcup_i F_i$  of linear maps  $F_i : \Sigma \rightarrow \Sigma$ . The family of quantum actions forms a *complete lattice* (with inclusion), having set-theoretic union  $R \cup R'$  as supremum. Notice also that this family is closed under *relational composition*  $R; R' := \{(s, t) \in \Sigma \times \Sigma : \exists w \in \Sigma (s, w) \in R, (w, t) \in R'\}$ , and iteration  $R^* := \bigcup_{k \geq 0} R^k$  (where  $R^0 = \text{id}$ ,  $R^1 = R$ ,  $R^2 = R; R$ ,  $R^3 = R; R; R$  is a composition of  $n$  terms). Quantum actions are a *relational (input-output) representation of quantum programs*. Indeed, in our dynamic logic we will interpret (the dynamic modalities for) quantum programs as (weakest preconditions of) quantum actions.

<sup>5</sup>The non-orthogonality relation has indeed been used to introduce an accessibility relation in the orthoframe semantics within quantum logic [22, 21].

<sup>6</sup>i.e. possibly infinite.

**Weakest Precondition, Image, Strongest Post-condition and Measurement Modalities.** For any property  $T \subseteq \Sigma$  and any quantum action  $R \subseteq \Sigma \times \Sigma$ , let  $[R]T := \{s \in \Sigma : \forall t \in \Sigma (sRt \Rightarrow t \in T)\}$  and  $\langle R \rangle T := \Sigma \setminus ([R](\Sigma \setminus T))$ . Similarly, put  $R(T) := \{s \in \Sigma : \exists t \in T \text{ such that } tRs\}$ . We also put  $R[T] := \overline{R(T)}$  for the biorthogonal closure of the image. Finally, put  $\Box T := \{s \in \Sigma : \forall t (s \rightarrow t \Rightarrow t \in T)\}$  and  $\Diamond T := \Sigma \setminus (\Box(\Sigma \setminus T))$ .

Observe that  $[R]T$  expresses the *weakest precondition* for the “program”  $R$  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  $T$ .  $R(T)$  is the *image* of  $T$  via  $R$ , which is in fact the *strongest property (among all properties in  $\mathcal{P}(\Sigma \times \Sigma)$ ) ensured to hold after applying program  $R$  if a precondition  $T$  holds at the input-state*. This is the “strongest postcondition” in an absolute sense. However, the *strongest testable postcondition* (ensured to hold after running  $R$  if precondition  $T$  holds at the input state) is given by  $R[T]$ .  $\Box T$  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  $[R]T \in \mathcal{L}$ , for every quantum relation  $R$ . For every state  $s \in \Sigma$ , we have  $\{s\} \in \mathcal{L}$ , i.e. “states are testable”.

**Proposition 2.** A property  $S \subseteq \Sigma$  is testable if and only if any of the following equivalent conditions hold:

- $S = \overline{S}$ ;
- $\exists T \in \Sigma$  such that  $S = T^\perp$ ;
- $\exists T \in \Sigma$  such that  $S = \Box T$ .

**Quantum Joins.** 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 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.** The following properties hold in every quantum frame  $\Sigma = \Sigma(\mathcal{H})$ :

1. *Partial functionality*: If  $s \xrightarrow{S?} t$  and  $s \xrightarrow{S?} v$  then  $t = v$ .
2. *Trivial tests*:  $\emptyset? = \emptyset$  and  $\Sigma? = \Delta_\Sigma$ , where  $\Delta_\Sigma = \{(s, s) : s \in \Sigma\}$  is the identity relation on  $\Sigma \times \Sigma$ .
3. *Atomicity*. States are testable, i.e.  $\{s\} \in \mathcal{L}$ .  
This is equivalent to requiring that “states can be distinguished by tests”, i.e. if  $s \neq t$  then  $\exists P \in \mathcal{L} : s \perp P, t \not\perp P$
4. *Adequacy*. Testing a true property does not change the state:  
if  $s \in P$  then  $s \xrightarrow{P?} s$
5. *Repeatability*. Any testable property holds after it has been successfully tested: if  $s \xrightarrow{P?} t$  then  $t \in P$
6. *Compatibility*:  
If  $S, T \in \mathcal{L}$  are testable and  $S?; T? = T?; S?$  then  $S?; T? = (S \cap T)?$ .
7. *Self-Adjointness*: if  $s \xrightarrow{P?} w \rightarrow t$  then there exists some element  $v \in \Sigma$  such that  $t \xrightarrow{P?} v \rightarrow s$
8. *Proper Superposition*. Every two states of a quantum system can be properly superposed into a new state:  $\forall s, t \in \Sigma \exists w \in \Sigma s \rightarrow w \rightarrow t$
9. *Unitary Reversibility and Totality*. Basic unitary evolutions are *total bijective functions, having as adjoint their inverse*:

$$U; U^\dagger = U^\dagger; U = id$$

where  $id$  is the identity map

10. *Orthogonality Preservation*. Basic unitary evolutions preserve (non) orthogonality: Let  $s, t, s', t' \in \Sigma$  be such that  $s \xrightarrow{U} s'$  and  $t \xrightarrow{U} t'$ . Then:  $s \rightarrow t$  iff  $s' \rightarrow t'$ .

*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. *Atomicity* follows from the fact that states are nothing

but one-dimensional closed linear subspaces, i.e. atoms of the lattice of all closed linear subspaces. *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 that projectors are self-adjoint (i.e.  $S^{\dagger} = S$ ). *Proper Superpositions* can be proved by cases: If  $s \not\perp t$ , i.e. let  $s \rightarrow t$ , then  $w = s \Rightarrow s \rightarrow s \rightarrow t$ . If  $s \perp t$ , i.e. let  $s \not\rightarrow t$  then let  $s = \bar{x}, t = \bar{y}$  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  $\langle x | x + y \rangle = 0$  and then  $\langle x | x \rangle + \langle x | y \rangle = 0$ ; but  $x \perp y$  implies  $\langle x | x \rangle = 0$ . So from  $\langle x | x \rangle = 0$  follows that  $x = 0$ , which yields a contradiction). Similarly, we get  $y \not\perp (x + y)$ . The last two conditions are immediate consequences of the definition of a unitary operator.

Note that, as a consequence of the ‘‘Proper Superpositions’’ property, *the double-box modality*  $\square\square$  coincides with the universal modality, i.e.:  $\square\square S \neq \emptyset$  iff  $S = \Sigma$ .

**Theorem 2.** (*Adjointness*) Let  $F$  be a quantum map and let  $s, w, t \in \Sigma$  be states: If  $s \xrightarrow{F} w \rightarrow t$  then there exists some state  $v \in \Sigma$  such that  $t \xrightarrow{F^{\dagger}} v \rightarrow s$ .

*Proof:* To prove this theorem we use the definition of adjointness in a Hilbert space:  $\langle Fx | y \rangle = \langle x | F^{\dagger}y \rangle$ . From this, we get the equivalence:  $\langle Fx | y \rangle = 0$  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  $s \rightarrow t$  is the same as non-orthogonality  $s \not\perp t$ , we obtain the equivalence:  $\exists w(\bar{x} \xrightarrow{F} \bar{w} \rightarrow \bar{y})$  iff  $\exists v(\bar{y} \xrightarrow{F^{\dagger}} \bar{v} \rightarrow \bar{x})$ .

This proves the adjointness property. As a consequence:

**Corollary 1.** For every property  $P \subseteq \Sigma$  and every linear map  $F$  we have:  $P \subseteq [F]\square\langle F^{\dagger} \rangle \diamond P$

**Corollary 2.** If  $F$  is a quantum map, then

$$F^{\dagger}(s) = ([F]s^{\perp})^{\perp}$$

*Proof:* Using the fact that the negation of the measurement accessibility relation  $\rightarrow$  is the orthogonality relation  $\perp$ , we immediately obtain from the above Theorem that:

$$s \perp F^{\dagger}(t) \text{ iff } t \perp F(s),$$

i.e.

$$s \in (F^\dagger(t))^\perp \text{ iff } F(s) \in t^\perp.$$

From this, we obtain that  $(F^\dagger(t))^\perp = [F]t^\perp$ . Since  $F^\dagger$  is a *map*,  $F^\dagger(t)$  is a (single) state, so it is a *testable* property. Hence, we have  $F^\dagger(t) = (F^\dagger(t))^{\perp\perp} = ([F]t^\perp)^\perp$ .

This result leads us to the following natural generalization of the notion of *adjoint to all quantum actions*:

**Adjoint of a Quantum Action.** For every quantum action  $R \subseteq \Sigma \times \Sigma$ , we define a relation  $R^\dagger \subseteq \Sigma \times \Sigma$  by:

$$sR^\dagger t \text{ iff } t \perp [R]s^\perp$$

or, in other words,

$$R^\dagger(s) = ([R]s^\perp)^\perp$$

**Proposition 3.** For all quantum actions  $R, Z \subseteq \Sigma \times \Sigma$ , states  $s, t \in \Sigma$  and properties  $S \subseteq \Sigma$ , we have the following:

1.  $R^\dagger$  is a quantum action;
2. if  $R = F$  is a (quantum, i.e. linear) map<sup>7</sup> then the relational adjoint  $R^\dagger$  coincides with the Hermitian adjoint  $F^\dagger$  (of  $F$  as linear map).
3.  $s \perp R^\dagger(t)$  iff  $t \perp R(s)$ .
4.  $(R; Z)^\dagger = Z^\dagger; R^\dagger$ .
5.  $(R \cup Z)^\dagger = R^\dagger \sqcup Z^\dagger$ .
6.  $R[S] = ([R^\dagger]S^\perp)^\perp$ .

---

<sup>7</sup>We identify a map  $F : \Sigma \rightarrow \Sigma$  with its graph  $F \subseteq \Sigma \times \Sigma$ , i.e. quantum maps are special cases of quantum relations, which happen to be partial functions. So  $R = F$  means that the two sides are equal, as relations.

## 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  $\{|0\rangle, |1\rangle\}$ . We fix a natural number  $n \geq 2$  (although later we will restrict to the case  $n \geq 4$ ), and we put  $N = \{1, 2, \dots, n\}$ . A *compound-system quantum frame* will be the quantum frame  $\Sigma(\mathcal{H}_n)$  build on a Hilbert space  $\mathcal{H}_n = H^{\otimes n} = H \otimes H \otimes \dots \otimes H$  ( $n$  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  $\mathcal{H}_I = H^{\otimes I} = \bigotimes_{i \in I} H^{(i)}$ . (So, in particular,  $\mathcal{H}_N = \mathcal{H}_n = \mathcal{H}$ .) We denote by  $\epsilon_i : H \rightarrow H^{(i)}$  the canonical isomorphism between  $\mathcal{H}$  and  $H^{(i)}$ . This notation can be extended to sets  $I \subseteq N$  of indices of length  $|I| = k$ , by putting  $\epsilon_I : H^{\otimes k} \rightarrow \mathcal{H}_I$  to be the canonical isomorphism between these spaces. Similarly, for each set  $I \subseteq N$ , we denote by  $\mu_I : \mathcal{H}_I \otimes \mathcal{H}_{N \setminus I} \rightarrow \mathcal{H}$  the canonical isomorphism between these two spaces. For any vector  $|x\rangle \in H$ , we denote by  $|x\rangle^{\otimes I} = \bigotimes_{i \in I} |x\rangle^{\otimes I}$  the corresponding vector in  $\mathcal{H}_I$  (obtained by tensoring  $|I|$  copies of  $|x\rangle$ ). 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). We say that the state  $s$  is  $I$ -separated iff  $s_I$  exists. In this case,  $s_I$  is called the ( $I$ -)local component (or local state) of  $s$ . In particular, when  $I = \{i\}$ , the local component  $s_i \in \mathcal{H}_{\{i\}} = H^{(i)}$  is called the  $i$ -th coordinate of the state  $s$ .

We will further denote the vector  $|0\rangle + |1\rangle$  by  $|+\rangle$ , and similarly denote  $|0\rangle - |1\rangle$  by  $|-\rangle$ . For the states generated by the vectors in a two dimensional Hilbert space we introduce the following abbreviations:  $+$  :=  $\overline{|+\rangle}$ ,  $-$  :=  $\overline{|-\rangle}$ ,  $0$  :=  $\overline{|0\rangle}$ ,  $1$  :=  $\overline{|1\rangle}$ . In order to refer to the state corresponding to a pair of qubits, we similarly delete the Dirac notation, e.g.  $00$  :=  $\overline{|00\rangle} = \overline{|0\rangle \otimes |0\rangle}$ . The Bell states will be abbreviated as follows:  $\beta_{00}$  :=  $\overline{|00\rangle + |11\rangle}$ ,  $\beta_{01}$  :=  $\overline{|01\rangle + |10\rangle}$ ,  $\beta_{10}$  :=  $\overline{|00\rangle - |11\rangle}$ ,  $\beta_{11}$  :=  $\overline{|01\rangle - |10\rangle}$  and  $\gamma$  :=  $\overline{|00\rangle + |01\rangle + |11\rangle + |10\rangle}$ .

The following two results are well-known:

**Proposition 4.** Let  $H^{(i)}$  and  $H^{(j)}$  be two Hilbert spaces. There exists a bijective correspondence  $\psi$  between the linear maps  $F : H^{(i)} \rightarrow H^{(j)}$  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  $\psi$  is given by the mapping  $F = \sum_{\alpha\beta} m_{\alpha\beta} \langle \epsilon_\alpha^{(i)} | - \rangle \cdot \epsilon_\beta^{(j)}$  into the state  $\psi(F) = \sum_{\alpha\beta} m_{\alpha\beta} \cdot \epsilon_\alpha^{(i)} \otimes \epsilon_\beta^{(j)}$ .

**Proposition 5.** Let  $\mathcal{H} = H^{\otimes n}$  and let  $W = \{x \otimes | 0\rangle^{\otimes(n-1)} : x \in H\}$  be given. Any linear map  $F : \mathcal{H} \rightarrow \mathcal{H}$  induces a linear map  $F_{(1)} : H \rightarrow H$  in a canonical manner: it is defined as the unique map on  $H$  satisfying  $F_{(1)}(x) = P_W \circ F(x \otimes | 0\rangle^{\otimes(n-1)})$ . Conversely, any linear map  $G : H \rightarrow H$  can be represented as  $G = F_{(1)}$  for some linear map  $F : \mathcal{H} \rightarrow \mathcal{H}$ .

**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  $F : \mathcal{H} \rightarrow \mathcal{H}$  is any such linear map, let  $F_{(1)} : H \rightarrow H$  be the map in the above proposition; this induces a corresponding map  $F_{(1)}^{(ij)} : H^{(i)} \rightarrow H^{(j)}$ , by putting  $F_{(1)}^{(ij)} := \epsilon_j \circ F_{(1)} \circ \epsilon_i^{-1}$ , where  $\epsilon_i$  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  $\psi$  between  $H^{(i)} \rightarrow H^{(j)}$  and  $H^{(i)} \otimes H^{(j)}$ . The following result is also known from the literature:

**Proposition 6.** Let  $F : \mathcal{H} \rightarrow \mathcal{H}$  be a linear map. Then the state  $\overline{F}_{(ij)}$  is “entangled according to  $F$ ”; i.e. if  $F_{(1)}(| x\rangle) = | y\rangle$  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  $y_j$ .

In our axiomatic proof system, we will take (a syntactic counterpart of) this result as our central axiom, the “Entanglement Axiom”.

**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  $F$ ”.

**Local properties and separation.** 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:  $S' = \overline{\{\mu_I(\psi \otimes \psi') : \bar{\psi} \in S', \psi' \in \mathcal{H}_{N \setminus I}\}}$ . An *example* is the property  $\bar{F}_{ij}$ , which is  $\{i, j\}$ -local. The family of local properties forms a *complete lattice* (with inclusion) in which the join is given by *union*  $S \cup T$ , the *atoms* correspond to *local states*, and the *greatest element* is the property

$$\top_I^\Sigma := \{s \in \Sigma : s \text{ is } I\text{-separated}\} = \bigcup \{S \subseteq \Sigma : S \text{ is } I\text{-local}\}$$

that defines *separation*: a state  $s$  is  $I$ -separated iff  $s \in \top_I^\Sigma$ . The family of local properties is closed under union, intersection but *not under complementation*.

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

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

A map  $F : \Sigma \rightarrow \Sigma$  is  $I$ -local if it is the map induced on  $\Sigma$  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  $\Sigma$  induced by) unitary transformations  $U_I : \mathcal{H} \rightarrow \mathcal{H}$  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  $U : \mathcal{H}_I \rightarrow \mathcal{H}_I$ . The family of local maps is closed under composition.

**Local actions.** A *local action* is a quantum action  $R \subseteq \Sigma \times \Sigma$  that that can be written as an arbitrary<sup>8</sup> union of local maps. The family of local actions forms a *complete lattice* (with inclusion), in which the join is given by *union*  $R \cup R'$ , and the *greatest element* is the action

$$\top_I^{\Sigma \times \Sigma} := \bigcup \{F : \Sigma \rightarrow \Sigma : F \text{ is an } I\text{-local map}\}$$

**Lemma 2.** (“*Teleportation Property*”) If  $s$  is an  $i$ -separated state having its  $i$ -th qubit  $s_i$  in the state  $x \in H$ , then after doing two successive bipartite measurements  $\bar{G}_{jk}$ ? followed by  $\bar{F}_{ij}$ ?, the  $k$ -th qubit ( $k$ -th component of) the output-state is:

$$(\bar{F}_{ij}? \circ \bar{G}_{jk}?)(s)_k = G_{(1)} \circ F_{(1)}(x)$$

---

<sup>8</sup>i.e. possibly infinite

**Lemma 3.** (“*Entanglement Composition Lemma*”) The main lemma in [15] states (in our notation) that, given a quadruple of *distinct* indices  $i, j, k, l$ , let  $F, G, H, U, V : H \rightarrow H$  be single-qubit linear maps (i.e. 1-local transformations), then we have:

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

[15] and [1] use these last two lemmas 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 formally proving (syntactic correspondents of) these lemmas in our axiomatic proof system, and then using them to analyze teleportation.

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 7.** (*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 8.** (“*Agreement Property*”) Let  $F_I, G_I : \Sigma \rightarrow \Sigma$  be two  $I$ -local maps on states, having the same domain<sup>9</sup>:  $\text{dom}(F) = \text{dom}(G)$ . Then their output-states agree on all non- $I$  qubits, i.e. for all  $s \in \Sigma$ :

$$F(s)_{N \setminus I} = G(s)_{N \setminus I}$$

whenever both sides of the identity *exist* (i.e. whenever both  $F(s)$  and  $G(s)$  are  *$I$ -separated*.)

### 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

<sup>9</sup>The domain of a map is defined by  $\text{dom}(F) = \{s \in \Sigma : F(s) \text{ is defined}\}$ . If  $F'$  is the corresponding linear map on  $\mathcal{H}$ , this means that  $\text{dom}(F) = \{\overline{\psi} : F'(\psi) \neq 0\}$ .

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

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

**Proposition 9.** 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:  $\overline{|0\rangle}, \overline{|1\rangle}, \overline{|+\rangle}$ .

**Corollary 3.** 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:

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

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  $\mathcal{U} = \{X, Z, H, CNOT, \dots\}$  where  $X, Z$  and  $H$  are defined by the following table:

	$ 0\rangle$	$ 1\rangle$	$ +\rangle$
$X$	$ 1\rangle$	$ 0\rangle$	$ +\rangle$
$Z$	$ 0\rangle$	$ 1\rangle$	$ -\rangle$
$H$	$ +\rangle$	$ -\rangle$	$ 0\rangle$

The transformation  $CNOT$  is given by the table:

	$ 00\rangle$	$ 01\rangle$	$ 0+\rangle$	$ 11\rangle$	$ 10\rangle$	$ 1+\rangle$	$ +0\rangle$	$ +1\rangle$	$ ++\rangle$
$CNOT$	$ 00\rangle$	$ 01\rangle$	$ 0+\rangle$	$ 10\rangle$	$ 11\rangle$	$ 1+\rangle$	$ \beta_{00}\rangle$	$ \beta_{01}\rangle$	$ \gamma\rangle$

### 3 The Logic $LQP$

#### Syntax of $LQP$

To build up the language of  $LQP$ , we are given a natural number  $n$ , and we put  $N = \{1, 2, \dots, n\}$ . We start from a set  $\mathcal{Q}$  of *propositional variables*, a set  $\mathcal{C}$  of *propositional constants*; and a set  $\mathcal{U}$  of program constants, denoting *basic programs*, to be interpreted as *quantum gates* (i.e. *unitary transformations*); each program constant  $U \in \mathcal{U}$  comes together with an index  $I$ , which is a sequence of distinct indices in  $N$ ; the index gives us the set of qubits on which the quantum gate  $U$  is active; when we want to make explicit the index, we write e.g.  $U_I$  for an  $I$ -local quantum gates. In particular, for every  $i, j \leq n$ , we are given some special program constants  $CNOT_{ij}, X_i, H_i, Z_i, \dots \in \mathcal{U}$ . Similarly, we are given two special propositional constants  $1, + \in \mathcal{C}$ , the first denoting the separated state  $|1\rangle^{\otimes n} = |1\rangle \otimes |1\rangle \cdots \otimes |1\rangle$  and the second denoting the state  $|+\rangle^{\otimes n} = |+\rangle \otimes |+\rangle \cdots \otimes |+\rangle$ . 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:

$$\begin{array}{l} \varphi ::= \top_I \mid p \mid c \mid \neg\varphi \mid \varphi \wedge \varphi \mid [\pi]\varphi \\ \pi ::= \top_I \mid \varphi? \mid U \mid \pi^\dagger \mid \pi \cup \pi \mid \pi; \pi \end{array}$$

Here, we take  $I$  to denote sequences of distinct indices in  $N = \{1, 2, \dots, n\}$ . The sentence  $\top_I$  expresses *I-separation*: it is true iff the qubits in  $I$  form a separated subsystem. So  $\top_I$  denotes the greatest element  $\top_I^\Sigma$  of the lattice of  $I$ -local properties. In particular, the sentence  $\top := \top_N$  denotes the “always true” proposition (*verum*), i.e. the “top” of the lattice of all properties.<sup>10</sup> The constructs  $\neg\varphi$  and  $\varphi \wedge \varphi$  denote classical negation and conjunction, while the construct given by dynamic modalities  $[\pi]\varphi$  denotes *the weakest precondition that ensures that property  $\varphi$  will hold after running program  $\pi$* .

On the program side:  $\top_I$  denotes the *trivial I-local action*  $\top_I^{\Sigma \times \Sigma}$ , which acts on any given  $I$ -separated state by keeping unchanged the  $N \setminus I$  subsystem, while changing the  $I$  subsystem to any randomly picked  $I$  system. In other words,  $\top_I$  is the union of all  $I$ -local actions. The meaning of quantum test  $\varphi?$ , adjoint  $\pi^\dagger$ , union  $\pi \cup \pi$  and composition  $\pi; \pi$  is given by the corresponding operations on quantum actions.

Notice that we did not include *iteration* (Kleene star) among our program constructs: this is only because we do not need it for any of the applications in

<sup>10</sup>Notice also the distinction between the constant  $1_i$  (characterizing the qubit  $|1\rangle_I$ ) and the constant  $\top_i$  (denoting the property of being  $i$ -separated).

this paper. Indeed, most quantum programming does not involve *while*-loops; but (as pointed in our Section 6) one can of course add iteration to our logic, if needed.

**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*  $\top := \top_N$ , and *falsum*  $\perp := \neg\top$ . 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  $\sim\varphi := [\varphi?]\perp$ . By means of the orthocomplement we define 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  $\varphi$  or  $\psi$ .

We also introduce some notions and notations for programs: we call a program  $\pi$  *deterministic* if  $\pi$  is constructed without the use of non-deterministic choice  $\cup$  or of the non-deterministic program  $\top_I$ . Also, we put

$$flip_{ij} := CNOT_{ij}; CNOT_{ji}; CNOT_{ij}$$

for the program which (given any  $\{i, j\}$ -separated input state) permutes the  $i^{th}$  and the  $j^{th}$  components. Finally, we put

$$id := \top?$$

for the *identity* map.

**Order, Equivalence, Orthogonality, I-equivalence, testability, locality, separation.** We can internalize the relations of *logical equivalence*, *being weaker than*, and *I-equivalence* between formulas, the properties of *locality* and *testability*, and the notion of *I-component* by defining the following formulas:

$$\begin{aligned} \varphi \leq \psi &:= \Box\Box(\varphi \rightarrow \psi) \\ \varphi = \psi &:= \Box\Box(\varphi \leftrightarrow \psi) \\ \varphi \perp \psi &:= \varphi \leq \sim\psi \\ T(\varphi) &:= \sim\sim\varphi \leq \varphi \\ \varphi_I &:= \top_I \wedge \langle\top_{N \setminus I}\rangle\varphi \\ \varphi =_I \psi &:= \varphi \leq \top_I \wedge \psi \leq \top_I \wedge \varphi_I = \psi_I \\ I(\varphi) &:= \varphi = \varphi_I \end{aligned}$$

Recall from Section 2.1 that the double-box modality coincides with the universal modality: so indeed  $\varphi \leq \psi$  means that  $\varphi$  is *logically weaker* than  $\psi$ , while  $\varphi = \psi$

means the formulas are *equivalent*. We read  $T(\varphi)$  as saying that “ $\varphi$  is testable”, and  $I(\varphi)$  as “ $\varphi$  is  $I$ -local”. We read  $\varphi_I$  as “the  $I$ -component of  $\varphi$ ”: a state satisfies this sentence iff (it is  $I$ -separated and) its  $I$ -subsystem is (a subsystem of some state) satisfying  $\varphi$ . For  $I = \{i\}$ , we write  $\varphi_i := \varphi_I$ . We read  $\varphi =_I \psi$  as “ $\varphi$  is  $I$ -equivalent to  $\psi$ ”: the meaning is that *both  $\varphi$  and  $\psi$  are  $I$ -separated and have the same  $I$ -component*. Finally, we say that  $\varphi$  is  *$I$ -separated* iff  $\varphi \leq \top_I$ .

Notice that it obviously follows from these definitions that *every  $I$ -component  $\varphi_I$  is  $I$ -local*.

**Special Local States.** We can introduce some more propositional constants (which will denote special local stateS), by putting:  $0_i := \sim 1_i$  and  $-_i := \sim +_i$ .

**Image and Strongest Post-condition.** We define the *strongest testable post-condition*  $\pi[\varphi]$  *ensured by (applying a program)  $\pi$  on (any state satisfying a given precondition)  $\varphi$* , by putting

$$\pi[\varphi] := \sim [\pi^\dagger] \sim \varphi$$

In the case that  $\varphi$  is assumed to be *testable* and  $\pi$  is *deterministic*, the strongest postcondition  $\pi[\varphi]$  coincides with the *image*  $\pi(\varphi)$  of  $\varphi$  via  $\pi$ . The definition of *image of a testable property via a program*  $\pi(\varphi)$  can be extended to *all programs which are finite unions of deterministic programs*, by putting, for all *testable* formulas  $\phi$ :  $\pi(\phi) = \pi[\phi]$  if  $\pi$  is deterministic, and  $(\pi \cup \pi')(\phi) = \pi(\phi) \vee \pi'(\phi)$  in rest.

Notice the *contrast with classical PDL*: unlike the classical version, our quantum *PDL* (as considered above, i.e. *without program converse*<sup>11</sup>) has enough expressive power to *define strongest post-conditions (and, in a restrict contexts, images) using weakest preconditions!* The reason is that, in some context, the notion of adjoint can replace the notion of converse. But notice that converse itself is *not* expressible in our logic. This is for the best: the converse of a quantum action has no physical meaning (except in the case of reversible, unitary evolutions), while the adjoint is physically meaningful.

**Notation:** For any sequence  $I \subseteq N$  of indices and any vector  $\vec{c} = (c(i))_{i \in I} \in \{0, 1, +\}^{|I|}$ , we set

$$\vec{c}_I := \bigwedge_{i \in I} c(i)_i$$

<sup>11</sup>There also exists a version of *PDL with a program converse operator*  $\pi^\smile$ , such that the accessibility relation for the converse  $\pi^\smile$  is defined as the converse of the accessibility relation for  $\pi$ . That stronger logic can obviously express strongest post-condition of a program  $\pi$ , using the existential dynamic modalities, since  $\pi(\varphi) = \langle \pi^\smile \rangle \varphi$ .

**The unary maps 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  $0_I! := 0_{i_1}!; 0_{i_2}!; \dots; 0_{i_k}!$ , where  $I = (i_1, i_2, \dots, i_k)$ . This maps any qubit in  $I$  to 0. Similarly, we put;  $0_I? := (0_{i_1} \wedge 0_{i_2} \wedge \dots \wedge 0_{i_k})?$ . 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. We also want to consider the  $H_i \rightarrow H_j$ -version of the transformation  $\pi_{(1)}$ , so we put:

$$\pi_{ij} := flip_{1i}; \pi_{(1)}; flip_{1j}$$

**Local programs.** We would like to isolate *local programs*, i.e. the ones that “affect only the qubits in a given set  $I \subseteq N$ ”. For this, we define a formula  $I(\pi)$  meaning “program  $\pi$  is  $I$ -local”:

$$I(\pi) := \bigwedge_{\vec{c}, \vec{d}, \vec{d}'} \left( \vec{d}_{N \setminus I} =_{N \setminus I} \pi(\vec{c}_I \wedge \vec{d}_{N \setminus I}) =_I \pi(\vec{c}_I \wedge \vec{d}'_{N \setminus I}) \right)$$

where the conjunction is taken over all  $\vec{c} \in \{0, 1, +\}^{|I|}$  and all  $\vec{d}, \vec{d}' \in \{0, 1, +\}^{n-|I|}$ .

Note that this definition is a simple formal translation of the semantic clauses that express the fact that program  $\pi$  “acts only locally” (affecting only the  $I$ -subsystem, and in a way that depends only on the  $I$ -subsystem of the input state) *on the states of the form  $\vec{c}$*  (with  $c \in \{0, 1, +\}$ ). As we will see, one of our axioms below (“Determinacy of deterministic programs”) ensures that this clause is enough to ensure that program  $\pi$  acts locally *on all ( $I$ -separated) states*.

**Entanglement according to  $\pi$ .** To describe states that are “entangled according to  $\pi$ ”, we introduce the following formula:

$$\bar{\pi}_{ij} := \top_{ij} \wedge \bigwedge_{c \in \{0, 1, +\}} ([c_i?](\pi_{ij}(c_i))_j \wedge (\sim c_i \rightarrow \pi_{ij}(c_i) = \perp))$$

Then, as a consequence, we will have the following obvious validity:

$$c_i?(\bar{\pi}_{ij}) =_j \pi_{ij}(c_i)$$

for every  $c_i \in \{0_i, 1_i, +_i\}$ .

Again, note that the identity in this definition is a formal translation of the semantic clause defining “entanglement according to an action”, *but only for the*

particular case of local states of the form  $c_i$  (with  $c \in \{1, 0, +\}$ ). And again, one of our axioms below (the ‘‘Entanglement Axiom’’) ensures that the above identity holds (not only for the elements  $c_i$ , but) for all  $i$ -local states (i.e. all testable  $i$ -local properties).

### Semantics of LQP

An LQP-model is a multi-partite quantum frame  $\Sigma = \Sigma(\mathcal{H})$  based on an  $n$ -dimensional Hilbert space  $\mathcal{H}$ , together with a valuation function, mapping each propositional variable  $p$  into a set of states  $\| p \| \subseteq \Sigma$ . We will use the valuation map to give an interpretation  $\| \varphi \| \subseteq \Sigma$  to all our formulas, in terms of quantum properties of our multi-partite frame, i.e. sets of states in  $\Sigma$ . In the same time, we give an interpretation  $\| \pi \| \subseteq \Sigma \times \Sigma$  to all our programs, in terms of quantum actions. The two interpretations are defined by mutual recursion.

#### Interpretation of Programs.

$$\begin{aligned} \| \top_I \| &:= \top_I^{\Sigma \times \Sigma} & , & \quad \| \varphi? \| &:= \| \varphi \|? \\ \| U \| &:= U & , & \quad \| \pi^\dagger \| &:= \| \pi \|^\dagger \\ \| \pi_1 \cup \pi_2 \| &:= \| \pi_1 \| \cup \| \pi_2 \| & , & \quad \| \pi_1; \pi_2 \| &:= \| \pi_2 \|; \| \pi_1 \| \end{aligned}$$

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

**Interpretation of Formulas.** We extend the valuation  $\| p \|$  from propositional variables to all formulas, by putting for the others:

$$\begin{aligned} \| 1 \| &= |1\rangle^{\otimes n} & , & \quad \| + \| &= |+\rangle^{\otimes n} \\ \| \varphi \wedge \psi \| &= \| \varphi \| \cap \| \psi \| & , & \quad \| \neg \varphi \| &= \Sigma \setminus \| \varphi \| \\ \| [\pi] \varphi \| &= \| \pi \| \| \varphi \| & , & \quad \| \top_I \| &= \top_I^\Sigma \end{aligned}$$

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

**Lemma 4.**  $\| \sim \varphi \| = \| \varphi^\perp \|$ ,  $\| [\varphi?] \psi \| = \| \varphi \|? \| \psi \|$ ,  $\| \square \varphi \| = \square \| \varphi \|$ ,  $\| \varphi \| = \| \sim \sim \varphi \|$

**Proposition 11.** *The following are equivalent, for every formula  $\varphi$ :*

1.  $\| \varphi \|$  is testable (i.e.  $T(\varphi)$  is valid)
2.  $\varphi$  is semantically equivalent to  $\sim \sim \varphi$
3.  $\varphi$  is semantically equivalent to some formula  $\square \psi$
4.  $\varphi$  is equivalent to some formula  $\sim \psi$

## 4 Proof Theory for $LQP$

### 4.1 Axioms for single systems

First, we admit *all the axioms and rules* of **classical PDL**, except for the ones concerning tests  $\varphi?$  and Kleene star<sup>12</sup>  $\pi^*$ . In particular, we have the

**Substitution Rule.** From  $\vdash \Theta$  infer  $\vdash \Theta[p/\varphi]$

and the “normality” conditions for the dynamic modalities  $[\pi]$ :

**Kripke Axiom.**  $\vdash [\pi](p \rightarrow q) \rightarrow ([\pi]p \rightarrow [\pi]q)$

**Necessitation Rule.** From  $\vdash p$  infer  $\vdash [\pi]p$

Considering  $\Box p$ , we introduce the following axioms:

**Test Generalization Rule.** If  $p$  does not occur in  $\varphi$  or  $\psi$ , then:

from  $\vdash \varphi \rightarrow [q?]\psi$  infer  $\vdash \varphi \rightarrow \Box\psi$

**Testability Axiom.**  $\vdash \Box p \rightarrow [q?]p$

Testability can be stated in its dual form by means of  $\langle q? \rangle p \rightarrow \Diamond p$  or equivalently as  $\langle q? \rangle p \rightarrow \langle p? \rangle \top$ . 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:

<b>Partial Functionality.</b>	$\vdash \neg[p?]q \rightarrow [p?]\neg q$
<b>Adequacy.</b>	$\vdash p \wedge q \rightarrow \langle p? \rangle q$
<b>Repeatability.</b>	$\vdash T(p) \rightarrow [p?]p$
<b>Proper Superpositions.</b>	$\vdash \langle \pi \rangle \Box \Box p \rightarrow [\pi']p$
<b>Unitary Functionality.</b>	$\vdash \neg[U]q \leftrightarrow [U]\neg q$
<b>Unitary Bijectivity 1.</b>	$\vdash p \leftrightarrow [U; U^\dagger]p$
<b>Unitary Bijectivity 2.</b>	$\vdash p \leftrightarrow [U^\dagger; U]p$
<b>Adjointness.</b>	$\vdash p \rightarrow [\pi]\Box\langle \pi^\dagger \rangle \Diamond p$

**Proposition 12.** *Testability is closed under conjunctions, weakest preconditions;  $\Box$ -sentences, orthocomplements and strongest postconditions are testable:*

$$\bullet \vdash T(p) \wedge T(q) \rightarrow T(p \wedge q)$$

<sup>12</sup>We skip the axioms for iteration  $\pi^*$  only because we chose not to include this construct in our logic. But if one adds  $\pi^*$  to our syntax, the usual  $PDL$  axioms for iteration are still sound, so they can be added to the proof system.

- $\vdash T(p) \rightarrow T([\pi]p)$
- $\vdash T(\Box p)$
- $\vdash T(\sim p)$
- $\vdash T(\pi[p])$

A formula  $\varphi$  is called *testable* if the theorem

$$\vdash T(\varphi)$$

is provable in our system. Observe that this notion is proof-theoretic. However, the above Proposition gives us a purely syntactical way to check testability:

**Corollary:** Any formula of the form  $\Box\varphi$ ,  $\sim\varphi$  or  $\top$ , or which can be obtained from these formulas using only conjunctions  $\phi \wedge \psi$  and weakest preconditions  $[\pi]\varphi$ , is testable.

**Proposition 13.** (*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”<sup>13</sup>  $\varphi \wedge [\varphi?]\psi \leq \psi$ . In its turn, this rule is equivalent to the condition known in quantum logic as Weak Modularity, stated as follows:  $\varphi \wedge (\sim\varphi \sqcup (\varphi \wedge \psi)) \leq \psi$ .

**Theorem 3.** (*Soundness and Completeness*) All the other axioms above are sound. Moreover, if we eliminate from the syntax of our logic all the special constants (both propositional constants  $\top_I$ ,  $1$  and  $+$ , and program constants  $\top_I$ , *CNOT*, *X*, *H*, *Z* etc.), then there exists a complete proof system, which includes the above axioms.<sup>14</sup>

The *proof* of this theorem is given in our paper [6], and it is based on an extension of (Mayet’s version [28] of) Solèr’s Theorem [36], itself an extension of Piron’s Representation Theorem for Piron lattices [31, 32, 2].

---

<sup>13</sup>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  $\varphi \xrightarrow{S} \psi$ .

<sup>14</sup>In addition, the system includes two more axioms of a rather technical nature, namely Piron’s “Covering Law” (due to C. Piron in [32]) and “Mayet’s Condition” (due to Mayet in [28]). See [6] for details.

**Proposition 14.** The formula  $\pi[\varphi]$  expresses the *strongest testable postcondition* ensured by executing program  $\pi$  on any state satisfying (precondition)  $\varphi$ . In other words: for every *testable*  $\psi$ , we have

$$\pi[\varphi] \leq \psi \text{ iff } \varphi \leq [\pi]\psi$$

**Proposition 15.** (*Adjointness Theorem*) For all *testable* formulas  $\varphi, \psi$ , we have:

$$\varphi \perp \pi[\psi] \text{ iff } \pi^\dagger[\varphi] \perp \psi$$

## 4.2 Axioms for compound systems

**Axioms for the trivial  $I$ -local program.** *The program  $\top_I$  is the weakest  $I$ -local program; i.e.:*

$$\vdash I(\pi) \rightarrow \langle \pi \rangle p \leq \langle \top_I \rangle p$$

and

$$\vdash I(\top_I).$$

As an immediate consequence, we obtain that

$$\sim \top_I = \perp$$

(since it is easy to see that the identity program  $id$  is  $I$ -local for every, so applying the first axiom above to the program  $\pi = id$ , we obtain that  $\top = \langle id \rangle \top \leq \langle \top_I \rangle \top$ , i.e.  $\top = \langle \top_I \rangle \top$ , and so  $\sim \top_I = [\top_I?]\perp = \neg \langle \top_I \rangle \top = \neg \top = \perp$ ).

Another immediate consequence is that *the formula  $\top_I$  is the weakest  $I$ -local property*, i.e. we have:

$$\vdash I(\top_I)$$

and

$$\vdash I(p) \rightarrow p \leq \top_I.$$

Syntactically, we define an “ $I$ -local state” to be any sentence  $\varphi$  such that

$$\vdash I(\varphi) \wedge \varphi \neq \perp \wedge (I(p) \wedge \perp \neq p \leq \varphi \rightarrow p = \varphi)$$

for some  $p$  not occurring in  $\varphi$ . In other words, these are propositions that can be proved to be atoms of the lattice of (consistent)  $I$ -local properties.

**Local States Axiom.** *Testable local properties are “local states” (in the above sense, i.e. atomic local properties): if  $I \neq N$  then*

$$\vdash T(p) \wedge I(p) \wedge I(q) \wedge \perp \neq q \leq p \rightarrow q = p$$

**Basic-State Testability Axiom.** *Our basic local states  $c_i, \overline{\pi_{ij}}$  are testable: If  $i, j \in N, c \in \{0, 1, +, -\}$  and  $\pi$  is a deterministic program, then we have*

$$\vdash T(c_i) \wedge T(\overline{\pi_{ij}})$$

As an immediate consequence of the last two axioms, we have that all constants of the form  $\vec{c}_I$  (with  $\vec{c} \in \{0, 1, +, -\}^{|I|}$ ) are (testable)  $I$ -local states; similarly, if  $\pi$  is deterministic then  $\overline{\pi_{ij}}$  is a (testable)  $\{i, j\}$ -local state.

The following inference rule says that the lattice of local properties is *atomic*:

**Local Atomicity Rule.** *Local properties are unions of testable local properties (i.e. of local states): if  $I \neq N$  and the variable  $p$  does not occur in  $\varphi, \psi$  or  $\theta$ , then*

from  $\vdash \psi \wedge T(p_I) \wedge p_I \leq \varphi \rightarrow p_I \leq \theta$   
infer  $\vdash \psi \wedge I(\varphi) \rightarrow \varphi \leq \theta$

As a consequence of the above axioms and rules, we obtain the following

**Corollary.** *For  $I \neq N$ , every local state is testable. In other words: if  $I \neq N$  and  $p$  does not occur in  $\varphi$ , then from*

$$\vdash I(\varphi) \wedge \varphi \neq \perp \wedge (I(p) \wedge \perp \neq p \leq \varphi \rightarrow p = \varphi)$$

we can infer  $\vdash T(\varphi)$ .

**Separation Axiom.** *If a state is both  $I$ -separated and  $J$ -separated, then it is also  $N \setminus I$ -separated,  $I \cup J$ -separated and  $I \cap J$ -separated:*

$$\vdash \top_I \wedge \top_J \rightarrow \top_{N \setminus I} \wedge \top_{I \cup J} \wedge \top_{I \cap J}$$

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  $\vdash -_i \rightarrow \diamond 0_i \wedge \diamond 1_i$ .

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

**Determinacy Axiom of Deterministic Programs.** For deterministic programs  $\pi, \pi'$ :

$$\vdash \bigwedge_{\vec{c} \in \{0,1,+ \}^n} (\pi(\vec{c}_N) = \pi'(\vec{c}_N) \rightarrow \pi(p) = \pi'(p))$$

The next axiom is the central one of our system, capturing the computational essence of entanglement, as a semantic counterpart of Proposition 6 of Section 2:

**Entanglement Axiom.** If  $\pi$  is deterministic and  $i \neq j$ , then:

$$\vdash T(p_i) \rightarrow p_i?(\bar{\pi}_{ij}) =_j \pi_{ij}(p_i)$$

Before presenting out next axioms, we note some consequence of the previous ones. First, as for testability, we can define a proof-theoretic notion of locality. A formula  $\varphi$  is *I-local* if  $\vdash I(\varphi)$  is a theorem; similarly, a program  $\pi$  is *I-local* if  $\vdash I(\pi)$  is a theorem.

**Proposition 16.** Any formula of the form  $\varphi_I$  is always *I-local*. Any formula of the form  $\bar{\pi}_{ij}$  is  $\{i, j\}$ -local. If  $\varphi$  and  $\psi$  are *I-local* formulas and  $\pi$  is an *I-local* program, then  $\varphi \vee \psi$ ,  $\varphi \wedge \neg\psi$  and  $\varphi \wedge [\pi]\psi$  are *I-local*. If  $\varphi$  is *I-local* and  $\psi$  is *J-local*, then  $\varphi \wedge \psi$  is  $I \cup J$ -local.

**Proposition 17.** If  $\varphi$  is a *testable I-local* formula, then  $\varphi?$  is an *I-local* program.  $\top_I$  is *I-local*. If  $\pi$  and  $\pi'$  are *I-local*, then  $\pi \cup \pi'$  and  $\pi; \pi'$  are *I-local*.

**Proposition 18.** *Local programs act locally.* In other words:

$$\vdash I(\pi) \wedge p =_I q \rightarrow p =_{N \setminus I} \pi(p) =_I \pi(q)$$

**Proposition 19.** *Systems composed of identical parts are identical:*

$$\vdash p =_I q \wedge p =_J q \rightarrow p =_{I \cup J} q$$

**Proposition 20.**  $\vdash p_I \perp q \leftrightarrow p_I \perp q_I$

**Proposition 21.** (*Dual Local Atomicity Rule*). If  $I \neq N$ ,  $\varphi$  and  $\theta$  are *I-separated*, and  $p$  does not occur in  $\varphi, \psi$  or  $\theta$ , then: from

$$\vdash \psi \wedge T(p_I) \wedge p_I \perp \varphi \rightarrow p_I \perp \theta$$

infer

$$\vdash \psi \wedge T(\varphi_I) \wedge T(\theta_I) \rightarrow \varphi =_I \theta$$

*Proof:* By using the fact that  $p_I \perp q \leftrightarrow p_I \perp q_I$  and the  $I$ -locality of  $p_I$ , we can rewrite the assumption as

$$\vdash \psi \wedge T(p_I) \wedge p_i \leq (\top_I \wedge \sim \varphi_I) \rightarrow p_I \leq (\top_I \wedge \sim \theta_I)$$

Assume now  $\psi \wedge T(\varphi_I) \wedge T(\theta_I)$ . Then the formula  $\top_I \wedge \sim \varphi_I = \top_I \wedge \neg(\top_I \wedge [\varphi_I?] \perp)$  is  $I$ -local (since  $\varphi_I$  is testable  $I$ -local, so  $\varphi_I?$  is an  $I$ -local program, so  $\top_I \wedge [\varphi_I?] \perp$  is  $I$ -local) and similarly  $\top_I \wedge \sim \theta_I$  is  $I$ -local. So we can apply the Local Atomicity Rule, obtaining that:  $(\top_I \wedge \sim \varphi_I) \leq (\top_I \wedge \sim \theta_I)$ . Applying orthocomplementation, we have that:  $\sim(\top_I \wedge \sim \theta_I) \leq \sim(\top_I \wedge \sim \varphi_I)$ . From this we get that:  $\theta_I = \sim \sim \theta_I = \perp \sqcup \sim \sim \theta_I = \sim \top_I \sqcup \sim \sim \theta_I = \sim(\top_I \wedge \sim \theta_I) \leq \sim(\top_I \wedge \sim \varphi_I) = \sim \top_I \sqcup \sim \sim \varphi_I = \perp \sqcup \varphi_I = \varphi_I$ . But by the Local States Axiom, this implies that  $\theta_I = \varphi_I$  (since both are testable  $I$ -local with  $I \neq N$ , thus they are local states). Since both  $\theta_I$  and  $\varphi_I$  are  $I$ -separated, it follows that  $\theta =_I \varphi$ .

**Theorem 4.** (*Compatibility of Programs Affecting Different Qubits*). If  $I \cap J = \emptyset$  and  $\pi, \pi'$  are deterministic, then

$$\vdash I(\pi) \wedge J(\pi') \rightarrow \pi; \pi'(p) = \pi'; \pi(p)$$

*Proof:* This is an immediate application of the Determinacy Axiom above. By that axiom, it is enough to show the required identity for all  $p$  of the form  $p = \vec{c}_N$ , with  $\vec{c} \in \{0, 1, +\}^n$ . Using the fact that  $I \cup (N \setminus (I \cup J)) \subseteq N \setminus J$  and  $J \cup (N \setminus (I \cup J)) \subseteq N \setminus I$  (since  $I \cap J = \emptyset$ ) and the Proposition saying that local programs “act locally”, we can easily show that  $(\pi; \pi')(\vec{c}_N) =_{N \setminus (I \cup J)} c_N =_{N \setminus (I \cup J)} (\pi'; \pi)(\vec{c}_N)$ ,  $(\pi; \pi')(\vec{c}_N) =_I \pi(\vec{c}_N) =_I (\pi'; \pi)(\vec{c}_N)$  and  $(\pi; \pi')(\vec{c}_N) =_J \pi'(\vec{c}_N) =_J (\pi'; \pi)(\vec{c}_N)$ . Using a previous Proposition, we put these together to conclude that  $(\pi; \pi')(\vec{c}_N) =_{I \cup J \cup (N \setminus (I \cup J))} (\pi'; \pi)(\vec{c}_N)$ , i.e. that  $(\pi; \pi;)(\vec{c}_N) = (\pi'; \pi)(\vec{c}_N)$ .

**Proposition 22.** (*Dual Entanglement*). If  $\pi$  is deterministic and  $i \neq j$ , then

$$\vdash T(q_j) \rightarrow q_j?(\overline{\pi_{ij}}) =_i \pi_{ij}^\dagger(q_j)$$

*Proof:* Assume  $T(q_j)$  and we need to show that  $q_j?(\overline{\pi_{ij}}) =_i \pi_{ij}^\dagger(q_j)$ . It is easy to see that both sides are  $i$ -separated (i.e.  $\leq \top_i$ ), and also that both  $(q_j?(\overline{\pi_{ij}}))_i$  and  $(\pi_{ij}^\dagger(q_j))_i$  are testable (since they are local states), so we are in the conditions of the Dual Local Atomicity Rule (Proposition 21) above. By that Proposition, to prove the above identity, it is enough to show that:

$$\vdash T(p_i) \wedge p_i \perp \pi_{ij}^\dagger(q_j) \rightarrow p_i \perp q_j?(\overline{\pi_{ij}}).$$

To show this, let  $p_i$  be such that  $T(p_i)$  and  $p_i \perp \pi_{ij}^\dagger(q_j)$ . By the Adjointness Theorem, we have then  $\pi_{ij}(p_i) \perp q_j$ , and so  $q_j?(p_i) = \perp$ . By the previous Proposition (on Compatibility of Programs on Different Qubits), we have:  $p_i?(q_j?(\overline{\pi_{ij}})) = (p_i?; q_j?)(\overline{\pi_{ij}}) = (q_j?; p_i?)(\overline{\pi_{ij}}) = q_j?(p_i?(\overline{\pi_{ij}})) = q_j?(\pi_{ij}(p_i)) = \perp$  (where we have used the Entanglement Axiom). So we obtain that  $p_i \perp q_j?(\overline{\pi_{ij}})$ . (So using the Dual Local Atomicity Rule, the desired conclusion follows).

**Proposition 23.** (*Entanglement Preparation Lemma*)

$$\vdash \pi_{ij}(p_i) \perp q_j \rightarrow \overline{\pi_{ij}} \perp (p_i \wedge q_j)$$

*Proof:* From the hypothesis, we obtain that  $q_j \perp (\pi_{ij}(p_i))_j$ , and so  $(p_i \wedge q_j) \perp (\pi_{ij}(p_i))_j$ , from which it follows that  $(p_i \wedge q_j) \perp [p_i?](\pi_{ij}(p_i))_j$  (using the fact that  $p_i?(p_i \wedge q_j) = p_i \wedge q_j$ , by Adequacy). On the other hand, we have  $\overline{\pi_{ij}} \leq [p_i?](\pi_{ij}(p_i))_j$  (since  $p_i?(\overline{\pi_{ij}}) \leq (p_i?(\overline{\pi_{ij}}))_j = (\pi_{ij}(p_i))_j$ , by the Entanglement Axiom), and so we obtain that  $(p_i \wedge q_j) \perp \overline{\pi_{ij}}$ .

**Theorem 5.** (*Teleportation Property*). If  $i, j, k$  are distinct indices then

$$\vdash (\overline{\sigma_{jk}^?}; \overline{\pi_{ij}^?})(p_i) =_k (\pi_{ij}; \sigma_{jk})(p_i)$$

*Proof:* By the same argument as above, it is enough to prove that:

$$\vdash T(q_k) \wedge q_k \perp (\pi_{ij}; \sigma_{jk})(p_i) \rightarrow q_k \perp (\overline{\sigma_{jk}^?}; \overline{\pi_{ij}^?})(p_i)$$

To show this, let  $q_k$  such that  $T(q_k)$  and  $q_k \perp (\pi_{ij}; \sigma_{jk})(p_i)$ . Then  $q_k \perp \sigma_{jk}(\pi_{ij}(p_i))$ , and by Adjointness Theorem we have  $\sigma_{jk}^\dagger(q_k) \perp \pi_{ij}(p_i)$ . By Dual Entanglement, it follows that  $q_k?(\overline{\sigma_{jk}}) \perp \pi_{ij}(p_i)$ . By the Entanglement Preparation Lemma, we have  $\overline{\pi_{ij}} \perp (q_k?(\overline{\sigma_{jk}}) \wedge p_i)$ . Hence we obtain:  $q_k?((\overline{\sigma_{jk}^?}; \overline{\pi_{ij}^?})(p_i)) = q_k?(\overline{\pi_{ij}^?}(\overline{\sigma_{jk}^?}(p_i))) = \overline{\pi_{ij}^?}(q_k?(\overline{\sigma_{jk}^?}(p_i))) =_{ijk} \overline{\pi_{ij}^?}(q_k?(\overline{\sigma_{jk}}) \wedge p_i) = \perp$  (where we have used Theorem 4 on the Compatibility of Programs on Different Qubits). So we obtain, as desired, that  $q_k \perp (\overline{\sigma_{jk}^?}; \overline{\pi_{ij}^?})(p_i)$ .

**Corollary.** If  $i, j, k$  are distinct then

$$\vdash \overline{\pi_{ij}^?}(p_i \wedge \overline{\sigma_{jk}}) =_k (\pi_{ij}; \sigma_{jk})(p_i)$$

*Proof:* By the Repeatability Axiom, we have  $\overline{\sigma_{jk}^?}(p_i) \leq \overline{\sigma_{jk}}$ . Assuming that  $\overline{\sigma_{jk}^?}(p_i) \neq \perp$ , we obtain that  $\overline{\sigma_{jk}^?}(p_i) =_{jk} \overline{\sigma_{jk}}$  (since  $\overline{\sigma_{jk}}$  is testable and

$\{j, k\}$ -local, and so it's a local state) and also that  $\overline{\sigma_{jk}}?(p_i) =_i p_i$  (since “local programs act locally”, by Proposition 18). Thus, we obtain that  $\overline{\sigma_{jk}}?(p_i) =_{ijk} p_i \wedge \overline{\sigma_{jk}}$ . Applying the  $\{i, j\}$  local program  $\overline{\pi_{ij}}$ , we obtain that  $\overline{\pi_{ij}}?(p_i \wedge \overline{\sigma_{jk}}) =_{ijk} \overline{\pi_{ij}}?(\overline{\sigma_{jk}}?(p_i)) = (\overline{\sigma_{jk}}?; \overline{\pi_{ij}}?)(p_i) =_k (\pi_{ij}; \sigma_{jk})(p_i)$ , from which we obtain the desired conclusion.

By a refinement of the proof of Teleportation Property, we can prove the following proof-theoretic version of Lemma 2 in Section 2.2:

**Proposition 24.** (*Entanglement Composition Lemma*). For distinct indices  $i, j, k, l$ , programs  $\pi, \pi', \pi''$  and local  $\{1\}$ -programs  $\sigma_1, \rho_1$  we have:

$$\vdash \overline{\pi_{ij}} \wedge \overline{\pi'_{kl}} \rightarrow [\sigma_j; \rho_k; \overline{\pi''_{jk}}?](\pi; \sigma_1; \pi''; \rho_1^\dagger; \pi')_{il}$$

The domain  $dom(\varphi)$  of a map  $\pi$  is defined as  $dom(\pi) := \langle \pi \rangle \top$ .

**Theorem 6.** (*Agreement Property*). If two  $I$ -local maps  $\pi, \pi'$  have the same domain and they separate the input-state, then their output states agree on all non- $I$  qubits: i.e. if  $I \cap J = \emptyset$  then for all deterministic programs  $\pi, \pi'$  we have  $\vdash T(p) \wedge I(\pi) \wedge I(\pi') \wedge dom(\pi) = dom(\pi') \wedge \pi(p) \leq \top_I \wedge \pi'(p) \leq \top_I \rightarrow \pi(p) =_{N \setminus I} \pi'(p)$ .

*Proof:* Let's put  $\psi := T(p) \wedge I(\pi) \wedge I(\pi') \wedge dom(\pi) = dom(\pi') \wedge \pi(p) \leq \top_I \wedge \pi'(p) \leq \top_I$ , and let us assume that  $\psi$  is true. By definition,  $\pi(p)$  is testable (since  $\pi$  is deterministic, so  $\pi(p) = \pi[p] = \sim [\pi^\dagger] \sim p$ , and every sentence of the form  $\sim \psi$  is testable), and the same is true for  $\pi'(p)$ . So we can use the Dual Local Atomicity Rule to prove the above identity. Let now  $q_{N \setminus I}$  be such that  $T(q_{N \setminus I})$  and  $q_{N \setminus I} \perp \pi(p)$ . Then  $(\pi; q_{N \setminus I}?) (p) = \perp$ . By the Compatibility of Programs on Different Qubits, we obtain that  $(q_{N \setminus I}; \pi)(p) = \perp$ , i.e.  $p \leq [q_{N \setminus I}][\pi] \perp = [q_{N \setminus I}] \neg z \langle \pi \rangle \top = [q_{N \setminus I}] \neg dom(\pi)$ . But  $dom(\pi) = dom(\pi')$ , so  $p \leq [q_{N \setminus I}] \neg dom(\pi') = [q_{N \setminus I}][\pi'] \perp$ , i.e.  $(q_{N \setminus I}; \pi')(p) = \perp$ . Working now in reverse, we apply again the Compatibility of Programs on Different Qubits, obtaining  $(\pi'; q_{N \setminus I}?) (p) = \perp$ , i.e.  $q_{N \setminus I} \perp \pi'(p)$ . So we have proved that:

$$\vdash \psi \wedge T(q_{N \setminus I}) \wedge q_{N \setminus I} \perp \pi(p) \rightarrow q_{N \setminus I} \perp \pi'(p).$$

By applying now the Dual Local Atomicity Rule, we obtain

$$\vdash \psi \rightarrow \pi(p) =_{N \setminus I} \pi'(p),$$

i.e. the desired conclusion.

**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
$\overline{ 00\rangle_{ij}} = \overline{ 0\rangle_i \otimes  0\rangle_j}$	$\langle 0_i? \rangle 0_j \wedge [1_i?] \perp$
<b>Bell states:</b> $\beta_{xy}^{i,j} = \overline{ 0\rangle_i \otimes  y\rangle_j + (-1)^x  1\rangle_i \otimes  \tilde{y}\rangle_j}$ 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 $x = 0$
$\gamma^{i,j} = \beta_{00}^{i,j} + \beta_{01}^{i,j} =$ $\overline{ 00\rangle_{ij} +  01\rangle_{ij} +  10\rangle_{ij} +  11\rangle_{ij}}$	$\langle 0_i? \rangle +_j \wedge \langle 1_i? \rangle +_j \wedge \langle +_i? \rangle +_j$

**Locality Axiom for Quantum Gates.** *Our special quantum gates are local, affecting only the specified qubits:*

$$\vdash \{i\}(X_i) \wedge \{i\}(Z_i) \wedge \{i\}(H_i) \wedge \{i, j\}(CNOT_{ij})$$

In addition to this, we require for  $X, Z, H$ :

**Characteristic Axioms for Quantum Gates  $X$  and  $Z$ .**

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

**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 25.** *The Bell states  $\beta_{xy}^{i,j}$  are characterized by the logic Bell formulas  $\beta_{xy}^{i,j}$ . 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  $\beta_{xy}^{i,j}$  imply the corresponding characteristic formulas in the above table. For this, we use the Entanglement Axiom and the following (easily checked) theorems:  $\vdash 0_1 \leftrightarrow \langle Z_1^x; X_1^y \rangle > y_1$ ,  $\vdash 1_1 \leftrightarrow \langle Z_1^x; X_1^y \rangle > \tilde{y}_1$ ,  $\vdash +_1 \rightarrow \langle Z_1^x; X_1^y \rangle > (-)_1^x$ .

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

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

**Proposition 26.** For all  $x, y \in \{0, 1\}$ :  $\vdash (H_i; CNOT_{i,j}(x_i \wedge y_j) = \beta_{xy}^{ij}$

**Corollary.** If  $i, j, k$  are all distinct then

$\vdash (CNOT_{i,j}; H_j; (x_i \wedge y_j)?) (p) =_k \beta_{xy}^{i,j}?(p)$ .

*Proof:* From the above Proposition and from  $H^\dagger = H$ ,  $CNOT^\dagger = CNOT$ , we get  $(CNOT_{i,j}; H_i)(\beta_{xy}^{ij}) = x_i \wedge y_j$ , and so  $dom(CNOT_{i,j}; H_i) = \langle CNOT_{i,j}; H_i; (x_i \wedge y_j) \rangle \top = \langle \beta_{xy}^{ij} \rangle \top = dom(\beta_{xy}^{ij}?)$ . The conclusion follows from this, together with the Agreement Property.

## 5 Correctness of the Teleportation Protocol

Following [29], 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  $\beta_{00}^{2,3} \in H^{(2)} \otimes H^{(3)}$ . Alice holds in addition to her part of the EPR pair also a qubit  $q_1 \in H^{(1)}$ , in an unknown local state  $q_1$ . (Note that  $q_1$  is a testable 1-local property, since it is a 1-local state.) Alice wants to “teleport” this unknown state to Bob, i.e. she will perform a program that will output a state satisfying  $id_{13}(q_1)$ . 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  $q_3$  into the state  $id_{13}(q_1)$  (corresponding to the qubit Alice had 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  $id_{13}(q_1)$ .

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

$$\vdash \pi(q_1 \wedge \beta_{00}^{2,3}) =_3 id_{13}(q_1).$$

To show this, observe that by applying the above Corollary (at the end of the last section) in which we take  $i = 1, j = 2, k = 3$ , we obtain that the validity above (to be proved) is equivalent to:  $\vdash (\beta_{xy}^{12?}; X_3^y; Z_3^x)(q_1 \wedge \beta_{00}^{2,3}) =_3 id_{13}(q_1)$ . 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:  $\vdash \overline{((Z_1^x; X_1^y)_{12?}; X_3^y; Z_3^x)}(q_1 \wedge \overline{id_{23}}) =_3 id_{13}(q_1)$ , where  $id = Z_1^0; X_1^0$  is the identity. This last validity follows from applying the (Corollary of) Teleportation Property and the validity  $Z_1^x; X_1^y; X_1^y; Z_1^x = id$  (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 [15] can be similarly treated using our logic.

## 6 Conclusions and Future Work

We presented here a dynamic logic for compound quantum systems, capable of *expressing and proving highly non-trivial features of quantum information flow, such as entanglement and teleportation, properties of local transformations, separation, Bell states* etc. The logic is Boolean, but has *modalities capturing the non-classical logical dynamics of quantum systems*; in addition, it has *spatial features*, allowing us to express properties of *subsystems* of a compound quantum system. The logic comes with a simple relational semantics, in terms of quantum states and quantum actions in a Hilbert space. We present a sound proof system, and we use it to prove interesting properties of quantum information, including a formal correctness proof for the Teleportation protocol.

However, there are a number of open problems left. Although in [6] we sketched a completeness result for the quantum dynamic logic of *single-system* quantum frames, *no corresponding completeness result is known for compound systems*. So the completeness problem for the logic *LQP* presented in this paper is still open.

Although in this paper we have only considered *iteration-free* quantum *PDL* (i.e. a logic that does not include *iteration*, or Kleene star,  $\pi^*$ , among the operations on programs), since iteration was not needed in our simple quantum programming applications. But one can of course add iteration and consider the resulting logic, which would be useful in applications to quantum programs involv-

ing *while*-loops. The usual *PDL* axioms for Kleene star are sound, but again completeness remains an open problem.

Another problem, of great importance for quantum computation, is extending our setting to deal with the *quantitative aspects of quantum information* (in particular with notions like phase and probability). Our aim in this paper was to develop a logic to reason about *qualitative* quantum information flow, so we neglected the *probabilistic* aspects of quantum systems. There are natural ways to extend our setting, using quantum versions of *probabilistic modal logic*, and we plan to investigate them in future work.

A similar, but deeper, open problem is the one of developing a logic that can deal with finer quantitative aspects of quantum, such as *(relative) phase*. This is an important concept for quantum computation, so a logic that can deal with phase aspects would be most useful.

**Acknowledgments.** We thank Bob Coecke for useful discussions, ideas and comments on this work, and especially for presenting (a preliminary version of) this paper at the 2nd International Workshop on Quantum Programming Languages (QPL2004) organised by Peter Selinger. We thank Samson Abramsky and Prakash Panangaden for the useful discussions that took place at COMLAB in 2004 on the topic of this paper. Sonja Smets thanks Amilcar Sernadas and Paulo Mateus for the useful discussions that took place at IST in November 2004 on exogenous and dynamic quantum logic.

## References

- [1] S. Abramsky and B. Coecke, “A Categorical Semantics of Quantum Protocols.”, to be published in the proceedings of the 19th IEEE conference on Logic in Computer Science (LiCS’04). Available at arXiv:quant-ph/0402130.
- [2] I. Amemiya and H. Araki, “A Remark on Piron’s paper”, *Publications of the Research Institute of Mathematical Sciences Kyoto University, series A*, **2**, 423-427 (1967)
- [3] H. Amira, B. Coecke and I. Stubbe, “How Quanta Emerge by Introducing Induction within the Operational Approach”, *Helvetica Physica Acta*, **71**, 554-572 (1998)
- [4] A. Baltag, “Dynamic and Epistemic Logics for Quantum Measurements”, Presented at PML’04, Brussels 2004.
- [5] A. Baltag and S. Smets: “The Logic of Quantum Programs ”, P. Selinger (ed.), Proceedings of the 2nd International Workshop on Quantum Programming Languages (QPL2004, affiliated with LICS’04), *TUCS General Publication No 33*, 39-56, Turku Center for Computer Science, 2004.

- [6] A. Baltag and S. Smets, “Complete Axiomatizations for Quantum Actions”, submitted to *International Journal of Theoretical Physics*, proceedings issue of IQSA2004.
- [7] A. Baltag and S. Smets, “What can Logic learn from Quantum Mechanics?”, submitted for presentation at the Workshop on “Quantum Information: Epistemological and Logic Lessons”, workshop affiliated with the European Conference for Analytic Philosophy (ECAP’05), Lisbon, Portugal, August 27-31 2005.
- [8] E.G. Beltrametti and G. Cassinelli, “On State Transformations Induced by Yes-No Experiments, in the Context of Quantum Logic”, *Journal of Philosophical Logic*, **6**, 369-379 (1977)
- [9] O. Brunet and P. Jorrand, “Dynamic Quantum Logic for Quantum Programs”, Grenoble 2003. Available at arXiv:quantph/0311143
- [10] B. Coecke, D.J. Moore and S. Smets, “Logic of Dynamics & Dynamics of Logic; Some Paradigm Examples”, in S. Rahman, J. Symons, D.M. Gabbay and J.P. Van Bendegem (eds.), *Logic, Epistemology and the Unity of Science* (2004)
- [11] B. Coecke, D.J. Moore and I. Stubbe: “Quantaloids describing Causation and Propagation for Physical Properties” (arXiv: quant-ph/0009100), *Foundations of Physics Letters* 14, 357-367 (2001).
- [12] B. Coecke and I. Stubbe, “On a Duality of Quantaes Emerging from an Operational Resolution”, *International Journal of Theoretical Physics*, **38**, 3269-3281 (1999)
- [13] B. Coecke and S. Smets, “The Sasaki Hook is not a [Static] Implicative Connective but Induces a Backward [in Time] Dynamic One that Assigns Causes”, *International Journal of Theoretical Physics*, to appear (arXiv: quant-ph/0111076)
- [14] B. Coecke, “Structural Characterization of Compoundness”, *International Journal of Theoretical Physics*, **39**, 585-594, 2000.
- [15] B. Coecke, “The Logic of Entanglement”, March 2004, arXiv: quant-ph/0402014.
- [16] M.L. Dalla Chiara and R. Giuntini, “Quantum Logics”, in D.M. Gabbay and F. Guenther, (eds.) *Handbook of Philosophical Logic*, Second Edition, vol. 6, Kluwer Ac. Pub., Dordrecht, 129-228, 2002.
- [17] M.L. Dalla Chiara, R. Giuntini and R. Greechie, *Reasoning in Quantum Theory*, Kluwer Ac. Pub., Dordrecht, 2004.
- [18] W. Daniel, “On the Non-Unitary Evolution of Quantum Systems”, *Helvetica Physica Acta*, **55**, 330-338 (1982)
- [19] W. Daniel, “Axiomatic Description of Irreversible and Reversible Evolution of a Physical System”, *Helvetica Physica Acta*, **62**, 941-968 (1989)
- [20] CL.-A. Faure, D.J. Moore and C. Piron, “Deterministic Evolutions and Schrodinger Flows”, *Helvetica Physica Acta*, **68**, 150-157 (1995)
- [21] R. Goldblatt, “Orthomodularity is not elementary”, *The Journal of Symbolic Logic*, **49**, 401-404 (1984)

- [22] R.I. Goldblatt, “Semantic Analysis of Orthologic”, *Journal of Philosophical Logic*, **3**, 19-35, 1974.
- [23] G. M. Hardegree, “Stalnaker Conditional and Quantum Logic”, *Journal of Philosophical Logic*, **4**, 399-421 (1975)
- [24] G. M. Hardegree, “The Conditional in Abstract and Concrete Quantum Logic”, in C.A. Hooker, *The Logico-Algebraic Approach to Quantum Mechanics*, vol. 2, D. Reidel Publishing Company, Dordrecht (1979)
- [25] D. Harel, D. Kozen, J. Tiuryn, *Dynamic Logic*, MIT-Press, Massachusetts (2000)
- [26] J.M. Jauch, *Foundations of Quantum Mechanics*, Addison-Wesley, Reading, Massachusetts (1968)
- [27] J.M. Jauch and C. Piron, “On the Structure of Quantal Proposition Systems”, *Helvetica Physica Acta*, **42**, 842-848 (1969)
- [28] R. Mayet “Some Characterizations of the Underlying Division Ring of a Hilbert Lattice by Automorphisms”, *International Journal of Theoretical Physics*, **37** (1), 109-114 (1998)
- [29] M. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, 2000.
- [30] P. Mateus and A. Sernadas, “Reasoning about Quantum Systems”, in J. Alferes and J. Leite (eds.) *Logics in Artificial Intelligence, Ninth European Conference, JELIA’04*, issue of *Lecture Notes in Artificial Intelligence*, **3229**, 239-251, 2004.
- [31] C. Piron, “Axiomatique quantique (PhD-Thesis)”, *Helvetica Physica Acta*, **37**, 439-468 (1964), English Translation by M. Cole: “Quantum Axiomatics” RB4 Technical memo 107/106/104, GPO Engineering Department (London).
- [32] C. Piron, *Foundations of Quantum Physics*, W.A. Benjamin Inc., Massachusetts (1976)
- [33] S. Smets, “On Causation and a Counterfactual in Quantum Logic: the Sasaki Hook”, *Logique et Analyse*, **173-175**, 307-325 (2001)
- [34] S. Smets, “On Quantum Propositional Dynamic Logic”, Presented at PML’04, Brussels 2004.
- [35] S. Smets, “From Intuitionistic Logic to Dynamic Operational Quantum Logic”, *Poznan Studies in Philosophy and the Humanities*, to appear.
- [36] M.P. Solèr, “Characterization of Hilbert spaces by orthomodular spaces”, *Communications in Algebra*, **23(1)**, 219-243 (1995)