Math. Struct. in Comp. Science (2006), *vol.* 16, *pp.* 491–525.
doi:10.1017/S0960129506005299 Printed in the United Kingdom

LQP: the dynamic logic of quantum information

ALEXANDRU BALTAG[†] and SONJA SMETS[‡]

[†]*Oxford University Computing Laboratory, UK*
[‡]*Vrije Universiteit Brussel, Flanders' Fund for Scientific Research Post-Doc, Belgium*

Received 4 April 2005; revised 5 December 2005

The main contribution of this paper is the introduction of a *dynamic logic* formalism for reasoning about information flow in *composite* quantum systems. This builds on our previous work on a *complete* quantum dynamic logic for *single* systems. Here we extend that work to a *sound* (but not necessarily complete) logic for composite systems, which brings together ideas from the quantum logic tradition with concepts from (dynamic) modal logic and from quantum computation. This *Logic of Quantum Programs* (*LQP*) is capable of expressing important features of quantum measurements and unitary evolutions of multi-partite states, as well as giving logical characterisations to various forms of entanglement (for example, the Bell states, the *GHZ* states etc.). We present a finitary syntax, a relational semantics and a sound proof system for this logic. As applications, we use our system to give formal correctness proofs for the Teleportation protocol and for a standard Quantum Secret Sharing protocol; a whole range of other quantum circuits and programs, including other well-known protocols (for example, superdense coding, entanglement swapping, logic-gate teleportation etc.), can be similarly verified using our logic.

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 *PDL*' has been one of the main objectives of our previous investigations into the logic of quantum information flow. In a series of presentations (Baltag 2004; Smets 2004) and papers (Baltag and Smets 2005a; Baltag and Smets 2004; Baltag and Smets 2005b), we have proposed several logical systems: in Baltag and Smets (2005a) we focused on *single systems*[1] and presented two equivalent

[1] A *single* system is just an isolated physical system; the possible states of such a system are represented in quantum mechanics as rays in some Hilbert space. By contrast, a *composite* (also called *compound*, or *multi-partite*) system is one that we can think of as being composed of two (or more) distinct physical (sub)systems. The corresponding Hilbert space is the *tensor product* of each of the spaces associated to the subsystems. So, in a sense, single systems *subsume* composite systems (since any tensor product of Hilbert

complete axiomatisations for a Logic of Quantum Actions, *LQA*, which allows 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 axiomatisation for *compound systems* was taken up in Baltag and Smets (2004), where a first proposal for a *logic of multi-partite quantum systems* was sketched.

In this paper we further elaborate, simplify and improve on the work outlined in Baltag and Smets (2004), and develop a full-fledged *Logic of Quantum Programs LQP*[1]. 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 (but not necessarily complete*[2]*) 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* and *quantum secret sharing protocols*.

More generally, the strength of *LQP* lies in the fact that it can provide *fully formal correctness proofs for a whole class of quantum circuits and protocols*, a class that includes logic-gate teleportation, superdense coding and entanglement swapping, as well as more complex circuits built using quantum gates and measurements.

The logic introduced here brings together a number of ideas from several fields: theoretical foundations of quantum mechanics, operational quantum logic, dynamic modal logic, spatial logic and quantum computation. In the rest of this section we give an overview of the main concepts underlying the logic *LQP*.

The first fundamental idea of our approach connects two independent lines of research. The first is the long tradition in the logical-algebraic foundations of quantum mechanics, which, in particular, has produced various ‘dynamic’ interpretations of quantum logic (*QL*) in Daniel (1982; 1989), Faure *et al.* (1995), Amira *et al.* (1998), Coecke (2000), Coecke *et al.* (2001), Coecke *et al.* (2004), Coecke and Smets (2005), Coecke and Stubbe (1999) and Smets (2001; 2005). The second line is the work on modal ‘action’ logics

spaces is just another Hilbert space). However, treating a system as being composite amounts to having a more detailed complex theory of the system (compared with treating it as a single system) – a theory that captures the specific features arising from being a *composite* structure, *in addition* to the general features of any physical system. A ‘logic’ for compound systems will thus be a *richer* logic than one for single systems.

[1] But note the difference between our logic *LQP* and the approach with a similar name in Brunet and Jorrand (2003): 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, for example, Dalla Chiara and Giuntini (2002), Dalla Chiara *et al.* (2004) and Goldblatt (1974)).

[2] Unlike the case of infinite-dimensional single systems, for which a complete logic was given in Baltag and Smets (2005a), the problem of finding a complete proof system for the logic *LQP* is still open.

in Computer Science, the main example being Dynamic Logic (*PDL*) and its relatives (Hoare logic, but also dynamic interpretations of basic modal logics as languages for 'processes' or labelled transition systems, for example, Hennessey–Milner logic).

We stress the fact that, until our recent work (Baltag and Smets 2005a), these two traditions were not only independent, but did not even share a common language. The use of the word 'dynamic' in the *QL* tradition did not have much in common with 'dynamic' logic; *QL* aimed for an algebraic axiomatisation of quantum systems based on the *non-distributive lattice of 'quantum properties'*, structure obtained by abstracting away from the lattice of *projectors in a Hilbert space H* (or, equivalently, the lattice of closed linear subspaces of *H*); the goal was to obtain representation theorems for these logical structures with respect to Hilbert spaces, thus allowing one to claim a 'rational', 'logical' (or 'operational') reconstruction of quantum mechanics[1]. In this context, the 'dynamic' twist as to do with the addition of features belonging to *physical dynamics* to the standard (static) *QL* description:

- First, a 'dynamic' interpretation was given to the main structure (the lattice of properties) and the logical connectives (quantum implication and quantum disjunction) of *QL*: in, for example, Smets (2001), Coecke and Smets (2005) and Coecke *et al.* (2004) (and partially anticipated in Hardegree (1975; 1979) and Beltrametti and Cassinelli (1977)) the quantum-logical connectives are interpreted dynamically, as expressing *potential causality* (that is, what in computer science is known as *weakest preconditions*).
- Second, some of the researchers in *QL* went on to incorporate 'true' physical dynamics, that is, Schrodinger flows (unitary evolutions), into the algebra as operators on the underlying lattice; the resulting structure is a *quantale* of 'quantum actions', which was introduced and investigated in Coecke *et al.* (2001) and Coecke and Stubbe (1999).

In contrast, the modal logician's (and the computer scientist's) use of 'dynamics' refers to modelling processes as *labelled transition systems* (Kripke models), in which the possible 'actions' are represented as *binary relations* between possible states, and the natural descriptive language is *modal*, having dynamic modalities to express *weakest preconditions* (ensuring given post-conditions after specific actions)[2]. Thus, the 'first fundamental idea' of our logic, an idea first presented in Baltag (2004) and Smets (2004) and published in Baltag and Smets (2005a), is to connect these two traditions by giving a *quantum (re)interpretation of Dynamic Logic*, in which *both (projective) measurements and unitary evolutions are treated as modal actions*, and to use this formalism in order to improve on the known representation theorems in *QL*. In this quantum interpretation, the 'test' actions φ? of *PDL* (which are used to capture conditional programs in dynamic logic) are to be read as *'successful measurements' of a quantum property* φ (that is, as projectors in a Hilbert space over the subspace generated by the set of states satisfying φ), while the other basic actions of *PDL* are taken to be *quantum gates* (that is, unitary operators on a Hilbert space). As shown in Baltag (2004), Smets (2004) and Baltag and Smets (2005a), this immediately

[1] This goal was partially realised in Piron (1964) and Piron (1976), and later improved on in Solèr (1995) and Mayet (1999), and related work.

[2] See, for example, Harel *et al.* (2000) for an introduction to dynamic modalities $[\pi]\psi$ describing weakest preconditions ensuring (the satisfaction of some post-condition) ψ after the execution of action π.

https://doi.org/10.1017/S0960129506005299 Published online by Cambridge University Press

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' $\sim \varphi$, which expresses the necessary failure of a measurement) and the 'quantum implication' (the so-called 'Sasaki hook' $\phi \stackrel{S}{\rightarrow} \psi$, which captures causality in quantum measurements) are all expressible using quantum-dynamic modalities $[\varphi?]\psi$ (which capture *weakest preconditions of quantum measurements*)[1]. In other words, in our logic (unlike other logical 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 was originally outlined in Baltag and Smets (2004), and consists of adding *spatial features* to dynamic quantum logic in order to capture relevant properties of *multi-partite (that is, compound) quantum systems* (for example, separation, locality and 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, +, and so on, to express the fact that qubits are in the state $|1\rangle$, $|0\rangle$, $|+\rangle$, and so on; we use a basic propositional formula $\top_I$ to express *'separation*[2]*'* (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 (that is, 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* φ_I *of a (global) property* φ, the notion of *(I-)local property* $I(\varphi)$ (that is, φ is a property of the separated I-subsystem) and the notion of *(I-)local program* $I(\pi)$ (that is, π is a program affecting only the I-subsystem).

The third fundamental idea that underlies our approach comes from Coecke (2000; 2004), and was further elaborated in a category-theoretical setting in Abramsky and Coecke (2005): 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 Coecke (2000; 2004), this isomorphism has a *physical meaning*: the entangled state $\overline{\pi_{ij}}$, which '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* π (that is, it is given by $\pi(q)_j$). So *the above isomorphism captures the correlations between the possible results of potential local measurements* (on the two qubits). We use this idea to define formulas $\overline{\pi_{ij}}$ that characterise such specifically

[1] Indeed, it turns out that a quantum implication $\phi \stackrel{S}{\rightarrow} \psi$ is simply equivalent to the weakest precondition $[\varphi?]\psi$. In quantum logic, this dynamic view can be traced back to the analysis of the Sasaki hook as a Stalnaker conditional presented in Hardegree (1975) and Hardegree (1979) and is reflected on in, for example, Beltrametti and Cassinelli (1977) and Smets (2001).

[2] This can be compared with the *exogenous quantum logic approach* in Mateus and Sernadas (2004), which makes use of general modal operators to separate subsystems.

https://doi.org/10.1017/S0960129506005299 Published online by Cambridge University Press

entangled states (by using weakest preconditions to express the potential behaviour 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.

This *combination of quantum-dynamic and spatial logic* is what allows us to give *a logical characterisation 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', '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, that is, 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 and for a Quantum Secret Sharing protocol*; more details, and similar proofs for other quantum programs (Logic-Gate Teleportation, Super-Dense Coding, Entanglement Swapping, and so on) can be found in Akatov (2005). More generally, our logic can be used for the formal verification of a whole range of quantum programs[1], including all the circuits covered by the 'entanglement networks' approach in Coecke (2004).

Finally, we should 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, as in, for example, Jauch (1968) and Jauch and Piron (1969), by 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[2], 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, so we will leave this development for future work. Similarly, although our dynamic logic *cannot express probabilities, but just 'possibilities'* (via the dynamic modalities, which capture the system's potential behaviour 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 and to develop a proof system for probabilistic *LQP*.

2. Preliminaries: quantum frames

In this section we organise Hilbert spaces into relational structures, called *quantum frames* (also called *quantum transition systems* in Baltag and Smets (2005a)). We first study the

[1] Indeed, one may claim that *any* quantum circuit in which *probabilities do not play an essential role* can, in principle, be verified using our logic (or some trivial extension obtained by adding constants for other relevant states and logic gates).
[2] A ray is a one-dimensional linear subspace.

quantum frames of *single* quantum systems, then we consider *compound systems*, that is, the quantum frames corresponding to tensor products of Hilbert spaces, which represent physical systems that can be thought of as being composed of *parts* (subsystems). In this latter 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 (generalised) *PDL frame* is a modal frame $(\Sigma, \{\stackrel{S?}{\rightarrow}\}_{S\in\mathscr{L}}, \{\stackrel{a}{\rightarrow}\}_{a\in\mathscr{A}})$, in which the relations on the set of states Σ are of two types: the first, called *tests* and denoted by $S?$, are labelled with subsets S of Σ, coming from a given family $\mathscr{L} \subseteq \mathscr{P}(\Sigma)$ of sets, called *testable properties*; the others, called *actions*, are labelled with action labels a from a given set $\mathscr{A}$.

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*: $s \stackrel{S?}{\rightarrow} t$ 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*. Such tests will obviously change the state of the system. To model them, we introduce a special kind of PDL frame: *quantum frames*. The tests are interpreted as *projectors* in a Hilbert space, while the other basic actions are given by *unitary evolutions*. In Baltag and Smets (2005a), we considered PDL with this non-standard semantics, having essentially the same truth clauses as in the classical case, but interpreted in quantum frames. What we obtained was a 'quantum PDL', in which the traditional (orthomodular) 'quantum logic[1]' could be embedded as a fragment (corresponding to the *negation-free, test-only* part of quantum PDL). In this paper, we extend the syntax of this logic to deal with subsystems and entanglements.

Recall that a *Hilbert space* $\mathscr{H}$ is a complex vector space with an inner product $\langle \cdot \mid \cdot \rangle$, which is complete in the induced metric. The *adjoint* (or *Hermitian conjugate*) of a linear map $F : \mathscr{H} \rightarrow \mathscr{H}$ is the unique linear map $F^{\dagger} : \mathscr{H} \rightarrow \mathscr{H}$ such that $\langle x \mid F(y)\rangle = \langle F^{\dagger}(x) \mid y\rangle$, for all $x, y \in \mathscr{H}$. For any closed linear subspace $W \subseteq \mathscr{H}$, the *projector* $P_W : H \rightarrow H$ 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 $\mathscr{H}$ such that $U \circ U^{\dagger} = U^{\dagger} \circ U = id$, where id is the identity on $\mathscr{H}$. 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 'actualised': 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*.

[1] See, for example, Dalla Chiara and Giuntini (2002), Dalla Chiara *et al.* (2004) and Goldblatt (1974).

Quantum frames

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

$$\Sigma(\mathscr{H}) := (\Sigma, \{\stackrel{S?}{\rightarrow}\}_{S\in\mathscr{L}}, \{\stackrel{U}{\rightarrow}\}_{U\in\mathscr{U}}).$$

1. Let Σ be the set of *one dimensional subspaces* of $\mathscr{H}$, called the set of *states*. We denote a state $s = \overline{x}$ of $\mathscr{H}$ using any of the non-zero vectors $x \in \mathscr{H}$ that generate it, as a subspace. Note that any two vectors that differ only in *phase* (that is, $x = \lambda y$, with $\lambda \in C$ with $|\lambda| = 1$) will generate the same state $\overline{x} = \overline{y} \in \Sigma$.
2. We call two states s and t in Σ *orthogonal*, and write $s \perp t$, if every two vectors $x \in s, y \in t$ are orthogonal, that is, if $\forall x \in s, \forall y \in t : \langle x \mid y\rangle = 0$. Equivalently, we can state that $s \perp t$ iff $\exists x \in s, y \in t$ with $x \neq 0$, $y \neq 0$ and $\langle x \mid y\rangle = 0$. We put $S^{\perp} := \{t \in \Sigma \mid t \perp s \text{ for all } s \in S\}$; and use $\overline{S} = S^{\perp\perp} := (S^{\perp})^{\perp}$ to denote the biorthogonal closure of S. In particular, for a singleton $\{x\}$, we just write $\overline{x}$ for $\overline{\{x\}}$, which agrees with the notation $\overline{x}$ used above to denote the state generated by x.
3. A set of states $S \subseteq \Sigma$ is called a *(quantum) testable property* iff it is *biorthogonally closed*, that is, if $\overline{S} = S$. (Note that $S \subseteq \overline{S}$ is always the case.) We use $\mathscr{L} \subseteq \mathscr{P}(\Sigma)$ to denote the family of all quantum testable properties. All the *other* sets $S \in \mathscr{P}(\Sigma) \setminus \mathscr{L}$ are called *non-testable properties*.
4. There is a natural bijective correspondence between the family $\mathscr{L}$ of all testable properties and the family $\mathscr{W}$ of all *closed linear subspaces* W of $\mathscr{H}$, the bijection being given by $S \mapsto W_S := \bigcup S$. Observe that, under this correspondence, the image of the biorthogonal closure $\overline{S}$ of any arbitrary set $S \subseteq \Sigma$ is the closed linear subspace $\overline{\bigcup S} \subseteq \mathscr{H}$ generated by the union $\bigcup S$ of all states in S.
5. For each testable property $S \in \mathscr{L}$, there exists a partial map $S?$ on Σ, called a *quantum test*. If $W = W_S = \bigcup S$ is the corresponding subspace of $\mathscr{H}$, then the quantum test is the map induced on states by the *projector* P_W onto the subspace W. In other words, it is given by

$$S?(\overline{x}) := \overline{P_W(x)} \in \Sigma, \text{ if } \overline{x} \notin S^{\perp} (\text{ that is, if } P_W(x) \neq 0)$$
$$S?(\overline{x}) := \text{undefined, otherwise.}$$

We use $\stackrel{S?}{\rightarrow} \subseteq \Sigma \times \Sigma$ to denote the binary relation corresponding to the partial map $S?$ that is given by $s \stackrel{S?}{\rightarrow} t$ if and only if $S?(s) = t$. So we have *a family of binary relations indexed by the testable properties* $S \in \mathscr{L}$.
6. For each unitary transformation U on $\mathscr{H}$, consider the corresponding binary relation $\stackrel{U}{\rightarrow} \subseteq \Sigma \times \Sigma$, given by $s \stackrel{U}{\rightarrow} t$ if and only if $U(x) = y$ for some non-zero vectors $x \in s, y \in t$. So we obtain *a family of binary relations indexed by the unitary transformations* $U \in \mathscr{U}$ (where $\mathscr{U}$ is the set of unitary transformations on $\mathscr{H}$).

So a quantum frame is just a PDL frame built on top of a given Hilbert space $\mathscr{H}$, 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.

https://doi.org/10.1017/S0960129506005299 Published online by Cambridge University Press

Operators on states, adjoints and generalised tests

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

Measurement (non-orthogonality) relation

For all $s, t \in \Sigma$, let $s \to t$ if and only if $s \stackrel{S?}{\to} t$ for some property $S \in \mathscr{L}$. In other words, $s \to t$ means that one can reach state t by doing *some measurement* on state s. An important observation is that *the measurement relation is the same as non-orthogonality*[1]: $s \to t$ iff $s \not\perp t$.

Quantum actions

A *quantum action* is any relation $R \subseteq \Sigma \times \Sigma$ that can be written as an arbitrary[2] union $R = \bigcup_i F_i$ of linear maps $F_i : \Sigma \to \Sigma$. 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*

$$R; R' := \{(s, t) \in \Sigma \times \Sigma : \exists w \in \Sigma \text{ such that } (s, w) \in R, (w, t) \in R'\},$$

and iteration $R^* := \bigcup_{k \geqslant 0} R^n$ (where $R^n = R; R; \cdots R$ 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.

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

$$[R]T := \{s \in \Sigma : \forall t \in \Sigma(sRt \Rightarrow t \in T)\} \text{ and } \langle R \rangle T := \Sigma \backslash ([R](\Sigma \backslash T)).$$

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 $\Box T := \{s \in \Sigma : \forall t(s \to t \Rightarrow t \in T)\}$ and $\Diamond T := \Sigma \backslash (\Box(\Sigma \backslash T))$.

[1] The non-orthogonality relation has indeed been used to introduce an accessibility relation in the orthoframe semantics within quantum logic (Goldblatt 1974; Goldblatt 1984).

[2] That is, possibly infinite.

https://doi.org/10.1017/S0960129506005299 Published online by Cambridge University Press

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 $\mathscr{P}(\Sigma\times\Sigma)$) 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 $S^{\perp} = [S?]\varnothing = \Sigma \setminus \Diamond S$ and $\overline{S} = \Box\Diamond S$.

Proposition 1. For every property $S \subseteq \Sigma$, if $T \in \mathscr{L}$ (in other words, is testable), then $\Box S, S^{\perp}, [S?]T \in \mathscr{L}$ (are testable), and, more generally, $[R]T \in \mathscr{L}$, for every quantum relation R. For every state $s \in \Sigma$, we have $\{s\} \in \mathscr{L}$, that is, '*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 $\mathscr{L}$ 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 $\overline{S} = \bigsqcup\{\{s\} : s \in S\} = \bigcap\{T \in \mathscr{L} : S \subseteq T\}$, 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 $\Sigma = \Sigma(\mathscr{H})$:

1. *Partial functionality*
   If $s \stackrel{S?}{\rightarrow} t$ and $s \stackrel{S?}{\rightarrow} v$, then $t = v$.
2. *Trivial tests*
   $\stackrel{\varnothing?}{\rightarrow} = \varnothing$ and $\stackrel{\Sigma?}{\rightarrow} = \Delta_{\Sigma}$, where $\Delta_{\Sigma} = \{(s,s) : s \in \Sigma\}$ is the identity relation on $\Sigma \times \Sigma$.
3. *Atomicity*
   States are testable, that is, $\{s\} \in \mathscr{L}$. This is equivalent to requiring that 'states can be distinguished by tests', that is, if $s \neq t$, then $\exists P \in \mathscr{L} :\ s \perp P, t \not\perp P$.
4. *Adequacy*
   Testing a true property does not change the state: if $s \in P$, then $s \stackrel{P?}{\rightarrow} s$.

https://doi.org/10.1017/S0960129506005299 Published online by Cambridge University Press

5. *Repeatability*
   Any testable property holds after it has been successfully tested: if $s \stackrel{P?}{\rightarrow} t$, then $t \in P$.
6. *Compatibility*
   If $S, T \in \mathscr{L}$ are testable and $S?; T? = T?; S?$, then $S?; T? = (S \cap T)?$.
7. *Self-adjointness*
   If $s \stackrel{P?}{\rightarrow} w \rightarrow t$, then there exists some element $v \in \Sigma$ such that $t \stackrel{P?}{\rightarrow} v \rightarrow s$.
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 $s \stackrel{U}{\rightarrow} s'$ and $t \stackrel{U}{\rightarrow} t'$; then, $s \rightarrow t$ iff $s' \rightarrow t'$.

Proofs.

1. *Partial functionality* follows from the fact that projectors correspond to partially defined maps in $\mathscr{H}$.
2. *Trivial tests* follows from the fact that projecting on the empty space yields the empty space and that projecting on the total space does not change anything.
3. *Atomicity* follows from the fact that states are nothing but one-dimensional closed linear subspaces, that is, atoms of the lattice of all closed linear subspaces.
4. *Adequacy* follows from the fact that for every $x \in W$ we have $P_W(x) = x$.
5. *Repeatability* follows from the fact that $P_W(x) \in W$ for every $x \in \mathscr{H}$.
6. *Compatibility* follows from the fact that if two projectors commute, that is, $P_W \circ P_V = P_V \circ P_W$, then $P_W \circ P_V = P_{W \cap V}$.
7. *Self-adjointness* follows from the more general Adjointness theorem stated below, together with the fact that projectors are self-adjoint (that is, $S?^{\dagger} = S?$).
8. *Proper superpositions* can be proved by cases:
   If $s \not\perp t$, that is, let $s \rightarrow t$, then $w = s \Rightarrow s \rightarrow s \rightarrow t$.
   If $s \perp t$, that is, let $s \not\rightarrow t$, then let $s = \overline{x}, t = \overline{y}$ with $x, y \in \mathscr{H}$. Take the superposition $x + y \in \mathscr{H}$ of x and y and note that $x + y \neq 0$ (since $x + y = 0 \Rightarrow x = -y \Rightarrow s = t$, which contradicts $s \not\perp t$). Next observe that $x \not\perp (x + y)$ (Indeed, supposing $x \perp (x + y)$, we get $\langle x \mid x + y \rangle = 0$, and then $\langle x \mid x \rangle + \langle x \mid y \rangle = 0$; but $x \perp y$ implies $\langle x \mid x \rangle = 0$. So from $\langle x \mid x \rangle = 0$, we get $x = 0$, which yields a contradiction). Similarly, we get $y \not\perp (x + y)$.

Conditions 9 and 10 are immediate consequences of the definition of a unitary operator.
□

Note that, as a consequence of the 'Proper superpositions' property, *the double-box modality* $\Box\Box$ *coincides with the universal modality*, that is, $\Box\Box S \neq \emptyset$ iff $S = \Sigma$.

https://doi.org/10.1017/S0960129506005299 Published online by Cambridge University Press

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: $\langle Fx \mid y\rangle = \langle x \mid F^\dagger y\rangle$. From this we get the equivalence $\langle Fx \mid y\rangle = 0$ iff $\langle x, F^\dagger y\rangle = 0$; or, put another way, $Fx \perp y$ 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 $\exists w(\overline{x} \xrightarrow{F} \overline{w} \rightarrow \overline{y})$ iff $\exists v(\overline{y} \xrightarrow{F^\dagger} \overline{v} \rightarrow \overline{x})$. □

This proves the adjointness property. As a consequence, we have the following corollaries.

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

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

Corollary 2. If F is a quantum map,

$$F^\dagger(s) = \left([F]s^\perp\right)^\perp.$$

Proof. Using the fact that the negation of the measurement accessibility relation $\rightarrow$ is the orthogonality relation $\perp$, we immediately get from the above Adjointness theorem that

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

that is,

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

From this, we get $(F^\dagger(t))^\perp = [F]t^\perp$. 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 generalisation 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, put another way,

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

https://doi.org/10.1017/S0960129506005299 Published online by Cambridge University Press

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, that is, linear) map[1], 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. $R[S] = ([R^\dagger]S^\perp)^\perp$.

2.2. *Compound-system quantum frames*

In this subsection we 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 $n \geqslant 2$ (although later we will restrict consideration to the case $n \geqslant 4$), and put $N = \{1, 2, \ldots, n\}$. Our global state space will be denoted as before by $\mathscr{H}$, but now we assume it is an n-qubit state, that is, we put $\mathscr{H} = \mathscr{H}_n := H^{\otimes n} = H \otimes H \otimes ... \otimes H$ (n times) for the tensor product of n copies of H. An *n-qubit quantum frame* will be the quantum frame $\Sigma := \Sigma(\mathscr{H})$ associated (as in the previous section) to the Hilbert space $\mathscr{H}$.

Notation

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

We will further use $|+\rangle$ to denote the vector $|0\rangle + |1\rangle$, and, similarly, $|-\rangle$ to denote $|0\rangle - |1\rangle$. 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, for example, $00 := \overline{|00\rangle} = \overline{|0\rangle \otimes |0\rangle}$. The Bell states will be abbreviated as

[1] We identify a map $F : \Sigma \to \Sigma$ with its graph $F \subseteq \Sigma \times \Sigma$, that is, 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.

https://doi.org/10.1017/S0960129506005299 Published online by Cambridge University Press

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 ψ between the linear maps $F : H^{(i)} \to H^{(j)}$ and the states of $H^{(i)} \otimes H^{(j)}$. For fixed bases $\{\epsilon_\alpha^{(i)}\}_\alpha$ and $\{\epsilon_\beta^{(j)}\}_\beta$ of these spaces, the correspondence ψ maps the linear function F, given by $F(|\, x\rangle) = \Sigma_{\alpha\beta}\, m_{\alpha\beta}\, \langle \epsilon_\alpha^{(i)} \mid x\rangle . \epsilon_\beta^{(j)}$ for all $|\, x\rangle \in H^{(i)}$, to the state $\psi(F) := \Sigma_{\alpha\beta}\, m_{\alpha\beta} . \epsilon_\alpha^{(i)} \otimes \epsilon_\beta^{(j)}$.

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

Notation

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

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

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

Proposition 6. Let $F : \mathscr{H} \to \mathscr{H}$ be a linear map. Then the state $\overline{F}_{(ij)}$ is 'entangled according to F'; that is, if $F_{(1)}(|x\rangle) = |y\rangle$ and 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) $\overline{F}_{ij} \subseteq \Sigma = \Sigma(\mathscr{H})$ by defining it as *the set of all states having the* $\{i,j\}$*-qubits in the state* $\overline{F}_{(ij)}$:

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

where $\mu_{\{i,j\}}$ is, as above, the canonical isomorphism between $\mathscr{H}_{\{i,j\}} \otimes \mathscr{H}_{N\setminus\{i,j\}}$. In other words, $\overline{F}_{ij}$ is simply the property of an n-qubit compound state 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 I*-local* if it corresponds to a property of the subsystem formed by the qubits in I; in other words, if there exists some property

https://doi.org/10.1017/S0960129506005299 Published online by Cambridge University Press

$S' \subseteq \Sigma(\mathscr{H}_I)$ such that

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

or, more explicitly, $S = \{\overline{\mu_I(\phi \otimes \psi)} : \overline{\phi} \in S', \psi \in \mathscr{H}_{N \setminus I}\}$. An *example* is the property $\overline{F}_{ij}$, which is $\{i, j\}$-local. For any $I \subseteq N$, the family of I-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 $s \in \top_I^\Sigma$. But note that the family of I-local properties is *not closed under complementation.*

Local maps

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

$$F \circ \mu_I (\phi \otimes \psi) \;=\; \mu_I (G(\phi) \otimes \psi).$$

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

Local actions

An I-*local action* is a quantum action $R \subseteq \Sigma \times \Sigma$ that can be written as an arbitrary[1] union of I-local maps. The family of I-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

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

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 $\overline{G_{jk}}$? followed by $\overline{F_{ij}}$?, the k-th qubit (k-th component) of the output-state is

$$\left(\overline{F_{ij}}? \circ \overline{G_{jk}}?(s)\right)_k = G_{(1)} \circ F_{(1)}(x).$$

Lemma 3 (Entanglement Composition Lemma). The main lemma given in Coecke (2004) states (in our notation) that, given a quadruple of *distinct* indices i, j, k, l, and letting $F, G, H, U, V : H \to H$ be single-qubit linear maps (that is, 1-local transformations), we have

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

Coecke (2004) and Abramsky and Coecke (2005) use these last two lemmas as the main tool in explaining teleportation, quantum gate teleportation and many other quantum

[1] That is, possibly infinite.

https://doi.org/10.1017/S0960129506005299 Published online by Cambridge University Press

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 analyse teleportation and quantum secret sharing.

Observe that in the above Lemma 3, 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 is an I-local map and G is a J-local map, we have

$$F \circ G = G \circ F.$$

Another important property of local maps (on *states*) is given by the following proposition.

Proposition 8 (Agreement Property). Let $F, G : \Sigma \to \Sigma$ be two I-local maps on states, having the same domain[1]: $dom(F) = dom(G)$. Then their output-states agree on all non-I qubits, that is, for all $s \in \Sigma$,

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

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

Dynamic characterisations of main unitary transformations

It is well known that a linear operator on a vector space in a given Hilbert space is *uniquely determined* by the values it takes on the vectors of an (orthonormal) basis. An important observation is that this fact is no longer 'literally true' when we move to 'states' as one-dimensional subspaces instead of vectors. The reason is that 'phase'-aspects (or, in particular, the signs '+' and '−') are not 'state' properties in our setting. In other words, two vectors that differ only in phase, that is, $x = \lambda y$ where λ is a complex number with $| \lambda |= 1$, belong to the same subspaces, so they correspond to the same state $\overline{x} = \overline{y}$.

Example 1 (Counterexample). Consider a 2-dimensional Hilbert space in which we use $|0\rangle$ and $|1\rangle$ to denote the basis vectors. 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:

$$I(0) = \overline{I(|0\rangle)} = 0 = \overline{J(|0\rangle)} = J(0),$$

$$I(1) = \overline{I(|\,1\rangle)} = 1 = \overline{-\,|\,1\rangle} = \overline{J(|\,1\rangle)} = J(1).$$

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

https://doi.org/10.1017/S0960129506005299 Published online by Cambridge University Press

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 $\Sigma(\mathscr{H}_1)$ 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 $\Sigma(\mathscr{H}_n)$ of the space $\mathscr{H}_n$ is uniquely determined by its images on the states:

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

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

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

The transformation $CNOT$ is given by the table:

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

3. The logic LQP

3.1. *Syntax of LQP*

To build up the language of LQP, we are given the following: a natural number n, for which we put $N = \{1, 2, \ldots, n\}$; a set $\mathscr{Q}$ of *propositional variables*; a set $\mathscr{C}$ of *propositional constants*; and a set $\mathscr{U}$ of program constants, denoting *basic programs*, to be interpreted as *quantum gates*. Each program constant $U \in \mathscr{U}$ *comes 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 the index explicit, we write, for example, U_I for an I-local quantum gate. In particular, for every $i, j \leqslant n$, we are given some special program constants $CNOT_{ij}, X_i, H_i, Z_i, \ldots \in \mathscr{U}$. Similarly, we are given two special propositional constants $1, + \in \mathscr{C}$, the first denoting the separated state $|1\rangle^{\otimes n} = |1\rangle \otimes |1\rangle \cdots \otimes |1\rangle$ and the second denoting the separated 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:

$$\varphi ::= \top_I \mid p \mid c \mid \neg\varphi \mid \varphi \wedge \varphi \mid [\pi]\varphi$$
$$\pi ::= \top_I \mid \varphi? \mid U \mid \pi^\dagger \mid \pi \cup \pi \mid \pi ; \pi$$

https://doi.org/10.1017/S0960129506005299 Published online by Cambridge University Press

Here, we take I to denote sequences of distinct indices in $N = \{1, 2, \ldots, n\}$. 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 $\top_N$ will denote the 'always true' proposition (*verum*, usually denoted $\top$), that is, the 'top' of the lattice of all properties[1]. 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 φ will hold after running program π.*

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 the $N \setminus I$*subsystem* unchanged, 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 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.

Abbreviations in *LQP*

We can enrich our basic language by introducing various abbreviations. In particular, we define the *classical disjunction* and *classical implication* in the usual way, that is, $\varphi \vee \psi := \neg(\neg\varphi \wedge \neg\psi)$, $\varphi \rightarrow \psi := \neg\varphi \vee \psi$. As in classical logic, we can introduce a propositional constant *falsum* $\bot_N := \neg\top_N$ for the 'always false' sentence (usually denoted $\bot$). In non-ambiguous contexts, we sometimes skip the subscript N, and simply write $\top$ and $\bot$ for $\top_N$ and $\bot_N$. 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 $\Diamond$ used in the quantum logic literature can be defined in *LQP* by putting $\Diamond\varphi := \langle\varphi?\rangle\top_N$ and $\Box\varphi := \neg\Diamond\neg\varphi$. The *orthocomplement* is defined as $\sim\varphi := \Box\neg\varphi$, or, equivalently, as $\sim\varphi := [\varphi?]\bot_N$. Using 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 that is a superposition of states satisfying φ or ψ.

We also introduce some notions and notation for programs: we call a program π *deterministic* if π 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 that (given any $\{i, j\}$-separated input state) permutes the i^{th} and j^{th} components. Finally, we put

$$id \;:=\; \top_N?$$

for the *identity* map.

[1] Note also the distinction between the constant 1_i (characterising the qubit $|1\rangle_i$) and the constant $\top_i$ (denoting the property of being i-separated).

https://doi.org/10.1017/S0960129506005299 Published online by Cambridge University Press

Order, equivalence, orthogonality, I-equivalence, testability, locality, separation

We can internalise the *logical equivalence, being weaker than, and I-equivalence* relations between formulas, the *locality* and *testability*, and the notion of *I-component* by defining the following properties of formulas:

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

Recall from Section 2.1 that the double-box modality coincides with the universal modality: so, indeed, $\varphi \leqslant \psi$ means that φ is *logically weaker* than ψ, while $\varphi = \psi$ means the formulas are *equivalent*. We read $T(\varphi)$ as saying that 'φ is testable', and $I(\varphi)$ as 'φ is I-local'. We read φ_I as 'the I-component of φ': a state satisfies this sentence iff (it is I-separated and) its I-subsystem is (a subsystem of some state) satisfying φ. For $I = \{i\}$, we write $\varphi_i := \varphi_I$. We read $\varphi =_I \psi$ as 'φ is I-equivalent to ψ': the meaning is that *both φ and ψ are I-separated and have the same I-component*. Finally, we say that φ is *I-separated* iff $\varphi \leqslant \top_I$.

Note that it obviously follows from these definitions that *every I-component φ_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) π on (any state satisfying a given precondition) φ*, by putting

$$\pi[\varphi] \;:= \sim [\pi^{\dagger}] \sim \varphi.$$

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

Note the *contrast with classical PDL*: unlike the classical version, our quantum PDL (as considered above, that is, *without program converse*[1]) has enough expressive power to *define strongest post-conditions (and, in a restricted context, images) using weakest preconditions*!

[1] 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 π. It is obvious that this stronger logic can express the strongest post-condition of a program π using the existential dynamic modalities, since $\pi(\varphi) = \langle \pi^{\smile} \rangle \varphi$.

The reason is that, in some context, the notion of adjoint can replace the notion of converse. But note that converse itself is *not* expressible in our logic. This is a good thing since 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

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

The unary maps induced by a program

In our syntax we want to capture the construction $F_{(1)}$, by which a linear map F on $H^{\otimes n}$ was used to describe a unary map $F_{(1)}$ on H. For this, we put $0_i! := 0_i? \cup (1_i?; X_i)$, and $0_I! := 0_{i_1}!; 0_{i_2}!; \cdots; 0_{i_k}!$, where $I = (i_1, i_2, \ldots, i_k)$. This maps any qubit in I to 0. Similarly, we put $0_I? := (0_{i_1} \wedge 0_{i_2} \wedge \cdots \wedge 0_{i_k})?$. Finally, we define

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

This is the map we need (which encodes a single qubit transformation). In fact, we shall only use $\pi_{(1)}$ in the rest of this paper. We also want to consider the $H_i \to H_j$-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*, that is, the ones that 'affect only the qubits in a given set $I \subseteq N$'. For this, we define a formula $I(\pi)$ meaning 'program π 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 π *acts '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 $c \in \{0, 1, +\}$). One of our axioms below ('Determinacy of deterministic programs') means that this clause is enough to ensure that program π acts locally *on all (I-separated) states*.

Entanglement according to π

To describe states that are 'entangled according to π', we introduce the formula

$$\overline{\pi}_{ij} := \top_{ij} \wedge \bigwedge_{c \in \{0,1,+\}} \left([c_i?](\pi_{ij}(c_i))_j \wedge (\sim c_i \to \pi_{ij}(c_i) = \bot) \right).$$

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

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

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

https://doi.org/10.1017/S0960129506005299 Published online by Cambridge University Press

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* (that is, all testable i-local properties).

3.2. *Semantics of LQP*

An *LQP-model* is a *multi-partite quantum frame* $\Sigma = \Sigma(\mathscr{H})$ based on an n-dimensional Hilbert space $\mathscr{H}$, 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, that is, sets of states in Σ. At 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

$$
\begin{array}{lll@{\qquad\qquad}lll}
\| \top_I \| & := & \top_I^{\Sigma\times\Sigma} & \| \varphi? \| & := & \| \varphi \|? \\
\| U \| & := & U & \| \pi^\dagger \| & := & \| \pi \|^\dagger \\
\| \pi_1 \cup \pi_2 \| & := & \| \pi_1 \| \cup \| \pi_2 \| & \| \pi_1 ; \pi_2 \| & := & \| \pi_2 \| ; \| \pi_1 \|
\end{array}
$$

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:

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

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.

$$
\begin{array}{rcl}
\| {\sim}\, \varphi \| & = & \| \varphi \|^\perp \\
\| [\varphi?]\psi \| & = & [\| \varphi \|?] \, \| \psi \| \\
\| \Box\varphi \| & = & \Box \, \| \varphi \| \\
\overline{\| \varphi \|} & = & \| {\sim}{\sim}\, \varphi \|
\end{array}
$$

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

1. $\| \varphi \|$ is testable (that is, $T(\varphi)$ is valid).
2. φ is semantically equivalent to ${\sim}{\sim}\, \varphi$.

https://doi.org/10.1017/S0960129506005299 Published online by Cambridge University Press

3. φ is semantically equivalent to some formula $\Box\psi$.
4. φ is equivalent to some formula $\sim \psi$.

Proposition 12. For deterministic programs π, the interpretation of the construct $\overline{\pi}_{ij}$ is the property of 'being entangled according to (the linear map denoted by) π'. More precisely, for deterministic π, we have

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

where we use the notation $\overline{F}_{ij}$ introduced (for any linear map F) after Proposition 6 of Section 2.2.

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 φ? and Kleene star[1] π^*. In particular, we have the following rules and axioms.

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

And the 'normality' conditions for the dynamic modalities $[\pi]$:

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

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

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

Test Generalisation Rule. If the variable q does not occur in φ or ψ, then,

$$\text{from } \vdash \varphi \to [q?]\psi \text{ infer } \vdash \varphi \to \Box\psi$$

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

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

Other *LQP*-axioms are:

Partial Functionality. $\vdash \neg[p?]q \to [p?]\neg q$
Adequacy. $\vdash p \wedge q \to \langle p?\rangle q$
Repeatability. $\vdash T(p) \to [p?]p$
Proper Superpositions. $\vdash \langle \pi\rangle\Box\Box p \to [\pi']p$

[1] We skip the axioms for iteration, π^*, only because we chose not to include this construct in our logic. However, if one adds π^* to our syntax, the usual *PDL* axioms for iteration are still sound, so they can be added to the proof system.

https://doi.org/10.1017/S0960129506005299 Published online by Cambridge University Press

Unitary Functionality. $\vdash \neg[U]q \leftrightarrow [U]\neg q$
Unitary Bijectivity 1. $\vdash p \leftrightarrow [U; U^{\dagger}]p$
Unitary Bijectivity 2. $\vdash p \leftrightarrow [U^{\dagger}; U]p$
Adjointness. $\vdash p \rightarrow [\pi]\Box\langle\pi^{\dagger}\rangle\Diamond p$

Proposition 13. Testability is closed under conjunctions, weakest preconditions; $\Box$-sentences, orthocomplements and strongest postconditions are testable:

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

A formula φ 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 the following purely syntactical way to check testability:

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

Proposition 14 (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[1]' $\varphi \wedge [\varphi?]\psi \leqslant \psi$. In its turn, this rule is equivalent to the condition known in quantum logic as weak modularity, which is stated as follows: $\varphi \wedge (\sim\varphi \sqcup (\varphi \wedge \psi)) \leqslant \psi$.

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, and so on), *then there exists a complete proof system for (single-system) Hilbert spaces*, which includes the above axioms[2].

The proof of this theorem is given in our paper Baltag and Smets (2005a), and is based on an extension of (Mayet's version (Mayet 1999) of) Solèr's Theorem (Solèr 1995), which is itself an extension of Piron's Representation Theorem for Piron lattices (Piron 1964; 1976; Amemiya and Araki 1967).

Proposition 15. The formula $\pi[\varphi]$ expresses the *strongest testable postcondition* ensured by executing program π on any state satisfying (precondition) φ. In other words, for every

[1] This explains why the weakest precondition $[\varphi?]\psi$ has been taken as the basic implicational connective in traditional quantum logic, under the name of the 'Sasaki hook' and denoted by $\varphi \stackrel{S}{\rightarrow} \psi$.

[2] In addition, the system includes two more axioms of a rather technical nature, namely Piron's 'Covering Law' (Piron 1976) and 'Mayet's Condition' (Mayet 1999). See Baltag and Smets (2005a) for details.

testable ψ, we have

$$\pi[\varphi] \leqslant \psi \quad \text{iff } \varphi \leqslant [\pi]\psi$$

Proposition 16 (Adjointness Theorem). For all *testable* formulas φ, ψ, we have

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

4.2. *Axioms for compound systems*

Separation Axioms. Every state is N-separated; 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:

$$\vdash \top_N$$

and

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

Axioms for the trivial I-local program. The program $\top_I$ is the weakest I-local program; that is,

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

and

$$\vdash I(\top_I)$$

As an immediate consequence, we obtain the following corollary.

Corollary 4. The formula $\top_I$ is the weakest I-local property; that is,

$$\vdash I(\top_I)$$

and

$$\vdash I(p) \rightarrow p \leqslant \top_I$$

Proof. By the definition of I-locality $I(\pi)$ of a program, it is easy to see that the identity program *id* is I-local for every I. Applying the first part of the above axiom (for $\top_I$), we obtain $\top_I = \langle id \rangle \top_I \leqslant \langle \top_I \rangle \top_I$, from which we deduce that $\top_I = \top_I \wedge \langle \top_I \rangle \top_I$. Applying the definition of φ_I, we conclude that $\top_I = (\top_I)_I$, and thus (by the definition of I-locality $I(\varphi)$ of a sentence) we derive $I(\top_I)$. The second part of the corollary follows trivially from the definition of $I(p)$. □

Syntactically, we define an *'I-local state'* to be any sentence φ such that

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

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

https://doi.org/10.1017/S0960129506005299 Published online by Cambridge University Press

Local States Axiom. Testable local properties are 'local states' (in the above sense, that is, atomic local properties): if $I \neq N$,

$$\vdash \; T(p) \wedge I(p) \wedge I(q) \wedge \bot \neq q \leqslant p \;\rightarrow\; q = p$$

Basic-State Testability Axiom. Our basic properties $c_i, \overline{\pi_{ij}}$ are testable and local (for the appropriate subsystem). More precisely, if $i, j \in N$, $c \in \{0, 1, +, -\}$ and π is a *deterministic* program, then

$$\vdash \; T(c_i) \wedge I(c_I) \wedge T(\overline{\pi_{ij}}) \wedge \{i, j\}(\overline{\pi_{ij}})$$

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

The following corollary is another immediate consequence.

Corollary 5. $\sim \top_I = \bot$

Proof. By the Adequacy axiom, we have $1_I \wedge \top_N \leqslant \langle 1_I ?\rangle \top_N$. But $\top_N$ is the 'always true' sentence, so we have $\neg\langle 0_I ?\rangle \top_N = [0_I ?]\bot_N = \sim 0_I = 1_I = 1_i \wedge \top_N \leqslant \langle 1_I ?\rangle \top_N$. From this, we get $\top_N = (\langle 0_I ?\rangle \top_N \vee \langle 1_I ?\rangle \top_N)$. By Adequacy again, we always have $\top_N \leqslant \langle 0_I ?\rangle 0_I \leqslant \langle 0_I ?\rangle \top_I$ (since 0_I is I-local, so $0_I \leqslant \top_I$) and, similarly, $\top_N \leqslant \langle 1_I ?\rangle \top_I$. Putting these three together, we deduce $\top_N \leqslant (\langle 0_I ?\rangle \top_I \vee \langle 1_I ?\rangle \top_I)$. But by the Testability axiom (in its dual form), we have $\langle 0_I ?\rangle \top_I \leqslant \Diamond \top_I$ and, similarly, $\langle 1_I ?\rangle \top_I \leqslant \Diamond \top_I$. Hence we have $\top_N \leqslant (\Diamond \top_I \vee \Diamond \top_I) = \Diamond \top_I = \langle \top_I ?\rangle \top_N$, and thus $\sim \top_I = [\top_I ?]\bot_N = \neg\langle \top_I ?\rangle \top_N \leqslant \neg \top_N = \bot_N = \bot$. □

To capture the fact that the lattice of local properties is *atomistic*, we accept the following inference rule.

Local Atomicity Rule. Local properties are unions of testable local properties (that is, of local states): if $I \neq N$ and the variable p does not occur in φ, ψ or θ, then

from $\quad \vdash \; \psi \wedge T(p_I) \wedge p_I \leqslant \varphi \;\rightarrow\; p_I \leqslant \theta$

infer $\quad \vdash \; \psi \wedge I(\varphi) \;\rightarrow\; \varphi \leqslant \theta$

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

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

$$\vdash I(\varphi) \wedge \varphi \neq \bot \wedge (I(p) \wedge \bot \neq p \leqslant \varphi \;\rightarrow\; p = \varphi)$$

we can infer

$$\vdash \; T(\varphi)$$

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 $\mathscr{H}$ of being uniquely determined by their values on all the states $|x\rangle_1 \otimes \cdots |x\rangle_n$, with $|x\rangle_i \in \{|0\rangle_i, |1\rangle_i, |+\rangle_i\}$.

https://doi.org/10.1017/S0960129506005299 Published online by Cambridge University Press

Determinacy Axiom of Deterministic Programs. For deterministic programs π, π',

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

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

Entanglement Axiom. If π is deterministic and $i \neq j$, then

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

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

Proposition 17. Any formula of the form φ_I is always I-local. Any formula of the form $\overline{\pi_{ij}}$ is $\{i, j\}$-local. If φ and ψ are I-local formulas and π is an I-local program, then $\varphi \vee \psi$, $\varphi \wedge \neg\psi$ and $\varphi \wedge [\pi]\psi$ are I-local. If φ is I-local and ψ is J-local, then $\varphi \wedge \psi$ is $I \cup J$-local.

Proposition 18. If φ is a *testable* I-local formula, then $\varphi?$ is an I-local program. $\top_I$ is I-local. If π and π' are I-local, then $\pi \cup \pi'$ and $\pi;\pi'$ are I-local.

Proposition 19. 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 20. Systems composed of identical parts are identical:

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

Proposition 21. $\vdash \ p_I \perp q \leftrightarrow p_I \perp q_I$

Proposition 22 (Dual Local Atomicity Rule). If $I \neq N$, φ and θ are I-separated, and p does not occur in φ, ψ or θ, 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. 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

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

Now assume $\psi \wedge T(\varphi_I) \wedge T(\theta_I)$. Then the formula $\top_I \wedge \sim \varphi_I = \top_I \wedge \neg(\top_I \wedge [\varphi_I?]\bot)$ is I-local (since φ_I is testable I-local, so $\varphi_I?$ is an I-local program, we have $\top_I \wedge [\varphi_I?]\bot$ is I-local) and, similarly, $\top_I \wedge \sim \theta_I$ is I-local. So we can apply the Local Atomicity Rule to get $(\top_I \wedge \sim \varphi_I) \leqslant (\top_I \wedge \sim \theta_I)$. Applying orthocomplementation, we have $\sim (\top_I \wedge \sim \theta_I) \leqslant \sim (\top_I \wedge \sim \varphi_I)$. From this we get

$$\begin{aligned} \theta_I &= \sim\sim \theta_I = \bot \sqcup \sim\sim \theta_I = \sim \top_I \sqcup \sim\sim \theta_I = \sim (\top_I \wedge \sim \theta_I) \\ &\leqslant \sim (\top_I \wedge \sim \varphi_I) = \sim \top_I \sqcup \sim\sim \varphi_I = \bot \sqcup \varphi_I = \varphi_I \end{aligned}$$

https://doi.org/10.1017/S0960129506005299 Published online by Cambridge University Press

However, by the Local States Axiom, this then implies that $\theta_I = \varphi_I$ (since both are testable I-local with $I \neq N$, and thus they are local states). Since both θ_I and φ_I are I-separated, it follows that $\theta =_I \varphi$. □

Theorem 4 (Compatibility of Programs Affecting Different Qubits). If $I \cap J = \emptyset$ and π, π' 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 Proposition 19 (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 Proposition 20, we put these together to conclude that

$$(\pi ; \pi')(\vec{c}_N) \;=_{I \cup J \cup (N \setminus (I \cup J))}\; (\pi' ; \pi)(\vec{c}_N);$$

that is, that

$$(\pi ; \pi')(\vec{c}_N) = (\pi' ; \pi)(\vec{c}_N)$$ □

Proposition 23 (Dual Entanglement). If π is deterministic and $i \neq j$, then

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

Proof. Assume $T(q_j)$ and we need to show that $q_j?(\overline{\pi_{ij}}) =_i \pi^{\dagger}_{ij}(q_j)$. It is easy to see that both sides are i-separated (that is, $\leqslant \top_i$), and also that both $(q_j?(\overline{\pi_{ij}}))_i$ and $(\pi^{\dagger}_{ij}(q_j))_i$ are testable (since they are local states), so we are in the conditions of the Dual Local Atomicity Rule (Proposition 22) above. By that Proposition, to prove the above identity, it is enough to show that

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

To show this, let p_i be such that $T(p_i)$ and $p_i \perp \pi^{\dagger}_{ij}(q_j)$. By the Adjointness Theorem, we then have $\pi_{ij}(p_i) \perp q_j$, and thus $q_j?(\pi_{ij}(p_i)) = \perp$. By the previous Proposition (on the Compatibility of Programs on Different Qubits), we have

$$\begin{aligned} p_i?(q_j?(\overline{\pi_{ij}})) &= (p_i?; q_j?)(\overline{\pi_{ij}}) \\ &= (q_j?; p_i?)(\overline{\pi_{ij}}) \\ &= q_j?(p_i?(\overline{\pi_{ij}})) \\ &= q_j?(\pi_{ij}(p_i)) \\ &= \perp \end{aligned}$$

https://doi.org/10.1017/S0960129506005299 Published online by Cambridge University Press

(where we have used the Entanglement Axiom). So we get $p_i \perp q_j?(\overline{\pi_{ij}})$. (Thus, using the Dual Local Atomicity Rule, the desired conclusion follows). □

Proposition 24 (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 get $q_j \perp (\pi_{ij}(p_i))_j$, and thus $(p_i \wedge q_j) \perp (\pi_{ij}(p_i))_j$, 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 $\overline{\pi_{ij}} \leqslant [p_i?](\pi_{ij}(p_i))_j$ (since $p_i?(\overline{\pi_{ij}}) \leqslant (p_i?(\overline{\pi_{ij}}))_j = (\pi_{ij}(p_i))_j$, by the Entanglement Axiom), so we get $(p_i \wedge q_j) \perp \overline{\pi_{ij}}$. □

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

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

To show this, let q_k be 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 the Adjointness Theorem, we have $\sigma^{\dagger}_{jk}(q_k) \perp \pi_{ij}(p_i)$. 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 get

$$\begin{aligned} q_k?\left((\overline{\sigma_{jk}}?;\overline{\pi_{ij}}?)(p_i)\right) &= q_k?\left(\overline{\pi_{ij}}?(\overline{\sigma_{jk}}?(p_i))\right) \\ &= \overline{\pi_{ij}}?\left(q_k?(\overline{\sigma_{jk}}?(p_i))\right) \\ &=_{ijk} \overline{\pi_{ij}}?(q_k?(\overline{\sigma_{jk}}) \wedge p_i) \\ &= \perp \end{aligned}$$

(where we have used Theorem 4 on the Compatibility of Programs on Different Qubits). So we get $q_k \perp (\overline{\sigma_{jk}}?;\overline{\pi_{ij}}?)(p_i)$, as desired. □

Corollary 6. If i, j, k are distinct,

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

Proof. By the Repeatability Axiom, we have $\overline{\sigma_{jk}}?(p_i) \leqslant \overline{\sigma_{jk}}$. Assuming $\overline{\sigma_{jk}}?(p_i) \neq \perp$, we get $\overline{\sigma_{jk}}?(p_i) =_{jk} \overline{\sigma_{jk}}$ (since $\overline{\sigma_{jk}}$ is testable and $\{j,k\}$-local, and hence it is a local state) and also that $\overline{\sigma_{jk}}?(p_i) =_i p_i$ (since 'local programs act locally', by Proposition 19). Thus, we get $\overline{\sigma_{jk}}?(p_i) =_{ijk} p_i \wedge \overline{\sigma_{jk}}$. Applying the $\{i,j\}$ local program $\overline{\pi_{ij}}$, we get

$$\begin{aligned} \overline{\pi_{ij}}?(p_i \wedge \overline{\sigma_{jk}}) &=_{ijk} \overline{\pi_{ij}}?(\overline{\sigma_{jk}}?(p_i)) \\ &= (\overline{\sigma_{jk}}?;\overline{\pi_{ij}}?)(p_i) \\ &=_k (\pi_{ij};\sigma_{jk})(p_i) \end{aligned}$$

from which we get the desired conclusion. □

By a refinement of the proof of Teleportation Property, we can prove the following proof-theoretic version of Lemma 3 in Section 2.2.

https://doi.org/10.1017/S0960129506005299 Published online by Cambridge University Press

Proposition 25 (Entanglement Composition Lemma). For distinct indices i, j, k, l, programs π, π', π'' and local $\{1\}$-programs σ_1, ρ_1, we have

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

The *domain* $dom(\varphi)$ of a map π is defined as $dom(\pi) := < \pi > \top$.

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

Proof. Put $\psi := T(p) \wedge I(\pi) \wedge I(\pi') \wedge dom(\pi) = dom(\pi') \wedge \pi(p) \leqslant \top_I \wedge \pi'(p) \leqslant \top_I$, and assume that ψ is true. By definition, $\pi(p)$ is testable (since π 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. Now let $q_{N \setminus I}$ 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 get $(q_{N \setminus I} ? ; \pi)(p) = \perp$, that is, $p \leqslant [q_{N \setminus I}][\pi]\perp = [q_{N \setminus I}]\neg z\langle \pi \rangle \top = [q_{N \setminus I}]\neg dom(\pi)$. But $dom(\pi) = dom(\pi')$, so $p \leqslant [q_{N \setminus I}]\neg dom(\pi') = [q_{N \setminus I}][\pi']\perp$, that is, $(q_{N \setminus I} ? ; \pi')(p) = \perp$. Working now in reverse, we again apply the Compatibility of Programs on Different Qubits, obtaining $(\pi' ; q_{N \setminus I} ?)(p) = \perp$, that is, $q_{N \setminus I} \perp \pi'(p)$. So we have proved that

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

By now applying the Dual Local Atomicity Rule, we get

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

which is, the desired conclusion. □

Characteristic formulas

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

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

https://doi.org/10.1017/S0960129506005299 Published online by Cambridge University Press

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 the following axioms for X, Z, H.

Characteristic Axioms for Quantum Gates X and Z.

$\vdash 0_i \to [X_i]1_i$	$\vdash 1_i \to [X_i]0_i$	$\vdash +_i \to [X_i]+_i$
$\vdash 0_i \to [Z_i]0_i$	$\vdash 1_i \to [Z_i]1_i$	$\vdash +_i \to [Z_i]-_i$
$\vdash 0_i \to [H_i]+_i$	$\vdash 1_i \to [H_i]-_i$	$\vdash +_i \to [H_i]0_i$

Notation (Bell formulas)

For $x, y \in \{0, 1\}$ and distinct indices $i, j \in N$, we make the abbreviations $\beta^{ij}_{xy} := \overline{(Z^x_1; X^y_1)_{ij}}$, and refer to these expressions as 'the *Bell formulas*'.

Proposition 26. The Bell states $\beta^{i,j}_{xy}$ are characterised by the logic Bell formulas β^{ij}_{xy}. In other words, a state satisfies one of these formulas iff it coincides with the corresponding Bell state.

Proof. It is enough to check that the formulas β^{ij}_{xy} imply the corresponding characteristic formulas in the above table. For this, we use the Entanglement Axiom and the following (easily checked) theorems:

$$\vdash\ 0_1 \leftrightarrow < Z^x_1; X^y_1 > y_1$$
$$\vdash\ 1_1 \leftrightarrow < Z^x_1; X^y_1 > \tilde{y}_1$$
$$\vdash\ +_1 \to < Z^x_1; X^y_1 > (-)^x_1$$

□

Generalised Bell formulas, GHZ States. As shown by the first author's student Dmitri Akatov in his Master's thesis (Akatov 2005), the above dynamic-logical characterisation of Bell states can be recursively extended to the so-called *generalised (k-qubit) Bell states* (which form an orthonormal basis for the k-qubit space), for all $k \leqslant n$. Here, we only mention a special case, that of the so-called *GHZ state* (after Greenberg, Horne and Zeilinger):

$$\beta^{i,j,k}_{000} = \overline{|\,000\rangle_{ijk} + |\,111\rangle_{ijk}}$$

This state, of a special significance for various quantum protocols, can be characterised by the formula

$$\beta^{ijk}_{000} := \langle 0_i?\rangle(0_j \wedge 0_k) \wedge \langle 1_i?\rangle(1_j \wedge 1_k) \wedge \langle +_i?\rangle\beta^{jk}_{00}$$

From this, it is obvious that we have $+_i?(\beta^{ijk}_{000}) =_{jk} \beta^{jk}_{00}$; but one can easily check that we also have $-_i?(\beta^{ijk}_{000}) =_{jk} \beta^{jk}_{10}$. Using the notation $(-)^z$ introduced above for $z = 0, 1$ (putting $(-)^z := -$ if $z = 1$ and $(-)^z := +$ if $z = 0$), we can summarise this as

$$(-)^z_i?(\beta^{ijk}_{000}) =_{jk} \beta^{jk}_{z0}$$

https://doi.org/10.1017/S0960129506005299 Published online by Cambridge University Press

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

$$\vdash 0_i \wedge c_j \to [CNOT_{ij}]c_j \qquad \vdash 1_i \wedge 0_j \to [CNOT_{ij}]1_j$$
$$\vdash 1_i \wedge 1_j \to [CNOT_{ij}]0_j \qquad \vdash 1_i \wedge +_j \to [CNOT_{ij}]+_j$$
$$\vdash +_i \wedge 0_j \to [CNOT_{ij}]\beta^{ij}_{00} \qquad \vdash +_i \wedge 1_j \to [CNOT_{ij}]\beta^{ij}_{01}$$
$$\vdash +_i \wedge +_j \to [CNOT_{ij}]\gamma^{ij}$$

where $\gamma^{ij} = \langle 0_i?\rangle +_j \wedge \langle 1_i?\rangle +_j \wedge \langle +_i?\rangle +_j$

Proposition 27. For all $x, y \in \{0, 1\}$,

$$\vdash (H_i; CNOT_{i,j})(x_i \wedge y_j) = \beta^{ij}_{xy}$$

Corollary 7. If i, j, k are all distinct,

$$\vdash (CNOT_{ij}; H_j; (x_i \wedge y_j)?)(p) =_k \beta^{ij}_{xy}?(p)$$

Proof. From the above Proposition and from $H^\dagger = H$, $CNOT^\dagger = CNOT$, we get $(CNOT_{i,j}; H_i)(\beta^{ij}_{xy}) = x_i \wedge y_i$, and thus

$$\begin{aligned} dom(CNOT_{i,j}; H_i) &= \langle CNOT_{ij}; H_i; (x_i \wedge y_j)?\rangle\top \\ &= \langle \beta^{ij}_{xy}?\rangle\top \\ &= dom(\beta^{ij}_{xy}?) \end{aligned}$$

The conclusion then follows from this, together with the Agreement Property. □

Theorem 7. All the above axioms and rules are sound for (quantum frames associated to) n-dimensional Hilbert spaces of the form $H^{\otimes n}$, where H is any two-dimensional Hilbert space.

The problem of obtaining a *complete* proof system for this logic is still open[1].

5. Applications: correctness of quantum programs

As applications to our logic, one can provide *formal correctness proofs* for a whole range of quantum programs; one could claim that *all* quantum circuits and protocols *in which probabilities do not play an essential role* can, in principle, be verified using our logic, or some trivial extension of this logic (obtained by introducing more basic constants for other relevant states and programs). In particular, all the quantum programs covered by the ‘entanglement networks’ approach in Coecke (2004) can be treated in this logic. In his Master’s thesis (Akatov 2005), D. Akatov has applied our logic to the verification of various other protocols, for example, *superdense coding, quantum secret sharing, entanglement swapping, logic gate teleportation, circuits for parallel computation*

[1] However, we have strong reasons to believe the above system is *not* complete. At least one other sound interesting axiom (of particular significance to quantum computing) has been proposed by the first author’s student D. Akatov in his Master’s thesis (Akatov 2005). This is the ‘Determinacy of States’ axiom, which captures the converse of our Entanglement axiom: any entangled state is ‘entangled according to some quantum program’ π (that is, it is of the form $\overline{\pi}_{ij}$); we chose not to include it here, as we have not used it in this paper.

https://doi.org/10.1017/S0960129506005299 Published online by Cambridge University Press

of (sequential) compositions of programs using Bell base measurements. The proofs are modular, using as ingredients the main lemmas proved above: the Compatibility Theorem, the Teleportation Property, the Entanglement Composition Lemma and the Agreement Property. For simplicity, we will only consider two basic examples here: quantum teleportation and quantum secret sharing.

Quantum teleportation

Following Nielsen and Chuang (2000), quantum teleportation is the name of a technique that makes it possible to 'teleport' (that is, move) a quantum state between two agents, even in the absence of a quantum communication channel[1] linking the sender and the recipient. We are working in $H \otimes H \otimes H$, with H being the two-dimensional (qubit) space, so $n = 3$. There are two agents, Alice and Bob, separated in space, each having one qubit of an entangled EPR pair, represented by $\beta_{00}^{2,3} \in H^{(2)} \otimes H^{(3)}$. In addition to her part of the EPR pair, Alice has another qubit 1, in an unknown 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 qubit to Bob, that is, to execute a program that will output a state satisfying $id_{13}(q_1)$. To do this, she entangles the qubit q_1 with her part q_2 of the EPR pair, by performing first a $CNOT_{1,2}$ gate on the two qubits and then a Hadamard transformation H_1 on the first component. Then Alice measures her qubits in the standard basis, thus destroying the entanglement, so that Bob's qubit is left in a separated state q_3. Though this state is unknown, the results of Alice's measurements indicate the actions that Bob will have to perform in order to transfer his qubit from state q_3 into the state $id_{13}(q_1)$ (corresponding to the initial qubit Alice had before the protocol). It is thus 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. To achieve 'teleportation', Bob will have to apply the X-gate y times, then apply the Z gate x times.

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

$$\vdash \pi(q_1 \wedge \beta_{00}^{23}) =_3 id_{13}(q_1)$$

To show this, observe that by applying the above Corollary to Proposition 27, in which we take $i = 1, j = 2, k = 3$, we get that the validity above (to be proved) is equivalent to

$$\vdash (\beta_{xy}^{12}?; X_3^y; Z_3^x)(q_1 \wedge \beta_{00}^{23}) =_3 id_{13}(q_1)$$

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:

$$\vdash (\overline{(Z_1^x; X_1^y)_{12}}?; X_3^y; Z_3^x)(q_1 \wedge \overline{id}_{23}) =_3 id_{13}(q_1),$$

[1] However, note that a *classical* communication channel *is* required!

https://doi.org/10.1017/S0960129506005299 Published online by Cambridge University Press

where $id = Z_1^0; X_1^0$ is the identity. This last validity follows from applying the (corollary of) the Teleportation Property and the validity $Z_1^x; X_1^y; X_1^y; Z_1^x = id$ (due to $X^{-1} = X, Z^{-1} = Z$).

Quantum secret sharing

As described in Gruska (1999), this protocol realises the *splitting of quantum information* into a given number m of 'shares' (among m agents), such that the original information (the 'secret') can be recovered only by pooling together the information in all the shares. The protocol uses GHZ states in a similar way to teleportation. We consider here the case $m = 3$ as an example: suppose Alice, Bob and Charles share a GHZ triple state $\beta_{000}^{2,3,4}$ (each 'having' one of the three entangled qubits, in increasing order: for example, Alice has qubit 2, and so on). In addition, Alice has another qubit 1, in an unknown state q. To split this information q_1 into three shares, Alice measures her two qubits 1 and 2 in the Bell basis, obtaining two bits x, y (corresponding to which of the four Bell states β_{xy}^{12} she obtained). After that, Bob measures his qubit 2 in the dual basis $\{+, -\}$, obtaining another bit $|-\rangle^z$ (with $z \in \{0, 1\}$)[1]. Finally, Charles is given qubit 4, which is now in one of 8 possible states $\psi_4^{(x,y,z)}$ (depending on the results obtained by Alice and Bob).

To recover the original 'secret' q from his qubit $\psi_4^{(x,y,z)}$, Charles can now apply a local unitary transformation $Z_4^z; X_4^y; Z_4^x$. But notice that for this, he needs to know x, y and z, that is, the three agents have to share their information in order to recover q.

The quantum program described here is

$$\pi = \bigcup_{x,y \in \{0,1\}} \beta_{xy}^{12}?; (-)_3^z?; Z_4^z; X_4^y; Z_4^x$$

To prove correctness, we need to show

$$\vdash \pi(q_1 \wedge \beta_{000}^{234}) =_4 id_{14}(q_1)$$

To show this, we use Compatibility and the 3-locality of $(-)_3^z$ to compute

$$\begin{aligned}(\beta_{xy}^{12}?; (-)_3^z?; Z_4^z; X_4^y; Z_4^x)(q_1 \wedge \beta_{000}^{234}) &= ((-)_3^z; \beta_{xy}^{12}?; Z_4^z; X_4^y; Z_4^x)(q_1 \wedge \beta_{000}^{234}) \\ &= (Z_4^z; X_4^y; Z_4^x)(\beta_{xy}^{12}?(q_1 \wedge (-)_3^z?(\beta_{000}^{234})))\end{aligned}$$

But recall that

$$(-)_3^z?(\beta_{000}^{234}) =_{24} \beta_{z0}^{24} =_{24} \overline{Z_1^z}_{24},$$

so we have

$$\begin{aligned}\pi(q_1 \wedge \beta_{000}^{234}) &=_{24} (Z_4^z; X_4^y; Z_4^x)(\beta_{xy}^{12}?(q_1 \wedge \overline{(Z_1^z)}_{24})) \\ &= Z_4^z; X_4^y; Z_4^x)(\overline{(Z_1^x; X_1^y)}_{12}?(q_1 \wedge \overline{(Z_1^z)}_{24}))\end{aligned}$$

[1] Here we use for vectors a similar notation to the notation $(-)^z$ introduced for states in the previous section, that is, $|-\rangle^z := |-\rangle$ for $z = 0$, and $|-\rangle^z := |+\rangle$ for $z = 1$.

https://doi.org/10.1017/S0960129506005299 Published online by Cambridge University Press

Applying the (Corollary of) the Teleportation Property, we get

$$\begin{aligned}
\pi(q_1 \wedge \beta_{000}^{234}) &=_4 (Z_4^z; X_4^y; Z_4^x)((((Z_1^x; X_1^y))_{12}; (Z_1^z)_{24})(q_1)) \\
&= (Z_1^z; X_1^y; Z_1^x)_{14}((Z_1^x; X_1^y; Z_1^z)_{14}(q_1)) \\
&= (Z_1^x; X_1^y; Z_1^z; Z_1^z; X_1^y; Z_1^x)_{14}(q_1) \\
&= id_{14}(q_1)
\end{aligned}$$

Note: This proof can be easily generalised to the case of an m-share split (among m agents) of the secret. See Akatov (2005) for details.

6. Conclusions and future work

We have 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*, and so on. 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 have presented a sound proof system, which can be used to prove many interesting properties of quantum information, including formal correctness proofs for a whole range of quantum protocols (we have treated teleportation and quantum secret sharing here, but there are also many others to be considered, such as superdense coding, entanglement swapping and logic-gate teleportation).

However, a number of open problems remain. While in Baltag and Smets (2005a) 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.

In this paper we have not included *iteration* (Kleene star) π^* among our operations on programs, since it 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 involving *while*-loops. The usual *PDL* axioms for Kleene star are sound, but, again, completeness remains an open problem.

Another problem, which is 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 have ignored 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.

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

Abramsky, S. and Coecke, B. (2005) A Categorical Semantics of Quantum Protocols. To appear in the Proceedings of the 19th IEEE Conference on Logic in Computer Science (LiCS'04). (Also available as arXiv:quant-ph/0402130.)

Akatov, D. (2005) The Logic of Quantum Program Verification. Master's Thesis, Oxford University Computing Laboratory (to appear).

Amemiya, I. and Araki, H. (1967) A Remark on Piron's paper. *Publications of the Research Institute of Mathematical Sciences Kyoto University, series A* **2** 423–427.

Amira, H., Coecke, B. and Stubbe, I. (1998) How Quantales Emerge by Introducing Induction within the Operational Approach. *Helvetica Physica Acta* **71** 554–572.

Baltag, A. (2004) Dynamic and Epistemic Logics for Quantum Measurements. Presented at PML'04, Brussels 2004.

Baltag, A. and Smets, S. (2004) The Logic of Quantum Programs. In: Selinger, P. (ed.) Proceedings of QPL2004 (LICS'04 Workshop), *TUCS General Publication* **33**, Turku Center for Computer Science 39–56.

Baltag, A. and Smets, S. (2005a) Complete Axiomatizations for Quantum Actions. Proceedings of IQSA'04. *International Journal of Theoretical Physics* (to appear).

Baltag, A. and Smets, S. (2005b) What can Logic learn from Quantum Mechanics? Presented at the Workshop on 'Quantum Information: Epistemological and Logic Lessons' of ECAP'05, Lisbon, Portugal.

Beltrametti, E. G. and Cassinelli, G. (1977) On State Transformations Induced by Yes-No Experiments, in the Context of Quantum Logic. *Journal of Philosophical Logic* **6** 369–379

Brunet, O. and Jorrand, P. (2003) Dynamic Quantum Logic for Quantum Programs. Available as arXiv:quant-ph/0311143

Coecke, B. (2000) Structural Characterization of Compoundness. *International Journal of Theoretical Physics* **39** 585–594.

Coecke, B. (2004) The Logic of Entanglement. arXiv: quant-ph/0402014.

Coecke, B., Moore, D. J. and Smets, S. (2004) Logic of Dynamics & Dynamics of Logic; Some Paradigm Examples. In: Rahman, S., Symons, J., Gabbay, D. M. and van Bendegem, J. P. (eds.) *Logic, Epistemology and the Unity of Science.*

Coecke, B., Moore, D. J. and Stubbe, I. (2001) Quantaloids describing Causation and Propagation for Physical Properties. *Foundations of Physics Letters* **14** 357–367. (Also available as arXiv: quant-ph/0009100.)

Coecke, B. and Smets, S. (2004) 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* **43**(7–8) 1705–1736. (Also available as arXiv: quant-ph/0111076.)

Coecke, B. and Stubbe, I. (1999) On a Duality of Quantales Emerging from an Operational Resolution. *International Journal of Theoretical Physics* **38** 3269–3281.

Dalla Chiara, M. L. and Giuntini, R. (2002) Quantum Logics. In: Gabbay, D. M. and Guenthner, F. (eds.) *Handbook of Philosophical Logic* **6**, second edition, Kluwer 129–228.

Dalla Chiara, M. L., Guintini, R. and Greechie, R. (2004) *Reasoning in Quantum Theory*, Kluwer.

Daniel, W. (1982) On the Non-Unitary Evolution of Quantum Systems. *Helvetica Physica Acta* **55** 330–338.

Daniel, W. (1989) Axiomatic Description of Irreversible and Reversible Evolution of a Physical System. *Helvetica Physica Acta* **62** 941–968.

Faure, C. A., Moore, D. J. and Piron, C. (1995) Deterministic Evolutions and Schrodinger Flows. *Helvetica Physica Acta* **68** 150–157.

Goldblatt, R. (1984) Orthomodularity is not elementary. *The Journal of Symbolic Logic* **49** 401–404.

Goldblatt, R. (1974) Semantic Analysis of Orthologic. *Journal of Philosophical Logic* **3** 19–35.

Gruska, J. (1999) *Quantum Computing*, McGraw-Hill, London.

Hardegree, G. M. (1975) Stalnaker Conditional and Quantum Logic. *Journal of Philosophical Logic* **4** 399–421.

Hardegree, G. M. (1979) The Conditional in Abstract and Concrete Quantum Logic. In: Hooker, C. A. (ed.) *The Logico-Algebraic Approach to Quantum Mechanics* **2**, Reidel.

Harel, D., Kozen, D. and Tiuryn, J. (2000) *Dynamic Logic*, MIT Press.

Jauch, J. M. (1968) *Foundations of Quantum Mechanics*, Addison-Wesley.

Jauch, J. M. and Piron, C. (1969) On the Structure of Quantal Proposition Systems. *Helvetica Physica Acta* **42** 842–848.

Mateus, P. and Sernadas, A. (2004) Reasoning about Quantum Systems. In: Alferes, J. and Leite, J. (eds.) *Springer-Verlag Lecture Notes in Artificial Intelligence* **3229** 239–251.

Mayet, R. (1998) Some Characterizations of the Underlying Division Ring of a Hilbert Lattice by Automorphisms. *International Journal of Theoretical Physics* **37** (1) 109–114.

Nielsen, M. and Chuang, I. L. (2000) *Quantum Computation and Quantum Information*, Cambridge University Press.

Piron, C. (1964) Axiomatique quantique (Ph.D. Thesis). *Helvetica Physica Acta* **37** 439–468. (English translation by Cole, M. *Quantum Axiomatics*, RB4 Technical memo 107/106/104, GPO Engineering Department, London).

Piron, C. (1976) *Foundations of Quantum Physics*, W. A. Benjamin.

Smets, S. (2001) On Causation and a Counterfactual in Quantum Logic: the Sasaki Hook. *Logique et Analyse* **173-175** 307–325.

Smets, S. (2004) On Quantum Propositional Dynamic Logic. Presented at PML'04, Brussels 2004.

Smets, S. (2005) From Intuitionistic Logic to Dynamic Operational Quantum Logic. *Poznan Studies in Philosophy and the Humanities* (to appear).

Solèr, M. P. (1995) Characterization of Hilbert spaces by orthomodular spaces. *Communications in Algebra* **23** (1) 219–243.