Soft Comput (2017) 21:1421–1441
DOI 10.1007/s00500-015-1802-6

FOCUS

Deriving the correctness of quantum protocols in the probabilistic logic for quantum programs

Jort Martinus Bergfeld[1] · **Joshua Sack**[2]

Published online: 20 August 2015

Abstract This paper presents a sound axiomatization for a probabilistic modal dynamic logic of quantum programs. The logic can express whether a state is separable or entangled, information that is local to a subsystem of the whole quantum system, and the probability of positive answers to quantum tests of certain properties. The power of this axiomatization is demonstrated with proofs of properties concerning bases of a finite-dimensional Hilbert space, composite systems, entangled and separable states, and with proofs of the correctness of two probabilistic quantum protocols (the quantum leader election protocol and the BB84 quantum key distribution protocol).

Keywords Probability · Quantum logic · Axiomatization · Quantum computation · Quantum protocols

Communicated by M. L. Dalla Chiara, R. Giuntini, E. Negri and S. Smets.

The research of these authors has been made possible by VIDI Grant 639.072.904 of the Netherlands Organization for Scientific Research (NWO).

✉ Jort Martinus Bergfeld
Jort.Bergfeld@gmail.com

Joshua Sack
joshua.sack@gmail.com

[1] Institute for Logic, Language and Computation (ILLC), University of Amsterdam, P.O. Box 94242, 1090 GE Amsterdam, The Netherlands

[2] Department of Mathematics and Statistics, California State University, Long Beach, 1250 Bellflower Blvd, Long Beach, CA 90840, USA

1 Introduction

There is a large literature on logics for classical computation. These include Hoare logic (1969), propositional dynamic logic (Fischer and Ladner 1979), other dynamic logics (Harel et al. 2000), and temporal logics (Hodkinson and Reynolds 2007), and they aid in proving correctness of protocols and programs. With the increased prospects of quantum devices and computers, there is a growing interest in quantum analogs for these logics.

Quantum logic, which was originally used to clarify properties of quantum physics (Birkhoff and Neumann 1936), has developed into a broader field, with many logics addressing algebraic structures of quantum systems (Dalla Chiara and Giuntini 2002; Dalla Chiara et al. 2004). A significant recent development is the strengthening of quantum logic to be able to address quantum computation as well (Dunn et al. 2013). This coincides with development to formalize the semantics of quantum programs (D'Hondt and Panangaden 2006b) and the development of model checkers and verification tools for quantum systems (Gay et al. 2008; Feng et al. 2013; Ying et al. 2013).

Recent work toward the development of quantum logics for computation yielded probabilistic dynamic quantum logics that are decidable, such as Baltag et al. (2013, 2014), and the correctness of many quantum protocols can be expressed in these languages. However, an axiomatization of these probabilistic systems is lacking. In the non-probabilistic setting, a sound axiomatization relevant to our work was developed in Baltag and Smets (2006) for the *Logic of Quantum Programs*, a quantum analog of the propositional dynamic logic, which was used to prove the correctness of the quantum teleportation protocol and the quantum secret sharing protocol. But the logic of quantum programs could not express quantities, and could only

account for the correctness of qualitative properties of algorithms and protocols considered, and that work considered a probabilistic extension to be a greater goal of the program.

This paper lays a foundation for an axiomatization for a probabilistic variant of the Logic of Quantum Programs. The language involves dynamic modalities for quantum programs as well as probabilistic modalities, and is similar to the decidable logic in Baltag et al. (2014), and hence we give it the same name: the *Probabilistic Logic of Quantum Programs*. Among the differences between our language here and the one in Baltag et al. (2014) is that our language here simplifies the formulas for locality to describing full separability with respect to a given set of components. This simplification of the language allows us to highlight basic properties in the proof system that are essential to properties of bases of a finite-dimensional Hilbert space. We develop a sound proof system for this logic, and we use it to prove properties of the quantum leader election protocol of D'Hondt and Panangaden (2006a) and the BB84 quantum key distribution protocol (Bennett and Brassard 1984, 2014).

The quantum leader election protocol is a method for selecting exactly one of n many members, giving each member equal chance of being selected. This is analogous to establishing a fair n-sided die, and such selections are important for distributive systems. We prove in our language the existence and correctness of the W-state as a shared state whose measurement would select a leader with the correct probability. The BB84 quantum key distribution protocol is a secure distribution key protocol. We prove in our language the correctness of this protocol in the event that there is no eavesdropping of communication. These two protocols are just examples of what our system can prove, and we are sure there are many others. But our logic also lays a foundation for further development in axiomatizing logics for quantum systems, particularly those that involve probability.

There have been other developments in forming axiomatizations of quantum logics. Goldblatt (1974), developed a complete axiomatization of orthologic and orthomodular quantum logic. There has also been development of Gentzen style proof systems for orthologic (Nishimura 2009). Selinger (2007), uses a graphical language to axiomatize properties for dagger compact closed categories, and shows in Selinger (2011, 2012) that this axiomatic system is also complete with respect to finite-dimensional Hilbert spaces. Abramsky and Bob (2009), use a diagrammatic axiomatization to prove the correctness of quantum teleportation, logic gate teleportation, and entanglement swapping protocols. An axiomatization of a quantum logic that involve probabilities is given in Mateus and Sernadas (2006). Our logic differs from these in that it builds on the work of Baltag and Smets (2006) and Baltag et al. (2014), and can be viewed as a probabilistic quantum analog of propositional dynamic logic.

Our paper is organized as follows. In Sect. 2, we introduce probabilistic quantum structures, the basic structures for our semantics, which are mild abstractions of Hilbert spaces. In Sect. 3, we introduce the syntax and semantics for our probabilistic logic of quantum programs. We then present in Sect. 4 the deductive system and prove some properties in the language from it, including properties concerning orthonormal bases. In Sect. 5, we prove the correctness of the quantum leader election protocol and the BB84 protocol.

2 Probabilistic quantum structure

Let $\mathcal{H}$ be a finite-dimensional Hilbert space with an orthonormal basis $\mathbf{B} = (\mathbf{b}_0, \ldots, \mathbf{b}_{n-1})$. Let $V_{\mathbf{B}}$ denote the set of all functions $f : \mathbf{B} \to \mathbb{C}$. It is well known that there is a bijective correspondence between the vectors in $\mathcal{H}$ and the elements of $V_{\mathbf{B}}$ given by mapping every $\mathbf{v}$ in $\mathcal{H}$ to the function $\mathbf{b}_i \mapsto \langle \mathbf{v}, \mathbf{b}_i \rangle$. A *state* of $\mathcal{H}$ is a one-dimensional subspace s of $\mathcal{H}$. We represent the states of $\mathcal{H}$ by a subset of $V_{\mathbf{B}}$, each representing a canonical representative of the one-dimensional subspace. This subset is the set of complex probability mass function defined as follows.

Definition 2.1 (*Complex probability mass functions*) Let $B = \{b_i \mid 0 \leq i < n\}$ for some positive $n \in \mathbb{N}$ be an ordered set (which we call an *ordered basis*). A function $f : B \to \mathbb{C}$ is called a *complex probability mass function* on B if

1. there exists an $i \in n$ such that
   (a) $f(b_j) = 0$ for all $j < i$, and
   (b) $f(b_i) \in (0, 1]$,
2. $|f(b_i)|^2 \in [0, 1]$, and
3. $\sum_{i \in N} |f(b_i)|^2 = 1$.

Let S_B denote the set of all complex probability mass functions on B.

Note that if f is a complex probability mass function, the function $f^2 : B \to [0, 1]$ is a (real) probability mass function. In this sense, a complex probability mass function can be seen as an appropriate "square root" of a probability mass function.

Every function $f \in V_B$ can be converted into a function S_B as follows.

Definition 2.2 (*Strong normalization*) For every nonzero function $f : \mathbf{B} \to \mathbb{C}$, where $c = f(\mathbf{b}_i)$ for the smallest i such that $f(\mathbf{b}_i) \neq 0$, we define the *strong normalization* $\mathsf{sn}(f)$ of f by

$$\mathsf{sn}(f) : \mathbf{b} \mapsto \frac{\overline{c}}{\sqrt{\sum_i |\overline{c} \cdot f(\mathbf{b}_i)|^2}} f(\mathbf{b}),$$

where in general $\overline{z}$ is the complex conjugate of z.

It is easy to see that the strong normalization transforms any nonzero function $f : \mathbf{B} \to \mathbb{C}$ into a complex probability mass function. The set of complex probability mass functions is identified with the set of states of a Hilbert spaces by the following proposition.

Proposition 2.3 *Let $\mathcal{H}$ be a Hilbert space with $\mathbf{B} = \{\mathbf{b_0}, \ldots, \mathbf{b_{n-1}}\}$ an ordered orthonormal basis. The following both hold.*

1. *Given a complex probability mass function $f : \mathbf{B} \to \mathbb{C}$, there exists a unique unit vector $\mathbf{v}$ in $\mathcal{H}$, such that for each j, $f(\mathbf{b_j}) = \langle \mathbf{v}, \mathbf{b_j} \rangle$.*
2. *Given any state s of $\mathcal{H}$, there is a* unique *unit vector $\mathbf{v}$ in s, such that the function $f_\mathbf{v} = \langle \mathbf{v}, \cdot \rangle : \mathbf{B} \to \mathbb{C}$ is a complex probability mass function over the ordered orthonormal basis $\mathbf{B}$.*

Proof 1. Given $f \in S_\mathbf{B}$, we define the vector $\mathbf{v}$ to be

$$\mathbf{v} = \sum_{j \in n} f(\mathbf{b_j}) \mathbf{b_j}.$$

Since the basis $\mathbf{B}$ is orthonormal, it is easy to see that $f(\mathbf{b_j}) = \langle \mathbf{v}, \mathbf{b_j} \rangle$. By condition 3 of the definition of a complex probability mass function, $\mathbf{v}$ is a unit vector.

2. Let s be a one-dimensional subspace of $\mathcal{H}$, and let $\mathbf{w}$ be any nonzero vector in s. We identify $\mathbf{w}$ with a nonzero function in $f_\mathbf{w} \in V_\mathbf{B}$. Let $\mathbf{v}$ be a vector corresponding to $\mathsf{sn}(f_\mathbf{w})$. As $\mathbf{v}$ only differs from $\mathbf{w}$ by a constant multiple, $\mathbf{v} \in s$. Furthermore, as $\mathsf{sn}(f_\mathbf{w})$ is a complex probability mass function, $\mathbf{v}$ is a unit vector. To see that $\mathbf{v}$ is unique, we observe that for any complex number $c \neq 1$ and any complex probability mass function f, the function $c \cdot f : \mathbf{b} \mapsto c \cdot f(\mathbf{b})$ is not a complex probability mass function. □

Because every state can be represented by a complex probability mass function, we will use the term *state* to mean either a one-dimensional subspace or a complex probability mass function. We will also use the same notation for both concepts. Also, throughout this paper, we will identify each natural number $n \in \mathbb{N} := \{0, 1, 2, \ldots\}$ with the set $\{0, 1, \ldots, n-1\}$ of elements preceding it. If we write $i < N$ without a lower bound, we intend for i to range from $i = 0$ to $i = N - 1$.

2.1 Maps between bases and states

We require the basis to be ordered so that we can have a canonical representation of each state via a vector representative of its one-dimensional subspace (for the same reason, vectors are written as ordered tuples, also assuming an order to its basis). Were we to reorder the basis elements, we could then map each vector representative in the original ordering to its unique corresponding representative in the new order (this mapping is, in this context, an identity map on states). This concept is generalized to change-of-basis maps as follows.

Definition 2.4 (*Change-of-basis isomorphism*) Let $B = \{b_i \mid i < d_B\}$ and $C = \{c_i \mid i < d_C\}$ be two ordered basis (where C could be a reordering of B). A function $h : S_B \to S_C$ is a *change-of-basis isomorphism* iff there is a bijection $\eta : C \to B$ (which implies $d_B = d_C$) such that for all $s \in S_B$ and for all $i < d_C$

$$h(s)(c_i) = \mathsf{sn}(s \circ \eta)(c_i).$$

We call h an *order isomorphism* if in addition $\eta(c_i) = b_i$ for all $i < d_C$. We write $B \cong C$ and $S_B \cong S_C$ if there is an order isomorphism between S_B and S_C. We write $s \cong t$ for $s \in S_B$ and $t \in S_C$ if there is an order isomorphism $h : S_B \to S_C$, such that $h(s) = t$.

The tensor product of two ordered bases is the Cartesian product of the elements ordered by the dictionary order.

Definition 2.5 (*Tensor product*) The *tensor product* of two ordered bases $B = (b_0, \ldots, b_{n-1})$ and $C = (c_0, \ldots, c_{m-1})$ is $D = (d_0, \ldots, d_{nm-1})$, such that $d_k = (b_i, c_j)$ where $i = \lfloor k/m \rfloor$ and $j = k \mod m$. The tensor product of $s \in S_B$ and $t \in S_C$, denoted $s \otimes t$, is given by

$$(s \otimes t)(b_i, c_j) = s(b_i) \cdot t(c_j).$$

It is easy to see that in general $(s \otimes t) \otimes r \cong s \otimes (t \otimes r)$. As the tensor product is associative given our strictest notion of isomorphism, we will ignore internal parentheses when taking tensor products of more than two bases.

2.2 Agents and separability

Definition 2.6 (*Multi-agent PQM and components*) Let $N = \{0, \ldots, N-1\}$ be a finite set of agents. An *N-probabilistic quantum model* (*N-PQM*) is a tuple $\mathfrak{M} = (B_0, \ldots, B_{N-1})$ of ordered bases. Let $I \subseteq N$. Then $\mathfrak{M}_I := \{B_i \mid i \in I\}$ is said to be a *component* of $\mathfrak{M}$.

If $I = \{x_1, \ldots, x_m\} \subseteq N$ for some $m < N$ (where (x_i) is strictly increasing), we write $\bigotimes \mathfrak{M}_I = B_{x_1} \otimes B_{x_2} \otimes \cdots \otimes B_{x_m}$.

We write $S_I^{\mathfrak{M}}$ (or S_I if $\mathfrak{M}$ is understood from context) for $S_{\bigotimes \mathfrak{M}_I}$, and S (or $S^{\mathfrak{M}}$) for S_N (or $S_N^{\mathfrak{M}}$). In what follows, given a finite ordered set $J = \{x_1, \ldots, x_m\}$ for some $m < N$ (with the sequence (x_i) being strictly increasing), we use the notation $(b_i)_{i\in J}$ for the tuple $(b_{x_1}, \ldots, b_{x_m})$.

Definition 2.7 (*Tensor product of agent components*) Let $\mathfrak{M} = (B_0, \ldots, B_{N-1})$ be an N-PQM, and let $I, J \subseteq N$, such that $I \cap J = \emptyset$. The $\mathfrak{M}$-*tensor product* $\mathfrak{M}_I \otimes^{\mathfrak{M}} \mathfrak{M}_J$ is defined to be $\mathfrak{M}_{I\cup J}$, but where for each $s \in S_I$ and $t \in S_J$, we have for each sequence (x_i) with $b_{x_i} \in B_i$ that

$$\left(s \otimes^{\mathfrak{M}} t\right)((b_{x_i})_{i\in I\cup J}) = s((b_{x_i})_{i\in I}) \cdot t((b_{x_i})_{i\in J}).$$

Give sets $X \subseteq S_I$ and $Y \subseteq S_J$, let $X \otimes^{\mathfrak{M}} Y := \{x \otimes^{\mathfrak{M}} y \mid x \in X, y \in Y\}$.

Note that although $\otimes$ is not commutative, $\otimes^{\mathfrak{M}}$ is. Also note that $\otimes^{\mathfrak{M}}$ is associative; hence we generally omit parentheses.

Definition 2.8 (*Separable and entangled states*) Given an N-PQM $\mathfrak{M}$, a set $J \subseteq N$, a partition $\Pi = \{X_1, \ldots, X_k\}$ of N, and a state $s \in S^{\mathfrak{M}}$, we say than

- s is $\mathfrak{M}$-*separable in* J if there exist $s_J \in S_J$ and $s_{N\setminus J} \in S_{N\setminus J}$ such that $s \cong s_J \otimes^{\mathfrak{M}} s_{N\setminus J}$. If s is not $\mathfrak{M}$-separable in J we say that s is $\mathfrak{M}$-*entangled in* J.
- s is $\mathfrak{M}$-*separable in* Π if there exists $s_i \in S_{X_i}$ such that $s \cong s_1 \otimes^{\mathfrak{M}} \cdots \otimes^{\mathfrak{M}} s_k$. If s is not $\mathfrak{M}$-separable in Π we say that s is $\mathfrak{M}$-*entangled in* Π. If $\mathfrak{M}$ is separable in $\{\{i\} \mid i \in N\}$, we say $\mathfrak{M}$ is *fully separable*.

Separability will play an important role in the semantics of the logic we define in the next section.

3 Probabilistic quantum logic

In this section, we define the syntax and semantics of our language, and provide some useful syntactic abbreviations.

3.1 Syntax

Let N be a set of agents and let Prop be a (countable) set of proposition letters denoted with $p, q, \ldots$. The language is three-sorted, with formulas ϕ, programs α, and probability terms t, and is defined by

$$\begin{aligned}
\phi &::= p \mid \neg\phi \mid \phi \wedge \phi \mid [\alpha]\phi \mid \\
&\qquad \mathsf{Atom}(\phi) \mid \mathsf{Sep}(\phi) \mid \phi_I \mid t \geq \rho \\
\alpha &::= \phi? \mid \alpha \cup \alpha \mid \alpha; \alpha \\
t &::= \rho \Pr(\phi) \mid t + t
\end{aligned}$$

where $p \in \text{Prop}$, $I \subseteq N$, $\Pi \subset \mathcal{P}(N)$ is a partition of N, and $\rho \in \mathbb{Q}$. The set of formulas ϕ is denoted by $\mathcal{L}_N$, and the set of terms t is denoted by Terms.

We have the standard logical connectives $\neg\phi$, $\phi \wedge \psi$ and $[\alpha]\phi$ with the meaning *not* ϕ, ϕ *and* ψ and *after any successful execution of program* α, ϕ *holds* respectively.

Here the programs α are $\phi?$, *a quantum test whether or not* ϕ *holds*; $\alpha \cup \beta$, *an arbitrary choice between two programs* α *and* β; and $\alpha; \beta$, *the sequential execution of two programs* α *and* β.

We also have three nonstandard, but useful connectives. $\mathsf{Atom}(\phi)$ intuitively means that ϕ *is only true at one and only one state*. $\mathsf{Sep}(\phi)$ means intuitively that all states making ϕ true *are separable into each agent*, that is, these states are of the form $\bigotimes_{i<N}^{\mathfrak{M}} s_{\{i\}}$ for some $s_{\{i\}} \in S_{\{i\}}$ for each $i < N$. ϕ_I intuitively represents *the information that the local system* I *has about* ϕ , that is, if any measurement that can be performed within the local system I cannot refute ϕ, then ϕ_I true.

Lastly, we have $t \geq \rho$, which intuitively means *the probability of* t *is greater than or equal to* ρ. Here t is a linear combination of $\Pr(\phi)$, the *probability that a test for* ϕ *is successful*.

We have chosen the language to express several examples in the simplest way. However, one could easily imagine ways to extend the expressibility of this language. For example, we could extend this language with unitary operators $\alpha ::= U \mid U^\dagger$; however, we do not use these operators in the examples we discuss.

3.2 Semantics

The semantics is defined with respect to an N-PQM $\mathfrak{M}$. We will make use of the following concepts. We first observe that from just an ordered basis $B = \{b_0, \ldots, b_{n-1}\}$ we can recover the Hilbert space structure, such as the inner product, as follows. For any two states $s, t \in S_B$, we define the *inner product* of s and t to be

$$\langle s, t\rangle := \sum_{i=0}^{n-1} \overline{s(b_i)}\, t(b_i) \tag{3.1}$$

where in general $\overline{z}$ is the complex conjugate of z. Then $R := \{(s, t) \mid \langle s, t\rangle \neq 0\}$ relates any two states that are non-orthogonal. We define the orthocomplement of a set of states X by

$$\sim X := \{s \in S \mid (s, x) \notin R \text{ for all } x \in X\}$$

and let $\mathcal{T} := \{P \subseteq S \mid P = \sim\sim P\}$ be the set of *testable properties*. For each $P \in \mathcal{T}$, we then let

$$R_P := \left\{ (s,t) \in S^2 \,\middle|\, \begin{array}{l} t \in P \text{ and } |\langle s,u\rangle|^2 < |\langle s,t\rangle|^2 \\ \text{for all } u \in P\backslash\{t\} \end{array} \right\}.$$

Note that each $P \in \mathcal{T}$ corresponds to a linear closed subspace in a Hilbert space and that the relation R_P in fact corresponds to the projection onto the subspace P.

It is easy to see that each singleton is testable, and hence that $R = \bigcup_{P\in\mathcal{T}} R_P$. Given an N-PQM $\mathfrak{M}$ with carrier set $S = S_{\bigotimes \mathfrak{M}}$ and a valuation $V : \mathrm{Prop} \to \mathcal{P}S$, we interpret formulas by a function $[\![\cdot]\!]^{\mathfrak{M}} : \mathcal{L}_N \to \mathcal{P}S$, we interpret each program α by a relation $R_\alpha^{\mathfrak{M}} \subseteq S \times S$, and we interpret probability terms by a family of functions $[\![\cdot]\!]_s^{\mathfrak{M}} : \mathrm{Terms} \to \mathbb{R}$ for each $s \in S$ as follows (we typically omit the superscript when it is understood by context). To interpret formulas ϕ:

$$\begin{aligned}
[\![p]\!] &:= V(p), \\
[\![\neg\phi]\!] &:= S\backslash[\![\phi]\!], \\
[\![\phi \wedge \psi]\!] &:= [\![\phi]\!] \cap [\![\psi]\!], \\
[\![[\alpha]\phi]\!] &:= \{s \in S \mid R_\alpha(s) \subseteq [\![\phi]\!]\}, \\
[\![\mathsf{Atom}(\phi)]\!] &:= \begin{cases} S & \text{if } [\![\phi]\!] = \{s\} \text{ for some } s \in S, \\ \emptyset & \text{otherwise,} \end{cases} \\
[\![\mathsf{Sep}(\phi)]\!] &:= \begin{cases} S & \text{if } [\![\phi]\!] \subseteq \{s \in S \mid s = \bigotimes_{i\in N}^{\mathfrak{M}} s_{\{i\}}\}, \\ \emptyset & \text{otherwise,} \end{cases} \\
[\![\phi_I]\!] &:= \left\{ s_I \otimes^{\mathfrak{M}} s_{N\backslash I} \,\middle|\, \begin{array}{l} (s_I \otimes^{\mathfrak{M}} t_{N\backslash I}) \in [\![\phi]\!] \\ \text{for some } t_{N\backslash I} \end{array} \right\}, \\
[\![t \geq \rho]\!] &:= \{s \in S \mid [\![t]\!]_s \geq \rho\}.
\end{aligned}$$

To interpret programs α:

$$\begin{aligned}
R_{\phi?} &:= R_P, \text{ where } P = {\sim}{\sim}[\![\phi]\!], \\
R_{\alpha\cup\beta} &:= R_\alpha \cup R_\beta, \\
R_{\alpha;\beta} &:= R_\alpha ; R_\beta.
\end{aligned}$$

To interpret terms t:

$$\begin{aligned}
[\![\rho\,\Pr(\phi)]\!]_s &:= \rho \sum_{t\in R_P(s)} |\langle s,t\rangle|^2, \text{ where } P = {\sim}{\sim}[\![\phi]\!], \\
[\![t_1 + t_2]\!]_s &:= [\![t_1]\!]_s + [\![t_2]\!]_s.
\end{aligned}$$

3.3 Abbreviations

With this language, we can express many notions in quantum mechanics. Some are so important and natural to use, we introduce abbreviations for them (Table 1). We have the standard abbreviations $\mathtt{tt}$, $\mathtt{ff}$ and $\vee$. Note that if $[\neg\phi?]\mathtt{ff}$ holds in a state s, then any test from s will result in a state with property ϕ, or equivalently, any non-orthogonal state has property ϕ. We abbreviate $[\neg\phi?]\mathtt{ff}$ using $\Box\phi$, where $\Box$ can be viewed as the modal operator for the non-orthogonality relation R. We abbreviate ${\sim}\phi$ by $\Box\neg\phi$ for the following reason. The orthocomplement of ϕ, denoted by ${\sim}\phi$, is true at any state s that is orthogonal to the set of states that make ϕ true. Equivalently, every state that makes ϕ true is orthogonal to s, and hence every state non-orthogonal to s makes $\neg\phi$ true. This means that $\Box\neg\phi$ is true at s. With the orthocomplement, we can also define the quantum join: $\phi \sqcup \psi := {\sim}({\sim}\phi \wedge {\sim}\psi)$. The quantum join $\phi \sqcup \psi$ can be thought of as the smallest testable property containing ϕ and ψ.

Table 1 Abbreviations for formulas

$\mathtt{ff}$	$:= p \wedge \neg p$
$\mathtt{tt}$	$:= \neg\mathtt{ff}$
$\langle\alpha\rangle\phi$	$:= \neg[\alpha]\neg\phi$
$\Box\phi$	$:= [\neg\phi?]\mathtt{ff}$
$\Diamond\phi$	$:= \neg\Box\neg\phi$
${\sim}\phi$	$:= \Box\neg\phi$
$\phi \vee \psi$	$:= \neg(\neg\phi \wedge \neg\psi)$
$\phi \sqcup \psi$	$:= {\sim}({\sim}\phi \wedge {\sim}\psi)$
$\forall\phi$	$:= \Box\Box\phi$
$\exists\phi$	$:= \Diamond\Diamond\phi$
$(\phi \leq \psi)$	$:= \forall(\phi \to \psi)$
$(\phi \equiv \psi)$	$:= \forall(\phi \leftrightarrow \psi)$
$\phi \perp \psi$	$:= \phi \leq {\sim}\psi$
$T(\phi)$	$:= {\sim}{\sim}\phi \equiv \phi$
$I(\phi)$	$:= (\phi \equiv \phi_I)$

Our quantum models satisfy the superposition principle: every state can reach any other state in two non-orthogonal steps, that is $R; R = S \times S$. This gives us the power to express that a formula is valid in a model: $\forall\phi := \Box\Box\phi$ is true at a state iff ϕ is true at every state in the model. With this global modality, we can express many relations between formulas that are globally true, such as inequality: $(\phi \leq \psi) := \forall(\phi \to \psi)$, equality: $(\phi \equiv \psi) := \forall(\phi \leftrightarrow \psi)$, and orthogonal formulas: $(\phi \perp \psi) := (\phi \leq {\sim}\psi)$.

As can be seen from the definition of the semantics, the logical operators for probability $\Pr(\phi)$ and for tests $\phi?$ are only meaningful if the formula ϕ is testable. Noting that every testable property is closed under taking double orthocomplement, we can express testability by $T(\phi) := (\phi \equiv {\sim}{\sim}\phi)$.

Similarly, in a multi-agent setting, the formula ϕ must be separable in I for ϕ_I to represent the information I has about ϕ (that is, *I's local state*). We say that ϕ is *I-local* if $I(\phi) := (\phi \equiv \phi_I)$, that is, the truth of ϕ is fully determined by the local state of I.

In Table 2, we have abbreviations concerning probabilities. All but the last two are standard abbreviations for terms and pure probabilistic formulas taken from (Fagin et al. 1990, p. 83). Concerning the last two, we are often interested in the probability of successfully testing ϕ as well as the outcome

Table 2 Probabilistic abbreviations

$\sum_{k=1}^{n} a_k \Pr(\phi_k)$	$:= a_1 \Pr(\phi_1) + \cdots + a_n \Pr(\phi_n)$
$\rho \sum_{k=1}^{n} a_k \Pr(\phi_k)$	$:= \sum_{k=1}^{n} \rho a_k \Pr(\phi_k)$
$t < \rho$	$:= \neg(t \geq \rho)$
$t_1 \geq t_2$	$:= t_2 - t_1 \geq 0$
$t \leq \rho$	$:= -t \geq -\rho$
$t = \rho$	$:= t \geq \rho \wedge t \leq \rho$
$t_1 \geq t_2$	$:= t_1 - t_2 \geq 0$
$t_1 = t_2$	$:= t_1 - t_2 = 0$
$\langle \phi ? \rangle_{=\rho} \psi$	$:= \Pr(\phi) = \rho \wedge \langle \phi ? \rangle \psi$
$\langle \phi ? \rangle_{>\rho} \psi$	$:= \Pr(\phi) > \rho \wedge \langle \phi ? \rangle \psi$

Table 3 Rules

MP	$\frac{\phi \quad \phi \to \psi}{\psi}$ (modus ponens)
Nec	$\frac{\phi}{[\alpha]\phi}$ (necessitation)
US	$\frac{\phi}{\phi^\sigma}$ for some $\sigma : \mathrm{Prop} \to \mathcal{L}_N$ (substitution)

of a successful test. We abbreviate this with the formulas $\langle \phi ? \rangle_{=\rho} \psi$ and $\langle \phi ? \rangle_{>\rho} \psi$.

4 Deductive system

Our deductive proof system contains three rules (Table 3), where ϕ^σ is obtained from ϕ by replacing all occurrences of p with $\sigma(p)$, and a list of axioms (Table 4), divided into the following five categories: standard propositional dynamic logic axioms, standard axioms about linear inequalities, basic axioms for quantum systems, probabilistic axioms for quantum systems and axioms for quantum systems concerning atoms and separability.

A proof for ϕ is a finite sequence of formulas, such that the last formula is ϕ and every formula is either an axiom listed below or obtained by applying an inference rule to (a) formula(s) appearing earlier in the sequence.

The three rules in Table 3 are standard, but we can deduce some nonstandard rules concerning the abbreviations $\forall$, $\leq$, $\equiv$ and $T(\cdot)$, which will be given in Lemma 4.3.

The axioms for programs and for linear inequalities are standard, so we will only discuss the axioms in the last three categories.

Basic axioms for quantum systems The first axiom Q1 states that equivalent formulas have equivalent tests. The second axiom Q2 expresses our design that when we test for a formula ϕ we actually test for the smallest closed linear subset containing $[\![\phi]\!]$, that is $\sim\!\sim\phi$.

For the axioms Q3 to Q9 one should remember that $\Box$ corresponds to the non-orthogonality relation and $[p?]$ corresponds to the projection onto P, where $P = \sim\!\sim[\![p]\!]$.

Axiom Q3 is related to the superposition principle, which is the principle that for every two states there is a third state that is non-orthogonal to both of them (or any two states can reach each other by two non-orthogonal steps).

Axiom Q4 states that if a successful test for p results in a state satisfying q, then the state is non-orthogonal to $[\![q]\!]$, so we can successfully test for q. Axiom Q5 corresponds to the fact that each projection is a partial function.

A successful test for a testable property P always results in a state inside P. When inquiring about a property Q that is not testable, our framework tests for the smallest testable property containing Q. Axiom Q6 corresponds to these facts, where $\sim\!\sim p$ corresponds to the smallest testable property containing p.

If $s \in P$, then the projection is reflexive on s, that is, $(s, s) \in R_P$. So if a state makes p true, a successful test for p always ends up in the same state. This is captured by axiom Q7.

Axiom Q8 corresponds to the self-adjointness of projections with respect to the inner product, that is,

$$\langle \mathrm{Proj}_P(s), t \rangle = \langle s, \mathrm{Proj}_P(t) \rangle,$$

where $\mathrm{Proj}_P(s)$ is the projection of vector s onto the space P ($s R_P t$ where $t = \mathsf{sn}(\mathrm{Proj}_P(s))$). In non-probabilistic terms, this means that if the projection of s onto P is non-orthogonal to a state t, then the projection of t onto P is non-orthogonal to s.

The projection t of a state s onto P should be the closest state to s that is inside P. This can be expressed by: $(s, t) \in R_P$ iff for all $u \in P$ we have uRs iff uRt. This statement is partially captured by axiom Q9: looking at the right-to-left part of the biconditional, if a state s is non-orthogonal to a state satisfying p, and if all states satisfying p that are non-orthogonal to s are also non-orthogonal to a state satisfying $p \wedge q$, then the property $p \wedge q$ is "close to s", and a successful test for p at state s results in a state that satisfies q.

Probabilistic axioms for quantum systems Axiom P1 and P2 are standard probability axioms ensuring the probability values are in the interval [0, 1]. Axiom P3 establishes the correspondence between orthogonality and zero probability.

Equivalent formulas should have equal probabilities, which is captured by axiom P4. Normally we can add the probabilities of disjoint sets, but in quantum systems we need the sets to be orthogonal. This is stated by axiom P5.

Axiom P6 is the probabilistic version of the superposition statement. If p and q are orthogonal we can superpose them into a state with probability ρ to p and probability $1 - \rho$ to q. Axiom P7 relates to conditional probabilities: the probability of $p \wedge q$ is equal to the probability of p given q (which is τ in the axiom) times the probability of q (which is ρ in the axiom).

Table 4 Axioms for quantum systems

Axioms for programs	
PL	All propositional tautologies
K[α]	$[\alpha](p \to q) \to ([\alpha]p \to [\alpha]q)$
PDL1	$[\alpha;\beta]p \leftrightarrow [\alpha][\beta]p$
PDL2	$[\alpha \cup \beta]p \leftrightarrow [\alpha]p \wedge [\beta]p$
Axioms for linear inequalities	
I1	$t \geq \beta \leftrightarrow t + 0P_a(\phi) \geq \beta$
I2	$\sum_{k=1}^{n} \alpha_k P_a(\phi_k) \geq \beta \to \sum_{k=1}^{n} \alpha_{j_k} P_a(\phi_{j_k}) \geq q\beta$ for any permutation $j_1, \ldots, j_n$ of $1, \ldots, n$
I3	$\sum_{k=1}^{n} \alpha_k P_a(\phi_k) \geq \beta \wedge \sum_{k=1}^{n} \alpha'_k P_a(\phi_k) \geq \beta' \to \sum_{k=1}^{n} (\alpha_k + \alpha'_k) P_a(\phi_k) \geq (\beta + \beta')$
I4	$t \geq \beta \leftrightarrow dt \geq d\beta$ if $d > 0$
I5	$t \geq \beta \vee t \leq \beta$
I6	$t \geq \beta \to t \geq \gamma$ if $\beta > \gamma$
Basic axioms for quantum systems	
Q1	$(p \equiv q) \to ([p?]r \leftrightarrow [q?]r)$
Q2	$[p?]q \leftrightarrow [\sim\sim p?]q$
Q3	$\Box\Box p \leftrightarrow \Box\Box\Box p$
Q4	$\langle p?\rangle q \to \langle q?\rangle \mathtt{tt}$
Q5	$\langle p?\rangle q \to [p?]q$
Q6	$[p?]\sim\sim p$
Q7	$p \to (q \to \langle p?\rangle q)$
Q8	$p \to [q?]\Box\langle q?\rangle\Diamond p$
Q9	$T(p) \wedge T(q) \to (\langle p?\rangle q \leftrightarrow (\Diamond p \wedge \Box(p \to \Diamond(p \wedge q))))$
Probabilistic axioms for quantum systems	
P1	$\Pr(\mathtt{tt}) = 1$
P2	$\Pr(p) \geq 0$
P3	$\Pr(p) = 0 \leftrightarrow \sim p$
P4	$(p \equiv q) \to \Pr(p) = \Pr(q)$
P5	$(p \perp q) \to \Pr(p \sqcup q) = \Pr(p) + \Pr(q)$
P6	$((p \perp q) \wedge \exists p \wedge \exists q) \to \exists(\langle p?\rangle_{=\rho} p \wedge \langle q?\rangle_{=1-\rho} q)$
P7	$(p \leq q) \wedge \langle q?\rangle_{=\rho}(\Pr(p) = \tau) \to (\Pr(p) = \rho\tau)$
Axioms for atoms and separability	
A1	$(\mathsf{Atom}(p) \wedge (q \not\equiv \mathtt{ff}) \wedge (q \leq p)) \to (q \equiv p)$
A2	$\mathsf{Atom}(p) \to (\exists(p \wedge q) \leftrightarrow (p \leq q))$
A3	$(\mathsf{Atom}(p) \wedge (p \leq \Diamond q) \wedge T(q)) \to \mathsf{Atom}((p \sqcup \sim q) \wedge q)$
A4	$\mathsf{Sep}(p) \to (\mathsf{Atom}(p) \leftrightarrow (\exists p \wedge \bigwedge_{i<N} T(p_{\{i\}})))$
A5	$\mathsf{Sep}(p) \wedge \mathsf{Sep}(q) \wedge \mathsf{Atom}(p) \wedge \mathsf{Atom}(q) \to ((p \equiv q) \leftrightarrow \bigwedge_{i<N}(p_{\{i\}} \equiv q_{\{i\}}))$
A6	$\mathsf{Sep}(p) \wedge \mathsf{Sep}(q) \to (\bigvee_{i<N}(p_{\{i\}} \perp q_{\{i\}}) \to (p \perp q))$

Axioms for atoms and separability Atoms are the smallest nonempty sets; therefore, any nonempty set smaller than an atom is equal to that atom. This is captured by axiom A1. As atoms are singleton states, a formula ϕ is satisfied at this state if and only if the atom implies ϕ. This is reflected by axiom A2.

For singleton states s that are non-orthogonal to a testable property Q, we have $(s,t) \in R_Q$ iff $\{t\} = (\{s\} \sqcup \sim Q) \cap Q$. In other words, the projection of an atom is again an atom. This is captured by axiom A3.

Axiom A4 provides a characterisation of an atom under the condition that the formula is separable. Axiom A5 asserts that two fully separable atoms are equivalent if and only if each of their local components are equivalent. Axiom A6 expresses the fact that two fully separable properties are orthogonal if one of their local components are orthogonal.

Theorem 4.1 *The rules in Table 3 and the axioms in Table 4 are sound with respect to multi-agent probabilistic quantum models (N-PQM).*

Proof Many of the axioms are standard from the literature. For example, PL, K, PDL1, and PDL2 are from propositional dynamic logic (see for example Harel et al. 2000). The axioms I1–I6 are from Fagin and Halpern (1994). The axioms P1, P2 and variations of P4 are common among probability logics (see for example Fagin and Halpern 1994). The axioms Q4–Q8 are from Baltag and Smets (2005) and Smets and Baltag (2006). The validity of some others may be obvious from the discussion above. We now prove the soundness of select axioms.

Q9: Suppose p and q are testable, i.e., $[\![p]\!] = {\sim\sim}[\![p]\!]$ and $[\![q]\!] = {\sim\sim}[\![q]\!]$. Let $s \in [\![\langle p?\rangle q]\!]$. Then, by definition of $R_{[\![p]\!]}$ there exists a $t \in S$ such that $(s,t) \in R_{[\![p]\!]}$ and $t \in [\![p]\!]$; since $s \in [\![\langle p?\rangle q]\!]$, it also holds that $t \in [\![q]\!]$. As $[\![p \wedge q]\!] = [\![p]\!] \cap [\![q]\!]$, we have $t \in [\![p \wedge q]\!]$. As $R_{[\![p]\!]}$ corresponds to the projection onto $[\![p]\!]$, we know each state $u \in [\![p]\!]$ that is non-orthogonal to s is also non-orthogonal to t. Since $t \in [\![p \wedge q]\!]$, this means that $s \in [\![\Diamond p \wedge \Box(p \to \Diamond(p \wedge q))]\!]$.

Now suppose $s \in [\![\Diamond p \wedge \Box(p \to \Diamond(p \wedge q))]\!]$. Then we have $s \in [\![\Diamond p]\!]$, so s is non-orthogonal to $[\![p]\!]$, and therefore we have $(s,t) \in R_{[\![p]\!]}$ for some unique $t \in [\![p]\!]$. Then since $s \in [\![\Box(p \to \Diamond(p \wedge q))]\!]$, we know that $t \in [\![\Diamond(p \wedge q)]\!]$; thus there exists a $u \in [\![p \wedge q]\!] = [\![p]\!] \cap [\![q]\!]$, such that tRu. Now

$$\begin{aligned}{\sim\sim}[\![p \wedge q]\!] &= {\sim\sim}([\![p]\!] \cap [\![q]\!]) \\ &= {\sim\sim}[\![p]\!] \cap {\sim\sim}[\![q]\!] = [\![p]\!] \cap [\![q]\!] = [\![p \wedge q]\!].\end{aligned}$$

Suppose towards a contradiction $t \notin [\![q]\!]$. Since $t \notin [\![p \wedge q]\!] = {\sim\sim}[\![p \wedge q]\!]$, we know there exists a $v \in {\sim}[\![p \wedge q]\!]$ such that tRv. Therefore, v is non-orthogonal to $[\![p]\!]$, so there exists a unique $w \in [\![p]\!]$ such that $(v,w) \in R_{[\![p]\!]}$.

Now w (as the projection of v onto $[\![p]\!]$) can be characterized by being the element of $[\![p]\!]$ where vRu iff wRu for all $u \in [\![p]\!]$ (see, for example, Bergfeld et al. 2015, Proposition 2.15). So we have wRx iff vRx for all $x \in [\![p]\!] \supset [\![p \wedge q]\!]$, and therefore we have $w \in [\![p]\!] \cap {\sim}[\![p \wedge q]\!]$. We also have wRt, which implies wRs (because t is the projection of s onto $[\![p]\!]$). Since $s \in [\![\Box(p \to \Diamond(p \wedge q))]\!]$ we have $w \in [\![\Diamond(p \wedge q)]\!]$, contradicting the fact that $w \in {\sim}[\![p \wedge q]\!]$. Thus $t \in [\![q]\!]$ and $s \in [\![\langle p?\rangle q]\!]$.

P6: Let $s \in [\![((p \perp q) \wedge \exists p \wedge \exists q)]\!]$. Let $x \in [\![p]\!]$ and $y \in [\![q]\!]$. Since $s \in [\![p \perp q]\!]$, $[\![p]\!] \subseteq [\![{\sim}q]\!]$, and hence $[\![p]\!]$ and $[\![q]\!]$ are orthogonal, and hence $\langle x, y\rangle = 0$. Consider the vector $z = \sqrt{\rho}x + \sqrt{(1-\rho)}y$. One can easily check that $z = \mathsf{sn}(z)$, and is hence in S. Furthermore, as $y \perp x$, the projection of z onto ${\sim\sim}[\![p]\!]$ is the vector $\sqrt{\rho}x$, whose normalization is $x \in [\![p]\!]$, and hence $z \in [\![\langle p?\rangle p]\!]$. The probability of projecting onto ${\sim\sim}[\![p]\!]$ is then $|\langle z, x\rangle|^2 = \rho$; thus $z \in [\![\langle p?\rangle_{=\rho} p]\!]$. We can similarly show that $z \in [\![\langle q?\rangle_{=1-\rho} q]\!]$. Therefore, $z \in [\![\langle p?\rangle_{=\rho} p \wedge \langle q?\rangle_{=1-\rho} q]\!]$, and thus $s \in [\![\exists(\langle p?\rangle_{=\rho} p \wedge \langle q?\rangle_{=1-\rho} q)]\!]$, as desired.

P7: Let $Q = {\sim\sim}[\![q]\!]$ and $P = {\sim\sim}[\![p]\!]$. Suppose $s \in [\![(p \le q) \wedge \langle q?\rangle_{=\rho}(\mathrm{Pr}(p) = \tau)]\!]$. Because $s \in [\![p \le q]\!]$, we have that $[\![p \le q]\!] \neq \emptyset$, and thus $[\![p]\!] \subseteq [\![q]\!]$, giving us $P \subseteq Q$. Also, $s \in [\![\langle q?\rangle_{=\rho}(\mathrm{Pr}(p) = \tau)]\!]$ and hence there exists a t, such that sR_Qt, $|\langle s,t\rangle|^2 = \rho$, and $t \in [\![\mathrm{Pr}(p) = \tau)]\!]$. Then there exists a $u \in P$, such that tR_Pu and $|\langle t,u\rangle|^2 = \tau$.

Now let $\eta = \langle s,t\rangle t$ be the actual vector when projecting s onto Q. Let $\xi = \langle \eta, u\rangle u$ be the actual vector when projecting η onto P. Let $\omega = \langle s, v\rangle v$ be the actual vector when projecting s onto P. Since $P \subseteq Q$, $\xi = \omega$ (to see this, one can change the basis so that P is the span of a subset of the basis elements, Q the span of a larger subset of the basis elements, and then project by removing the coefficients for basis elements not in the set we are projecting onto). Thus $u = v$ and $\langle \eta, u\rangle = \langle s, u\rangle$. Expanding η, we have $\overline{\langle s,t\rangle}\langle t, v\rangle = \langle s, u\rangle$. Hence $\rho\tau = |\langle s,t\rangle|^2|\langle t,v\rangle|^2 = |\langle s,u\rangle|^2$ is the probability of projecting s onto P. Hence $s \in [\![\mathrm{Pr}(p) = \rho\tau]\!]$.

A4: First, we claim that for any $\emptyset \subsetneq I \subsetneq N$ and any p we have $[\![T(p_I) \wedge \exists p_I]\!] = S$ (where S is the whole state space) if and only if it holds that $[\![p_I]\!] = \{s_I\} \otimes^{\mathfrak{M}} S_{N\setminus I}$ for some fixed $s_I \in S_I$. Before we prove this claim, let us show the soundness of A4 with this claim.

Suppose we have that $s \in [\![\mathsf{Sep}(p) \wedge \mathsf{Atom}(p)]\!]$. Then $[\![\mathsf{Sep}(p) \wedge \mathsf{Atom}(p)]\!] = S$. Then $[\![p]\!] = \{\bigotimes^{\mathfrak{M}}_{i<N} s_{\{i\}}\}$ for some $s_{\{i\}} \in S_{\{i\}}$ for each $i < N$. Therefore, we have $[\![p_{\{i\}}]\!] = \{s_{\{i\}}\} \otimes^{\mathfrak{M}} S_{N\setminus\{i\}}$, and thus by the claim, $p_{\{i\}}$ is testable, i.e., $[\![T(p_{\{i\}})]\!] = S$ for each $i < N$. Because p is an atom, we also know that $[\![\exists p]\!] = S$. Thus $s \in [\![\exists p \wedge \bigwedge_{i<N} T(p_{\{i\}})]\!]$.

Now suppose $s \in [\![\mathsf{Sep}(p) \wedge \exists p \wedge \bigwedge_{i<N} T(p_{\{i\}})]\!]$. Then we have $[\![\mathsf{Sep}(p) \wedge \exists p \wedge \bigwedge_{i<N} T(p_{\{i\}})]\!] = S$. From $[\![\exists p]\!] = S$, we deduce $[\![p]\!] \neq \emptyset$. By $[\![\mathsf{Sep}(p)]\!] = S$ we know $[\![p]\!] \subseteq \bigcap_{i<N} [\![p_{\{i\}}]\!]$. By the claim we know $\bigcap_{i<N} [\![p_{\{i\}}]\!] = \{\bigotimes^{\mathfrak{M}}_{i<N} s_{\{i\}}\}$ for some $s_{\{i\}} \in S_{\{i\}}$ for each $i < N$. Combining these results, we know $[\![p]\!] = \{s\}$, and therefore p is an atom, i.e., $[\![\mathsf{Atom}(p)]\!] = S$. Therefore, $s \in [\![\mathsf{Atom}(p)]\!]$.

To prove the claim, we first note that if $[\![T(q)]\!] = S$, we have $[\![q]\!] = {\sim\sim}[\![q]\!]$. Therefore, if $s, t \in [\![q]\!]$ we also have $\sqrt{\rho}s + \sqrt{1-\rho}t \in [\![q]\!]$ for any $\rho \in [0,1]$, because any state that is orthogonal to both s and t is also orthogonal to $\sqrt{\rho}s + \sqrt{1-\rho}t$, so we find $\sqrt{\rho}s + \sqrt{1-\rho}t \in {\sim\sim}\{s,t\} \subseteq {\sim\sim}[\![q]\!] = [\![q]\!]$.

By definition of $[\![p_I]\!]$, any $s \in [\![p_I]\!]$ is of the form $s_I \otimes^{\mathfrak{M}} s_{N\setminus I}$. Suppose $s_I \otimes^{\mathfrak{M}} s_{N\setminus I}, t_I \otimes^{\mathfrak{M}} t_{N\setminus I} \in [\![p_I]\!]$ such that $s_I \neq t_I$. Without loss of generality we may also assume $s_{N\setminus I} \neq t_{N\setminus I}$, because if $s_I \otimes^{\mathfrak{M}} s_{N\setminus I} \in [\![p_I]\!]$, then $s_I \otimes^{\mathfrak{M}} s'_{N\setminus I} \in [\![p_I]\!]$ for any other $s'_{N\setminus I} \in S_{N\setminus I}$. If we look at the sum $\sqrt{\rho}(s_I \otimes^{\mathfrak{M}} s_{N\setminus I}) + \sqrt{1-\rho}(t_I \otimes^{\mathfrak{M}} t_{N\setminus I})$, with $\rho \neq 0, 1$, it is not hard to see that this sum is not equal to $u_I \otimes^{\mathfrak{M}} u_{N\setminus I}$ for any $u_I \in S_I$ and $u_{N\setminus I} \in S_{N\setminus I}$. In other words, $\sqrt{\rho}(s_I \otimes^{\mathfrak{M}} s_{N\setminus I}) + \sqrt{1-\rho}(t_I \otimes^{\mathfrak{M}} t_{N\setminus I}) \notin [\![p_I]\!]$.

Combining the above two results, we have that if $[\![p_I]\!] \neq \emptyset$ and $[\![T(p_I)]\!] = S$, then $[\![p_I]\!] = \{s_I\} \otimes^{\mathfrak{M}} S_{N\setminus I}$ for some fixed $s_I \in S_I$.

For the other direction, we have that $\{s_I\} \otimes^{\mathfrak{M}} S_{N\setminus I}$ is isomorphic to $S_{N\setminus I}$, because every vector in the space spanned by $\{s_I\} \otimes^{\mathfrak{M}} S_{N\setminus I}$ is a constant multiple of an element of $\{s_I\} \otimes^{\mathfrak{M}} S_{N\setminus I}$. Hence $\{s_I\} \otimes^{\mathfrak{M}} S_{N\setminus I}$ represents a subspace, and is therefore bi-orthogonally closed. Every topologically closed linear subspace is bi-orthogonally closed (Birkhoff and Neumann 1936), and it is well known that every subspace of a finite-dimensional Hilbert space is isomorphic to $\mathbb{C}^n$ and therefore topologically closed. This finishes the proof of the claim. □

4.1 Deducible basic properties of quantum models

We will now use our system to deduce several properties that are standard in most quantum logics, like weak modularity. In the first lemma, we will show the connection between projections ($\langle\phi?\rangle$) and non-orthogonality ($\Diamond$). Also we show non-orthogonality is both reflexive and symmetric.

Lemma 4.2 *The following formulas are deducible.*

$$\vdash \langle p?\rangle \mathtt{tt} \leftrightarrow \Diamond p \tag{4.1}$$
$$\vdash \langle p?\rangle q \rightarrow \Diamond q \tag{4.2}$$
$$\vdash p \rightarrow \Diamond p \quad \text{(reflexivity)} \tag{4.3}$$
$$\vdash p \rightarrow \Box\Diamond p \quad \text{(symmetry)} \tag{4.4}$$

Proof To prove $\vdash \langle p?\rangle \mathtt{tt} \leftrightarrow \Diamond p$, we first observe that $\vdash p \equiv \neg\neg p$. Then using universal substitution on Q1 and propositional logic, we obtain $\vdash \neg[p?]\mathtt{ff} \leftrightarrow \neg[\neg\neg p?]\mathtt{ff}$, which is precisely what $\vdash \langle p?\rangle \mathtt{tt} \leftrightarrow \Diamond p$ abbreviates.

To prove $\vdash \langle p?\rangle q \rightarrow \Diamond q$, observe by axiom Q4 that $\vdash \langle p?\rangle q \rightarrow \langle q?\rangle \mathtt{tt}$, where the right side is equivalent to $\Diamond q$. The proofs for $\vdash p \rightarrow \Diamond p$ and $\vdash p \rightarrow \Box\Diamond p$ can be found in Table 5.

Table 5 A proof of $\vdash p \rightarrow \Diamond p$ and $\vdash p \rightarrow \Box\Diamond p$

1	$\mathtt{tt}$	PL
2	$\mathtt{tt} \rightarrow (p \rightarrow \langle \mathtt{tt}?\rangle p)$	Q7 + US
3	$p \rightarrow \langle \mathtt{tt}?\rangle p$	MP(1,2)
4	$\langle \mathtt{tt}?\rangle p \rightarrow \Diamond p$	(4.2) + US
5	$p \rightarrow \Diamond p$	PL(3,4)
6	$\langle \mathtt{tt}?\rangle p \rightarrow [\mathtt{tt}?]p$	Q5 + US
7	$p \rightarrow [\mathtt{tt}?]p$	PL(3,6)
8	$[\mathtt{tt}?]p \rightarrow p$	PL(3) + US
9	$\langle \mathtt{tt}?\rangle p \rightarrow p$	PL(7) + US
10	$p \rightarrow [\mathtt{tt}?]\Box\langle \mathtt{tt}?\rangle\Diamond p$	Q8 + US
11	$p \rightarrow \Box\Diamond p$	PL(8,9,10) + US

With a proof of reflexivity, we can deduce the following four bidirectional rules (each column has both directions):

Lemma 4.3 *The following rules hold true:*

$$\frac{\vdash p}{\vdash \forall p} \qquad \frac{\vdash p \rightarrow q}{\vdash p \leq q} \qquad \frac{\vdash p \leftrightarrow q}{\vdash p \equiv q} \qquad \frac{\vdash p \leftrightarrow {\sim}{\sim}p}{\vdash T(p)}$$

$$\frac{\vdash \forall p}{\vdash p} \qquad \frac{\vdash p \leq q}{\vdash p \rightarrow q} \qquad \frac{\vdash p \equiv q}{\vdash p \leftrightarrow q} \qquad \frac{\vdash T(p)}{\vdash p \leftrightarrow {\sim}{\sim}p}$$

Proof The upper row follows from two applications of necessitation; the lower row follows from reflexivity (Lemma 4.2-(4.3), which is equivalent to $\vdash \Box p \rightarrow p$). □

Throughout this text, we will often apply the above lemma without reference. The following lemma states that every atom is nonempty.

Lemma 4.4 *The following formula is deducible.*

$$\vdash \exists p \leftrightarrow (p \not\equiv \mathtt{ff}).$$

As a consequence $\vdash \mathsf{Atom}(p) \rightarrow (p \not\equiv \mathtt{ff})$.

Proof $p \not\equiv \mathtt{ff}$ abbreviates $\neg\Box\Box(p \leftrightarrow \mathtt{ff})$, which is equivalent to $\Diamond\Diamond((p \wedge \neg\mathtt{ff}) \vee (\neg p \wedge \mathtt{ff}))$. By standard modal reasoning, this is equivalent to $\Diamond\Diamond p$, or in abbreviated form $\exists p$.

We have $\vdash p \leq \mathtt{tt}$, so by A2 we have $\vdash \mathsf{Atom}(p) \rightarrow \exists(p \wedge \mathtt{tt})$ and as we have $\vdash p \equiv (p \wedge \mathtt{tt})$ we have $\vdash \mathsf{Atom}(p) \rightarrow (p \not\equiv \mathtt{ff})$. □

The following lemma collects several properties of the orthocomplement, in particular the three defining properties $p \leq {\sim}{\sim}p$, $p \leq q$ implies ${\sim}q \leq {\sim}p$, and $(p \wedge {\sim}p) \equiv \mathtt{ff}$. Note that the first property $p \leq {\sim}{\sim}p$ is weaker than the standard property found in many quantum logics $p \equiv {\sim}{\sim}p$, but the latter only holds in quantum models that only consider testable properties.

Lemma 4.5 (Orthocomplement) *The following formulas are deducible.*

$$\vdash p \leq {\sim}{\sim}p \tag{4.5}$$
$$\vdash (p \leq q) \rightarrow ({\sim}q \leq {\sim}p) \tag{4.6}$$
$$\vdash (p \wedge {\sim}p) \equiv \mathtt{ff} \tag{4.7}$$
$$\vdash {\sim}p \equiv {\sim}{\sim}{\sim}p \tag{4.8}$$
$$\vdash p \perp q \leftrightarrow q \perp p \tag{4.9}$$

Proof The proofs of these formulas can be found in Table 6. □

Table 6 A proof of $\vdash p \leq \sim\sim p$, $\vdash (p \leq q) \to (\sim q \leq \sim p)$, $\vdash \sim p \equiv \sim\sim\sim p$, $\vdash (p \wedge \sim p) \equiv \mathtt{ff}$ and $\vdash (p \perp q) \leftrightarrow (q \perp p)$

1	$p \to \Box\Diamond p$	Lemma 4.2
2	$p \to \sim\sim p$	Abb.(1)
3	$p \leq \sim\sim p$	Lemma 4.3
4	$\Box\Box(p \to q) \to \Box\Box(\neg q \to \neg p)$	ML
5	$\Box\Box(p \to q) \to \Box\Box\Box(\neg q \to \neg p)$	Q3
6	$\Box\Box(p \to q) \to \Box\Box(\Box\neg q \to \Box\neg p)$	ML(5)
7	$(p \leq q) \to (\sim q \leq \sim p)$	Abb.(6)
8	$\Box\neg p \to \neg p$	Lemma 4.2
9	$(p \wedge \Box\neg p) \to \mathtt{ff}$	PL(8)
10	$(p \wedge \sim p) \equiv \mathtt{ff}$	Lemma 4.3
11	$\sim p \leq \sim\sim\sim p$	US(3)
12	$(p \leq \sim\sim p) \to (\sim\sim\sim p \leq \sim p)$	US(7)
13	$(\sim\sim\sim p \leq \sim p)$	MP(3,12)
14	$\sim p \equiv \sim\sim\sim p$	PL(11,13)
15	$(p \leq \sim q) \to (\sim\sim q \leq \sim p)$	US(7)
16	$(p \leq \sim q) \to (q \leq \sim p)$	PL(2,15)
17	$(p \perp q) \to (q \perp p)$	Abb.(16)
18	$(q \perp p) \to (p \perp q)$	US(17)
19	$(p \perp q) \leftrightarrow (q \perp p)$	PL(17,18)

As shown in Baltag and Smets (2006), the set of testable properties $\mathcal{T}$ contains all singletons and is closed under taking orthocomplement and intersections. The following lemma establishes the latter property. The former property will be deduced in Lemma 4.11, because we first need to show weak modularity.

Lemma 4.6 (Testable properties) *The following formulas are deducible.*

Table 7 A proof of $T(\sim p)$ and $\vdash T(p) \wedge T(q) \to T(p \wedge q)$

1	$\sim p \equiv \sim\sim\sim p$	(4.8)
2	$T(\sim p)$	Abb.(1)
3	$(p \wedge q) \leq \sim\sim(p \wedge q)$	(4.5)
4	$(p \wedge q) \leq p$	PL
5	$\sim\sim(p \wedge q) \leq \sim\sim p$	(4.6)
6	$\sim\sim(p \wedge q) \leq \sim\sim q$	US(5)
7	$\sim\sim(p \wedge q) \leq (\sim\sim p \wedge \sim\sim q)$	PL(5,6)
8	$(T(p) \wedge T(q)) \to ((\sim\sim p \wedge \sim\sim q) \equiv (p \wedge q))$	ML
9	$(T(p) \wedge T(q)) \to (\sim\sim(p \wedge q) \leq (p \wedge q))$	ML(7,8)
10	$(T(p) \wedge T(q)) \to ((p \wedge q) \equiv \sim\sim(p \wedge q))$	PL(3,9)
11	$(T(p) \wedge T(q)) \to T(p \wedge q)$	Abb.(10)

$$\vdash T(\sim p) \tag{4.10}$$

$$\vdash T(p) \wedge T(q) \to T(p \wedge q) \tag{4.11}$$

Proof The proof of these formulas can be found in Table 7. □

The following lemma collects several properties of the quantum join. Most of these properties are intuitive when one thinks of the quantum join $p \sqcup q$ as the smallest closed linear subspace containing both p and q. For (4.16), if r is orthogonal to both p and q, then r is orthogonal to each element in the span of p and q, which is the quantum join $p \sqcup q$.

Lemma 4.7 (Quantum join) *The following formulas are deducible.*

$$\vdash p \leq (p \sqcup q) \tag{4.12}$$

$$\vdash (p \sqcup q) \equiv (\sim\sim p) \sqcup (\sim\sim q) \tag{4.13}$$

$$\vdash (T(p) \wedge T(q)) \to (\sim(p \wedge q) \equiv (\sim p \sqcup \sim q)) \tag{4.14}$$

$$\vdash \sim(p \sqcup q) \equiv (\sim p \wedge \sim q) \tag{4.15}$$

$$\vdash ((r \perp p) \wedge (r \perp q)) \leftrightarrow (r \perp (p \sqcup q)) \tag{4.16}$$

Table 8 A proof of $\vdash p \leq p \sqcup q$, $\vdash (p \sqcup q) \equiv (\sim\sim p \sqcup \sim\sim q)$, $(T(p) \wedge T(q)) \to (\sim(p \wedge q) \equiv (\sim p \sqcup \sim q))$, $\sim(p \sqcup q) \equiv (\sim p \wedge \sim q)$, and $\vdash ((r \perp p) \wedge (r \perp q)) \leftrightarrow (r \perp (p \sqcup q))$

1	$p \leq \sim\sim p$	Lemma 4.5
2	$(\sim p \wedge \sim q) \leq \sim p$	PL + Lemma 4.3
3	$\sim\sim p \leq \sim(\sim p \wedge \sim q)$	Lemma 4.5 + US
4	$p \leq \sim(\sim p \wedge \sim q)$	ML(1,3)
5	$p \leq (p \sqcup q)$	Abb.(4)
6	$\sim p \equiv \sim\sim\sim p$	Lemma 4.5
7	$\sim(\sim p \wedge \sim q) \equiv \sim(\sim\sim\sim p \wedge \sim\sim\sim q)$	ML(6)
8	$(p \sqcup q) \equiv (\sim\sim p \sqcup \sim\sim q)$	Abb.(7)
9	$(T(p) \wedge T(q)) \to (\sim(p \wedge q) \equiv \sim(\sim\sim p \wedge \sim\sim p))$	ML
10	$(T(p) \wedge T(q)) \to (\sim(p \wedge q) \equiv (\sim p \sqcup \sim q))$	Abb.(9)
11	$T(\sim\sim(\sim p \wedge \sim q))$	Lemma 4.6
12	$\sim\sim(\sim p \wedge \sim q) \equiv (\sim p \wedge \sim q)$	Abb.(11)
13	$\sim(p \sqcup q) \equiv (\sim p \wedge \sim q)$	Abb.(12)
14	$(r \perp p) \leftrightarrow \forall(r \to \sim p)$	Abb.
15	$(r \perp q) \leftrightarrow \forall(r \to \sim q)$	Abb.
16	$((r \perp p) \wedge (r \perp q)) \leftrightarrow \forall(r \to (\sim p \wedge \sim q))$	PL(14,15)
17	$T(\sim p \wedge \sim q)$	Lemma 4.6
18	$(\sim p \wedge \sim q) \leftrightarrow \sim\sim(\sim p \wedge \sim q)$	Lemma 4.3(17)
19	$((r \perp p) \wedge (r \perp q)) \leftrightarrow \forall(r \to \sim\sim(\sim p \wedge \sim q))$	PL(16,18)
20	$((r \perp p) \wedge (r \perp q)) \leftrightarrow (r \perp (p \sqcup q))$	Abb.(19)

$$\vdash (p \sqcup {\sim}p) \equiv \mathtt{tt} \tag{4.17}$$

$$\vdash (T(r) \wedge (p \leq r) \wedge (q \leq r)) \rightarrow ((p \sqcup q) \leq r) \tag{4.18}$$

Proof The proof for the first five formulas can be found in Table 8.

To show $\vdash (p \sqcup {\sim}p) \equiv \mathtt{tt}$, we observe by Lemma 4.5-(4.7) that $\vdash (p \wedge {\sim}p) \equiv \mathtt{ff}$. Hence $\vdash \neg(p \wedge {\sim}p) \equiv \mathtt{tt}$. By modal logic, we have that $\vdash {\sim}(p \wedge {\sim}p) \equiv \Box\mathtt{tt}$. Using necessitation and propositional logic, we have $\vdash \mathtt{tt} \equiv \Box\mathtt{tt}$. The desired result follows from this and modal logic.

To prove (4.18), we use Lemma 4.5-(4.6) to get $\vdash (p \leq r) \rightarrow ({\sim}r \leq {\sim}p)$ and $\vdash (q \leq r) \rightarrow {\sim}r \leq {\sim}p$, and hence $\vdash (p \leq r) \wedge (q \leq r) \rightarrow ({\sim}r \leq ({\sim}p \wedge {\sim}q))$. Using Lemma 4.5-(4.6) again we have $\vdash (p \leq r) \wedge (q \leq r) \rightarrow {\sim}({\sim}p \wedge {\sim}q) \leq {\sim}{\sim}r$. Adding $T(r)$ to the antecedent, the desired result follows from the previous observation and modal logic. □

We need a more general version of Lemma 4.7-(4.16) that considers the quantum join of n formulas instead of just two.

Corollary 4.8 *For all finite n and for all sets of formulas $\mathcal{B}$ of size n, the following formula is deducible.*

$$\vdash \bigwedge_{b \in \mathcal{B}} (p \perp b) \rightarrow p \perp \bigsqcup \mathcal{B} \tag{4.19}$$

$$\vdash \exists p \wedge (p \leq \bigsqcup_{b \in \mathcal{B}} b) \rightarrow \bigvee_{b \in \mathcal{B}} (p \not\perp b) \tag{4.20}$$

Proof We prove this by induction on n. For $n = 1$ the statement holds trivially. Now suppose the statement holds for n. Let $\mathcal{B}$ be a set of formulas of size n and let b_{n+1} be a formula. By the induction hypothesis we have $\vdash (\bigwedge_{b \in \mathcal{B}} p \perp b) \rightarrow (p \perp \bigsqcup \mathcal{B})$. By Lemma 4.7-(4.16) we have $\vdash (p \perp b_{n+1}) \wedge (p \perp \bigsqcup \mathcal{B}) \rightarrow (p \perp (\bigsqcup \mathcal{B}) \sqcup b_{n+1})$. Combining the two results gives the desired result.

For (4.20), Note that $\vdash (\exists p \wedge (p \leq \bigsqcup \mathcal{B}) \rightarrow (p \not\perp \bigsqcup \mathcal{B})$. Thus by the contrapositive of (4.19), we have $\vdash (\exists p \wedge (p \leq \bigsqcup \mathcal{B}) \rightarrow \bigvee_{b \in \mathcal{B}} (p \not\perp b)$. □

One of the main difference between classical logic and quantum logic is the lack of distributivity. Classical models satisfy distributivity $(p \wedge (q \vee r) = (p \wedge q) \vee (p \wedge r))$, but quantum models only satisfy a weaker version of distributivity called weak modularity, which we will show in the following lemma.

Lemma 4.9 (Weak modularity) *The following formula is deducible.*

$$\vdash T(p) \wedge T(q) \wedge (q \leq p) \rightarrow (q \equiv p \wedge ({\sim}p \sqcup q)).$$

Proof The proof can be found in Table 9. □

Table 9 A proof of $\vdash (T(p) \wedge T(q) \wedge (q \leq p)) \rightarrow (q \equiv (p \wedge ({\sim}p \sqcup q)))$

1	$q \leq ({\sim}p \sqcup q)$	Lemma 4.7
2	$(q \leq p) \rightarrow (q \leq (p \wedge ({\sim}p \sqcup q)))$	ML(1)
3	$p \rightarrow \Diamond p$	Lemma 4.2
4	$(q \leq p) \rightarrow (q \equiv (p \wedge q))$	ML
5	$T(p) \rightarrow ((p \wedge ({\sim}p \sqcup q)) \equiv (p \wedge \Box\neg(p \wedge \Box\neg q)))$	ML
6	$(q \leq p) \rightarrow (\Box\neg(p \wedge \Box\neg q) \leftrightarrow \Box(p \rightarrow \Diamond(p \wedge q)))$	ML(4)
7	$(q \leq p) \rightarrow (p \wedge \Box\neg(p \wedge \Box\neg q) \rightarrow \Diamond p \wedge \Box(p \rightarrow \Diamond(p \wedge q)))$	PL(3,6)
8	$(T(p) \wedge T(q) \wedge \Diamond p \wedge \Box(p \rightarrow \Diamond p \wedge q)) \rightarrow \langle p? \rangle q$	Q9
9	$(T(p) \wedge T(q) \wedge (q \leq p)) \rightarrow ((p \wedge ({\sim}p \sqcup q)) \rightarrow \langle p? \rangle q)$	PL(5,7,8)
10	$p \rightarrow ([p?]q \rightarrow q)$	Q7
11	$\langle p? \rangle q \rightarrow [p?]q$	Q5
12	$(p \wedge \langle p? \rangle q) \rightarrow q$	PL(10,11)
13	$(T(p) \wedge T(q) \wedge (q \leq p)) \rightarrow ((p \wedge ({\sim}p \sqcup q)) \rightarrow q)$	PL(9,12)
14	$(T(p) \wedge T(q) \wedge (q \leq p)) \leftrightarrow \forall (T(p) \wedge T(q) \wedge (q \leq p))$	Lemma 4.3
15	$(T(p) \wedge T(q) \wedge (q \leq p)) \rightarrow ((p \wedge ({\sim}p \sqcup q)) \leq q)$	Nec(13,14)
16	$(T(p) \wedge T(q) \wedge (q \leq p)) \rightarrow (q \equiv (p \wedge ({\sim}p \sqcup q)))$	ML(2,15)

Table 10 A proof of $\vdash (T(q) \wedge (p \leq q)) \rightarrow (q \equiv p \sqcup ({\sim}p \wedge q))$

1	$(p \leq q) \rightarrow ({\sim}q \leq {\sim}p)$	Lemma 4.5
2	$T({\sim}p)$	Lemma 4.6
3	$({\sim}q \leq {\sim}p) \rightarrow ({\sim}q \equiv {\sim}p \wedge ({\sim}{\sim}p \sqcup {\sim}q))$	Lemma 4.9
4	$(p \leq q) \rightarrow ({\sim}{\sim}q \equiv {\sim}({\sim}p \wedge (p \sqcup {\sim}q)))$	ML(1,2,3)
5	$(p \leq q) \rightarrow ({\sim}{\sim}q \equiv ({\sim}{\sim}p \sqcup {\sim}(p \sqcup {\sim}q)))$	Lemma 4.7
6	$(p \leq q) \rightarrow ({\sim}{\sim}q \equiv (p \sqcup ({\sim}p \wedge {\sim}{\sim}q)))$	Lemma 4.7
7	$(T(q) \wedge (p \leq q)) \rightarrow (q \equiv p \sqcup ({\sim}p \wedge q))$	ML(6)

We also need the dual of weak modularity, which we will show in the following corollary.

Corollary 4.10 *The following formula is deducible.*

$$\vdash T(q) \wedge (p \leq q) \rightarrow (q \equiv p \sqcup ({\sim}p \wedge q))$$

Proof This is basically the dual of Lemma 4.9, that is, taking the orthocomplement. See Table 10. □

With weak modularity we can show each atom is testable.

Lemma 4.11 *The following formula is deducible.*

$$\mathit{Atom}(p) \rightarrow T(p).$$

Proof By Lemma 4.5 we have $\vdash p \leq \sim\sim p$, and by Lemma 4.2-(4.3) we have $\vdash \sim\sim p \leq \Diamond\sim\sim p$. So we can deduce $\vdash p \leq \Diamond\sim\sim p$. By Lemma 4.6, we have $\vdash T(\sim\sim p)$. Therefore, we can apply axiom A3 and (4.8) to deduce $\vdash \mathsf{Atom}(p) \to \mathsf{Atom}((p \sqcup \sim p) \wedge \sim\sim p)$. By Lemma 4.7 we have $\vdash (p \sqcup \sim p) \equiv \mathtt{tt}$, so we can deduce $\vdash \mathsf{Atom}(p) \to \mathsf{Atom}(\sim\sim p)$. By Lemma 4.4 we have $\vdash \mathsf{Atom}(p) \to (\mathtt{ff} \not\equiv p)$, and we already have $\vdash p \leq \sim\sim p$, so we can deduce $\vdash \mathsf{Atom}(p) \to (p \equiv \sim\sim p)$ by axiom A1. This is equivalent to the desired result. □

4.2 Deducible probabilistic properties of quantum models

The following lemma collects several deducible properties of probabilistic quantum logic.

Lemma 4.12 *The following formulas are deducible:*

$$\vdash \Diamond p \leftrightarrow \Pr(p) > 0 \tag{4.21}$$
$$\vdash \Pr(p) + \Pr(\sim p) = 1 \tag{4.22}$$
$$\vdash \Pr(p) = \Pr(\sim\sim p) \tag{4.23}$$
$$\vdash T(p) \to (p \leftrightarrow \Pr(p) = 1) \tag{4.24}$$
$$\vdash p \to \Pr(p) = 1 \tag{4.25}$$

Proof The proof of (4.21) is in Table 11.

We now show (4.22). By Lemma 4.5 we have $\vdash p \perp \sim p$ and $\vdash p \sqcup \sim p$, and hence by axiom P1, P4 and P5 we obtain the desired result $\vdash \Pr(p) + \Pr(\sim p) = 1$.

We now show (4.23). By uniform substitution in (4.22) we have $\vdash \Pr(\sim p) + \Pr(\sim\sim p) = 1$. From this we can use the inequality axioms to show the second result $\vdash \Pr(p) = \Pr(\sim\sim p)$.

We now show (4.24). Since $T(p)$ abbreviates $p \equiv \sim\sim p$, from the axiom $\vdash \Pr(p) = 0 \leftrightarrow \sim p$ it follows that $\vdash T(p) \to p \leftrightarrow \Pr(\sim p) = 0$. From the inequality axioms and propositional reasoning we obtain the third result $\vdash T(p) \to p \leftrightarrow \Pr(p) = 1$.

We now show (4.25). By Lemma 4.5 we also have $\vdash p \to \sim\sim p$ and $\vdash T(\sim(\sim p))$, combining this with $\vdash \Pr(p) = \Pr(\sim\sim p)$, we obtain the last result $\vdash p \to \Pr(p) = 1$. □

The following lemma shows that probability $(\Pr(\cdot))$ is monotone.

Table 11 A proof of $\vdash \Diamond p \leftrightarrow \Pr(p) > 0$

1	$\Pr(p) \neq 0 \leftrightarrow \Diamond p$	P3 + PL
2	$\Pr(p) > 0 \leftrightarrow \Diamond p$	PL(1) + P2

Proposition 4.13 *The following formula is deducible.*

$$\vdash p \leq q \to \Pr(p) \leq \Pr(q).$$

Proof First, by (4.5) and modal logic, we have $\vdash p \leq q \to p \leq \sim\sim q$ and by Lemma 4.6, we have $\vdash T(\sim\sim q)$. Therefore, by Corollary 4.10 we have $\vdash p \leq q \to \sim\sim q \equiv p \sqcup (\sim p \wedge \sim\sim q)$. Hence by P4, $\vdash p \leq q \to P(\sim\sim q) = P(p \sqcup (\sim p \wedge \sim\sim q))$. Note that $\vdash p \perp (\sim p \wedge \sim\sim q)$, since clearly $\vdash \sim p \wedge \sim\sim q \leq \sim p$. Thus by P5, $\vdash \Pr(p \sqcup (\sim p \wedge \sim\sim q)) = \Pr(p) + \Pr(\sim p \wedge \sim\sim q)$. By (4.23), $\vdash \Pr(q) = \Pr(\sim\sim q)$. Using inequality axioms, we obtain $\vdash p \leq q \to \Pr(q) = \Pr(p) + \Pr(\sim p \wedge \sim\sim q)$. The desired result follows from this and the inequality axioms. □

Axiom P5 only considers a pair of orthogonal states, but can be generalized to a finite set of n pairwise orthogonal states.

Lemma 4.14 *For all n, the following formula is deducible.*

$$\vdash \left(\bigwedge_{i<j<n} b_i \perp b_j \right) \to \left(\Pr\left(\bigsqcup_{i \leq n} b_i \right) = \sum_{i<n} \Pr(b_i) \right).$$

Proof We prove this by induction. For $n = 2$, the statement holds by Axiom P5. Now suppose the statement holds for n (IH). Given the induction hypothesis (IH), the proof of

$$\vdash \left(\bigwedge_{i<j<n+1} b_i \perp b_j \right) \to \left(\Pr\left(\bigsqcup_{i \leq n} b_i \right) = \sum_{i<n+1} \Pr(b_i) \right).$$

is given in Table 12. □

Using Lemma 4.14, we obtain a nice characterisation for the quantum join of a set of orthogonal states involving probabilities, which we show in the following corollary.

Table 12 A proof of $\vdash (\bigwedge_{i<j<n} b_i \perp b_j) \to (\Pr(\bigsqcup_{i \leq n} b_i) = \sum_{i<n} \Pr(b_i))$

1	$\bigwedge_{i<j<n+1}(b_i \perp b_j) \to (b_n \perp \bigsqcup_{i<n} b_i)$	Corollary 4.8
2	$\Pr(\bigsqcup_{i<n+1} b_i) = \Pr((\bigsqcup_{i<n} b_i) \sqcup b_n)$	Abb.
3	$(b_n \perp \bigsqcup_{i<n} b_i) \to (\Pr((\bigsqcup_{i<n} b_i) \sqcup b_n) = \Pr(\bigsqcup_{i<n} b_i) + \Pr(b_n))$	P5
4	$\bigwedge_{i<j<n}(b_i \perp b_j) \to \Pr(\bigsqcup_{i<n} b_i) = \sum_{i<n} \Pr(b_i)$	(IH)
5	$\bigwedge_{i<j<n+1}(b_i \perp b_j) \to \Pr(\bigsqcup_{i<n+1} b_i) = \sum_{i<n+1} \Pr(b_i)$	I1–I3

Corollary 4.15 *For all finite n the following formula is deducible.*

$$\vdash \bigwedge_{i<j\leq n} (b_i \perp b_j) \rightarrow \left(\left(\bigsqcup_{i<n} b_i\right) \equiv \left(\sum_{i<n} \Pr(b_i) = 1\right)\right).$$

Proof For $n \geq 2$ we know $\vdash T(\bigsqcup_{i<n} b_i)$ is derivable by Lemma 4.6, so by Lemma 4.12-(4.24), we have $\vdash (\Pr(\bigsqcup_{i\leq n} b_i) = 1) \leftrightarrow \bigsqcup_{i\leq n} b_i$. By Lemma 4.14, we know

$$\vdash \left(\bigwedge_{i<j\leq n} b_i \perp b_j\right) \rightarrow \Pr\left(\bigsqcup_{i\leq n} b_i\right) = \sum_{i\leq n} \Pr(b_i).$$

Combining these results, we get our desired result. □

Similar to axiom P5, we can generalize axiom P7 by considering the quantum join of a finite set of formulas.

Lemma 4.16 *The following formula is deducible.*

$$\vdash \langle \bigsqcup_{i\leq n} b_i ? \rangle_{=\rho} \bigwedge_{i\leq n} (\Pr(b_i) = \rho_i) \rightarrow \bigwedge_{i\leq n} (\Pr(b_i) = \rho\rho_i)$$

Proof By modal logic, $\vdash \langle \bigsqcup_{i\leq n} b_i ? \rangle_{=\rho} \bigwedge_{i\leq n} (\Pr(b_i) = \rho_i) \rightarrow \bigwedge_{i\leq n} \langle \bigsqcup_{i\leq n} b_i ? \rangle_{=\rho} (\Pr(b_i) = \rho_i)$. By Lemma 4.7-(4.12), we also know $\vdash b_i \leq \bigsqcup_{j\leq n} b_j$, so the statement follows from axiom P7 and propositional logic. □

4.3 Deducible properties of a basis

Since the notion of an orthonormal basis is very important in the two protocols we will discuss in Section 5, as well as many other protocols, we discuss the definition of a basis and prove several properties.

Let $\mathfrak{M}$ be an N-PQM and let $\mathcal{B}$ be a finite set of formulas. The set $\mathcal{B}$ is called an orthosubbasis of $\mathfrak{M}$ if the following formula is satisfied in $\mathfrak{M}$:

$$\mathsf{SubBasis}(\mathcal{B}) := \bigwedge_{b\in\mathcal{B}} (b \not\equiv \mathtt{ff}) \wedge \bigwedge_{b\neq b'\in\mathcal{B}} (b \perp b') \wedge \left(\bigsqcup_{b\in\mathcal{B}} b \equiv \mathtt{tt}\right).$$

In the following lemmas, we show that the probabilities of elements in an orthosubbasis $\mathcal{B}$ add up to 1.

Lemma 4.17 *For a finite set of testable formulas $\mathcal{B}$ the following formula is deducible.*

$$\vdash \mathit{SubBasis}(\mathcal{B}) \rightarrow \sum_i \Pr(b_i) = 1.$$

Proof This lemma follows directly from the definition of an orthosubbasis combined with Lemma 4.14 and axiom P1. □

An orthosubbasis $\mathcal{B}$ is an orthobasis if any proper superset of $\mathcal{B}$ is not a subbasis. This happens precisely when $\mathcal{B}$ consists only of atoms.

$$\mathsf{Basis}(\mathcal{B}) := \mathsf{SubBasis}(\mathcal{B}) \wedge \bigwedge_{b\in\mathcal{B}} \mathsf{Atom}(b).$$

We are going to show that each basis has the same number of elements. To show this we will first show that within a quantum join we can replace one atom p by another atom q without changing the quantum join $p \sqcup r$, so long as these two atoms are "close" enough (q is also under the join, but not under r).

Lemma 4.18 *The following formula is deducible.*

$$\vdash \big(\mathit{Atom}(p) \wedge \mathit{Atom}(q) \wedge T(r) \wedge (q \leq (p \sqcup r)) \wedge (q \not\leq r)\big) \rightarrow ((p \sqcup r) \equiv (q \sqcup r))$$

Proof Let us abbreviate the antecedent with

$$\mathsf{Ant} := \mathsf{Atom}(p) \wedge \mathsf{Atom}(q) \wedge T(r) \wedge (q \leq (p \sqcup r)) \wedge (q \not\leq r).$$

By Lemma 4.7-(4.12), we know $\vdash r \leq (p \sqcup r)$ and together with the assumption $q \leq (p \sqcup r)$ from the antecedent and $\vdash T(p \sqcup r)$ by Lemma 4.6, we get $\vdash \mathsf{Ant} \rightarrow (q \sqcup r \leq p \sqcup r)$ by Lemma 4.7-(4.18). As $\vdash \mathsf{Ant} \rightarrow (q \not\leq r)$ we get by basic reasoning $\vdash \mathsf{Ant} \rightarrow (q \sqcup r \not\leq r)$, and by the above $\vdash \mathsf{Ant} \rightarrow (p \sqcup r \not\leq r)$. Thus $\vdash \mathsf{Ant} \rightarrow (p \not\leq r)$.

Because $\vdash \mathsf{Ant} \rightarrow T(r)$ we have $\vdash \mathsf{Ant} \rightarrow (p \not\leq r \leftrightarrow p \not\leq \sim\sim r)$. Hence, we have $\vdash \mathsf{Ant} \rightarrow (p \not\leq \sim\sim r)$. Unpacking the notation, this is equivalent to $\vdash \mathsf{Ant} \rightarrow \exists(p \wedge \Diamond\sim r)$. Because $\vdash \mathsf{Ant} \rightarrow \mathsf{Atom}(p)$, we find that $\vdash \mathsf{Ant} \rightarrow (\exists(p \wedge \Diamond\sim r)p \leftrightarrow (p \leq \Diamond\sim r))$ by A2. Hence, $\vdash \mathsf{Ant} \rightarrow (p \leq \Diamond\sim r)$.

Since $\vdash \mathsf{Ant} \rightarrow ((q \sqcup r) \leq (p \sqcup r))$, we know that $\vdash \mathsf{Ant} \rightarrow (((q \sqcup r) \wedge \sim r) \leq ((p \sqcup r) \wedge \sim r))$. Applying A1 and A3 we obtain $\vdash \mathsf{Ant} \rightarrow (((q \sqcup r) \wedge \sim r) \equiv ((p \sqcup r) \wedge \sim r))$. Now we can apply weak modularity (Corollary 4.10) to get the desired result.

$$\vdash \mathsf{Ant} \rightarrow (q \sqcup r) \equiv (r \sqcup ((q \sqcup r) \wedge \sim r)) \equiv (r \sqcup ((p \sqcup r) \wedge \sim r)) \equiv (p \sqcup r).$$

□

The following lemma uses the previous lemma to establish that a quantum join of n formulas can contain at most n orthogonal states.

Lemma 4.19 *For any finite n and any set $\mathcal{B}$ of size n and any set $\mathcal{C}$ of finite size $m > n$, the following is deducible.*

$$\vdash \left(\bigwedge_{a \in \mathcal{B} \cup \mathcal{C}} \mathit{Atom}(a) \wedge \bigwedge_{c \neq c' \in \mathcal{C}} (c \perp c') \right) \rightarrow \bigvee_{c \in \mathcal{C}} \left(c \not\leq \bigsqcup \mathcal{B} \right).$$

Proof We prove this by induction on n. For $n = 1$, the formula follows immediately from A1 and Lemma 4.4.

Suppose the formula holds true for any set $\mathcal{B}$ of size smaller than n and any set $\mathcal{C}$ of size bigger than the size of $\mathcal{B}$ (IH). Consider the following formula (which is the negation of the desired formula):

$$\chi := \bigwedge_{a \in \mathcal{B} \cup \mathcal{C}} \mathsf{Atom}(a) \wedge \bigwedge_{c \neq c' \in \mathcal{C}} (c \perp c')) \wedge \bigwedge_{c \in \mathcal{C}} \left(c \leq \bigsqcup \mathcal{B} \right).$$

It suffices to prove $\vdash \chi \rightarrow \mathtt{ff}$. Take any order on $\mathcal{B} = \{b_0, \ldots, b_{n-1}\}$. We will use Lemma 4.18 to replace each b by a c one by one, such that the quantum join remains the same.

First step, remove b_0: By the induction hypothesis (IH) and propositional logic, there exists a $c_0 \in \mathcal{C}$ such that $\vdash \chi \rightarrow c_0 \not\leq \bigsqcup \mathcal{B} \backslash \{b_0\}$. Given that $c_0 \leq \bigsqcup \mathcal{B}$, $\mathsf{Atom}(b_0)$ and $\mathsf{Atom}(c_0)$ are also provable from χ, we can apply Lemma 4.18 and obtain $\vdash \chi \rightarrow (\bigsqcup \mathcal{B} \equiv (\bigsqcup (\mathcal{B} \backslash \{b_0\}) \sqcup \{c_0\}))$.

Steps 2–n. Suppose we have a set $\mathcal{C}'$ of l elements such that for $\mathcal{B}' = \{b_l, \ldots, b_{n-1}\}$ we have

$$\vdash \chi \rightarrow \left(\bigsqcup \mathcal{B} \equiv \left(\bigsqcup \mathcal{B}' \sqcup \bigsqcup \mathcal{C}' \right) \right).$$

Now we remove b_l and obtain a $c_l \in \mathcal{C} \backslash \mathcal{C}'$ in a completely similar way as in step 1, such that

$$\vdash \chi \rightarrow \left(\bigsqcup \mathcal{B} \equiv \left(\bigsqcup (\mathcal{B}' \backslash \{b_l\}) \sqcup \bigsqcup (\mathcal{C}' \cup \{c_l\}) \right) \right).$$

Final step. After n steps, we have a set $\mathcal{C}' \subsetneq \mathcal{C}$ such that $\vdash \chi \rightarrow (\bigsqcup \mathcal{B} \equiv \bigsqcup \mathcal{C}')$. We know there exists a $c \in \mathcal{C} \backslash \mathcal{C}'$ for which we have $\vdash \chi \rightarrow \bigwedge_{c' \in \mathcal{C}'} c \perp c'$ and therefore by Corollary 4.8, we have $\vdash \chi \rightarrow (c \perp \bigsqcup \mathcal{C}')$, which means $\vdash \chi \rightarrow (c \not\leq \bigsqcup \mathcal{B})$. Recall that $c \leq \bigsqcup \mathcal{B}$ is a conjunct of χ. Thus $\vdash \chi \rightarrow \mathtt{ff}$. □

Now we can show that each basis contains the same number of atoms.

Theorem 4.20 *For any two finite sets of formulas $\mathcal{B}$ and $\mathcal{C}$ such that $|\mathcal{B}| = |\mathcal{C}|$ the following formula is deducible.*

$$\vdash \mathit{Basis}(\mathcal{B}) \wedge \bigwedge_{c \in \mathcal{C}} \left(\mathit{Atom}(c) \wedge \bigwedge_{c' \in \mathcal{C} \backslash \{c\}} (c \perp c') \right) \rightarrow \mathit{Basis}(\mathcal{C}).$$

Proof We first abbreviate the antecedent with:

$$\psi := \mathsf{Basis}(\mathcal{B}) \wedge \bigwedge_{c \in \mathcal{C}} \left(\mathsf{Atom}(c) \wedge \bigwedge_{c' \in \mathcal{C} \backslash \{c\}} (c \perp c') \right).$$

We wish to show that $\vdash \psi \rightarrow \mathsf{Basis}(\mathcal{C})$. As many conditions for $\mathcal{C}$ to be a basis are already in ψ, it suffices to show that $\vdash \psi \rightarrow (\bigsqcup \mathcal{C} \equiv \mathtt{tt})$. Since $\vdash \psi \rightarrow \mathsf{Basis}(\mathcal{B})$, it suffices to show $\vdash \psi \rightarrow (\bigsqcup \mathcal{C} \equiv \bigsqcup \mathcal{B})$. To prove this, we follow a similar construction as was given in the inductive step for Lemma 4.19. We enumerate $\mathcal{B} = \{b_0, \ldots, b_{n-1}\}$, and will replace these elements with elements of $\mathcal{C}$ one by one.

First step, remove b_0: by Lemma 4.19, there is a $c_0 \in \mathcal{C}$, such that $\vdash \psi \rightarrow c_0 \not\leq \bigsqcup \mathcal{B} \backslash \{b_0\}$. Just as we did in the proof of Lemma 4.19, we then apply Lemma 4.18 and obtain $\vdash \psi \rightarrow (\bigsqcup \mathcal{B} \equiv (\bigsqcup (\mathcal{B} \backslash \{b_0\}) \sqcup \{c_0\}))$. Note that the only difference between this step and that of the proof of Lemma 4.19 is that we applied Lemma 4.19 directly rather than used induction. Steps 2–n differ from those of Lemma 4.19 in precisely the same way.

In the final step we have obtained a set $\mathcal{C}' \subseteq \mathcal{C}$ such that $\vdash \psi \rightarrow (\bigsqcup \mathcal{B} \equiv \bigsqcup \mathcal{C}')$ and $|\mathcal{B}| = |\mathcal{C}'|$. But we know that $|\mathcal{C}| = |\mathcal{B}|$ and therefore $\mathcal{C} = \mathcal{C}'$ (thus instead of a contradiction we get the desired result). □

Corollary 4.21 *If $\mathfrak{M} \vDash \mathit{Basis}(\mathcal{B})$ and $\mathfrak{M} \vDash \mathit{Basis}(\mathcal{C})$ then $|\mathcal{B}| = |\mathcal{C}|$.*

For most protocols, we do not just require a basis for the whole system, but a basis for each local subsystem. In those cases, the basis for the whole system will be the tensor product of the basis for the local subsystems. We will refer to these basis as locally orthogonal (fully) separable orthobasis (LOSB), which can be expressed by

$$\begin{aligned} \mathsf{LOSB}(\mathcal{B}) := \mathsf{Basis}(\mathcal{B}) &\wedge \bigwedge_{b \in \mathcal{B}} \mathsf{Sep}(b) \\ &\wedge \bigwedge_{i < N} \bigwedge_{b \in \mathcal{B}} \bigwedge_{c \in \mathcal{B}} (b_{\{i\}} \equiv c_{\{i\}} \vee b_{\{i\}} \perp c_{\{i\}}) \\ &\wedge \bigwedge_{b \in \mathcal{B}} \bigwedge_{i < N} \bigvee_{c \in \mathcal{B}} (b_{\{i\}} \not\equiv c_{\{i\}}). \end{aligned}$$

The second to last line asserts that local components that are not equal must be orthogonal, and the last line asserts that each local component has dimension at least two.

The following lemma states that any LOSB $\mathcal{B}$ is the tensor product of its local states.

Lemma 4.22 *For a finite set of formulas $\mathcal{B}$, Let $\mathcal{B}^N$ be the set of functions from $\{0, \ldots, N-1\}$ to $\mathcal{B}$.*

The following formula is deducible:

$$\vdash \mathit{LOSB}(\mathcal{B}) \rightarrow \bigwedge_{f \in \mathcal{B}^N} \bigvee_{b \in \mathcal{B}} \bigwedge_{i < N} \left(b_{\{i\}} \equiv f(i)_{\{i\}} \right).$$

Proof Let χ be the negation of what we are trying to prove:
Let

$$\chi := \mathsf{LOSB}(\mathcal{B}) \wedge \neg \left(\bigwedge_{f \in \mathcal{B}^N} \bigvee_{b \in \mathcal{B}} \bigwedge_{i<N} (b_{\{i\}} \equiv f(i)_{\{i\}}) \right).$$

It suffices to show that $\vdash \chi \to \mathtt{ff}$. First note that

$$\vdash \chi \to \left(\bigvee_{f \in \mathcal{B}^N} \bigwedge_{b \in \mathcal{B}} \bigvee_{i<N} (b_{\{i\}} \not\equiv f(i)_{\{i\}}) \right).$$

Furthermore by definition of LOSB and propositional logic, for every $f \in \mathcal{B}^N$ and $b \in \mathcal{B}$,

$$\vdash \mathsf{LOSB}(\mathcal{B}) \to \left(\left(b_{\{i\}} \not\equiv f(i)_{\{i\}}\right) \to \left(b_{\{i\}} \perp f(i)_{\{i\}}\right) \right).$$

Thus

$$\vdash \chi \to \left(\bigvee_{f \in \mathcal{B}^N} \bigwedge_{b \in \mathcal{B}} \bigvee_{i<N} (b_{\{i\}} \perp f(i)_{\{i\}}) \right).$$

By $\mathsf{A6}$ we have $\vdash \chi \to (\bigvee_{f \in \mathcal{B}^N} \bigwedge_{b \in \mathcal{B}} (b \perp f(i)))$. Then by Lemma 4.8, $\vdash \chi \to (\bigvee_{f \in \mathcal{B}^N} (f(i) \perp \bigsqcup \mathcal{B}))$. Written another way, we have $\vdash \chi \to (\bigvee_{f \in \mathcal{B}^N} (\bigsqcup \mathcal{B} \leq \sim f(i)))$.

By modal reasoning $\vdash \mathtt{tt} \equiv \sim \mathtt{ff}$ and by Lemma 4.5-(4.6), $\vdash (\phi \not\equiv \mathtt{ff}) \leftrightarrow (\sim\phi \not\equiv \mathtt{tt})$. As for each $i < N$, $f(i) \in \mathcal{B}$ and $f(i) \not\equiv \mathtt{ff}$ is a conjunct of $\mathsf{SubBasis}(\mathcal{B})$ and hence a conjunct of χ, we have that $\vdash \chi \to (\sim f(i) \not\equiv \mathtt{tt})$. As $\vdash (\phi \leq \psi) \wedge (\psi \not\equiv \mathtt{tt}) \to (\phi \not\equiv \mathtt{tt})$, we have from this and $\vdash \chi \to (\bigvee_{f \in \mathcal{B}^N} (\bigsqcup \mathcal{B} \leq \sim f(i)))$ that $\vdash \chi \to (\bigsqcup \mathcal{B} \not\equiv \mathtt{tt})$. This together with the fact that $\bigsqcup \mathcal{B} = \mathtt{tt}$ is a conjunct of $\mathsf{SubBasis}(\mathcal{B})$ and hence of χ gives us that $\vdash \chi \to \mathtt{ff}$. □

Given two LOSBs $\mathcal{B}$ and $\mathcal{C}$, we can construct a new LOSB $\mathcal{D}$, such that for all $i < N$, either for all $d \in \mathcal{D}$ we have $d_{\{i\}} \equiv b_{\{i\}}$ for some $b \in \mathcal{B}$ or for all $d \in \mathcal{D}$ we have $d_{\{i\}} \equiv c_{\{i\}}$ for some $c \in \mathcal{C}$. The following lemma proves this fact.

Lemma 4.23 *Let $\mathcal{B}, \mathcal{C}$ and $\mathcal{D}$ be three sets of proposition letters of equal size, i.e., $|\mathcal{B}| = |\mathcal{C}| = |\mathcal{D}|$. The following formula is deducible:*

$$\vdash \mathit{Ant} \to \mathit{LOSB}(\mathcal{D}).$$

where

$$\begin{aligned} \mathit{Ant} := {} & \mathit{LOSB}(\mathcal{B}) \wedge \mathit{LOSB}(\mathcal{C}) \\ & \wedge \bigwedge_{d \in \mathcal{D}} \mathsf{Sep}(d) \wedge \bigwedge_{d \neq d' \in \mathcal{D}} d \not\equiv d' \\ & \wedge \bigwedge_{i<N} \left(\begin{array}{l} \left(\bigwedge_{d \in \mathcal{D}} \bigvee_{b \in \mathcal{B}} d_{\{i\}} \equiv b_{\{i\}} \right) \\ \vee \left(\bigwedge_{d \in \mathcal{D}} \bigvee_{c \in \mathcal{C}} d_{\{i\}} \equiv c_{\{i\}} \right) \end{array} \right) \end{aligned}$$

Proof To show $\vdash \mathsf{Ant} \to \mathsf{LOSB}(\mathcal{D})$ it suffices to show that $\mathsf{Basis}(\mathcal{D})$, $\bigwedge_{d \in \mathcal{D}} \mathsf{Sep}(d)$,

$$\bigwedge_{i<N} \bigwedge_{d \in \mathcal{D}} \bigwedge_{d' \in \mathcal{D}} \left((d_{\{i\}} \equiv d'_{\{i\}}) \vee (d_{\{i\}} \perp d'_{\{i\}}) \right), \tag{4.26}$$

and

$$\bigwedge_{i<N} \bigwedge_{d \in \mathcal{D}} \bigvee_{d' \in \mathcal{D}} (d_{\{i\}} \not\equiv d'_{\{i\}}) \tag{4.27}$$

are provable from Ant.

By extracting a conjunct from Ant, we already have $\vdash \mathsf{Ant} \to \bigwedge_{d \in \mathcal{D}} \mathsf{Sep}(d)$.

As an intermediate step, we show that $\vdash \mathsf{Ant} \to \bigwedge_{d \in \mathcal{D}} \mathsf{Atom}(d)$. By axiom $\mathsf{A4}$ we have $\vdash \mathsf{Ant} \to T(b_{\{i\}})$ and $\vdash \mathsf{Ant} \to T(c_{\{i\}})$ for all $b \in \mathcal{B}$, $c \in \mathcal{C}$ and $i < N$. As Ant asserts the equivalence of each $d_{\{i\}}$ with either $b_{\{i\}}$ or $c_{\{i\}}$, propositional reasoning gives us $\vdash \mathsf{Ant} \to T(d_{\{i\}})$ for all $d \in \mathcal{D}$ and $i < N$. So, by axiom $\mathsf{A4}$, we have $\vdash \mathsf{Ant} \to \mathsf{Atom}(d)$ for all $d \in \mathcal{D}$.

We next show that (4.26) is provable from Ant. By propositional logic, using the conjunct for $\mathsf{LOSB}(\mathcal{B})$ and for $\mathsf{LOSB}(\mathcal{C})$, we have

$$\vdash \mathsf{Ant} \to \bigwedge_{i<N} (\chi(\mathcal{B}) \vee \chi(\mathcal{C})),$$

where

$$\chi(\mathcal{B}) := \bigwedge_{d,d' \in \mathcal{D}} \bigvee_{b,b' \in \mathcal{B}} \left((d_{\{i\}} \equiv b_{\{i\}}) \wedge (d'_{\{i\}} \equiv b'_{\{i\}}) \wedge \left(\left(b_{\{i\}} \equiv b'_{\{i\}}\right) \vee (b_{\{i\}} \perp b_{\{i\}}) \right) \right).$$

Then by modal logic we have

$$\vdash \chi(\mathcal{B}) \to \bigwedge_{d,d' \in \mathcal{D}} \left(\left(d_{\{i\}} \equiv d'_{\{i\}}\right) \vee \left(d_{\{i\}} \perp d_{\{i\}}\right) \right)$$

and similarly

$$\vdash \chi(\mathcal{C}) \to \bigwedge_{d,d' \in \mathcal{D}} \left(\left(d_{\{i\}} \equiv d'_{\{i\}} \right) \vee \left(d_{\{i\}} \perp d_{\{i\}} \right) \right)$$

Putting these together, we obtain by propositional logic

$$\vdash \mathsf{Ant} \to \bigwedge_{i<N} \bigwedge_{d \in \mathcal{D}} \bigwedge_{d' \in \mathcal{D}} \left(\left(d_{\{i\}} \equiv d'_{\{i\}} \right) \vee \left(d_{\{i\}} \perp d'_{\{i\}} \right) \right)$$

To show $\vdash \mathsf{Ant} \to \mathsf{Basis}(\mathcal{D})$, by Theorem 4.20, it remains to show that $\vdash \mathsf{Ant} \to \bigwedge_{d \neq d' \in \mathcal{D}} d \perp d'$. For each $d, d' \in \mathcal{D}$, because $\mathsf{Sep}(d)$ is a conjunct of Ant for each $d \in \mathcal{D}$, and because $\vdash \mathsf{Ant} \to \bigwedge_{d \in \mathcal{D}} \mathsf{Atom}(d)$, we apply axiom A5 to get

$$\vdash \mathsf{Ant} \to \bigwedge_{d,d' \in \mathcal{D}} \left((d \equiv d') \leftrightarrow \bigwedge_{i} \left(d_{\{i\}} \equiv d'_{\{i\}} \right) \right).$$

Then

$$\vdash \mathsf{Ant} \to \bigwedge_{d \neq d' \in \mathcal{D}} \bigvee_{i} \left(d_{\{i\}} \not\equiv d'_{\{i\}} \right).$$

Because

$$\vdash \mathsf{Ant} \to \bigwedge_{d \in \mathcal{D}} \bigwedge_{d' \in \mathcal{D}} \bigwedge_{i<N} \left(\left(d_{\{i\}} \equiv d'_{\{i\}} \right) \vee \left(d_{\{i\}} \perp d'_{\{i\}} \right) \right),$$

we have by propositional logic

$$\vdash \mathsf{Ant} \to \bigwedge_{d \neq d' \in \mathcal{D}} \bigvee_{i} (d_{\{i\}} \perp d'_{\{i\}})$$

Thus by axiom A6, $\vdash \mathsf{Ant} \to \bigwedge_{d \neq d' \in \mathcal{D}} (d \perp d')$.

To show (4.27), let us fix an $i < N$ and let $\phi(i, \mathcal{B})$ be

$$\phi(i, \mathcal{B}) := \bigvee_{d \in \mathcal{D}} \bigwedge_{d' \in \mathcal{D}} (d_{\{i\}} \equiv d'_{\{i\}}) \wedge \bigwedge_{d \in \mathcal{D}} \bigvee_{b \in \mathcal{B}} (d_{\{i\}} \equiv b_{\{i\}}).$$

So for a fixed i we assume the negation of (4.27) and we assume all $d \in \mathcal{D}$ are equal to some $b \in \mathcal{B}$ at location i. We wish to show $\vdash \mathsf{Ant} \wedge \phi(i, \mathcal{B}) \to \mathtt{ff}$.

By definition of $\equiv$ and modal reasoning, the first conjunct of $\phi(i, \mathcal{B})$ implies $\bigwedge_{d,d' \in \mathcal{D}} (d_{\{i\}} \equiv d'_{\{i\}})$, that is, all $d \in \mathcal{D}$ are locally equivalent at location i. Combined with the second conjunct we get

$$\vdash \mathsf{Ant} \wedge \phi(i, \mathcal{B}) \to \bigvee_{b \in \mathcal{B}} \bigwedge_{d \in \mathcal{D}} \left(d_{\{i\}} \equiv b_{\{i\}} \right).$$

As $\mathsf{LOSB}(\mathcal{B})$ is a conjunct of Ant, we have

$$\bigwedge_{b \in \mathcal{B}} \bigvee_{b' \in \mathcal{B}} \left(b_{\{i\}} \not\equiv b'_{\{i\}} \right).$$

Moreover, we have

$$\bigwedge_{b,b' \in \mathcal{B}} \left((b_{\{i\}} \equiv b'_{\{i\}}) \vee (b_{\{i\}} \perp b'_{\{i\}}) \right).$$

Using propositional reasoning we obtain

$$\vdash \mathsf{Ant} \wedge \phi(i, \mathcal{B}) \to \bigvee_{b \in \mathcal{B}} \bigwedge_{d \in \mathcal{D}} (d_{\{i\}} \perp b_{\{i\}}).$$

By axiom A6, this implies

$$\vdash \mathsf{Ant} \wedge \phi(i, \mathcal{B}) \to \bigvee_{b \in \mathcal{B}} \bigwedge_{d \in \mathcal{D}} (d \perp b).$$

Now we can apply Corollary 4.8

$$\vdash \mathsf{Ant} \wedge \phi(i, \mathcal{B}) \to \bigvee_{b \in \mathcal{B}} \left(b \perp \bigsqcup \mathcal{D} \right).$$

We have already shown that $\vdash \mathsf{Ant} \to \mathsf{Basis}(\mathcal{D})$, and as $\bigsqcup \mathcal{D} \equiv \mathtt{tt}$ is a conjunct of $\mathsf{Basis}(\mathcal{D})$ we conclude

$$\vdash \mathsf{Ant} \wedge \phi(i, \mathcal{B}) \to \mathtt{ff}.$$

We can show this result for any $i < N$ and replacing $\mathcal{B}$ by $\mathcal{C}$. As a result we get

$$\vdash \mathsf{Ant} \wedge \bigvee_{i<N} \bigvee_{d \in \mathcal{D}} \bigwedge_{d' \in \mathcal{D}} (d_{\{i\}} \equiv d'_{\{i\}}) \to \mathtt{ff}.$$

This is equivalent to the desired result:

$$\vdash \mathsf{Ant} \to \bigwedge_{i<N} \bigwedge_{d \in \mathcal{D}} \bigvee_{d' \in \mathcal{D}} (d_{\{i\}} \not\equiv d'_{\{i\}}).$$

□

5 Examples

In this section, we will discuss how to express and prove correctness for two quantum protocols: the quantum leader election protocol (Sect. 5.1) and the BB84 quantum key distribution protocol (Sect. 5.2).

5.1 Example 1: quantum leader election

The quantum leader election protocol aims to randomly select a leader in a group of agents such that each agent has equal probability to be selected as the leader. There exist several ways to solve this problem using quantum theory, e.g., D'Hondt and Panangaden (2006a) and Tani et al. (2012). The ones given in Tani et al. (2012) rely heavily on communication, and as we do not explicitly model communication, we

will discuss the version given in D'Hondt and Panangaden (2006a), which omits explicit communication.

Given a set N of agents, the protocol assigns a quantum bit (a two dimensional Hilbert space) to each agent $i \in N$ together with a basis $\{|0\rangle_i, |1\rangle_i\}$. Then the following state, called the W-state, is considered:

$$\sum_{i\in N} \frac{1}{\sqrt{N}} \left(\bigotimes^{\mathfrak{M}}_{j\in N\setminus\{i\}} |0\rangle_j \right) \otimes^{\mathfrak{M}} |1\rangle_i .$$

This state entangles the qubits in such a way that, after the agents measure their qubit, only one agent measures $|1\rangle$ and all other agents measure $|0\rangle$.

In our logic, we express and prove the existence of the W-state, showing that it has the desired probabilistic behavior. Our formula for correctness applies not only to the case where each agent has a qubit, but where each agent has a Hilbert space with dimension at least 2 (no smaller than a qubit). We could alternatively have enforced the property that each agent has precisely one qubit using as a conjunct

$$\begin{aligned}\mathsf{LOSB}(\mathcal{B}) \to \bigwedge_{i<N} \bigwedge_{b,c,d\in\mathcal{B}} ((b_{\{i\}} \perp c_{\{i\}}) \\ \to ((d_{\{i\}} \equiv b_{\{i\}}) \vee (d_{\{i\}} \equiv c_{\{i\}}))),\end{aligned}$$

and the proofs in this section would have been essentially the same.

Let $\mathcal{B}$ be a LOSB. Then an ordered subset $\mathcal{W} = \{W^i \mid i \in N+1\} \subset \mathcal{B}$ is *Quantum Leader Election compatible* (QLE compatible) if the following formula is satisfied (somewhere in) $\mathfrak{M}$:

$$\mathsf{QLE}(\mathcal{W}) := \bigwedge_{i\in N} \left(\begin{array}{c} \left(W^i_{\{i\}} \not\equiv W^N_{\{i\}}\right) \\ \wedge \bigwedge_{j\in N\setminus i} \left(W^i_{\{j\}} \equiv W^N_{\{j\}}\right) \end{array} \right).$$

We interpret this formula as follows. The last element W^N should be seen as the tensor product $\bigotimes^{\mathfrak{M}}_{i\in N} \mathbf{0}_i$, where $\mathbf{0}_i$ is the qubit for agent i corresponding to the classical bit 0 (one of the basis elements of the qubit). For $i < N$, the element W^i is similarly a tensor product of classical bits, where each component $k \neq i$ is similarly $\mathbf{0}_k$, but where component $k = i$ is $\mathbf{1}_k$ instead. Note that we are interpreting basis elements of the components as classical bits, rather that defining the basis elements of the components with respect to predetermined classical bits.

The *correctness* of the quantum leader election is expressed by

$$\mathsf{QLE\text{-}Cor}(\mathcal{B}) := \mathsf{LOSB}(\mathcal{B}) \to \bigvee_{\mathcal{W}\subset_{N+1}\mathcal{B}} \left(\begin{array}{l} \mathsf{QLE}(\mathcal{W}) \wedge \\ \exists \bigwedge_{i<N} \Pr(W^i) = \frac{1}{N} \end{array} \right),$$

where $\mathcal{W} \subset_{N+1} \mathcal{B}$ ranges over all subsets $\{W^0, \ldots, W^N\}$ of $\mathcal{B}$ of size $N+1$.

We will first show that for any set $\mathcal{B} = \{b_0, \ldots, b_{n-1}\}$ of n pairwise orthogonal properties we have a state that has probability $\frac{1}{n}$ for each property in $\mathcal{B}$. Let us define

$$\mathsf{Ort}(\mathcal{B}) := \bigwedge_{i<n} (T(b_i) \wedge (b_i \not\equiv \mathtt{ff})) \wedge \bigwedge_{i<j<n} b_i \perp b_j .$$

Proposition 5.1 *For all $n \geq 1$ and for any set $\mathcal{B} = \{b_0, \ldots, b_{n-1}\}$ of n formulas, the following formula is deducible.*

$$\vdash \mathsf{Ort}(\mathcal{B}) \to \exists \left(\bigwedge_{i\in n} \Pr(b_i) = \frac{1}{n} \right).$$

Proof With induction: for $n = 1$ we have $\vdash \mathsf{Ort}(\mathcal{B}) \to (b \not\equiv \mathtt{ff})$, which by Lemma 4.4 implies $\vdash \mathsf{Ort}(\mathcal{B}) \to \exists b$. By Lemma 4.12-(4.25), we have $\vdash b \to \Pr(b) = 1$, so we have $\vdash \mathsf{Ort} \to \exists(\Pr(b) = 1)$, which finishes the case $n = 1$.

Induction hypothesis (IH): suppose for n we have $\vdash \mathsf{Ort}(\mathcal{B}_n) \to \exists(\bigwedge_{i\in n} \Pr(b_i) = \frac{1}{n})$. Let $\mathcal{B}_{n+1} = \mathcal{B}_n \cup \{b_n\}$. In Table 13, we show how to deduce

$$\vdash \mathsf{Ort}(\mathcal{B}_{n+1}) \to \exists \left(\bigwedge_{i\leq n+1} \Pr(b_i) = \frac{1}{n+1} \right)$$

□

The following theorem proves the correctness of the quantum leader election.

Theorem 5.2 *For any finite set of formulas $\mathcal{B}$, it is provable that $\vdash$ QLE-Cor($\mathcal{B}$), that is,*

$$\vdash \mathit{LOSB}(\mathcal{B}) \to \bigvee_{\mathcal{W}\subset_{N+1}\mathcal{B}} \left(\begin{array}{l} \mathsf{QLE}(\mathcal{W}) \\ \wedge \exists \bigwedge_{i<N} \Pr(W^i) = \frac{1}{N} \end{array} \right),$$

where $\mathcal{W} \subset_{N+1} \mathcal{B}$ ranges over all subsets $\{W^0, \ldots, W^N\}$ of $\mathcal{B}$ of size $N+1$.

Proof For any $\mathcal{W} = \{W^0, \ldots, W^N\} \subset_{N+1} \mathcal{B}$, we can extract conjuncts from $\mathsf{LOSB}(\mathcal{B})$ and apply Lemma 4.11 to obtain $\vdash \mathsf{LOSB}(\mathcal{B}) \to \mathsf{Ort}(\mathcal{W})$. It is easy to see that for any

Table 13 A proof of $\mathsf{Ort}(\mathcal{B}_{n+1}) \to \exists\left(\bigwedge_{i\leq n+1} \Pr(b_i) = \frac{1}{n+1}\right)$

1	$\mathsf{Ort}(\mathcal{B}_{n+1}) \to \exists b_n$	Lemma 4.4
2	$\mathsf{Ort}(\mathcal{B}_{n+1}) \to \exists\left(\bigwedge_{i<n} \Pr(b_i) = \frac{1}{n}\right)$	IH
3	$\mathsf{Ort}(\mathcal{B}_{n+1}) \to (b_n \perp \bigsqcup_{i\in n} b_i)$	Corollary 4.8
4	$\mathsf{Ort}(\mathcal{B}_{n+1}) \to (\bigwedge_{i<n} \Pr(b_i) = \frac{1}{n}) \leq (\bigsqcup_{i<n} b_i)$	Corollary 4.15
5	$\mathsf{Ort}(\mathcal{B}_{n+1}) \to (b_n \perp (\bigwedge_{i<n} \Pr(b_i) = \frac{1}{n}))$	ML(3,4)
6	$\mathsf{Ort}(\mathcal{B}_{n+1}) \to \exists\begin{pmatrix}\langle b_n ?\rangle_{=\frac{1}{n+1}} b_n \\ \wedge \langle q ?\rangle_{=\frac{n}{n+1}} q\end{pmatrix}$ with $q = \bigwedge_{i<n} \Pr(b_i) = \frac{1}{n}$	P6
7	$\mathsf{Ort}(\mathcal{B}_{n+1}) \to \exists\left(\Pr(b_n) = \frac{1}{n+1} \wedge \bigwedge_{i<n} \Pr(b_i) = \frac{1}{n+1}\right)$	Lemma 4.16
8	$\mathsf{Ort}(\mathcal{B}_{n+1}) \to \exists\left(\bigwedge_{i\leq n+1} \Pr(b_i) = \frac{1}{n+1}\right)$	PL(8)

$\mathcal{W}' \subset_N \mathcal{W}$, we have that $\vdash \mathsf{Ort}(\mathcal{W}) \to \mathsf{Ort}(\mathcal{W}')$. Thus by this and Proposition 5.1, we have for any $\mathcal{W} \subset_{N+1} \mathcal{B}$

$$\vdash \mathsf{LOSB}(\mathcal{B}) \to \exists\left(\bigwedge_{i<N} \Pr(W^i) = \frac{1}{N}\right). \tag{5.1}$$

To show that $\vdash \mathsf{LOSB}(\mathcal{B}) \to \bigvee_{\mathcal{W}\subset_{N+1}\mathcal{B}} \mathsf{QLE}(\mathcal{W})$, we select any $b \in \mathcal{B}$ to be W^N. Note that

$$\vdash \mathsf{LOSB}(\mathcal{B}) \to \bigvee_{\{b^i \mid i<N\}\subset\mathcal{B}} \left(\bigwedge_{i<N} (b^i_{\{i\}} \not\equiv W^N_{\{i\}})\right). \tag{5.2}$$

For a given set $\mathcal{V} = \{b^i \mid i < N\} \subset \mathcal{B}$ and each $i < N$, let $f_i^{\mathcal{V}} : \{0, \ldots, N-1\} \to \mathcal{B}$, such that $f_i^{\mathcal{V}}(j) = W^N$ if $i \neq j$ and $f_i^{\mathcal{V}}(i) = b^i$. Then for each $i < N$, we can apply Lemma 4.22 using $f_i^{\mathcal{V}}$ to obtain a $W^i \in \mathcal{B}$ such that $W^i_{\{i\}} \equiv b^i_{\{i\}}$ and $W^i_{\{j\}} \equiv W^N_{\{j\}}$ for any $j \neq i$. By (5.2) we know that for some $\mathcal{V} \subset \mathcal{B}$ the resulting set $\mathcal{W} = \{W^0, \ldots, W^{N-1}, W^N\}$ will be QLE compatible. Hence, using Lemma 4.22 and (5.2), we obtain $\vdash \mathsf{LOSB}(\mathcal{B}) \to \bigvee_{\mathcal{W}\subset_{N+1}\mathcal{B}} \mathsf{QLE}(\mathcal{W})$. The desired result follows from this, (5.1), and propositional logic. □

5.2 Example 2: BB84

The BB84 protocol is designed to provide two agents with the same random bitstring, to be used as a key for both encryption and description. The protocol works as follows: the first agent Alice has the ability to produce qubits in two different basis: $\{|0\rangle, |1\rangle\}$ and $\{|-\rangle, |+\rangle\}$. Alice chooses two equally sized random bitstrings; the first is the message to be sent, the second determines the basis in which each individual bit of the message bitstring is sent. She sends the qubits to Bob, who has chosen a random bitstring as well to determine which basis he uses to measure each received qubit. After all qubits have been sent and measured, Alice and Bob publicly compare the basis bitstring they have used to create and measure the qubits respectively. On those positions where the basis bitstring matches, the corresponding bit in the message bitstring should correspond as well. On all other positions, those bits in the message bitstring could be different and are thus discarded. In the end, Alice and Bob have a corresponding random bitstring which is in general about half the size of the random bitstring Alice started with. Of course, this is in the ideal situation where no eavesdropper disturbs the channel. This section proves properties of this ideal situation.

We first need to characterize the message space. Let us fix the number of qubits at N and let $\mathfrak{M}$ be the tensor product of N identical two dimensional quantum models. Let $\mathcal{B}_1$ and $\mathcal{B}_+$ be two LOSB's that are locally probabilistically far apart (PFA), that is

$$\mathsf{PFA}(\mathcal{B}_1, \mathcal{B}_+) := \mathsf{LOSB}(\mathcal{B}_1) \wedge \mathsf{LOSB}(\mathcal{B}_+) \wedge \bigwedge_{b\in\mathcal{B}_1} \bigwedge_{c\in\mathcal{B}_+} \bigwedge_{i<N} \begin{pmatrix} b \leq \left(\Pr(c_{\{i\}}) = \frac{1}{2}\right) \\ \wedge\, c \leq \left(\Pr(b_{\{i\}}) = \frac{1}{2}\right)\end{pmatrix}$$

Intuitively, $\mathcal{B}_1$ represents the N tensor product of the local basis $\{|0\rangle, |1\rangle\}$ and $\mathcal{B}_+$ represents the N tensor product of the local basis $\{|-\rangle, |+\rangle\}$. We introduce two new abbreviations for the remainder of this section:

$$m_{\{i\}} \in \{0,1\} := \bigvee_{b\in\mathcal{B}_1} m_{\{i\}} \equiv b_{\{i\}},$$
$$m_{\{i\}} \in \{-,+\} := \bigvee_{b\in\mathcal{B}_+} m_{\{i\}} \equiv b_{\{i\}}.$$

The message space $\mathcal{M}$ of 4^N proposition letters can be defined by requiring each proposition to be locally equivalent either to some $b \in \mathcal{B}_1$ or to some $b \in \mathcal{B}_+$.

$$\mathsf{Mes}(\mathcal{M}) := \bigwedge_{m\in\mathfrak{M}} \mathsf{Sep}(m) \wedge \bigwedge_{m\in\mathfrak{M}} \begin{pmatrix} \bigwedge_{i<N} \bigvee_{a\in\mathcal{B}_1\cup\mathcal{B}_+} (m_{\{i\}} \equiv a_{\{i\}}) \\ \wedge \bigwedge_{m'\in\mathfrak{M}\setminus\{m\}} (m \not\equiv m')\end{pmatrix}.$$

Let k be some element of $\mathcal{M}$. This represents Ann's message and choice of basis for each component.

For any string $s \in \{1, +\}^N$, let s_i denote the i'th coordinate. We define the set of propositions $\mathcal{B}_s \subseteq \mathcal{M}$ by

$$\mathcal{B}_s := \left\{ b \in \mathcal{M} \;\middle|\; b_{\{i\}} \equiv b'_{\{i\}} \quad \begin{array}{l} \text{for some } b' \in \mathcal{B}_{s_i} \\ \text{for all } i < N \end{array} \right\}.$$

In words, $\mathcal{B}_s$ is the set of formulas where the i'th coordinate of each element b of $\mathcal{B}_s$ is in $\{0, 1\}$ if the i'th coordinate of s is 1, and where the i'th coordinate of b in $\{-, +\}$ otherwise. Note that by Lemma 4.23, for each $s \in \{1, +\}^N$ the resulting set $\mathcal{B}_s$ is an LOSB.

Furthermore, given a string $s \in \{1, +\}^N$, define the term abbreviation:

- $\Pr_s(\phi) := \sum_{b \in \mathcal{B}_s} \Pr(b \wedge \phi)$
- $\Pr_{\mathcal{M}}(\phi) := \sum_{s \in \{1,+\}^N} \frac{1}{2^N} \Pr_s(\phi)$

The term $\Pr_s(\phi)$ represents the probability of ϕ holding true after measuring the state using basis $\mathcal{B}_s$, in the event that ϕ is testable (ϕ needs to be testable for this reading to hold). The term $\Pr_{\mathcal{M}}(\phi)$ represents the probability of ϕ holding true after using a randomly selected one of the 2^N chosen bases of states in $\mathcal{M}$.

The correctness of the BB84 protocol, when there is no eavesdropper, can be expressed by

$$\mathsf{Ant} \to \Pr_{\mathcal{M}}(\mathsf{Match}) = 1,$$

where

$$\mathsf{Ant} := \mathsf{PFA}(\mathcal{B}_1, \mathcal{B}_+) \wedge \mathsf{Mes}(\mathcal{M}) \wedge k$$

and Match states that at those coordinates where the choice of basis of Alice and Bob agree, Bob's measured result agrees with Alice's original message k. Formally this is expressed by

$$\mathsf{Match} := \bigwedge_{i<N} \begin{pmatrix} \mathsf{BasisOf}(k_{\{i\}}) \\ \to \bigvee \{m \in \mathcal{M} \mid m_{\{i\}} \equiv k_{\{i\}}\} \end{pmatrix},$$

where

$$\mathsf{BasisOf}(k_{\{i\}}) = \begin{cases} \bigvee \{m \in \mathcal{M} \mid m_{\{i\}} \in \{0, 1\}\} \\ \qquad\qquad \text{if } k_{\{i\}} \in \{0, 1\}, \\ \bigvee \{m \in \mathcal{M} \mid m_{\{i\}} \in \{-, +\}\} \\ \qquad\qquad \text{if } k_{\{i\}} \in \{-, +\}. \end{cases}$$

The probability of Match being equal to 1 reflects that without interference Bob should have received Ann's message perfectly among those coordinates where they used the same basis.

Lemma 5.3 *The following formula is deducible.*

$$\vdash \mathsf{Ant} \to \Pr_{\mathcal{M}}(\mathsf{Match}) = 1.$$

Proof We will first show $\vdash \mathsf{Ant} \to \Pr_s(\mathsf{Match}) = 1$ for all $s \in \{1, +\}^N$. The desired result will then follow from the inequality axioms. By Lemma 4.23, we know $\vdash \mathsf{Ant} \to \mathsf{LOSB}(\mathcal{B}_s)$, and therefore by Lemma 4.17, $\vdash \mathsf{Ant} \to \sum_{b \in \mathcal{B}_s} \Pr(b) = 1$. So all we need to show is that $\vdash \mathsf{Ant} \to \Pr(b) = \Pr(b \wedge \mathsf{Match})$ for all $b \in \mathcal{M}$.

Let us define

$$\mathsf{Match}_i := \begin{pmatrix} \mathsf{BasisOf}(k_{\{i\}}) \\ \to \bigvee \{m \in \mathcal{M} \mid m_{\{i\}} \equiv k_{\{i\}}\} \end{pmatrix}.$$

Thus $\mathsf{Match} = \bigwedge_{i<N} \mathsf{Match}_i$. We will show that for each $b \in \mathfrak{M}$,

$$\vdash \bigwedge_{i<N} (\mathsf{Ant} \to (\Pr(b) = 0 \vee (b \equiv (b \wedge \mathsf{Match}_i)), \tag{5.3}$$

hence

$$\vdash \mathsf{Ant} \to (\Pr(b) = 0 \vee \left(b \equiv \left(b \wedge \bigwedge_{i<N} \mathsf{Match}_i \right) \right))$$

By P4, $\vdash (b \equiv (b \wedge \mathsf{Match}) \to \Pr(b) = \Pr(b \wedge \mathsf{Match})$. By Proposition 4.13, $\vdash (\Pr(b \wedge \mathsf{Match}) \leq \Pr(b))$. Thus by P2 and inequality axioms $\vdash \Pr(b) = 0 \to \Pr(b) = \Pr(b \wedge \mathsf{Match})$. Hence, from (5.3), we use these steps to arrive at $\vdash \mathsf{Ant} \to \Pr(b) = \Pr(b \wedge \mathsf{Match})$.

To prove (5.3), let us fix an $i < N$. We will discuss several cases, expressed by the following formulas:

$$\begin{aligned} \phi &:= b_{\{i\}} \equiv k_{\{i\}} \\ \psi &:= b_{\{i\}} \not\equiv k_{\{i\}} \wedge (b_{\{i\}} \in \{0, 1\} \leftrightarrow k_{\{i\}} \in \{0, 1\}) \\ \chi &:= b_{\{i\}} \not\equiv k_{\{i\}} \wedge (b_{\{i\}} \in \{0, 1\} \leftrightarrow k_{\{i\}} \notin \{0, 1\}) \end{aligned}$$

By propositional logic, we have $\vdash \phi \vee \psi \vee \chi$.

Case ϕ: First note that $\vdash \mathsf{Ant} \wedge \phi \to \bigvee \{b \in \mathcal{M} \mid b_{\{i\}} \equiv k_{\{i\}}\}$

Therefore, we have

$$\vdash \mathsf{Ant} \wedge (b_{\{i\}} \equiv k_{\{i\}}) \to b \leq \begin{pmatrix} \mathsf{BasisOf}(k_{\{i\}}) \\ \to \bigvee \{m \in \mathcal{M} \mid m_{\{i\}} \equiv k_{\{i\}}\} \end{pmatrix}.$$

Rewriting, we have $\vdash \mathsf{Ant} \wedge \phi \to (b \equiv (b \wedge \mathsf{Match}_i))$. Hence $\vdash \mathsf{Ant} \wedge \phi \to (\Pr(b) = 0 \vee (b \equiv (b \wedge \mathsf{Match}_i))$.

Case ψ: By extracting conjuncts from Ant, we have $\vdash \mathsf{Ant} \wedge \psi \rightarrow \mathsf{LOSB}(\mathcal{B}_1) \wedge \mathsf{LOSB}(\mathcal{B}_+)$. Expanding ψ, we have

$$\vdash \mathsf{Ant} \wedge \psi \rightarrow (b_{\{i\}} \in \{0,1\} \wedge k_{\{i\}} \in \{0,1\}) \vee (b_{\{i\}} \in \{-,+\} \wedge k_{\{i\}} \in \{-,+\}).$$

Thus by propositional logic, $\vdash \mathsf{Ant} \wedge \psi \rightarrow (b_{\{i\}} \perp k_{\{i\}})$ for each $i < N$. By axiom A6, $\vdash \mathsf{Ant} \wedge \psi \rightarrow (b \perp k)$ and therefore by axiom P3, $\vdash \mathsf{Ant} \wedge \psi \rightarrow (k \leq \Pr(b) = 0)$. By Lemma 4.2-(4.3), $\vdash \mathsf{Ant} \wedge \psi \rightarrow \Pr(b) = 0$. Hence $\vdash \mathsf{Ant} \wedge \psi \rightarrow (\Pr(b) = 0 \vee (b \equiv (b \wedge \mathsf{Match}_i))$.

Case χ: By expanding χ, we have

$$\vdash \mathsf{Ant} \wedge \chi \rightarrow (b_{\{i\}} \notin \{0,1\} \wedge k_{\{i\}} \in \{0,1\}) \vee (b_{\{i\}} \notin \{-,+\} \wedge k_{\{i\}} \in \{-,+\}).$$

By this and modal logic, we have that $\vdash \mathsf{Ant} \wedge \chi \rightarrow (b \leq \neg\mathsf{BasisOf}(k_{\{i\}}))$. Thus $\vdash \mathsf{Ant} \wedge \chi \rightarrow (b \leq \mathsf{Match}_i)$, which is equivalent to $\vdash \mathsf{Ant} \wedge \chi (b \equiv b \wedge \mathsf{Match}_i)$. Thus $\vdash \mathsf{Ant} \wedge \chi \rightarrow (\Pr(b) = 0 \vee (b \equiv (b \wedge \mathsf{Match}_i))$.

Now we have $\vdash \mathsf{Ant} \wedge \omega \rightarrow (\Pr(b) = 0 \vee (b \equiv (b \wedge \mathsf{Match}_i))$, for each $\omega \in \{\phi, \psi, \chi\}$. Together with $\vdash \phi \vee \psi \vee \chi$, and repeating for each $i < N$, we have (5.3). □

6 Conclusion

This paper lays a foundation for an axiomatization of probabilistic quantum logics in the style of propositional dynamic logic. The axiomatization provided in this work is powerful enough to prove the correctness of quantum protocols, such as the quantum leader election of D'Hondt and Panangaden (2006a) and the BB84 quantum key distribution. As probability plays an important role in so many quantum protocols, we expect that our logic can be used and adapted to a much wider range of quantum protocols. We also hope that future work will clarify the prospects for a complete proof system.

This work may pave the way for powerful axiomatic system of stronger logics. For example, an axiomatic analysis of the construction of the W-state is left for future work; such an analysis would benefit from a more powerful logic that explicitly reasons about unitary operations. When involving unitaries for quantum protocols and programs, it would be further beneficial to either characterize commonly used logic gates, such as the Hadamard gate, or to include them as constants.

Another potential extension of the logic is to add the power to explicitly express both the quantum and classical communication involved in various protocols. This may help in expressing important properties of a communication-rich variant of the quantum leader election protocol given in Tani et al. (2012), as well as the relationships among the classical and quantum communication in the quantum teleportation protocol.

References

Abramsky S, Coecke B (2009) Categorical quantum mechanics. In: Lehmann D, Engesser K, Gabbay DM (eds) Handbook of quantum logic and quantum structures. Elsevier, Amsterdam, pp 261–323

Baltag A, Smets S (2005) Complete axiomatizations for quantum actions. Int J Theor Phys 44(12):2267–2282

Baltag A, Smets S (2006) LQP: the dynamic logic of quantum information. Math Struct Comput Sci 16(3):491–525

Baltag A, Bergfeld J, Kishida K, Sack J, Smets S, Zhong S (2013) Quantum probabilistic dyadic second-order logic. In: Libkin L, Kohlenbach U, de Queiroz R (eds) Logic, language, information, and computation, lecture notes in computer science, vol 8071. Springer, Berlin, Heidelberg, pp 64–80

Baltag A, Bergfeld J, Kishida K, Sack J, Smets S, Zhong S (2014) PLQP & company: decidable logics for quantum algorithms. Int J Theor Phys 53(10):3628–3647

Bennett CH, Brassard G (1984) Quantum cryptography: public key distribution and coin tossing. In: Proceedings of IEEE international conference on computers, systems and signal processing, pp 175–179

Bennett CH, Brassard G (2014) Quantum cryptography: public key distribution and coin tossing. In: Theoretical computer science 560, Part 1, theoretical aspects of quantum cryptography—celebrating 30 years of BB84, pp 7–11

Bergfeld JM, Kishida K, Sack J, Zhong S (2015) Duality for the logic of quantum actions. Stud Log 103(4):781–805. doi:10.1007/s11225-014-9592-x

Birkhoff G, von Neumann J (1936) The logic of quantum mechanics. Ann Math 37:823–843

Dalla Chiara ML, Giuntini R (2002) Quantum logics. In: Gabbay D, Guenthner F (eds) Handbook of philosophical logic. Kluwer Academic Publishers, Dordrecht, pp 129–228

Dalla Chiara ML, Giuntini R, Greechie R (2004) Reasoning in quantum theory: sharp and unsharp quantum logics, trends in logic, vol 22. Kluwer Academic Press, Dordrecht

D'Hondt E, Panangaden P (2006a) The computational power of the W and GHZ states. Quantum Inf Comput 6(2):173–183

D'Hondt E, Panangaden P (2006b) Quantum weakest preconditions. Math Struct Comput Sci 16:429–451 6

Dunn JM, Moss LS, Wang Z (2013) Editors' introduction: the third life of quantum logic: quantum logic inspired by quantum computing. J Philos Log 42(3):443–459

Fagin R, Halpern JY (1994) Reasoning about knowledge and probability. J ACM 41(2):340–367

Fagin R, Halpern JY, Megiddo N (1990) A logic for reasoning about probabilities. Inf Comput 87(1):78–128

Feng Y, Nengkun Y, Ying M (2013) Model checking quantum Markov chains. J Comput Syst Sci 79(7):1181–1198

Fischer MJ, Ladner RE (1979) Propositional dynamic logic of regular programs. J Comput Syst Sci 18(2):194–211

Gay SJ, Nagarajan R, Papanikolaou N (2008) QMC: a model checker for quantum systems. In: Proceedings of the 20th international conference on computer aided verification, CAV '08. Springer, Berlin, Heidelberg, pp 543–547

Goldblatt RI (1974) Semantic analysis of orthologic. J Philos Log 3(1–2):19–35

Harel D, Tiuryn J, Kozen D (2000) Dynamic logic. MIT Press, Cambridge

Hoare TCAR (1969) An axiomatic basis for computer programming. Commun ACM 12(10):576–580

Hodkinson I, Reynolds M (2007) Temporal logic. In: Blackburn P, Van Benthem J, Wolter F (eds) Handbook of modal logic, studies in logic and practical reasoning, chapter 11, vol 3. Elsevier, pp 655–720

Mateus P, Sernadas A (2006) Weakly complete axiomatization of exogenous quantum propositional logic. Inf Comput 204(5):771–794

Nishimura H (2009) Gentzen methods in quantum logic. In: Lehmann D, Engesser K, Gabbay DM (eds) Handbook of quantum logic and quantum structures. Elsevier, Amsterdam, pp 227–260

Selinger P (2007) Dagger compact closed categories and completely positive maps: (extended abstract). In: Electronic notes in theoretical computer science. Proceedings of the 3rd international workshop on quantum programming languages (QPL 2005), vol 170, pp 139–163

Selinger P (2011) Finite dimensional Hilbert spaces are complete for dagger compact closed categories (extended abstract). In: Electronic notes in theoretical computer science. Proceedings of the joint 5th international workshop on quantum physics and logic and 4th workshop on developments in computational models (QPL/DCM 2008), vol 270(1), pp 113–119

Selinger P (2012) Finite dimensional Hilbert spaces are complete for dagger compact closed categories. Log Methods Comput Sci 8:1–12

Smets S, Baltag A (2006) Logics for quantum information flow. In: Presented at the 18-th European Summer School of Logic, Language and Information. http://www.vub.ac.be/CLWF/SS/slides.html. Accessed 14 Dec 2014

Tani S, Kobayashi H, Matsumoto K (2012) Exact quantum algorithms for the leader election problem. ACM Trans Comput Theory 4(1):1:1–1:24

Ying M, Nengkun Y, Feng Y, Duan R (2013) Verification of quantum programs. Sci Comput Program 78(9):1679–1700