Fundamenta Informaticae XX (2012) 1–14
DOI 10.3233/FI-2012-620
IOS Press

Epistemic Quantum Computational Structures in a Hilbert-space Environment

Enrico Beltrametti
Dipartimento di Fisica
Università di Genova
via Dodecaneso 33, I-16146 Genova, Italy
enrico.beltrametti@ge.infn.it

Maria Luisa Dalla Chiara
Dipartimento di Filosofia
Università di Firenze
via Bolognese 52, I-50139 Firenze, Italy
dallachiara@unifi.it

Roberto Giuntini*
Dipartimento di Filosofia e Teoria delle Scienze Umane
Università di Cagliari
via Is Mirrionis 1, I-09123 Cagliari, Italy
giuntini@unica.it

Roberto Leporini
Dipartimento di Matematica, Statistica,
Informatica e Applicazioni
Università di Bergamo
via dei Caniana 2, I-24127 Bergamo, Italy
roberto.leporini@unibg.it

Giuseppe Sergioli†
Dipartimento di Filosofia e Teoria delle Scienze Umane
Università di Cagliari
via Is Mirrionis 1, I-09123 Cagliari, Italy
giuseppe.sergioli@gmail.com

Abstract. Quantum computation and quantum computational logics are intrinsically connected with some puzzling epistemic problems. In the framework of a quantum computational approach to epistemic logic we investigate the following question: is it possible to interpret the basic epistemic operations (*having information*, *knowing*) as special kinds of Hilbert-space operations? We show that non-trivial knowledge operations cannot be represented by unitary operators. We introduce the notions of *strong epistemic quantum computational structure* and of *epistemic quantum computational structures*, where knowledge operations are identified with special examples of *quantum operations*. This represents the basic tool for developing an epistemic quantum computational se-

*Address for correspondence: Dipartimento di Filosofia e Teoria delle Scienze Umane, Università di Cagliari, via Is Mirrionis 1, I-09123 Cagliari, Italy
†Giuseppe Sergioli was supported by Regione Autonoma della Sardegna, POR Sardegna FSE-M.S. 2007-2013 L.R. 7/2007

mantics, where epistemic sentences (like "Alice knows that the spin-value in the x-direction is up") are interpreted as quantum pieces of information that may be stored by quantum objects.

Keywords: quantum computational logics, epistemic structures.

1. Introduction

Quantum computation and quantum computational logics are intrinsically connected with some puzzling epistemic problems. In [3] we have proposed a simplified semantics for a language that consists of two parts: 1) the quantum computational sub-language, whose sentences α represent pieces of quantum information (which are supposed to be stored by some quantum systems); 2) the classical epistemic sub-language, whose atomic sentences have the following forms:

- *agent* $\mathbf{a}$ *has a probabilistic information about the sentence* α ($\mathcal{I}\mathbf{a}\alpha$);
- *agent* $\mathbf{a}$ *knows the sentence* α ($\mathcal{K}\mathbf{a}\alpha$).

Interestingly enough, some conceptual difficulties of the standard approaches to epistemic logics can be overcome in this framework. For instance, the unrealistic *logical omniscience* of epistemic agents, according to which knowing a given sentence should imply knowing all its logical consequences, is here avoided.

Generally, we have:

1. If $\mathcal{K}\mathbf{a}\alpha$ is true at a given time, then $\neg_C\mathcal{K}\mathbf{a}\neg\alpha$ is true at the same time (where $\neg_C$ and $\neg$ represent the classical and the quantum computational negation, respectively). But not the other way around!

   Hence, knowledge is consistent at any particular time.

2. If $\mathcal{K}\mathbf{a}(\alpha \wedge \beta)$ is true at a given time, then $\mathcal{K}\mathbf{a}\alpha$ and $\mathcal{K}\mathbf{a}\beta$ are true at the same time. But not the other way around!

   Hence, knowledge is not generally closed under conjunction.

3. If $\mathcal{K}\mathbf{a}\alpha$ is true at a given time and β is a logical consequence of α (in the framework of a convenient form of *quantum computational logic*), then $\mathcal{K}\mathbf{a}\beta$ is not necessarily true at the same time.

   This permits us to avoid the unpleasant logical omniscience of epistemic agents.

The semantics presented in [3] is, in a sense, *semiclassical*; for, the epistemic operators *having information*, *knowing* are expressed in a classical epistemic language. We have seen how such semantics can find natural applications in the discussion of some puzzling quantum phenomena, where information and actions of epistemic agents play a fundamental role (as happens, for instance, in teleportation-experiments).

In this paper we will investigate the following problem: is it possible to interpret the basic epistemic operators (*having information*, *knowing*) as special kinds of Hilbert-space operations? A positive answer to this question would permit us to develop a "genuine" epistemic quantum computational semantics, where also epistemic sentences like $\mathcal{I}\mathbf{a}\alpha$ and $\mathcal{K}\mathbf{a}\alpha$ can be represented as pieces of quantum information.

2. Truth-perspectives

We will first sum up some basic concepts that play an essential role in the construction of our epistemic structures. Reference to the canonical orthonormal basis $B^{(1)}$ of the two dimensional Hilbert space $\mathbb{C}^2$ will be made, as usual in quantum computation and quantum computational logics. We have: $B^{(1)} = \{|0\rangle, |1\rangle\}$, where $|0\rangle = (1,0)$ and $|1\rangle = (0,1)$ represent the two classical bits in this context. A *qubit* is defined as a unit vector of $\mathbb{C}^2$ whose canonical form is $|\psi\rangle = a|0\rangle + b|1\rangle$. Let $\mathcal{H}^{(n)} = \bigotimes^n \mathbb{C}^2$ be the n-fold tensor product of $\mathbb{C}^2$. The canonical basis of $\mathcal{H}^{(n)}$ is the set $B^{(n)} = \left\{|x_1\rangle \otimes \ldots \otimes |x_n\rangle : |x_1\rangle, \ldots, |x_n\rangle \in B^{(1)}\right\}$. As usual, we will briefly write $|x_1, \ldots, x_n\rangle$ instead of $|x_1\rangle \otimes \ldots \otimes |x_n\rangle$. By definition, a *quregister* is a unit vector of $\mathcal{H}^{(n)}$. Quregisters thus correspond to pure states, namely to maximal pieces of information about the quantum systems that are supposed to store a given amount of quantum information. We shall also make reference to *mixtures* of quregisters, to be called *qumixes*, associated to density operators ρ of $\mathcal{H}^{(n)}$. We will denote by $\mathfrak{D}(\mathcal{H}^{(n)})$ the set of all qumixes of $\mathcal{H}^{(n)}$, and also reference to the set $\mathfrak{D} = \bigcup_n \left\{\mathfrak{D}(\mathcal{H}^{(n)})\right\}$ will be made.

Since the choice of an orthonormal basis for the Hilbert space $\mathcal{H}^{(n)}$ is obviously a matter of convention, we may ask what happens if the whole semantic construction is developed by adopting a different basis for $\mathbb{C}^2$. [3]

Any basis-change can be regarded as determined by a unitary operator U of $\mathbb{C}^2$. As an example, let U be the Hadamard operator $\sqrt{\mathtt{I}}$. Then, U determines the following new orthonormal basis:

$$B_U^{(1)} = \left\{\sqrt{\mathtt{I}}|0\rangle, \sqrt{\mathtt{I}}|1\rangle\right\} = \left\{\left(\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}\right), \left(\frac{1}{\sqrt{2}}, -\frac{1}{\sqrt{2}}\right)\right\}.$$

Any basis-change can be viewed as a change of our *truth-perspective*. While in the canonical case, the truth-values *truth* and *falsity* are identified with the two classical bits $|1\rangle$ and $|0\rangle$, assuming a different basis corresponds to a different idea of *truth* and *falsity*. Thus, we can guess that epistemic agents having different semantic ideas might be associated to different bases of the space $\mathbb{C}^2$.

Any unitary operator U of $\mathcal{H}^{(1)}$ can be canonically extended to a unitary operator $U^{(n)}$ of $\mathcal{H}^{(n)}$ (for any $n \geq 1$), which is defined as follows:

$$U^{(n)}|x_1, \ldots, x_n\rangle = U|x_1\rangle \otimes \ldots \otimes U|x_n\rangle.$$

Any choice of a unitary operator U of $\mathcal{H}^{(1)}$ determines an orthonormal basis $B_U^{(n)}$ for $\mathcal{H}^{(n)}$ such that:

$$B_U^{(n)} = \left\{U^{(n)}|x_1, \ldots, x_n\rangle : |x_1, \ldots, x_n\rangle \in B^{(n)}\right\}.$$

Instead of $U^{(n)}|x_1, \ldots, x_n\rangle$ we will also write $|x_1, \ldots, x_n\rangle_U$. Of course, we will have:

$$U^{(n)^{-1}}|x_1, \ldots, x_n\rangle_U = |x_1, \ldots, x_n\rangle.$$

The elements of $B_U^{(1)}$ are called the *U-bits* of $\mathcal{H}^{(1)}$, while the elements of $B_U^{(n)}$ are called the *U-registers* of $\mathcal{H}^{(n)}$.

Let B_U represent the infinite sequence $B_U^{(1)}, B_U^{(2)}, \ldots$ that is determined by the unitary operator U. We will call B_U a *general basis*, while B will represent the *canonical general basis*. Of course, $B_U = B$ iff U is the identity operator $\mathtt{I}$.

We come now to the notions of *truth*, *falsity* and *probability* with respect to the general basis B_U.

Definition 2.1. *(True and false registers)*

- $|x_1, \ldots, x_n\rangle_U$ is a *true register* of $B_U^{(n)}$ iff $|x_n\rangle_U = |1\rangle_U$.
- $|x_1, \ldots, x_n\rangle_U$ is a *false register* of $B_U^{(n)}$ iff $|x_n\rangle_U = |0\rangle_U$.

In other words, the *truth-value* of an U-register (which corresponds to a sequence of U-bits) is determined by its last element.[1]

Let $\mathfrak{R}_T^U$ ($\mathfrak{R}_F^U$) represent the set of the true registers (the false registers) of $B_U^{(n)}$.

Definition 2.2. *(Truth and falsity)*

- The *U-truth* of $\mathcal{H}^{(n)}$ is the projection operator $P_1^{U(n)}$ that projects over the closed subspace spanned by $\mathfrak{R}_T^U$.
- The *U-falsity* of $\mathcal{H}^{(n)}$ is the projection operator $P_0^{U(n)}$ that projects over the closed subspace spanned by $\mathfrak{R}_F^U$.

In this way, truth and falsity are dealt with as mathematical representatives of possible physical properties. Accordingly, by applying the Born-rule, one can naturally define the probability-value of any qumix with respect to the general basis B_U.

Definition 2.3. *(U-Probability)*
For any $\rho \in \mathfrak{D}(\mathcal{H}^{(n)})$,

$$\mathtt{p}_U(\rho) := \mathtt{Tr}(P_1^{U(n)}\rho),$$

where $\mathtt{Tr}$ is the trace-functional.

We interpret $\mathtt{p}_U(\rho)$ as the probability that the information ρ satisfies the truth-property (with respect to the basis B_U). In the case of the canonical general basis we will write $\mathtt{p}(\rho)$ instead of $\mathtt{p}_\mathtt{I}(\rho)$.

In the particular cases of quregisters living in $\mathcal{H}^{(1)}$, we will obtain:

$$\mathtt{p}_U(a_0|0\rangle_U + a_1|1\rangle_U) = |a_1|^2.$$

As is well known, quantum information is processed by *quantum logical gates* (briefly, *gates*): unitary operators that transform quregisters into quregisters in a reversible way. Let us recall the definition of some gates that play a special role both from the computational and from the logical point of view.

Definition 2.4. *(The negation)*
For any $n \geq 1$, the *negation* on $\mathcal{H}^{(n)}$ is the linear operator $\mathtt{NOT}^{(n)}$ such that, for every element $|x_1, \ldots, x_n\rangle$ of the basis $B^{(n)}$,

$$\mathtt{NOT}^{(n)}(|x_1, \ldots, x_n\rangle) = |x_1, \ldots, x_{n-1}\rangle \otimes |1 - x_n\rangle.$$

In particular, we obtain:

$$\mathtt{NOT}^{(1)}|0\rangle = |1\rangle;\ \mathtt{NOT}^{(1)}|1\rangle = |0\rangle,$$

(according to the classical truth-table of negation).

[1] As we will see, the application of a classical reversible gate to a register $|x_1, \ldots, x_n\rangle$ transforms the bit $|x_n\rangle$ into the target-bit $|x'_n\rangle$, which behaves as the final truth-value. This justifies our choice in Definition 2.1.

Definition 2.5. *(The Toffoli gate)*
For any $n, m, p \geq 1$, the *Toffoli gate* is the linear operator $\mathtt{T}^{(n,m,p)}$ defined on $\mathcal{H}^{(n+m+p)}$ such that, for every element $|x_1, \ldots, x_n\rangle \otimes |y_1, \ldots, y_m\rangle \otimes |z_1, \ldots, z_p\rangle$ of the basis $B^{(n+m+p)}$,

$$\mathtt{T}^{(n,m,p)}(|x_1, \ldots, x_n\rangle \otimes |y_1, \ldots, y_m\rangle \otimes |z_1, \ldots, z_p\rangle) \\ = |x_1, \ldots, x_n\rangle \otimes |y_1, \ldots, y_m\rangle \otimes |z_1, \ldots, z_{p-1}, x_n y_m \widehat{+} z_p\rangle,$$

where $\widehat{+}$ represents the addition modulo 2.

Definition 2.6. *(The Hadamard-gate)*
For any $n \geq 1$, the *Hadamard-gate* on $\mathcal{H}^{(n)}$ is the linear operator $\sqrt{\mathtt{I}}^{(n)}$ such that for every element $|x_1, \ldots, x_n\rangle$ of the basis $B^{(n)}$:

$$\sqrt{\mathtt{I}}^{(n)}(|x_1, \ldots, x_n\rangle) = |x_1, \ldots, x_{n-1}\rangle \otimes \frac{1}{\sqrt{2}} \left((-1)^{x_n}|x_n\rangle + |1 - x_n\rangle\right).$$

In particular we obtain:

$$\sqrt{\mathtt{I}}^{(1)}(|0\rangle) = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle); \sqrt{\mathtt{I}}^{(1)}(|1\rangle) = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle).$$

Hence, $\sqrt{\mathtt{I}}^{(1)}$ transforms bits into genuine qubits.

The system consisting of the gates *Negation*, *Toffoli* and *Hadamard* is, to a certain extent, redundant. As proved by Shi and Aharanov ([15], [1]), *Toffoli* and *Hadamard* give rise to an *approximately universal* system of gates, in the sense that any gate G (defined on $\mathcal{H}^{(n)}$) can be approximately simulated by a convenient combination of *Toffoli* and *Hadamard* up to an arbitrary accuracy. In this system *Toffoli* plays the role of a classical universal gate, which permits us to define exactly all classical reversible gates. For instance, the reversible conjunction `AND` and the reversible negative conjunction `NAND` can be defined as follows, for any $|\psi\rangle \in \mathcal{H}^{(n)}$ and any $|\varphi\rangle \in \mathcal{H}^{(m)}$:

$$\mathtt{AND}(|\psi\rangle, |\varphi\rangle) = \mathtt{T}^{(n,m,1)}(|\psi\rangle \otimes |\varphi\rangle \otimes |0\rangle);$$

$$\mathtt{NAND}(|\psi\rangle, |\varphi\rangle) = \mathtt{T}^{(n,m,1)}(|\psi\rangle \otimes |\varphi\rangle \otimes |1\rangle).$$

The gate *Hadamard*, instead, represents a genuine quantum gate, that creates uncertain outputs (quregisters), starting from certain inputs (classical registers). Using an independent definition of `NOT` is, however, more useful for computational aims, since such definition permits us to avoid a non-economical increasing of the dimension of the Hilbert spaces in play.

All gates can be naturally transposed from the canonical (general) basis B to the (general) basis B_U that is determined by the unitary operator U. Let $G^{(n)}$ be any gate defined with respect to the canonical basis $B^{(n)}$. The *twin-gate* $G_U^{(n)}$, defined with respect to the basis $B_U^{(n)}$, is determined as follows:

$$\forall |x_1, \ldots, x_n\rangle_U \in B_U^{(n)} : G_U^{(n)}(|x_1, \ldots, x_n\rangle_U) := U^{(n)}(G^{(n)}(|x_1, \ldots, x_n\rangle)).$$

Of course, $G_U^{(n)} = G^{(n)}$ iff U is the identity operator $\mathtt{I}$.

All U-gates can be canonically extended to the set $\mathfrak{D}$ of all qumixes. Let $G_U^{(n)}$ be any gate defined on $\mathcal{H}^{(n)}$. The corresponding *qumix gate* (also called *unitary quantum operation*) ${}^{\mathfrak{D}}G_U^{(n)}$ is defined as follows for any $\rho \in \mathfrak{D}(\mathcal{H}^{(n)})$:

$$ {}^{\mathfrak{D}}G_U^{(n)}(\rho) = G_U^{(n)} \rho G_U^{(n)^*}, $$

where $G_U^{(n)^*}$ is the adjoint of $G_U^{(n)}$.

On this basis, one can uniformly define on the set $\mathfrak{D}$ a system of operations that correspond to the U-gates considered above.

Definition 2.7. *(The operations Negation, Hadamard and Toffoli)*

1. For any $\rho \in \mathfrak{D}(\mathcal{H}^{(n)}), \mathbb{N}_U(\rho) = {}^{\mathfrak{D}}\mathtt{NOT}_U^{(n)}(\rho)$.
2. For any $\rho \in \mathfrak{D}(\mathcal{H}^{(n)}), \sqrt{\mathbb{I}}_U(\rho) = {}^{\mathfrak{D}}\sqrt{\mathtt{I}}_U^{(n)}(\rho)$.
3. For any $\rho \in \mathfrak{D}(\mathcal{H}^{(n)})$, for any $\sigma \in \mathfrak{D}(\mathcal{H}^{(m)})$ and for any $\tau \in \mathfrak{D}(\mathcal{H}^{(p)}), \mathbb{T}_U(\rho, \sigma, \tau) = {}^{\mathfrak{D}}\mathtt{T}_U^{(m,n,p)}(\rho \otimes \sigma \otimes \tau)$.

3. Epistemic structures

We will now discuss our basic question: is it possible to interpret the epistemic operators as special kinds of Hilbert space operations? To this aim, let us first introduce the notion of *strong epistemic quantum computational structure* $\mathcal{S}$. From an intuitive point of view S can be described as a system consisting of a time-sequence and of a set of epistemic agents evolving in time. Any agent has a truth-perspective that determines his/her idea of truth and probability. We assume that the truth-perspective of each agent is constant in time. Furthermore, we have a map $\mathbf{I}$ that assigns to any agent at any time an *information-operation* that determines the pieces of information *available* for our agent with respect to any space $\mathcal{H}^{(n)}$. Another map $\mathbf{K}$ assigns to any agent at any time a *strong knowledge operation* that determines the pieces of information *known* by our agent with respect to any space $\mathcal{H}^{(n)}$. The precise definition of $\mathcal{S}$ is the following.

Definition 3.1. *(Strong epistemic quantum computational structure)*
A strong epistemic quantum computational structure is a system

$$ \mathcal{S} = (T,\ Ag,\ TrPersp,\ \mathbf{I},\ \mathbf{K}) $$

where:

1. T is a time-sequence.
2. Ag is a set of epistemic agents $\mathfrak{a}$ represented as functions of t in T. We will write $\mathfrak{a}_t$ instead of $\mathfrak{a}(t)$.
3. $TrPersp$ is a map that assigns to any agent $\mathfrak{a}$ a general basis $B_{\mathfrak{a}}$: the truth-perspective of $\mathfrak{a}$.

4. $\mathbf{I}$ is a map that assigns to any agent $\mathfrak{a}_t$ and to any $n \geq 1$ a map (called *information-operation*)

$$\mathbf{I}^{(n)}_{\mathfrak{a}_t} : \mathcal{B}(\mathcal{H}^{(n)}) \mapsto \mathcal{B}(\mathcal{H}^{(n)}),$$

where $\mathcal{B}(\mathcal{H}^{(n)})$ is the set of all bounded operators of $\mathcal{H}^{(n)}$. For any $\rho \in \mathfrak{D}(\mathcal{H}^{(n)})$ the condition $\mathbf{I}^{(n)}_{\mathfrak{a}_t}\rho \in \mathfrak{D}(\mathcal{H}^{(n)})$ is required.

5. $\mathbf{K}$ is a map that assigns to any agent $\mathfrak{a}_t$ and to any $n \geq 1$ a map (called *strong knowledge operation*)

$$\mathbf{K}^{(n)}_{\mathfrak{a}_t} : \mathcal{B}(\mathcal{H}^{(n)}) \mapsto \mathcal{B}(\mathcal{H}^{(n)}).$$

The following conditions are required:

a) For any agent $\mathfrak{a}_t$ and for any $n \geq 1$, $\mathbf{K}^{(n)}_{\mathfrak{a}_t}$ is an information-operation.

b) $\mathtt{p}_{B_\mathfrak{a}}(\mathbf{K}^{(n)}_{\mathfrak{a}_t}\rho) \leq \mathtt{p}_{B_\mathfrak{a}}(\rho)$, for any $\rho \in \mathfrak{D}(\mathcal{H}^{(n)})$.

Let us outline the intuitive interpretation of $\mathbf{I}^{(n)}_{\mathfrak{a}_t}\rho$ and $\mathbf{K}^{(n)}_{\mathfrak{a}_t}\rho$ by the following remarks. For any qumix ρ (which lives in the space $\mathcal{H}^{(n)}$), $\mathbf{I}^{(n)}_{\mathfrak{a}_t}\rho$ is a qumix (living in the same space) that represents the following piece of quantum information: at time t agent $\mathfrak{a}$ *has information* about ρ. It appears natural not to assume any relationship about the probability-values of ρ and $\mathbf{I}^{(n)}_{\mathfrak{a}_t}\rho$. The qumix $\mathbf{K}^{(n)}_{\mathfrak{a}_t}\rho$ represents instead the following piece of quantum information: at time t agent $\mathfrak{a}$ *knows* ρ. Unlike the case of $\mathbf{I}^{(n)}_{\mathfrak{a}_t}\rho$, it seems reasonable to assume that the probability-values of ρ and $\mathbf{K}^{(n)}_{\mathfrak{a}_t}\rho$ are correlated: the probability of the quantum information expressed by the sentence "at time t agent $\mathfrak{a}$ knows ρ" should always be less than or equal to the probability of ρ. Hence, in particular, we obtain that:

$$\mathtt{p}_{B_\mathfrak{a}}(\mathbf{K}^{(n)}_{\mathfrak{a}_t}\rho) = 1 \;\;\Rightarrow\;\; \mathtt{p}_{\mathtt{B}_\mathfrak{a}}(\rho) = 1.$$

But generally, not the other way around! In other words, pieces of quantum information that are known by our agents are true!

As an example, suppose that the qumix ρ in $\mathcal{H}^{(1)}$ represents the proposition "the spin-value in the x-direction is up". Clearly, the probability-value of the sentence $\mathbf{I}^{(1)}_{\mathfrak{a}_t}\rho$ (say, "Alice has information about the proposition asserting that that the spin-value in the x-direction is up") does not have any correlation with the probability of the proposition in question. At the same time, the probability of $\mathbf{K}^{(1)}_{\mathfrak{a}_t}\rho$ ("Alice knows that the spin-value in the x-direction is up") should always be less than or equal to the probability of ρ.

A strong knowledge operation $\mathbf{K}^{(n)}_{\mathfrak{a}_t}$ will be called *non-trivial* iff for at least one qumix ρ, $\mathtt{p}_{B_\mathfrak{a}}(\mathbf{K}^{(n)}_{\mathfrak{a}_t}\rho) < \mathtt{p}_{B_\mathfrak{a}}(\rho)$.

Notice that strong knowledge operations do not generally preserve pure states. As a counterexample consider the map

$$\tfrac{1}{2}\mathbf{K}^{(1)}_{\mathtt{I}} : \mathcal{B}(\mathcal{H}^{(1)}) \mapsto \mathcal{B}(\mathcal{H}^{(1)}),$$

that is defined as follows for any operator $\begin{pmatrix} a\,b \\ c\,d \end{pmatrix}$ in $\mathcal{B}(\mathcal{H}^{(1)})$:

$$\tfrac{1}{2}\mathbf{K}^{(1)}_{\mathtt{I}} \begin{pmatrix} a\,b \\ c\,d \end{pmatrix} := \begin{pmatrix} a + \frac{d}{2} & \frac{b}{\sqrt{2}} \\ \frac{c}{\sqrt{2}} & \frac{d}{\sqrt{2}} \end{pmatrix}$$

One can easily show that $\frac{1}{2}\mathbf{K}_{\mathtt{I}}^{(1)}$ is a strong knowledge operation with respect to the canonical general basis $B_{\mathtt{I}}$. Denoting $P_1^{(1)} = \begin{pmatrix} 0\,0 \\ 0\,1 \end{pmatrix}$ we have:

$$\tfrac{1}{2}\mathbf{K}_{\mathtt{I}}^{(1)} P_1^{(1)} = \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{pmatrix} = \frac{1}{2}\mathtt{I}^{(1)}.$$

Hence, $\frac{1}{2}\mathbf{K}_{\mathtt{I}}^{(1)}$ transforms the bit $P_1^{(1)}$ into the proper mixture $\frac{1}{2}\mathtt{I}^{(1)}$.

By *strong knowledge operator* we will mean the restriction to quregisters of a strong knowledge operation that satisfies the property of preserving pure states.

Definition 3.2. *(Strong knowledge operator)*
A linear operator

$$K : \mathcal{H}^{(n)} \mapsto \mathcal{H}^{(n)}$$

is called a *strong knowledge operator* with respect to the general basis B_U iff

1. for any quregister $|\psi\rangle$ of $\mathcal{H}^{(n)}$, $K|\psi\rangle$ is a quregister.
2. $\mathtt{p}_U(K|\psi\rangle) \leq \mathtt{p}_U(|\psi\rangle)$, for any quregister $|\psi\rangle$ of $\mathcal{H}^{(n)}$.

By *non-trivial strong knowledge operator* (on the space $\mathcal{H}^{(n)}$ with respect to general basis B_U) we will mean a strong knowledge operator K such that for at least one quregister $|\psi\rangle$: $\mathtt{p}_U(K|\psi\rangle) < \mathtt{p}_U(|\psi\rangle)$.

We will now prove that non-trivial strong knowledge operators cannot be represented by unitary operators. To this aim, let us first define the notion of *probabilistic identity operator*.

Definition 3.3. *(Probabilistic identity operator)*
A probabilistic identity operator with respect to the general basis B_U is a linear operator

$$A : \mathcal{H}^{(n)} \mapsto \mathcal{H}^{(n)},$$

such that for any quregister $|\psi\rangle$ of $\mathcal{H}^{(n)}$:

$$\mathtt{p}_U(|\psi\rangle) = \mathtt{p}_U(A(|\psi\rangle)).$$

In other words, A may change $|\psi\rangle$, but not its probability!

Theorem 3.4. A linear operator A of $\mathcal{H}^{(1)}$ is a probabilistic identity operator with respect to the general basis B_U iff

$$A = \begin{pmatrix} e^{i\theta} & 0 \\ 0 & e^{i\eta} \end{pmatrix}$$

with θ, $\eta \in \mathbb{R}$.

Proof:
Suppose that

$$A = \begin{pmatrix} a\,b \\ c\,d \end{pmatrix}$$

is a probabilistic identity operator with respect to the general basis B_U. Then,

$$\mathtt{p}_U(|1\rangle_U) = 1;\ \ \mathtt{p}_U(|0\rangle_U) = 0.$$

Hence:

$$b = 0,\ d = e^{i\eta},\ \text{for some } \eta \in \mathbb{R}; c = 0,\ a = e^{i\theta},\ \text{for some } \theta \in \mathbb{R}.$$

Conversely, let

$$A = \begin{pmatrix} e^{i\theta} & 0 \\ 0 & e^{i\eta} \end{pmatrix}$$

We obtain, for $|\psi\rangle = a_0|0\rangle_U + a_1|1\rangle_U$,

$$A|\psi\rangle = a_0 e^{i\theta}|0\rangle_U + a_1 e^{i\eta}|1\rangle_U.$$

Furthermore, we have:

$$\mathtt{p}_U(|\psi\rangle) = |a_1|^2;$$
$$\mathtt{p}_U(A|\psi\rangle) = \mathtt{p}_U(a_0 e^{i\theta}|0\rangle_U + a_1 e^{i\eta}|1\rangle_U) = |a_1|^2.$$

Hence A is a probabilistic identity operator (with respect to the general basis B_U). □

Theorem 3.5. Let A be a unitary operator of $\mathcal{H}^{(1)}$ such that for all quregisters $|\psi\rangle, \mathtt{p}_U(A|\psi\rangle) \leq \mathtt{p}_U(|\psi\rangle)$. Then A is a probabilistic identity operator with respect to the general basis B_U.

Proof:

Let $A = \begin{pmatrix} a\, b \\ c\, d \end{pmatrix}$. We have: $\mathtt{p}_U(|0\rangle_U) = 0$. Thus, $\mathtt{p}_U(A|0\rangle_U) = 0$. Hence, $c = 0$ and $a = e^{i\theta}$, fore some $\theta \in \mathbb{R}$. Consequently, $A = \begin{pmatrix} e^{i\theta} & b \\ 0 & d \end{pmatrix}$. Since A is unitary, we have: $AA^* = \mathtt{I}^{(1)}$. Thus:

$$\begin{pmatrix} e^{i\theta} & b \\ 0 & d \end{pmatrix} \begin{pmatrix} (e^{i\theta})^* & 0 \\ b^* & d^* \end{pmatrix} = \begin{pmatrix} 1\,0 \\ 0\,1 \end{pmatrix}$$

Hence, $dd^* = 1$, i.e. $d = e^{i\eta}$ for some $\eta \in \mathbb{R}$. Moreover $b = 0$, because $e^{i\theta}(e^{i\theta})^* + b\, b^* = 1$. Consequently, A is a probabilistic identity operator with respect to the general basis B_U. □

Corollary 3.6.

- Non-trivial strong knowledge operators cannot be represented by unitary operators.
- Non-trivial strong knowledge operations cannot be represented by qumix gates.

We will now prove that strong knowledge operations can be represented by the notion of *quantum operation* defined below. Interestingly enough, the concept of quantum operation is a quite general notion that permits us to represent at the same time *quantum states*, *effects* and *measurements*. In particular, it has been shown that for *open systems*, interacting with an environment, the Schrödinger-equation should be generalized to a superoperator-equation, describing how an initial pure state evolves into a mixed state, that has the form of a quantum operation.[2]

[2] See, for instance, [13], [14], [4], [11].

Definition 3.7. *(Quantum operation)*
A *quantum operation* on $\mathcal{H}^{(n)}$ is a linear map $\mathcal{E}$ from $\mathcal{B}(\mathcal{H}^{(n)})$ to $\mathcal{B}(\mathcal{H}^{(n)})$ that satisfies the following properties:

- for any $A \in \mathcal{B}(\mathcal{H}^{(n)})$, $\mathtt{Tr}(\mathcal{E}(A)) \leq \mathtt{Tr}(A)$;
- $\mathcal{E}$ is completely positive.

In our applications we will use a stricter notion of quantum operation that is usually called *quantum channel*.

Definition 3.8. *(Quantum channel)*
A *quantum channel* on $\mathcal{H}^{(n)}$ is a quantum operation $\mathcal{E}$ on $\mathcal{H}^{(n)}$ that satisfies the following property: for any $A \in \mathcal{B}(\mathcal{H}^{(n)})$, $\mathtt{Tr}(\mathcal{E}(A)) = \mathtt{Tr}(A)$.

From the definition one immediately obtains that any quantum channel maps density operators into density operators.

A neat characterization of quantum channels is stated by *Kraus first representation theorem* [12].

Theorem 3.9. A map

$$\mathcal{E} : \mathcal{B}(\mathcal{H}^{(n)}) \mapsto \mathcal{B}(\mathcal{H}^{(n)})$$

is a quantum channel on $\mathcal{H}^{(n)}$ iff for some set I of indices there exists a set $\{E_i\}_{i\in I}$ of elements of $\mathcal{B}(\mathcal{H}^{(n)})$ satisfying the following conditions:

1. $\sum_i E_i^* E_i = \mathtt{I}^{(n)}$
2. $\forall A \in \mathcal{B}(\mathcal{H}^{(n)}) : \mathcal{E}(A) = \sum_i E_i A E_i^*$.

Of course, qumix gates ${}^{\mathfrak{D}}G$ are special cases of quantum channels, for which $\{E_i\}_{i\in I} = \{{}^{\mathfrak{D}}G\}$.

Theorem 3.10. There exist uncountably many quantum channels that are non-trivial strong knowledge operations of the space $\mathcal{H}^{(1)}$ with respect to the canonical general basis.

Proof:
Let ${}^rE_1 = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{r} \end{pmatrix}$, and ${}^rE_2 = \begin{pmatrix} 0 & \sqrt{1-r} \\ 0 & 0 \end{pmatrix}$ with $r \in [0,1]$.

Define ${}^r\mathbf{K}^{(1)} : \mathcal{B}(\mathcal{H}^{(n)}) \mapsto \mathcal{B}(\mathcal{H}^{(n)})$ as follows:

$$\forall A \in \mathcal{B}(\mathcal{H}^{(n)}) : \ {}^r\mathbf{K}^{(1)}(A) = {}^rE_1 A ({}^rE_1)^* + {}^rE_2 A ({}^rE_2)^*.$$

It is easy to see that $({}^rE_1)^*({}^rE_1) + ({}^rE_2)^*({}^rE_2) = \mathtt{I}^{(1)}$. Hence ${}^r\mathbf{K}^{(1)}$ is a quantum channel. An easy computation shows that for all $\rho \in \mathfrak{D}(\mathcal{H}^{(1)})$:

$$\mathtt{p}({}^r\mathbf{K}^{(1)}\rho) = r\mathtt{p}(\rho) \leq \mathtt{p}(\rho).$$

If $r \neq 1$, ${}^r\mathbf{K}^{(1)}$ turns out to be a non-trivial strong knowledge operation with respect to the canonical general basis. Consequently there are uncountably many quantum channels that are non-trivial strong knowledge operations. □

Notice that:

$$\mathtt{p}(\sqrt{\mathbb{I}}({}^{r}\mathbf{K}^{(1)}(\rho))) \geq \mathtt{p}(\sqrt{\mathbb{I}}(\rho)).$$

As expected, strong knowledge operations ${}^{r}\mathbf{K}_{U}^{(n)}$ that behave like ${}^{r}\mathbf{K}^{(1)}$ can be defined for any space $\mathcal{H}^{(n)}$ and for any general basis B_U. Such operations are similar to the *amplitude damping channels* (described, for instance, in [14]), which have some interesting physical interpretations.

Definition 3.11. *(Introspection and consistency)*
A strong knowledge operator $\mathbf{K}_{U}^{(n)}$ (with respect to the general basis B_U) is called

1. *positively introspective* iff for any $\rho \in \mathfrak{D}(\mathcal{H}^{(n)})$:

$$\mathtt{p}_U(\mathbf{K}_{U}^{(n)}(\rho)) \leq \mathtt{p}_U(\mathbf{K}_{U}^{(n)}(\mathbf{K}_{U}^{(n)}(\rho)));$$

2. *negatively introspective* iff for any $\rho \in \mathfrak{D}(\mathcal{H}^{(n)})$:

$$\mathtt{p}_U(\mathbb{N}_U(\mathbf{K}_{U}^{(n)}(\rho))) \leq \mathtt{p}_U(\mathbf{K}_{U}^{(n)}(\mathbb{N}_U(\mathbf{K}_{U}^{(n)}(\rho))));$$

3. *probabilistically consistent* iff for any $\rho \in \mathfrak{D}(\mathcal{H}^{(n)})$:

$$\mathtt{p}_U(\mathbf{K}_{U}^{(n)}(\rho)) \leq \mathtt{p}_U(\mathbb{N}_U(\mathbf{K}_{U}^{(n)}(\mathbb{N}_U(\rho)))).$$

Theorem 3.12.

1. All strong knowledge operations ${}^{r}\mathbf{K}_{U}^{(1)}$ are probabilistically consistent;
2. for any ${}^{r}\mathbf{K}_{U}^{(1)}$ the following conditions are equivalent:
   - ${}^{r}\mathbf{K}_{U}^{(1)}$ is both positively and negatively introspective;
   - ${}^{r}\mathbf{K}_{U}^{(1)} = \mathtt{I}^{(1)}$, i.e. $r = 1$.

Proof:

1. For all strong knowledge operations ${}^{r}\mathbf{K}_{U}^{(1)}$ we have: $\mathtt{p}_U({}^{r}\mathbf{K}_{U}^{(1)}\rho) = r\mathtt{p}_U(\rho)$. By a straightforward calculation, one can prove that:

   $$\mathtt{p}_U(\mathbb{N}_U({}^{r}\mathbf{K}_{U}^{(1)}(\mathbb{N}_U(\rho)))) = 1 - r + r\mathtt{p}_U(\rho).$$

   Since $r \in [0, 1]$, our claim follows from the definition of *probabilistically consistent* strong knowledge operation.

2. One can prove that:
   - $\mathtt{p}_U({}^{r}\mathbf{K}_{U}^{(1)}({}^{r}\mathbf{K}_{U}^{(1)}(\rho))) = r^2\mathtt{p}_U(\rho)$;
   - $\mathtt{p}_U({}^{r}\mathbf{K}_{U}^{(1)}(\mathbb{N}_U({}^{r}\mathbf{K}_{U}^{(1)}(\rho)))) = \frac{1}{2}r(2 - r + rr_3)$;
   - $\mathtt{p}_U(\mathbb{N}_U({}^{r}\mathbf{K}_{U}^{(1)}(\rho))) = \frac{1}{2}(2 - r + rr_3)$.

Since $\mathtt{p}_U({}^r\mathbf{K}_U^{(1)}\rho) = r\mathtt{p}_U(\rho)$, our claim follows from the definitions of *positively* and *negatively introspective* strong knowledge operation.

□

Theorem 3.12 can be easily extended to all strong knowledge operations living in a space $\mathcal{H}^{(n)}$.

Theorem 3.13. All strong knowledge operations ${}^r\mathbf{K}_U^{(n)}$ are monotonic:

$$\mathtt{p}_U(\rho) \leq \mathtt{p}_U(\sigma) \;\Rightarrow\; \mathtt{p}_U({}^r\mathbf{K}_U^{(n)}\rho) \leq \mathtt{p}_U({}^r\mathbf{K}_U^{(n)}\sigma).$$

Proof:
Straightforward □

Now, monotonicity gives rise to a weak form of *logical omniscience* for our epistemic agents. Let ρ and σ be two qumixes of $\mathcal{H}^{(n)}$, linguistically expressed by two sentences α and β, such that β is a logical consequence of α (in a convenient quantum computational semantics[3]). We will have, for any general basis B_U:

$$\mathtt{p}_U(\rho) \leq \mathtt{p}_U(\sigma).$$

Hence,

$$\mathtt{p}_U(\mathbf{K}_{B_\mathfrak{a}}^{(n)}\rho) \leq \mathtt{p}_U(\mathbf{K}_{B_\mathfrak{a}}^{(n)}\sigma).$$

And in particular:

$$\mathtt{p}_U(\mathbf{K}_{B_\mathfrak{a}}^{(n)}\rho) = 1 \;\Rightarrow\; \mathtt{p}_U(\mathbf{K}_{B_\mathfrak{a}}^{(n)}\sigma) = 1.$$

In other words, knowing a sentence implies knowing all its logical consequences whose meanings belong to the same space $\mathcal{H}^{(n)}$.

We will now introduce a weaker notion of epistemic quantum computational structure, which more realistically describes the characteristic epistemic limitations of our agents.

Definition 3.14. *(Epistemic quantum computational structure)*
An epistemic quantum computational structure is a system

$$\mathcal{S} = (T,\, Ag,\, TrPersp,\, Inf,\, \mathbf{I},\, \mathbf{K})$$

where:

1. T is a time-sequence;
2. Ag is a set of epistemic agents $\mathfrak{a}$ represented as functions of t in T. We will write $\mathfrak{a}_t$ instead of $\mathfrak{a}(t)$;
3. $TrPersp$ is a map that assigns to any agent $\mathfrak{a}$ a general basis $B_\mathfrak{a}$: the truth-perspective of $\mathfrak{a}$.
4. Inf is a map that assigns to any $\mathfrak{a}_t$ a finite subset of $\bigcup_n \mathfrak{D}(\mathcal{H}^{(n)})$. From an intuitive point of view, $Inf(\mathfrak{a}_t)$ represents the epistemic universe of $\mathfrak{a}_t$: the set of qumixes that $\mathfrak{a}_t$ is able to understand and to valuate probabilistically.

[3] See [8].

5. $\mathbf{I}$ is a map that assigns to any agent $\mathfrak{a}_t$ and to any $n \geq 1$ a map (called *information-operation*)

$$\mathbf{I}_{\mathfrak{a}_t}^{(n)} : \mathcal{B}(\mathcal{H}^{(n)}) \mapsto \mathcal{B}(\mathcal{H}^{(n)}).$$

The following conditions are required:

a) For any $\rho \in \mathfrak{D}(\mathcal{H}^{(n)})$, $\mathbf{I}_{\mathfrak{a}_t}^{(n)}\rho \in \mathfrak{D}(\mathcal{H}^{(n)})$.

b) $\forall \rho \in \mathfrak{D}(\mathcal{H}^{(n)}) : \rho \notin Inf(\mathfrak{a}_t) \Rightarrow \mathbf{I}_{\mathfrak{a}_t}^{(n)}\rho = \frac{1}{2}\mathtt{I}^{(n)}$.

6. $\mathbf{K}$ is a map that assigns to any agent $\mathfrak{a}_t$ and to any $n \geq 1$ a map (called *knowledge operation*)

$$\mathbf{K}_{\mathfrak{a}_t}^{(n)} : \mathcal{B}(\mathcal{H}^{(n)}) \mapsto \mathcal{B}(\mathcal{H}^{(n)}).$$

The following conditions are required, for any $\mathfrak{a}_t$ and any $n \geq 1$:

a) $\mathbf{K}_{\mathfrak{a}_t}^{(n)}$ is an information-operation.

b) $\mathbf{K}_{\mathfrak{a}_t}^{(n)}$ restricted to the set $\mathfrak{D}(\mathcal{H}^{(n)}) \cap Inf(\mathfrak{a}_t)$ is a strong knowledge operation.

The intuitive interpretation of $\mathbf{I}_{\mathfrak{a}_t}^{(n)}\rho$ and of $\mathbf{K}_{\mathfrak{a}_t}^{(n)}\rho$ is the following:

- whenever ρ belongs to the epistemic universe of $\mathfrak{a}_t$, $\mathbf{I}_{\mathfrak{a}_t}^{(n)}\rho$ means "$\mathfrak{a}_t$ has information about ρ". Otherwise, $\mathbf{I}_{\mathfrak{a}_t}^{(n)}\rho$ represents the indeterminate qumix $\frac{1}{2}\mathtt{I}^{(n)}$.

- whenever ρ belongs to the epistemic universe of $\mathfrak{a}_t$, $\mathbf{K}_{\mathfrak{a}_t}^{(n)}\rho$ means "$\mathfrak{a}_t$ knows the quantum information ρ". Otherwise, $\mathbf{K}_{\mathfrak{a}_t}^{(n)}\rho$) represents the indeterminate qumix $\frac{1}{2}\mathtt{I}^{(n)}$.

The notion of *epistemic quantum computational structure* represents the basic tool that permits us to develop a *genuine* epistemic quantum computational semantics, where also epistemic sentences (like "Alice knows α") are interpreted as quantum pieces of information that may be stored by quantum objects. In this framework one can study the behavior of *nested* epistemic operators (say, "Alice knows that Bob does not know α"). We will investigate these logical problems in a future paper.

References

[1] D. Aharonov, "A simple proof that Toffoli and Hadamard are quantum universal", [arXiv:quant-ph/0301040], 2003.

[2] D. Aharonov, A. Kitaev, N. Nisan, "Quantum circuits with mixed states", *STOC '98: Proceedings of the thirtieth annual ACM symposium on Theory of computing*, ACM Press, pp. 20–30, 1998.

[3] E. Beltrametti, M. L. Dalla Chiara, R. Giuntini, G. Sergioli, "Quantum teleportation and quantum epistemic semantics", to appear.

[4] G. Chiribella, G. M. D'Ariano, P. Perinotti, "Transforming quantum operations: Quantum supermaps", *A Letters Journal Exploring the Frontiers of Physics* **83**, pp. 30004-p1–30004-p6, 2008.

[5] M. L. Dalla Chiara, R. Giuntini, H. Freytes, A. Ledda, G. Sergioli, "The algebraic structure of an approximately universal system of quantum computational gates", *Foundations of Physics* **39**, pp. 559–572, 2009.

[6] M. L. Dalla Chiara, R. Giuntini, R. Greechie, *Reasoning in Quantum Theory*, Kluwer, Dordrecht, 2004.

[7] G. Cattaneo, M. L. Dalla Chiara, R. Giuntini, "An Unsharp Quantum Logic from Quantum Computation", in P. Weingartner (ed.), *Alternative Logics. Do Sciences need them?*, Springer, Berlin-Heidelberg, 2003, pp. 323–338.

[8] M. L. Dalla Chiara, R. Giuntini, A. Ledda, R. Leporini, G. Sergioli, "Entanglement as a semantic resource" *Foundations of Physics* **40**, pp. 1494–1518, 2010.

[9] M. L. Dalla Chiara, R. Giuntini, R. Leporini, "Logics from quantum computation", *International Journal of Quantum Information* **3**, pp. 293–337, 2005.

[10] G. Gudder, "Quantum computational logics", *International Journal of Theoretical Physics* **42**, pp. 39–47, 2003.

[11] Hong-yi Fan, Li-yun Hu, "Infinite-dimensional Kraus operators for describing amplitudue-damping channel and laser process", *Optics Communications* **282**, pp. 932–935, 2009.

[12] K. Kraus, *States, Effects and Operations*, Springer, Berlin, 1983.

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

[14] J. Preskill, *Quantum Information and Computation*, Lecture Notes for Physics 229, 1998 (available at www.theory.caltech.edu/people/preskill/ph229).

[15] Y. Shi, "Both Toffoli and controlled-Not need little help to do universal quantum computation", [arXiv:quant-ph/0205115], 2002.