A formal system for quantum communication environments*

Anderson de Araújo[1], **Marcelo Finger**[1]

[1]Department of Computer Science
Institute of Mathematics and Statistics (IME)
University of Sao Paulo (USP)
CEP 05508 090 – São Paulo – SP – Brazil

aaraujo@gmail.com, mfinger@ime.usp.br

Abstract. *The present paper provides a complete first-order system for quantum communication environments. These environments are static reliable synchronous systems of quantum communication among agents and the formal system defined combines probability and knowledge operators to describe them.*

1. Introduction

In these days quantum computing is one of the main lines of research in computer science [Nielson and Chuang 2000]. The interest basically relies on results that show, first, that quantum computers can efficiently perform tasks for which nowadays we do not know efficient classical algorithm [Shor 1994] and, second, on results that indicates the total security of quantum communication protocols [Mayers 2001]. Although some scientists are suspicious about the viability of quantum computers (see, for instance, [Landauer 1995]), the majority of them beliefs that quantum computation and information are physically implementable and they will be a reality in the future (see, for instance, [Preskill 1998]).

In particular, according to [Ying 2010], quantum computing will have a strong interplay with artificial intelligence, mainly with respect to distributed computation and communication systems, because the physical implementation of functional quantum computers is difficult and an important alternative is the distributed implementation [Yimsiriwattana and Lomonaco 2004]. Nonetheless, the possible physical implementation of quantum distributed systems still has foundational problems, associated to the quantum decoherence and the accumulation and propagation of errors in quantum computers. These problems are summarized in the question raised by Landauer in [Landauer 1996]: how can coding prevent our quantum gates from making small errors, if the code and the device have no way of knowing what gate we are trying to implement?

Landauer's question indicates two central features of computing at the level of quantum systems: probability and knowability. From the one hand, it is necessary to have sophisticated devices to control the probability of errors during computations and, from the other hand, the postulates of quantum mechanics establish that measurements change these probability, that is to say, in a certain sense we have knowledge limitations about quantum systems. In order to make explicit these features in the case of distributed computing, the present paper we will provide a logical analysis of quantum communication systems.

In section 2, the main previous works related to the theme of this paper are presented. In section 3, a formal description of quantum communication environments will

*This work was supported by Fapesp Thematic Project 2008/03995-5 (LOGPROB).

be given. Only static synchronous communication of quantum messages among agents in distributed environments is analyzed, which means that the time evolution of the messages and adversaries are not considered. In section 4, it will be associated a first-order language to quantum communication environments that is able to express facts about probability and knowability in these quantum systems. In section 5, first-order multimodal structures with probability operator are defined, which provides semantics for the language defined. In section 6, a complete axiomatization of the quantum communication structures will be given.

2. Previous works

Quantum communication systems were analyzed for the first time in [van der Meyden and Patra 2003a], where it is proposed a modal logic for knowledge and time in quantum protocols. No axiomatization was presented in that work, its description of the quantum distributed systems will be, however, the main reference for our definition of quantum communication environment. Our perspective is logical oriented and restricted to communication systems, but an overview about others approaches to distributed quantum system can be found in [Denchev and Pandurangan 2008].

It is important to emphasize that our approach to quantum communication systems, differently from [van der Meyden and Patra 2003a], is based on density operators. According to [Cohen-Tannoudji et al. 1977], the formalization of quantum mechanics in terms of density operators is more convenient than the formalization using the state vector language for thinking about scenarios whose states are not completely known, although both being mathematically equivalent. Communication environments are just such a kind of scenario. For this reason, it seems to us that this approach is preferable.

Many logical system have been defined to axiomatize the characteristics of quantum probability; the main references can be found in [K. Engesser and Lehmann 2009]. We mention in special the paper [van der Meyden and Patra 2003b] which provides a clear axiomatization for measurement probabilities in quantum systems. In what follows we will incorporate some of the strategies of [van der Meyden and Patra 2003b]; the differences will be indicated when we reach at the description of our axiomatic.

With respect to knowledge operators in distributed quantum system, the main works are again [van der Meyden and Patra 2003a] and [Baltag and Smets 2010]. Our treatment of knowability presented bellow is similar to that in [Baltag and Smets 2010]. Nevertheless, the axiomatic presented here is essentially different from the previous approaches, because we will relate knowability to quantum communication. In fact, the axiomatics defined here for the knowledge operator in communication environments permits to express many properties that the previous ones are not able to express. Unfortunately, there is no space to show this expressive power in the present paper. In section 7, we will indicate some future works, and to analyse the expressive power of the system outlined in this paper is indeed one of these works.

In what follows we will presuppose knowledge about quantum mechanics, as presented for instance in [Cohen-Tannoudji et al. 1977, Nielson and Chuang 2000], and about modal logics, for instance [Carnielli and Pizzi 2008].

3. Quantum communication environments

We will define quantum communication environments in terms of the concepts of *agents* and *informational states*. This analysis is restricted to static reliable synchronous communication among agents.

Definition 3.1. *An* agent g *is a finite set of* propositions*, i.e.,* $g = \{p_1, \ldots, p_n\}$ *where each* p_i *is a proposition. A* group of agents *is a non-empty finite set of agents. The notion of proposition is primitive.*

To model the communication among agents, we assume that for each agent g in a group G there is a codification cod of the propositions of g as sequences of bits.

Definition 3.2. *Let* $G = \{g_1, \ldots, g_n\}$ *be a group of agents. The* message assignment *is the function* $msg : \{1, 2, \ldots, n\} \rightarrow cod_i$ *where* $cod_i : g_i \rightarrow \{0, 1\}^m$ *is a function which associates a code of length* m *to each proposition of agent* g_i *(this code is a sequence of bits with length* m*). Each* $msg(i)$ *will be called a* message*, and we will write* M_G *to denote the set of all messages of* G*.*

By the first postulate of quantum mechanics [Cohen-Tannoudji et al. 1977, Nielson and Chuang 2000], to the agents' messages there is a corresponding Hilbert space that represents these messages as physical entities.

Definition 3.3. *Let* $G = \{g_1, \ldots, g_n\}$ *be a group of agents. The set of* possible messages H_G *of* G *is the complex Hilbert space generated by* M_G*, i.e.,* H_G *is a set of normalized vectors* $|\ \rangle : M_G \rightarrow \mathbb{C}$*, equipped with the inner product, such that* $\sum_{m \in M_G} ||m\rangle|^2 < \infty$*.*

As we said in the previous section, in communications environments the states of the systems may be not completely known. Then, to formalize the messages while quantum states, we will use the density operator language.

Definition 3.4. *Given a set of vectors* $|msg_1\rangle, \ldots, |msg_k\rangle$ *in* H_G *associated to the messages in* M_G *with respective probability amplitudes* $p_1, \ldots, p_k$*, the density operator for the system* H_G *is the operador* ρ_G *defined by the equation*

$$\rho_G \stackrel{def}{=} \sum_{i=1}^{k} p_i |msg_i\rangle\langle msg_i|,$$

where $|msg_i\rangle\langle msg_i|$*, the outer product of* $msg_i \in M_G$*, is called a* quantum message.

Due to one of the postulates of quantum mechanics [Cohen-Tannoudji et al. 1977, Nielson and Chuang 2000], any vector in H_G can be represented as sequences of *quantum bits* (*qubit* for short), which are represented by the two dimensional Hilbert space $\overline{H}_G$, with a preferred orthonormal basis given by the two vectors $|0\rangle$ and $|1\rangle$. More precisely, an m-qubit Hilbert space is a space $\overline{H}_G^m$ of dimension 2^m with the form

$$\overline{H}_G \overbrace{\otimes \cdots \otimes}^{m} \overline{H}_G,$$

where $\otimes$ is the tensor product. We write $|v_1, \ldots, v_m\rangle$ for the vector $|v_1\rangle \otimes \cdots \otimes |v_m\rangle$ in $\overline{H}_G^m$, where each v_j is either 0 or 1. The set of vectors $|v_1, \ldots, v_m\rangle$ is a basis of $\overline{H}_G^m$, called the *computational basis*. We will identify H_G with $\overline{H}_G^m$ and will just write H_G.

In a quantum passing message system, each message is thought of as being in the possession of some agent, but this agent may change from time to time, as an agent can send some of its message to another. Following [van der Meyden and Patra 2003a], we define a function to denote the location of each message.

Definition 3.5. *Let H_G be the Hilbert space of the group of agents $G = \{g_1, \ldots, g_n\}$. The* m-location assignment *is the function $loc : H_G \to \{1, 2, \ldots, n\}$ such that $loc(msg(i))$ denotes that agent g_i has the message $msg(i)$ of H_G.*

Note that the letter m in the expression "m-location assignment" is to remember that the codes are sequences of qubits with length m. These sequences of qubits represent in quantum terms the previous codes of the messagens in M_G. Now we can model the reliable synchronous communication of quantum messages among the agents as the transmission of quantum messages from one agent to another agent in a group.

Definition 3.6. *Let H_G be the Hilbert space of group of agents $G = \{g_1, \ldots, g_n\}$. The* channel assignment *is the function $chan : \{1, 2, \ldots, n\}^2 \to H_G$ such that $chan(i, j) = |msg\rangle$ means that the quantum message $|msg\rangle$ has been transmitted from agent g_i to agent g_j.*

Suppose that $loc^{-1}(i) = \{i_l, \ldots, i_k\}$ is the set of indices of the quantum messages located at agent i. Then agent i is able to perform a general measurement on these k messages. We represent a quantum operation on k messages by a finite sequence of operators $M = (M_1, \ldots, M_l)$ with each M_j operating on H_G. Suppose the agents simultaneously perform the quantum measurements $(M_1, \ldots, M_l)$ where each M_i is a measurement on the $k_i = |loc^{-1}(i)|$ quantum message located at agent i. Each operation M_i products some outcome m_i, the index of some linear transformation M_j operating on H_G. We represent a combined outcome of these measurements by a new function from agents to outcomes.

Definition 3.7. *Let H_G be the set of possible messages of a group of agents $G = \{g_1, \ldots, g_n\}$ and $M = (M_1, \ldots, M_l)$ be a finite sequence of operators on H_G. The* measurement assignment *is the function $res : G \to M \times \mathbb{R}$ such that $res(i) = (M_i, m_i)$ records the measurement performed and the outcome obtained by the agent i.*

By one of postulates of quantum mechanics [Cohen-Tannoudji et al. 1977, Nielson and Chuang 2000], each measurement M_i is a self-adjoint linear operator and the outcome of a measurement is a real number. So the measurement assignment res is well-defined. In this way, we conclude our description of the quantum communication environments.

Definition 3.8. *A* quantum communication environment *is a tuple $E = (G, S)$ where G is a group of agents and $S = \{s_1, \ldots, s_m\}$ is the set of* informational states *for $s_j = (msg, loc, chan, res)$.*

Since we are confined to a static description of quantum communication environments, we will not consider the postulate of quantum mechanics that expresses which the time evolution of quantum systems is given by an unitary operator [Cohen-Tannoudji et al. 1977, Nielson and Chuang 2000].

4. Quantum communication languages

A quantum communication language is specified by defining its *alphabet*, *terms* and *formulas*.

Definition 4.1. *Let $E = (G, S)$ be a quantum communication environment. The* language *of E is the multimodal first-order language with equality $\mathcal{L}$ such that:*

1. *The alphabet of $\mathcal{L}$ has two sorts of variables, one sort for* scalars *and other for* vectors*, as well as an infinite set of* basis variables $\{\vec{v}, \vec{w}, \ldots\}$ *to represent the basis set considered for H_G*[1]*;*
2. *For each of these basis variables $\vec{v}$, the alphabet of $\mathcal{L}$ also has a finite set of* constant vectors $\vec{v}_0, \ldots, \vec{v}_m$ *representing the vectors in the basis of H_G;*
3. *The alphabet of $\mathcal{L}$ has the* scalar constants 0 *and* 1 *and the* vector constants $\vec{0}$ *and* $\vec{1}$*;*
4. *The alphabet of $\mathcal{L}$ has the functions symbols $-$, $+$ and $\times$ for the usual operations on elements in a real-closed field, the function symbols $\neg_v$, $+_v$, $\times_s$ and $\times_v$ for the orthocomplement, matrix addition, multiplication by a scalar and matrix multiplication on vector spaces;*
5. *The alphabet of $\mathcal{L}$ has a unary* probability operator P *and a binary* basis transformation M_{ij}*;*
6. *The alphabet of $\mathcal{L}$ has* knowledge operators K_I*, one for each subgroup of agents $I \subseteq G$;*
7. *Nothing more except the symbols specified above are in the* alphabet *of $\mathcal{L}$.*

The definitions of all syntactic notions are as in [Carnielli and Pizzi 2008], including the *terms* and *formulas*, except by the following differences.

Definition 4.2. *The set of terms of $\mathcal{L}$ is such that:*

1. *The* matrix terms *of $\mathcal{L}$ are defined in the following way:*
   (a) *The constant vectors and variables for constant vectors are matrix terms;*
   (b) *If α and β are matrix terms and a is an scalar constant, then $\neg_v\alpha$, $a \times_s \alpha$, $\alpha +_v \beta$ and $\alpha \times_v \beta$ also are terms.*
2. *If α is a matrix term, then $P(\alpha)$ is a term of $\mathcal{L}$. These terms are called* probability terms*.*
3. *If $\vec{v}$ and $\vec{w}$ are basis variables, then $M_{ij}(\vec{v}, \vec{w})$ is a term of $\mathcal{L}$. These terms are called* transformation terms*.*
4. *The matrix, probability and transformation terms are just the terms of $\mathcal{L}$ defined by the conditions (1), (2) and (3) above.*

Moreover, the scalar terms *are just the terms defined in $\mathcal{L}$ from 0 and 1 using $-$, $+$ or $\times$ as well as any pseudo-term defined using these scalar constants and funtions*[2]*.*

[1] Since the expressiveness of many-sorted logic and first-order logic is the same [Hodges 2005, p.202-206], we will omit the reference to sorts.

[2] Pseudo-terms are formulas that defines elements is the structure considered. For example, terms for denoting real numbers and complex numbers can be defined in $\mathcal{L}$ as pseudo-terms.

In quantum mechanics probability has a crucial role. Hence it is important to designate some special formulas that express facts about probabilities in quantum communication environments.

Definition 4.3. *In the set of formulas of $\mathcal{L}$ a* linear probability atom *is an expression of the form $a_1 \times P^1(\alpha_1) + \cdots + a_k \times P^1(\alpha_k) = a$, where each a_i is a scalar term as well as a, and each α_i is a matrix term.*

As the language $\mathcal{L}$ has knowledge operators K_I for subgroups of agents, it can state facts about distributed knowledge in communication environments, such as in [Baltag and Smets 2010]. In particular, the description of the knowledge of an individual agent i is described by $K_{\{i\}}$, which we abbreviate by K_i. Besides, $\mathcal{L}$ has probability and transformation operators similar to [van der Meyden and Patra 2003b], and so it can also state properties about quantum distributed knowledge. Concepts like entanglement of information, phase relations, uncertainty relation, etc, also can be expressed in $\mathcal{L}$. This shows that the language $\mathcal{L}$ has enough expressiveness with respect to quantum communication environments. For instance, the statement that agent i knows the message α with probability $\frac{1}{\sqrt{2}}$ can be expressed by the sentence $K_i P(\alpha) = \frac{1}{\sqrt{2}}$ of the language $\mathcal{L}$[3].

5. Quantum communication structures

Quantum communication environments are distributed systems, so we need a semantics for the language $\mathcal{L}$ which permits us to consider the transmission of quantum messages among the agents. For such an aim, we define the notion of *informational range*.

Definition 5.1. *Let $E = (G, S)$ be a communication environment. The* informational range *R_G of the group G is a family of binary relations $\approx_I$ on H^2_G, one for each $I \subseteq G$, i.e,*

$$R_G = \{\approx_I \subseteq H^2_G : I \subseteq G\}.$$

Intuitively, an informational range shows how the information is available among the subgroups of agents. From this concept, we can define equivalence relations among the information associated to the agent's messages.

Definition 5.2. *Let $E = (G, S)$ be a communication environment and R_G be the informational range of G. An E-*quantum communication frame *is a multi-modal frame (H_G, R_G) such that:*

Equivalence *: For each $I \subseteq G$, $\approx_I$ is an equivalence relation;*
Observability *: For all $s, r, \in H_G$ and $I \subseteq G$, if $s = r$ then $s \approx_I r$;*
Monotonicity *: For all $I, J \subseteq G$, if $I \subseteq J$ then $\approx_J \subseteq \approx_I$;*
Vacuousness *: For all $s, r, \in H_G$, $s \approx_\emptyset r$.*

The equivalence condition establishes that if $s \approx_I r$ then the subgroup I cannot distinguish the informational state s from r, that is to say, s and r are *indistinguishable* to I. One the other hand, by the observability condition, if r and s are equals then every

[3]The expression $\frac{1}{\sqrt{2}}$ is a pseudo-term that is definable using the symbols for field expression of the language $\mathcal{L}$.

group of agents cannot distinguish between r and s. The monotonicity expresses that if some informational states are indistinguishable for a group of agents I then these states are also indistinguishable for any subgroup J of I. Finally, the vacuouness says that the empty group cannot distinguish between any two informational states, which is true for it is unable to make any observation.

Definition 5.3. *Let $E = (G, S)$ be a communication environment and (H_G, R_G) be an E-quantum communication frame. A* quantum communication structure *$\mathcal{A}$ for the language $\mathcal{L}$ is the tuple $\mathcal{A} = (H_G, R_G, I_G)$ in which I_G is an interpretation function from $\mathcal{L}$ to H_G such that:*

1. *$I_G(0)$ is the number zero and $I_G(1)$ is the number one in the complex field $\mathbb{C}$ of H_G;*
2. *$I_G(\vec{0})$ is the null matrix and $I_G(\vec{1})$ is the identity matrix of H_G;*
3. *For each state constant $\vec{v}_i$ of $\mathcal{L}$, $I_G(\vec{v}_i)$ is the matrix $|v_i\rangle\langle v_i|$ where $|v_i\rangle$ is the i-th vector of the computational basis of H_G;*
4. *$I_G(-)$, $I_G(+)$ and $I_G(\times)$ are the functions inverse, plus and times, respectively, on the complex field $\mathbb{C}$ of H_G;*
5. *$I_G(\neg_b)$ is the projection operator $\perp$ projecting onto the orthogonal complement of the image of H_G under the state considered, $I_G(+_v)$ is the matrix addition of H_G, $I_G(\times_s)$ is matrix multiplication by a scalar and $I_G(\times_v)$ is the matrix multiplication of H_G[4];*
6. *$I_G(P)$ is the unary operator on H_G such that $I_G(P)(|v_i\rangle)$ is the trace of the matrix $|v_i\rangle\langle v_i||v_i\rangle\langle v_i|$, i.e., $I_A(P)(|v_i\rangle) := \mathit{Tr}(|v_i\rangle\langle v_i||v_i\rangle\langle v_i|) := \sum_j(|v_i\rangle\langle v_i||v_i\rangle\langle v_i|)_{jj} = |\langle v_i|v_i\rangle|^2$;*
7. *$I_G(M_{i,j})$ is the binary operator on H_G such that $I_G(M_{i,j})(|v\rangle, |w\rangle)$ is the element v_{ij} such that $M = (v_{ij})$ is the $m \times m$ unitary complex matrix for which $M|v\rangle = |w\rangle$.*

From the notion of quantum communication structure, we define the *satisfatibility relation* $\models_s$ as in [Carnielli and Pizzi 2008]. We only emphasize the case for modal formulas:

$$\mathcal{A} \models_s K_I\phi \text{ if, and only if, for all } r \in H_G \text{ such that } r \approx_I s, \mathcal{A} \models_r \phi.$$

6. Quantum communication axiomatics

In this section we will define a theory $\mathcal{T}$ for quantum communication environments. We will presuppose a *derivability relation* $\vdash$ defined according to some classical calculus for first-order logic, for instance the one in [Carnielli and Pizzi 2008], and we will only specify the new axioms and rules of $\mathcal{T}$. The axiomatization of $\mathcal{T}$ consists of four parts, each dealing with one aspect of these communication systems.

The first part of $\mathcal{T}$ has axioms to express that the set of possible messages is an m-dimensional Hilbert space, where m is the maximum length of the messages in M_G, and that the Hilbert space is a orthocomplemented lattice.

(A1) $(\vec{v}_1 \vee \cdots \vee \vec{v}_n) \wedge (\neg i = j \rightarrow \neg(\vec{v}_i \wedge \vec{v}_j))$

[4]We will omit $\times_v$ when it is clear that we are considering the matrix multiplication.

(A2) $(\alpha \times_v \neg_v \alpha = \vec{0}) \wedge (\alpha +_v \neg_v \alpha = \vec{1}) \wedge (\neg_v \neg_v \alpha = \alpha)$
(A3) $(\alpha \leq \beta \rightarrow \neg_v \beta \leq \neg_v \alpha) \wedge (\alpha \times_v (\neg_v \alpha +_v (\alpha \times_v \beta)) \leq \beta)$

The second part of $\mathcal{T}$ has axioms to state the properties of the quantum probability operator for quantum communication environments.

(A4) $0 \leq P(\alpha) \wedge P(\alpha) \leq 1$.
(A5) $P(\alpha +_v \neg_v \beta) = 1$
(A6) $P(\alpha \times_v \beta) + P(\alpha \times_v \neg_v \beta) = P(\alpha)$
(A7) $\alpha = (a_1 \times_s \vec{v}_1) +_v \cdots +_v (a_n \times_s \vec{v}_n) \rightarrow (P(\beta) = |a_1|^2 + \cdots + |a_m|^2 \wedge \beta = (\sqrt{P(\beta)})^{-1} \times ((a_1 \times_s \vec{v}_1) +_v \cdots +_v (a_m \times_s \vec{v}_m)))$ if the measurement was done on the vectors in $\{\vec{v}_i\}_{i \leq n}$.

Note that these axioms are different from those given in [van der Meyden and Patra 2003b]. They explicitly formalize the main property of measuments in quantum mechanics. Besides, in our approach the distributivity of probability is the sentence $\alpha = \beta \rightarrow P(\alpha) = P(\beta)$, which is an immediate theorem due to the Leibniz's law for equality.

The third part of $\mathcal{T}$ has axioms for basis transformation, which corresponds to the identity matrix when the basis is not changed and consecutive basis transformations correspond to matrix multiplication.

(A8) $M_{ij}(\vec{v}, \vec{w}) = M^*_{ij}(\vec{w}, \vec{v})$
(A9) $(i = j \rightarrow M_{ij}(\vec{v}, \vec{v}) = 1) \wedge (\neg i = j \rightarrow M_{ij}(\vec{v}, \vec{v}) = 0)$
(A10) $M_{ij}(\vec{v}, \vec{x}) = (M_{i1}(\vec{v}, \vec{w}) \times M_{i1}(\vec{w}, \vec{x})) + \cdots + (M_{im}(\vec{v}, \vec{w}) \times M_{im}(\vec{w}, \vec{x}))$

Differently from [van der Meyden and Patra 2003b], we have fixed the computational basis for the transformations, which is in accordance with the fact that quantum measurements in other bases can be carried out by combining unitary transformation and measurements on the computational basis [Cohen-Tannoudji et al. 1977, Nielson and Chuang 2000]. In this way, we can define the transition probability operator T (a quantum analogue of conditional probabilities) defined in [van der Meyden and Patra 2003b] stating that $T(\vec{v}_i, \vec{w}_j) = |M_{i,j}(\vec{v}, \vec{w})|^2$. Note, moreover, that from axioms $A8$ and $A10$, it is possible to derive unitarity of the transformations $((M_{i1}(\vec{v}, \vec{w}) \times M^*_{j1}(\vec{v}, \vec{w})) + \cdots + (M_{im}(\vec{v}, \vec{w}) \times M^*_{jm}(\vec{v}, \vec{w}))) = 1$.

The fourth, and last, part of $\mathcal{T}$ has axioms for knowledge operators. These axioms are the usual axioms of the epistemic logic [Baltag and Smets 2010], but in the context of the general framework for distributed knowledge developed here.

(A11) If $\mathcal{T} \vdash \phi$ then $\mathcal{T} \vdash K_G \phi$.
(A12) If $I \subseteq J$ then $\mathcal{T} \vdash K_I \phi \rightarrow K_J \phi$.
(A13) $K_G(\phi \rightarrow \psi) \rightarrow (K_G \phi \rightarrow K_G \psi)$
(A14) $K_G \phi \rightarrow K_G K_G \phi$
(A15) $\neg K_G \phi \rightarrow K_G \neg K_G \phi$

In this way, we end the definition of $\mathcal{T}$.

Definition 6.1. *Let $E = (G, S)$ be a quantum communication environment. The* theory *of E is the first-order theory $\mathcal{T}$ with the axioms and rules $A1$-$A15$ defined above plus a complete axiomatization for algebraically closed fields.*

Since Tarski showed in [Tarski 1951] that the algebraically closed fields can be completely axiomatized, the theory $\mathcal{T}$ is well-defined. Furthermore, we can prove the adequacy of $\mathcal{T}$ with respect to quantum communication structures $\mathcal{A}$.

Theorem 6.1. *For all sentence ϕ of $\mathcal{L}$, $\mathcal{T} \vdash \phi$ if, and only if, $\mathcal{A} \vDash \phi$.*

Proof sketch: The soundness, $\mathcal{T} \vdash \phi$ implies $\mathcal{A} \vDash \phi$, is straightforward. The completeness, $\mathcal{A} \vDash \phi$ implies $\mathcal{T} \vdash \phi$, is a non-trivial task. It comprises an appropriate combination of the completeness proof given in [van der Meyden and Patra 2003b], for the probability and transformation part of $\mathcal{T}$, and the completeness proof for the calculus of orthocomplemented lattice, for the algebraic part of $\mathcal{T}$, with a construction of canonical models for multi-modal logics, for the epistemic part of $\mathcal{T}$[5]. □

7. Future works

The completeness of the theory $\mathcal{T}$ with respect to quantum communication structures shows the adequacy of our approach from a logical point of view. Nonetheless, we have not explored the expressiveness of this framework with respect to distributed quantum systems. An interesting development of our work is to examine that expressiveness.

In our approach we have not considered the time evolution of quantum systems. An interesting approach would be to extend our axiomatic with modalities for time. In [van der Meyden and Patra 2003a], a first attempt was realized, but it is to much restricted and no axioms were exhibited. We believe that a more compelling approach would be to use the logic CTL with probability, for instance as that showed in [Brázdil et al. 2008] or as in [Baltazar et al. 2008].

In quantum mechanics, tensor product has a crucial significance. We can already handle this to some extent simply by applying our language to the case where the dimension of the Hilbert space H_G is a restricted product, but it is desirable to have the tensor product as a more integral part of the language. In [Mateus and Sernadas 2006], it was showed a quantum logic capable to expresses tensor product, but such a logical system is so complicated and we cannot foresee how to combine it with multi-modal logic, as we need in quantum communication environments.

To conclude, it is important to mention that we have not analyzed questions of computational complexity. As we work with probability operators in quantum systems, it would be desirable to analyze the *probabilistic satisfiability problem* [Georgakopoulos et al. 1988] in the context of quantum communication environments. In fact it is the quantum version of the satisfiability problem [Bravyi 2006] which is in question, for quantum systems have quantum probability and not the classical one. We do not know if the logical system presented in this paper is able to express the quantum satisfiability problem. If it can, then we can analyze open problems about quantum satisfiability using our logical system, from the one hand, and to examine the complexity of quantum communication in distributed systems, for the other.

[5]The complete proof will be presented in the extended version of this paper.

References

Baltag, A. and Smets, S. (2010). Correlated knowledge: an epistemic-logic view on quantum entanglement. *International Journal of Theoretical Physhics*, 49:3005–3021.

Baltazar, P., Chadha, R., and Mateus, P. (2008). Quantum computation tree logic - model checking and complete calculus. *International Journal of Quantum Information*, 6(2):219–236.

Bravyi, S. (2006). Efficient algorithm for a quantum analogue of 2-sat. ArXiv Quantum Physics e-prints.

Brázdil, T., Forejt, V., and Kucera, J. K. A. (2008). The satisfiability problem for probabilistic ctl. In *LICS 2008*, volume 1043-6871/08 of *IEEE Computer Science Society*, pages 391–402.

Carnielli, W. and Pizzi, C. (2008). *Modalities and Multimodalities*. Logic, Epistemology, and the Unity of Science. Springer Verlag, Berlin.

Cohen-Tannoudji, C., Diu, B., and Laloë, F. (1977). *Quantum Mechanics*. Wiley, New York.

Denchev, V. and Pandurangan, G. (2008). Distributed quantum computing: A new frontier in distributed systems or science fiction? *ACM SIGACT News*, 39(3):77–95.

Georgakopoulos, G., Kavvadias, D., and Papadimitriou, C. H. (1988). Probabilistic satisfiability. *Journal of Complexity*, 4(1):1–11.

Hodges, W. (2005). *Model Theory*. Encyclopedia of Mathematics and Applications. Cambridge University Press, Cambridge.

K. Engesser, D. M. G. and Lehmann, D. (2009). *Handbook of quantum logic and quantum structures*. North-Holland. Elsevier, Amsterdan.

Landauer, R. (1995). Is quantum mechanics useful? *Philosophical Transactions: Physical Sciences and Engineering*, 353(1703):367–376.

Landauer, R. (1996). The physical nature of information. *Physics Letters A*, 217:188–193.

Mateus, P. and Sernadas, A. (2006). Weakly complete axiomatization of exogenous quantum propositional logic. *Information and Computation*, 204:771–794.

Mayers, D. (2001). Unconditional security in quantum cryptography. *Journal of the ACM*, 48(3):351–406.

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

Preskill, J. (1998). Quantum computing: Pro and con. In *Quantum Coherence and Decoherence*, volume 454 of *Mathematical, Physical and Engineering Sciences*, pages 469–486. The Royal Society.

Shor, P. (1994). Algorithms for quantum computation: Discrete log and factoring. In Goldwasser, S., editor, *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, pages 124–134. IEEE Computer Society Press, Los Alamitos.

Tarski, A. (1951). *A Decision Method for Elementary Algebra and Geometry*. 2nd ed. University of California Press, Berkeley.

van der Meyden, R. and Patra, M. (2003a). Knowledge in quantum systems. In Tennenholtz, M., editor, *Theoretical Aspects of Rationality and Knowledge*, volume 6433, pages 104–117. ACM.

van der Meyden, R. and Patra, M. (2003b). A logic for probability in quantum systems. In Baaz, M. and Makowsky, J., editors, *Computer Science Logic*, volume 2803 of *Lecture Notes in Computer Science*, pages 427–440, Berlin. Springer.

Yimsiriwattana, A. and Lomonaco, S. J. (2004). Distributed quantum computing: A distributed shor algorithm. In Donkor, E., Pirich, A. R., and Brandt, H. E., editors, *Quantum Information and Computation II*, volume 5436 of *MSPIE*, pages 360–372.

Ying, M. (2010). Quantum computation, quantum theory and ai. *Artificial Intelligence*, 174:162–176.