

Dynamic Quantum Logic for Quantum Programs

Olivier Brunet, Philippe Jorrand
Leibniz Laboratory, University of Grenoble
46, avenue Félix Viallet, 38000 Grenoble, France
olivier.brunet@imag.fr
philippe.jorrand@imag.fr

November 20, 2003

Abstract

We present a way to apply quantum logic to the study of quantum programs. This is made possible by using an extension of the usual propositional language in order to make transformations performed on the system appear explicitly. This way, the evolution of the system becomes part of the logical study. We show how both unitary operations and two-valued measurements can be included in this formalism and can thus be handled logically.

1 Introduction

The logical study of quantum mechanics, originated in the thirties by von Neumann and Birkhoff[4], aims at investigating formally what makes quantum mechanics so different from the classical world. To quote the pioneering article: “*One of the aspects of quantum theory which has attracted the most general attention, is the novelty of the logical notions which it presupposes... The object of the present paper is to discover what logical structures one may hope to find in physical theories which, like quantum mechanics, do not conform to classical logic.*” The starting point of this study is based on the use of *closed subspaces* of a Hilbert space \mathcal{H} for representing properties about the system. The operations defined on subspaces, such as the orthocomplementation and the intersection, are interpretations of the negation and conjunction on propositions, thus allowing to define a full-fledged propositional logic. This constitutes the *standard quantum logic* or *orthomodular quantum logic*[9, 14, 6].

Since its origins, many variations have been studied, and different attempts have been made to identify some axioms or conditions which would permit to recapture the Hilbert space formalism[11, 12, 13]. Unfortunately, despite the large amount of publications on this topic, these works have remained extremely theoretical, and have led to very little applications. However, it is possible to use the quantum logic formalism to express and study properties in a quantum

computation context, by extending the language in order to have quantum operations appear explicitly and thus having the possibility to include the evolution of a system in the logical study.

In the present article, we present such a kind of extension of the quantum logic formalism. It is based on the use of closed subspaces as partial descriptions of states of the system (with statements of the form “the actual state lies in this subspace”), and logical assertions can then be seen as relating knowledge about the system’s state at different moments during the computation. With this approach, we will consider the application of unitary operators, which modify the knowledge without losing information, and the process of measurement, where some loss of information occurs.

2 Standard Quantum Logic

2.1 Basic definitions

Our formalism for representing subspaces by terms of a propositional language relies on two elements: a language (i.e. a set of propositional terms) \mathcal{L} and an *interpretation* function $\llbracket \cdot \rrbracket$ which maps each term of the language to a closed subspace of \mathcal{H} . This way, each term $p \in \mathcal{L}$ is associated to a closed subspace of \mathcal{H} , denoted $\llbracket p \rrbracket$. Our language \mathcal{L} contains two connectives: negation \neg and conjunction \wedge , and a set of constants Ψ . Thus, every constant $p \in \Psi$ is a term (i.e. $p \in \mathcal{L}$) and given two terms $p, q \in \mathcal{L}$, both $\neg p$ and $p \wedge q$ are terms.

The definition of the interpretation function is based on the structure of the terms, and on the correspondance between the negation $\neg \cdot$ and the orthocomplementation \cdot^\perp on the one hand, and between the conjunction $\cdot \wedge \cdot$ and the intersection $\cdot \cap \cdot$ on the other hand. Thus, the definition of $\llbracket \cdot \rrbracket$ is given by:

$$\forall p \in \mathcal{L}, \llbracket \neg p \rrbracket = \llbracket p \rrbracket^\perp \quad \forall p, q \in \mathcal{L}, \llbracket p \wedge q \rrbracket = \llbracket p \rrbracket \cap \llbracket q \rrbracket \quad (1)$$

The definition is completed by the interpretation of each atomic proposition. In the following, we will consider the restricted case where the Hilbert space \mathcal{H} is of the form $\otimes^n \mathbf{C}^2$, and atomic propositions are z_i and x_i with $1 \leq i \leq n$. Intuitively, the propositions relate to the corresponding direction of the i^{th} qubit. If $n = 1$, the interpretations are defined by $\llbracket z \rrbracket = \mathbf{C}|1\rangle$ and $\llbracket x \rrbracket = \mathbf{C}|-\rangle = \mathbf{C}(|0\rangle - |1\rangle)$, and for $n > 1$, this definition is extended by using tensor products. For instance:

$$\llbracket x_i \rrbracket = (\otimes^{i-1} \mathbf{C}^2) \otimes \mathbf{C}|-\rangle \otimes (\otimes^{n-i} \mathbf{C}^2) \quad (2)$$

Finally, two constants are useful to define: the true proposition \top , verified everywhere (its interpretation $\llbracket \top \rrbracket$ equals the whole Hilbert space \mathcal{H}) and the absurd proposition \perp which cannot be verified, so that $\llbracket \perp \rrbracket = \{0\}$.

2.2 Additional connectives

Even though the logical language as defined above is expressive enough, it is interesting to introduce other connectives, using the two already available op-

erations (negation \neg and conjunction \wedge). First, we define the disjunction $p \vee q$ as $\neg(\neg p \wedge \neg q)$. In terms of subspaces, this connective has a simple formulation, since it corresponds to the sum of two subspaces:

$$\llbracket p \vee q \rrbracket = \llbracket \neg(\neg p \wedge \neg q) \rrbracket = (\llbracket p \rrbracket^\perp \cap \llbracket q \rrbracket^\perp)^\perp = \llbracket p \rrbracket \oplus \llbracket q \rrbracket \quad (3)$$

An implication connective $p \rightarrow q$ can also be defined, using its classical definition, that is $\neg p \vee q$ or equivalently $\neg(p \wedge \neg q)$, so that $\llbracket p \rightarrow q \rrbracket = \llbracket p \rrbracket^\perp \oplus \llbracket q \rrbracket$. With this connective, it is easy to define the equivalence connective: $p \leftrightarrow q$ stands for $(p \rightarrow q) \wedge (q \rightarrow p)$. This connective will be very useful in our approach, as it can be used to express some kind of equality between different qubit states. Finally, we also introduce the exclusive disjunction connective $p \vee\!\!\!\! \vee q$ as the negation of the equivalence, that is $\neg(p \leftrightarrow q)$. Its interpretation can be expressed as:

$$\llbracket p \vee\!\!\!\! \vee q \rrbracket = (\llbracket p \rrbracket \wedge \llbracket q \rrbracket^\perp) \oplus (\llbracket p \rrbracket^\perp \wedge \llbracket q \rrbracket) \quad (4)$$

This operator appears frequently in the study of quantum program, since it is the logical equivalent to the addition modulo 2 for integers.

2.3 Example: Description of an e.p.r. pair

This simple logical language permits to fully describe many interesting states of a quantum system. To illustrate this, we show that proposition $(z_1 \leftrightarrow z_2) \wedge (x_1 \leftrightarrow x_2)$ is a complete description of an *e.p.r.* pair [8, 5]:

$$\begin{aligned} \llbracket z_1 \leftrightarrow z_2 \rrbracket &= \llbracket z_1 \rightarrow z_2 \rrbracket \wedge \llbracket z_2 \rightarrow z_1 \rrbracket \\ &= (\llbracket z_1 \rrbracket^\perp \oplus \llbracket z_2 \rrbracket) \cap (\llbracket z_1 \rrbracket \oplus \llbracket z_2 \rrbracket^\perp) \\ &= (\mathbf{C}|00\rangle \oplus \mathbf{C}|10\rangle \oplus \mathbf{C}|11\rangle) \oplus (\mathbf{C}|00\rangle \oplus \mathbf{C}|01\rangle \oplus \mathbf{C}|11\rangle) \\ &= \mathbf{C}|00\rangle \oplus \mathbf{C}|11\rangle \end{aligned}$$

$$\llbracket x_1 \leftrightarrow x_2 \rrbracket = \mathbf{C}|++\rangle \oplus \mathbf{C}|--\rangle$$

$$\begin{aligned} \llbracket (z_1 \leftrightarrow z_2) \wedge (x_1 \leftrightarrow x_2) \rrbracket &= \llbracket z_1 \leftrightarrow z_2 \rrbracket \cap \llbracket x_1 \leftrightarrow x_2 \rrbracket \\ &= (\mathbf{C}|00\rangle \oplus \mathbf{C}|11\rangle) \cap (\mathbf{C}|++\rangle \oplus \mathbf{C}|--\rangle) \\ &= \mathbf{C}(|00\rangle + |11\rangle) \end{aligned}$$

Equivalently, one can use $(z_1 \vee\!\!\!\! \vee z_2 \leftrightarrow \perp) \wedge (x_1 \vee\!\!\!\! \vee x_2 \leftrightarrow \perp)$ to describe e.p.r. pairs. In that case, one can interpret $\vee\!\!\!\! \vee$ as the addition modulo 2, \leftrightarrow as the equality and \perp as 0. Similarly, it can be shown that proposition $(z_1 \vee\!\!\!\! \vee z_2 \leftrightarrow \perp) \wedge (z_1 \vee\!\!\!\! \vee z_3 \leftrightarrow \perp) \wedge (x_1 \vee\!\!\!\! \vee x_2 \vee\!\!\!\! \vee x_3 \leftrightarrow \perp)$ is a complete characterization of a GHZ state.

2.4 Entailment

In order to be able to relate propositions seen as different descriptions of a system, we introduce a last notion, corresponding to the inclusion of interpretations: given two terms p and q , p will be said to entail q (which we will denote

$p \Vdash q$) if and only if $\llbracket p \rrbracket \subseteq \llbracket q \rrbracket$. If both interpretations are equal, we may also write $p \dashv\vdash q$.

This entailment relation can be related to the implication connective, and more precisely, to terms p and q verifying $\llbracket p \rightarrow q \rrbracket = \mathcal{H}$, which can be written as $\top \Vdash p \rightarrow q$, or more shortly $\Vdash p \rightarrow q$. For instance, it can be easily shown that if $p \Vdash q$, then $\Vdash p \rightarrow q$, but the converse is not true, as illustrated by the fact that for a single qubit, one has $\Vdash z \rightarrow x$ but $\llbracket z \rrbracket \not\subseteq \llbracket x \rrbracket$.

Contrary to the implication, it is possible to express and perform deductions using the entailment relation: from $p \Vdash q$ and $q \Vdash r$, it is possible to deduce that $p \Vdash r$. This motivates the fact that this relation will be used in the following to express relations among properties verified by a system at different steps of a quantum program.

3 Dynamic Aspects, Unitary Operations

3.1 Extension of the language

In order to include an explicit reference to the dynamic evolution of a system, we will extend our propositional language by adding a collection of unary connectives (denoted $[u]$), each corresponding to the application of an unitary operator U on the system. The idea is to associate a proposition $[u]p$ to a system initially verifying p (that is in a state $|\varphi\rangle$ in $\llbracket p \rrbracket$) and on which U is applied. This permits to define the interpretation of such a connective:

$$\llbracket [u]p \rrbracket = \{U|\varphi\rangle \mid |\varphi\rangle \in \llbracket p \rrbracket\} \quad (5)$$

With the introduction of these additional connectives, it becomes possible to express relationships between the different states of a system along the execution of unitary transformations. For instance, simple calculations show that the subspace spanned by $|1\rangle$ is left unchanged by the application of the Hadamard operator, since $\sigma_z|1\rangle = -|1\rangle$. This can be written logically as: $[\sigma_z]z \dashv\vdash z$. Similarly, one has $[\sigma_y]x \dashv\vdash \neg x$, since $\sigma_y|-\rangle = i|+\rangle$. It is possible to express similar assertions for more complex propositions. For instance:

$$[\oplus_{1,2}](z_2 \leftrightarrow \perp) \dashv\vdash z_1 \leftrightarrow z_2 \quad (6)$$

The linearity and invertibility of unitary operators implies that the application of such an operator does commute with both orthocomplementation and intersection operations. Logically, one can thus write:

$$[u](\neg p) \dashv\vdash \neg([u]p) \quad [u](p \wedge q) \dashv\vdash ([u]p) \wedge ([u]q)$$

This means in particular that the definition of the behaviour of different operators can be done by just specifying their behaviour for atomic propositions. For instance, the complete description of $\sigma_{z,i}$ (where the i indice means that σ_z acts on the i th qubit) for atomic propositions z and x is given by:

$$[\sigma_{z,i}]z_i \dashv\vdash z_i \quad [\sigma_{z,i}]x_i \dashv\vdash \neg x_i \quad (7)$$

Pauli operators

$$\begin{array}{ll} [\sigma_{z,i}] z_i & \Vdash z_i & [\sigma_{z,i}] x_i & \Vdash \neg x_i \\ [\sigma_{x,i}] z_i & \Vdash \neg z_i & [\sigma_{x,i}] x_i & \Vdash x_i \\ [\sigma_{y,i}] z_i & \Vdash \neg z_i & [\sigma_{y,i}] x_i & \Vdash \neg x_i \end{array}$$

Hadamard operator

$$[H_i] z_i \Vdash x_i \quad [H_i] x_i \Vdash z_i$$

Controlled-Not operator

$$\begin{array}{ll} [\oplus_{i,j}] z_i & \Vdash z_i & [\oplus_{i,j}] x_i & \Vdash x_i \vee x_j \\ [\oplus_{i,j}] x_j & \Vdash x_j & [\oplus_{i,j}] z_j & \Vdash z_j \vee z_i \end{array}$$

Toffoli operator

$$\begin{array}{ll} [T_{i,j,k}] z_i & \Vdash z_i & [T_{i,j,k}] x_i & \Vdash x_i \vee (z_j \wedge x_k) \\ [T_{i,j,k}] z_j & \Vdash z_j & [T_{i,j,k}] x_j & \Vdash x_j \vee (z_i \wedge x_k) \\ [T_{i,j,k}] x_k & \Vdash x_k & [T_{i,j,k}] z_k & \Vdash z_k \vee (z_i \wedge z_j) \end{array}$$

Figure 1: Definition of some usual unitary operators

Properties corresponding to other qubits are left unchanged. For instance, one has: $[\sigma_{z,1}] x_2 \Vdash x_2$. With atomic terms z , x and y for each qubit, it is possible to provide the complete description of many common operators, such as the Pauli and Hadamard operators, the controlled-not and the Toffoli operator[2, 7]. They are given in figure 1.

It should be noted that since the action of the Toffoli operator can be described, it follows that this formalism is more general than of stabilizers which plays a central role in the Gottesman-Knill theorem[5], if one considers unitary operations only. However, we will see in section 4 how measurements can be included in our formalism.

3.2 Example: Creation of an *epr* pair

The usual process for creating an *epr* pair is to start from $|00\rangle$ (which is logically expressed as $\neg z_1 \wedge \neg z_2$ or equivalently as $(z_1 \leftrightarrow \perp) \wedge (z_2 \leftrightarrow \perp)$) to apply H_1 and then $\oplus_{1,2}$ to the system, as represented in figure 2. Logically, the quantum circuit can be studied by the following calculation:

$$\begin{aligned} [H_1](\neg z_1 \wedge \neg z_2) & \Vdash [H_1](\neg z_1) \wedge [H_1](\neg z_2) \\ & \Vdash \neg([H_1] z_1) \wedge \neg([H_1] z_2) \\ & \Vdash \neg x_1 \wedge \neg z_2 \end{aligned}$$

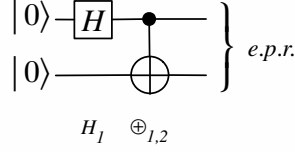


Figure 2: e.p.r. pair creation circuit

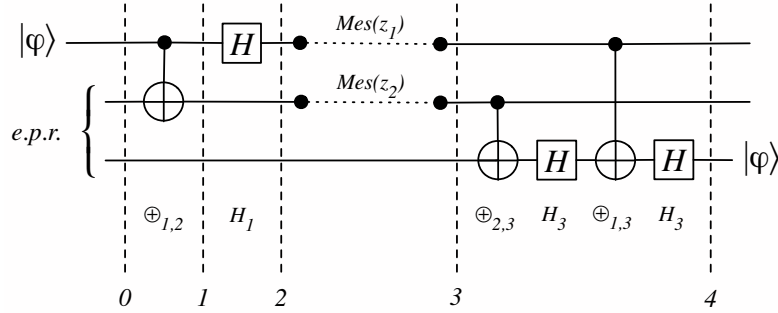


Figure 3: Teleportation circuit

$$\begin{aligned}
[\oplus_{1,2}] [H_1] (\neg z_1 \wedge \neg z_2) &\Vdash [\oplus_{1,2}] (\neg x_1 \wedge \neg z_2) \\
&\Vdash \neg([\oplus_{1,2}] x_1) \wedge \neg([\oplus_{1,2}] z_2) \\
&\Vdash \neg(x_1 \underline{\vee} x_2) \wedge \neg(z_1 \underline{\vee} z_2) \\
&\Vdash (x_1 \leftrightarrow x_2) \wedge (z_1 \leftrightarrow z_2)
\end{aligned}$$

As expected, the final proposition, that is $(x_1 \leftrightarrow x_2) \wedge (z_1 \leftrightarrow z_2)$, provides a complete characterization of the subspace spanned by e.p.r. pairs as we have seen in example 2.3.

3.3 Example: A teleportation circuit

In order to illustrate the use of our formulation of quantum logic for the study of more complex programs, we develop a teleportation circuit [1, 3] and show how it is possible to relate properties verified by a qubit before and after the teleportation. The circuit is defined in figure 3.

Let us first concentrate on the left part of the circuit, from step 0 to step 2. One has for the first qubit:

$$z_1 \Vdash [H_1] x_1 \Vdash [\oplus_{1,2}] [H_1] (x_1 \underline{\vee} x_2) \quad (8)$$

We simplify these notations by using exponents to indicate the stage of the computation (i.e. the number of the vertical dashed lines). This permits to remove the unary connectives corresponding to the gates, so that for instance

the previous proposition rewrites as:

$$z_1^2 \dashv\vdash x_1^1 \dashv\vdash x_1^0 \vee x_2^0 \quad (9)$$

Likewise, the second qubit verifies $z_2^2 \dashv\vdash z_1^0 \vee z_2^0$. The third qubit is left unchanged, so that $z_3^2 \dashv\vdash z_3^0$ and $x_3^2 \dashv\vdash x_3^0$. Now, since qubits 2 and 3 were part in the beginning of an e.p.r. pair, it follows that $z_2^0 \dashv\vdash z_3^0$ and $x_2^0 \dashv\vdash x_3^0$. From this, some manipulations can be done on properties, so that the first part of the system can be fruitfully characterized by these two propositions:

$$x_1^0 \dashv\vdash x_3^2 \vee z_1^2 \quad z_1^0 \dashv\vdash z_3^2 \vee z_2^2 \quad (10)$$

Concerning the second part of the circuit, similar calculations permit to express the following properties about the third qubit :

$$z_3^4 \dashv\vdash z_2^3 \vee z_3^3 \quad x_3^4 \dashv\vdash z_1^3 \vee x_3^3 \quad (11)$$

If we remove the measurements and bit-transmissions and identify steps 2 and 3, these two portions can be combined, and lead to:

$$z_3^4 \dashv\vdash z_1^0 \quad x_3^4 \dashv\vdash x_1^0 \quad (12)$$

This shows that properties z and x on the first qubit at the beginning are transformed into the same properties on the third qubit at the end of the circuit.

4 Dealing with Measurements

4.1 A new unary connective

We have explained how unitary operators can be included in our logical formalism by the introduction of unary connectives and explore now the way measurements can be expressed in our formalism. For simplicity, we will consider only one form of measurement, that of qubit i along the z -direction, which we will represent by a collection of unary connectives $[m_z(i)]$.

One needs, given a proposition p , to determine the interpretation of $[m_z(i)]p$. This is done as before, with $\llbracket [m_z(i)]p \rrbracket$ defined as the smallest subspace containing every state which can be obtained after the measurement when starting from elements of $\llbracket p \rrbracket$.

For this, suppose that our system is in a state $|\varphi\rangle$ and verifies property p (so that $|\varphi\rangle \in \llbracket p \rrbracket$) and let us perform the measurement of the first qubit along z . After that, the state $|\varphi\rangle$ has been transformed either into state $\frac{1}{2}(|\varphi\rangle + \sigma_z|\varphi\rangle)$ or $\frac{1}{2}(|\varphi\rangle - \sigma_z|\varphi\rangle)$ (rigourously, if the system is made of n qubits, one should write $\sigma_z \otimes I^{n-1}$ but we voluntarily use a simplified notation, since it does not add any ambiguity). Thus, if proposition p represents knowledge about the system before the measurement, the new state belongs to the set:

$$S_p = \left\{ \frac{1}{2}(|\varphi\rangle + \sigma_z|\varphi\rangle) \mid |\varphi\rangle \in \llbracket p \rrbracket \right\} \cup \left\{ \frac{1}{2}(|\varphi\rangle - \sigma_z|\varphi\rangle) \mid |\varphi\rangle \in \llbracket p \rrbracket \right\} \quad (13)$$

But propositions are represented by closed subspaces, so that $\llbracket [m_z(1)] p \rrbracket$ is actually the subspace spanned by S_p . Now, let $|\varphi\rangle$ be a state in $\llbracket p \rrbracket$. From its definition, S_p contains both $\frac{1}{2}(|\varphi\rangle + m|\varphi\rangle)$ and $\frac{1}{2}(|\varphi\rangle - m|\varphi\rangle)$, so that by additivity $|\varphi\rangle \in \llbracket [m_z(1)] p \rrbracket$. It follows that $\llbracket p \rrbracket \subseteq \text{span}(S_p)$. Similarly, considering the difference, $\sigma_z|\varphi\rangle$ is also in $\llbracket [m_z(1)] p \rrbracket$. We have thus shown that:

$$\llbracket p \vee [\sigma_{z,1}] p \rrbracket = \llbracket p \rrbracket \oplus \llbracket [\sigma_{z,1}] p \rrbracket \subseteq \llbracket [m_z(1)] p \rrbracket \quad (14)$$

Conversely, if $|\varphi\rangle$ is in $\llbracket p \rrbracket$, then $\frac{1}{2}(|\varphi\rangle \pm \sigma_z|\varphi\rangle) \in \llbracket p \vee [\sigma_{z,1}] p \rrbracket$, which implies by linearity that actually, one has:

$$\llbracket p \vee [\sigma_{z,1}] p \rrbracket = \text{span}(S_p) = \llbracket [m_z(1)] p \rrbracket \quad (15)$$

Thus, we have shown that starting from a system verifying property p and after measuring its first qubit along z , the most precise proposition describing the system is $p \vee [\sigma_{z,1}] p$. This result can be generalized to other qubits, and one has:

$$[m_z(i)] p \dashv\vdash p \vee [\sigma_{z,i}] p \quad (16)$$

It should be noted that the measurement need not be restricted to the z -direction of a qubit. Actually, any hermitian operator o which has ± 1 as eigenvalues and is formalizable in our logic can be used to define a measurement operation, which interpretation for a proposition p would then be equivalent to that of $p \vee [o] p$.

4.2 Example: A teleportation circuit, continued

Now that we have introduced measurements in our formalism, we can finish the study of the previous example, by expressing the relations between properties at points 2 and 3. Consider for instance the way proposition $x_3 \vee z_1$ is transformed during a measurement of qubit 1 along z :

$$\begin{aligned} [m_z(1)] (x_3 \vee z_1) &\dashv\vdash (x_3 \vee z_1) \vee [\sigma_{z,1}] (x_3 \vee z_1) \\ &\dashv\vdash (x_3 \vee z_1) \vee ([\sigma_{z,1}] x_3 \vee [\sigma_{z,1}] z_1) \\ &\dashv\vdash (x_3 \vee z_1) \vee (x_3 \vee z_1) \\ &\dashv\vdash (x_3 \vee z_1) \end{aligned} \quad (17)$$

From this, we deduce $x_3^2 \vee z_1^2 \dashv\vdash x_3^3 \vee z_1^3$, and similarly, one has $z_3^2 \vee z_2^2 \dashv\vdash z_3^3 \vee z_2^3$, so that the measurement process does not affect our program in the sense that regarding properties, their succession is the same as if one had a simple wire instead. As a consequence, the expected relations between the first qubit at step 0 and the third qubit at step 4 still hold despite the measurement:

$$z_3^4 \dashv\vdash z_1^0 \quad x_3^4 \dashv\vdash x_1^0 \quad (18)$$

4.3 Measurements and partial representations

Thanks to its simple logical characterization, it is possible to express interesting properties about connective $[m_z(i)]$. A first remark that can be done is that

performing a measurement on the system acts for propositions as an approximation operation, so that the result is less informative than the starting argument. In other words, the interpretation of the result contains the interpretation of the initial proposition:

$$p \Vdash [m_z(i)]p \quad \text{or equivalently} \quad \llbracket p \rrbracket \subseteq \llbracket [m_z(i)]p \rrbracket \quad (19)$$

In some situations, no information is lost (for instance, $[m_z(1)]z_1 \dashv\vdash z_1$) whereas it might also happen that every information is lost, leading to \top as a result: $[m_z(1)]x_1 \dashv\vdash x_1 \vee \neg x_1 \dashv\vdash \top$. This illustrates the irreversibility of the measurement process.

Moreover, relation \Vdash can be seen as a partial order, making operation $[m_z(i)]$ monotonous and idempotent, that is $[m_z(i)][m_z(i)]p$ and $[m_z(i)]p$ are equivalent with regards to $\dashv\vdash$. These three properties form the definition of *upper closure operators*, which are a general formalization of the notion of approximation. This suggests to envision propositions about the system as partial descriptions of its state. From this point of view, measurements correspond to loss of information and unitary operation to transformation of information (with neither loss nor addition).

Addition of information can also be formalized using conjunctions. This situation arises for instance after measurements, when one takes into account the result of the measurement. Starting from a proposition p , the resulting proposition then becomes either $[m_z(i)]p \wedge z_i$ or $[m_z(i)]p \wedge \neg z_i$. And since a system cannot verify the absurd proposition \perp , this type of construction provides some informations about the possibility of a given outcome, since for instance if $[m_z(i)]p \wedge z_i \dashv\vdash \perp$, then the outcome corresponding to z_i can not occur. A important example for this is when starting from a proposition p such that $p \Vdash z_i$ (which can be interpreted as “one knows that z_i holds”), one has $[m_z(i)]p \Vdash z_i$ (by monotony of $[m_z(i)]$ and the fact that $z_i \dashv\vdash [m_z(i)]z_i$) so that $[m_z(i)]p \wedge \neg z_i \Vdash \perp$, meaning that outcome $\neg z_i$ is not possible.

This discussion shows that it is rather natural to consider knowledge about a quantum system from a partial description point of view, and that it is possible to describe the behaviour of usual operations in terms of knowledge.

5 Conclusion

In this article, we have shown how the basic quantum logic formalism can be extended into a dynamic quantum logic by the addition of several unary connectives which do all correspond to an action that can be performed of a quantum system. This provides a method for the logical study of quantum programs.

A few comments can be done about this approach. First, it is purely non-statistical, so that for measurements in particular, no information is provided about the probability of a particular outcome. This problem could be studied by, for instance, adding probability measures on the different subspaces or equivalently on properties.

Moreover, this approach suffers from the use of orthomodular quantum logic as underlying logic. This logic is extremely uneasy to manipulate, due to the fact that the distributivity of disjunction over conjunction and vice versa do not hold. A weaker property, called orthomodularity, holds but does not permit efficient formula manipulations. As a result, during a computation, the size of propositions tend to grow exponentially. A solution to this problem is suggested by the fact that, as developed in section 4.3, a interesting approach is to view properties as partial descriptions. In that case, a convenient logic is provided by intuitionistic logic, a non-classical logic which main specificity is that the excluded middle principle ($\varphi \vee \neg\varphi$) does not hold. The advantage would be the obtention of a distributive and decidable logic for representing and studying quantum programs. This is the type of approach that we have started to investigate in Ref. [15].

References

- [1] Charles H. Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres, and William K. Wootters. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Physical Review Letters*, 70(13):1895–1899, 1993.
- [2] Adriano Barenco, Charles H. Bennett, Richard Cleve, David P. DiVincenzo, Norman H. Margolus, Peter W. Shor, Tycho Sleator, John A. Smolin, and Harald Weinfurter. Elementary gates for quantum computation. *Physical Review Letters A*, 52(5):3457–3467, 1995.
- [3] Gilles Brassard, Samuel Braunstein, and Richard Cleve. Teleportation as a quantum computation, 1998.
- [4] Garrett Birkhoff and John von Neumann. The logic of quantum mechanics. *Annals of Mathematics*, 37(4):823 – 843, 1936.
- [5] Isaac L. Chuang and Michael A. Nielsen. *Quantum Computation and Quantum Information*. Cambridge, 2000.
- [6] Maria Luisa Dalla Chiara and Roberto Giuntini. Quantum logic. In D. Gabbay and F. Guenther, editors, *Handbook of Philosophical Logic*, volume III. Kluwer, 2001.
- [7] David P. DiVincenzo. Quantum gates and circuits. *Proc. R. Soc. London A*, 454:261 – 276, 1998.
- [8] Albert Einstein, Boris Podolsky, and Nathan Rosen. Can quantum-mechanical description of physical reality be considered complete? *Physical Review*, 47:777–780, 1935.
- [9] R.I.G. Hughes. *The Structure and Interpretation of Quantum Mechanics*. Harvard University Press, 1989.

- [10] Gudrun Kalmbach. *Orthomodular Lattices*. Academic Press, London, 1983.
- [11] George Mackey. *The Mathematical Foundations of Quantum Mechanics*. Benjamin, 1957.
- [12] Constantin Piron. *Foundations of Quantum Physics*. Benjamin, 1976.
- [13] Pavel Pták and Sylvia Pulmannová. *Orthomodular Structures as Quantum Logics*. Kluwer, 1991.
- [14] Karl Svozil. *Quantum Logic*. Springer, 1998.
- [15] Olivier Brunet. *Representation Systems and Orthomodular Posets*. Submitted to *International Journal of Theoretical Physics*, 2003.