A Qualitative Modal Representation of Quantum Register Transformations

Andrea Masini   Luca Viganò   Margherita Zorzi

Department of Computer Science

University of Verona, Italy

{andrea.masini | luca.vigano | margherita.zorzi}@univr.it

Abstract

We introduce two modal natural deduction systems that are suitable to represent and reason about transformations of quantum registers in an abstract, qualitative, way. Quantum registers represent quantum systems, and can be viewed as the structure of quantum data for quantum operations. Our systems provide a modal framework for reasoning about operations on quantum registers (unitary transformations and measurements) in terms of possible worlds (as abstractions of quantum registers) and accessibility relations between these worlds. We give a Kripke–style semantics that formally describes quantum register transformations, and prove the soundness and completeness of our systems with respect to this semantics.

1. Introduction

Quantum computing defines an alternative computational paradigm, based on a quantum model [4] rather than a classical one. The basic units of the quantum model are the *quantum bits*, or *qubits* for short (mathematically, normalized vectors of the Hilbert Space $\mathbb{C}^2$). Qubits represent informational units and can assume both classical values 0 and 1, and all their superpositional values.

A *quantum register* is a generalization of the qubit: a generic quantum register is the representation of a quantum state of n qubits (mathematically, it is a normalized vector of the Hilbert space $\mathbb{C}^{2^n}$). In this paper, we are not interested in the structure of quantum registers, but rather in the way quantum registers are transformed. Hence, we will abstract away from the internals of quantum registers and represent them in a generic way in order to describe how operations transform a register into another one.

It is possible to modify a quantum register in two ways: by applying a unitary transformation or by measuring. Unitary transformations (corresponding to the so-called unitary operators of the Hilbert space) model the internal evolution of a quantum system, whereas measurements correspond to the results of the interaction between a quantum system and an observer. The outcome of an observation can be either the reduction to a quantum state or the reduction to a classical (non quantum) state. In particular, in this paper, we say that a quantum register w is *classical* iff w is idempotent with respect to measurement, i.e. each measurement of w has w as outcome. We call a measurement *total* when the outcome of the measurement is a classical register.

We propose to model measurement and unitary transformations by means of suitable modal operators. More specifically, the main contribution of this paper is the formalization of a modal natural deduction system [12, 14] in order to represent (in an abstract, qualitative, way) the fundamental operations on quantum registers: unitary transformations and total measurements. We call this system MSQR. We also formalize a variant of this system, called MSpQR, to represent the case of generic (not necessarily total) measurements.

It is important to observe that our logical systems are not a quantum logic. Since 1936 [5], various logics have been investigated as a means to formalize reasoning about propositions taking into account the principles of quantum theory, e.g. [6, 7]. In general, it is possible to view quantum logic as a logical axiomatization of quantum theory, which provides an adequate foundation for a theory of reversible quantum processes, e.g. [1, 2, 3, 10].

Our work moves from quite a different point of view: we do not aim to propose a general logical formalization of quantum theory, rather we describe how it is possible to use modal logic to reason in a simple way about quantum register transformations. Informally, in our proposal, a modal world represents (an abstraction of) a quantum register. The discrete temporal evolution of a quantum register is controlled and determined by a sequence of unitary transformations and measurements that can change the description of a quantum state into other descriptions. So, the evolution of a quantum register can be viewed as a graph, where the nodes are the (abstract) quantum registers and the arrows represent quantum transformations. The arrows give us the so-called accessibility relations of Kripke mod-

els and two nodes linked by an arrow represent two related quantum states: the target node is obtained from the source node by means of the operation specified in the decoration of the arrow.

Modal logic, as a logic of possible worlds, is thus a natural way to represent this description of a quantum system: the worlds model the quantum registers and the relations of accessibility between worlds model the dinamical behavior of the system, as a consequence of the application of measurements and unitary transformations. To emphasize this semantic view of modal logic, we give our deduction system in the style of *labelled deduction* [8, 13, 15], a framework for giving uniform presentations of different non-classical logics. The intuition behind labelled deduction is that the labelling (sometimes also called prefixing, annotating or subscripting) allows one to explicitly encode in the syntax additional information, of a semantic or proof-theoretical nature, that is otherwise implicit in the logic one wants to capture. Most notably, in the case of modal logic, this additional information comes from the underlying Kripke semantics: the labelled formula $x{:}A$ intuitively means that A holds at the world denoted by the label x within the underlying Kripke structure (i.e. model), and labels also allow one to specify at the syntactic level how the different worlds are related in the Kripke structures (e.g. the formula xRy specifies that the world denoted by y is accessible from that denoted by x).

We proceed as follows. In Section 2, we define the labelled modal natural deduction system MSQR, which contains two modal operators suitable to represent and reason about unitary transformations and total measurements of quantum registers. In Section 3, we give a possible worlds semantics that formally describes these quantum register transformations, and prove the soundness and completeness of MSQR with respect to this semantics. In Section 4, we formalize MSpQR, a variant of MSQR that provides a modal system representing all the possible (thus not necessarily total) measurements. We conclude in Section 5 with a brief summary and a discussion of future work. Full proofs of the technical results are given in [9].

2 The deduction system MSQR

Our labelled modal natural deduction system MSQR, which formally represents unitary transformations and total measurements of quantum registers, comprises of rules that derive formulas of two kinds: modal formulas and relational formulas. We thus define a modal language and a relational language.

The alphabet of the *relational language* consists of:

- the binary symbols U and M,

- a denumerable set $x_0, x_1, \ldots$ of *labels*.

Metavariables x, y, z, possibly annotated with subscripts and superscripts, range over the set of labels. For brevity, we will sometimes speak of a "world" x meaning that the label x stands for a world $\mathscr{I}(x)$, where $\mathscr{I}$ is an interpretation function mapping labels into worlds as formalized in Definition 2 below.

The set of *relational formulas* (*r–formulas*) is given by expressions of the form $x\mathsf{U}y$ and $x\mathsf{M}y$.

The alphabet of the *modal language* consists of:

- a denumerable set $r, r_0, r_1, \ldots$ of *propositional symbols*,

- the standard *propositional connectives* $\bot$ and $\supset$,

- the unary *modal operators* $\square$ and $\blacksquare$.

The set of *modal formulas* (*m–formulas*) is the least set that contains $\bot$ and the propositional symbols, and is closed under the propositional connectives and the modal operators. Metavariables A, B, C, possibly indexed, range over modal formulas. Other connectives can be defined in the usual manner, e.g. $\neg A \equiv A \supset \bot$, $A \wedge B \equiv \neg(A \supset \neg B)$, $A \leftrightarrow B \equiv (A \supset B) \wedge (B \supset A)$, $\Diamond A \equiv \neg\square\neg A$, $\blacklozenge A \equiv \neg\blacksquare\neg A$, etc.

Let us give, in a rather informal way, the intuitive meaning of the modal operators of our language:

- $\square A$ means: A is true after the application of any unitary transformation.

- $\blacksquare A$ means: A is true in each quantum register obtained by a total measurement.

A *labelled formula* (*l–formula*) is an expression $x{:}A$, where x is a label and A is an m–formula. A *formula* is either an r–formula or an l–formula. The metavariable α, possibly indexed, ranges over formulas. We write $\alpha(x)$ to denote that the label x occurs in the formula α, so that $\alpha(y/x)$ denotes the substitution of the label y for all occurences of x in α.

Figure 1 shows the rules of MSQR, where the notion of *discharged/open assumption* is standard [12, 14], e.g. the formula $[x{:}A]$ is discharged in the rule $\supset I$:

Propositional rules: The rules $\supset I$, $\supset E$ and RAA are just the labelled version of the standard ([12, 14]) natural deduction rules for implication introduction and elimination and for *reductio ad absurdum*, where we do not enforce Prawitz's side condition that $A \neq \bot$.[1] The "mixed" rule $\bot E$ allows us to derive a generic formula α whenever we have obtained a contradiction $\bot$ at a world x.

---

[1] See [15] for a detailed discussion on the rule RAA, which in particular explains how, in order to maintain the duality of modal operators like $\square$ and $\Diamond$, the rule must allow one to derive $x{:}A$ from a contradiction $\bot$ at a possibly different world y, and thereby discharge the assumption $x{:}\neg A$.

$$\frac{\begin{array}{c}[x{:}A]\\ \vdots\\ x{:}B\end{array}}{x{:}A \supset B}\ \supset I \qquad \frac{x{:}A \supset B \quad x{:}B}{x{:}B}\ \supset E \qquad \frac{\begin{array}{c}[x{:}\neg A]\\ \vdots\\ y{:}\bot\end{array}}{x{:}A}\ RAA \qquad \frac{x{:}\bot}{\alpha}\ \bot E \qquad \frac{\begin{array}{c}[xRy]\\ \vdots\\ y{:}A\end{array}}{x{:}\bigstar A}\ \bigstar I^{*} \qquad \frac{x{:}\bigstar A \quad xRy}{y{:}A}\ \bigstar E$$

$$\frac{}{x\mathsf{U}x}\ \mathsf{U}\mathit{refl} \qquad \frac{x\mathsf{U}y}{y\mathsf{U}x}\ \mathsf{U}\mathit{symm} \qquad \frac{x\mathsf{U}y \quad y\mathsf{U}z}{x\mathsf{U}z}\ \mathsf{U}\mathit{trans} \qquad \frac{x\mathsf{M}y}{x\mathsf{U}y}\ \mathsf{U}I \qquad \frac{\begin{array}{c}[x\mathsf{M}y]\\ \vdots\\ \alpha\end{array}}{\alpha}\ \mathsf{M}\mathit{ser}^{*} \qquad \frac{x\mathsf{M}y}{y\mathsf{M}y}\ \mathsf{M}\mathit{srefl}$$

$$\frac{\alpha(x) \quad x\mathsf{M}x \quad x\mathsf{M}y}{\alpha(y/x)}\ \mathsf{M}\mathit{sub1} \qquad \frac{\alpha(y) \quad x\mathsf{M}x \quad x\mathsf{M}y}{\alpha(x/y)}\ \mathsf{M}\mathit{sub2}$$

In $\bigstar I$, y is fresh: it is different from x and does not occur in any assumption on which $y{:}A$ depends other than xRy.
In $\mathsf{M}ser$, y is fresh: it is different from x and does not occur in α nor in any assumption on which α depends other than $x\mathsf{M}y$.

Figure 1. The rules of MSQR

Modal rules: We give the rules for a generic modal operator $\bigstar$, with a corresponding generic accessibility relation R, since all the modal operators share the structure of these basic introduction/elimination rules; this holds because, for instance, we express $x{:}\Box A$ as the metalevel implication $x\mathsf{U}y \Longrightarrow y{:}A$ for an arbitrary y accessible from x. In particular:

- if $\bigstar$ is $\Box$ then R is U,
- if $\bigstar$ is $\blacksquare$ then R is M.

Other rules:

- In order to axiomatize $\Box$, we add rules $\mathsf{U}\mathit{refl}$, $\mathsf{U}\mathit{symm}$, and $\mathsf{U}\mathit{trans}$, formalizing that U is an equivalence relation.
- In order to axiomatize $\blacksquare$, we add rules formalizing the following properties:
  - If $x\mathsf{M}y$ then there is specific unitary transformation (depending on x and y) that generates y from x: rule $\mathsf{U}I$.
  - The total measurement process is serial: rule $\mathsf{M}ser$ says that if from the assumption $x\mathsf{M}y$ we can derive α for a *fresh* y (i.e. y is different from x and does not occur in α nor in any assumption on which α depends other than $x\mathsf{M}y$), then we can discharge the assumption (since there always is some y such that $x\mathsf{M}y$) and conclude α.
  - The total measurement process is shift-reflexive: rule $\mathsf{M}srefl$.
  - Invariance with respect to classical worlds: rules $\mathsf{M}\mathit{sub1}$ and $\mathsf{M}\mathit{sub2}$ say that, if $x\mathsf{M}x$

and $x\mathsf{M}y$, then y must be equal to x and so we can substitute the one for the other in any formula α.

Definition 1 (Derivations and proofs). *A derivation of a formula α from a set of formulas Γ in MSQR is a tree formed using the rules in MSQR, ending with α and depending only on a finite subset of Γ; we then write $\Gamma \vdash \alpha$. A derivation of α in MSQR depending on the empty set, $\vdash \alpha$, is a* proof *of α in MSQR and we then say that α is a theorem of MSQR.*

For instance, the following labelled formula schemata are all provable in MSQR (where, in parentheses, we give the intuitive meaning of each formula in terms of quantum register transformations):

1. $x{:}\Box A \supset A$
   (the identity transformation is unitary).

2. $x{:}A \supset \Box\Diamond A$
   (each unitary transformation is invertible).

3. $x{:}\Box A \supset \Box\Box A$
   (unitary transformations are composable).

4. $x{:}\blacksquare A \supset \blacklozenge A$
   (it is always possible to perform a total measurement of a quantum register).

5. $x{:}\blacksquare(A \leftrightarrow \blacksquare A)$
   (it is always possible to perform a total measurement with a complete reduction of a quantum register to a classical one).

6. $x{:}\blacksquare A \supset \blacksquare\blacksquare A$

   (total measurements are composable).

As concrete examples, Figure 2 contains the proofs of the formulas 5 and 6, where, for simplicity, here and in the following (cf. Figure 5), we employ the rules for equivalence ($\leftrightarrow I$) and for negation ($\neg I$ and $\neg E$), which are derived from the propositional rules as is standard. For instance,

$$\dfrac{\begin{array}{c}[x{:}A]^1\\ \vdots\\ y{:}\bot\end{array}}{x{:}\neg A}\ \neg I^1 \qquad \text{abbreviates} \qquad \dfrac{\dfrac{\begin{array}{c}[x{:}A]^1\\ \vdots\\ y{:}\bot\end{array}}{x{:}\bot}\ \bot E\ (\text{or } RAA)}{x{:}A \supset \bot}\ \supset I^1$$

We can similarly derive rules about r–formulas. For instance, we can derive a rule for the transitivity of M as shown at the top of the proof of the formula 6 in Figure 2:

$$\dfrac{x\mathsf{M}y \quad y\mathsf{M}z}{x\mathsf{M}z}\ \mathsf{M}trans$$

abbreviates

$$\dfrac{y\mathsf{M}z \quad \dfrac{\dfrac{y\mathsf{M}z}{z\mathsf{M}z}\ \mathsf{M}srefl \quad x\mathsf{M}y}{x\mathsf{M}z}\ \mathsf{M}sub1}{}$$

3. A semantics for unitary transformations and total measurements

We give a semantics that formally describes unitary transformations and total measurements of quantum registers, and then prove that MSQR is sound and complete with respect to this semantics. Together with the corresponding result for generic measurements in Section 4, this means that our modal systems indeed provide a representation of quantum registers and operations on them, which was the main goal of the paper.

Definition 2 (Frames, models, structures). *A frame is a tuple $\mathscr{F} = \langle W, U, M \rangle$, where:*

- *W is a non-empty set of worlds (representing abstractly the quantum registers);*

- *$U \subseteq W \times W$ is an equivalence relation (vUw means that w is obtained by applying a unitary transformation to v; U is an equivalence relation since identity is a unitary transformation, each unitary transformation must be invertible, and unitary transformations are composable);*

- *$M \subseteq W \times W$ (vMw means that w is obtained by means of a total measurement of v);*

with the following properties:

- (i) *$\forall v, w.\ vMw \Longrightarrow vUw$*
- (ii) *$\forall v.\ \exists w.\ vMw$*
- (iii) *$\forall v, w.\ vMw \Longrightarrow wMw$*
- (iv) *$\forall v, w.\ vMv \ \&\ vMw \Longrightarrow v = w$*

(i) *means that although it is not true that measurement is a unitary transformation, locally for each v, if vMw then there is a particular unitary transformation, depending on v and w, that generates w from v; the vice versa cannot hold, since in quantum theory measurements cannot be used to obtain the unitary evolution of a quantum system.* (ii) *means that each quantum register is totally measurable.* (iii) *and* (iv) *together mean that after a total measurement we obtain a classical world. Figure 3 shows properties* (ii), (iii) *and* (iv), *respectively, as well as the combination of* (iii) *and* (iv).[2]

A model *is a pair $\mathscr{M} = \langle \mathscr{F}, V \rangle$, where $\mathscr{F}$ is a frame and $V : W \to 2^{Prop}$ is an interpretation function mapping worlds into sets of formulas.*

A structure *is a pair $\mathscr{S} = \langle \mathscr{M}, \mathscr{I} \rangle$, where $\mathscr{M}$ is a model and $\mathscr{I} : Var \to W$ is an interpretation function mapping variables (labels) into worlds in W, and mapping a relation symbol $R \in \{\mathsf{U}, \mathsf{M}\}$ into the corresponding frame relation $\mathscr{I}(R) \in \{U, M\}$. We extend $\mathscr{I}$ to formulas and sets of formulas in the obvious way: $\mathscr{I}(x{:}A) = \mathscr{I}(x){:}A$, $\mathscr{I}(xRy) = \mathscr{I}(x)\mathscr{I}(R)\mathscr{I}(y)$, and $\mathscr{I}(\{\alpha_1, \ldots, \alpha_n\}) = \{\mathscr{I}(\alpha_1), \ldots, \mathscr{I}(\alpha_n)\}$.*

Given this semantics, we can define what it means for formulas to be true, and then prove the soundness and completeness of MSQR.

Definition 3 (Truth). Truth *for an m–formula in a model $\mathscr{M} = \langle W, U, M, V \rangle$ is the smallest relation $\vDash$ satisfying:*

$$\begin{array}{lll}
\mathscr{M}, w \vDash r & iff & r \in V(w)\\
\mathscr{M}, w \vDash A \supset B & iff & \mathscr{M}, w \vDash A \Longrightarrow \mathscr{M}, w \vDash B\\
\mathscr{M}, w \vDash \Box A & iff & \forall w'.\ wUw' \Longrightarrow \mathscr{M}, w' \vDash A\\
\mathscr{M}, w \vDash \blacksquare A & iff & \forall w'.\ wMw' \Longrightarrow \mathscr{M}, w' \vDash A
\end{array}$$

Thus, for an m–formula A, we write $\mathscr{M} \vDash A$ iff $\mathscr{M}, w \vDash A$ for all w.

Truth *for a formula α in a structure $\mathscr{S} = \langle \mathscr{M}, \mathscr{I} \rangle$ is then the smallest relation $\vDash$ satisfying:*

$$\begin{array}{lll}
\mathscr{M}, \mathscr{I} \vDash x\mathsf{M}y & iff & \mathscr{I}(x)M\mathscr{I}(y)\\
\mathscr{M}, \mathscr{I} \vDash x\mathsf{U}y & iff & \mathscr{I}(x)U\mathscr{I}(y)\\
\mathscr{M}, \mathscr{I} \vDash x{:}A & iff & \mathscr{M}, \mathscr{I}(x) \vDash A
\end{array}$$

We will omit $\mathscr{M}$ when it is not relevant, and we will denote $\mathscr{I} \vDash x{:}A$ also by $\vDash \mathscr{I}(x){:}A$ or even $\vDash w{:}A$ for $\mathscr{I}(x) = w$.

---

[2]Note that while (iv) says that v is idempotent with respect to M, a unitary transformation U could still be applied to v (and hence the dotted arrow decorated with a "?" for U).

$$\frac{\dfrac{[y{:}A]^2 \quad \dfrac{\dfrac{[x\mathsf{M}y]^1}{y\mathsf{M}y}\,\mathsf{M}srefl \quad [y\mathsf{M}z]^3}{z{:}A}\,\mathsf{M}sub1}{\dfrac{y{:}\blacksquare A}{y{:}A \supset \blacksquare A}\supset I^2}\,\blacksquare I^3 \qquad \dfrac{[y{:}\blacksquare A]^4 \quad \dfrac{[x\mathsf{M}y]^1}{y\mathsf{M}y}\,\mathsf{M}srefl}{\dfrac{y{:}A}{y{:}\blacksquare A \supset A}\supset I^4}\,\mathsf{M}sub1}{\dfrac{y{:}A \leftrightarrow \blacksquare A}{x{:}\blacksquare(A \leftrightarrow \blacksquare A)}\,\blacksquare I^1}\leftrightarrow I$$

$$\frac{[x{:}\blacksquare A]^1 \quad \dfrac{[y\mathsf{M}z]^3 \quad \dfrac{\dfrac{[y\mathsf{M}z]^3}{z\mathsf{M}z}\,\mathsf{M}srefl \quad [x\mathsf{M}y]^2}{x\mathsf{M}z}\,\mathsf{M}sub1}{\;}}{\dfrac{\dfrac{\dfrac{z{:}A}{y{:}\blacksquare A}\,\blacksquare I^3}{x{:}\blacksquare\blacksquare A}\,\blacksquare I^2}{x{:}\blacksquare A \supset \blacksquare\blacksquare A}\supset I^1}\,\blacksquare E$$

Figure 2. Examples of proofs in MSQR

$v \xrightarrow{\;M\;} w$ (ii) $\qquad$ $v \xrightarrow{\;M\;} w \circlearrowleft M$ (iii) $\qquad$ $\circlearrowleft M \; v \xrightarrow{\;M\;}\!\!\!\!/ \;\; U\overset{?}{\dashrightarrow}$ (iv) $\qquad$ $v \xrightarrow{\;M\;} w \circlearrowleft M,\; w \xrightarrow{M}\!\!\!\!/ \;\; U\overset{?}{\dashrightarrow}$ (iii) and (iv)
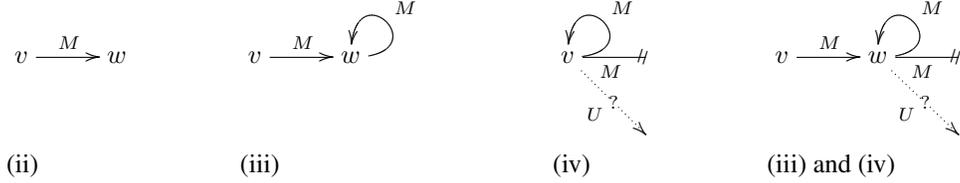
Figure 3. Some properties of the relation M

By extension, $\mathscr{M}, \mathscr{I} \vDash \Gamma$ *iff* $\mathscr{M}, \mathscr{I} \vDash \alpha$ *for all* α *in the set of formulas* Γ. *Thus, for a set of formulas* Γ *and a formula* α,

$$\begin{aligned}\Gamma \vDash \alpha \quad &\text{iff} \quad \forall \mathscr{M}, \mathscr{I}.\; \mathscr{M} \vDash \mathscr{I}(\Gamma) \implies \mathscr{M} \vDash \mathscr{I}(\alpha) \\ &\text{iff} \quad \forall \mathscr{M}, \mathscr{I}.\; \mathscr{M}, \mathscr{I} \vDash \Gamma \implies \mathscr{M}, \mathscr{I} \vDash \alpha\end{aligned}$$

By adapting standard proofs (see, e.g., [8, 12, 13, 14, 15] and the proofs in [9]), we have:

Theorem 1 (Soundness and completeness of MSQR). $\Gamma \vdash \alpha$ *iff* $\Gamma \vDash \alpha$.

4. Generic measurements

In quantum computing, not all measurements are required to be total: think, for example, of the case of observing only the first qubit of a quantum register. To this end, in this section, we formalize MSpQR, a variant of MSQR that provides a modal system representing all the possible (thus not necessarily total) measurements. We obtain MSpQR from MSQR by means of the following changes:

- The alphabet of the modal language contains the unary modal operator $\boxdot$ instead of $\blacksquare$, with corresponding $\diamondsuit$, where $\boxdot A$ intuitively means that A is true in each quantum register obtained by a measurement.

- The set of relational formulas contains expressions of the form $x\mathsf{P}y$ instead of $x\mathsf{M}y$.

- The rules of MSpQR are given in Figure 4. In particular, $\bigstar$ is either $\square$ (as before) or $\boxdot$, for which then R is P, and whose properties are formalized by the following additional rules:

  - If $x\mathsf{P}y$ then there is a specific unitary transformation (depending on x and y) that generates y from x: rule $\mathsf{P}U I$.

  - The measurement process is transitive: rule $\mathsf{P}trans$.

  - There are (always reachable) classical worlds: $class$ says that y is a classical world reachable from world x by a measurement.

  - Invariance with respect to classical worlds for measurement: rules $\mathsf{P}sub1$ and $\mathsf{P}sub2$.

Derivations and proofs in MSpQR are defined as for MSQR. For instance, in addition to the formulas for

$\supset I$, $\supset E$, RAA, $\perp E$, $\bigstar I^*$, $\bigstar E$, $\mathsf{U}refl$, $\mathsf{U}symm$, $\mathsf{U}trans$,

$$\frac{x\mathsf{P}y}{x\mathsf{U}y}\ \mathsf{PU}I \qquad \frac{x\mathsf{P}y \quad y\mathsf{P}z}{x\mathsf{P}z}\ \mathsf{P}trans \qquad \frac{\begin{array}{c}[x\mathsf{P}y]\ [y\mathsf{P}y]\\ \vdots\\ \alpha\end{array}}{\alpha}\ class^* \qquad \frac{\alpha(x) \quad x\mathsf{P}x \quad x\mathsf{P}y}{\alpha(y/x)}\ \mathsf{P}sub1 \qquad \frac{\alpha(y) \quad x\mathsf{P}x \quad x\mathsf{P}y}{\alpha(x/y)}\ \mathsf{P}sub2$$

In $\bigstar I$, y is fresh: it is different from x and does not occur in any assumption on which $y{:}A$ depends other than xRy.
In $class$, y is fresh: it is different from x and does not occur in α nor in any assumption on which α depends other than $x\mathsf{P}y$ and $y\mathsf{P}y$.

Figure 4. The rules of MSpQR

$$\frac{\dfrac{[x{:}\boxdot\neg(A\supset\boxdot A)]^2 \quad [x\mathsf{P}y]^1}{y{:}\neg(A\supset\boxdot A)}\ \boxdot E \qquad \dfrac{\dfrac{\dfrac{[y{:}A]^3 \quad [y\mathsf{P}y]^1 \quad [y\mathsf{P}z]^4}{z{:}A}\ \mathsf{P}sub1}{y{:}\boxdot A}\ \boxdot I^4}{y{:}A\supset\boxdot A}\ \supset I^3}{\dfrac{\dfrac{y{:}\perp}{x{:}\neg\boxdot\neg(A\supset\boxdot A)}\ \neg I^2}{x{:}\neg\boxdot\neg(A\supset\boxdot A)}\ class^1}\ \neg E$$

Figure 5. An example proof in MSpQR

$\square$ already listed for MSQR, the following labelled formula schemata are all provable in MSpQR (as shown, e.g., for formula 3 in Figure 5):

1. $x{:}\boxdot A\supset\Diamond A$
   (it is always possible to perform a measurement of a quantum register).
2. $x{:}\boxdot A\supset\boxdot\boxdot A$
   (measurements are composable).
3. $x{:}\Diamond(A\supset\boxdot A)$, i.e. $x{:}\neg\boxdot\neg(A\supset\boxdot A)$
   (it is always possible to perform a measurement with a complete reduction of a quantum register to a classical one).

The semantics is also obtained by simple changes with respect to the definitions of Section 3. A *frame* is a tuple $\mathscr{F}=\langle W,U,P\rangle$, where $P\subseteq W\times W$ and vPw means that w is obtained by means of a measurement of v, with the following properties:

(i) $\forall v,w.\ vPw\Longrightarrow vUw$
   (as for (i) in Section 3).
(ii) $\forall v,w',w''.\ vPw'\ \&\ w'Pw''\Longrightarrow vPw''$
   (measurements are composable).
(iii) $\forall v.\ \exists w.\ vPw\ \&\ wPw$
   (each quantum register v can be reduced to a classical one w by means of a measurement).

(iv) $\forall v,w.\ vPv\ \&\ vPw\Longrightarrow v=w$
   (each measurement of a classical register v has v as outcome).

Models and *structures* are defined as before, with $\mathscr{I}(\mathsf{P})=P$, while the *truth* relation now comprises the clauses

$$\begin{array}{lll}\mathscr{M},w\vDash\boxdot A & \text{iff} & \forall w'.\ wPw'\Longrightarrow\mathscr{M},w'\vDash A\\ \mathscr{M},\mathscr{I}\vDash x\mathsf{P}y & \text{iff} & \mathscr{I}(x)P\mathscr{I}(y)\end{array}$$

Finally, MSpQR is also sound and complete.

Theorem 2 (Soundness and completeness of MSpQR)**.** $\Gamma\vdash\alpha$ *iff* $\Gamma\vDash\alpha$.

5. Conclusions and future work

We have shown that our modal natural deduction systems MSQR and MSpQR provide suitable representations of quantum register transformations. As future work, we plan to investigate the proof theory of our systems (e.g. normalization, subformula property, (un)decidability), in view of a possible mechanization of reasoning in MSQR and MSpQR (e.g. encoding them into a logical framework [11]). We are also working at extending our approach to represent and reason about further quantum notions, such as entanglement.

References

[1] S. Abramsky and R. Duncan. A categorical quantum logic. *Math. Structures Comput. Sci.*, 16(3):469–489, 2006.

[2] A. Baltag and S. Smets. The logic of quantum programs. In *Proceedings of the 2nd International Workshop on Quantum Programming Languages QPL*, 2004.

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

[4] J.-L. Basdevant and J. Dalibard. *Quantum mechanics*. Springer-Verlag, 2005.

[5] G. Birkhoff and J. von Neumann. The logic of quantum mechanics. *Ann. of Math. (2)*, 37(4):823–843, 1936.

[6] M. L. Dalla Chiara. Quantum logic and physical modalities. *J. Philos. Logic*, 6(4):391–404, 1977.

[7] M. L. Dalla Chiara. Quantum logic. In D. Gabbay and F. Guenthner, editors, *Handbook of Philosophical Logic: Volume III: Alternatives to Classical Logic*, pages 427–469. Reidel, 1986.

[8] D. M. Gabbay. *Labelled Deductive Systems*, volume 1. Clarendon Press, 1996.

[9] A. Masini, L. Viganò, and M. Zorzi. A Qualitative Modal Representation of Quantum Register Transformations (Extended Version). arXiv:0802.4057v1: `http://arxiv.org/abs/0802.4057v1`, 2008.

[10] P. Mittelstaedt. The modal logic of quantum logic. *J. Philos. Logic*, 8(4):479–504, 1979.

[11] F. Pfenning. Logical frameworks. In A. Robinson and A. Voronkov, editors, *Handbook of Automated Reasoning*, chapter 17, pages 1063–1147. Elsevier Science and MIT Press, 2001.

[12] D. Prawitz. *Natural deduction, a proof-theoretical study*. Almqvist and Wiksell, 1965.

[13] A. Simpson. *The proof theory and semantics of intuitionistic modal logic*. PhD thesis, University of Edinburgh, UK, 1993.

[14] A. S. Troelstra and H. Schwichtenberg. *Basic proof theory*. Cambridge University Press, 1996.

[15] L. Viganò. *Labelled Non-Classical Logics*. Kluwer Academic Publishers, 2000.