Available online at www.sciencedirect.com
ScienceDirect
Electronic Notes in Theoretical Computer Science
ELSEVIER
Electronic Notes in Theoretical Computer Science 192 (2008) 71–83
www.elsevier.com/locate/entcs

A Hierarchy of Quantum Semantics

Simon Perdrix[1]

Oxford University Computing Laboratory

Abstract

Several domains [1,4,12,16] can be used to define the semantics of quantum programs. Among them Abramsky [1] has introduced a semantics based on probabilistic power domains, whereas the one by Selinger [16] associates with every program a completely positive map. In this paper, we mainly introduce a semantical domain based on admissible transformations, i.e. multisets of linear operators. In order to establish a comparison with existing domains, we introduce a simple quantum imperative language (QIL), equipped with three different denotational semantics, called pure, observable, and admissible respectively. The pure semantics is a natural extension of probabilistic (classical) semantics and is similar to the semantics proposed by Abramsky [1]. The observable semantics, à la Selinger [16], associates with any program a superoperator over density matrices. Finally, we introduce an admissible semantics which associates with any program an admissible transformation. These semantics are not equivalent, but exact abstraction [7] or interpretation relations are established between them, leading to a hierarchy of quantum semantics.

Keywords: Quantum programming semantics, admissable transformation, QIL

1 Introduction

Which formalism is adapted to the representation of quantum states and quantum evolutions ? It turns out that at least two formalisms can be used for representing quantum states: pure states (i.e vectors in a Hilbert space) and mixed states (i.e. density matrices). For the representation of quantum evolutions, at least three candidates exist: superoperators [2] acting on density matrices, probabilistic functions acting on pure states, and admissible transformations [3].

In the context of quantum programming, several semantic domains based on the above formalisms have been designed: the domain of superoperators [16], the domain of probabilistic functions acting on pure states [1], and a new quantum semantic domain based on admissible transformations, which is introduced in this paper.

[1] Email: simon.perdrix@comlab.ox.ac.uk

[2] Trace decreasing, completely positive maps.

[3] Multisets of linear operators satisfying a completeness condition, see section 2.

doi:10.1016/j.entcs.2008.10.028

In order to compare these three domains, a simple quantum programming language QIL is introduced, together with three denotational semantics. These three semantics are not equivalent, however exact abstraction or interpretation relations are established between them, leading to a hierarchy of quantum semantics.

The domain of admissible transformations is the most concrete domains, and the domain of superoperators is the most abstract. Notice that an even more abstract domain have been introduced in [14] in order to realise an analysis of entanglement evolution based on abstract interpretation. Finally, the main differences and specific properties of these three non equivalent domains are discussed.

This work is related to several works consisting in establishing hierarchies of 'classical' semantics, for instance [8]. In the case of quantum semantics, a connection between the domain of pure states and the one of density matrices have been established by Selinger in a categorical framework [17], by means of a CPM-construction.

2 Quantum Computing Basics

The basic carrier of information in quantum computing is a 2-level quantum system (*qubit*), or more generally a register of n qubits. The state of a n-qubit register is a normalized vector of a Hilbert space $\mathbb{C}^{2^n}$. So, for a given basis A, a general state $|\varphi\rangle \in \mathbb{C}^{|A|}$ can be written as:

$$\sum_{x\in A} \alpha_x |x\rangle,$$

with $\sum_{x\in A} |\alpha_x|^2 = 1$. Vectors, inner and outer products are expressed in the notation introduced by Dirac. Vectors are denoted $|\varphi\rangle$; the inner product of two vectors $|\varphi\rangle$, $|\psi\rangle$ is denoted by $\langle\varphi|\psi\rangle$. If $|\varphi\rangle = \sum_{x\in A} \alpha_x|x\rangle$ and $|\psi\rangle = \sum_{x\in A} \beta_x|x\rangle$, then $\langle\varphi|\psi\rangle = \sum_{x\in A} \alpha_x^*\beta_x$ (where α^* stands for the complex conjugate). The left hand side $\langle\varphi|$ of the inner product is a *bra-vector*, and the right hand side $|\psi\rangle$ is a *ket-vector*. A bra-vector is defined as the adjoint of the corresponding ket-vector: if $|\varphi\rangle = \sum_{x\in A} \alpha_x|x\rangle$, then $\langle\varphi| = |\varphi\rangle^\dagger = \sum_{x\in A} \alpha_x^*\langle x|$. The bra-ket notation can also be used to describe outer products: $|\varphi\rangle\langle\psi|$ is a linear operator such that $(|\varphi\rangle\langle\psi|)|\epsilon\rangle = \langle\psi|\epsilon\rangle\,|\varphi\rangle$. The state of a register composed of 2 sub-systems in state $|\varphi\rangle \in \mathbb{C}^{|A|}$ and $|\psi\rangle \in \mathbb{C}^{|B|}$ respectively, is the normalized vector $|\varphi\rangle \otimes |\psi\rangle \in \mathbb{C}^{|A|} \otimes \mathbb{C}^{|B|} \cong \mathbb{C}^{|A|\times|B|}$, where $\otimes$ is the tensor product. For any $x \in A, y \in B$, $|x, y\rangle$ denotes $|x\rangle \otimes |y\rangle$.

An isolated system evolves according to a unitary transformation [4] $U \in \mathbf{L}(\mathbb{C}^{|A|})$, transforming a state $|\varphi\rangle \in \mathbb{C}^{|A|}$ into $U|\varphi\rangle$. A projective measurement is a probabilistic evolution described by a set $\{P_i\}_{i\in B}$ of orthogonal projectors [5] which is complete [6]. A measurement produces a classical outcome $i \in B$ and transforms the state $|\varphi\rangle \in \mathbb{C}^{|A|}$ into $\frac{P_i|\varphi\rangle}{\sqrt{\langle\varphi|P_i|\varphi\rangle}}$ with probability $\langle\varphi|P_i|\varphi\rangle$.

The composition of two projective measurements is not necessary a projective measurement. However, any quantum evolution, can be described in a more general

[4] U is unitary if and only if $U^\dagger U = I$.

[5] $\forall i, j \in B, P_iP_j = \delta_{i,j}P_i$ where δ is the Kronecker delta.

[6] $\sum_{i\in B} P_i = I$

framework the *admissible transformations*, which is closed under composition. An admissible transformation is a countable multiset $\{M_i\}_{i\in A}$ of linear operators which satisfy the completeness condition $\sum_{i\in A} M_i^\dagger M_i = I$. An admissible transformation composed of a unique operator U is an isometry since $U^\dagger U = I$, moreover if $UU^\dagger = I$ then U is a unitary transformation. An admissible transformation composed of only projectors is a projective measurement.

A probability distribution of quantum states of $\mathbb{C}^{|A|}$ can be represented by a density matrix $\rho \in D(\mathbb{C}^{|A|}) \subseteq \mathbf{L}(\mathbb{C}^{|A|})$, i.e. a self adjoint [7] positive-semidefinite [8] complex matrix of trace [9] less than one. A unitary transformation U transforms ρ into $U\rho U^\dagger$ and a projective measurement $\{P_i\}_{i\in B}$ transforms ρ into $\sum_{i\in B} P_i\rho P_i$. Such a projective measurement produces the classical outcome $i \in B$ with probability $Tr(P_i\rho P_i) = Tr(P_i\rho)$.

Any n-qubit unitary transformation U can be approximated within an arbitrary accuracy [10] by composing unitary transformations from the universal set of unitary transformations $\{H, T, CNot\}$, composed of two 1-qubit and one 2-qubit unitary transformations. Notice that there exist several universal families of unitary transformations in the literature [13].

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}, CNot = \begin{pmatrix} 1\,0\,0\,0 \\ 0\,1\,0\,0 \\ 0\,0\,0\,1 \\ 0\,0\,1\,0 \end{pmatrix}$$

3 A Quantum Programming Language

Several quantum programming languages have been introduced recently, for a complete overview see [9] and [15]. In this paper, we introduce a *Quantum Imperative Language* (QIL), the syntax is similar to the one of the language introduced by Abramsky [1], except for quantum measurements which are treated implicitly in QIL, like in QML [2].

A QIL program is a pair (Q, C), where $Q = \{q_0, \ldots, q_n\}$ is a finite set of symbols

[7] M is self adjoint (or Hermitian) if and only if $M^\dagger = M$

[8] M is positive-semidefinite if all the eignenvalues of M are non-negative.

[9] The trace of M ($tr(M)$) is the sum of the diagonal elements of M

[10] U is approximated by V within $\epsilon > 0$ if $||U - V|| < \epsilon$

representing a finite memory of qubits, and C is a command defined as follows:

$$
\begin{aligned}
C ::= \ & \mathsf{skip} \\
| \ & C_1; C_2 \\
| \ & \mathsf{if}\ q\ \mathsf{then}\ C_1\ \mathsf{else}\ C_2 \\
| \ & \mathsf{while}\ q\ \mathsf{do}\ C \\
| \ & \mathsf{H}(q) \\
| \ & \mathsf{T}(q) \\
| \ & \mathsf{CNot}(q,q)
\end{aligned}
$$

Notice that QIL is not limited to a unitary fragment, since according to the semantics of the language, quantum measurements are encoded into the conditional structures of the language: when a qubit q is used as a condition, q is first measured, then the classical outcome of the measurement plays the role of the boolean evaluation of the condition.

Example 3.1

ex1 : while q do $H(q)$

ex2 : while q do $H(q)$;
H(q) ;
if q then
skip
else
skip

ex3 : while q do $H(q)$;
H(q) ;
if q then
H(q)
else
H(q)

3.1 A Probabilistic Semantics

According to the postulates of quantum mechanics, the state of a quantum system is a normalised vector in a Hilbert space, and its evolution is probabilistic. Thus, a natural way to define a quantum semantics consists in a quantum version of a classical probabilistic semantics, based for instance on probabilistic power domains [10].

For a given qubit q, let $|\mathsf{tt}_q\rangle$ (*true*) and $|\mathsf{ff}_q\rangle$ (*false*) be the two basis states of q. The state of q is then a normalised vector of the Hilbert space $\mathcal{H}_q = \{\alpha|\mathsf{tt}_q\rangle + \beta|\mathsf{ff}_q\rangle \mid \alpha, \beta \in \mathbb{C}\} \cong \mathbb{C}^2$. For a given finite set Q of qubits, the state of Q is a normalised vector of $\mathcal{H}_Q = \bigotimes_{q\in Q} \mathcal{H}_q \cong \mathbb{C}^{2^{|Q|}}$, i.e. an element of the unit sphere $\mathcal{H}_Q^{\mathbf{1}} = \{|\varphi\rangle \in \mathcal{H}_Q \mid |||\varphi\rangle|| = 1\}$ of $\mathcal{H}_Q$.

Since the evolution of a quantum system is probabilistic, the state of memory is not, in general, a pure state but a probabilistic distribution of pure

states. Such a probabilistic distribution is represented by a valuation $\nu : \mathcal{H}_Q^{\mathbf{1}} \to \overline{\mathbb{R}^+}$ which associates with every pure state its probability. Let $\mathcal{V}_Q = \{\nu \in V(\mathcal{H}_Q^{\mathbf{1}}) \mid \mathrm{supp}(\nu)$ is discrete and $\sum_{|\varphi\rangle \in \mathrm{supp}(\nu)} \nu(|\varphi\rangle) \leq 1\}$ be the set of discrete valuations.

Theorem 3.2 ([10]) *$(\mathcal{V}_Q, \sqsubseteq)$ is a complete partial order with $\mathbf{0}$ (i.e. the valuation with an empty support) as least element, where $\nu \sqsubseteq \mu$ if and only if $\forall |\varphi\rangle \in \mathrm{supp}(\nu), \nu(|\varphi\rangle) \leq \mu(|\varphi\rangle)$.*

Since any unitary transformation U is reversible, with $U^{-1} = U^\dagger$, the probability that a quantum system is in state $|\varphi\rangle$ after the application of U is equal to the probability that the system was in state $U^\dagger|\varphi\rangle$ before the application of U. Thus, U transforms a discrete valuation ν into $\lambda|\varphi\rangle.\nu(U^\dagger|\varphi\rangle)$ [11].

A projective measurement $\{P_i\}_{i\in B}$, which is not reversible, produces the classical outcome $i \in B$ and transforms a state $|\varphi\rangle$ into $\frac{P_i|\varphi\rangle}{\sqrt{\langle\varphi|P_i|\varphi\rangle}}$ with probability $\langle\varphi|P_i|\varphi\rangle$. Thus, $\{P_i\}_{i\in B}$ produces the classical outcome $i \in B$, and transforms a discrete valuation ν into $\sum_{|\varphi\rangle\in\mathrm{supp}(\nu)} \nu(|\varphi\rangle)\langle\varphi|P_i|\varphi\rangle\delta_{\frac{P_i|\varphi\rangle}{\sqrt{\langle\varphi|P_i|\varphi\rangle}}}$, where $\delta_x(y) = \begin{cases} 1 & \text{if } x = y \\ 0 & \text{otherwise} \end{cases}$.

Definition 3.3 (Pure semantics) For any finite set Q, for any command C, let $[\![C]\!]_{\mathrm{p}} : \mathcal{V}_Q \to \mathcal{V}_Q$ be defined as follows:

$$
\begin{aligned}
[\![\mathsf{skip}]\!]_{\mathrm{p}} &= I \\
[\![C_1; C_2]\!]_{\mathrm{p}} &= [\![C_2]\!]_{\mathrm{p}} \circ [\![C_1]\!]_{\mathrm{p}} \\
[\![\mathsf{T}(q)]\!]_{\mathrm{p}} &= \lambda\nu.\lambda|\varphi\rangle.\nu(T_q^\dagger|\varphi\rangle) \\
[\![\mathsf{H}(q)]\!]_{\mathrm{p}} &= \lambda\nu.\lambda|\varphi\rangle.\nu(H_q^\dagger|\varphi\rangle) \\
[\![\mathsf{CNot}(q_1,q_2)]\!]_{\mathrm{p}} &= \lambda\nu.\lambda|\varphi\rangle.\nu(CNot_{q_1,q_2}^\dagger|\varphi\rangle) \\
[\![\text{if } q \text{ then } C_1 \text{ else } C_2\ ]\!]_{\mathrm{p}} &= \lambda\nu.[\![C_1]\!]_{\mathrm{p}}\left(\sum_{|\varphi\rangle\in\mathrm{supp}(\nu)} |\langle\varphi|\mathsf{tt}_q\rangle|^2\nu(|\varphi\rangle)\delta_{\frac{(|\mathsf{tt}_q\rangle\langle\mathsf{tt}_q|)|\varphi\rangle}{|\langle\varphi|\mathsf{tt}_q\rangle|}}\right) \\
&\quad + [\![C_2]\!]_{\mathrm{p}}\left(\sum_{|\varphi\rangle\in\mathrm{supp}(\nu)} |\langle\varphi|\mathsf{ff}_q\rangle|^2\nu(|\varphi\rangle)\delta_{\frac{(|\mathsf{ff}_q\rangle\langle\mathsf{ff}_q|)|\varphi\rangle}{|\langle\varphi|\mathsf{ff}_q\rangle|}}\right) \\
[\![\text{while } q \text{ do } C\ ]\!]_{\mathrm{p}} &= \mathsf{lfp}\Big(\lambda f.\lambda\nu.f \circ [\![C]\!]_{\mathrm{p}}\left(\sum_{|\varphi\rangle\in\mathrm{supp}(\nu)} |\langle\varphi|\mathsf{tt}_q\rangle|^2\nu(|\varphi\rangle)\delta_{\frac{(|\mathsf{tt}_q\rangle\langle\mathsf{tt}_q|)|\varphi\rangle}{|\langle\varphi|\mathsf{tt}_q\rangle|}}\right) \\
&\quad + \sum_{|\varphi\rangle\in\mathrm{supp}(\nu)} |\langle\varphi|\mathsf{ff}_q\rangle|^2\nu(|\varphi\rangle)\delta_{\frac{(|\mathsf{ff}_q\rangle\langle\mathsf{ff}_q|)|\varphi\rangle}{|\langle\varphi|\mathsf{ff}_q\rangle|}}\Big)
\end{aligned}
$$

where M_q means that M is applied on qubit q.

One can prove by induction on the command C that $[\![C]\!]_{\mathrm{p}} : \mathcal{V}_Q \to \mathcal{V}_Q$ is conti-

[11] In this paper, functions are represented using λ-notation: $\lambda x.y$ is a function which associates y with x, i.e. the function $x \mapsto y$.

nuous [12] and that the least fixed point used for defining the semantics of the while command exists, thanks to the fixed point theorem [13].

Example 3.4 $[\![\mathsf{ex1}]\!]_{\mathrm{p}} = \lambda\nu.\delta_{|\mathsf{ff}\rangle}$, $[\![\mathsf{ex2}]\!]_{\mathrm{p}} = \lambda\nu.(\frac{1}{2}\delta_{|\mathsf{tt}\rangle} + \frac{1}{2}\delta_{|\mathsf{ff}\rangle})$, and $[\![\mathsf{ex3}]\!]_{\mathrm{p}} = \lambda\nu.(\frac{1}{2}\delta_{(|\mathsf{tt}\rangle+|\mathsf{ff}\rangle)/2} + \frac{1}{2}\delta_{(|\mathsf{tt}\rangle-|\mathsf{ff}\rangle)/2)})$

3.2 Observable Semantics

The pure semantics introduced in the previous section does not take into account quantum properties like indistinguishability. For instance, according to the postulates of quantum mechanics, a qubit in state $|\mathsf{tt}\rangle$ or $|\mathsf{ff}\rangle$ with equal probability cannot be distinguished from a qubit in state $\frac{1}{\sqrt{2}}(|\mathsf{tt}\rangle + |\mathsf{ff}\rangle)$ or $\frac{1}{\sqrt{2}}(|\mathsf{tt}\rangle - |\mathsf{ff}\rangle)$ with equal probability. In order to take into account this phenomenon, one can use the formalism of density matrices (see section 2) for representing quantum states.

For a finite set of variables $Q = \{q_0, \ldots, q_n\}$, let $\mathcal{D}_Q = D(\mathcal{H}_Q)$ be the set of density matrices on Q.

Theorem 3.5 ([16]) *The poset $(\mathcal{D}_Q, \sqsubseteq)$ is a complete partial order with $\mathbf{0}$ as least element, where $M \sqsubseteq N$ if $N - M$ is positive (Löwner partial order).*

Definition 3.6 (Observable semantics) For any finite set Q, for any command C, let $[\![C]\!]_{\mathrm{o}} : \mathcal{D}_Q \to \mathcal{D}_Q$ be defined as follows:

$$
\begin{aligned}
[\![\mathsf{skip}]\!]_{\mathrm{o}} &= I \\
[\![C_1; C_2]\!]_{\mathrm{o}} &= [\![C_2]\!]_{\mathrm{o}} \circ [\![C_1]\!]_{\mathrm{o}} \\
[\![\mathsf{H}(q)]\!]_{\mathrm{o}} &= \lambda\rho.H_q\rho H_q^\dagger \\
[\![\mathsf{T}(q)]\!]_{\mathrm{o}} &= \lambda\rho.T_q\rho T_q^\dagger \\
[\![\mathsf{CNot}(q_1,q_2)]\!]_{\mathrm{o}} &= \lambda\rho.CNot_{q_1,q_2}\rho CNot_{q_1,q_2}^\dagger \\
[\![\mathsf{if}\ q\ \mathsf{then}\ C_1\ \mathsf{else}\ C_2\ ]\!]_{\mathrm{o}} &= \lambda\rho.\left([\![C_1]\!]_{\mathrm{o}}(P_q^{\mathsf{tt}}\rho P_q^{\mathsf{tt}}) + [\![C_2]\!]_{\mathrm{o}}(P_q^{\mathsf{ff}}\rho P_q^{\mathsf{ff}})\right) \\
[\![\mathsf{while}\ q\ \mathsf{do}\ C\ ]\!]_{\mathrm{o}} &= \mathsf{lfp}\left(\lambda f.\lambda\rho.\left(f \circ [\![C]\!]_{\mathrm{o}}(P_q^{\mathsf{tt}}\rho P_q^{\mathsf{tt}}) + P_q^{\mathsf{ff}}\rho P_q^{\mathsf{ff}}\right)\right) \\
&= \lambda\rho.\sum_{n\in\mathbb{N}}(F_{P^{\mathsf{ff}}} \circ ([\![C]\!]_{\mathrm{o}} \circ F_{P^{\mathsf{tt}}})^n(\rho))
\end{aligned}
$$

where $P^{\mathsf{tt}} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ and $P^{\mathsf{ff}} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$, $F_M = \lambda\rho.M\rho M^\dagger$.

Example 3.7 $[\![\mathsf{ex1}]\!]_{\mathrm{o}} = \lambda\rho.P^{\mathsf{ff}}$, $[\![\mathsf{ex2}]\!]_{\mathrm{o}} = \lambda\rho.\begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{pmatrix}$, and $[\![\mathsf{ex3}]\!]_{\mathrm{o}} = \lambda\rho.\begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{pmatrix}$

[12] A continuous function is monotonic and preserves least upper bounds.

[13] The fixed point theorem states that for a given complete partial order $(D, \leq)$ and a continuous function $f : D \to D$, f has a least fixed point $\mathsf{lfp}(f)$. Notice that here, the fixed point theorem is applied with the complete partial order $([\mathcal{V}_Q \to \mathcal{V}_Q], \sqsubseteq)$ of continuous functions where $\sqsubseteq$ is defined pointwise.

The observable semantics associates with any command C a map $[\![C]\!]_{\mathrm{o}}$ that is a superoperator [14], thus for any $\rho \in \mathcal{D}_Q, [\![C]\!]_{\mathrm{o}}(\rho) \in \mathcal{D}_Q$.

Observable and probabilistic semantics of QIL are not equivalent, as it is illustrated in example 3.4 and 3.7: $[\![\mathsf{ex2}]\!]_{\mathrm{o}} = [\![\mathsf{ex3}]\!]_{\mathrm{o}}$ whereas $[\![\mathsf{ex2}]\!]_{\mathrm{p}} \neq [\![\mathsf{ex3}]\!]_{\mathrm{p}}$. However, observable semantics is an exact abstraction [7] of the probabilistic semantics. Any probability distribution over quantum states ν can be abstracted into a density matrix $\rho = \alpha(\nu)$, where $\alpha : \mathcal{V}_Q \to \mathcal{D}_Q$ is defined as $\alpha = \lambda\nu. \sum_{|\varphi\rangle \in supp(\nu)} \nu(|\varphi\rangle)\, |\varphi\rangle\langle\varphi|$.

Lemma 3.8 $[\![.]\!]_{\mathrm{o}}$ *is an* α*-abstraction of* $[\![.]\!]_{\mathrm{p}}$*, i.e. for any command* C*,*

$$[\![C]\!]_{\mathrm{o}} \circ \alpha = \alpha \circ [\![C]\!]_{\mathrm{p}}$$

$$\begin{array}{ccc} \mathcal{D}_Q & \xrightarrow{[\![.]\!]_{\mathrm{o}}} & \mathcal{D}_Q \\ \alpha \uparrow & & \uparrow \alpha \\ \mathcal{V}_Q & \xrightarrow{[\![.]\!]_{\mathrm{p}}} & \mathcal{V}_Q \end{array}$$

Proof. (sketch) The proof is by induction on the command C. The proof is immediate for the commands skip, the composition and the unitary transformations H, T, and CNot. For the if case, the main two ingredients of the proof are:
– for any $\nu \in \mathcal{V}_Q$,

$$\alpha\left(\sum_{|\varphi\rangle \in \mathrm{supp}(\nu)} |\langle\varphi|\mathsf{tt}_q\rangle|^2 \nu(|\varphi\rangle)\delta_{\frac{(|\mathsf{tt}_q\rangle\langle\mathsf{tt}_q|)|\varphi\rangle}{|\langle\varphi|\mathsf{tt}_q\rangle|}}\right) = P^{\mathsf{tt}}\alpha(\nu)P^{\mathsf{tt}}$$

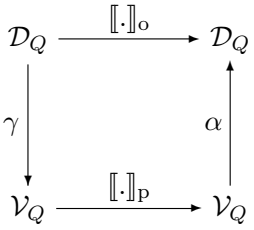
– α is linear: for any ν_1, ν_2, $\alpha(\nu_1 + \nu_2) = \alpha(\nu_1) + \alpha(\nu_2)$
For the while case, in order to preserve the least fixed point, the continuity of α is used. □

Lemma 3.8 establishes a connection between two domains used in quantum computation. Observable and pure semantics are not equivalent, however the observable semantics is an abstraction of the pure one. This abstraction carries the indistinguishability to the pure semantics: let C_1 and C_2 be two commands such that $[\![C_1]\!]_{\mathrm{p}} \neq [\![C_2]\!]_{\mathrm{p}}$ and $[\![C_1]\!]_{\mathrm{o}} = [\![C_2]\!]_{\mathrm{o}}$, then for any $\nu \in \mathcal{V}_Q$, $[\![C_1]\!]_{\mathrm{p}}(\nu)$ and $[\![C_1]\!]_{\mathrm{p}}(\nu)$ are indistinguishable. However, even if observable and pure semantics are not equivalent, none of them violate the postulates of quantum mechanics. Notice that the author have established a similar exact abstract connection for the semantics of the quantum calculus [11].

[14] F is a superoperator if $Tr(F(\rho)) \leq Tr(\rho)$, and $(I_k \otimes F)(\rho')$ is positive for any $k \geq 0$ and any ρ, ρ' positive, where $I_k : \mathbb{C}^k \to \mathbb{C}^k$ is the identity map.

Additionally to the abstraction function $\alpha : \mathcal{V}_Q \to \mathcal{D}_Q$, a concretisation function $\gamma : \mathcal{D}_Q \to \mathcal{V}_Q$ can be defined. The concretisation function is based on spectral decomposition of density matrices. For any $\rho \in \mathcal{D}_Q$, since ρ is self-adjoint, there exist an orthonormal basis $\{|\varphi_i\rangle\}_{i=0\ldots 2^{|Q|}-1}$ and λ_is such that $\rho = \sum_{i=0\ldots 2^{|Q|}-1} \lambda_i |\varphi_i\rangle\langle\varphi_i|$. Moreover, since ρ is positive, $\lambda_i \geq 0$ for any i. The function γ is such that $\mathrm{supp}(\gamma(\rho)) = \{|\varphi_i\rangle\}_{i\in 0\ldots 2^{|Q|}-1}$, and for any i, $\gamma(\rho)(|\varphi_i\rangle) = \lambda_i$. Notice that the orthonormal basis of eigenvectors is not unique, as a consequence, for any ρ, the support of $\gamma(\rho)$ is one among all the possible orthonormal basis of eigenvectors of ρ. Since $\alpha \circ \gamma = I$, a corollary of lemma 3.8 is that for any command,

$$[\![C]\!]_{\mathrm{o}} = \alpha \circ [\![C]\!]_{\mathrm{p}} \circ \gamma$$



3.3 Admissible semantics

According to the postulates of quantum mechanics, any quantum evolution can be described by an admissible transformation, i.e. a countable multiset of linear operators (see section 2). In this section, we introduce a denotational semantics associating with every program an admissible transformation.

Let $\mathcal{M}_Q$ be the set of all countable multisets $\{M_i\}_{i\in A}$ such that $\forall i \in A, M_i \in \mathbf{L}(\mathcal{H}_Q)$ and $\sum_{i\in A} M_i^\dagger M_i \sqsubseteq I$. Let $m_K(x)$ be the multiplicity of x in the multiset K, i.e. the number of occurrences of x in K. For any two multisets K and L, $K \subseteq L$ if for any x, $m_K(x) \leq m_L(x)$. The join $K \uplus L$ is such that for any x, $m_{K\uplus L}(x) = m_K(x)+m_L(x)$. Moreover, composition $\bullet$ of admissible transformations is defined as follows: for any $\{M_i\}_{i\in A}, \{M'_j\}_{j\in B} \in \mathcal{M}_Q$, $\{M_i\}_{i\in A} \bullet \{M'_j\}_{j\in B} = \{M_i M'_j\}_{(i,j)\in A\times B}$.

Theorem 3.9 *$(\mathcal{M}_Q, \subseteq)$ is a complete partial order with $\{0\}$ as least element.*

Proof. Let $F_0 \subseteq F_1 \ldots$ be an increasing sequence. Assume w.l.o.g that $F_i = \{M_j\}_{j\in I_i}$ where I_i is an interval of $\mathbb{N}$ such that $0 \in I_i$ and $I_i \subseteq I_{i+1}$. The increasing sequence $I_0 \subseteq I_1 \subseteq \ldots$ has a limit $J \subseteq \mathbb{N}$, thus the least upper bound of $F_0 \subseteq F_1 \ldots$ is $F = \{M_i\}_{i\in J}$. Moreover, $\sum_{i\in j} M_i^\dagger M_i = lim_{n\to\infty} \sum_{i\in I_n} M_i^\dagger M_i \sqsubseteq I$, so $F \in \mathcal{M}_Q$. □

Definition 3.10 (Admissible semantics) For any finite set Q, for any command C, let $[\![C]\!]_{\mathrm{p}} : \mathcal{M}_Q \to \mathcal{M}_Q$ be defined as follows:

$$\begin{aligned}
[\![\mathsf{skip}]\!]_{\mathrm{a}} &= \{I\} \\
[\![C_1; C_2]\!]_{\mathrm{a}} &= [\![C_2]\!]_{\mathrm{a}} \bullet [\![C_1]\!]_{\mathrm{a}} \\
[\![\mathsf{H}(q)]\!]_{\mathrm{a}} &= \{H_q\} \\
[\![\mathsf{T}(q)]\!]_{\mathrm{a}} &= \{T_q\} \\
[\![\mathsf{CNot}(q_1, q_2)]\!]_{\mathrm{a}} &= \{CNot_{q_1,q_2}\} \\
[\![\text{if } q \text{ then } C_1 \text{ else } C_2 \,]\!]_{\mathrm{a}} &= \left([\![C_1]\!]_{\mathrm{a}} \bullet \{P_q^{\mathsf{tt}}\}\right) \uplus \left([\![C_2]\!]_{\mathrm{a}} \bullet \{P_q^{\mathsf{ff}}\}\right) \\
[\![\text{while } q \text{ do } C \,]\!]_{\mathrm{a}} &= \biguplus_{k=0}^{\infty} \left(\{P_q^{\mathsf{ff}}\} \bullet ([\![C]\!]_{\mathrm{a}} \bullet \{P_q^{\mathsf{tt}}\})^n\right)
\end{aligned}$$

Example 3.11 Since for any $n > 1$, $(HP^{\mathsf{tt}})^n = \frac{1}{2^{n/2}} \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$,

$$[\![\mathsf{ex1}]\!]_{\mathrm{a}} = \{ \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \} \uplus \{ \begin{pmatrix} 0 & 0 \\ \frac{1}{2^{n/2}} & 0 \end{pmatrix} \}_{n>0}$$

$$[\![\mathsf{ex2}]\!]_{\mathrm{a}} = \{ \frac{1}{\sqrt{2}} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \frac{1}{\sqrt{2}} \begin{pmatrix} 0 & 0 \\ 0 & -1 \end{pmatrix} \} \uplus \{ \begin{pmatrix} \frac{1}{2^{(n+1)/2}} & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ \frac{-1}{2^{(n+1)/2}} & 0 \end{pmatrix} \}_{n>0}$$

$$[\![\mathsf{ex3}]\!]_{\mathrm{a}} = \{ \frac{1}{2} \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}, \frac{1}{2} \begin{pmatrix} 0 & -1 \\ 0 & 1 \end{pmatrix} \} \uplus \{ \begin{pmatrix} \frac{1}{2^{(n+2)/2}} & 0 \\ \frac{1}{2^{(n+2)/2}} & 0 \end{pmatrix}, \frac{1}{2} \begin{pmatrix} \frac{-1}{2^{(n+2)/2}} & 0 \\ \frac{1}{2^{(n+2)/2}} & 0 \end{pmatrix} \}_{n>0}$$

Admissible transformations and superoperators are related by the Krauss representation theorem [3]: for any superoperator F, there exists a set of linear operators $\{M_i\}_{i\in A}$ such that $F = \lambda\rho. \sum_{i\in A} M_i \rho M_i^\dagger$. Notice that this set of linear operators is not unique. Any admissible transformation can be seen as the representation of a superoperator. $\chi_{\mathrm{o}} : \mathcal{M}_Q \to (\mathcal{D}_Q \to \mathcal{D}_Q)$ is an interpretation function which associates with any admissible transformation $\{M_i\}_{i\in A}$ a superoperator $\chi_{\mathrm{o}}(\{M_i\}_{i\in A}) = \lambda\rho. \sum_{i\in A} M_i \rho M_i^\dagger$. The observable semantics is an interpretation of the admissible semantics:

Lemma 3.12 *For any command C, $[\![C]\!]_{\mathrm{o}} = \chi_{\mathrm{o}}([\![C]\!]_{\mathrm{a}})$.*

Proof. (sketch) The proof is by induction on the command C. The proof is immediate for the commands skip and the unitary transformations H, T, CNot. The composition is treated as follows, for any command C_1 and C_2, let $[\![C_1]\!]_{\mathrm{a}} = \{M_i\}_{i\in A}$ and $[\![C_2]\!]_{\mathrm{a}} = \{N_j\}_{j\in B}$. $\chi_{\mathrm{o}}([\![C1; C2]\!]_{\mathrm{a}}) = \chi_{\mathrm{o}}([\![C_2]\!]_{\mathrm{a}} \bullet [\![C_1]\!]_{\mathrm{a}}) = \chi_{\mathrm{o}}(\{N_j M_i\}_{(i,j)\in A\times B}) = \lambda\rho. N_j M_i \rho M_i^\dagger N_j^\dagger = [\![C_1; C_2]\!]_{\mathrm{o}}$. The if and while cases are based on the linearity of χ_{o} : $\chi_{\mathrm{o}}(K \uplus L) = \chi_{\mathrm{o}}(K) + \chi_{\mathrm{o}}(L)$. □

Moreover, admissible transformations can also be interpreted in terms of probabilistic evolutions via the function $\chi_{\mathrm{p}} : \mathcal{M}_Q \to (\mathcal{V}_Q \to \mathcal{V}_Q)$ which associates with

any admissible transformation $\{M_i\}_{i\in A}$ a probabilistic evolution $\chi_{\mathrm{p}}(\{M_i\}_{i\in A}) = \lambda\nu.\sum_{i\in A,|\varphi\rangle\in\mathrm{supp}(\nu)}\nu(|\varphi\rangle)\langle\varphi|M_i^\dagger M_i|\varphi\rangle\delta_{\frac{M_i|\varphi\rangle}{\sqrt{\langle\varphi|M_i^\dagger M_i|\varphi\rangle}}}$. The pure semantics is an interpretation of the admissible semantics:

Lemma 3.13 *For any command C, $[\![C]\!]_{\mathrm{p}} = \chi_{\mathrm{p}}([\![C]\!]_{\mathrm{a}})$.*

Proof. The proof, by induction on the command C, is based on the linearity of χ_{p} ($\chi_{\mathrm{p}}(K \uplus L) = \chi_{\mathrm{p}}(K) + \chi_{\mathrm{p}}(L)$), and its continuity which preserves least fixed points. □

Notice that lemma 3.12 can be seen as a consequence of lemmas 3.8 and 3.13: for any command C, $[\![C]\!]_{\mathrm{o}} = \alpha\circ[\![C]\!]_{\mathrm{p}}\circ\gamma$ and $[\![C]\!]_{\mathrm{p}} = \chi_{\mathrm{p}}([\![C]\!]_{\mathrm{a}})$, so $[\![C]\!]_{\mathrm{o}} = \alpha\circ\chi_{\mathrm{p}}([\![C]\!]_{\mathrm{a}})\circ\gamma$.

The admissible semantics associates with any program an admissible transformation. Since an admissible transformation is not a function but a multiset of linear operators, no connection based on abstraction function can be realised with the pure and observable semantics introduced in previous sections. However, interpretation functions, χ_{p} and χ_{o} transform the admissible semantics into the pure and the observable semantics, showing that the admissible semantics is a more concrete semantics. As admissible semantics is more concrete than pure semantics, the indistinguishability phenomenon is not taken into account as it is illustrated in example 3.11 since $[\![\mathsf{ex2}]\!]_{\mathrm{a}} \neq [\![\mathsf{ex3}]\!]_{\mathrm{a}}$. In order to illustrate the concreteness of the admissible semantics, one can notice in the definition of the semantics that the existence of while loop in a command C implies that the admissible semantics of C is an infinite multiset: each linear operator of the admissible transformation represents a computational path.

Exact abstraction and interpretations between the semantics established in lemmas 3.8, 3.12, and 3.13 lead to a semantical hierarchy:

Theorem 3.14 (Hierarchy of quantum semantics) *For any commands C_1, C_2,*

$$[\![C_1]\!]_{\mathrm{a}} = [\![C_2]\!]_{\mathrm{a}} \implies [\![C_1]\!]_{\mathrm{p}} = [\![C_2]\!]_{\mathrm{p}} \quad \textit{and} \quad [\![C_1]\!]_{\mathrm{p}} = [\![C_2]\!]_{\mathrm{p}} \implies [\![C_1]\!]_{\mathrm{o}} = [\![C_2]\!]_{\mathrm{o}}$$

4 Discussion and Perspectives

Three non equivalent semantics can be used for defining the semantics of a quantum program. One can wonder which one has to be used in which context. This question is discussed in this section. First, a natural extension of the language is considered: the parallel composition of programs.

4.1 Parallel composition

For given programs (Q_1, C_1) and (Q_2, C_2), such that $Q_1 \cap Q_2 = \emptyset$, a natural extension of the language consists in allowing the parallel composition of these two programs, leading to a program $(Q_1 \cup Q_2, C_1 \,|\, C_2)$.

Observable and admissible semantics can be extended as follows: $[\![C_1 \mid C_2]\!]_{\mathrm{o}} = [\![C_1]\!]_{\mathrm{o}} \otimes [\![C_2]\!]_{\mathrm{o}}$ and $[\![C_1 \mid C_2]\!]_{\mathrm{a}} = [\![C_1]\!]_{\mathrm{a}} \otimes [\![C_2]\!]_{\mathrm{a}}$, where the tensor product on multisets is defined as $\{M_i\}_{i\in A} \otimes \{N_j\}_{j\in B} = \{M_i \otimes N_j\}_{(i,j)\in A\times B}$.

The pure semantics cannot be easily extended to the parallel composition. One way to explain this difference between observable, admissible and pure semantics is that the Hilbert space structure is not explicitly represented in the pure semantics, avoiding a natural representation of the tensor product.

4.2 Indistinguishability of quantum evolutions

The introduction of density matrices is mainly motivated by the indistinguishability of some probability distributions over pure states (see section 3.2.) In order to decide which domain among the superoperators, the probabilistic functions and the admissible transformations is the most suitable for the representation of quantum evolution, the indistinguishability of quantum evolutions is a relevant question to address.

Indistinguishability of quantum evolutions can be derived from indistinguishability of quantum states. Since the indistinguishability of quantum states is captured by density matrices, indistinguishability of two evolutions f and g can be stated as $\forall \rho, f(\rho) = g(\rho)$ (i.e. $f = g$) if f and g are superoperators, or as $\chi_{\mathrm{o}}(f) = \chi_{\mathrm{o}}(g)$ if f and g are admissible transformations, or finally as $\alpha \circ f \circ \gamma = \alpha \circ g \circ \gamma$ if f and g are probabilistic functions. As a consequence, it turns out that the observable semantics is the best candidate to take into account such an indistinguishability of quantum evolutions.

However, additionally to the indistinguishability of the quantum states produced by quantum evolutions, one can also take into account the classical outcomes produced during the computation in order to distinguish two evolutions. For instance, consider the following two admissible transformations: $\mathcal{A}_1 = \{M_0\}$ and $\mathcal{A}_2 = \{N_0, N_1\}$, where $M_0 = I$ and $N_0 = N_1 = \frac{1}{\sqrt{2}} I$. One can prove that $\chi_{\mathrm{p}}(\mathcal{A}_1) = \chi_{\mathrm{p}}(\mathcal{A}_2)$ and $\chi_{\mathrm{o}}(\mathcal{A}_1) = \chi_{\mathrm{o}}(\mathcal{A}_2)$. However, for any input state, $\mathcal{A}_1$ produces always the same classical outcome 0, whereas $\mathcal{A}_2$ produces 0 with probability 1/2 and 1 with probability 1/2, making these two evolutions easily distinguishable.

As a consequence, the question of indistinguishability of quantum evolutions might be stated within a framework allowing hybrid memories, i.e. memories composed of a classical part and a quantum part such that the classical outcomes produced during the computation can be taken into account for distinguishing quantum evolutions.

4.3 Hybrid computation

In this paper, a purely quantum programming language has been introduced in the sense that the memory is entirely quantum. However, hybrid computation, where the memory is composed of a quantum part and a classical part, is a natural architecture to consider for a quantum computer. As a consequence, the ability to represent classical variables and classical evolutions is a relevant parameter for

comparing pure, observable and admissible semantics.

In the case of the pure semantics, the use of valuations makes the representation of classical data an easy task, since this formalism is largely used for classical probabilistic computations. Instead of valuations over $\mathcal{H}^Q$, one can use valuations over $E \times \mathcal{H}^Q$ where E is the state space of the classical variables.

One way to represent classical variables in the formalism of density matrices is to encode classical data as quantum basis states. The hybrid domain is then $\mathcal{D}^{E\times Q}$. This solution is used in [16], however such an encoding does not point out the proper properties of classical data like the ability of copying data [5,6].

The probabilistic interpretation of an admissible transformation $\{M_i\}_{i\in A}$ is such that A represents the possible classical outcomes, and if the outcome $i \in A$ occurs, then the quantum system evolves according to M_i. Thus, an admissible transformation is already a natural representation of the classical-quantum interactions. Hence, the extension of the admissible transformation formalism to classical-quantum evolutions is a promising perspective.

4.4 Lattices

Finally, the choice of the semantics can be based on some specific properties of the domain, for instance whether the domain is a lattice or not. For any finite set Q, $(\mathcal{V}_Q, \sqsubseteq, \sqcap, 0)$ is a lower semilattice, with $\nu_1 \sqcap \nu_2 = \lambda|\varphi\rangle.\mathsf{min}(\nu_1(|\varphi\rangle), \nu_2(|\varphi\rangle))$. $(\mathcal{M}_Q, \subseteq, \cap, 0)$ is a lower semilattice as well, with $m_{K\cap L} = \lambda x.\mathsf{min}(m_K(x), m_L(x))$. Notice that the previous domains can be turned into lattices by relaxing the condition $\sum_{|\varphi\rangle\in\mathrm{supp}(\nu)} \nu(|\varphi\rangle) \leq 1$ in the definition of $\mathcal{V}_Q$ (see in section 2.1) and the condition $\sum_{i\in A} M_i^\dagger M_i \sqsubseteq I$ in the definition of $\mathcal{M}_Q$ (see section 2.3).

The domain of density matrices is neither an upper nor a lower semilattice. It is proved in [16], that $(\mathcal{D}_Q, \sqsubseteq)$ is not an upper semilattice. Moreover, $(\mathcal{D}_Q, \sqsubseteq)$ is not a lower semilattice, since

$$\begin{pmatrix} 0.3 & 0 \\ 0 & 0 \end{pmatrix} \text{ and } \begin{pmatrix} 0 & 0 \\ 0 & 0.3 \end{pmatrix}$$

are two different maximal lower bounds of

$$\begin{pmatrix} 0.3 & 0 \\ 0 & 0.3 \end{pmatrix} \text{ and } \begin{pmatrix} 0.4 & 0.2 \\ 0.2 & 0.4 \end{pmatrix}$$

5 Conclusion

We have mainly proved that the semantics of a quantum program can be based on admissible transformations, i.e. multisets of linear operators. We have introduced a complete partial order over admissible transformations and defined an admissible semantics, based on admissible transformations, of a simple quantum imperative

language (QIL). In order to compare this new semantic domain with existing ones, two additional semantics based on probability distributions over pure states (pure semantics) and on density matrices (observable semantics) are defined. These three semantics are not equivalent and lead to a hierarchy where the admissible semantics is the most concrete one. The pure semantics, based on probabilistic power domain is more abstract, whereas the most abstract semantics is the one based on density matrices.

References

[1] S. Abramsky. A Cook's tour of a simple quantum programming language. *3rd International Symposium on Domain Theory, Xi'an, China*, May 2004.

[2] T. Altenkirch and J. Grattage. QML: Quantum data and control. Manuscript, 2005.

[3] M.-D. Choi. Completely positive linear maps on complex matrices. *Linear Algebra Appl.*, 10:285, 1975.

[4] B. Coecke and K. Martin. A partial order on classical and quantum states. Technical report, PRG-RR-02-07, 2002.

[5] B. Coecke, D. Pavlovic. Quantum measurements without sums In Mathematics of Quantum Computing and Technology, 2007.

[6] B. Coecke, E. O. Paquette, and S. Perdrix. Bases in diagramatic quantum protocols In the proceedings of the 24th conference on the Mathematical Foundations of Programming Semantics (MFPS), 2008.

[7] P. Cousot. Types as abstract interpretations. In *POPL*, pages 316–331, 1997.

[8] P. Cousot. Constructive Design of a Hierarchy of Semantics of a Transition System by Abstract Interpretation. Theoretical Computer Science, vol 277, 2002.

[9] S. J. Gay. Quantum programming languages: Survey and bibliography. *Mathematical Structures in Computer Science*, 16(4), 2006.

[10] C. Jones and G. D. Plotkin. A probabilistic powerdomain of evaluations. In *LICS*, pages 186–195, 1989.

[11] Ph. Jorrand and S. Perdrix. Towards a quantum calculus. In *To appear in Proceedings of the 4th International Workshop on Quantum Programming Languages, ENTCS*, 2006.

[12] E. Kashefi. Quantum domain theory — definitions and applications. In *Proceedings of the International Conference on Computability and Compexity in Analysis*, number 302 – 8/2003 in Fernuniversität Hagen Informatik Berichte, 2003.

[13] M. A. Nielsen and I. L. Chuang. *Quantum computation and quantum information*. Cambridge University Press, New York, NY, USA, 2000.

[14] S. Perdrix. *Quantum entanglement analysis based on abstract interpretation*. In *Proceedings of the 15th International Static Analysis Symposium (SAS'08)*, LNCS 5079, (preprint arXiv:0801.4230), 2008.

[15] P. Selinger. A brief survey of quantum programming languages. In *Proceedings of the 7th International Symposium on Functional and Logic Programming*, volume 2998 of *Lecture Notes in Computer Science*, pages 1–6. Springer, 2004.

[16] P. Selinger. Towards a quantum programming language. *Mathematical Structures in Computer Science*, 14(4):527–586, 2004.

[17] P. Selinger. Dagger compact closed categories and completely positive maps In Proceedings of the 3rd International Workshop on Quantum Programming Languages (QPL 2005), Chicago. ENTCS 170:139-163, 2007.