Exogenous Quantum Logic

P. Mateus and A. Sernadas
CLC, Department of Mathematics, IST

April 27, 2004

1 Context

Most of the work on quantum logic (since the seminal paper [4]) has continued to adopt the lattice of closed subspaces of a Hilbert space as the basis for its semantics [11, 8].

Here we take a quite different approach, what we call the exogenous approach. The key idea is to keep the models of the classical logic (say propositional logic) as they are, to produce models for the envisaged quantum logic as superpositions of classical models, and, finally, to design a suitable language for constraining such superpositions.

The exogenous approach is a variation of the possible worlds approach originally proposed by Kripke [14] for modal logic, and it is also akin to the society semantics introduced in [7] for many-valued logic and to the possible translations semantics proposed in [6] for paraconsistent logic. In fact, Kripke structures can be described as binary relations between classical models, the models in [7] are just collections of classical models, and the models in [6] are obtained using translation maps into the original logic(s). The possible worlds approach was also used in [19, 20] for probabilistic logic[1]: the models turn out to be probability spaces of classical models, as first recognized in [10].

The difference between the possible worlds approach and the exogenous approach is subtle but full of consequences. The exogenous approach is used in [16] to develop a probabilistic version of any given logic where, as in [10], each model is a probability space of the original models, but where the connectives are different from those of the logic being probabilized. As explained in Section 2, the global semantics of the new connectives arises naturally when using the new models.

Note that the endogenous approach to probabilistic logic is also useful and, actually, widely used. By endogenous approach we mean that we tinker with the classical models in order to make them suitable for a specific type of probabilistic reasoning. For instance, if we want a logic for reasoning about probabilistic transition systems (probabilistic automata) we can modify the Kripke models of dynamic logic by labelling the transition pairs (pairs of the accessibility relation) with probabilities [12, 15]. As another example of the endogenous approach, consider the probabilization of first-order logic obtained by enriching

[1]Later on, the relationship to epistemic logic was made clear in [3, 2].

the domain of individuals with a probability distribution [1], having in mind notions like almost everywhere.

Returning to quantum logic, the exogenous approach seems promising for several reasons: (i) it can be applied to any given logic[2]; (ii) it settles once and for all the issue of the nature of the quantum models (as superpositions of models from the original logic); and, finally, (iii) it also guides the design of the quantum language (that should provide the means to write assertions about both the original models and the quantum models). Furthermore, since quantum logic involves probabilistic reasoning (because of the stochastic nature of the results of observing quantum systems), the successful exogenous development of probabilistic logic in [16] reinforces this idea.

It is to be expected that the lattice approach to quantum logic will play a similar role to the one played by modal algebras in modal logic, by Heyting algebras in intuitionistic logic, by Boolean algebras in classical logic, etc. But, as in those cases, the algebraic approach is not the right source of inspiration for discovering the linguistic ingredients of the envisaged logic. For instance, modal algebras appeared much later than Kripke structures, well after the modal language was widely accepted.

In Section 2, we start by showing how to set up the exogenous probabilistic version of propositional logic. Afterwards, we continue the process, first, in Section 3, towards the exogenous quantum version of propositional logic (including the probabilistic one), and finally, in Section 4, towards a dynamic version of the latter (for reasoning also about changes in the quantum state of a system).

2 EPPL

Assume a fixed set $\{\mathbf{p}_k : k \in \mathbb{N}\}$ of propositional constants. Recall that a classical valuation is a map $v : \{\mathbf{p}_k : k \in \mathbb{N}\} \to \{0,1\}$. The exogenous approach to probabilistic logic suggests that we identify a probabilistic valuation with a probability space of classical valuations. A Nilsson[3] structure $\mathbf{V}$ is a tuple $\langle V, \mathcal{B}, \nu \rangle$ where: V is a nonempty set of classical valuations; $\mathcal{B}$ is a σ-algebra over V (that is, $\mathcal{B} \subseteq \wp V$ and $\mathcal{B}$ is closed under complements and countable unions) such that $\{v \in V : v \Vdash \mathbf{p}_k\} \in \mathcal{B}$ for each $k \in \mathbb{N}$; and ν is a map from $\mathcal{B}$ to $[0,1]$ such that $\nu(V) = 1$ and $\nu(\bigcup_{j \in \mathbb{N}} B_j) = \sum_{j \in \mathbb{N}} \nu(B_j)$ whenever $B_{j_1} \cap B_{j_2} = \emptyset$ for every $j_1 \neq j_2 \in \mathbb{N}$. In short, a Nilsson structure is a probability space where outcomes are classical valuations and the extent of every propositional constant is among the events.

This exogenous semantics for probabilistic reasoning suggests that we adopt the probabilistic language composed of formulae of the form[4]

$$\gamma := \omega_k \curlyvee \varphi \curlyvee (t \leq t) \curlyvee (\boxminus \gamma) \curlyvee (\gamma \sqsupset \gamma)$$

[2] Herein, we just address the problem of designing the quantum version of classical propositional logic, but it is feasible to repeat the process for any given logic fulfilling some minimal requirements as it was done in [16] for probabilistic logic.

[3] In recognition of the significance of [19] for the development of probabilistic logic.

[4] When defining languages, we use the abstract Backus-Naur notation [17], but adopting $\curlyvee$ instead of the traditional | in order to avoid confusions with the object language.

where φ is a classical formula of the form

$$\varphi := \xi_k \curlyvee \mathbf{p}_k \curlyvee (\neg\,\varphi) \curlyvee (\varphi \Rightarrow \varphi)$$

and t is a real term of the form

$$t := \theta_k \curlyvee r \curlyvee (\textstyle\int \varphi) \curlyvee (\textstyle\int \varphi \,|\, \varphi) \curlyvee (t + t) \curlyvee (t\, t)$$

where r is a computable real number. The ξ's, ω's and θ's are variables (to be used in rules) that can be the target of substitutions respecting the syntactic categories. An expression is said to be ground if it does not contain any such variable. As usual, other (classical and probabilistic) connectives can be used as abbreviations. Furthermore, we write $(t_1 = t_2)$ for $((t_1 \leq t_2) \sqcap (t_2 \leq t_1))$.

Clearly, for each ground classical formula φ, $[\varphi]_{\mathbf{V}} = \{v \in V : v \Vdash \varphi\} \in \mathcal{B}$. So, from the probabilistic point of view, it is worthwhile to look at classical formulae as describing events. The denotation of ground terms is inductively defined as follows:

- $[\![r]\!]_{\mathbf{V}} = r$;
- $[\![(\int \varphi)]\!]_{\mathbf{V}} = \nu([\varphi]_{\mathbf{V}})$;
- $[\![(\int \varphi_2 \,|\, \varphi_1)]\!]_{\mathbf{V}} = \begin{cases} \frac{\nu([\varphi_1]_{\mathbf{V}} \cap [\varphi_2]_{\mathbf{V}})}{\nu([\varphi_1]_{\mathbf{V}})} & \text{if } \nu([\varphi_1]_{\mathbf{V}}) \neq 0 \\ 1 & \text{otherwise} \end{cases}$;
- $[\![(t_1 + t_2)]\!]_{\mathbf{V}} = [\![t_1]\!]_{\mathbf{V}} + [\![t_2]\!]_{\mathbf{V}}$;
- $[\![(t_1 t_2)]\!]_{\mathbf{V}} = [\![t_1]\!]_{\mathbf{V}} \times [\![t_2]\!]_{\mathbf{V}}$.

According to the exogenous approach, the satisfaction of formulae by $\mathbf{V}$ and ground substitution ρ is as follows:

- $\mathbf{V}\rho \Vdash \omega_j$ iff $\mathbf{V}\rho \Vdash \omega_j\rho$;
- $\mathbf{V}\rho \Vdash \varphi$ iff $v \Vdash \varphi\rho$ for every $v \in V$;
- $\mathbf{V}\rho \Vdash (t_1 \leq t_2)$ iff $[\![t_1\rho]\!]_{\mathbf{V}} \leq [\![t_2\rho]\!]_{\mathbf{V}}$;
- $\mathbf{V}\rho \Vdash (\boxminus\,\gamma)$ iff $\mathbf{V}\rho \nVdash \gamma$;
- $\mathbf{V}\rho \Vdash (\gamma_1 \sqsupset \gamma_2)$ iff $\mathbf{V}\rho \nVdash \gamma_1$ or $\mathbf{V}\rho \Vdash \gamma_2$.

The global nature of satisfaction is a key ingredient of the exogenous approach (contrarily to the local nature of satisfaction within the possible worlds approach). The exogenous approach has the advantage of uncoupling the two layers: the probabilistic connectives are defined independently of the original logic. Note that the global probabilistic connectives are still classical but should not be confused with the connectives of the original logic. Indeed, consider the following probabilistic formulae where φ is a classical formula: (i) $(\varphi \vee (\neg\,\varphi))$; (ii) $(\varphi \sqcup (\boxminus\,\varphi))$; and (iii) $(\varphi \sqcup (\neg\,\varphi))$. Clearly, (i) and (ii) hold in every Nilsson structure for every ground substitution, while (iii) does not hold in general.

Observe also that the exogenous probabilization procedure applied above to classical propositional logic is generic in the sense that it can be applied to any given logic as explained in [16]. So, probabilization is akin to temporalization and other cases of parameterization of logics. The same comment applies to the procedure described in Section 3 for building quantum logic.

Finally, the notion of probabilistic entailment is introduced as follows: $\Gamma \vDash \delta$ iff, for every $\mathbf{V}$ and ground ρ, $\mathbf{V}\rho \Vdash \delta$ whenever $\mathbf{V}\rho \Vdash \gamma$ for each $\gamma \in \Gamma$. This entailment enjoys the properties that one would expect from classical and probabilistic reasoning, such as:

- $\vDash ((0 \leq (\int \varphi)) \sqcap ((\int \varphi) \leq 1))$;
- $\vDash ((\int(\neg \varphi)) = (1 - (\int \varphi)))$;
- $\vDash ((\int(\varphi_1 \vee \varphi_2)) = (((\int \varphi_1) + (\int \varphi_2)) - (\int(\varphi_1 \wedge \varphi_2))))$;
- $\varphi \vDash ((\int \varphi) = 1)$;
- $(\varphi_1 \Leftrightarrow \varphi_2) \vDash ((\int \varphi_1) = (\int \varphi_2))$;
- $(\varphi_1 \Rightarrow \varphi_2) \vDash ((\int \varphi_2 \,|\, \varphi_1) = 1)$.

A Hilbert calculus is proposed in [16] that is sound and weakly complete[5] with respect to the above semantics, with the following rules on probability:

PM	$\vdash ((\int \mathbf{t}) = 1)$;
FA	$\vdash (((\int(\neg(\xi_1 \wedge \xi_2))) = 1) \sqsupset ((\int(\xi_1 \vee \xi_2)) = ((\int \xi_1) + (\int \xi_2))))$;
CP	$\vdash (((\int \xi_2 \,|\, \xi_1)(\int \xi_1)) = (\int(\xi_1 \wedge \xi_2)))$;
UCP	$\vdash (((\int \xi_1) = 0) \sqsupset ((\int \xi_2 \,|\, \xi_1) = 1))$;
MON	$\vdash ((\xi_1 \Rightarrow \xi_2) \sqsupset ((\int \xi_1) \leq (\int \xi_2)))$;
MP	$\omega_1, (\omega_1 \sqsupset \omega_2) \vdash \omega_2$.

Observe that EPPL, the exogenous probabilistic propositional logic just described, allows us to work with both classical and probabilistic assertions. The former constrain the outcome space of the Nilsson structure and the latter constrain the probability measure. This feature was already present in the possible worlds probabilistic logics proposed in [10]. For a comparison between the two approaches see [16].

3 EQPL

Taking into account the postulates of quantum physics as stated for example in [18], the exogenous approach to quantum logic suggests that we should identify a quantum state (or quantum valuation) with a unit superposition of classical valuations. That is, the envisaged quantum logic should provide the means for

[5]Since we are using only finitary rules, strong completeness is out of question because probabilistic entailment (as defined herein) is not compact.

reasoning about a quantum system composed of a denumerable set of qubits (one for each propositional constant $\mathbf{p}_k$) and where the (classical projective) observation values are classical valuations. The basic idea is to find a suitable Hilbert space containing the envisaged superpositions of classical valuations. Given a nonempty set V of observable classical valuations, $\mathcal{H}(V)$ is the following inner product space over $\mathbb{C}$:

- each element is a map $|w\rangle : V \to \mathbb{C}$ such that:
  - $\text{supp}(|w\rangle) = \{v : |w\rangle(v) \neq 0\}$ is countable;
  - $\displaystyle\sum_{v \in \text{supp}(|w\rangle)} ||w\rangle(v)|^2 < \infty$.
- $|w_1\rangle + |w_2\rangle = \lambda v.\, |w_1\rangle(v) + |w_2\rangle(v)$.
- $\alpha|w\rangle = \lambda v.\, \alpha|w\rangle(v)$.
- $\langle w_1|w_2\rangle = \displaystyle\sum_{v \in V} |w_1\rangle(v)\overline{|w_2\rangle(v)}$.

As usual, the inner product induces the norm $|||w\rangle|| = \sqrt{\langle w|w\rangle}$ and, so, the distance $d(|w_1\rangle, |w_2\rangle) = |||w_1\rangle - |w_2\rangle||$. Since $\mathcal{H}(V)$ is complete for this distance, $\mathcal{H}(V)$ is a Hilbert space[6]. Clearly, $\{|v\rangle : v \in V\}$ is an orthonormal basis of $\mathcal{H}(V)$ where $|v\rangle(v) = 1$ and $|v\rangle(v') = 0$ for every $v' \neq v$.

A quantum structure $\mathbf{w}$ is a pair $\langle V, |w\rangle\rangle$ where: V is a nonempty set of classical valuations; and $|w\rangle \in \mathcal{H}(V)$ such that $|||w\rangle|| = 1$. This structure provides the means for reasoning about a quantum system composed of a denumerable set of qubits (one for each $\mathbf{p}_k$) such that by observing it we get a classical valuation in V. The current state of the system is the unit vector $|w\rangle$ (a unit superposition of the observable classical valuations). The stochastic result of observing the system at that quantum state is described by the Nilsson structure $\mathcal{N}(\mathbf{w}) = \langle V, \wp V, \nu_{|w\rangle}\rangle$ where, for each $U \subseteq V$, $\nu_{|w\rangle}(U) = \displaystyle\sum_{u \in U} |\langle u|w\rangle|^2$.

Given a set S of propositional constants (qubits), we denote by $V_{[S]}$ the set $\{v|_S : v \in V\}$ and by $V_{]S[}$ the set $\{v|_{S^c} : v \in V\}$. The Hilbert spaces $\mathcal{H}(V_{[S]})$ and $\mathcal{H}(V_{]S[})$ will be useful when asserting facts about a target set S of qubits. Clearly, $\mathcal{H}(\mathcal{V}) = \mathcal{H}(\mathcal{V}_{[S]}) \otimes \mathcal{H}(\mathcal{V}_{]S[})$ where $\mathcal{V}$ is the set of all classical valuations. But, $\mathcal{H}(V) \subseteq \mathcal{H}(V_{[S]}) \otimes \mathcal{H}(V_{]S[})$ where equality does not hold in general. When it does, we say that the quantum system is composed of two independent subsystems (one with the qubits in S and the other with rest of the qubits). Furthermore, given a unit $|w\rangle \in \mathcal{H}(V)$, if there are unit $|w'\rangle \in \mathcal{H}(V_{[S]})$ and unit $|w''\rangle \in \mathcal{H}(V_{]S[})$ such that $|w\rangle = |w'\rangle \otimes |w''\rangle$ then we say that, in state

[6] Actually, $\mathcal{H}(V)$ is isomorphic to L^2 over the counting measure on V. Since we have in mind applications to quantum computation and information where all bits have the same importance, the choice of the counting measure is appropriate. However, other applications may require a different approach leading to a quite different logic. For instance, when looking at a quantum system with a physical real quantity such that each $\mathbf{p}_k$ reflects the k-th bit in its binary representation (and we could use sequences of other propositional symbols for representing other quantities), the Hilbert space proposed above would not be suitable. We should use instead L^2 over the Lebesgue measure on $[0, 1]$.

$|w\rangle$, the qubits in S are not entangled with the qubits not in S and, therefore, that the qubits in S are independent of the other qubits at that state $|w\rangle$.

This exogenous semantics for reasoning about a quantum system (and its subsystems) suggests that we adopt the quantum language composed of formulae of the form[7]

$$\gamma := \omega_k \curlyvee \varphi \curlyvee (t \leq t) \curlyvee ([S] \between \overrightarrow{\psi : u}) \curlyvee (\boxminus \gamma) \curlyvee (\gamma \sqsupset \gamma)$$

where φ is a classical formula, t is a real term, u is a complex term, S is a nonempty recursive set of propositional constants (qubits), and ψ is a classical formula over S. The classical language is as before. The enriched set of real terms and the set of complex terms are jointly defined as follows:

$$\begin{cases} t := \theta_k \curlyvee r \curlyvee (\textstyle\int \varphi) \curlyvee (\textstyle\int \varphi \,|\, \varphi) \curlyvee (t+t) \curlyvee (t\,t) \curlyvee \mathrm{Re}(u) \curlyvee \mathrm{Im}(u) \curlyvee \arg(u) \curlyvee |u| \\ u := v_k \curlyvee (t+it) \curlyvee te^{it} \curlyvee \overline{u} \curlyvee (u+u) \curlyvee (u\,u) \end{cases}.$$

The denotation at $\mathbf{w}$ of ground terms is straightforward, but it is worthwhile to mention that the probability terms are interpreted using $\mathcal{N}(\mathbf{w})$. For instance: $[\![(\int \varphi)]\!]_{\mathbf{w}} = \nu_{|w\rangle}([\varphi]_{\mathbf{w}})$. The satisfaction of formulae by $\mathbf{w}$ and ground substitution ρ is as follows:

- $\mathbf{w}\rho \Vdash \omega_j$ iff $\mathbf{w}\rho \Vdash \omega_j \rho$;
- $\mathbf{w}\rho \Vdash \varphi$ iff $v \Vdash \varphi\rho$ for every $v \in V$;
- $\mathbf{w}\rho \Vdash (t_1 \leq t_2)$ iff $[\![t_1\rho]\!]_{\mathbf{w}} \leq [\![t_2\rho]\!]_{\mathbf{w}}$;
- $\mathbf{w}\rho \Vdash ([S] \between \psi_1 : u_1, \ldots, \psi_n : u_n)$ iff there are unit $|w'\rangle \in \mathcal{H}(V_{[S]})$ and unit $|w''\rangle \in \mathcal{H}(V_{]S[})$ such that $|w\rangle = |w'\rangle \otimes |w''\rangle$ and there are distinct $v_1, \ldots, v_n \in \mathrm{supp}(|w'\rangle)$ such that $v_k \Vdash \psi_k\rho$ and $|w'\rangle(v_k) = [\![u_k\rho]\!]_{\mathbf{w}}$ for $k = 1, \ldots, n$;
- $\mathbf{w}\rho \Vdash (\boxminus \alpha)$ iff $\mathbf{w}\rho \not\Vdash \alpha$;
- $\mathbf{w}\rho \Vdash (\alpha_1 \sqsupset \alpha_2)$ iff $\mathbf{w}\rho \not\Vdash \alpha_1$ or $\mathbf{w}\rho \Vdash \alpha_2$.

The language of EQPL, the exogenous quantum propositional logic just introduced, is quite powerful. Some abbreviations are useful for expressing some important derived concepts:

- $(\between \varphi_1 : u_1, \ldots, \varphi_n : u_n)$ for $([\{\mathbf{p}_k : k \in \mathbb{N}\}] \between \varphi_1 : u_1, \ldots, \varphi_n : u_n)$;
- $[S]$ for $([S] :)$ — qubits in S are not entangled with those outside S;
- $(\Diamond\varphi)$ for $((\int \varphi) > 0)$ and $(\Box\varphi)$ for $((\int \varphi) = 1)$;
- $(\bigwedge_F A)$ for $((\wedge_{p_k \in A} \mathbf{p}_k) \wedge (\wedge_{p_k \in (F \setminus A)} (\neg \mathbf{p}_k)))$ whenever F is a finite set of propositional constants and $A \subseteq F$.

[7]Here we need to extend the Backus-Naur notation: we write $\vec{\delta}$ for a finite sequence of elements of the form δ.

As an illustration, consider the following consistent assertions about an enriched Schrödinger's cat (where **cat-in-box**, **cat-alive** and **cat-moving** are propositional constants):

- $[\mathbf{cat\text{-}in\text{-}box}, \mathbf{cat\text{-}alive}, \mathbf{cat\text{-}moving}]$;
- $(\mathbf{cat\text{-}in\text{-}box} \wedge (\mathbf{cat\text{-}moving} \Rightarrow \mathbf{cat\text{-}alive}))$;
- $((\Diamond \mathbf{cat\text{-}alive}) \sqcap (\Diamond (\neg\, \mathbf{cat\text{-}alive})))$;
- $([\mathbf{cat\text{-}alive}, \mathbf{cat\text{-}moving}] \sqcap (\boxminus [\mathbf{cat\text{-}alive}]))$;
- $(((\int \mathbf{cat\text{-}alive}) = \frac{1}{3}) \sqcap ((\int \mathbf{cat\text{-}moving} \,|\, \mathbf{cat\text{-}alive}) = \frac{1}{2}))$;
- $([\mathbf{cat\text{-}alive}, \mathbf{cat\text{-}moving}] \Diamond \mathbf{cat\text{-}alive} : \frac{1}{\sqrt{6}}, \mathbf{cat\text{-}alive} : \frac{1}{\sqrt{6}})$;
- $([\mathbf{cat\text{-}alive}, \mathbf{cat\text{-}moving}] \Diamond (\mathbf{cat\text{-}alive} \wedge \mathbf{cat\text{-}moving}) : \frac{1}{\sqrt{6}},$
  $(\mathbf{cat\text{-}alive} \wedge (\neg\, \mathbf{cat\text{-}moving})) : \frac{1}{\sqrt{6}},$
  $((\neg\, \mathbf{cat\text{-}alive}) \wedge (\neg\, \mathbf{cat\text{-}moving})) : e^{i\frac{\pi}{3}} \sqrt{\frac{2}{3}})$.

The notion of quantum entailment is introduced as expected: $\Gamma \vDash \delta$ iff, for every quantum structure $\mathbf{w}$ and ground substitution ρ, $\mathbf{w}\rho \Vdash \delta$ whenever $\mathbf{w}\rho \Vdash \gamma$ for each $\gamma \in \Gamma$. Our ultimate goal is to establish a deduction calculus complete in some useful sense with respect to this semantics. Meanwhile, the following are examples of interesting entailments:

- $\vDash (\boxminus ([S] \Diamond \psi : 0))$;
- $\vDash (([S] \Diamond \psi_1 : u_1, \ldots, \psi_n : u_n) \sqsupset ([S] \Diamond \psi_k : e^{it} u_k))$ for $k = 1, \ldots, n$;
- $\vDash (([S] \Diamond (\psi \vee \psi') : u) \equiv (([S] \Diamond \psi : u) \sqcup ([S] \Diamond \psi' : u)))$;
- $\vDash (([S] \Diamond \psi_1 : u_1, \ldots, \psi_n : u_n) \sqsupset ((|u_1|^2 + \cdots + |u_n|^2) \leq (\int (\psi_1 \vee \ldots \vee \psi_n))))$;
- $\vDash (([F] \Diamond (\bigwedge_F A) : u) \sqsupset ((\int (\bigwedge_F A)) \leq |u|^2))$;
- $\vDash ((\psi_1 \Rightarrow \psi_2) \sqsupset (([S] \Diamond \psi_1 : u) \leq ([S] \Diamond \psi_2 : u)))$.

4 DEQPL

For reasoning about changes in the state of a quantum system (including transitions resulting from projective observations of a single qubit), we need to enrich the language. Following [18], according to postulate 2 of quantum physics, the evolution of a closed quantum system is described by a unitary operator. And postulate 3 tells us what is the resulting state when a qubit is projectively observed with result $|b\rangle$ in $\mathcal{H}(2)$. We need transition terms for denoting all such state transitions, of the form

$$Z := \tau_k \curlyvee U \curlyvee P \curlyvee (Z \circ Z)$$

where U is a unitary operator term of the form

$$U := \mathbf{I} \curlyvee \mathbf{H}_k \curlyvee \mathbf{S}_k \curlyvee \left(\frac{\pi}{\mathbf{8}}\right)_k \curlyvee \mathbf{X}_k \curlyvee \mathbf{Y}_k \curlyvee \mathbf{Z}_k \curlyvee \mathbf{cN}_{k_2}^{k_1} \curlyvee U^{-1} \curlyvee (U \circ U)$$

and P is a projective observation transition term of the form

$$P := \mathbf{P}_k^{c|\mathbf{0}\rangle + c|\mathbf{1}\rangle}$$

where c is a complex number of the form $r + ir$ where r is, as before, a computable real number. The eight symbols in U denote the eight basic unitary operators (identity, Hadamard, phase, $\pi/8$, Pauli X, Y, Z, and control not, respectively). Any finitary, unitary operator can be approximated as close as desired by a finite composition of these basic operators [9]. We also need transition formulae of the form[8]

$$H := \{\gamma\}\, Z\, \{\gamma\} \curlyvee \{\gamma\}\, \Omega Z$$

where γ is a quantum formula as defined in the previous section.

The denotation $[\![Z]\!]$ of a transition term Z is a partial map from the unit circle of $\mathcal{H}(\mathcal{V})$ to itself (recall that $\mathcal{V}$ is the set of all classical valuations). In the case of every unitary operator term this map is total. Partiality only arises for observation transitions (as illustrated below).

Observe that, given $V \subseteq \mathcal{V}$, it may happen that $[\![Z]\!]|w\rangle \notin \mathcal{H}(V)$ even when $|w\rangle \in \mathcal{H}(V)$ and $[\![Z]\!]$ is defined on $|w\rangle$. We must keep this in mind when defining the satisfaction of transition formulae[9]:

- $V\rho \Vdash \{\gamma_1\}\, Z\, \{\gamma_2\}$ iff, for every $|w\rangle \in \mathcal{H}(V)$, if $\langle V, |w\rangle\rangle\rho \Vdash \gamma_1$ then $\langle V, [\![Z]\!]|w\rangle\rangle\rho \Vdash \gamma_2$ whenever $[\![Z]\!]|w\rangle\!\downarrow$ and $[\![Z]\!]|w\rangle \in \mathcal{H}(V)$;

- $V\rho \Vdash \{\gamma\}\, \Omega Z$ iff, for every $|w\rangle \in \mathcal{H}(V)$, if $\langle V, |w\rangle\rangle\rho \Vdash \gamma$ then $[\![Z]\!]|w\rangle\!\downarrow$ and $[\![Z]\!]|w\rangle \in \mathcal{H}(V)$.

That is, $\{\gamma_1\}\, Z\, \{\gamma_2\}$ means that if the quantum system evolves by Z from a state where γ_1 holds to a legitimate state (that is, in $\mathcal{H}(V)$) then γ_2 holds at the resulting state. If the resulting state is not legitimate the transition formula is vacuously satisfied. And $\{\gamma\}\, \Omega Z$ means that the quantum system reaches a legitimate state when it evolves by Z from a state where γ holds.

It is worthwhile to spell out in detail the semantics of the basic unitary operators. To this end, we need the notion of the dual of a valuation on a qubit: $\overline{v}^k$ is the valuation that agrees with v on all propositional symbols barring $\mathbf{p}_k$ and gives the other Boolean value to $\mathbf{p}_k$. For instance:

- $[\![\mathbf{H}_k]\!]|w\rangle(v) = \begin{cases} \frac{1}{\sqrt{2}}(|w\rangle(v) + |w\rangle(\overline{v}^k)) & \text{if } v \not\Vdash \mathbf{p}_k \\ \frac{1}{\sqrt{2}}(|w\rangle(\overline{v}^k) - |w\rangle(v)) & \text{otherwise} \end{cases}$;

[8] Adapting from the Hoare (pre- and post-condition) triplets in the logic of imperative programs [13].

[9] As usual when dealing with partial maps, we write $[\![Z]\!]|w\rangle\!\downarrow$ for asserting that $[\![Z]\!]$ is defined on $|w\rangle$.

- $[\![\mathbf{S}_k]\!]|w\rangle(v) = \begin{cases} |w\rangle(v) & \text{if } v \not\Vdash \mathbf{p}_k \\ i|w\rangle(v) & \text{otherwise} \end{cases}$;

- $[\![\mathbf{cN}^{k_1}_{k_2}]\!]|w\rangle(v) = \begin{cases} |w\rangle(v) & \text{if } v \not\Vdash \mathbf{p}_{k_1} \\ |w\rangle(\overline{v}^{k_2}) & \text{otherwise} \end{cases}$.

Before describing the semantics of the projective observation operators, we need some notation. Given a set S of propositional constants (qubits), we denote by $I_{[S]}$ the identity operator on $\mathcal{H}(\mathcal{V}_{[S]})$ and by $I_{]S[}$ the identity operator on $\mathcal{H}(\mathcal{V}_{]S[})$. Given $|b\rangle = \alpha_0|\mathbf{0}\rangle + \alpha_1|\mathbf{1}\rangle$ in $\mathcal{H}(2)$ we also need to use the projector along $|b\rangle$, the operator $|b\rangle\langle b|$ on $\mathcal{H}(2)$ defined by the following matrix:

$$\begin{pmatrix} \alpha_0\overline{\alpha_0} & \alpha_0\overline{\alpha_1} \\ \alpha_1\overline{\alpha_0} & \alpha_1\overline{\alpha_1} \end{pmatrix} .$$

Letting $P^{|b\rangle}_k$ be the projector along $|b\rangle$ for qubit k in $\mathcal{H}(\mathcal{V})$ that is given by $I_{[\{\mathbf{p}_0,\dots,\mathbf{p}_{k-1}\}]} \otimes |b\rangle\langle b| \otimes I_{]\{\mathbf{p}_0,\dots,\mathbf{p}_k\}[}$, the semantics of the projective observation transition terms is as follows:

- $[\![\mathbf{P}^{c_0|\mathbf{0}\rangle+c_1|\mathbf{1}\rangle}_k]\!]|w\rangle = \frac{P^{c_0|\mathbf{0}\rangle+c_1|\mathbf{1}\rangle}_k|w\rangle}{||P^{c_0|\mathbf{0}\rangle+c_1|\mathbf{1}\rangle}_k|w\rangle||}$.

Observe that $[\![\mathbf{P}^{c_0|\mathbf{0}\rangle+c_1|\mathbf{1}\rangle}_k]\!]$ is undefined at $|w\rangle$ if $||P^{c_0|\mathbf{0}\rangle+c_1|\mathbf{1}\rangle}_k|w\rangle|| = 0$. In particular, $[\![\mathbf{P}^{|\mathbf{0}\rangle}_k]\!]$ is undefined at $|w\rangle$ whenever $|w\rangle \Vdash ((\textstyle\int(\neg\,\mathbf{p}_k)) = 0)$. In fact, it is not possible to observe 0 on $\mathbf{p}_k$ when all valuations in the support of the state of the system satisfy $\mathbf{p}_k$.

The projective observation transition terms play the role of qubit assignments in quantum computation since they impose the superposition of the target qubit in the resulting state. But, contrarily to classical computation, an assignment to qubit $\mathbf{p}_k$ may also affect other qubits (those that were entangled with $\mathbf{p}_k$). For instance, the transition formula

$$\begin{aligned} &\{([\mathbf{Earth\text{-}cat\text{-}alive}, \mathbf{Mars\text{-}cat\text{-}alive}] \lozenge \\ &\qquad\qquad (\mathbf{Earth\text{-}cat\text{-}alive} \wedge \mathbf{Mars\text{-}cat\text{-}alive}) : \tfrac{1}{\sqrt{2}}, \\ &\qquad\qquad ((\neg\,\mathbf{Earth\text{-}cat\text{-}alive}) \wedge (\neg\,\mathbf{Mars\text{-}cat\text{-}alive})) : \tfrac{1}{\sqrt{2}})\} \\ &\mathbf{P}^{|\mathbf{0}\rangle}_{\mathbf{Earth\text{-}cat\text{-}alive}} \\ &\{([\mathbf{Mars\text{-}cat\text{-}alive}] \lozenge (\neg\,\mathbf{Mars\text{-}cat\text{-}alive}) : 1)\} \end{aligned}$$

states, among other things, that if the two cats are entangled then after observing the Earth cat dead we end up in a state where the Mars cat is also dead.

The proposed quantum transition language is quite powerful. We envisage to set up a relatively complete calculus for DEQPL (the dynamic exogenous quantum propositional logic with the above semantics). The key ingredients of this calculus will be the rules for the primitive operators since dealing with composition and relating with valid formulae of EQPL will be straightforward.

5 Concluding remarks and acknowledgments

The proposed exogenous approach to quantum reasoning provided us with a working semantics for a powerful quantum logic. The resulting logic is promising and interesting in itself, but further work is necessary, namely towards a complete axiomatization and a clarification of the relationship to other quantum logics.

Since it is feasible to repeat the construction starting from any other logic (fulfilling some weak requirements), it seems worthwhile to investigate the construction of quantum logics as a form of parameterization of logics (as defined in [5]), like it is done for probabilistic logic in [16].

Assessing the effective role of the chosen basis for $\mathcal{H}(V)$ is also an interesting line of research. Indeed, EQPL satisfaction, as defined herein, strongly relies upon using the orthonormal basis $\{|v\rangle : v \in V\}$. One wonders if we can relax the semantics, while preserving the intended entailment, in order to be able to deal with classical formulae when we do not know V but we are just given a Hilbert space isomorphic to $\mathcal{H}(V)$.

The authors wish to express their deep gratitude to João Marcos who carefully proofread the draft and to the regular participants in the QCI Seminar who suffered early presentations of this work and gave very useful feedback that helped us to get over initial difficulties and misunderstandings of quantum physics, specially Jorge Buescu, Manuel Ricou, António Serra, Gabriel Pires, Pedro Resende, Vítor Rocha Vieira, Walter Carnielli, João Pimentel Nunes, and, last but not least, José Cidade Mourão.

This work was partially supported by FCT and FEDER through POCTI, namely via FibLog 2001/MAT/37239 Project and within the recent QuantLog initiative of CLC.

References

[1] M. Abadi and J. Y. Halpern. Decidability and expressiveness for first-order logics of probability. *Information and Computation*, 112(1):1–36, 1994.

[2] F. Bacchus. On probability distributions over possible worlds. In *Uncertainty in Artificial Intelligence, 4*, volume 9 of *Machine Intelligence and Pattern Recognition*, pages 217–226. North-Holland, 1990.

[3] F. Bacchus. *Representing and Reasoning with Probabilistic Knowledge*. MIT Press Series in Artificial Intelligence. MIT Press, 1990.

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

[5] C. Caleiro, C. Sernadas, and A. Sernadas. Parameterisation of logics. In J. Fiadeiro, editor, *Recent Trends in Algebraic Development Techniques - Selected Papers*, volume 1589 of *Lecture Notes in Computer Science*, pages 48–62. Springer-Verlag, 1999.

[6] W. A. Carnielli. Possible-translations semantics for paraconsistent logics. In *Frontiers of Paraconsistent Logic (Ghent, 1997)*, volume 8 of *Studies in Logic and Computation*, pages 149–163. Research Studies Press, 2000.

[7] W. A. Carnielli and M. Lima-Marques. Society semantics and multiple-valued logics. In *Advances in Contemporary Logic and Computer Science (Salvador, 1996)*, volume 235 of *Contemporary Mathematics*, pages 33–52. AMS, 1999.

[8] M. L. D. Chiara, R. Giuntini, and R. Greechie. *Reasoning in Quantum Theory*. Kluwer Academic Publishers, 2004.

[9] D. P. DiVincenzo. Two-bit gates are universal for quantum computation. *Physics Reviews A*, 51(2):1015–1022, 1995.

[10] R. Fagin, J. Y. Halpern, and N. Megiddo. A logic for reasoning about probabilities. *Information and Computation*, 87(1-2):78–128, 1990.

[11] D. J. Foulis. A half-century of quantum logic. What have we learned? In *Quantum Structures and the Nature of Reality*, volume 7 of *Einstein Meets Magritte*, pages 1–36. Kluwer Acad. Publ., 1999.

[12] S. Hart and M. Sharir. Probabilistic propositional temporal logics. *Information and Control*, 70(2-3):97–155, 1986.

[13] C. Hoare. An axiomatic basis for computer programming. *Communications of the ACM*, 12:576–583, 1969.

[14] S. A. Kripke. Semantical analysis of modal logic. I. Normal modal propositional calculi. *Zeitschrift für Mathematische Logik und Grundlagen der Mathematik*, 9:67–96, 1963.

[15] P. Mateus, A. Pacheco, J. Pinto, A. Sernadas, and C. Sernadas. Probabilistic situation calculus. *Annals of Mathematics and Artificial Intelligence*, 32(1/4):393–431, 2001.

[16] P. Mateus, A. Pacheco, A. Sernadas, and C. Sernadas. Exogenous probabilization of an arbitrary logic. In preparation, 2004.

[17] P. Naur. Revised report on the algorithmic language Algol 60. *The Computer Journal*, 5:349–367, 1963.

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

[19] N. J. Nilsson. Probabilistic logic. *Artificial Intelligence*, 28(1):71–87, 1986.

[20] N. J. Nilsson. Probabilistic logic revisited. *Artificial Intelligence*, 59(1-2):39–42, 1993.