Quantum institutions

C. Caleiro, P. Mateus, A. Sernadas and C. Sernadas

CLC, Department of Mathematics, IST,
Av. Rovisco Pais, 1000-149 Lisbon, Portugal

Abstract. The exogenous approach to enriching any given base logic for probabilistic and quantum reasoning is brought into the realm of institutions. The theory of institutions helps in capturing the precise relationships between the logics that are obtained, and, furthermore, helps in analyzing some of the key design decisions and opens the way to make the approach more useful and, at the same time, more abstract.

1 Introduction

A new logic was proposed in [1–3] for modeling and reasoning about quantum states, embodying the relevant postulates of quantum physics (as presented, for instance, in [4]) and adopting the exogenous approach (the original models are kept). The logic was designed from the semantics upwards, starting with the key idea of adopting superpositions of classical models as the models of the quantum logic. In [5], other instances of the exogenous approach to enriching logics were presented in detail. In short, the exogenous approach is based on adopting as models of the new envisaged logic (enriched) sets of models of the given base logic without tampering with the models of the original logic. As an example assume that we want to introduce probabilities to a certain logic. Doing so, using the exogenous approach, means that we consider the possible outcomes to be the semantic structures and we assign probabilities to sets of such structures.

This novel approach to quantum logic semantics is completely different from the traditional approach [6, 7] to the problem, as initially proposed by Birkhoff and von Neumann [8], that focuses on the lattice of closed subspaces of a Hilbert space. The main drawback of Birkhoff and von Neumann's approach is that it does not yield an extension of classical logic. Our semantics has the advantage of closely guiding the design of the language around the underlying concepts of quantum physics while keeping the classical connectives and was inspired by the Kripke semantics for modal logic. The possible worlds approach was also used in [9–13] for probabilistic logic. Our semantics to quantum logic, although inspired by modal logic, is also completely different from the alternative Kripke semantics given to traditional quantum logics (as first proposed in [14]) still closely related to the lattice-based operations. The resulting quantum logic also incorporates probabilistic reasoning (in the style of Nilsson's calculus [9, 10]) since the postulates of quantum physics impose uncertainty on the outcome of measurements. From a quantum state (superposition of classical valuations living in a suitable Hilbert space) it is straightforward to generate a probability space of classical valuations in order to provide the semantics for reasoning about the probabilistic measurements made on that state.

Herein, we present within the theory of institutions (a logic is identified with an institution, as originally proposed in [15, 16]), the exogenous-style construction of a quantum logic from any given base logic in order to assess how general the construction is. The construction is carried out in three main steps. Given an arbitrary institution we first build its global extension (globalization) where each model is just a set of models of the original institution. Then, we proceed with the construction of its probabilistic extension (probabilization) where each model is a probability space where the outcomes are models of the original institution. Finally, we obtain the quantum extension (quantization) of the given institution where each model is a unit vector in the Hilbert space freely generated from a set of models of the original institution. Obviously, in each step the language is enriched to take advantage and to express properties of the new models. For instance, in the globalization step, global classical connectives are added for reasoning about formulas of the original logic. The institutional perspective allows us to conclude that the first two constructions are fully general, in the sense that nothing is assumed about the given institution and also that nothing else is needed. But quantization requires some additional information (the choice of qubit formulae).

In Section 2, we briefly present the relevant notions and results of the theory of institutions. The globalization step is described in Section 3. The probabilization step is presented in Section 4. Finally, in Section 5 we carry out the quantization step of the enrichment. We conclude with an outline of further research directions.

2 Institutional preliminaries

In this paper, as a first step towards the full understanding of the proposed approach to enriching logics, we shall adopt a variant of the original notion of institution, without morphisms between models (c.f. [17]). For simplicity we shall just call it an institution, without any further qualifiers. We denote by **Cls** the category with classes as objects and maps between classes as morphisms.

An *institution* is a tuple $I = \langle \mathbf{Sig}, \mathbf{Sen}, \mathbf{Mod}, \Vdash \rangle$ where: **Sig** is a category (of *signatures*); $\mathbf{Sen} : \mathbf{Sig} \to \mathbf{Set}$ is a (*formula*) functor; $\mathbf{Mod} : \mathbf{Sig} \to \mathbf{Cls}^{\mathbf{op}}$ is a (*model*) functor; and $\Vdash = \{\Vdash_\Sigma\}_{\Sigma \in |\mathbf{Sig}|}$ is a family of (*satisfaction*) relations $\Vdash_\Sigma \subseteq \mathbf{Mod}(\Sigma) \times \mathbf{Sen}(\Sigma)$, such that the following *satisfaction condition* holds, for every signature morphism $\sigma : \Sigma \to \Sigma'$, every formula $\varphi \in \mathbf{Sen}(\Sigma)$, and every model $m' \in \mathbf{Mod}(\Sigma')$: $\mathbf{Mod}(\sigma)(m') \Vdash_\Sigma \varphi$ iff $m' \Vdash_{\Sigma'} \mathbf{Sen}(\sigma)(\varphi)$.

As usual, given a set $\Gamma \subseteq \mathbf{Sen}(\Sigma)$ of formulas and a model $m \in \mathbf{Mod}(\Sigma)$, we will write $m \Vdash_\Sigma \Gamma$ to denote the fact that $m \Vdash_\Sigma \varphi$ for every $\varphi \in \Gamma$. Mutatis mutandis, given a set $M \subseteq \mathbf{Mod}(\Sigma)$ of models and a formula $\varphi \in \mathbf{Sen}(\Sigma)$, we will write $M \Vdash_\Sigma \varphi$ to denote the fact that $m \Vdash_\Sigma \varphi$ for every $m \in M$. Recall that I induces a family $\vDash = \{\vDash_\Sigma\}_{\Sigma \in |\mathbf{Sig}|}$ of (*entailment*) relations $\vDash_\Sigma \subseteq$

$\mathbf{Pw}(\mathbf{Sen}(\Sigma)) \times \mathbf{Sen}(\Sigma)$ defined by $\Gamma \vDash_\Sigma \varphi$ if, for every $m \in \mathbf{Mod}(\Sigma)$, if $m \Vdash_\Sigma \Gamma$ then $m \Vdash_\Sigma \varphi$.

The notions of arrow between institutions are at least as important as the notion of institution itself. There is a rather extensive and prolific bibliography on this subject, where various meaningful notions of arrows between institutions are proposed, used, exemplified, and related with each other. A recent systematization of the field can be found in [17]. The notion of arrow that we will be using in this paper can be classified as a *comorphism* (or a *plain map* as originally named in [18], or also a *representation* as renamed in [19]). It is however a modified comorphism that maps models to sets of models, which can be explained as an instance of the general monad construction of [20]. The definition will take advantage of the usual covariant powerset endofunctor $\mathbf{Pw}$, in this case extended to classes, that is, $\mathbf{Pw} : \mathbf{Cls} \to \mathbf{Cls}$ is such that $\mathbf{Pw}(X) = 2^X$, and $\mathbf{Pw}(f : X \to X')$ maps each $Y \subseteq X$ to $f[Y] = \{f(x) : x \in Y\}$.

Definition 1. A *power-model comorphism* from institution I to institution I' is a tuple $\langle \Phi, \alpha, \beta \rangle$ where $\Phi : \mathbf{Sig} \to \mathbf{Sig}'$ is a (*signature translation*) functor; $\alpha : \mathbf{Sen} \to \mathbf{Sen}' \circ \Phi$ is a (*formula translation*) natural transformation; and $\beta : \mathbf{Mod}' \circ \Phi \to \mathbf{Pw} \circ \mathbf{Mod}$ is a (*power-model translation*) natural transformation, such that the following *coherence condition* holds, for every signature $\Sigma \in |\mathbf{Sig}|$, formula $\varphi \in \mathbf{Sen}(\Sigma)$, and model $m' \in \mathbf{Mod}'(\Phi(\Sigma))$: $\beta_\Sigma(m') \Vdash_\Sigma \varphi$ iff $m' \Vdash'_{\Phi(\Sigma)} \alpha_\Sigma(\varphi)$.

In the definition above, $\beta_\Sigma(m')$ is a set of models. Thus, the coherence condition states that $m' \Vdash'_{\Phi(\Sigma)} \alpha_\Sigma(\varphi)$ iff, for every $m \in \beta_\Sigma(m')$, $m \Vdash_\Sigma \varphi$. Clearly, the possibility that $\beta_\Sigma(m') = \emptyset$ is not excluded. In that case, m' must satisfy the translation via α of any formula whatsoever. A particularly interesting case corresponds to the situation when $\beta_\Sigma(m')$ is a singleton. If this happens for every model then we can recast the power-model natural transformation simply to $\beta : \mathbf{Mod}' \circ \Phi \to \mathbf{Mod}$, thus obtaining the usual notion of comorphism.

It is a well known fact that comorphisms preserve entailment. A further simple condition on the surjectivity of the translation of models can also guarantee the reflection of entailment. Such properties were studied in [21]. These results can easily be lifted to the level of power-model comorphisms, as stated below. (Power-model) comorphisms compose in the usual way.

Proposition 1. *Let I and I' be institutions and $\langle \Phi, \alpha, \beta \rangle : I \to I'$ a power-model comorphism. Then $\Gamma \vDash_\Sigma \varphi$ implies $\alpha_\Sigma[\Gamma] \vDash_{\Phi(\Sigma)} \alpha_\Sigma(\varphi)$. Additionally, if for each $m \in \mathbf{Mod}(\Sigma)$ there exists $m' \in \mathbf{Mod}'(\Phi(\Sigma))$ such that $\beta_\Sigma(m') = \{m\}$, then $\Gamma \vDash_\Sigma \varphi$ iff $\alpha_\Sigma[\Gamma] \vDash_{\Phi(\Sigma)} \alpha_\Sigma(\varphi)$.*

Proof. Given the power-model comorphism, assume that $\Gamma \vDash_\Sigma \varphi$. If $m' \in \mathbf{Mod}'(\Phi(\Sigma))$ is such that $m' \Vdash'_{\Phi(\Sigma)} \alpha_\Sigma[\Gamma]$ then, using the coherence condition of the power-model comorphism, we have that $\beta_\Sigma(m') \Vdash_\Sigma \Gamma$. Thus, by definition of entailment, it follows from $\Gamma \vDash_\Sigma \varphi$ that $\beta_\Sigma(m') \Vdash_\Sigma \varphi$. Using again the coherence condition, we now get $m' \Vdash'_{\Phi(\Sigma)} \alpha_\Sigma(\varphi)$. Hence, $\alpha_\Sigma[\Gamma] \vDash_{\Phi(\Sigma)} \alpha_\Sigma(\varphi)$.

Assume now that the additional surjectivity condition holds and $\alpha_\Sigma[\Gamma] \vDash_{\Phi(\Sigma)} \alpha_\Sigma(\varphi)$. If $m \in \mathbf{Mod}(\Sigma)$ is such that $m \Vdash_\sigma \Gamma$ then $\{m\} \Vdash_\sigma \Gamma$. But we know that there exists $m' \in \mathbf{Mod}'(\Phi(\Sigma))$ such that $\beta_\Sigma(m') = \{m\}$. Thus, $\beta_\Sigma(m') \Vdash_\sigma \Gamma$ and it follows from the coherence condition of the power-model comorphism that $m' \Vdash'_{\Phi(\Sigma)} \alpha_\Sigma[\Gamma]$. Hence, by definition of entailment, it follows that $m' \Vdash'_{\Phi(\Sigma)} \alpha_\Sigma(\varphi)$. Using again the coherence condition we obtain that $\beta_\Sigma(m') \Vdash_\sigma \varphi$, or equivalently, $m \Vdash_\sigma \varphi$. Therefore, $\Gamma \vDash_\Sigma \varphi$. ▷

Hence, the existence of a power-model comorphism that fulfills the *surjectivity condition* stated in the second half of Proposition 1, for every signature, allows one to say that the target institution is a conservative extension of the source institution. Note that, for comorphisms, the surjectivity condition stated above simply boils down to requiring that each map $\beta_\Sigma : \mathbf{Mod}'(\Phi(\Sigma)) \to \mathbf{Mod}(\Sigma)$ is surjective. It is also a trivial task to check that the surjectivity condition is preserved by composing (power-model) comorphisms.

3 Global institution

As a first step in our development, we aim at characterizing the exogenous enrichment of a given logic with a layer of global reasoning. For the purpose, let $I = \langle \mathbf{Sig}, \mathbf{Sen}, \mathbf{Mod}, \Vdash \rangle$ be the starting institution. We now proceed by defining the envisaged global institution I^g and then showing, by means of a power-model comorphism, that it extends I in a conservative way.

Definition 2. The *global institution* $I^g = \langle \mathbf{Sig}, \mathbf{Sen}^g, \mathbf{Mod}^g, \Vdash^g \rangle$ based on I is defined as follows:

- $\mathbf{Sen}^g(\Sigma)$ is the least set containing $\mathbf{Sen}(\Sigma)$ such that, if $\delta, \delta_1, \delta_2 \in \mathbf{Sen}^g(\Sigma)$ then $(\boxminus\, \delta), (\delta_1 \sqsupset \delta_2) \in \mathbf{Sen}^g(\Sigma)$.
- $\mathbf{Sen}^g(\sigma) = \sigma^g$ is defined inductively by: $\sigma^g(\varphi) = \mathbf{Sen}(\sigma)(\varphi)$, $\sigma^g(\boxminus\, \delta) = (\boxminus\, \sigma^g(\delta))$, and $\sigma^g(\delta_1 \sqsupset \delta_2) = (\sigma^g(\delta_1) \sqsupset \sigma^g(\delta_2))$;
- $\mathbf{Mod}^g(\Sigma) = \{M : \emptyset \neq M \subseteq \mathbf{Mod}(\Sigma)\}$,
- $\mathbf{Mod}^g(\sigma)(M') = \mathbf{Mod}(\sigma)[M']$;
- $\Vdash^g_\Sigma$ is defined inductively by: $M \Vdash^g_\Sigma \varphi$ iff $M \Vdash_\Sigma \varphi$, $M \Vdash^g_\Sigma (\boxminus\, \delta)$ iff $M \nVdash^g_\Sigma \delta$, and $M \Vdash^g_\Sigma (\delta_1 \sqsupset \delta_2)$ iff $M \nVdash^g_\Sigma \delta_1$ or $M \Vdash^g_\Sigma \delta_2$.

Clearly, I^g is an institution. Indeed, the functoriality of $\mathbf{Sen}^g$ and $\mathbf{Mod}^g$ is straightforward. The satisfaction condition of I^g can be established by a simple induction on formulas. The only interesting case is the base case, that we analyze below, the other cases being immediate by induction hypotheses. Let $\sigma : \Sigma \to \Sigma'$ be a signature morphism, $\varphi \in \mathbf{Sen}(\Sigma)$ and $M' \in \mathbf{Mod}^g(\Sigma')$. Then, by definition of $\mathbf{Sen}^g$ and $\Vdash^g$, $M' \Vdash^g_{\Sigma'} \mathbf{Sen}^g(\sigma)(\varphi)$ iff $M' \Vdash_{\Sigma'} \mathbf{Sen}(\sigma)(\varphi)$, that is, $m' \Vdash_{\Sigma'} \mathbf{Sen}(\sigma)(\varphi)$ for every $m' \in M'$. Therefore, using the satisfaction condition of I, this is equivalent to having $\mathbf{Mod}(\sigma)(m') \Vdash_\Sigma \varphi$ for every $m' \in M'$, that is, $\mathbf{Mod}^g(\sigma)(M') \Vdash^g_\Sigma \varphi$.

In the resulting logic, the connectives $\boxminus$ and $\sqsupset$ correspond to global negation and global implication, respectively. Other connectives can be easily introduced, like global conjunction $(\delta_1 \sqcap \delta_2) \equiv \boxminus(\delta_1 \sqsupset (\boxminus \delta_2))$. If the base institution has a negation $\neg$ and an implication $\Rightarrow$, which can be understood as local, these connectives do not collapse with the global ones. For implication, for instance, we have that $\{(\varphi_1 \Rightarrow \varphi_2)\} \vDash^g_\Sigma (\varphi_1 \sqsupset \varphi_2)$, but the converse does not hold in general, given two base formulas $\varphi_1, \varphi_2 \in \mathbf{Sen}(\Sigma)$. Namely, assume that I is the institution of classical propositional logic, $\pi_1, \pi_2 \in \Sigma$ are two propositional symbols and $v_1, v_2 \in \mathbf{Mod}(\Sigma)$ are two classical valuations such that $v_1(\pi_1) = 0$, $v_1(\pi_2) = 0$, $v_2(\pi_1) = 1$ and $v_2(\pi_2) = 0$. Then, $\{v_1, v_2\} \Vdash^g_\Sigma (\pi_1 \sqsupset \pi_2)$ but $\{v_1, v_2\} \nVdash^g_\Sigma (\pi_1 \Rightarrow \pi_2)$. The logic resulting from globalizing classical propositional logic was carefully studied in [5], where a sound and complete calculus could be obtained by capitalizing on a calculus for classical logic and adding an axiomatization of the new connectives. It is an open question if the same sort of enterprise can be done in the general case. However, it seems possible to generalize the technique used there, at least if the base logic enjoys an expressibility property analogous to the disjunctive normal form of classical logic.

More interesting, at the moment, is to establish the precise relationship between the institutions I and I^g.

Proposition 2. The triple $C^g = \langle \Phi^g, \alpha^g, \beta^g \rangle$, where Φ^g is the identity functor on $\mathbf{Sig}$; for each Σ, α^g_Σ translates $\varphi \in \mathbf{Sen}(\Sigma)$ to φ; and for each Σ, β^g_Σ translates $M \in \mathbf{Mod}^g(\Sigma)$ to M, is a power-model comorphism $C^g : I \to I^g$ and fulfills the surjectivity condition.

Proof. The naturality of α^g and β^g is straightforward. Given a signature morphism $\sigma : \Sigma \to \Sigma'$ and $\varphi \in \mathbf{Sen}(\Sigma)$, we have $\mathbf{Sen}^g(\sigma)(\alpha^g_\Sigma(\varphi)) = \mathbf{Sen}^g(\sigma)(\varphi) = \mathbf{Sen}(\sigma)(\varphi) = \alpha^g_{\Sigma'}(\mathbf{Sen}(\sigma)(\varphi))$. Similarly, given $M' \in \mathbf{Mod}^g(\Sigma')$, then we have $\mathbf{Pw}(\mathbf{Mod}(\sigma))(\beta^g_{\Sigma'}(M')) = \mathbf{Pw}(\mathbf{Mod}(\sigma))(M') = \mathbf{Mod}(\sigma)[M'] = \mathbf{Mod}^g(\sigma)(M')$ $= \beta^g_\Sigma(\mathbf{Mod}^g(\sigma)(M'))$. The coherence condition is trivial. ▷

As a corollary, by Proposition 1, C^g shows that I^g is in fact a conservative extension of I.

4 Probability institution

Let us now characterize the exogenous enrichment of a given logic with probabilistic reasoning. We start by introducing the essential definitions and properties of probability spaces. A *probability space* over a non-empty set Ω of *outcomes* is a pair $P = \langle \mathcal{B}, \mu \rangle$ where $\mathcal{B}$ is a Borel field over Ω, that is, $\mathcal{B} \subseteq 2^\Omega$ contains Ω and is closed for complements and countable unions; and $\mu : \mathcal{B} \to [0, 1]$ is a measure with unitary mass, that is, $\mu(M) = 1$ and $\mu(\bigcup_{i=1}^\infty B_i) = \sum_{i=1}^\infty \mu(B_i)$ if $\{B_i\}_{i=1}^\infty \subseteq \mathcal{B}$ is a family of pairwise disjoint sets.

In due course, we will need to map probability spaces along functions on their outcomes. Let $f : U \to U'$ be a function, $\Omega \subseteq U$ and $P = \langle \mathcal{B}, \mu \rangle$ a probability space over Ω. The *image of P along f* is the probability space $f(P) = \langle \mathcal{B}', \mu' \rangle$ over $\Omega' = f[\Omega]$ where $\mathcal{B}' = \{B' \subseteq \Omega' : f^{-1}(B') \cap \Omega \in \mathcal{B}\}$; and μ' is such that $\mu'(B') = \mu(f^{-1}(B') \cap \Omega)$.

Let $I = \langle \mathbf{Sig}, \mathbf{Sen}, \mathbf{Mod}, \Vdash \rangle$ be the starting institution. As before, we shall first define the envisaged probability institution I^p and then show, using power-model comorphisms, that I^p extends conservatively both I and I^g. Indeed, the whole idea is to work with sets of models of the original institution, as in the global case, but now endow them with a certain probability measure. Of course, also the linguistic resources of the logic will be augmented to allow probabilistic assertions and reasoning. For that sake, we assume fixed a set X of variables. We shall also denote by R the set of all computable real numbers (see [22]).

Definition 3. The *probability institution* $I^p = \langle \mathbf{Sig}, \mathbf{Sen}^p, \mathbf{Mod}^p, \Vdash^p \rangle$ based on I is defined as follows:

- $\mathbf{Sen}^p(\Sigma)$ is the least set containing $\mathbf{Sen}(\Sigma)$ such that: $(\boxminus \delta), (\delta_1 \sqsupset \delta_2) \in \mathbf{Sen}^p(\Sigma)$ if $\delta, \delta_1, \delta_2 \in \mathbf{Sen}^p(\Sigma)$, and $(t_1 \leq t_2) \in \mathbf{Sen}^p(\Sigma)$ if $t_1, t_2 \in T^p(\Sigma)$, where $T^p(\Sigma)$ is the least set (of *probabilistic terms*) such that: $X, R \subseteq T^p(\Sigma)$, $(\int \varphi) \in T^p(\Sigma)$ if $\varphi \in \mathbf{Sen}(\Sigma)$, and $(t_1 + t_2), (t_1 . t_2) \in T^p(\Sigma)$ if $t_1, t_2 \in T^p(\Sigma)$;
- $\mathbf{Sen}^p(\sigma) = \sigma^p$ is defined inductively by: $\sigma^p(\varphi) = \mathbf{Sen}(\sigma)(\varphi)$, $\sigma^p(\boxminus \delta) = (\boxminus \sigma^p(\delta))$, $\sigma^p(\delta_1 \sqsupset \delta_2) = (\sigma^p(\delta_1) \sqsupset \sigma^p(\delta_2))$, and $\sigma^p(t_1 \leq t_2) = (T^p(\sigma)(t_1) \leq T^p(\sigma)(t_2))$, where $T^p(\sigma)$ is inductively defined by: $T^p(\sigma)(x) = x$, $T^p(\sigma)(r) = r$, $T^p(\sigma)(\int \varphi) = (\int \mathbf{Sen}(\sigma)(\varphi))$, $T^p(\sigma)(t_1 + t_2) = (T^p(\sigma)(t_1) + T^p(\sigma)(t_2))$, and $T^p(\sigma)(t_1 . t_2) = (T^p(\sigma)(t_1) . T^p(\sigma)(t_2))$;
- $\mathbf{Mod}^p(\Sigma)$ is the class of all triples $S = \langle M, P, \rho \rangle$ where M is non-empty set subset of $\mathbf{Mod}(\Sigma)$, $P = \langle \mathcal{B}, \mu \rangle$ is a probability space over M such that $\{m \in M : m \Vdash_\Sigma \varphi\} \in \mathcal{B}$ for every $\varphi \in \mathbf{Sen}(\Sigma)$, and $\rho : X \to \mathbb{R}$ is an assignment;
- $\mathbf{Mod}^p(\sigma)(\langle M', P', \rho' \rangle) = \langle \mathbf{Mod}(\sigma)[M'], \mathbf{Mod}(\sigma)(P'), \rho' \rangle$;
- $\Vdash^p_\Sigma$ is defined inductively by: $S \Vdash^p_\Sigma \varphi$ iff $M \Vdash_\Sigma \varphi$, for $\varphi \in \mathbf{Sen}(\Sigma)$, $S \Vdash^p_\Sigma (\boxminus \delta)$ iff $S \nVdash^p_\Sigma \delta$, $S \Vdash^p_\Sigma (\delta_1 \sqsupset \delta_2)$ iff $S \nVdash^p_\Sigma \delta_1$ or $S \Vdash^p_\Sigma \delta_2$, and $S \Vdash^p_\Sigma (t_1 \leq t_2)$ iff $[\![t_1]\!]^S \leq [\![t_2]\!]^S$, where the denotation of probabilistic terms $[\![\_]\!]^S : T^p(\Sigma) \to \mathbb{R}$ is defined inductively by: $[\![x]\!]^S = \rho(x)$, for $x \in X$ and $[\![r]\!]^S = r$, for $r \in R$, $[\![\int \varphi]\!]^S = \mu(\{m \in M : m \Vdash_\Sigma \varphi\})$, $[\![t_1 + t_2]\!]^S = [\![t_1]\!]^S + [\![t_2]\!]^S$ and $[\![t_1 . t_2]\!]^S = [\![t_1]\!]^S . [\![t_2]\!]^S$.

I^p is an institution. Indeed the functoriality of $\mathbf{Sen}^p$ is straightforward. Concerning $\mathbf{Mod}^p$, and given $\sigma : \Sigma \to \Sigma'$, just note that indeed $\langle M, P, \rho \rangle = \mathbf{Mod}^p(\sigma)(\langle M', P', \rho' \rangle) \in \mathbf{Mod}^p(\Sigma)$. Given $\varphi \in \mathbf{Sen}(\Sigma)$, $\{m \in M : m \Vdash_\Sigma \varphi\}$ is measurable, because $M = \mathbf{Mod}(\sigma)[M']$, and it is also measurable the set $\mathbf{Mod}(\sigma)^{-1}(\{m \in M : m \Vdash_\Sigma \varphi\}) \cap M' = \{m' \in M' : \mathbf{Mod}(\sigma)(m') \Vdash_\Sigma \varphi\} = \{m' \in M' : m' \Vdash_{\Sigma'} \mathbf{Sen}(\sigma)(\varphi)\}$.

The satisfaction condition of I^p can be established by a simple induction on formulas. The only interesting case is that of inequalities. Let $t \in T^p(\Sigma)$. For ease of notation let $S' = \langle M', P', \rho' \rangle$ and $P' = \langle \mathcal{B}', \mu' \rangle$, $S = \mathbf{Mod}^p(\sigma)(S') = \langle M, P, \rho \rangle$ and $P = \mathbf{Mod}(\sigma)(P') = \langle \mathcal{B}, \mu \rangle$. We need to show that $[\![t]\!]^S = [\![T^p(\sigma)(t)]\!]^{S'}$. This fact can be shown by a simple induction on terms. The interesting case concerns the terms $(\int \varphi)$. Given $\varphi \in \mathbf{Sen}(\Sigma)$, using the definitions of term denotation and of image of a probability space, the satisfaction condition of the base institution I, and the definition of term translation, along with a little set-theoretical manipulation, we have that

$[\![\int\varphi]\!]^S = \mu(\{m \in M : m \Vdash_\Sigma \varphi\}) =$
$\mu'(\mathbf{Mod}(\sigma)^{-1}(\{m \in M : m \Vdash_\Sigma \varphi\}) \cap M') =$
$\mu'(\{m' \in M' : \mathbf{Mod}(\sigma)(m') \Vdash_\Sigma \varphi\}) =$
$\mu'(\{m' \in M' : m' \Vdash_{\Sigma'} \mathbf{Sen}(\sigma)(\varphi)\}) = [\![\int\mathbf{Sen}(\sigma)(\varphi)]\!]^{S'} = [\![T^p(\sigma)(\int\varphi)]\!]^{S'}.$

The term $(\int\varphi)$ denotes the probability of φ, interpreted as the probability of the models of the base institution that satisfy φ. The logic resulting from the probabilization of classical propositional logic was carefully studied in [5], where a sound and weak complete calculus could be obtained. The calculus extends the one for the globalization of classical propositional logic by exploring the interplay between the classical connectives and probability, and uses an oracle rule for reasoning with real numbers. Although the logic enjoys the deduction theorem with respect to global implication, strong completeness is out of reach simply because the logic is not compact. Take, for instance, $\Delta = \{(r \leq x) : r < \frac{1}{2}\}$. Clearly, $\Delta \vDash^p_\Sigma (\frac{1}{2} \leq x)$ but no finite subset of Δ does. Another interesting relevant remark is the fact that the operators $\Box$ and $\Diamond$ defined by $(\Box\varphi) \equiv (1 \leq \int\varphi)$ and $(\Diamond\varphi) \equiv \boxminus(\int\varphi \leq 0)$ behave as normal modalities.

In the general case depicted here, however, our aim is to establish the precise relationship between the institutions I, I^g and I^p.

Proposition 3. The triple $C^{gp} = \langle \Phi^{gp}, \alpha^{gp}, \beta^{gp} \rangle$, where Φ^{gp} the identity functor on **Sig**; for each Σ, α^{gp}_Σ translates each $\delta \in \mathbf{Sen}^g(\Sigma)$ to δ; and for each Σ, β^{gp}_Σ translates each $\langle M, P, \rho \rangle \in \mathbf{Mod}^p(\Sigma)$ to $M \in \mathbf{Mod}^g(\Sigma)$, is a comorphism and fulfills the surjectivity condition.

Proof. The naturality of α^{gp} and β^{gp} and the coherence condition are straightforward. As for surjectivity, given a non-empty $M \subseteq \mathbf{Mod}(\Sigma)$ and $m \in M$, take for instance the triple $S = \langle M, \langle \mathcal{B}, \mu \rangle, \rho \rangle$ where $\mathcal{B} = 2^M$, $\mu(B) =$ and ρ is any assignment. Then $\langle \mathcal{B}, \mu \rangle$ is a probability space over M, and $\beta^{gp}_\Sigma(S) = M$. ▹

As a corollary, by Proposition 1 and the observations therein, C^{gp} shows that I^p is a conservative extension of I^g. By transitivity, I^p is also a conservative extension of I. Indeed, by composition, we also obtain a power-model comorphism $C^p = C^{gp} \circ C^g : I \to I^p$ that fulfills the surjectivity condition.

5 Quantum institution

Finally, we turn our attention to the exogenous enrichment of a given logic with quantum reasoning. In order to materialize the key idea of adopting superpositions of models of the given logic as the models of the envisaged quantum logic, let us start by recalling the essential concepts of quantum systems. Let us recall the relevant postulates of quantum physics (following closely [4]) and set up some important mathematical structures.

Postulate 4 *Associated to any isolated quantum system is a Hilbert space. The state of the system is described by a unit vector $|w\rangle$ in the Hilbert space.*

For example, a quantum bit or *qubit* is associated to a Hilbert space of dimension two: a state of a qubit is a vector $\alpha_0|0\rangle + \alpha_1|1\rangle$ where $\alpha_0, \alpha_1 \in \mathbb{C}$ and $|\alpha_0|^2 + |\alpha_1|^2 = 1$. That is, the quantum state is a *superposition* of the two classical states $|0\rangle$ and $|1\rangle$ of a classical bit. Therefore, from a logical point of view, representing the qubit by a propositional constant, a *quantum valuation* is a superposition of the two classical valuations.

Postulate 5 *The Hilbert space associated to a quantum system composed of finitely many independent component systems is the tensor product of the component Hilbert spaces.*

For instance, a system composed of two independent qubits is associated to a Hilbert space of dimension four: a state of such a system is a vector $\alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$ where $\alpha_{00}, \alpha_{10}, \alpha_{01}, \alpha_{11} \in \mathbb{C}$ and $|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1$. Again, representing the two qubits by two propositional constants, a *quantum valuation* is a superposition of the four classical valuations. So, the Hilbert space of the system composed of two independent qubits is indeed the tensor product of the two Hilbert spaces, each corresponding to a single qubit.

Since we want to work with an arbitrary set of qubits, we will need the following general construction. Given a nonempty set E, the *free Hilbert space* over E is $\mathcal{H}(E)$, the *inner product* space over $\mathbb{C}$ defined as follows: each element is a map $|w\rangle : E \to \mathbb{C}$ such that $\{e \in E : |w\rangle(e) \neq 0\}$ is countable, and $\sum_{e\in E} ||w\rangle(e)|^2 < \infty$; addition, scalar multiplication and inner product are defined by $|w_1\rangle + |w_2\rangle = \lambda e.\, |w_1\rangle(e) + |w_2\rangle(e)$, $\alpha|w\rangle = \lambda e.\, \alpha|w\rangle(e)$, and $\langle w_1|w_2\rangle = \sum_{e\in E} |w_1\rangle(e)\overline{|w_2\rangle(e)}$.

As usual, the inner product induces the *norm* $|||w\rangle|| = \sqrt{\langle w|w\rangle}$, which on its turn induces the *distance* $d(|w_1\rangle, |w_2\rangle) = |||w_1\rangle - |w_2\rangle||$. Since $\mathcal{H}(E)$ is complete for this distance, $\mathcal{H}(E)$ is a Hilbert space. Clearly, $\{|e\rangle : e \in E\}$ is an *orthonormal basis* of $\mathcal{H}(E)$, where $|e\rangle(e) = 1$ and $|e\rangle(e') = 0$ for every $e' \neq e$. A *unit vector* of $\mathcal{H}(E)$ is just a vector $|w\rangle \in \mathcal{H}(E)$ such that $|||w\rangle|| = 1$.

Let Q be the set of qubits in hand. If there are no dependencies between the qubits then the system is described by the Hilbert space $\mathcal{H}(2^Q)$, where 2^Q is the set of all classical valuations. However, in many cases, we will be given a finite partition $\mathcal{S} = \{Q_1, \ldots, Q_n\}$ of Q, giving rise to n independent subsystems. In the sequel, we will use $\bigcup \mathcal{S}$ to denote the set $\{\bigcup_{Q_i \in \mathcal{R}} Q_i : \mathcal{R} \subseteq \mathcal{S}\}$. Moreover, it may also be that the qubits Q_i of each isolated subsystem are also constrained and some of the classical valuations in 2^{Q_i} are impossible. Any set $V \subseteq 2^Q$ of *admissible* classical valuations induces a set of admissible classical valuations for each subsystem, that is, $V_i = \{v_i : v \in V\}$ with $v_i = v|_{Q_i}$. Analogously, we will use v_R to denote the restriction $v|_R$ of a valuation v to $R \in \bigcup S$, and $V_R = \{v_R : v \in V\}$. Then, the space describing the corresponding quantum system will be the tensor product $\bigotimes_{i=1}^n \mathcal{H}(V_i)$. Still, note that although $(2^Q)_i = 2^{Q_i}$ and $2^Q = \prod_{i=1}^n 2^{Q_i}$, in general $V \subsetneq \prod_{i=1}^n V_i$. Moreover, although $\mathcal{H}(2^Q) = \bigotimes_{i=1}^n \mathcal{H}(2^{Q_i}) = \bigotimes_{i=1}^n \mathcal{H}(\prod_{i=1}^n 2^{Q_i})$, in general we have that $\mathcal{H}(V) \subsetneq \bigotimes_{i=1}^n \mathcal{H}(V_i) \subsetneq \mathcal{H}(\prod_{i=1}^n V_i)$.

Hence, we should only consider quantum states of $\bigotimes_{i=1}^n \mathcal{H}(V_i)$ that are compatible with V. Given the subspace relations stated above, we shall call a *structured quantum state* over V and $\mathcal{S}$ to a family $|w\rangle = \{|w_i\rangle\}_{i=1}^n$ such that each $|w_i\rangle$ is a unit vector of $\mathcal{H}(V_i)$; and $\langle v|(\bigotimes_{i=1}^n |w_i\rangle) = \prod_{i=1}^n \langle v_i|w_i\rangle = 0$ if $v \notin V$.

Note that it is easy to identify $\bigotimes_{i=1}^n |w_i\rangle$ with a unique unit vector in $\mathcal{H}(V)$ since all the amplitudes on valuations not in V are null. Hence, by abuse of notation, we shall also use $|w\rangle$ to denote $\bigotimes_{i=1}^n |w_i\rangle$.

Now, we turn our attention to the postulates concerning measurements of physical quantities.

Postulate 6 *Every measurable physical quantity of an isolated quantum system is described by an observable*[1] *acting on its Hilbert space.*

Postulate 7 *The possible outcomes of the measurement of a physical quantity are the eigenvalues of the corresponding observable. When the physical quantity is measured using observable A on a system in a state $|w\rangle$, the resulting outcomes are ruled by the probability space* $\mathrm{Prob}^A_{|w\rangle} = \langle \Omega, \mathcal{B}|_\Omega, \mu^A_{|w\rangle}\rangle$ *where in the case of a countable spectrum* $\mu^A_{|w\rangle} = \lambda B. \sum_{\lambda\in\Omega} \chi_B(\lambda)|P_\lambda|w\rangle|^2$.

For the applications we have in mind in quantum computation and information, only *logical projective measurements* are relevant. In general, the stochastic result of making a logical projective measurement of the system at a structured quantum state $|w\rangle$ determined as above is fully described by the probability space $\langle 2^V, \mu_{|w\rangle}\rangle$ over V where $\mu_{|w\rangle}(B) = \sum_{v\in B} |\langle v|w\rangle|^2$ for every $B \subseteq 2^V$.

In the sequel, we will need to be able to map quantum systems and states across qubit maps. Let $f : U \to U'$, $Q \subseteq U$ and $Q' = f[Q]$. Then, the function $f^\bullet : 2^{Q'} \to 2^Q$ defined by $f^\bullet(v')(q) = v'(f(q))$ is injective: if $f^\bullet(v'_1) = f^\bullet(v'_2)$ then, for each $q \in Q$, $v'_1(f(q)) = v'_2(f(q))$, which implies that $v'_1 = v'_2$ since $Q' = f[Q]$. Hence, $f^\bullet$ establishes a bijection between any given set of classical valuations $V' \subseteq 2^{Q'}$ and $V = f^\bullet[V'] \subseteq 2^Q$. Therefore, $f^\bullet$ also establishes an isomorphism between the Hilbert spaces $\mathcal{H}(V')$ and $\mathcal{H}(V)$ obtained my mapping $|w'\rangle \in \mathcal{H}(V')$ to $|w\rangle = f^\bullet(|w'\rangle)$ such that $|w\rangle(f^\bullet(v')) = |w'\rangle(v')$. Moreover, note that every finite partition $\mathcal{S}' = \{Q'_1, \dots, Q'_n\}$ induces a partition $\mathcal{S} = f^{-1}[\mathcal{S}'] = \{Q_1, \dots, Q_n\}$ of Q with each $Q_i = f^{-1}(Q'_i) \cap Q$. Hence, since surjectivity guarantees that each $Q'_i = f[Q_i]$, the Hilbert space isomorphism established in the preceding paragraph by $f^\bullet$ also applies to the subsystems, that is, $\mathcal{H}(V'_i)$ and $\mathcal{H}(V_i)$ are isomorphic.

---

[1] Recall that an observable is a Hermitian operator such that the direct sum of its eigensubspaces coincides with the underlying Hilbert space. Since the operator is Hermitian, its spectrum Ω (the set of its eigenvalues) is a subset of $\mathbb{R}$. For each $\lambda \in \Omega$, we denote the corresponding eigensubspace by E_λ and the projector onto E_λ by P_λ.

We now characterize the exogenous enrichment of a given institution I with quantum reasoning. As in the previous cases, we shall first define the envisaged quantum institution I^q and then characterize its relationship to I, as well as to the institutions previously built. To this end, qubits will be selected formulas of the original logic, that induce upon observation a probability distribution on models of the original institution. The notation I^q is a little abusive here, since the enrichment will be parameterized by a functor that chooses the qubits of interest. Hence, we consider fixed a functor $\mathbf{Qb} : \mathbf{Sig} \to \mathbf{Set}$ such that, for every signature Σ, $\mathbf{Qb}(\Sigma) \subseteq \mathbf{Sen}(\Sigma)$ and, for every signature morphism $\sigma : \Sigma \to \Sigma'$, $\mathbf{Qb}(\sigma) = \mathbf{Sen}(\sigma)|_{\mathbf{Qb}(\Sigma)}$ and $\mathbf{Sen}(\sigma)[\mathbf{Qb}(\Sigma)] = \mathbf{Qb}(\Sigma')$. Note that $\mathbf{Sen}(\sigma)$ is required to be surjective on qubits, and that this requirement is essential in the subsequent development of the I^q institution.

Clearly, models of the given institution induce classical valuations on the qubits. We denote by $V_\Sigma : \mathbf{Mod}(\Sigma) \to 2^{\mathbf{Qb}(\Sigma)}$ defined, for each qubit $\varphi \in \mathbf{Qb}(\Sigma)$, by

$$V_\Sigma(m)(\varphi) = \begin{cases} 1 \text{ if } m \Vdash_\Sigma \varphi \\ 0 \text{ otherwise} \end{cases}.$$

To fulfill the original idea of working with quantum *superpositions* of models of the original institution, we will have to restrict our attention to sets of models $M \subseteq \mathbf{Mod}(\Sigma)$ on which V_Σ is injective, that is, if $m_1, m_2 \in M$ and $m_1 \neq m_2$ then $V_\Sigma(m_1) \neq V_\Sigma(m_2)$. In this way, we have a bijection between M and $V_\Sigma[M]$.

Given $A \subseteq F \subseteq \mathbf{Qb}(\Sigma)$, we shall denote by $v_A^F \in 2^F$ the classical valuation of the qubits in F defined by $v_A^F(\varphi)$ is 1 if $\varphi \in A$ and is 0 otherwise.

The syntax of the logic will also be augmented, not only with probabilistic reasoning, but also in order to allow us to manipulate complex amplitudes and to talk about qubit independence. Hence, besides for the set X of real variables, we also assume fixed a set Z of complex variables.

Definition 8. The *quantum institution* $I^q = \langle \mathbf{Sig}, \mathbf{Sen}^q, \mathbf{Mod}^q, \Vdash^q \rangle$ based on I (and $\mathbf{Qb}$) is defined as follows:

- $\mathbf{Sen}^q(\Sigma)$ is the least set including $\mathbf{Sen}(\Sigma)$ such that: $(\boxminus \delta), (\delta_1 \sqsupset \delta_2) \in \mathbf{Sen}^q(\Sigma)$ if $\delta, \delta_1, \delta_2 \in \mathbf{Sen}^q(\Sigma)$; $[F] \in \mathbf{Sen}^q(\Sigma)$ if $F \subseteq \mathbf{Qb}(\Sigma)$; and $(t_1 \leq t_2) \in \mathbf{Sen}^q(\Sigma)$ if $t_1, t_2 \in T_R^q(\Sigma)$, where the sets $T_R^q(\Sigma)$ and $T_C^q(\Sigma)$ (of *real valued* and *complex valued* terms, respectively) are defined by mutual induction as follows: $X, R \subseteq T_R^q(\Sigma)$; $(\int \varphi) \in T_R^q(\Sigma)$ if $\varphi \in \mathbf{Sen}(\Sigma)$, $(t_1 + t_2), (t_1.t_2) \in T_R^q(\Sigma)$ if $t_1, t_2 \in T_R^q(\Sigma)$, and $\mathrm{Re}(u), \mathrm{Im}(u), \arg(u), |u| \in T_R^q(\Sigma)$ if $u \in T_C^q(\Sigma)$; $Z \subseteq T_C^q(\Sigma)$, $|\top\rangle_{FA} \in T_C^q(\Sigma)$ if $A \subseteq F \subseteq \mathbf{Qb}(\Sigma)$, $(t_1 + it_2), (t_1.e^{it_2}) \in T_C^q(\Sigma)$ if $t_1, t_2 \in T_R^q(\Sigma)$, $\overline{u} \in T_C^q(\Sigma)$ if $u \in T_C^q(\Sigma)$, $(u_1 + u_2), (u_1.u_2) \in T_C^q(\Sigma)$ if $u_1, u_2 \in T_C^q(\Sigma)$, and $(\varphi \rhd u_1; u_2) \in T_C^q(\Sigma)$ if $\varphi \in \mathbf{Sen}(\Sigma)$ and $u_1, u_2 \in T_C^q(\Sigma)$,
- $\mathbf{Sen}^q(\sigma) = \sigma^q$ is defined inductively by: $\sigma^q(\varphi) = \mathbf{Sen}(\sigma)(\varphi)$, $\sigma^q(\boxminus \delta) = (\boxminus \sigma^q(\delta))$, $\sigma^q(\delta_1 \sqsupset \delta_2) = (\sigma^q(\delta_1) \sqsupset \sigma^q(\delta_2))$, $\sigma^q([F]) = [\mathbf{Sen}(\sigma)[F]]$, and $\sigma^q(t_1 \leq t_2) = (T_R^q(\sigma)(t_1) \leq T_R^q(\sigma)(t_2))$, where $T_R^q(\sigma) = \sigma_R^q$ and $T_C^q(\sigma) = \sigma_C^q$ are defined by mutual induction: $\sigma_R^q(x) = x$, $\sigma_R^q(r) = r$, $\sigma_R^q(\int \varphi) = (\int \mathbf{Sen}(\sigma)(\varphi))$, $\sigma_R^q(t_1 + t_2) = (\sigma_R^q(t_1) + \sigma_R^q(t_2))$, $\sigma_R^q(t_1.t_2) = (\sigma_R^q(t_1).\sigma_R^q(t_2))$, $\sigma_R^q(\mathrm{Re}(u)) = \mathrm{Re}(\sigma_C^q(u))$, $\sigma_R^q(\mathrm{Im}(u)) = \mathrm{Im}(\sigma_C^q(u))$, $\sigma_R^q(\arg(u)) = \arg(\sigma_C^q(u))$, $\sigma_R^q(|u|) =$

$|\sigma^q_C(u)|$, $\sigma^q_C(z) = z$, $\sigma^q_C(|\top\rangle_{FA}) = |\top\rangle_{\mathbf{Sen}(\sigma)[F],\mathbf{Sen}(\sigma)[A]}$, $\sigma^q_C(t_1 + it_2) = (\sigma^q_R(t_1) + i\sigma^q_R(t_2))$, $\sigma^q_C(t_1.e^{it_2}) = (\sigma^q_R(t_1).e^{i\sigma^q_R(t_2)})$, $\sigma^q_C(\overline{u}) = \overline{\sigma^q_C(u)}$, $\sigma^q_C(u_1 + u_2) = (\sigma^q_C(u_1) + \sigma^q_C(u_2))$, $\sigma^q_C(u_1.u_2) = (\sigma^q_C(u_1).\sigma^q_C(u_2))$, $\sigma^q_C(\varphi \rhd u_1; u_2) = (\mathbf{Sen}(\sigma)(\varphi) \rhd \sigma^q_C(u_1); \sigma^q_C(u_2))$;

- $\mathbf{Mod}^q(\Sigma)$ is the class of all tuples $\langle M, \mathcal{S}, |w\rangle, \nu, \rho\rangle$ where: $\emptyset \neq M \subseteq \mathbf{Mod}(\Sigma)$ such that V_Σ is injective on M, $\mathcal{S}$ is a finite partition of $\mathbf{Qb}(\Sigma)$, $|w\rangle$ is a structured quantum state over $V_\Sigma[M]$ and $\mathcal{S}$, $\nu = \{\nu_{FA}\}_{A\subseteq F\subseteq \mathbf{Qb}(\Sigma)}$ is a family of complex numbers such that, whenever $F \in \bigcup\mathcal{S}$, $\nu_{FA} = \langle v^F_A | \bigotimes_{Q_i\subseteq F} w_i\rangle$ if $v^F_A \in V_F$, and $\nu_{FA} = 0$ if $v^F_A \notin V_F$, and ρ is an assignment such that $\rho(x) \in \mathbb{R}$ for every $x \in X$, and $\rho(z) \in \mathbb{C}$ for every $z \in Z$;
- $\mathbf{Mod}^q(\sigma)(\langle M', \mathcal{S}', |w'\rangle, \nu', \rho'\rangle) = \langle \mathbf{Mod}(\sigma)[M'], \sigma^{-1}[\mathcal{S}'], \sigma^\bullet(|w'\rangle), \nu, \rho'\rangle$ with $\sigma^\bullet = \mathbf{Sen}(\sigma)^\bullet$, $\sigma^{-1} = \mathbf{Sen}(\sigma)^{-1}$ and $\nu_{FA} = \nu'_{\mathbf{Sen}(\sigma)[F]\mathbf{Sen}(\sigma)[A]}$;
- $\Vdash^q_\Sigma$ is defined inductively by $W \Vdash^q_\Sigma \varphi$ iff $M \Vdash_\Sigma \varphi$, for $\varphi \in \mathbf{Sen}(\Sigma)$, $W \Vdash^q_\Sigma (\boxminus\delta)$ iff $W \nVdash^q_\Sigma \delta$, $W \Vdash^q_\Sigma (\delta_1 \sqsupset \delta_2)$ iff $W \nVdash^q_\Sigma \delta_1$ or $W \Vdash^q_\Sigma \delta_2$, $W \Vdash^q_\Sigma [F]$ iff $F \in \bigcup\mathcal{S}$, and $W \Vdash^q_\Sigma (t_1 \leq t_2)$ iff $[\![t_1]\!]^W_R \leq [\![t_2]\!]^W_R$, where the denotations of real terms $[\![\_]\!]^W_R : T^q_R(\Sigma) \to \mathbb{R}$ and of complex terms $[\![\_]\!]^W_C : T^q_C(\Sigma) \to \mathbb{C}$ are defined by mutual induction as follows: $[\![x]\!]^W_R = \rho(x)$, for $x \in X$, $[\![r]\!]^W_R = r$, for $r \in R$, $[\![\int\varphi]\!]^W_R = \mu_{|w\rangle}(V_\Sigma[\{m \in M : m \Vdash_\Sigma \varphi\}])$, $[\![t_1 + t_2]\!]^W_R = [\![t_1]\!]^W_R + [\![t_2]\!]^W_R$, $[\![t_1.t_2]\!]^W_R = [\![t_1]\!]^W_R.[\![t_2]\!]^W_R$, $[\![\mathrm{Re}(u)]\!]^W_R = \mathrm{Re}([\![u]\!]^W_C)$, $[\![\mathrm{Im}(u)]\!]^W_R = \mathrm{Im}([\![u]\!]^W_C)$, $[\![\arg(u)]\!]^W_R = \arg([\![u]\!]^W_C)$, and $[\![|u|]\!]^W_R = |[\![u]\!]^W_C|$, $[\![z]\!]^W_C = \rho(z)$, for $z \in Z$, $[\![|\top\rangle_{FA}]\!]^W_C = \nu_{FA}$, $[\![t_1 + it_2]\!]^W_C = [\![t_1]\!]^W_R + i[\![t_2]\!]^W_R$, $[\![t_1.e^{it_2}]\!]^W_C = [\![t_1]\!]^W_R.e^{i[\![t_2]\!]^W_R}$, $[\![\overline{u}]\!]^W_C = \overline{[\![u]\!]^W_C}$, $[\![u_1 + u_2]\!]^W_C = [\![u_1]\!]^W_C + [\![u_2]\!]^W_C$, $[\![u_1.u_2]\!]^W_C = [\![u_1]\!]^W_C.[\![u_2]\!]^W_C$, and $[\![\varphi \rhd u_1; u_2]\!]^W_C = \begin{cases} [\![u_1]\!]^W_C & \text{if } M \Vdash_\Sigma \varphi \\ [\![u_2]\!]^W_C & \text{otherwise} \end{cases}$.

I^q is an institution. Indeed the functoriality of $\mathbf{Sen}^q$ is straightforward. Concerning $\mathbf{Mod}^q$, and given a signature morphism $\sigma : \Sigma \to \Sigma'$, note that indeed $W = \langle M, |w\rangle, \nu, \rho\rangle = \mathbf{Mod}^q(\sigma)(W') \in \mathbf{Mod}^q(\Sigma)$ if $W' = \langle M', |w'\rangle, \nu', \rho'\rangle \in \mathbf{Mod}^q(\Sigma')$. In particular, since $M = \mathbf{Mod}(\sigma)[M']$, then $\mathbf{Sen}(\sigma)^\bullet[V_{\Sigma'}[M']] = V_\Sigma[M]$ just because $V_\Sigma(\mathbf{Mod}(\sigma)(m'))(\varphi) = V_{\Sigma'}(m')(\mathbf{Sen}(\sigma)(\varphi))$ for every $m' \in \mathbf{Mod}(\Sigma')$ and $\varphi \in \mathbf{Qb}(\Sigma)$, due to the satisfaction condition of the original institution. Moreover, if $A \subseteq F \subseteq \mathbf{Qb}(\Sigma)$, and we let $F' = \mathbf{Sen}(\sigma)[F]$ and $A' = \mathbf{Sen}(\sigma)[A]$, the definition of $\nu_{FA} = \nu'_{F'A'}$ is suitable. First note that $v^{F'}_{A'} \in V_{\Sigma'}[M']$ iff $v^F_A \in V_\Sigma[M]$ just because $\mathbf{Sen}(\sigma)^\bullet(v^{F'}_{A'}) = v^F_A$. Moreover, $F \in \bigcup\mathcal{S}$ iff $F' \in \bigcup\mathcal{S}'$.

The satisfaction condition of I^q can be established by a simple induction on formulas and on terms. The only interesting cases concern independence formulas $[F]$, plus probability $(\int\varphi)$ and amplitude $|\top\rangle_{FA}$ terms. In the first case, we need to show that $W \Vdash^q_\Sigma [F]$ iff $W' \Vdash^q_{\Sigma'} [F']$. The result follows immediately because $F \in \cup\mathcal{S}$ iff $\mathbf{Sen}(\sigma)[F] \in \cup\mathcal{S}'$. In the second case, we need to show that $[\![\int\varphi]\!]^W_R = [\![\int\mathbf{Sen}(\sigma)(\varphi)]\!]^{W'}_R$. Indeed, using the bijection between M and $V_\Sigma[M]$, the fact that $M = \mathbf{Mod}(\sigma)[M']$, the satisfaction condition of the institution I, and as a result the fact that $\mathbf{Sen}(\sigma)^\bullet(V_{\Sigma'}(m')) = V_\Sigma(\mathbf{Mod}(\sigma)(m'))$, we have that

$[\![\int\varphi]\!]_R^W = \mu_{|w\rangle}(V_\Sigma[\{m \in M : m \Vdash_\Sigma \varphi\}]) =$
$\sum_{m\in M:m\Vdash_\Sigma\varphi} |\langle V_\Sigma(m)|w\rangle|^2 = \sum_{m\in M:m\Vdash_\Sigma\varphi} ||w\rangle(V_\Sigma(m))|^2 =$
$\sum_{m\in M:m\Vdash_\Sigma\varphi} |\mathbf{Sen}(\sigma)^\bullet(|w'\rangle)(V_\Sigma(m))|^2 =$
$\sum_{m'\in M':m'\Vdash_{\Sigma'}\mathbf{Sen}(\sigma)(\varphi)} |\mathbf{Sen}(\sigma)^\bullet(|w'\rangle)(\mathbf{Sen}(\sigma)^\bullet(V_{\Sigma'}(m')))|^2 =$
$\sum_{m'\in M':m'\Vdash_{\Sigma'}\mathbf{Sen}(\sigma)(\varphi)} ||w'\rangle(V_{\Sigma'}(m'))|^2 =$
$\sum_{m'\in M':m'\Vdash_{\Sigma'}\mathbf{Sen}(\sigma)(\varphi)} |\langle V_{\Sigma'}(m')|m'\rangle|^2 =$
$\mu_{|w'\rangle}(V_{\Sigma'}[\{m' \in M' : m' \Vdash_{\Sigma'} \mathbf{Sen}(\sigma)(\varphi)\}]) = [\![\int\mathbf{Sen}(\sigma)(\varphi)]\!]_R^{W'}$.

In the third case, we need to show that $[\![|\top\rangle_{FA}]\!]_R^W = [\![|\top\rangle_{F'A'}]\!]_R^W$. Since we already know that $F \in \bigcup\mathcal{S}$ iff $F' \in \bigcup\mathcal{S}'$, and that $v_{A'}^{F'} \in V_{\Sigma'}[M']$ iff $v_A^F \in V_\Sigma[M]$, it suffices to verify that, when it makes sense,
$\langle v_A^F|(\bigotimes_{Q_i\subseteq F}|w_i\rangle) = \prod_{Q_i\subseteq F}\langle (v_A^F)_{Q_i}|w_i\rangle = \prod_{Q_i\subseteq F} ||w_i\rangle((v_A^F)_{Q_i})|^2 =$
$\prod_{Q_i\subseteq F} |\mathbf{Sen}(\sigma)^\bullet(|w_i'\rangle)(\mathbf{Sen}(\sigma)^\bullet((v_{A'}^{F'})_{Q_i'}))|^2 = \prod_{Q_i'\subseteq F'} ||w_i'\rangle((v_{A'}^{F'})_{Q_i'})|^2 =$
$\prod_{Q_i'\subseteq F'}\langle (v_{A'}^{F'})_{Q_i'}|w_i'\rangle = \langle v_{A'}^{F'}|(\bigotimes_{Q_i'\subseteq F'}|w_i'\rangle)$.

Most of the syntactic constructions introduced in I^q are self explanatory. The quantum specific constructs, besides all the operations on complex numbers, are the $[F]$ formulas and the $|\top\rangle_{FA}$ terms. Intuitively, $[F]$ holds if the qubits in F form an independent subsystem of the whole, whereas $|\top\rangle_{FA}$ evaluates, whenever it is meaningful, to the complex amplitude of the vector $|v_A^F\rangle$ in the current state of the systems. The logic resulting from the quantization of classical propositional logic was introduced and studied in [1, 2]. A sound and weak complete calculus for the logic was obtained in [3] using an iterated Henkin construction inspired by the technique in [13]. The qubits of interest in this case were the propositional symbols. Using the logic it is possible, for instance, to model and reason about quantum states corresponding to the famous case of Schrödinger's cat. The relevant attributes of the cat are **cat-in-box**, **cat-alive**, **cat-moving** being inside or outside the box, alive or dead, and moving, respectively. The following formulas constrain the state of the cat at different levels of detail:

1. [**cat-in-box**, **cat-alive**, **cat-moving**];
2. (**cat-moving** $\Rightarrow$ **cat-alive**);
3. (($\Diamond$ **cat-alive**) $\sqcap$ ($\Diamond$ ($\neg$ **cat-alive**)));
4. ($\boxminus$[**cat-alive**]);
5. ($\int$**cat-alive** $= \frac{1}{3}$).

Observe that the assertions are jointly consistent. They characterize the quantum states where: the qubits **cat-in-box**, **cat-alive**, **cat-moving** are not entangled with other qubits; the cat is moving only if it is alive; it is possible that the cat is alive and also that the cat is dead; the qubit **cat-alive** is entangled with the others; and the probability of observing the cat alive (after collapsing the wave function) is $\frac{1}{3}$. Our aim is now to relate I^q with I, I^g, I^p.

Proposition 4. The triple $C^{pq} = \langle \Phi^{pq}, \alpha^{pq}, \beta^{pq}\rangle$, where Φ^{pq} the identity functor on **Sig**; for each Σ, α_Σ^{pq} translates each $\delta \in \mathbf{Sen}^p(\Sigma)$ to δ; and for each Σ, β_Σ^{pq}

translates each $\langle M, \mathcal{S}, |w\rangle, \nu, \rho\rangle \in \mathbf{Mod}^q(\Sigma)$ to $\langle M, \langle 2^M, \mu\rangle, \rho|_X\rangle$ with $\mu(B) = \mu_{|w\rangle}(V_\Sigma[B])$, is a comorphism $C^{pq} : I^p \to I^q$.

Proof. The naturality of the transformation α^{pq} is straightforward. Concerning β^{pq} just note that given $W = \langle M, \mathcal{S}, |w\rangle, \nu, \rho\rangle \in \mathbf{Mod}^q(\Sigma)$, $\beta^{pq}(W)$ is well defined. The probability space $\langle 2^M, \mu\rangle$ over M is just an isomorphic copy of $\langle 2^{V_\Sigma[M]}, \mu_{|w\rangle}\rangle$ over $V_\Sigma[M]$. It is clearly a probability space, and its naturality follows easily. The coherence condition is trivial. ▹

Note however that, in general, C^{pq} does not satisfy the surjectivity condition, and thus I^q is not a conservative extension of I^p. This happens for two essential reasons: first, the sets M of models that appear in quantum models must be in one-to-one correspondence with their induced classical valuations on the qubits; second, even for such an M, due to the independence partitions, not all probability spaces over M can be obtained from a quantum structure. Of course, by composition, we also obtain a comorphism $C^{gq} = C^{pq} \circ C^{gp} : I^g \to I^q$, and a power-model comorphism $C^q = C^{pq} \circ C^p : I \to I^q$. It is very easy to check that C^q meets the necessary surjectivity condition, and therefore I^q is still a conservative extension of I. Given Σ, and a model m of I, we just need to consider any quantum structure of the form $\langle \{m\}, \{\mathbf{Qb}(\Sigma)\}, 1|V_\sigma(m)\rangle, \nu, \rho\rangle$ with $\nu_{FA} = 1$ if $F = \mathbf{Qb}(\Sigma)$ and $v^F_A = V_\sigma(m)$, or $F = \emptyset$, and $\nu_{FA} = 0$ otherwise. On the other hand, it is easy to see that also C^{gq} will be surjective, and hence I^q a conservative extension of I^g, whenever the first of the above mentioned restrictions is trivial. That is, requiring that M is in one-to-one correspondence with its induced set of valuations should not exclude any possible set of models. For this condition to hold, it suffices to require that the qubit functor $\mathbf{Qb}$ is chosen in such a way that, for each Σ and $m_1, m_2 \in \mathbf{Mod}(\Sigma)$, if m_1 and m_2 coincide on the satisfaction of all qubits then $m_1 = m_2$. If the qubits are *representative* typically one ends up with logically equivalent models, but in many institutions it is possible to avoid having logically equivalent models. The case of classical propositional logic is paradigmatic, once we take as qubits all the propositional symbols. But similar choices are possible in many other logics. In [23] it is shown how to do this choice in any suitable finitely-valued logic. For instance, in Lukasiewicz's three-valued logic it suffices to consider as qubits all propositional symbols and negations of propositional symbols. This possibility also helps in shedding light on the usefulness of considering restricted sets of admissible valuations.

6 Conclusion

Figure 1 is the diagram of the institutions and (power-model) comorphisms we have built, where $\rightarrowtail$ is used to distinguish the arrows that guarantee a conservative extension from their source to target. Our main goal in bringing into the realm of institutions the exogenous approach to globalization, probabilization and quantization of logics was to assess how general these constructions were. The first two constructions are fully general, in the sense that nothing is assumed about the given institution and also that nothing else is needed. But quantization

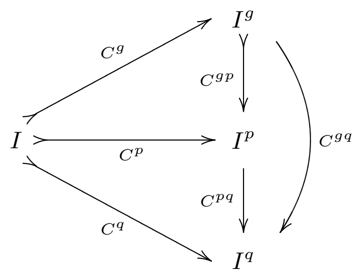

Fig. 1. Institutions and (power-model) comorphisms.

requires some additional information (the choice of qubit formulae). On the other hand, the quantum logic, as pointed out by the institutional approach, is not general enough (namely, injectivity of V_Σ on models, and surjectivity of the qubit translations). The solution seems to suggest a slight generalization of the exogenous approach towards working with multisets of models (as in Kripke structures), a promising line of further development of the approach. Furthermore, many interesting institution-theoretic questions remain open about these logics and the construction mechanisms discussed herein, like analyzing the properties of the constructions as functors on the category of institutions (or better, on some category of institutions), studying the underlying categories of models, and study their impact on the properties of the resulting categories of specifications. From a logic-theoretic point of view, the next step is to attempt at extending the completeness results in [5, 3] for a general base institution.

Acknowledgments

This work was partially supported by FCT and FEDER through POCI, namely via the QuantLog POCI/MAT/55796/2004 Project of CLC. The authors wish to express their gratitude to the regular participants in the QCI Seminar. Till Mossakowski deserves a special acknowledgment due to his prompt will to serve as an oracle on any question related to institutions and their notions of arrow. Last, but not least, we are all much indebted to Joseph Goguen for many inspirational discussions on institutions in particular, and the world at large, over the last two decades.

References

1. Mateus, P., Sernadas, A.: Exogenous quantum logic. In Carnielli, W.A., Dionísio, F.M., Mateus, P., eds.: Proceedings of CombLog'04, Workshop on Combination of Logics: Theory and Applications, 1049-001 Lisboa, Portugal, Departamento de Matemática, Instituto Superior Técnico (2004) 141–149 Extended abstract.

2. Mateus, P., Sernadas, A.: Reasoning about quantum systems. In Alferes, J., Leite, J., eds.: Logics in Artificial Intelligence, JELIA'04. Volume 3229 of Lecture Notes in Artificial Intelligence. Springer-Verlag (2004) 239–251
3. Mateus, P., Sernadas, A.: Weakly complete axiomatization of exogenous quantum propositional logic. Information and Computation (in print) ArXiv math.LO/0503453.
4. Nielsen, M.A., Chuang, I.L.: Quantum Computation and Quantum Information. Cambridge University Press (2000)
5. Mateus, P., Sernadas, A., Sernadas, C.: Exogenous semantics approach to enriching logics. In Sica, G., ed.: Essays on the Foundations of Mathematics and Logic. Volume 1 of Advanced Studies in Mathematics and Logic. Polimetrica (2005) 165–194
6. Foulis, D.J.: A half-century of quantum logic. What have we learned? In: Quantum Structures and the Nature of Reality. Volume 7 of Einstein Meets Magritte. Kluwer Acad. Publ. (1999) 1–36
7. Chiara, M.L.D., Giuntini, R., Greechie, R.: Reasoning in Quantum Theory. Kluwer Academic Publishers (2004)
8. Birkhoff, G., von Neumann, J.: The logic of quantum mechanics. Annals of Mathematics **37** (1936) 823–843
9. Nilsson, N.J.: Probabilistic logic. Artificial Intelligence **28** (1986) 71–87
10. Nilsson, N.J.: Probabilistic logic revisited. Artificial Intelligence **59** (1993) 39–42
11. Bacchus, F.: Representing and Reasoning with Probabilistic Knowledge. MIT Press Series in Artificial Intelligence. MIT Press (1990)
12. Bacchus, F.: On probability distributions over possible worlds. In: Uncertainty in Artificial Intelligence, 4. Volume 9 of Machine Intelligence and Pattern Recognition. North-Holland (1990) 217–226
13. Fagin, R., Halpern, J.Y., Megiddo, N.: A logic for reasoning about probabilities. Information and Computation **87** (1990) 78–128
14. Dishkant, H.: Semantics of the minimal logic of quantum mechanics. Studia Logica **30** (1972) 23–32
15. Goguen, J., Burstall, R.: A study in the foundations of programming methodology: specifications, institutions, charters and parchments. In: Category Theory and Computer Programming. Volume 240 of LNCS. Springer (1986) 313–333
16. Goguen, J., Burstall, R.: Institutions: abstract model theory for specification and programming. Journal of the ACM **39** (1992) 95–146
17. Goguen, J., Roşu, G.: Institution morphisms. Formal Aspects of Computing **13** (2002) 274–307
18. Meseguer, J.: General logics. In: Proceedings of the Logic Colloquium'87. North-Holland (1989) 275–329
19. Tarlecki, A.: Moving between logical systems. In: Recent Trends in Data Type Specification. Volume 1130 of LNCS. Springer (1996) 478–502
20. Mossakowski, T.: Different types of arrow between logical frameworks. In auf der Heide, F.M., Monien, B., eds.: Procs. ICALP'96. Volume 1099 of LNCS. Springer (1996) 158–169
21. Cerioli, M., Meseguer, J.: May I borrow your logic? (Transporting logical structures along maps). Theoretical Computer Science **173** (1997) 311–347
22. Bridges, D.S.: Computability. Volume 146 of Graduate Texts in Mathematics. Springer-Verlag (1994)
23. Caleiro, C., Carnielli, W.A., Coniglio, M.E., Marcos, J.: Two's company: "The humbug of many logical values". In Béziau, J.Y., ed.: Logica Universalis. Birkhäuser Verlag (2005) 169–189