Fibred Coalgebraic Logic and Quantum Protocols

Daniel Marsden
Department of Computer Science
University of Oxford
daniel.marsden@cs.ox.ac.uk

Motivated by applications in modelling quantum systems using coalgebraic techniques, we introduce a fibred coalgebraic logic. Our approach extends the conventional predicate lifting semantics with additional modalities relating conditions on different fibres. As this fibred setting will typically involve multiple signature functors, the logic incorporates a calculus of modalities enabling the construction of new modalities using various composition operations. We extend the semantics of coalgebraic logic to this setting, and prove that this extension respects behavioural equivalence.

We show how properties of the semantics of modalities are preserved under composition operations, and then apply the calculational aspect of our logic to produce an expressive set of modalities for reasoning about quantum systems, building these modalities up from simpler components. We then demonstrate how these modalities can describe some standard quantum protocols. The novel features of our logic are shown to allow for a uniform description of unitary evolution, and support local reasoning such as "Alice's qubit satisfies condition φ" as is common when discussing quantum protocols.

1 Introduction

In [1] a coalgebraic model of quantum systems was constructed using a novel fibrational structure to introduce "enough contravariance" to represent the important physical symmetries of a quantum system. The paper then raised the question of what a suitable "fibred coalgebraic logic" would look like, and that is the question we address in this paper.

In the first half of the paper we propose an extension of coalgebraic logic based upon predicate liftings [12, 14] (see also the excellent introduction [13]) which provides a convenient setting in which to produce practical modal logics in a lightweight manner. New types of modalities are introduced that allow explicit reasoning between different fibres, and composition operations are provided to build modalities from simpler components. In the second half of the paper we exploit the calculational aspects of our logic to construct modalities suitable for reasoning about quantum protocols. The new features of our logic provide mechanisms for describing important features such as unitary evolution, restriction to subsystems and local measurements. Finally, we illustrate these features by applying them to two standard quantum protocols.

Fibred constructions involving coalgebras are also considered in [7] and [6], in order to capture parameterization of signature functors. The question of fibred coalgebraic logic using predicate liftings is explored in the later paper, but primarily from the perspective of the relationship to the logical structure of institutions [3] and this question is further pursued in [11]. In contrast to the work in this paper, the logic discussed in these papers is exactly a conventional coalgebraic logic in each fibre, and the relationship between the fibres does not appear directly in the syntax of the logic. In [9] a pseudo coalgebraic setting was introduced for modelling quantum systems, in order to develop the representation result of [1] in a simpler and more easily motivated setting. A coalgebraic logic was discussed in this setting, supporting a single signature functor and modalities induced by its natural isomorphisms.

M.J. Hoban, B. Coecke (Eds.): 10th International
Workshop on Quantum Physics and Logic (QPL 2013)
EPTCS 171, 2014, pp. 90–99, doi:10.4204/EPTCS.171.9

2 Fibred Coalgebraic Logic

Each fibre of our modal logic will correspond to a different signature functor. A fibred signature will describe a basic set of modalities that are available on each fibre.

Definition 2.1 (Modal Signature)**.** A **modal signature** Λ is a set of modality symbols, each with an associated cardinal referred to as the arity of the modality.

Definition 2.2 (Fibred Modal Signature)**.** A **fibred modal signature** Φ is a small monoidal category $\mathscr{C}^{\Phi}$ and for each object A in $\mathscr{C}^{\Phi}$ an associated modal signature Λ_A^{Φ}. For each pair of objects A, B with $A \neq B$ we require that $\Lambda_A^{\Phi} \cap \Lambda_B^{\Phi} = \emptyset$.

Given the basic set of modalities provided by the fibred modal signature, additional modalities can be constructed via various composition operations.

Definition 2.3 (Modality Expressions)**.** Let Φ be a fibred modal signature. We inductively define a typed language of **modality expressions**, with conjunctions bounded by a maximum cardinality κ.

We have one introduction rule:

$$\frac{\Box_\lambda \in \Lambda_A^{\Phi} \text{ with arity } \alpha}{\Box_\lambda : A^\alpha \to A}$$

We can apply logical operations to modality expressions:

$$\frac{\bigcirc : A^\alpha \to A}{\neg\bigcirc : A^\alpha \to A}$$

$$\frac{0 < \text{card}(I) < \kappa \text{ and } \bigcirc_i : A^\alpha \to A \text{ for each } i \in I}{\bigwedge_{i\in I} \bigcirc_i : A^\alpha \to A}$$

We have 2 rules for constructing new modality expressions by composition:

$$\frac{\bigcirc_1 : A^\alpha \to A \qquad \bigcirc_2 : B \to B}{\bigcirc_2 \lhd \bigcirc_1 : (B \otimes A)^\alpha \to (B \otimes A)} \qquad \frac{\bigcirc : B^\alpha \to B \qquad f \in \mathscr{C}^{\Phi}(A,B)}{\bigcirc^f : A^\alpha \to A}$$

The formulae applicable on each fibre are described by mutual induction, allowing the application of appropriate modality expressions as modalities:

Definition 2.4 (Syntax and Typing)**.** For a fibred modal signature Φ we now define a language of typed formulae. We write $\varphi : A$ for formula φ is of type A, in which case we will refer to φ as an A-**formula**.

Our language is defined inductively by the following rules, starting with the typing rules for standard logical connectives for A an object in $\mathscr{C}^{\Phi}$:

$$\frac{}{\top^A : A} \qquad \frac{\varphi : A}{\neg\varphi : A} \qquad \frac{\varphi_i : A \text{ for each } i \in I \text{ and } 0 < \text{card}(I) < \kappa}{\bigwedge(\varphi_i)_{i\in I} : A}$$

We have two application rules for the different types of modalities:

$$\frac{\varphi : B \qquad f \in \mathscr{C}^{\Phi}(A,B)}{f\varphi : A} \qquad \frac{\varphi_i : A \text{ for each } i \in \alpha \qquad \bigcirc : A^\alpha \to A}{\bigcirc(\varphi_i)_{i\in\alpha} : A}$$

Modalities of the form f for f a $\mathscr{C}^\Phi$ morphism will be referred to as **adaptation modalities**. These modalities permit lifting of subformulae from different fibres in a suitable manner.

We will write $\mathscr{L}^\Phi_\kappa$ for the formulae with conjunctions of cardinality at most κ and $\mathscr{L}^\Phi_\kappa(A)$ for the A-formulae with conjunctions of cardinality at most κ.

Remark 2.5. The category $[\mathbf{Set},\mathbf{Set}]$ of endofunctors on **Set** and natural transformations between them can be given the structure of a strict monoidal category, with the tensor given by functor composition.

Definition 2.6. We will write $2 : \mathbf{Set}^{\mathbf{op}} \to \mathbf{Set}$ for the contravariant powerset functor. Define natural transformation $\neg : 2 \Rightarrow 2$ on components as:

$$\neg_X(U) := X \setminus U \tag{1}$$

For each set I define natural transformation $\bigwedge : 2^I \Rightarrow 2$ on components as:

$$\bigwedge_X((X_i)_{i\in I}) := \bigcap_{i\in I} X_i \tag{2}$$

The semantics for our logic are described by providing a structure identifying types with signature functors, and the morphisms between types as suitable natural transformations. The tensor product then corresponds to the composition of signature functors.

Definition 2.7 (Structure)**.** For a given fibred modal signature Φ, a **Φ-structure** S is a strict monoidal functor $[\![-]\!]^S : \mathscr{C}^\Phi \to [\mathbf{Set},\mathbf{Set}]$, and for each object A in $\mathscr{C}^\Phi$ and modality $\Box_\lambda$ in Λ^Φ_A of arity α an associated natural transformation $[\![\Box_\lambda]\!]^S : 2^\alpha \Rightarrow 2 \circ [\![A]\!]^S$, referred to as a **predicate lifting** of arity α.

Remark 2.8. For a given fibred monoidal signature Φ, the category $\mathscr{C}^\Phi$ will often be a monoidal subcategory of $[\mathbf{Set},\mathbf{Set}]$, with the functor $[\![-]\!] : \mathscr{C}^\Phi \to [\mathbf{Set},\mathbf{Set}]$ given by the inclusion. In later sections we will often identify the two when this is assumed to be the case.

Definition 2.9 (Modality Expression Semantics)**.** The semantics of modality expressions are given by suitable predicate liftings. Let Φ be a fibred modal signature and S a Φ-structure. Assume that α is a cardinal, A,B are objects of $\mathscr{C}^\Phi$, $\Box_\lambda \in \Lambda^\Phi_A$, $f : B \to A$ is a $\mathscr{C}^\Phi$ morphism, $\bigcirc : A^\alpha \to A$, for each $i \in I$ $\bigcirc_i : A^\alpha \to A$ and $\bigcirc' : B \to B$. The semantics for modality expressions are given inductively as follows:

$$[\![\Box_\lambda]\!] := [\![\Box_\lambda]\!]^S \tag{3}$$

$$[\![\neg\bigcirc]\!] := (\neg * [\![A]\!]^S) \circ [\![\bigcirc]\!] \tag{4}$$

$$[\![\bigwedge_{i\in I} \bigcirc_i]\!] := (\bigwedge * [\![A]\!]^S) \circ \langle [\![\bigcirc_i]\!] \mid i \in I\rangle \tag{5}$$

$$[\![\bigcirc^f]\!] := (2 * [\![f]\!]^S) \circ [\![\bigcirc]\!] \tag{6}$$

$$[\![\bigcirc' \lhd \bigcirc]\!] := ([\![\bigcirc']\!] * [\![A]\!]^S) \circ [\![\bigcirc]\!] \tag{7}$$

Above $\circ$ and $*$ denote vertical and horizontal composition of natural transformations respectively.

Definition 2.10 (Semantics of A-formulae)**.** Let Φ be a fibred modal signature and S a Φ-structure. Assume α is a cardinal, A is an object of $\mathscr{C}^\Phi$, $\bigcirc : A^\alpha \to A$ is a modality expression, and $f : A \to B$ a $\mathscr{C}^\Phi$ morphism. The semantics for a formula $\varphi : A$, is given inductively for $[\![A]\!]$-coalgebra (X,γ) as follows:

$$[\![\top^A]\!]_{X,\gamma} := X \tag{8}$$

$$[\![\neg\varphi]\!]_{X,\gamma} := X \setminus [\![\varphi]\!]_{X,\gamma} \tag{9}$$

$$[\![\bigwedge(\varphi_i)_{i\in I}]\!]_{X,\gamma} := \bigcap_{i\in I} [\![\varphi_i]\!]_{X,\gamma} \tag{10}$$

$$[\![\bigcirc(\varphi_i)_{i\in\alpha}]\!]_{X,\gamma} := \gamma^{-1} \circ [\![\bigcirc]\!]_X([\![\varphi_i]\!]_{X,\gamma})_{i\in\alpha}) \tag{11}$$

$$[\![f\varphi]\!]_{X,\gamma} := [\![\varphi]\!]_{X,[\![f]\!]^S_X \circ \gamma} \tag{12}$$

Remark 2.11. The obvious relationships hold between logical operations on modality expressions and logical operations on formulae. Also the logical operations commute appropriately with adaption modalities. We will not need these properties for our examples, so the details are omitted.

We now define a translation that will produce an equivalent formula with adaptation modalities removed. This will allow use to reduce questions in the extended syntax to questions in the well understood setting of coalgebraic logic with predicate liftings.

Definition 2.12 (Translation)**.** For a given fibred modal signature Φ, for $f : A \to B$ in $\mathscr{C}^{\Phi}$, define the syntax translation τ_f as follows:

$$\tau_f(\top^B : B) := \top^A : A \tag{13}$$
$$\tau_f(\neg\varphi : B) := \neg\tau_f(\varphi) : A \tag{14}$$
$$\tau_f(\bigwedge(\varphi_i)_{i\in I} : B) := \bigwedge(\tau_f(\varphi_i))_{i\in I} : A \tag{15}$$
$$\tau_f(\bigcirc(\varphi_i)_{i\in\alpha} : B) := \bigcirc^f(\tau_f(\varphi_i))_{i\in\alpha} : A \tag{16}$$
$$\tau_f(f'\varphi : B) := \tau_{f'\circ f}(\varphi) : A \tag{17}$$

Proposition 2.13. *For a given fibred modal signature Φ and Φ-structure, for $f : A \to B$ in $\mathscr{C}^{\Phi}$:*

$$[\![\varphi]\!]_{X,[\![f]\!]_X\circ\gamma} = [\![\tau_f(\varphi)]\!]_{X,\gamma} \tag{18}$$

Theorem 2.14. *The semantics of fibred coalgebraic logic respects behavioural equivalence.*

Proof. By setting f to the identity in proposition 2.13 we get:

$$[\![\varphi]\!]_{X,\gamma} = [\![\tau_1(\varphi)]\!]_{X,\gamma} \tag{19}$$

So the semantics of fibred coalgebraic logic is equivalent to the semantics of suitable formulae in standard coalgebraic logic with predicate liftings, and this respects behavioural equivalence. □

Example 2.15 (Simple combination of modality expressions)**.** For a unary functor $F : \mathbf{Set} \to \mathbf{Set}$, and arbitrary set A, for each $a \in A$ we have an obvious evaluation natural transformation $ev^a : F(-)^A \Rightarrow F(-)$.

Now for signature functor $\mathscr{P}$ (the powerset functor), giving Kripke frames as coalgebras, the semantics of the usual $\Box$ modality is given by the following predicate lifting:

$$[\![\Box]\!]_X(U) := \mathscr{P}(U) \tag{20}$$

If we consider the signature functor $\mathscr{P}(-)^A$ for (unbounded) labelled transition systems, the usual $\Box_a$ modality can be constructed as the modality expression $\Box^{ev^a}$

2.1 Semantics of Modality Expressions

In this section we consider some properties of predicate liftings such as monotonicity, continuity and being a separating set, and how this is preserved under some of the composition operations described in section 2. We restrict our attention to unary predicate liftings to simplify the presentation.

Lemma 2.16. *Let Φ be a fibred modal signature and S be a Φ-structure. Let $\bigcirc : A \to A$ and $\bigcirc' : B \to B$ be modality expressions. Then if $[\![\bigcirc]\!]$ and $[\![\bigcirc']\!]$ are monotone (continuous) then $[\![\bigcirc' \lhd \bigcirc]\!]$ is monotone (continuous).*

Lemma 2.17. *Let Φ be a fibred modal signature and S a Φ-structure. Let $\bigcirc : A \to A$ be a modality expression and $f : B \to A$ a $\mathscr{C}^\Phi$ morphism. Then if $[\![\bigcirc]\!]$ is monotone (continuous) then $[\![\bigcirc^f]\!]$ is monotone (continuous).*

We now consider how expressive sets of predicate liftings are preserved under various operations. Results of this type are known and described in [10]. We provide some results here for completeness and in a form suitable for application in later examples.

Expressivity can be lifted to products and exponentials from a fixed domain.

Lemma 2.18. *Let Φ be a fibred modal signature and S a Φ-structure. Let $(A_i)_{i\in I}$ be a family of objects in $\mathscr{C}^\Phi$. Assume $[\![A]\!]^S = \prod_{i\in I}[\![A_i]\!]^S$ and that there exist $\mathscr{C}^\Phi$ morphisms $(\pi^i : A \to A_i)_{i\in I}$ such that $[\![\pi^i]\!]^S$ is the corresponding projection natural transformation. For each $i \in I$ let $([\![\bigcirc_{i,j}]\!])_{j\in J_i}$ be a separating set of predicate liftings for $[\![A_i]\!]^S$. Then the predicate liftings $([\![\bigcirc_{i,j}^{\pi_i}]\!])_{i\in I, j\in J}$ are separating for $[\![A]\!]^S$.*

Lemma 2.19. *Let Φ be a fibred modal signature and S a Φ-structure. Let A, B be an objects in $\mathscr{C}^\Phi$ with $[\![B]\!] = [\![A]\!]^A$. Also let $(ev^a : B \to A)_{a\in A}$ be $\mathscr{C}^\Phi$ morphisms such that $[\![ev^a]\!]$ is the corresponding evaluation natural transformation as defined in example 2.15. Let $([\![\bigcirc_i]\!])_{i\in I}$ be a separating set of predicate liftings for $[\![A]\!]^S$. Then the predicate liftings $([\![\bigcirc_i^{ev^a}]\!])_{i\in I, a\in A}$ are separating for $[\![B]\!]^S$.*

In general if we have separating sets of predicate liftings for two endofunctors, they do not combine (in any way) to give a separating set for the composite functor. This is easily seen as, for example, the functor $\mathscr{P}_\omega$ has a separating set of liftings, but no separating set exists for $\mathscr{P}_\omega \circ \mathscr{P}_\omega$. (See parts of (1) and (5) of example 23 in [14]). We examine a simple common case that we will require later, in which the behaviour is much better. The following notions will be useful:

Definition 2.20. Let T : **Set** $\to$ **Set** be an endofunctor. Consider a set of predicate liftings $\{\lambda^i\}$.

- The liftings are said to **separate by singletons** if for an arbitrary set X, and $x, y \in T(X)$, it is sufficient to consider the image of singleton sets under the λ^i to separate x and y.
- The liftings are said to be **mutually surjective on singletons** if for an arbitrary set X and each $t \in TX$ the singleton set $\{t\}$ is in $\mathrm{im}(\lambda^i_X)$ for some λ^i.

Lemma 2.21. *For endofunctor T : **Set** $\to$ **Set**, any mutually surjective on singletons set of predicate liftings is a separating set.*

Lemma 2.22. *Let Φ be a fibred modal signature and S a Φ-structure. Let A, B objects in $\mathscr{C}^\Phi$, $([\![\bigcirc_i^B]\!])_{i\in I}$ a set of predicate liftings on $[\![B]\!]$ that are mutually surjective on singletons, and $([\![\bigcirc_j^A]\!])_{j\in J}$ a separating set of predicate liftings on $[\![A]\!]$ that separate by singletons. Then the liftings $([\![\bigcirc_j^A \lhd \bigcirc_i^B]\!])_{i\in I, j\in J}$ are separating for $[\![A \otimes B]\!]^S$.*

3 Quantum Applications

We now consider a suitable signature functor for modelling quantum systems. In [1] a signature functor describing a "question and answer system" for projective measurements was used. We instead introduce a new functor based upon distributions of measurement outcomes for different physical quantities. When reasoning about quantum protocols it is common to consider measurements in a suitable basis, rather than projective measurements, and this signature functor make the physical quantities and distribution over measurement outcomes explicit.

3.1 Constructing a Fibred Logic for Quantum Systems

As an extended example, we construct an expressive set of modalities for reasoning about quantum systems using simple components from well understood areas such as labelled transition systems and probabilistic logics. An alternative modular approach to the construction of coalgebraic logics is presented in [2], based on a notion of syntax constructors. Preservation of properties of modalities, such as expressivity, under operations including composition, products and coproducts is analyzed in [10], and is probably closer in spirit to the approach of this section. Many proofs are omitted throughout this section for space reasons, all conclusions are based upon the composition based ideas in section 2.1 and standard results, mainly from [14].

Definition 3.1. Let $D : \mathbf{Set} \to \mathbf{Set}$ denote the finite distribution functor, defined on objects as follows:

$$D(X) := \{ f : X \to [0,1] \mid f \text{ has finite support and } \Sigma_{x \in X} f(x) = 1 \} \tag{21}$$

and on morphisms:

$$D(f : X \to Y)(g \in D(X))(y \in Y) := \Sigma_{x \in X.\, f(x)=y} g(x) \tag{22}$$

Lemma 3.2. *The finite distribution functor D is ω-accessible.*

Now we introduce our two basic building block modalities from which all others will be constructed.

Lemma 3.3. *For the finite distribution functor D, for each $p \in [0,1]$ there is a unary predicate lifting $[\![\mathrm{Eq}_p]\!] : 2 \Rightarrow 2 \circ D$ given by:*

$$[\![\mathrm{Eq}_p]\!]_X(U) := \{ d \mid \Sigma_{u \in U} d(u) = p \} \tag{23}$$

These modalities separate by singletons.

Lemma 3.4. *For a label set Σ, and $\sigma \in \Sigma$, define the unary predicate lifting $[\![\mathrm{Next}_\sigma]\!] : 2 \Rightarrow 2 \circ (\Sigma \times (-))$ as follows:*

$$[\![\mathrm{Next}_\sigma]\!](U) := \{ (\sigma, u) \mid u \in U \} \tag{24}$$

These liftings are monotone and mutually surjective on singletons.

Now we lift to distributions over eigenvalues.

Lemma 3.5. *For $p \in [0,1]$ and $r \in \mathbb{R}$ define predicate lifting $[\![\mathrm{Eq}_{p,r}]\!] : 2 \Rightarrow D(\mathbb{R} \times (-))$ as the composite $[\![\mathrm{Eq}_p \lhd \mathrm{Next}_r]\!]$. This lifting is given explicitly by:*

$$[\![\mathrm{Eq}_{p,r}]\!]_X(U) := \{ d \mid \Sigma_{u \in U} d(r,u) = p \} \tag{25}$$

These liftings are separating.

Definition 3.6. For finite dimensional Hilbert space $\mathscr{H}$ with dimension n, let $\mathscr{A}_n$ denote the set of self adjoint operators. Define the **distribution based quantum signature functor** Q_n^d as follows:

$$Q_n^d := D(\mathbb{R} \times (-))^{\mathscr{A}_n} \tag{26}$$

There is an obvious **quantum coalgebra** for this signature, mapping pure states to distributions over measurement outcomes and subsequent states.

Lemma 3.7. *For a finite dimensional Hilbert space with dimension n, the functor Q_n^d is accessible.*

Now we can lift to distributions for each self adjoint operator (physical quantity), giving a set of liftings for our quantum signature functor Q_n^d:

Lemma 3.8. *For finite dimensional Hilbert space $\mathscr{H}$ with dimension n, for $p \in [0,1]$, $r \in \mathbb{R}$ and $\hat{A} \in \mathscr{A}_n$ define unary predicate lifting $[\![\mathrm{Eq}_{p,r,\hat{A}}]\!] : 2 \Rightarrow 2 \circ Q_n^d$ as follows:*

$$[\![\mathrm{Eq}_{p,r,\hat{A}}]\!] = [\![\mathrm{Eq}_{p,r}^{ev^{\hat{A}}}]\!] \tag{27}$$

Where $ev^{\hat{A}}$ is as defined in example 2.15. These liftings are given explicitly by:

$$[\![\mathrm{Eq}_{p,r,\hat{A}}]\!]_X(U) := \{ f \mid \Sigma_{u \in U} f(\hat{A})(r,u) = p \} \tag{28}$$

and are separating.

Theorem 3.9. *For finite dimensional Hilbert space $\mathscr{H}$ with dimension n, any coalgebraic logic with at least modalities with semantics given by the predicate liftings in lemma 3.8 is expressive if we allow conjunctions of sufficient cardinality.*

Proof. By lemma 3.7 and proposition 3.8 the claim follows immediately by applying theorem 14 of [14]. □

Although the unary predicate liftings based on equalities given in lemma 3.8 are very straightforward and separating, they are not monotone. It is easy to follow similar steps to those above to construct a monotone set of modalities, based on lower bounds on the required probabilities rather than equalities. This can be done for example by taking conjunctions of equality based modalities above the required threshold. This gives an expressive logic using monotone modalities with semantics similar to those of probabilistic modal logics [8, 5]. For reasons of space, this direction is not pursued further here as the equality based predicate liftings are sufficient for the quantum protocols we will address.

In reality, although we have good expressivity results for the liftings above, they are not particularly natural for the needs of describing quantum protocols. To aid reasoning about these protocols, we would like our modalities to better match the actions that are performed during their implementation. We now introduce some additional more "practical" modalities.

Definition 3.10. By noting that the natural transformations $\top : 1 \Rightarrow 2$ and $\neg : 2 \Rightarrow 2$ are predicate lifting for the identity functor, we can define 0-ary modality:

$$\hat{P} := \mathrm{Eq}_{1,1,\hat{P}} \lhd \top \tag{29}$$

Intuitively, in the quantum model, this describes "a projective measurement $\hat{P}$ is certain to have a positive outcome". We can also define unary modality:

$$\mathrm{C}_{r,\hat{A}} := \mathrm{Eq}_{0,r,\hat{A}} \lhd \neg \tag{30}$$

with the reading "it is certain that after getting measurement outcome r when measuring physical quantity $\hat{A}$, φ will hold".

Definition 3.11. Using similar tools to those above, we can combine our unary modalities to provide a possibilistic polyadic modality, describing how subsequent states relate to possible measurement outcomes:

$$\hat{A}(r_1 \mapsto (-), ..., r_n \mapsto (-)) \tag{31}$$

Informally this has semantics "after measuring $\hat{A}$, if outcome r_i occurs then the i^{th} postcondition will hold."

3.2 Basic Quantum Operations

We first consider how some of the features of our fibred coalgebraic logic can be applied to describe notions commonly considered when analyzing quantum systems and protocols.

Example 3.12 (Unitary Evolution)**.** For an arbitrary Hilbert space $\mathscr{H}$ we consider the quantum signature functor. A unitary $\hat{U}$ on $\mathscr{H}$ induces a function $\hat{P} \mapsto \hat{U}\hat{P}\hat{U}^{\dagger}$ giving a natural transformations $Q_n^d \Rightarrow Q_n^d$ by precomposition. These give adaptation modalities in our fibred coalgebraic logic, which in the case of the quantum coalgebra encode unitary (Heisenberg type) evolution of the system. In this approach the unitary evolution is encoded *uniformly* across each coalgebra without extending the signature functor. We will write $\hat{\mathrm{U}}\,\varphi$ for "after applying unitary transformation $\hat{U}$, φ holds".

Example 3.13 (Restriction to Subsystems)**.** We consider a 2 qubit quantum system, with corresponding Hilbert space $\mathscr{H}_2 \otimes \mathscr{H}_2$. We then fix a basis and define a linear map $|ij\rangle \mapsto |i\rangle$, and then define natural transformations Alice : $Q_4^d \Rightarrow Q_2^d$ by precomposition with the inverse image of this linear map. This natural transformation induces adaptation modalities in our logic such that we can read $\mathrm{Alice}\,\varphi$ as "if we restrict our attention to Alice's qubit, φ holds." Note that we have not needed to explicitly introduce mixed states to handle restriction to subsystems as this is encoded in the measurements selected by the Alice natural transformation.

Example 3.14 (Local Measurements)**.** If we consider a single qubit system, the $[\![\hat{P}]\!]$ predicate lifting given in definition 3.10 describes certainty of projective measurement $\hat{P}$. The natural transformation Alice defined in example 3.13 then gives modality $\hat{P}^{\mathrm{Alice}}$ giving certainty of measurement $\hat{P}$ locally on Alice's qubit in a 2 qubit composite system.

3.3 Quantum Teleportation

Definition 3.15. We will write $\hat{P}_{\psi_i}$ for the projection operator corresponding to the i^{th} Bell state.

We consider the standard example of the quantum teleportation protocol [4]. This is a 3 qubit protocol that can be informally described as follows:

> Initially Alice has a qubit in (arbitrary) state φ and she also shares half of a two qubit pair in the Bell state (the channel) with Bob. After a Bell basis measurement on both of Alice's qubits, if Bob applies a suitable correcting unitary, dependent on the outcome of the measurement, he can be certain his qubit is now in state φ.

We can formalize this in our logic as the following formula:

$$\hat{P}_{\varphi}^{\mathrm{Alice}} \wedge \hat{P}_{\psi_1}^{\mathrm{Channel}} \Rightarrow \hat{A}_{\mathrm{Bell}}^{\mathrm{Both}}(r_1 \mapsto \mathrm{Bob}\,\hat{\mathrm{U}}_1\,\hat{P}_{\varphi}, \tag{32}$$

$$r_2 \mapsto \mathrm{Bob}\,\hat{\mathrm{U}}_2\,\hat{P}_{\varphi}, \tag{33}$$

$$r_3 \mapsto \mathrm{Bob}\,\hat{\mathrm{U}}_3\,\hat{P}_{\varphi}, \tag{34}$$

$$r_4 \mapsto \mathrm{Bob}\,\hat{\mathrm{U}}_4\,\hat{P}_{\varphi}) \tag{35}$$

As our modality is built from a conjunction of smaller modalities, we can adopt a more "post selection" style perspective and decompose our teleportation protocol into various possible measurement outcomes. Here we consider formulae capturing each of the $i \in \{1..4\}$ measurement outcomes separately:

$$\hat{P}_{\varphi}^{\mathrm{Alice}} \wedge \hat{P}_{\psi_1}^{\mathrm{Channel}} \Rightarrow \mathrm{C}_{r_i,\hat{A}_{\mathrm{Bell}}}^{\mathrm{Both}}(\mathrm{Bob}\,\hat{\mathrm{U}}_{\mathrm{i}}\,\hat{P}_{\varphi}) \tag{36}$$

3.4 Entanglement Swapping

Definition 3.16. To simplify notation for multi-qubit systems we will now write $[\mathrm{i},\mathrm{j}]$ for the restrict to bits i and j, rather than define a proliferation of named subsystems such as Alice, Channel etc. as in the previous protocol and examples.

We now consider the 4 qubit entanglement swapping protocol [15], informally this protocol can be summarized as:

> Initially qubits 1 and 2, and qubits 3 and 4 are in the Bell state. After a measurement on qubits 2 and 3 in the Bell basis and applying suitable corrective unitaries, dependent on the measurement outcome, we can be certain to leave qubits 1 and 4 and qubits 2 and 3 in the Bell state.

This can be encoded in our modal logic for the $i \in 1..4$ measurement outcomes as formulae of the form:

$$\hat{P}_{\psi_1}^{[1,2]} \wedge \hat{P}_{\psi_1}^{[3,4]} \Rightarrow \mathrm{C}^{[2,3]}_{r_i,\hat{A}_{\mathrm{Bell}}}([1,4]\,\hat{\mathrm{U}}_{\mathrm{i}}\,\hat{P}_{\psi_1} \wedge [2,3]\,\hat{\mathrm{U}}_{\mathrm{i}}\text{'}\,\hat{P}_{\psi_1}) \tag{37}$$

4 Conclusions and Future Work

We have presented a fibred coalgebraic logic and shown that it respects behavioural equivalence. A distribution based signature functor for modelling finite dimensional quantum systems was introduced and the calculational aspects of our logic were exploited to construct suitable modalities for reasoning about quantum protocols. It was shown that expressivity of the logic could be lifted via the composition operations from modalities for simpler and well understood signature functors. The fibred aspects of our logic were exploited to capture key components of quantum computation, including a uniform description of unitary evolution, restriction to local subsystems and encoding of local measurements on composite systems.

The current work primarily concerns semantics. Proof theoretic aspects, particularly their suitability for analysis of quantum protocols, will be pursued in later work. The logic presented here seems to potentially be a special case of a general construction that could be applied to a suitable class of institutions [3], this should be investigated further. Connections to the existing automated tools in coalgebraic logic, and their application to analyzing quantum protocols should also be pursued.

Acknowledgements

I would like to thank Andreas Döring and Samson Abramsky for their feedback and suggestions. I would also like to thank the anonymous referees for their valuable comments and detailed recommendations.

References

[1] S. Abramsky (2010): *Coalgebras, Chu spaces, and representations of physical systems*. Logic in Computer Science (LICS 2010), pp. 411–420, doi:10.1007/s10992-013-9276-4.

[2] C. Cîrstea & D. Pattinson (2007): *Modular construction of complete coalgebraic logics*. *Theor. Comput. Sci.* 338, pp. 83–108, doi:10.1016/j.tcs.2007.06.002.

[3] J. A. Goguen & R. M. Burstall (1992): *Institutions: Abstract model theory for specification and programming*. *J. ACM* 39, pp. 95–146, doi:10.1145/147508.147524.

[4] C. H. Bennett, J. A. Brassard, J. A. Crépeau, J. A. Jozsa, J. A. Peres & R. M. Wootters (1993): *Teleporting an unknown state via dual classical and Einstein-Podolsky-Rosen channels*. *Phys. Rev. Lett.* 70, pp. 1895–1899, doi:10.1103/physrevlett.70.1895.

[5] A. Heifetz & P. Mongin (2001): *Probability logic for type spaces*. *Games and Economic Behavior* 35, pp. 31–53, doi:10.1006/game.1999.0788.

[6] A. Kurz & D. Pattinson (2000): *Coalgebras and modal logic for parameterized endofunctors*. Technical Report SEN-R0040, CWI, 2000.

[7] A. Kurz & D. Pattinson (2000): *Notes on coalgebras, cofibrations and concurrency*. *Electr. Notes Theor. Comput. Sci.* 33, pp. 196–229, doi:10.1016/s1571-0661(05)80349-4.

[8] K. G. Larsen & A. Skou (1991): *Bisimulation through probabilistic testing*. *Inf. Comput.* 94, pp. 1–28, doi:10.1016/0890-5401(91)90030-6.

[9] D. Marsden (2013): *Coalgebras with symmetries and modelling quantum systems*. In CALCO 2013), pp. 205–219, doi:10.1007/978-3-642-40206-7-16.

[10] D. Pattinson (2001): *Expressivity Results in the Modal Logic of Coalgebras*. PhD thesis, Universität München).

[11] D. Pattinson (2002): *Translating logics for coalgebras*. WADT 2002, pp. 393–408, doi:10.1007/978-3-540-40020-2-23.

[12] D. Pattinson (2003): *Coalgebraic modal logic, soundness, completeness and decidability of local consequence*. *Theor. Comp. Sci.* 309, pp. 177–193, doi:10.1016/s0304-3975(03)00201-9.

[13] D. Pattinson (2008): *Coalgebraic logics and application*. Course notes: IJCAR 2008 Tutorial.

[14] L. Schröder (2008): *Expressivity of coalgebraic modal logic: The limits and beyond*. *Theor. Comput. Sci.* 390, pp. 230–247, doi:10.1016/j.tcs.2007.09.023

[15] M. Źukowski, A. Zeilinger, M. A. Horne & A. K. Ekert (1993): *"Event ready detectors" Bell experiments via entanglement swapping*. *Phys. Rev. Lett.* 71, pp. 4287–4290, doi:10.1103/physrevlett.71.4287.