Relating Coalgebraic and Algebraic Logics of Knowledge and Update

Mehrnoosh Sadrzadeh and Corina Cîrstea

School of Electronics and Computer Science, University of Southampton**,
cc2,ms6@ecs.soton.ac.uk

One of the active fields of research in epistemic logic is modeling interactive multi-agent systems where agents communicate and as a result their knowledge gets updated. This research line has led to the development of dynamic and temporal epistemic logics [8, 5, 9, 14, 4, 2, 7] and their applications in reasoning about multi-agent protocols of Artificial Intelligence, Security and E-commerce. Another active field of research in logic in Computer Science is coalgebraic models for the study of automata and dynamic systems [13, 10, 3]; models of epistemic logic are examples of such systems. Coalgebraic models provide a more general framework for the underlying systems, one that treats different functionalities of the systems in a uniform and modular way.

In this paper we develop a coalgebraic model for dynamic and epistemic systems and a coalgebraic logic in the style of the Temporal coalgebraic logic of [10]. This is a *new* model for dynamic epistemic logic with several benefits: it is more general than the existing models, but nicely relates to them, for example it can be seen as an action-labelled version of models of Temporal Epistemic Logic. It introduces new colagebraic proof techniques, e.g. co-induction and co-recursion to modeling of multi-agent systems. As an example we sketch a new recursive proof of the muddy children puzzle, which nicely illustrates the importance of father's initial announcement, as the halting condition for recursion. It provides a base for modeling other aspects of such systems, for example probabilistic knowledge and update. It encodes actions and agents uniformly: both as state transformers formalized by coalgebra maps. This uniformity makes our approach different from that of [4] where first epistemic states are defined and fixed and then the effect of actions is defined on them co-recursively in the final coalgebra. On the logic side, we use *projective predicate lifting* instead of the usual predicate lifting method to obtain our coalgebraic logic and thus directly get a logic with both dynamic and epistemic modalities. This logic inspires by ways of application, new research in the field of coalgebraic modal logic, for example proving completeness for modular modal logics [3] other than K with nested modal properties and also for coalgebras with axiomatic restrictions.

Another contribution of our work is connecting our coalgebraic logic to the order-theoretic models of temporal logic [12] and dynamic epistemic logic [2, 16]. The connection between the Temporal coalgebraic logic of [10] and the Galois algebras of [12] has been investigated in [10]. On our part, we show how our dynamic epistemic coalgebraic logic gives rise to a *dual Galois Algebra* and also to an *appearance-update* system, an instance of the algebraic logic of [2]. The importance of this connection is three-fold: firstly, it relates our colagebraic model to the existing model-theoretic approaches of multi-agent systems, for example through the representation theorem of [2, 16] that shows models of Baltag-Moss-Solecki logic are instances of this order-theoretic models. Secondly, the coalgebraic logic relates to the Gentzen-style sequent calculus of [2, 16], proven to be complete with regard to the order-theroetic model. Finally, it places our

** Research supported by EPSRC grant EP/D000033/1.

colagebraic model in the wider area of modeling concurrent and distributed systems, since similar order-theoretic models have been used to study the semantics of concurrent systems in terms of quantales [1].

To summarize, our work brings together current research from algebraic logic, coalgebraic logic and dynamic epistemic logic communities, in the context of their applications to modeling multi-agent scenarios.

1 From Relations to Coalgebraic and Sup-Lattice Maps

Multi-agent systems are usually modelled by relational structures such as Kripke structures. A Kripke structure is a triple $(S, R, V)_{At}$ consisting of a set of states S, an accessibility relation R on states $R \subseteq S \times S$ and a valuation relation $V \subseteq S \times At$ between the states and the set of facts At. The accessibility relation tells us how one state is perceived by, or appears to an agent, for example if we have $(s, s'), (s, s'') \in R$, we say that s appears as s' or s'' to an agent. The choice between s' and s'' expresses the non-deterministic appearance of the agent, and his uncertainty about the real state. The valuation relation tells us which facts are satisfied in a state, for example $(s, p), (s, q) \in V$ says that s satisfies p and q. The appearance of multiple agents is encoded by considering a family of accessibility relations $\{R_A\}_{A \in Ag}$, one for each agent $A \in Ag$; the corresponding Kripke structure is denoted as $(S, \{R_A\}_{A \in Ag}, V)_{At}$.

The passage from Kripke structures to coalgebras is made by considering functions for relations. The accessibility relation R is lifted to a function $ap : S \to \mathcal{P}(S)$ by gathering the multiple outputs of R in one set. For example instead of $(s, s'), (s, s'') \in R$ we will have $ap(s) = \{s', s''\}$. We refer to the set of states S as the *carrier* of the coalgebra and the function ap as the *coalgebra map*; the pair (S, ap) is called a *coalgebra*. More precisely, we have the powerset functor $\mathcal{P} : Set \to Set$ on the category of sets and functions, and a $\mathcal{P}$-coalgebra $ap : S \to \mathcal{P}(S)$ maps each state to its appearance. The valuation relation is encoded in our coalgebra in a similar way: by considering it as a function $val : S \to \mathcal{P}(At)$. So instead of $(s, p), (s, q) \in V$ we have $val(s) = \{p, q\}$. We put the accessibility and valuation functions together and obtain a pair $\langle ap, val\rangle : S \to \mathcal{P}(S) \times \mathcal{P}(At)$, corresponding to the coalgebra $(S, \langle ap, val\rangle)$. Our coalgebra functor becomes the product of a powerset and a constant functor.

We encode the appearance of multiple agents by making our ap map depend on two inputs: a state and an agent $ap : S \times Ag \to \mathcal{P}(S)$. So ap takes a state s and an agent A and returns agent A's appearance of s, for example $ap(s, A) = \{s', s''\}$. In order to use this in our coalgebraic map $\langle ap, val\rangle$, we need ap to act on S rather than $S \times Ag$, so we use the equivalent (curried) form $ap : S \to \mathcal{P}(S)^{Ag}$. The coalgebra corresponding to a multi-agent Kripke structure is

$$(S, \langle ap, val\rangle) \qquad \text{where} \qquad ap : S \to \mathcal{P}(S)^{Ag} \quad \text{and} \quad val : S \to \mathcal{P}(At)$$

The passage from coalgebra maps to complete lattice maps is done by lifting the appearance function on the set of states S to a union preserving map on its powerset $\overline{ap} : \mathcal{P}(S) \to \mathcal{P}(S)$. This map acts on singletons of states $\{s\}$ rather than states s, so instead of $ap(s) = \{s', s''\}$, we have $\overline{ap}(\{s\}) = \{s', s''\}$. By union preservation, this map extends to subsets of states $P \subseteq S$ by taking the union of appearances of all states in P, that is $\overline{ap}(P) = \bigcup\{ap(s) \mid s \in P\}$. The appearance of multiple agents is encoded by considering a family of these maps $\{\overline{ap}_A\}_{A \in Ag}$, one for each agent. The set of facts and its valuation map get internalised in the lattice, in the sense that each fact p will be represented by the set of states satisfying it $\{s \in S \mid p \in val(s)\}$. We call a powerset with appearance maps an *appearance powerset lattice*:

Definition 1. *An* appearance powerset lattice $(\mathcal{P}(S), \{\overline{ap}_A\}_{A\in Ag})$ *is a powerset lattice with a family of union-preserving maps on it.*

The Galois theory [11] tells us that this map has a Galois right adjoint which preserves intersections. So we directly get an algebraic logic on the subsets of states P (or predicates), with inclusion as entailment and union and intersection as disjunction and conjunction, respectively. Moreover, we have the appearance of agents $\overline{ap}_A\, P$, and its right adjoint $\Box_A\, P$ which stands for the information or knowledge of agents.

2 Coalgebra for Actions and Agents

We aim to make our epistemic coalgebra dynamic by incorporating (the effect of) actions into it. We start by thinking about actions in the same way as agents, as a set Ac whose elements change the states. The effect of an action $a \in Ac$ on a state s is modelled by a function $up : S \to (1 + S)^{Ac}$. For example $up(s)(a)$ stands for the effect of action a on the state s, or the update of s by a. If this effect is the unique element $*$ of 1, that is, $ap(s)(a) = \iota_1(*)$, we say that action a can not apply to state s; this is the case, for instance, when the content of an announcement action is not in the valuation of the state. We add the action map to our coalgebra and obtain an *appearance-update coalgebra*:

Definition 2. *A T-coalgebra (S, ζ) for the functor $T : Set \to Set$ defined by $TX = \mathcal{P}(X)^{Ag} \times (1 + X)^{Ac} \times \mathcal{P}(At)$ is called an* appearance-update coalgebra*.*

The coalgebraic map is a triple $\zeta = \langle ap, up, val\rangle : S \to \mathcal{P}(S)^{Ag} \times (1 + S)^{Ac} \times \mathcal{P}(At)$. One unfolding or application of the coalgebra map provides us with the appearance of states to the agents $ap(s)(A)$, the effect of actions $up(s)(a)$ on states, and the valuations of states $val(s)$. Two successive unfoldings of the coalgebra map provide us with the appearance to agents about the appearance of states to other agents, and moreover, with the appearance to agents of the effect of an action $ap(up(s)(a))(A)$ whenever the action can apply, and the effect of an action on the appearance of states to agents $up(ap(s)(A))(a)$. Valuations of each of these $val(ap(up(s)(a))(A))$, $val(up(ap(s)(A))(a))$ are obtained from three successive unfoldings of the coalgebra map. So we can tell how an agent perceives the effect of an action, and how an action affects the appearance of an agent, and the facts satisfied by them. The iteration or repeated unfolding of the coalgebra map reveals the behaviour of the system. Reasoning about this behaviour is done in the final coalgebra (which exists if the first occurrence of the powerset functor in the definition of T is replaced by the *finite* powerset functor), via the coalgebraic proof method of coinduction.

Restrictions to the Coalgebras. We are interested in modeling the effect of *epistemic actions*, these are actions that only affect the information state of agents and leave the facts of the world unchanged. Examples of such actions are public or secret announcements made in a multi-agent system. In order to limit the behaviour of our system to the effect of epistemic actions, we restrict the coalgebra map by requiring that it satisfies some axioms. The first axiom is *rationality*; it says that if action a can apply to state s, then the appearance of its effect to an agent $ap(up(s)(a))(A)$ is the same as the effect of a on the appearance to the agent of the original state $up(ap(s)(A))(a)$. So if $up(s)(a) \neq \iota_1(*)$, our axiom is

$$ap(up(s)(a))(A) \;=\; \big\{up(t)(a) \mid t \in ap(s)(A), up(t)(a) \neq \iota_1(*)\big\}$$

Our second restriction is the *preservation of facts*; it says that if applicable to a state, an announcement does not change the valuation of that state, that is, the valuation of the effect of the state is the same as the valuation of the state before the action. So if $up(s)(a) \neq \iota_1(*)$, we have $val(s) = val(up(s)(a))$. Finally, our third restriction requires each agent to have at least one view of the state, that is $ap(s)(A) \neq \emptyset$.

An example of an epistemic action is a public announcement $\alpha!$ of α, for α a fact p (or conjunction or negation of a fact) or knowledge of a fact $\Box_A p$. So $\alpha!$ can apply to the states s that satisfy α, that is, if $p \in val(s)$ for the case $\alpha = p$, or $\forall t \in ap(s)(A), p \in val(t)$ for the case $\alpha = \Box_A p$. The first two restrictions to the coalgebras correspond to the familiar axioms of Public Announcement Logic [5]: rationality corresponds to the knowledge-announcement commutation axiom, while the preservation axiom corresponds to the basic axiom for atoms. Another example of an epistemic action is a private announcement $\alpha!_\beta$ to a subgroup $\beta \subseteq Ag$, with α as above. These announcements are encoded by assuming rationality with regard to the announcement for the insiders $B \in \beta$, and rationality with regard to a neutral action $\tau \in Ac$ for the outsiders $C \notin \beta$.

The Muddy Children Puzzle. There are n children playing in the mud and k of them have dirty foreheads. Their father announces that at least one of them is muddy, and asks if they know it is them who is muddy. They look around and think and reply no, but after $k-1$ rounds of no answers, the dirty children know that they are dirty. We encode the assumptions of the puzzle as further restrictions on our coalgebra and denote by D_i the proposition saying child i is dirty, by q_0 the father's initial announcement, and by q a round of no answers from the children. We sketch the proof for the proposition saying that on a state s^k with k dirty children, if father's first announcement followed by $k-1$ rounds of no answers go through, the k'th round of no answers does not go through

$$up^{k-1}(up(s^k)(q_0))(q) \in \iota_2(S) \implies up^k(up(s^k)(q_0))(q) = \iota_1(*)$$

where $up^{k-1}(s)(q)$ stands for $k-1$ times updating state s with action q. Assuming the antecedent, we have to show that the k'th round of no answers will not go through, which by restrictions to the coalgebra is equivalent to showing that the appearance of the state after $k-1$updates to any dirty child i satisfies D_i, that is

$$\forall t \in ap(up^{k-1}(up(s^k)(q_0))(q))(i), \quad D_i \in val(t)$$

By the rationality restriction applied k times, it suffices to show $D_i \in val(t)$ for all t in the following set:

$$\begin{aligned}&\big\{up^{k-1}(up(w)(q_0))(q) \mid w \in ap(s^k)(i),\\ &up(w)(q_0) \in \iota_2(S), up(up(w)(q_0))(q) \in \iota_2(S), \ldots, up^{k-1}(up(w)(q_0))(q) \in \iota_2(S)\big\}\end{aligned}$$

We denote this set by $\mathcal{K}$ and show that all of its elements satisfy D_i, by doing a case analysis on w. If in w child i is dirty, that is, $D_i \in val(w)$, then by preservation of facts we get $D_i \in val(up^{k-1}(up(w)(q_0))(q))$. But if in w child i is not dirty, then w has one less dirty child than s^k and we denote it by w^{k-1}. We show that this state does not belong to $\mathcal{K}$ by showing that $up^{k-1}(up(w^{k-1})(q_0))(q) = \iota_1(*)$. We distinguish two cases: (1) $up^{k-2}(up(w^{k-1})(q_0))(q) = \iota_1(*)$, in which case we are done, and (2) $up^{k-2}(up(w^{k-1})(q_0))(q) \in \iota_2(S)$. In the second case, we know that $k-2$ rounds of no answers are possible after father's initial announcement, and

have to show that for all other dirty children $j \neq i$, they get to know after the $k-2$ rounds, that is

$$\forall t' \in ap(up^{k-2}(up(w^{k-1})(q_0))(q))(j), \quad D_j \in val(t')$$

In order to prove this, we repeat the steps above but on a state with one less dirty child, and assuming one less update is possible; these steps get repeated ($k-2$ times) until we reach a point where we need to show $up^1(up(w^1)(q_0))(q) = \iota_1(*)$. For this we repeat the above steps one last time and have to show that $up(w^0)(q_0) = \iota_1(*)$, which is true by our assumption since father's announcement can not go through in a state with no dirty child. This is where the repetition stops and we are done.

3 Algebraic Logic for Actions and Agents

In this section we review the results from previous work [2, 16] and show how actions are added to our appearance powerset lattice $(\mathcal{P}(S), \{\overline{ap}_A\}_{A\in Ag})$, and an *appearance-update* algebraic logic is obtained from the setting. The results of [2, 16] are developed in the more general setting of sup-lattices, of which the powerset lattices of this paper are an instance.

In this setting, actions are considered as elements of another powerset lattice $\mathcal{P}(\Sigma)$ where Σ is the set of atomic or deterministic actions. The order on this lattice is the order of information or non-determinism, for example $\{\sigma\} \subseteq \{\sigma, \sigma'\}$ says that the atomic action σ is more deterministic than the mixed action $\{\sigma, \sigma'\}$, which stands for the choice of σ and σ'. From this it follows that the union on actions is the non-deterministic choice of them. The intersection of actions does not have an intuitive meaning so we do not interpret it. Sequential composition is a key operation on actions which is missing from the powerset. We incorporate it by first assuming that Σ carries a monoid structure $(\Sigma, \bullet, \tau)$, where we read $\sigma \bullet \sigma'$ as first do σ then do σ'. The order of execution matters and thus $- \bullet -$ is a non-commutative operation. The unit of sequential composition is the action τ or the skip action, which does not do anything, and we have $\tau \bullet \sigma = \sigma \bullet \tau = \sigma$. We then lift the monoid structure on Σ to a monoid structure on $\mathcal{P}(\Sigma)$, such that the monoid multiplication $- \bullet -$ is union preserving. We denote the resulting structure by $(\mathcal{P}(\Sigma), \cup, \bullet, \{\tau\})$. This type of structure is referred to as a quantale in the literature [1] and has applications in concurrency [1] and quantum physics [6], also in the semantics of Linear Logic [17].

The effect of actions on predicates (subsets of states) is modelled by defining an *update* product $- \cdot - : \mathcal{P}(S) \times \mathcal{P}(\Sigma) \to \mathcal{P}(S)$ between the appearance powerset lattice and the quantale of actions, satisfying the following properties for $P_i \subseteq S$ and $\Sigma_i \subseteq \Sigma$

$$(\bigcup_i P_i) \cdot \Sigma_1 = \bigcup_i (P_i \cdot \Sigma_1), \quad P_1 \cdot (\bigcup_i \Sigma_i) = \bigcup_i (P_1 \cdot \Sigma_i) \tag{1}$$

$$P_1 \cdot (\Sigma_1 \bullet \Sigma_2) = (P_1 \cdot \Sigma_1) \cdot \Sigma_2, \quad P_1 \cdot \{\tau\} = P_1 \tag{2}$$

$$\overline{ap}_A(P_1 \cdot \Sigma_1) \subseteq \overline{ap}_A(P_1) \cdot \Sigma_1 \tag{3}$$

The first two conditions ask the update product to preserve unions of predicates and of actions, be consistent with the order of sequential compositions of actions, and have the unit of composition of actions as a right unit. These make the lattice of predicates a *right module* of the quantale of actions. The pair $(\mathcal{P}(S), \mathcal{P}(\Sigma))$ is referred to as a *system* in the literature [1]. The last property, called the *update inequality*, is in line with the rationality restriction on the coalgebras: the appearance of the update of a predicate is stronger than the update of the appearance of the predicate. We refer to this system as an *appearance-update system*:

Definition 3. *A system with the update inequality* $(\mathcal{P}(S), \mathcal{P}(\Sigma), \cdot, \{\overline{ap}_A\}_{A \in Ag})$ *is called an* appearance-update system.

Our actions are epistemic, so they do not change the facts of the world. The content of an action is modelled by a map $ker : \mathcal{P}(\Sigma) \to \mathcal{P}(S)$, which assigns to each action the set of states to which the action cannot be applied, that is $ker(\Sigma_1) \cdot \Sigma_1 = \emptyset$. Facts can now be formalised in a better way than before: as the subsets of states (in which the fact is true) that are not changed by any update called stabilizer $Stab(\mathcal{P}(\Sigma)) = \{P_1 \subseteq S \mid \forall \Sigma_1 \subseteq \Sigma, P_1 \cdot \Sigma_1 \subseteq P_1\}$. This says that if a fact is true before doing an action, it will remain true after the action.

Other operations of our logic are the right adjoint to the appearance of predicates, and the right adjoint to the update product. The former $\Box_A P$ stands for the knowledge of agent A about predicate P. The latter $[\Sigma_1] P$ says after action Σ_1 predicate P holds, and stands for the dynamic modality of Propositional Dynamic Logic and the weakest precondition of Hoare Logic. The adjunction equations are the usual ones, $\overline{ap}_A(P) \subseteq P' \;\Leftrightarrow\; P \subseteq \Box_A P'$ and a similar one for update. These allow us to derive knowledge from appearances, and the updated predicate from the update product. Applications of this logic to multi-agent scenarios such as the muddy children puzzle and security protocols have been discussed in detail in [16]. More complicated actions such as cheating and lying are encoded in this setting by endowing the quantale of actions with union preserving appearance maps and also encoding them in the update inequality. The system with the endowed quantale is called an *Epistemic System*, for details see [2, 16].

4 Coalgebraic Logic for Actions and Agents

Coalgebras give rise to modal logics in different ways, for example the coalgebraic logic of Moss [13], the temporal logic of Jacobs [10] and the modular logic of Cîrstea and Pattison [3]. In this section we show how our appearance-update coalgebra admits a coalgebraic logic in the style of Jacobs.

The method is based on the notion of *predicate lifting*, which sends a subset P of a set X to its image under the coalgebra functor $F(P)$, and we have $F(P) \subseteq F(X)$. The lifting of P under F is denoted by $Pred(F)(P)$, and can be defined inductively for *polynomial functors* (i.e. functors built from constant and identity functors using binary products and coproducts, exponentials with constant exponent, and powersets) [10]. We apply the inductive definition to our appearance-update coalgebra functor T and obtain $Pred(T)(P)$ as follows

$$\{\langle a, u, v\rangle \mid \forall A \in Ag.\, a(A) \subseteq P,\ \forall q \in Ac.\, u(q) \in \iota_2(X) \Rightarrow u(q) \in P,\ v \subseteq \top_{\mathcal{P}(At)}\}$$

which is equivalent to $T(P) = \mathcal{P}(P)^{Ag} \times \mathcal{P}(P)^{Ac} \times \mathcal{P}(At)$. Using this predicate lifting and the coalgebra map $\zeta = \langle ap, up, val\rangle$, we define a modality for the whole functor $\bigcirc : \mathcal{P}(S) \to \mathcal{P}(S)$ on the powerset of the carrier set of a T-coalgebra (S, ζ) as follows

$$\bigcirc P = \zeta^{-1}(Pred(T)(P)) = \{s \in S \mid \zeta(s) \in Pred(T)(P)\}$$

Jacobs interprets this modality as a temporal next time modality and reads $\bigcirc P$ as 'in the next state of the system, P holds'. This logic is a powerset or a Boolean Algebra with an operator providing the base for a Coalgebraic Temporal Logic. However, we want a logic with dynamic and epistemic modalities to interpret our appearance-update coalgebra on information flow in multi-agent systems. So instead of using predicate lifting and defining one modality for the whole

functor, (as a first approximation) we use *projective predicate lifting* and define two modalities for each projection of the functor as follows

$$\Box\, P = ap^{-1}((Pred(\pi_1 \circ T)(P))), \quad [\,]P = up^{-1}((Pred(\pi_2 \circ T)(P)))$$

where $\pi_1 : \mathcal{P}(S)^{Ag} \times (1+S)^{Ac} \times \mathcal{P}(At) \to \mathcal{P}(S)^{Ag}$ and $\pi_2 : \mathcal{P}(S)^{Ag} \times (1+S)^{Ac} \times \mathcal{P}(At) \to (1+S)^{Ac}$ are the first and second projections, respectively. The first modality will stand for our epistemic modality and the second one for the dynamic modality. However, since we would like to reason about the next state of the system after *specific* actions, and about the knowledge of *specific* agents, we consider labelled versions of these modalities as follows

$$\begin{aligned} \Box_A\, P &= \{s \in S \mid ap(s)(A) \subseteq P\} \\ [a]\, P &= \{s \in S \mid up(s)(a) \in \iota_2(S) \Rightarrow up(s)(a) \in P\} \end{aligned}$$

More precisely, the labelled modalities arise from the *labelled projective predicate lifting* as follows

$$\begin{aligned} \Box_A\, P &= (ap_A)^{-1}((Pred(\pi_A \circ \pi_1 \circ T)(P))) \\ [a]\, P &= (up_a)^{-1}((Pred(\pi_a \circ \pi_2 \circ T)(P))) \end{aligned}$$

where $\pi_A : \mathcal{P}(S)^{Ag} \to \mathcal{P}(S)$ selects the A component, $ap_A : S \to \mathcal{P}(S)$ is given by $ap_A(s) = ap(s)(A)$, $\pi_a : (1+S)^{Ac} \to 1+S$ selects the a component, and $up_a : S \to 1+S$ is given by $up_a(s) = up(s)(a)$.

We interpret the first modality $\Box_A\, P$ as 'agent A knows that P', and the second one $[a]\, P$ as 'if action a is possible, then after action a predicate P holds'. Similar to Jacobs's next time modality, our labelled projective modalities are intersection preserving and have unique Galois left adjoints that preserve unions. We will have two adjoint modalities as follows

$$\begin{aligned} \underset{\longleftarrow}{\Box}_A\, P &= \bigcup\{ap(s)(A) \mid s \in P\} \\ \underset{\longleftarrow}{[a]} P &= \bigcup\{up(s)(a) \mid s \in P,\ up(s)(a) \in \iota_2(S)\} \end{aligned}$$

The adjoint modality of Jacobs is interpreted as the temporal previous time modality. We do not provide new interpretations for our adjoint modalities, since they are extensions of our appearance and update maps to subsets of the set of states, discussed in the appearance powerset lattice of the first section.

From Jacobs's construction, one obtains a Temporal coalgebraic logic on the power set of the carrier set, that is, a powerset logic with operators and their adjoints. The application of Boolean Algebras and adjoint maps to reason about the temporal evolution of systems has also been considered by von Karger in [12], where he shows how a Boolean Algebra with adjoint operators gives rise to a Computational Tree Logic (CTL). Jacobs shows how his Temporal coalgebraic logic gives rise to a Galois Algebra and that the two methods yield the same logic. Our constructions provide us with a coalgebraic powerset logic but with two families of operators and their adjoints $(\mathcal{P}(S), \Box_A, [a])$. This logic gives rise to the new notion of a *dual Galois Algebra*, defined as

Definition 4. *A dual Galois algebra is a Galois Algebra with two meet-preserving operators (GA, f, g), each of them having join-preserving Galois left adjoints $f^* \dashv f$ and $g^* \dashv g$.*

However, we have restrictions on our coalgebras that should also be accounted for in the dual Galois Algebra. We discuss the logical form of these restrictions below, and in the next section we show how the algebraic logic of the previous sections is the counter part of this coalgebraic logic.

Restrictions to the dual Galois Algebras. We reflect the rationality restriction on coalgebras in our logic by using the adjoint modalities $\underset{\leftarrow}{\Box}_A$ and $\underset{\leftarrow}{[a]}$, since these correspond to the appearance and update maps. We ask for the following as our rationality axioms

$$\underset{\leftarrow}{\Box}_A \underset{\leftarrow}{[a]} P \subseteq \underset{\leftarrow}{[a]} \underset{\leftarrow}{\Box}_A P$$

We use the inclusion rather than the equality in the logic so that we do not have to mention the empty domain of the update. In this version, we do not need to exclude the states in which a cannot apply since if $\underset{\leftarrow}{[a]} P = \emptyset$ then by union preservation of $\underset{\leftarrow}{\Box}_A$ we have $\underset{\leftarrow}{\Box}_A \emptyset = \emptyset$, and $\emptyset$ is the subset of any set. In dealing with concrete examples, one wants to compute the right hand side to be able to derive the effect of an action on the knowledge of agents. This axiom tells us that it is enough to compute the left hand side, which is itself derivable by applying the initial assumptions on the appearances of states and the content of actions.

A similar form is derivable for the knowledge and dynamic modalities

Proposition 1. Learning. *The effect of an action on the knowledge of an agent is derivable from his knowledge about the effect of the action* $\Box_A[a]P \subseteq [a]\Box_A P$.

Proof. By adjunction it suffices to show that $\underset{\leftarrow}{\Box}_A \underset{\leftarrow}{[a]} \Box_A [a]P \subseteq P$. But because of the rationality axioms, this can be reduced to showing that $\underset{\leftarrow}{[a]} \underset{\leftarrow}{\Box}_A \Box_A [a]P \subseteq P$, which, in turn, follows easily from the corollary of adjunction that $\underset{\leftarrow}{\Box}_A \Box_A Q \subseteq Q$ and similarly for $\underset{\leftarrow}{[a]}[a]$, together with the monotonicity of $\underset{\leftarrow}{[a]}$.

In the same lines as in the previous section on algebraic logic, facts $\phi \in \mathcal{P}(At)$ are considered as sets of states Φ that satisfy them. The logical form of our second restriction to the coalgebras, that is preservation of facts, is $\underset{\leftarrow}{[a]} \Phi \subseteq \Phi$. which reflects the algebraic notion of stability of facts under any update. Finally, the third restriction on coalgebras can be captured in our logic using the axiom $\Box_A \emptyset \subseteq \emptyset$.

5 Embedding of the Coalgebraic Logic in the Algebra

In this section we show how our coalgebraic logic $(\mathcal{P}(S), \Box_A, [a])$ with rationality and preservation of facts as restrictions can be embedded in our appearance-update algebraic logic. By definition and union preservation of $\underset{\leftarrow}{\Box}_A$ it follows easily that

Proposition 2. *The powerset of states and the adjoints of the epistemic modalities form an appearance powerset lattice* $(\mathcal{P}(S), \{\underset{\leftarrow}{\Box}_A\}_{A \in Ag})$.

Similarly, by the union preservation of $\underset{\leftarrow}{[a]}$ and the rationality restriction on coalgebras it follows that

Proposition 3. *In the powerset of states with the adjoints of the epistemic modalities and the adjoints of the dynamic modalities* $(\mathcal{P}(S), \{\underset{\leftarrow}{\Box}_A\}_{A\in Ag}, \{\underset{\leftarrow}{[a]}\}_{A\in Ac})$*, we have that* $\underset{\leftarrow}{[a]}$ *is union preserving and also satisfies the update inequality.*

From this we define this powerset as

Definition 5. *The triple* $(\mathcal{P}(S), \{\underset{\leftarrow}{\Box}_A\}_{A\in Ag}, \{\underset{\leftarrow}{[a]}\}_{a\in Ac})$ *where* $(\mathcal{P}(S), \{\underset{\leftarrow}{\Box}_A\}_{A\in Ag})$ *is an appearance powerset lattice and the above proposition holds is called an appearance-update powerset lattice.*

Gathering the previous two propositions we obtain our main theorem

Theorem 1. *Every appearance-update powerset lattice can be embedded in an appearance-update system.*

We draw a sketch of the proof, the details are easy and follow by set-theoretic constructions on powerset and the adjunction equations.

Proof Sketch. The family of adjoints to the dynamic modalities $\{\underset{\leftarrow}{[a]}\}_{A\in Ac} : \mathcal{P}(S) \to \mathcal{P}(S)$ is generalized to a binary map $\underset{\leftarrow}{[\,]} : \mathcal{P}(S) \times Ac \to \mathcal{P}(S)$. By Proposition 3 above, this map has the properties of the update map of an appearance-update system, but with regard to a set Ac, rather than a quantale. We freely generate a quantale $Q(Ac)$ on Ac; this is obtained by first generating the free monoid $(Ac^*, \bullet, \tau)$ over Ac, and then lifting this monoid structure to a monoid structure on $\mathcal{P}(Ac^*)$, such that $- \bullet -$ preserves unions of actions. The set of actions embeds in the resulting quantale by inclusion, so we have $Ac \subseteq Q(Ac)$. We extend our update map $\underset{\leftarrow}{[\,]} : \mathcal{P}(S) \times Ac \to \mathcal{P}(S)$ first to a map $\mathcal{P}(S) \times Ac^* \to \mathcal{P}(S)$, which preserves the monoid multiplication, and then to a map $\mathcal{P}(S) \times \mathcal{P}(Ac^*) \to \mathcal{P}(S)$, which preserves both the union of actions and the monoid multiplication. It then follows that $(\mathcal{P}(S), Q(Ac), \{\underset{\leftarrow}{\Box}_A\}_{A\in Ag}, \underset{\leftarrow}{[\,]})$ satisfies all the properties of an appearance-update system.

6 Future Work

Fixed Point Operators. We can follow Jacobs's construction and add dynamic and epistemic fixed point modalities to our appearance-update coalgebraic logic. On the part of dynamics, we obtain labelled temporal fixed-point operators, defined as $[\alpha]^* P := \nu Z.(P \cap \bigcap_{a\in\alpha}[a]Z)$ and $\langle\alpha\rangle^* P = \mu Z.(P \cup \bigcup_{a\in\alpha}\langle a\rangle Z)$ (where $\langle a\rangle$ denotes the de Morgan dual of $[a]$, and therefore $\langle a\rangle P$ is interpreted as 'action a is possible, and after action a, predicate P holds'). Similarly, the addition of epistemic fixed-point operators allows us to formalise common knowledge between (a subset of) the agents as $\Box^*_\beta P := \nu Z.(P \cap \bigcap_{B\in\beta} \Box_B Z)$. These fixed points enable us to use the *invariant* proof method of Jacobs's logic to solve the muddy children puzzle in our logic, where we have to show that eventually after the repetition of the announcement q, it will become common knowledge between the dirty children $\mathcal{D}$ that the dirty ones know that they are dirty: $\langle\{q\}\rangle^* \Box^*_{\mathcal{D}} \bigwedge_{i\in\mathcal{D}} D_i$.

Applications to Security Protocols. One nice feature of the coalgebraic approach to deriving a specification logic is that we have a uniform way of adding probabilistic information to the modelling of both actions and appearances. We aim to use this feature in encoding and reasoning about security protocols. A typical security protocol is a series of send and receive actions by

agents who aim to reach 'authentication' to be able to share a secret. But the communication is done over an unsafe channel watched by an active intruder, and this makes it hard for honest agents to be sure of the originality of messages. We use the elements of Ac for communication actions and the power set structure to capture the non-deterministic views of agents about actions. The algebraic way of reasoning about authentication in security has been exploited in [16]. We hope to mirror these algebraic constructs in the coalgebraic setting, and to use the coalgebraic approach to reason about the non-deterministic and probabilistic behaviour of these systems.

References

1. S. Abramsky and S. Vickers. 'Quantales, observational logic and process semantics'. *Mathematical Structures in Computer Science* **3**, 161–227, 1993.
2. A. Baltag, B. Coecke, and M. Sadrzadeh, 'Epistemic actions as resources', in Proceedings of Logics for Resources Programs Processes (LRPP) workshop in LiCS 2004, submitted to the journal of *Logic and Computation*, `http://www.ecs.soton.ac.uk/~ms6/JLC.pdf`
3. C. Cîrstea, 'A compositional approach to defining logics for coalgebras', Theoretical Computer Science 327(1) pp.45-69, 2004.
4. A. Baltag, L.S. Moss and S. Solecki, 'The logic of public announcements, common knowledge and private suspicions', CWI Technical Report SEN-R9922, 1999.
5. J. van Benthem, 'One is a Lonely Number', Technical Report PP-2002-27, ILLC, Amsterdam, 2002, to appear in P. Kopke, ed., *Colloquium Logicum*, Munster, 2001, AMS Publications.
6. B. Coecke, D. J. Moore and I. Stubbe. 'Quantaloids describing causation and propagation of physical properties'. *Foundations of Physics Letters* **14**, 133–145, 2001.
7. W. van Der Hoek and M. Wooldridge, 'Time, Knowledge, and Cooperation: Alternating-Time Temporal Epistemic Logic', COORDINATION 2002.
8. R. Fagin, J. Y. Halpern, Y. Moses and M. Y. Vardi. *Reasoning about Knowledge*. MIT Press, 1995.
9. J. Gerbrandy, 'Dynamic Epistemic Logic', in L.S. Moss, et al (eds.) *Logic, Language, and Information* **2**, Stanford University, CSLI Publication, 1999.
10. B. Jacobs, 'The Temporal Logic of Coalgebras via Galois Algebras', emphMath. Struc. in Comp. Sci. **12**, pp. 875-903, 2002.
11. A. Joyal and M. Tierney. 'An extension of the Galois theory of Grothendieck'. *Memoirs of the American Mathematical Society* **309**, 1984.
12. B. von Karger, 'Temporal Algebras', *Math. Struc. in Comp. Sci.* **8**, pp. 277-320, 1998.
13. L.S. Moss, 'Coalgebraic Logic', *Annals of Pure and Applied Logic* **96**, pp. 241-259, 1999.
14. J. Plaza, 'Logics of public communications', *Proceedings of 4th International Symposium on Methodologies for Intelligent Systems*, 1989.
15. J. Power, ' Towards a Theory of Mathematical Operational Semantics', *Electronic Notes in Theoretical Computer Science* **82**, pp. 1-16, 2003.
16. M. Sadrzadeh, 'Actions and Resources in Epistemic Logic', Ph.D. Thesis, submitted to University of Quebec at Montreal, December 2005, `www.ecs.soton.ac.uk/~ms6/all.pdf`.
17. D.N. Yetter, 'Quantales and (non-commutative) Linear Logic', *Journal of Symbolic Logic* **55**, pp. 41-64, 1990.