Algebra and sequent calculus for epistemic actions

Alexandru Baltag [1,2]

Computing laboratory
Oxford University
Oxford, U.K.

Bob Coecke [3]

Computing laboratory
Oxford University
Oxford, U.K.

Mehrnoosh Sadrzadeh [4]

Department of Philosophy
Université du Québec À Montréal
Montreal, Canada

Abstract

We introduce an algebraic approach to Dynamic Epistemic Logic. This approach has the advantage that: (i) its semantics is a transparent algebraic object with a minimal set of primitives from which most ingredients of Dynamic Epistemic Logic arise, (ii) it goes with the introduction of non-determinism, (iii) it naturally extends beyond boolean sets of propositions, up to intuitionistic and non-distributive situations, hence allowing to accommodate constructive computational, information-theoretic as well as non-classical physical settings, and (iv) introduces a structure on the actions, which now constitute a quantale. We also introduce a corresponding sequent calculus (which extends Lambek calculus), in which propositions, actions as well as agents appear as *resources* in a resource-sensitive dynamic-epistemic logic.

Key words: dynamic epistemic logic, quantale, module, resources.

[1] We thank S. Abramsky, A. Joyal, D. Pavlovic and I. Stubbe for valuable discussions. M. S. thanks S. Abramsky and Oxford University Computer Laboratory for their hospitality and M. Marion for logistic support.

[2] Email: baltag@comlab.ox.ac.uk

[3] Email: coecke@comlab.ox.ac.uk

[4] Email: sadrzadeh.mehrnoosh@courrier.uqam.ca

1 Introduction

Dynamic Epistemic Logic (DEL) is a PDL-style logic to reason about epistemic actions and updates in a *multi-agent system*. It focuses in particular on epistemic programs, i.e. programs that update the information state of agents, and it has applications to modelling and reasoning about information-flow and information exchange between agents. This is a major problem in several fields such as *secure communication* where one has to deal with the privacy and authentication of communication protocols, *Artificial Intelligence* where agents are to be provided with reliable tools to reason about their environment and each other's knowledge, and *e-commerce* where agents need to have knowledge acquisition strategies over complex networks.

The standard approach to information flow in a multi-agent system has been presented in [9] but it does not present a formal description of epistemic programs and their updates. The first attempts to formalize such programs and updates were done by Plaza [22], Gerbrandy and Groeneveld [13], and Gerbrandy [11,12]. However, they only studied a restricted class of epistemic programs. A general notion of epistemic programs and updates for DEL was introduced in [4,5]. However, in this approach the underlying logic on propositions is boolean. For computational purposes one might want to relax this to an intuitionistic setting, hence conceiving propositions as being structured in a Heyting algebra. On the other hand, continuous lattices are also models of partiality of knowledge [10], and are in general not distributive. Finally, actual physical computational situations such as quantum computation require (at least) a non-boolean setting.

In this paper we generalize 'boolean' DEL by introducing the notion of an *abstract epistemic system*. This generalization goes hand-in-hand with the introduction of non-determinism for states and actions and brings algebraic clarity to the semantics. The particular algebraic object which we introduce is a refinement of previously used objects tailored to study concurrency in computer science [1,23] and the dynamics and interaction of physical systems [7]. Such an abstract epistemic system consists of a *quantale Q of epistemic programs*, a *Q-right module M of epistemic propositions*, and each agent is encoded by an *appearance map* i.e. an *endomorphism of the (M, Q)-structure*. We show that the boolean DEL of [5] is a concrete example of such an abstract epistemic system. The axioms of the modal operators follow immediately from abstract properties of quantales and modules over them. Crucial notions of DEL are definable abstractly and some new notions emerge naturally. The passage to a non-boolean theory also provides a new insight into epistemic programs such as *public announcement* and, of a surprisingly different status, *public refutation*. We sketch an analysis of the muddy children puzzle and of a cryptographic attack in our setting and also provide a motivating example for the passage to a non-boolean theory. We also provide a corresponding sequent calculus in which sequents will typically look like

$$m_1, \ldots, q_1, \ldots, A_1, \ldots, m_k, \ldots, q_l, \ldots, A_n \vdash \delta$$

where $m_1, \ldots, m_k$ are propositions, $q_1, \ldots, q_l$ are actions and $A_1, \ldots A_n$ are agents which resolve into a single proposition or action δ. The fragment of the calculus restricted to actions is the Lambek calculus [19], hence resource sensitive.

2 Epistemic propositions and epistemic programs

In this section we slightly recast and enrich the Dynamic Epistemic Logic of [5] in such a way that it enables a smooth passage to the algebraic setting to be introduced in Section 4. Part of this involves the introduction of non-determinism for both states and actions.

State models.

For a set of *facts* Φ and a finite set of *agents* $\mathcal{A}$, a *state model* is a triple

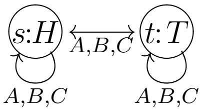
$$\mathbf{S} = (S, \xrightarrow{A}, \mu)_{A \in \mathcal{A}}$$

where S is the set of *states*, $\xrightarrow{A} \subseteq S \times S$ the *accessibility relation* for each agent $A \in \mathcal{A}$, and $\mu : S \to \mathcal{P}(\Phi)$ the *valuation map* which encodes satisfaction $s \models \varphi \Leftrightarrow \varphi \in \mu(s)$. The "facts" $\varphi \in \Phi$ are simple, objectives features of the world ("objective" in the sense of non-epistemic, i.e. independent of the agents' knowledge or beliefs), and the valuation map tell us what facts hold in a given state $s \in S$. Each accessibility relation can be repackaged as a map

$$f_A : S \to \mathcal{P}(S) :: s \mapsto f_A(s) := \{t \in S \mid s \xrightarrow{A} t\} \,,$$

called the *appearance map* of agent A. The significance of the appearance maps is as follows: if $t \in f_A(s)$ then, whenever agent A is in state s he considers state t as a 'possible world'. In other words, if the actual state of the system is s, agent A thinks t may be the actual state.

As an example,[5] consider two players A, B and a referee C. In front of everybody, the referee throws a fair coin, catches it in his palm and fully covers it, before anybody (including himself) can see on which side the coin has landed. There are two possible states here, state s in which 'the coin lies Heads' up ($= H \in \Phi$), hence $\mu(s) = \{H\}$, and state t in which the coin lies Tails up ($= T \in \Phi$), hence $\mu(t) = \{T\}$. We depict the state model **Toss** as



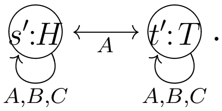
.

For every agent there are arrows between any two states (including identical states), which means that nobody knows the 'real state'.

We can also consider a case in which agents B and C can see the face of the coin, but agent A cannot see it (although he knows that the others see it), so he is

[5] For a more elaborated example of an authentication protocol we refer the reader to [2].

still uncertain if the coin is heads or tails. In this case only agent A has several arrows between states whereas agents B and C have only one arrow in each state, which means that if the coin is heads up they know it and similarly for tails up. Hence **PToss** gets depicted as

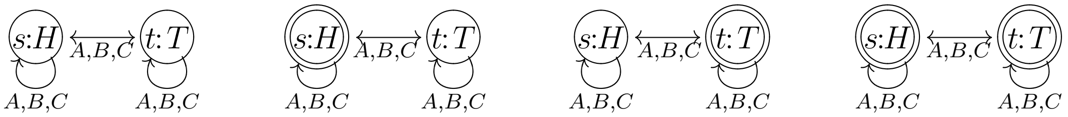


An *epistemic proposition* P *over a state model* **S** is a subset P of S, containing all the states at which the proposition is 'true'. The maps μ and f_A of the state model are extended to elements of P as follows

$$\mu(P) := \bigcap\{\mu(s) \mid s \in P\} \in \mathcal{P}(\Phi) \qquad f_A(P) := \bigcup\{f_A(s) \mid s \in P\} \in \mathcal{P}(S)\,.$$

Note that we have to use intersection and not union in defining $\mu(P)$ since a fact is entailed by an epistemic proposition when it holds at all the states of the proposition. This makes the passage from $\mathcal{P}(S)$ to $\mathcal{P}(\Phi)$ contravariant. In other words, the actual algebra of facts is $\mathcal{P}(\Phi)^{op}$, that is, the complete boolean algebra $\mathcal{P}(\Phi)$ where the order is reversed i.e. $\varphi_1 \leq^{op} \varphi_2 \Leftrightarrow \varphi_1 \supseteq \varphi_2$. While facts are simple and non-epistemic, and thus cannot be altered by epistemic actions (see further), epistemic propositions can express complex features of the world, which may depend on the agents' knowledge (and so may be changed by epistemic actions). However, notice that each fact $\varphi \in \Phi$ corresponds to an epistemic proposition $P_\varphi := \{s \in S \mid \varphi \in \mu(s)\}$, saying that the fact holds in the current state.

In the **Toss** model, H and T are facts expressing the heads up or tails up of the coin. The epistemic propositions that correspond to these facts are the states in which the fact holds. The epistemic propositions are $\emptyset, \{s\}, \{t\}, \{s,t\} \subseteq \{s,t\}$. We depict an epistemic proposition over a state model by double-circling the included states, hence



represent the four epistemic propositions of **Toss**.

When a proposition P has exactly one state $s \in P$ (i.e. $P = \{s\}$ is a singleton), we shall use systematic ambiguity, identifying the proposition with the state and writing e.g. $P = \{P\}$.

Action models.

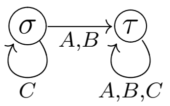
Given a state model **S**, *an action model over* **S** is a triple

$$\sum = (\Sigma,\ \xrightarrow{A}\ , \mu)_{A\in\mathcal{A}}$$

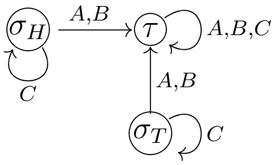
similar to a state model except that we think of the elements of Σ as possible *actions* instead of possible states and the valuation $\mu : \Sigma \to \mathcal{P}(S)$ assigns to each action

σ a *precondition*, i.e. a proposition $\mu(\sigma)$ definining the domain of applicability of σ: action σ can happen in a state s iff $s \in \mu(\sigma)$; e.g. a truthful announcement of a fact can only happen in those states where that fact holds. Note that since $\mathcal{P}(S)$ is boolean we can equivalently consider the states at which the action *cannot take place* . These states, which are the complements of the precondition of an action are denoted as $Ker(\sigma) := S \setminus \mu(\sigma)$ for each $\sigma \in \Sigma$. The *effect* of an action on states and appearance maps will be defined below in terms of an *epistemic update* product.

We introduce an action model over **Toss**. After catching the coin in his hand the referee might secretly take a peek at the coin before covering it while nobody notices this. The action model is now depicted as



where σ stands for 'cheating' and τ for 'nothing happens' and $\mu(\sigma) = \{s, t\}$. The action model can be refined when replacing σ by σ_H and σ_T where $\mu(\sigma_H) = \{s\}$ and $\mu(\sigma_T) = \{t\}$, specifying what the referee saw in case of deceit. Pictorially

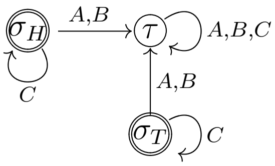


An *epistemic program* π *over an action model* Σ is a subset π of Σ; the μ and f_A maps are both extended covariantly by continuity

$$\mu(\pi) := \bigcup\{\mu(\sigma) \mid \sigma \in \pi\} \in \mathcal{P}(S) \quad \text{and} \quad f_A(\pi) := \bigcup\{f_A(\sigma) \mid \sigma \in \pi\} \in \mathcal{P}(\Sigma)\,.$$

The union in the definition of μ maps for programs says that an epistemic program is applicable where at least one of its actions is applicable. This makes the Ker map follow contravariantly by boolean negation i.e. $Ker(\pi) := S \setminus \mu(\pi)$ or equivalently $Ker(\pi) := \bigcap\{Ker(\sigma) \mid \sigma \in \pi\}$. Epistemic programs introduce non-determinism: whenever $\pi_1 \subseteq \pi_2$ then π_2 is obtained from π_1 by increasing nondeterminism; $\pi = \{\sigma_1, \sigma_2\}$ stands for "either action σ_1 or action σ_2 takes place".

In our example with actions σ_H, σ_T and τ the epistemic program $\{\sigma_H, \sigma_T\}$ stands for the non-deterministic action σ, in the sense that the outcome of the toss can be either. We depict the program over an action by double-circling the including actions. Hence the picture of the program $\pi = \{\sigma_H, \sigma_T\}$ over $\sum$ is



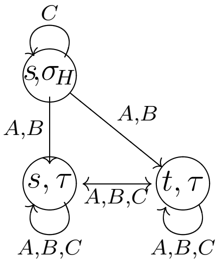
As in the case of states and propositions, we use systematic ambiguity to identify *deterministic* programs $\pi = \{\sigma\}$ with their unique underlying action σ.

Update.

Given a state model **S** and an action model $\sum$ over **S** we define their *update product* **S** $\otimes \sum$ to be a new state model given by

$$S\otimes\Sigma := \bigcup_{\sigma\in\Sigma} \mu(\sigma)\times\{\sigma\} \quad f_A(s,\sigma) := (f_A(s)\times f_A(\sigma))\cap(S\otimes\Sigma) \quad \mu(s,\sigma) := \mu(s)\,.$$

In simpler terms we have $S \otimes \Sigma = \{(s,\sigma) \mid s \in \mu(\sigma), \sigma \in \Sigma\} \subseteq S \times \Sigma$ and also $f_A(s,\sigma) \subseteq f_A(s) \times f_A(\sigma)$ that is $(s',\sigma') \in f_A(s,\sigma)$ iff $s' \in f_A(s)$ and $\sigma' \in f_A(\sigma)$. As it will become more explicit in the abstract algebra of next section, update is a structure preserving operation in the sense that it has no *side effect* on the state model that it acts on. In our example, after the cheating action σ_H where the coin has lied Heads up, A and B think that nobody knows on which side the coin is lying. But they are wrong! The system after this action can be updated by taking the update product of the two models **Toss** and σ_H depicted above:



Note that in general $S \otimes \Sigma$ and S are not necessarily disjoint.[6]

Definition 2.1 We define the *update product* of an epistemic proposition P over **S** and an epistemic program π over $\sum$ as the epistemic proposition

$$P \otimes \pi := \bigcup_{\sigma\in\pi}(\mu(\sigma)\cap P)\times\{\sigma\} \subseteq\; P \times \pi \;\text{ over }\; \mathbf{S}\otimes\sum\,.$$

The proposition $P \otimes \pi$ provides the *strongest postcondition* for P with respect to epistemic program π. This means that if proposition P is true at the input of program π then $P \otimes \pi$ is the strongest proposition that is true at the output of π. It can be seen that $P \otimes \pi = \emptyset$ iff $P \cap \mu(\pi) = \emptyset$, where $\emptyset$ is the *falsum* (i.e. the trivially false epistemic proposition over **S**).

Modalities.

We define the *epistemic modality* for each agent $A \in \mathcal{A}$ as the unary connective which assigns to proposition $P \subseteq S$ over **S** another proposition

$$\Box_A P := \big\{s \in S \;\big|\; f_A(s) \subseteq P\big\} \;\text{ over }\; \mathbf{S}.$$

[6] In fact later, the most important models we shall consider later (DEL models) are closed with respect to update product, i.e. $S \otimes \Sigma \subseteq S$.

We read $\Box_A P$ as 'agent A knows or believes P'.[7]

We define the *dynamic modality* for each epistemic program π over $\sum$ as the unary connective which assigns to proposition $P \subseteq S$ over $\mathbf{S}$ another proposition

$$[\pi]P := \big\{s \in S \;\big|\; \{s\} \otimes \pi \subseteq P\big\} = \bigcup \big\{Q \in \mathcal{P}(S) \;\big|\; Q \otimes \pi \subseteq P\big\} \;\text{ over }\; \mathbf{S}\,.$$

Note that (as mentioned before) some states $s \in S$ can be themselves pairs of states and actions (s, σ) which make the above definition well defined. The proposition $[\pi]P$ provides the *weakest precondition* for P with respect to the epistemic program π. This means that if proposition P is true at the output of program π then $[\pi]P$ is the weakest proposition that should have been true before π.

Sequential composition.

The *sequential composition* $\sum_1 \bullet \sum_2$ over $\mathbf{S}$ of two action models $\sum_1$ and $\sum_2$ both over $\mathbf{S}$ means 'first do $\sum_1$ and then do $\sum_2$' and is defined as

$$\Sigma_1 \bullet \Sigma_2 := \Sigma_1 \times \Sigma_2 \qquad f_A(\sigma_1, \sigma_2) := f_A(\sigma_1) \times f_A(\sigma_2) \qquad \mu(\sigma_1, \sigma_2) := \mu(\sigma_1) \cap [\sigma_1]\mu(\sigma_2).$$

In simpler terms, $(\sigma'_1, \sigma'_2) \in f_A(\sigma_1, \sigma_2)$ iff $\sigma'_1 \in f_A(\sigma_1)$ and $\sigma'_2 \in f_A(\sigma_2)$ and also $\mu(\sigma_1, \sigma_2) = \{s \in S \mid s \in \mu(\sigma_1), s \otimes \sigma_1 \in \mu(\sigma_2)\}$. Again note that $\Sigma_1 \bullet \Sigma_2$ and Σ_1 (or Σ_2) are not necessarily disjoint.[8] The action model over a state model $\mathbf{S}$ contains an action *skip* in which nothing happens iff [9]

$$\text{skip} = \{\text{skip}\} \qquad \mu_{\text{skip}} = S = \top_{P(S)} \qquad f_A(\text{skip}) = \{\text{skip}\}\,.$$

Notice the use of systematic ambiguity: we denoted with the same name (*skip*) both the program *skip* and its only action. It is easy to see that skip is a unit, up to isomorphism, both for update product and sequential composition.

Definition 2.2 We define the *sequential composition* of two epistemic programs π_1 over $\sum_1$ and π_2 over $\sum_2$ as the epistemic proposition $\pi_1 \bullet \pi_2 := \pi_1 \times \pi_2$ over $\sum_1 \bullet \sum_2$.

Concrete epistemic systems.

We now have all the tools to make the passage of DEL in the sense of [5] to 'concrete epistemic systems' which we put forward as a stepping-stone towards 'abstract epistemic systems'. A DEL model is essentially one that is closed under update product and sequential composition (and contains a *skip*), while a concrete epistemic system consists of all the epistemic propositions and all the epistemic programs of a DEL model:

Definition 2.3 A DEL model is a pair $(\mathbf{S}, \sum)$ where $\mathbf{S}$ is a state model and $\sum$ is an action model over $\mathbf{S}$ such that *skip* $\in \Sigma$, $(S \otimes \Sigma) \subseteq S$ and $(\Sigma \bullet \Sigma) \subseteq \Sigma$.

[7] Taking either 'knows' or 'beliefs' depends on the context.

[8] In fact later we only consider models where $\Sigma \bullet \Sigma \subseteq \Sigma$.

[9] This action has been denoted as τ in the preceding examples.

Definition 2.4 Given a DEL model $(\mathbf{S}, \sum)$, a *concrete epistemic system* is the pair $(\mathcal{P}(S), \mathcal{P}(\Sigma))$ which goes equipped with valuation μ, appearance maps $\{f_A\}_{A\in\mathcal{A}}$ and all other operations of the DEL model extended to $\mathcal{P}(S)$ and $\mathcal{P}(\Sigma)$ as we showed before.

3 The algebra of programs and propositions

A *sup-lattice* L is a complete lattice with maps which preserve arbitrary joins as homomorphism. Recall that each sup-lattice also has arbitrary meets, namely

$$\bigwedge_i a_i = \bigvee\{b \in L \mid \forall i, b \leq a_i\}$$

for any $A \subseteq L$. Hence the designation ‘sup-lattice refers to the fact that we require structure-preserving maps only to preserve arbitrary joins (cf. the designations *locales* and *frames* for complete Heyting algebras [17]). We denote *bottom* and *top* of L by $\bot$ and $\top$ respectively and define its set of *atoms* as

$$Atm(L) := \{p \in L \setminus \{\bot\} \mid a \leq p \Rightarrow a = \bot\}.$$

A lattice L is *atomistic* iff

$$\forall a \in L, a = \bigvee\{p \in Atm(L) \mid p \leq a\}\,.$$

Every sup-morphism $f^* : L \to M$ has a (unique) right Galois adjoint f_* satisfying

$$\frac{f^*(a) \leq b}{\overline{a \leq f_*(b)}}$$

and can be explicitly given as

$$f_* : M \to L :: b \mapsto \bigvee\{a \in L \mid f^*(a) \leq b\}.$$

The *left Galois adjoint* f^* moreover preserves arbitrary meets. We denote an adjoint pair by $f^* \dashv f_*$. In computational terms, one can think of the left Galois adjoint f_* as assigning weakest preconditions with respect to the program f^*.

A *quantale*[10] is a sup-lattice Q equipped with a monoid structure $(Q, \bullet, 1)$ satisfying

$$a \bullet \left(\bigvee_i b_i\right) = \bigvee_i (a \bullet b_i) \qquad\qquad \left(\bigvee_i a_i\right) \bullet b = \bigvee_i (a_i \bullet b)\ .$$

Hence for all $a \in Q$ the maps $a \bullet - : Q \to Q$ and $- \bullet a : Q \to Q$ preserve arbitrary joins and hence they have Galois adjoints $(a \bullet -) \dashv (a \setminus -)$ and $(- \bullet a) \dashv (-/a)$

[10] The term ‘quantale’ was introduced in [21]. For a survey on quantales we refer to [24]. For insightful categorical perspectives on quantales and Q-modules we refer to [18] and [25].

explicitly given by

$$a \setminus b := \bigvee\{c \in Q \mid a \bullet c \leq b\} \qquad\qquad b/a := \bigvee\{c \in Q \mid c \bullet a \leq b\}.$$

We refer to $(a \setminus -)$ and $(-/a)$ as the *residual* operations. A *quantale homomorphism* is both a sup-homomorphism and a monoid-homomorphism. Examples of quantales are: the set $\mathsf{sup}(L)$ of all sup-endomorphisms of a complete lattice L ordered pointwisely; the set of all relations from a set X to itself ordered by pointwise inclusion — this quantale is isomorphic to $\mathsf{sup}(\mathcal{P}(X))$; the powerset of any monoid with composition extended by continuity.

A Q-*right module* for a quantale Q is a sup-lattice M which goes equipped with a *module action* $- \otimes - : M \times Q \to M$, that is,

$$m \otimes 1 = m$$
$$m \otimes (q_1 \bullet q_2) = (m \otimes q_1) \otimes q_2$$
$$m \otimes (\bigvee_i q_i) = \bigvee_i (m \otimes q_i) \qquad (\bigvee_i m_i) \otimes q = \bigvee_i (m_i \otimes q)$$

Again we have two right Galois adjoints $- \otimes q \dashv [q]-$ and $m \otimes - \dashv \{m\}-$ where

$$[q]m := \bigvee\{m' \in M \mid m' \otimes q \leq m\} \qquad\qquad \{m\}m' := \bigvee\{q \in Q \mid m \otimes q \leq m'\}.$$

As for some examples, a quantale Q is a Q-right module over itself with composition as the tensor and a complete lattice L is a $\mathsf{sup}(L)$-right module with function application as the tensor.

Definition 3.1 A *system* is a pair (M, Q) with Q a quantale and M a Q-right module **[1]**.

A system is *atomistic* when both M and Q are atomistic and the following equations hold

$$m \in Atm(M), q \in Atm(Q) \Longrightarrow m \otimes q \in Atm(M) \cup \{\bot\}$$
$$q_1, q_2 \in Atm(Q) \Longrightarrow q_1 \bullet q_2 \in Atm(Q)\,.$$

These conditions can be interpreted as the fact that ‘the atoms of both the quantale and the module behave deterministically’.

Proposition 3.2 **i.** *Epistemic programs $\mathcal{P}(\Sigma)$ with $\bigcup$ as $\bigvee$, sequential composition as $\bullet$ and ‘skip’ as 1 form a quantale.*[11] **ii.** *Epistemic propositions $\mathcal{P}(S)$ with $\bigcup$ as $\bigvee$ and update product as $\otimes$ form a right $\mathcal{P}(\Sigma)$-module*[12]. **iii.** *The pair $(\mathcal{P}(S), \mathcal{P}(\Sigma))$ is an atomistic system. The atoms of the module $\mathcal{P}(S)$ correspond to the* states $s \in S$, *while the atoms of the quantale $\mathcal{P}(\Sigma)$ correspond to the* actions $\sigma \in \Sigma$.

[11] This construction is implicit in the relational composition of dynamic actions in [15].

[12] By this construction it becomes clear that update is a structure preserving map on epistemic propositions and has no *side effects*.

Proposition 3.3 **i.** *The appearance maps $f_A : \mathcal{P}(S) \to \mathcal{P}(S)$, and for all $\pi \in \Sigma$ the maps $- \otimes \pi : \mathcal{P}(S) \to \mathcal{P}(S)$ are all sup-homomorphisms.* **ii.** *The appearance maps $f_A : \mathcal{P}(\Sigma) \to \mathcal{P}(\Sigma)$, and for all $\pi \in \Sigma$ the maps $\pi \bullet -, - \bullet \pi : \mathcal{P}(\Sigma) \to \mathcal{P}(\Sigma)$ are quantale-homomorphisms.* **iii.** *For every epistemic proposition $P \in \mathcal{P}(S)$ and every epistemic program $\pi \in \mathcal{P}(\Sigma)$, we have*

$$f_A(P \otimes \pi) \subseteq f_A(P) \otimes f_A(\pi)\,.$$

iv. *For every* state *(i.e. atomic proposition) $s \in S$ and every* action *(i.e. atomic program) $\sigma \in \Sigma$ we have that:*

$$\textit{if} \quad s \otimes \sigma \neq \emptyset \quad \textit{then} \quad f_A(s \otimes \sigma) = f_A(s) \otimes f_A(\sigma)\,.$$

The last property can be generalised by introducing a notion of *coherence*:

Definition 3.4 A pair (P, π) where P is an epistemic proposition and π is an epistemic program is *coherent* iff

$$\forall s \in P,\ \forall \sigma \in \pi\ \ s \otimes \sigma \neq \emptyset$$

i.e. iff $P \subseteq \mu(\sigma)$ for every $\sigma \in \pi$. This means that proposition P ensures the possibility of all the actions subsumed by program π. An equivalent definition which doesn't refer to states or actions is the following:

$$\forall P' \subseteq P,\ \forall \pi' \subseteq \pi\ (P' \otimes \pi' = \emptyset\ \Rightarrow\ P' = \emptyset \text{ or } \pi' = \emptyset)\,.$$

Proposition 3.5 *If (P, π) is a coherent pair then we have*

$$f_A(P \otimes \pi) = f_A(P) \otimes f_A(\pi)\,.$$

Proposition 3.6 **i.** *For $A \in \mathcal{A}$ the right Galois adjoint to appearance $f_A^{\mathbf{S}}(-) : \mathcal{P}(S) \to \mathcal{P}(S)$ is knowledge $\Box_A^{\mathbf{S}}-$ (=the epistemic modality).* **ii.** *For $\pi \in \mathcal{P}(\Sigma)$ the right Galois adjoint to update $- \otimes \pi : \mathcal{P}(S) \to \mathcal{P}(S)$ is the dynamic modality $[\pi]-$.* **iii.** *The right Galois adjoint to appearance $f_A^{\Sigma}(-) : \mathcal{P}(\Sigma) \to \mathcal{P}(\Sigma)$ introduces an epistemic modality $\Box_A^{\Sigma}-$ on actions.* **iv.** *The right Galois adjoint to left- and right-composition $\pi \bullet -, - \bullet \pi : \mathcal{P}(\Sigma) \to \mathcal{P}(\Sigma)$ introduce respectively weakest pre-specification $\pi \backslash -$ and strongest post-specification $\pi / -$, and the right Galois adjoint to $P \otimes - : \mathcal{P}(\Sigma) \to \mathcal{P}(S)$ introduces $\{m\}-$, a variant on this.* [13]

Proof. All follows by construction and basic facts on sets, cartesian products and relations. □

[13] The residual $\pi \setminus -$ assigns to its argument δ the weakest program $\pi \setminus \delta$ which one has to effectuate *after* effectuating π such that the net effect is below δ. The residual $-/\pi$ assigns to its argument δ the strongest program δ/π which one has to effectuate *before* effectuating π such that the net effect is below δ. The right Galois adjoint does $\{m\}-$ assigns to its argument δ the weakest proposition $\{m\}P$ before effectuating π which guarantees P after. For a discussion on pre- and post-specification we refer to [8,16].

4 Abstract epistemic systems

The propositions of the previous section lead us to the following definitions:

Definition 4.1 A *system-endomorphism* $(M, Q) \xrightarrow{f} (M, Q)$ is a pair

$$\big(f^M : M \to M\,,\; f^Q : Q \to Q\big)$$

where f^M is a sup-homomorphism, f^Q is a quantale homomorphism and

$$f^M(m \otimes q) \leq f^M(m) \otimes f^Q(q) \tag{1}$$

for all $m \in M$ and $q \in Q$.

Definition 4.2 An *(abstract) epistemic system* is a tuple $(M, Q, \{f_A\}_{A\in\mathcal{A}})$ where (M, Q) is a system and $\{f_A\}_{A\in\mathcal{A}}$ are system-endomorphisms.

Interpretation.

The elements of the quantale Q are to be thought of as the *epistemic programs* and its unit as *skip*, the elements of the module M are to be thought of as the *epistemic propositions*, or if one wants, the not necessarily deterministic states, the labels $A \in \mathcal{A}$ are the *agents* with the endomorphisms $\{f_A\}_{A\in\mathcal{A}}$ as their *appearance maps*. The *kernel* of a program $q \in Q$ is

$$Ker(q) := \{m \in M \mid m \otimes q = \bot\}$$

and comprises the *preconditions*: it contains the epistemic propositions to which q cannot be applied. The *stabilizer*

$$Stab(Q) := \{m \in M \mid \forall q \in Q, [q]m = m\}$$

comprises the *facts*: it consists of those epistemic propositions which are stable under epistemic actions. The *satisfaction* relation is included in the partial ordering of M: for a state $m \in M$ and fact $\varphi \in Stab(Q)$ we have $m \models \varphi \Leftrightarrow m \leq \varphi$. All modalities and other right Galois adjoints discussed and introduced in Proposition 3.6 arise also here as right Galois adjoints and hence their interpretation still holds e.g. "knowledge $\Box_A^M$ is the adjoint to appearance f_A^M".

Nature of the modalities.

We identify the basic properties of the modalities.

Proposition 4.3 *In any epistemic system we have*

$$\Box_A^M \top = \top \qquad\qquad \Box_A^M(m \wedge m') = \Box_A^M m \wedge \Box_A^M m' \qquad\qquad \frac{m \leq m'}{\Box_A^M m \leq \Box_A^M m'}\,.$$

Proof: Since $\Box_A^M$ is a right Galois adjoint it preserves arbitrary meets, that is $\Box_A^M(\bigwedge_i m_i) = \bigwedge_i \Box_A^M m_i$, and hence it preserves the empty meet and binary meets, and is monotone. □

Since all other modalities preserve arbitrary meets the same result holds for them and for all other right Galois adjoints. In an intuitionistic context where one might take M to be a *frame* (i.e. a (complete) Heyting algebra with sup-homomorphisms) we can internalize the partial order using the defining property of a Heyting algebra so we obtain

$$\frac{\vdash m \to m'}{\vdash \Box_A^M m \to \Box_A^M m'} \,.$$

Hence in the special case that $Q = \{1\}$ and $A = \{*\}$ we obtain the intuitionistic modal logic $\mathbf{IntK}_\Box$ of [27]. We conclude that *intuitionistic epistemic systems*, that is epistemic systems for which M is a frame, generalize intuitionistic modal logic to multiple agents and dynamics in terms of epistemic programs. If M is moreover a complete boolean algebra such as the powerset of Section 2 then Kripke's axiom **K** follows i.e.

$$\Box_A^M(m \to m') \to (\Box_A^M m \to \Box_A^M m').$$

Diamonds and corresponding rules arise in that case by duality.

Learning.

The fact that eq(1) in definition 4.1 is an *inequality* expresses learning of agents. Some of the clauses of the appearance of an agent on an update product might get eliminated from the left hand side of eq(1) simply because some of the sub-action of the program might not be applicable on some of the sub-states of the proposition. This implies that the agent learns something new as the result of update (left hand side is stronger than the right hand side).

We can also force the equality by introducing the notion of coherence:

Definition 4.4 A pair (m, q) where $m \in M$ and $q \in Q$ is *coherent* iff

$$\forall m' \leq m,\ \forall q' \leq q\ (m' \otimes q' = \bot\ \Rightarrow\ m' = \bot \text{ or } q' = \bot)$$

For example in an *atomistic* system, every atomic pair $(m, q) \in Atm(M) \times Atm(Q)$ where $m \notin ker(q)$ is coherent.

Definition 4.5 A *strong epistemic system* is a tuple $(M, Q, \{f_A\}_{A \in \mathcal{A}})$ where (M, Q) is a system and for all coherent pairs (m, q) we have the following equality

$$f^M(m \otimes q) = f^M(m) \otimes f^Q(q)\,.$$

Representation Theorems.

Theorem 4.6 *Every atomistic strong epistemic system for which both M and Q are completely distributive boolean algebras can be represented as a concrete epis-*

temic system.

Proof: It suffices to set $S := Atm(M)$, $\Sigma := Atm(Q)$ and $\Phi := Stab(Q)$. The accessibility relations arise from the appearance maps, satisfaction from $\varphi \in \mu(s) \Leftrightarrow s \leq \varphi$ for $s \in S$ and $\varphi \in \Phi$ and preconditions from $\mu(\sigma) := S \setminus Ker(\sigma)$ for $\sigma \in \Sigma$. □

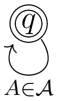
Theorem 4.7 *Every concrete epistemic system* $(\mathcal{P}(S), \mathcal{P}(\Sigma))$ *is an atomistic strong (abstract) epistemic system* $(M, Q, \{f_A\}_{A\in\mathcal{A}})$ *.*

Proof: By propositions 3.2, 3.3, and 3.5. □

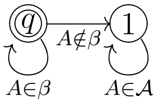
5 Some dynamic epistemic situations

For a given epistemic system $(M, Q, f_A)_{A\in\mathcal{A}}$ the following are some examples of some special epistemic programs that can be defined in the system. Note that $Ker(q) = \downarrow(\bigvee Ker(q))$, where $\downarrow a := \{b \in L \mid b \leq a\}$, and hence "being not in the precondition of q" exists as a proposition in M for all $q \in Q$.

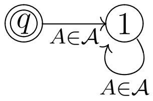
(i) **Public refutation** of the proposition $m \in M$ is an epistemic program $q \in Q$ with $\{f_A(q)\}_{A\in\mathcal{A}} = q$ and $Ker(q) = \downarrow m$. We depict it as



(ii) **Private refutation to subgroup** This is also a program that privately refutes a proposition m to the subgroup β of agents. $Ker(q)$ is the same as before and $\{f_A(q)\}_{A\in\beta} = q$ and $\{f_A(q)\}_{A\in\mathcal{A}\setminus\beta} = 1$. It is depicted as



(iii) **Failure test** of a proposition m is a program q that tests when m fails. It is a particular case of private refutation where m is refuted to an empty set of agents $Ker(q) = \downarrow m$ and $\{f_A(q)\}_{A\in\mathcal{A}} = 1$. Pictorially



(iv) **Public announcement** is also definable in our setting. However, while "being not in the precondition of q" is a proposition in M for all $q \in Q$, this is not the case for "being in the precondition of q". To see this consider the lattice $\{\bot \leq a, b, c \leq \top\}$ with q such that $Ker(q) = \{\bot, a\}$ where in the language of Section 2 we have $\mu(q) = \{b, c\}$, which can not be represented by a single element of M. The reason for this is that this lattice is non-boolean. Hence public announcement of the proposition $m \in M$ is an epistemic program $q \in$

Q for which $f_A(q) = q$ and for which $\bigvee Ker(q)$ has a *boolean complement* $(\bigvee Ker(q))^c$, satisfying $(\bigvee Ker(q))^c = m$.

We now present some case studies. Given an epistemic system $(M, Q, f_A)_{A \in \mathcal{A}}$ on which we impose particular conditions which encode the desired state and action models.

Cheating.

Consider the 'cheating' scenario of the first section where the set of agents is $\mathcal{A} = \{A, B, C\}$. Recall that there are two possibilities in the state model **Toss**, s in which the coin is Heads up and t in which it is Tails up. We model this abstractly by assuming as given an epistemic system (M, Q), with $s, t \in M$ and $\sigma_H \in Q$. The facts are encoded as stabilizers, i, e. we are given propositions $H, T \in Stab(Q)$. All these are assumed to satisfy the following conditions: $f_i(s) = f_i(t) = s \vee t$ for all $i \in \mathcal{A}$ $s \leq H, t \leq T, H \wedge T = \bot$; the epistemic program $\sigma_H \in Q$ has maps $f_A(\sigma_H) = f_B(\sigma_H) = 1$ and $f_C(\sigma_H) = \sigma_H$, and kernel $Ker(\sigma_H) = \downarrow t$. This program describes an instance of cheating where the coin is heads up. $s \otimes \sigma_H \in M$ is the proposition s after it is updated by σ_H.

Let us reason about this scenario, using our algebraic setting, e. to prove that $s \otimes \sigma_H \leq \Box_C H$. Indeed by $\{f_A\}_{A \in \mathcal{A}}$ being system homomorphisms and eq(1) we have

$$f_A(s \otimes \sigma_H) \leq f_A(s) \otimes f_A(\sigma_H) = (s \vee t) \otimes 1 = s \vee t\,,$$

and the same goes for f_B. On the other hand

$$f_C(s \otimes \sigma_H) \leq f_C(s) \otimes f_C(\sigma_H) = (s \vee t) \otimes \sigma_H = (s \otimes \sigma_H) \vee (t \otimes \sigma_H) = s \otimes \sigma_H$$

since $t \in Ker(\sigma_H)$. We have $s \leq H$ iff $s \otimes \sigma_H \leq H \otimes \sigma_H$ and by the definition of $Stab(Q)$ we get $s \otimes \sigma_H \leq H$. Thus $f_C(s \otimes \sigma_H) \leq H$ and by adjunction we get $s \otimes \sigma_H \leq \Box_C H$ which means after updating his initial state by taking a peek, the referee knows that the coin is heads up.

If the referee is honest he uncovers the coin without taking a peek. He then publicly refutes the 'coin being tails'. The epistemic program in this case is the public refutation of proposition t where $f_A(q) = f_B(q) = f_C(q) = q$ and $Ker(q) = \{t\}$. It follows that $s \otimes q \leq \Box_A H$, and the same goes for B and C. Hence all the agents know that the coin is Heads up after the public refutation.

The muddy children puzzle.

We refer the reader for a detailed description of the general case of the muddy children puzzle to [9]. This general version has been encoded and as usual solved by induction in our algebraic setting in [6]. In this paper we treat the case of three children A, B, C playing in the mud with A and B having muddy foreheads. Their father publicly announces that at least one of them has mud on his forehead and asks once if they know that they are dirty. After they all simultaneously reply "No!" once, the muddy children A and B will know that they are muddy. This simple case has only one round (since the number of dirty children is 2), but the general case with k dirty children shall have $k-1$ rounds of ”No!” replies.

As before, we model this by postulating as given an epistemic system (M, Q). The set of agents $\mathcal{A}$ includes children $\{A, B, C\}$. The module M includes all possible initial states s_β with $\beta \subseteq \mathcal{A}$ being those children that are dirty. Since the children cannot see their own foreheads (which might be dirty or not) we have $f_i^M(s_\beta) = s_{\beta \setminus \{i\}} \vee s_{\beta \cup \{i\}}$ for each child i. Let $D_\emptyset$ be the fact that no child has a dirty forehead and D_i be the fact that child i has a dirty forehead, hence $\{D_\emptyset\} \cup \{D_i \in M \mid i \in \mathcal{A}\} \subseteq Stab(Q)$, and also $s_\beta \leq D_i$ for all $i \in \beta$. Let q be a round of no answers of the 3 children, i.e. q is the public refutation of $\Box_A D_A \vee \Box_B D_B \vee \Box_C D_C$ and hence $Ker(q) = \Box_A D_A \vee \Box_B D_B \vee \Box_C D_C$ and $f_i(q) = q$ for each child i. Let $q_0 \in Q$ be the be father’s announcement that at least one child has mud on his forehead hence $Ker(q_0) = \downarrow D_\emptyset$ and $f_i(q_0) = q_0$ for each child i. We have to show that after the first round of refutation q each muddy child (e.g. A) knows that he is dirty, i.e. $s_{\{A,B\}} \leq [q_0 \bullet q] \Box_A D_A$ and similarly for child B. By adjunction on dynamic and epistemic modalities and module equation $(m \otimes q_1) \otimes q_2 = m \otimes (q_1 \bullet q_2)$ we get

$$f_A((s_{\{A,B\}} \otimes q_0) \otimes q) \leq D_A \,. \tag{2}$$

By the f_A inequality (i.e. eq(1)) it suffices to show

$$f_A(s_{\{A,B\}} \otimes q_0) \otimes f_A(q) \leq D_A$$

Again by eq(1) and the assumption $f_A(q_0) = q_0$

$$f_A(s_{\{A,B\}} \otimes q_0) \leq f_A(s_{\{A,B\}}) \otimes q_0$$

update both sides by $f_A(q) = q$

$$f_A(s_{\{A,B\}} \otimes q_0) \otimes q \leq (f_A(s_{\{A,B\}}) \otimes q_0) \otimes q$$

So to prove eq(2) it suffices to show

$$(f_A(s_{\{A,B\}}) \otimes q_0) \otimes q \leq D_A$$

Replacing f_A by its value will get us

$$((s_{\{A,B\}} \vee s_{\{B\}}) \otimes q_0) \otimes q \leq D_A$$

hence

$$((s_{\{A,B\}} \otimes q_0) \otimes q) \vee ((s_{\{B\}} \otimes q_0) \otimes q) \leq D_A \,.$$

The first disjunct is given by the assumptions $s_{\{A,B\}} \leq D_A$ and D_A being a fact and thus stable under updates, i.e. $(D_A \otimes q_0) \otimes q \leq D_A$. For the other disjunct we shall show that $s_{\{B\}} \otimes q_0 \leq \Box_B D_B \in Ker(q)$ which gives us $(s_{\{B\}} \otimes q_0) \otimes q = \bot$ and $\bot \leq D_A$. To see this use the adjunction to get $f_B(s_{\{B\}} \otimes q_0) \leq D_B$, by eq(1) it suffices to show $f_B(s_{\{B\}}) \otimes f_B(q_0) \leq D_B$. Now replace f_B with its values and get

$(s_{\{B\}} \vee s_{\{A,B\}}) \otimes q_0 \leq D_B$ which is equal to $(s_{\{B\}} \otimes q_0) \vee (s_{\{A,B\}} \otimes q_0) \leq D_B$. This inequality holds since by assumption $s_{\{B\}} \leq D_B$ and also $s_{\{A,B\}} \leq D_B$. Hence the result follows.

Note that this proof can be straightforwardlly extended to the general case by induction on the number of dirty children.

A cryptographic attack.

Two agents A and B share a secret key so that they can send each other encrypted messages over some communication channel. The channel is not secure: some outsider C may interpret the messages or prevent them from being delivered (although he cannot read them because he does not have the key). Suppose the encryption method is publicly known but the key is secret. It is also known that A is the only one who knows an important secret for example if some fact P holds or not. Suppose now that A sends an encrypted message to B communicating the secret. B gets the message and he is convinced that it must be authentic. Now both A and B are convinced that they share the secret and that C doesn't. However suppose that C notices two features of the specific encryption method: first that the shape of the encrypted message can show whether it contains a secret or it is just junk, second that without knowing the key or the content of the message he can modify the encrypted message to its opposite i.e. if it originally said P hold, it will now say that P does not hold. Now the outsider C will secretly intercept the message, change it appropriately and send it to B without knowing the secret. Now A and B mistakenly believe that they share the secret, while in fact B got the wrong secret instead! C has succeeded to manipulate their beliefs.

We can encode this situation in an epistemic system. The agents involved include $\{A, B, C\}$. Let $s, t \in M$ satisfy $s \leq P$ and $t \not\leq P$. The only agent that knows if P holds or not is A thus $f_A(s) = s$ and similarly $f_A(t) = t$. On the other hand B and C do not know this so $f_B(s) = f_C(s) = f_B(t) = f_C(t) = s \vee t$. Call the message in which P holds P and the one in which it does not hold $\bar{P}$. The epistemic actions that correspond to the cryptographic attack are the following: α in which the message P is intercepted, modified and sent to B, β in which the message $\bar{P}$ is intercepted, modified and sent to B, α' in which A sends the message P to B, β' in which A sends the message $\bar{P}$ to B, and finally γ which corresponds to sending a junk message. Thus

$$\{\alpha, \beta, \alpha', \beta', \gamma\} \subseteq Q \quad \text{and} \quad P, \bar{P} \in Stab(Q) \quad \text{and} \quad P \wedge \bar{P} = \bot,\ P \vee \bar{P} = \top\,.$$

In actions α and β agent C is uncertain about which message P or $\bar{P}$ has been sent so $f_C(\alpha) = f_C(\beta) = \alpha \vee \beta$. On the other hand, agent A is sure that he has sent a message (either that P holds or that it doesn't) to B and that B has received exactly the same secret i.e. $f_A(\alpha) = \alpha'$ and $f_A(\beta) = \beta'$. However if P has been sent, B has received $\bar{P}$ so $f_B(\alpha) = \beta'$ and the other way around $f_B(\beta) = \alpha'$. Furthermore

$$f_A(\alpha') = f_B(\alpha') = \alpha'\ ,\ f_A(\beta') = f_B(\beta') = \beta'\ ,\ f_C(\alpha') = f_C(\beta') = \alpha' \vee \beta' \vee \gamma\,.$$

C also considers possible that only a junk message has been sent and that is why he sees γ while in α' and β'. If a junk message has been sent, A and B are sure about it $f_A(\gamma) = f_B(\gamma) = \gamma$ while C is unsure if it was a junk message or P or $\bar{P}$, thus $f_C(\gamma) = \alpha' \vee \beta' \vee \gamma$. The kernel of each action is the states to which the actions cannot be applied. Thus we encode

$$Ker(\alpha) = Ker(\alpha') = \downarrow \bar{P} \;\text{ and }\; Ker(\beta) = Ker(\beta') = \downarrow P\,.$$

The epistemic program $\alpha \vee \beta$ expresses the action of communicating the secret P or $\bar{P}$ in the above scenario. Now let us update the state s with the epistemic program $\alpha \vee \beta$ and show that after update, if P holds, then A knows that B knows that P holds

$$s \otimes (\alpha \vee \beta) \leq \Box_A \Box_B P\,.$$

Since this is equal to

$$(s \otimes \alpha) \vee (s \otimes \beta) \leq \Box_A \Box_B P\,,$$

and $s \leq P \in Ker(\beta)$, we get $s \otimes \beta = \bot$, so it suffices to show that

$$s \otimes \alpha \leq \Box_A \Box_B P\,,$$

but by adjunction $f_B(f_A(s \otimes \alpha)) \leq P$. By eq(1) we get $f_A(s \otimes \alpha) \leq f_A(s) \otimes f_A(\alpha)$, order preservation of f_B will give us

$$f_B(f_A(s \otimes \alpha)) \leq f_B(f_A(s) \otimes f_A(\alpha)) \leq f_B(f_A(s)) \otimes f_B(f_A(\alpha)).$$

Now it suffices to show

$$f_B(f_A(s)) \otimes f_B(f_A(\alpha)) \leq P.$$

Replace the f_A with its values and show $f_B(s) \otimes f_B(\alpha') \leq P$, do the same for f_B and get $(s \vee t) \otimes \alpha' \leq P$, hence $(s \otimes \alpha') \vee (t \otimes \alpha') \leq P$ which is equal to $(s \otimes \alpha') \leq P$ since $t \leq \bar{P} \in Ker(\alpha')$. By the assumption $s \leq P$ we obtain $s \otimes \alpha' \leq P \otimes \alpha'$ which leads to $s \otimes \alpha' \leq P$ because P is a fact.

A non-boolean example.

An intuitive example of an epistemic system $(M, Q, f_A)_{A \in \mathcal{A}}$ where refutations are first class citizens rather than announcements is the refutation of theories in scientific practice. Hence the underlying lattice M is naturally non-boolean. Let the elements of the module M be *theories* written in some logical language e.g. DEL; a theory being a consistent set of sentences closed under logical deduction. For obvious reasons negating a theory $th \in M$ is in general itself not a theory — algebraically a theory should be conceived as a filter. The join in M is the intersection of the sentences belonging to the corresponding theories while the meet is the closure of their union. The quantale Q consists of *experiments* performed by (groups of) agents in order to check some testable consequences of theories. This experiment might be public or private, and some of the outsiders might be deluded into rejecting, misunderstanding or misinterpreting the outcome.[14] The appearance $f_A^M(m)$ of a theory to an agent can be thought of as the agent's interpretation of the theory m, and similarly the appearance $f_A^Q(q)$ is the agent's interpretation of the outcome of an experiment q. Following Popper's conception, a positive result of an experiment cannot provide a proof of a theory but a negative one provides a falsification of the theory, hence we can refute it. For each such refutation $r \in Q$ we have a kernel $Ker(r) \in M$ which tells us which theories can be refuted, namely those which satisfy $th \otimes r = \bot$.

6 The sequent calculus of epistemic systems

We define the objects of our sequent calculus by mutual induction on two sets, the set of *formulas* denoted as $m \in L_M$ and the set of epistemic programs denoted as $q \in L_Q$, respectively

$$m ::= \bot \mid \top \mid p \mid s \mid m \wedge m \mid m \vee m \mid \Box_A m \mid f_A(m) \mid [q]m \mid m \otimes q$$
$$q ::= \bot \mid 1 \mid \sigma \mid q \bullet q \mid q \vee q \mid f_A(q)$$

where A is in the set $\mathcal{A}$ of agents, p is in the set Φ of facts, s is in a set V_M of atomic propositional variables, and σ is in a set V_Q of atomic action variables. We denote by L_M the set of all m-formulas, L_Q the set of all q-formulas, and $\mathcal{A}$ the set of agents. We have two kinds of sequents, M-sequents $\Gamma \vdash_M \delta$ where $\Gamma \in (L_M \cup L_Q \cup \mathcal{A})^*$ and $\delta \in L_M$, and Q-sequents $\Gamma \vdash_Q \delta$ where $\Gamma \in (L_Q \cup \mathcal{A})^*$ and $\delta \in L_Q$. To describe what these sequents mean, we extend the notation to two operations

$$- \odot - : L_M \times (L_M \cup L_Q \cup \mathcal{A}) \to L_M \quad \text{and} \quad - \odot - : L_Q \times (L_Q \cup \mathcal{A}) \to L_Q$$

by putting $q \odot q' := q \bullet q'$, $m \odot A := f_A(m)$, $q \odot A := f_A(q)$, $m \odot q := m \otimes q$, and $m \odot m' := m \wedge m'$. For a sequent

$$\Gamma = (\gamma_1, \cdots, \gamma_n) \in (L_M \cup L_Q \cup \mathcal{A})^* \cup (L_Q \cup \mathcal{A})^*$$

we put $\bigodot \Gamma := ((((\sharp \odot \gamma_1) \odot \gamma_2) \odot \gamma_3) \cdots) \odot \gamma_n$, where $\sharp$ is the top element of M for M-sequents, and the unit element of Q for Q-sequents.[15] Obviously we have

$$\Gamma \in (L_M \cup L_Q \cup \mathcal{A})^* \Rightarrow \bigodot \Gamma \in L_M \quad \text{and} \quad \Gamma \in (L_Q \cup \mathcal{A})^* \Rightarrow \bigodot \Gamma \in L_Q\,.$$

Define a *satisfaction relation* $\models$ on L_M as $m \models m' \Leftrightarrow m \leq m'$ and similarly on L_Q as $q \models q' \Leftrightarrow q \leq q'$. Now a sequent $\Gamma \vdash \delta$ (for either $\vdash_M$ or $\vdash_Q$) is said to be *valid* iff $\bigodot \Gamma \models \delta$. We also allow sequents with empty consequents, denoted as

[14] E.g. arguments for Darwinism such as the discovery of fossils are interpreted by creationists as "the fossils have been put in place by God".

[15] Note that the top element of M is the unit for $\bigodot$ on M (i.e. $\wedge$) and that the unit element of Q (i.e. 1) is the unit for $\bigodot$ on Q (i.e. $\bullet$)

$\Gamma \vdash$. We interpret such a sequent as being equivalent to $\Gamma \vdash \bot$, or in other words $\bigodot \Gamma = \bot$.

The meaning of a sequent.

The *meaning* of a sequent $\Gamma \vdash \delta$ is given by its corresponding satisfaction statement $\bigodot \Gamma \models \delta$. To provide the reader with a way to "read out" our sequents in natural language, we capture the *intuitive meaning* of an M-sequent (Q-sequents can be read in a similar way) $\Gamma \vdash_M \delta$ in the following inductive manner:

- $A, \Gamma \vdash_M \delta$ means that agent A knows, or believes, that $\Gamma \vdash_M \delta$ holds. So this captures features of A's own reasoning: the sequent $\Gamma \vdash_M \delta$ is accepted by A as a valid argument.
- $q, \Gamma \vdash_M \delta$ means that, after action q happens, the sequent $\Gamma \vdash_M \delta$ will hold.
- $m, \Gamma \vdash_M \delta$ means that, in context m (i.e. in any situation in which m is true), the sequent $\Gamma \vdash_M \delta$ must hold.

For instance, the sequent $m, A, q, B, m' \vdash_M m''$ can be read as: in context m, agent A believes that after action q agent B will believe that, in context m', proposition m'' must hold .

This reading shows that our sequent calculus expresses two forms of resource sensitivity. One is the use-once form of linear logic [14] that comes from the quantale structure on epistemic programs. This, as will be seen later, is encoded in the Lambek calculus rules on Q-sequents. One could call these *dynamic resources* . The other form deals with *epistemic resources* : the resources available to each agent that enable him to reason in a certain way (i.e. to deduct a result from some assumptions). These resources are encoded in the way the context appears to the agent in sequents, for instance Γ in the sequent $\Gamma, A, \Gamma' \vdash_M \delta$ is the context and hence the $f_A(\Gamma)$ is the resource that enables agent A to do the $\Gamma' \vdash_M \delta$ reasoning. Note that $\Gamma' \vdash_M \delta$ might not be a valid sequent in the context Γ, but it is valid in the context given by Γ's appearance to agent A. To summerize, in our setting not only propositions, but also actions and agents are treated as resources (available or not for other actions or for reasoning of other agents).

Sequent rules.

The rules for identity, $\bot$, and 1 (on the left) are the same for both M and Q sequents. So in the following we drop the subscripts of $\vdash$ where applicable:

$$\frac{}{\bot,\Gamma \vdash \delta}\ (\bot L) \qquad \frac{\Gamma \vdash}{\Gamma \vdash \bot}\ (\bot R) \qquad \frac{}{\Gamma \vdash_M \top}\ (\top R)$$

$$\frac{}{\delta \vdash \delta}\ (Id) \qquad \frac{}{\vdash_Q 1}\ (1R) \qquad \frac{\Gamma,\Gamma' \vdash \delta}{\Gamma,1,\Gamma' \vdash \delta}\ (1L)$$

The **operational rules for M-sequents** are

$$\frac{\Gamma,q \vdash_M \delta}{\Gamma \vdash_M [q]\delta}\ ([\,]R) \qquad \frac{m,\Gamma \vdash_M \delta}{[q]m,q,\Gamma \vdash_M \delta}\ ([\,]L)$$

$$\frac{\Gamma,A \vdash_M \delta}{\Gamma \vdash_M \Box_A \delta}\ (\Box R) \qquad \frac{m,\Gamma \vdash_M \delta}{\Box_A m,A,\Gamma \vdash_M \delta}\ (\Box L)$$

$$\frac{\Gamma \vdash_M \delta}{\Gamma,A \vdash_M f_A^M(\delta)}\ (f_A^M R) \qquad \frac{m,A,\Gamma \vdash_M \delta}{f_A^M(m),\Gamma \vdash_M \delta}\ (f_A^M L)$$

$$\frac{\Gamma,m,m',\Gamma' \vdash_M \delta}{\Gamma,m \wedge m',\Gamma' \vdash_M \delta}\ (\wedge L) \qquad \frac{\Gamma \vdash_M \delta \qquad \Gamma \vdash_M \delta'}{\Gamma \vdash_M \delta \wedge \delta'}\ (\wedge R)$$

$$\frac{\Gamma \vdash_M \delta}{\Gamma \vdash_M \delta \vee \delta'}\ (\vee R_1) \qquad \frac{\Gamma \vdash_M \delta'}{\Gamma \vdash_M \delta \vee \delta'}\ (\vee R_2)$$

$$\frac{m,\Gamma \vdash_M \delta \quad m',\Gamma \vdash_M \delta}{m \vee m',\Gamma \vdash_M \delta}\ (\vee_M L) \qquad \frac{\Gamma,q,\Gamma' \vdash_M \delta \quad \Gamma,q',\Gamma' \vdash_M \delta}{\Gamma,q \vee q',\Gamma' \vdash_M \delta}\ (\vee_Q L)$$

$$\frac{\Gamma \vdash_M \delta}{\Gamma,q \vdash_M \delta \otimes q}\ (\otimes R) \qquad \frac{\Gamma_M,\, q,\Gamma' \vdash_M \delta}{\Gamma_M \otimes q,\Gamma' \vdash_M \delta}\ (\otimes L)$$

$$\frac{\Gamma,q,q',\Gamma' \vdash_M \delta}{\Gamma,q \bullet q',\Gamma' \vdash_M \delta}\ (\bullet ML)$$

where $\Gamma_M \in L_M^*,\ \Gamma_Q \in L_Q^*,\ \Gamma_A \in \mathcal{A}^*,\ \delta, \delta' \in L_M$ and if $\Gamma_M = (m_1, \cdots, m_n)$ then $\Gamma_M \otimes q := (m_1 \otimes q, \cdots, m_n \otimes q)$.

The **operational rules for Q-sequents** consist of Lambek calculus rules for $\vee$, plus the following rules for $\bullet$ and f_A

$$\frac{\Gamma_Q,\Gamma_A \vdash_Q \delta \qquad \Gamma'_Q,\Gamma_A \vdash_Q \delta'}{\Gamma_Q,\Gamma'_Q,\Gamma_A \vdash_Q \delta \bullet \delta'}\ (\bullet QR) \qquad \frac{\Gamma,q_1,q_2,\Gamma' \vdash_Q \delta}{\Gamma,q_1 \bullet q_2,\Gamma' \vdash_Q \delta}\ (\bullet QL)$$

$$\frac{\Gamma \vdash_Q \delta}{\Gamma,A \vdash_Q f_A^Q(\delta)}\ (f_A^Q R) \qquad \frac{\Gamma_Q,A,\Gamma \vdash_Q \delta}{f_A^Q(\Gamma_Q),\Gamma \vdash_Q \delta}\ (f_A^Q L)$$

where $\delta, \delta' \in L_Q$ and for $\Gamma_Q = (q_1, q_2, \cdots)\,,\ f_A(\Gamma_Q) = f_A(q_1) \bullet f_A(q_2) \bullet \cdots$.

As **structural rules** we have two M-Weakenings, Q-Weakening, M-Contraction, and M-Exchange, respectively

$$\frac{\Gamma \vdash_M \delta}{\Gamma',\Gamma \vdash_M \delta}\ (weak_1) \qquad \frac{\Gamma,\Gamma' \vdash_M \delta}{\Gamma,m,\Gamma' \vdash_M \delta}\ (weak_2) \qquad \frac{\Gamma \vdash_Q \delta}{A,\Gamma \vdash_Q \delta}\ (weak_A)$$

$$\frac{\Gamma,m,m,\Gamma' \vdash_M \delta}{\Gamma,m,\Gamma' \vdash_M \delta}\ (contr) \qquad \frac{\Gamma,m,m',\Gamma'' \vdash_M \delta}{\Gamma,m',m,\Gamma'' \vdash_M \delta}\ (exch)$$

two rules expressing *Invariance of facts (under epistemic actions)* (rules which can be seen as “Action Weakening’ and “Action Strengthening” in M-sequents)

$$\boxed{\frac{\Gamma \vdash_M P}{\Gamma, q \vdash_M P}\ (fact_1) \quad \frac{\Gamma, q \vdash_M P}{\Gamma \vdash_M P}\ (fact_2)}$$

where $P \in \Phi$ (the set of facts), and finally several restricted versions of the Cut Rule: propositional cut in M-sequents, action cut in Q sequents and action cut in mixed $M - Q$ sequents [16]

$$\boxed{\begin{array}{ll} \dfrac{\Gamma \vdash_M m \quad m, \Gamma' \vdash_M \delta}{\Gamma, \Gamma' \vdash_M \delta}\ (MCut) & \dfrac{\Gamma \vdash_Q q \quad q, \Gamma' \vdash_Q \delta}{\Gamma, \Gamma' \vdash_Q \delta}\ (QCut) \\ \dfrac{\Gamma_Q, \Gamma_A \vdash_Q q \quad \Gamma, \Gamma_A,\, q \vdash_M \delta}{\Gamma, \Gamma_Q, \Gamma_A \vdash_M \delta}\ (MQCut) & \end{array}}$$

Theorem 6.1 (Completeness). The rules presented above are sound and complete with regard to the algebraic semantics given by epistemic systems.

Proof (Sketch). Denote the equivalence relation created by logical consequence $\vdash\dashv$ as $\cong$. We construct two Lindenbaum-Tarski algebras: M_0 of equivalence classes of M-formulas over $\cong_M$ and Q_0 of equivalence classes of Q-formulas over $\cong_Q$. Using the sequent rules we first show that all the algebraic operations of epistemic systems $\vee, f_A, \Box_A, \otimes, [\,], \bullet$ are well-defined over equivalence classes of formulas. We then show that $(M_0, Q_0, \{f_A\}_{A \in \mathcal{A}})$ satisfies the finite versions of all the equations of an epistemic system. We embed this structure into an epistemic system $(M, Q, \{f_A\}_{A \in \mathcal{A}})$ by taking $M = Idl(M_0)$ and $Q = Idl(Q_0)$ where e.g. $Idl(M_0)$ is the family of ideals over M_0 with inclusion as order and intersection as meet. The rest of operations $\vee, f_A, \otimes, \bullet$ are extended to ideals by applying them pointwise and then taking the downward closure. Finally we show that $(M, Q, \{f_A\}_{A \in \mathcal{A}})$ forms an epistemic system and that $(M_0, Q_0, \{f_A\}_{A \in \mathcal{A}})$ is faithfully embedded in it. □

7 Conclusion and elaborations

We have developed an algebraic axiomatics in terms of a simple mathematical object: a sup-lattice M, which encodes states, epistemic propositions as well as facts; a quantale Q (acting on M) which encodes update by epistemic programs; and a family of endomorphisms of the $(M, Q, \bigvee_M, \bigvee_Q, \otimes, \bullet, 1)$-structure encoding the agents in terms of their epistemic modalities. From this structure many useful other modalities arise, including dynamic modalities and residuals. This algebraic axiomatics generalizes Dynamic Epistemic Logic to non-boolean settings, while still capturing the same concepts. Furthermore it provides an algebraic way of dealing with epistemic scenarios such as the muddy children puzzle. We list some possible further elaborations on this line of thought.

- We would like to develop a boolean version of the sequent calculus presented

[16] We think these cuts are eliminable and are working on the **Cut-Elimination** theorem.

here for concrete epistemic systems and prove its completeness with regard to Kripke semantics. Such a development will lead to a more refined version of our representation Theorem 4.6 for a boolean dynamic epistemic logic.

- In this paper, following dynamic epistemic logic, we dealt with the same update schema for all agents. This is a postulate of "uniform rationality" and it means that the mechanism for information update is the same for all agents. It makes sense, if not being necessary, to consider personalized updates, where each agent updates his information in a different way than other agents do. We think that such personalized updates could be better dealt with by moving to a categorical semantics. We are currently working on such semantics. It would also be interesting to compare our categorical approach with coalgebraic epistemic features which are currently studied e.g. [3].
- Part of the motivation of this work was a marriage of epistemics and resource-sensitivity [20]. Although we have introduced dynamic and epistemic resources in our setting, we would like to refine our logic and make it more resource-sensitive by relativizing our notion of "consequence" to "logical" actions available to agents. This will allow us to deal with classical resource sensitive problems such as the problem of logical omniscience.

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, 'Logics for communication: reasoning about information flow in dialogue games', *Second North American Summer School in Logic, Language, and Information*, http:// www.indiana.edu/˜nasslli/program.html, Indiana University, 2003.

[3] A. Baltag, 'A coalgebraic semantics for epistemic programs', Proceedings of *Coalgebraic Methods in Computer Science 03*, 2003.

[4] A. Baltag, and L.S. Moss, 'Logics for epistemic programs', *Synthese* **139**, 2004.

[5] A. Baltag, L.S. Moss and S. Solecki, 'The logic of public announcements, common knowledge and private suspicions', CWI Technical Report SEN-R9922, 1999.

[6] A. Baltag, B. Coecke, M. Sadrzadeh, 'Epistemic actions as resources' in Proceedings of *Logics for Resources, Programs, Processes* (LRPP) workshop in LiCS 2004,`http://www.er.uqam.ca/nobel/philmath/LicsWSPROC.pdf`.

[7] B. Coecke, D.J. Moore and I. Stubbe, 'Quantaloids describing causation and propagation of physical properties', *Foundations of Physics Letters* **14**, 133-145, 2001.

[8] E.W. Dijkstra, *A Discipline of Programming*, Prentice-Hall, 1976.

[9] R. Fagin, J.Y. Halpern, Y. Moses and M.Y. Vardi, *Reasoning about Knowledge*, MIT Press, 1995.

[10] G. Gierz, K.H. Hofmann, K. Keimel, J.D. Lawson, M.W. Mislove and D.S. Scott, *A Compendium of Continuous Lattices*, Springer-Verlag, 1980.

[11] J. Gerbrandy, ‘Dynamic Epistemic Logic’, in L.S. Moss, et al (eds.) *Logic, Language, and Information* **2**, Stanford University, CSLI Publication, 1999.

[12] J. Gerbrandy, *Bisimulation on Planet Kripke*, Ph.D. dissertation, University of Amesterdam, 1999.

[13] J. Gerbrandy, and W. Groenveld, ‘Reasoning about information change’, *Journal of Logic, Language, and Information* **6**, 1997.

[14] J-Y. Girard, ’Linear logic’, *Theoretical Computer Science* **50**,1-102, 1987.

[15] D. Harel, D. Kozen and J. Tiuryn, *Dynamic Logic*, MIT Press, 2000.

[16] C.A.R. Hoare and Jifeng, HE, ‘The weakest prespecification’, *Information Processing Letters* **24**, 127-132, 1987.

[17] P.T. Johnstone, *Stone Spaces*, Cambridge University Press, 1982.

[18] A. Joyal and M. Tierney, ‘An extension of the Galois theory of Grothendieck’, *Memoirs of the American Mathematical Society* **309**, 1984.

[19] J. Lambek, ‘The mathematics of sentence structure’, *American Mathematics Monthly* **65**, 154-169, 1958.

[20] M. Marion and M. Sadrzadeh, ‘Reasoning about knowledge in linear logic: modalities and complexity’, D. Gabbay, S. Rahman, J.M. Torres and J.-P. Van Bendegem (eds.), *Logic, Epistemology, and the Unity of Science*, Kluwer, 2004.

[21] C.J. Mulvey, &, *Supplemento ai Rendiconti del Circolo Matematico di Palermo* **II**, 99-104, 1986.

[22] J. Plaza, ‘Logics of public communications’, *Proceedings of 4th International Symposium on Methodologies for Intelligent Systems*, 1989.

[23] P. Resende, ‘Quantales and observational semantics’, B. Coecke, D.J. Moore and A. Wilce (eds.), *Current Research in Operational Quantum Logic*, Kluwer, 263-288, 2000.

[24] K.I. Rosenthal, *Quantales and their Applications*, Pitman Research Notes in Mathematics Series **234**, Longman, 1990.

[25] I. Stubbe, *Categorical Structures Enriched in a Quantaloid: Categories and Semicategories*, Ph.D. Thesis, Université Catholique de Louvain, 2003.

[26] J. Van Benthem, ‘Logic in action’, *Journal of Philosophical Logic* **20**, 225-263, 1989.

[27] F. Wolter and M. Zakharyaschev, ‘The relation between intuitionistic and classical modal logics, *Algebra and logic* **36**, 73-92, 1997.