Reasoning about Dynamic Epistemic Logic

Alexandru Baltag and Bob Coecke
Oxford University Computing laboratory
baltag / coecke@comlab.ox.ac.uk

Mehrnoosh Sadrzadeh
Université du Québec À Montréal
sadrzadeh.mehrnoosh@courrier.uqam.ca

Abstract

We present an algebra and sequent calculus to reason about dynamic epistemic logic, a logic for information update in multi-agent systems. We contribute to it by equipping it with a logical account of resources, a semi-automatic way of reasoning through the algebra and sequent calculus, and finally by generalizing it to non-boolean settings.

Dynamic Epistemic Logic (DEL) is a PDL-style logic [14] 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, software reliability for concurrent programs, *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 [8] 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 [19], Gerbrandy and Groeneveld [12], and Gerbrandy [10, 11]. However, they only studied a restricted class of epistemic programs. A general notion of epistemic programs and updates for DEL was introduced in [5]. In our papers [2, 3], we introduced an algebraic semantics based on the notion of *epistemic systems* and a sequent calculus for a version of DEL, but the completeness of the sequent calculus was still an open problem. In this paper, we summarize the material in [2, 3] and present an updated version of the sequent calculus for which we have proved the completeness theorem with regard to the algebraic semantics.

Our work contributes to DEL in three ways. First, it introduces a logical account of actions and agents as *dynamic* and *epistemic resources* in situations of information exchange. In these situations each new repetition of the same announcement might add new information to the agents. Thus it makes a difference whether or not unlimited "supplies" of these actions are available. We consider epistemic action as *dynamic resources* , which are similar to the usual use-only-once resources of linear logic [13]. We will also deal with *epistemic resources* to capture the presence of agents in a given situation (or availability of agents as computing resources for other agents). These resources capture the cases where presence of agents makes a difference in the validity of some deductions and execution of some actions by other agents. In other words, some deductions are only valid (and some actions are only executable) in the presence of certain agents, i.e. valid not in the real world, but in the world as it *appears* to these agents. Note that agents and actions are not only resources but also "consumers of resources"; actions need certain preconditions to be executable and agents need certain contexts to be able do their reasoning.

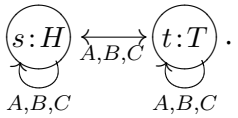
Our second contribution to DEL focuses on the structure of epistemic programs by considering them as fundamental operations of an abstract algebraic structure rather than concrete constructions on Kripke structures. This move enables us to reason about epistemic programs and their updates in a semi-automatic way through algebraic equations as well as proof search in a sequent calculus (whose development was much facilitated by the algebraic structure). In this setting, agents and propositions as well as actions are considered in Lambek-calculus style sequents which will typically look like

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

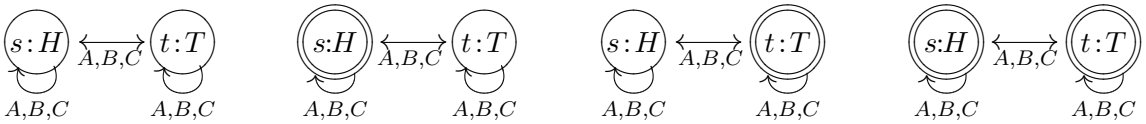
where $m_1, \ldots, m_k$ are propositions, $q_1, \ldots, q_l$ are programs and $A_1, \ldots A_n$ are agents which resolve into a single proposition or program δ. The fragment of the calculus restricted to programs is the Lambek calculus [17], which can be modelled by a quantale Q. The interaction between programs and states is modelled by the action of Q on a Q-right module. This fragment of our structure has been used to study concurrency in computer science [1, 21] and the dynamics and interaction of physical systems [7]. The crucial additional epistemic features are captured by (lax) endomorphisms of the above structure, one endomorphism for each agent.

Finally, in our third contribution we generalize the boolean setting of DEL to non-boolean contexts that model partiality of knowledge and information update. In such settings the negation of a propositions or program is not necessarily a proposition or program. An example would be information update in AI where refutation of a robot's beliefs via epistemic programs such as communication with other robots or environment, would not necessarily be a new belief. In the same line, the negation of an epistemic program might not be a program . The generalization to non-boolean settings also enables us to encode information update in an intuitionistic and thus computational way. For a more elaborated example please refer to [2].

Cheating scenario. As an example consider a game **Toss** with 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), and state t in which the coin lies Tails up (T). We depict the state model **Toss** as

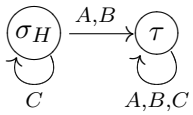


For every agent there are arrows between any two states (including identical states), which means that nobody knows the 'real state'. These arrows signify the accessibility relation for each agent and can be re-packaged as appearance maps f_A for each agent A. The significance of these maps is that if $t \in f_A(s)$ then whenever state s is possible for agent A, he also considers state t as possible. H and T are facts, i.e. the objective part of the world that in this case expresses the heads up or tails up of the coin. The subsets of states i.e. $\emptyset, \{s\}, \{t\}, \{s, t\} \subseteq \{s, t\}$ correspond to *epistemic propositions* over **Toss**. The epistemic propositions corresponding to facts are the states in which the facts hold, in this case $\{s\}, \{t\}$ are epistemic propositions corresponding to facts H and T. Depicting an epistemic proposition over a state model by double-circling the included states gives us the following models



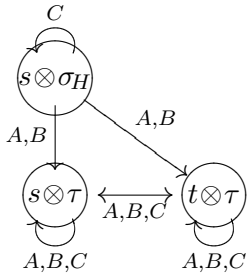
that represent the four epistemic propositions of **Toss**.

Now consider the **cheating program** where after catching the coin in his hand the referee secretly takes a peek at the coin before covering it and realizes that it is heads up while nobody notices this. This is an epistemic program and can be expressed by the action model **Cheat** depicted as



where σ_H stands for 'cheating' and τ for 'nothing happens'. The states where this cheating action cannot happen are the states in which the fact H is not true. In other words the 'kernel' of σ_H is $\{t\}$. In σ_H, the appearance maps for agents are $f_C(\sigma_H) = \{\sigma_H\}$ and $f_A(\sigma_H) = f_B(\sigma_H) = \{\tau\}$ that is agent C knows that a cheating has happened where as agents A and B think nothing has happened.

Update. Given the state model **Toss** and the action model **Cheat**,their update product is a new state model that expresses the state of the world after the cheating action. In this example, after **Cheat** the coin has lied heads up, and agent C knows it. However, agents A and B think that nobody knows on which side the coin is lying. But they are wrong! This is expressed by the update product **Toss** $\otimes$ **Cheat** depicted as



In the updated model, we denote for example by $s \otimes \sigma_H$ the output state obtained by applying action σ_H to input state s. The updated appearance of the cheating action to agent C i.e. $f_C(s \otimes \sigma_H)$ is equal to $\{s \otimes \sigma_H\}$ which implies that agent C has certain knowledge of the situation. On the other hand $f_A(s \otimes \sigma_H) = f_B(s \otimes \sigma_H) = \{s \otimes \tau, t \otimes \tau\}$ implies A and B are still uncertain about the face of the coin. To complete our pictorial introduction of epistemic concepts, we define the sequential composition of two epistemic actions σ and σ' as $\sigma \bullet \sigma' \subseteq \sigma \times \sigma'$ and interpret it as 'first do σ, then do σ''. For a more detailed discussion of the concepts introduced here, we refer the reader to [2].

Algebraic model: epistemic systems. The algebraic semantics of epistemic propositions and updates is given by *epistemic systems* i.e. $(M, Q, \{f_A\}_{A\in\mathcal{A}})$. The first part of an epistemic system (M, Q) is a *system*, i.e. a pair quantale Q and module M with a right action $- \otimes - : M \times Q \to Q$. A quantale Q is a complete lattice with join preserving maps (sup-lattice for short) together with a monoid structure $(Q, \bullet, 1)$ on it. An example of a complete lattice is the power set of a set X. An example of a quantale would be the set of relations on a set X or $\mathcal{P}(X \times X)$. A Q-right module M is also a sup-lattice with a right action $- \otimes - : M \times Q \to M$ on the quantale. The module right action has to preserve the unit of quantale $m \otimes 1 = m$ and all joins on both arguments $(\vee_M m_i) \otimes q = \vee_M (m_i \otimes q)$ and $m \otimes (\vee_Q q_i) = \vee_M (m \otimes q_i)$. Note that for a set X its powerset $\mathcal{P}(X)$ forms a right module over its quantale $\mathcal{P}(X \times X)$. For more details and examples of these concepts refer to [1]. The second part of an epistemic system consists of a family of endomorphisms $\{f_A\}_{A\in\mathcal{A}}$ of the system $f_A = (f_A^M, f_A^Q)$ where $f_A^M : M \to M$ and $f_A^Q = Q \to Q$. These maps are required to satisfy an *update inequality*

$$f_A^M(m \otimes q) \leq f_A^M(m) \otimes f_A^Q(q)\,.$$

We call the elements of the quantale *epistemic programs*, the elements of the module *epistemic propositions* and the endomorphisms f_A the *appearance maps* of agent A. The module right action $M \otimes Q \to M$ is the epistemic update of a proposition by a program. The update relation $f_A^M(m \otimes q) \leq f_A^M(m) \otimes f_A^Q(q)$ says that agents update their knowledge according to the way they perceive the proposition and the program. Since the partial order on M i.e. $m \leq m'$ is the logical entailment between propositions $m \vdash m'$, the update relation being an inequality insists on learning of agents after update, since the perception of the updated proposition entails the perception of the non-updated ones. Comparing the entailment on the appearance maps $f_A^M(m) \vdash f_A^M(m')$ with the entailment of propositions $m \vdash m'$ enables us to deal with interesting situations such as having a wrong perception of the world due to deceit. For example if $m \nvdash m'$ but $f_A^M(m) \vdash f_A^M(m')$ then agent A has been deceived since in reality m does not imply m' but he thinks it does! In the same way if $f_A^M(m) = m$ then agent A has certain knowledge of what is going on in reality where as if $f_A^M(m) = \top$ then he has absolutely no knowledge of reality (everything is possible for him).

The appearance map of programs $f_A^Q(q)$ to agents expresses how agents perceive the programs. The partial order on the programs in Q is also the entailment between programs. For example $q \vdash q'$ says that program q is more deterministic than program q'. Epistemic actions of **DEL** such as *information hiding* or *encryption* and *misinformation* such as lying and cheating are dealt with in sequents like $q \vdash f_A^Q(q)$ and $q \nvdash f_A^Q(q)$ respectively.

The module action or the update product can be seen as a one argument map $- \otimes q : M \to M$ on M. By definition this map preserves all joins and thus has a meet-preserving Galois right adjoint. The Galois right adjoint to the update $- \otimes q \dashv [q]-$ is the dynamic modality of dynamic logic or the weakest precondition [15] of program q. Recall that in dynamic logic $[q]m$ means after running program q the proposition m holds. The epistemic modality $\Box_A m$, which says agent A *knows* or *believes* that m[1], also comes from an adjunction. It is the Galois right adjoint to appearance maps $f_A(-) \dashv \Box_A -$. In any epistemic system we have

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

In the special case where the module M is a boolean algebra, the first property corresponds to axioms T, and the last correspond to axiom K or monotonicity of normal modal logics [8].

Using the dynamic modality we can now define *facts* as a part of the system that is *stable* under update

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

The kernel of each action q that consists of propositions to which q cannot be applied is defined as

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

where $\bot$ is the false proposition. For a more detailed discussion of the algebra and its interpretation, in particular the appearance maps, we refer the reader to [3].

Cheating scenario revisited. As an example we will now encode the 'cheating' scenario algebraically. We will then briefly show how this encoding enables us to reason about the knowledge of agents after update in a semi-automatic way. For the set of agents $\mathcal{A} = \{A, B, C\}$, 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, that is given

[1]The $\Box$ modality covers both knowledge and belief. In contexts where no wrong belief is allowed it can be read as knowledge, i.e. justified true belief, in the rest as justified belief.

an epistemic system $(M, Q, \{f_A\}_{A\in\mathcal{A}})$, $s, t \in M$ and $\sigma_H \in Q$. Facts are stable propositions of module $H, T \in M$. All these are assumed to satisfy the following conditions: $f_i(s) = f_i(t) = s\vee t$ for all $i \in \mathcal{A}$ and $s \leq H, t \leq T, H \wedge T = \bot$; the epistemic program $\sigma_H \in Q$ has maps $f_A(\sigma_H) = f_B(\sigma_H) = \tau$ and $f_C(\sigma_H) = \sigma_H$, and kernel $Ker(\sigma_H) = t$. 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.

We can now prove propositions about the impact of update on the knowledge of agents. For example after the cheating update agent C knows that the coin is heads up

$$s \otimes \sigma_H \leq \Box_C H\,.$$

The proofs goes smoothly by using the adjunction and moving the epistemic modality to the left hand side of the inequality

$$f_C(s \otimes \sigma_H) \leq H\,.$$

We will then use the update inequality to distribute the f_C over its arguments and then replace the parameters by their encoded values

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

which is equal to $s \otimes \sigma_H$ since $t \in Ker(\sigma_H)$. All we have to do now is to show $s \otimes \sigma_H \leq H$, which is obvious recalling the order $s \leq H$ and the stability of H under σ_H.

More examples including the muddy children puzzle and a MITM cryptographic attack have been discussed in full detail in [2, 3]. The muddy children puzzle shows the importance of repetition of epistemic actions where as the cryptographic attack uses different sorts of epistemic programs that signify private and public message passing that might lead to deceit of agents in the internet.

Sequent Calculus. 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

$$\begin{array}{rcl} m & ::= & \bot \mid \top \mid p \mid s \mid m \wedge m \mid m \vee m \mid \Box_A m \mid f_A^M(m) \mid [q]m \mid m \otimes q \\ q & ::= & \bot \mid 1 \mid \sigma \mid q \bullet q \mid q \vee q \mid f_A^Q(q) \end{array}$$

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.

We have two kinds of sequents

- M-sequents $\Gamma \vdash_M \delta$ where Γ is a sequence of propositions, programs and agents $\Gamma \in (L_M \cup L_Q \cup \mathcal{A})^*$ and δ is a proposition $\delta \in L_M$.
- Q-sequents $\Gamma \vdash_Q \delta$ where Γ is a sequence of programs and agents $\Gamma \in (L_Q \cup \mathcal{A})^*$ and δ is a program $\delta \in L_Q$.

To describe what these sequents mean, we require commas to apply to the left and we define their role as follows

$$q, q' := q \bullet q' \qquad m, A := f_A(m) \qquad q, A := f_A(q) \qquad m, q := m \otimes q \qquad m, m' := m \wedge m'\,.$$

For example, a sequence $\Gamma = (m, A, q, B, m')$ means $m' \wedge f_B(f_A(m) \bullet q)$. In this way we identify any M-sequence Γ with a corresponding element of M and similarly for Q-sequences[2].

The *satisfaction relation* $\models$ on each sequence is defined as

[2] If the M-sequence does not start with an element of M, we have to add $\top_M$ to its left. Similarly for a Q-sequence we add 1 to its left.

- $\Gamma \models_M m'$ iff $\Gamma \leq_M m'$,
- $\Gamma \models_Q q'$ iff $\Gamma \leq_Q q'$,

The *meaning* of a sequent $\Gamma \vdash \delta$ is given by the corresponding satisfaction statement $\Gamma \models \delta$. To provide the reader with a way to "read out" our sequents in natural language, we capture the *intuitive meaning* of a sequent $\Gamma \vdash \delta$ in the following inductive manner [3]:

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

This more "intuitive" reading can be obtained by taking the adjoints (which live on the right-side of $\vdash$) of the formulas on the left hand side of a sequent. That is why the reading has a reverse order (left to right) than the comma application (right to left). For instance, the sequent $m, A, B \vdash_M m'$ after applying commas on the left would mean $f_B(f_A(m)) \leq m'$, and after applying the adjoints would correspond to $m \leq \Box_A \Box_B m'$. This has now the exact shape of its intuitive meaning which is 'in context m agent A believes that agent B believes that m''[4].

This reading shows that our sequent calculus expresses two forms of resource sensitivity. One is the use-once form of linear logic [13] 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 summarize, 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

[3] Sequents with empty consequents, denoted as $\Gamma \vdash$ are equivalent to $\Gamma \vdash \bot$.

[4] Examples such as $\Gamma, m \vdash m'$ make more sense when M is a Heyting Algebra with the adjunction between implication and conjunction i.e. $a \wedge b \leq c$ iff $a \leq b \to c$

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

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

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

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

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

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

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

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

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)

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

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[5]

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

$$\frac{\Gamma \vdash_M m \quad m,\Gamma' \vdash_M \delta}{\Gamma,\Gamma' \vdash_M \delta}\ (MCut) \qquad \frac{\Gamma \vdash_Q q \quad q,\Gamma' \vdash_Q \delta}{\Gamma,\Gamma' \vdash_Q \delta}\ (QCut)$$

$$\frac{\Gamma_Q,\Gamma_A \vdash_Q q \quad \Gamma,\Gamma_A,\, q \vdash_M \delta}{\Gamma,\Gamma_Q,\Gamma_A \vdash_M \delta}\ (MQCut)$$

Theorem (completeness). The sequent calculus presented above is sound and complete with regard to the algebraic semantics given by epistemic systems.

Example of derivation. We prove a non-Boolean version of the so-called "Action-Knowledge Axiom" of DEL, stated in [5], which allows one to permute the dynamic and epistemic modalities in a certain way:

$$\Box_A[f_A^Q(q)]m \vdash [q]\Box_A m\,.$$

To prove this axiom, let Γ be the formula $\Box_A[f_A^Q(q)]m$. Then we have $\Gamma \vdash \Box_A[f_A^Q(q)]m$, by the Identity rule (Id), and so we have the derivation :

$$\dfrac{\dfrac{\Gamma \vdash \Box_A[f_A^Q(q)]m \quad \dfrac{[f_A^Q(q)]m \vdash [f_A^Q(q)]m}{\Box_A[f_A^Q(q)]m, A \vdash [f_A^Q(q)]m}\,\Box L}{\dfrac{\Gamma, A \vdash [f_A^Q(q)]m}{\Gamma, A, f_A^Q(q) \vdash [f_A^Q(q)]m \otimes f_A^Q(q)}\,\otimes R} MCut \qquad \dfrac{q \vdash q}{q, A \vdash f_A^Q(q)}\,f_A^Q R \qquad \dfrac{\dfrac{m \vdash m}{[f_A^Q(q)]m, f_A^Q(q) \vdash m}\,DyL}{[f_A^Q(q)]m \otimes f_A^Q(q) \vdash m}\,\otimes L}{\dfrac{\Gamma, q, A \vdash [f_A^Q(q)]m \otimes f_A^Q(q)}{\dfrac{\Gamma, q, A \vdash m}{\dfrac{\Gamma, q \vdash \Box_A m}{\Gamma \vdash [q]\Box_A m}\,DyR}\,\Box R}\,MQCut}\,MCut$$

Application: *A "Coordinated Attack"*. The derived rule corresponding to the "Action-Knowledge Axiom" can be used to predict the knowledge (or beliefs) of an agent after an action, based only on action's appearance to the agent and on his prior beliefs (before the action). For instance, suppose that in order to coordinate their attacks, general A sends to general B a message m, meaning "Atack at dawn!"; but suppose the messenger has been caught by the enemy, who substitutes him with a fake messenger bearing another message m', saying "Attack in the morning!". Suppose general B *does not suspect* this was hapenning. We denote by q the "real" action going on (i.e. the action of A sending message m), and by q' the action of A sending message m'. Then we encode the *content* of (the message sent during) these actions by stating as additional axioms: $q \vdash_M m$ and $q' \vdash_M m'$. We also encode the *appearance* of these actions, e.g. putting $f_B(q) = q'$, to encode the fact that, when q happens, B thinks that q' is happening. To predict what will B believe after the action q, first use the $[\,]$-right introduction to derive from $q' \vdash_M m'$ that $\vdash [q']m'$, then apply M-Weakening $(weak_1)$ to get $B \vdash [q']m'$. Apply $\Box$-introduction to the right to get $\vdash \Box_B[q']m'$. Then use the above derived rule corresponding to the "Action-Knowledge Axiom" and the fact that $f_B(q) = q'$, to conclude that $\vdash [q]\Box_B m'$. So we can predict that, after receiving the fake message, general B will believe that he is supposed to attack in the morning.

More generally, by adding additional rules, we can encode various dynamic epistemic scenarios [2, 3], such as the Cheating Scenario discussed above, and prove their properties using the sequent rules. For example, in [3] we have encoded a version of the *Man-in-the-Middle* cryptographic attack, and we have proved some of its properties using the sequent calculus above.

Further elaborations

1. Concerete epistemic systems. We would like to develop a boolean version of our sequent calculus and prove its completeness with regard to kripke semantics.

2. Coalgebras. We are enriching our algebra with personalized updates by moving to a categorical algebraic semantics studied in [22]. It would be interesting to investigate the connection between our categorical methods and the coalgebraic methods studied in e.g. [4].

3. Resource sensitivity. We would like to make our systems more resource sensitive to deal with classical resource sensitive problems in epistemic logic such as *logical omniscience* [18]. The *money games* of [16] and The *logic of bunched implications* of [20] might provide useful insights, fragments and tools.

Acknowledgements. We thank Samson Abramsky, André Joyal, Dusko Pavlovic, and Isar Stubbe for valuable discussions. M. S. thanks Samson Abramsky and Oxford University Computer Laboratory for their hospitality and thanks Mathieu Marion for his logistic support.

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, 'Algebra and sequent calculus for epistemic actions' in Proceedings of *Logic and Communication in Multi-Agent Systems* (LCMAS) workshop in ESSLLI 2004, `http://www.er.uqam.ca/nobel/philmath/esslliPROC2.pdf`.

[3] A. Baltag, B. Coecke and 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`.

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

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

[6] B. Coecke and K. Martin. *A Partial Order on Classical and Quantum States*. Research Report PRG-RR-02-07, Oxford University Computing Laboratory, 2002.

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

[9] 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.

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

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

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

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

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

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

[16] A. Joyal. 'Free lattices, communication and money games'. In: M. L. Dalla Chiara et al. (eds.), *Logic and Scientific Methods*, Kluwer, 29–68 (1997).

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

[18] 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.

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

[20] P. W. O'Hearn and D. J. Pym. 'The logic of bunched implications'. *Bulletin of Symbolic Logic* **5**, 215–244 (1999).

[21] 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.

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

[23] J. Van Benthem, 'Logic in action', *Journal of Philosophical Logic* **20**, 225-263, 1989.