

Available online at www.sciencedirect.com**SciVerse ScienceDirect****Electronic Notes in
Theoretical Computer
Science**

Electronic Notes in Theoretical Computer Science 286 (2012) 157–172

www.elsevier.com/locate/entcs

Algebra, Proof Theory and Applications for a Logic of Propositions, Actions and Adjoint Modal Operators

Roy Dyckhoff^{a,1} Mehrnoosh Sadrzadeh^{b,2,3} Julien Truffaut^{b,3}^a *School of Computer Science
University of St Andrews
St Andrews, Scotland, UK*^b *Department of Computer Science
University of Oxford
Oxford, England, UK*

Abstract

We develop a cut-free (and hence analytic) nested sequent calculus for a modal logic of actions and propositions. The actions act on propositions via a dynamic modality (the *weakest precondition* of program logics), whose left adjoint we refer to as ‘update’ (the *strongest postcondition*). Both logics are positive and have adjoint pairs of epistemic modalities: the left adjoints express agents’ uncertainties and the right adjoints express their beliefs. The rules for ‘update’ encode learning as a result of discarding uncertainty. We prove admissibility of *Cut*, and hence the completeness of the logic w.r.t. an algebraic semantics. We interpret the logic on epistemic scenarios with honest and dishonest communication actions, add assumption rules to encode them and prove that the extended calculus still has the admissibility results. We apply the calculus to encode and solve the classic epistemic puzzle of *muddy children* and a modern version of it with dishonest agents.

Keywords: Proof Theory, Cut-Admissibility, Algebra, Adjoint Modalities, Epistemic Scenarios

1 Introduction

Temporal and epistemic logics can express properties of programs [10] and distributed system protocols [7]. The modalities of epistemic logics encode attitudes such as knowledge and belief, but dynamic changes to these attitudes, e.g. after announcements, have traditionally been formalised only in a semantic fashion. Dynamic program logics are, on the other hand, developed for the specific purpose of syntactic reasoning about changes of properties. Adding epistemic modalities

¹ Email: rd@st-andrews.ac.uk

² M. Sadrzadeh acknowledges support by EPSRC grant EP/F042728/1.

³ Email: mehrs@cs.ox.ac.uk, truffaut.julien@gmail.com

to dynamic logics led to logics [3,4] allowing reasoning about belief updates, both syntactically and semantically. But, lacking cut-admissibility, the calculus proposed in [3] is not a basis for automatic proof search. Here we develop a cut-free sequent calculus as basis for a proof search procedure for one such logic. The calculus is *nested*, in the sense of calculi studied in, e.g., [5,8,9,11,12,15,16,18].

The logic from [3] comprises a linear logic of actions Q and a logic of propositions M . The former act on the latter via modalities, similar to the *dynamic modality* of PDL, known there as the *weakest precondition*, and its right adjoint, the *strongest postcondition*. We develop an algebraic semantics for these logics in terms of a residuated lattice-monoid of actions and its right lattice of propositions; their completions are referred to as “quantale-module pairs” and their application to program semantics has been studied in [1]. We endow both M and Q with families of epistemic adjoint operators. We present sequent calculi for the logics, such that the logic of actions admits a cut rule and that the logic of propositions admits two cut rules (and weakening and contraction rules). The calculi are thus complete w.r.t. the algebraic semantics. Finally, after [3], we interpret the actions Q as announcements (public or private, honest or dishonest), the operations of Q on M as the effects of the actions on propositions, the epistemic modalities in terms of agents’ uncertainties and beliefs, and distributivity properties involving the dynamic modalities in terms of properties of belief update procedures. We add rules to allow encoding of epistemic scenarios and show that the admissibility results are unaffected. We apply this to encode the classic epistemic scenario of *muddy children* and new versions of it with dishonest agents. The calculus (with some optimisations) and some example scenarios are implemented in [19].

The sequent calculus of actions and adjoint modalities enriches the calculus of [12] with the two classical operators of \vee and \wedge . The rules for the logic of propositions include those of [17], together with new rules for the dynamic modalities, their distributivity interactions with epistemic modalities, and rules for action connectives in propositional contexts. The admissibility theorems are novel contributions. The algebraic semantics is a finite version of [3]; our formalisation allows for a completeness proof without lattice completions. Proving admissibility of the cut rules involves hundreds of cases, some already considered in [17]. Our solution of the muddy children puzzle is new; it does not rely on negation or the fix point operator of common knowledge, e.g. that in [10]. The sequent proof offers a unified method of solving such puzzles and is a major improvement on the inductive algebraic proof in [3].

Detailed proofs are available in a long version available from the authors.

2 Syntax, Algebra and Semantics for Actions

We give here the syntax and the intended algebraic semantics of our *action logic*; in Section 3 we present a cut-free sequent calculus. In Sections 4 and 5 we add the syntax, an algebraic semantics and a sequent calculus for propositions, including those formed by the interaction of actions and propositions. In Section 6 we give a

soundness and completeness theorem.

2.1 Syntax and Algebra of Actions

The set Q of *actions* q of the action logic is generated over a set \mathcal{A} of *agents* A and a set B of *basic actions* σ by the following grammar:

$$q ::= \perp \mid \top \mid 1 \mid \sigma \mid q \wedge q \mid q \vee q \mid q \bullet q \mid \Box_A q \mid \Diamond_A q$$

The binary connectives \wedge and \vee will be interpreted as lattice operations of meet and join, with \top and \perp as their units; \bullet is a monoid multiplication with 1 as its unit, the modalities \Box_A and \Diamond_A will be adjoint endo-operators on the lattice monoid. We make this more precise as follows:

Definition 2.1 Let \mathcal{A} be a set, with elements called *agents*. A *lattice monoid with adjoint modalities* (an LMAM) over \mathcal{A} is both a bounded lattice $(Q, \vee, \wedge, \top, \perp)$ and a unital monoid $(Q, 1, \bullet, \leq)$, where \bullet preserves joins, with two \mathcal{A} -indexed families $\{\Diamond_A\}_{A \in \mathcal{A}}: Q \rightarrow Q$ and $\{\Box_A\}_{A \in \mathcal{A}}: Q \rightarrow Q$ of order-preserving maps, each \Diamond_A being left adjoint to \Box_A .

Thus, in addition to the lattice axioms, the following hold, for all $q, q', q'' \in Q$ and all $A \in \mathcal{A}$:

$$q \bullet (q' \vee q'') = (q \bullet q') \vee (q \bullet q'') \quad \text{and} \quad (q' \vee q'') \bullet q = (q' \bullet q) \vee (q'' \bullet q) \tag{1}$$

$$q \bullet 1 = q \quad \text{and} \quad 1 \bullet q = q \tag{2}$$

$$q \leq q' \text{ implies } \Diamond_A q \leq \Diamond_A q' \tag{3}$$

$$q \leq q' \text{ implies } \Box_A q \leq \Box_A q' \tag{4}$$

$$\Diamond_A q \leq q' \quad \text{iff} \quad q \leq \Box_A q' \tag{5}$$

Proposition 2.2 In any LMAM Q over \mathcal{A} , the following hold:

6	$\Diamond_A(q \vee q') = \Diamond_A q \vee \Diamond_A q'$	7	$\Box_A(q \wedge q') = \Box_A q \wedge \Box_A q'$
8	$\Diamond_A(q \wedge q') \leq \Diamond_A q \wedge \Diamond_A q'$	9	$\Box_A q \vee \Box_A q' \leq \Box_A(q \vee q')$
10	$\Diamond_A \perp = \perp$	11	$\Box_A \top = \top$
12	$q \bullet (q' \wedge q'') \leq (q \bullet q') \wedge (q \bullet q'')$	13	$(q' \wedge q'') \bullet q \leq (q' \bullet q) \wedge (q'' \bullet q)$
14	$\Diamond_A \Box_A q \leq q$	15	$q \leq \Box_A \Diamond_A q$

Definition 2.3 An LMAM Q over \mathcal{A} is *multiplicative* iff we have the following:

$$(16) \quad \Diamond_A(q \bullet q') \leq (\Diamond_A q) \bullet (\Diamond_A q') \tag{16} \qquad (17) \quad \Diamond_A 1 \leq 1 \tag{17}$$

Proposition 2.4 In any multiplicative LMAM Q over \mathcal{A} , the following hold:

$$(18) \quad (\Box_A q) \bullet (\Box_A q') \leq \Box_A(q \bullet q') \tag{18} \qquad (19) \quad 1 \leq \Box_A 1 \tag{19}$$

The qs are for interpretation of epistemic actions, such as announcements, which may change belief, and \leq is the information order; hence \vee is non-deterministic

choice and \perp is failure, \bullet is sequential composition and 1 is skip (the null action), $\blacklozenge_A q$ is the “uncertainty” of agent A about action q and $\square_A q$ is the agent’s belief about it. As argued in [3], these epistemic operators allow encoding of various types of announcements such as public and private. Inequality (16) encodes a form of belief update, that the uncertainty about a composite action is derived from the composition of the uncertainties of the component actions.

2.2 Semantics of Actions

Let Q be a multiplicative LMAM over \mathcal{A} . An *interpretation in Q* of the action logic (over \mathcal{A} , and with set B of basic actions) is a map $\llbracket - \rrbracket : B \rightarrow Q$. The interpretations of compound actions are obtained by induction: $\llbracket q_1 \vee q_2 \rrbracket = \llbracket q_1 \rrbracket \vee \llbracket q_2 \rrbracket$, $\llbracket q_1 \wedge q_2 \rrbracket = \llbracket q_1 \rrbracket \wedge \llbracket q_2 \rrbracket$, $\llbracket q_1 \bullet q_2 \rrbracket = \llbracket q_1 \rrbracket \bullet \llbracket q_2 \rrbracket$, $\llbracket \blacklozenge_A q \rrbracket = \blacklozenge_A \llbracket q \rrbracket$, $\llbracket \square_A q \rrbracket = \square_A \llbracket q \rrbracket$, $\llbracket \top \rrbracket = \top$, $\llbracket \perp \rrbracket = \perp$ and $\llbracket 1 \rrbracket = 1$.

Note that we use Q both for the set of actions of the logic and for the LMAM interpreting them; the context will always make clear which is intended.

3 Sequent Calculus for Actions

3.1 Preliminaries

We have *action items* T and *action contexts* Θ generated by the following syntax:

$$T ::= q \mid \Theta^A \quad \Theta ::= T \text{ list}$$

where Θ^A will be interpreted as $\blacklozenge_A(\odot \Theta)$, for $\odot \Theta$ the sequential composition of the interpretations of elements in the list Θ . The use of lists rather than sets or multi-sets reflects the non-commutativity (and non-idempotence) of the composition of actions.

Thus, *action contexts* (abbreviated to *a-contexts*) are finite lists of action items, where *action items* (abbreviated to *a-items*) are either actions or agent-annotated action contexts. The term *context* is **not** in the sense of “having a gap waiting to be filled” but as a short name for the antecedent of a sequent, i.e. the context in which the succedent action is performed (or, when we discuss propositions, asserted). If one of the a-items inside an a-context is replaced by a “hole” $[\]$, we have an *a-context* with an *a-hole*. More precisely, we have the notions of an *a-context-with-an-a-hole* Σ and an *a-item-with-an-a-hole* R , defined using mutual recursion as follows:

$$\Sigma ::= \Theta, R, \Theta' \quad R ::= [\] \mid \Sigma^A$$

Given an a-context-with-an-a-hole Σ and an a-context Θ , the result $\Sigma[\Theta]$ of *applying* the first to the second, i.e. replacing the hole $[\]$ in Σ by Θ , is an a-context, defined recursively (together with the application of an a-item-with-an-a-hole R to an a-context, to form an a-context) as follows:

$$(\Theta', R', \Theta'')[\Theta] = \Theta', R'[\Theta], \Theta'' \quad ([\])[\Theta] = \Theta \quad (\Sigma^A)[\Theta] = (\Sigma[\Theta])^A.$$

This notion of “context with a hole” allows, in the expression of the inference rules, a precise notation for replacement deep inside contexts. For example, with $\Sigma = c, d, (e, \square)^1, f$ and $\Theta = a, b$, we obtain $\Sigma[\Theta] = c, d, (e, a, b)^1, f$.

Given a-contexts-with-an-a-hole Σ', Σ , and an a-item-with-an-a-hole R , the *combinations* $\Sigma' \bullet \Sigma$ and $R \bullet \Sigma$ are defined to be a-contexts with a-holes, as follows, by mutual recursion on the structures of Σ' and R :

$$(\Theta, R', \Theta') \bullet \Sigma = \Theta, (R' \bullet \Sigma), \Theta' \quad (\square) \bullet \Sigma = \Sigma \quad (\Sigma''^A) \bullet \Sigma = (\Sigma'' \bullet \Sigma)^A$$

and satisfy $(\Sigma' \bullet \Sigma)[\Theta] = \Sigma'[\Sigma[\Theta]]$ and $(R \bullet \Sigma)[\Theta] = R[\Sigma[\Theta]]$.

3.2 Sequents and their Interpretations

[Action] *sequents* consist of an a-context Θ (on the left), a turnstile and an action q (on the right). We omit the list constructors, e.g. we write $1, \sigma, \perp \vdash \sigma'$ rather than $\langle 1, \sigma, \perp \rangle \vdash \sigma'$; the empty list $\langle \rangle$ is often omitted.

The meanings of a-items and of a-contexts, given an interpretation, are obtained by mutual induction on their structure: $\llbracket \Theta^A \rrbracket = \blacklozenge_A \llbracket \Theta \rrbracket$, $\llbracket I_1, \dots, I_n \rrbracket = \llbracket I_1 \rrbracket \bullet \dots \bullet \llbracket I_n \rrbracket$ and $\llbracket \langle \rangle \rrbracket = 1$

A sequent $\Theta \vdash q$ is *true* in an interpretation $\llbracket - \rrbracket$ in Q iff $\llbracket \Theta \rrbracket \leq \llbracket q \rrbracket$; it is *true* in Q iff true in all interpretations in Q ; it is *valid* iff true in every multiplicative LMAM. When checking validity of the rules, we use the easy fact that if $\Theta \leq \Theta'$ then $\Sigma[\Theta] \leq \Sigma[\Theta']$.

3.3 Sequent Calculus

We have the following initial sequents (in which σ is restricted to being a basic action, i.e. is from \mathbf{B}):

$\overline{\vdash 1} \ 1R$	$\overline{\sigma \vdash \sigma} \ Id$	$\overline{\Sigma[\perp] \vdash q} \ \perp L$	$\overline{\Theta \vdash \top} \ \top R$
----------------------------	--	---	--

The rules for the lattice operations, composition and the modalities are:

$\frac{\Sigma[\] \vdash q}{\Sigma[1] \vdash q} 1L$	
$\frac{\Sigma[q_i] \vdash q}{\Sigma[q_1 \wedge q_2] \vdash q} \wedge L_i$	$\frac{\Theta \vdash q_1 \quad \Theta \vdash q_2}{\Theta \vdash q_1 \wedge q_2} \wedge R$
$\frac{\Sigma[q_1] \vdash q \quad \Sigma[q_2] \vdash q}{\Sigma[q_1 \vee q_2] \vdash q} \vee L$	$\frac{\Theta \vdash q_1}{\Theta \vdash q_1 \vee q_2} \vee R_1 \quad \frac{\Theta \vdash q_2}{\Theta \vdash q_1 \vee q_2} \vee R_2$
$\frac{\Sigma[q_1, q_2] \vdash q}{\Sigma[q_1 \bullet q_2] \vdash q} \bullet L$	$\frac{\Theta_1 \vdash q_1 \quad \Theta_2 \vdash q_2}{\Theta_1, \Theta_2 \vdash q_1 \bullet q_2} \bullet R$
$\frac{\Sigma[q^A] \vdash q'}{\Sigma[\blacklozenge_A q] \vdash q'} \blacklozenge_{AL}$	$\frac{\Theta \vdash q}{\Theta^A \vdash \blacklozenge_A q} \blacklozenge_{AR}$
$\frac{\Sigma[q] \vdash q'}{\Sigma[(\square_A q)^A] \vdash q'} \square_{AL}$	$\frac{\Theta^A \vdash q}{\Theta \vdash \square_A q} \square_{AR}$

We also have structural rules, i.e. rules not involving the algebraic operators:

$\frac{\Sigma[\Theta^A, \Theta'^A] \vdash q}{\Sigma[(\Theta, \Theta')^A] \vdash q} Dist$	$\frac{\Sigma[\langle \rangle] \vdash q}{\Sigma[\langle \rangle^A] \vdash q} Unit$
--	--

The two indicated occurrences of σ in the *Id* rule are *principal*. Each right rule has its conclusion's succedent as its *principal action* (but we will always just call it a *principal formula*); in addition, the \blacklozenge_{AR} rule has Θ^A as a *principal item*. Each left rule has a *principal item*: these are as usual.

The *size of an action* q is just the (weighted) number of operator occurrences, counting each operator \blacklozenge_A and \square_A as having weight 2; the *size of an a-item* Θ^A is the size of Θ plus 1, and the *size of an a-context* Θ is the sum of the sizes of its items. The *size of a sequent* $\Theta \vdash q$ is just the sum of the sizes of Θ and q . Note that each premiss of a rule instance has lower size than the conclusion, except for the rule *Dist*, whose presence leads to non-termination of a naive implementation of the calculus.

Lemma 3.1 *For every action q , the sequent $q \vdash q$ is derivable.*

Following this, in proofs and examples below, we shall allow the use of *Id* in the form $q \vdash q$ even where the action q is not a basic action.

Lemma 3.2 *The $1L$, $\vee L$, $\bullet L$, \blacklozenge_{AL} , $\wedge R$ and \square_{AR} rules are invertible.*

Lemma 3.3 *The rules $\top L^-$ and $\perp R^-$ are admissible:*

$$\frac{\Sigma[\top] \vdash q}{\Sigma[\Theta] \vdash q} \top L^- \quad \frac{\Theta \vdash \perp}{\Sigma[\Theta] \vdash q} \perp R^-$$

4.2 Algebraic semantics for propositions

Definition 4.1 Let \mathcal{A} be a set, with elements called *agents*. A DLAM over \mathcal{A} is a bounded distributive lattice $(M, \wedge, \vee, \top, \perp)$ with two \mathcal{A} -indexed families $\{\blacklozenge_A\}_{A \in \mathcal{A}}: M \rightarrow M$ and $\{\square_A\}_{A \in \mathcal{A}}: M \rightarrow M$ of order-preserving maps, with each \blacklozenge_A left adjoint to \square_A , i.e. $\blacklozenge_A(l) \leq l'$ iff $l \leq \square_A(l')$.

For a detailed list of derived properties of a DLAM, see [17].

Definition 4.2 A multiplicative LMAM Q acts on a DLAM M (over the same sets of agents) whenever we have a pointwise order-preserving map $-\cdot -: M \times Q \rightarrow M$, with each $-\cdot q$ having a right adjoint $[q]-: M \rightarrow M$, s.t. the following hold, for all $q, q' \in Q$ and all $m \in M$:

$$m \cdot (q \bullet q') = (m \cdot q) \cdot q' \tag{20}$$

$$m \cdot 1 = m \tag{21}$$

$$\blacklozenge_A(m \cdot q) \leq \blacklozenge_A m \cdot \blacklozenge_A q \tag{22}$$

Equations 20 and 21 are axioms for a Quantale-Module [1]; inequation 22 encodes a form of learning: the uncertainty of an “updated” proposition $m \cdot q$ is learnt from the update of the uncertainty of m by the uncertainty of q .

Proposition 4.3 Whenever a multiplicative LMAM Q acts on a DLAM M , the following hold, for all $q, q' \in Q$ and $m, m' \in M$:

23	$q \leq q'$ implies $m \cdot q \leq m \cdot q'$ and $[q']m \leq [q]m$
24	$m \leq m'$ implies $m \cdot q \leq m' \cdot q$ and $[q]m \leq [q]m'$
25	$m \cdot q \leq m'$ iff $m \leq [q]m'$

26	$(m \vee m') \cdot q = (m \cdot q) \vee (m' \cdot q)$	27	$(m \wedge m') \cdot q \leq (m \cdot q) \wedge (m' \cdot q)$
28	$[q](m \wedge m') = [q]m \wedge [q]m'$	29	$[q]m \vee [q]m' \leq [q](m \vee m')$
30	$\perp \cdot q = \perp$	31	$[q]\top = \top$
32	$([q]m) \cdot q \leq m$	33	$m \leq [q](m \cdot q)$
34	$[q \bullet q']m = [q][q']m$	35	$[1]m = m$

Let Q be a multiplicative LMAM acting on a DLAM M and $\llbracket - \rrbracket$ an interpretation of the set of actions of the action logic (over a set \mathbf{B} of basic actions) in Q , as defined and extended in subsection 2.2. An *interpretation* of the set of propositions of the propositional logic (over a set At of atoms) in M is given by a map $\llbracket - \rrbracket: At \rightarrow M$; extension of the two interpretations to an interpretation of compound propositions is obtained by structural induction:

$$\begin{aligned} \llbracket m_1 \vee m_2 \rrbracket &= \llbracket m_1 \rrbracket \vee \llbracket m_2 \rrbracket, & \llbracket m_1 \wedge m_2 \rrbracket &= \llbracket m_1 \rrbracket \wedge \llbracket m_2 \rrbracket, \\ \llbracket \blacklozenge_A(m) \rrbracket &= \blacklozenge_A(\llbracket m \rrbracket), & \llbracket \square_A m \rrbracket &= \square_A \llbracket m \rrbracket, \\ & \llbracket \top \rrbracket = \top, & \llbracket \perp \rrbracket &= \perp, \\ \llbracket m \cdot q \rrbracket &= \llbracket m \rrbracket \cdot \llbracket q \rrbracket, & \llbracket [q]m \rrbracket &= \llbracket [q] \rrbracket \llbracket m \rrbracket. \end{aligned}$$

5 Sequent Calculus for Propositions

5.1 Preliminaries

As in the action logic, we have *propositional contexts* Γ and *propositional items* I (abbreviated to *p-contexts* and *p-items*), generated by the following grammar:

$$\Gamma ::= I \text{ multiset} \qquad I ::= m \mid \Gamma^A \mid \Gamma^\Theta.$$

The union of two multi-sets is indicated by a comma, as in Γ, Γ' or (treating an item I as a one element multiset) as in Γ, I . A *p-item* I can be either a proposition or an agent-annotated p-context, as in [17]; but it can also be a p-context Γ annotated by an a-context Θ .

To express the rules correctly, we need, as in Section 3, some notion of p-context (or item) with a hole. There are now two kinds of hole, one for propositions and one for actions, both represented by $[]$; we use the notations Δ for a *p-context-with-a-p-hole*, J for a *p-item-with-a-p-hole*, Λ for a *p-context-with-an-a-hole* and K for a *p-item-with-an-a-hole*, defined, using mutual recursion, as follows:

$$\Delta ::= \Gamma, J \qquad J ::= [] \mid \Delta^A \mid \Delta^\Theta \qquad \Lambda ::= \Gamma, K \qquad K ::= \Gamma^\Sigma \mid \Lambda^\Theta$$

in which we recall from Section 3 that Σ indicates an a-context-with-an-a-hole. Various applications of something with an appropriate hole to p-contexts and p-items and combinations of these can be defined in a way similar to that presented in the action calculus.

5.2 Sequents for Propositions and their Interpretations

Our second sequent calculus (see Sub-section 5.3) allows reasoning about relationships between propositions. *Sequents* are now of the form $\Gamma \vdash m$. Given the meanings of action items and contexts in a multiplicative LMAM Q as defined above, and with the obvious notion of an interpretation of atomic propositions in a DLAM acted on by Q , extended as in Section 4.2 to compound propositions, the meanings of p-items and of p-contexts are obtained by mutual induction on their structure: $\llbracket \Gamma^A \rrbracket = \blacklozenge_A(\llbracket \Gamma \rrbracket)$, $\llbracket \Gamma^\Theta \rrbracket = \llbracket \Gamma \rrbracket \cdot \llbracket \Theta \rrbracket$, $\llbracket [I_1, \dots, I_n] \rrbracket = \llbracket I_1 \rrbracket \wedge \dots \wedge \llbracket I_n \rrbracket$ and $\llbracket [\emptyset] \rrbracket = \top$. A sequent $\Gamma \vdash m$ is *true* in an interpretation $\llbracket - \rrbracket$ in M iff $\llbracket \Gamma \rrbracket \leq \llbracket m \rrbracket$; it is *true* in M iff true in all interpretations in M , and it is *valid* iff true in every DLAM M over any multiplicative LMAM Q . That the initial sequents of the following calculus are valid and that the rules preserve truth are proved using ideas familiar from the action calculus: if $\llbracket \Gamma \rrbracket \leq \llbracket \Gamma' \rrbracket$ then $\llbracket \Delta[\Gamma] \rrbracket \leq \llbracket \Delta[\Gamma'] \rrbracket$ and if $\llbracket \Theta \rrbracket \leq \llbracket \Theta' \rrbracket$ then $\llbracket \Lambda[\Theta] \rrbracket \leq \llbracket \Lambda[\Theta'] \rrbracket$.

5.3 Sequent Calculus

We have the following initial sequents (in which p is restricted to being an atom, i.e. in At):

$$\overline{\Gamma, p \vdash p} \text{ Id} \qquad \overline{\Delta[\perp] \vdash m} \perp L \qquad \overline{\Gamma \vdash \top} \top R$$

The rules for the lattice operations and the modal operators are:

$$\begin{array}{c} \frac{\Delta[m_1, m_2] \vdash m}{\Delta[m_1 \wedge m_2] \vdash m} \wedge L \qquad \frac{\Gamma \vdash m_1 \quad \Gamma \vdash m_2}{\Gamma \vdash m_1 \wedge m_2} \wedge R \\ \frac{\Delta[m_1] \vdash m \quad \Delta[m_2] \vdash m}{\Delta[m_1 \vee m_2] \vdash m} \vee L \qquad \frac{\Gamma \vdash m_1}{\Gamma \vdash m_1 \vee m_2} \vee R_1 \qquad \frac{\Gamma \vdash m_2}{\Gamma \vdash m_1 \vee m_2} \vee R_2 \\ \frac{\Delta[m^A] \vdash m'}{\Delta[\blacklozenge_A m] \vdash m'} \blacklozenge_A L \qquad \frac{\Gamma \vdash m}{\Gamma', \Gamma^A \vdash \blacklozenge_A m} \blacklozenge_A R \\ \frac{\Delta[(\Box_A m, \Gamma)^A, m] \vdash m'}{\Delta[(\Box_A m, \Gamma)^A] \vdash m'} \Box_A L \qquad \frac{\Gamma^A \vdash m}{\Gamma \vdash \Box_A m} \Box_A R \end{array}$$

The rules for the dynamic operations are:

$$\begin{array}{c} \frac{\Delta[m^q] \vdash m'}{\Delta[m \cdot q] \vdash m'} \cdot L \qquad \frac{\Gamma \vdash m \quad \Theta \vdash q}{\Gamma', \Gamma^\Theta \vdash m \cdot q} \cdot R \\ \frac{\Theta \vdash q \quad \Delta[(q]m, \Gamma)^\Theta, m] \vdash m'}{\Delta[(q]m, \Gamma)^\Theta] \vdash m'} DyL \qquad \frac{\Gamma^q \vdash m}{\Gamma \vdash [q]m} DyR \end{array}$$

The structural rules are, with Γ' in the first two to ensure admissibility of Wk :

$$\frac{\Delta[(\Gamma^A)^{(\Theta^A)}] \vdash m}{\Delta[(\Gamma', \Gamma^\Theta)^A] \vdash m} DyDist \qquad \frac{\Delta[\Gamma^{\Theta, \Theta'}] \vdash m}{\Delta[(\Gamma', \Gamma^\Theta)^{\Theta'}] \vdash m} ReArr \qquad \frac{\Delta[(\Gamma^\Theta)^{\Theta'}] \vdash m}{\Delta[\Gamma^{\Theta, \Theta'}] \vdash m} ReArr'$$

As in the action logic, the two indicated occurrences of p in the Id rule are *principal* and each right rule has its conclusion's succedent as its *principal formula*. But in addition, the $\blacklozenge_A R$ rule has Γ^A as its *principal item* and Γ' (which is there to ensure admissibility of Wk) as its *parameter*. Similarly, the $\cdot R$ rule has Γ^Θ as its *principal item* and Γ' as its *parameter*. [More detailed definitions of such matters are in the long version.]

We also include all the four kinds of initial sequent and all the fifteen rules of the action logic, and all the variants of the L rules (including $\perp L$, $Dist$ and $Unit$) of the action logic obtained by replacing any Σ by Λ and the succedent action q by a proposition m . These rules are $\perp L$, $1L$, $\wedge L$, $\vee L$, $\bullet L$, \blacklozenge_L , $\Box L$, $Dist$ and $Unit$; we thus obtain *propositional variants*:

$\frac{}{\Lambda[\perp] \vdash m} \perp L$	$\frac{\Lambda[\] \vdash m}{\Lambda[1] \vdash m} 1L$	$\frac{\Lambda[q_i] \vdash m}{\Lambda[q_1 \wedge q_2] \vdash m} \wedge L_i$
$\frac{\Lambda[q_1] \vdash m \quad \Lambda[q_2] \vdash m}{\Lambda[q_1 \vee q_2] \vdash m} \vee L$	$\frac{\Lambda[q_1, q_2] \vdash m}{\Lambda[q_1 \bullet q_2] \vdash m} \bullet L$	$\frac{\Lambda[q^A] \vdash m}{\Lambda[\blacklozenge_A q] \vdash m} \blacklozenge_{AL}$
$\frac{\Lambda[q] \vdash m}{\Lambda[(\Box_A q)^A] \vdash m} \Box_{AL}$	$\frac{\Lambda[\Theta^A, \Theta'^A] \vdash m}{\Lambda[(\Theta, \Theta')^A] \vdash m} Dist$	$\frac{\Lambda[\langle \] \vdash m}{\Lambda[\langle \ \rangle^A] \vdash m} Unit$

The next four lemmas are provable by routine methods:

Lemma 5.1 *All sequents $\Gamma, m \vdash m$ are derivable.*

Lemma 5.2 *The following Weakening and Contraction rules are admissible:*

$$\frac{\Delta[\Gamma] \vdash m}{\Delta[\Gamma, \Gamma'] \vdash m} Wk \quad \frac{\Delta[\Gamma, \Gamma] \vdash m}{\Delta[\Gamma] \vdash m} Contr$$

Lemma 5.3 *The rules $\wedge L, \vee L, \blacklozenge_{AL}, \Box_{AL}, \bullet L, \wedge R, \Box_{AR}$ and DyR are invertible.*

Lemma 5.4 *The rules $\perp R^-$ and $\top L^-$ are admissible:*

$$\frac{\Gamma \vdash \perp}{\Delta[\Gamma] \vdash q} \perp R^- \quad \frac{\Theta \vdash \perp}{\Lambda[\Theta] \vdash q} \perp R^- \quad \frac{\Delta[\top] \vdash m}{\Delta[\Gamma] \vdash m} \top L^- \quad \frac{\Lambda[\top] \vdash m}{\Lambda[\Theta] \vdash m} \top L^-$$

5.4 Admissibility of DyCut and PrCut

Theorem 5.5 *The following DyCut and PrCut rules are admissible:*

$$\frac{\Theta \vdash q \quad \Lambda[q] \vdash m}{\Lambda[\Theta] \vdash m} DyCut \quad \frac{\Gamma \vdash m \quad \Delta[m] \vdash m'}{\Delta[\Gamma] \vdash m'} PrCut$$

Proof. Strong induction on the rank of the cut, where the *rank* is given by the pair: (size of cut formula m , sum of heights of derivations of premisses). Full details are in the long version. □

6 Main Result

Theorem 6.1 (Soundness and Completeness) *Any derivable sequent is valid; any valid sequent is derivable.*

Proof. First, we show that the initial sequents of the sequent calculus of actions are valid and that the rules are truth-preserving. For the converse, we follow the Lindenbaum-Tarski proof method. As usual, cut-admissibility is essential for showing transitivity of \vdash . Similar methods are followed for the calculus of propositions. Full details are in the long version. □

7 Interpretation and Assumption Rules

The interpretations of propositional and action connectives are as usual [1]: \wedge, \vee for conjunction and disjunction on propositions and non-deterministic choice and parallel composition for actions, \bullet (\otimes of linear logic) is the sequential composition of actions, 1 is the skip action. The dynamic connectives $[q]m$ and $m \cdot q$ are the weakest precondition and strongest postcondition, with interpretations as explained above in Subsection 4.1. As for the epistemic modalities, \blacklozenge_A expresses the appearance to agent A of, or uncertainty of agent A about, a proposition (or an action), and \square_A expresses the belief of agent A about a proposition (or an action). The uncertainties are all the propositions (or actions) that appear to A as true (or as happening in case of actions) when the proposition m is indeed true (or the action q is indeed happening).

In a relational semantics, these assumptions are given by the accessibility relation, e.g. that a state (or action) can access certain other states (or actions). In the case of actions, these enable us to express honest and dishonest public and private announcements. The *Dist* and *DyDist* rules allow for the uncertainty of a proposition updated by a composition of actions to be decomposed to the uncertainties of the actions and the uncertainties of the proposition. A belief after a sequential composition of actions can thus be derived from the belief before it.

Each epistemic scenario has assumptions about the basic actions and atomic propositions involved in the scenario. These are represented algebraically in [3] and we present them proof theoretically here. First, not every action is applicable to every proposition; we can represent the assumption, that a basic action σ is inapplicable when a proposition k holds, by the rule $Ker_{(\sigma,k)}$. Second, the facts of the world (i.e. atomic propositions p) are stable under basic actions such as announcements; so if a propositional atom p is true before a basic action σ , it will stay true after it; this is represented by the rule $Stab_{(p,\sigma)}$. Finally, each agent A has some uncertainty about each atomic proposition p (or basic action σ). So we have one or more assumptions of the form “appearance to agent A of atomic proposition p is proposition n ” and “appearance to agent A of basic action σ is the action w ”, represented by $PrApp_{(A,p,n)}$ and $App_{(A,\sigma,w)}$ respectively:

$\frac{\Gamma \vdash k}{\Delta[\Gamma^\sigma] \vdash m} Ker_{(\sigma,k)}$	$\frac{\Delta[(\Gamma, p)^\sigma, p] \vdash m}{\Delta[(\Gamma, p)^\sigma] \vdash m} Stab_{(p,\sigma)}$
$\frac{\Delta[(\Gamma, p)^A, n] \vdash m}{\Delta[(\Gamma, p)^A] \vdash m} PrApp_{(A,p,n)}$	$\frac{\Delta[\Gamma^w] \vdash m}{\Delta[\Gamma^{\sigma^A}] \vdash m} App_{(A,\sigma,w)}$

Lemma 7.1 *The calculus with the assumption rules admits Wk and Contr.*

Theorem 7.2 *The calculus with the assumption rules admits DyCut and PrCut.*

Proof. The *Ker* rules have σ basic; the *Stab* rule has p atomic and σ basic; similarly the *PrApp* and *App* rules have p atomic and (resp.) σ basic. So, no new principal cuts can be formed. The admissibility of the various forms of *Cut* is then just an

adaptation of the previous proof, with more permutations but no new principal cuts. A similar method is used in [14]. \square

8 Application

A well-known epistemic scenario is that of the muddy children, as follows: n children are playing in the mud and k of them have muddy foreheads. Each child can see the other children’s foreheads, but cannot see his own. Father announces to them “At least one of you has a muddy forehead.” and then asks “Do you know it is you who has a muddy forehead?”. After $k - 1$ rounds of honest “no” answers by all the children, the muddy ones infer that they are muddy. We can also reason about variants with dishonesty. For instance, if the father falsely announces that at least one child is muddy, then all the children will wrongly believe that they are muddy. Or the muddy children are liars and after $k - 1$ honest answers they lie that they do not know that they are muddy; the clean children then wrongly infer that they are muddy.

For a formalization of the honest version, assume the children are enumerated and the first k are muddy. Consider the propositional atoms D_i for “child i is muddy” and C_i for “child i is clean”. Since the actions of this scenario are all epistemic, these propositional atoms are stable under all basic actions. Child i can see the other children’s foreheads: we capture this by $PrApp_{(i,D_j,D_j)}$ and $PrApp_{(i,C_j,C_j)}$ for $i \neq j$. But he cannot see his own, so he is uncertain about himself being muddy or not, captured by $PrApp_{(i,D_i,D_i \vee C_i)}$ and $PrApp_{(i,C_i,D_i \vee C_i)}$. We denote father’s initial announcement by basic action σ and children’s “no” replies by basic action σ' . These actions are honest public announcements, so their appearance to any child i is identity, captured by $App_{(i,\sigma,\sigma)}$ and $App_{(i,\sigma',\sigma')}$. Father’s initial announcement cannot happen when there is no muddy child, and children’s “no” replies cannot happen if any of them knows that he is muddy: these are captured by $Ker_{(\sigma, \bigwedge_{i=1}^n C_i)}$ and $Ker_{(\sigma', \bigvee_{i=1}^n \Box_i D_i)}$, respectively.

Fig. 1 presents the proof tree for $n = 3, k = 2$ for the proposition that, after father’s announcement and one round of “no” answers, a muddy child $j = 1$ knows that he is muddy. Consider the first dishonest variant of the puzzle; we denote father’s lying action by the basic action $\bar{\sigma}$, which appears (in the honest version of the puzzle) to a child i as his honest announcement σ ; this is captured by the assumption rule $App_{(i,\bar{\sigma},\sigma)}$. The action $\bar{\sigma}$ cannot happen when a child is muddy; this is captured by the assumption rule $Ker_{(\bar{\sigma}, \bigvee_i D_i)}$. Figure 2 presents the proof of the proposition that, when no child is muddy and after father’s lie that at least one child is muddy, child $i = 2$ believes that he is muddy. Assumption rule instances and the proof tree for the second dishonest variant are presented in the appendix of the long version.

Our calculus allows a proof procedure close to human reasoning. In Figure 1, the lowest four steps $\wedge L, DyR, \bullet L$ and $\Box_1 R$ rewrite the original statement into a normal form. Then $DyDist$ and $Dist$ apply the belief update procedure and decompose the uncertainty of child 1 about the updated proposition to the update of his propositional uncertainty by his action uncertainty. The forking rule $\vee L$

9 Decidability and Complexity

Our sequent calculus has a weak form of the sub-formula property (of a kind studied in [6]) adequate to allow the calculi to be called “analytic”; proof search is therefore effective (even if not efficient) and decidability is routine (since there are none of the issues from first-order logic of choosing terms).

A proof search procedure has been implemented in [19] using a loop-checking technique and variations of the Bounded Depth-First tree expansion strategy. These all have a polynomial space complexity ($n \log n$), but the worst case time complexity of our optimal terminating strategy is $O(b^d)$ for b the branching factor and d the depth of the shortest proof.

10 Summary and future work

Our nested sequent calculus, for a positive logic of propositions and actions with ad-joint epistemic and dynamic modalities, admits cut, and is sound and complete with regard to an algebraic semantics inspired by [1,3]. With added assumption rules) the calculus is applicable to reasoning about dynamic epistemic scenarios. Existing proof theoretic treatments of dynamic epistemic logics, e.g. [2,13], only consider specific actions of public announcements. The only other calculus [3] that allows for arbitrary announcements (public/private, honest/dishonest) lacks cut-admissibility. Our work shows that dynamic epistemic logics can be represented in terms of a cut-free sequent calculus, albeit one with rules admitting substantial non-determinism in root-first proof search. The implementation [19] of this sequent calculus provides an automated tool for encoding scenarios involving both epistemic operators and actions. Refinements of the calculus, addressing issues such as termination and backtracking, are yet to be developed.

References

- [1] Abramsky, S. and S. J. Vickers, *Quantales, observational logic and process semantics*, *Mathematical Structures in Computer Science* **3** (1993), pp. 161–227.
- [2] Balbiani, P., et al, *Tableaux for public announcement logic*, *Journal of Logic and Computation* **20** (2010), pp. 55–76.
- [3] Baltag, A., B. Coecke and M. Sadrzadeh, *Epistemic actions as resources*, *Journal of Logic and Computation* **17** (2007), pp. 555–585.
- [4] Baltag, A. and L.S. Moss, *Logics for epistemic programs*, *Synthese* **139** (2004), pp. 165–224.
- [5] Brännler, K., “Nested Sequents”, Habilitation thesis, Universität Bern, 2010.
- [6] Brännler, K. and A. Guglielmi, *A first order system with finite choice of premises*, in: *First-Order Logic Revisited*, Logos Verlag Berlin (2004), pp. 59–74.
- [7] Fagin, R. et al., “Reasoning about Knowledge”, MIT Press 1995.
- [8] Fitting, M., *Prefixed tableaux and nested sequents*, *Annals of Pure and Applied Logic* **163** (2012), pp. 291–313.
- [9] Goré, R. et al, *On the correspondence between display postulates and deep inference in nested sequent calculi for tense logics*, *Logical Methods in Comp. Science* **7** (2011), pp. 1–38.

- [10] Huth, M. and M. Ryan, “Logic in Computer Science”, Cambridge Univ. Press, 2000.
- [11] Kashima, R., *Cut-free sequent calculi for some tense logics*, *Studia Logica* **53** (1994), pp. 119–135.
- [12] Moortgat, M., *Multimodal linguistic inference*, *Logic J. of the IGPL* **3** (1995), pp. 371–401.
- [13] Negri, S. and P. Maffezioli, *A proof theoretical perspective on public announcement logic*, *Logic and Philosophy of Science* (2012 (to appear)).
- [14] Negri, S. and J. von Plato, *Cut elimination in the presence of axioms*, *Bulletin of Symbolic Logic* **4** (1998), pp. 418–435.
- [15] Poggiolesi, F., “Gentzen Calculi for Modal Propositional Logic”, Springer, 2010.
- [16] Restall, G., “An Introduction to Substructural Logics”, Routledge, 2000.
- [17] Sadrzadeh, M. and R. Dyckhoff, *Positive logic with adjoint modalities: Proof theory, semantics and reasoning about information*, *Review of Symbolic Logic* **3** (2010), pp. 351–373.
- [18] Strassburger, L., *Nested sequents for intuitionistic modal logics*, submitted January 2012
- [19] Truffaut, J., “Implementation and Improvements of a Cut-Free Sequent Calculus for Dynamic Epistemic Logic,” Department of Computer Science, University of Oxford, 2011.