Sharing Beliefs about Actions: A Parallel Composition Operator for Epistemic Programs

Penelope Economou

Oxford University

Computing Laboratory

Oxford, OX1 3QD, UK

penelope.economou@comlab.ox.ac.uk

Themes

- A **new operator on epistemic programs** expressing the action of sharing a belief about the current action inside a subgroup.
- An **equational calculus** for this operator.
- **Examples** of its usage.

State Models

- Given a set Φ_0 of atomic propositions and a set of agents $\mathcal{A}$, an **(epistemic) state model** is a Kripke model

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

  consisting of

  1. a set S of "states"
  2. a family of binary accessibility relations $\xrightarrow{A}_{\mathbf{S}} \subseteq S \times S$, one for each agent $A \in \mathcal{A}$
  3. and a *valuation* $\|.\|_{\mathbf{S}} : \Phi_0 \to \mathcal{P}(S)$, assigning to each fact $p \in \Phi_0$ a set $\|p\|_{\mathbf{S}}$ of states

Epistemic Propositions

- Let $\mathbf{SMod}$ be the collection of all state models.
  An **epistemic proposition** is an operation φ defined on $\mathbf{SMod}$ such that for all $\mathbf{S} \in \mathbf{SMod}$, $\varphi_{\mathbf{S}} \subseteq S$.
- If $s \in \varphi_{\mathbf{S}}$, we say that *state* $s \in \mathbf{S}$ *satisfies proposition* φ, or that φ is *true* at state s in model $\mathbf{S}$.

Action Models and Epistemic Programs

- An **(epistemic) action model** is a Kripke model

$$\mathbf{\Sigma} = (\Sigma, \xrightarrow{A}, \mathsf{pre})_{A \in \mathcal{A}}$$

  where

  1. Σ is a set of *simple actions*,
  2. $\xrightarrow{A}$ is an A-indexed family of relations on Σ, and
  3. pre $: \Sigma \to \mathcal{P}(\mathbf{\Phi}_0)$.

- An **epistemic program** is defined as a pair $\pi = (\mathbf{\Sigma}, \Gamma)$ consisting of an action model $\mathbf{\Sigma}$ and a set $\Gamma \subseteq \Sigma$ of *designated simple actions*, which we often denote by $|\pi|$.

Repackaging the Arrows

- Epistemic programs can alternatively be presented by having maps:

$$\pi_A : \Sigma \to \mathcal{P}(\Sigma), \ \sigma \mapsto \sigma_A \subseteq \Sigma,$$

  for every agent $A \in \mathcal{A}$, instead of the arrows.

- If we are given the arrows $\xrightarrow{A}$, we can define the *appearance*[a]: $\sigma_A = \{\sigma' : \sigma \xrightarrow{A} \sigma'\}$ to each agent A. $\dashv$

[a] The appearance sets express the agents beliefs about the very action that is taking place. Thus, $\sigma' \in \sigma_A$ represents the actions that an agent considers as 'alternatives' of the 'real' action.

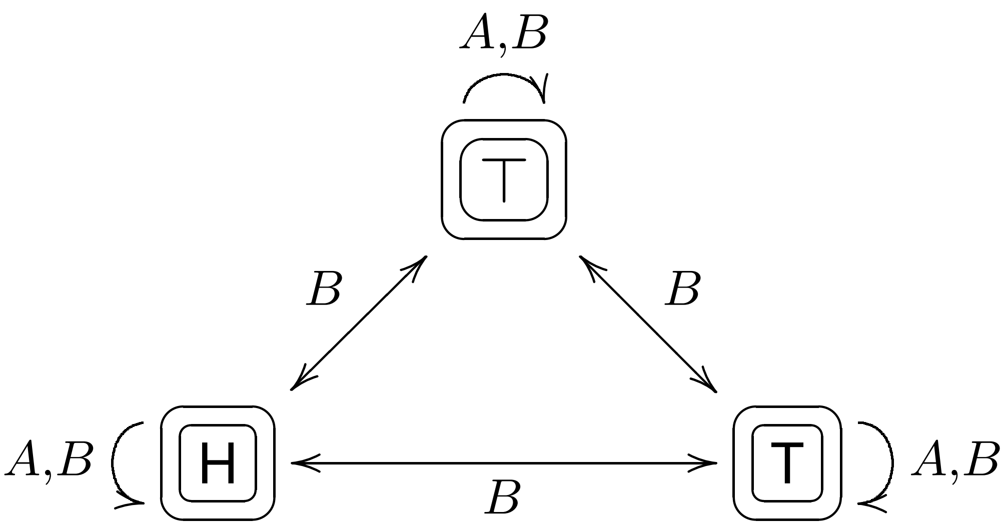
pecifying Epistemic Actions and Program

- To give an abstract specification of an *epistemic action* in a (given) epistemic model it is enough to define its:
  1. preconditions $\mathsf{pre}(\sigma)$
  2. appearance $\sigma_A = \{\sigma' : \sigma \xrightarrow{A} \sigma\}$ to each agent A.
- An epistemic program is specified by defining all the actions $\sigma \in \Sigma$ in the model, and in addition giving the set of designated actions $|\pi|$.

Motivation: An Epistemic Scenario

SCENARIO 1: PICK A CARD. A and B enter a large room containing a remote-control mechanical coin flipper. One presses the button and the coin spins through the air and then lands in a small box on a table. A card is shown to A, in the presence of B, which either says heads (H), tails (T), or is blank. In the first two cases the card describes truly the state of the coin in the box, and in the last case the intention is that no information is given.

A Representation of the Epistemic Program



Our goal

- Propose a theoretical understanding of the above representation.

Our goal

- Propose a theoretical understanding of the above representation.
- ‘How are we going to model this epistemic action?’

Our goal

- Propose a theoretical understanding of the above representation.
- ‘How are we going to model this epistemic action?’
- Introduce a new operation that models the beliefs of the agents about the current action taking place and the justifiable changes affecting these beliefs.

Our goal

- Propose a theoretical understanding of the above representation.
- ‘How are we going to model this epistemic action?’
- Introduce a new operation that models the beliefs of the agents about the current action taking place and the justifiable changes affecting these beliefs.
- Introduce and discuss our logic after which we revisit the example scenario and show how it can be modeled.

Our goal

- Propose a theoretical understanding of the above representation.
- 'How are we going to model this epistemic action?'
- Introduce a new operation that models the beliefs of the agents about the current action taking place and the justifiable changes affecting these beliefs.
- Introduce and discuss our logic after which we revisit the example scenario and show how it can be modeled.
- Demonstrate the usage of our new operation by examining a more complicated epistemic scenario.

A New Operation on Epistemic Programs

Sharing Beliefs: While π, $\mathcal{B}$ announces π' to $\mathcal{C}$. Given a group of agents $\mathcal{B}, \mathcal{C} \subseteq \mathcal{A} = \{A, B \ldots\}$, and epistemic programs π, and π', we introduce a new operation $\pi \,!^{\mathcal{B}}_{\mathcal{C}}\, \pi'$, to be read as : *while* π, $\mathcal{B}$ *announces* π' *to* $\mathcal{C}$.

Remarks:

- It represents a kind of *parallel composition*: program π is happening in parallel with a *sincere, private*, (but *not necessarily truthful*) announcement (from $\mathcal{B}$ to $\mathcal{C}$) that the program π' is happening.

A New Operation on Epistemic Programs

Sharing Beliefs: While π, $\mathcal{B}$ announces π' to $\mathcal{C}$. Given a group of agents $\mathcal{B}, \mathcal{C} \subseteq \mathcal{A} = \{A, B \ldots\}$, and epistemic programs π, and π', we introduce a new operation $\pi \,!^{\mathcal{B}}_{\mathcal{C}}\, \pi'$, to be read as : *while* π, $\mathcal{B}$ *announces* π' *to* $\mathcal{C}$.

Remarks:

- It represents a kind of *parallel composition*: program π is happening in parallel with a *sincere, private*, (but *not necessarily truthful*) announcement (from $\mathcal{B}$ to $\mathcal{C}$) that the program π' is happening.
- While π is happening (all members of) $\mathcal{B}$ believe that π' is happening instead, and moreover, they *communicate* this belief to (all members) of $\mathcal{C}$ by sending (them) a message over a fully private, secure and reliable channel.

A New Operation on Epistemic Programs

Sharing Beliefs: While π, $\mathcal{B}$ announces π' to $\mathcal{C}$. Given a group of agents $\mathcal{B}, \mathcal{C} \subseteq \mathcal{A} = \{A, B \ldots\}$, and epistemic programs π, and π', we introduce a new operation $\pi \,!_{\mathcal{C}}^{\mathcal{B}}\, \pi'$, to be read as : *while* π, $\mathcal{B}$ *announces* π' *to* $\mathcal{C}$.

Remarks:

- After the group announcement by $\mathcal{B}$ it becomes *common knowledge* among (the agents of) $\mathcal{B} \cup \mathcal{C}$ that $\mathcal{B}$ believes π'.

A New Operation on Epistemic Programs

Sharing Beliefs: While π, $\mathcal{B}$ announces π' to $\mathcal{C}$. Given a group of agents $\mathcal{B}, \mathcal{C} \subseteq \mathcal{A} = \{A, B \ldots\}$, and epistemic programs π, and π', we introduce a new operation $\pi \,!_{\mathcal{C}}^{\mathcal{B}}\, \pi'$, to be read as : *while π, $\mathcal{B}$ announces π' to $\mathcal{C}$*.

Remarks:

- After the group announcement by $\mathcal{B}$ it becomes *common knowledge* among (the agents of) $\mathcal{B} \cup \mathcal{C}$ that $\mathcal{B}$ believes π'.
- However, the beliefs of the agents in $\mathcal{C}$ are not changed by $\mathcal{B}$'s announcement, i.e. they don't assume that $\mathcal{B}$'s beliefs are truthful.

Abstract Definition of the New Operation

We can characterize our new operation by specifying the preconditions and appearances:

$$
\begin{array}{rcl}
|\,\pi\,!^{\mathcal{B}}_{\mathcal{C}}\,\pi'\,| & = & \{\sigma\,!^{\mathcal{B}}_{\mathcal{C}}\,\pi' : \sigma \in |\pi|\} \\
\mathsf{pre}(\sigma\,!^{\mathcal{B}}_{\mathcal{C}}\,\pi') & =: & \mathsf{pre}(\sigma) \\
(\sigma\,!^{\mathcal{B}}_{\mathcal{C}}\,\pi')_B & =: & \{\sigma'\,!^{\mathcal{B}}_{\mathcal{C}}\,\pi' : \sigma' \in |\pi'|\},\ \text{for all}\ B \in \mathcal{B} \\
(\sigma\,!^{\mathcal{B}}_{\mathcal{C}}\,\pi')_C & =: & \{\lambda\,!^{\mathcal{B}}_{\mathcal{C}}\,\pi' : \lambda \in \sigma_C\},\ \text{for all}\ C \in \mathcal{C} \setminus \mathcal{B} \\
(\sigma\,!^{\mathcal{B}}_{\mathcal{C}}\,\pi')_D & =: & \sigma_D,\ \text{for all}\ D \notin \{\mathcal{B}, \mathcal{C}\}
\end{array}
$$

Language of Dynamic Epistemic Calculus

Definition. Given a set of *atomic propositions* Φ_0 whose elements are usually denoted by $\boldsymbol{p}$, $\boldsymbol{q}$, $\boldsymbol{r}$ and so on, the top and bottom element $\top$, and $\bot$, and a set of agents $\mathcal{B}, \mathcal{C} \subseteq \mathcal{A} = \{A, B \dots\}$, the formal definition of the well-formed *basic programs* of the *language* of **DEC** is given by

$$\pi \quad ::= \quad ?\boldsymbol{p} \quad | \quad \pi + \pi' \quad | \quad \pi \cdot \pi' \quad | \quad \pi \, !^{\mathcal{B}}_{\mathcal{C}} \pi'$$

where $\boldsymbol{p}$ ranges over Φ_0.

Reasons for Choosing our Basic Operation

They are the natural operations on epistemic programs and most others can be defined in terms of them.
For example,

- *skip* $\stackrel{\text{def}}{=} ?\top$, and *crash* $\stackrel{\text{def}}{=} ?\bot$

As far as $\pi\, !^{\mathcal{B}}_{\mathcal{C}}\, \pi'$ and according to the choice of π, π', $\mathcal{B}$, and $\mathcal{C}$, we get:

- $\pi\, !^{\mathcal{B}}_{\mathcal{A}}\, \pi' \stackrel{\text{def}}{=} \pi\, !^{\mathcal{B}}\, \pi'$, obtained by taking $\mathcal{C} = \mathcal{A}$. We call this: *public announcement of a program by subgroups*.

Reasons for Choosing our Basic Operation

- $\pi\,!^{\mathcal{B}}_{\mathcal{B}}\,\pi' \stackrel{\text{def}}{=} \pi\,|^{\mathcal{B}}\,\pi'$, obtained by taking $\mathcal{B}=\mathcal{C}$. We read this: *while* π, $\mathcal{B}$ *thinks* π'.

The following are all special cases of the above:

- ${}^{\mathcal{B}}\pi \stackrel{\text{def}}{=}$ *skip*$|^{\mathcal{B}}\pi$. We call this: *gratuitous (i.e. mistaken) group updating with a program*.
- $\mathcal{L}^{\mathcal{B}}\pi \stackrel{\text{def}}{=} \pi\,|^{\mathcal{B}}\pi$. We call this: *group learning of a program*.

Finally, we have

- $?\boldsymbol{p}\,!^{\mathcal{B}}_{\mathcal{B}}\,?\boldsymbol{p} \stackrel{\text{def}}{=} \boldsymbol{p}!_{\mathcal{B}}$, where $\boldsymbol{p}!_{\mathcal{B}}$ is the *totally private, truthful announcement* of an atomic proposition $\boldsymbol{p}$ to *only* to a subgroup $\mathcal{B}\subseteq\mathcal{A}$.

Axioms of DEC

We propose some natural axioms for each of our operators:

- $(+)$ is associative, commutative, idempotent, and and has *crash* as a neutral element.
- $(\cdot)$ is associative as well as right and left distributive over $(+)$.
- A natural axiom for $(\cdot)$ is: *skip* $\cdot\, x = x \cdot$ *skip* $= x$.

Axioms of DEC

We continue with some natural axioms for ($?$)

$$?\boldsymbol{p} \cdot ?\boldsymbol{p} \quad = \quad ?\boldsymbol{p} \tag{t1}$$

$$?\boldsymbol{p} \cdot x \quad = \quad x \cdot ?\boldsymbol{p} \tag{t2}$$

$$?\boldsymbol{p} \quad = \quad ?\boldsymbol{p} \,!^{\mathcal{B}}_{\mathcal{C}}\, \textit{skip} \tag{t3}$$

$$?\boldsymbol{p} \cdot (?\boldsymbol{p} \,!^{\mathcal{B}}_{\mathcal{C}}\, x) \quad = \quad ?\boldsymbol{p} \,!^{\mathcal{B}}_{\mathcal{C}}\, x \tag{t4}$$

Axioms of DEC

Finally, here are some natural axioms for $(!^{\mathcal{B}}_{\mathcal{C}})$

$$(x + y) \,!^{\mathcal{B}}_{\mathcal{C}}\, z = x \,!^{\mathcal{B}}_{\mathcal{C}}\, z + y \,!^{\mathcal{B}}_{\mathcal{C}}\, z \tag{a1}$$

$$(x \,!^{\mathcal{B}}_{\mathcal{C}}\, y) \cdot (z \,!^{\mathcal{B}}_{\mathcal{C}}\, w) = ((x \,!^{\mathcal{B}}_{\mathcal{C}}\, y) \cdot z) \,!^{\mathcal{B}}_{\mathcal{C}}\, ((y \,!^{\mathcal{B}}_{\mathcal{C}}\, y) \cdot w) \tag{a2}$$

$$(x \,!^{\mathcal{B}}_{\mathcal{C}}\, y) \,!^{\mathcal{B}}_{\mathcal{C}}\, (z \,!^{\mathcal{B}}_{\mathcal{C}}\, w) = x \,!^{\mathcal{B}}_{\mathcal{C}}\, z \tag{a3}$$

$$\textit{skip} \,!^{\mathcal{B}}_{\mathcal{C}}\, \textit{skip} = \textit{skip} \tag{a4}$$

The epistemic Scenario Revisited

The total action describing the epistemic scenario PICK A CARD is:

$$\pi = \sigma + \rho + \mu$$

where

$$\sigma = (\mathcal{L}^A?\mathsf{H})\,!^B(\mathcal{L}^A?\mathsf{H} + \mathcal{L}^A?\mathsf{T} + \textit{skip})$$

$$\rho = (\mathcal{L}^A?\mathsf{T})\,!^B(\mathcal{L}^A?\mathsf{H} + \mathcal{L}^A?\mathsf{T} + \textit{skip})$$

$$\mu = \textit{skip}\,!^B(\mathcal{L}^A?\mathsf{H} + \mathcal{L}^A?\mathsf{T} + \textit{skip})$$

The Epistemic Scenario Revisited

- As π is non-deterministic, it can be resolved in any way σ, ρ, or μ are resolved:
  $|\pi| = \{\sigma\} \cup \{\rho\} \cup \{\mu\}$.
- Simple actions σ, ρ, and μ can happen if the card is showing heads, tails or nothing, respectively:
  $\mathsf{pre}(\sigma) = \mathsf{H}$, $\mathsf{pre}(\rho) = \mathsf{T}$, and $\mathsf{pre}(\mu) = \top$.

And finally:

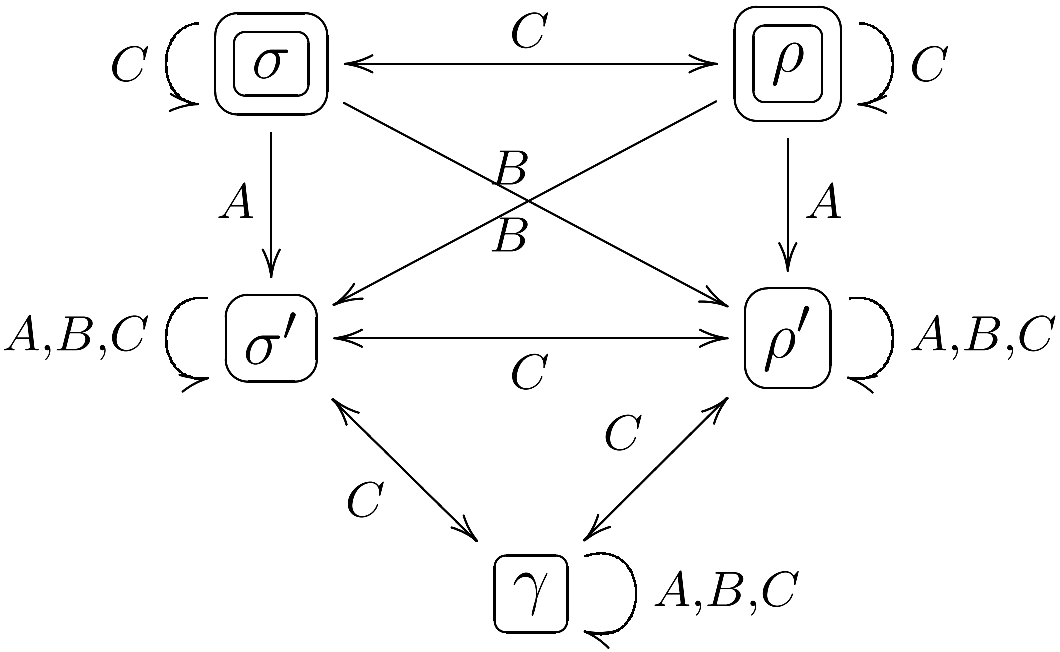
- $(\sigma)_A = \sigma$, $(\rho)_A = \rho$ and $(\mu)_A = \mu$
- $(\sigma)_B = (\rho)_B = (\mu)_B = \{\sigma\} \cup \{\rho\} \cup \{\mu\}$.

Man-in-the-middle (MITM) Attack

- **Problem**: Epistemic operators already existing in the literature (Baltag, Gerbrandy, and van Ditmarsh) are too simple or not enough to handle the MITH scenario.
- **Solution**: We claim that the epistemic program describing the variant of the MITM attack (to be described shortly) can be expressed in (the language of) **DEC** using the parallel composition operator introduced earlier.

Modelling of a Variant of the (MITM) Attack

The epistemic program describing a variant of the (MITM) attack has the following representation:



A Representation of the Epistemic Progra

The total action where the secret ($\boldsymbol{p}$, or $\neg\boldsymbol{p}$) is intercepted, modified and resent to B is $\sigma + \rho$. We claim that:

$$\sigma = \sigma'' \,|^{C}\, (\sigma'' + \rho'') \text{ and } \rho = \rho'' \,|^{C}\, (\sigma'' + \rho''),$$

where

$$\begin{aligned}
\sigma'' &= (?\boldsymbol{p} \cdot ({}^{A}(\boldsymbol{p}!_{A,B}) \cdot {}^{B}((\neg\boldsymbol{p})!_{A,B}))\, !^{C}\, (\boldsymbol{p}!_{A,B} + (\neg\boldsymbol{p})!_{A,B} + \textit{skip}\\
\rho'' &= (?(\neg\boldsymbol{p}) \cdot ({}^{A}((\neg\boldsymbol{p})!_{A,B}) \cdot {}^{B}(\boldsymbol{p}!_{A,B}))\, !^{C}\, (\boldsymbol{p}!_{A,B} + (\neg\boldsymbol{p})!_{A,B} + \textit{skip})
\end{aligned}$$

A Representation of the Epistemic Program

We also claim that

$$\sigma' = (\boldsymbol{p}!_{A,B})\,!^{C}(\boldsymbol{p}!_{A,B} + (\neg\boldsymbol{p})!_{A,B} + \textit{skip}),$$

$$\rho' = ((\neg\boldsymbol{p})!_{A,B})\,!^{C}(\boldsymbol{p}!_{A,B} + (\neg\boldsymbol{p})!_{A,B} + \textit{skip}),$$

and

$$\gamma = \textit{skip}\,!^{C}\,(\boldsymbol{p}!_{A,B} + (\neg\boldsymbol{p})!_{A,B} + \textit{skip}).$$

A Representation of the Epistemic Program

According to the action model above, we should have:

- $\sigma_C = \rho_C = \{\sigma\} \cup \{\rho\}$
- $\sigma_A = \rho_B = \sigma'$, $\rho_A = \sigma_B = \rho'$, $\gamma_A = \gamma_B = \gamma$,
- $\sigma'_C = \rho'_C = \gamma_= \{\sigma'\} \cup \{\rho'\} \cup \{\gamma\}$
- $\sigma'_A = \sigma'_B = \sigma'$, $\rho'_A = \rho'_B = \rho'$.

Conclusions

- We introduced a new operation with epistemic programs i.e. $\pi \,!^{\mathcal{B}}_{\mathcal{C}}\, \pi'$ expressing the action of sharing a belief about the current action inside a subgroup.

Conclusions

- We introduced a new operation with epistemic programs i.e. $\pi \,!^{\mathcal{B}}_{\mathcal{C}}\, \pi'$ expressing the action of sharing a belief about the current action inside a subgroup.
- We showed that many useful programs can be defined by $\pi \,!^{\mathcal{B}}_{\mathcal{C}}\, \pi'$.

Conclusions

- We introduced a new operation with epistemic programs i.e. $\pi \,!^{\mathcal{B}}_{\mathcal{C}}\, \pi'$ expressing the action of sharing a belief about the current action inside a subgroup.
- We showed that many useful programs can be defined by $\pi \,!^{\mathcal{B}}_{\mathcal{C}}\, \pi'$.
- We proposed an equational calculus for this operation.

Conclusions

- We introduced a new operation with epistemic programs i.e. $\pi \,!^{\mathcal{B}}_{\mathcal{C}}\, \pi'$ expressing the action of sharing a belief about the current action inside a subgroup.
- We showed that many useful programs can be defined by $\pi \,!^{\mathcal{B}}_{\mathcal{C}}\, \pi'$.
- We proposed an equational calculus for this operation.
- We gave two examples of its usage, of which is a variant of the well-known (MITM) attack.

Future Work

- Prove completeness of the equational calculus.

Future Work

- Prove completeness of the equational calculus.
- Explore the expressive power of the calculus. For example, a natural question would be: ”Which actions and action operations can be defined by terms in the equational calculi”?

Future Work

- Prove completeness of the equational calculus.
- Explore the expressive power of the calculus. For example, a natural question would be: ”Which actions and action operations can be defined by terms in the equational calculi”?
- Demonstrate the use of the calculus in the analysis of distributed systems.

Future Work

- Prove completeness of the equational calculus.
- Explore the expressive power of the calculus. For example, a natural question would be: ”Which actions and action operations can be defined by terms in the equational calculi”?
- Demonstrate the use of the calculus in the analysis of distributed systems.
- Extend the range of p (in our proposed syntax) from atomic to epistemic propositions and try and develop a complete calculus for epistemic programs and epistemic propositions.