Observing Distributed Computation
A Dynamic-Epistemic Approach

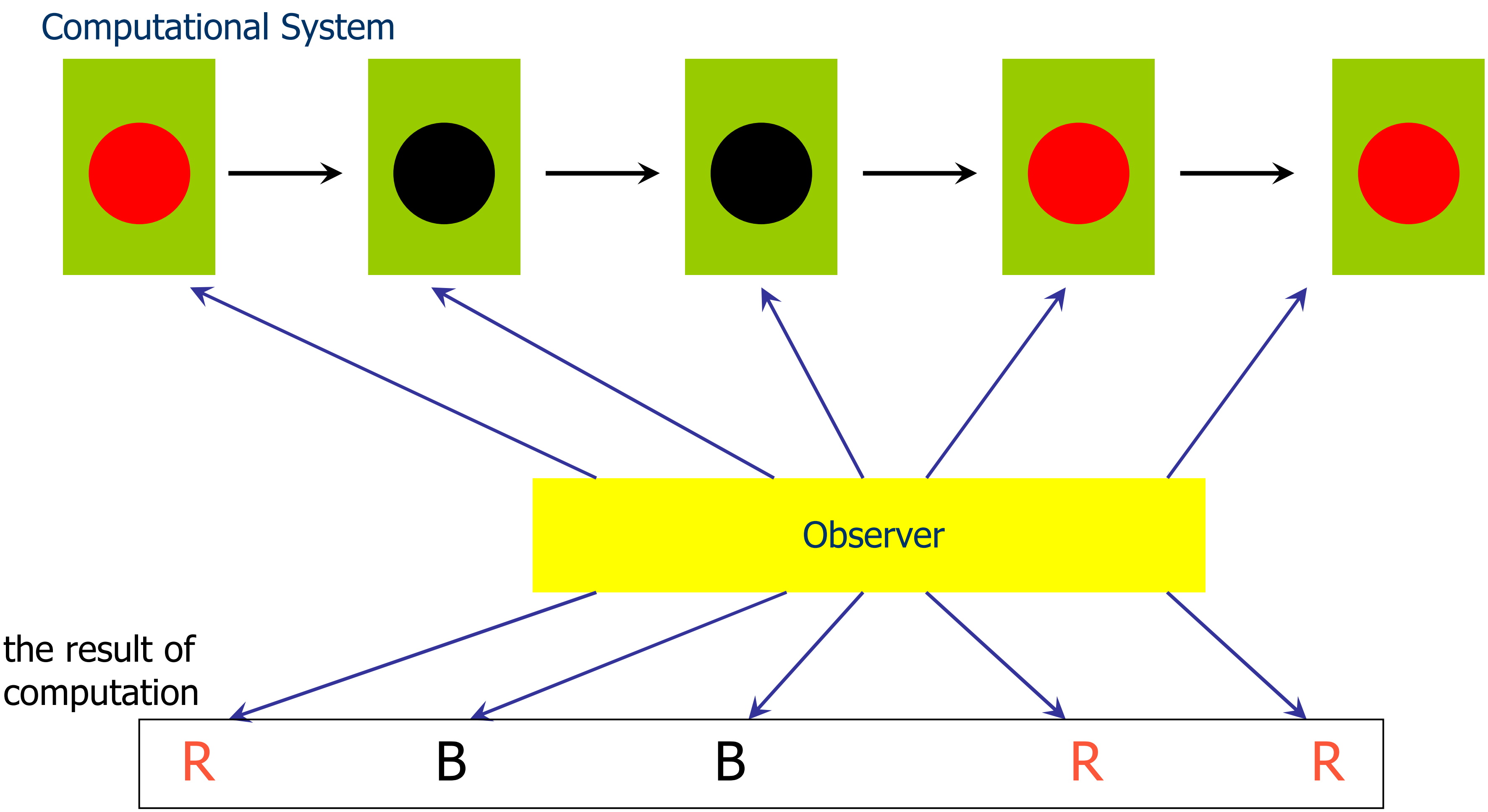
Radu Mardare

Microsoft Research-University of Trento

Centre for Computational and Systems Biology

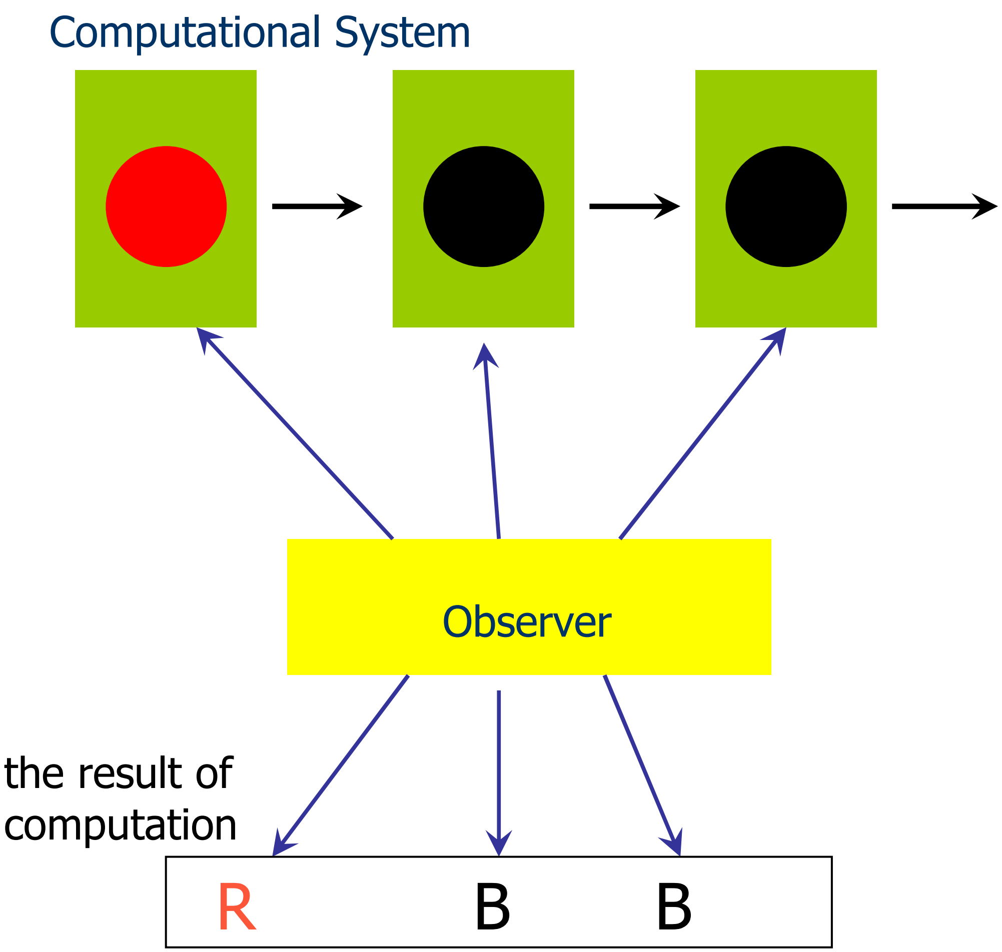
mardare@cosbi.eu

Observing computational systems



The "result" of a computation is the observation (interpretation) of a process

Observing computational systems



REG	CF	Splicing systems
+	+	+
REG	REG	REG
=	=	=
REG	RE	RE

M. Cavaliere, P. Leupold, TCS 2004

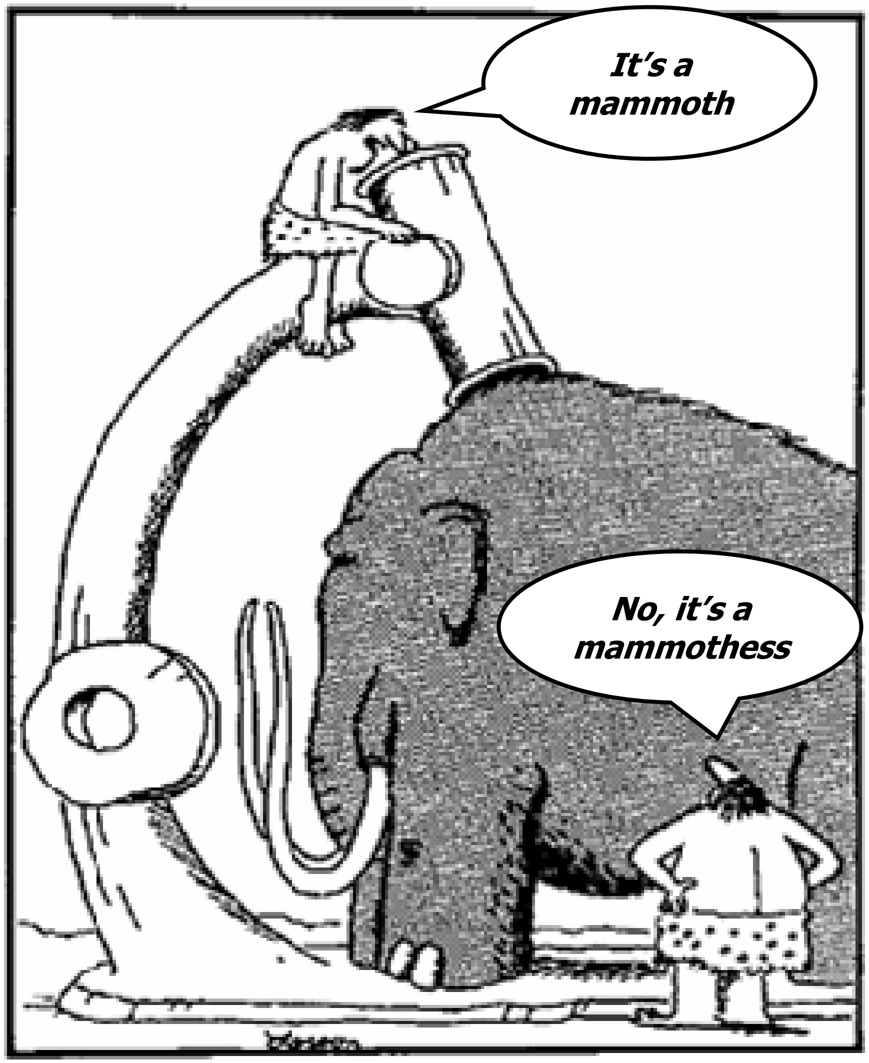
M. Cavaliere, N. Jonoska, P. Leupold, Natural Computing 2007

The “lesson” of the complexity results

A **computing device** can be seen ascomposed by two parts:

- An (observed) **dynamic system** that simply "lives", passing from a state to the next one.
- An **observer** (or more), placed outside, that watches and interpret the **evolution** of the system (parts of the system).

The observer uses the trace of the (observed) computational process as a computational resource; thus he can obtain **every** possibile computational device without changing the observed system but only by finding the "correct" external **observer**....



"The real voyage of discovery consists not in seeking new landscapes but in having new eyes"

(Marcel Proust)

•**MultiAgent Systems**: are composed of **agents**

=> an agent is a spatially localised and independently observable unit of behavior and computation (e.g. programs or processors running in parallel)

“An agent is a computational system capable of autonomous action on behalf of its user or owner” (Michael Wooldridge, *MultiAgent Systems*)

=> is projecting the agent on the observed system

=> no storing/processing information, no knowledge

•**Concurrency**: an **external observer** is a witness of a process

=> for an observer, a process is a black box (observational power)

=> but two distinct observers witnessing the same process have same observational capabilities

=> the observers: no knowledge, no memory, no processing capabilities

•**Epistemic/Doxastic Logics**: multimodal logics

=> formalize the notions of **knowledge** or **belief** possessed by an agent or a group of agents

$$K_A\phi \quad \text{“}\textit{agent } A \textit{ knows } \phi\text{”}$$

$$K_{A_1}K_{A_2}\phi \quad \text{“}\textit{agent } A_1 \textit{ knows that agent } A_2 \textit{ knows } \phi\text{”}$$

=> semantically based on Kripke structures

=> **Dynamic-Epistemic Logics** combine the epistemic operators with dynamic operators => more information about the observed system

=> **Logics for Epistemic Programs** (Baltag, Moss, Solecki) plays with Kripke structures on different levels and with their “products”

An alternative approach

•A multimodal logic – **decidable** and **completely axiomatized** (Hilbert style)

⇒For a **process algebraical semantics** (representation of the observed distributed system)

⇒That contains **dynamic and epistemic modalities**

⇒ and operators for expressing the **modular features** of the system **Spatial Logics** – Cardelli, Gordon (2000), Cardelli, Caires (2003)

⇒ The agents observe subsystems and their dynamics; an agent can observe a process more or less depending on his observational abilities

⇒For the agents, the observed processes are not only black boxes, but structurally organized

⇒The society of agents has an algebraical structure that reflects the relation between the subsystems/processes they observe

$K_A\langle\alpha\rangle\top$ $\quad\quad$ $K_B\langle\alpha\rangle\top$

$$K_E(K_A\langle\alpha\rangle\top \wedge K_B\langle\alpha\rangle\top) \rightarrow K_E\langle\alpha\rangle\top$$

$$K_E(K_A\langle\alpha\rangle\top \parallel K_B\langle\alpha\rangle\top) \rightarrow K_E(\langle\alpha\rangle\top \parallel \langle\alpha\rangle\top) \rightarrow K_E\langle\alpha\rangle\langle\alpha\rangle\top$$

$$E = A \parallel B$$

Society of agents over $\mathbb{A}$ is a subset $\mathfrak{A}$ of the set generated by

$$E := e \mid \alpha.E \mid E \parallel E \qquad \alpha \in \mathbb{A}$$

s.t. $e \in \mathfrak{A}$ (atomic agent)

if $A \parallel B \in \mathfrak{A}$ then $A, B \in \mathfrak{A}$

if $\alpha.A \in \mathfrak{A}$ then $A \in \mathfrak{A}$

The agents are unique up to commutativity of $\parallel$.

$$(\mathfrak{A}, e, \parallel, \alpha.)_{\alpha\in\mathbb{A}}$$

CCS processes

Let $\mathbb{A}$ be a denumerable set of *actions*.

an involution $\bar{} : \mathbb{A} \longrightarrow \mathbb{A}$
associates to each $\alpha \in \mathbb{A}$ the element $\overline{\alpha} \in \mathbb{A}$ such that $\overline{\overline{\alpha}} = \alpha$.

The class $\mathbb{P}$ of *processes* is given inductively by

$$P := 0 \mid \alpha.P \mid P \parallel P, \text{ where } \alpha \in \mathbb{A}.$$

Structural congruence on $\mathbb{P}$

$\equiv \subseteq \mathbb{P} \times \mathbb{P}$ the smallest congruence relation on the structure of $\mathbb{P}$ s.t.
$(\mathbb{P}, \parallel, 0)$ is a commutative monoid with respect to $\equiv$.

$$(\mathit{congruence}) \;\; \mathit{if}\ P' \equiv P''\ \mathit{then} \begin{cases} \alpha.P' \equiv \alpha.P'' \;\; \mathit{for\ any}\ \alpha \in \mathbb{A} \\ P'||P \equiv P''||P \;\; \mathit{for\ any}\ P \in \mathbb{P}. \end{cases}$$

Labeled transition system on $\mathbb{P}$

1. $$\frac{}{\alpha.P \xrightarrow{\alpha} P}$$

2. $$\frac{P \equiv Q \qquad P \xrightarrow{\alpha} P'}{Q \xrightarrow{\alpha} P'}$$

3. $$\frac{P \xrightarrow{\alpha} P' \qquad Q \xrightarrow{\overline{\alpha}} Q'}{P \parallel Q \xrightarrow{(\alpha,\overline{\alpha})} P' \parallel Q'}$$

4. $$\frac{P \xrightarrow{\alpha} P'}{P \parallel Q \xrightarrow{\alpha} P' \parallel Q}$$

We denote

$P \longrightarrow Q$ if $P \xrightarrow{\alpha} Q$ or $P \xrightarrow{(\alpha,\overline{\alpha})} Q$ for some $\alpha \in \mathbb{A}$.

$P \xrightarrow{Q:\alpha} P'$ whenever $P \equiv Q \parallel R$, $P' \equiv Q' \parallel R$ and $Q \xrightarrow{\alpha} Q'$.

$P \parallel Q \xrightarrow{P,Q:\alpha} P' \parallel Q'$ whenever $P \xrightarrow{P:\alpha} P'$ and $Q \xrightarrow{Q:\overline{\alpha}} Q'$.

$$\mathbb{A}^+ = \{\alpha,\ P:\alpha,\ P,Q:\alpha \mid \alpha \in \mathbb{A} \text{ and } P,Q \in \mathbb{P}\} \ni l$$

Kripke frames on CCS processes

Given a family of agents $(\mathfrak{A}, e, \|, \alpha.)$ and a morfism

$$i : (\mathfrak{A}, e, \|, \alpha.) \to (\mathbb{P}, 0, \|, \alpha.),$$

a frame over i is

$$\mathcal{M}_i = \langle \Pi, \mathcal{R}_{\|}, \mathcal{R}_l, \mathcal{R}_A \rangle \text{ for } l \in \mathbb{A}^+ \text{ and } A \in \mathfrak{A}$$

$$\Pi = i(\mathfrak{A})$$

$$\mathcal{R}_{\|} \subseteq \Pi \times \Pi \times \Pi,\ (P, Q, R) \in \mathcal{R}_{\|} \text{ iff } P \equiv Q \parallel R$$

$$\mathcal{R}_l \subseteq \Pi \times \Pi,\ (P, Q) \in \mathcal{R}_l \text{ iff } P \xrightarrow{l} Q$$

$$\mathcal{R}_A \subseteq \Pi \times \Pi,\ (P, Q) \in \mathcal{R}_A \text{ iff } P \equiv i(A) \parallel P' \text{ and } Q \equiv i(A) \parallel Q'$$

Syntax

Let $\mathfrak{A}$ be a society of epistemic agents

$$\phi := \ 0 \mid \neg\phi \mid \phi \wedge \phi$$

Process Semantics

$$\mathcal{M}_i = \langle \Pi, \mathcal{R}_{\|}, \mathcal{R}_l, \mathcal{R}_A \rangle \quad P \in \Pi$$

$$\mathcal{M}, P \models 0 \ \mathit{iff} \ P \equiv 0$$

$$\mathcal{M}, P \models \neg\phi \ \mathit{iff} \ \mathcal{M}, P \not\models \phi$$

$$\mathcal{M}, P \models \phi \wedge \psi \ \mathit{iff} \ \mathcal{M}, P \models \phi \ \mathit{and} \ \mathcal{M}, P \models \psi$$

Syntax $\phi := \ 0 \mid \neg\phi \mid \phi \wedge \phi \mid \langle a \rangle \phi$

$\langle a \rangle := \langle \alpha \rangle \mid \langle \alpha, \overline{\alpha} \rangle \mid \langle A : \alpha \rangle \mid \langle A, A' : \alpha \rangle.$

Process Semantics $\mathcal{M}_i = \langle \Pi, \mathcal{R}_{\|}, \mathcal{R}_l, \mathcal{R}_A \rangle \quad P \in \Pi$

$$\mathcal{M}, P \models \langle a \rangle \phi \ \textit{iff} \begin{cases} P \xrightarrow{a} P' \\ \mathcal{M}, P' \models \phi \end{cases}$$

$$\mathcal{M}, P \models \langle A : \alpha \rangle \phi \text{ iff } \begin{cases} P \xrightarrow{i(A):\alpha} P' \\ \mathcal{M}, P' \models \phi \end{cases}$$

$$\mathcal{M}, P \models \langle A, A' : \alpha \rangle \phi \text{ iff } \begin{cases} P \xrightarrow{i(A),i(A'):\alpha} P' \\ \mathcal{M}, P' \models \phi \end{cases}$$

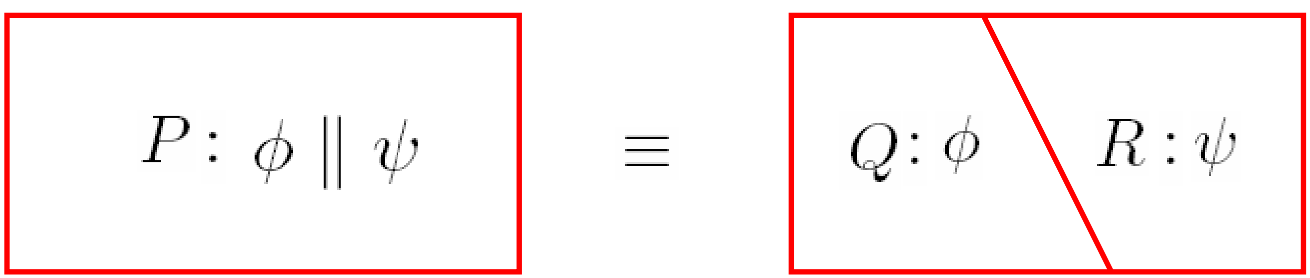
$$\boxed{P : \langle a \rangle \phi} \xrightarrow{a} \boxed{P' : \phi}$$

Syntax $\phi := \ 0 \mid \neg\phi \mid \phi \wedge \phi \mid \langle a \rangle \phi \mid \phi \parallel \phi$

Process Semantics $\mathcal{M}_i = \langle \Pi, \mathcal{R}_{\parallel}, \mathcal{R}_l, \mathcal{R}_A \rangle \qquad P \in \Pi$

$$\mathcal{M}, P \models \phi \parallel \psi \text{ iff } P \equiv Q \parallel R \text{ and } \begin{cases} \mathcal{M}, Q \models \phi \\ \mathcal{M}, R \models \psi \end{cases}$$

$$(P, Q, R) \in \mathcal{R}_{\parallel}$$



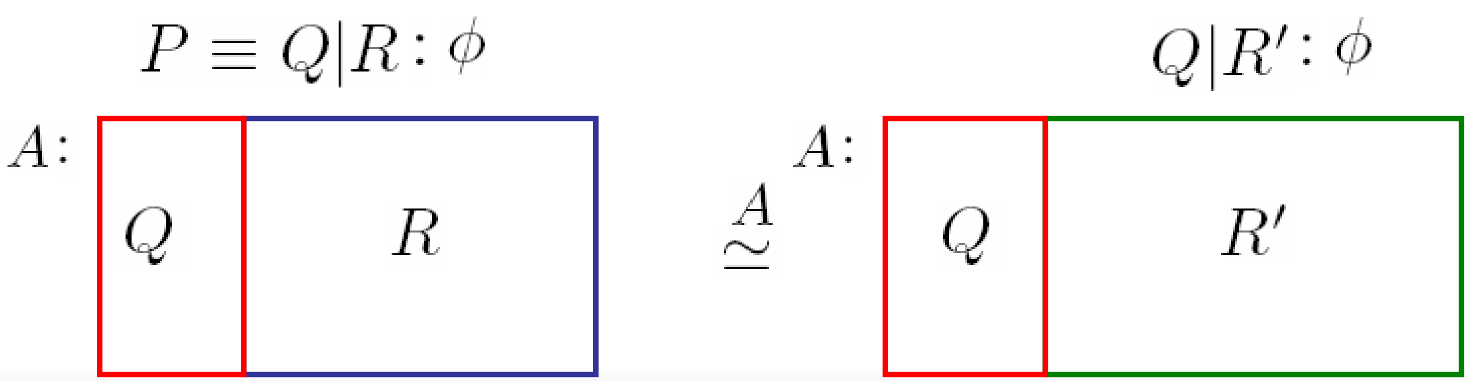
Syntax $\phi := 0 \mid \neg\phi \mid \phi \wedge \phi \mid \langle a \rangle \phi \mid \phi \parallel \phi \mid K_A \phi$

$K_A\phi$ *"agent A knows ϕ"*

$K_{A_1}K_{A_2}\phi$ *"agent A_1 knows that agent A_2 knows ϕ"*

Process Semantics $\mathcal{M}_i = \langle \Pi, \mathcal{R}_{\parallel}, \mathcal{R}_l, \mathcal{R}_A \rangle \quad P \in \Pi$

$$\mathcal{M}, P \models K_A\phi \text{ iff } \begin{cases} \forall Q \in \Pi \text{ s.t. } (P,Q) \in \mathcal{R}_A,\ \mathcal{M}, Q \models \phi \\ \begin{cases} P \equiv i(A) \parallel P' \\ \forall i(A) \parallel Q' \in \Pi,\ \mathcal{M}, i(A) \parallel Q' \models \phi \end{cases} \end{cases}$$



Derived operators

$$1 \stackrel{def}{=} \neg((\neg 0) \parallel (\neg 0)) \qquad \alpha.\psi \stackrel{def}{=} (\langle\alpha\rangle\psi) \wedge 1$$

$$\widetilde{K}_A\phi \stackrel{def}{=} \neg K_A \neg\phi$$

$$\mathcal{M}, P \models 1 \text{ iff } P \equiv 0 \text{ or } P \equiv \alpha.Q$$

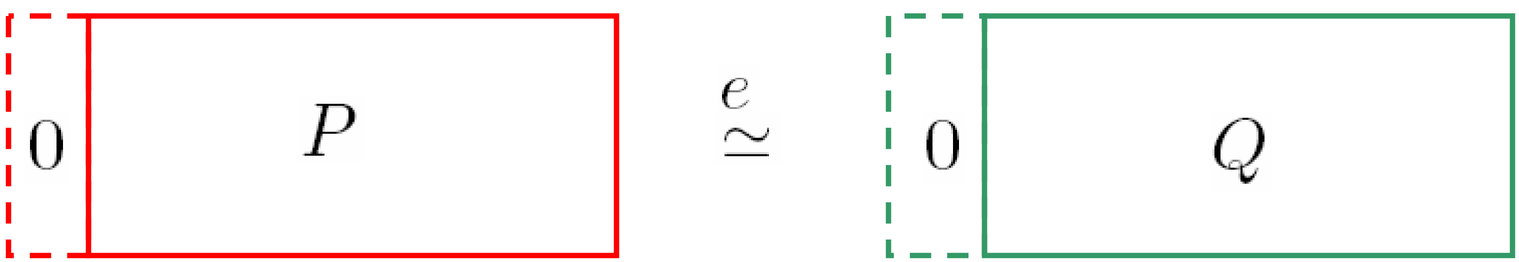
$$\mathcal{M}, P \models \alpha.\phi \text{ iff } P \equiv \alpha.Q \text{ and } \mathcal{M}, Q \models \phi$$

$$\mathcal{M}, P \models \widetilde{K}_A\phi \quad \text{iff} \quad \begin{cases} \text{either } P \not\equiv I(A) \| R \\ \text{or } \exists I(A) \| S \in \Pi,\ \mathcal{M}, I(A) \| S \not\models \phi \end{cases}$$

Consider the atomic agent $e \in \mathfrak{A}$

$$\mathcal{M}, P \models K_e\phi \text{ iff } \begin{cases} P \equiv P|0 \\ \forall Q \in \Pi, \quad \mathcal{M}, Q \models \phi. \end{cases}$$

$$\mathcal{M}, P \models \widetilde{K}_e\phi \text{ iff } \begin{cases} \text{either } P \not\equiv P|0 \quad \text{not possible} \\ \text{or} \quad \exists Q \in \Pi \quad \mathcal{M}, Q \models \phi. \end{cases}$$



$P \equiv P|0$ $\qquad$ $Q \equiv Q|0$

$$\mathcal{F}_{\mathbb{P}} = \{(f_P) \mid P \in \mathbb{P}\}$$

$$f_0 \stackrel{def}{=} 0 \qquad f_{P|Q} \stackrel{def}{=} f_P | f_Q \qquad f_{\alpha.P} \stackrel{def}{=} \alpha.f_P$$

Proposition $\mathcal{M}, P \models f_Q$ *iff* $P \equiv Q$.

Let Φ *be a finite set of formulas*

$$\Delta\Phi \stackrel{def}{=} K_e(\bigvee_{\phi\in\Phi} \phi) \wedge (\bigwedge_{\phi\in\Phi} \widetilde{K}_e\phi).$$

$\mathcal{M}, P \models \Delta\Phi$ iff

for any $Q \in \Pi$ there exists $\phi \in \Phi$ such that $\mathcal{M}, Q \models \phi$

for any $\phi \in \Phi$ there exists $Q \in \Pi$ such that $\mathcal{M}, Q \models \phi$.

Spatial axioms

S1: $\vdash \top | \bot \rightarrow \bot$

S2: $\vdash (\phi|\psi)|\rho \rightarrow \phi|(\psi|\rho)$

S3: $\vdash \phi|0 \leftrightarrow \phi$

S4: $\vdash \phi|(\psi \vee \rho) \rightarrow (\phi|\psi) \vee (\phi|\rho)$

S5: $\vdash \phi|\psi \rightarrow \psi|\phi$

Spatial rules

SR1: $\vdash \phi \rightarrow \psi$ then $\vdash \phi|\rho \rightarrow \psi|\rho$

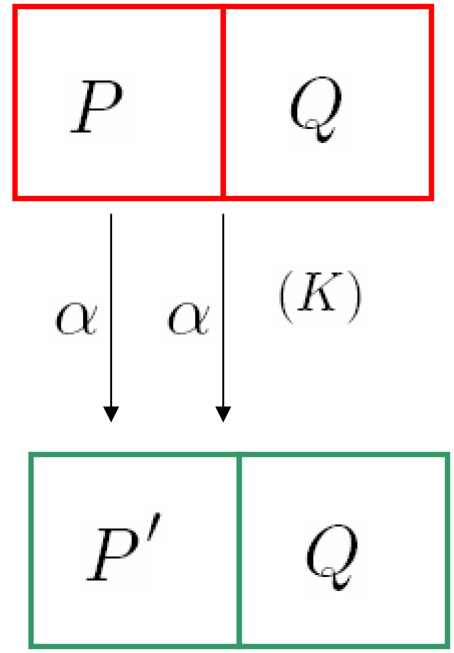
Dynamic axioms

D1: $\vdash \langle a \rangle \phi | \psi \longrightarrow \langle a \rangle (\phi | \psi)$

D2: $\vdash [a](\phi \longrightarrow \psi) \longrightarrow ([a]\phi \longrightarrow [a]\psi)$

D3: $\vdash 0 \vee \alpha.\top \longrightarrow [\beta]\bot$

D4: $\vdash \alpha.\phi \longrightarrow [\alpha]\phi$



Dynamic rules

DR1: If $\vdash \phi$ then $\vdash [a]\phi$ (Nec)

DR2: If $\vdash \phi_1 \longrightarrow [a]\phi_1'$ and $\vdash \phi_2 \longrightarrow [a]\phi_2'$

$then \vdash \phi_1 | \phi_2 \longrightarrow [a](\phi_1' | \phi_2 \vee \phi_1 | \phi_2')$

Epistemic axioms

E12: $\vdash K_A\phi \wedge K_A(\phi \rightarrow \psi) \rightarrow K_A\psi$ (K)

E13: $\vdash K_A\phi \rightarrow \phi$ (T)

E14: $\vdash K_A\phi \rightarrow K_AK_A\phi$

E15: $\vdash K_A\top \rightarrow (\neg K_A\phi \rightarrow K_A\neg K_A\phi)$ (5)

Epistemic rules

ER5: $\vdash \phi$ then $\vdash K_A\top \rightarrow K_A\phi$ (Nec)

Mixed axioms

M3: $\vdash \langle A : \alpha \rangle \phi \wedge \langle A | A' : \alpha \rangle \top \rightarrow \langle A | A' : \alpha \rangle \phi$

M4: $\vdash \langle A : \alpha \rangle \phi | \langle A' : \overline{\alpha} \rangle \psi \rightarrow \langle A, A' : \alpha \rangle (\phi | \psi)$

Theorem $\vdash K_A \phi \rightarrow K_A \top$

Theorem (Monotonicity of knowledge)

$$If \vdash \phi \rightarrow \psi \text{ } then \vdash K_A \phi \rightarrow K_A \psi$$

Theorem (Consistency of knowledge)

$$\vdash K_A \phi \rightarrow \neg K_A \neg \phi$$

Metatheorem (Soundness)
The system $\mathcal{L}_{\mathbb{A}}^{\mathfrak{A}}$ is *sound w.r.t. process semantics.*

Metatheorem (Completeness)
The system $\mathcal{L}_{\mathbb{A}}^{\mathfrak{A}}$ is *complete w.r.t. process semantics.*

Metatheorem (Finite model property)
The system $\mathcal{L}_{\mathbb{A}}^{\mathfrak{A}}$ *has the finite model property w.r.t. process semantics.*

Metatheorem (Decidability)
For $\mathcal{L}_{DES}$ *validity, satisfiability and model checking are decidable against the process semantics.*

Potential applications

- Secure Communication => checking secrecy and authentication for given communication protocols in contextual situations
- Artificial Intelligence => endowing artificial agents with good and flexible tools to reason about their changing environment and about each other
- Semantic Web => in designing strategies for knowledge acquisition over complex networks (such as the Internet)
- Debugging and Diagnosis => identifying the agents that generates errors
- Performance Analysis => identifying the “expensive” agent
- Systems Biology => biological agents are membrane-bounded and mobile chemical soups; they interact by exchanging chemical elements

- A new logic for knowledge in Multiagent-Systems
  - the semantic is based on process algebra
  - agents have (ontological) structures
  - agents can "develop knowledge" about dynamic distributed systems
  - agents are individuals, societies of individuals, societies of societies
  - agents are active: they can update information (knowledge) and can change their spatial position
  - has a sound and complete Hilbert-style axiomatic system
  - validity, satisfiability and model-checking are decidable