数理解析研究所講究録
906 巻 1995 年 32-38

マルチエージェントの知識論理における 多様相化した推論の正当性について

森 雅生
Masao Mori
九州大学総合理工学研究科情報システム学専攻
Interdisciplinary Graduate School of Engineering Sciences
Kyushu University

平成 7 年 1 月 31 日

概要

We introduce a new formalization of Kripke frame for knowledge logic using relational calculus and transitions of state into Kripke frame. Though knowledge logic was applied to verification of communication protocol, transition of systems has not directly been dealt with yet. Assuming commutativity of relations in Kripke frame and a transition relation, we investigate propriety that agents in systems infer a fact from information at state before transition.

1 Introduction

We introduce a new formalization of Kripke frame for knowledge logic using relational calculus and transitions of state into Kripke frame. Knowledge logic is applied to verification of communication protocol in [HM89], [HM90] and [HZ89]. Their work shows axiomatization of knowledge logic to be useful to design and verify communicating systems but Kripke frame does not provide some notion about transition of states, because relations in Kripke frame is treated as *indistinguishability* of global states for each agent. Assuming commutativity of relations in Kripke frame and transition relation, we investigate propriety that agents in systems infer a fact from information at state before transition.

2 Preliminaries

In this section we give a brief introduction to relational calculus. One may refer [SS85], [Tar41] [KM92] and [Kaw90] for detail explanation.

A relation $\alpha : A \rightharpoonup B$ from a set A into a set B is a subset $\alpha \subseteq A \times B$. The composition of relations is defined as follows; for relations $\alpha : A \rightharpoonup B$, $\beta : B \rightharpoonup C$, the composite $\alpha\beta : A \rightharpoonup C$ is;

$$\alpha\beta = \{(a,c) \subseteq A \times C \mid \exists b : (a,b) \in \alpha \ \& \ (b,c) \in \beta\}.$$

To avoid confusion with sets inclusion, intersection and union of relations are denoted by squared symbols; $\alpha \sqsubseteq \beta$, $\alpha \sqcap \beta$ and $\alpha \sqcup \beta$, respectively.

The whole collection of relations forms the involution category; for relations $\alpha, \alpha' : A \rightharpoonup B$, $\beta, \beta' : B \rightharpoonup C$, and $\gamma : C \rightharpoonup D$,

- the composition is commutative; $(\alpha\beta)\gamma = \alpha(\beta\gamma)$,
- each domain has an identity relation; $1_A\alpha = \alpha 1_B$,
- involution of each relation is defined; $\alpha^{\sharp\sharp} = \alpha$, $(\alpha\beta)^{\sharp} = \beta^{\sharp}\alpha^{\sharp}$
- If $\alpha \sqsubseteq \alpha'$ and $\beta \sqsubseteq \beta'$, then $\alpha\beta \sqsubseteq \alpha'\beta'$ and $\alpha^{\sharp} \sqsubseteq \alpha'^{\sharp}$.

For sets A and B, let **Rel**(A,B) be the set of all relations from A to B. $(\mathbf{Rel}(A,B), \sqsubseteq, \sqcap)$ is a Heyting algebra. We denote the minimum element standing for the empty relation and the maximum element standing for the total relation, respectively. We denote one–point set by $\star$ and the total relation (all the whole pair) from $\star$ to a set A by ∇_A.

Note 2.1: In relational calculus we express an element $x \in A$ by a relation from one–point set $\star$ to A. □

Functions are relations satisfying *univalency* and *totality*; i.e. a relation $\alpha : A \rightharpoonup B$ is a function if and only if it holds that $\alpha^{\sharp}\alpha \sqsubseteq 1_B$ and $1_A \sqsubseteq \alpha\alpha^{\sharp}$. We denote a function α by $\alpha : A \to B$. If $\alpha^{\sharp}\alpha = 1_B$ or $1_A = \alpha\alpha^{\sharp}$ hold then the relation α is *surjective* or *injective*, respectively.

We provide some axiom called *Dedekind's formula*.

[Dedekind's formula] For any relations $\alpha : A \rightharpoonup B$, $\beta : B \rightharpoonup C$, and $\gamma : A \rightharpoonup C$, it holds that $\alpha\beta \sqcap \gamma \sqsubseteq \alpha(\beta \sqcap \alpha^{\sharp}\gamma)$.

We should mention the fact about composition of relations without proof.

Proposition 2.1 *Let $\alpha, \alpha_i : A \rightharpoonup B$ and $\beta, \beta_j : B \rightharpoonup C$ where $i = 1,2$.*

1. *composition preserves inclusion; If $\alpha_1 \sqsubseteq \alpha_2$ and $\beta_1 \sqsubseteq \beta_2$, then $\alpha_1\beta_1 \sqsubseteq \alpha_2\beta_2$.*
2. *$\alpha(\beta_1 \sqcup \beta_2) = \alpha\beta_1 \sqcup \alpha\beta_2$, $(\alpha_1 \sqcup \alpha_2)\beta = \alpha_1\beta \sqcup \alpha_2\beta$.*
3. *$\alpha(\beta_1 \sqcap \beta_2) \sqsubseteq \alpha\beta_1 \sqcap \alpha\beta_2$, $(\alpha_1 \sqcap \alpha_2)\beta \sqsubseteq \alpha_1\beta \sqcap \alpha_2\beta$.*

In this paper the *quotient* relation will play an important role in expressing semantics of knowledge logic.

Definition 2.1 *For relations $\alpha : A \rightharpoonup B$, $\gamma : B \rightharpoonup C$ and $\beta : A \rightharpoonup C$, the* quotient *relation $\beta \div \gamma : A \rightharpoonup B$ is a relation such that $\alpha\gamma \sqsubseteq \beta \Leftrightarrow \alpha \sqsubseteq \beta \div \gamma$.*

$$\begin{tikzcd}
& A \arrow[dl, "\beta"'] \arrow[dr, shift left, "\beta\div\gamma"] \arrow[dr, shift right, "\alpha"'] & \\
C & & B \arrow[ll, "\gamma"]
\end{tikzcd}$$

In other words, the quotient relation $\beta \div \gamma$ is the greatest relation α satisfying that $\alpha\gamma \sqsubseteq \beta$.

Proposition 2.2 *Let $\beta, \beta' : A \rightharpoonup C$, $\gamma, \gamma' : B \rightharpoonup C$, $\delta : D \rightharpoonup B$ be relations and a function $f : B \to C$.*

1. *If $\beta \sqsubseteq \beta'$ and $\gamma' \sqsubseteq \gamma$ then $\beta \div \gamma \sqsubseteq \beta' \div \gamma'$.*
2. *$(\beta \div \gamma) \div \delta = \beta \div \delta\gamma$.*
3. *$(\beta \sqcap \beta') \div \gamma = (\beta \div \gamma) \sqcap (\beta' \div \gamma)$, $(\beta \sqcup \beta') \div \gamma = (\beta \div \gamma) \sqcup (\beta' \div \gamma)$.*
4. *$\beta \div (\gamma \sqcup \gamma') = (\beta \div \gamma) \sqcap (\beta \div \gamma')$*
5. *If f is a function then $\beta \div f = \beta f^{\sharp}$.*

Note 2.2: As an identity relation is a function, for a relation $\beta : A \rightharpoonup B$ it hold that $\beta \div 1_B = \beta 1_B^{\sharp} = \beta$. □

3 Interpretations for knowledge logic

We give syntacs and semantics of knowledge logic for concurrent system in this section. Semantics with relational calculus is originated by Kawahara [Kaw94].

Firstly, we define *knowledge dynamics* to describe concurrent systems. Let I be a finite set of names of agents. For each agent i the set Q_i is a collection of *(local) states* of i. A knowledge dynamics consists of a cartesian product $Q = Q_1 \times \cdots \times Q_n$ of *(global) states*, a set E of *environments*, transition relation $\rho : Q \rightharpoonup Q$, an equivalence relation $\delta_i : Q \rightharpoonup Q$ for each $i \in I$ and an observation function $q : Q \rightarrow E$ such that for each $i \in I$ the square commutes;

$$\begin{tikzcd}
Q \arrow[r, "\rho"] \arrow[d, "\delta_i"] & Q \arrow[d, "\delta_i"] \\
Q \arrow[r, "\rho"'] & Q
\end{tikzcd}$$

Each equivalence relation δ_i is defined as follows; $(s, s') \in \delta_i$ if and only if $p_i(s) = p_i(s')$ where p_i is a projection.

Example 3.1 The choice of the ways describing concurrent processes depends on which purpose one aim at[Hoa85][Mil89]. In this example, following [CM86] and [Hoa85] we represent process behaviours as atomic actions, and transition of states as sequences of atomic actions. Atomic actions are classified into two kinds. One is internal and the other is about interactions. We give the set A of atomic actions which consists of ; $(j!m)_i$ process i receives a message m from process j, $(j?m)_i$ process i sends a message m to process j and $a_1, b_1, \cdots, a_i, b_i, \cdots$ internal actions where $i, j \in \{1, \cdots, n\}$ is names of processes. We assume finite number of processes. The set A may be divided in terms of their owner. We denote the set of process i's actions by A_i. Transitions of processes' states are specified with finite sequences of actions: they are histories of behavior so far. We call them *traces*, and their sets T_i must satisfy the following conditions.

- It includes an empty sequence; $\epsilon \in T_i$.
- If t belongs to T_i and s is prefixed in t then s belongs to T_i.

We mean a process by a pair (A_i, T_i). Generally speaking, when we models a concurrent system it inherits somewhat structure from its components. A concurrent system is a pair of cartesian product of actions and traces with some constraint. As each process acts independently from other processes except interactions, we manage synchronization of system behavior. Asynchronization is not significant problem because asynchronous concurrent systems can be rearranged as synchronous ones. Actions of concurrent systems are represented by means of vectors in $A_1 \times \cdots \times A_n$, called *action vectors.* Transitions of systems are defined as vectors of traces, called *trace vectors.* We providea constraint of synchronization for trace vectors: all of components in a trace vector must be in the same length. We denote the cartesian products $T_1 \times \cdots \times T_n$ and $A_1 \times \cdots \times A_n$ by $\mathcal{T}$ and $\mathcal{A}$. The function σ is a suffixing function from $\mathcal{T}$ to $\mathcal{A}$. Its value means a action vector corresponding to the latest action of each process. Assuming that the communication is done synchronously a successful communication in trace vector t is expressed by

$$\sigma(t) = (\cdots, (j!m)_i, \cdots, (i?m)_j, \cdots).$$

Then the transition relation $\rho \subseteq \mathcal{T} \times \mathcal{T}$ is defined as follows: $(t, s) \in \rho$ if and only if $s \cdot \sigma(t) = t$ where $\cdot$ is concatenation for each component of vectors. □

Definition 3.1 *Knowledge propositions are defined as follows.*

- *Every relation $\sigma : 1 \rightharpoonup E$ is an atomic proposition.*
- *if φ and ψ are knowledge propositions, then*

$$\bot,\ \varphi \vee \psi,\ \varphi \wedge \psi,\ \neg\varphi,\ \varphi \rightarrow \psi,\ K_i\varphi\ (i \in I),\ C\varphi$$

  are knowledge propositions. The symbol K_i and C show i's knowledge and common knowledge, respectively.

An Interpretation of knowledge propositions is given as relations from one point set to the set of states for each transision steps. We introduce the *interpretation* using relational calculus from [Kaw94], denoted by [ ], as follows:

- $[\bot] = 0_Q : 1 \rightharpoonup Q$ (empty relation).
- For a atomic proposition $\sigma : 1 \rightharpoonup E$, $[\sigma] = \sigma \div q$.
- For logical symbols $\vee$, $\wedge$ and $\neg$ the assignment function assigns union, intersection and complement of relations, respectively;

$$[\varphi \vee \psi] = [\varphi] \sqcup [\psi],\ \ [\varphi \wedge \psi] = [\varphi] \sqcap [\psi]$$

- The implication is assigned to pseudo compliment;

$$[\varphi \rightarrow \psi] = [\varphi] \Rightarrow [\psi],\ \ [\neg\varphi] = [\varphi] \Rightarrow [\bot]$$

- For modal symbols *quotient* relation is assigned;

$$[K_i\varphi] = [\varphi] \div \delta_i,$$

The next proposition shows that axiom schemata S5 of knowledge logic is valid in terms of the interpretation [ ].

Proposition 3.1 *[Kaw94] For the following principle of the relation δ_i we have the facts;*

1. $[K_i\varphi \wedge K_i(\varphi \rightarrow \psi)] \sqsubseteq [K_i\psi]$,
2. *if δ_i is reflexive, then $[K_i\varphi] \sqsubseteq [\varphi]$ and $[C\varphi] \sqsubseteq [CK_i\varphi]$,*
3. *if δ_i is transitive, then $[K_i\varphi] \sqsubseteq [K_iK_i\varphi]$,*
4. *if δ_i is an equivalence relation, then $[\neg K_i\varphi] \subseteq [K_i\neg K_i\varphi]$,*
5. *if $[\varphi] = \nabla_Q$, then $[K_i\varphi] = \nabla_Q$ where ∇ is the total relation from $\star$ to Q, and*
6. *if each δ_i is reflexive, then $[C\varphi] = [\varphi] \sqcup [K_1C\varphi] \sqcup \cdots \sqcup [K_nC\varphi]$.*

4 Propriety of inference

The validity in one step transitions before is formalized using a quotient relation as follows;

$$[\varphi] \div \rho^{\sharp}.$$

While the interpretation has a commutative correspondence of semantic and syntactic operations, the interpretation with respect to one step previous transition has only the case of conjenction and disjenction.

Lemma 4.1 *Let φ, ψ be knowledge propositions including only disjunction and conjunction symbols. Then*

$$[\varphi \vee \psi] \div \rho^\sharp = [\varphi] \div \rho^\sharp \sqcap [\psi] \div \rho^\sharp$$
$$[\varphi \wedge \psi] \div \rho^\sharp = [\varphi] \div \rho^\sharp \sqcup [\psi] \div \rho^\sharp$$

Each agent infers from previous message and determines its next action and its next message to send. We provide a property which guarantees that agents reasonably infer proposition from some messages.

Definition 4.1 *Let $s \in Q$ and let φ be a knowledge proposition and $\Gamma \equiv \psi_1 \wedge \cdots \wedge \psi_m$ be a conjunctive knowledge propositions. We say that* agent i knows φ from the condition set Γ at s *if and only if*

$$s\delta_i \sqcap [\Gamma] \div \rho^\sharp \sqsubseteq [\varphi]$$

As mentioned in the previous section, the quotient relation is the greatest relation α satisfing the commutative diagram:

$$\begin{tikzcd} & \star \arrow[dl, "{[\Gamma]_{k-1}}"'] \arrow[dr, "\alpha"] & \\ Q & & Q \arrow[ll, "\rho^\sharp"] \end{tikzcd}$$

Lemma 4.2 *Let $s \in Q$. Assume that i knows φ from Γ at s. For every state t such that $(t, s) \in \rho$, if $t \models K_i\varphi$ then $s \models K_i\varphi$.*

Proof : Suppose that for every state $t \in Q$ such that $t \sqsubseteq s\rho^\sharp$, $t \sqsubseteq [\varphi] \div \delta_i$, that is

$$s\rho^\sharp \sqsubseteq [\varphi]_k \div \delta_i$$

As ρ and δ_i are commutative,

$$\begin{aligned} s &\sqsubseteq ([\varphi] \div \delta_i) \div \rho^\sharp \\ s &\sqsubseteq [\varphi] \div \rho^\sharp \delta_i \\ s &\sqsubseteq [\varphi] \div \delta_i \rho^\sharp \\ s &\sqsubseteq ([\varphi] \div \rho^\sharp) \div \delta_i \\ s\delta_i &\sqsubseteq [\varphi] \div \rho^\sharp \end{aligned}$$

From assumption it holds that

$$s\delta_i \sqcap [\varphi] \div \rho^\sharp \sqsubseteq [\psi]$$

Then we have $s\delta_i \sqsubseteq [\psi]$. □

Remark 4.1: If the transition relation ρ is reflexive, then it holds that $[\varphi] \div \rho \sqsubseteq [\varphi]$ for any knowledge proposition φ. □

Theorem 4.1 *Let the transition relation ρ be reflexive, and $[\Gamma] \sqsubseteq [\varphi]$ where Γ is a conjunctive knowledge proposition and φ is a knowledge proposition. For any transition $(t, s) \in \rho$, if $t \models K_i\Gamma$ then $s \models K_i\varphi$.*

Proof : Assume that $t \sqsubseteq [\Gamma] \div \delta_i$ for every $t \sqsubseteq s\rho^\sharp$, that is,

$$s\rho^\sharp \sqsubseteq [\Gamma] \div \delta_i.$$

参考文献

As ρ and δ_i are commutative, we have

$$s\delta_i\rho^\sharp = s\rho^\sharp\delta_i \sqsubseteq [\Gamma]$$

so that $s\delta_i \sqsubseteq [\Gamma] \div \rho^\sharp$. From assumption

$$\begin{aligned} s\delta_i &= s\delta_i \sqcap [\Gamma] \div \rho^\sharp \\ &\sqsubseteq s\delta_i \sqcap [\varphi] \div \rho^\sharp \\ &\sqsubseteq s\delta_i \sqcap [\varphi] \end{aligned}$$

therefore $s\delta_i \sqsubseteq [\varphi]$, hence $s \sqsubseteq [\varphi] \div \delta_i$. □

Corollary 4.1 *(In the same condition of theorem.) For every transition $(t, s) \in \rho$, if $t \models K_i\varphi$ then $s \models K_i\varphi$ then $s \models K_i\varphi$.*

Proof : By theorem in the case of $\Gamma \equiv \varphi$. □

Proposition 4.1 *Let ρ be reflexive. For every transition $(t, s) \in \rho$, if $t \models K_i\varphi$ and $t \models K_i\psi$ then i knows $\varphi \vee \psi$ from $\varphi \wedge \psi$.*

Proof : By assumption we have

$$\begin{aligned} s\rho^\sharp &\sqsubseteq [K_i\varphi] \sqcap [K_i\psi] \\ &= ([\varphi] \div \delta_i) \sqcap ([\psi] \div \delta_i) \\ &= ([\varphi] \sqcap [\psi]) \div \delta_i. \end{aligned}$$

As ρ and δ_i commutes

$$\begin{aligned} s\delta_i &\sqsubseteq ([\varphi] \sqcap [\psi]) \div \rho^\sharp \\ &= [\varphi \wedge \psi] \div \rho^\sharp \\ &\sqsubseteq [\varphi \vee \psi] \div \rho^\sharp \\ &\sqsubseteq [\varphi \vee \psi] \end{aligned}$$

from assumption. Hence we have $s\delta_i \sqcap ([\varphi \wedge \psi] \div \rho^\sharp) \sqsubseteq [\varphi \vee \psi]$. □

参考文献

[CM86] K. M. Chandy and J. Misra. How processes learn. *Distributed Computing*, 1:40–52, 1986.

[FH88] R. Fagin and J. Y. Halpern. I'm ok if you're ok: On the notion of trusting communication. *Journal of Philosophical Logic*, 17:329–354, 1988.

[HM89] J. Y. Halpern and Y. Moses. Modelling knowledge and action in distributed systems. *Distributed Computing*, 3:159–177, 1989.

[HM90] J. Y. Halpern and Y. Moses. Knowledge and common knowledge in a distributed environment. *Journal of the Association for Computing Machinery*, 37(3):549–587, 1990.

[Hoa85] C.A.R. Hoare. *Communicating Sequential Processes.* Prentice Hall, 1985.

参考文献

[HZ89] J. Y. Halpern and L. D. Zuck. A little knowledge goes a long way: Simple knowledge–based derivation and correctness proofs for a family for protocols. Technical Report RJ 5857, IBM Research Division, 1989.

[Kaw90] Y. Kawahara. Pushout–complements and basic concepts of grammers in toposes. *Theoretical Computer Science*, 77:267–289, 1990.

[Kaw94] Y. Kawahara. Relational formalization of knowledge dynamics. draft, 1994.

[KM92] Y. Kawahara and Y. Mizoguchi. Categorical assertion semantics in topoi. *Advances in Software and Technology*, 4:137–150, 1992.

[LL90] L. Lamport and N. Lynch. Distributed computing: Models and methods. In van Leeuwen J., editor, *Handbook of theoretical computer science*, pages 1157–1199. Elsevier Science Publishers B.V., 1990.

[Mil89] R. Milner. *Communication and Concurrency*. Prentice Hall, 1989.

[SS85] G. Schmidt and T. Ströhlein. Relation algebras: Concept of points and represetntability. *Discrete Mathematics*, 54:83–92, 1985.

[Tar41] A. Tarski. On the calculus of relations. THE JOURNAL OF SYMBOLIC LOGIC, 6(3), 1941.