通信サービス記述のための知識と動作に基づく様相不動点論理 SSL

楢崎 修二　堀田 英一
NTT ソフトウェア研究所

様相不動点論理 Service Specification Logic(SSL) を提案する．これはプロセス論理と共通知識論理，不動点論理を融合したものである．その目的は通信サービスに対する利用者の要求の形式的な記述手段を与え，これによって利用者の視点からのサービスの検証・分類を実現することにある．本稿では，SSL の構文と意味論を紹介し，有限記憶の状態遷移機械上で SSL 式の充足性が決定可能であることを示す．

Modal Fixpoint Logic SSL Based on Knowledge and Action for Describing Communication Services

Shuji NARAZAKI　Eiichi HORITA
NTT Software Laboratories

This paper proposes a modal fixpoint logic 'Service Specification Logic' (SSL) which is an integration of *process logic*, *logics of common knowledge*, and *fixpoint logics*. The purpose of the logic is to provide a language in which the user can describe his requirement formally, and thereby classify communication services from his viewpoint. First, the syntax and semantics of SSL are introduced. Then it is shown to be decidable whether a given formula is satisfied by a given finite state transition machine with a finite memory for its history.

1 はじめに

従来の通信サービスはその実現にどのような機能を必要とするかという観点から分類され，論じられることが多かった．しかし，通信網が高度化し，通信サービスが多様化した現在では，どのような通信サービスがユーザの要求に答えられるのか，あるいは，どのような通信サービスをユーザは欲しているのかなどを記述し，論じる手段が望まれている．

そこで，我々は，通信サービスに対するユーザの要求を「通信に関わる人間達（エージェント群）の知識所有状態を特定の状態に変化させること」であると考え，この要求（抽象サービス仕様）を形式的に記述し，実際のサービスと要求との間を関係付ける手段として，様相論理 **SSL**(Service Specification Logic) を提案した [5].

これは，従来提案されている，並行プロセスの性質記述のためのプロセス論理 [1] と，複数エージェント間の知識の所有状態を記述・推論するための Logics of Common Knowledge(LCK)[2] との両者を融合させた様相論理体系である．この二者を融合させることにより，プロセス論理あるいは LCK 単独では記述できなかった，並行プロセスの処理の進行に伴うエージェント（プロセス）の知識所有状態の変化を記述・推論することが出来るようになる．従って，様相論理 SSL を用いることによって，先に述べたような通信サービスに対するユーザの要求を記述することが可能になり，サービス仕様の形式的記述・分類・model checking などが可能になる．

本稿では以前提案した SSL へ不動点演算子 [6] の導入を行なう．この結果，

- 様相論理で提案されている種々の様相演算子を不動点演算子を用いて記述できる，
- 通信サービスのような終了しないプロセスの性質を直接的に表現でき，SSL 式の本質的な表現力が増加する

という利点が得られる．

本稿の構成を以下に示す．2 節にて本稿において用いる数学的記法を説明する．3 節では様相不動点論理 SSL の構文および意味論を示す．4 節では打ち切り履歴という概念を導入することによって，任意の SSL 式の充足性が有限状態遷移システム上で決定可能であることを示す．5 節では例題により SSL を用いた model checking による通信サービスの仕様検証や分類が可能であることを示す．6 節はまとめおよび今後の課題である．

2 数学的準備

自然数 n はそれより小さいものの集合と同一視される．すなわち $n = \{0, 1, \cdots, n-1\}$ である．順序数全体のクラスを Ord で表す．

定義 1 (列) 列（組）の添字は *0* から始まるものとする．列 s の i 番目の要素を s_i または $s(i)$ で表す．列 s の長さを $\sharp s$ で表す．'.' を列の結合演算子とする．

列 s の i 番目から j 番目の要素までから構成される部分列を $sub(s, i, j)$ とし，列 s の最後の *(*多くとも*)*i 個の要素からなる部分列 $last_i(s)$ を以下のように定義する．

$$last_i(s) = sub(s, max(0, \sharp s - i), \sharp s - 1)$$

また $last(s) = s_{\#s-1}$ とする．すなわち，$last(s)$ は列 s の最後の要素である．逆に列 s の最後の要素のみを除いた列 $butlast(s)$ を以下のように定義する．

$$butlast(s) = sub(s, 0, \sharp s - 2)$$

集合 S の要素からなる長さ l の列を S^l で表す．また，l までの長さからなる列を $S^{\leq l} = \bigcup_{k \in (l+1)}[S^k]$ で表す．更に，$S^* = \bigcup_{k \in \omega}[S^k]$ とする．

定義 2 (関係) X を集合，R, R' を X 上の *2* 項関係とする（すなわち $R, R \subseteq X \times X$ とする）．R と R' からなる合成関係を $R \circ R'$ と書く（従って $R \circ R' = \{\langle x, z\rangle \mid \exists y \in X \left[\langle x, y\rangle \in R \wedge \langle y, z\rangle \in R' \right]\}$）．次に，$n \in \omega$ に対して $R^{[n]}$ を以下のように定義する．

$$R^{[0]} = EQ_x = \{\langle x, x\rangle \mid x \in X\}$$

$$R^{[n+1]} = R^{[n]} \circ R$$

さらに $R^{[<n]}$，$R^{[*]}$ を以下のように定義する．

$$R^{[<n]} = \bigcup_{i \in n}[R^{[i]}]$$

$$R^{[*]} = \bigcup_{i \in \omega}[R^{[i]}]$$

定義 3 (不動点) 集合 S の冪集合 $\wp(S)$ 上で定義された単調関数 $f: \wp(S) \to \wp(S)$ に対し，最小不動点および最大不動点が存在する *(*例えば *[7]* 参照*)*．そこで関数 f の最小不動点を $\mathrm{fix}_\ell(f)$ で，最大不動点を $\mathrm{fix}_g(f)$ で表すことにする．

補題 1 S を集合，f を $\wp(S)$ からそれ自身への単調な写象とする．このとき，κ を $\sharp(\wp(S))$ より大きい基数のうち最小のものとすると，ある順序数 $\xi \in \kappa$ について，次のことがなりたつ．

$$\mathrm{fix}_\ell(f) = f^\xi(\emptyset). \tag{1}$$

ここで，各順序数 ξ に対して f^ξ は f の ξ 次の繰り返しであり，次のように帰納的に定義される．各 $X \in \wp(S)$ に対して，

$$f^{\xi}(X) = \begin{cases} X & \xi = 0 \text{ のとき,} \\ f(f^{\zeta}(X)) & \xi = \zeta + 1 \text{ のとき,} \\ \bigcup_{\zeta<\xi}[f^{\zeta}(X)] & \xi \text{ が極限順序数のとき.} \end{cases}$$

証明は付録Aに回す.

3 様相不動点論理 SSL

様相不動点論理SSLは，並行プロセス記述のための様相論理であるプロセス論理[1, 4]にLogics of Common Knowledge(LCK) [2]を付加した様相不動点論理体系である．有限状態遷移システムとして与えられる実現(implementation)の性質を記述し，記述をした性質について推論するための体系である．

3.1 構文

Φを原子式の集合，Aを動作の集合，Iをエージェントの集合とする．エージェントを表す添字にiを用いる．$a_i \in A_i$をエージェントiの観測可能動作と呼ぶ．$(\Phi, A, I$に基づく)SSL式の集合$(\phi \in)\mathcal{L}_{SSL}(\Phi, A, I)$を次のBNFにより定義する．

$$\phi ::= p \mid \neg\phi \mid (\phi \wedge \phi) \mid \exists x.\phi \mid \langle\alpha\rangle\phi \mid \mathrm{K}_i\phi \mid \mathrm{E}_g^n\phi \mid \mu X.\phi \mid X$$

ここで，$p \in \Phi$, $\alpha \in A \cup AVar$, $i \in I$, $g \in \wp(I)$, $x \in AVar$, $n \geq 1$である．$\langle\,\rangle$はプロセス論理の様相演算子であり，K, E^nおよび後で定義するCはLCKのそれである．特にE^1をEと表す．

また，μのϕ中に出現する変数Xは$\neg$が偶数回掛かっているものに限る．

記述の簡易化のため，

$$\begin{aligned} \phi_1 \vee \phi_2 &= \neg((\neg\phi_1) \wedge (\neg\phi_2)) \\ \phi_1 \Rightarrow \phi_2 &= \neg(\phi_1 \wedge \neg\phi_2) \\ \langle.\rangle^*\phi &= \mu X.(\phi \vee \exists a\,[\,\langle a\rangle true \wedge \langle a\rangle X\,]) \\ \nu X.\phi &= \neg\mu X.(\neg\phi[\neg X/X]) \\ \mathrm{C}_g\phi &= \nu X.(\mathrm{E}_g^1\phi \wedge \mathrm{E}_g^1 X) \end{aligned}$$

を導入する．また，$[a]\phi = \neg\langle a\rangle\neg\phi$とし，$[.]^*\phi = \neg\langle.\rangle^*\neg\phi$とする．$[a], [.]^*$はそれぞれ$\langle a\rangle, \langle.\rangle^*$の双対演算子である．

自由変数Xを持つSSL式ϕの変数Xへのψの代入の結果を$\phi[\psi/X]$と書く．

3.2 有限状態遷移システム

SSLの意味論を述べるために，本節では，SSLの構造として用いる状態遷移システムを説明する．

定義 4 (有限状態遷移システム) 有限状態遷移システムとして表されるI個のエージェントを並行合成して得られる有限状態遷移システムTを下式で表す．

$$T = \langle S, S^0, \Phi, A, (\xrightarrow{\alpha})_{\alpha\in A}, \pi\rangle$$

ここで，$S \subseteq \Pi_{i\in I}S_i$は大域状態(各エージェントの状態（局所状態）$S_i$からなるタプル）の集合，$S^0 \subseteq S$は初期状態の集合，$\xrightarrow{\alpha} = \{(s_1, s_2) \in S \times S \mid s_1 \xrightarrow{\alpha} s_2\}$は状態遷移を表す二項関係，$\pi: S \times \Phi \to \{true, false\}$は各状態での原子式の値の割り当てである．

定義 5 (状態動作対) 有限状態遷移システムTにおける全域状態$s \in S(T)$と動作$a \in A(T)$との組を$t \in SA(T) = \{\langle s, \alpha\rangle \mid \exists s' \in A(T)\,[\,s \xrightarrow{\alpha} s'\,]\} \subseteq S(T) \times A(T)$で表し，これを状態動作対と呼ぶ．$stat(t)$は状態動作対$t$における大域状態を，$act(t)$は動作を表すものとする．また，エージェント$i$の局所状態とエージェント$i$から観測可能な動作$a_i \in A_i$の組を局所動作状態対と呼び，$SA_i(T) \subseteq S_i(T) \times A_i(T)$で表す．

定義 6 (履歴) 有限状態遷移システムTの動作履歴は状態動作対の任意有限回の繰り返しと最終大域状態との列として表すことが出来る．そこでシステムの履歴hを以下のように定義する．

$$h \in (SA(T))^* \times S(T)$$

有限状態遷移システムTを定めると取り得る履歴の集合が決定する．これを$H(T) \subseteq (AS(T))^* \times S(T)$で表す．特に，始点$s \in S(T)$から始まる履歴の集合を$H(T; s)$とする．

定義 7 (履歴の結合) 2つの履歴h_1, h_2の結合演算子$\oplus$を以下のように定義する．これは履歴h_1で表される遷移を行なった後にh_2で表される遷移を行なうことを意味する．

$$h_1 \oplus h_2 = butlast(h_1) \cdot h_2$$

定義 8 (判別不能関係) 有限状態遷移システム上のエージェントiから見た判別可能性関係$\mathcal{K}_i$を以下のように定義する．ここでエージェントiの記憶の長さをそれぞれ$l(i) \in \omega$とする．

$$\mathcal{K}_i = \{(h_1, h_2) \mid last_{l(i)}(\rho_i(h_1)) = last_{l(i)}(\rho_i(h_2))\}$$
$$\rho_i(h) = sqsh((\langle act(h(j)), stat(h(j))(i)\rangle)_{j\in vis(h,i)})$$

上式中，$sqsh$は列を作る関数であり，関数fの定義域が$\{i_0, i_1, \cdots, i_n\} \subseteq \omega$,(但し$i_0 < i_1 < \cdots < i_n$)である時，$sqsh(f) = \langle f(i_0), f(i_1), \cdots, f(i_n)\rangle$である．また，$vis(h, i) = \{j \in \sharp(h) \mid act(h(j)) \in A_i\}$である．

$\mathcal{K}_i$はエージェントiから見た履歴の等価関係である．すなわち，$h_1\mathcal{K}_ih_2$ならば，エージェントiは履歴h_1とh_2を区別することはできない．上記のように履歴間の判別不能関係を定めることは，各エージェントとも自分が観測可能な動作状態対列の最後の$l(i)$個分の過去しか直接には知り得ないことを意味する．

次いで，グループ $g \in \wp(I)$ に対する判別不能関係 $\mathcal{K}_g$ を以下のように定義する．

$$\mathcal{K}_g = \bigcup_{i \in g} \mathcal{K}_i$$

定義 9 (SSL 構造) *SSL* に対する *(Kripke)* 構造 $\mathcal{M}$ を $\mathcal{M} = \langle T, (\mathcal{K}_i)_{i \in I} \rangle$ と定め，*SSL* 構造と呼ぶ．

3.3 意味論

定義 10 (履歴上の SSL 式の意味論) *SSL* 式 ϕ のモデル（ϕ を満たす履歴）の集合 $V: \mathcal{L}_{SSL} \to (VAR \to \wp(H(T))) \to \wp(H(T))$ を *SSL* 式の構造に関する帰納法を用いて、次のように定義する．

$$\begin{aligned}
V[\![p]\!]\eta &= \{h \in H(T) | p \in \pi(last(h))\} \\
V[\![X]\!]\eta &= \eta(X) \\
V[\![\neg\phi]\!]\eta &= H(T) \setminus V[\![\phi]\!]\eta \\
V[\![\phi \wedge \psi]\!]\eta &= V[\![\phi]\!]\eta \cap V[\![\psi]\!]\eta \\
V[\![\langle a \rangle \phi]\!]\eta &= \{h \in H(T) \mid last(h) \xrightarrow{a} s, \\
&\qquad h \oplus (\langle last(h), a \rangle, \langle s \rangle) \in V[\![\phi]\!]\eta\} \\
V[\![\exists x.\phi]\!]\eta &= \bigcup_{\alpha \in A(T)} V[\![\phi[\alpha/x]]\!]\eta \\
V[\![\mu X.\phi]\!]\eta &= \mathrm{fix}_\ell(f) = \bigcup_{\nu \in Ord} [f^\nu(\emptyset)] \\
&\quad f = \lambda H \in \wp(H(T)).V[\![\phi]\!](\eta[H/X]) \\
V[\![\mathrm{K}_i\phi]\!]\eta &= \{h \in H(T) \mid \forall h' \in H(T), \\
&\qquad h\mathcal{K}_i h' \Rightarrow h' \in V[\![\phi]\!]\eta\} \\
V[\![\mathrm{E}_g^n\phi]\!]\eta &= \{h \in H(T) \mid \forall h' \in H(T), \\
&\qquad h\mathcal{K}_g^{[n]} h' \Rightarrow h' \in V[\![\phi]\!]\eta\}
\end{aligned}$$

ここで $\eta \in (VAR \to \wp(H(T)))$ は付値 *(valuation)* を表す。また $A \setminus B$ は集合 A と B との差集合を表す．

定義 11 (充足関係) ϕ が自由変数を持たない場合は η のとり方によらず $V[\![\phi]\!]\eta$ が一意に定まる。そこで、自由変数を持たない *SSL* 式に対して、充足関係 $\models$ を以下のように定義する。

$$\begin{aligned}
\langle \mathcal{M}, h \rangle \models \phi &\Leftrightarrow h \in V[\![\phi]\!] \\
\mathcal{M} \models \phi &\Leftrightarrow \forall s \in S^0(T) \ [\ (\langle s \rangle) \in V[\![\phi]\!]\ ]
\end{aligned}$$

直観的な説明を与える．基本的に履歴 h の最後の状態で ϕ が成立する時に $\langle \mathcal{M}, h \rangle \models \phi$ が成立する．$\langle a \rangle \phi$ は動作 a の後には ϕ が成り立つ可能性があることを意味する．$\mathrm{K}_i\phi$ はエージェント i が ϕ を知っていることを，$\mathrm{C}_g\phi$ は「グループ g は ϕ をお互いに知っていることをお互いに知っていることを…」を意味する (図 1参照)．$\mathrm{C}_g\phi$ が成立する時，知識 ϕ はグループ g の中で**共通知識** (common knowledge) になっているという．

4 SSL 式の充足性の決定可能性

有限状態遷移システムでは履歴は無限に存在し，その長さも無限である．従って上の定義だけでは，任意の SSL 式が充足可能かどうかの決定が可能であることは自明ではない．そこで，履歴を有限長で打ち切って考えることにより，SSL 式の充足性が有限記憶長のエージェントからなる有限状態遷移システム上で決定可能であることを証明する．

4.1 打ち切り履歴

定義 12 (打ち切り履歴 : Truncated History) 任意の履歴 $h \in H(T)$ に対して以下のように定義される**打ち切り履歴** $tr(h) \subseteq (SA_i(T))^{<l(i)} \times A_i(T))^I$ を対応づける．また，関数 tr を“打ち切り”と呼ぶ．

$$tr(h) = (\rho_i(h))_{i \in I}$$

打ち切り履歴 $\widetilde{h}$ に対して最後の状態 $\widetilde{last}(\widetilde{h}) = (last(\widetilde{h}(i)))_{i \in I}$ を定義する．$\widetilde{last}(\widetilde{h})$ は打ち切り履歴 $\widetilde{h}$ で表された履歴の最後の大域状態である．また，$\forall h \in H(T) \ [\ last(h) = \widetilde{last}(tr(h))\ ]$ という性質が成り立つ．

補題 2 打ち切り履歴 $\widetilde{h}$ の領域は有限である．

証明 $\widetilde{h}$ の列の各要素は有限集合 $A_i(T) \times S_i(T)$ の要素である．$\widetilde{h}$ は有限種類の要素を高々 l 回並べたものであり，従って，打ち切り履歴 $\widetilde{h}$ の領域は有限である．ここで $l = \max_{i \in I} l(i)$ である． ∎

定義 13 (打ち切り履歴の結合) 打ち切り履歴に対する結合演算子 $\widetilde{\oplus}: \widetilde{H}(T) \times \widetilde{H}(T) \to \widetilde{H}(T)$ を以下のように定義する．

$$\widetilde{h} \widetilde{\oplus} \widetilde{h'} = (last_{l(i)}(butlast(\widetilde{h}(i)) \cdot \widetilde{h'}(i)))_{i \in I}$$

補題 3 $\forall h, h' \in H(T) \ [\ tr(h) \widetilde{\oplus} tr(h') = tr(h \oplus h')\ ]$

証明 打ち切り履歴の各要素が等しいことによる．

$$\begin{aligned}
&\forall i \in I \ [\ (tr(h) \widetilde{\oplus} tr(h'))(i) \\
&\quad = last_{l(i)}(butlast(tr(h)(i)) \cdot tr(h')(i)) \\
&\quad = last_{l(i)}(butlast(\rho_i(h)) \cdot \rho_i(h')) \\
&\quad = last_{l(i)}(\rho_i(butlast(h) \cdot h')) \\
&\quad = \rho_i(butlast(h) \cdot h') = tr(h \oplus h')(i)\ ]
\end{aligned}$$

∎

定義 14 (打ち切り履歴集合) システム T 上で取り得る打ち切り履歴集合 $\widetilde{H}(T)$ を以下のように定義する．

$$\widetilde{H}(T) = \{tr(h) \mid h \in H(T)\}$$

また，始点を $s \in S(T)$ に限った打ち切り履歴の集合を $\widetilde{H}(T; s)$ と表す．

補題 4 大域状態 $s \in S$ から実行可能な全ての履歴に対する打ち切り履歴集合 $\widetilde{H}(T; s)$ は計算可能である．

この証明は [5] で行なったので，本稿では省略する．

定義 15 打ち切り履歴に対する判別不能関係を以下のように定義する．

$$\widetilde{\mathcal{K}}_i = \{(\widetilde{h}_1, \widetilde{h}_2) \mid \widetilde{h}_1(i) = \widetilde{h}_2(i)\}$$

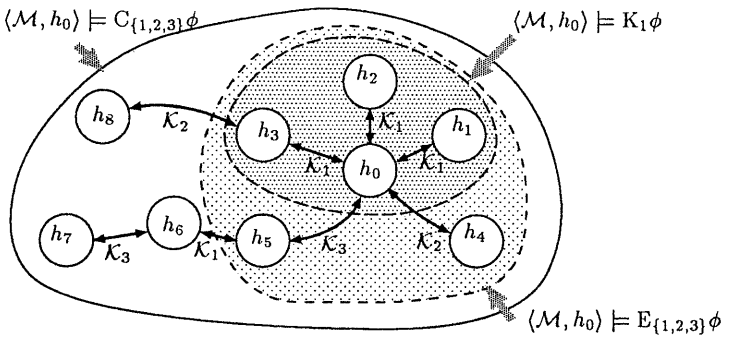

図 1: $\mathcal{K}_i$ 関係

$\forall j \in 10\ [\ \langle \mathcal{M}, h_j \rangle \models \phi\ ]$ が成り立っているとする．この時，例えば，h_0 と $\mathcal{K}_i$ 関係にある h_1, h_2, h_3 で ϕ が成り立つことから，$\langle \mathcal{M}, h_0 \rangle \models \mathrm{K}_1\phi$ が成り立つ．

定義 16 (打ち切り履歴上の意味論) 打ち切り履歴に対する SSL 式の意味を以下のように定義する．

$$
\begin{aligned}
\widetilde{V}[\![p]\!]\tilde{\eta} &= \{\tilde{h} \in \widetilde{H}(T) \mid p \in \pi(\widetilde{last}(\tilde{h}))\} \\
\widetilde{V}[\![X]\!]\tilde{\eta} &= \tilde{\eta}(X) \\
\widetilde{V}[\![\neg\phi]\!]\tilde{\eta} &= \widetilde{H}(T) - \widetilde{V}[\![\phi]\!]\tilde{\eta} \\
\widetilde{V}[\![\phi \wedge \psi]\!]\tilde{\eta} &= \widetilde{V}[\![\phi]\!]\tilde{\eta} \cap \widetilde{V}[\![\psi]\!]\tilde{\eta} \\
\widetilde{V}[\![\langle\!\langle a \rangle\!\rangle \phi]\!]\tilde{\eta} &= \{\tilde{h} \in \widetilde{H}(T) \mid \exists s \in S(T) \\
&\qquad \widetilde{last}(\tilde{h}) \xrightarrow{a} s \wedge \\
&\qquad \tilde{h} \oplus (\widetilde{last}(\tilde{h}), s), \langle s \rangle) \in \widetilde{V}[\![\phi]\!]\tilde{\eta}\} \\
\widetilde{V}[\![\exists x.\phi]\!]\tilde{\eta} &= \bigcup_{\alpha \in A(T)} \widetilde{V}[\![\phi[\alpha/x]]\!]\tilde{\eta} \\
\widetilde{V}[\![\mu X.\phi]\!]\tilde{\eta} &= \mathrm{fix}_l(f) = \bigcup_{n \in \omega} \tilde{f}^n(\emptyset) \\
&\quad \tilde{f} = \lambda \widetilde{H} \in \wp(\widetilde{H}(T)).\widetilde{V}[\![\phi]\!]\tilde{\eta}[\widetilde{H}/X] \\
\widetilde{V}[\![\mathrm{K}_i\phi]\!]\tilde{\eta} &= \{\tilde{h} \in \widetilde{H}(T) \mid \forall \tilde{h'} \in \widetilde{H}(T), \\
&\qquad \tilde{h} \widetilde{\mathcal{K}_i} \tilde{h'} \Rightarrow \tilde{h'} \in \widetilde{V}[\![\phi]\!]\tilde{\eta}\} \\
\widetilde{V}[\![\mathrm{E}_g^n\phi]\!]\tilde{\eta} &= \{\tilde{h} \in \widetilde{H}(T) \mid \forall \tilde{h'} \in \widetilde{H}(T), \\
&\qquad \tilde{h} \widetilde{\mathcal{K}}_g^{[n]} \tilde{h'} \Rightarrow \tilde{h'} \in \widetilde{V}[\![\phi]\!]\tilde{\eta}\}
\end{aligned}
$$

ここで $\tilde{\eta} = tr \circ \eta$ である．

自由変数を持たない SSL 式に対する充足関係を定義する。

$$
\begin{aligned}
\langle \mathcal{M}, \tilde{h} \rangle \tilde{\models} \phi &\Leftrightarrow \tilde{h} \in \widetilde{V}[\![\phi]\!] \\
\mathcal{M} \tilde{\models} \phi &\Leftrightarrow \forall s \in S^0(T)\ [\ tr(\langle s \rangle) \in \widetilde{V}[\![\phi]\!]\ ]
\end{aligned}
$$

補題 5 任意の履歴 h_1, h_2 に対して $h_1 \mathcal{K}_i h_2 \Leftrightarrow tr(h_1) \widetilde{\mathcal{K}_i} tr(h_2)$ が成り立つ．

証明 $h_1(i)$ および $h_2(i)$ の長さによって場合分けをする．

Case 1. $\sharp(h_1(i)) \geq l(i) \wedge \sharp(h_2(i)) \geq l(i)$ の場合．任意の履歴 $h \in H(T)$ に対して $tr(h)$ は，h のエージェント i から見た観測可能動作列の最後の $l(i)$ 個の動作を正確に保存する．一方，任意の $h_1, h_2 \in H(T)$ が記憶長 $l(i)$ の判別不能関係となるためには，$\mathcal{K}_i$ の定義よりエージェント i から見た観測可能動作は h_1 および h_2 中の最後の $l(i)$ 個が一致しなければならない．故に $tr(h_1) \widetilde{\mathcal{K}_i} tr(h_2) \Rightarrow h_1 \mathcal{K}_i h_2$ である．

逆に，$h_1 \mathcal{K}_i h_2$ ならば，$\mathcal{K}_i$ の定義より h_1 および h_2 中の観測可能動作列の最後の $l(i)$ 個は一致する．一方，$tr(h_1), tr(h_2)$ においても，エージェント i から見た観測可能動作の最後の $l(i)$ は正確に保存されている．従って $tr(h_1)$ および $tr(h_2)$ の観測可能動作の最後の 1 個は一致する．これは $tr(h_1) \widetilde{\mathcal{K}_i} tr(h_2)$ を意味する．すなわち $h_1 \mathcal{K}_i h_2 \Rightarrow tr(h_1) \widetilde{\mathcal{K}_i} tr(h_2)$ である．

Case 2. $\sharp(h_1(i)) < l(i) \wedge \sharp(h_2(i)) < l(i)$ の場合．任意の履歴 $h \in H(T)$ に対して $tr(h)$ は h のエージェント i から見た観測可能動作を全て正確に保存する．したがって先の議論と同様の結果を得る．

Case 3. $\sharp(h_1(i)) < l(i) \wedge \sharp(h_2(i)) \geq l(i)$ の場合．$\sharp(tr(h_1)(i)) < l$ かつ $\sharp((tr(h_2)(i)) \geq l$ より自明．

Case 4. $\sharp(h_1(i)) \geq l(i) \wedge \sharp(h_2(i)) < l(i)$ の場合．Case 3. と同様．

以上より $h_1 \mathcal{K}_i h_2 \Leftrightarrow tr(h_1) \widetilde{\mathcal{K}_i} tr(h_2)$ が成り立つ．■

4.2 打ち切り履歴上での決定可能性

補題 6 任意の SSL 式 ϕ に対する $\widetilde{V}[\![\phi]\!]$ は計算可能である．

証明 式の構造に関する帰納法を用いて証明する．

Induction Base: $\phi \in \Phi$ の場合． $\widetilde{V}[\![\phi]\!]$ は，$\pi(\widetilde{last}(\tilde{h}), \phi) = true$ か否かによって決まるが，$\widetilde{H}(T)$ は有限なので明らかに計算可能である．

Induction Step: $\phi = \neg\psi$, $\phi = (\phi_1 \wedge \phi_2)$, $\phi = \exists x.\psi$ の場合は明らか．

Case 1. $\phi = \langle a \rangle \psi$ の場合. 定義は下式であった.

$$\widetilde{V}[\![\langle a \rangle \psi]\!] = \{\tilde{h} \in \widetilde{H}(T) \mid \exists s' \in S(T), \widetilde{last}(\tilde{h}) \xrightarrow{a} s' \wedge \tilde{h} \widetilde{\oplus} (\langle \widetilde{last}(\tilde{h}), s' \rangle, \langle s' \rangle) \in \widetilde{V}[\![\phi]\!]\tilde{\eta}\}$$

$S(T), \widetilde{H}(T)$ は有限集合なので帰納法の仮定より計算可能である.

Case 2. $\phi = \mathrm{K}_i \psi$ の場合. 定義式の右辺に出現する $\tilde{h}, \tilde{h}'$ は $\widetilde{H}(T)$ が有限集合であることから数え上げ可能であり, 帰納法の仮定より $\widetilde{V}[\![\phi]\!]$ は計算可能となる.

Case 3. $\phi = \mathrm{E}_g^n$ の場合. $\widetilde{\mathcal{K}}_i$ ではなく, $\widetilde{\mathcal{K}}_g{}^{[n]}$ について議論を進めることにより, K_i の場合と同様の結果を得る.

Case 4. $\phi = \mu X.\psi$ の場合. ψ に対して定義される f の単調性と $\widetilde{H}(T)$ が有限であることより, $\bigcup_{\xi \in \omega} f^{\xi}(\emptyset)$ は有限ステップで飽和する. この事実と帰納法の仮定より $\widetilde{V}[\![\mu X.\psi]\!]$ は計算可能である.

以上より補題が成立する. ∎

系 1 打ち切り履歴上の SSL 式の充足性は決定可能である.

補題 7 打ち切りは SSL 式の充足性を保存する.

$$\forall \phi \in \mathcal{L}_{SSL}, \eta \in VAR \to \wp(H(T)) \quad [\, tr[V[\![\phi]\!]\eta] = \widetilde{V}[\![\phi]\!]\tilde{\eta} \,]$$

証明は付録 B にまわす.

定理 1 SSL 式は有限記憶を持つ有限状態遷移システム上でその充足性が決定可能である.

証明 補題 6, 7. より明らかである. ∎

4.3 [5] での意味付けとの同値性

本稿では $\langle . \rangle^*, C_g$ を構文糖衣として定義した. これは [5] で様相演算子として与えた定義とは異なっている. そこで, 両者の定義が同値であることを以下に示す.

以前与えた定義は以下のものである.

$$\langle \mathcal{M}, h \rangle \models_{old} \langle . \rangle^* \phi \Leftrightarrow \exists h' \in H(T; last(h)) \; [\, h \oplus h' \models \phi \,]$$

新しい定義では, 以下の性質が成り立っている.

$$\forall a \in A(T), s \in S(T) \quad [h \oplus (\langle last(h), a \rangle, \langle s \rangle) \in V[\![\langle . \rangle^* \phi]\!] \Rightarrow h \in V[\![\langle . \rangle^* \phi]\!]]$$

従って, 以下の式が成立する.

$$\begin{aligned} &\langle \mathcal{M}, h \rangle \models_{old} \langle . \rangle^* \phi \\ &\Leftrightarrow \exists h' \in H(T; last(h)) \; [\, h \oplus h' \models \phi \,] \\ &\Leftrightarrow \exists h' \in H(T; last(h)) \; [\, h \oplus h' \in V[\![\phi]\!] \,] \\ &\Rightarrow \exists h' \in H(T; last(h)) \; [\, h \oplus h' \in V[\![\langle . \rangle^* \phi]\!] \,] \\ &\Rightarrow h \in V[\![\langle . \rangle^* \phi]\!] \end{aligned}$$

逆に, $h \in V[\![\langle . \rangle^* \phi]\!]$ ならば, $h \in f^n(\emptyset)$ となる最小の n が存在する. これは

$$\exists h' \in H(T; last(h)) \; [\, \sharp(h') = n \wedge h \oplus h' \in V[\![\phi]\!] \,]$$

であることを意味する. 従って, 新旧の定義は等しい.

次に C_g である. 古い定義は以下のものであった。

$$\langle \mathcal{M}, h \rangle \models_{old} \mathrm{C}_g \phi \Leftrightarrow \forall h' \in H(T) \; [\, h' \mathcal{K}_g^{[*]} h \Rightarrow \langle \mathcal{M}, h' \rangle \models \phi \,]$$

新しい定義では下式が成立する.

$$\begin{aligned} V[\![\mathrm{C}_g \phi]\!] &= V[\![\neg \nu X.(\neg \phi[\neg X/X])]\!] \\ &= H(T) \setminus \bigcup_{\xi \in \omega} f^{\xi}(\emptyset) \\ &= \bigcap_{\xi \in \omega} H(T) \setminus f^{\xi}(\emptyset) \end{aligned}$$

ここで f は以下のように定義される.

$$f = \lambda H \in \wp(H(T)).(\neg(\mathrm{K}_g^1 \psi \wedge \mathrm{K}_g^1(\neg X)))$$

帰納法を用いて下式を証明する.

$$\forall \xi \in \omega \; [\, \{h \mid h \in V[\![\mathrm{K}_g^{\xi} \phi]\!]\} = H(T) \setminus f^{\xi}(\emptyset) \,]$$

Induction Base $\xi = 1$ の場合.

$$\begin{aligned} &H(T) \setminus f(\emptyset) \\ &= H(T) - \lambda H.(\neg(K_g^1 \psi \wedge K_g^1(\neg X)))(\emptyset) \\ &= V[\![K_g^1 \psi \wedge K_g^1 true]\!] \\ &= V[\![K_g^1 \psi]\!] \end{aligned}$$

Induction Step

$$\begin{aligned} &H(T) \setminus f^{\xi+1}(\emptyset) \\ &= H(T) \setminus \lambda H.(\neg(K_g^1 \psi \wedge K_g^1(\neg X)))(f^{\xi}(\emptyset)) \\ &= H(T) \setminus \lambda H.(\neg(K_g^1 \psi \wedge K_g^1(\neg X)))(\neg K_g^{\xi} \phi) \\ &= V[\![\neg(K_g^1 \psi \wedge K_g^1(K_g^{\xi} \phi))]\!] \\ &= V[\![K_g^1 \psi \wedge K_g^{\xi+1} \phi]\!] \\ &= V[\![K_g^{\xi+1} \phi]\!] \end{aligned}$$

これより両者の定義が等価であることは容易に示せる.

5 SSL による通信サービスの検証・分類

model checking とは SSL 構造上である式が成り立つかどうかを検証することをいう. すなわち, 抽象サービス仕様 ϕ に対し, $\mathcal{M} \models \phi$ が成立するならば, SSL 構造 $\mathcal{M}$ はその仕様 ϕ の一つの実現 (モデル) であり, model checking は $\mathcal{M}$ が要求 ϕ を満足するかどうかの検証となっている. ここで, **抽象サービス仕様**とは, SSL 式のうち具体的な動作名を含まないものとする. これは, 通信サービスの利用者にはサービスを構成するエージェントの動作名を知りようがないことに由来する制限である.

適当な抽象サービス仕様を定め, model checking によって SSL 構造の集合を分割することにより,

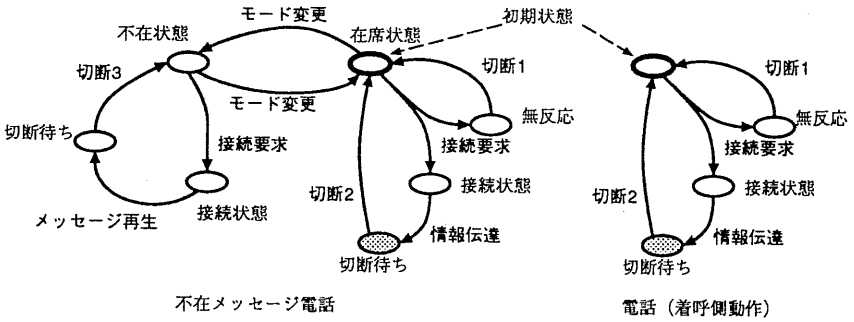

図 2: 不在メッセージ電話の状態遷移図

▒▒は着呼側 r が情報 info を知っていることを意味する原子命題 has(r,info) がその状態で成り立っていることを示す.

$$\exists x_1.\exists x_2.\nu X.([x_1][.]^*X \wedge [x_2]\nu Y.([x_1][.]^*Y \wedge [x_2]X)) \tag{2}$$

$$\exists x.(\langle . \rangle^* \langle x \rangle true \wedge [.]^*[x]\mathrm{C}_{\{s,r\}}\mathrm{has}(r,\text{info})) \tag{3}$$

SSL 構造の分類が可能となる. 通信サービスの実現に相当する遷移システム T を決めるとそれに応じて $(\mathcal{K}_i)_{i\in I}$ が具体的に決まるので, $\mathcal{M} = \langle T, (\mathcal{K}_i)_{i\in I}\rangle$ が一意に決定される. すなわち, model checking による SSL 構造の分類は遷移システム（通信サービス）の分類となる.

以下に抽象サービス仕様の例を示す. ここで, $\mathrm{has}(r,\text{info}) \in \Phi$ は受け手 r が情報 info を持っていることを表す原子式とする.

$[.]^*\langle . \rangle^*\mathrm{has}(r,\text{info})$
どのような動作列を実行しても, 必ずいつかは受け手 r は情報 info を持っている (知っている).

$\exists x.(\langle . \rangle^* \langle x \rangle true \wedge [.]^*[x]\mathrm{C}_{\{s,r\}}\mathrm{has}(r,\text{info}))$
ある動作 x は実行可能であり, 実行後には情報 info を受け手が知っていることがいつでも送り手 s と受け手 r との間の共通知識となっている.

SSL の model checking を機械的に行なうため, 有限状態遷移システムを対象とした model checker を計算機上に実現した. これは Common Lisp で記述した 700 行程度のプログラムである.

これを用いた通信サービスの仕様検証例として不在メッセージ電話を考える. この不在メッセージ電話は掛かってきた電話を受け取るべき人間がいない時に, 代わりにメッセージを流すサービスである. この仕様は以下のように考えられる.

- 在席時には, 不在状態に変更されるまで通常の電話サービスを実行する
- 不在時に, 在席状態に変更されるまで着呼した場合にはメッセージを流す
- 特定の操作（ボタンを押す）が行なわれるまで, 在席 / 不在状態は変更されない.

この仕様は SSL 式では図-2(2) 式のように記述できる. ここで各エージェントの記憶長は 1 とした.

また, 図-2(3) 式が電話および不在メッセージ電話において成立することにより, この不在メッセージ電話は通常の電話サービスの拡張であることがわかる.

6 まとめ

本稿では様相不動点論理 SSL を提案し, これによりユーザ要求の記述や検証, 分類ができることを示した. また, SSL が有限記憶の有限状態遷移システム上で充足性の決定が可能であることを証明した.

今後は実際のサービスの分類を行ない, SSL の有効性を確かめていく予定である. 計算機上に実現した model checker に対する計算量の評価は今後の課題である. また, それに基づく効率化も必要であろう.

本稿では SSL の言語および意味論を提示した. しかし, 厳密な意味で SSL を論理と呼ぶには, この言語に基づく演繹体系を定めることが必要である. そこで, それを定め, その体系の中で証明される含意関係を用いて抽象サービス仕様の階層化を行なうことを考えている.

参考文献

[1] Milner, R. : *Communication and Concurrency*, Prentice-Hall International, 1985.

[2] Halpern, J. Y. : "Knowledge and Common Knowledge in a Distributed Environment",

Journal of the ACM, Vol.37, No.3, July 1990, pp.549-587.

[3] 内平直志, "様相論理による並行プログラムの積重ね式検証法", 信学会論文誌, Vol.J75-D-I, No.2(1992年2月), pp.76-87.

[4] Stirling, C. : "Modal Logics for Communicating Systems", *Theoretical Computer Science* 49(1987), pp.311-347.

[5] 楢崎, 堀田 : "通信サービスのための知識と動作に基づく様相論理SSL", 信学技報, COMP92-9(1992), pp.69-78.

[6] Kozen, D.: "Results on the propositional μ-calculus", *Theoretical Computer Science* 27(1983), pp.333-354.

[7] Tarski, A. : "A lattice-theoretical fixpoint theorem and its applications", *Pacific J. Math.* 55 (1955), pp.285-309.

[8] Davey, B.A. and Priestley, H.A. : *Introduction to Lattices and Order*, Chapter 4. Fixpoint Theorem, Cambridge mathematical textbook, 1990.

A 補題1の証明

証明 S_0 を f の任意の不動点とすると

$$\forall \xi < \kappa[\ f^{\xi}(\emptyset) \subseteq S_0\ ] \tag{4}$$

であること, 及び

$$\forall \xi < \kappa[\ f^{\xi}(\emptyset) \subseteq f(f^{\xi}(\emptyset))\ ] \tag{5}$$

であることは, $\xi < \kappa$ についての帰納法により容易に示される. ある $\xi < \kappa$ について, $f^{\xi}(\emptyset) = f(f^{\xi}(\emptyset))$ であることを背理法で示す.

$$\forall \xi < \kappa[\ f^{\xi}(\emptyset) \neq f(f^{\xi}(\emptyset))\ ] \tag{6}$$

と仮定する. このとき (5) により, $\forall \xi < \kappa[\ f^{\xi}(\emptyset) \subset f(f^{\xi}(\emptyset))\ ]$ となる. 選択公理により, ある関数 $\chi : (\wp(S)\backslash\{\emptyset\}) \to S$ で, $\forall X \in (\wp(S)\backslash\{\emptyset\})[\ \chi(X) \in X\ ]$ となるものがある. このような χ を一つ固定する. このとき関数 $(\lambda \xi \in \kappa : \chi(f^{\xi+1}(\emptyset) \setminus f^{\xi}(\emptyset)))$ は κ から S への単射であるので, $\sharp(\kappa) \leq \sharp(S)$ となるが, これは κ の決め方と矛盾する. 従って, (6) は誤りであり, ある $\xi < \kappa$ について, $f^{\xi}(\emptyset) = f(f^{\xi}(\emptyset))$ となる. これと (4) からこの ξ について (1) が成り立つことが導かれる. ∎

B 補題7の証明

証明 式の構造に関する帰納法を用いて証明する.

Induction Base: $\phi \in \Phi$ の場合. 下式が成立することより明らか.

$$\forall h \in H(T)\ [\ \pi(last(h), \phi) = \pi(\widetilde{last}(\widetilde{h}), \phi)\ ]$$

Induction Step: $\phi = \neg\psi$, $\phi = (\phi_1 \wedge \phi_2)$, $\phi = \exists x.\psi$, $\phi = X$ の場合は明らか.

Case 1. $\phi = \langle\alpha\rangle\psi$ の場合. $\langle\alpha\rangle$ の定義と帰納法の仮定より下式が成り立つ.

$$\begin{aligned}&\forall s, s' \in S(T), \forall h \in H(T)\\ &\quad [\ \ s \xrightarrow{a} s' \wedge h \in V[\![\psi]\!]\\ &\qquad \Leftrightarrow \forall \widetilde{h} \in \widetilde{H}(T)\ [\ s \xrightarrow{a} s' \wedge \widetilde{h} \in \widetilde{V}[\![\psi]\!]\ ]]\end{aligned}$$

従って $tr[V[\![\langle\alpha\rangle\psi]\!]\eta] = \widetilde{V}[\![\langle\alpha\rangle\psi]\!]\widetilde{\eta}$ となり成立する.

Case 2. $\phi = \mathrm{K}_i\psi$ の場合.

$$\begin{aligned}&tr[V[\![\mathrm{K}_i\phi]\!]\eta]\\ &= tr[\{h \in H(T) \mid h' \in H(T),\\ &\qquad hK_ih' \Rightarrow h' \in V[\![\phi]\!]\eta\}]\\ &= \{\widetilde{h} \in \widetilde{H}(T) \mid \widetilde{h}' \in \widetilde{H}(T),\\ &\qquad \widetilde{h}\widetilde{K_i}\widetilde{h}' \Rightarrow \widetilde{h}' \in \widetilde{V}[\![\phi]\!]\widetilde{\eta}\}\\ &= \widetilde{V}[\![\mathrm{K}_i\phi]\!]\widetilde{\eta}\end{aligned}$$

Case 3. $\phi = \mathrm{E}_g^n$ の場合. K_i の場合と同様.

Case 5. $\phi = \mu X.\psi$ の場合. 下式を証明すればよい.

$$tr[\bigcup_{\xi \in Ord}[f^{\xi}(\emptyset)]] = \bigcup_{\xi \in Ord}[\widetilde{f}^{\xi}(\emptyset)]$$

ここで, 打ち切りは和集合の中に入れることができるので任意の順序数 ξ について下式が成立することを示せばよい.

$$tr[f^{\xi}(\emptyset)] = \widetilde{f}^{\xi}(\emptyset) \tag{7}$$

ξ に関する超限帰納法を用いて上式の証明を行なう.

Induction Base. $\xi = 0$ の場合. 明らか.

Induction Step: Case 1. ξ が孤立順序数の場合. 任意の孤立順序数 ξ に対して, それよりも小さな順序数 ξ' で (7) 式が成立しているとする. $\xi = \xi' + 1$ とする.

$$\begin{aligned}&tr[f^{\xi}(\emptyset)] = tr[f(f^{\xi'}(\emptyset))]\\ &\quad = tr[V[\![\phi]\!](\eta[f^{\xi'}(\emptyset)/X])]\\ &\quad = \widetilde{V}[\![\phi]\!](tr \circ (\eta[f^{\xi'}(\emptyset)/X]))\\ &\quad = \widetilde{V}[\![\phi]\!](\widetilde{\eta}[tr[f^{\xi'}(\emptyset)]/X])\\ &\quad = \widetilde{V}[\![\phi]\!](\widetilde{\eta}[\widetilde{f}^{\xi'}(\emptyset)/X]) \qquad \text{(帰納法の仮定より)}\\ &\quad = \widetilde{f}^{\xi'+1}(\emptyset) = \widetilde{f}^{\xi}(\emptyset)\end{aligned}$$

Case 2. ξ が極限順序数の場合.

$$\begin{aligned}tr[f^{\xi}(\emptyset)] &= tr[\bigcup_{\xi' \in \xi}[f^{\xi'}(\emptyset)]]\\ &= \bigcup_{\xi' \in \xi}[\widetilde{f}^{\xi'}(\emptyset)] \qquad \text{(帰納法の仮定)}\\ &= \widetilde{f}^{\xi}(\emptyset)\end{aligned}$$

以上より (7) 式が成立する. 従って補題が証明された. ∎