4K−9

通信サービス記述のための知識と動作に基づく様相論理SSL

楢崎修二，堀田英一
NTTソフトウェア研究所

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，サービスが多様化した現在，どのようなサービスがユーザの要求に答えられるのか，何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る．

そこで，ユーザの要求（抽象サービス仕様）は何か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，並行プロセスの知識所有状態を記述する様相論理**SSL**(Service Specification Logic)を提案する．これにより，通信サービスに対する仕様をユーザの知識所有状態の変更過程として捉えることができ，サービス仕様の形式的記述・分類・model checkingなどが可能になることを示す．

2　知識と動作に注目した様相論理:SSL

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]にlogics of common knowledge(LCK)[2]を付加した様相論理体系である．

2.1　構文

Φを原子式の集合，Aをアクションの集合，Iをエージェントの集合とする．(Φ, 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．

$$\phi ::= p \mid \neg\phi \mid (\phi_1\wedge\phi_2) \mid \exists x.\phi \mid \langle\alpha\rangle\phi \mid \langle.\rangle^*\phi \mid \mathrm{K}_i\phi \mid \mathrm{E}_g^n\phi \mid \mathrm{C}_g\phi$$

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($\wp(S)$は集合Sの冪集合を表す)．$\langle\ \rangle$, $\langle.\rangle^*$はプロセス論理の様相オペレータであり，K, E^n, Cは LCKのそれである．

記述の簡易化のため，$\vee$, $\rightarrow$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．

2.2　意味論

各エージェントに対応する状態遷移システムを並行合成した状態遷移システムを下式で表す．

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

ここで，$S\subseteq\Pi_{i\in I}S_i$は各エージェントの状態（局所状態）$S_i$のタプル（大域状態）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，$\pi:S\times\Phi\rightarrow\{true,false\}$は各状態での原子式の値の割り当てである．

状態遷移システムTを定めると，システムの動作履歴をアクションと大域状態のタプルの列として表すことができる．そこで履歴hの集合を$H(T)\subseteq(A\times S)^*$で表す．

次に，SSLに対する(Kripke)構造$\mathcal{M}$を以下のように定め，SSL構造と呼ぶことにする．

$$\mathcal{M}=\langle T,(\mathcal{K}_i)_{i\in I}\rangle$$

ここで$\mathcal{K}_i\subseteq H(T)\times H(T)$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．

以上の準備の基で，各式の意味を以下のように定める．

$\langle\mathcal{M},h\rangle\models\phi \quad\Leftrightarrow \pi(\mathrm{stat}(\mathrm{lst}(h)),\phi)=true \quad \phi\in\Phi$の時
stat は遷移システムの大域状態を返す関数であり，lst は列中の最後の要素を返す関数である．

$\langle\mathcal{M},h\rangle\models\neg\phi \quad\Leftrightarrow \langle\mathcal{M},h\rangle\not\models\phi$

$\langle\mathcal{M},h\rangle\models(\phi\wedge\varphi)\Leftrightarrow\langle\mathcal{M},h\rangle\models\phi\ \wedge\ \langle\mathcal{M},h\rangle\models\varphi$

$\langle\mathcal{M},h\rangle\models\langle\alpha\rangle\phi$
$\Leftrightarrow \exists s\in S.[\mathrm{stat}(\mathrm{lst}(h))\xrightarrow{\alpha}s\ \wedge\ \langle\mathcal{M},h\cdot(\langle\alpha,s\rangle)\rangle\models\phi]$
'·'は列の結合関数とする．

$\langle\mathcal{M},h\rangle\models\exists x.\phi \quad\Leftrightarrow \exists\alpha\in A.[\langle\mathcal{M},h\rangle\models\phi[\alpha/x]]$

$\langle\mathcal{M},h\rangle\models\langle.\rangle^*\phi \quad\Leftrightarrow \exists h'\in H(T).[h\preceq_p h'\wedge\langle\mathcal{M},h'\rangle\models\phi]$
$\preceq_p=\{(h,h')\mid \mathrm{lgt}(h)\leq\mathrm{lgt}(h')\wedge h=h'\restriction\mathrm{lgt}(h)]\}$
$\mathrm{lgt}(s)$は列sの長さ．また$f\restriction D$は関数fの定義域をDに制限したものである．自然数はそれより小さいものの集合と同一視される．

$\langle\mathcal{M},h\rangle\models\mathrm{K}_i\phi \quad\Leftrightarrow \forall h'\in H(T).[h\mathcal{K}_ih'\rightarrow\langle\mathcal{M},h'\rangle\models\phi]$

$\langle\mathcal{M},h\rangle\models\mathrm{E}_g^1\phi \quad\Leftrightarrow \forall i\in g.[\langle\mathcal{M},h\rangle\models\mathrm{K}_i\phi]$

$\langle\mathcal{M},h\rangle\models\mathrm{E}_g^n\phi \quad\Leftrightarrow \mathrm{E}_g^1\mathrm{E}_g^{n-1}\phi \qquad n\geq 2$

$\langle\mathcal{M},h\rangle\models\mathrm{C}_g\phi \quad\Leftrightarrow \forall k\in\omega.[\langle\mathcal{M},h\rangle\models\mathrm{E}_g^k\phi]$

$\mathcal{M}\models\phi \quad\Leftrightarrow \forall s\in S^0.[\langle M,(\langle\iota,s\rangle)\rangle\models\phi]$
ιは初期状態に至る仮想的なアクションを表す．

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．直観的には，$\langle a\rangle\phi$はアクション$a$の後には$\phi$が成り立つ可能性があることを意味し，$\mathrm{K}_i\phi$はエージェント$i$が$\phi$を知っていることを，$\mathrm{C}_g\phi$は「グループ$g$は$\phi$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．

Modal Logic SSL Based on Knowledge and Action for Describing Communication Services
Shuji NARAZAKI, Eiichi HORITA
NTT Software Labs.

3 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，$\mathcal{M}$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式のうち具体的なアクション名を含まないものとする．

また，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，SSL構造の分類が可能となる．

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

$[.]^*\langle.\rangle^*\mathrm{has}(r, \mathrm{info})$

どのようなアクション列を実行しても，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)．

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

あるアクション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，有限の遷移システムを対象としたmodel checkerを計算機上に実現した．これを用いた通信サービスへの適用例を以下に示す．ここで$\mathcal{K}_i$を個々の遷移システムに対して以下のように定めることにする．これは各エージェントは観測可能なアクションに関して完全な記憶を持つことを意味する．

$$\mathcal{K}_i = \{(h_1, h_2) \mid \rho_i(h_1) = \rho_i(h_2)\}$$

$$\rho_i(h) = \mathrm{sqsh}((\langle \mathrm{act}(h(j)), \mathrm{stat}(h(j))(i)\rangle)_{j \in \mathrm{vis}(h,i)})$$

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，$\mathrm{sqsh}(f) = \langle f(i_0), f(i_1), \cdots, f(i_n)\rangle$である．$\mathrm{act}(t)$はタプル$t$の第一要素，$\mathrm{vis}(h,i) = \{j \in \mathrm{lgt}(h) \mid \mathrm{act}(h(j)) \in A_i \cup \{\iota\}\}$である．

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（通信システム）の分類となる．

POTS POTS[1]を実現する状態遷移システムTを，図1のように与える(ただし，受け手のみを示す)．この時，SSL構造は以下のような性質を持つ．

$[.]^*\langle.\rangle^*\mathrm{has}(r, \mathrm{info})$ 不成立

必ずしも情報は伝達されない(相手が不在・会話中)．

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

FAX POTSとの違いは，送信を行なっても受け手が受けとったかどうかの確認が出来ないことである(図2)．

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

受け手が情報を所有しても送り手はその事を知ることができない．

[1]通常の電話サービス

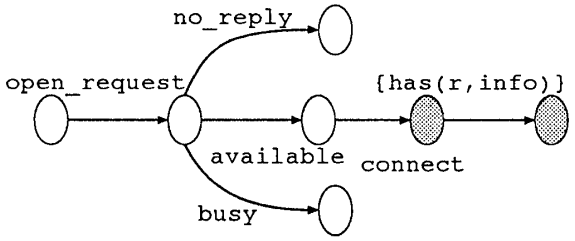

図 1: POTSの遷移図

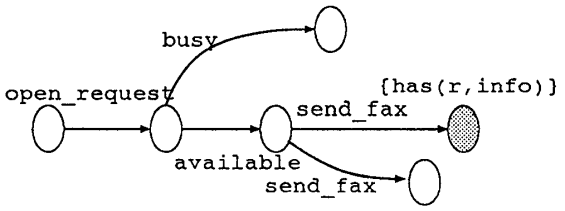

図 2: FAXの遷移図

到着通知付き FAX 先のFAXの欠点を除くために，POTSと組み合わせることを考える．すなわち，情報が正しく伝わった場合，受け手はPOTSにより返事を返すようにする．この時，

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

到着通知を行なうアクションがxに相当する．

となる．これより，POTSとFAXを組み合わせた到着通知付きFAXは共通知識を達成出来るという意味で，POTSと同じ範疇に入ることが分かる．

4 結論

本稿では様相論理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．

現在は例にあげた程度のサービスについての分類しか行なっていないため，例えばCLASS系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．しかし，現在のmodel checkerは対象遷移システムを履歴の集合が有限なものに限っている．実際には有限状態システムに対して，任意の$\phi \in \mathcal{L}_{SSL}$の真偽を決定することが可能である．そこで，この制約を取り除き対象範囲を広げることが必要と思われる．

また，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.