A-004

混合型時間アンビアント計算の CTL モデル検査

CTL Model Checking for Hybrid Timed Ambient Calculus

稲森 啓太 †　　**樋口 昌宏** †
Keita Inamori　　Masahiro Higuchi

1 はじめに

混合型時間アンビアント計算 (以下、HTAC とする)[1] とは、アンビアント計算 [2] を時間拡張したプロセス代数であり、物流システムの持つ動的な階層構造を簡潔に表現することができる。この HTAC によって物流システムを記述したプロセス式が所期の目的を満たしているかを確認するためには、プロセス式に対して CTL モデル検査を行う必要がある。しかし、CTL モデル検査で用いられる通常の様相論理だけでは、動的な階層構造の変化や時間的制約などの HTAC 特有の性質を表現することができない。そこで本研究では、これらの性質を表現するための時間アンビアント論理を提案し、HTAC 式に対して CTL モデル検査を行うプログラムを開発した。

2 混合型時間アンビアント計算 (HTAC)

2.1 構文規則

HTAC の構文規則は文献 [1] にて以下のように定義されている。

$P, Q ::=$	processes	$M,\ N ::=$	capabilities
$(\nu n)P$	restriction	x	variable
0	inactivity	n	name
$P \mid Q$	composition	$in\ M$	enter into M
$!P$	replication	$out\ M$	exit out of M
$M[P]$	ambient	$open\ M$	open M
$M.P$	capability action	$in(t')\ M$	enter into M within t' time unit
$(x).P$	input action		
$\langle M \rangle$	async output action	$out(t')\ M$	exit out of M within t' time unit
		$open(t')\ M$	open M within t' time unit
		$wait(t)$	wait t time unit
		ε	null
		$M.N$	path
$t ::=$	time	$t' ::=$	time with infinity
$1, 2, ...$	positive integer	t	time
		∞	infinity

HTAC では、アンビアント計算で用いられる通常のケーパビリティ $in, out, open$ に加えて、有効期限付きケーパビリティ $in(t'), out(t'), open(t')$、及び待機ケーパビリティ $wait(t)$ を持つ。

2.2 遷移規則

以下では、文献 [2] で示されている通常のケーパビリティの消費による遷移を「$\rightarrow$」で表し、$P \rightarrow Q$ なる Q を持たない式 P を安定な式、そうでない式を非安定な式と呼ぶ。また、有効期限付きケーパビリティによる遷移、及び時間経過による遷移は安定な式でのみ適用可能であり、それぞれ「$\xrightarrow{P}$」、「$\xrightarrow{T}$」で表す。これらの遷移は文献 [1] にて、以下の規則で定義されている。ここでは in についての遷移規則のみを示すが、$out, open$ についても同様の遷移規則を持つ。

$$n[in(t')m.P \mid Q] \mid m[R] \xrightarrow{P} m[n[P \mid Q] \mid R]$$
$$in\ M.P \xrightarrow{T} in\ M.P$$
$$in(\infty)m.P \xrightarrow{T} in(\infty)m.P$$
$$in(t)m.P \xrightarrow{T} in(t-1)m.P \quad (t \geq 2)$$
$$in(1)m.P \xrightarrow{T} 0$$
$$wait(t).P \xrightarrow{T} wait(t-1).P \quad (t \geq 2)$$
$$wait(1).P \xrightarrow{T} P$$
$$P \xrightarrow{P} Q \Rightarrow n[P] \xrightarrow{P} n[Q]$$
$$P \xrightarrow{P} Q \Rightarrow P \mid R \xrightarrow{P} Q \mid R$$
$$P \xrightarrow{T} P' \Rightarrow n[P] \xrightarrow{T} n[P']$$
$$P \xrightarrow{T} Q \Rightarrow P \mid R \xrightarrow{T} Q \mid R$$

また、「$\xrightarrow{P}$」と「$\xrightarrow{T}$」の和集合を「$\xrightarrow{PT}$」で表し、「$\rightarrow$」の反射推移的閉包を「$\xrightarrow{*}$」で表す。HTAC における安定な式 F からの遷移は

$$F = F_0 \xrightarrow{PT} F'_0 \xrightarrow{*} F_1 \xrightarrow{PT} F'_1 \xrightarrow{*} ... \xrightarrow{PT} F'_{n-1} \xrightarrow{*} F_n \xrightarrow{PT} ...$$

のようになる。ここで F' は非安定な式、F は安定な式である。

HTAC において、例えば $P \mid Q$ と $Q \mid P$ は同様に振る舞う。このような式は互いに構造合同であるといい、HTAC ではこれらをを同一視する。

3 HTAC による物流システムの記述

3.1 物流システム

物流システムとはモノの移動順序を表すものであり、例として「人がタクシーに乗って移動する」という物流システムを考える。この場合、「人がタクシーに乗る」というイベントの発生を確認した後、「タクシーが移動する」というイベントが可能となる。そのため、前者が発生すると、瞬時的にその情報をシステム全体に通知することで、後者が実行可能な状態に遷移させる必要がある。このように物流システムでは、物理的な動作が行われる度に、それに対する同期のための制御情報のやりとりを行うことが一般的であると考えられる。

3.2 HTAC 式の物流システムとしての妥当性

HTAC を用いて物流システムを記述する際には、人やタクシー、駅などの移動するモノや場所を表す物理アンビアント、及び同期のための制御情報のやりとりに用いる制御アンビアントの 2 種類のアンビアントを利用する。また、3.1 節で述べたように実際の物流システムでは、物理アンビアントの移動は離散的に発生するのに対し、制御アンビアントの一連の移動はそれが可能となった時に瞬時的に実行される必要がある。更に、1 つの物理アンビアントの動作後の制御アンビアントの一連の遷移は必ず終了する必要があり、制御アンビアントの移動順序の違いによる非決定性を含まないことが望ましい。HTAC 式 F から到達可能なすべての F' について以下の条件 (妥当性条件) が満たされるとき、F は物流システムとして妥当であるという。

† 近畿大学 大学院総合理工学研究科, Kindai University

F' が安定な式の場合
　　実行可能な遷移は物理アンビアント間の遷移のみである
F' が非安定な式の場合
(a) 実行可能な遷移は制御アンビアントに関する遷移のみである
(b) $F \to F'_1 \to F'_2 \to ... \to F'_n \to ...$ となる無限遷移列が存在しない (収束性)
(c) $F' \xrightarrow{*} F''$ なる安定な式 F'' は 1 つのみである (合流性)

4 CTL モデル検査

モデル検査とは、システムを表現したモデル (プロセス式を状態とする状態遷移グラフ) が、与えられた条件を表す様相論理式を満たすかどうかを検査することである。

4.1 時間アンビアント論理

HTAC における CTL モデル検査において、所期の目的を様相論理式として表現する際、通常の時相論理で用いられる様相演算子だけでは、HTAC 特有の動的な階層構造の変化や時間的制約を表現することができない。そこで、以下に示す時間アンビアント論理を導入する。

時間アンビアント論理は、通常の様相演算子に加えて以下の 4 つの演算子を持つ。

$\phi \mid \psi$	ϕを満たすプロセスとψを満たすプロセスの並列合成により構成されているプロセスである
$N[\phi]$	ϕを満たすプロセスを持つ N というアンビアントである (ただし、N は物理アンビアントに限る)
$\downarrow \phi$	その状態の階層構造のどこかでϕを満たすプロセスを持つ
$(n)\ \phi$	その経路上で n 単位時間以内にϕが成り立つ

これらを用いることで、「必ず貨物は目的地に輸送される」、「貨物が指定した時間内に必ず目的地に輸送される」などの性質を表現することができる。

物流システムと見なせる HTAC 式 F について、F が非安定な式であれば、$F \xrightarrow{*} F'$ なる安定な式 F' はただ 1 つ存在し、F と F' は共に物理アンビアント間の階層構造、及び経過時間は同じである。このため、時間アンビアント論理により記述された様相論理式に対してモデル検査を行う場合、安定な式のみ考慮すれば十分である。

4.2 可達性解析プログラムによるモデル生成

HTAC 式の可達性解析とは、与えられた HTAC 式からケーパビリティの消費、及び時間経過による遷移によって到達可能な安定な式をすべて列挙することである。

可達性解析プログラムはまず、安定な式 F において $F \xrightarrow{PT} F'$ なる F' を全て求める。その際、遷移前の状態、遷移方法等の各 F についての遷移情報 (ここでは A とする) を保持しておく。一般に F' は非安定な式となるため、各 F' について合流性、及び収束性を確認し、それらが満たされていれば、各 F' について 1 つの安定な式 F'' が得られる。ここで、これまでに列挙された式の中に、先ほど得た式 F'' と構造合同な式があるかどうかを確認する。もし F'' と構造合同な式 F_{old} が存在する場合は $F \xrightarrow{A} F_{old}$ という辺を、構造合同な式が存在しない場合は $F \xrightarrow{A} F''$ という辺を作成する。更に、同様の動作を新たな辺が作成できなくなるまで繰り返す。このように式の妥当性を確認しながら到達可能な式を列挙し、最終的に、列挙された式と遷移関係を表す辺からなる状態遷移グラフを出力する。

4.3 様相論理式に対する検査プログラム

検査プログラムでは、可達性解析によって導出された状態遷移グラフをもとに、初期状態からの経過時間を含めた経路木を構築し、与えられた様相倫理式の真偽を検査する。例えば、「全ての経路で必ず 10 単位時間以内に N が M の中に入る」ということを表す様相論理式「$All(10)(\downarrow M[N[True]])$」を検査する場合、経路木の全ての経路で、$\downarrow M[N[True]]$ を満たし、かつ経過時間が 10 単位時間以内の状態が存在するかどうかを確認する。

5 検査実験・考察

本研究で開発した CTL モデル検査プログラムを用いて様々な検査実験を行った。その際、規模の小さい単純な HTAC 式に対してモデル検査を行った場合でも、有効期限付きケーパビリティ、及び待機ケーパビリティの時間パラメータの値を増加させると、実行時間が長くなってしまった。例として、N が外部から t 単位時間以内に M の中に移動するように記述したプロセス式が、実際に式 $All(t)(\downarrow M[N[True]])$ を満たすかどうかを検査する際、時間パラメータ t の値を増加させた時の、出力されるモデルのノード数、プログラムの実行時間を表 1 に示す。

表 1　時間パラメータに対するノード数と実行時間

t の値	ノード数	実行時間 (秒)
1	6	1 秒以下
20	301	2 秒
100	5501	40 秒

表 1 より、t の値を増加させると、ノード数が増加し、実行時間も長くなってしまっていることがわかる。これは状態遷移グラフを生成する際に、ある式から 1 単位時間経過させる度に、それを新たなノードとして生み出しているからである。これに対し、経過時間を変数とした式と、変数間の関係を表す連立不等式をノードとする遷移グラフを生成することで、ノード数が大幅に削減されると考えられる。

6 おわりに

本稿では、新たに提案した時間アンビアント論理、及び CTL モデル検査プログラムを用いて混合型時間アンビアント計算によって記述された物流記述式が所期の目的を満たしているかを確認できることを示した。今後は変数と連立不等式を利用し、状態遷移グラフの簡約化とそれに伴う検査プログラムの修正を行う予定である。

謝辞　本研究は科研費 (25330095) の助成を受けたものである.

参考文献

[1] 樋口昌宏: 時間付き Ambient Calculus, 情報処理学会プログラミング研究会, (2013-01)
[2] Gardelli, L. and Gordon, A.D.: Mobile Ambients, Theoretical Computer Science, Vol.240, pp.177-213 (2000).