ソフトウェア基礎論　23－9
（1987. 12. 10）

効率的時間論理証明システムの構成

Construction of Efficient Theorem Proving System for Temporal Logic

米崎 直樹　　端山 毅
YONEZAKI Naoki　HAYAMA Takeshi

東京工業大学工学部情報工学科(Department of Computer Science, Tokyo Institute of Technology)

あらまし　本時間論理証明システムは、様相記号の統一化の概念を用いた一般的様相論理証明器を時間論理に適用したものである。基本的な証明手続きは、結合法に基づいている。様相論理の体系による違いは様相記号列の統一化規則にのみ反映される。この一般的様相論理証明器を線形時間に適用し、next-time(○)を加えて、時間論理に拡張した。本時間論理証明システムの特徴は、証明手続き全体が幾つかの部分手続きに分解されるため、部分手続き毎に効率化が可能であり、有効な戦略の追加による効率化が期待できることである。

Abstract　A new theorem proving system for propositional temporal logic is presented. This systemis based on the conection method in which unification of modal operator sequences is used. Only constraint of the unification refrects diference of various modal logic systems. Firstly, the unification constraint and general proof procedure are exprained. Then, we specialize the method for lineir time tempral logic by introdusing next time operator. The problem of deciding the satisfiability of the formulas for the logic is PSPACE-complete, however, it is possible to introduce stratrgies for the algorithm in order to get efficinecy for general cases. By formalizing the system in our frame work, it becomes possible to find out some heuristics in each prooving step.

1．はじめに

時間論理はプログラム言語やプロトコルの意味記述、あるいは論理プログラム言語そのものとして用いられている。特に並列動作の記述等時間的要素を含む動的な仕様の記述、及びその検証にも利用されることが分かっている。さらに、ハードウェアの仕様記述・検証等にも使われている。

これらの方法を実際的にするためには、時間論理の効率的証明システムが必須である。時間論理の定理証明については分解証明法によるもの[2][6]等も研究されているが、ここでの方法は、様相記号列の統一化[4]を結合法[1][3]に応用することにより、体系による違いを局所的に封じ込める一般的様相論理証明器[5]に基づいている。これを体系Ｓ４に適用し、next-time演算子(○)を追加して時間論理の定理証明を可能にしている。

以下の証明方法の特徴は、証明が段階的に進行し、証明手続きが複数の部分手続きに分解できるために、体系による違いが全体におよぼす影響が小さく、演算子の追加が容易であることと、各部分毎に効率化できることである。

以下では、まず時間論理証明器の元になる一般的様相論理証明器について述べ、これを時間論理に適用する。

2．諸定義

2.1.様相論理式

(1)リテラル（命題変数またはその否定）は様相論理式である。

(2)Ａ，Ｂが様相論理式であるとき、

$$A \wedge B,\ A \vee B,\ A \supset B,\ \Box A,\ \Diamond A$$

は様相論理式である。

2.2.構造

構造Ｓは、組＜Ｗ，Ｒ＞で表される。Ｗは可能世界（状態）の集合であり、ＲはＷにおける到達可能関係を与える二項関係である。

2.3.付値関数、モデル

Ｓにおける付値関数Ｖは、各命題変数ＰにＷの部分集合Ｖ(Ｐ)を割り当てる。組Ｍ＝＜Ｓ，Ｖ＞をモデルと呼

ぶ。

2.4.式の値

Mが与えられたとき、世界$w_i \in W$における式Aの値$D(A, w_i) \in \{t, f\}$は、∧, ∨, ⊃, ¬については、古典論理と同様に帰納的に定義される。様相記号については以下のように定義される。

(1)$D(\Box A, w_i) = t$であるのは、$w_i R w_j$なるすべての$w_j \in W$において、$D(A, w_j) = t$であるときのみである。

(2)$D(\Diamond A, w_i) = t$であるのは、$w_i R w_j$かつ$D(A, w_j) = t$なる$w_j \in W$が存在するときのみである。

2.5.恒真

Aがどんなモデルについても、いかなる世界$w_i \in W$においても$D(A, w_i) = t$であるとき、Aは恒真であるという。

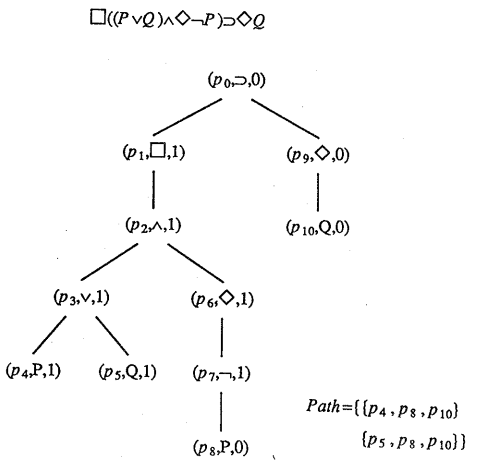


図2.1 論理式の木表現の例

2.6.論理式の木表現

式Aの木表現は対$<P_A, <_A>$で表される。P_AはA中のアルファベットの位置集合である。L(p)で位置$p \in P_A$のアルファベットを表す。P_A上の半順序関係$<_A$は式の構文に従って定義される。図2.1で各枝は順序関係を表し、各ノードは対(p,L(p))で表される。$P_1 <_A P_2$のとき、P_1はP_2を支配するという。

2.7.部分木

$A_{:p}$により、位置pを根とするAの部分式を表す。

2.8.極性

論理式Aの極性$n \in \{0,1\}$が与えられたとき、各位置pの極性N(p)は以下のように帰納的に定義される。

(1)$A_{:p} = A$のとき、N(p)=n

(2)$A_{:p} = \neg A_{:q}$のとき、$N(q) = (N(p)+1) \bmod 2$

(3)$A_{:p} = A_{:q} \wedge A_{:r}$(又は$A_{:q} \vee A_{:r}$)のとき、
$N(q) = N(r) = N(p)$

(4)$A_{:p} = A_{:q} \supset A_{:r}$のとき、
$N(q) = (N(p)+1) \bmod 2$
$N(r) = N(p)$

(5)$A_{:p} = \Box A_{:q}$(又は$\Diamond A_{:q}$)のとき、
$N(q) = N(p)$

2.9.結合

式Aにおける結合とは、以下の条件を満たす位置の対(p_1, p_2)である。

(1)$N(p_1) \neq N(p_2)$

(2)$L(p_1) = L(p_2) = P$　　但し、Pは命題変数。

2.10.π型様相記号とγ型様相記号

Π_A、Υ_Aは様相記号をラベルとして持ち、以下の条件を満たすP_Aの位置集合である。

$\Pi_A = \{p \in P_A \mid L(p) = \Diamond$かつ$N(p) = 1$
または$L(p) = \Box$かつ$N(p) = 0\}$

$\Upsilon_A = \{p \in P_A \mid L(p) = \Box$かつ$N(p) = 1$
または$L(p) = \Diamond$かつ$N(p) = 0\}$

Π_A中の位置のラベルである様相記号をπ型様相記号、Υ_A中の位置のラベルである様相記号をγ型様相記号という。様相記号をラベルとする位置の集合

$$M_A = \Pi_A \cup \Upsilon_A$$

である。

2.11.重複数

関数$m : \Upsilon_A \to N$（Nは自然数の集合）を様相記号の重複数という。式Aの重複数mに対するインデックス付きの木表現$<P_{A,m}, <_A'>$は以下のように定義される。

$P_{A,m} \subseteq P_A \times N^*$であり、$(p,l) \in P_{A,m}$であるのは、以下の条件を満たすときのみである。

(1)$p \in P_A$

(2)$\gamma_1 <_A \gamma_2 <_A \cdots <_A \gamma_n$を$<P_A, <_A>$においてpを支配するすべての$\Upsilon_A$の要素とすると、
$l \in \{j_1, \ldots, j_n \mid 1 \leq n \leq m(\gamma_i)\}$である。

順序$<_A' \subseteq P_{A,m} \times P_{A,m}$は以下のように定義される。
$(p,l) <_A' (p',l')$であるのは、$p <_A p'$かつ、
$l' = l \cdot l''$なる部分列l''が存在するときのみである。

なお、$L((p,l)) = L(p)$、$N((p,l)) = N(p)$とする。

2.12.前置関数pre

命題変数に作用する様相記号列を表す関数

$$pre : P_A \rightarrow M_A^*$$

を以下のように定義する。

$pre(p)=y_1 \cdots y_n$ となるのは、すべての$1 \leqq i \leqq n$について、$y_i <_A y_{i+1}$, $y_i \in M_A$, $y_n <_A p$ であり、かつ$z \neq y_i$, $z \in M_A$, $z <_A p$なるzが存在しないときである。

2.13.パス

論理式Aの根の極性を0としたとき、AのパスGは、以下のように帰納的に定義されるインデックス付き木の位置の集合の族である。なお便宜上、集合Sから要素eを除いた集合を$S \setminus e$で表す。

(1)pが式Aの根の位置であるとき、

$G = \{\{p\}\}$ はAのパスである。

(2)$p \in S$なる$S \in G$が存在し、L(p)が命題変数でない場合、

(2-1)$A_{:p} = \neg A_{:q}$のとき、

$G \setminus S \cup \{S \setminus p \cup \{q\}\}$ はパスである。

(2-2)$A_{:p} = A_{:q} \wedge A_{:r}$のとき、

(2-2-1)N(p)=1のとき、

$G \setminus S \cup \{S \setminus p \cup \{q,r\}\}$ はパスである。

(2-2-2)N(p)=0のとき、

$G \setminus S \cup \{S \setminus p \cup \{q\}\} \cup \{S \setminus p \cup \{r\}\}$ はパスである。

(2-3)$A_{:p} = A_{:q} \vee A_{:r}$(又は$A_{:q} \supset A_{:r}$)のとき、

(2-3-1)N(p)=0のとき、

$G \setminus S \cup \{S \setminus p \cup \{q,r\}\}$ はパスである。

(2-3-2)N(p)=1のとき、

$G \setminus S \cup \{S \setminus p \cup \{q\}\} \cup \{S \setminus p \cup \{r\}\}$ はパスである。

(2-4)$A_{:p} = \Box A_{:q}$ (又は$\Diamond A_{:q}$) のとき、

$G \setminus S \cup \{S \setminus p \cup \{q\}\}$ はパスである。

パス中に現れる位置のラベルがすべて命題変数であるとき、特にプリミティブパスという。

プリミティブパスを求めることは、古典論理において加法標準形を求めることと同値である。極性と併せて考えると、与式を与えられた極性にするための命題変数への真理値の割当、すなわち付値関数の満たすべき条件を表している。

根の極性を0としたのは、与式を偽と仮定したことに相当し、プリミティブパスによって得られる条件を満たす付値関数が、すべて矛盾を含むことが示せれば、与式を充足するモデルが存在しないことを示せる。

古典論理においては、パス中のすべての集合に結合が存在すれば、与式の否定は充足不能である。様相論理においては、各結合（ひとつの命題変数に対する2値の割当）が同一世界内でそれぞれ発生することを示さなければならない。

3．様相記号の統一化

3.1.様相論理の一般化

様相論理は到達可能関係Rに対する条件によって、以下のように分類される。

	体　系								
条　件	S5	S4	B	T	DT	DS4	KS4	KT(K)	KD45
Reflexive	○	○	○	○					
Transitive	○	○				○	○		○
Symmetric	○		○						
Euclidean	○								○
Serial	○	○	○	○	○	○			○

表3.1　様相論理の到達可能関係

ここで各条件は以下のことを表す。

Reflexive : $\forall w \in W$, wRw

Transitive : $\forall u,v,w \in W$, $uRv, vRw \rightarrow uRw$

Symmetric : $\forall u,v \in W$, $uRv \rightarrow vRu$

Euclidean : $\forall u,v,w \in W$, $uRv, uRw \rightarrow vRw$

Serial : $\forall u \in W, \exists v \in W$, uRv

各条件は以下のような公理スキーマとして表現される。

Condition on R	Axiom schema	Equivalent schema
Reflexive	$P \supset \Diamond P$	$P \equiv P \wedge \Diamond P$
		$\Box P \equiv P \wedge \Box P$
Transitive	$\Diamond\Diamond P \supset \Diamond P$	$\Diamond\Diamond P \equiv \Diamond P \wedge \Diamond\Diamond P$
		$\Box P \equiv \Box P \wedge \Box\Box P$
Symmetric	$P \supset \Box\Diamond P$	$P \equiv P \wedge \Box\Diamond P$
		$\Diamond\Box P \equiv P \wedge \Diamond\Box P$
Euclidean	$\Diamond P \supset \Box\Diamond P$	$\Diamond P \equiv \Diamond P \wedge \Box\Diamond P$
		$\Diamond\Box P \equiv \Diamond P \wedge \Diamond\Box P$
Serial	$\Diamond true$	$\Box P \supset \Diamond P$

表3.2　各条件の公理による表現

3.2.様相記号の統一化規則

結合(p_1, p_2)の前置関数$pre(p_1)$, $pre(p_2)$が以下の規則で統一化可能なとき、結合が同一世界内で発生するこ

とが証明される。

基本的にはγ型様相記号を変数と考え、π型様相記号をスコーレム定数と考え、Rに対応する代入規則に応じて、preの値の整合をとる。γ型様相記号はすべての世界で真あるいは偽であることを意味する。π型様相記号はある世界で真あるいは偽であることを意味し、そのある世界を定数値と見なしている。

以下では、γでγ型様相記号を、πでπ型様相記号を表し、δでγ型あるいはπ型様相記号を表す。また、x/yでxがyに代入可能であることを表す。φは空列を表す。

すべての様相論理体系に共通の代入規則として、π／γがいえる。これはγによって到達可能な世界のうち、πが到達可能な世界に注目することを表している。

また表3.2の等価なスキーマから各関係ごとの統一化規則を求めると以下のようになる。

	自己書換え規則	統一化規則
Reflexive	π／φ, φ／γ	φ／γ
Transitive	π／π⁺, γ⁺／γ	π⁺／γ
Symmetric	γπ／φ, φ／πγ	φ／πγ
Euclidean	γπ／π, γ／πγ	γ／πγ
Serial	π／γ	γ／γ
General		π／γ

表3.3 代入規則スキーマ

これを体系毎に組み合わせて整理すると以下のようになる。ただし、Ｓ５においては最後（命題変数の直前）の要素のみ考えればよい。

Ｓ５	δ／γ, φ／γ
Ｓ４	δ⁺／γ
Ｂ	δ／γ, φ／γ, φ／δγ
Ｔ	δ／γ, φ／γ
ＤＴ	δ／γ
ＤＳ４	δ⁺／γ
ＫＳ４	π⁺／γ
ＫＴ	π／γ
ＫＤ４５	δ／γ

表3.4 統一化における代入規則スキーマ

pre(p_1), pre(p_2)に現れるγ型様相記号に上記の規則に従った代入を行うことにより、一致が取れば統一化成功である。

４．様相論理証明器

4.1.分配

□（A∧B） ≡ □A∧□B

◇（A∨B） ≡ ◇A∨◇B

であるので、□は∧、◇は∨に関して分配しても同値である。

あるパスが、{....,{r_x,r_a,r_b},{r_y,r_a,r_b},....}のようになっていて、r_a,r_bはそれぞれ上式のＡ，Ｂの位置を表し、r_xとr_aおよびr_yとr_bがそれぞれ結合をなしているとする。上式の様相記号がγ型のときは、極性と∧，∨の関係からr_a,r_bは同一のパス要素に含まれる。

□（A∧B）においては、r_a,r_bはともに同一の□に支配される。この部分を□A∧□Bと書換えることにより、r_a,r_bは別々の□に支配されることになり、このγ型様相記号に関し、独立に代入を決定できるので統一化の可能性が増える。つまり、分配しない表現では統一化できなくとも、分配することにより統一化が成功することがある。

またπ型の場合、{....,{r_x,r_a},{r_x,r_b},....}のようになっていて、r_xとr_aおよびr_bがそれぞれ結合をなしているとする。r_a,r_bは異なるパス要素に含まれる。r_aとr_bがことなるπ型様相記号に支配されるときこれを同時にr_xを支配するγ型様相記号に代入することはできないが、上記の等価変換を右から左に用いれば、r_aとr_bを支配する様相記号が同一になり、ひとつの代入要素で(r_x,r_a),(r_x,r_b)の両方の結合を統一化できることがある。したがって、このようなπ型様相記号に対する変換も、統一化の可能性を増す。

4.2.重複

各γ型様相記号毎に任意の重複数を与えることにより、複数の等価な表現が得られる。

重複を木表現の操作で考えると、

□A ≡ □A∧□A

◇A ≡ ◇A∨◇A

のような書換えを行っていることになる。これは、上式の□Aにおいて、□に支配される命題変数の位置r_aの複製r_a'を作ることを意味する。そして、r_aとr_a'を支配するγ型様相記号を独立に用意するので、分配と同様に統一化の可能性が増える。

4.3.証明器

与えられた論理式に対し、そのパスを計算し、各パス要素毎に結合(p_1,p_2)を探し、その前置関数pre(p_1),pre(p_2)の統一化を各体系に従った代入規則のもとで実行する。この際、分配および重複を考慮した等価な論理式のうち、ひとつでも全パス要素中の結合の統一化に成功

するものがあれば、与式は証明されたことになる。

4.3.1.様相記号列の統一化

$\{\{r_{11}, r_{12}\} \cdots\cdots \{r_{n1}, r_{n2}\}\}$

ようにパス中に結合が存在するとき、様相記号列の統一化は、

$$\begin{aligned} &pre(r_{11})\,\theta = pre(r_{12})\,\theta \\ &\qquad\vdots \\ &pre(r_{n1})\,\theta = pre(r_{n2})\,\theta \end{aligned}$$

を満たす代入

$$\theta = \{t_1/\gamma_1, \cdots, t_n/\gamma_n\}$$

を求めることである。t_iは任意の様相記号列、γ_iはγ型様相記号である。ここで、上の等式ひとつを様相方程式と呼び、様相方程式の集合を連立様相方程式と呼ぶ。θの各要素は体系毎に定められた代入規則を満たさなければならない。また、θ中の各代入要素は以下の条件を満たさなければならない。

> $t_1/\gamma_x, t_2/\gamma_x \in \theta$のとき、$t_1, t_2$は統一化可能でなければならない。さらに、$t_1, t_2$を統一化する代入を$\theta'$とすることき、$\theta \cup \theta'$も本条件を満たさなければならない。

複数の様相記号の列をγ型様相記号に代入するのはtransitiveな体系のみであるが、このような体系では、$\gamma_i\, t/\gamma_i$のような自己代入を許す。様相記号列の統一化は、統一化の成否が問題であって、実際にpreにθを適用して代入の結果を求める必要はない。

5．時間論理証明器

これまでに述べた一般的様相論理証明器を時間論理に適用する。

基本的に時間論理は体系Ｓ４に基づき、到達可能関係RはReflexive,Transitive,Serialである。

5.1.next-time○の追加

5.1.1.時間論理式

2.1.の様相論理式の定義において、様相論理式を時間論理式と読み換え、下の規則を加える。

(3)Aが時間論理式であるとき、○Aは時間論理式である。

5.1.2.世界の構造

ここでの時間論理においては、世界の集合Wを状態の列$w_0, w_1, w_2, \cdots$ととらえ、線形時間のみを考える。ここで、W上に順序関係≪を定義する。

$w_i \ll w_j$となるのは、j=i+1のときのみである。

また、$w_i \ll w_j$ならば$w_i R w_j$であり、RはＳ４の到達可能関係である。

5.1.3.付値関数

2.4.の定義に以下の規則を加える。

(3)$D(\bigcirc A, w_i) = t$であるのは、$w_i \ll w_j$かつ$D(A, w_j) = t$であるときのみである。

5.1.4.極性

2.8.の定義に以下の規則を加える。

(6)$A_{:p} = \bigcirc A_{:q}$のとき、$N(q)=N(p)$である。

5.1.5.パス

2.14.の定義に以下の規則を加える。

(2-5)$A_{:p} = \bigcirc A_{:q}$のとき、$G \setminus S \cup \{S \setminus p \cup \{q\}\}$はパスである。

5.2.next-time○の統一化規則

$\Box A \equiv A \wedge \bigcirc A \wedge \cdots\cdots \wedge \bigcirc\cdots\bigcirc \Box A$

$\Diamond A \equiv A \vee \bigcirc A \vee \cdots\cdots \vee \bigcirc\cdots\bigcirc \Diamond A$

であるので、□および◇は○を任意個含む表現に書換えられる。

□または◇がγ型の場合には、展開された表現（上記右辺）の葉のノードは、すべて左辺のAが含まれていたパス要素中に含まれ、もとのAに関する結合は、展開後の複数のAに関する様相記号列のどれかひとつと統一できればよい。

□または◇がπ型の場合には、展開前にAが含まれていたパス要素は、展開後のノードをひとつずつ含む複数のパス要素になる。

以下のことを図示すると以下のようになる。

γ型のとき

$$\{\cdots, \{\cdots, r_a, \cdots\}, \cdots\}$$

$$\downarrow$$

$$\{\cdots, \{\cdots, r_{a1}, r_{a2}, \cdots, r_{an}, \cdots\}, \cdots\}$$

π型のとき

$$\{\cdots, \{\cdots, r_a, \cdots\}, \cdots\}$$

$$\downarrow$$

$$\{\cdots, \{\cdots, r_{a1}, \cdots\}, \{\cdots, r_{a2}, \cdots\}, \vdots, \{\cdots, r_{an}, \cdots\}, \cdots\}$$

ただし、$pre(r_a)$に含まれるγ型様相記号が、$r_{a1}, r_{a2}, \cdots, r_{an}$に展開されたものとする。

γ型の場合については自己書換え規則として、

$\gamma/\bigcirc,\ \gamma/\bigcirc\bigcirc,\ \cdots,\ \gamma/\bigcirc\cdots\bigcirc\gamma$

があるといえる。また時間の線形性より、

$$\neg\bigcirc A \equiv \bigcirc\neg A$$

であるから極性は○に影響せず、式中の○はすべて同一の定数と見なせる。

これをＳ４の規則と併せて代入規則を考えると、

$$\{\delta,\bigcirc\}^{*}/\gamma$$

が得られる。

5.3.π型様相記号の展開

時間論理においては、上記の統一化規則に基づく結合のpreの統一化を行うのみでなく、π型様相記号の展開について考えなければならない。γ型様相記号の展開については、統一化規則に含まれているので、明示的に考慮する必要はない。

様相記号の統一化は、π型様相記号に対して任意の展開を施した表現のうち、ひとつでも統一化に成功するものがあればよい。

5.4.Next-time○の移動

$$\bigcirc(A\wedge B)\equiv\bigcirc A\wedge\bigcirc B$$

$$\bigcirc(A\vee B)\equiv\bigcirc A\vee\bigcirc B$$

であるので、○の分配は常に許される。しかし、他の様相記号異なり、論理式中のすべての○を同一の定数と見なすので、単にこのような分配（もしくはその逆）を行っても、木表現は異なるがpreは変化しない。ところが、線形時間においては次のことがいえる。

$$\bigcirc\Box A\equiv\Box\bigcirc A$$

$$\bigcirc\Diamond A\equiv\Diamond\bigcirc A$$

したがって、○は□や◇と入れ換えて構わない。

○の分配によって、それが□や◇と出会い交換が起きるとpreが変化する。したがって、□、◇の分配、重複、展開と同様、○について上の分配と交換に伴う変形を考慮し、それら複数の論理式の中で、ひとつでも、パス中のすべての要素に統一化可能な結合を持つものが存在すれば、与式が証明されたことになる。

６．証明上の戦略

6.1.時間論理証明器

これまで述べた時間論理の定理証明の手順を構成するのは、

(1)パスの計算
(2)結合の選択
(3)様相記号の統一化
(4)分配
(5)重複
(6)□，◇の展開（π型のみ）
(7)○の移動
(8)帰納法（$P\wedge\Box(P\supset\bigcirc P)\supset\Box P$）の導入

である。このうち(1)と(2)は古典論理における結合法の証明手続きと本質的に同じものである。(3)が様相を処理するための手続きであり、(5)までが一般的な様相論理の証明手続きに必要な処理であり、(6),(7),(8)が時間論理特有の処理である。(4)から(7)はこれによって生ずる等価な論理式に(8)を加えて、そのうちひとつでも(1)から(3)に成功すれば、与式は証明されたことになる。ただし、そもそも各パス要素に結合が存在しない場合に、(4)から(7)の操作によって結合がすべてのパス要素に現れることはない。本来この様相記号の統一化による証明器の特徴は、等価な論理式の問題を様相記号の統一化規則で吸収するところにある。(4)から(8)の問題は統一化規則に対する制約や１レベル上の処理として扱われている。

6.2.戦略

上の手順では、「これらのひつとについて」あるいは「これらのすべてについて」何等かの処理をするとなっているので、しかるべき戦略を付加しなければ実現できない。「すべて試す」という基本的手続きから出発して、効率化するための戦略を以下に述べる。

6.2.1.パスの計算

パスの計算は決定的に処理できる。ただし、完全にパスを求める必要はなくこの点に効率化の余地がある。ひとつには、結合に関与しない位置は早い時期に除外することが挙げられる。

6.2.2.結合の選択

結合の選択では、ひとつのパス要素中に複数の結合が存在することがあり、各パス要素について採用する結合の組合せを非決定的に処理（様相記号の統一化を試みる）必要がある。また、同じ結合が複数のパス要素に含まれることがあり、いかに少数の結合ですべてのパス要素に結合を生じさせるかという基準で、結合を選択することも考えられる。

論理式中の出現が少ない命題変数は、結合を生じさせる位置が容易に決定できる。また、パス要素中で結合を生じさせる位置の組合せが一通りしかない場合、その組合せで様相記号の統一化が成功しなければならないので、その結合から先に統一化を試みるべきである。

6.2.3.様相記号の統一化

ある結合を支配するふたつの様相記号列を統一化する際、統一化を達成する代入は複数存在することがあり、ここでも非決定的に処理が進行する。

Ｓ４の代入規則はδ^{*}/γで示されるが、これは以下

のような場合も含む。x，yをγ型様相記号、a，b，cをπ型様相記号とするとき、

$$xa = by$$

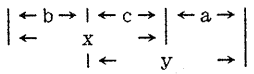
なる様相方程式を満足する代入は、

$$\{b/x,\ a/y\}$$

のように思われるが、連立様相方程式中の他の方程式による制約から、最終的には、

$$\{bc/x,\ ac/y\}$$

となることもある。これは下の図のようにxとyの領域に重なりがある場合と考えられる。



統一化手続きとしては、上のような場合に、bx'/xのように新しいγ型様相記号x'を用意し、様相方程式を$x'a = y$と書換えて、統一化を進める。この場合、$xa = by$からは、bx'/xと$x'a/y$なる代入要素を抽出するにとどめておく。これによって他の様相方程式の統一化によって、x'に対する代入が決まる。

6.2.4.分配

γ型様相記号については、

$$\Box(A \wedge B) \rightarrow \Box A \wedge \Box B$$
$$\Diamond(A \vee B) \rightarrow \Diamond A \vee \Diamond B$$

のように、ひとつの様相記号を複数の独立なγ型様相記号に分割することにより、統一化の可能性が増す。また、π型様相記号については、

$$\Box(A \wedge B) \leftarrow \Box A \wedge \Box B$$
$$\Diamond(A \vee B) \leftarrow \Diamond A \vee \Diamond B$$

のように、複数の様相記号をひとつの様相記号にまとめることにより、統一化の可能性が増す。また、このような変形により、重複や自己代入を行わずに済むことがある。

したがって、証明手続きとしては、あらかじめ可能な限り上のような変形を施しておくことが効率的である。

6.2.5.重複

重複が必要にはる場合を以下に整理する。

以下で∧は、極性1の∧、極性0の∨または⊃を表す。この記号の下のノードは同一パス要素に含まれる。∨は極性1の∨または⊃、極性0の∧を表す。この記号の下のノードは異なるパス要素に含まれる。また、木の葉の情報は（位置,ラベル,極性）で表す。

(1)図6.1のように、結合$(p_1,p_2),(p_1,p_3)$が存在し、p_1はγ型様相記号γ_1によって支配され、p_2,p_3はそれぞれ異なる様相記号列によって支配されているとき、γ_1を重複する。重複によって生成されるノードをp_1'とすると、重複前にp_1が含まれていたパス要素には、p_1,p_1'が共に含まれ、p_1,p_1'は異なるγ型様相記号γ,γ'に支配される。したがって、p_2,p_3を支配する様相記号は別々にγ,γ'と統一化される。

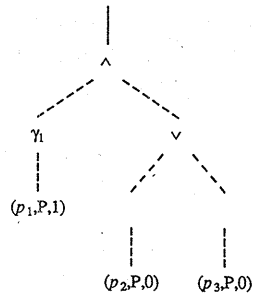


図6.1

(2)図6.2のように、結合$(p_1,p_3),(p_1,p_4)$が存在し、p_1はγ型様相記号γ_1によって支配され、p_3,p_4はそれぞれ異なる様相記号列によって支配されているが、(1)とことなり、γ_1の支配下で分岐がある。この場合p_2,p_3を含むパス要素と、p_2,p_4を含むパス要素が存在し、これらのパス要素中にはp_2を含む結合が存在しなければならない。また、p_2を含む結合の統一化を行う代入要素は、p_1とp_3もしくはp_4の統一化を行う代入要素とは矛盾してはならない。このとき、位置p_1のPを支配するγ_1を重複するかどうかは、p_2を含む結合の状況による。

すなわち、γ_1が重複されることにより、p_2も重複されるのでp_2の相手も重複する必要がある。したがってp_2の結合の相手p_5($L(p_5)=L(p_2), N(p_5)=(N(p_2)+1) \bmod 2$))が、γ型様相記号$\gamma_2$に支配される単独の葉ならば、$\gamma_1$を重複してよい。しかし、複数の異なるパス要素に含まれる葉がγ_2に支配される場合は、これらの葉はすべてp_2と結合をなし、様相記号の統一化が成功しなければならない。

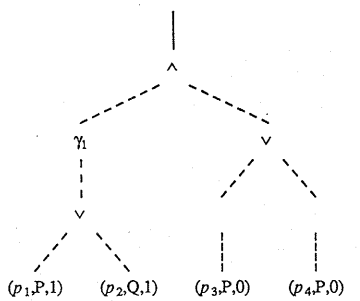


図6.2

これ以外の場合には、分配、自己代入の働きにより、重複せずとも統一化可能であるか、重複しても統一化できない。

6.2.6. π型様相記号の展開

π型様相記号の展開によって、変形前の論理式の木表現において、根から葉に至る経路に含まれる○の数以上に○を増やす必要はない。また展開を施すと下のようにパスの要素数が増加するので、重複が必要になることがある。ここではrを支配するπ型様相記号を展開したものとする。

$$\{\ldots,p_1,\ldots,p_n,\ldots,r,\ldots.\}$$
$$\downarrow$$
$$\{\ldots,p_1,\ldots,p_n,\ldots,r_1,\ldots\}$$
$$\vdots$$
$$\{\ldots,p_1,\ldots,p_n,\ldots,r_n,\ldots\}$$

展開を行うひとつの指針として以下のことがいえる。$r_1 \ldots r_n$は展開によって、新たに0,1,...,n-1個の○に支配されるようになるので、これらと一致する様相記号列に支配された位置$p_1,\ldots p_n$が、展開前のパス要素に含まれていなければならない。

6.2.7.○の移動

○の移動は、移動可能な範囲を明確にするため、まず前処理として可能な限り木表現の根に向けて移動しておき、統一化に失敗したならば、葉に向けて移動する。すべての移動に効果があるわけではないので、適当な戦略の存在が予想される。

6.2.8.帰納法の導入

帰納法を用いらなければ証明できない時間論理式Aに対しては、

$$(P\wedge\Box(\dot{P}\supset\bigcirc P)\supset\Box P)\supset A$$

とすることにより証明されるが、PはAに応じて適当な命題変数、論理式をあてはめなければならない。与式Aに対する適切なPを決定する戦略が必要である。

6.3.処理間の相互関係

重複、π型様相記号の○を含む形式への展開、○の移動の３種の変形をどの順序で探索するかは、証明手続き全体の効率に大きく影響する。展開はパスの数を増やし重複を必要にすることがあるので、展開を重複の先に行い、○の移動はパスや結合に影響しないので、展開や重複の後で行うことが考えられる。

しかし、展開、重複、移動が必要になるのは、もとの式のままでは統一化に失敗したからであり、その統一化における情報が、どのような変形を行えばよいか、示唆を与えていると考えられる。したがって、統一化をも含めて処理の順序考える必要があると思われる。（例7.2.参照）

7．例

7.1.

$$P\supset\Box\neg Q\vee\bigcirc(\neg P\vee\bigcirc\Diamond\neg P)\vee\Diamond(P\wedge Q)$$

を証明する。この式の木表現は図7.1のようになる。

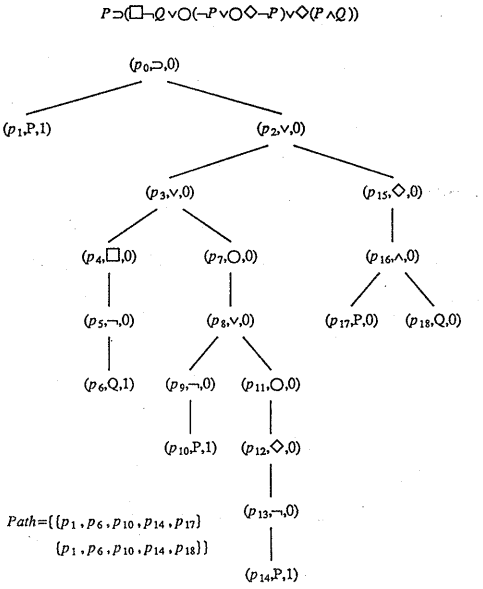


図7.1

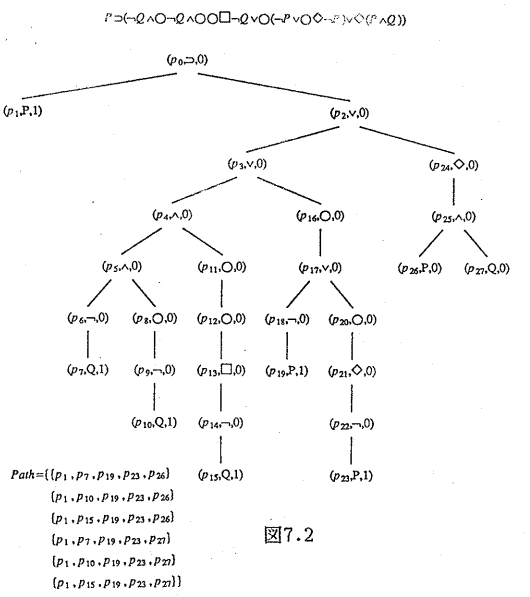


図7.2

各ノード(p,L,n)は、（位置，ラベル，極性）を表す。なお以下のでは、γ_n，π_mで、それぞれ位置p_nのγ型様相記号、位置p_mのπ型様相記号を表すとする。○は複数の出現を位置によって区別する必要はない。

様相記号の統一化を行うと、結合(p_6,p_{18})によってπ_4/γ_{15}が得られるが、p_{17}との結合はγ_{15}にπ型様相記号が代入されているために、統一化できない。そこで、π_4を展開すると、図7.2のようになる。

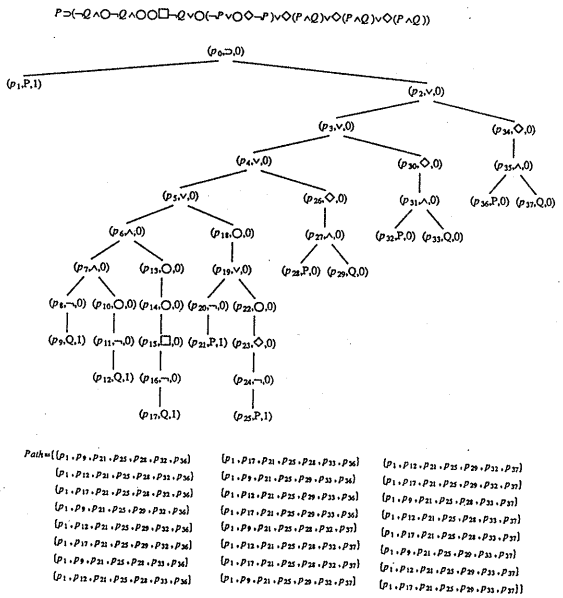


図7.3

ここでγ_{24}を３重に重複させると図7.3のようになる。ここで、{ϕ/γ_{26},○/γ_{30},○○π_{15}/γ_{34},π_{15}/γ_{23}}なる代入を考えれば、

(p_1,p_{28}),(p_{29},p_9),(p_{32},p_{21}),

(p_{33},p_{12}),(p_{36},p_{25}),(p_{37},p_{17})

なる結合が統一化されれ、パスの各要素には必ずこれらのうち少なくともひとつが存在する。　以上のようにして与式は証明される。この例では分配や○の移動は必要なかった。

7.2.

7.1.では展開をしてから重複をした。ここでは統一化の過程で木の変形を行って証明する。

図7.1において(p_6,p_{18})を結合として統一化すると、γ_{15}にγ_{14}が代入され図7.4のようになる。

ここでp_{11}を展開すれば、図7.5のようになる。(p_1,p_{13}),(p_6,p_{15}),(p_{10},p_{19})を結合とし、γ_8にπ_{18}を代入すれば、統一化が成功し証明できる。

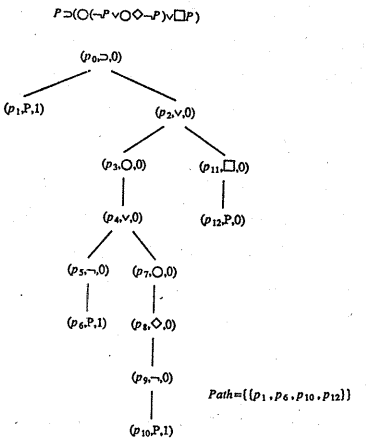


図7.4

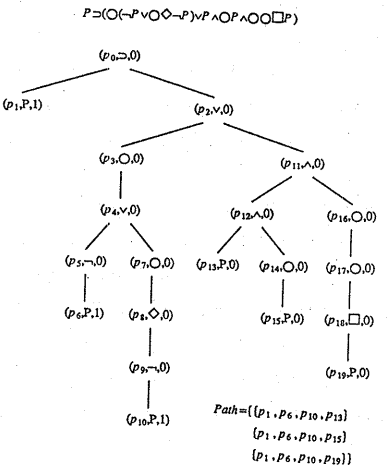


図7.5

この場合、Qに関する結合は一通りしかなかったので、図7.1の(p_6,p_{18})を結合とすることは明かであり、π_4をγ_{15}に代入するのは必然ともいえる。 7.1.に比較して、重複を行わなかったので木を大きくせずに証明できた。このような木への操作を中心に証明を進めることによって、より効率的戦略を発見できるかもしれないが、今のところこのような操作を形式的にまとめるには至っていない。

8．まとめ

様相記号の統一化の概念を、結合法に応用して一般的様相論理証明器を構築し、体系Ｓ４にnext-time(○)を導入して、時間論理証明器を構成する方法について述べた。様相記号の統一化は体系毎の違いを局所的な手続きで吸収できるが、線形時間を仮定して時間論理に適用すると、□、◇の○への展開、○の移動に関して等価な論理式について統一化を実行しなければならない。また重複数による変形と複合されると、さらに探索の範囲が広がる。今後の課題としては、実用的時間論理証明システムとするために、これらの変形に対する効率的戦略の定式化が必要である。また、より一般的利用には帰納法の公理スキーマを適切に取り入れなければならない。

＜参考文献＞

[1]Bibel,W.：Automated Theorem Proving
Braunschweig;Wiesbaden:Viewweg,1982
[2]Cavalli,A.R. & Farinas del Cerro,L.：
A Decision Method for Linear Temporal Logic：
Proc.of 7th International Conference on Automated Deduction L.N. in C.S. vol.170 1984 p113-127
[3]Wallen,L.A.：Generating Connection Calculi from Tableaux and Sequent Based Proof System：
Dept. of AI, Univ. of Edinburgh,Research Paper No.258 1985
[4]米崎直樹：様相論理証明器の一般化
日本ソフトウェア科学会第３会大会論文集 D-5-1
[5]西田晴彦：一般的様相論理証明器の研究
東京工業大学情報工学科昭和６１年度修士論文
[6]Abadi,M. & Manna,Z.：A Timely Resolution
Dept. of Computer Science, Stanford Univ.
Technical report No.STAN-CS-86-1106 April 1986