

## 正則集合に表現等価なテンポラル・ロジック

京大工学部 平石裕実 (Hiromi Hiraishi)

京大工学部 矢島脩三 (Shuzo Yajima)

### 1. まえがき

超大規模論理回路 (VLSI) により大規模論理システムの構築が可能となりつつある現在、大規模論理システムを誤りなく正しく設計し、かつ実現して正しく動作していることの確認できる論理設計手法の確立が益々重要となってきている。このため、従来より論理設計の CAD/DA、論理設計手法、故障検査、設計検証等の研究が行われているが、論理設計検証については未だ実用的な手法が確立されておらず、設計対象システムの形式的仕様記述や形式的検証手法の研究が重要と考えられる。

形式的仕様記述や形式的検証のアプローチとしては、命題論理や第 1 階述語論理、テンポラル・ロジック [1] 等の論理体系に基づく方法や、VDM [2] や抽象データ型 [3] による仕様記述等の代数的方法、また、正則集合や第 1 井表現 [4] 等の系列記

述に基づく方法等がある。特にテンポラル・ロジックは時間の概念を陽に表現できるため、現在、並行プロセスやハードウェアの設計検証との関連で研究が進められており、種々のクラスのテンポラル・ロジックが提案されている。拡張テンポラル・ロジック (E T L) [5] は無限長系列を取り扱い、正則集合を表現できるが、そのためには無限個のテンポラル演算子を必要とする。一方、インターバル・テンポラル・ロジック (I T L) [6] は有限長系列を取り扱い、その表現能力は真に正則集合を含んでいるが、充足可能性判定問題が決定不能になる等の問題点を含んでいる。設計対象を有限オートマトンと考えると、正則集合と表現能力が等価なテンポラル・ロジックの体系を明らかにすることが重要であると考えられる。そこで本稿ではこのような観点から正則集合と等価な表現能力を持つ新たなテンポラル・ロジック (R T L) を示す。

## 2. R T L

### 2. 1 R T L のシンタックス

#### 【定義 1】 R T L の原始記号

以下に述べる原始命題、論理記号、補助記号を R T L の原始記号という。

(1) 原始命題  $p, q, r, \dots$

(2) 論理記号  $\sim, \vee, \circ, \boxplus, :$

(3) 補助記号  $(, )$

□

原始命題の集合を以下  $AP$  で表わす。

【定義 2】  $RTL$  の論理式 ( $RTL$  式)

(1)  $p$  が原始命題の時、 $p$  は  $RTL$  式である。

(2)  $\eta$  が  $RTL$  式の時、 $(\sim \eta)$  も  $RTL$  式である。

(3)  $\eta, \xi$  が  $RTL$  式の時、 $(\eta \vee \xi)$  も  $RTL$  式である。

(4)  $\eta$  が  $RTL$  式の時、 $(\circ \eta)$  も  $RTL$  式である。

(5)  $\eta$  が  $RTL$  式の時、 $(\boxplus \eta)$  も  $RTL$  式である。

(6)  $\eta, \xi$  が  $RTL$  式の時、 $(\eta : \xi)$  も  $RTL$  式である。

(7) 以上の (1) - (6) を有限回適用して得られるもののみが  $RTL$  式である。 □

$RTL$  式全体の集合を  $LF$  で表わす。又、論理記号  $\sim, \circ, \boxplus$  は  $\vee, :$  よりも高い優先順位を持つものとし、論理記号の適用範囲が明確な場合は補助記号  $(, )$  を省略することがある。更に、次の略記を適宜用いる。

$$\eta \wedge \xi \triangleq \sim (\sim \eta \vee \sim \xi), \quad \eta \supset \xi \triangleq \sim \eta \vee \xi, \quad \eta \equiv \xi \triangleq (\eta \supset \xi) \wedge (\xi \supset \eta), \quad \diamond \eta \triangleq \sim \boxplus \sim \eta, \quad \forall \eta \triangleq \eta \vee \sim \eta,$$

$$U_r \triangleq \sim V_r \quad .$$

## 2. 2 R T L のセマンティックス

### 【定義 3】 R T L の解釈

$\Sigma$  を状態の有限集合、 $B = \{T, F\}$  を真理値の集合とし、各状態  $s$  における原始命題  $p$  の真理値を与える関数  $m_s: \Sigma \times AP \rightarrow B$  と、状態の空系列を表わす  $\lambda$  に対する原始命題  $p$  の真理値を与える関数  $m_\lambda: AP \rightarrow B$  を考える。この時、 $\langle \Sigma, m_s, m_\lambda \rangle$  を R T L の解釈という。  $\square$

### 【定義 4】 R T L 式の真理値

$\Sigma$  上の系列  $\sigma \in \Sigma^*$  ( $\sigma = \lambda$  又は  $\sigma = s_0 s_1 \cdots s_n$  とする) に対して R T L 式の真理値を与える関数  $M: \Sigma^* \times LF \rightarrow B$  を次のように定義する。但し、 $p \in AP$ ,  $\eta, \xi \in LF$  とし、 $|\sigma|$  は系列  $\sigma$  の長さを表わし、 $|\sigma| \geq 2$  の時  $\sigma_1 = s_1 s_2 \cdots s_n$ 、 $|\sigma| = 1$  の時  $\sigma_1 = \lambda$  とする。

$$(1) \quad M(\sigma, p) = m_s(s_0, p) \cdots \quad |\sigma| \geq 1 \text{ の時} \\ m_\lambda(p) \quad \cdots \quad \sigma = \lambda \text{ の時}$$

$$(2) \quad M(\sigma, \sim \eta) = T \quad \cdots \quad M(\sigma, \eta) = F \text{ の時} \\ F \quad \cdots \quad M(\sigma, \eta) = T \text{ の時}$$

$$(3) M(\sigma, \eta \vee \xi) = T \cdots \cdots M(\sigma, \eta) = T$$

または  $M(\sigma, \xi) = T$  の時

F  $\cdots \cdots$  それ以外の時

$$(4) M(\sigma, \bigcirc \eta) = T \cdots \cdots \sigma = \lambda \text{ で } M(\lambda, \eta) = T$$

または  $\sigma \neq \lambda$  で  $M(\sigma_1, \eta) = T$  の時

F  $\cdots \cdots$  それ以外の時

$$(5) M(\sigma, \boxplus \eta) = T \cdots \cdots M(\alpha_i, \eta) = T \text{ なる}$$

$\alpha_i \in \Sigma^* (1 \leq i \leq m \leq n)$  が存在して、

$\sigma = \alpha_1 \alpha_2 \cdots \alpha_m$  と表わせる時

F  $\cdots \cdots$  それ以外の時

$$(6) M(\sigma, \eta : \xi) = T \cdots \cdots M(\alpha_1, \eta) = T,$$

$M(\alpha_2, \xi) = T$  なる  $\alpha_i \in \Sigma^* (i=1, 2)$

が存在して、 $\sigma = \alpha_1 \alpha_2$  と表わせる時

F  $\cdots \cdots$  それ以外の時  $\square$

$M(\sigma, \eta) = T$  の時、 $\langle m_s, m_i, \sigma \rangle \models \eta$  と表わし、  
 $m_s, m_i$  が明確な場合は単に  $\sigma \models \eta$  と表わす。又、任意の  
 $m_s, m_i, \sigma$  に対して  $\langle m_s, m_i, \sigma \rangle \models \eta$  の時、 $\eta$  は恒真  
 であるといい  $\models \eta$  と表わす。

### 3. RTL の表現能力

解釈  $\langle \Sigma, m_s, m_i \rangle$  のもとで RTL 式  $\eta$  の真理値を T と

するような  $\Sigma$  上の系列全体の集合を  $L < \Sigma, m_s, m_i > (\eta)$

とする。即ち、

$$L < \Sigma, m_s, m_i > (\eta) = \{ \sigma \mid \sigma \in \Sigma^*, < m_s, m_i, \sigma > \models \eta \}$$

この時、 $\eta$  は  $L < \Sigma, m_s, m_i > (\eta)$  を表わすという。以

下、混乱の恐れがない時は  $L < \Sigma, m_s, m_i > (\eta)$  を単に

$L(\eta)$  と表わす。

R T L の表現能力に関して以下の補題が成立する。

【補題 1】  $L(\eta)$  は  $\Sigma$  上の正則集合である。

(略証) R T L 式の構成方法に基づく帰納法により示す。

(1)  $p \in A P$ ,  $S(p) = \{ s \mid s \in \Sigma, m_s(s, p) = T \}$  とすると、

$$m_i(p) = T \text{ ならば、} L(p) = \lambda + S(p) \cdot \Sigma^*$$

$$m_i(p) = F \text{ ならば、} L(p) = S(p) \cdot \Sigma^*$$

$$(2) \quad L(\sim \eta) = \Sigma^* - L(\eta)$$

$$(3) \quad L(\eta \vee \xi) = L(\eta) + L(\xi)$$

$$(4) \quad L(\bigcirc \eta) = \lambda + \Sigma \cdot L(\eta) \quad \lambda \in L(\eta) \text{ の時} \\ \Sigma \cdot L(\eta) \quad \dots \dots \lambda \notin L(\eta) \text{ の時}$$

$$(5) \quad L(\boxplus \eta) = L(\eta)^*$$

$$(6) \quad L(\eta : \xi) = L(\eta) \cdot L(\xi) \quad \square$$

【補題 2】  $\Sigma$  上の任意の正則集合  $R$  に対し、ある解釈  $\langle \Sigma, m_s, m_l \rangle$  のもとで  $R$  を表わす R T L 式  $\eta$  が存在する。

(略証)  $\lceil \log_2 |\Sigma| \rceil + 1$  個の原始命題  $p_0, p_1, \dots, p_{\lceil \log_2 |\Sigma| \rceil}$  を用い、 $m_l, m_s$  を次のように決める。

|       |                | $p_0$   | $p_1$   | $p_2$   | $\dots$ | $p_{\lceil \log_2  \Sigma  \rceil}$ |
|-------|----------------|---------|---------|---------|---------|-------------------------------------|
| $m_l$ | $\lambda$      | T       | F       | F       | $\dots$ | F                                   |
|       | $s_1$          | F       | F       | F       | $\dots$ | F                                   |
| $m_s$ | $s_2$          | F       | F       | F       | $\dots$ | T                                   |
|       | $s_3$          | F       | F       | F       | $\dots$ | F                                   |
|       | $\cdot$        | $\cdot$ | $\cdot$ | $\cdot$ | $\dots$ | $\cdot$                             |
|       | $\cdot$        | $\cdot$ | $\cdot$ | $\cdot$ | $\dots$ | $\cdot$                             |
|       | $s_{ \Sigma }$ | F       | T       | T       | $\dots$ | $\cdot$                             |
|       |                |         |         |         |         |                                     |

即ち、 $s_i$  に対して真となる  $p_1' \wedge p_2' \wedge \dots \wedge p_{\lceil \log_2 |\Sigma| \rceil}'$  の形の論理式は一意的に定まり、異なる  $s_i$  と  $s_j$  に対しては異なる論理式が対応する (但し、 $p_k'$  は  $p_k$  あるいは  $\sim p_k$  を表わす)。又、 $p_0$  は  $\lambda$  に対してのみ真となる原始命題である。

この時、正則集合  $R$  を表わす R T L 式を  $R T L (R)$  とすると、 $R T L (R)$  は下記のように再帰的に構成できる。但し、 $R_1, R_2$  は  $\Sigma$  上の任意の正則集合とする。

$$R T L (\phi) = U_f$$

$$RTL(\lambda) = p_0$$

$$RTL(s_1) = \sim p_1 \wedge \sim p_2 \wedge \cdots \wedge \sim p_{\log_2 |Z|} \\ \wedge \bigcirc p_0 \wedge \sim p_0$$

.

.

$$RTL(R_1 \cdot R_2) = (RTL(R_1)) : (RTL(R_2))$$

$$RTL(R_1 + R_2) = (RTL(R_1)) \vee (RTL(R_2))$$

$$RTL(R_1^*) = p_0 \vee \square (RTL(R_1)) \quad \square$$

これより次の定理が成立する。

【定理 1】  $RTL$  は正則集合と等価な表現能力を持つ。□

#### 4. $RTL$ 式の恒真性判定問題

$RTL$  式の恒真性判定について以下の定理が成立する。

【定理 2】 与えられた  $RTL$  式  $\eta$  が恒真かどうかの判定問題は決定可能である。

(略証) まず、 $m_1, m_s$  を固定して考える。この時、 $\eta$  が表わす系列集合を正則表現  $R$  で表現すると、任意の  $\sigma \in \Sigma^*$  に対して  $\langle m_s, m_1, \sigma \rangle \models \eta$  かどうかの判定問題は  $R$  の空補集合判定問題に帰着できるので決定可能である。

次に、任意の  $m_1, m_s$  について考える。 $m_1$  は  $AP \rightarrow B$  なる



関数で、 $m_s$ は  $\Sigma \times A^P \rightarrow B$  なる関数であるが、 $\eta$  の長さは有限であり高々有限個の原始命題しか含んでいない。 $\eta$  に含まれていない原始命題の各状態に対する T / F の値は  $\eta$  の真理値に影響を与えないので、 $\eta$  に含まれる有限個の原始命題に対する T / F の割り当てのみを考えれば十分である。又、 $\Sigma$  は有限集合であるので、 $m_i$ 、 $m_s$  としては高々有限個の関数のみを考えればよい。

以上により、 $\eta$  が恒真かどうかの判定問題は決定可能である。 □

【定理 3】 RTL 式の恒真性判定問題の DTM 領域複雑度は非初等的である。

(略証) RTL 式と拡張正則表現との間の変換は多項式時間で可能であり、拡張正則表現の空集合問題の DTM 領域複雑度は非初等的である [7] ことより明らか。 □

## 5. あとがき

正則集合と等価な表現能力を持つテンポラル・ロジック RTL を導入し、その恒真性判定問題が決定可能であり DTM 領域複雑度がであることを示した。今後 RTL の公理系を明らかにすると共に、論理設計検証への応用を考えていきたい。

謝 辞 種々御議論頂いた矢島研究室の諸氏に感謝します。

参考文献

- [1] N.Rescher and A.Urquhart: Temporal Logic,  
Springer-Verlag, 1971.
- [2] D.Bjorner: Formal Specification & Software  
Development.
- [3] 稲垣, 坂部: 抽象データタイプの代数的仕様記述の基礎  
(1)(2), 情報処理, vol.25, no.1, pp.47-53, no.5,  
pp.491-501, 1984.
- [4] 木村, 矢島: 論理回路の入力制約および入出力仕様の記  
述とその検証, 信学技報, AL85-65, 1986.
- [5] P.Wolper: Temporal Logic Can Be More Expressive,  
Proc. 22nd Annual Symp. on Foundations of Computer  
Science, pp.340-348, 1981.
- [6] B.Moszkowski: Reasoning about Digital Circuit,  
STAN-CS-83-970, 1983.
- [7] A.V.Aho, J.E.Hopcroft and J.D.Ullman: The Design  
and Analysis of Computer Algorithms, Addison-  
Wesely, 1974.