ビット列を捉える無限様相論理

佐野 勝彦

(**要旨**) 次の表で代数の「等式的論理」に余代数で対応するものは何だろうか？**様相論理** [1] だ, というのが本発表で与えたい解答である．無論、解答の与え方は複数ありうるが，本発表では，(i) 二つのシステムの**振舞の同値性**を捉えることができる，(ii) 代数のクラスが等式で「書ける」必要十分条件を与える**バーコフの定理**の双対が成立する，という二つの要請の下での解答を探る．こういった試みを通じて，様相論理が，可能世界意味論を備えた必然性について語る言語であるだけではなく，システムの（無限に続きうる）プロセスについて語る言語であることを強調したい．以下では，本発表の内容を,「余帰納原理」とは何かを含め，やや詳しくレジュメ形式で解説してある．本発表後に，内容に興味を持たれた方に参照していただければ幸いである．

代数	余代数
Bottom Up	Top Down
帰納法	余帰納法
始代数	終余代数
等式的論理	???

1. ビット列計算と余帰納原理

1.1. **ビット列.** $\{0,1\}^{\mathbb{N}}$ の要素 (**ビット列**) は $S \to \{0,1\} \times S$ という形の**ストリームオートマトン**から生成できる (cf. [2]). $\{0,1\}$ を出力するシステム．一般に $S \to T(S)$ で書ける（T は**函手**）.

1.2. **ストリームオートマトンの振舞.** どのような $S \to \{0,1\} \times S$ の振舞も一つの特殊なストリームオートマトン $\langle \mathsf{hd}, \mathsf{tl} \rangle : \{0,1\}^{\mathbb{N}} \to \{0,1\} \times \{0,1\}^{\mathbb{N}}$ で「記述」できる．但し，$x \in \{0,1\}^{\mathbb{N}}$ に対し $\mathsf{hd}(x)$ は x の第 0 成分，$\mathsf{tl}(x)$ は x から第 0 成分を切り落とした残り (第 1 成分以降)．下の図式を可換にする beh が一意に存在し，beh が $\langle \gamma_0, \gamma_1 \rangle : S \to \{0,1\} \times S$ の振舞を記述.

$$\begin{array}{ccc} \{0,1\} \times S & \xrightarrow{\mathrm{id} \times beh} & \{0,1\} \times \{0,1\}^{\mathbb{N}} \\ \uparrow{\scriptstyle \langle \gamma_0, \gamma_1 \rangle} & & \uparrow{\scriptstyle \langle \mathsf{hd}, \mathsf{tl} \rangle} \\ S & \xrightarrow{beh} & \{0,1\}^{\mathbb{N}} \end{array}$$

1.3. **ビット列計算の定義を導く余帰納原理.**

1.3.1. even. $x \in \{0,1\}^{\mathbb{N}}$ の偶数番目を取り出す操作を $\mathsf{even}(x)$ として定めたい.

$$\begin{array}{ccc} \{0,1\} \times \{0,1\}^{\mathbb{N}} & \xrightarrow{\mathrm{id} \times \mathsf{even}} & \{0,1\} \times \{0,1\}^{\mathbb{N}} \\ \uparrow{\scriptstyle \langle \gamma_0, \gamma_1 \rangle} & & \uparrow{\scriptstyle \langle \mathsf{hd}, \mathsf{tl} \rangle} \\ \{0,1\}^{\mathbb{N}} & \xrightarrow{\mathsf{even}} & \{0,1\}^{\mathbb{N}} \end{array}$$

としたい．どうやって $\langle \gamma_0, \gamma_1 \rangle$ を決めるか？まずは $x \in \{0,1\}^{\mathbb{N}}$ の第 0 成分を取り出して，第 1 成分を飛ばして，第 2 成分以降のビット列を切り離す．その後は同じ操作を繰り返せばよい．これを反映し $\gamma_0(x) = \mathsf{hd}(x)$, $\gamma_1(x) = \mathsf{tl} \circ \mathsf{tl}(x)$ とすればよい．すると，可換性を用いて次の定義式を導ける.

$$\begin{array}{rcl} \mathsf{hd}(\mathsf{even}(x)) & = & \mathsf{hd}(x); \\ \mathsf{tl}(\mathsf{even}(x)) & = & \mathsf{even}(\mathsf{tl}(\mathsf{tl}(x))). \end{array}$$

Date: 11th November, 2012. 北陸先端科学技術大学院大学, 情報科学研究科, v-sano@jaist.ac.jp.

1.3.2. zip. 二つのビット列 $x, y \in \{0,1\}^{\mathbb{N}}$ を交互に組み合わせて新しいビット列 $\mathsf{zip}(x,y)$ を作りたい.

$$\begin{array}{ccc} \{0,1\} \times \left(\{0,1\}^{\mathbb{N}} \times \{0,1\}^{\mathbb{N}}\right) & \xrightarrow{\mathrm{id}\times\mathsf{zip}} & \{0,1\} \times \{0,1\}^{\mathbb{N}} \\ \uparrow{\scriptstyle \langle \gamma_0, \gamma_1 \rangle} & & \uparrow{\scriptstyle \langle \mathsf{hd},\mathsf{tl} \rangle} \\ \{0,1\}^{\mathbb{N}} \times \{0,1\}^{\mathbb{N}} & \xrightarrow{\mathsf{zip}} & \{0,1\}^{\mathbb{N}} \end{array}$$

としたい. even と同じように繰り返す操作を考える. まずは x の第 0 成分を取り出して, x の第 1 成分以降は後にまわして, 次は y の第 0 成分をとって, y の第 0 成分は後にまわして, x の第 1 成分をとって $\cdots$ と繰り返す. そこで, $\gamma_0(x,y) = \mathsf{hd}(x)$, $\gamma_1(x,y) = (y, \mathsf{tl}(x))$ とすればよい. 可換性を用いて次の定義式が手に入る.

$$\begin{array}{lcl} \mathsf{hd}(\mathsf{zip}(x,y)) & = & \mathsf{hd}(x); \\ \mathsf{tl}(\mathsf{zip}(x,y)) & = & \mathsf{zip}(y, \mathsf{tl}(x)). \end{array}$$

1.4. **証明法としての余帰納原理.** zip, even については次がいえるはず.

> **命題 1.** 任意の $x \in \{0,1\}^{\mathbb{N}}$ に対して $\mathsf{even}(\mathsf{zip}(x,x)) = x$.

(∵) 次を満たす **双模倣関係** $R \subseteq \{0,1\}^{\mathbb{N}} \times \{0,1\}^{\mathbb{N}}$:

- xRy ならば $\mathsf{hd}(x) = \mathsf{hd}(y)$.
- xRy ならば $\mathsf{tl}(x) R \mathsf{tl}(y)$.

を見出し, $\mathsf{even}(\mathsf{zip}(x,x))Rx$ を示せば**よい**. $R = \left\{ \langle \mathsf{even}(\mathsf{zip}(x,x)), x \rangle \,|\, x \in \{0,1\}^{\mathbb{N}} \right\}$ とおけ. (**証明終**)
しかし, なぜこの議論が証明として認められるのだろうか? 次節では余代数的観点からこれに答える.

2. 余代数的観点からの余帰納原理

そもそも余帰納原理とは何か. 前節の話を $S \to T(S)$ (T-**余代数**) という一般的な形式で再考察 (cf. [3]).

2.1. **終余代数.** $\langle \mathsf{hd}, \mathsf{tl} \rangle : \{0,1\}^{\mathbb{N}} \to \{0,1\} \times \{0,1\}^{\mathbb{N}}$ は $T(S) := \{0,1\} \times S$ としたときの**終余代数**. $\delta : Z \to T(Z)$ が T-**終余代数**であるのは, 任意の $\gamma : S \to T(S)$ に対して

$$\begin{array}{ccc} T(S) & \xrightarrow[T(f)]{} & T(Z) \\ \uparrow{\scriptstyle \gamma} & & \uparrow{\scriptstyle \delta} \\ S & \xrightarrow[f]{!} & Z \end{array}$$

を可換にする f が一意に存在. 定義法としての余帰納原理は終余代数で捉えられる.

2.2. **振舞同値 (behavioural equivalence).** $\gamma : S \to T(S)$ の $s \in S$ と $\gamma' : S' \to T(S')$ の $s' \in S'$ が**振舞同値**なのは, ある $\delta : Z \to T(Z)$, $f : S \to Z$, $g : S' \to Z$ が存在して:

$$\begin{array}{ccccc} T(S) & \xrightarrow[T(f)]{} & T(Z) & \xleftarrow[T(g)]{} & T(S') \\ \uparrow{\scriptstyle \gamma} & & \uparrow{\scriptstyle \delta} & & \uparrow{\scriptstyle \gamma'} \\ S & \xrightarrow[f]{} & Z & \xleftarrow[g]{} & S' \end{array}$$

かつ $f(s) = g(s')$ となること. これを $s \equiv_T s'$ と書こう. T-終余代数が存在するなら $\delta : Z \to T(Z)$ として終余代数をとればよい.

> **命題 2.** $\delta : Z \to T(Z)$ は終余代数とせよ. $z, z' \in Z$ に対し $z \equiv_T z'$ なら $z = z'$.

2.3. **双模倣同値.** $\gamma : S \to T(S)$ の $s \in S$ と $\gamma' : S' \to T(S')$ の $s' \in S'$ が**双模倣的** (bisimilar) なのは, ある $R \subseteq S \times S'$ と $\rho : R \to T(R)$ が存在して,

$$\begin{array}{ccccc} T(S) & \xleftarrow{T(\pi_0)} & T(R) & \xrightarrow{T(\pi_1)} & T(S') \\ \uparrow{\scriptstyle \gamma} & & \uparrow{\scriptstyle \rho} & & \uparrow{\scriptstyle \gamma'} \\ S & \xleftarrow{\pi_0} & R & \xrightarrow{\pi_1} & S' \end{array}$$

かつ $(s,s') \in R$ となる場合（但し π_0, π_1 は射影）．これを $s \underline{\leftrightarrow}_T s'$ と書こう．T がどのような函手でも双模倣関係は振舞同値を含意する．

命題 3. $\gamma : S \to T(S)$ の $s \in S$ と $\gamma' : S' \to T(S')$ の $s' \in S'$ について，$s \underline{\leftrightarrow}_T s'$ なら $s \equiv_T s'$.

2.4. **余帰納法証明原理 (coinduction proof principle).** 命題 2 と命題 3 から **余帰納法証明原理** (cf. [3]):

定理 1. $\delta : Z \to T(Z)$ は終余代数とせよ．$z, z' \in Z$ に対し $z \underline{\leftrightarrow}_T z'$ なら $z = z'$.

が成立し，命題 1 の証明方法が正当化される．

3. ビット列を捉える様相論理

以下では，様相論理に対する要請として

(i) 振舞同値・双模倣同値を捉える
(ii) 代数の**バーコフの定理**の対応物をもつ

の二つ課す．ここで**バーコフの定理** (Birkhoff's Variety Theorem) とは，代数のあるクラス K が等式の集合で定義できるのは K が**準同型像・部分代数・直積**について閉じる場合でありその場合に限る，という定理．以下では $T(S) = \{0,1\} \times S$ としてこの要請を満たす様相論理を与える．

3.1. **言語 $\mathcal{L}_T$ とその意味論.** 命題変数の集合 P, 否定 $\neg$, **無限選言** $\bigvee$, 様相記号 $\Box_0, \Box_1$ からなる．T-余代数 $\gamma = \langle \gamma_0, \gamma_1 \rangle : S \to \{0,1\} \times S$ と $V : S \to \mathcal{P}(\mathsf{P})$ に対して，

$$\begin{array}{ll} (S,\gamma,V), s \models \bigvee \Delta & \iff \text{ ある } \varphi \in \Delta \text{ に対し } (S,\gamma,V), s \models \varphi \\ (S,\gamma,V), s \models \Box_0 \varphi & \iff \gamma_0(s) = 0 \text{ かつ } (S,\gamma,V), \gamma_1(s) \models \varphi \\ (S,\gamma,V), s \models \Box_1 \varphi & \iff \gamma_0(s) = 1 \text{ かつ } (S,\gamma,V), \gamma_1(s) \models \varphi \end{array}$$

と通常の条項で意味論を定める．例えば，S, γ の s から始めた振舞が $(01)^*$ (010101... の略記) だとすると，

$$(S,\gamma,V), s \models \Box_0\top \wedge \Box_0\Box_1\top \wedge \Box_0\Box_1\Box_0\top \wedge \Box_0\Box_1\Box_0\Box_1\top \wedge \cdots$$

により振舞が記述できる．また，$\{(01)^*, (10)^*\} \subseteq \{0,1\}^{\mathbb{N}}$ は

$$\Box_0\top \wedge \Box_0\Box_1\top \wedge \Box_0\Box_1\Box_0\top \wedge \Box_0\Box_1\Box_0\Box_1\top \wedge \cdots$$
$$\Box_1\top \wedge \Box_1\Box_0\top \wedge \Box_1\Box_0\Box_1\top \wedge \Box_1\Box_0\Box_1\Box_0\top \wedge \cdots$$

の二つの論理式の選言で記述できる．

3.2. **要請 (i)：振舞同値は様相同値を含意.** 二つの (S,γ,V) の $s \in S$, (S',γ',V') の $s' \in S'$ が **様相同値** ($s \leftrightsquigarrow_{\mathcal{L}_T} s'$ と表記) であるのは，二つの状態が論理式で区別できないこと，すなわち，任意の $\mathcal{L}_T$-論理式 φ について $(S,\gamma,V), s \models \varphi \iff (S',\gamma',V'), s \models \varphi$ を満たす場合．$T = \{0,1\} \times (-)$ のとき，

命題 4. (S,γ,V) の $s \in S$, (S',γ',V') の $s' \in S'$ について，$s \equiv_{T \times \mathcal{P}(\mathsf{P})} s'$ なら $s \leftrightsquigarrow_{\mathcal{L}_T} s'$.

3.3. **要請 (ii).** $T = \{0,1\} \times (-)$ とせよ．$\mathsf{Mod}(\varphi) = \{(S,\gamma) \mid (S,\gamma) \models \varphi\}$ とすると，T-余代数のあるクラス K が φ で**定義できる**のは $\mathsf{Mod}(\varphi) = \mathsf{K}$ となる場合である．バーコフの定理の余代数版 [1] は次のように述べられる．

定理 2. $T = \{0,1\} \times (-)$ とせよ．T-余代数のあるクラス K が φ で定義できるのは，K が**余代数準同型・部分余代数・直和**について閉じる場合であり，その場合に限る．

右向きは選言が有限でも証明できる．しかし左向きには，**終余代数のドメインのどんな部分集合もある様相論理式で書ける**，という補題が必要となる．

References

[1] A. Kruz. A co-variety-theorem for modal logic. In Maarten de Rijke Michael Zakharyaschev, Krister Segerberg and Heinrich Wansing, editors, *Advances in Modal Logic*, volume 2, pages 385–398. CSLI Publications, 2000.

[2] D. Pattinson. An introduction to the theory of coalgebras, 2003. Lecture Notes, Second North American Summer School on Logic, Language and Information. Available from `http://www.doc.ic.ac.uk/~dirk/Publications/nasslli2003.pdf`.

[3] Yde Venema. Algebras and coalgebras. In J. van Benthem et.al., editor, *Handbook of modal logic*. Elsvier, 2007.