B-3

連を用いたwhileプログラムの意味論
Semantics of **while** programs by sets of runs

木下 佳樹 [†] 古澤 仁 [‡]
Yoshiki KINOSHITA Hitoshi Furusawa

1 はじめに

本稿では，停止する while プログラムの代数的構造を while 代数として提示し，任意の while 代数における意味解釈を与える函手意味論を展開する．また，テスト付きクリーニ代数 [2, 3] の圏から while 代数への忠実函手 $\mathcal{I}$: **Kat** $\to$ **While** が存在し，これを用いて任意のテスト付きクリーニ代数における while プログラムの意味解釈ができることに注意する．とくに，著者らが [3] で与えたテスト付きクリーニ代数 $\mathcal{Q}_{B,\Sigma}$ における意味解釈は，連の集まりによる意味論になっている．

2 while プログラムの代数構造

定義 2.1 (while 代数) while 代数を多ソート代数として次のように定める．簡便のため，*CASL*, *OBJ* などの代数的仕様記述言語様の記法を用いることにする．

- **sort** Test, Com.
- **op** abort, skip: $\to$ Com.
- **op** ;, []: Com $\times$ Com $\to$ Com.
- **op** if: Test $\times$ Com $\times$ Com $\to$ Com.
- **op** while: Test $\times$ Com $\to$ Com.
- **op** tt, ff: $\to$ Test.
- **op** $\neg$: Test $\to$ Test.
- **op** $\wedge, \vee$: Test $\times$ Test $\to$ Test.
- **infix** ;, [], $\wedge, \vee$.
- **eq** (Com, skip, ;) が単（*monoid*）であることを示す等式
- **eq** (Com, abort, []) が半束であることを示す等式
- **eq** $c;y \,[]\, c;z \le c;(y \,[]\, z)$.
  comment $x \le y \overset{\text{def}}{\Longleftrightarrow} x \,[]\, y = y$.
- **eq** abort;c = abort = c;abort
- **eq** if(tt, c, c') = c. **eq** if(ff, c, c') = c'.
- **eq** while(b, c) = if(b, c;while(b, c), skip).
- **eq** (Test, ff, tt, $\vee, \wedge, \neg$) がブール代数であることを示す等式

いいかえると，while 代数 **W** は，二つの台集合 $W_{\mathbf{Test}}$, $W_{\mathbf{Com}}$ をもち，$W_{\mathbf{Test}}$ を台集合とするブール代数の構造，$W_{\mathbf{Com}}$ を台集合とする冪等半環 (後出) の構造を備え，さらにそれらをつなぐ **if** と **while** の構造をもつものである．while 代数の準同型は，多ソート代数の準同型として定義する．詳しくいうと，while 代数 **W** から **V** への準同型 f とは $W_{\mathbf{Test}}$ から $V_{\mathbf{Test}}$ へのブール代数準同型 $f_{\mathbf{Test}}$ と $W_{\mathbf{Com}}$ から $V_{\mathbf{Com}}$ への冪等半環準同型 $f_{\mathbf{Com}}$ との対で，**if** と **while** を保つものである．

while 代数の公理は，等式のみで与えられているから，任意の集合 B, Σ について，それが自由生成する while 代数 $F(B,\Sigma)$ が存在する．つまり，任意の while 代数 **W** に対して，写像 $f_1 : B \to W_{\mathbf{Test}}$，$f_2 : \Sigma \to W_{\mathbf{Com}}$ は常に while 代数準同型 $(\hat{f_1}, \hat{f_2})$: $F(B,\Sigma) \to \mathbf{W}$ に一意的に拡張される．

$F(B,\Sigma)$ の元は，B の元を原子テストとし，Σ の元を原子コマンドとする while プログラムの文面の，「等価なプログラムは等しい」ことを表わす合同関係に関する同値類である．そこで，以下では $F(B,\Sigma)$ の元をwhile プログラムと呼ぶことにする．

while 代数とそれらの間の準同型のなす圏を **While** と書くと，上記の自由生成は次のようにいいかえることができる．

定理 2.2 while 代数をその二つの台集合の組へ写す，**While** から **Set** $\times$ **Set** への忘却函手 U: **While** $\to$ **Set** $\times$ **Set** は左随伴 F を持つ．

定義 2.3 $F(B,\Sigma)$ から while 代数 **W** への while 代数準同型を，B を原子テストとし，Σ を原子コマンドとする while プログラムの **W** における意味解釈と呼ぶ．

定理 2.2 により，**W** における while プログラムの意味解釈は，B から $W_{\mathbf{Test}}$ への写像と Σ から $W_{\mathbf{Com}}$ への写像の対により一意的にきまる．

while 代数におけるソート **Com** の値がコマンドの意味領域，**Test** の値が条件判定の意味領域と考えると，以上のような意味解釈の与え方は，停止する while プログラムの意味として十分であると考えられる．しかし，停止しない while プログラムについては，意味をつぶしすぎる場合がある．while 代数では，while 文の意味が $W_{\mathbf{Test}} \times W_{\mathbf{Com}}$ 上の変換 $\Psi(b,c) = \mathbf{if}(b, c;\Psi(b,c), \mathbf{skip})$ の不動点であることを要求しているだけなので，最小不動点である場合もあれば最大不動点である場合もあり，その他の不動点である場合もある．とくに最小不動点である場合には，停止しない while 文はすべて abort と一致しなければならず，意味対象が一つにつぶれてしまう．

3 テスト付クリーニ代数

定義 3.1 (半環) 半環とは二つの定数 0，1 と二項演算子 +（和），$\cdot$（積）を備えた集合 S で $(S,0,+)$ は可換単（*commutative monoid*），$(S,1,\cdot)$ は単であり，しかも以下の条件を満足するようなものである．

$$x \cdot (y+z) = x \cdot y + x \cdot z$$
$$(x+y) \cdot z = x \cdot z + y \cdot z$$
$$x \cdot 0 = 0 = 0 \cdot x$$

+ がさらに冪等律 $x + x = x$ を満たすものを冪等半環（*idempotent semiring*）と呼ぶ．

(独) 産業技術総合研究所 情報処理研究部門 情報科学連携研究体,
C.R.T. of Informatics, AIST, E-mail: yoshiki@ni.aist.go.jp [†], hitoshi.furusawa@aist.go.jp [‡]

注意 3.2 冪等律を満たす可換単は，半束に他ならないが，よく知られているように，半束では

$$x \leq y \iff x + y = y$$

によって半順序 $\leq$ を定義することができる．以下では冪等半環に関してこの方法で定める半順序 $\leq$ を用いる．

定義 3.3 (クリーニ代数 [1]) クリーニ代数とは $(K, 0, 1, +, \cdot, ^*)$ で，$(K, 0, 1, +, \cdot)$ が冪等半環であり，* は K 上の単項演算で以下の四つの条件を満足するようなものである．

$$\begin{aligned} 1 + (p \cdot p^*) &= p^* \\ 1 + (p^* \cdot p) &= p^* \\ q + (p \cdot r) \leq r &\Longrightarrow p^* \cdot q \leq r \\ q + (r \cdot p) \leq r &\Longrightarrow q \cdot p^* \leq r \end{aligned}$$

定義 3.4 (テスト付きクリーニ代数 [3]) テスト付きクリーニ代数はブール代数 $\mathbf{B} = (B, 0_B, 1_B, +_B, \cdot_B, \neg)$，クリーニ代数 $\mathbf{K} = (K, 0_K, 1_K, +_K, \cdot_K, ^*)$，$B$ から K への写像 j: $B \to K$ で 0，1，+，$\cdot$ を保つもの，の三つ組 $(\mathbf{B} \xrightarrow{j} \mathbf{K})$ である．K の元をコマンド，B の元をテストと呼ぶ．

テスト付きクリーニ代数は Kozen[2] によって導入されたが，ここでは著者らが [3] において拡張した多ソート代数としての定義を採用する．

テスト付きクリーニ代数 $(\mathbf{K}, \mathbf{B}, j)$ におけるソート **Test** の値を $\mathbf{B}$，演算子 **tt**，**ff**，$\neg$，$\wedge$，$\vee$ の値をそれぞれ 1_B，0_B，$\neg$，$\cdot_B$，$+_B$ とし，ソート **Com** の値を $\mathbf{K}$，演算子 **abort**，**skip**，**;**，**[]**，**if**，**while** の値をそれぞれ 0_K，1_K，$\cdot_K$，$+_K$，$[(b, c, c') \mapsto j(b) \cdot_K c +_K j(\neg b) \cdot_K c']$，$[(b, c) \mapsto (j(b) \cdot_K c)^* \cdot_K j(\neg b)]$ とすることにより，**while** 代数が得られる．$(\mathbf{K}, \mathbf{B}, j)$ をこの **while** 代数に写すことにより，テスト付きクリーニ代数から **while** 代数への忠実函手 $\mathcal{I}$: **Kat** $\to$ **While** を定めることができる．定義 2.3 と $\mathcal{I}$ を組み合わせて，テスト付きクリーニ代数における意味解釈を次のように定める．

定義 3.5 $\mathbf{T}$ をテスト付きクリーニ代数とするとき，B を原子テストとし，Σ を原子コマンドとする **while** プログラムの **while** 代数 $\mathcal{I}(\mathbf{T})$ における意味解釈を $\mathbf{T}$ における意味解釈と呼ぶ．

この意味解釈は Kozen[2] で与えられている **while** プログラムの解釈に一致する．定理 2.2 により，$\mathbf{T}$ における意味解釈は，B から $\mathbf{B}$ への写像と Σ から $\mathbf{K}$ への写像の対により，一意的に定まる．

筆者ら [3] は，単位クォンテール (unital quantale) の直和，良く知られている自由ブール代数の構成などを用いて，集合 B と Σ からテスト付きクリーニ代数 $\mathcal{Q}_{B,\Sigma}$ の構成を与えた．ここでは，$\mathcal{Q}_{B,\Sigma}$ の要素毎の明示的な構成を与える．

構成 3.6 $\mathcal{Q}_{B,\Sigma} = (\mathbf{B} \xrightarrow{j} \mathbf{K})$ は以下のように構成される．$\mathbf{B}$ は，B によって自由生成されるブール代数であり，それはよく知られているように，B の二階の冪集合 $P(P(B))$ がつくるブール代数である．$\mathcal{Q}_{B,\Sigma}$ のコマンドがつくるクリーニ代数 $\mathbf{K} = (K, 0_K, 1_K, +_K, \cdot_K, ^*)$ は次のように定義される．K は $B \uplus B \uplus \Sigma$ の元を並べた有限列（空列 ϵ を含む）の全体がなす集合

$$X_0 = \{\, x_1 \ldots x_n \mid x_j \in B \uplus B \uplus \Sigma,\ 0 \leq n \}$$

の冪集合 $P(X_0)$ を $\{\, x_1 \ldots x_n \mid x_j \in B \uplus B,\ 0 \leq n \} \equiv \{\epsilon\}$，$\{\, a \cdot \neg a \} \equiv \emptyset$，$\{\, a \cdot b \} \equiv \{\, b \cdot a \}$，$\{\, a \cdot a \} \equiv \{\, a \}$（ただし，$a, b \in B$）で生成されるクリーニ代数合同関係 $\equiv$ で割って得られる商集合である．つまり，

$$X = P(X_0)/\equiv$$

$\mathbf{K}$ の演算は，$U \in P(X_0)$ の $\equiv$ に関する同値類を $[U]$ と書くことにすると，

$$\begin{aligned} 0_K = [\emptyset] \qquad [U] +_K [V] &= [U \cup V] \\ [U] \cdot_K [V] &= [\{\, uv \mid u \in U,\ v \in V \}] \\ [U]^* &= [\{\, u^n \mid u \in B,\ 0 \leq n \}] \end{aligned}$$

である．最後に，j は

$$\begin{aligned} &P(P(B)) \ni \mathcal{A} \mapsto \\ &\qquad [\{\, x_1 \ldots x_n \mid x_j \in A \uplus (B \setminus A),\ 0 \leq n,\ A \in \mathcal{A} \}] \end{aligned}$$

である．

さて，**while** プログラムの状態は，用意されたテストの値によって完全に決まる．したがって，B 上の命題をシステムの状態と見なすことができる．一方，Σ 上の語をシステムの状態遷移と見なすことができる．このような立場をとると，構成 3.6 における X_0 の元はシステムの連とみなすことができ，$\mathcal{Q}_{B,\Sigma}$ のコマンドは連の集合の同値類である．さらに，定義 3.5 を組みあわせて，B を原子テストとし，Σ を原子コマンドとする **while** プログラムのテスト付きクリーニ代数における意味解釈で，特にテスト付きクリーニ代数として $\mathcal{Q}_{B,\Sigma}$ を考えると，**while** プログラムの，連を用いた意味解釈が得られるのである．

参考文献

[1] Dexter Kozen. A completeness theorem for kleene algebras and the algebra of regular events. *Information and Computation*, Vol. 110, pp. 366–390, 1994.

[2] Dexter Kozen. Kleene algebra with tests. *ACM Transactions on Programming Languages and Systems*, Vol. 19, No. 3, pp. 427–443, May 1997.

[3] 木下佳樹, 古澤仁. テスト付きクリーニ代数の準代数構造. 日本ソフトウェア科学会第 19 回大会 (2002 年度) 論文集に掲載予定, 2002.