ソフトウェア基礎論 配布資料(4)

五十嵐 淳

平成 15 年 11 月 4 日

5 IMP の表示的意味論

5.1 動機づけ — 操作的意味論への考察

操作的意味論の特徴:

- 実装に近い記述 — 言語処理系の仕様
- 評価/実行関係の定義に任意性

  初期状態と終了状態を伴なう関係ではなく，計算途中の段階を明示した関係で定義することもできた．(small-step semantics)
- 評価/実行関係にプログラム文面が現れる: 異なる言語で書かれたプログラム同士の比較 (性質の議論) には向いていない？

表示的意味論へ: 操作的意味論でのプログラム等価 ($c_0 \sim c_1$) の概念に基づき，プログラムの意味をより抽象的に捉える:

プログラム = 開始状態と終了状態との関係 (部分関数)

つまり,

プログラムの**表示**($denotation$) $\in \Sigma \rightharpoonup \Sigma$

5.2 表示的意味論

意味領域と意味関数 プログラムの表示が属する集合を**意味領域**($semantic\ domain$)，プログラムを構成する集合に対しその表示を対応づける関数を**意味関数**($semantic\ function$) と呼ぶ．ここでは，$a \in \mathbf{Aexp}$, $b \in \mathbf{Bexp}$, $c \in \mathbf{Com}$ に対し，それぞれ，$\mathcal{A}, \mathcal{B}, \mathcal{C}$ という意味関数を定義してゆく．それぞれの意味領域は以下に示される．

$$\begin{aligned} \mathcal{A}[\![a]\!] &\in \Sigma \to \mathbf{Num} \\ \mathcal{B}[\![b]\!] &\in \Sigma \to \mathbf{T} \\ \mathcal{C}[\![c]\!] &\in \Sigma \rightharpoonup \Sigma \end{aligned}$$

ここで $\mathcal{A}[\![\cdot]\!]$ 自体は $\mathbf{Aexp} \to (\Sigma \to \mathbf{Num})$ の元，つまり，算術式から関数に対応づける関数である，と考えられる．

各意味関数は，構造的帰納法によって定義する．(配布資料 (3) 3.5 参照) この際，操作的意味論の評価/実行関係と「同じ」意味を示すように定義していく．最終的には表示的意味論と操作的意味論が一致することを定理として示す．

算術式の表示

$$
\begin{aligned}
\mathcal{A}[\![n]\!] &= \{(\sigma, n) \mid \sigma \in \Sigma\} \\
\mathcal{A}[\![X]\!] &= \{(\sigma, \sigma(X)) \mid \sigma \in \Sigma\} \\
\mathcal{A}[\![a_0 + a_1]\!] &= \{(\sigma, n) \mid (\sigma, n_0) \in \mathcal{A}[\![a_0]\!] \,\&\, (\sigma, n_1) \in \mathcal{A}[\![a_1]\!] \,\&\, n \text{ は } n_0 \text{ と } n_1 \text{ の和 }\} \\
\mathcal{A}[\![a_0 - a_1]\!] &= \{(\sigma, n) \mid (\sigma, n_0) \in \mathcal{A}[\![a_0]\!] \,\&\, (\sigma, n_1) \in \mathcal{A}[\![a_1]\!] \,\&\, n \text{ は } n_0 \text{ と } n_1 \text{ の差 }\} \\
\mathcal{A}[\![a_0 \times a_1]\!] &= \{(\sigma, n) \mid (\sigma, n_0) \in \mathcal{A}[\![a_0]\!] \,\&\, (\sigma, n_1) \in \mathcal{A}[\![a_1]\!] \,\&\, n \text{ は } n_0 \text{ と } n_1 \text{ の積 }\}
\end{aligned}
$$

右辺は，あたかも関係 ($\Sigma \times \mathbf{Num}$ の部分集合) であるかのように定義しているが，$\mathcal{A}[\![a]\!]$ が (全値) 関数であることは a の構造に関する帰納法で容易に証明できる．

意味関数 $\mathcal{A}[\![a]\!]$ を σ に適用して得られる整数を $\mathcal{A}[\![a]\!]\sigma$ と表記する．例えば，任意の状態 σ に対して

$$\mathcal{A}[\![3 + 5]\!]\sigma = \mathcal{A}[\![3]\!]\sigma + \mathcal{A}[\![5]\!]\sigma = 3 + 5 = 8$$

である．[1]

真偽値式の表示

$$
\begin{aligned}
\mathcal{B}[\![\mathbf{true}]\!] &= \{(\sigma, \mathbf{true}) \mid \sigma \in \Sigma\} \\
\mathcal{B}[\![\mathbf{false}]\!] &= \{(\sigma, \mathbf{false}) \mid \sigma \in \Sigma\} \\
\mathcal{B}[\![a_0 = a_1]\!] &= \{(\sigma, \mathbf{true}) \mid \sigma \in \Sigma \,\&\, \mathcal{A}[\![a_0]\!]\sigma \text{ と } \mathcal{A}[\![a_1]\!]\sigma \text{ が等しい }\} \cup \\
&\quad \{(\sigma, \mathbf{false}) \mid \sigma \in \Sigma \,\&\, \mathcal{A}[\![a_0]\!]\sigma \text{ と } \mathcal{A}[\![a_1]\!]\sigma \text{ は等しくない }\} \\
\mathcal{B}[\![a_0 \le a_1]\!] &= \{(\sigma, \mathbf{true}) \mid \sigma \in \Sigma \,\&\, \mathcal{A}[\![a_0]\!]\sigma \text{ は } \mathcal{A}[\![a_1]\!]\sigma \text{ 以下である }\} \cup \\
&\quad \{(\sigma, \mathbf{false}) \mid \sigma \in \Sigma \,\&\, \mathcal{A}[\![a_0]\!]\sigma \text{ は } \mathcal{A}[\![a_1]\!]\sigma \text{ 以下ではない }\} \\
\mathcal{B}[\![\neg b_0]\!] &= \{(\sigma, \mathbf{false}) \mid \sigma \in \Sigma \,\&\, (\sigma, \mathbf{true}) \in \mathcal{B}[\![b_0]\!]\} \cup \\
&\quad \{(\sigma, \mathbf{true}) \mid \sigma \in \Sigma \,\&\, (\sigma, \mathbf{false}) \in \mathcal{B}[\![b_0]\!]\} \\
\mathcal{B}[\![b_0 \wedge b_1]\!] &= \{(\sigma, \mathbf{true}) \mid \sigma \in \Sigma \,\&\, (\sigma, \mathbf{true}) \in \mathcal{B}[\![b_0]\!] \,\&\, (\sigma, \mathbf{true}) \in \mathcal{B}[\![b_1]\!]\} \cup \\
&\quad \{(\sigma, \mathbf{false}) \mid \sigma \in \Sigma \,\&\, (\sigma, t_0) \in \mathcal{B}[\![b_0]\!] \,\&\, (\sigma, t_1) \in \mathcal{B}[\![b_1]\!] \,\&\, (t_0 = \mathbf{false} \text{ or } t_1 = \mathbf{false})\} \\
\mathcal{B}[\![b_0 \vee b_1]\!] &= \{(\sigma, \mathbf{true}) \mid \sigma \in \Sigma \,\&\, (\sigma, t_0) \in \mathcal{B}[\![b_0]\!] \,\&\, (\sigma, t_1) \in \mathcal{B}[\![b_1]\!] \,\&\, (t_0 = \mathbf{true} \text{ or } t_1 = \mathbf{true})\} \cup \\
&\quad \{(\sigma, \mathbf{false}) \mid \sigma \in \Sigma \,\&\, (\sigma, \mathbf{false}) \in \mathcal{B}[\![b_0]\!] \,\&\, (\sigma, \mathbf{false}) \in \mathcal{B}[\![b_1]\!]\}
\end{aligned}
$$

[1] 意味関数の引数に現れる $+$ と外側の $+$ は別物 (前者は **IMP** の世界での記号，後者はメタ言語における和を計算する演算子) であるので注意．

$\mathcal{A}[\![a]\!]$ と同様，$\mathcal{B}[\![b]\!]$ が実際には関数であることは b の構造に関する帰納法で証明可能であるので，以降では $\mathcal{B}[\![b]\!]\sigma$ という表記を用いる．

コマンドの表示　まずは，**while** 以外の定義を示す．

$$\begin{aligned}
\mathcal{C}[\![\mathbf{skip}]\!] &= \{(\sigma,\sigma) \mid \sigma \in \Sigma\} \\
\mathcal{C}[\![X := a]\!] &= \{(\sigma,\sigma[n/X]) \mid \sigma \in \Sigma \,\&\, n = \mathcal{A}[\![a]\!]\sigma\} \\
\mathcal{C}[\![c_0; c_1]\!] &= \mathcal{C}[\![c_1]\!] \circ \mathcal{C}[\![c_0]\!] \quad \text{(関係の合成)} \\
\mathcal{C}[\![\mathbf{if}\ b\ \mathbf{then}\ c_0\ \mathbf{else}\ c_1]\!] &= \{(\sigma,\sigma') \mid \mathcal{B}[\![b]\!]\sigma = \mathbf{true} \,\&\, (\sigma,\sigma') \in \mathcal{C}[\![c_0]\!]\} \cup \\
&\quad \{(\sigma,\sigma') \mid \mathcal{B}[\![b]\!]\sigma = \mathbf{false} \,\&\, (\sigma,\sigma') \in \mathcal{C}[\![c_1]\!]\}
\end{aligned}$$

while コマンドの表示は，実行規則から素直に定義を導こうとしても帰納的な定義にならない．(なぜか？) そのため，プログラムの等価関係から導く．操作的意味論において，$w \equiv \mathbf{while}\ b\ \mathbf{do}\ c$ として

$$w \sim \mathbf{if}\ b\ \mathbf{then}\ c; w\ \mathbf{else}\ \mathbf{skip}$$

が成立したことから，$\mathcal{C}[\![w]\!]$ と $\mathcal{C}[\![\mathbf{if}\ b\ \mathbf{then}\ c; w\ \mathbf{else}\ \mathbf{skip}]\!]$ が等しくなるべきである．つまり，

$$\begin{aligned}
\mathcal{C}[\![w]\!] &= \{(\sigma,\sigma') \mid \mathcal{B}[\![b]\!]\sigma = \mathbf{true} \,\&\, (\sigma,\sigma') \in \mathcal{C}[\![c; w]\!]\} \cup \\
&\quad \{(\sigma,\sigma') \mid \mathcal{B}[\![b]\!]\sigma = \mathbf{false} \,\&\, (\sigma,\sigma') \in \mathcal{C}[\![\mathbf{skip}]\!]\} \\
&= \{(\sigma,\sigma') \mid \mathcal{B}[\![b]\!]\sigma = \mathbf{true} \,\&\, (\sigma,\sigma') \in \mathcal{C}[\![w]\!] \circ \mathcal{C}[\![c]\!]\} \cup \\
&\quad \{(\sigma,\sigma) \mid \mathcal{B}[\![b]\!]\sigma = \mathbf{false}\}
\end{aligned}$$

が成立するべきである．$\mathcal{C}[\![c]\!]$ を γ, $\mathcal{B}[\![b]\!]$ を β と書くと，$\mathcal{C}[\![w]\!]$ は

$$\begin{aligned}
\varphi &= \{(\sigma,\sigma') \mid \beta(\sigma) = \mathbf{true} \,\&\, (\sigma,\sigma') \in \varphi \circ \gamma\} \cup \\
&\quad \{(\sigma,\sigma) \mid \beta(\sigma) = \mathbf{false}\}
\end{aligned}$$

という「方程式」を φ に関して解いた解であることが求められる．さて，Γ を

$$\begin{aligned}
\Gamma(\varphi) &\stackrel{\text{def}}{=} \{(\sigma,\sigma') \mid \beta(\sigma) = \mathbf{true} \,\&\, (\sigma,\sigma') \in \varphi \circ \gamma\} \cup \\
&\quad \{(\sigma,\sigma) \mid \beta(\sigma) = \mathbf{false}\} \\
&= \{(\sigma,\sigma') \mid \beta(\sigma) = \mathbf{true} \,\&\, (\sigma,\sigma'') \in \gamma \,\&\, (\sigma'',\sigma') \in \varphi\} \cup \\
&\quad \{(\sigma,\sigma) \mid \beta(\sigma) = \mathbf{false}\}
\end{aligned}$$

という $\varphi(\in \Sigma \rightharpoonup \Sigma)$ から $\Gamma(\varphi)$ を返す関数と定義すると，方程式の解は Γ の不動点を求めることと一致する．この不動点は Γ に対応する規則インスタンスがあることを示せば，存在することがいえる．規則インスタンスの集合 R を

$$R \stackrel{\text{def}}{=} \{((\sigma'',\sigma')/(\sigma,\sigma')) \mid \beta(\sigma) = \mathbf{true} \,\&\, (\sigma,\sigma'') \in \gamma\} \cup \{(\emptyset/(\sigma,\sigma)) \mid \beta(\sigma) = \mathbf{false}\}$$

とすると，Γ は R から導かれる関数 $\widehat{R}$ と一致することが確かめられ，最小不動点 $fix(\widehat{R})$ が存在することがわかる．この最小不動点を **while** コマンドの表示とする．つまり，

$$\begin{aligned}\mathcal{C}[\![\textbf{while } b \textbf{ do } c]\!] &= fix(\Gamma)\\ \text{ただし } \Gamma(\varphi) &= \{(\sigma,\sigma') \mid \mathcal{B}[\![b]\!]\sigma = \textbf{true} \,\&\, (\sigma,\sigma') \in \varphi \circ \mathcal{C}[\![c]\!]\} \cup\\ &\quad \{(\sigma,\sigma) \mid \mathcal{B}[\![b]\!]\sigma = \textbf{false}\}\end{aligned}$$

Γ の不動点が他にある (かもしれない) 中で,「最小」不動点をとる理由は，操作的意味論との等価性を証明する部分で明らかになる．

算術式，真偽値式の意味関数と同様 $\mathcal{C}[\![c]\!]$ が部分関数であることが c の構造に関する帰納法で証明できる．

このようにして定義された意味関数は算術式やコマンドの構造に関する帰納法を用いて定義された．つまり，あるコマンドの表示はその部分コマンドの表示から求まるものである，という性質 (compositionality) が成立する．

5.3 ふたつの意味論の等価性

補題 5.1 任意の $a \in \textbf{Aexp}$ に対して，

$$\mathcal{A}[\![a]\!] = \{(\sigma, n) \mid \langle a, \sigma\rangle \to n\}$$

が成立する．

補題 5.2 任意の $b \in \textbf{Bexp}$ に対して，

$$\mathcal{B}[\![b]\!] = \{(\sigma, t) \mid \langle b, \sigma\rangle \to t\}$$

が成立する．

定理 5.3 任意の $c \in \textbf{Com}$ に対して，

$$\mathcal{C}[\![c]\!] = \{(\sigma, \sigma') \mid \langle c, \sigma\rangle \to \sigma'\}$$

が成立する．