ソフトウェア基礎論 配布資料(2)

五十嵐 淳

平成 15 年 10 月 14 日

2 操作的意味論

2.1 対象言語 – IMP

2.1.1 IMP の特徴

- 整数，真偽値のみを扱う単純な**命令型言語**(*imperative language*) である．
- 変数は整数のみを格納できる．
- 代入文，while 文などを並べてプログラムを構成する．

2.1.2 IMP の文法

文法に関する集合

- 整数の集合: $\mathbf{Num} \stackrel{\text{def}}{=} \{\ldots, -3, -2, -1, 0, 1, 2, 3, 4, \ldots\}$
- 真偽値の集合: $\mathbf{T} \stackrel{\text{def}}{=} \{\mathbf{true}, \mathbf{false}\}$
- ロケーションの集合: **Loc**
- 算術式の集合: **Aexp**
- 真偽値式の集合: **Bexp**
- コマンドの集合: **Com**

Loc はプログラム変数 (計算機のメモリアドレス) の予め与えられた集合である．正確な要素は特に明示しないが，英字で始まる英数字列が要素に含まれるとしておく．以下では，**Aexp**, **Bexp**, **Com** を定義していく．

メタ変数と BNF 記法による文法定義: 文法 = 各集合の要素がどのように構成されるかの記述:

例: a_0 と a_1 が算術式 (**Aexp** の要素) ならば，$a_0 + a_1$ も算術式である．

a_0, a_1 は，定義する側の言語—メタ言語，ここでは日本語—で，**IMP** の文法に関する集合の要素を示すための変数で，**メタ変数**(*metavariable*) と呼ばれる．**IMP** のメタ変数は以下の通り．

- n, m は **Num** 上を動くメタ変数である.
- t は **T** 上を動くメタ変数である.
- X, Y は **Loc** 上を動くメタ変数である.
- a は **Aexp** 上を動くメタ変数である.
- b は **Bexp** 上を動くメタ変数である.
- c は **Com** 上を動くメタ変数である.

これらに添字，プライム ($'$) をつけたものも使用する.

集合 $\mathbf{Aexp}, \mathbf{Bexp}, \mathbf{Com}$ の BNF(*Backus-Naur form*) による定義:

$$\begin{aligned} a &::= n \mid X \mid a_0 + a_1 \mid a_0 - a_1 \mid a_0 \times a_1 \\ b &::= \mathbf{true} \mid \mathbf{false} \mid a_0 = a_1 \mid a_0 \leq a_1 \mid \neg b \mid b_0 \wedge b_1 \mid b_0 \vee b_1 \\ c &::= \mathbf{skip} \mid X := a \mid c_0; c_1 \mid \mathbf{if}\ b\ \mathbf{then}\ c_0\ \mathbf{else}\ c_1 \mid \mathbf{while}\ b\ \mathbf{do}\ c \end{aligned}$$

抽象文法と具象文法: 構文木構造を規定する**抽象文法**(*abstract syntax*) と，文字列から構文解析するのに必要な情報 (括弧づけ，演算子の優先順位) を含んだ文法である**具象文法**(*concrete syntax*).

Syntactic equality $\equiv$: e_0, e_1 を同じ文法集合の要素とする．これらが同一の要素であるとき $e_0 \equiv e_1$ と記述する.

2.2 算術式の評価

状態と評価関係: メモリ**状態**(*states*) を $\sigma \in \Sigma = \mathbf{Loc} \to \mathbf{Num}$ とする．$\sigma(X)$ はメモリアドレス X に格納された (整数) 値.

算術式の**評価関係**(*evaluation relation*):

$$\langle a, \sigma \rangle \to n$$

「算術式 a は σ の下で n に評価される」と読む．(**Aexp**, Σ, **Num** 間の三項関係としてもとらえられる．)

規則と導出による関係の定義 ある関係 (特に無限の大きさ) を定義するのに，その関係を満す組を，**規則**(*rule*) を使って導くことがよく行われる．その方法では，ある関係が成立することを示すのに，規則をいくつか組み合わせて，**導出**(*derivation*) という「関係が成り立つ証拠」を示すことになる.

規則に関するいくつかの概念:

- 規則は

$$\frac{A_1 \qquad \cdots \qquad A_n}{B} \qquad \text{(Rule-Name)}$$

という形 (n は 0 以上の有限の整数) で書かれる．Rule-Name を規則の名前，各 A_i を規則の**前提**(*premise*)，B を規則の**結論**(*conclusion*) という．前提が 0 個であるような規則を**公理**(*axiom*) という．以下で具体的な規則をみるとわかるが，通常，A_i や B はメタ変数を含む表現であるため，規則を使用する際にはこれらを具体化する必要がある．(そのため，規則は「規則スキーム (図式)」と呼ぶほうが的確である．)

- 規則に現れるメタ変数を具体的な値で置き換えたものを**規則のインスタンス**(*rule instance*) と呼ぶ.

以下，導出を $\mathcal{D}$ で表す．導出にはその結論が同時に定義される．導出の構成方法は以下の通り:

- 導出 $\mathcal{D}_1, \ldots, \mathcal{D}_n$ があってそれらの結論が $A_1, \ldots, A_n$ とする．ある規則のインスタンスがあって，それらの前提が $A_1, \ldots, A_n$，結論が B であるとき，

$$\frac{\mathcal{D}_1 \qquad \cdots \qquad \mathcal{D}_n}{B}$$

は導出でありその結論は B である．特に，規則が公理の場合，そのインスタンスを結論とする導出が他の導出を必要とすることなく得られる.

通常「規則を用いて関係を定義する」といった場合，その関係が成り立つのは導出が存在する場合のみである.

算術式の評価関係の導出規則

$$\frac{}{\langle n, \sigma\rangle \to n} \qquad \text{(EA-Num)}$$

$$\frac{}{\langle X, \sigma\rangle \to \sigma(X)} \qquad \text{(EA-Loc)}$$

$$\frac{\langle a_0, \sigma\rangle \to n_0 \qquad \langle a_1, \sigma\rangle \to n_1 \qquad (n \text{ は } n_0 \text{ と } n_1 \text{ の和})}{\langle a_0 + a_1, \sigma\rangle \to n} \qquad \text{(EA-Sum)}$$

$$\frac{\langle a_0, \sigma\rangle \to n_0 \qquad \langle a_1, \sigma\rangle \to n_1 \qquad (n \text{ は } n_0 \text{ と } n_1 \text{ の差})}{\langle a_0 - a_1, \sigma\rangle \to n} \qquad \text{(EA-Sub)}$$

$$\frac{\langle a_0, \sigma\rangle \to n_0 \qquad \langle a_1, \sigma\rangle \to n_1 \qquad (n \text{ は } n_0 \text{ と } n_1 \text{ の積})}{\langle a_0 \times a_1, \sigma\rangle \to n} \qquad \text{(EA-Mul)}$$

() で囲まれた前提は，上の形式的な扱いとしての前提ではなく，規則のインスタンスを作る際のメタ変数の値についての付帯条件である.

評価関係を用いた，算術式の同値関係

$$a_0 \sim a_1 \stackrel{\text{def}}{=} (\forall n \in \mathbf{Num}.\forall \sigma \in \Sigma.\langle a_0, \sigma\rangle \to n \iff \langle a_1, \sigma\rangle \to n)$$

2.3 真偽値式の評価

真偽値式の評価関係を $\langle b, \sigma\rangle \to t$ と表記し「真偽値式 b は σ の下で t に評価される」と読む．(集合 **Bexp**, Σ, **T** 間の三項関係としてもとらえられる．)

導出規則

$$\frac{}{\langle \mathbf{true}, \sigma\rangle \to \mathbf{true}} \quad \text{(EB-True)}$$

$$\frac{}{\langle \mathbf{false}, \sigma\rangle \to \mathbf{false}} \quad \text{(EB-False)}$$

$$\frac{\langle a_0, \sigma\rangle \to n_0 \qquad \langle a_1, \sigma\rangle \to n_1 \qquad (n_0 \text{ と } n_1 \text{ が等しい})}{\langle a_0 = a_1, \sigma\rangle \to \mathbf{true}} \quad \text{(EB-Eq)}$$

$$\frac{\langle a_0, \sigma\rangle \to n_0 \qquad \langle a_1, \sigma\rangle \to n_1 \qquad (n_0 \text{ と } n_1 \text{ が等しくない})}{\langle a_0 = a_1, \sigma\rangle \to \mathbf{false}} \quad \text{(EB-NEq)}$$

$$\frac{\langle a_0, \sigma\rangle \to n_0 \qquad \langle a_1, \sigma\rangle \to n_1 \qquad (n_0 \text{ が } n_1 \text{ 以下である})}{\langle a_0 \le a_1, \sigma\rangle \to \mathbf{true}} \quad \text{(EB-Leq)}$$

$$\frac{\langle a_0, \sigma\rangle \to n_0 \qquad \langle a_1, \sigma\rangle \to n_1 \qquad (n_0 \text{ が } n_1 \text{ 以下ではない})}{\langle a_0 \le a_1, \sigma\rangle \to \mathbf{false}} \quad \text{(EB-NLeq)}$$

$$\frac{\langle b, \sigma\rangle \to \mathbf{true}}{\langle \neg b, \sigma\rangle \to \mathbf{false}} \quad \text{(EB-Not1)}$$

$$\frac{\langle b, \sigma\rangle \to \mathbf{false}}{\langle \neg b, \sigma\rangle \to \mathbf{true}} \quad \text{(EB-Not2)}$$

$$\frac{\langle b_0, \sigma\rangle \to t_0 \qquad \langle b_1, \sigma\rangle \to t_1 \qquad (t_0 \equiv \mathbf{true} \,\&\, t_1 \equiv \mathbf{true} \text{ ならば } t \equiv \mathbf{true} \text{ さもなくば } t \equiv \mathbf{false})}{\langle b_0 \wedge b_1, \sigma\rangle \to t} \quad \text{(EB-And)}$$

$$\frac{\langle b_0, \sigma\rangle \to t_0 \qquad \langle b_1, \sigma\rangle \to t_1 \qquad (t_0 \equiv \mathbf{true} \text{ or } t_1 \equiv \mathbf{true} \text{ ならば } t \equiv \mathbf{true} \text{ さもなくば } t \equiv \mathbf{false})}{\langle b_0 \vee b_1, \sigma\rangle \to t} \quad \text{(EB-Or)}$$

評価関係を用いた，真偽値式の同値関係

$$b_0 \sim b_1 \stackrel{\text{def}}{=} (\forall t \in \mathbf{T}. \forall \sigma \in \Sigma. \langle b_0, \sigma\rangle \to t \iff \langle b_1, \sigma\rangle \to t)$$

2.4 命令の実行

コマンドの**実行**(*execution*) 関係:

$$\langle c, \sigma \rangle \to \sigma'$$

「コマンド c は σ の下で実行すると終了して終了時の状態は σ' に評価される」と読む. (**Com**, Σ, Σ 間の三項関係としてもとらえられる.)

X に n が格納され, その他のロケーションには σ と同じ整数が格納されている状態を $\sigma[n/X]$ と書き, 以下のように定義する.

$$(\sigma[n/X])(Y) = \begin{cases} n & \text{if } Y = X \\ \sigma(Y) & \text{if } Y \neq X \end{cases}$$

導出規則

$$\frac{}{\langle \mathbf{skip}, \sigma \rangle \to \sigma} \quad \text{(EC-Skip)}$$

$$\frac{\langle a, \sigma \rangle \to n}{\langle X := a, \sigma \rangle \to \sigma[n/X]} \quad \text{(EC-Asgn)}$$

$$\frac{\langle c_0, \sigma \rangle \to \sigma'' \qquad \langle c_1, \sigma'' \rangle \to \sigma'}{\langle c_0; c_1, \sigma \rangle \to \sigma'} \quad \text{(EC-Seq)}$$

$$\frac{\langle b, \sigma \rangle \to \mathbf{true} \qquad \langle c_0, \sigma \rangle \to \sigma'}{\langle \mathbf{if}\ b\ \mathbf{then}\ c_0\ \mathbf{else}\ c_1, \sigma \rangle \to \sigma'} \quad \text{(EC-If1)}$$

$$\frac{\langle b, \sigma \rangle \to \mathbf{false} \qquad \langle c_1, \sigma \rangle \to \sigma'}{\langle \mathbf{if}\ b\ \mathbf{then}\ c_0\ \mathbf{else}\ c_1, \sigma \rangle \to \sigma'} \quad \text{(EC-If2)}$$

$$\frac{\langle b, \sigma \rangle \to \mathbf{false}}{\langle \mathbf{while}\ b\ \mathbf{do}\ c, \sigma \rangle \to \sigma} \quad \text{(EC-While1)}$$

$$\frac{\langle b, \sigma \rangle \to \mathbf{true} \qquad \langle c, \sigma \rangle \to \sigma'' \qquad \langle \mathbf{while}\ b\ \mathbf{do}\ c, \sigma'' \rangle \to \sigma'}{\langle \mathbf{while}\ b\ \mathbf{do}\ c, \sigma \rangle \to \sigma'} \quad \text{(EC-While2)}$$

評価関係を用いた, コマンドの同値関係

$$c_0 \sim c_1 \stackrel{\text{def}}{=} (\forall \sigma, \sigma' \in \Sigma. \langle c_0, \sigma \rangle \to \sigma' \iff \langle c_1, \sigma \rangle \to \sigma')$$

2.5 簡単な性質の証明

定理 2.1 $w \equiv \mathbf{while}\ b\ \mathbf{do}\ c$ (但し $b \in \mathbf{Bexp}, c \in \mathbf{Com}$) とする. このとき,

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

が成立する.