ソフトウェア基礎論配布資料 (2)
算術式の言語

五十嵐 淳
京都大学 大学院情報学研究科知能情報学専攻
e-mail: igarashi@kuis.kyoto-u.ac.jp

平成 18 年 10 月 10 日

1 算術式の文法定義

自然数上の加算・乗算式の集合を算術式の集合 **Aexp** を定義する．構成要素は最小の自然数 `Z`, 「次の数」を示す `S`, 加算・乗算の `+`, `*` である．算術式は無限に存在するので，集合を厳密に定義するためには，要素を列挙するわけにはいかない．以下ではそのような集合を定義する方法をいくつか見る．

1.1 BNF 記法による定義

BNF 記法(*Backus-Naur form*) は，プログラミング言語の文法を定義する際の標準的な記法である．以下に実際の例を示すが，"::=" は「〜は以下のもので構成される」，"|" は「または」と読む．

1.1.1 定義: 算術式 (メタ変数 a) の集合 **Aexp** は以下の文法[1]で定義する．

$$a \in \mathbf{Aexp} ::= \texttt{Z} \mid \texttt{S(}a\texttt{)} \mid a \texttt{ + } a \mid a \texttt{ * } a$$

□

演算子の優先順位と抽象構文木　上の文法から，例えば `S(Z)` や `S(Z) + Z` は **Aexp** の要素である．これらを組み合わせて，`S(Z) + Z * S(Z)` も算術式である．しかし，`S(Z)` と `Z * S(Z)` を `+` で組み合わせても，(文字列として) 見た目が同じ算術式が得られる．別の言い方をすると，上の文法は，文字列からそれに対応する算術式が一意に得られないので曖昧である．より厳密には，上の文法は算術式を木構造として定義していると考えるのが正しい．

[1] 細かい違いだが $a \in \mathbf{Aexp} ::= \texttt{Z} \mid \texttt{S(}\mathbf{Aexp}\texttt{)} \mid \mathbf{Aexp} \texttt{ + } \mathbf{Aexp} \mid \mathbf{Aexp} \texttt{ * } \mathbf{Aexp}$ と記述する方法もある．

このような木構造は言語処理系で**抽象構文木**(*abstract syntax tree*) と呼ばれるものである．また，このような (文字列の解析のためではない) 文法を**抽象構文**(*abstract syntax*) と呼ぶ．

もちろん，上の例のような「生成の仕方」の違いを区別する必要はでてくるので適宜 (メタな記号である) “(” “)” を使用し，(S(Z) + Z) * S(Z) などと記述する．以下では，木構造として「等しい」ことを示すために $\equiv$ という記号を用いる．また，記号の優先度を指定して括弧を省略していく．ここでは，メタ言語の常識に合わせて * は + よりも強く結合し，+, * ともに左結合するとする．よって，

$$\begin{array}{rcrcrcl}
\texttt{S(Z) + Z * S(Z)} & \equiv & \texttt{S(Z) + (Z * S(Z))} & \not\equiv & \texttt{(S(Z) + Z) * S(Z)} \\
\texttt{Z + Z + Z} & \equiv & \texttt{(Z + Z) + Z} & \not\equiv & \texttt{Z + (Z + Z)} \\
\texttt{Z * Z * Z} & \equiv & \texttt{(Z * Z) * Z} & \not\equiv & \texttt{Z * (Z * Z)}
\end{array}$$

である．

1.2 帰納的な定義

上の BNF 記法は，より厳密には以下のような**帰納的定義**(*inductive definition*) の簡潔な記法と考えられる．

1.2.1 定義: 算術式の集合 **Aexp** は，以下の条件を満たす集合 A のうち最小のものである．

1. $\{\texttt{Z}\} \subseteq A$
2. もし $a \in A$ ならば $\{\texttt{S(}a\texttt{)}\} \subseteq A$
3. もし $a_1 \in A$ かつ $a_2 \in A$ ならば $\{a_1\ \texttt{+}\ a_2, a_1\ \texttt{*}\ a_2\} \subseteq A$

□

「最小の」というのは，上の条件を満たす集合はいくらでも考えられるので,「ゴミ」が入っていないことを保証するための条件である．例えば，上の条件を満たす集合があったときに，1, S(1), 1+1, . . . などを加えたような集合も，同じ条件を満たすので，最小性を言うことは非常に大事である．BNF 記法での定義ではわざわざ言わないことが多い．

上の「定義」は **Aexp** の満たすべき条件のみが記述されており，その存在は自明ではない[2]．**Aexp** が具体的がどのような集合かは以下のように与えられる．

まず，関数 F を以下のように定義する．

$$F(S) = \{\texttt{Z}\} \cup \{\texttt{S(}a\texttt{)} \mid a \in S\} \cup \{a_1\ \texttt{+}\ a_2, a_1\ \texttt{*}\ a_2 \mid a_1, a_2 \in S\}$$

そして，$F^n(S) = \underbrace{F(F(\cdots(F}_{n}(S))\cdots))$ $(F^0(S) = S)$ とすると，

$$\mathbf{Aexp} = \bigcup_{i \in \mathbf{Nat}} F^i(\emptyset)$$

と与えられる．この集合が上の定義の条件を満たしていることの証明はここでは割愛する．

[2] このような定義を超越的な定義と呼ぶ

1.3 帰納法による証明・帰納法による関数定義

自然数 (を表現する算術式) の帰納的な定義

$$n \in \mathbf{Nv} ::= \mathtt{Z} \mid \mathtt{S(}n\mathtt{)}$$

からは以下の数学的帰納法

$$(P(\mathtt{Z}) \,\&\, \forall n \in \mathbf{Nv}.(P(n) \Longrightarrow P(\mathtt{S(}n\mathtt{)}))) \Longrightarrow \forall n \in \mathbf{Nv}.P(n)$$

が導かれる．これと同様に帰納的に集合を定義すると，それに対応した**帰納法の証明原理**(*induction principle*) が導かれる．

算術式の構造に関する帰納法　a が算術式ということは，その構成の仕方より以下のどれかが成立する．

1. $a \equiv \mathtt{Z}$.
2. $a \equiv \mathtt{S(}a_0\mathtt{)}$ であり，a_0 は a より「小さい」算術式.
3. $a \equiv a_1 \mathtt{\ +\ } a_2$ であり，a_1, a_2 は a より「小さい」算術式.
4. $a \equiv a_1 \mathtt{\ *\ } a_2$ であり，a_1, a_2 は a より「小さい」算術式.

これより算術式の**構造に関する帰納法**(*structural induction*) の原理は以下のようになる．

1.3.1 定理 [算術式の構造に関する帰納法]: $\forall a \in \mathbf{Aexp}.P(a)$ を示すには,

1. $P(\mathtt{Z})$
2. $\forall a \in \mathbf{Aexp}.P(a) \Longrightarrow P(\mathtt{S(}a\mathtt{)})$
3. $\forall a_1, a_2 \in \mathbf{Aexp}.P(a_1) \,\&\, P(a_2) \Longrightarrow P(a_1 \mathtt{\ +\ } a_2)$
4. $\forall a_1, a_2 \in \mathbf{Aexp}.P(a_1) \,\&\, P(a_2) \Longrightarrow P(a_1 \mathtt{\ *\ } a_2)$

を示せばよい. □

また，帰納法の原理から,「帰納法による関数定義」が可能になる．例えば，算術式の大きさを示す関数 $size \in \mathbf{Aexp} \to \mathbf{Nat}$ は以下の 4 行だけで定義したことになる (以下の 4 式を満たすような関係はただひとつしかないということが帰納法の原理から証明できる).

$$\begin{aligned}
size(\mathtt{Z}) &= 1 \\
size(\mathtt{S(}a_0\mathtt{)}) &= size(a_0) + 1 \\
size(a_1 \mathtt{\ +\ } a_2) &= size(a_1) + size(a_2) + 1 \\
size(a_1 \mathtt{\ *\ } a_2) &= size(a_1) + size(a_2) + 1
\end{aligned}$$

1.3.2 例: $depth \in \mathbf{Aexp} \to \mathbf{Nat}$ を以下のように定義する.

$$\begin{aligned} depth(\mathtt{Z}) &= 1 \\ depth(\mathtt{S(}a_0\mathtt{)}) &= depth(a_0) + 1 \\ depth(a_1 \mathtt{\ +\ } a_2) &= \max(depth(a_1), depth(a_2)) + 1 \\ depth(a_1 \mathtt{\ *\ } a_2) &= \max(depth(a_1), depth(a_2)) + 1 \end{aligned}$$

このとき, $\forall a \in \mathbf{Aexp}.size(a) \leq 2^{depth(a)} - 1$ である.

Proof: 算術式の構造に関する帰納法で証明する.

1. $size(\mathtt{Z}) \leq 2^{depth(\mathtt{Z})} - 1$ は各関数の定義より明らか.
2. $size(a) \leq 2^{depth(a)} - 1$ を仮定して, $size(\mathtt{S(}a\mathtt{)}) \leq 2^{depth(\mathtt{S(}a\mathtt{)})} - 1$ を示す.

$$\begin{aligned} size(\mathtt{S(}a\mathtt{)}) &= size(a) + 1 \\ &\leq 2^{depth(a)} \leq 2^{depth(a)+1} - 1 \\ &\leq 2^{depth(\mathtt{S(}a\mathtt{)})} - 1 \end{aligned}$$

3. $size(a_1) \leq 2^{depth(a_1)} - 1$ と $size(a_2) \leq 2^{depth(a_2)} - 1$ を仮定して, $size(a_1 \mathtt{\ +\ } a_2) \leq 2^{depth(a_1 \mathtt{\ +\ } a_2)} - 1$ を示す.

$$\begin{aligned} size(a_1 \mathtt{\ +\ } a_2) &= size(a_1) + size(a_2) + 1 \\ &\leq 2^{depth(a_1)} - 1 + 2^{depth(a_2)} - 1 + 1 \\ &\leq 2^{\max(depth(a_1), depth(a_2))} + 2^{\max(depth(a_1), depth(a_2))} - 1 \\ &\leq 2^{depth(a_1 \mathtt{\ +\ } a_2)} - 1 \end{aligned}$$

4. $size(a_1) \leq 2^{depth(a_1)} - 1$ と $size(a_2) \leq 2^{depth(a_2)} - 1$ を仮定して, $size(a_1 \mathtt{\ *\ } a_2) \leq 2^{depth(a_1 \mathtt{\ *\ } a_2)} - 1$ を示す. (省略)

□

2 規則による定義・判断と導出

帰納的な集合 (とくに関係) の定義を行う際に, 特定の形の**規則**(*rule*) を使って記述することがある. 具体例として, **Aexp** の定義を規則を使った定義に書き直してみる.

2.1 定義: 算術式の集合 **Aexp** は, 以下の規則で定義される.

$$\frac{}{\mathtt{Z} \in \mathbf{Aexp}} \quad \text{(A-Zero)} \qquad \frac{a \in \mathbf{Aexp}}{\mathtt{S(}a\mathtt{)} \in \mathbf{Aexp}} \quad \text{(A-Succ)}$$

$$\frac{a_1 \in \textbf{Aexp} \qquad a_2 \in \textbf{Aexp}}{a_1 \texttt{ + } a_2 \in \textbf{Aexp}} \text{ (A-Plus)} \qquad \frac{a_1 \in \textbf{Aexp} \qquad a_2 \in \textbf{Aexp}}{a_1 \texttt{ * } a_2 \in \textbf{Aexp}} \text{ (A-Mult)}$$

□

直感的には，各規則は「線の上の事柄が成立するならば，線の下の事柄が成立する」という意味で，例えば A-Plus は「a_1 が **Aexp** の要素で a_2 が **Aexp** の要素ならば，a_1+a_2 は **Aexp** の要素である」と読める．これを使うと `Z + S(Z)` $\in$ **Aexp** ということは A-Zero を二回，A-Succ を一回，A-Plus を一回使うことで導くことができる．このように，規則を有限回組合せて $a \in$ **Aexp** が言えるような a の集合を以って **Aexp** を定義したと考えるのが，規則で定義するということである．この規則と BNF 記法の対応は明らかであろう．

2.1 判断と導出

一般的に規則は

$$\frac{J_1 \qquad \cdots \qquad J_n}{J} \text{ (規則名)}$$

という形をしている．ここで J_1 は**判断**(*judgment*) と呼ばれる何らかの事実について述べた文 (もしくは，そういう意味を持つ記号列) である．規則は，判断 $J_1, \ldots, J_n$ から 新しい判断 J を導くものであり，その判断を導く過程を**導出**(*derivation*) という．導出は，しばしば，木構造をもつ**導出木**(*derivation tree*) という形で表現される．例えば，`Z + S(Z)` $\in$ **Aexp** という判断の導出は

$$\dfrac{\dfrac{}{\texttt{Z} \in \textbf{Aexp}}\text{ A-Zero} \quad \dfrac{\dfrac{}{\texttt{Z} \in \textbf{Aexp}}\text{ A-Zero}}{\texttt{S(Z)} \in \textbf{Aexp}}\text{ A-Succ}}{\texttt{Z + S(Z)} \in \textbf{Aexp}}\text{ A-Plus}$$

という導出木で表現することができる[3].

厳密にいうと，規則には a などのメタ変数が含まれていることが多く，実際に導出する時には，それらのメタ変数を具体的なもので置換することになる．この具体化する前後の規則を区別して，前者を規則のスキーマ，後者を規則のインスタンスと呼ぶことがある．

2.2 部分式とパス

演習システムでは,「この式のこの部分を表示せよ」といった，式の一部を指定する表記が使われる．規則による定義に慣れるために，`sub` p `of` a `is` a' という「算術式 a のパス p に位置する部分式は a」であるという判断を導出する規則を考えてみる．ここで**パス**(*path*) は `0` もしくは `1` を有限個並べた文字列であり，ファイルシステムのディレクトリ・パスのよ

[3]導出木のことを単に導出と呼ぶことも多い.

うに，先頭から項の i 番目の部分式を辿っていく動作を表現する．このことを考えると，規則は以下のように定義できる．

$$\frac{a \in \mathbf{Aexp}}{\texttt{sub}\ \varepsilon\ \texttt{of}\ a\ \texttt{is}\ a}\ (\textsc{Sub-Empty}) \qquad \frac{a_1 \in \mathbf{Aexp} \quad \texttt{sub}\ p\ \texttt{of}\ a_2\ \texttt{is}\ a'}{\texttt{sub}\ 1p\ \texttt{of}\ a_1\texttt{+}a_2\ \texttt{is}\ a'}\ (\textsc{Sub-PlusR})$$

$$\frac{\texttt{sub}\ p\ \texttt{of}\ a_0\ \texttt{is}\ a'}{\texttt{sub}\ 0p\ \texttt{of}\ \texttt{S(}a_0\texttt{)}\ \texttt{is}\ a'}\ (\textsc{Sub-Succ}) \qquad \frac{\texttt{sub}\ p\ \texttt{of}\ a_1\ \texttt{is}\ a' \quad a_2 \in \mathbf{Aexp}}{\texttt{sub}\ 0p\ \texttt{of}\ a_1\texttt{*}a_2\ \texttt{is}\ a'}\ (\textsc{Sub-MultL})$$

$$\frac{\texttt{sub}\ p\ \texttt{of}\ a_1\ \texttt{is}\ a' \quad a_2 \in \mathbf{Aexp}}{\texttt{sub}\ 0p\ \texttt{of}\ a_1\texttt{+}a_2\ \texttt{is}\ a'}\ (\textsc{Sub-PlusL}) \qquad \frac{a_1 \in \mathbf{Aexp} \quad \texttt{sub}\ p\ \texttt{of}\ a_2\ \texttt{is}\ a'}{\texttt{sub}\ 1p\ \texttt{of}\ a_1\texttt{*}a_2\ \texttt{is}\ a'}\ (\textsc{Sub-MultR})$$

ここでは，長さ 0 のパス (空文字列) を便宜上 ε と記述している．この判断を導出する規則には前提に $a \in \mathbf{Aexp}$ が現れているので，実際には，A-XX も組み合わせて導出することになる．

2.2.1 練習問題: 以下の判断を導出せよ:

1. `sub 01 of (S(S(Z))+Z)*S(Z+S(Z)) is Z`
2. `sub 101 of (S(S(Z))+Z)*S(Z+S(Z)) is S(Z)`

2.2.2 練習問題: $\forall a \in \mathbf{Aexp}.\exists a' \in \mathbf{Aexp}.\texttt{sub}\ \underbrace{\texttt{0}\ldots\texttt{0}}_{depth(a)-1}\ \texttt{of}\ a\ \texttt{is}\ a'$ を証明せよ．

3 算術式の操作的意味論

算術式の集合が定義できたところで，算術式に対しその値を与える評価関係を定義する．例えば算術式 `S(S(Z))+S(S(Z))` の値は `S(S(S(S(Z))))` として与えられる．この講義では値は特別な形の式，すなわち **Nv** の要素として与えるが，別の集合—例えば自然数の集合 **Nat**—を考えて，`S(S(Z))+S(S(Z))` の値は 4 である，という関係を考えてもよい．

評価関係は算術式をプログラムとしてとらえたときの実行結果と考えられる．また，その定義は，算術式をいかに計算して値を求めるかの過程の記述を示している，式の操作的意味の定義とも考えられる．

3.1 定義: 評価関係 $a \Downarrow n$ は，図 1 の規則で定義される．

各規則を「時計まわりに」読むと，式の値をどう求めるかの手続きを読みとることができる．

$$\frac{}{\mathtt{Z} \Downarrow \mathtt{Z}} \quad \text{(E-Zero)} \qquad \frac{a_1 \Downarrow \mathtt{S}^n(\mathtt{Z}) \qquad a_2 \Downarrow \mathtt{S}^m(\mathtt{Z})}{a_1 \ \mathtt{+} \ a_2 \Downarrow \mathtt{S}^{n+m}(\mathtt{Z})} \quad \text{(E-Plus)}$$

$$\frac{a \Downarrow n}{\mathtt{S}(a) \Downarrow \mathtt{S}(n)} \quad \text{(E-Succ)} \qquad \frac{a_1 \Downarrow \mathtt{S}^n(\mathtt{Z}) \qquad a_2 \Downarrow \mathtt{S}^m(\mathtt{Z})}{a_1 \ \mathtt{*} \ a_2 \Downarrow \mathtt{S}^{n \cdot m}(\mathtt{Z})} \quad \text{(E-Mult)}$$

図 1: 算術式の評価関係

評価関係はプログラムの実行を表現している関係である．ここから，**文脈同値**(*contextual equivalence*) という，ふたつの算術式の等しさ，を定義する．文脈同値は「あるプログラム中の一部の式を別の式で入れかえても，挙動が変わらないとき，ふたつの式は等しい意味をもつといえる」という直感を，数学的に表現する．この定義を与えるために，まず，**文脈**context という，後で式で埋めることになる「穴ボコ」を一箇所持つ式を定義する．

3.2 定義: 文脈 $C \in \mathbf{Ctx}$ を以下の文法で定義する．

$$C \in \mathbf{Ctx} ::= [\,] \mid \mathtt{S}(C) \mid C \ \mathtt{+} \ a \mid a \ \mathtt{+} \ C \mid C \ \mathtt{*} \ a \mid a \ \mathtt{*} \ C$$

$C[a]$ で C 中の $[\,]$ を a で置換して得られる式を表すことにする．

3.3 定義: 算術式 a_1 と a_2 が**文脈同値**であること $a_1 \cong a_2$ を以下のように定義する．

$$a_1 \cong a_2 \iff (\forall C \in \mathbf{Ctx}, n \in \mathbf{Nv}. C[a_1] \Downarrow n \iff C[a_2] \Downarrow n)$$

評価関係も帰納的に定義されたので，やはり，それに対応する帰納法の証明原理が導かれる．

3.4 定理 [評価関係の導出に関する帰納法]: $\forall a \in \mathbf{Aexp}, n \in \mathbf{Nv}. a \Downarrow n \Longrightarrow P(a, n)$ を示すには，以下を示せばよい．

1. $\forall a \in \mathbf{Aexp}. P(\mathtt{Z}, \mathtt{Z})$
2. $\forall a \in \mathbf{Aexp}, n \in \mathbf{Nv}. P(a, n) \Longrightarrow P(\mathtt{S}(a), \mathtt{S}(n))$
3. $\forall a_1, a_2 \in \mathbf{Aexp}, n, m \in \mathbf{Nat}. P(a_0, \mathtt{S}^n(\mathtt{Z})) \Longrightarrow P(a_1, \mathtt{S}^m(\mathtt{Z})) \Longrightarrow P(a_1 \ \mathtt{+} \ a_2, \mathtt{S}^{n+m}(\mathtt{Z}))$
4. $\forall a_1, a_2 \in \mathbf{Aexp}, n, m \in \mathbf{Nat}. P(a_0, \mathtt{S}^n(\mathtt{Z})) \Longrightarrow P(a_1, \mathtt{S}^m(\mathtt{Z})) \Longrightarrow P(a_1 \ \mathtt{+} \ a_2, \mathtt{S}^{n \cdot m}(\mathtt{Z}))$

□

$$\frac{}{a_0 \texttt{ + Z} \longrightarrow a_0}\ \text{(R-PlusZero)} \qquad \frac{a_1 \longrightarrow a_1'}{a_1 \texttt{ + } a_2 \longrightarrow a_1' \texttt{ + } a_2}\ \text{(R-PlusL)}$$

$$\frac{}{a_1 \texttt{ + S(}a_2\texttt{)} \longrightarrow \texttt{S(}a_1 \texttt{ + } a_2\texttt{)}}\ \text{(R-PlusSucc)} \qquad \frac{a_2 \longrightarrow a_2'}{a_1 \texttt{ + } a_2 \longrightarrow a_1 \texttt{ + } a_2'}\ \text{(R-PlusR)}$$

$$\frac{}{a_0 \texttt{ * Z} \longrightarrow \texttt{Z}}\ \text{(R-MultZero)}$$

$$\frac{}{a_1 \texttt{ * S(}a_2\texttt{)} \longrightarrow a_1 \texttt{ * } a_2 \texttt{ + } a_1}\ \text{(R-MultSucc)} \qquad \frac{a_1 \longrightarrow a_1'}{a_1 \texttt{ * } a_2 \longrightarrow a_1' \texttt{ * } a_2}\ \text{(R-MultL)}$$

$$\frac{a \longrightarrow a'}{\texttt{S(}a\texttt{)} \longrightarrow \texttt{S(}a'\texttt{)}}\ \text{(R-Succ)} \qquad \frac{a_2 \longrightarrow a_2'}{a_1 \texttt{ * } a_2 \longrightarrow a_1 \texttt{ * } a_2'}\ \text{(R-MultR)}$$

図 2: 簡約規則 (1)

4 算術式の簡約

4.1 簡約関係の定義

簡約(*reduction*) とは，プログラムの一部分を「意味を変えずにより簡単」な断片で置き換えて別のプログラムを得ることである．プログラムの最適化といってもよいかもしれない．簡約は，プログラムの意味を定義するの別アプローチである．すなわち，

- 簡約関係から同値関係を導くことで，プログラムの等価性の別の定義を与えることができる．しかも，簡約関係を規則で定義することにより，等しさの規則による定義を与えることができる．
- 簡約の繰返しを計算とみなすことで，操作的意味の別の定義を与えることができる．

算術式 a_1 が 1 ステップで a_2 に簡約されることを $a_1 \longrightarrow a_2$ と書く．

4.1.1 定義: 関係 $\longrightarrow$ は，図 2 の規則で定義される．また，$\longrightarrow^*$ を $\longrightarrow$ の反射推移閉包，$\leftrightarrow$ を $\longrightarrow$ の同値閉包とする．

$\longrightarrow^*$ は複数ステップで簡約されることを示しており，$\leftrightarrow$ は，簡約から導かれる同値関係であり，プログラムが簡約を通じて等しいことを表している．

4.1.2 練習問題: 以下の判断の導出木を示せ.

$$\texttt{(S(S(Z)) + Z) * S(Z+S(Z))} \longrightarrow \texttt{S(S(Z)) * S(Z+S(Z))}$$
$$\texttt{S(S(Z)) * S(Z+S(Z))} \longrightarrow \texttt{S(S(Z)) * S(S(Z+Z))}$$
$$\texttt{(S(S(Z)) + Z) * S(Z+S(Z))} \longrightarrow \texttt{(S(S(Z)) + Z) * S(S(Z+Z))}$$
$$\texttt{(S(S(Z)) + Z) * S(Z+S(Z))} \longrightarrow \texttt{(S(S(Z)) + Z) * (Z+S(Z)) + S(Z+S(Z))}$$

与えられた式の中で，実際に式の変形が起こりうる部分式 (例えば a_0`+ Z` や `S(`a_2`)` という形をしているもの) を**簡約基**(*redex*) と呼ぶ.

簡約関係も帰納的に定義されたので，やはり，それに対応する帰納法の証明原理が導かれる.

4.1.3 定理 [簡約関係の導出に関する帰納法]: $\forall a_1, a_2 \in \mathbf{Aexp}.a_1 \longrightarrow a_2 \Longrightarrow P(a_1, a_2)$ を示すには，以下を示せばよい.

1. $\forall a \in \mathbf{Aexp}.P(a_0\ \texttt{+}\ \texttt{Z}, a_0)$
2. $\forall a_1, a_2 \in \mathbf{Aexp}.P(a_1\ \texttt{+}\ \texttt{S(}a_2\texttt{)}, \texttt{S(}a_1\ \texttt{+}\ a_2\texttt{)})$
3. $\forall a \in \mathbf{Aexp}.P(a_0\ \texttt{*}\ \texttt{Z}, \texttt{Z})$
4. $\forall a_1, a_2 \in \mathbf{Aexp}.P(a_1\ \texttt{*}\ \texttt{S(}a_2\texttt{)}, a_1\ \texttt{*}\ a_2\ \texttt{+}\ a_1)$
5. $\forall a, a' \in \mathbf{Aexp}.P(a, a') \Longrightarrow P(\texttt{S(}a\texttt{)}, \texttt{S(}a'\texttt{)})$
6. $\forall a_1, a_1', a_2 \in \mathbf{Aexp}.P(a_1, a_1') \Longrightarrow P(a_1\ \texttt{+}\ a_2, a_1'\ \texttt{+}\ a_2)$
7. $\forall a_1, a_2, a_2' \in \mathbf{Aexp}.P(a_2, a_2') \Longrightarrow P(a_1\ \texttt{+}\ a_2, a_1\ \texttt{+}\ a_2')$
8. $\forall a_1, a_1', a_2 \in \mathbf{Aexp}.P(a_1, a_1') \Longrightarrow P(a_1\ \texttt{*}\ a_2, a_1'\ \texttt{*}\ a_2)$
9. $\forall a_1, a_2, a_2' \in \mathbf{Aexp}.P(a_2, a_2') \Longrightarrow P(a_1\ \texttt{*}\ a_2, a_1\ \texttt{*}\ a_2')$

□

4.2 簡約関係の性質

算術式は簡約を続けていくと必ずそれ以上計算できない状態になるという，簡約の停止性を証明する.

4.2.1 定義: $a \in \mathbf{Aexp}$ が，$\neg\exists a' \in \mathbf{Aexp}.a \longrightarrow a'$ の時，a を**正規形**(*normal form*) である，という.

4.2.2 定理 [簡約の停止性, termination of evaluation]: 任意の算術式 a に対し，$a \longrightarrow^* a'$ なる正規形の a' が存在する.

Proof: $a \longrightarrow \cdots \longrightarrow a' \longrightarrow \cdots$ なる無限列がないことを示す．まず，$w(a) \in \mathbf{Aexp} \to \mathbf{Nat}$ を以下のように定義する．

1. $w(\mathtt{Z}) = 1$
2. $w(\mathtt{S(}a\mathtt{)}) = w(a) + 1$
3. $w(a_1 \ \mathtt{+} \ a_2) = w(a_1) + 2w(a_2)$
4. $w(a_1 \ \mathtt{*} \ a_2) = 3 \cdot w(a_1) \cdot w(a_2)$

このとき，$\forall a, a' \in \mathbf{Aexp}.a \longrightarrow a' \Longrightarrow w(a) > w(a')$ である．また $\forall a \in \mathbf{Aexp}.w(a) > 0$ なので，$a \longrightarrow \cdots \longrightarrow a' \longrightarrow \cdots$ が成立したとすると，$w(a) > \cdots > w(a') > \cdots$ なる無限列が存在することになり矛盾． □

次の定理は，簡約の複数の過程で途中経過が異なっても，再び同一の式へと簡約することができる，という性質で**合流性**(*confluence*) と呼ぶ．

4.2.3 定理 [合流性, confluence]: $\forall a_1, a_2, a_3.a_1 \longrightarrow^* a_2 \ \& \ a_1 \longrightarrow^* a_3 \Longrightarrow \exists a_4.a_2 \longrightarrow^* a_4 \ \& \ a_3 \longrightarrow^* a_4$.

Proof: (省略) □

また，この系として，等しい算術式同士は，同一の算術式に簡約することができることがいえる．

4.2.4 系: $\forall a_1, a_2, a_3.a_1 \leftrightarrow a_2 \Longrightarrow \exists a_3.a_1 \longrightarrow^* a_3 \ \& \ a_2 \longrightarrow^* a_3$.

また，ある式を簡約して正規形になった時には，その形は一意であることがいえる．

4.2.5 系 [正規形の唯一性, uniqueness of normal forms]: $a \longrightarrow^* a'$ かつ $a \longrightarrow^* a''$ かつ a', a'' が正規形ならば，$a' \equiv a''$ である．

これらの結果から，簡約を計算，正規形を計算結果として見れば，算術式に対して一意に計算結果を与えることができるという意味で，算術式の意味を与えていると考えることができる．

5 ふたつの意味の関係

ふたつの等しさは等しい．

5.1 定理: $\forall a_1, a_2.a_1 \leftrightarrow a_2 \iff a_1 \cong a_2$.

より複雑な言語になると，右から左を成立させるような，$\leftrightarrow$ の帰納的な定義は存在しない．算術式の場合は，表現力が低いので文脈同値関係を規則によって完全に把握することができる．

また，ふたつの計算の定義は等しい．

5.2 定理: $\forall a \in \mathbf{Aexp}, n \in \mathbf{Nv}. a \Downarrow n \iff a \longrightarrow^* n.$

Proof: 左から右は，$a \Downarrow n$ の導出に関する帰納法．右から左は，次節で証明． □

6 簡約戦略・eager/lazy な戦略

6.1 簡約戦略の定義

実際の (逐次) プログラミング言語の実行においては，上で定義した簡約関係のように与えられた式に対して複数の実行過程があることはなく，そのうちのひとつに固定されているのが普通である．そのように，式に対して簡約後の式を複数あり得る中からただ一つ定めることを**簡約戦略**(*reduction strategy*) を与えるという．

6.1.1 定義: $F \in \mathbf{Aexp} \rightharpoonup \mathbf{Aexp}$ が簡約関係 $\longrightarrow$ の戦略である，とは 任意の $a \in dom(F)$ について $a \longrightarrow F(a)$ が成立することである．($f \in A \rightharpoonup B$ に対して $dom(f)$ は f の定義域 A を示す．)

まず，評価関係の定義の直観と対応する戦略を考える．評価関係の規則を眺めると，例えば a_1 `+` a_2 はまず a_1, a_2 を値に評価 (計算) すべし，という気持が読みとれる．つまり評価関係に対応する戦略は「演算子の引数はまず『値』になるまで計算する」というものである．(どちらの引数から値にするかは任意性があるが，ここでは左の引数から計算していくことを考える．)

もうひとつの戦略の例として「演算子の引数は，計算を進めねばならなくなった時に始めて計算する」というものを考える．この戦略によれば，`(S(Z) + S(Z)) * Z` のような式は，`S(Z) + S(Z)` の計算をせずに (しなくても計算が進められるので)，いきなり `Z` に簡約される．それぞれを eager な・lazy な簡約と呼ぶ．

以下では，どちらの戦略も，まず規則を使って算術式上の関係 ($\longrightarrow_e$ と $\longrightarrow_l$) として定義した後，それが戦略となっていることを示す．

6.1.2 定義: 関係 $\longrightarrow_e$ と $\longrightarrow_l$ は，それぞれ図 3 と図 4 の規則で定義される．

ここで，規則のメタ変数を置き換える時には，メタ変数の名前に応じて具体化を行なうことが暗黙のうちに仮定されている．例えば，Ee-PlR を使用するときには，n_1 は上で定義した「自然数」(`S(S(...(Z)...))`) で具体化しなければならない．

6.1.3 例:

$$(\texttt{S(S(Z))} \texttt{ + } \texttt{Z}) \texttt{ * } \texttt{S(Z+S(Z))} \longrightarrow_e \texttt{S(S(Z))} \texttt{ * } \texttt{S(Z+S(Z))}$$

は導出できるが,

$$(\texttt{S(S(Z))} \texttt{ + } \texttt{Z}) \texttt{ * } \texttt{S(Z+S(Z))} \longrightarrow_e (\texttt{S(S(Z))} \texttt{ + } \texttt{Z}) \texttt{ * } \texttt{S(S(Z+Z))}$$

や

$$(\texttt{S(S(Z))} \texttt{ + } \texttt{Z}) \texttt{ * } \texttt{S(Z+S(Z))} \longrightarrow_e (\texttt{S(S(Z))} \texttt{ + } \texttt{Z}) \texttt{ * } (\texttt{Z+S(Z)}) \texttt{ + } \texttt{S(Z+S(Z))}$$

は導出できない.

$\longrightarrow$ と同様に，この規則より導出に関する帰納法の原理が導かれる．下には $\longrightarrow_e$ についてのみ示す.

6.1.4 定理 [**eager 簡約関係の導出に関する帰納法**]: $\forall a_1, a_2 \in \mathbf{Aexp}.a_1 \longrightarrow_e a_2 \Longrightarrow P(a_1, a_2)$ を示すには，以下を示せばよい.

1. $\forall n \in \mathbf{Nv}.P(n_0 \texttt{ + } \texttt{Z}, n_0)$
2. $\forall n_1, n_2 \in \mathbf{Nv}.P(n_1 \texttt{ + } \texttt{S(}n_2\texttt{)}, \texttt{S(}n_1 \texttt{ + } n_2\texttt{)})$
3. $\forall n \in \mathbf{Nv}.P(n_0 \texttt{ * } \texttt{Z}, \texttt{Z})$
4. $\forall n_1, n_2 \in \mathbf{Nv}.P(n_1 \texttt{ * } \texttt{S(}n_2\texttt{)}, n_1 \texttt{ * } n_2 \texttt{ + } n_1)$
5. $\forall a, a' \in \mathbf{Aexp}.P(a, a') \Longrightarrow P(\texttt{S(}a\texttt{)}, \texttt{S(}a'\texttt{)})$
6. $\forall a_1, a_1', a_2 \in \mathbf{Aexp}.P(a_1, a_1') \Longrightarrow P(a_1 \texttt{ + } a_2, a_1' \texttt{ + } a_2)$
7. $\forall n_1 \in NV, a_2, a_2' \in \mathbf{Aexp}.P(a_2, a_2') \Longrightarrow P(n_1 \texttt{ + } a_2, n_1 \texttt{ + } a_2')$
8. $\forall a_1, a_1', a_2 \in \mathbf{Aexp}.P(a_1, a_1') \Longrightarrow P(a_1 \texttt{ * } a_2, a_1' \texttt{ * } a_2)$
9. $\forall n_1 \in NV, a_2, a_2' \in \mathbf{Aexp}.P(a_2, a_2') \Longrightarrow P(n_1 \texttt{ * } a_2, n_1 \texttt{ * } a_2')$

□

6.2 eager / lazy な簡約に関する性質

ここでは $\longrightarrow_e$ が $\longrightarrow$ の戦略になっていることのみを示すが，$\longrightarrow_l$ に関しても同様に示すことができる.

6.2.1 定理: 任意の算術式 a, a' に対して $a \longrightarrow_e a'$ ならば $a \longrightarrow a'$ である.

$$\frac{}{n_0 \texttt{ + Z} \longrightarrow_e n_0} \text{(RE-PlZ)} \qquad \frac{a_1 \longrightarrow_e a_1'}{a_1 \texttt{ + } a_2 \longrightarrow_e a_1' \texttt{ + } a_2} \text{(RE-PlL)}$$

$$\frac{}{n_1 \texttt{ + S(}n_2\texttt{)} \longrightarrow_e \texttt{S(}n_1 \texttt{ + } n_2\texttt{)}} \text{(RE-PlSc)} \qquad \frac{a_2 \longrightarrow_e a_2'}{n_1 \texttt{ + } a_2 \longrightarrow_e n_1 \texttt{ + } a_2'} \text{(RE-PlR)}$$

$$\frac{}{n_0 \texttt{ * Z} \longrightarrow_e \texttt{Z}} \text{(RE-MuZ)}$$

$$\frac{}{n_1 \texttt{ * S(}n_2\texttt{)} \longrightarrow_e n_1 \texttt{ * } n_2 \texttt{ + } n_1} \text{(RE-MuSc)} \qquad \frac{a_1 \longrightarrow_e a_1'}{a_1 \texttt{ * } a_2 \longrightarrow_e a_1' \texttt{ * } a_2} \text{(RE-MuL)}$$

$$\frac{a \longrightarrow_e a'}{\texttt{S(}a\texttt{)} \longrightarrow_e \texttt{S(}a'\texttt{)}} \text{(RE-Succ)} \qquad \frac{a_2 \longrightarrow_e a_2'}{n_1 \texttt{ * } a_2 \longrightarrow_e n_1 \texttt{ * } a_2'} \text{(RE-MuR)}$$

図 3: eager な簡約

$$\frac{}{a_0 \texttt{ + Z} \longrightarrow_l a_0} \text{(RL-PlZ)} \qquad \frac{a_2 \texttt{ + } a_3 \longrightarrow_l a_2'}{a_1 \texttt{ + (}a_2 \texttt{ + } a_3\texttt{)} \longrightarrow_l a_1 \texttt{ + } a_2'} \text{(RL-PlPl)}$$

$$\frac{}{a_1 \texttt{ + S(}a_2\texttt{)} \longrightarrow_l \texttt{S(}a_1 \texttt{ + } a_2\texttt{)}} \text{(RL-PlSc)} \qquad \frac{a_2 \texttt{ * } a_3 \longrightarrow_l a_2'}{a_1 \texttt{ + } a_2 \texttt{ * } a_3 \longrightarrow_l a_1 \texttt{ + } a_2'} \text{(RL-PlMu)}$$

$$\frac{}{a_0 \texttt{ * Z} \longrightarrow_l \texttt{Z}} \text{(RL-MuZ)}$$

$$\frac{}{a_1 \texttt{ * S(}a_2\texttt{)} \longrightarrow_l a_1 \texttt{ * } a_2 \texttt{ + } a_1} \text{(RL-MuSc)} \qquad \frac{a_2 \texttt{ + } a_3 \longrightarrow_l a_2'}{a_1 \texttt{ * (}a_2 \texttt{ + } a_3\texttt{)} \longrightarrow_l a_1 \texttt{ * } a_2'} \text{(RL-MuPl)}$$

$$\frac{a \longrightarrow_l a'}{\texttt{S(}a\texttt{)} \longrightarrow_l \texttt{S(}a'\texttt{)}} \text{(RL-Succ)} \qquad \frac{a_2 \texttt{ * } a_3 \longrightarrow_l a_2'}{a_1 \texttt{ * (}a_2 \texttt{ * } a_3\texttt{)} \longrightarrow_l a_1 \texttt{ * } a_2'} \text{(RL-MuMl)}$$

図 4: lazy な簡約

Proof: $\longrightarrow_e$ を定義する規則のどのインスタンスも，$\longrightarrow$ を定義する規則のインスタンスになるので，ほぼ自明であるが，厳密には $a \longrightarrow_e a'$ の導出に関する帰納法で証明する．$P(a, a')$ は $a \longrightarrow a'$ である． □

6.2.2 定理 [**eager 簡約の決定性**]: $\longrightarrow_e \in \mathbf{Aexp} \rightharpoonup \mathbf{Aexp}$ である．すなわち，$\forall a, a', a'' \in \mathbf{Aexp}. a \longrightarrow_e a' \,\&\, a \longrightarrow_e a'' \Longrightarrow a' \equiv a''$.

Proof: これも直感的には，どの規則も結論部の $a \longrightarrow_e a'$ の左側の形に重なりがないので，ほぼ自明に見えるが，厳密には $a \longrightarrow_e a'$ の導出に関する帰納法で証明する．$P(a, a')$ に対応する述語は $\forall a'' \in \mathbf{Aexp}. a \longrightarrow_e a'' \Longrightarrow a' \equiv a''$ である． □

また，eager 簡約を使ってで，定理 5.2 の残りが証明できる．

6.2.3 定理: $\forall a \in \mathbf{Aexp}, n \in \mathbf{Nv}. a \longrightarrow^* n \Longrightarrow a \longrightarrow_e^* n$.

Proof: $\longrightarrow_e$ に関する正規形は **Nv** の要素であること，eager 簡約 $\longrightarrow_e$ も停止すること，合流性より． □

6.2.4 定理: $\forall a \in \mathbf{Aexp}, n \in \mathbf{Nv}. a \longrightarrow_e^* n \Longrightarrow a \Downarrow n$.

Proof: $a \longrightarrow_e^* n$ のステップ数 k に関する数学的帰納法. □