プログラミング言語の基礎概念

導出システム … プログラミング言語の意味論（semantics）や型システムを記述するための枠組み
derivation system

自然演繹(←数理論理学で形式的証明を記述するための)やシーケント計算といった体系を一般化した汎用的な枠組み

議論の対象(論理式、プログラム、型など)に対する様々な判断を推論規則に従って導くための記述体系

判断の形式とそれに対する推論規則群を与えることによって定められる

例) 自然数の大小比較を対象とした導出システム
判断の例：3は5より小さい
推論規則の例：任意の自然数 n_1, n_2, n_3 について、
n_1 が n_2 より小さく、かつ n_2 が n_3 より小さいならば、
n_1 は n_3 より小さい

1.1 自然数の加算・乗算：導出システム Nat

定義1.1 導出システム Nat で我々が扱う判断の一般的な形式は
n_1, n_2, n_3 をペアノ自然数
- n_1 plus n_2 is n_3
- n_1 times n_2 is n_3

のいずれかとする。

※ 形式上は正しいが内容的には正しくない判断も考えてよい
例) $S(S(Z))$ plus $S(S(S(Z)))$ is $S(Z)$

今後、単に「判断」といったら、形式的に正しい判断を指す

定義1.2 判断"n_1 plus n_2 is n_3"のための推論規則は次のふたつである

規則 P-ZERO：任意のペアノ自然数 n に対して、
n_1 plus n_2 is n_3 を導いてよい。

規則 P-SUCC：任意のペアノ自然数 n_1, n_2, n_3 に対して、
n_1 plus n_2 is n_3 ならば
$S(n_1)$ plus n_2 is $S(n_3)$ を導いてよい。

規則 P-SUCC のような、「J_1 ならば J_2」という形の、前提(premise)のある推論規則は、前提となる判断 J_1 が既に得られている場合に限り J_2 の判断を導いてよい

定義 1.3 判断 "n_1 times n_2 is n_3" のための推論規則は以下のふたつ

任意のペアノ自然数

規則 T-ZERO： Z times n is Z

規則 T-SUCC： n_1 times n_2 is n_3 かつ n_2 plus n_3 is n_4 ならば、$S(n_1)$ times n_2 is n_4

- $n_1 \times n_2 = n_3$
- $n_2 + n_3 = n_4$

$$\boxed{S(n_1) \times n_2 = n_4}$$

$$n_2 + (n_1 \times n_2) = n_4$$

$$n_2 \underbrace{(n_1 + 1)}_{= S(n_1)} = n_4$$

S(S(Z)) times S(S(Z)) is S(S(S(S(Z))))

規則 T-ZERO より Z times S(S(Z)) is Z …①

〃 Z plus Z is Z

P-SUCC → S(Z) plus Z is S(Z)

P-SUCC → S(S(Z)) plus Z is S(S(Z)) …②

規則 T-SUCC、①、② より S(Z) times S(S(Z)) is S(S(Z)) …③

規則 P-ZERO より Z plus S(S(Z)) is S(S(Z))

P-SUCC → S(Z) plus S(S(Z)) is S(S(S(Z)))

P-SUCC → S(S(Z)) plus S(S(Z)) is S(S(S(S(Z)))) …④

規則 T-SUCC, ③, ④ より S(S(Z)) times S(S(Z)) is S(S(S(S(Z)))) 終

規則の適用によって判断を導く過程を導出(derivation)と呼ぶ。

練習 1.2 (1) S(S(S(Z))) plus S(Z) is S(S(S(S(Z))))

n = S(Z) とすると P-ZERO より Z plus S(Z) is S(Z)

P-SUCC より S(Z) plus S(Z) is S(S(Z))

P-SUCC より S(S(Z)) plus S(Z) is S(S(S(Z)))

P-SUCC より S(S(S(Z))) plus S(Z) is S(S(S(S(Z))))

プログラミング言語の基礎概念

(2) $S(Z)$ plus $S(S(S(Z)))$ is $S(S(S(S(Z))))$

$n = S(S(S(Z)))$ と P-ZERO より Z plus $S(S(S(Z)))$ is $S(S(S(Z)))$

P-SUCC より $S(Z)$ plus $S(S(S(Z)))$ is $S(S(S(S(Z))))$

(3)

メモ

$S(\underset{n_1}{\underline{S(S(Z))}})$ times $\underset{n_2}{\underline{Z}}$ is $\underset{n_4}{\underline{Z}}$

$\underset{n_1}{\underline{S(S(Z))}}$ times $\underset{n_2}{\underline{Z}}$ is $\underset{n_3}{\underline{Z}}$

$\underset{n_2}{\underline{Z}}$ plus $\underset{n_3}{\underline{Z}}$ is $\underset{n_4}{\underline{Z}}$

$n = Z$ とするとP-ZERO より Z plus Z is Z …①

メモ

$S(Z)$ times Z is Z

Z times Z is Z $(n = Z)$

$n = Z$ とすると T-ZERO より Z times Z is Z …②

規則 T-SUCC, ①, ② より $S(Z)$ times Z is Z …③

規則 T-SUCC, ①, ③ より $S(S(Z))$ times Z is Z …④

規則 T-SUCC, ①, ④ より $S(S(S(Z)))$ times Z is Z 終

練習1.3 判断"n_1 plus n_2 is n_3"が導出できる時、その導出には何回の規則の適用が必要か?

1回目の適用

P-ZERO Z plus n is n (n_2, n_2)

$(n_1 + 1)$ 回 //

"n_1 times n_2 is n_3" についてはどうか.

$(n_1 + 1)$ 回、T-SUCC (最後の1回だけはT-ZERO)を適用する

T-SUCC を適用するごとに、$(n_2 + 1)$ 回の適用が必要になる

T-SUCC & T-ZERO

$(n_1 + 1) + (n_2 + 1) \times (n_1 + 1)$

1.2 推論規則と導出の記法

規則 X: J_1 かつ … かつ J_n ならば J。 $\dfrac{J_1 \cdots J_n}{J}$

※ 前提のない規則の場合 $n = 0$

(P-ZERO) $$\frac{}{z \text{ plus } n \text{ is } n}$$

(P-SUCC) $$\frac{n_1 \text{ plus } n_2 \text{ is } n}{S(n_1) \text{ plus } n_2 \text{ is } S(n)}$$

(T-ZERO) $$\frac{}{z \text{ times } n \text{ is } z}$$

(T-SUCC) $$\frac{n_1 \text{ times } n_2 \text{ is } n_3 \qquad n_2 \text{ plus } n_3 \text{ is } n_4}{S(n_1) \text{ times } n_2 \text{ is } n_4}$$

derivation tree
導出木 … 判断をノード、結論となる判断を根とする木構造

```
S(S(S(z))) plus S(z) is S(S(S(S(z)))) by P-SUCC{
  S(S(z)) plus S(z) is S(S(S(z))) by P-SUCC {
    S(z) plus S(z) is S(S(z)) by P-SUCC{
      z plus S(z) is S(z) by P-ZERO{}
    }
  }
}
```

$$\cfrac{\cfrac{\cfrac{\cfrac{}{z \text{ plus } S(z) \text{ is } S(z)}\,\text{P-ZERO}}{S(z) \text{ plus } S(z) \text{ is } S(S(z))}\,\text{P-SUCC}}{S(S(z)) \text{ plus } S(z) \text{ is } S(S(S(z)))}\,\text{P-SUCC}}{S(S(S(z))) \text{ plus } S(z) \text{ is } S(S(S(S(z))))}\,\text{P-SUCC}$$

```
(3) S(S(S(z))) times z is z by T-SUCC {
      S(S(z)) times z is z by T-SUCC{
        S(z) times z is z by T-SUCC{
          z times z is z by T-ZERO{};
        }; z plus z is z by P-ZERO{}
        z plus z is z by P-ZERO{}
      };
      z plus z is z by P-ZERO{}
    }
```

プログラミング言語の基礎概念

CompareNat 1

$$\frac{}{n \text{ is less than } S(n)} \quad (\text{L-SUCC})$$

$$\frac{n_1 \text{ is less than } n_2 \qquad n_2 \text{ is less than } n_3}{n_1 \text{ is less than } n_3} \quad (\text{L-TRANS})$$

練習問題1.5 (1) Z is less than S(S(Z))

$$\dfrac{\dfrac{}{Z \text{ is less than } S(Z)}\,\text{L-Succ} \qquad \dfrac{}{S(Z) \text{ is less than } S(S(Z))}\,\text{L-Succ}}{Z \text{ is less than } S(S(Z))}\,\text{L-TRANS}$$

CompareNat 2

$$\frac{}{Z \text{ is less than } S(n)} \quad (\text{L-ZERO})$$

$$\frac{n_1 \text{ is less than } n_2}{S(n_1) \text{ is less than } S(n_2)} \quad (\text{L-SuccSucc})$$

1.5 (1)

$$\frac{}{Z \text{ is less than } S(S(Z))}\,\text{L-ZERO}$$

CompareNat 3

$$\frac{}{n \text{ is less than } S(n)} \quad (\text{L-SUCC})$$

$$\frac{n_1 \text{ is less than } n_2}{n_1 \text{ is less than } S(n_2)} \quad (\text{L-SUCCR})$$

1.5 (1)

$$\dfrac{\dfrac{}{Z \text{ is less than } S(Z)}\,\text{L-SUCC}}{Z \text{ is less than } S(S(Z))}\,\text{L-SUCCR}$$

- Natを使って定義された加算が交換法則を満たすことを示す
- EvalNatExpを使って定義された評価は、与えられた算術式に対して、その値を一意的に定める

といった、具体的な導出システムにおける、判断についての一般的な性質を考える

↳ このような、判断についての一般的な性質(のうち数学的に証明されたもの)をメタ定理と呼ぶ
metatheorem

帰納法 ここではメタ定理の証明に用いる
induction

操作的意味論 … 評価・簡約を使った意味論
operational semantics (ここでは算術式に意味を与えている)

ある判断が導出できているかどうかは、単なる記号操作の問題

$\overline{Z \text{ plus } n \text{ is } S(n)}$ (P-WRONG) といった規則を考えれば

Z plus S(Z) is S(S(Z)) という内容的には誤った判断を導出できるが、

P-ZEROしかないような導出システムでは
内容的には正しいはずの S(Z) plus S(Z) is S(S(Z)) を導出することができない

導出システムを「何らかの概念を表現した理論」と考えたとき、こういった導出システムの「出来」を考察した理論はメタ理論(理論に関する理論)である。

健全性 … 導出された判断が全て内容的に正しいという性質

完全性 … 内容的に正しい判断は全て導出できるという性質

構造帰納法　ペアノ自然数は自然数と1対1対応

(1) 任意のペアノ自然数 n に対し、Z plus n is n
(2) 任意のペアノ自然数 n に対し、n plus Z is n

(1) 規則P-ZEROにより、n が実際にどんなペアノ自然数であるかによらず $\overline{Z \text{ plus } n \text{ is } n}$ P-ZERO という導出木が作れる

(2) ペアノ自然数に関する帰納法より、以下の2つを証明すればよい
(a) Z plus Z is Z が導出できる
(b) 任意のペアノ自然数 k について k plus Z is k が導出できるなら、S(k) plus Z is S(k) が導出できる
※ここでは P(n) は「判断 n plus Z is n が導出できる」
(証明) (a) は P-ZERO を使えば導出できる
(b) k plus Z is k の導出を

$$D \stackrel{def}{=} \frac{\vdots}{k \text{ plus } Z \text{ is } k}$$ とすると、

規則 P-SUCC を用いて

$$\frac{\mathcal{D}}{S(k) \text{ plus } Z \text{ is } S(k)} \text{P-SUCC}$$

が導出できるので (b) がいえる $\boxed{\text{終}}$

(1) Z plus n is n は P-ZERO より 1ステップで導出できる。

(2) n plus Z is n は P-SUCC の n 回適用により導出できる。
↳ この直観を、数学的帰納法を使った証明という形で記述している

定理 2.2 任意のペアノ自然数 n_1, n_2, n_3, n_4 に対して、
n_1 plus n_2 is n_3 かつ n_1 plus n_2 is n_4 ならば、
$n_3 \equiv n_4$ である。

方針：n_1 についての (ペアノ自然数に関する) 帰納法で証明する。

(証明) (1) $n_1 \equiv Z$ の場合 P(Z)を示す

判断 Z plus n_2 is n_3, Z plus n_2 is n_4 の導出をそれぞれ D_1, D_2 とすると、これらは以下のような形をしている。

$$D_1 \equiv \frac{}{Z \text{ plus } n_2 \text{ is } n_3} \text{P-ZERO}$$

$$D_2 \equiv \frac{}{Z \text{ plus } n_2 \text{ is } n_4} \text{P-ZERO}$$

さらに、P-ZERO の形より、$n_3 \equiv n_4 \equiv n_2$

P(n)：n plus n_2 is n_3, n plus n_2 is n_4 が導出できるなら $n_3 \equiv n_4$

(2) ある k に対して $n_1 \equiv S(k)$ の場合

まず、判断 $S(k)$ plus n_2 is n_3, $S(k)$ plus n_2 is n_4 が導出できていると仮定する。これらの導出を D_1, D_2 とすると、$n_3 \equiv S(n_3')$, $n_4 \equiv S(n_4')$ が成り立つようなペアノ自然数 n_3', n_4' が存在して、D_1, D_2 は以下のような形をしている

$$D_1 \equiv \frac{\begin{array}{c}\vdots \\ \hline k \text{ plus } n_2 \text{ is } n_3'\end{array}}{S(k) \text{ plus } n_2 \text{ is } n_3} \text{P-SUCC} \qquad D_2 \equiv \frac{\begin{array}{c}\vdots \\ \hline k \text{ plus } n_2 \text{ is } n_4'\end{array}}{S(k) \text{ plus } n_2 \text{ is } n_4} \text{P-SUCC}$$

部分に注目

帰納法の仮定 P(k) より、$n_3' \equiv n_4'$

よって $n_3 \equiv S(n_3') \equiv S(n_4') \equiv n_4$ $\boxed{\text{終}}$

定理2.4 任意のペアノ自然数 n_1, n_2, n_3 に対して、
n_1 plus n_2 is n_3 ならば、n_2 plus n_1 is n_3 である。

(証明) n_1 についての帰納法で証明する。

(1) $n_1 \equiv Z$ の場合(ここで示すべきは「任意のペアノ自然数 n_2, n_3 に対して、Z plus n_2 is n_3 ならば n_2 plus Z is n_3」である)。
判断 Z plus n_2 is n_3 の導出をDとすると、Dは以下のような形をしている

$$D \equiv \dfrac{}{Z \text{ plus } n_2 \text{ is } n_3}\ \text{P-ZERO}$$

P-ZERO の形より、$n_2 \equiv n_3$ である。
定理2.1「Zは加算の単位元である」より、n_2 plus Z is n_3 である。
↳任意のペアノ自然数 n に対し、Z plus n is n, n plus Z is n

(2) ある k に対して $n_1 \equiv S(k)$ の場合、
まず、判断 $S(k)$ plus n_2 is n_3 が導出できるとする。
この導出をDとすると、最後に適用される規則はP-SUCCで、
さらに あるペアノ自然数 n_3' に対して $n_3 \equiv S(n_3')$ が成立して、

$$D \equiv \dfrac{\dfrac{\vdots}{k \text{ plus } n_2 \text{ is } n_3'}}{S(k) \text{ plus } n_2 \text{ is } n_3}\ \text{P-SUCC}$$

である。
Dの一部として、判断 k plus n_2 is n_3' が導出できていることに注目すると、帰納法の仮定より、判断 n_2 plus k is n_3' が導出できる。
補題より、n_2 plus $S(k)$ is n_3

(1), (2) より、任意のペアノ自然数 n_1, n_2, n_3 に対して、
n_1 plus n_2 is n_3 ならば、n_2 plus n_1 is n_3 である。 $\boxed{\text{終}}$

定理2.4の証明のための補題

任意のペアノ自然数 n_1, n_2, n_3 に対し、
判断 n_1 plus n_2 is n_3 が導出できるならば、
n_1 plus $S(n_2)$ is $S(n_3)$ も導出できる.

(証明) n_1 についての帰納法で証明する.

(1) $n_1 \equiv Z$ の場合、示すべきは「任意のペアノ自然数 n_2, n_3 に対して Z plus n_2 is n_3 ならば Z plus $S(n_2)$ is $S(n_3)$」である.
定理2.1「Zは加算の単位元である」より. 判断 n_2 plus Z is n_3 が導出できる.

$$\dfrac{n_2 \text{ plus } Z \text{ is } n_3}{S(n_2) \text{ plus } Z \text{ is } S(n_3)}\text{P-SUCC}$$

よって、定理2.1より. Z plus $S(n_2)$ is $S(n_3)$ が導出できる.

(2) ある k に対して $n_1 \equiv S(k)$ の場合.
まず、判断 $S(k)$ plus n_2 is n_3 が導出できるとする.
この導出をDとすると、最後に適用される規則は P-SUCC で、
さらにあるペアノ自然数 n_3' に対して $n_3 \equiv S(n_3')$ が成立して、

$$D \equiv \dfrac{\dfrac{\vdots}{k \text{ plus } n_2 \text{ is } n_3'}}{S(k) \text{ plus } n_2 \text{ is } n_3}\text{P-SUCC}$$

である.
ここで、Dの一部として、判断 k plus n_2 is n_3' が導出できている
ことに注目すると、帰納法の仮定「任意のペアノ自然数 n_2, n_3 に対して、k plus n_2 is n_3 が導出できるならば、k plus $S(n_2)$ is $S(n_3)$ も導出できる」より、判断 k plus $S(n_2)$ is $S(n_3')$ が導出できる. $n_3 \equiv S(n_3')$ より.

$$\dfrac{k \text{ plus } S(n_2) \text{ is } n_3}{S(k) \text{ plus } S(n_2) \text{ is } S(n_3)}\text{P-SUCC}$$

(1), (2) より、任意のペアノ自然数 n_1, n_2, n_3 に対して
判断 n_1 plus n_2 is n_3 が導出できるなら、n_1 plus $S(n_2)$ is $S(n_3)$ も導出できる。 $\boxed{\text{終}}$

（Natの規則）P-ZERO, P-SUCC

（すでに証明できている定理）

Zは加算の単位元、加算の結果は一意、交換法則

定理2.3 任意のペアノ自然数 n_1, n_2 に対して、あるペアノ自然数 n_3 が存在して、n_1 plus n_2 is n_3 である。

（証明）n_1 についての帰納法で証明する。

(1) $n_1 \equiv Z$ の場合、示すべきは「任意のペアノ自然数 n_2 に対して、あるペアノ自然数 n_3 が存在して、Z plus n_2 is n_3」である。規則P-ZERO「Z plus n is n」と定理2.2（加算結果の一意性）より、$n_2 \equiv n_3$ であり、成り立つ。

(2) $n_1 \equiv k$ のとき成り立つ、すなわち「任意のペアノ自然数 n_2 に対して、あるペアノ自然数 n_3 が存在して、k plus n_2 is n_3」が成り立つと仮定する。このとき規則P-SUCCを適用して $S(k)$ plus n_2 is $S(n_3)$ を導出でき、$n_1 \equiv S(k)$ のときも成り立つ。

(1), (2) より、任意のペアノ自然数 n_1, n_2 に対して、あるペアノ自然数 n_3 が存在して、n_1 plus n_2 is n_3 である。$\boxed{終}$

結合法則

定理2.5 任意のペアノ自然数 $n_1, \cdots, n_5$ に対して、n_1 plus n_2 is n_4 かつ n_4 plus n_3 is n_5 ならば、あるペアノ自然数 n_6 がが存在し、n_2 plus n_3 is n_6 かつ n_1 plus n_6 is n_5 である。

$n_1 + n_2 + n_3 = n_5$

n_4 n_6

（証明）n_1 についての帰納法で証明する。

(1) $n_1 \equiv Z$ の場合、Z plus n_2 is n_4 が導出でき、規則P-ZEROと定理2.2より $n_2 \equiv n_4$ である。また、n_2 plus n_3 is n_5 が導出でき、定理2.2より $n_6 \equiv n_5$ である。さらに、Z plus n_5 is n_5 が導出できる。よって、$n_1 \equiv Z$ のとき成り立つ。

(2) $n_1 \equiv k$ のとき成り立つ、すなわち「任意のペアノ自然数 $n_1, \cdots, n_5$ に対して、k plus n_2 is n_4 かつ n_4 plus n_3 is n_5 ならば、あるペアノ自然数 n_6 が存在し、n_2 plus n_3 is n_6 かつ k plus n_6 is n_5」が成り立つと仮定する。$n_1 \equiv S(k)$ のとき、判断 $S(k)$ plus n_2 is n_4、n_4 plus n_3 is n_5 が成り立つとする。定理2.3より、あるペアノ自然数 n_6 が存在し、n_2 plus n_3 is n_6 である。