帰納法によるプログラムの証明

胡 振江
東京大学 計数工学科

2006 年度

内容

- 自然数上の帰納法によるプログラムの証明
- リスト上の帰納法によるプログラムの証明
- 補助定理と一般化

自然数の上の帰納法 1

自然数 n について，命題 $p(n)$ が成立することを帰納法によって証明するには，次の 2 つのことを示す.

- **場合** 0．$P(0)$ が成立する.
- **場合** $(n+1)$．$P(n)$ が成立するならば，$P(n+1)$ も成立する.

例題

次のように定義されている関数

$$
\begin{aligned}
x^0 &= 1 \\
x^{n+1} &= x * x^n
\end{aligned}
$$

に対して，任意の x と，任意の自然数 m と n について，

$$x^{m+n} = x^m * x^n$$

が成立することを証明せよ．

証明：m に関する帰納法で証明する．

場合 0.

$$
\begin{array}{ll}
 & x^{0+n} \\
= & \quad \{\ + \text{の法則}\ \} \\
 & x^{n} \\
= & \quad \{\ * \text{の法則}\ \} \\
 & 1 * x^{n} \\
= & \quad \{\ \text{ベキ関数の定義}\ \} \\
 & x^{0} * x^{m}
\end{array}
$$

場合 $m+1$

$$
\begin{array}{ll}
 & x^{(m+1)+n} \\
= & \quad \{\ +\ \text{の法則}\ \} \\
 & x^{(m+n)+1} \\
= & \quad \{\ \text{ベキ関数の定義}\ \} \\
 & x * x^{m+n} \\
= & \quad \{\ \text{帰納法の仮定}\ \} \\
 & x * x^{m} * x^{n} \\
= & \quad \{\ \text{ベキ関数の定義}\ \} \\
 & x^{m+1} * x^{n}
\end{array}
$$

自然数の上の帰納法 2

自然数 n について，命題 $p(n)$ が成立することを帰納法によって証明するには，次のことを示す．

- *base* **ケース**． $P(0), P(1), \ldots, P(k)$ が成立する．
- *Inductive* **ケース**． $P(n), P(n+1), \ldots, p(n+k)$ が成立するならば，$P(n+k+1)$ も成立する．

例題

次のように定義されている関数

$$
\begin{aligned}
\mathsf{fib}\ 0 &= 0 \\
\mathsf{fib}\ 1 &= 1 \\
\mathsf{fib}\ (n+2) &= \mathsf{fib}\ n + \mathsf{fib}\ (n+1)
\end{aligned}
$$

に対して，$n \geq 1, m \geq 0$ であるすべての自然数について

$$\mathsf{fib}\ (n+m) = \mathsf{fib}\ n * \mathsf{fib}\ (m+1) + \mathsf{fib}\ (n-1) * \mathsf{fib}\ m$$

であることを証明せよ.

証明：m に関する帰納法で証明する．

場合 0.

$$
\begin{array}{ll}
& \mathsf{fib}\ (n+0) \\
= & \quad \{ + \text{の法則} \} \\
& \mathsf{fib}\ n \\
= & \quad \{ * \text{と} + \text{の法則} \} \\
& \mathsf{fib}\ n * 1 + \mathsf{fib}\ (n-1) * 0 \\
= & \quad \{ \mathsf{fib}\ \text{関数の定義} \} \\
& \mathsf{fib}\ n * \mathsf{fib}\ 1 + \mathsf{fib}\ (n-1) * \mathsf{fib}\ 0 \\
= & \quad \{ + \text{の法則} \} \\
& \mathsf{fib}\ n * \mathsf{fib}\ (0+1) + \mathsf{fib}\ (n-1) * \mathsf{fib}\ 0
\end{array}
$$

場合 1.

$$
\begin{array}{ll}
 & \mathsf{fib}\ (n+1) \\
= & \quad \{\ \mathsf{fib}\ 関数の定義\ \} \\
 & \mathsf{fib}\ n + \mathsf{fib}\ (n-1) \\
= & \quad \{\ *\ と\ +\ の法則\ \} \\
 & \mathsf{fib}\ n * 1 + \mathsf{fib}\ (n-1) * 1 \\
= & \quad \{\ \mathsf{fib}\ 関数の定義\ \} \\
 & \mathsf{fib}\ n * \mathsf{fib}\ 2 + \mathsf{fib}\ (n-1) * \mathsf{fib}\ 1 \\
= & \quad \{\ +\ の法則\ \} \\
 & \mathsf{fib}\ n * \mathsf{fib}\ (1+1) + \mathsf{fib}\ (n-1) * \mathsf{fib}\ 1
\end{array}
$$

場合 $m+2$

$$
\begin{aligned}
& \mathsf{fib}\ (n+m+2) \\
= & \quad \{\ \mathsf{fib}\ \text{関数の定義}\ \} \\
& \mathsf{fib}\ (n+m+1) + \mathsf{fib}\ (n+m) \\
= & \quad \{\ \text{帰納法の仮定}\ \} \\
& \mathsf{fib}\ n * \mathsf{fib}\ (m+2) + \mathsf{fib}\ (n-1) * \mathsf{fib}\ (m+1) + \\
& \mathsf{fib}\ n * \mathsf{fib}\ (m+1) + \mathsf{fib}\ (n-1) * \mathsf{fib}\ m \\
= & \quad \{\ * \text{ と } + \text{ の法則}\ \} \\
& \mathsf{fib}\ n * (\mathsf{fib}\ (m+2) + \mathsf{fib}\ (m+1)) + \mathsf{fib}\ (n-1) * (\mathsf{fib}\ (m+1) + \mathsf{fib}\ m) \\
= & \quad \{\ \mathsf{fib}\ \text{関数の定義}\ \} \\
& \mathsf{fib}\ n * \mathsf{fib}\ (m+2+1) + \mathsf{fib}\ (n-1) * \mathsf{fib}\ (m+2)
\end{aligned}
$$

リストの上の帰納法

任意の有限リスト x について $P(x)$ が成立することを帰納法で証明するには次の 2 つのことを示さなくてはならない.

- 場合 $[\,]$. $P([\,])$ が成立すること.
- 場合 $(a : x)$: $P(x)$ が成立すると仮定するとき，すべての a について $P(a : x)$ が成立すること.

問題：任意の有限リスト x, y, z に対して,

$$x +\!\!+ (y +\!\!+ z) = (x +\!\!+ y) +\!\!+ z$$

が成立することを証明せよ.

証明：x に関する帰納法で証明する.

- 場合 $[\,]$:

$$\begin{aligned}
& [\,] +\!\!+ (y +\!\!+ z) \\
= & \quad \{ \text{ def. of } +\!\!+ \text{ } \} \\
& y +\!\!+ z \\
= & \quad \{ \text{ def. of } +\!\!+ \text{ } \} \\
& ([\,] +\!\!+ y) +\!\!+ z
\end{aligned}$$

- 場合 $(a : x)$.

$$
\begin{array}{cl}
 & (a : x) +\!\!\!+ (y +\!\!\!+ z) \\
= & \quad \{ \text{ def. of } +\!\!\!+ \ \} \\
 & a : (x +\!\!\!+ (y +\!\!\!+ z)) \\
= & \quad \{ \text{ 帰納仮定 } \} \\
 & a : ((x +\!\!\!+ y) +\!\!\!+ z) \\
= & \quad \{ \text{ def. of } +\!\!\!+ \ \} \\
 & (a : (x +\!\!\!+ y)) +\!\!\!+ z \\
= & \quad \{ \text{ def. of } +\!\!\!+ \ \} \\
 & ((a : x) +\!\!\!+ y) +\!\!\!+ z
\end{array}
$$

問題：任意の有限リスト x, y に対して,

$$\mathsf{length}\ (x +\!\!+\, y) = \mathsf{length}\ x + \mathsf{length}\ y$$

が成立することを証明せよ.

証明：x に関する帰納法で証明する.

- 場合 $[\,]$:

$$\begin{aligned}
& \mathsf{length}\ ([\,] +\!\!+\, y) \\
= & \quad \{\ \text{def. of } +\!\!+\ \} \\
& \mathsf{length}\ y \\
= & \quad \{\ + \text{の法則}\ \} \\
& 0 + \mathsf{length}\ y \\
= & \quad \{\ \text{def. of } +\!\!+\ \} \\
& \mathsf{length}\ [\,] + \mathsf{length}\ y
\end{aligned}$$

- 場合 $(a : x)$.

$$
\begin{aligned}
& \mathsf{length}\ ((a : x) +\!\!+\, y) \\
= & \quad \{\ \text{def. of } +\!\!+\ \} \\
& \mathsf{length}\ (a : (x +\!\!+\, y)) \\
= & \quad \{\ \text{def. of } \mathsf{length}\ \} \\
& 1 + \mathsf{length}\ (x +\!\!+\, y) \\
= & \quad \{\ \text{帰納仮定}\ \} \\
& 1 + (\mathsf{length}\ x + \mathsf{length}\ y) \\
= & \quad \{\ + \text{の法則}\ \} \\
& (1 + \mathsf{length}\ x) + \mathsf{length}\ y \\
= & \quad \{\ \text{def. of } \mathsf{length}\ \} \\
& \mathsf{length}\ (a : x) + \mathsf{length}\ y
\end{aligned}
$$

問題：任意の自然数 n と有限リスト x に対して，

$$\mathsf{take}\ n\ x \mathbin{+\!\!+} \mathsf{drop}\ n\ x = x$$

が成立することを証明せよ．

$$\begin{array}{lcl}
\mathsf{take} & :: & \mathsf{Int} \rightarrow [a] \rightarrow [a] \\
\mathsf{take}\ 0\ x & = & [\,] \\
\mathsf{take}\ (n+1)\ [\,] & = & [\,] \\
\mathsf{take}\ (n+1)\ (a:x) & = & a : \mathsf{take}\ n\ x
\end{array}$$

$$\begin{array}{lcl}
\mathsf{drop} & :: & \mathsf{Int} \rightarrow [a] \rightarrow [a] \\
\mathsf{drop}\ 0\ x & = & x \\
\mathsf{drop}\ (n+1)\ [\,] & = & [\,] \\
\mathsf{drop}\ (n+1)\ (a:x) & = & \mathsf{drop}\ n\ x
\end{array}$$

証明：n と x に関する帰納法で証明する.

- 場合 $0, x$:

$$
\begin{array}{cl}
 & \mathsf{take}\ 0\ x \mathbin{+\!\!+} \mathsf{drop}\ 0\ x \\
= & \quad \{ \text{def. of } \mathsf{take} \text{ and } \mathsf{drop} \} \\
 & [\,] \mathbin{+\!\!+} x \\
= & \quad \{ \text{def. of } \mathbin{+\!\!+} \} \\
 & x
\end{array}
$$

- 場合 $n+1$, $[\,]$:

$$
\begin{array}{cl}
 & \mathsf{take}\ (n+1)\ [\,] \mathbin{+\!\!+} \mathsf{drop}\ (n+1)\ [\,] \\
= & \quad \{\ \text{def. of}\ \mathsf{take}\ \text{and}\ \mathsf{drop}\ \} \\
 & [\,] \mathbin{+\!\!+} [\,] \\
= & \quad \{\ \text{def. of}\ \mathbin{+\!\!+}\ \} \\
 & [\,]
\end{array}
$$

- 場合 $n+1$, $(a:x)$.

$$
\begin{aligned}
& \mathsf{take}\ (n+1)\ (a:x) \mathbin{+\!\!+} \mathsf{drop}\ (n+1)\ (a:x) \\
= & \quad \{\ \text{def. of } \mathsf{take} \text{ and } \mathsf{drop}\ \} \\
& (a:\mathsf{take}\ n\ x) \mathbin{+\!\!+} \mathsf{drop}\ n\ x \\
= & \quad \{\ \text{def. of } \mathbin{+\!\!+}\ \} \\
& a:(\mathsf{take}\ n\ x \mathbin{+\!\!+} \mathsf{drop}\ n\ x) \\
= & \quad \{\ \text{帰納仮定}\ \} \\
& a:x
\end{aligned}
$$

問題：任意の関数 f と g について,

$$\mathsf{map}\ f \circ \mathsf{map}\ g = \mathsf{map}\ (f \circ g)$$

が成立することを証明せよ.

証明：任意の有限リスト x について,

$$(\mathsf{map}\ f \circ \mathsf{map}\ g)\ x = (\mathsf{map}\ (f \circ g))\ x$$

が成立することを証明できればよい. (略)

補助定理と一般化

定理を証明する際に，直接行わないで，より一般的な結果の証明を試みると容易になることがある．

問題: 任意の x について,

$$\textsf{reservse}\ (\textsf{reverse}\ x) = x$$

が成立することを証明せよ.

$$\begin{array}{lcl} \textsf{reverse} & :: & [a] \to [a] \\ \textsf{reverse}\ [\,] & = & [\,] \\ \textsf{reverse}\ (a : x) & = & \textsf{reverse} +\!\!+ [a] \end{array}$$

x **について帰納法での証明はうまく行かない.**

補助定理: すべての a と有限リスト x について,

$$\text{reverse }(x +\!\!+ [a]) = a : \text{reverse }x$$

証明：x について帰納法で証明する.（略）

補助定理を使って,

$$\textsf{reservse}\ (\textsf{reverse}\ x) = x$$

を x に関する帰納法で証明する.

- 場合 $[\,]$.

$$\begin{array}{ll} & \textsf{reservse}\ (\textsf{reverse}\ [\,]) \\ = & \quad \{\ \text{def. of}\ \textsf{reverse}\ \} \\ & \textsf{reservse}\ [\,] \\ = & \quad \{\ \text{def. of}\ \textsf{reverse}\ \} \\ & [\,] \end{array}$$

- 場合 $(a : x)$.

$$
\begin{array}{cl}
 & \textsf{reservse}\ (\textsf{reverse}\ (a : x)) \\
= & \quad \{\ \text{def. of}\ \textsf{reverse}\ \} \\
 & \textsf{reservse}\ (\textsf{reverse}\ x +\!\!+ [a]) \\
= & \quad \{\ \text{補助定理}\ \} \\
 & a : \textsf{reverse}\ (\textsf{reverse}\ x) \\
= & \quad \{\ \text{帰納仮定}\ \} \\
 & a : x
\end{array}
$$

練習問題

- 教科書の 5.1, 5.2, 5.3, 5.4 を復習し，教科書中の練習問題をやること．