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

2008 年 12 月 8 日

自然数の上の帰納法

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．

自然数の上の帰納法

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

証明：m に関する帰納法で証明する.
場合 0.

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

証明

場合 $m + 1$.

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

自然数上のより一般的な帰納法

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．

- $P(0), P(1), \ldots, P(k)$ が成立する．
- $P(n), P(n+1), \ldots, p(n+k)$ 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

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

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

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

であることを証明せよ．

証明

証明：m に関する帰納法で証明する.
場合 0.

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

証明

場合 1.

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

証明

場合 $m+2$.

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

リスト上の帰納法

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.

例題 1

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.

復習：

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

例題 1

証明：x に関する帰納法で証明する.
場合 [ ].

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

例題 1

場合 $(a : x)$.

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

例題 2

問題：任意の有限リスト x, y に対して,

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

が成立することを証明せよ.

$$\begin{array}{lcl} \mathit{length} & :: & [\alpha] \to \mathit{Int} \\ \mathit{length}\ [\,] & = & 0 \\ \mathit{length}\ (a : x) & = & 1 + \mathit{length}\ x \end{array}$$

例題 2

証明：x に関する帰納法で証明する．
場合 $[\,]$.

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

例題 2

場合 $(a : x)$.

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

例題 3

問題：任意の自然数 n と有限リスト x に対して,

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

が成立することを証明せよ.

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

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

例題 3

証明：n と x に関する帰納法で証明する.
場合 0, x.

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

例題 3

場合 $n+1$, $[\,]$.

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

例題 3

場合 $n+1$, $(a : x)$.

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

例題 4

問題：任意の関数 f と g について，

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

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，

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

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，

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

が成立することを証明せよ．

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

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）

補助定理の利用

補助定理を使って,

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

を x に関する帰納法で証明する.

証明：場合 [ ].

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

補助定理の利用

場合 $(a : x)$.

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

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.