LA-009

高階関数型プログラムにおける帰納的定理証明
Proving Inductive Theorems of Higher-Order Functional Programs

青戸 等人 † 山田 俊行 ‡ 外山 芳人 †
Takahito Aoto Toshiyuki Yamada Yoshihito Toyama

1. まえがき

関数型プログラムを等式公理の集合と見なせば，プログラムにおいて成立する等式は，等式論理における帰納的定理に相当する．このため，等式論理における帰納的定理の自動証明法を活用すれば，仕様やプログラムの検証を効率化できる．

高階関数の利用は，関数型プログラムの特徴の 1 つである．しかし，帰納的定理の自動証明の研究対象として，高階関数を使うプログラムが取り上げられることは少なかった．この理由の 1 つは，高階関数型プログラムの帰納的定理の自動証明に必要な，高階項書換え系における停止性の自動証明が困難なことである．これに対して，λ 束縛を省いた高階項書換えの体系である単純型付き項書換え系 [4] に対しては，停止性の自動証明法が知られている [1].

本論文では，与えられた等式が，単純型付き項書換え系における帰納的定理であることを示す方法を与える．まず，従来の第 1 階項書換え系における帰納的定理証明法をそのまま適用し，その問題点を指摘する．次に，高階項書換え系に適した帰納的定理の定義を新しく導入する．最後に，この新しい枠組みのもとでの帰納的定理証明法を与え，具体例を示す．

2. 単純型付き項書換え系の帰納的定理証明

単純型付き項書換え系についての記法は文献 [1, 4] に従う．ただし，本論文では複数の基本型を許す．つまり，単純型付き項書換え系を，基本型集合 B，定数集合 C，単純型付き書換え規則の有限集合 R からなる組 $\langle B, C, R\rangle$ で与える．単純型付き項書換え系の合流性について，以下の結果が第 1 階項書換えの場合と同様に証明される．

定理 1 (合流条件) 停止性を持つ単純型付き項書換え系 $\mathcal{R}$ において，$\mathcal{R}$ が合流性を持つことの必要十分条件は $\mathcal{R}$ のすべての危険対が合流することである．

次の，抽象簡約系の等価条件が知られている．

命題 2 (抽象簡約系の等価性 [3]) 2 つの抽象簡約系 $\mathcal{A}_1 = \langle A, \to_1\rangle$ と $\mathcal{A}_2 = \langle A, \to_2\rangle$ が条件 (1) $\to_1 \subseteq \to_2$, (2) $\mathrm{WN}(\mathcal{A}_1)$, (3) $\mathrm{CR}(\mathcal{A}_2)$, (4) $\mathrm{NF}(\mathcal{A}_1) = \mathrm{NF}(\mathcal{A}_2)$, を満たすならば，$\leftrightarrow_1^* = \leftrightarrow_2^*$ が成立する．

ここで，$\mathrm{WN}(\mathcal{A})$ と $\mathrm{CR}(\mathcal{A})$ は抽象簡約系 $\mathcal{A}$ が弱停止性や合流性を持つことを，$\mathrm{NF}(\mathcal{A})$ は $\mathcal{A}$ の正規形集合を表す．

変数を含まない項を基底項と呼び，基底項集合上で成立する等式を帰納的定理という．関数型プログラムの評価式は基底項として与えられるので，帰納的定理は関数型プログラムの性質と見なせる．第 1 階項書換えの場合 [2] と同様，単純型付き項書換え系における帰納的定理証明法が命題 2 より導かれる．

定理 3 (単純型付き項書換え系の帰納的定理証明法 I) $\mathcal{R}_1 = \langle B, C, R_1\rangle$ を単純型付き項書換え系，l, r を単純型付き項とし，$\mathcal{R}_2 = \langle B, C, R_1 \cup \{l \to r\}\rangle$ とおく．また，S を $\mathcal{R}_1$ の被覆代入集合とする．条件 (1) $\mathrm{WN}_g(\mathcal{R}_1)$, (2) $\mathrm{CR}_g(\mathcal{R}_2)$, (3) $\forall\sigma \in S\ l\sigma \notin \mathrm{NF}(\mathcal{R}_1)$, が満たされるとき，$l = r$ は $\mathcal{R}_1$ の帰納的定理である．

ここで，$\mathrm{WN}_g(\mathcal{R})$ と $\mathrm{CR}_g(\mathcal{R})$ は $\mathcal{R}$ が基底項上で弱停止性や合流性を持つことを，$\mathrm{NF}(\mathcal{R})$ は $\mathcal{R}$ の正規項集合を表す．明らかに $\mathrm{WN}_g(\mathcal{R})$ と $\mathrm{CR}_g(\mathcal{R})$ は $\mathcal{R}$ の停止性や合流性からそれぞれ導かれる．また，$\mathcal{R}$ の被覆代入集合 S とは，任意の項 s と $\theta_g \in \Sigma_g(\Sigma_g$ は基底項代入集合) に対して，$s\theta_g$ が基底項 $\Longrightarrow \exists\sigma \in S \exists\theta'_g \in \Sigma_g(s\theta_g \to_{\mathcal{R}}^* s\sigma\theta'_g)$ が成立するものをいう．

例 4 (帰納的定理証明) $B = \{\ \mathrm{Nat}, \mathrm{List}\ \}$, $C = \{\ \mathsf{0}^{\mathrm{Nat}}, \mathsf{s}^{\mathrm{Nat}\to\mathrm{Nat}}, [\,]^{\mathrm{List}}, :^{\mathrm{Nat}\times\mathrm{List}\to\mathrm{List}}, \mathsf{append}^{\mathrm{List}\times\mathrm{List}\to\mathrm{List}}, \mathsf{map}^{(\mathrm{Nat}\to\mathrm{Nat})\times\mathrm{List}\to\mathrm{List}}\ \}$,

$$R_1 \left\{ \begin{array}{lcl} \mathsf{map}\ F\ [\,] & \to & [\,] \\ \mathsf{map}\ F\ (x : xs) & \to & (F\ x) : (\mathsf{map}\ F\ xs) \\ \mathsf{append}\ [\,]\ ys & \to & ys \\ \mathsf{append}\ (x : xs)\ ys & \to & x : (\mathsf{append}\ xs\ ys) \end{array} \right.$$

とし，単純型付き項書換え系 $\mathcal{R}_1 = \langle B, C, R_1\rangle$ を考える．このとき，定理 3 を使い，等式

$$\begin{array}{l} \mathsf{map}\ F\ (\mathsf{append}\ xs\ ys) \\ \qquad = \mathsf{append}\ (\mathsf{map}\ F\ xs)\ (\mathsf{map}\ F\ ys) \end{array} \tag{1}$$

が $\mathcal{R}_1$ の帰納的定理であることを示す．$\mathcal{R}_2 = \langle B, C, R_1 \cup \{(1)^{\to}\}\rangle$ とおく．ただし，$(1)^{\to}$ は等式 (1) の等号 $=$ を矢印 $\to$ に置き換えて得られる書換え規則を表す．論文 [1] の手法により，$\mathcal{R}_2$ の停止性が示され，これより $\mathrm{WN}_g(\mathcal{R}_1)$ が導かれる．また，$\mathcal{R}_2$ は 2 つの危険対を持つが，どちらも合流する．これと $\mathcal{R}_2$ の停止性と定理 1 により，$\mathcal{R}_2$ は合流性を持つ．従って $\mathrm{CR}_g(\mathcal{R}_2)$ が成立する．また，被覆代入集合 $S = \{\{xs \leftarrow [\,]\}, \{xs \leftarrow y : ys\}\}$ を考えると，条件 (3) が満たされる．

しかし，高階関数を用いる場合，定理 3 に基づく証明法にはいくつかの問題点がある．

例 5 (帰納的定理証明の失敗 I) $B = \{\ \mathrm{Nat},\ \mathrm{List}\ \}$, $C = \{\ \mathsf{0}^{\mathrm{Nat}}, \mathsf{s}^{\mathrm{Nat}\to\mathrm{Nat}}, [\,]^{\mathrm{List}}, :^{\mathrm{Nat}\times\mathrm{List}\to\mathrm{List}}, \mathsf{map}^{(\mathrm{Nat}\to\mathrm{Nat})\to(\mathrm{List}\to\mathrm{List})}, \circ^{(\mathrm{Nat}\to\mathrm{Nat})\times(\mathrm{Nat}\to\mathrm{Nat})\to(\mathrm{Nat}\to\mathrm{Nat})}, \bullet^{(\mathrm{List}\to\mathrm{List})\times(\mathrm{List}\to\mathrm{List})\to(\mathrm{List}\to\mathrm{List})}\ \}$,

$$R_1 \left\{ \begin{array}{lcl} (\mathsf{map}\ F)\ [\,] & \to & [\,] \\ (\mathsf{map}\ F)\ (x : xs) & \to & (F\ x) : ((\mathsf{map}\ F)\ xs) \\ (F \circ G)\ x & \to & F\ (G\ x) \\ (X \bullet Y)\ xs & \to & X\ (Y\ xs) \end{array} \right.$$

†東北大学電気通信研究所
‡三重大学工学部情報工学科

とし，単純型付き項書換え系 $\mathcal{R}_1 = \langle B, C, R_1 \rangle$ を考える．このとき，等式

$$\mathsf{map}\ (F \circ G) = (\mathsf{map}\ F) \bullet (\mathsf{map}\ G) \qquad (2)$$

が $\mathcal{R}_1$ の帰納的定理であると示したい．$\mathcal{R}_2 = \langle B, C, R_1 \cup \{(2)^{\rightarrow}\} \rangle$ とおく．$\mathrm{WN}_g(\mathcal{R}_1)$ と $\mathrm{CR}_g(\mathcal{R}_2)$ は例 4 と同様に導かれる．次に被覆代入集合を考えるが，等式 (2) の変数はすべて関数変数であるため，被覆代入集合を関数変数に対しても導入しないことには，条件 (3) が成立しない．

例 6 (帰納的定理証明の失敗 II) 例 5 において，C に定数 $\mathsf{maptwice}^{(\mathrm{Nat}\to\mathrm{Nat})\to(\mathrm{List}\to\mathrm{List})}$ を，R_1 に次の 2 つの書換え規則を追加する．

$$\begin{array}{lcl} \mathsf{maptwice}\ F & \to & \mathsf{map}\ (F \circ F) \\ \mathsf{maptwice}\ F & \to & (\mathsf{map}\ F) \bullet (\mathsf{map}\ F) \end{array}$$

このとき，等式

$$(\mathsf{map}\ (F \circ G))\ xs = ((\mathsf{map}\ F) \bullet (\mathsf{map}\ G))\ xs \qquad (3)$$

が $\mathcal{R}_1$ の帰納的定理であると示したい．$\mathcal{R}_2 = \langle B, C, R_1 \cup \{(3)^{\rightarrow}\} \rangle$ とおく．$\mathrm{WN}_g(\mathcal{R}_1)$ は例 4 と同様に導かれる．次に，$\mathrm{CR}_g(\mathcal{R}_2)$ を示すために，$\mathcal{R}_2$ の危険対 $\langle \mathsf{map}\ (F \circ G),\ (\mathsf{map}\ F) \bullet (\mathsf{map}\ F) \rangle$ を考えるが，これは合流しない．このため，定理 3 を用いる方法では，式 (3) が $\mathcal{R}_1$ の帰納的定理であることが示せない．

例 7 (帰納的定理証明の失敗 III) $B = \{\ \mathrm{Nat}\ \}$, $C = \{\ 0^{\mathrm{Nat}},\ \mathsf{s}^{\mathrm{Nat}\to\mathrm{Nat}},\ \mathsf{id}_0^{\mathrm{Nat}\to\mathrm{Nat}},\ \mathsf{id}_1^{\mathrm{Nat}\to\mathrm{Nat}}\ \}$,

$$R_1 \left\{ \begin{array}{lcl} \mathsf{id}_0\ 0 & \to & 0 \\ \mathsf{id}_0\ (\mathsf{s}\ x) & \to & \mathsf{s}\ (\mathsf{id}_0\ x) \\ \mathsf{id}_1\ x & \to & x \end{array} \right.$$

とし，単純型付き項書換え系 $\mathcal{R}_1 = \langle B, C, R_1 \rangle$ を考える．このとき，等式

$$\mathsf{id}_0 = \mathsf{id}_1 \qquad (4)$$

が $\mathcal{R}_1$ の帰納的定理であると示したい．$\mathcal{R}_2 = \langle B, C, R_1 \cup \{(4)^{\rightarrow}\} \rangle$ とおく．$\mathrm{WN}_g(\mathcal{R}_1)$ と $\mathrm{CR}_g(\mathcal{R}_2)$ は例 4 と同様に導かれる．しかし，どのような被覆代入集合を考えても，id_0 も id_1 も正規形であるため，条件 (3) が満たされない．従って，定理 3 を用いる方法では，式 (4) が $\mathcal{R}_1$ の帰納的定理であることが示せない．

このように，高階関数がある場合，第 1 階項書換え系での帰納的定理証明の枠組みをそのまま適用することは困難である．一方，高階関数を使う場合でも，関数型プログラムの評価式は基本型の基底項として与えられる．従って，単純型付き項書換え系の枠組みでは，第 1 階項書換えの場合とは異なる帰納的定理の定義をするのが自然である．

定義 8 (単純型付き項の外延拡張形) 単純型付き項 t の型を $\tau_{11} \times \cdots \times \tau_{1n_1} \to (\tau_{21} \times \cdots \times \tau_{2n_2} \to \cdots \to (\tau_{m1} \times \cdots \times \tau_{mn_m} \to \rho) \cdots)$ (ただし，$\rho \in B$) とおく．このとき，互いに異なる新変数 $x_{11}, \ldots, x_{mn_m}$ を付加して得られる項 $((\cdots((t\ x_{11} \cdots x_{1n_1})\ x_{21} \cdots x_{2n_2}) \cdots)\ x_{m1} \cdots x_{mn_m})$ を t の外延拡張形と呼び，$t{\uparrow}$ で表す．

定義 9 (単純型付き項書換え系における帰納的定理) $\mathcal{R} = \langle B, C, R \rangle$ を単純型付き項書換え系，l, r を単純型付き項とする．等式 $l = r$ が帰納的定理であるとは，任意の $\theta_g \in \Sigma_g$ について，$l{\uparrow}\theta_g \leftrightarrow^*_{\mathcal{R}} r{\uparrow}\theta_g$ が成立することをいう．

基本型の項 t の外延拡張形は t 自身なので，この帰納的定理の定義は，第 1 階項書換え系の場合の拡張になっている．新しい定義のもとで，以下の定理が成立する．

定理 10 (単純型付き項書換え系の帰納的定理証明法 II) $\mathcal{R}_1 = \langle B, C, R_1 \rangle$ を単純型付き項書換え系，l, r を単純型付き項とし，$\mathcal{R}_2 = \langle B, C, R_1 \cup \{l{\uparrow} \to r{\uparrow}\} \rangle$ とおく．また，S を $\mathcal{R}_1$ の被覆代入集合とする．条件 (1) $\mathrm{WN}^B_g(\mathcal{R}_1)$，(2) $\mathrm{CR}^B_g(\mathcal{R}_2)$，(3) $\forall \sigma \in S\ l{\uparrow}\sigma \notin \mathrm{NF}(\mathcal{R}_1)$，が満たされるとき，$l = r$ は $\mathcal{R}_1$ の帰納的定理である．

ここで，$\mathrm{WN}^B_g(\mathcal{R})$ と $\mathrm{CR}^B_g(\mathcal{R})$ は $\mathcal{R}$ が基本型の基底項上で弱停止性や合流性を持つことを表す．

例 11 (帰納的定理証明 II) 例 5 の帰納的定理証明を考える．このとき，等式 (2) の両辺の項を外延拡張形にすると等式 (3) になる．すると，被覆代入集合 $S = \{\{xs \leftarrow [\,]\}, \{xs \leftarrow y : ys\}\}$ を考えることにより条件 (3) が満たされ，等式 (2) が $\mathcal{R}_1$ の帰納的定理であることが上記の定理により導かれる．

例 12 (帰納的定理証明 III) 例 6 の帰納的定理証明を考える．このとき，$\mathrm{CR}^B_g(\mathcal{R}_2)$ は容易に示せる．従って，等式 (3) が $\mathcal{R}_1$ の帰納的定理であることが上記の定理により導かれる．

例 13 (帰納的定理証明 IV) 例 7 の帰納的定理証明を考える．このとき，等式 (4) の両辺を外延拡張形にすると等式 $\mathsf{id}_0\ x = \mathsf{id}_1\ x$ が得られる．すると，被覆代入集合 $S = \{\{x \leftarrow 0\}, \{x \leftarrow \mathsf{s}\ y\}\}$ により条件 (3) が成立し，従って，等式 (4) が $\mathcal{R}_1$ の帰納的定理であることが上記の定理により導かれる．

参考文献

[1] 青戸等人, 山田俊行. 単純型付き項書換え系における停止性の自動証明. 情報処理学会論文誌：プログラミング, Vol. 44, No. SIG 4 (PRO 17), pp. 67–77, 2003.

[2] 小池広高, 外山芳人. 潜在帰納法と書換え帰納法の比較. コンピュータソフトウェア, Vol. 17, No. 6, pp. 1–12, 2000.

[3] Y. Toyama. How to prove equivalence of term rewriting systems without induction. *Theoretical Computer Science*, Vol. 90, pp. 369–390, 1991.

[4] T. Yamada. Confluence and termination of simply typed term rewriting systems. In *Proceedings of the 12th International Conference on Rewriting Techniques and Applications*, Vol. 2051 of *LNCS*, pp. 338–352. Springer-Verlag, 2001.