文脈移動法によるプログラム変換の正当性について

菊池 健太郎　青戸 等人　外山 芳人

プログラムの自動検証を容易にすることを目的としたプログラム変換法として，Giesl(2000) により文脈移動法および文脈分割法が提案されている．それらの手法は，先行評価の関数型言語における末尾再帰プログラムを自動検証に適した非末尾再帰プログラムへと変換する．本稿では，佐藤ら (2015) によって定式化された項書き換えシステムに対する文脈移動法の正当性を，先行評価に基づく意味論と始代数に基づく意味論に対して証明し，二種類の意味論における正当性の違いについて説明する．

1　はじめに

末尾再帰プログラムは，最後の再帰呼び出しの結果を返り値に用い，呼び出し時の実行状態を保持する必要のない効率的なプログラムである．末尾再帰プログラムは，一般に計算の途中結果を保存するためアキュムレータとよばれる引数をもつ．しかし，その値は再帰呼び出しで変化するため，末尾再帰プログラムに対して帰納法に基づく自動証明を適用することは困難であることが知られている．

Giesl [2] は，先行評価の関数型プログラムを対象に，検証のための変換法として文脈移動法・文脈分割法を提案した．それらの手法は，適当な条件のもとで，末尾再帰プログラムを等価な非末尾再帰プログラムへと変換する．変換で得られた非末尾再帰プログラムは，帰納法による自動証明に適した構造となっている．

本稿では，佐藤ら [4] によって定式化された項書き換えシステムに対する文脈移動法の正当性を，先行評価に基づく意味論と始代数に基づく意味論に対して証明し，二種類の意味論における正当性の違いについて説明する．

On the Correctness of Context-Moving Transformations.
Kentaro Kikuchi, Takahito Aoto, Yoshihito Toyama, 東北大学電気通信研究所, Research Institute of Electrical Communication, Tohoku University.

2　準備

本節では，項書き換えシステムに関する用語や概念を文献 [1] に従って定義する．

関数記号と変数の集合をそれぞれ $\mathcal{F}, \mathcal{V}$ とする．$\mathcal{F}, \mathcal{V}$ で構成できる項全体の集合を $\mathcal{T}(\mathcal{F}, \mathcal{V})$ と記す．項 t に含まれる変数全体の集合を $\mathcal{V}(t)$，関数記号全体の集合を $\mathcal{F}(t)$ で表す．項の列 $t_1, t_2, \ldots, t_n$ を $\bar{t}$ で表す．このとき $\mathcal{V}(\bar{t}) = \bigcup_{i=1}^{n} \mathcal{V}(t_i)$，$\mathcal{F}(\bar{t}) = \bigcup_{i=1}^{n} \mathcal{F}(t_i)$ と定める．$\mathcal{V}(t) = \emptyset$ であるとき項 t を基底項とよび，基底項の集合を $\mathcal{T}(\mathcal{F})$ で表す．項 t の根記号 $root(t)$ は，$t \in \mathcal{V}$ のとき t，$t = f(t_1, \ldots, t_n)$ のとき f である．特別な定数記号 $\Box$ をちょうど 1 つ含む項を文脈とよび，文脈 C の $\Box$ を t で置き換えた項を $C[t]$ で表す．文脈 C は $C[\,]$ とも表す．写像 $\theta : \mathcal{V} \to \mathcal{T}(\mathcal{F}, \mathcal{V})$ を代入とよび，$\theta : \mathcal{T}(\mathcal{F}, \mathcal{V}) \to \mathcal{T}(\mathcal{F}, \mathcal{V})$ へ自然に拡張する．代入 $\theta_g : \mathcal{V} \to \mathcal{T}(\mathcal{F})$ を基底代入とよぶ．以下では $\theta(t)$ を $t\theta$ と表記する．

項の対 (l, r) が $l \notin \mathcal{V}$ かつ $\mathcal{V}(l) \supseteq \mathcal{V}(r)$ をみたすとき (l, r) を書き換え規則といい，$l \to r$ と表す．項書き換えシステム R は書き換え規則の有限集合である (なお，項書き換えシステム中の変数は必要に応じて名前替えを行う)．項書き換えシステム R の定義関数記号の集合を $\mathcal{D} = \{root(l) \mid l \to r \in R\}$，$R$ の構成子記

号の集合を $\mathcal{C} = \mathcal{F} \setminus \mathcal{D}$ と定める．項 $v \in \mathcal{T}(\mathcal{C}, \mathcal{V})$ を構成子項という．項書き換えシステム R のすべての書き換え規則 $f(l_1, \ldots, l_n) \to r$ について $l_i (1 \leq i \leq n)$ が構成子項であるとき，R を構成子システムとよぶ．項 $v \in \mathcal{T}(\mathcal{C})$ を基底構成子項という．$\theta_{gc} : \mathcal{V} \to \mathcal{T}(\mathcal{C})$ を基底構成子代入とよぶ．

3 項書き換えシステムに対する文脈移動法

本節では，文献[4] で定式化された項書き換えシステムに対する文脈移動法の正当性が，先行評価に基づく意味論と始代数に基づく意味論において成り立つことを示す．また，それらの意味論における正当性の違いについて議論する．

3.1 文脈移動法による項書き換えシステムの変換

関数型プログラムの文脈移動法[2] は，末尾再帰呼び出しにおけるアキュムレータ位置の文脈を，再帰呼び出しの外側に移動する．項書き換えシステムに対する文脈移動法[4] も同様な考え方に基づいて定式化される．

定義 3.1 (項書き換えシステムに対する文脈移動法)．項書き換えシステムに対する文脈移動法は，以下の項書き換えシステム R から R' への変換である．

$R = R_A \cup R_B \cup R_C$
$R_A = \{f(\bar{l}_i, z) \to f(\bar{r}_i, C_i[z]) \mid 1 \leq i \leq m\}$
$R_B = \{f(\bar{l}_j, z) \to C_j[z] \mid m+1 \leq j \leq n\}$
$R_C = \{l_k \to r_k \mid n+1 \leq k \leq p\}$
$R' = R'_A \cup R_B \cup R_C$
$R'_A = \{f(\bar{l}_i, z) \to C_i[f(\bar{r}_i, z)] \mid 1 \leq i \leq m\}$

R_A, R'_A は m 個の f の再帰規則，R_B は $n-m$ 個の f の非再帰規則，R_C は $p-n$ 個の補助関数の書き換え規則を表す．関数記号 f を変換対象，文脈 $C_1[\,], \ldots, C_n[\,]$ を移動文脈，変数 z をアキュムレータとよぶ．変換対象 f とアキュムレータ z は上記の変換規則で明示された場所以外には出現しないものとする．すなわち，以下の (i), (ii) を仮定する．(i) $f \notin (\bigcup_{i=1}^{m} \mathcal{F}(\bar{l}_i, \bar{r}_i, C_i)) \cup (\bigcup_{j=m+1}^{n} \mathcal{F}(\bar{l}_j, C_j)) \cup (\bigcup_{k=n+1}^{p} \mathcal{F}(l_k, r_k))$．(ii) $z \notin (\bigcup_{i=1}^{m} \mathcal{V}(\bar{l}_i, \bar{r}_i, C_i)) \cup (\bigcup_{j=m+1}^{n} \mathcal{V}(\bar{l}_j, C_j))$．

例 3.2 (文脈移動法による変換例)．乗算を行う次の項書き換えシステム R を考える．

$$R = \begin{cases} Mult(S(x), y, z) \to Mult(x, y, Add(y, z)) \\ Mult(0, y, z) \to z \\ Add(S(x), y) \to S(Add(x, y)) \\ Add(0, y) \to y \end{cases}$$

関数記号 $Mult$ を変換対象，z をアキュムレータとして文脈移動法を適用する．R の規則は以下のように分割される．

$$R_A = \{Mult(S(x), y, z) \to Mult(x, y, Add(y, z))$$
$$R_B = \{Mult(0, y, z) \to z$$
$$R_C = \begin{cases} Add(S(x), y) \to S(Add(x, y)) \\ Add(0, y) \to y \end{cases}$$

ここで，移動文脈は $C_1 = Add(y, \Box)$, $C_2 = \Box$ である．このとき

$$R'_A = \{Mult(S(x), y, z) \to Add(y, Mult(x, y, z))$$

となる．よって，以下の項書き換えシステム R' が得られる．

$$R' = \begin{cases} Mult(S(x), y, z) \to Add(y, Mult(x, y, z)) \\ Mult(0, y, z) \to z \\ Add(S(x), y) \to S(Add(x, y)) \\ Add(0, y) \to y \end{cases}$$

□

本節の残りでは，二種類の意味論における文脈移動法の正当性について議論する．

3.2 先行評価意味論における文脈移動法の正当性

まず，文献[2] と同様な先行評価に基づく意味論における文脈移動法の正当性について議論する．本小節では，文脈移動法による変換の対象となる項書き換えシステムとして，構成子システム R を考える．

項 s が項 t に先行戦略によって書き換えられるとは，書き換え規則 $l \to r \in R$，文脈 $C[\,]$，基底構成子代入 θ_{gc} が存在して，$s = C[l\theta_{gc}]$ かつ $t = C[r\theta_{gc}]$ となることである．以下では，決定性をもつ書き換えを考え，s が t に書き換えられるとき $s \xrightarrow{\mathrm{ev}}_R t$ と記す．$\xrightarrow{\mathrm{ev}}_R$ の反射推移閉包を $\xrightarrow{\mathrm{ev}}{}^*_R$ で表す．$s \equiv^{\mathrm{ev}}_R t$ とは，任意の基底構成子項 v に対して，$s \xrightarrow{\mathrm{ev}}{}^*_R v$ が成り立つとき，かつそのときに限り $t \xrightarrow{\mathrm{ev}}{}^*_R v$ が成り立つことである．

先行評価意味論における文脈移動法の正当性を保証するため，文献[2] を参考に，移動文脈の交換律を以下で定義する．

定義 3.3 (文脈交換律)．$C_1[\,], \ldots, C_n[\,]$ を移動文脈とする．このとき，以下の条件を文脈交換律とよぶ．

$$\forall i(1 \leq i \leq m).\forall j(1 \leq j \leq n).\forall \theta_{gc}.$$
$$C_i[C_j[z]]\theta_{gc} \overset{\mathrm{ev}}{\equiv}_R C_j[C_i[z]]\theta_{gc} \qquad (\mathsf{CCOM}^{\mathrm{ev}})$$

ただし，$C_i[\,], C_j[\,]$ は共通変数をもたないように，変数の名前替えを行う．

例 3.4 (文脈交換律の例)．例 3.2 の文脈移動法による変換を考える．移動文脈は，$C_1 = Add(y, \Box)$ $(m = 1)$, $C_2 = \Box$ $(n = 2)$ であるから，文脈交換律の条件 ($\mathsf{CCOM}^{\mathrm{ev}}$) は，$\forall \theta_{gc}.Add(x, Add(y, z))\theta_{gc} \overset{\mathrm{ev}}{\equiv}_R Add(y, Add(x, z))\theta_{gc}$ となる． □

定義 3.5 ($R \overset{\mathrm{ev}}{\Rightarrow}^f_{\mathrm{cm}} R'$)．$R$ を構成子システムとする．関数記号 f を変換対象とする文脈移動法によって R から R' が得られ，文脈交換律の条件 ($\mathsf{CCOM}^{\mathrm{ev}}$) がみたされているとき，$R \overset{\mathrm{ev}}{\Rightarrow}^f_{\mathrm{cm}} R'$ と書く．

以下の補題が成り立つ (証明は文献[5] を参照)．

補題 3.6. $R \overset{\mathrm{ev}}{\Rightarrow}^f_{\mathrm{cm}} R'$ とし，$1 \leq i \leq m$ とする．任意の基底構成子代入 θ_{gc} と基底項 $\bar{t}, u$，基底構成子項 v に対して，以下が成立する．

1. $C_i\theta_{gc}[f(\bar{t}, u)] \overset{\mathrm{ev}}{\to}^*_R v$ ならば $f(\bar{t}, C_i\theta_{gc}[u]) \overset{\mathrm{ev}}{\to}^*_R v$.
2. $f(\bar{t}, C_i\theta_{gc}[u]) \overset{\mathrm{ev}}{\to}^*_{R'} v$ ならば $C_i\theta_{gc}[f(\bar{t}, u)] \overset{\mathrm{ev}}{\to}^*_{R'} v$.

上の補題を用いて，先行評価意味論における文脈移動法の正当性が示される．

定理 3.7. $R \overset{\mathrm{ev}}{\Rightarrow}^f_{\mathrm{cm}} R'$ とする．任意の基底項 s と基底構成子項 v に対して，$s \overset{\mathrm{ev}}{\to}^*_R v$ が成り立つとき，かつそのときに限り $s \overset{\mathrm{ev}}{\to}^*_{R'} v$ が成り立つ．

3.3 始代数意味論における文脈移動法の正当性

前小節で示された文脈移動法の正当性は，文脈交換律の条件 ($\mathsf{CCOM}^{\mathrm{ev}}$) に基づいているが，それは先行評価の概念に依存しており，始代数上の等式に対応するとは限らない．本小節では，始代数上の等式に正確に対応する文脈交換律の条件に基づいて，前小節とは異なる文脈移動法の正当性を示す．

はじめに，項書き換えシステムにおける標準的な定義をいくつか導入する．項 s が項 t に書き換えられるとは，書き換え規則 $l \to r \in R$，文脈 $C[\,]$，代入 θ が存在して，$s = C[l\theta]$ かつ $t = C[r\theta]$ をみたすことであり，このとき $s \to_R t$ と記す．$\to_R$ の反射推移閉包を $\overset{*}{\to}_R$ で表す．$s \to_R t$ となる t が存在しないとき s を正規形という．$t \overset{*}{\to}_R s$ かつ s が正規形であるとき s は t の正規形であるという．t の正規形 s が存在して一意に定まるとき，s を $t{\downarrow_R}$ と記す．任意の基底項 t, t_1, t_2 について $t \overset{*}{\to}_R t_1$ かつ $t \overset{*}{\to}_R t_2$ ならばある基底項 s が存在して $t_1 \overset{*}{\to}_R s$ かつ $t_2 \overset{*}{\to}_R s$ となるとき R は基底合流性をもつという．任意の基底項 s に対してある基底構成子項 v が存在して $s \overset{*}{\to}_R v$ が成立するとき，R は十分完全性[3] をもつという．R が基底合流性と十分完全性をもつとき，任意の基底項 s に対して $s{\downarrow_R}$ が定義され，基底構成子項となる．本小節では，変換対象として，基底合流性と十分完全性をもつ項書き換えシステム R を考える．

本小節で考える意味論における文脈移動法の正当性を保証するため，移動文脈の交換律を以下で定義する．

定義 3.8 (文脈交換律)．$C_1[\,], \ldots, C_n[\,]$ を移動文脈とする．このとき，以下の条件を文脈交換律とよぶ．

$$\forall i(1 \leq i \leq m).\forall j(1 \leq j \leq n).\forall \theta_g.$$
$$C_i[C_j[z]]\theta_g{\downarrow_R} = C_j[C_i[z]]\theta_g{\downarrow_R} \qquad (\mathsf{CCOM})$$

ただし，$C_i[\,], C_j[\,]$ は共通変数をもたないように，変数の名前替えを行う．

定義 3.3 における条件 ($\mathsf{CCOM}^{\mathrm{ev}}$) とは異なり，上の条件 ($\mathsf{CCOM}$) は，$R$ の始代数上で成り立つ等式，すなわち R の帰納的定理に対応する．したがって，帰納的定理証明器による検証が可能である．

定義 3.9 ($R \Rightarrow^f_{\mathrm{cm}} R'$)．$R$ を基底合流性と十分完全性をもつ項書き換えシステムとする．関数記号 f を変換対象とする文脈移動法によって R から R' が得られ，文脈交換律の条件 (CCOM) がみたされているとき，$R \Rightarrow^f_{\mathrm{cm}} R'$ と書く．

以下の補題が成り立つ (証明は文献[5] を参照)．

補題 3.10. $R \Rightarrow^f_{\mathrm{cm}} R'$ のとき，任意の基底代入 $\theta_{g\setminus f} : \mathcal{V} \to \mathcal{T}(\mathcal{F} \setminus \{f\})$ と基底構成子項 v に対して，$f(\bar{x}, z)\theta_{g\setminus f} \overset{*}{\to}_R v$ ならば $f(\bar{x}, z)\theta_{g\setminus f} \overset{*}{\to}_{R'} v$ が成立する．

補題 3.11. $R \Rightarrow^f_{\mathrm{cm}} R'$ のとき，任意の基底項 s と基底構成子項 v に対して，$s \overset{*}{\to}_R v$ ならば $s \overset{*}{\to}_{R'} v$ が

成立する．

補題 3.12. $R \Rightarrow^{f}_{\mathrm{cm}} R'$ のとき，R' は十分完全性をもつ．

補題 3.13. $R \Rightarrow^{f}_{\mathrm{cm}} R'$ のとき，任意の基底項 s と基底構成子項 v に対して，$s \xrightarrow{*}_{R'} v$ ならば $s \xrightarrow{*}_{R} v$ が成立する．

補題 3.14. $R \Rightarrow^{f}_{\mathrm{cm}} R'$ のとき，R' は基底合流性をもつ．

以上より，前小節とは異なる文脈移動法の正当性を表す次の定理が示される．

定理 3.15. $R \Rightarrow^{f}_{\mathrm{cm}} R'$ であるとき，任意の基底項 s について $s{\downarrow_R} = s{\downarrow_{R'}}$ が成立する．

例 3.16. 本例では，ソート Nat と $NatStream$ をもつ多ソート項書き換えシステム R を考える．ここで，ソート $Nat \times NatStream \to NatStream$ をもつ ":" は，ソート $NatStream$ の唯一の構成子記号である．

$$R = \left\{ \begin{array}{ll} (a) & Sum(S(x), \alpha, z) \to \\ & \qquad Sum(x, Tl(\alpha), Add(Hd(\alpha), z)) \\ (b) & Sum(0, \alpha, z) \to z \\ (c) & Hd(x : \alpha) \to x \\ (d) & Tl(x : \alpha) \to \alpha \\ (e) & Inc \to 0 : Succ(Inc) \\ (f) & Succ(x : \alpha) \to S(x) : Succ(\alpha) \\ (g) & Add(S(x), y) \to S(Add(x, y)) \\ (h) & Add(0, y) \to y \end{array} \right.$$

関数記号 Sum を変換対象，z をアキュムレータとして文脈移動法を適用する．ここで，ソート Nat の項に対しては十分完全性が成り立つ．すなわち，ソート Nat の任意の基底項は，ある基底構成子項に書き換えられる．R の規則は $R_A = \{(a)\}$, $R_B = \{(b)\}$, $R_C = \{(c)\text{–}(h)\}$ のように分割される．移動文脈は $C_1 = Add(Hd(\alpha), \Box)$, $C_2 = \Box$ である．このとき

$$R'_A = \left\{ \begin{array}{ll} (a)' & Sum(S(x), \alpha, z) \to \\ & \qquad Add(Hd(\alpha), Sum(x, Tl(\alpha), z)) \end{array} \right.$$

となる．また

$$\forall \theta_g . Add(Hd(\alpha), Add(Hd(\beta), z))\theta_g{\downarrow_R} = Add(Hd(\beta), Add(Hd(\alpha), z))\theta_g{\downarrow_R} \quad (\mathsf{CCOM})$$

が成立する．したがって，$R \Rightarrow^{Sum}_{\mathrm{cm}} R'$ が成り立ち，$R' = R'_A \cup \{(b)\text{–}(h)\}$ が得られる．

以上の変換において，ソート Nat の項に対しては，本小節で行った文脈移動法の正当性に関する議論が成立する (ソート $NatStream$ の項に対しては，定理 3.15 の形での変換の正当性は要求しない)．

この変換に対しては，定理 3.7 による文脈移動法の正当性も成立する．しかし，関数記号 Inc を含む基底項については，規則 (e) により先行戦略による書き換えが停止しない．したがって，それらの項に対して定理 3.7 で示されることは，書き換えの非停止性が変換によって保存されるということのみである． □

4 おわりに

本稿では，項書き換えシステムに対する文脈移動法の正当性が，先行評価意味論と始代数意味論という二種類の意味論において成立することを示した．また，それらの意味論における正当性の違いを明らかにする例を与えた．それぞれの正当性を保証するための条件を判定する手続きの実装については今後の課題である．

参 考 文 献

[1] F. Baader and T. Nipkow. *Term Rewriting and All That*. Cambridge University Press, 1998.

[2] J. Giesl. Context-moving transformations for function verification. In *Proc. of 9th LOPSTR*, volume 1817 of *LNCS*, pages 293–312. Springer-Verlag, 2000.

[3] D. Kapur, P. Narendran, and H. Zhang. On sufficient-completeness and related properties of term rewriting systems. *Acta Informatica*, 24(4):395–415, 1987.

[4] 佐藤洸一, 菊池健太郎, 青戸等人, 外山 芳人. 項書き換えシステムの変換を利用した帰納的定理自動証明. コンピュータソフトウェア, 32(1):179–193, 2015.

[5] K. Sato, K. Kikuchi, T. Aoto, and Y. Toyama. Correctness of context-moving transformations for term rewriting systems. In *Pre-proc. of 25th LOPSTR*, 2015. Available at `http://www.nue.riec.tohoku.ac.jp/user/kentaro/cntxt/`.