情報処理学会論文誌　プログラミング　Vol. 2　No. 2　80–96 (Mar. 2009)

制約付き項書換え系における書換え帰納法

坂田　翼[†1]　西田直樹[†1]　坂部俊樹[†1]
酒井正彦[†1]　草刈圭一朗[†1]

帰納的定理の証明原理の 1 つである潜在帰納法が制約付き項書換え系に対応するように拡張され，命令型プログラムの等価性検証に応用されている．本論文では，別の証明原理である書換え帰納法を制約付き項書き換え系に対応するように拡張するとともに，その正しさを証明する．また，拡張された書換え帰納法に基づいた帰納的定理の証明法を提案する．さらに，帰納的定理でないことを示す反証の手法についても議論する．

Rewriting Induction for Constrained Term Rewriting Systems

Tsubasa Sakata,[†1] Naoki Nishida,[†1] Toshiki Sakabe,[†1]
Masahiko Sakai[†1] and Keiichirou Kusakari[†1]

The implicit induction, which is one of induction principles for proving inductive theorems of equational theories, has been extended to deal with constrained term rewriting systems. It has been applied to a method for proving equivalence of imperative programs. In this paper, we extend another induction principle, the rewriting induction, to cope with the case of constrained term rewriting systems, and show its correctness. We also propose a method for proving inductive theorems being based on the extended rewriting induction. Moreover, we show a technique to disprove inductive theorems.

†1 名古屋大学大学院情報科学研究科
Graduate School of Information Science, Nagoya University

1. はじめに

命令型プログラムと関数型プログラムでは，それぞれにプログラム検証手法の研究がされている．命令型プログラムに対しては，モデル検査[8),16),19)] やホーア論理に基づく検証手法[11),14),16)] が代表的である．しかし，モデル検査では仕様を満たす検査式の付与など，ホーア論理ではループ不変式の発見や事前条件・事後条件の付与などといったヒューリスティックな作業が必要であり，検証の自動化は困難である．一方，関数型プログラムに対しては，帰納的定理の自動証明手法である潜在帰納法[15),17)] や書換え帰納法[4),20)] などが項書換え系上で広く研究されている．関数の等価性は項書換え系における帰納的定理として定式化できるので，等価性検証に帰納的定理の自動証明法を利用できる．しかし，入力によっては検証手続きが暴走し，検証が失敗することがある．自然数の比較演算子を用いた項書換え系の検証では，手続きが暴走してしまうことが多い．

命令型プログラムの等価性を，制約付き項書換え系の帰納的定理に帰着させて検証する手法が潜在帰納法に基づいて提案された[24)]．この手法は制約の意味論が特定されている環境を対象とした枠組みであり，制約の真偽判定と項の書換えを分離させた体系で帰納的定理の検証を行う．この手法の実際の手続きは制約付き項書換え系の完備化手続きである．この手法により，自然数の比較演算子が原因で起こる検証手続きの暴走を抑えることが可能になった．しかし，この手法では等式の制約部分の分解の処理の自動化という新たな課題が出現した．これは，完備化手続きに基づいた手法では，帰納的定理の証明に適した分解の指針を明らかにしにくいことが原因である．また，文献 24) の手法で整数を慣例的な表現で扱うと，完備化手続きが暴走し，検証に失敗することが多い．完備化手続きでの制限の下では本質的に整数の扱いが難しい．

本論文では，制約付き項書換え系における帰納的定理を書換え帰納法によって検証する方法を提案する．これは，項書換え系における書換え帰納法の推論規則を制約付き項書換え系に対応するように拡張することによって実現する．しかし，制約付き項書換え系の書換え関係では項書換え系には存在しない制約の意味を考慮しなければならない．このため，拡張した推論規則が健全であるためには，制約に含まれる変数に代入する項の部分を書き換えると制約の真偽値が変化するという問題を解決する必要がある．また，意味論での等式と書換え関係での等価関係との対応関係を考慮しなければ帰納的定理であることを検証できない例が存在する．そこで，本論文では，制約付き項書換え系が制約に与えられている意味論に対して満たすべき性質を明らかにし，それらの性質が成り立つときには提案した推論規則で構

成される書換え帰納法の証明手続きが正しいことを示す．本論文で提案する検証手続きが停止したとき，成功であれば入力のすべての等式は帰納的定理であり，そうでないならば入力した等式が帰納的定理であるかは不明である．また，手続きが停止せず暴走してしまう場合もある．

さらに，本論文では帰納的定理の反証法についても提案する．書換え帰納法による検証手続きに反証機能を組み込むことにより，帰納的定理であることを証明すると同時に帰納的定理の反証も可能にする．反証を手続きに導入することで，反証を導入しない手続きでは停止するが成功でない場合には入力に帰納的定理でない等式が含まれていることを示すことが可能な場合が生じる．帰納的定理でないことが分かった場合には，補題等式などを追加して再度検証する必要がないことを示せる．さらに，入力に帰納的定理でない等式が含まれていながら手続きが暴走している場合，反証を行うことにより停止して帰納的定理でない等式の証明を得られる場合もある．よって，手続きの暴走を抑制することを期待できる．

また，本論文では入力として与える制約付き項書換え系の正規形すべての意味が解釈可能である場合に書換え帰納法の推論規則の適用条件を緩和できることを示す．本論文で提案した書換え帰納法では交換律を含む等式の多くは証明することが難しい．しかし，適用条件を緩和した推論規則を用いれば，制約の意味論を定めるモデル上で等価だと証明できる交換律は帰納的定理であるということが証明できる．たとえば，加算，乗算の交換律，結合律，分配律からなる複雑な等式であっても，モデルで等価だと判定できれば帰納的定理であるという証明が可能となる．よって，拡張した書換え帰納法の検証手続きをより強力にすることができる．

本論文は次のように構成される．2 章では抽象書換え系，項，制約に関する記法を説明する．3 章では制約付き項書換え系の定義を与え，意味論に対して満たすべき性質を提案する．また，それらの性質の十分条件，必要十分条件を示す．4 章では制約付き項書換え系における書換え帰納法について提案する．5 章では R 完全な出現の判定法について提案する．6 章では制約付き項書換え系における帰納的定理の反証法を提案する．7 章では拡張された書換え帰納法の推論規則の適用条件の緩和について議論する．8 章では関連研究との比較を述べ，9 章では今後の課題をあげる．

2. 準　　備

本論文では，項書換え系の一般的な記法に従う[3]．

抽象書換え系 S は，対象となる集合 A と A 上の**簡約化関係**と呼ばれる二項関係 $\rightarrow$ の組 $(A, \rightarrow)$ である．$a \rightarrow b$ となるような b が存在しないとき，a は S の**正規形**という．このとき，$c \stackrel{*}{\rightarrow} a$ である $c \in A$ について，c **は** S **における正規形を持つ**という．S の正規形の集合を NF_S で表す．$a \stackrel{*}{\rightarrow} c \stackrel{*}{\leftarrow} b$ となるような $c \in A$ が存在するとき，a と b は**会同関係にある**といい，$a \downarrow b$ と表記する．任意の $x, y \in A$ に対して $x \stackrel{*}{\leftrightarrow} y$ ならば $x \downarrow y$ のとき，S は**チャーチ・ロッサー（CR）性**を持つという．任意の $a \in A$ に対して a から始まる $\rightarrow$ の無限系列が存在しないとき，S は**停止性**（または**強正規性**）を持つという．$(A, \rightarrow_1)$，$(A, \rightarrow_2)$ に対して，$\rightarrow_{1\cup2}$ を $\rightarrow_1 \cup \rightarrow_2$ と，$\leftrightarrow_{1\cup2}$ を $\leftrightarrow_1 \cup \leftrightarrow_2$ と定義する．また，$\stackrel{*}{\rightarrow}_{1\cup2}$ と $\stackrel{*}{\leftrightarrow}_{1\cup2}$ をそれぞれ $\rightarrow_{1\cup2}$ と $\leftrightarrow_{1\cup2}$ の反射推移閉包とする．

関数記号の集合 $\mathcal{F}$，**変数**の可算無限集合 $\mathcal{V}$ から生成されるすべての**項**の集合を $T(\mathcal{F}, \mathcal{V})$ とする．また，変数を含まない項を**基底項**と呼び，基底項の集合を $T(\mathcal{F})$ とする．項 t に現れるすべての変数の集合を $\mathcal{V}ar(t)$ で表す．項 s と t が同一であるときは $s \equiv t$ と記述する．項 s の位置 p にある項を t に置き換えて得られる項を $s[t]_p$ と書く．**ホール** $\Box \notin \mathcal{F}$ を特別な定数記号とする．**文脈**とは，$\Box$ を 1 つだけ含む項である．ホール自身も文脈であり，このような文脈を空の文脈という．文脈 $C[\,]$ において位置 p に出現するホール $\Box$ を項 t で置き換えることによって得られる項を $C[t]_p$ と記す．なお，p を省略してもよい．$\mathcal{F}$，$\mathcal{V}$ 上のすべての文脈の集合を $T_\Box(\mathcal{F}, \mathcal{V})$ とする．項 t，u に対して $t \equiv C[u]_p$ となるような文脈 $C[\,]$ が存在するとき，u を t の**部分項**と呼ぶ．また，p における部分項 u を $t|_p$ と記す．

代入 σ の定義域と値域をそれぞれ $\mathcal{D}om(\sigma)$（$= \{x \mid x \neq \sigma(x)\}$）と $\mathcal{R}an(\sigma)$（$= \{\sigma(x) \mid x \in \mathcal{D}om(\sigma)\}$）で表す．$\mathcal{D}om(\sigma) = \{x_1, \ldots, x_n\}$ であり，かつ $\sigma(x_i) \equiv t_i$ のとき，σ を $\{x_1 \mapsto t_1, \cdots, x_n \mapsto t_n\}$ と記す．項 t に対して，$\sigma(t)$ を t の**インスタンス**と呼び，$t\sigma$ と略記する．代入 σ，σ' について，$\mathcal{D}om(\sigma) = \mathcal{D}om(\sigma')$ かつすべての $x \in \mathcal{D}om(\sigma)$ において $\sigma(x) \equiv \sigma'(x)$ のとき，$\sigma = \sigma'$ と記述する．σ と σ' の合成を $\sigma\sigma'$ と記述し，$x(\sigma\sigma') \equiv \sigma'(\sigma(x))$ で定義する．σ の定義域を $X \subseteq \mathcal{V}$ に制限した代入 $\sigma|_X$ を $\{x \mapsto x\sigma \mid x \in \mathcal{D}om(\sigma) \cap X\}$ と定義する．代入 σ，θ に対して $\sigma\delta = \theta$ となる代入 δ が存在するとき，$\sigma \lesssim \theta$ と記す．項 t に対して，$t\sigma_g$ が基底項となるような代入 σ_g を t に対する**基底代入**という．単純に基底代入と呼ぶときには，それ以降に現れる項にその代入を行うと基底項になる代入を指す．抽象書換え系 S を $(T(\mathcal{F}, \mathcal{V}), \rightarrow)$ としたとき，$\mathcal{R}an(\sigma) \subseteq NF_S$ となるような基底代入を**基底正規形代入**という．

項 s と t が**単一化可能**とは，ある代入 σ が存在して $s\sigma \equiv t\sigma$ となることである．このと

き，σ を s と t の**単一化子**という．s と t の単一化子 σ が，s，t の任意の単一化子 θ について $\sigma \lesssim \theta$ を満たすとき，σ は**最汎**であるという．s と t の最汎単一化子を $mgu(s,t)$ で表す．

項上の半順序 $\succ$ が整礎であり，文脈と代入に閉じているとき，$\succ$ を**簡約化順序**と呼ぶ．

$\mathcal{G}$ を関数記号の集合，$\mathcal{P}$ を述語記号の集合とする．$\mathcal{G}$ と $\mathcal{P}$ で定義される論理式を BNF 記法を用いて以下のように定める．

$$\phi := P(t_1, \cdots, t_n) \mid \neg\phi \mid \phi \wedge \phi \mid \phi \vee \phi \mid \top \mid \bot$$

ただし，$P \in \mathcal{P}$，$t_1, \cdots, t_n \in T(\mathcal{G}, \mathcal{V})$ である．$\top$ と $\bot$ はそれぞれ真と偽に相当する．なお，本論文では限量子は用いない．また，変数を含まない論理式を**閉じた**論理式と呼ぶ．

$\mathcal{G}$ と $\mathcal{P}$ の解釈である**モデル** $\mathcal{M}$ は，**領域**と呼ばれる空でない集合 A，$\mathcal{G}$ と $\mathcal{P}$ の解釈から成り立つ．任意の n 引数関数記号 $g \in \mathcal{G}$ は，$A^n \to A$ の関数によって解釈され，その関数を $g^{\mathcal{M}}$ と書く．任意の n 引数述語記号 $P \in \mathcal{P}$ は，$A^n \to \{\top, \bot\}$ の関数によって解釈され，その関数を $P^{\mathcal{M}}$ と書く．また，A 上の等価関係を表す 2 引数の述語記号 EQ は $\mathcal{P}$ に必ず含まれているとする．EQ の解釈は，引数で与えられた 2 つの項の解釈が等価ならば $\top$ を，そうでないならば $\bot$ を返す関数 $EQ^{\mathcal{M}}$ とする．

モデル $\mathcal{M}$ が与えられているとき，$\mathcal{G}$，$\mathcal{P}$ から成る論理式を $\mathcal{M}$ 上の**制約**と呼ぶ．

基底項 $f(t_1, \cdots, t_n)$ の解釈は $(f(t_1, \cdots, t_n))^{\mathcal{M}} = f^{\mathcal{M}}((t_1)^{\mathcal{M}}, \cdots, (t_n)^{\mathcal{M}})$ とし，閉じた原始論理式 $P(t_1, \cdots, t_n)$ の解釈は $(P(t_1, \cdots, t_n))^{\mathcal{M}} = P^{\mathcal{M}}((t_1)^{\mathcal{M}}, \cdots, (t_n)^{\mathcal{M}})$ とする．また，$\neg$，$\wedge$，$\vee$，$\top$，$\bot$ の解釈については通常どおりである．閉じた制約 c に対して $(c)^{\mathcal{M}} = \top$ ならば c **は真である**とし，$(c)^{\mathcal{M}} = \bot$ ならば c **は偽である**という．制約は限量子を含んでいないため，閉じた制約の真偽値判定は決定可能である．

制約 c に含まれる自由変数の集合を $fv(c)$ と書く[⋆1]．制約 c への代入 σ の適用 $\sigma(c)$ は，c に含まれる各自由変数 x を $\sigma(x)$ で置き換えることであり，σ は $\mathcal{R}an(\sigma|_{fv(c)}) \subseteq T(\mathcal{G}, \mathcal{V})$ を満たすとする．

制約 c が $\mathcal{M}$ **に関して恒真**であるとは，$fv(c) \subseteq \mathcal{D}om(\sigma_g)$ を満たす c への任意の基底代入 σ_g に対して $c\sigma_g$ が真であることである．また，制約 c **が** $\mathcal{M}$ **に関して充足可能**であるとは，$fv(c) \subseteq \mathcal{D}om(\sigma_g)$ を満たす c へのある基底代入 σ_g が存在し $c\sigma_g$ が真であることである．さらに，c が充足可能でないとき，c **は** $\mathcal{M}$ **に関して充足不能**であるという．

例 2.1　$\mathcal{G}_{PA} = \{0, s, p, +\}$，$\mathcal{P}_{PA} = \{=, \neq, <, \leq, >, \geq\}$，$\mathcal{M}_{PA}$ の領域を整数とし，$0^{\mathcal{M}_{PA}}$ は整数の 0，$s^{\mathcal{M}_{PA}}(x) = x + 1$，$p^{\mathcal{M}_{PA}}(x) = x - 1$，$+$ と $\mathcal{P}_{PA}$ の述語記号の解釈は整数論上の意味と同じとする．ここで，$\mathcal{P}_{PA}$ は EQ を含まないが，$=$ は EQ と同じ解釈を持つため $=$ を EQ と見なす．このとき，$\mathcal{G}_{PA}$ と $\mathcal{P}_{PA}$ 上の制約は**プレスブルガー算術**と呼ばれる加減算を持つ整数の理論（整数，整数上の変数，整数の加減演算 $+$，$-$，整数の比較演算 $=$，$\neq$，$<$，$\leq$，$>$，$\geq$，論理演算 $\wedge$，$\vee$，$\neg$，限量子 $\forall$，$\exists$ からなる理論）に含まれる．自由変数が存在しないプレスブルガー算術の論理式を**プレスブルガー文**と呼ぶ．プレスブルガー文は真偽値判定が決定可能であることが知られている[18),21),22),⋆2]．このため，$\mathcal{G}_{PA}$ と $\mathcal{P}_{PA}$ 上の任意の制約 c について，$\mathcal{M}_{PA}$ に関しての恒真性，充足可能性，充足不能性は決定可能である．

3. 制約付き項書換え系とその性質

本章では，文献 24) で扱われる制約付き項書換え系をモデルを明示した形式で定義し，制約に対して満たすべき性質を明らかにする．

$\mathcal{F}$，$\mathcal{G}$ を $\mathcal{F} \cap \mathcal{G} = \emptyset$ となる関数記号の集合，$\mathcal{P}$ を述語記号の集合，$\mathcal{M}$ を $\mathcal{G}$ と $\mathcal{P}$ のモデルとする．このとき，$(\mathcal{F}, \mathcal{G}, \mathcal{P}, \mathcal{M})$ **上の制約付き書換え規則** (l, r, c) は，$l \notin \mathcal{V}$，l，$r \in T(\mathcal{F} \cup \mathcal{G}, \mathcal{V})$，$\mathcal{V}ar(l) \supseteq \mathcal{V}ar(r)$ を満たす左辺項 l，右辺項 r と，制約部と呼ばれる $\mathcal{V}ar(l) \supseteq fv(c)$ を満たす $\mathcal{G}$ と $\mathcal{P}$ 上の制約 c の 3 つ組であり，$l \to r \Leftarrow c$ と記す．c が $\top$ のときは制約を省略して $l \to r$ と書くこともある．

R を $(\mathcal{F}, \mathcal{G}, \mathcal{P}, \mathcal{M})$ 上の制約付き書換え規則の有限集合とする．R で定められる**書換え関係** $\to_R$ を $\to_R = \{(C[l\sigma], C[r\sigma]) \mid l \to r \Leftarrow c \in R, C[\,] \in T_{\Box}(\mathcal{F} \cup \mathcal{G}, \mathcal{V}), fv(c) \subseteq \mathcal{D}om(\sigma), \mathcal{R}an(\sigma|_{fv(c)}) \subseteq T(\mathcal{G}), c\sigma$ は真 $\}$ と定義する．$(\mathcal{F}, \mathcal{G}, \mathcal{P}, \mathcal{M})$ **上の制約付き項書換え系**は項の集合 $T(\mathcal{F} \cup \mathcal{G}, \mathcal{V})$ と書換え関係 $\to_R$ で定められる抽象書換え系 $(T(\mathcal{F} \cup \mathcal{G}, \mathcal{V}), \to_R)$ であり，単に書換え規則の集合 R のみで表す．

$(\mathcal{F}, \mathcal{G}, \mathcal{P}, \mathcal{M})$ **上の制約付き等式** (s, t, c) は，s，$t \in T(\mathcal{F} \cup \mathcal{G}, \mathcal{V})$ を満たす項 s，t と，制約部と呼ばれる $\mathcal{G}$ と $\mathcal{P}$ 上の制約 c の 3 つ組であり，$s \approx t \Leftarrow c$ と記す．c が $\top$ のときは制約部を省略して $s \approx t$ と書くこともある．また，$s \simeq t \Leftarrow c$ は $s \approx t \Leftarrow c$ または $t \approx s \Leftarrow c$ のどちらかを表す．

⋆1 限量子を含まないので，変数はすべて自由変数である．

⋆2 本論文では，閉じた制約が決定可能であることを仮定するため，限量子を扱わないこととした．しかし，プレスブルガー文は限量子を含んでいても決定可能である．このため，制約がプレスブルガー算術に含まれる場合は，限量子を用いてもこれ以降の議論に影響を与えない．

E を $(\mathcal{F},\mathcal{G},\mathcal{P},\mathcal{M})$ 上の制約付き等式の有限集合とする．E で定められる 2 項関係 $\leftrightarrow_E$ を $\leftrightarrow_E = \{(C[s\sigma], C[t\sigma]) \mid s \simeq t \Leftarrow c \in E, C[\ ] \in T_\Box(\mathcal{F},\mathcal{V}), fv(c) \subseteq \mathcal{D}om(\sigma), \mathcal{R}an(\sigma|_{fv(c)}) \subseteq T(\mathcal{G}), c\sigma$ は真 $\}$ と定義する．

等式 $s \approx t \Leftarrow c$ が R **の帰納的定理**であるとは，$\mathcal{V}ar(s,t) \cup fv(c) \subseteq \mathcal{D}om(\sigma_g)$ を満たす任意の基底代入 σ_g に対して，$c\sigma_g$ が真ならば $s\sigma_g \overset{*}{\leftrightarrow}_R t\sigma_g$ を満たすことである．位置 p が制約 c の下での項 t の R **完全な出現**であるとは，$c\sigma_{NF}$ が真となるような任意の基底正規形代入 σ_{NF} に対して，$t\sigma_{NF}$ が位置 p で書換え可能である，すなわち，$t|_p\sigma_{NF} \equiv l\theta$ かつ $d\theta$ が真である書換え規則 $l \to r \Leftarrow c$ が存在することである．

次に，本論文で提案する書換え帰納法の正しさに必要となる性質について考える

定義 3.1（健全性と完全性） R を $(\mathcal{F},\mathcal{G},\mathcal{P},\mathcal{M})$ 上の制約付き項書換え系とする．このとき，R が $\mathcal{M}$ **に対して健全**であるとは，任意の基底項 s_g，$t_g \in T(\mathcal{G})$ に対して，$s_g \overset{*}{\leftrightarrow}_R t_g$ ならば $EQ(s_g,t_g)$ が真となることである．一方，R が $\mathcal{M}$ **に対して完全**であるとは，任意の基底項 s_g，$t_g \in T(\mathcal{G})$ に対して，$EQ(s_g,t_g)$ が真ならば $s_g \overset{*}{\leftrightarrow}_R t_g$ となることである．

定義 3.2（局所健全性） R を $(\mathcal{F},\mathcal{G},\mathcal{P},\mathcal{M})$ 上の制約付き項書換え系とする．このとき，R が $\mathcal{M}$ **に対して局所健全**であるとは，任意の基底項 $s_g \in T(\mathcal{G})$ に対して，$s_g \to_R t_g$ ならば $t_g \in T(\mathcal{G})$ かつ $EQ(s_g,t_g)$ が真となることである．

健全性は，2 つの項が書換え関係上で等価ならば意味論上でも等価であることを表す．完全性は，2 つの項が意味論上で等価ならば書換え関係上でも等価であることを表す．局所健全性は，意味を持つ項を書き換えて得られる項は等価の意味を持つことを表し，文献 24) で提案された制約部安定性と等価な概念である．

以降では，健全性，完全性を満たすための十分条件，および，局所健全性を満たすための必要十分条件を示す．

まずは，健全性の十分条件を示す．

定理 3.3（健全性の十分条件） R を $(\mathcal{F},\mathcal{G},\mathcal{P},\mathcal{M})$ 上の制約付き項書換え系とする．R が以下のすべての性質を満たすとき，R は $\mathcal{M}$ に対して健全である．

- 局所健全性
- CR 性

［証明］　s_g，$t_g \in T(\mathcal{G})$ かつ $s_g \overset{*}{\leftrightarrow}_R t_g$ とする．このとき，CR 性からある u_g が存在して $s_g \overset{*}{\to}_R u_g \overset{*}{\leftarrow}_R t_g$ である．R の局所健全性から，$u_g \in T(\mathcal{G})$ かつ $EQ(s_g,u_g)$ が真かつ $EQ(u_g,t_g)$ が真である．よって，$(s_g)^{\mathcal{M}} = (u_g)^{\mathcal{M}} = (t_g)^{\mathcal{M}}$ であるので，$EQ(s_g,t_g)$ が真である．ゆえに，R は健全性を持つ．　□

次に，完全性の十分条件を与える．

定理 3.4（完全性の十分条件） R を $(\mathcal{F},\mathcal{G},\mathcal{P},\mathcal{M})$ 上の制約付き項書換え系とする．R が以下のすべての性質を満たすとき，R は $\mathcal{M}$ に対して完全である．

(1)　局所健全性
(2)　停止性
(3)　任意の s_g，$t_g \in T(\mathcal{G})$ に対して，s_g，$t_g \in NF_R$ かつ $EQ(s_g,t_g)$ が真ならば，$s_g \equiv t_g$

［証明］　s_g，$t_g \in T(\mathcal{G})$ かつ $EQ(s_g,t_g)$ が真とする．このとき，局所健全性と停止性より，正規形 s'_g と t'_g が存在し以下のすべてを満たす．

- $s_g \overset{*}{\to}_R s'_g$ かつ $t_g \overset{*}{\to}_R t'_g$
- s'_g，$t'_g \in T(\mathcal{G})$
- $EQ(s_g,s'_g)$ が真かつ $EQ(t_g,t'_g)$ が真，すなわち $EQ(s'_g,t'_g)$ が真

よって，仮定 (3) から $s'_g \equiv t'_g$ が成り立つ．ゆえに，$s_g \overset{*}{\to}_R s'_g \equiv t'_g \overset{*}{\leftarrow}_R t_g$ である．したがって，$s_g \overset{*}{\leftrightarrow}_R t_g$．　□

次に，局所健全性の必要十分条件を与える．

補題 3.5 R が $(\mathcal{F},\mathcal{G},\mathcal{P},\mathcal{M})$ 上の制約付き項書換え系とする．以下が成り立つとき，任意の項 s_g，$t_g \in T(\mathcal{G})$ に対して $s_g \to_R t_g$ ならば $EQ(s_g,t_g)$ は真である．

- R の任意の規則 $l \to r \Leftarrow c$ について，$l \in T(\mathcal{G},\mathcal{V})$ かつ $r \in T(\mathcal{G},\mathcal{V})$ ならば $\neg c \vee EQ(l,r)$ は $\mathcal{M}$ に関して恒真である．

［証明］　s_g，$t_g \in T(\mathcal{G})$ かつ $s_g \to_R t_g$ とする．$\to_R$ の定義より，$l \to r \Leftarrow c \in R$ と文脈 $C[\ ]$ と基底代入 σ_g が存在し，$s_g \equiv C[l\sigma_g]$ かつ $t_g \equiv C[r\sigma_g]$ かつ $c\sigma_g$ は真である．s_g，$t_g \in T(\mathcal{G})$ より，$l \in T(\mathcal{G},\mathcal{V})$，$l\sigma_g \in T(\mathcal{G})$，$r \in T(\mathcal{G},\mathcal{V})$，$r\sigma_g \in T(\mathcal{G})$，$C[\ ] \in T_\Box(\mathcal{G})$ である．$l \in T(\mathcal{G},\mathcal{V})$ かつ $r \in T(\mathcal{G},\mathcal{V})$ が成り立つため，仮定より $\neg c \vee EQ(l,r)$ は $\mathcal{M}$ に関し

て恒真である．よって，$\neg c\sigma_g \vee EQ(l\sigma_g, r\sigma_g)$ は真である．$c\sigma_g$ は真なので，$\neg c\sigma_g$ は偽であり，$EQ(l\sigma_g, r\sigma_g)$ は真である．ゆえに，$C[\,] \in T_\Box(\mathcal{G})$ より $EQ(C[l\sigma_g], C[r\sigma_g])$ は真である．よって，$EQ(s_g, t_g)$ は真である．　□

補題 3.6　R を $(\mathcal{F}, \mathcal{G}, \mathcal{P}, \mathcal{M})$ 上の制約付き項書換え系とする．以下が成り立つとき，任意の基底項 $s_g \in T(\mathcal{G})$ に対して，$s_g \to_R t_g$ ならば $t_g \in T(\mathcal{G})$ である．

- 任意の書換え規則 $l \to r \Leftarrow c \in R$ について，$l \in T(\mathcal{G}, \mathcal{V})$ ならば $r \in T(\mathcal{G}, \mathcal{V})$

［証明］　$s_g \in T(\mathcal{G})$ かつ $s_g \to_R t_g$ とする．このとき，$l \to r \Leftarrow c \in R$ と文脈 $C[\,]$ と基底代入 σ_g が存在し，$s_g \equiv C[l\sigma_g]$ かつ $t_g \equiv C[r\sigma_g]$ かつ $c\sigma_g$ が真となる．$s_g \in T(\mathcal{G})$ より $l \in T(\mathcal{G}, \mathcal{V})$，$\mathcal{R}an(\sigma_g|_{\mathcal{V}ar(l)}) \subseteq T(\mathcal{G})$，$C[\,] \in T_\Box(\mathcal{G})$ である．$\mathcal{V}ar(l) \supseteq \mathcal{V}ar(r)$，$\mathcal{R}an(\sigma_g|_{\mathcal{V}ar(l)}) \subseteq T(\mathcal{G})$，$C[\,] \in T_\Box(\mathcal{G})$ より $C[r\sigma_g] \in T(\mathcal{G})$ である．よって，$t_g \in T(\mathcal{G})$ である．　□

定理 3.7（局所健全性の必要十分条件）　R を $(\mathcal{F}, \mathcal{G}, \mathcal{P}, \mathcal{M})$ 上の制約付き項書換え系とする．このとき，以下の 2 つは等価である．

(1)　R は $\mathcal{M}$ に対して局所健全である．

(2)　任意の書換え規則 $l \to r \Leftarrow c \in R$ について，$l \in T(\mathcal{G}, \mathcal{V})$ かつ c が $\mathcal{M}$ に関して充足可能ならば，$r \in T(\mathcal{G}, \mathcal{V})$ かつ $\neg c \vee EQ(l, r)$ が $\mathcal{M}$ に関して恒真である．

［証明］　補題 3.5，3.6 より，(2) ならば (1) は成り立つ．よって，(1) ならば (2) を背理法で示す．

(2) でないと仮定する．このとき，$l \to r \Leftarrow c$ が存在して，$l \in T(\mathcal{G}, \mathcal{V})$ かつ c が充足可能かつ以下のどちらかが成り立つ．

- $r \notin T(\mathcal{G}, \mathcal{V})$
- $r \in T(\mathcal{G}, \mathcal{V})$ かつ $(\neg c \vee EQ(l, r))\sigma_g$ が偽となる基底代入 σ_g が存在

$r \notin T(\mathcal{G}, \mathcal{V})$ が成り立つ場合，c が充足可能なので $\mathcal{R}an(\theta_g|_{\mathcal{V}ar(l)}) \subseteq T(\mathcal{G})$ かつ $c\theta_g$ が真となる基底代入 θ_g が存在する．$l \in T(\mathcal{G}, \mathcal{V})$ かつ $\mathcal{R}an(\theta_g|_{\mathcal{V}ar(l)}) \subseteq T(\mathcal{G})$ かつ $c\theta_g$ が真から $l\theta_g \in T(\mathcal{G})$ かつ $l\theta_g \to_R r\theta_g$ が成り立つので，局所健全性より $r\sigma_g \in T(\mathcal{G})$ となる．これは $r \notin T(\mathcal{G}, \mathcal{V})$ に矛盾する．

$r \in T(\mathcal{G}, \mathcal{V})$ の場合，$(\neg c \vee EQ(l, r))\sigma_g$ が偽となる基底代入 σ_g が存在する．すなわち，$c\sigma_g$ は真かつ $EQ(l\sigma_g, r\sigma_g)$ は偽である．$l \in T(\mathcal{G}, \mathcal{V})$ かつ $\mathcal{R}an(\sigma_g|_{\mathcal{V}ar(l)}) \subseteq T(\mathcal{G})$ から $l\sigma_g \in T(\mathcal{G})$ が成り立ち，$c\sigma_g$ が真であることから $l\sigma_g \to_R r\sigma_g$ が成り立つので，局所健全性より $EQ(l\sigma_g, r\sigma_g)$ は真となり矛盾する．　□

例 3.8　例 2.1 の $\mathcal{G}_{PA}$，$\mathcal{P}_{PA}$，$\mathcal{M}_{PA}$ で表現されるプレスブルガー算術を制約に持つ以下の $(\mathcal{F}, \mathcal{G}_{PA}, \mathcal{P}_{PA}, \mathcal{M}_{PA})$ 上の制約付き項書換え系を考える．

$$R_{add} = \left\{ \begin{array}{c} 0 + y \to y \\ s(x) + y \to s(x + y) \\ p(x) + y \to p(x + y) \end{array} \right.$$

このとき，任意の規則の左辺項と右辺項は $T(\mathcal{G}_{PA}, \mathcal{V})$ に含まれ，$0 + y = y$，$s(x) + y = s(x + y)$，$p(x) + y = p(x + y)$ はいずれも $\mathcal{M}_{PA}$ に関して恒真であるため R_{add} は $\mathcal{M}_{PA}$ に対して局所健全である．また，R_{add} は CR 性を持つため，$\mathcal{M}_{PA}$ に対して健全である．しかし，0 と $s(p(0))$ を考えると，$0 = s(p(0))$ は真であるが $0 \overset{*}{\leftrightarrow}_{R_{add}} s(p(0))$ を満たさない．このため，R_{add} は $\mathcal{M}_{PA}$ に対して完全ではない．

次に，以下の $(\mathcal{F}, \mathcal{G}_{PA}, \mathcal{P}_{PA}, \mathcal{M}_{PA})$ 上の制約付き項書換え系を考える．

$$R_{PA} = R_{add} \cup \left\{ \begin{array}{l} s(p(x)) \to x \\ p(s(x)) \to x \end{array} \right.$$

R_{PA} は停止性と $\mathcal{M}_{PA}$ に対しての局所健全性を持ち，任意の s_g，$t_g \in T(\mathcal{G})$ に対して s_g，$t_g \in NF_R$ かつ $s_g = t_g$ が真ならば $s_g \equiv t_g$ がいえる．このため，R_{PA} は $\mathcal{M}_{PA}$ に対して完全である．

4. 制約付き項書換え系における書換え帰納法

本章では，制約付き項書換え系における帰納的定理を書換え帰納法を用いて検証する方法を提案する．また，書換え帰納法による帰納的定理の検証例を示す．

4.1 書換え帰納法による検証法

制約付き項書換え系における書換え帰納法の推論規則を**図 1** に記す．$Expd$ は $Expd(s, t, c, p) = \{(C[r]_p)\sigma \approx t\sigma \Leftarrow c\sigma \wedge d\sigma \mid s \equiv C[u]_p, l \to r \Leftarrow d \in R, \sigma = mgu(u, l)\}$ と定義する．また，(E, H) に図 1 の推論規則を 1 回適用させて (E', H') になるとき，

Simplification

$$\frac{(E \uplus \{C[l\sigma] \simeq t \Leftarrow c\}, H)}{(E \cup \{C[r\sigma] \approx t \Leftarrow c\}, H)}$$

ただし，$l \to r \Leftarrow d \in R \cup H$ かつ c は $\mathcal{M}$ に関して充足可能かつ
$fv(d\sigma) \subseteq fv(c)$ かつ $\neg c \vee d\sigma$ は $\mathcal{M}$ に関して恒真

Deletion

$$\frac{(E \uplus \{s \simeq t \Leftarrow c\}, H)}{(E, H)}$$

ただし，$s \equiv t$ または c は $\mathcal{M}$ に関して充足不能

Expansion

$$\frac{(E \uplus \{s \simeq t \Leftarrow c\}, H)}{(E \cup Expd(s,t,c,p), H \cup \{s \to t \Leftarrow c\})}$$

ただし，$s \succ t$ かつ $s \notin \mathcal{V}$ かつ $\mathcal{V}ar(s) \supseteq \mathcal{V}ar(t)$ かつ
$fv(c) \subseteq \mathcal{V}ar(s)$ かつ位置 p は c の下での s の R 完全な出現

EQ-Deletion

$$\frac{(E \uplus \{C[s_1, \cdots, s_n] \simeq C[t_1, \cdots, t_n] \Leftarrow c\}, H)}{(E \cup \{C[s_1, \cdots, s_n] \approx C[t_1, \cdots, t_n] \Leftarrow c \wedge \neg(\bigwedge_{i=1}^{n} EQ(s_i, t_i))\}, H)}$$

ただし，任意の i について $s_i, t_i \in T(\mathcal{G}, \mathcal{V})$ かつ $\mathcal{V}ar(s_i, t_i) \subseteq fv(c)$

図 1　制約付き項書換え系における書換え帰納法のための推論規則
Fig. 1　Inference rules of rewriting induction for constrained term rewriting systems.

$(E, H) \vdash_{RI} (E', H')$ と書き，$\vdash_{RI}$ の反射推移閉包を $\vdash^*_{RI}$ と書く．さらに，Simplification，Deletion，Expansion，EQ-Deletion を 1 回適用させたときは，特に $\vdash^s_{RI}$，$\vdash^d_{RI}$，$\vdash^e_{RI}$，$\vdash^{eq}_{RI}$ と書く．

Simplification，Deletion，Expansion は項書換え系における書換え帰納法の推論規則[20),23)]を制約付き項書換え系に対応するように拡張を行った推論規則であり，Simplification，Deletion は文献 24) の推論規則と同様である．EQ-Deletion は文献 24) で提案されたプレスブルガー文付き項書換え系における潜在帰納法のための推論規則 MGU-Deletion を一般化かつ強力にした推論規則である．

これらの推論規則に対して，以下の定理が成り立つ．

定理 4.1　R を $(\mathcal{F}, \mathcal{G}, \mathcal{P}, \mathcal{M})$ 上の制約付き項書換え系とする．また，E を $(\mathcal{F}, \mathcal{G}, \mathcal{P}, \mathcal{M})$ 上の制約付き等式の有限集合，$\succ$ を $\to_R \subseteq \succ$ を満たす簡約化順序とする．さらに，R は $\mathcal{M}$ に対しての完全性と局所健全性を持つとする．このとき，$(E, \emptyset) \vdash^*_{RI} (\emptyset, H)$ ならば，E に含まれるすべての等式は R の帰納的定理である．

［証明］　付録 A.1 を参照．　□

R を $(\mathcal{F}, \mathcal{G}, \mathcal{P}, \mathcal{M})$ 上の制約付き項書換え系とする．また，E を $(\mathcal{F}, \mathcal{G}, \mathcal{P}, \mathcal{M})$ 上の制約付き等式の有限集合，$\succ$ を $\to_R \subseteq \succ$ を満たす簡約化順序とする．さらに，R は $\mathcal{M}$ に対しての完全性と局所健全性を持つとする．このとき，図 1 の書換え帰納法のための推論規則を用いた**帰納的定理の検証手続き**を**図 2** に提案する．この検証手続きにより $(E, \emptyset)$ が $(\emptyset, H)$ となれば E に含まれるすべての等式は R の帰納的定理であると判定する．定理 4.1 から図 1 の推論規則をどのような戦略で適用させたとしても帰納的定理の検証として正しいため，図 2 の手続きは正しいことは明らかである．

$(E, \emptyset)$ に推論規則を以下の順に適用させる．
(1)　Simplification を可能な限り適用．
(2)　EQ-Deletion を適用可能なすべての等式に 1 回ずつ適用．
(3)　Deletion を可能な限り適用し，$E = \emptyset$ ならば終了．
(4)　Expansion を 1 回だけ適用し (1) へ．

図 2　書換え帰納法に基づいた検証手続き
Fig. 2　Procedure of verification based on rewriting induction.

4.2　書換え帰納法による検証例

本節では，文献 24) で提案された潜在帰納法により検証に成功した例について，本論文で提案した書換え帰納法では自然数だけではなく整数を扱えるように拡張しても検証が成功することを示す．

文献 24) の手法を用いて整数論上の帰納的定理を検証しようとすると，暴走してしまうことが多い．このため，文献 24) では自然数上に限定して検証を行っていた．しかし，本論文で提案する手法では，整数上の検証であっても暴走せずに手続きが成功する例が存在する．

例 4.2　R を $(\{sum, sum1, u\}, \mathcal{G}_{PA}, \mathcal{P}_{PA}, \mathcal{M}_{PA})$ 上の制約付き項書換え系とし，書換え規則は以下のとおりとする．

$$R = R_{PA} \cup \left\{ \begin{array}{r} sum(x) \to 0 \Leftarrow x \leq 0 \\ sum(s(x)) \to sum(x) + s(x) \ \Leftarrow \ x \geq 0 \\ sum1(n) \to u(n, s(0), 0) \\ u(n, i, z) \to u(n, s(i), z + i) \ \Leftarrow \ i \leq n \\ u(n, i, z) \to z \ \Leftarrow \ i > n \end{array} \right.$$

このとき，以下の等式を検証した様子を**図 3** に示す．

$$E = \left\{ \begin{array}{r} u(s(n), i, z) \approx u(n, i, z) + s(n) \ \Leftarrow \ i \leq s(n) \\ sum(n) \approx sum1(n) \end{array} \right.$$

上記の R は停止性，$\mathcal{M}_{PA}$ に関する完全性と局所健全性を満たしている．よって，$sum(n) \approx sum1(n)$ は R の帰納的定理である．さらに，R は CR 性を持つ[24] ので，任意の項 $t \in T(\{sum, sum1, u\} \cup \mathcal{G}_{PA})$ に対して $sum(t) \downarrow_R sum1(t)$ である．ゆえに，関数 sum と関数 $sum1$ は入力が等しいときには出力も等しいことがいえる．　□

5. R 完全な出現の判定法

項書換え系において，位置 p が項 s の R 完全な出現であるかの判定は決定可能である[13]．しかし，制約付き項書換え系における R 完全な出現の判定方法は分かっていない．そこで，制約付き項書換え系における R 完全な出現の判定のための十分条件を与える．

定理 5.1　R を $(\mathcal{F}, \mathcal{G}, \mathcal{P}, \mathcal{M})$ 上の制約付き項書換え系とし，$NF_{(T(\mathcal{F}\cup\mathcal{G}),\ \to_R)} \subseteq T(\mathcal{G})$，$s \equiv C[f(s_1, \cdots, s_n)]_p$，$s_1, \cdots, s_n \in T(\mathcal{G}, \mathcal{V})$ とする．このとき，$\bigvee_{f(x_1,\cdots,x_n)\to r \Leftarrow d \in R} d$ が $\mathcal{M}$ に関して恒真であるならば，s の位置 p は任意の制約 c の下で R 完全な出現である．ただし，$x_1, \cdots, x_n$ は相異なる変数とする．

［証明］　$\bigvee_{f(x_1,\cdots,x_n)\to r \Leftarrow d \in R} d$ が $\mathcal{M}$ に関して恒真とする．このとき，任意の基底正規形代入 σ_{NF} に対して，$\mathcal{R}an(\sigma_{NF}) \subseteq T(\mathcal{G})$ となるため $s_1\sigma_{NF}, \cdots, s_n\sigma_{NF} \in T(\mathcal{G})$ である．ここで，$x_i\sigma_g \equiv s_i\sigma_{NF}$ となる代入 σ_g について考える．$\mathcal{R}an(\sigma_g|_{\{x_1,\cdots,x_n\}}) \subseteq T(\mathcal{G})$，$\bigvee_{f(x_1,\cdots,x_n)\to r \Leftarrow d \in R} d$ が $\mathcal{M}$ に関して恒真より，$(\bigvee_{f(x_1,\cdots,x_n)\to r \Leftarrow d \in R} d)\sigma_g$ は真である．

$$\begin{array}{l} (E, \emptyset) \\ \vdash^s_{RI} \vdash^s_{RI} \\ \left(\left\{ \begin{array}{ll} (1) & u(s(n), s(i), z + i) \approx u(n, i, z) + s(n) \ \Leftarrow \ i \leq s(n) \\ (2) & sum(n) \approx u(n, s(0), 0) \end{array} \right\}, \emptyset \right) \\ \vdash^e_{RI} \\ \left(\left\{ \begin{array}{c} (2) \\ z + i \ \approx \ u(n, i, z) + s(n) \ \Leftarrow \ i \leq s(n) \wedge s(i) > s(n) \\ u(s(n), s(s(i)), (z + i) + s(i)) \ \approx \ u(n, i, z) + s(n) \ \Leftarrow \ i \leq s(n) \wedge s(i) \leq s(n) \end{array} \right\}, \right. \\ \qquad \left. \left\{ \ (3) \quad u(s(n), s(i), z + i) \to u(n, i, z) + s(n) \ \Leftarrow \ i \leq s(n) \ \right\} \right) \\ \vdash^s_{RI} \vdash^s_{RI} \vdash^s_{RI} \\ \left(\left\{ \begin{array}{c} (2) \\ z + i \approx z + s(n) \ \Leftarrow \ i \leq s(n) \wedge s(i) > s(n) \\ (4) \ u(n, s(i), z + i) + s(n) \\ \approx u(n, s(i), z + i) + s(n) \ \Leftarrow \ i \leq s(n) \wedge s(i) \leq s(n) \end{array} \right\}, \{ \ (3) \ \} \right) \\ \vdash^{eq}_{RI} \\ \left(\left\{ \begin{array}{c} (2) \\ z + i \approx z + s(n) \ \Leftarrow \ i \leq s(n) \wedge s(i) > s(n) \wedge \neg(i = s(n)) \\ (4) \end{array} \right\}, \{ \ (3) \ \} \right) \\ \vdash^d_{RI} \vdash^d_{RI} \\ \left(\ \{ \ (2) \ \}, \{ \ (3) \ \} \ \right) \\ \vdash^e_{RI} \\ \left(\left\{ \begin{array}{c} 0 \approx u(n, s(0), 0) \ \Leftarrow \ n \leq 0 \\ sum(n) + s(n) \approx u(s(n), s(0), 0) \ \Leftarrow \ n \geq 0 \end{array} \right\}, \left\{ \begin{array}{c} (3) \\ (5) \ sum(n) \ \to \ u(n, s(0), 0) \end{array} \right\} \right) \\ \vdash^s_{RI} \vdash^s_{RI} \vdash^s_{RI} \vdash^s_{RI} \\ \left(\left\{ \begin{array}{c} 0 \approx 0 \ \Leftarrow \ n \leq 0 \\ u(n, s(0), 0) + s(n) \approx u(n, s(0), 0) + s(n) \ \Leftarrow \ n \geq 0 \end{array} \right\}, \left\{ \begin{array}{c} (3) \\ (5) \end{array} \right\} \right) \\ \vdash^d_{RI} \vdash^d_{RI} \\ \left(\ \emptyset, \ \{ \ (3), (5) \ \} \ \right) \end{array}$$

図 3　書換え帰納法による帰納的定理の証明例
Fig. 3　Example of proving inductive theorems for rewriting induction.

よって，ある $f(x_1, \cdots, x_n) \ \to \ r \ \Leftarrow \ d \ \in \ R$ が存在して，$d\sigma_g$ が真である．ゆえに，$f(x_1\sigma_g, \cdots, x_n\sigma_g)$ は ε の位置で書換え可能なため，$C[f(s_1, \cdots, s_n)]_p\sigma_{NF}$ は位置 p で書換え可能である．　□

ここで，$\bigvee_{f(x_1,\cdots,x_n)\to r \Leftarrow d \in R} d$ が $\mathcal{M}$ に関して恒真であるということは，f が $\mathcal{G}$ 上の基

底項に関して全域関数であることを意味している．以下に $\bigvee_{f(x_1,\cdots,x_n)\to r\Leftarrow d\in R} d$ が $\mathcal{M}$ に関して恒真となる関数の一例をあげる．

$$R=\left\{\begin{array}{lcl} f(x) & \to & 0 \ \Leftarrow x\le 0 \\ f(x) & \to & s(0) \ \Leftarrow x=s(0) \\ f(x) & \to & f(p(x))+f(p(p(x))) \ \Leftarrow x\ge s(s(0)) \end{array}\right.$$

この関数 f は整数上でのフィボナッチ数を表現している．このように，数学的に定義される関数の多くは $\bigvee_{f(x_1,\cdots,x_n)\to r\Leftarrow d\in R} d$ が $\mathcal{M}$ に関して恒真となるように書くことが可能であると考えられる．さらに，命令型プログラムを制約付き項書換え系に帰着させて帰納的定理を証明することにより元のプログラムの等価性を判定する手法[24] において，命令型プログラムを変換して得られた制約付き項書換え系はこの条件を満たす．よって，この手法は十分に実用的な条件といえる．一方で，$f(x_1,\cdots,x_n)\to r\Leftarrow c$ の形式の規則に対して，$\to_{\{f(x_1,\cdots,x_n)\to r\Leftarrow c\}}\subseteq\succ$ となるように LPO などの経路順序で方向付けすることは難しい．

例 5.2　例 4.2 において，R は $NF_{(T(\mathcal{F}\cup\mathcal{G}),\ \to_R)}\subseteq T(\mathcal{G})$ を満たしている．また，関数記号 u については $\bigvee_{u(n,i,z)\to r\Leftarrow d} d$ は $\mathcal{M}_{PA}$ に関して恒真である．このため，(1) の等式について，位置 ε が $i\le s(n)$ の下での $u(s(n),s(i),z+i)$ の R 完全な出現であることは定理 5.1 よりいえる．逆に，関数記号 sum については $\bigvee_{sum(x)\to r\Leftarrow d} d$ は $\mathcal{M}_{PA}$ に関して恒真でない．このため，(2) の等式について，位置 ε が $\top$ の下での $sum(n)$ の R 完全な出現であることを定理 5.1 により示すことはできない．□

6. 帰納的定理の反証

帰納的定理の反証法とは，等式集合 E が R の帰納的定理でない等式を含むことを証明する手法であり，文献 4), 6) では書換え帰納法による検証に反証機能が組み込まれている．本章では，制約付き項書換え系に対する書換え帰納法の検証に反証機能を組み込む．帰納的定理の証明で検証したい等式集合に帰納的定理でない等式が含まれている場合，検証手続きが暴走してしまう場合が多い．検証の途中で帰納的定理でない等式の存在を判定できたならば，その時点で検証を終えることができるためより効率的な検証を期待できる．

定理 6.1（帰納的定理の反証）　R を $(\mathcal{F},\mathcal{G},\mathcal{P},\mathcal{M})$ 上の制約付き項書換え系とし，R は $\mathcal{M}$ に対して健全性を持つとする．このとき，$(E,\emptyset)\vdash^*_{RI}(E'\cup\{s\approx t\Leftarrow c\},H')$ かつ $s,t\in T(\mathcal{G},\mathcal{V})$ かつ $c\wedge\neg EQ(s,t)$ が $\mathcal{M}$ に関して充足可能のとき，E は R の帰納的定理ではない等式を含む．

［証明］　付録 A.2 を参照．□

この定理から，R が健全性を満たし，帰納的定理の証明のために推論規則を適用させて $(E,\emptyset)\vdash^*_{RI}(E',H')$ となっているときに $s,t\in T(\mathcal{G},\mathcal{V})$ かつ $c\wedge\neg EQ(s,t)$ が $\mathcal{M}$ に関して充足可能である等式 $s\approx t\Leftarrow c$ が E' に出現したならば E が R の帰納的定理ではない等式を含むことが証明される．

反証を図 2 の書換え帰納法の検証手続きに組み込む場合は，図 2 (3) ですべての等式に Deletion が適用可能かを判定する際に，同時に反証の判定を行い，定理 6.1 の条件を満たす等式が存在したときには検証手続きを終了する．この場合には，E には帰納的定理でない等式が存在すると判定する．

例 6.2　R を $(\{sum,fib\},\mathcal{G}_{PA},\mathcal{P}_{PA},\mathcal{M}_{PA})$ 上の制約付項書換え系とし，書換え規則は以下のとおりとする．

$$R=R_{PA}\cup\left\{\begin{array}{rcl} sum(x) & \to & 0 \ \Leftarrow \ x\le 0 \\ sum(s(x)) & \to & sum(x)+s(x) \ \Leftarrow \ x\ge 0 \\ fib(x) & \to & 0 \ \Leftarrow \ x\le 0 \\ fib(s(0)) & \to & s(0) \\ fib(s(s(x))) & \to & fib(s(x))+fib(x) \ \Leftarrow \ x\ge 0 \end{array}\right.$$

このとき，$E=\{sum(n)\approx fib(n)\}$ の等価性を検証した様子を**図 4** に示す．

図 4 の R は $\mathcal{M}_{PA}$ に関する健全性を満たしている．また，図 4 の (5) の等式について考えると，$s(n+0),s(n+s(s(n)))\in T(\mathcal{G},\mathcal{V})$ を満たす．また，$n\ge 0\wedge n\le 0\wedge\neg(s(n+0)=s(n+s(s(n))))$ は n に 0 を代入すると真となるため，$n\ge 0\wedge n\le 0\wedge\neg(s(n+0)=s(n+s(s(n))))$ は $\mathcal{M}_{PA}$ に関して充足可能である．ゆえに，定理 6.1 より $sum(n)\approx fib(n)$ は R の帰納的定理ではない．このため，関数 sum と関数 fib は入力が等しくても出力が一致しない場合が存在することが示された．□

$$
\begin{array}{l}
(E,\emptyset)\\
\vdash^{e}_{RI}\\
\left(\left\{\begin{array}{c} 0\approx sum(n)\ \Leftarrow\ n\le 0\\ s(0)\approx sum(s(0))\\ fib(s(n))+fib(n)\approx sum(s(s(n)))\ \Leftarrow\ n\ge 0\end{array}\right\},\left\{\begin{array}{ll}(1) & fib(n)\to sum(n)\end{array}\right\}\right)\\
\vdash^{s}_{RI}\vdash^{s}_{RI}\vdash^{s}_{RI}\vdash^{s}_{RI}\vdash^{s}_{RI}\vdash^{s}_{RI}\vdash^{s}_{RI}\vdash^{s}_{RI}\vdash^{s}_{RI}\\
\left(\left\{\begin{array}{c} 0\approx 0\ \Leftarrow\ n\le 0\\ s(0)\approx s(0)\\ (2)\quad (sum(n)+s(n))+sum(n)\approx (sum(n)+s(n))+s(s(n))\ \Leftarrow\ n\ge 0\end{array}\right\},\right.\\
\qquad\left.\begin{array}{c}\{\ (1)\ \}\end{array}\right)\\
\vdash^{d}_{RI}\vdash^{d}_{RI}\\
\left(\ \{\ (2)\ \},\{\ (1)\ \}\ \right)\\
\vdash^{e}_{RI}\\
\left(\left\{\begin{array}{c} (sum(n)+s(n))+0\approx (sum(n)+s(n))+s(s(n))\ \Leftarrow\ n\ge 0\wedge n\le 0\\ (3)\quad (sum(s(n))+s(s(n)))+(sum(n)+s(n))\approx\\ \qquad (sum(s(n))+s(s(n)))+s(s(s(n)))\ \Leftarrow\ s(n)\ge 0\wedge n\ge 0\end{array}\right\},\right.\\
\qquad\left.\left\{\begin{array}{c}(1)\\ (4)\quad (sum(n)+s(n))+sum(n)\ \to\ (sum(n)+s(n))+s(s(n))\ \Leftarrow\ n\ge 0\end{array}\right\}\right)\\
\vdash^{s}_{RI}\vdash^{s}_{RI}\vdash^{s}_{RI}\vdash^{s}_{RI}\vdash^{s}_{RI}\vdash^{s}_{RI}\vdash^{s}_{RI}\\
\left(\left\{\begin{array}{ll}(5) & s(n+0)\approx s(n+s(s(n)))\ \Leftarrow\ n\ge 0\wedge n\le 0\\ & (3)\end{array}\right\},\left\{\begin{array}{l}(1)\\ (4)\end{array}\right\}\right)
\end{array}
$$

図 4　帰納的定理の反証例
Fig. 4　Example of disproving inductive theorems.

7. 推論規則の適用条件の緩和

等式 $x+y\approx y+x$ が例 3.8 の R_{PA} の帰納的定理であるかどうかを考える．$(\{x+y\approx y+x\},\emptyset)$ を図 1 の推論規則により検証しようと考えると，どの推論規則も適用できないため検証に失敗する．ここで，a，$b\in\mathcal{F}$ かつ a，b は定数項となる場合を考える．a，b は R_{PA} で書き換えることはできない．このため，$a+b\overset{*}{\leftrightarrow}_{R_{PA}}b+a$ を満たさない．よって，この場合には $x+y\approx y+x$ は R_{PA} の帰納的定理ではない．整数上の $+$ は交換律を満たすにもかかわらず $x+y\approx y+x$ が帰納的定理とならない理由は，a と b が整数として解釈を持つ $T(\mathcal{G}_{PA})$ に書き換えることができないためである．

一方，任意の基底項が $T(\mathcal{G}_{PA})$ 上の項に書き換えることができ，かつ完全性を満たすような

- Simplificaton
  $l\to r\Leftarrow d\in R\cup H$ かつ c は $\mathcal{M}$ に関して充足可能かつ $\neg c\vee d\sigma$ は $\mathcal{M}$ に関して恒真
- Deletion
  $s\equiv t$，または，c は $\mathcal{M}$ に関して充足不能，または，$s\equiv s'\sigma$ かつ $t\equiv t'\sigma$ かつ $s',t'\in T(\mathcal{G},\mathcal{V})$ かつ $EQ(s',t')$ は $\mathcal{M}$ に関して恒真
- EQ-Deletion
  任意の i について $s_i,t_i\in T(\mathcal{G},\mathcal{V})$

図 5　拡張した推論規則の適用条件
Fig. 5　Relaxed side conditions of expanded inference rules.

$(\mathcal{F},\mathcal{G}_{PA},\mathcal{P}_{PA},\mathcal{M}_{PA})$ 上の制約付き項書換え系を $R\cup R_{PA}$ とする．このとき，$x+y\approx y+x$ が $R\cup R_{PA}$ の帰納的定理となるかどうかを考える．任意の s，$t\in T(\mathcal{F}\cup\mathcal{G}_{PA})$ に対して $s\overset{*}{\to}_{R\cup R_{PA}}s'$ かつ $t\overset{*}{\to}_{R\cup R_{PA}}t'$ かつ s'，$t'\in T(\mathcal{G}_{PA})$ とすると，$s+t\overset{*}{\to}_{R\cup R_{PA}}s'+t'$ かつ $t+s\overset{*}{\to}_{R\cup R_{PA}}t'+s'$ となる．ここで，$(s'+t')^{\mathcal{M}}=(t'+s')^{\mathcal{M}}$ は同じ整数に解釈されるため，$s'+t'=t'+s'$ は真である．よって，R の完全性より $s'+t'\overset{*}{\leftrightarrow}_{R\cup R_{PA}}t'+s'$ である．ゆえに，$x+y\approx y+x$ は $R\cup R_{PA}$ の帰納的定理である．

このように，任意の項が必ず解釈を持つ項に書き換えられる制約付き項書換え系では交換律を必要とする等式が帰納的定理であることを証明できる場合が存在する．制約付き項書換え系がこの条件を満たす場合に推論規則の適用条件を緩めてこの例が帰納的定理であると検証できるならば，より強力な検証手法となる．

本章では，制約付き項書換え系がこのような条件を満たす場合に推論規則の適用条件が緩められることを示す．また，この推論規則を用いて証明できる帰納的定理の例を紹介する．

R を $(\mathcal{F},\mathcal{G},\mathcal{P},\mathcal{M})$ 上の制約付き項書換え系とする．R が $NF_{(T(\mathcal{F}\cup\mathcal{G}),\to_R)}\subseteq T(\mathcal{G})$ を満たすとき，図 1 の適用条件は**図 5** のように変更できる．このとき，以下の 2 つの定理が成り立つ．(E,H) に図 5 の適用条件を用いた図 1 の推論規則を 1 回適用させて (E',H') になるとき，$(E,H)\vdash^{*}_{RI'}(E',H')$ と書く．

定理 7.1　R を $(\mathcal{F},\mathcal{G},\mathcal{P},\mathcal{M})$ 上の制約付き項書換え系とする．また，E を $(\mathcal{F},\mathcal{G},\mathcal{P},\mathcal{M})$ 上の制約付き等式の有限集合，$\succ$ を $\to_R\ \subseteq\succ$ を満たす簡約化順序とする．さらに，R は $\mathcal{M}$ に対して完全性と局所健全性を持ち，$NF_{(T(\mathcal{F}\cup\mathcal{G}),\to_R)}\subseteq T(\mathcal{G})$ とする．このとき，$(E,\emptyset)\vdash^{*}_{RI'}(\emptyset,H)$ ならば，E に含まれるすべての等式は R の帰納的定理である．

［証明］　付録 A.3 を参照. □

定理 7.2（帰納的定理の反証） R を $(\mathcal{F},\mathcal{G},\mathcal{P},\mathcal{M})$ 上の制約付き項書換え系とし，R は $\mathcal{M}$ に対して健全性を持つとする．このとき，$(E,\emptyset)\vdash^{*}_{RI'}(E'\cup\{s\approx t\Leftarrow c\},H')$ かつ s, $t\in T(\mathcal{G},\mathcal{V})$ かつ $c\wedge\neg EQ(s,t)$ が $\mathcal{M}$ に関して充足可能のとき，E は R の帰納的定理ではない等式を含む.

［証明］　定理 6.1 の証明と同様である. □

適用条件を緩和した推論規則を用いた帰納的定理の検証手続きは図 2 のままでよい．よって，$NF_{(T(\mathcal{F}\cup\mathcal{G}),\to_R)}\subseteq T(\mathcal{G})$ が判定できなければ図 1 の推論規則で，判定できれば図 5 の適用条件に緩めた推論規則で帰納的定理を検証すればよい.

$NF_{(T(\mathcal{F}\cup\mathcal{G}_{PA}),\to_{R\cup R_{PA}})}\subseteq T(\mathcal{G}_{PA})$ を満たすような制約付き項書換え系 $R\cup R_{PA}$ について，$x+y\approx y+x$ を検証することを考える．適用条件を緩和する前では，$(\{x+y\approx y+x\},\emptyset)$ は $\mathcal{V}ar(x+y)\subseteq fv(\top)$ を満たさないため EQ-Deletion を適用することはできなかった．しかし，適用条件を図 5 のように緩めると，$\mathcal{V}ar(x+y)\subseteq fv(\top)$ を満たす必要がなくなる．このため，EQ-Deletion が適用可能になり $(\{x+y\approx y+x\Leftarrow\neg(x+y=y+x)\},\emptyset)$ となる．$\neg(x+y=y+x)$ は $\mathcal{M}_{PA}$ に対して充足不能なため Deletion が適用でき，$(\emptyset,\emptyset)$ となるため検証に成功する.

例 7.3 R を $(\{pwr,pwr1\},\{0,s,+,\times,h\},\{=,Ev\},\mathcal{M})$ 上の制約付き項書換え系とし，書換え規則は以下のとおりとする.

$$R=\left\{\begin{array}{ll}
pwr(x,0)\to s(0) & \\
pwr(x,s(y))\to pwr(x,y)\times x & \\
pwr1(x,0)\to s(0) & \\
pwr1(x,s(y))\to(pwr1(x,h(y))\times pwr1(x,h(y)))\times x & \Leftarrow Ev(y)\\
pwr1(x,s(y))\to pwr1(x,h(s(y)))\times pwr1(x,h(s(y))) & \Leftarrow\neg Ev(y)\\
0+y\to y & s(x)+y\to s(x+y)\\
0\times y\to 0 & s(x)\times y\to(x\times y)+y\\
h(0)\to 0 & h(s(0))\to 0\\
h(s(s(x)))\to s(h(x)) &
\end{array}\right.$$

$$\begin{array}{l}
(E,\emptyset)\\
\vdash^{e}_{RI'}\\
\left(\left\{\begin{array}{c} s(0)\approx pwr1(x,0)\\ pwr(x,y)\times x\approx pwr1(x,s(y))\end{array}\right\},\left\{\begin{array}{ll}(1) & pwr(x,y)\to pwr1(x,y)\end{array}\right\}\right)\\
\vdash^{s}_{RI'}\vdash^{d}_{RI'}\\
\left(\left\{\begin{array}{c} pwr1(x,y)\times x\approx pwr1(x,s(y))\end{array}\right\},\{(1)\}\right)\\
\vdash^{e}_{RI'}\\
\left(\begin{array}{c}\left\{\begin{array}{ll}& (pwr1(x,h(y))\times pwr1(x,h(y)))\times x\approx pwr1(x,y)\times x\ \Leftarrow Ev(y)\\ (2)& pwr1(x,h(s(y)))\times pwr1(x,h(s(y)))\approx pwr1(x,y)\times x\ \Leftarrow\neg Ev(y)\end{array}\right\},\\ \left\{\begin{array}{lll}(1), & (3) & pwr1(x,s(y))\to pwr1(x,y)\times x\end{array}\right\}\end{array}\right)\\
\vdash^{e}_{RI'}\\
\left(\begin{array}{c}\left\{\begin{array}{c}(2)\\ pwr1(x,0)\times x\approx(q(x,h(0))\times pwr1(x,h(0)))\times x\ \Leftarrow Ev(0)\\ ((pwr1(x,h(y))\times pwr1(x,h(y)))\times x)\times x\\ \quad\approx(pwr1(x,h(s(y)))\times pwr1(x,h(s(y))))\times x\ \Leftarrow Ev(s(y))\wedge Ev(y)\\ pwr1(x,h(s(y)))\times pwr1(x,h(s(y)))\times x\\ \quad\approx(pwr1(x,h(s(y)))\times pwr1(x,h(s(y))))\times x\ \Leftarrow Ev(s(y))\wedge\neg Ev(y)\end{array}\right\},\\ \left\{\begin{array}{ll}(1),(3),\ (4) & pwr1(x,y)\times x\to(pwr1(x,h(y))\times pwr1(x,h(y)))\times x\ \Leftarrow Ev(y)\end{array}\right\}\end{array}\right)\\
\vdash^{d}_{RI'}\vdash^{d}_{RI'}\vdash^{d}_{RI'}\vdash^{e}_{RI'}\\
\left(\begin{array}{c}\left\{\begin{array}{l}pwr1(x,0)\times x\approx pwr1(x,h(s(0)))\times q(x,h(s(0)))\ \Leftarrow\neg Ev(0)\\ ((pwr1(x,h(y))\times pwr1(x,h(y)))\times x)\times x\\ \quad\approx pwr1(x,h(s(s(y))))\times pwr1(x,h(s(s(y))))\ \Leftarrow\neg Ev(s(y))\wedge Ev(y)\\ pwr1(x,h(s(y)))\times pwr1(x,h(s(y)))\times x\\ \quad\approx pwr1(x,h(s(s(y))))\times pwr1(x,h(s(s(y))))\ \Leftarrow\neg Ev(s(y))\wedge\neg Ev(y)\end{array}\right\},\\ \left\{\begin{array}{l}(1),(3),(4),(5)\ pwr1(x,y)\times x\to pwr1(x,h(s(y)))\times pwr1(x,h(s(y)))\ \Leftarrow\neg Ev(y)\end{array}\right\}\end{array}\right)\\
\vdash^{d}_{RI'}\vdash^{d}_{RI'}\vdash^{s}_{RI'}\\
\left(\begin{array}{c}\left\{\begin{array}{ll}(6) & ((pwr1(x,h(y))\times pwr1(x,h(y)))\times x)\times x\\ & \quad\approx(pwr1(x,h(y))\times x)\times(pwr1(x,h(y))\times x)\ \Leftarrow\neg Ev(s(y))\wedge Ev(y)\end{array}\right\},\\ \{(1),(3),(4),(5)\}\end{array}\right)
\end{array}$$

図 6　拡張した推論規則による帰納的定理の証明例
Fig. 6　Example of proving inductive theorems for expanded inference rule.

ここで，$\mathcal{M}$ の領域を自然数とし，$\times^{\mathcal{M}}$ は自然数上の乗算，$h^{\mathcal{M}}$ は自然数を 2 で割る関数，$Ev^{\mathcal{M}}$ は偶数ならば $\top$，奇数ならば $\bot$ を返す関数とする．このとき，$E=\{pwr(x,y)\approx pwr1(x,y)\}$ の等価性を検証した様子を**図 6** に示す．図 6 の R は停止性，$\mathcal{M}$ に関する完全性と局所健全性を満たし，$NF_{(T(\mathcal{F}\cup\mathcal{G}),\to_R)}\subseteq T(\mathcal{G})$ である．図 6 の (6) は $(((z\times z)\times x)\times x)\sigma\approx$

$((z \times x) \times (z \times x))\sigma \Leftarrow c$ の形をしている．多項式の正規表現を定めればこれらの式は同一の表現になるので，$((z \times z) \times x) \times x = (z \times x) \times (z \times x)$ は $\mathcal{M}$ に対して恒真であることは明らかである．ゆえに，等式 (6) は Deletion により削除でき検証手続きは成功するため，$pwr(x, y) \approx pwr1(x, y)$ は R の帰納的定理である．□

図 6 の等式 (6) は交換律と結合律を組み合わせることにより成り立つ等式を削除できる例である．項書換え系における書換え帰納法において，交換律を満たす等式は証明できない場合が多い．これは，交換律を満たす等式を Expansion により書換え規則として H に追加しようとすると，H は停止性を満たさなくなるからである．このため，書換え帰納法を順序付き書換えに拡張する必要がある[1),4),10)]．しかし，今回提案した推論規則ではモデル上の等価性を用いて等式を削除することが可能なため，順序付き書換えに拡張せずに交換律を必要とする等式を証明できる場合が存在する．

8. 関 連 研 究

本章では，関連研究との比較を述べる．

文献 24) の潜在帰納法に基づいた検証法では，制約部分を分解する推論規則が必要であった．しかし，本論文ではそのような規則がなくても，文献 24) の例の検証に成功した．さらに，自然数だけでなく整数も容易に扱うことも可能となった．文献 24) の手法は前述の制約分解のための推論規則をどのように適用すればよいかが十分に分かっておらず，手続きの自動化に課題を残していた．一方で，本論文の手法ではそのような推論規則は用いないので，手続きの自動化は比較的簡単である．

$\mathcal{G}$ が空集合かつ等式および書換え規則が制約を持たない場合，EQ-Deletion を適用する状況は生じない．また，この場合は制約を考慮しないので他の推論規則は項書換え系の場合と一致する[20),23)]．よって，本論文の手法は，項書換え系における書換え帰納法を制約付き項書換え系に拡張した手法といえる．また，交換律のような従来の書換え帰納法では証明できなかった等式の帰納的定理を証明するため，順序付き書換えにおける書換え帰納法に関する研究が行われている[1),4),10)]．しかし本手法では，モデル上でに意味の解釈で交換律を吸収できるならば，交換律を含むような等式でも帰納的定理であると判定することが可能な場合が存在する．特に，$NF_{(T(\mathcal{F} \cup \mathcal{G}),\ \rightarrow_R)} \subseteq T(\mathcal{G})$ を満たす制約付き項書換え系ならばモデル上で等価だと証明できる等式のほとんどが判定可能になると期待できる．

我々が知る限りでは制約付き項書換え系の書換え帰納法の研究は他にはないが，類似する研究として条件付き項書換え系における書換え帰納法があげられる．文献 6) では条件付き項書換え系における書換え帰納法が提案されており，文献 2) では文献 7) に基づき条件の判定に決定手続きを組み込む手法が提案されている．文献 2)，6) の手法は定理自動証明器 SPIKE[5)] に導入されている．

本論文では，ユーザが与えたモデルを用いて制約の真偽判定を行う．一方，文献 2) では，ユーザが公理を与え，その公理の下で任意のモデルが条件を満たすことを判定する．よって，文献 2) ではモデルを特定せずに条件の判定を行っているため，文献 2) の条件付き項書換え系はモデルを特定する制約付き項書換え系よりも一般的な枠組みであり，条件部の記述により表現力が豊かである．また，文献 2) では公理によって条件の判定と項の書換えを行うため，本論文で提案した健全性，完全性に相当するものは必要とならない．

本論文の目的である手続き型プログラムの等価性の検証では，整数などのすでに意味を与えられているようなデータを扱うことがほとんどである．このため，文献 2) のようにモデルを特定しない一般的な枠組みで検証を行う必要はない．本論文では，モデルを特定することによって制約の判定を効率良く行える．また，制約の判定と項の書換えは完全に分離しているため，制約部の判定に既存の手続きをそのまま組み込むことが可能である．

本論文と文献 2) との大きな違いは制約の恒真性の判定である．本論文では，制約への任意の基底代入が真であることを示す．文献 2) では，公理を用いて条件の否定が充足不能であることを示す．このため，本論文と文献 2) では，制約と条件の恒真性を判定する場合に，同様の制約ソルバを用いたとしても結果が異なる場合が存在すると考えられる．さらに，モデルや公理の与え方により帰納的定理の証明能力に差が出るため，本論文と文献 2) の検証能力を理論的に比較することは困難である．

9. お わ り に

本論文では，制約付き項書換え系が意味論に対して満たすべき性質を提案し，制約付き項書換え系における書換え帰納法の推論規則を提案した．また，帰納的定理の反証法についても提案し，さらに，すべての正規形が解釈可能である場合に書換え帰納法の推論規則の適用条件を緩和できることを示した．

今後の課題として，型付き制約付き項書換え系への拡張があげられる．今回提案した制約付き項書換え系では型の導入を見送った．このため，リストや集合などを制約にすることは難しい．なぜならば，制約で整数とリストを同時に表現しようとすると，モデルの領域は整数とリストを含む集合でなければならず，その領域で関数記号，述語記号の解釈を考える必

要があるからである．型を考えることで，モデルの領域を整数とリストで分けることが可能になり，そのような問題は起きない．リストを用いた帰納的定理の証明ではリストに関する制約を表現する必要があり，型付き制約付き項書換え系に拡張する必要がある．

制約付き項書換え系における停止性の判定，正規形の集合の判定は，現在のところ人間が行う必要がある．このため，これらの判定方法の提案は今後の課題である．文献 12) では自然数上のプレスブルガー算術を制約に持つ等式付き書換えの体系である CES の停止性証明の手法が提案された．この停止性証明法は本論文の制約付き項書換え系の停止性証明に応用できると予想される．

謝辞　本研究は一部，文部科学省科学研究費#18500011，#20300010，#20500008，および栢森情報科学振興財団の補助を受けている．

参 考 文 献

1) Aoto, T.: Soundness of rewriting induction based on an abstract principle, *IPSJ Trans. Programming*, Vol.49, No.Sig 1(PRO 35), pp.26–38 (2008).
2) Armando, A., Rusinowitch, M. and Stratulat, S.: Incorporating Decision Procedures in Implicit Induction, *Journal of Symbolic Computation*, Vol.34, pp.241–258 (2002).
3) Baader, F. and Nipkow, T.: *Term Rewriting and All That*, Cambridge University Press (1998).
4) Bouhoula, A.: Automated Theorem Proving by Test Set Induction, *Journal of Symbolic Computation*, Vol.23, No.1, pp.47–77 (1997).
5) Bouhoula, A., Kounalis, E. and Rusinowitch, M.: Automated Mathematical Induction, *Journal of Logic and Computation*, Vol.5, No.5, pp.631–668 (1995).
6) Bouhoula, A. and Rusinowitch, M.: Implicit Induction in Conditional Theories, *Journal of Automated Reasoning*, Vol.14, pp.189–235 (1995).
7) Boyer, R.S. and Moore, J.S.: Integrating Decision Procedures into Heuristic Theorem Provers: A Case Study of Linear Arithmetic, *Machine Intelligence*, Vol.11, pp.83–124 (1988).
8) Clarke, E.M. and Emerson, E.A.: Design and Synthesis of Synchronization Skeletons Using Branching Time Temporal Logic, *Proc. Logic and Programs Workshop*, Lecture Notes in Computer Science, Vol.131, pp.52–71, Springer (1981).
9) Cooper, D.: Theorem Proving in Arithmetic without Multiplication, *Proc. 7th Annual Machine Intelligence Workshop, Machine Intelligence*, No.7, pp.91–99, Edinburgh University Press (1972).
10) Dershowitz, N. and Reddy, U.S.: Deductive and inductive synthesis of equational programs, *Journal of Symbolic Computation*, Vol.15, pp.467–494 (1993)
11) Dijkstra, E.W.: *A Discipline of Programming*, Prentice-Hall (1976).
12) Falke, S. and Kapur, D.: Dependency Pairs for Rewriting with Built-in Numbers and Semantic Data Structures, *Proc. 19th International Conference on Rewriting Techniques and Applications*, Lecture Notes of Computer Science, Vol.5117, pp.94–109 (2008).
13) Fribourg, L.: A strong restriction of the inductive completion procedure, *Journal of Symbolic Computation*, Vol.8, pp.253–276 (1989).
14) Hoare, C.A.R.: An Axiomatic Basis for Computer Programming, *Comm. ACM*, Vol.12, No.10, pp.576–580 (1969).
15) Huet, G.P. and Hullot, J.-M.: Proofs by Induction in Equational Theories with Constructors, *Journal of Computer and System Sciences*, Vol.25, No.2, pp.239–266 (1982).
16) Huth, M. and Ryan, M.: *Logic in Computer Science: Modelling and Reasoning about Systems*, Cambridge University Press (2000).
17) Musser, D.R.: On Proving Inductive Properties of Abstract Data Types, *Conference Record of the 7th Annual ACM Symposium on Principles of Programming Languages*, pp.154–162 (1980).
18) Presburger, M.: Uber die Vollstandigkeit eines gewissen Systems der Arithmetic ganzer Zahlen, in welchem die Addition als einzige Operation hervortritt, *Compte-Rendus dei Congres des Mathematiciens des Pays Slavs* (1929).
19) Queille, J.-P. and Sifakis, J.: Specification and Verification of Concurrent Systems in CESAR, *Proc. 5th International Symposium on Programming*, Lecture Notes in Computer Science, Vol.137, pp.337–351, Springer (1982).
20) Reddy, U.S.: Term Rewriting Induction, *Proc. 10th International Conference on Automated Deduction*, Lecture Notes in Computer Science, Vol.449, pp.162–177, Springer (1990).
21) 伊理正夫，野崎明弘，野下浩平（編）：計算の効率とその限界，入門現代の数学 [13]，日本評論社 (1980).
22) 東野輝夫，北道淳司，谷口健一：整数上の線形制約の処理と応用，コンピュータソフトウェア，Vol.9, No.6, pp.31–39 (1992).
23) 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.162–170 (2000).
24) 古市祐樹，西田直樹，酒井正彦，草刈圭一朗，坂部俊樹：制約付き項書換え系の潜在帰納法を利用した手続きプログラム検証の試み，情報処理学会論文誌：プログラミング，Vol.1, No.2, pp.100–121 (2008).

付　　録

A.1　定理 4.1 の証明

文献 23) では以下の抽象書換え系での原理を用いて項書換え系における書換え帰納法の正しさを証明している．

命題 A.1.1　$\rightarrow_1$, $\rightarrow_2$ を A 上の抽象書換え系とする．このとき，以下の性質が成り立つならば $\overset{*}{\leftrightarrow}_1 = \overset{*}{\leftrightarrow}_2$ である．

- $\rightarrow_1 \subseteq \rightarrow_2$.
- $\rightarrow_2$ は停止性を持つ．
- $\rightarrow_{1\cup 2} \subseteq \rightarrow_1 \circ \overset{*}{\rightarrow}_{1\cup 2} \circ \overset{*}{\leftarrow}_{1\cup 2}$.

しかし，本論文では EQ-Deletion を導入したためにこの原理を用いて本論文で提案した制約付き項書換え系における帰納的定理の正しさを証明することはできない．よって，定理 4.1 の証明に利用できるようにこの原理の条件を緩める．

定理 A.1.2　$\rightarrow_1$, $\rightarrow_2$ を A 上の抽象書換え系とする．このとき，以下の性質が成り立つならば $\overset{*}{\leftrightarrow}_1 = \overset{*}{\leftrightarrow}_2$ である．

- $\rightarrow_1 \subseteq \rightarrow_2$.
- $\rightarrow_2$ は停止性を持つ．
- $\rightarrow_2 \subseteq \rightarrow_1 \circ \overset{*}{\rightarrow}_2 \circ \overset{*}{\leftrightarrow}_1 \circ \overset{*}{\leftarrow}_2$.

［証明］　仮定 $\rightarrow_1 \subseteq \rightarrow_2$ より $\overset{*}{\leftrightarrow}_1 \subseteq \overset{*}{\leftrightarrow}_2$ は成り立つ．よって，任意の x，$y \in A$ について，$x \overset{*}{\rightarrow}_2 y$ ならば $x \overset{*}{\leftrightarrow}_1 y$ であることを $\rightarrow_2$ に関するネータ帰納法で証明することによって $\overset{*}{\leftrightarrow}_2 \subseteq \overset{*}{\leftrightarrow}_1$ を示す．

- $x = y$ のとき，明らかに $x \overset{*}{\leftrightarrow}_1 y$ である．
- $x \rightarrow_2 z \overset{*}{\rightarrow}_2 y$ のとき，ある u，v，w が存在して $x \rightarrow_1 u \overset{*}{\rightarrow}_2 v \overset{*}{\leftrightarrow}_1 w \overset{*}{\leftarrow}_2 z$ が成り立つ．ここで，$x \rightarrow_2 z \overset{*}{\rightarrow}_2 y$ かつ $x \rightarrow_2 z \overset{*}{\rightarrow}_2 w$ かつ $x \rightarrow_2 u \overset{*}{\rightarrow}_2 v$ から，帰納法の仮定より，$z \overset{*}{\leftrightarrow}_1 y$ かつ $u \overset{*}{\leftrightarrow}_1 v$ かつ $w \overset{*}{\leftrightarrow}_1 z$．ゆえに，$x \overset{*}{\leftrightarrow}_1 y$ である．　□

次に，代入に対しての書換えの性質を示す．

補題 A.1.3　R を $(\mathcal{F}, \mathcal{G}, \mathcal{P}, \mathcal{M})$ 上の制約付き項書換え系とし，R は停止性，$\mathcal{M}$ に対して局所健全性を持つとする．また，s，$t \in T(\mathcal{F} \cup \mathcal{G}, \mathcal{V})$，$c$ を制約，σ_g を基底代入とする．このとき，$c\sigma_g$ が真ならば $s\sigma_g \overset{*}{\rightarrow}_R s\sigma_{NF}$ かつ $t\sigma_g \overset{*}{\rightarrow}_R t\sigma_{NF}$ となる基底正規形代入 σ_{NF} が存在して，$c\sigma_{NF}$ が真である．

［証明］　R の停止性より任意の変数 x に対して $x\sigma_g$ の正規形は存在する．よって，局所健全性から明らかに成り立つ．　□

次に，$Expd$ の性質を示す．

補題 A.1.4　R を $(\mathcal{F}, \mathcal{G}, \mathcal{P}, \mathcal{M})$ 上の制約付き項書換え系，s，$t \in T(\mathcal{F} \cup \mathcal{G}, \mathcal{V})$，$c$ を制約，s の位置 p を c の下での R 完全な出現とする．このとき $c\sigma_{NF}$ を真とする任意の基底正規形代入 σ_{NF} に対して，$s\sigma_{NF} \rightarrow_R \circ \leftrightarrow_{Expd(s,t,c,p)} t\sigma_{NF}$ である．

［証明］　$s \equiv C[u]_p$，σ_{NF} を $c\sigma_{NF}$ を真とする基底正規形代入とする．このとき，$s\sigma_{NF} \equiv C\sigma_{NF}[u\sigma_{NF}]_p$ であり，位置 p が c の下での s の R 完全な出現なので，$s\sigma_{NF}$ を位置 p で書き換える規則 $l \rightarrow r \Leftarrow d \in R$ と，$l\theta_g \equiv u\sigma_{NF}$ かつ $d\theta_g$ が真となる基底代入 θ_g が存在する．ここで，$\mathcal{V}ar(l) \cap \mathcal{V}ar(u) = \emptyset$ としても一般性を失わない．このとき，$\mathcal{D}om(\sigma_{NF}) \cap \mathcal{D}om(\theta_g) = \emptyset$ とすると，$u\sigma_{NF} \equiv u\theta_g\sigma_{NF}$，$l\theta_g \equiv l\theta_g\sigma_{NF}$ であるため，$\theta_g\sigma_{NF}$ は u と l の単一化子である．よって，$\sigma = mgu(u, l)$ が存在し，$\theta_g\sigma_{NF} = \sigma\sigma_g$ となる基底代入 σ_g が存在する．また，$c\sigma_{NF}$ が真かつ $d\theta_g$ が真のため，$c\theta_g\sigma_{NF}$ が真かつ $d\theta_g\sigma_{NF}$ が真である．さらに，$\theta_g\sigma_{NF} = \sigma\sigma_g$ であることから，$(c\sigma \wedge d\sigma)\sigma_g$ も真である．また，$C[r]_p\sigma \approx t\sigma \Leftarrow c\sigma \wedge d\sigma \in Expd(s, t, c, p)$ である．ゆえに，$s\sigma_{NF} \equiv s\theta_g\sigma_{NF} \equiv C\theta_g\sigma_{NF}[u\theta_g\sigma_{NF}]_p \equiv C\theta_g\sigma_{NF}[l\theta_g\sigma_{NF}]_p \rightarrow_{\{l\rightarrow r\Leftarrow d\}} C\theta_g\sigma_{NF}[r\theta_g\sigma_{NF}]_p \equiv C[r]_p\theta_g\sigma_{NF} \equiv C[r]_p\sigma\sigma_g \leftrightarrow_{Expd(s,t,c,p)} t\sigma\sigma_g \equiv t\theta_g\sigma_{NF} \equiv t\sigma_{NF}$ である．　□

次に，EQ-Deletion で変形する等式の性質を示す．

補題 A.1.5　R を $(\mathcal{F}, \mathcal{G}, \mathcal{P}, \mathcal{M})$ 上の制約付き項書換え系とし，$s_1, \cdots, s_n, t_1, \cdots, t_n \in T(\mathcal{G}, \mathcal{V})$，$C[\,] \in T_\Box(\mathcal{F} \cup \mathcal{G}, \mathcal{V})$，$c$ を制約，$\mathcal{V}ar(s_1, \cdots, s_n, , t_1, \cdots, t_n) \subseteq fv(c)$ とする．このとき，R が $\mathcal{M}$ に対して完全性を持つならば，基底項上で $\leftrightarrow_{\{C[s_1,\cdots,s_n]\simeq C[t_1,\cdots,t_n]\Leftarrow c\}} \subseteq \leftrightarrow_{\{C[s_1,\cdots,s_n]\approx C[t_1,\cdots,t_n]\Leftarrow c\wedge\neg(\bigwedge_{i=1}^{n} EQ(s_i,t_i))\}} \cup \overset{*}{\leftrightarrow}_R$ である．

［証明］　$(C[s_1,\cdots,s_n])\sigma_g \leftrightarrow_{\{C[s_1,\cdots,s_n]\simeq C[t_1,\cdots,t_n]\Leftarrow c\}} (C[t_1,\cdots,t_n])\sigma_g$ とする．このとき，$c\sigma_g$ は真である．ここで，$\mathcal{V}ar(s_1,\cdots,s_n,,t_1,\cdots,t_n) \subseteq fv(c)$ より $\mathcal{R}an(\sigma_g|_{\mathcal{V}ar(s_1,\cdots,s_n,,t_1,\cdots,t_n)}) \subseteq T(\mathcal{G})$ を満たすため，任意の i について $s_i\sigma_g,\ t_i\sigma_g \in T(\mathcal{G})$ となり $EQ(s_i\sigma_g, t_i\sigma_g)$ の真偽が決まる．

- $\bigwedge_{i=1}^{n} EQ(s_i\sigma_g, t_i\sigma_g)$ が真のとき，R の完全性より $s_i\sigma_g \overset{*}{\leftrightarrow}_R t_i\sigma_g$．よって，$(C[s_1,\cdots,s_n])\sigma_g \overset{*}{\leftrightarrow}_R (C[t_1,\cdots,t_n])\sigma_g$ である．
- $\bigwedge_{i=1}^{n} EQ(s_i\sigma_g, t_i\sigma_g)$ が偽のとき，$c\sigma_g \wedge \neg(\bigwedge_{i=1}^{n} EQ(s_i\sigma_g, t_i\sigma_g))$ が真より $(C[s_1,\cdots,s_n])\sigma_g \leftrightarrow_{\{C[s_1,\cdots,s_n]\simeq C[t_1,\cdots,t_n]\Leftarrow c\wedge\neg(\bigwedge_{i=1}^{n} EQ(s_i,t_i))\}} (C[t_1,\cdots,t_n])\sigma_g$ である．　□

次に，推論規則を 1 回だけ適用した際の性質を明らかにする．

補題 A.1.6　R を $(\mathcal{F},\mathcal{G},\mathcal{P},\mathcal{M})$ 上の制約付き項書換え系とし，R は $\mathcal{M}$ に対して完全性を持つとする．このとき，$(E,H) \vdash_{RI} (E',H')$ ならば，基底項上で $\leftrightarrow_E \subseteq \overset{*}{\rightarrow}_{R\cup H'} \circ (\leftrightarrow_{E'} \cup \overset{*}{\leftrightarrow}_R) \circ \overset{*}{\leftarrow}_{R\cup H'}$ である．

［証明］　適用した推論規則で場合分けを行う．

- Simplification のとき，$\leftrightarrow_{E\setminus E'} \subseteq (\rightarrow_{R\cup H'} \circ \leftrightarrow_{E'}) \cup (\leftrightarrow_{E'} \circ \leftarrow_{R\cup H'})$ より成り立つ．
- Deletion のとき，$\leftrightarrow_{E'} \subseteq \leftrightarrow_E \cup \equiv$ より成り立つ．
- Expansion のとき，$\leftrightarrow_{E\setminus E'} = \leftrightarrow_{H'\setminus H}$ より $\leftrightarrow_E \subseteq \leftrightarrow_{E'\cup H'}$ なので成り立つ．
- EQ-Deletion のとき，補題 A.1.5 より $\leftrightarrow_{E\setminus E'} \subseteq \leftrightarrow_{E'} \cup \overset{*}{\leftrightarrow}_R$．よって，成り立つ．

□

補題 A.1.7　R を $(\mathcal{F},\mathcal{G},\mathcal{P},\mathcal{M})$ 上の制約付き項書換え系とし，R は停止性，$\mathcal{M}$ に対して完全性と局所健全性を持つとする．さらに，$(E,H) \vdash_{RI} (E',H')$ とする．このとき，基底項上で $\rightarrow_{R\cup H} \subseteq \rightarrow_R \circ \overset{*}{\rightarrow}_{R\cup H} \circ (\leftrightarrow_E \cup \overset{*}{\leftrightarrow}_R) \circ \overset{*}{\leftarrow}_{R\cup H}$ ならば，基底項上で $\rightarrow_{R\cup H'} \subseteq \rightarrow_R \circ \overset{*}{\rightarrow}_{R\cup H'} \circ (\leftrightarrow_{E'} \cup \overset{*}{\leftrightarrow}_R) \circ \overset{*}{\leftarrow}_{R\cup H'}$ である．

［証明］　$\rightarrow_{H'} \subseteq \rightarrow_R \circ \overset{*}{\rightarrow}_{R\cup H'} \circ (\leftrightarrow_{E'} \cup \overset{*}{\leftrightarrow}_R) \circ \overset{*}{\leftarrow}_{R\cup H'}$ を示せば十分である．基底項上で $\rightarrow_{R\cup H} \subseteq \rightarrow_R \circ \overset{*}{\rightarrow}_{R\cup H} \circ (\leftrightarrow_E \cup \overset{*}{\leftrightarrow}_R) \circ \overset{*}{\leftarrow}_{R\cup H}$ かつ $s_g \rightarrow_{H'} t_g$ とする．推論規則の定義より $H \subseteq H'$ である．

- $s_g \rightarrow_H t_g$ のとき，仮定より $s_g \rightarrow_R \circ \overset{*}{\rightarrow}_{R\cup H} \circ (\leftrightarrow_E \cup \overset{*}{\leftrightarrow}_R) \circ \overset{*}{\leftarrow}_{R\cup H} t_g$．$H \subseteq H'$ より $s_g \rightarrow_R \circ \overset{*}{\rightarrow}_{R\cup H'} \circ (\leftrightarrow_E \cup \overset{*}{\leftrightarrow}_R) \circ \overset{*}{\leftarrow}_{R\cup H'} t_g$．よって，補題 A.1.6 より $\leftrightarrow_E \subseteq \overset{*}{\rightarrow}_{R\cup H'} \circ (\leftrightarrow_{E'} \cup \overset{*}{\leftrightarrow}_R) \circ \overset{*}{\leftarrow}_{R\cup H'}$ なので，$s_g \rightarrow_R \circ \overset{*}{\rightarrow}_{R\cup H'} \circ (\leftrightarrow_{E'} \cup \overset{*}{\leftrightarrow}_R) \circ \overset{*}{\leftarrow}_{R\cup H'} t_g$ である．
- $s_g \rightarrow_{H'\setminus H} t_g$ のとき，$H'\setminus H \neq \emptyset$ となるのは Expansion を適用したときのみである．$s \rightarrow t \Leftarrow c \in H'\setminus H$，$s_g \equiv C[s\sigma_g]$，$t_g \equiv C[t\sigma_g]$，$c\sigma_g$ は真とする．このとき，補題 A.1.3 からある基底正規形代入 σ_{NF} が存在して $s\sigma_g \overset{*}{\rightarrow}_R s\sigma_{NF}$ かつ $t\sigma_g \overset{*}{\rightarrow}_R t\sigma_{NF}$ かつ $c\sigma_{NF}$ が真である．また，補題 A.1.4 より $s\sigma_{NF} \rightarrow_R \circ \leftrightarrow_{E'} t\sigma_{NF}$．よって，$s_g \overset{*}{\rightarrow}_R \circ \rightarrow_R \circ \overset{*}{\rightarrow}_{R\cup H'} \circ (\leftrightarrow_{E'} \cup \overset{*}{\leftrightarrow}_R) \circ \overset{*}{\leftarrow}_{R\cup H'} \circ \overset{*}{\leftarrow}_R t_g$ が成り立つ．ゆえに，$s_g \rightarrow_R \circ \overset{*}{\rightarrow}_{R\cup H'} \circ (\leftrightarrow_{E'} \cup \overset{*}{\leftrightarrow}_R) \circ \overset{*}{\leftarrow}_{R\cup H'} t_g$ である．　□

補題 A.1.8　R を $(\mathcal{F},\mathcal{G},\mathcal{P},\mathcal{M})$ 上の制約付き項書換え系とし，$\succ$ を $\rightarrow_R \subseteq \succ$ を満たす簡約化順序とする．さらに $(E,H) \vdash_{RI} (E',H')$ とする．このとき，$\rightarrow_H \subseteq \succ$ ならば $\rightarrow_{H'} \subseteq \succ$ である．

［証明］　Simplification，Deletion，EQ-Deletion を適用したときは $H = H'$ より成り立つ．また，Expansion を適用したときは推論規則の適用条件より $\rightarrow_{H'} \subseteq \succ$ である．　□

以下で，推論規則を複数回適用したときの性質をまとめる．

補題 A.1.9　R を $(\mathcal{F},\mathcal{G},\mathcal{P},\mathcal{M})$ 上の制約付き項書換え系とし，$\succ$ を $\rightarrow_R \subseteq \succ$ を満たす簡約化順序とする．また，R は $\mathcal{M}$ に対して完全性と局所健全性を持つとする．さらに，$(E,H) \vdash^{*}_{RI} (E',H')$ とする．このとき，以下のすべてが成り立つ．

(1)　基底項上で $\leftrightarrow_E \subseteq \overset{*}{\rightarrow}_{R\cup H'} \circ (\leftrightarrow_{E'} \cup \overset{*}{\leftrightarrow}_R) \circ \overset{*}{\leftarrow}_{R\cup H'}$．

(2)　基底項上で $\rightarrow_{R\cup H} \subseteq \rightarrow_R \circ \overset{*}{\rightarrow}_{R\cup H} \circ (\leftrightarrow_E \cup \overset{*}{\leftrightarrow}_R) \circ \overset{*}{\leftarrow}_{R\cup H}$ ならば，基底項上で $\rightarrow_{R\cup H'} \subseteq \rightarrow_R \circ \overset{*}{\rightarrow}_{R\cup H'} \circ (\leftrightarrow_{E'} \cup \overset{*}{\leftrightarrow}_R) \circ \overset{*}{\leftarrow}_{R\cup H'}$．

(3)　$\rightarrow_H \subseteq \succ$ ならば $\rightarrow_{H'} \subseteq \succ$．

［証明］　(1) は補題 A.1.6 より，(2) は補題 A.1.7 より，(3) は補題 A.1.8 より成り立つ．　□

最後に定理 4.1 の証明を与える．

［証明］　E のすべての等式が R の帰納的定理であることを示すには，基底項上で $\leftrightarrow_E \subseteq \overset{*}{\leftrightarrow}_R$ を示せばよい．補題 A.1.9(1) より $\leftrightarrow_E \subseteq \overset{*}{\rightarrow}_{R\cup H} \circ \overset{*}{\leftrightarrow}_R \circ \overset{*}{\leftarrow}_{R\cup H}$．ここで，$\rightarrow_R \subseteq \rightarrow_{R\cup H}$ は明らかに成り立つ．また，補題 A.1.9(3) より $\rightarrow_{R\cup H} \subseteq \succ$．よって，$\rightarrow_{R\cup H}$ は停止性を持つ．さらに，補題 A.1.9(2) より，$\rightarrow_{R\cup H} \subseteq \rightarrow_R \circ \overset{*}{\rightarrow}_{R\cup H} \circ \overset{*}{\leftrightarrow}_R \circ \overset{*}{\leftarrow}_{R\cup H}$．よって，定理 A.1.2 より $\overset{*}{\rightarrow}_{R\cup H} = \overset{*}{\leftrightarrow}_R$．ゆえに，$\leftrightarrow_E \subseteq \overset{*}{\rightarrow}_{R\cup H} \circ \overset{*}{\leftrightarrow}_R \circ \overset{*}{\leftarrow}_{R\cup H} \subseteq \overset{*}{\leftrightarrow}_R \circ \overset{*}{\leftrightarrow}_R \circ \overset{*}{\leftrightarrow}_R = \overset{*}{\leftrightarrow}_R$ である．□

A.2　定理 6.1 の証明

まずは，$Expd$ に関する性質を示す．

補題 A.2.1　R を $(\mathcal{F},\mathcal{G},\mathcal{P},\mathcal{M})$ 上の制約付き項書換え系とし，$s,\ t \in T(\mathcal{F}\cup\mathcal{G},\mathcal{V})$ とする．このとき，基底項上で $\leftrightarrow_{Expd(s,t,c,p)} \subseteq (\leftarrow_R \circ \leftrightarrow_{\{s\simeq t\Leftarrow c\}}) \cup (\leftrightarrow_{\{s\simeq t\Leftarrow c\}} \circ \rightarrow_R)$ である．

［証明］　$v_g \leftrightarrow_{Expd(s,t,c,p)} w_g$ とする．このとき，ある基底文脈 C_g，ある基底代入 σ_g が存在して $s \equiv C[u]_p$ かつ $l \rightarrow r \Leftarrow c \in R$ かつ $\theta = mgu(u,l)$ かつ $(c\theta \wedge d\theta)\sigma_g$ が真かつ $v_g \equiv C_g[C[r]_p\theta\sigma_g]$ かつ $w_g \equiv C_g[t\theta\sigma_g]$ とする．このとき，$v_g \equiv C_g[C[r]_p\theta\sigma_g] \equiv C_g[C\theta\sigma_g[r\theta\sigma_g]_p] \leftarrow_{\{l\rightarrow r\Leftarrow d\}} C_g[C\theta\sigma_g[l\theta\sigma_g]_p] \equiv C_g[C\theta[l\theta]_p\sigma_g] \equiv C_g[C\theta[u\theta]_p\sigma_g] \equiv C_g[C[u]_p\theta\sigma_g] \equiv C_g[s\theta\sigma_g] \leftrightarrow_{\{s\simeq t\Leftarrow c\}} C_g[t\theta\sigma_g] \equiv w_g$．同様に $v_g \equiv C_g[t\theta\sigma_g]$ かつ $w_g \equiv C_g[C[r]_p\theta\sigma_g]$ も考えれば，基底項上で $\leftrightarrow_{Expd(s,t,c,p)} \subseteq (\leftarrow_R \circ \leftrightarrow_{\{s\simeq t\Leftarrow c\}}) \cup (\leftrightarrow_{\{s\simeq t\Leftarrow c\}} \circ \rightarrow_R)$ である．□

次に，推論規則を 1 回だけ適用したときの性質を明らかにする．

補題 A.2.2　R を $(\mathcal{F},\mathcal{G},\mathcal{P},\mathcal{M})$ 上の制約付き項書換え系とする．このとき，$(E,H) \vdash_{RI} (E',H')$ ならば，基底項上で $\leftrightarrow_{H'\cup E'} \subseteq \overset{*}{\leftrightarrow}_{R\cup H\cup E}$．

［証明］　適用された推論規則に場合分けを行う．

- Simplification の場合，$\leftrightarrow_{E'} \subseteq (\leftarrow_{R\cup H} \circ \leftrightarrow_E) \cup (\leftrightarrow_E \circ \rightarrow_{R\cup H})$ かつ $H = H'$ より成り立つ．
- Deletion の場合，$E' \subseteq E$ かつ $H = H'$ より成り立つ．
- Expansion の場合，補題 A.2.1 から $\leftrightarrow_{E'\setminus E} \subseteq (\leftarrow_R \circ \leftrightarrow_{\{s\simeq t\Leftarrow c\}}) \cup (\leftrightarrow_{\{s\simeq t\Leftarrow c\}} \circ \rightarrow_R)$．また，$\leftrightarrow_{H'} \subseteq \leftrightarrow_{H\cup E}$ より成り立つ．
- $(E,H) \vdash^{eq}_{RI} (E',H')$ の場合，$\leftrightarrow_{\{C[s_1,\cdots,s_n]\approx C[t_1,\cdots,t_n]\Leftarrow c\wedge\neg(\bigwedge_{i=1}^{n} EQ(s_i,t_i))\}} \subseteq \leftrightarrow_{\{C[s_1,\cdots,s_n]\simeq C[t_1,\cdots,t_n]\Leftarrow c\}}$ は明らかに成り立つ．よって，$\leftrightarrow_{E'\setminus E} \subseteq \leftrightarrow_E$．また，$H = H'$ より成り立つ．□

補題 A.2.3　R を $(\mathcal{F},\mathcal{G},\mathcal{P},\mathcal{M})$ 上の制約付き項書換え系とする．このとき，$(E,H) \vdash^{*}_{RI} (E',H')$ ならば，基底項上で $\leftrightarrow_{H'\cup E'} \subseteq \overset{*}{\leftrightarrow}_{R\cup H\cup E}$．

［証明］　補題 A.2.2 より成り立つ．□

最後に定理 6.1 の証明を与える．

［証明］　E のすべての等式は R の帰納的定理とする．このとき，基底項上で $\leftrightarrow_E \subseteq \overset{*}{\leftrightarrow}_R$．補題 A.2.3 より $\leftrightarrow_{\{s\simeq t\Leftarrow c\wedge\neg EQ(s,t)\}} \subseteq \overset{*}{\leftrightarrow}_{R\cup E} \subseteq \overset{*}{\leftrightarrow}_R$ である．このとき，$c\sigma_g$ と $\neg EQ(s\sigma_g,t\sigma_g)$ を真とする σ_g が存在し，$s\sigma_g \overset{*}{\leftrightarrow}_R t\sigma_g$．$s\sigma_g, t\sigma_g \in T(\mathcal{G})$ かつ R は $\mathcal{M}$ に対して健全であるため $EQ(s\sigma_g,t\sigma_g)$ は真である．これは $\neg EQ(s\sigma_g,t\sigma_g)$ が真であることに矛盾する．よって，帰納的定理でない等式が E に存在する．□

A.3　定理 7.1 の証明

定理 7.1 の証明はほぼ定理 4.1 の証明と同様である．ただし，定理 4.1 の証明のままでは補題 A.1.5，A.1.6 で問題が生じるため，その部分の証明のみを行う．

まず，補題 A.1.5 を定理 7.1 の証明に用いることが可能な形にし，その証明を行う．

補題 A.3.1　R を $(\mathcal{F},\mathcal{G},\mathcal{P},\mathcal{M})$ 上の制約付き項書換え系とし，$s_1,\cdots,s_n,t_1,\cdots,t_n \in T(\mathcal{G},\mathcal{V})$，$C[\,] \in T_{\Box}(\mathcal{F}\cup\mathcal{G},\mathcal{V})$，$c$ を制約とする．このとき，R が停止性，$\mathcal{M}$ に対して完全性と局所健全性を持ち，$NF_R \subseteq T(\mathcal{G})$ ならば，基底項上で $\leftrightarrow_{\{C[s_1,\cdots,s_n]\simeq C[t_1,\cdots,t_n]\Leftarrow c\}} \subseteq (\overset{*}{\rightarrow}_R \circ \leftrightarrow_{\{C[s_1,\cdots,s_n]\approx C[t_1,\cdots,t_n]\Leftarrow c\wedge\neg(\bigwedge_{i=1}^{n} EQ(s_i,t_i))\}} \circ \overset{*}{\leftarrow}_R) \cup \overset{*}{\leftrightarrow}_R$ である．

［証明］　$(C[s_1,\cdots,s_n])\sigma_g \leftrightarrow_{\{C[s_1,\cdots,s_n]\simeq C[t_1,\cdots,t_n]\Leftarrow c\}} (C[t_1,\cdots,t_n])\sigma_g$ とする．このとき，$c\sigma_g$ は真である．ここで，R は停止性と局所健全性を持つため補題 A.1.3 から

$(C[s_1,\cdots,s_n])\sigma_g \xrightarrow{*}_R (C[s_1,\cdots,s_n])\sigma_{NF}$ かつ $(C[t_1,\cdots,t_n])\sigma_g \xrightarrow{*}_R (C[t_1,\cdots,t_n])\sigma_{NF}$ となる基底正規形代入 σ_{NF} が存在し，$c\sigma_{NF}$ は真である．$NF_R \subseteq T(\mathcal{G})$ から $s_i\sigma_{NF}, t_i\sigma_{NF} \in T(\mathcal{G})$ となるため $EQ(s_i\sigma_{NF}, t_i\sigma_{NF})$ の真偽が決まる．

- $\bigwedge_{i=1}^n EQ(s_i\sigma_{NF}, t_i\sigma_{NF})$ が真であるとき，R の完全性より $s_i\sigma_{NF} \xleftrightarrow{*}_R t_i\sigma_{NF}$ である．よって，$(C[s_1,\cdots,s_n])\sigma_g \xleftrightarrow{*}_R (C[t_1,\cdots,t_n])\sigma_g$ である．
- $\bigwedge_{i=1}^n EQ(s_i\sigma_{NF}, t_i\sigma_{NF})$ が偽であるとき，$c\sigma_{NF} \wedge \neg(\bigwedge_{i=1}^n EQ(s_i\sigma_{NF}, t_i\sigma_{NF}))$ が真であることより $(C[s_1,\cdots,s_n])\sigma_g \xrightarrow{*}_R \circ \leftrightarrow_{\{C[s_1,\cdots,s_n] \simeq C[t_1,\cdots,t_n] \Leftarrow c \wedge \neg(\bigwedge_{i=1}^n EQ(s_i,t_i))\}} \circ \xleftarrow{*}_R (C[t_1,\cdots,t_n])\sigma_g$ である． □

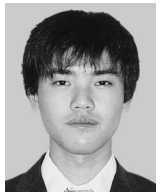
次に，補題 A.1.6 を定理 7.1 の証明に用いることが可能な形にし，その証明を行う．

補題 A.3.2　R を $(\mathcal{F},\mathcal{G},\mathcal{P},\mathcal{M})$ 上の制約付き項書換え系とし，R は停止性，$\mathcal{M}$ に対して完全性と局所健全性を持ち，$NF_R \subseteq T(\mathcal{G})$ とする．このとき，$(E,H) \vdash_{RI'} (E',H')$ ならば基底項上で $\leftrightarrow_E \subseteq \xrightarrow{*}_{R\cup H'} \circ (\leftrightarrow_{E'} \cup \xleftrightarrow{*}_R) \circ \xleftarrow{*}_{R\cup H'}$ である．

［証明］　適用した推論規則で場合分けを行う．

- Simplification のとき，$E\backslash E' = \{C[l\sigma] \simeq t \Leftarrow c\}$ かつ $l \to r \Leftarrow d \in R\cup H$ かつ $\neg c \vee d\sigma$ は $\mathcal{M}$ に関して恒真とする．$s_g \leftrightarrow_{\{C[l\sigma]\simeq t \Leftarrow c\}} t_g$ とすると，$s_g \equiv C'[C[l\sigma]\sigma_g]$ かつ $t_g \equiv C'[t\sigma_g]$ かつ $c\sigma_g$ が真である．ここで，R は停止性と局所健全性を持つため，補題 A.1.3 から $C'[C[l\sigma]\sigma_g] \xrightarrow{*}_R C'[C[l\sigma]\sigma_{NF}]$ かつ $C'[t\sigma_g] \xrightarrow{*}_R C'[t\sigma_{NF}]$ となる基底正規形代入 σ_{NF} が存在し，$c\sigma_{NF}$ は真である．$\neg c \vee d\sigma$ は $\mathcal{M}$ に関して恒真のため，$\neg c\sigma_{NF} \vee d\sigma\sigma_{NF}$ は真，すなわち，$d\sigma\sigma_{NF}$ が真である．よって，$C'[C[l\sigma]\sigma_{NF}] \to_R C'[C[r\sigma]\sigma_{NF}]$ が成り立つ．また，$C[r\sigma] \approx t \Leftarrow c \in E'$ かつ $c\sigma_{NF}$ は真から $C'[C[r\sigma]\sigma_{NF}] \leftrightarrow_E C'[t\sigma\sigma_{NF}]$ が成り立つ．ゆえに，$s_g \xrightarrow{*}_R \circ \to_R \circ \leftrightarrow_{E'} \circ \xleftarrow{*}_R t_g$ である．
- Deletion のとき，$E\backslash E' = \{s \simeq t \Leftarrow c\}$ とする．$s \equiv t$ または c は $\mathcal{M}$ に関して充足不能の場合は補題 A.1.6 と同様に証明できる．$s \equiv s'\sigma$ かつ $t \equiv t'\sigma$ かつ $s', t' \in T(\mathcal{G},\mathcal{V})$ かつ $EQ(s',t')$ は $\mathcal{M}$ に関して恒真の場合を考える．$s_g \leftrightarrow_{\{s\simeq t \Leftarrow c\}} t_g$ とすると，$s_g \equiv C[s'\sigma\sigma_g]$ かつ $t_g \equiv C[t'\sigma\sigma_g]$ かつ $c\sigma_g$ は真である．ここで，R は停止性と局所健全性を持つため，補題 A.1.3 から $C[s'\sigma\sigma_g] \xrightarrow{*}_R C[s'\sigma_{NF}]$ かつ $C[t'\sigma\sigma_g] \xrightarrow{*}_R C[t'\sigma_{NF}]$ となる基底正規形代入 σ_{NF} が存在し，$c\sigma_{NF}$ は真である．また，$EQ(s',t')$ は恒真であるため，$EQ(s'\sigma_{NF}, t'\sigma_{NF})$ は真である．よって，完全性から $s'\sigma_{NF} \xleftrightarrow{*}_R t'\sigma_{NF}$ が成り立つ．ゆえに，$s_g \xrightarrow{*}_R \circ \xleftrightarrow{*}_R \circ \xleftarrow{*}_R t_g$ である．
- Expansion のとき，補題 A.1.6 と同様に証明できる．
- EQ-Deletion のとき，補題 A.3.1 より $\leftrightarrow_{E\backslash E'} \subseteq (\xrightarrow{*}_R \circ \leftrightarrow_{E'} \circ \xleftarrow{*}_R) \cup \xleftrightarrow{*}_R$．よって，成り立つ． □

(平成 20 年 9 月 28 日受付)
(平成 20 年 12 月 26 日採録)



坂田　翼

2007 年名古屋大学工学部電気電子・情報工学科卒業．現在，同大学大学院情報科学研究科修士課程在学中．項書換え系，定理自動証明に関する研究に従事．

西田　直樹

2000 年名古屋大学工学部電気電子・情報工学科卒業．2002 年同大学大学院工学研究科計算理工学博士前期課程修了．2004 年同大学院工学研究科情報工学専攻博士後期課程修了．2004 年同大学院情報科学研究科助手，2007 年より同助教，現在に至る．項書換え系，プログラム変換に関する研究に従事．工学博士．電子情報通信学会，日本ソフトウェア科学会各会員．

坂部　俊樹（正会員）

1972 年名古屋大学工学部電気学科卒業．1977 年同大学大学院博士課程満了．名古屋大学助手，三重大学助教授，名古屋大学助教授を経て，1993 年より名古屋大学教授．ソフトウェアの基礎理論全般に興味を持つ．抽象データ型の理論，プログラミング言語の形式的意味論，自動プログラミング，書換え型計算モデル，並行プロセスの理論等の研究に従事．工学博士．電子情報通信学会，人工知能学会，日本ソフトウェア科学会，EATCS 各会員．

酒井　正彦

1989 年名古屋大学大学院博士課程満了．同年同大学工学部助手．1993 年北陸先端科学技術大学院大学助教授．1997 年名古屋大学工学研究科助教授．2002 年同教授．2003 年同大学院情報科学研究科教授，現在に至る．この間，1996 年 3 月〜8 月ニューヨーク州立大学スートーニーブルック校客員研究教授．項書換え系等のソフトウェア基礎理論に関する研究に従事．工学博士．平成 3 年度電子情報通信学会論文賞受賞．電子情報通信学会，日本ソフトウェア科学会各会員．

草刈圭一朗（正会員）

1994 年東京工業大学理学部生命理学科卒業．1996 年北陸先端科学技術大学院大学情報科学研究科博士前期課程修了．2000 年同大学博士後期課程にて博士（情報科学）取得．同年東北大学電気通信研究所助手．2003 年名古屋大学大学院情報科学研究科情報システム学専攻講師．2006 年より同大学院同研究科計算機数理科学専攻助教授，2007 年より同准教授．項書換え系・プログラム理論・定理自動証明の研究に従事．電子情報通信学会，日本ソフトウェア科学会各会員．