潜在帰納法と書換え帰納法の比較

小池 広高　外山 芳人

潜在帰納法と書換え帰納法は，数学的帰納法を直接適用せずに帰納的な定理を自動証明する手法として広く使われている．本論文では，統一された抽象的な枠組の中で潜在帰納法と書換え帰納法の関係を考察する．潜在帰納法では合流性と弱正規性が本質的であるのに対し，書換え帰納法では退行性と強正規性が本質的であることを明らかにし，両者の証明能力が異なることを示す．さらに，反駁証明と組み合わせると両者の証明能力が一致することも明らかにする．

1 はじめに

関数型言語や代数的仕様記述法などの等式論理を基礎とする系では，さまざまな性質を等式論理の帰納的定理として取り扱うことができる．それゆえ，等式論理における帰納的定理の自動証明手法 [3] [4] [6] [14]は，代数的仕様やプログラムの検証，また仕様とプログラムの等価性判定などを自動的に行なうために重要である．

等式論理における帰納的定理の自動証明手法は，明示帰納法 (explicit induction) と暗黙帰納法 (implicit induction) に大きくわけられる．明示帰納法とは帰納的図式を直接もちいて帰納的定理の証明を行なう手法である．Boyer と Moore によって研究された Nqthm [4]は，この手法による自動証明システムとして有名である．一方，暗黙帰納法とは，帰納的図式を直接もちいずに帰納的定理の証明を行なう手法で，Musser [14]により提案され Huet と Hullot [6]により拡張された潜在帰納法 (inductionless induction) や，Reddy [15]らによって提案された書換え帰納法 (rewriting induction) が知られている．また，潜在帰納法にもとづく自動証明システムとしては RRL [9]，書換え帰納法にもとづく自動証明システムとしては SPIKE [3]が実現されている．

本研究の目的は，暗黙帰納法による自動証明手法として重要な潜在帰納法と書換え帰納法を理論的に比較することである．ここでは，潜在帰納法と書換え帰納法を抽象的に形式化することで理論的に整理し，両者の本質的な差異が，合流性と退行性，および弱正規性と強正規性の差異にもとづくことを明らかにする．また，実際の自動証明システム [3] [6] [8]で広くもちいられている反駁証明法についても考察し，反駁証明法を組み合わせると潜在帰納法と書換え帰納法の証明能力が一致することを明らかにする．このような統一的な観点から両者を理論的に比較した研究はこれまではほとんどなされておらず，ここで示された結果は新しい自動証明手法を確立する上で極めて有用であると考えられる．

本論文の構成は次のとおりである．2節では必要となる定義を与える．3節では潜在帰納法，書換え帰納法，反駁証明法を抽象的な枠組で整理する．4節では潜在帰納法と書換え帰納法の証明能力の比較を行なう．5節では自動証明システムでの実現法について考察を行なう．

Inductionless Induction and Rewriting Induction.

Hirotaka Koike, 三洋電機株式会社 ハイパーメディア研究所, SANYO Electric Co., Hypermedia Research Center.

Yoshihito Toyama, 東北大学 電気通信研究所, Research Institute of Electrical Communication, Tohoku University.

コンピュータソフトウェア, Vol.17, No.6 (2000), pp.1–12.
[論文] 1999年3月25日受付.

2 準備

本節では，抽象リダクションシステムと項書換えシステムに関する用語や概念を文献 [1] [17]にもとづき定義する．

2.1 抽象リダクションシステム

抽象リダクションシステム $R = \langle A, \rightarrow \rangle$ は，対象集合 A と A 上の二項関係 $\rightarrow$ の対で定められる．$\rightarrow$ をリダクション関係と呼ぶ．R のリダクション系列とは $x_0 \rightarrow x_1 \rightarrow x_2 \rightarrow \cdots$ のことである．A 上の同一関係を $\equiv$ で表す．$\overset{*}{\rightarrow}$，$\overset{+}{\rightarrow}$ をそれぞれ $\rightarrow$ の反射・推移閉包，推移閉包，$=$ を $\rightarrow$ から生成される同値関係とする．$x \rightarrow y$ なる $y \in A$ が存在しないとき，$x \in A$ は正規形であるという．$x \overset{*}{\rightarrow} y$ となる正規形 $y \in A$ が存在するとき，$x \in A$ は正規形 y をもつという．NF で正規形の集合を表す．

定義 2.1 $R = \langle A, \rightarrow \rangle$ におけるすべてのリダクション系列が有限であるとき，R は強正規性 (*Strongly Normalization*) あるいは停止性をもつといい，$\rightarrow$: SN と記す．すべての $a \in A$ が正規形をもつとき，R は弱正規性 (*Weakly Normalization*) をもつといい $\rightarrow$: WN と記す．

定義 2.2 $R = \langle A, \rightarrow \rangle$ は次の条件を満たすとき，合流性あるいはチャーチ・ロッサ ($Church - Rosser$) 性をもつといい $\rightarrow$: CR と記す．

$\forall x, y, z[x \overset{*}{\rightarrow} y \wedge x \overset{*}{\rightarrow} z \Rightarrow \exists w.\ y \overset{*}{\rightarrow} w \wedge z \overset{*}{\rightarrow} w]$ (図1)

R が停止性と合流性をもつとき，R は完備 (complete) であるという．

定義 2.3 $R_2 = \langle A, \rightarrow_2 \rangle$ は次の条件を満たすとき，$R_1 = \langle A, \rightarrow_1 \rangle$ に退行 (*Retrogressive*) するといい $\rightarrow_2 RET \rightarrow_1$ と記す．

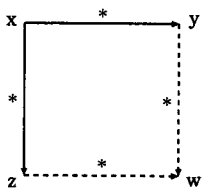

図 1 合流性

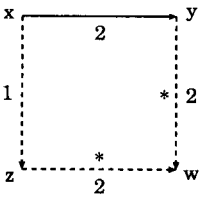

図 2 退行性

$\forall x, y[x \rightarrow_2 y \Rightarrow$
$\exists z, w.\ x \rightarrow_1 z \wedge z \overset{*}{\rightarrow}_2 w \wedge y \overset{*}{\rightarrow}_2 w]$ (図2)

命題 2.4 R が合流性をもつとき以下が成り立つ [1].

(1) $\forall x, y \in A[x = y \Rightarrow \exists w \in A.x \overset{*}{\rightarrow} w \wedge y \overset{*}{\rightarrow} w]$,

(2) $\forall x, y \in NF[x = y \Rightarrow x \equiv y]$.

命題 2.5 (ネータ帰納法) $\rightarrow$ が強正規性をもつとき以下が成り立つ [1].

$$\forall x \in A[\forall y \in A[x \overset{+}{\rightarrow} y \Rightarrow P(y)] \Rightarrow P(x)] \Rightarrow \forall x \in A.P(x)$$

2.2 項書換えシステム

関数記号 $f, g, h, \cdots$ の集合を F，変数記号 $x, y, z, \cdots$ の集合を V とする．ここで，$F \cap V = \emptyset$ とする．F と V から生成される項の集合を $T(F, V)$ と記す．以下では項を t, s, l, r, e, u 等で表す．変数を含まない項を基底項と呼びその集合を $T(F)$ と記す．以下では，少なくとも 1 個の定数記号 (項数 (arity) が 0 の関数記号) の存在を仮定し，基底項の集合 $T(F)$ は空集合ではないものとする．

代入 θ は変数から項への写像であり，$\theta(f(t_1, \cdots, t_n)) \equiv f(\theta(t_1, \cdots, t_n))$ のように項から項への写像に拡張される．以下では，θ の定義域が $\{x_1, \cdots, x_n\}$ のとき，θ を $\{x_1 \leftarrow \theta(x_1), \cdots, x_n \leftarrow \theta(x_n)\}$ で表す．項 t に代入 θ を適用した結果を $t\theta$ で表す．特に $t\theta \in T(F)$ となるとき θ は項 t に対する基底代入と呼ぶ．以下では，適用する項に対する基底代入を θ_g で表す．基底項の正規形全体からなる集合を NF^G で表す．文脈とは，特別な定数 □ をただ 1 つ含む項である．文脈 C の □ を項 t で置き換えて得られた項を $C[t]$ で表す．

定義 2.6 正整数の列の集合 N_+^* を用いて項に出現する関数記号の出現位置を以下のように定める．

1. 根記号 (最外の関数記号) の出現位置を ε(空列) と

する.

2. $C[f(t_1,\cdots,t_n)]$ における f の出現位置が u のとき各 t_i の根記号の出現位置を $u\cdot i$ とする.

項 t の部分項で出現位置 u を根とする部分項を $t|_u$ で記す.

規則 $l\to r$ は,左辺 l が変数でなく,右辺 r に現れる変数は必ず左辺 l にも出現するものとする.項書換えシステム R は規則の有限集合によって定義される.

定義 2.7 項書換えシステム R における2項関係 $\to_R$ を以下のように定義する.

$$t\to_R s \overset{\text{def}}{\Leftrightarrow} \exists\, l\to r\in R, \exists C[\,],\ \exists\theta. t\equiv C[l\theta] \wedge s\equiv C[r\theta]$$

また,項 t の部分項 $l\theta$ をリデックスと呼ぶ. $\to_R$ の反射・推移・対称閉包を $\to_R$ によって生成される合同関係と呼び $=_R$ と書く.以下では,特に明記しないかぎり F は R に出現する関数記号のみからなる集合と考える.

定義 2.8 $l_1\to r_1$ と $l_2\to r_2$ を R の書換え規則とする.ここで,一般性を失うことなく2つの規則は変数を共有しないものと仮定する.ある文脈 C で $l_1\equiv C[s]$ かつ $s\notin V$ で,最汎単一化子 θ が存在して, $s\theta\equiv l_2\theta$ であれば, 2つの書換え規則 $l_1\to r_1$ と $l_2\to r_2$ は重なるという.このとき, $\langle C[r_2]\theta, r_1\theta\rangle$ を危険対という.ただし,同じ書換え規則同士の重なりについて考えるときは, $C\neq\Box$ とする.

定義 2.9 等式 $e=e'$ が項書換えシステム R における帰納的定理であるとは, e と e' に対する任意の基底代入 θ_g について $e\theta_g =_R e'\theta_g$ となることである.

例 2.10 次の項書換えシステム R を考える.

$$R:\begin{cases} x+0\to x \\ x+s(y)\to s(x+y)\end{cases}$$

このとき, $0+x\ =_R\ x$ は成立しない.しかし, $\forall\theta_g\ [(0+x)\theta_g =_R x\theta_g]$ は成立するので $0+x=x$ は項書換えシステム R における帰納的定理となる. □

2.3 被覆代入集合

本節では,項書換えシステムにおける基底項の到達可能性の判定手法として被覆集合や被覆代入集合[2] [3] [5] [6] [7] [8] [10] [15] [16] [17]が広く使われている.ここでは被覆代入集合の概念を説明する.

定義 2.11 代入の有限集合 $\{\sigma_i\}_i$ が項書換えシステム R の被覆代入集合とは以下が成立することである.

$$\forall s\in T(F,V), \forall\theta_g, \exists\sigma_i, \exists\theta'_g\ [s\theta_g \overset{*}{\to}_R s\sigma_i\theta'_g]$$

例 2.12 例2.10の項書換えシステム R に対して, $\{\{x\leftarrow 0\},\{x\leftarrow s(z)\}\}$ と $\{\{x\leftarrow 0\},\{x\leftarrow s(0)\},\{x\leftarrow s(s(z))\}\}$ はそれぞれ R の被覆代入集合となる. □

補題 2.13 項書換えシステム R_1 の被覆代入集合 $\{\sigma_i\}_i$ と $R_2=R_1\cup\{e\to e'\}$ を考える.このとき以下が成立する.

$$\forall\sigma_i. e\sigma_i\notin NF_{R_1}\Rightarrow NF^G_{R_1}=NF^G_{R_2}$$

証明 $NF^G_{R_2}\subseteq NF^G_{R_1}$ は自明. $NF^G_{R_1}\subseteq NF^G_{R_2}$ を示すために, $\forall s,t\in T(F), \exists u\in T(F)[s\to_{R_2} t\Rightarrow s\overset{+}{\to}_{R_1} u]$ が成立することを示す. $s\to_{R_1} t$ の場合は自明. $s\equiv C[e\theta_g]\to_{R_2} C[e'\theta_g]\equiv t$ の場合を考える.このとき,定義2.11と $\forall\sigma_i. e\sigma_i\notin NF_{R_1}$ より, $s\overset{*}{\to}_{R_1} C[e\sigma_i\theta'_g]\to_{R_1} u$ が成立する. □

例 2.14 例2.10の項書換えシステム R と $R'=R\cup\{0+x\to x\}$ を考える.このとき,被覆代入集合 $S=\{\{x\leftarrow 0\},\{x\leftarrow s(z)\}\}$ に対して, $\forall\sigma\in S.(0+x)\sigma\notin NF_R$ は明らか.よって, $NF^G_R=NF^G_{R'}$ が示される. □

被覆代入集合が与えられていると,例2.14のように2つの項書換えシステム R_1 と $R_2=R_1\cup\{e\to e'\}$ において, $NF^G_{R_1}=NF^G_{R_2}$ の判定は容易に実行可能となる.

3 潜在帰納法と書換え帰納法

本節では2つの抽象リダクションシステムの適当な集合上での等価性を判定する手法を示す.さらに, 2つの項書換えシステムの基底項集合上での等価性判定法を示し,これを応用した帰納的定理の証明法を説明する.

抽象リダクションシステム $R_1=\langle A,\to_1\rangle$ と $R_2=\langle A,\to_2\rangle$ を考える.それぞれのシステムによって定められる同値関係を $=_i$,正規形の集合を $NF_i(i=1,2)$ で表す. $\to_1\subseteq\to_2$ は $\forall x,y\in A[x\to_1 y\Rightarrow x\to_2 y]$ を意味する. A の部分集合 A' 上で R_1 と R_2 が等しい同値関係をもつとは $\forall x,y\in A'[x=_1 y\Leftrightarrow x=_2 y]$ が成立することである.これを $=_1\ =\ =_2\ in\ A'$ と記す[17].特に $=_1\ =\ =_2\ in\ A$ の場合は $=_1\ =\ =_2$ と略記する.

3.1 潜在帰納法

潜在帰納法 [6] [7] [8] [14]は，異なる2つのシステムの等価性の判定手法として以下のように定式化することが可能である．

命題 3.1 [17] 次の条件が成立するものと仮定する．
(1) $\rightarrow_1 \subseteq \rightarrow_2$ (2) $\rightarrow_1$: WN (3) $\rightarrow_2$: CR
(4) $NF_1 = NF_2$
このとき，$=_1 = =_2$ が成立する．

証明 $=_1 \subseteq =_2$ は(1)より明らか．$=_2 \subseteq =_1$ を示す．$x =_2 y$ とすると，(2)より $\exists z \in NF_1[x \stackrel{*}{\rightarrow}_1 z]$ かつ $\exists w \in NF_1[y \stackrel{*}{\rightarrow}_1 w]$．(1)より $z =_2 w$ となる．(4)より $z, w \in NF_2$ となるので(3)と命題2.4(2)より $z \equiv w$ が成立．したがって $x =_1 y$．□

通常は適当なデータ構造上の帰納法が必要とされる帰納的定理の証明を，命題3.1をもちいると直接的な帰納法の適用なしで証明することが可能となる．以下では，潜在帰納法の原理を命題3.1にもとづいて説明する [17]．

潜在帰納法の原理

項書換えシステム R_1 のもとで等式 $e = e'$ の証明を行なう．$R_2 = R_1 \cup \{e \rightarrow e'\}$ とおく．このとき R_1 と R_2 が基底項上で命題3.1の条件(1)(2)(3)(4)を満たすことを示す．これが成功すると命題3.1より $=_{R_1} = =_{R_2}$ in $T(F)$ が成立する．ここで R_2 は書換え規則として $e \rightarrow e'$ を含んでいる．よって明らかに，$\forall\theta_g.\ e\theta_g =_{R_2} e'\theta_g$ である．したがって，$\forall\theta_g.\ e\theta_g =_{R_1} e'\theta_g$ が得られ，$e = e'$ が R_1 における帰納的定理であることが証明される．

例 3.2 次の項書換えシステム R_1 を考える．

$$R_1 : \begin{cases} x + 0 \rightarrow x \\ x + s(y) \rightarrow s(x + y) \end{cases}$$

$0 + z = z$ が R_1 における帰納的定理であることを示す．$R_2 = R_1 \cup \{0 + z \rightarrow z\}$ とおく．このとき，$N = \{0, s(0), s(s(0)), \cdots\}$ とすると明らかに $\forall s \in T(F), \exists n \in N[s \stackrel{*}{\rightarrow}_{R_1} n]$ が成立する．よって R_1 は弱正規性を満たす．停止性と危険対を調べることにより，R_2 が合流性をもつことは容易に示すことができる [1]．また，被覆代入集合を利用すると，$NF^G_{R_1} = NF^G_{R_2}$ が成立することが示せる(例2.14)．R_1 と R_2 は基底項上で，命題3.1の条件(1)(2)(3)(4)を満たすので $=_{R_1} = =_{R_2}$ in $T(F)$．よって $0 + z = z$ は R_1 の帰納的定理である．□

例3.2の場合は R_2 が命題3.1の条件を満たすので，潜在帰納法の原理を直接適用することができた．しかし，$R_2 = R_1 \cup \{e \rightarrow e'\}$ が命題3.1の条件を満たさない場合には，R_2 のかわりに基底項上で $=_{R2} = =_{R3}$ かつ命題3.1の条件(3) $\rightarrow_3$: CR および(4)$NF_1 = NF_3$ を満たす R_3 を見つけても良い [17]．このとき，$\forall\theta_g.\ e\theta_g =_{R2} e'\theta_g \Leftrightarrow \forall\theta_g.\ e\theta_g =_{R3} e'\theta_g \Leftrightarrow \forall\theta_g.\ e\theta_g =_{R1} e'\theta_g$ が成立することから $e = e'$ は R_1 の帰納的定理となる．このような R_3 を発見する手法の1つとしてKnuth-Bendixの完備化手続き [13]が利用されている [6] [7] [8] [14]．

例 3.3 次の項書換えシステム R_1 を考える．

$$R_1 : \begin{cases} append(Nill, x) \rightarrow x \\ append(cons(x, y), z) \\ \qquad \rightarrow cons(x, append(y, z)) \\ rev(Nill) \rightarrow Nill \\ rev(cons(x, y)) \\ \qquad \rightarrow append(rev(y), cons(x, Nill)) \end{cases}$$

$rev(rev(x)) = x$ が R_1 における帰納的定理であること示す．$R_2 = R_1 \cup \{rev(rev(x)) \rightarrow x\}$ をKnuth-Bendixの完備化手続きによって完備化すると以下の R_3 が得られる [6]．

$$R_3 : \begin{cases} append(Nill, x) \rightarrow x \\ append(cons(x, y), z) \\ \qquad \rightarrow cons(x, append(y, z)) \\ rev(Nill) \rightarrow Nill \\ rev(cons(x, y)) \\ \qquad \rightarrow append(rev(y), cons(x, Nill)) \\ rev(rev(x)) \rightarrow x \\ rev(append(x, cons(y, Nill))) \\ \qquad \rightarrow cons(y, rev(x)) \end{cases}$$

R_3 は基底項上で $=_{R_2} == _{R_3}$ かつ命題3.1の(3) $\rightarrow_3$: CR および $(4)NF_1 = NF_3$ を満たす．よって $rev(rev(x)) = x$ は R_1 の帰納的定理である．□

3.2 書換え帰納法

書換え帰納法はReddyにより提案された帰納的定理の証明法である [15]．潜在帰納法と書換え帰納法の証明能力を比較するため，3.1節と同様に抽象リダクション

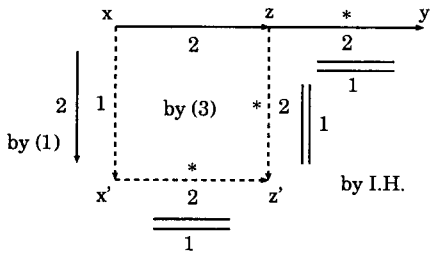

図3 補題 3.4 の証明

システムの枠組で書換え帰納法を考察する.

補題 3.4 次の条件が成立するものと仮定する.

(1) $\to_1 \subseteq \to_2$ (2) $\to_2$: SN (3) $\to_2 RET \to_1$

このとき, $=_1 = =_2$ が成立する.

証明 $=_1 \subseteq =_2$ は (1) より明らか. (2) より $\to_2$ は強正規である. $=_2 \subseteq =_1$ を示すために, $\to_2$ 上のネータ帰納法で $x \xrightarrow{*}_2 y \Rightarrow x =_1 y$ を示す. $x \in NF_2$ のときは $x \equiv y$ となり成立. $x \to_2 z \xrightarrow{*}_2 y$ について, (3) より $\exists x', z'[x \to_1 x' \wedge x' \xrightarrow{*}_2 z' \wedge z \xrightarrow{*}_2 z']$. (1) より $x \to_2 x'$. 帰納法の仮定より $x' =_1 z'$, $z =_1 z'$, $z =_1 y$ (図3). よって $x =_1 y$. □

この補題で明らかなように, 書換え帰納法で重要となるのは退行性と強正規性である. 以下では書換え帰納法の原理を補題 3.4にもとづいて説明する.

書換え帰納法の原理

項書換えシステム R_1 のもとで等式 $e = e'$ の証明を行なう. $R_2 = R_1 \cup \{e \to e'\}$ とおく. このとき R_1 と R_2 が基底項上で補題 3.4の条件 (1)(2)(3) を満たすことを示す. これが成功すると補題 3.4より $=_{R_1} = =_{R_2}$ *in* $T(F)$ が成立する. ここで R_2 は書換え規則として $e \to e'$ を含んでいる. よって明らかに, $\forall \theta_g.\ e\theta_g =_{R_2} e'\theta_g$ である. したがって, $\forall \theta_g.\ e\theta_g =_{R_1} e'\theta_g$ が得られ, $e = e'$ が R_1 における帰納的定理であることが証明される.

このように書換え帰納法では基底項上での退行性を示す必要がある. しかし, これを直接示すのは困難であるので, 項書換えシステム R_1 の被覆代入集合 $\{\sigma_i\}_i$ をもちいた次の条件 (3′) が利用されている [15].

(3′) $\forall \sigma_i, \exists u, \exists v.\ e\sigma_i \to_{R_1} u \xrightarrow{*}_{R_2} v \xleftarrow{*}_{R_2} e'\sigma_i$

被覆代入集合は有限集合なので, $\to_{R_2}$: SN の場合には条件 (3′) が成立するか否かを判定することが可能である.

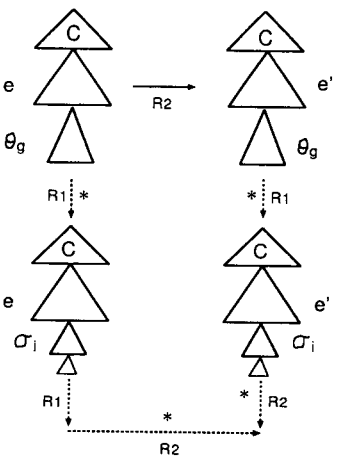

図4 補題 3.5 の証明

補題 3.5 $\{\sigma_i\}_i$ を項書換えシステム R_1 の被覆代入集合とし, $R_2 = R_1 \cup \{e \to e'\}$ とする. このとき (3′) が成立するならば, 基底項上で (3) $\to_{R_2} RET \to_{R_1}$ が成立する.

証明 次の条件 (3″) を考える.

(3″) $\forall x, y[x \to_{R_2} y \Rightarrow \exists x', y', z, w.\ x \xrightarrow{*}_{R_1} x' \to_{R_1} z \wedge y \xrightarrow{*}_{R_1} y' \xrightarrow{*}_{R_2} w \wedge z \xrightarrow{*}_{R_2} w]$

(3″) $\Leftrightarrow$ (3) は明らか. 以下では (3″) が基底項上で成立することを示す. $\forall s, t \in T(F)[s \to_{R_2} t]$ とする. このとき $\exists s', t', u, v \in T(F)[s \xrightarrow{*}_{R_1} s' \to_{R_1} u \wedge t \xrightarrow{*}_{R_1} t' \xrightarrow{*}_{R_2} v \wedge u \xrightarrow{*}_{R_2} v]$ が成立することを示す. $s \to_{R_1} t$ の場合は自明. $s \equiv C[e\theta_g] \to_{R_2} C[e'\theta_g] \equiv t$ の場合を考える. 定義 2.11と (3′) より

$$s \equiv C[e\theta_g] \xrightarrow{*}_{R_1} C[e\sigma_i\theta'_g] \equiv s' \to_{R_1} u \xrightarrow{*}_{R_2} v \xleftarrow{*}_{R_2} t' \equiv C[e'\sigma_i\theta'_g] \xleftarrow{*}_{R_1} C[e'\theta_g] \equiv t$$

が成立する (図4). □

例 3.6 次の項書換えシステム R_1 を考える.

$$R_1 : \begin{cases} x + 0 \to x \\ x + s(y) \to s(x + y) \end{cases}$$

$0 + z = z$ が R_1 の帰納的定理であることを示す. $R_2 = R_1 \cup \{0 + z \to z\}$ とおく. 補題 3.4 の条件 (1), (2) が成立することは明らか. 次に (3′) が成立することを被覆代入集合をもちいて示す. 被覆代入集合 $S = \{\{z \leftarrow 0\}, \{z \leftarrow s(w)\}\}$ に対し, $\forall \sigma \in S[0 + z\sigma \to_{R_1} \cdot \xrightarrow{*}_{R_2} \cdot \xleftarrow{*}_{R_2} z\sigma]$ は以下のように成立する.

$0+0 \to_{R_1} 0$, $0+s(w) \to_{R_1} s(0+w) \to_{R_2} s(w)$. R_1 と R_2 は基底項上で，補題 3.4 の条件 (1)(2)(3) を満たすので，$=_{R_1} \;=\; =_{R_2}$ *in* $T(F)$. よって $0+z=z$ は R_1 の帰納的定理である．□

例 3.7 次の項書換えシステム R_1 を考える．

$$R_1: \begin{cases} x+0 \to x \\ x+s(y) \to s(x+y) \\ s(x)+y \to s(x+y) \\ double(0) \to 0 \\ double(s(x)) \to s(s(double(x))) \end{cases}$$

$double(z)=z+z$ が R の帰納的定理であることを示す．$R_2=R_1 \cup \{double(z) \to z+z\}$ とおく．補題 3.4 の条件 (1)(2) が成立することは明らか．次に (3′) が成立することを被覆代入集合をもちいて示す．被覆代入集合 $S=\{\{z \leftarrow 0\},\{z \leftarrow s(w)\}\}$ に対し，$\forall\sigma \in S[(double(z))\sigma \to_{R_1} \cdot \overset{*}{\to}_{R_2} \cdot \overset{*}{\leftarrow}_{R_2} (z+z)\sigma]$ は以下のように成立する．

$double(0) \to_{R_1} 0 \leftarrow_{R_1} 0+0$,

$double(s(w)) \to_{R_1} s(s(double(w))) \to_{R_2}$

$s(s(w+s(w))) \leftarrow_{R_1} s(w+s(w)) \leftarrow_{R_1} s(w)+s(w)$.

よって $double(z)=z+z$ は R_1 の帰納的定理である．□

上記の例の場合は R_2 が補題 3.4の条件を満たすので，書換え帰納法の原理を直接適用することができた．しかし，一般には R_2 が補題 3.4の条件を満たすとは限らない．このような場合は R_2 のかわりに基底項上で $=_{R2} \;=\; =_{R3}$ を満たし，かつ補題 3.4の条件 (1) $\to_1 \;\subseteq\; \to_3$, (2) $\to_3$: SN, (3) $\to_3$ RET $\to_1$ を満たす R_3 を見つけても良い†1．このとき，$\forall\theta_g.\ e\theta_g =_{R2} e'\theta_g \Leftrightarrow \forall\theta_g.\ e\theta_g =_{R3} e'\theta_g \Leftrightarrow \forall\theta_g.\ e\theta_g =_{R1} e'\theta_g$ が成立することから $e=e'$ が R_1 の帰納的定理であることが示される．

被覆代入集合をもちいてこのような R_3 を発見する手法について説明する．$\{\sigma_i\}_i$ を R_1 の被覆代入集合とし，$R_2=R_1 \cup \{e \to e'\}$ は強正規性をもつとする．あるσ_j と s,t $(s \neq t) \in NF_{R_2}$ が存在して $e\sigma_j \to_{R_1} \cdot \overset{*}{\to}_{R_2} s$ かつ $e'\sigma_j \overset{*}{\to}_{R_2} t$ かつ $\forall\sigma_{i(\neq j)}$ $[e\sigma_i \to_{R_1} \cdot \overset{*}{\to}_{R_2} \cdot \overset{*}{\leftarrow}_{R_2} e'\sigma_i]$ であったとする．ここで s と t に向きづけを行ない，$R_3=R_2 \cup \{s \to t$ (あるいは $t \to s)\}$ が強正規性を満たすようにする．このとき $\forall\sigma_i$ $[s\sigma_i \to_{R_1} \cdot \overset{*}{\to}_{R_3} \cdot \overset{*}{\leftarrow}_{R_3} t\sigma_i]$ が成立するなら，基底項上で $=_{R_2} \;=\; =_{R_3}$ かつ (1)$\to_{R_1} \subseteq \to_{R_3}$ (2)$\to_{R_3}$: SN (3) $\to_{R_3}$ RET $\to_{R_1}$ は明らかに成立する (図 5)．よって，$e=e'$ が R_1 の帰納的定理であることが示される．そうでない場合は，$e \to e'$ のかわりに $s \to t$ (あるいは $t \to s$) に対して同様にこの手続きを繰り返す．このようにして R_3 が求まれば，直接 R_2 が条件を満たさなくても帰納的定理であることが証明可能となる．

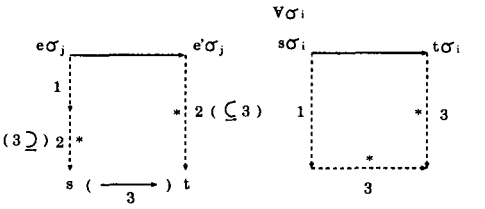

図 5 基底項上で $\to_{R_3}$ RET $\to_{R_1}$

実際に，このような被覆代入集合をもちいた証明手法は，Reddy による手続き [15]，Bouhoula による SPIKE [3]などで利用されている．

3.3 反駁証明法

反駁証明法とは，等式 $e=e'$ が項書換えシステム R の帰納的定理でないことを証明する手法である [2] [3] [5] [6] [7] [8] [12] [14]．ここでは，反駁証明法を抽象リダクションシステムの枠組で考察する．

補題 3.8 次の条件が成立するものと仮定する．

(1) $\to_1 \;\subseteq\; \to_2$ (2) $\to_2$: SN (3) $\to_1$: CR

(4)$NF_1 \neq NF_2$

このとき，$=_1 \;\neq\; =_2$ が成立する．

証明 (1) と (4) より $\exists x \in NF_1[x \to_2 y]$. (1) と (2) より $\exists z \in NF_1[y \overset{*}{\to}_1 z]$. (1) より $y \overset{*}{\to}_2 z$ となり $x =_2 z$. ここで $=_1 \;=\; =_2$ と仮定すると $x =_1 z$. (3) と命題 2.4(2) より $x \equiv z$ となる．$x \overset{+}{\to}_2 x$ より (2) に矛盾．□

補題 3.8をもちいると，項書換えシステム R_1 のもとで等式 $e=e'$ が帰納的定理でないことを証明することが可能となる．以下では，反駁証明法の原理を補題 3.8にもとづいて説明する．

†1 潜在帰納法の場合と異なり，書換え帰納法はネータ帰納法にもとづいているため条件 (1) を省くことはできない．

反駁証明法の原理

項書換えシステム R_1 のもとで等式 $e = e'$ が帰納的定理でないことを証明する．$R_2 = R_1 \cup \{e \to e'\}$ とおく．このとき R_1 と R_2 が基底項上で補題3.8の条件(1)(2)(3)(4)を満たすことを示す．これが成功すると補題3.8より $=_{R_1} \neq =_{R_2}$ *in* $T(F)$ が成立する．ここで $\forall\theta_g.\ e\theta_g =_{R_1} e'\theta_g$ が成立するなら，$=_{R_1} = =_{R_2}$ *in* $T(F)$ が成立することは明らか．したがって，$\exists\theta_g.\ e\theta_g \neq_{R_1} e'\theta_g$ が得られ，$e = e'$ が R_1 の帰納的定理でないことが証明される．

以下に，補題3.8にもとづいた反駁証明法の例を示す．

例 3.9 次の項書換えシステム R_1 を考える．

$$R_1 : \begin{cases} x + 0 \to x \\ x + s(y) \to s(x + y) \end{cases}$$

$s(z) = 0$ が R_1 の帰納的定理でないことを示す．$R_2 = R_1 \cup \{s(z) \to 0\}$ とおく．補題3.8の条件(1)(2)(3)が成立することは明らか．また，$NF^G_{R_1} = \{0, s(0), s(s(0)), \cdots\} \neq \{0\} = NF^G_{R_2}$ より(4)も成立する．したがって，$=_{R_1} \neq =_{R_2}$ *in* $T(F)$．よって $s(z) = 0$ は R_1 の帰納的定理でないことが示された．□

上記の例は R_2 が補題3.8の条件を満たすので，反駁証明法の原理が直接適用することができた．しかし，$R_2 = R_1 \cup \{e \to e'\}$ が補題3.8の条件を満たしていないなら，R_2 のかわりに基底項上で $=_{R_2} = =_{R_3}$ を満たし，かつ補題3.8の条件(1) $\to_1 \subseteq \to_3$, (2) $\to_3$: SN, (4) $NF_1 \neq NF_3$ を満たす R_3 を見つけても良い．このとき，$=_{R_2} = =_{R_3} \neq =_{R_1}$ *in* $T(F)$ が成立することから $e = e'$ が R_1 の帰納的定理でないことが示される．このような R_3 は3.1節，3.2節で説明した方法と同様な方法で求めることができる[2] [3] [5] [6] [7] [8] [12].

例 3.10 次の項書換えシステム R_1 を考える．

$$R_1 : \begin{cases} x + 0 \to x \\ x + s(y) \to s(x + y) \end{cases}$$

$0 + x = 0$ が R_1 の帰納的定理でないことを示す．$R_2 = R_1 \cup \{0 + x \to 0\}$ とする．このとき $NF^G_{R_1} = NF^G_{R_2} = \{0, s(0), s(s(0)), \cdots\}$ であるため補題3.8を直接適用できない．ここで3.2節で説明した方法で R_2 を変形して次の項書換えシステム R_3 を得る．

$$R_3 : \begin{cases} x + 0 \to x \\ x + s(y) \to s(x + y) \\ 0 + x \to 0 \\ s(0) \to 0 \end{cases}$$

このとき $NF^G_{R_1} \neq NF^G_{R_3}$ は明らか．R_3 は基底項上で $=_{R_2} = =_{R_3}$ かつ補題3.8を満たす．よって $0 + x = 0$ は R_1 の帰納的定理でないことが示された．□

補題3.8にもとづく反駁証明法では，項書換えシステム R_1 が基底項上で完備(基底完備[2] [3] [5])でなければならない．しかし，R_1 が基底完備でない場合でも，$=_{R_1} = =_{R'_1}$ *in* $T(F)$ を満たし基底完備な項書換えシステム R'_1 を R_1 のかわりにもちいることによって反駁証明法が可能となる．

4 証明能力の比較

前節では，潜在帰納法と書換え帰納法を抽象リダクションシステムの枠組で定式化した．本節では，潜在帰納法と書換え帰納法の証明能力を比較するとともに，反駁証明法との組み合わせについても考察する．

4.1 帰納的定理の証明能力

潜在帰納法と書換え帰納法に必要な条件は図6で表される．以下では両者で必要とされる条件の間にどのような関係が成立するかを考察する．まず次の補題を示す．

補題 4.1 抽象リダクションシステム $R_1 = \langle A, \to_1 \rangle$ と $R_2 = \langle A, \to_2 \rangle$ を考える．$\to_1 \subseteq \to_2$ を仮定すると以下が成り立つ．

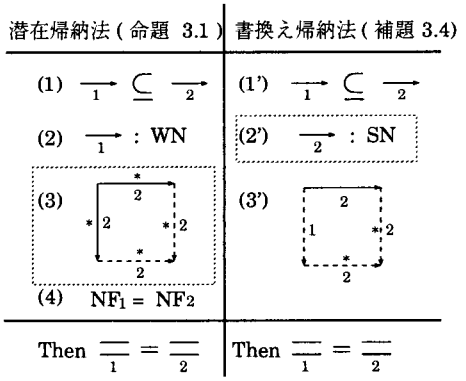

図6 命題3.1と補題3.4の比較

(a) $\rightarrow_2$: $CR \wedge NF_1 = NF_2 \Rightarrow \ \rightarrow_2 RET \rightarrow_1$.

(b) $\rightarrow_2 RET \rightarrow_1 \ \Rightarrow \ NF_1 = NF_2$.

証明

(a) $NF_1 = NF_2$ より $\forall x, y, \exists z[x \rightarrow_2 y \Rightarrow x \rightarrow_1 z]$. $x \rightarrow_2 z$ と $\rightarrow_2$:CR より $\rightarrow_2 RET \rightarrow_1$.

(b) $NF_2 \subseteq NF_1$ は自明. $NF_1 \subseteq NF_2$ を示す. $x \notin NF_2$ とする. すると $\exists y[x \rightarrow_2 y]$. このとき $\rightarrow_2 RET \rightarrow_1$ より $\exists z[x \rightarrow_1 z]$. よって $x \notin NF_1$. □

補題 4.1 から図6における条件に対して，以下の関係が容易に導ける.

$$(1),(3),(4) \Rightarrow (3')$$
$$(2) \Leftarrow (1'),(2')$$
$$(4) \Leftarrow (1'),(3')$$

一方，$(1),(2),(3),(4) \Rightarrow (2')$ は一般には成立しない. 以下がその反例となる.

$$R_1 : \begin{cases} a \rightarrow b \end{cases} \qquad R_2 : \begin{cases} a \rightarrow b \\ a \rightarrow a \end{cases}$$

また，$(3) \Leftarrow (1'),(2'),(3')$ も一般には成立しない. 以下がその反例となる.

$$R_1 : \begin{cases} a \rightarrow b \\ a \rightarrow c \end{cases} \qquad R_2 : \begin{cases} a \rightarrow b \\ a \rightarrow c \end{cases}$$

したがって，潜在帰納法の条件 (1)(2)(3)(4) は書換え帰納法の条件 $(1')(2')(3')$ を一般には保証しない. その逆も同様である. 特に，上記の反例から明らかなように潜在帰納法の合流性 (3) と書換え帰納法の強正規性 $(2')$ は互いに独立した条件となっている. したがって両者の適用範囲は異なり，それぞれの証明能力は一致しない.

4.2 反駁証明法との組み合わせ

自動証明システムの多くは潜在帰納法と書換え帰納法にそれぞれ反駁証明法を組み合わせて実現されている [3] [6] [8] [14]. ここでは，自動証明システムでもちいられる反駁証明法との組み合せを定式化する. 以下の補題 4.2は命題 3.1と補題 3.8，補題 4.3は補題 3.4と補題 3.8から容易に示すことができる.

補題 4.2 [8]（潜在帰納法＋反駁証明法） 抽象リダクションシステム $R_1 = \langle A, \rightarrow_1 \rangle$ と $R_2 = \langle A, \rightarrow_2 \rangle$ を考える. 次の条件が成立するものと仮定する.

(1) $\rightarrow_1 \ \subseteq \ \rightarrow_2$ (2) $\rightarrow_2$: SN (3) $\rightarrow_1$: CR

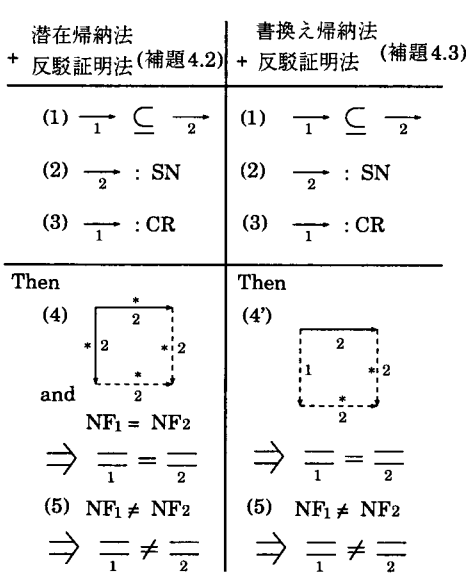

図 7 補題 4.2 と補題 4.3 の比較

このとき以下が成立する.

(4) $\rightarrow_2$: $CR \wedge NF_1 = NF_2 \Rightarrow \ =_1 \ = \ =_2$

(5) $NF_1 \neq NF_2 \Rightarrow \ =_1 \ \neq \ =_2$

補題 4.3（書換え帰納法＋反駁証明法） 抽象リダクションシステム $R_1 = \langle A, \rightarrow_1 \rangle$ と $R_2 = \langle A, \rightarrow_2 \rangle$ を考える. 次の条件が成立するものと仮定する.

(1) $\rightarrow_1 \ \subseteq \ \rightarrow_2$ (2) $\rightarrow_2 : SN$ (3) $\rightarrow_1 : CR$

このとき以下が成立する.

$(4')$ $\rightarrow_2 RET \rightarrow_1 \ \Rightarrow \ =_1 \ = \ =_2$

(5) $NF_1 \neq NF_2 \Rightarrow \ =_1 \ \neq \ =_2$

反駁証明法を組み合わせた潜在帰納法 (補題 4.2) と書換え帰納法 (補題 4.3) の関係を図 7に示す.

補題 4.2と 4.3で示したように，反駁証明法を組み合わせてもちいるときは，それぞれの条件 (1)(2)(3) は一致している. さらに，反駁証明のための条件 (5) は同じである. したがって，(1)(2)(3) を仮定して条件 (4) と $(4')$ が等価であることを示せば，反駁証明法と組み合わせた潜在帰納法と書換え帰納法の証明能力が一致することが示される. このために以下の補題を証明する.

補題 4.4 抽象リダクションシステム $R_1 = \langle A, \rightarrow_1 \rangle$ と $R_2 = \langle A, \rightarrow_2 \rangle$ を考える. (1) $\rightarrow_1 \ \subseteq \ \rightarrow_2$,(2) $\rightarrow_2$: SN, (3) $\rightarrow_1$: CR を仮定すると以下が成立する.

$$\rightarrow_2 RET \rightarrow_1 \ \Rightarrow \ \rightarrow_2 : CR$$

証明

$\to_2$ は強正規であるので，$\to_2$ 上のネータ帰納法で $\forall x,y,z[x \overset{*}{\to}_2 y \wedge x \overset{*}{\to}_2 z \Rightarrow \exists w.\ y \overset{*}{\to}_2 w \wedge z \overset{*}{\to}_2 w]$ を示す．$x \equiv y$ あるいは $x \equiv z$ のときは明らかに成り立つ．$x \to_2 y' \overset{*}{\to}_2 y$，$x \to_2 z' \overset{*}{\to}_2 z$ とする．$\to_2 RET \to_1$ より $\exists a,b[x \to_1 a \overset{*}{\to}_2 b \wedge y' \overset{*}{\to}_2 b]$，$\exists a',b'[x \to_1 a' \overset{*}{\to}_2 b' \wedge z' \overset{*}{\to}_2 b']$ が成立．$\to_1$:CR より $\exists c[a \overset{*}{\to}_1 c \wedge a' \overset{*}{\to}_1 c]$．また，$\to_1 \subseteq \to_2$ より，$x \to_2 a \overset{*}{\to}_2 c$，$x \to_2 a' \overset{*}{\to}_2 c$．帰納法の仮定を y', a, a', z' に繰り返し適用することにより $\exists w[y \overset{*}{\to}_2 w \wedge z \overset{*}{\to}_2 w]$．よって $\to_2$:CR．□

定理 4.5 抽象リダクションシステム $R_1 = \langle A, \to_1 \rangle$ と $R_2 = \langle A, \to_2 \rangle$ を考える．反駁証明法と組み合わせた潜在帰納法 (補題4.2) と書換え帰納法 (補題4.3) の証明能力は一致する．

証明 補題 4.1$(a)(b)$ と補題 4.4より条件 (4) と条件 (4′) の等価性は明らか．□

5 自動証明システムでの実現法

前節では，反駁証明法と組み合わせた潜在帰納法と書換え帰納法の証明能力が理論的には一致することを示した．しかし，実際の自動証明システムでは，潜在帰納法の原理や書換え帰納法の原理を直接適用可能な場合は少なく，与えられた項書換えシステムをそれぞれの原理が適用可能なように変形することが必要となる．このため，どのように項書換えシステムの変形を行なうかで，実際の証明システムの振舞いが異なってくる．本節では，潜在帰納法と書換え帰納法がどのような手続きで実現されているかを説明し，両者の証明動作の違いを例をもちいて明らかにする．

5.1 完備化を利用した証明手続き

完備でない項書換えシステムを，合同関係を保存したまま完備な項書換えシステムへ変換する手続きとして Knuth-Bendix の完備化手続きがある [11]．この完備化手続きを利用した帰納的定理の自動証明手続きとして Kapur らによる手続き [8]と Fribourg による手続き [5]がある．本節では，これらの手続きでどのように帰納的定理の証明が行なわれるかを補題 4.2(潜在帰納法＋反駁証明法) と補題 4.3(書換え帰納法＋反駁証明法) にもとづいて説明する．

公理となる等式システムのもとで等式 $e = e'$ が帰納的定理であるか否かを補題 4.2と補題 4.3の枠組で証明するためには，まず公理となる等式システムを合同関係を保存したまま完備な項書換えシステム R_1 へと変形する．そして，次に証明すべき等式 $e = e'$ に向き付けを行ない $R_2 = R_1 \cup \{e \to e'\}$ とする．ここで R_2 が補題 4.2あるいは補題 4.3の条件を満たすことが示されると証明 (もしくは反駁証明) は成功する．しかしながら，R_2 が条件を直接満たすとは限らない．よって，3節と 4節で述べたように，R_2 の合同関係を保存し，補題 4.2あるいは補題 4.3の条件を満たす R_3 を構成する必要がある．基底項上で R_3 が満たすべき条件を整理すると以下のようになる．

潜在帰納法＋反駁証明法

基底項上で次の条件が成立しているものとする．

(0) $=_{R_2} \ = \ =_{R_3}$ (1) $\to_{R_1} \subseteq \to_{R_3}$ (2) $\to_{R_3}$: SN

(3) $\to_{R_1}$: CR

このとき基底項上で以下が成立する．

(4) $\to_3$: $CR \wedge NF_{R_1} = NF_{R_3} \Rightarrow \ =_{R_1} \ = \ =_{R_2}$

(5) $NF_{R_1} \neq NF_{R_3} \Rightarrow \ =_{R_1} \neq \ =_{R_2}$

書換え帰納法＋反駁証明法

基底項上で次の条件が成立しているものとする．

(0) $=_{R_2} \ = \ =_{R_3}$ (1) $\to_{R_1} \subseteq \to_{R_3}$ (2) $\to_{R_3}$: SN

(3) $\to_{R_1}$: CR

このとき基底項上で以下が成立する．

(4) $\to_{R_3} RET \to_{R_1} \Rightarrow \ =_{R_1} \ = \ =_{R_2}$

(5) $NF_{R_1} \neq NF_{R_3} \Rightarrow \ =_{R_1} \neq \ =_{R_2}$

Kapur らの手続き [8]は，潜在帰納法＋反駁証明法にもとづいた R_3 の構成法とみなすことができ，一方 Fribourg の手続き [5]は書換え帰納法＋反駁証明法にもとづく R_3 の構成法とみなすことができる．以下では，それぞれの手続きが具体的にどのように R_3 を構成しているかについて説明する．なお，実際の手続きでは効率を改善するための様々な工夫が行なわれている．しかし，ここでは両者の差異を明確にするため，手続きの本質的な部分のみを説明する．

Kapur らの手続き (潜在帰納法＋反駁証明法).

入力: R_1: 完備な項書換えシステム； $e = e'$: 証明すべき等式; $>$: 停止性を保証する項上の順序

(1) $R_2 = R_1$; $E = \{e = e'\}$ とする.

(2) E が空なら終了. このとき $e = e'$ は R_1 の帰納的定理であることが示される. E が空でないなら (2-1) から (2-4) を繰り返す.

(2-1) E から $s > t$ を満たす等式 $s = t$ (あるいは $t = s$) を 1 つ取り出し, $s \to t$ を R_2 に付け加える. もしそのような等式がないなら終了. このとき証明は失敗.

(2-2) $NF^G_{R_1} \neq NF^G_{R_2}$ なら終了. このとき $e = e'$ は R_1 の帰納的定理でないことが示される.

(2-3) $s \to t$ と R_2 によって生じたすべての危険対を E に加える.

(2-4) R_2 をもちいて E の等式の両辺をすべて正規形にする. 両辺が一致した等式は E から取り除く.

次に, Fribourg の手続きを紹介する. この手続きでは, R 完全な出現という概念が重要となる.

定義 5.1 [5] 項 t における出現位置 p が R 完全な出現 (*complete position*) とは以下が成立することである. t に出現する任意の x に対して $x\theta_g \in NF^G_R$ となる任意の基底代入 θ_g を考えると, $t\theta_g|_p$ はリデックスとなる.

例 5.2 次の項書換えシステム R を考える.

$$R: \begin{cases} x + 0 \to x \\ x + s(y) \to s(x + y) \end{cases}$$

このとき項 $x + (y + z)$ について出現位置 $p = 2$ は R 完全な出現となる. □

Fribourg の手続き (書換え帰納法+反駁証明法).

入力: R_1: 完備な項書換えシステム; $e = e'$: 証明すべき等式; $>$: 停止性を保証する項上の順序

(1) $R_2 = R_1$; $E = \{e = e'\}$ とする.

(2) E が空なら終了. このとき $e = e'$ は R_1 の帰納的定理であることが示される. E が空でないなら (2-1) から (2-4) を繰り返す.

(2-1) E から $s > t$ を満たす等式 $s = t$ (あるいは $t = s$) を 1 つ取り出し, $s \to t$ を R_2 に付け加える. もしそのような等式がないなら終了. このとき証明は失敗.

(2-2) $NF^G_{R_1} \neq NF^G_{R_2}$ なら終了. このとき $e = e'$ は R_1 の帰納的定理でないことが示される.

(2-3) $s \to t$ と R_1 の間で, 項 s の R_1 完全な出現位置[†2]を適当に 1 箇所以上選び, そこで生成されるすべての危険対を E に加える. もしそのような出現位置がなければ終了. このとき証明は失敗.

(2-4) R_2 をもちいて E の等式の両辺をすべて正規形にする. 両辺が一致した等式は E から取り除く.

Kapur らの手続と Fribourg の手続きは, 基底項上で正規形の集合の等価性判定が行なえるように, Kunuth-Bendix の完備化手続きを改良したものとなっている. それゆえに, これらの手続きは帰納的完備化手続き (inductive completion procedure) とも呼ばれる [2] [5] [7].

しかし, Kapur らの手続きは潜在帰納法にもとづいているため, 合流性の判定が必要となり, (2-3) ではすべての危険対を E につけ加えている. 一方, Fribourg の手続きは書換え帰納法にもとづいているため, 合流性のかわりに退行性の判定を行なえば十分であり, (2-3) では R_1 完全な出現位置での危険対のみを付け加えている. したがって, Fribourg の手続きは Kapur らの手続きと比較して等式の生成が制限されており, 一般にはより効率の良い証明が可能となる. このような手続きは線形戦略 (linear strategy) と呼ばれている [2] [5]. したがって, 直観的には Kapur らの手続きは横型探索による R_3 の構成法, Fribourg の手続きは縦型探索による R_3 の構成法とみなすことが可能である.

5.2 例による証明手続きの比較

前節では, Kapur らの手続きと Fribourg の手続きの違いについて説明した. 本節では, それぞれの手続きの違いが, 実際の自動証明においてはどのような差異となって現れるかを, 文献 [5] [13]の例にもとづいて考察する. まず, Kapur らの手続きでは失敗するが, Fribourg の手続きでは成功する例を示す [5].

例 5.3 次の完備な項書換えシステム R_1 を考える.

$$R_1: \begin{cases} 0 + x \to x \\ s(x) + y \to s(x + y) \end{cases}$$

†2 項 s の出現位置 p が R_1 完全であるかどうかは決定可能である [5].

このとき，$x+(y+z)=(x+y)+z$ の証明を行なう．

Fribourg の手続きでは，次のように証明が実行される．等式に向きづけを行ない $x+(y+z)\rightarrow(x+y)+z$ とする．このとき $p=\{\varepsilon,2\}$ は項 $x+(y+z)$ の R_1 完全な出現位置となる．ここで，出現位置 ε を選び危険対の生成を行なうと，$(y+z)=(0+y)+z$ と $s(x+(y+z))=(s(x)+y)+z$ の 2 つの等式が E に付け加えられる．これらの等式を $R_1\cup\{x+(y+z)\rightarrow(x+y)+z\}$ をもちいて正規形にすると，両辺が一致するため削除される．この結果，次の R_3 が作られ証明は完了する．

$$R_3:\begin{cases}0+x\rightarrow x\\ s(x)+y\rightarrow s(x+y)\\ x+(y+z)\rightarrow(x+y)+z\end{cases}$$

一方，Kapur らの手続きでは出現位置 2 における危険対も生成されるため，$x+s^n(y+z)=(x+s^n(y))+z$ $(n\geq 1)$ の形の等式が無限に生成されて証明に失敗する．□

次に，Kapur らの手続きでは成功するが，Fribourg の手続きでは失敗する例を示す [13]．

例 5.4 [13] 次の完備なシステム R_1 を考える．

$$R_1:\begin{cases}(1)\ app(Nill,x)\rightarrow x\\ (2)\ app(cons(x,y),z)\\ \qquad\rightarrow cons(x,app(y,z))\\ (3)\ rev(Nill)\rightarrow Nill\\ (4)\ rev(cons(x,y))\\ \qquad\rightarrow app(rev(y),cons(x,Nill))\end{cases}$$

このとき，$rev(rev(x))=x$ の証明を行なう．

Kapur らの手続きでは，次のように証明が実行される．(5) $rev(rev(x))\rightarrow x$ とする．(4)(5) の危険対から次の規則が作られる．

(6) $rev(app(rev(y),cons(x,Nill)))\rightarrow cons(x,y)$.

(5)(6) の危険対から次の規則が作られる．

(7) $rev(app(y,cons(x,Nill)))\rightarrow cons(x,rev(y))$.

(6) の規則は削除され結果として完備な次の R_3 が作られ証明は完了する．

$$R_3:\begin{cases}app(Nill,x)\rightarrow x\\ app(cons(x,y),z)\rightarrow cons(x,app(y,z))\\ rev(Nill)\rightarrow Nill\\ rev(cons(x,y))\\ \qquad\rightarrow app(rev(y),cons(x,Nill))\\ rev(rev(x))\rightarrow x\\ rev(app(y,cons(x,Nill)))\\ \qquad\rightarrow cons(x,rev(y))\end{cases}$$

一方，Fribourg の手続きでは証明の実行途中に次のような等式が無限に生成されるため証明に失敗する．

$rev(app(rev(y),cons(x,Nill)))=cons(x,y)$,

$rev(app(app(rev(z),cons(y,Nill)),cons(x,Nill)))$
$=cons(x,cons(y,Nill))$,

・・・．

つまり Fribourg の手続きは本質的に縦型探索なので，(7) のような適当な補題が発見できず，証明に失敗している．□

このように，Kapur らの手続きと Fribourg の手続きに対して，一方では証明に成功するが他方では失敗する例がそれぞれ存在している．しかし，定理 4.5で示した反駁証明法と組み合わせた潜在帰納法と書換え帰納法の証明能力の等価性に，このことは矛盾しているわけではない．なぜなら，定理 4.5は以下を示しているにすぎないからである．(1)Kapur らの手続きで合流性を満たす R_3 が構成できたならば，この R_3 は退行性も満たす．(2)Fribourg の手続きで退行性を満たす R_3 が構成できたならば，この R_3 は合流性も満たす．しかし，Kapur らの手続きでは合流性を満たす R_3 の構成を目標としており，Fribourg の手続きでは退行性を満たす R_3 の構成を目標としている．したがって，それぞれの手続きにおける R_3 の構成法 (具体的には，付け加えるべき危険対の選択方法の戦略) は異なっている．つまり，Kapur らの手続きで R_3 が構成できたとしても，Fribourg の手続きで全く同じ R_3 が構成できる保証はなく，逆も同様である．これが，定理 4.5で反駁証明法と組み合わせた潜在帰納法と書換え帰納法の証明能力の等価性が示されているにもかかわらず，実際の手続きの証明能力に差が生じた理由である．このように，実際の証明手続きでは，R_3 を構成する戦略が，証明能力に大きな影響を与えてい

る.

6 おわりに

本研究では，帰納的定理の自動証明手続きとして，従来は具体的な形でのみ論じられてきた書換え帰納法を，抽象リダクションシステムの等価性判定法として定式化した．この定式化にもとづき，統一された抽象的な枠組の中で潜在帰納法と書換え帰納法の関係を考察し，潜在帰納法では合流性と弱正規性が本質であるのに対し，書換え帰納法では退行性と強正規性が本質的であることを示した．さらに，合流性と強正規性は互いに独立した条件であることを明らかにし，両者の証明能力が異なることを示した．また，反駁証明法と組み合わせた潜在帰納法と書換え帰納法は，証明能力が一致していることを明らかにした．次に，多くの自動証明システムで実装されている反駁証明法と組み合わせた潜在帰納法と書換え帰納法について考察し，証明手続きの戦略の違いによって，両者の証明能力に差の生じることを明らかにした．

このような統一的な形で潜在帰納法と書換え帰納法を理論的に比較した研究はこれまでほとんど知られておらず，従来は必ずしも明確でなかった両者の差異が本論文ではじめて理論的に整理されたといってよい．ここで得られた結果にもとづいて，新しい帰納的定理証明法を提案することは今後の課題である．

謝辞

本論文の改善のために貴重なコメントを頂いた査読者，および外山研究室 鈴木大郎氏と草刈圭一朗氏に感謝いたします．本研究は一部文部省科学研究費 10680346，09245102 の補助による．

参考文献

[1] Baader, F. and Nipkow, T.: *Term rewriting and all that*, Cambridge University Press (1998).

[2] Bachmair, L.: *Canonical equational proof*, Birkhauser Press (1991).

[3] Bouhoula, A.: Automated theorem proving by test set induction, *Journal of Symbolic Computation*, 23 (1997), pp. 47–77.

[4] Boyer, R. S. and Moore, J. S.: *A computational logic*, Academic Press, New York (1979).

[5] Fribourg, L.: A strong restriction of the inductive completion procedure, *Journal of Symbolic Computation*, 8 (1989), pp. 253–276.

[6] Huet, G. and Hullot, J. M.: 'roof by induction in equational theories with constructors, *Journal of Computer and System Science*, 25 (1982), pp. 239–266.

[7] Jouannand, J. P. and Kounalis, E.: Automatic proof by induction in theories without constructors, *Information and Computation*, 82 (1) (1989), pp. 1–33.

[8] Kapur, D., Narendran, P. and Zhang, H.: Automating inductionless induction using test set, *Journal of Symbolic Computation*, 11 (1991), pp. 83–111.

[9] Kapur, D. and Zhang, H.: A rewrite rule laboratory, *Lecture Notes in Computer Science*, No. 310 (1988), pp. 768–769.

[10] Kapur, D., Narendran, P. and Zhang, H.: On sufficient-completeness and related properties of term rewriting system, *Acta Information*, 24 (1987), pp. 395–415.

[11] Knuth, D. and Bendix, P.: Simple word problems in universal algebras, In *Computational Problems in Abstract Algebras*, Oxford Pregamon Press (1970), pp. 263–297.

[12] Kounalis, E. and Rusinowitch, M.: Mechanizing inductive reasoning, In *Proc. of the American Association for Artificial Intelligence* (1990), pp. 240–245.

[13] Küchlin, W.: Inductive completion by ground proof transformation, In *Resolution of Equation in Algebraic Structures (Vol. 2): Rewriting Techniques*, Boston Academic Press (1989).

[14] Musser, D. R.: On proving induction properties of abstract data types, In *Proc. 7th ACM Symp. Principles of Programming Languages* (1980), pp. 154–162.

[15] Reddy, U. S.: Term rewriting induction, *Lecture Notes in Computer Science*, No. 449 (1990), pp. 162–177.

[16] Thiel, J. J.: Stop losing sleep over incomplete data type specifications, In *Proc. 11th ACM Symp. Principles of Programing Languages* (1984), pp. 76–82.

[17] Toyama, Y.: How to prove equivalence of term rewriting system without induction, *Theoretical Computer Science*, 90 (1991), pp. 369–390.