項書換えシステム「Metis 」における帰納的証明機能

5B－1

大須賀昭彦　　坂井公
（新世代コンピュータ技術開発機構）

1．はじめに

HuetとHullotはHusser[5] らの仕事を拡張し，Knuth& Bendixの完備化手続き[4] が等式論理における帰納的定理の証明に利用できることを示した[3]．直接に帰納法を使わず帰納的定理を証明するこの方法は，潜在帰納法 (inductionless induction) と呼ばれ，最近さかんにその応用が研究されている．これは，等式論理の公理系Ｅに証明すべき等式を加え新しい公理系Ｅ´をつくったとき，ＥとＥ´が等しい始代数モデルを持てば加えた等式はＥ上の定理であるという考え方に基づいた定理証明手法である．今回，項書換えシステム生成系Metis 上に潜在帰納法を実現したので，その証明手続きについて報告する．

2．項書換えシステム生成系 Metis

Metisは，TRSに関する技術研究を目的とした実験システムであり，現在DEC-2060とPSI に実装されている．基本機能として①等式の書換え規則化（停止性保証）機能，②完備化機能，③定理証明機能，④簡約機能等を備えている．これらの処理はすべて会話的に行われる[6]．

3．潜在帰納法

通常の完備，簡約，既約等の概念は既知とする[7]．Ｅ，Ｅ´に対応する完備なTRS Ｒ，Ｒ´に於いて始代数モデルが一致するとは，Ｒの基礎項(ground term) 上の既約項がＲ´でも既約項であることを意味する．そこで，Ｒ上の帰納的定理は次の手順で証明可能となる．(1)完備なTRS Ｒに証明すべき等式を追加してＲ´を得る (2) Ｒ´を完備化する (3)得られた完備なTRS Ｒ´がＲの基礎項上の既約項を簡約しないことを確認する．これが潜在帰納法といわれる定理証明手法である[3][7]．

ここで，(3)の判定は一般に容易ではない．いくつかの判定方法が提案されているが，我々は実現の効率を考慮して，定義原理に基づくものを採用した．

3.1.定義原理[3][7]

Ｆを関数記号の集合，Ｖを変数の集合，T(F,V)をＦ，Ｖからつくられる項の集合，T(F)をＦのみからつくられる変数を含まない基礎項の集合とする．Ｆは演算子Ｄと構成子Ｃに分割されているものとし，T(C,V),T(C) も同様に定義する．

定義．完備なTRS Ｒが定義原理をみたすとは，任意の基礎項 t∈T(F)に対し，tがＲに於ける標準形となるのは t∈T(C)のとき，かつこのときに限られることをいう．

この原理をみたす完備なTRS に関しては，次の定理により (3)の判定が可能となる．

定理．新たな書換え規則がＲの既約項を簡約しない<=> 書換え規則の左辺 l が l∈T(C,V)．

また，完備なTRS が定義原理をみたすことを確認する十分条件として，次が知られている．

定理．完備なTRS Ｒに於て，任意の書換え規則の左辺が d∈Ｄを含み，かつ任意の d∈Ｄ，ci∈Ｃについて，項 d(c1,....,cn)が可約 => Ｒは定義原理をみたす．

3.2.向付自由規則の導入

従来の潜在帰納法では，新たな等式に向付ができない場合Ｒ´の停止性が保証できなくなり，証明は失敗に終わっていた．我々はこの問題に対し，向付自由規則の考え方を導入した．これは，＞を適当な強単純化順序[2] としたとき，等式l=r に対して，l＞r (r＞l)となるならば従来通り書換え規則として l→r (r→l)を得るが，順序付できない場合は，それを両方向に適用可能な向付自由規則 l↔r として扱うというものである．これに伴い，要対法，簡約等の概念が以下のように拡張される．

定義．項g が部分項s を持つことをg[s]と表すと，２つの書換え規則g[s]→d，l→r が与えられ，θ(s)=θ(l)，θ(r) ≧θ(l) かつθ(d) ≧θ(g[s])なる代入θが存在するとき，θ(d)=θ(g[r])を拡張要対という．

定義．g[s]は，s=θ(l)，θ(l) ＞θ(r) なる代入θが存在するとき l↔r によって，g[θ(r)]へ拡張簡約される．

3.3.無限実行の検出

潜在帰納法は，定理が成立する場合無限の要対を生成し続け停止しないことがある．しかし，多くの場合新たな補題（等式）を追加することによって，そのような無限実行は回避できる．そこで，この状況の検出が重要な問題となってくる．我々は無限実行の検出にHermann の結果[1] に類似の交差対の概念を導入した．

定義．２つの書換え規則g[s]→d，l→r[t]，が与えられ，θ(s)=θ(l)，θ(r[t])≧θ(l) かつθ(d) ≧θ(g[s])なる代入θが存在し，さらに，θ(t) とl が単化可能かつθ(d) ≧θ(g[r[t]]) であるときこの２つの規則を拡張交差対と呼ぶ．

拡張交差対は同時に拡張要対θ(d)=θ(g[r[t]]) を生成する．必要とされる補題は，この要対をさらに一般化するような等式である．しかし，拡張交差対の存在は無限実行の十分条件ではないため，現在の実現では，補題の必要性の判断はユーザに任される．

4．アルゴリズム

以下に潜在帰納法のアルゴリズムを与える．以降，拡張要対，拡張簡約，拡張交差対を単に要対，簡約，交差対と記す．また，＞は適当な強単純化順序を表し，構成子は任意の演算子より小さいことを仮定する．

0.R0:=定義原理を満足する完備なTRS
　E0:=証明すべき等式の集合

Inductionless Induction by Metis
Akihiko OHSUGA, Ko SAKAI
Institute for New Generation Computer Technology

```
i:=0
1.if Ei=φ
    停止［定理成立］
  else
    Ei中のM=N を選択し，既約項 M↓,N↓を求める
    if M↓≡ N↓
      Ri+1:=Ri, Ei+1:=Ei-{M=N}, i:=i+1とし1.へ戻る
    else
      2.へすすむ
2.if M↓≡c(M1,...,Mm),N↓≡c(N1,...,Nn),c∈C
    Ri+1:=Ri, Ei+1:=Ei-{M=N}+{Mj=Nj  1≦j ≦n},
    i:=i+1  とし1.へ戻る
  eleseif M↓≡c1(M1,...,Mm), N↓≡c2(N1,...,Nn),
    停止［定理不成立］          c1,c2 ∈C, c1≠c2
  eleseif M↓≡c(M1,...,Mn),c∈C,N↓∈V
    停止［定理不成立］
  eleseif M↓∈V,N↓≡c(N1,...,Nn),c∈C
    停止［定理不成立］
  eleseif M↓,N↓∈V,M↓≠ N↓
    停止［定理不成立］
  eleseif M↓> N↓
    F:={M ↓→ N↓} とし3.へすすむ
  eleseif M↓< N↓
    F:={N ↓→ M↓} とし3.へすすむ
  else
    F:={N ↓← M↓} とし3.へすすむ
3.if  Ri中の規則とF との間に交差対が存在
    Ei+1:=Ei-{M=N}+{補題}+{FとRi間の要対}
  else
    Ei+1:=Ei-{M=N}+{FとRi間の要対}
  Ri+1:=Ri+{F}, i:=i+1とし1.へ戻る
```

5．実行例

異る定義を与えられたリストの反転プログラムが始代数モデル上で等価であることを証明する．以下のようにR0として書換え規則による２種類のreverse の定義を与え，E0を２つの定義が等価であることを示す等式の集合とする．演算子Dを{reverse,append,nrev}，構成子Cを{[],[:]}として適当な順序を仮定すると，このR0は完備でありかつ定義原理を満足する．

```
R0={reverse([]) →[],                                  (r1)
    reverse([X:Y])→append(reverse(Y),[X]),            (r2)
    append([],X)→X,                                   (r3)
    append([X:Y],Z) →[X:append(Y,Z)],                 (r4)
    nrev([],X)→X,                                     (r5)
    nrev([X:Y],Z) →nrev(Y,[X:Z])}                     (r6)
E0={reverse(X) = nrev(X,[])}                          (e1)
```

手続きを開始すると，E0から等式(e1)が選択される．左辺↓＞右辺↓により，R1,E1 は

```
R1=R0+{reverse(X) →nrev(X,[])}                        (r7)
E1={append(reverse(Y),[X])=nrev([X:Y],[])}            (e2)
```

となる．ここで，(e2)は(r2)と(r7)間の要対である．

E1から(e2)を選択し両辺を簡約すると，等式

```
append(nrev(Y,[]),[X])=nrev(Y,[X])                    (e2)↓
```

が得られる．左辺↓＞右辺↓により，Tとして，

```
append(nrev(Y,[]),[X])→ nrev(Y,[X])}                  (r8)
```

が得られるが，(r6)と(r8)は交差対になっており，無限実行の可能性がでてくる．そこで，補題を獲得し併せてE2へ追加する．

```
R2=R1+{(r8)}
E2={append(nrev(X,Y),Z) = nrev(X,append(Y,Z)),(e3)
    append(nrev(X,[Y]),[Z])=nrev([Y:X],[Z])}  (e4)
```

ここで，(e3)は補題，(e4)は(r6)と(r8)間の要対である．

E2から(e3)を選択すると，左辺↓＞右辺↓により，

```
R3=R2+{append(nrev(X,Y),Z)→nrev(X,append(Y,Z))}
E3={(e4)}                                             (r9)
```

となる．続けてE3から(e4)を選択し，両辺を簡約すると，

```
nrev(X,[Y,Z])=nrev(X,[Y,Z])                           (e4)↓
```

が得られ，左辺↓＝右辺↓により，

```
R4=R3
E4=E3-{(e4)}= φ
```

となる．これにより手続きは停止し，最初に与えた等式が帰納的定理であることが確認される．

6．おわりに

Hetis上の潜在帰納法について説明した．従来の手続きには，①結果（成立・不成立）と共に停止する②証明に失敗して停止する③停止しないの３つの場合があったのに対し，我々の方法は，(1)向付自由規則の導入によって②の場合を防ぎ，また，(2)無限実行の検出基準により，ユーザの介入によって③の多くの場合を回避することにも成功した．

今後はさらに定理証明能力の向上を目指していく予定であるが，今のところ以下の課題について検討している．

- 基礎項上に限定された合流性の判定
- 補題の自動獲得

参考文献

[1] Hermann,M.and Privara,I.:"On nontermination of Knuth-Bendix algorithm",Research Report VUSEI-AR-OPS-3/85,Institute of Socio-Economic Information and Automation,CS-842 21,1985.

[2] Hsiang,J.:"On word problems in equational theories",private communication(1985).

[3] Huet,G.and Hullot,J.M.:"Proofs by induction in equational theories with constructors", J. Comput.Syst.Sci.,Vol.25,No.2(1982),pp.239-266.

[4] Knuth,D.E.and Bendix,P.B.:"Simple Word Problems in Universal Algebras",Computational Problems in Abstract Algebra (J.Leech eds.), Pergamon Press,Oxford(1970),pp.263-297.

[5] Musser,D.R.:"On proving inductive properties of abstract data types",7th ACM Symposium on Principle of Programming Language(1980), pp.154-162.

[6] Ohsuga,A.and Sakai,K.:"Metis:A Term Rewriting System generator",RIMS Symposium on Software Science and Engineering(1986).

[7] 坂井公:"Knuth-Bendixの完備化手続きとその応用", コンピュータソフトウェア,Vol4,No.1(1987), pp.2-22.