2P－5

論理体系 CLC を用いた定理証明支援システムにおけるアラー分解方法の提案 [i]

林久志
早稲田大学理工学部[ii]

辰己丈夫
早稲田大学理工学研究科[iii]

1 はじめに

定理証明支援システムを考える上で、最も困難な問題の1つとして、アラー分解が挙げられる。アラー分解は他の分解と異なり、何回でも分解することが可能で、分解したからといって必ずしも証明を1歩前進させることにはならない。さらに、いたずらにアラー分解をすれば単に時間がかかるだけでなく、恒真の判定の際に必要となるシーケントの左右の比較の量を増やし、メモリーの使用量を増やし、アラー変数の代入の可能性を増やすことになる。

そこで、できるだけ必要のないアラー分解を避けて、証明の方針を見つけやすくする方法の1つとして、我々は本論文において、どのアラー分解をいつ行なうのかを、ユーザと協調して行なう方法を提案する。

2 論理体系 CLC

扱う論理式は、1階述語論理式である。以下、

A, B : 論理式,

$\Gamma, \Delta, \Sigma, \Pi$: 論理式の列 (空列含む)

とする。

シーケントの定義

$$\Gamma | \Delta$$

CLC の公理

$$\Gamma, A, \Delta | \Sigma, A, \Pi$$

CLC の推論規則

ただし、推論規則 (9)-(12) においては、t は任意の term、e は下式には存在しない自由変数とする。

$$\neg(\mathrm{left}): \frac{\Gamma, \Delta | A, \Sigma}{\Gamma, \neg A, \Delta | \Sigma} \tag{1}$$

$$\neg(\mathrm{right}): \frac{A, \Gamma | \Delta, \Sigma}{\Gamma | \Delta, \neg A, \Sigma} \tag{2}$$

$$\wedge(\mathrm{left}): \frac{\Gamma, A, B, \Delta | \Sigma}{\Gamma, A \wedge B, \Delta | \Sigma} \tag{3}$$

$$\wedge(\mathrm{right}): \frac{\Gamma | \Delta, A, \Sigma \quad \Gamma | \Delta, B, \Sigma}{\Gamma | \Delta, A \wedge B, \Sigma} \tag{4}$$

$$\vee(\mathrm{left}): \frac{\Gamma, A, \Delta | \Sigma \quad \Gamma, B, \Delta | \Sigma}{\Gamma, A \vee B, \Delta | \Sigma} \tag{5}$$

$$\vee(\mathrm{right}): \frac{\Gamma | \Delta, A, B, \Sigma}{\Gamma | \Delta, A \vee B, \Sigma} \tag{6}$$

$$\Rightarrow(\mathrm{left}): \frac{\Gamma, \Delta | A, \Sigma \quad \Gamma, B, \Delta | \Sigma}{\Gamma, A \Rightarrow B, \Delta | \Sigma} \tag{7}$$

$$\Rightarrow(\mathrm{right}): \frac{A, \Gamma | \Delta, B, \Sigma}{\Gamma | \Delta, A \Rightarrow B, \Sigma} \tag{8}$$

$$\forall(\mathrm{left}): \frac{\Gamma, \forall x A(x), A(t), \Delta | \Sigma}{\Gamma, \forall x A(x), \Delta | \Sigma} \tag{9}$$

$$\forall(\mathrm{right}): \frac{\Gamma | \Delta, A(e), \Sigma}{\Gamma | \Delta, \forall x A(x), \Sigma} \tag{10}$$

$$\exists(\mathrm{left}): \frac{\Gamma, A(e), \Delta | \Sigma}{\Gamma, \exists x A(x), \Delta | \Sigma} \tag{11}$$

$$\exists(\mathrm{right}): \frac{\Gamma | \Delta, \exists x A(x), A(t), \Sigma}{\Gamma | \Delta, \exists x A(x), \Sigma} \tag{12}$$

3 論理体系 CLC を使った証明

アラー分解、アラー変数の定義

CLC を使った論理式の証明で、推論規則 (9) または推論規則 (12) を使ってシーケントを分解することをアラー分解と呼ぶ。

---

[i] Yet Another Theorem Proving, CLC - alah reduction and its implementation

[ii] HAYASHI Hisashi, School of Science and Engineering, Waseda University
[iii] TATSUMI Takeo, Graduate School of Science and Engineering, Waseda University

このアラー分解をするとき、term t を決定しなければならないのだが、仮にこの t をアラー変数という変数 a にしておき、後で a に具体的な term を代入して、証明を完成させる。

a に代入する term の候補は推論規則 (9) または、推論規則 (12) の下式の自由変数から選ぶ。

定理自動証明システムの設計の問題点

分解の順番が決まっていれば、アラー分解を除いて、シーケントの分解の方法は一通りしかないので、機械に証明を進めさせることが出来る。

しかし、アラー分解では、アラー変数にどんな term を代入しても良いので、一通りにシーケントの分解が出来ない。アラー変数の代入の仕方によって、証明の成功・不成功が決まる。

問題点の解決方法の提案

アラー変数への具体項の代入の難しさを考え、我々は完全に機械が自動的に証明を進めるシステムでなく、アラー分解をするタイミングや、アラー変数に代入する候補の決定などを、基本的にユーザに任せる定理証明支援システムを提案する。

現在、我々はこのシステムを開発中であり、将来的には、機械が見て明らかに意味のないアラー分解やアラー変数の代入などを警告し、ユーザの判断をサポートするようなシステムを作る計画である。

定理証明支援システム

定理証明支援システムの基本的な仕組は以下の手順の繰り返しである。

1. アラー分解以外の分解を分解できなくなるまで繰り返す。
2. ユーザに判断を求める。(主にアラー分解について)

例

$\forall x \neg P(x) \Rightarrow \neg\exists x P(x)$ を証明する。

1. $|\forall x \neg P(x) \Rightarrow \neg\exists x P(x)$
2. $\forall x \neg P(x) | \neg\exists x P(x)$
3. $\exists x P(x), \forall x \neg P(x)|$
4. $P(e), \forall x \neg P(x)|$
5. $P(e), \forall x \neg P(x), \neg P(a)|$
6. $P(e), \forall x \neg P(x) | P(a)$
7. $P(e), \forall x \neg P(x) | P(e)$

- 1. から 4. は機械が自動的に行なう。
- 4. から 5. はユーザがシーケントの左側の左から 2 番目のアラー分解をするように命令している。a はアラー変数である。
- 5. から 6. は機械が自動的に行なう。
- 6. から 7. はユーザがアラー変数 a の代入をするように指示している。代入候補は 1 つしかないので、e を機械は代入し、公理判定する。このシーケントは公理なので、証明成功である。

4 おわりに

以上の方法により、少なくとも、人間が見て明らかに無駄なアラー分解は避けることができる。今後は、本システムを拡張して、人間の判断をサポートする予定である。

参考文献

[1] 加藤雅英, 辰己丈夫. 論理体系 CLC を用いた定理証明支援システムにおけるアラー変数代入方法の提案. 情報処理学会第 50 回全国大会講演論文集, 1995.

[2] 林晋, 八杉満利子. 情報系の数学入門,1993.

[3] 竹内外史, 八杉満利子. 証明論入門,1956.

[4] 廣瀬健, 筧捷彦.-新世代コンピュータの技術開発動向等に関する調査研究-証明支援系に関する調査研究報告書,1993.