# シークエント計算を用いた自動証明システム

2001MM010 橋本慧
指導教員: 佐々木克巳

## はじめに

本研究では、森[1]で研究されたGentzenのシークエント計算の体系の証明可能性を判別するプログラムをとりあげる。証明可能か否かを判別するアルゴリズムを作成する過程において、シークエント計算に対する理解をより深めることを目的とする。

## 1 体系LKと体系LK*

### 1.1 論理式について

基本となる論理的操作を形式化したものが論理結合子である。論理結合子としては次のものを使う。

| | | |
|---|---|---|
| $\wedge$ | かつ | 論理積 |
| $\vee$ | または | 論理和 |
| $\supset$ | ならば | 含意 |
| $\neg$ | でない | 否定 |

これらの論理結合子を繰り返し用いることにより、論理式が定義される。

**定義**

1. それぞれの命題変数は論理式である。
2. $A, B$がともに論理式ならば、$(A \wedge B)$、$(A \vee B)$、$(A \supset B)$、$(\neg A)$はいずれも論理式である。

### 1.2 体系LKについて

ここでは小野[3]にしたがって、体系LKを定義する。

体系LKにおける基本的な表現は式である。式とは以下のような形をしたものである。

$$A_1, \cdots, A_m \to B_1, \cdots, B_n$$

ここで、$m$と$n$は0でもよく、$A_i, B_j$は論理式である。

体系LKの公理に相当するのは始式である。LKの始式は以下の形である。

$$A \to A$$

体系LKの論理結合子に関する推論規則は、次の10個である。

$$\frac{\Gamma \to \Delta, A \quad \Gamma \to \Delta, B}{\Gamma \to \Delta, A \wedge B}\ (\wedge右) \qquad \frac{A, \Gamma \to \Delta \quad B, \Gamma \to \Delta}{A \vee B, \Gamma \to \Delta}\ (\vee左)$$

$$\frac{\Gamma \to \Delta, A}{\Gamma \to \Delta, A \vee B}\ (\vee右1) \qquad \frac{\Gamma \to \Delta, B}{\Gamma \to \Delta, A \vee B}\ (\vee右2)$$

$$\frac{A, \Gamma \to \Delta, B}{\Gamma \to \Delta, A \supset B}\ (\supset右) \qquad \frac{\Gamma \to \Delta, A \quad B, \Gamma \to \Delta}{A \supset B, \Gamma \to \Delta}\ (\supset左)$$

$$\frac{A, \Gamma \to \Delta}{A \wedge B, \Gamma \to \Delta}\ (\wedge左1) \qquad \frac{B, \Gamma \to \Delta}{A \wedge B, \Gamma \to \Delta}\ (\wedge左2)$$

$$\frac{A, \Gamma \to \Delta}{\Gamma \to \Delta, \neg A}\ (\neg右) \qquad \frac{\Gamma \to \Delta, A}{\neg A, \Gamma \to \Delta}\ (\neg左)$$

体系LKの構造に関する推論規則は、次の7個である。

$$\frac{\Gamma \to \Delta}{A, \Gamma \to \Delta}\ (weakening左) \qquad \frac{\Gamma \to \Delta}{\Gamma \to \Delta, A}\ (weakening右)$$

$$\frac{A, A, \Gamma \to \Delta}{A, \Gamma \to \Delta}\ (contraction左) \qquad \frac{\Gamma \to \Delta, A}{\Gamma \to \Delta, A, A}\ (contraction右)$$

$$\frac{\Gamma, A, B, \Pi \to \Delta}{\Gamma, B, A, \Pi \to \Delta}\ (exchange左) \qquad \frac{\Gamma \to \Delta, A, B, \Sigma}{\Gamma \to \Delta, B, A, \Sigma}\ (exchange右)$$

$$\frac{\Gamma \to \Delta, A \quad A, \Pi \to \Sigma}{\Gamma, \Pi \to \Delta, \Sigma}\ (cut)$$

ただし、$\Gamma$と$\Delta$は論理式の列である。

### 1.3 LK*について

体系LK*はGentzenによるシークエント計算の体系LKを変形したものである。体系LK*の式は以下のような形をしたものである。

$$\{A_1, \cdots, A_m\} \to \{B_1, \cdots, B_n\}$$

また、体系LK*の公理は、

$$\{A_1, \cdots, A_m, C\} \to \{B_1, \cdots, B_n, C\}$$

体系LK*の推論規則は次の８個である。

$$\frac{\Gamma \to \Delta \cup \{A\} \quad \Gamma \to \Delta \cup \{B\}}{\Gamma \to \Delta \cup \{A \wedge B\}}\ (\wedge右) \qquad \frac{\Gamma \to \Delta \cup \{A, B\}}{\Gamma \to \Delta \cup \{A \vee B\}}\ (\vee右)$$

$$\frac{\{A\} \cup \Gamma \to \Delta \cup \{B\}}{\Gamma \to \Delta \cup \{A \supset B\}}\ (\supset右) \qquad \frac{\{A\} \cup \Gamma \to \Delta}{\Gamma \to \Delta \cup \{\neg A\}}\ (\neg右)$$

$$\frac{\{A, B\} \cup \Gamma \to \Delta}{\{A \wedge B\} \cup \Gamma \to \Delta}\ (\wedge左) \qquad \frac{\{A\} \cup \Gamma \to \Delta \quad \{B\} \cup \Gamma \to \Delta}{\{A \vee B\} \cup \Gamma \to \Delta}\ (\vee左)$$

$$\frac{\Gamma \to \Delta \cup \{A\} \quad \{B\} \cup \Gamma \to \Delta}{\{A \supset B\} \cup \Gamma \to \Delta}\ (\supset左) \qquad \frac{\Gamma \to \Delta \cup \{A\}}{\{\neg A\} \cup \Gamma \to \Delta}\ (\neg左)$$

ただし、$\Gamma$と$\Delta$は論理式の有限集合である。

## 2 LKとLK*の比較と同等性

### 2.1 LKとLK*の比較

ここでは恒川[2]にしたがって体系LKとLK*の同等性を示す。

#### 2.1.1 式の形

LK*はLKにおける左辺と右辺を集合として扱うことで、contraction,exchangeを推論規則とする必要がない。

#### 2.1.2 公理

LK*は、左辺と右辺の共通部分が空でない式を公理とすることで、weakeningも必要ない。

#### 2.1.3 推論規則

LKの$(\vee$右1$)$と$(\vee$右2$)$の２つは、LK*の$(\vee$右$)$に対応する。また、LKの$(\wedge$左1$)$と$(\wedge$左2$)$の２つは、LK*の$(\wedge$左$)$に対応する。

#### 2.1.4 LK*の利点

体系LK*は、LKにおけるシークエントの左辺と右辺を集合として扱うことで証明しやすくなっている。

### 2.2 LKとLK*の同等性

LKとLK*の同等性、すなわち次の２条件の同等性を証明する。

(I) $\{A_1, \cdots, A_m\} \to \{B_1, \cdots, B_n\}$がLK*で証明可能

(II) $A_1, \cdots, A_m \to B_1, \cdots, B_n$がLKで証明可能

#### 2.2.1 LK*⇒LK((I)から(II)を証明)

(I)を仮定すると$\{A_1, \cdots, A_m\} \to \{B_1, \cdots, B_n\}$を終式とする証明図$P$がある。$P$の式の数を$l$とし、$l$についての数学的帰納法で(II)を示す。

ここでは証明は省略する。

#### 2.2.2 LK⇒LK*((II)から(I)を証明)

**LK*でのweakening右･左** LK*にはLKのweakeningに対応する推論規則が存在しないため、(I)から(II)を証明したときのようには(II)から(I)を証明することができない。そのため、weakeningに対応する２つの推論規則を次のように定め、これらがLK*で成立することを証明できる。

$$\frac{\Gamma \to \Delta}{\{A\} \cup \Gamma \to \Delta} \qquad \frac{\Gamma \to \Delta}{\Gamma \to \Delta \cup \{A\}}$$

**同等性の証明** (II)を仮定すると、cut除去定理より$A_1, \cdots, A_m \to B_1, \cdot, B_n$を終式とするcutのない証明図$P$がある。$P$の式の数を$l$とする。$l$についての数学的帰納法で(I)を示す。

ここでは証明は省略する。

## 3 アルゴリズム

### 3.1 証明可能性を判別するアルゴリズム

LK*の証明可能性は、証明したい論理式$A$に対して$\to A$を終式とする証明図が与えられるか否かで判定することができる。前章で、LK*の証明図における上式、下式の同等性が確認できているため、まず終式を$\to A$として、この式に各推論規則を適用し、論理記号を一つずつ減らしていき、証明図が始式に到達できるか否かで判定できる。具体的には以下のように判定する。

**Step1**

$\to A$を$S$とする。

**Step2**

(i) $S$に論理記号がない場合で、公理なら”証明可能”を返す。

(ii) $S$に論理記号がない場合で、公理でないなら”証明不可能”を返す。

(iii) $S$の右辺に論理記号‘⊃’がある場合、(⊃右)の推論規則を適用し、$S$を下式とする(⊃右)の上式を$S_1$とする。$S_1$を新しい$S$として**Step2**の先頭部に戻す。

(iv) $S$の右辺に論理記号‘∧’がある場合、(∧右)の推論規則を適用し、$S$を下式とする(∧右)の推論規則を適用し、$S$を下式とする(∧右)の上式を$S_1, S_2$とする。$S_1$を新しい$S$として**Step2**の先頭部に戻す。この時、$S$が証明可能なら$S_2$を新しい$S$として**Step2**の先頭部に戻す。$S$が証明不可能なら”証明不可能”を返す。

以下、同様に論理記号に対応する推論規則を適用して**Step2**の先頭部に戻す。

### 3.2 アルゴリズムの正当性

ここでは3.1節のアルゴリズムによって証明可能か否かを判定できることを証明する。そのためには、次を証明すれば十分である。

**定理：式$S$の証明可能性をアルゴリズムのStep2で判定できる。**

**証明：**$S$にあらわれる論理記号の数を$n$とし、$n$についての数学的帰納法で証明する。

$n = 0$**のとき**

論理記号の数が0個であるため、推論規則を適用できない。よって、$S$が公理であるか否かによって証明可能性を判定できる。すなわち**Step2**の$(i), (ii)$によって判定できる。

$n \leq k$**のとき題意が成立しているとする。**

$n = k + 1$のとき、**Step2**により、ある推論規則Iが適用される。一方で、LK*の8つの推論規則をみると、各上式にあらわれる論理記号の数は、下式の論理記号の数より1つ以上小さいことがわかる。推論規則Iもこの性質をみたすの で、その各上式にあらわれる論理記号の数は、$S$より1つ以上小さい。すなわち、その数は$k$である。帰納法の仮定より、各上式の証明可能性は$Step2$より判定できる。

上式が1つの場合は、その上式が、証明可能なら下式は明らかに証明可能であり、証明不可能なら、2.2節の同等性より下式も証明不可能可能である。同様に、上式が2つの場合は、その上式の両方が証明可能なら、下式は明らかに証明可能である。しかし、一方または両方が証明不可能のときは、2.2節の同等性より下式も証明不可能である。

## 4 おわりに

本研究で、LK*を用いて証明可能か否かを判別するアルゴリズムまでを示した。これをプログラムに翻訳することで、難解な証明も容易にできるようになるだろう。本来ならば、プログラムまで作成するはずだったが、そこまで研究が進まなかったことが残念である。

## 謝辞

本研究を進めるにあたり、暖かく御指導いただきました、佐々木克巳教授に心から感謝いたします。また、ともに励ましあって支えてくれたゼミ生の皆さんに心から感謝致します。

## 参考文献

[1] 森裕記：「計算機のためのシークエント計算」,南山大学経営学部情報管理学科卒業論文 (2001年).

[2] 恒川健次：「古典論理に対するいくつかの体系の比較」,南山大学経営学部情報管理学科卒業論文 (2001年).

[3] 小野寛晰：「情報科学における論理」,日本評論社 (1994年).