証明探索と反例生成を同時に行なうアルゴリズムについて

5AH－6

長野大介[1] 佐塚秀人[1,2] 廣川佐千男[3]

1: 九州大学大学院システム情報科学研究科 2: 久留米工業大学電子情報工学科 3: 九州大学大型計算機センター

1　はじめに

直観主義論理は、型理論との対応や、構成的プログラミングとの関連で重要性が広く認識されるようになってきた。自然推論の形での証明図を求める手法や証明図を全て求めるアルゴリズムなどが知られている ([2, 5]). しかしその意味論の取扱は、古典論理に比べて容易ではない。古典命題論理では真偽の２値の真理値表により、恒真性が判定でき、これが証明可能性と一致している。従って、ある命題が古典論理で証明できないことを示すには、その命題の真理値が偽となるような命題変数への割り当てを示せばよい。これに対し直観主義の意味論はクリプケ・モデルや擬ブール代数によるもので、古典論理におけるように単純なものではない (例えば [1] 参照)。命題が証明できるかどうかを機械的に判定するアルゴリズムはいずれの論理についてもすでに古くから知られているが、証明出来る場合に証明を返すだけでなく、証明できない場合には反例を具体的に構成するのは容易ではない。

我々は直観主義命題論理のシーケント計算の形式化を用いて逆向きの証明探索を行い、その過程で証明不能と判断できる場合にはその情報を用いて反例のクリプケ・モデルを生成するアルゴリズムを構成した。これまで辿ってきたシーケントを保存することにより、証明探索の打ちきりと反例の構成を統一的に行うことが可能となった。小さな命題については、人間が手で計算しても分かるくらい単純なものである。実働化は http://whale.i.kyushu-u.ac.jp/prover.html に公開している。

2　シーケント体系による証明探索

証明探索の元となる体系としては、下のようなシーケント計算の体系 NJ^* を用いる。本発表では含意命題のみを扱うが、論理和、論理積、否定についても同様に扱える。

公理

$\Gamma \vdash A (A \in \Gamma$のとき$)$

推論規則

$$\frac{A_1, \cdots, A_n, \Gamma \vdash A}{\Gamma \vdash A_1 \to \cdots \to A_n \to A}\ (I)$$

$$\frac{\Gamma \vdash A_1 \quad \cdots \quad \Gamma \vdash A_n \quad A_1 \to \cdots \to A_n \to A \in \Gamma}{\Gamma \vdash A}\ (E)$$

ここで、公理、推論規則における A は素論理式とする。この体系は、ラムダ計算での long normal form 、あるいは Prawitz [3] の自然推論体系の expanded normal form に対応している。

仮定の集合 Γ から結論 A への証明を探索をするためにシーケント $\Gamma \vdash A$ が推論の下式となるような上式を生成する。この操作を続けて最終的に公理にたどり着けるかどうかを判定することが証明探索である。我々が用いるのはこの後向き探索である。

シーケントの右側の A が素論理式ではないとき、例えば $\Gamma \vdash A_1 \to \cdots \to A_n \to A$ のようなシーケントの証明を探すには、推論 (I) を適用して、$A_1, \cdots, A_n, \Gamma \vdash A$ を生成し、これについて再帰的に証明探索を行う。シーケントの結論 A が素論理式であれば、仮定 Γ の中に $A_1 \to \cdots \to A_n \to A$ の形のものがあるかどうか調べ、あればそのような論理式について推論 (E) を後向きに適用する。このように後向きの推論の適用を繰り返し、最終的に公理に到達できた場合は、入力シーケントは証明が可能であるので、それまでに辿ってきた木の経路が証明となる。図１は証明探索が成功する例を示す。

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{A, (A \to B) \to A, A \to B, C \vdash A}}{A, (A \to B) \to A, A \to B, C \vdash B}}{(A \to B) \to A, A \to B, C \vdash A \to B}}{(A \to B) \to A, A \to B, C \vdash A}}{(A \to B) \to A, A \to B, C \vdash B}}{\vdash ((A \to B) \to A) \to (A \to B) \to C \to B}$$

図１：直観主義論理 NJ^* での証明

3　モデルの再帰的生成方法

証明を探すシーケントに対し推論を後向きに適用してそれ以上 (I) も (E) も逆向きに適用できないという状況に陥った場合は証明探索を打ち切る (図２)。この場合、証明が打ち切られた位置で反例としてクリプケモデルを生成し、証明が出来ないことを示す。具体的には、証明が打ち切られた時点でそのシーケントに含まれる素論理式に対し、シーケントの左側を真、右側を偽とするような古典論理での真理値の割当を行う。このような一点からなる可能世界のモデルを一点モデルということにし、反例として返す。

$$\dfrac{\dfrac{\dfrac{}{A, (A \to B) \to A \vdash B}}{(A \to B) \to A \vdash A \to B}}{\vdash ((A \to B) \to A) \to A}$$

図２：証明探索が停止する例

推論 (I) については、推論の上と下のシーケントの証明可能性は同等である。従って、推論の上についての反例モデルが求まれば、推論の下のシーケントについての反例にもなっている。

Proof Search and Counter-Model Generation for Intutitionistic Logic
Daisuke Nagano, Kyushu University
Hideto Sazuka, Kurume Institute of Technology
Sachio Hirokawa, Kyushu University
6-10-1,Hakozaki,Higashiku,Fukuoka 812-81,Japan

Aが素論理式のときには、推論 (E) しか適用できない。もし、$\Gamma \vdash A$が証明できないならば、どのような$A^i_1 \to \cdots \to A^i_{n_i} \to A \in \Gamma (i = 1, \cdots, m)$について (E) を適用しても$\Gamma \vdash A^i_1, \cdots, \Gamma \vdash A^i_{n_i}$のどれかが証明不可能となるはずである。それを$A^i_{j_i} (1 \leq j_i \leq n_i)$とすると$m$個の反例モデル$D_j, (i = 1, \cdots, m)$が求まる。これらのモデル$D_{j_1}, \cdots, D_{j_m}$の下に新しい点$p$を加え、すべての世界$D_{j_1}, \cdots, D_{j_m}$で成り立つもののみを$p$で成り立つようにする (ただし、$A$は除く)。この$D_{j_1}, \cdots, D_{j_m}$の$A$に関する 連結モデル を返す。

証明が出来ないという状況は、それ以上推論が適用できなくなった場合だけではなく、これ以上推論を続けても以前行なった推論と全く同じことを繰り返すだけになった場合も含まれる (図3)。すなわち推論が無限ループに陥ったと分かった場合である。この場合に返すモデルは先程の 一点モデル と同様であるが、繰り返しのシーケントにおいて、結論に現われていた素論理式は偽にするようにしなければならない。

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{B, C, A \to B, (B \to C \to A) \to A \vdash A}{B, C, A \to B, (B \to C \to A) \to A \vdash B \to C \to A}}{B, C, A \to B, (B \to C \to A) \to A \vdash A}}{A \to B, (B \to C \to A) \to A \vdash B \to C \to A}}{A \to B, (B \to C \to A) \to A \vdash A}}{A \to B, (B \to C \to A) \to A \vdash B}$$

図 2：証明探索が繰り返しに陥る例

4 アルゴリズム

命題 A に対する証明探索 $pm(A)$ は、空の仮定から結論 A を導くシーケントの証明の探索として行う。この一般的なシーケント$\Gamma \vdash A$の証明探索を行うアルゴリズムが $pm^*(\Gamma \vdash A; \xi)$ である。ξは入力シーケント以前に推論に現れたシーケントを格納したリストである。また、下のpm^*の定義における$core(\Gamma)$とは、Γに含まれる各論理式のそれぞれおいて最も右側に現われる素論理式を集めた集合を表す。例えば、A, Bが素論理式のとき$core(A \to B, (C \to B) \to A) = \{B, A\}$である。このアルゴリズム$pm(A)$の停止性、ならびに正当性、すなわち、$A$が証明可能であれば証明図を、証明が不可能であれば反例としてのモデルを返すことの証明は別の機会に報告する。

$pm^*(\Gamma \vdash A; \xi)$のアルゴリズムは以下の通り。

1. $A = B_1 \to \cdots \to B_n \to B$ (つまりAが素論理式でない場合)．
u=$pm^*(B_1, \cdots, B_n, \Gamma \vdash B; \Gamma \vdash A + \xi)$とする。

1.1. uが証明図の場合. 証明図

$$\dfrac{u}{B_1, \cdots, B_n, \Gamma \vdash B}$$

を返す。

1.2. uがモデルの場合. uを返す。

2. Aが素論理式の場合.

2.1. $A \in \Gamma$の場合. 公理 $A \in \Gamma$ を返す。

2.2. $A \notin \Gamma$の場合.

2.2.1. $\Gamma \vdash A \in \xi$の場合.
$\xi = \Gamma_n \vdash A_n, \cdots, \Gamma_1 \vdash A_1$とすると$\Gamma_k = \Gamma, A_k = A$ となる$1 \leq k \leq n$がある。そこで$core(\Gamma) - \{core(A_j) | k \leq j \leq n\}$できまる一点モデルを返す。

2.2.2. $\Gamma \vdash A \notin \xi$の場合.

2.2.2.1. $core(B) = A$となる $B \in \Gamma$がない場合. $core(\Gamma)$できまる一点モデルを返す。

2.2.2.2. $core(B) = A$となる$B \in \Gamma$がある場合. それらを$B_1 = A^1_1 \to \cdots \to A^1_{n_1} \to A, \cdots B_i = A^i_1 \to \cdots \to A^i_{n_i} \to A, \cdots B_m = A^m_1 \to \cdots \to A^m_{n_m} \to A$とし、$u^i_j = pm^*(\Gamma \vdash A^i_j)$を再帰的に求める$(i = 1, \cdots, m, j = 1, \cdots, n_i)$.

2.2.2.2.1. ある$1 \leq i \leq m$に対し$u^i_1, \cdots, u^i_{n_i}$がすべて証明図の場合. $\dfrac{u^i_1 \quad \cdots \quad u^i_{n_i}}{\Gamma \vdash A}$ を返す.

2.2.2.2.2. 任意の$i = 1, \cdots, m$に対し$u^i_{j_i}$がモデルとなるような$1 \leq j_i \leq n_i$がある場合. $u^1_{j_1}, \cdots, u^m_{j_m}$の$A$に関する連結モデルを返す。

5 アルゴリズムの実現

このアルゴリズムを用いて、証明・反例の生成を行なうシステムを製作した。証明・反例生成の主要部分はLispで製作し、インターフェイス部分をJAVAで製作した。その2つを協調運用することで、Netscapeなどのウェブブラウザからインターネット経由で利用出来るようになっている。結合方式については [4] 参照。

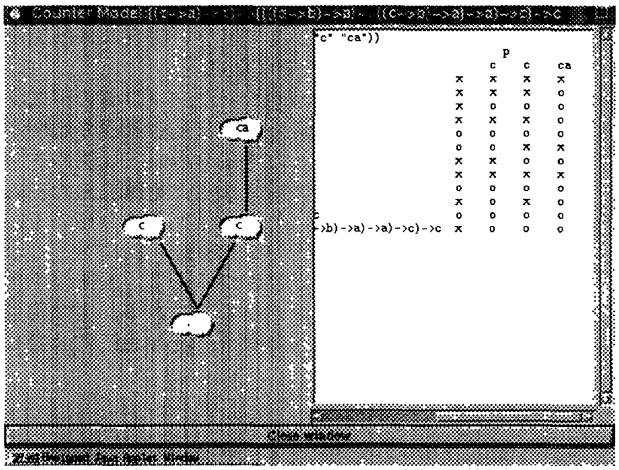

図 3：$((c \to a) \to c) \to ((((a \to b) \to a) \to ((c \to b) \to a) \to a) \to c) \to c$に対するモデル生成例

References

[1] 林晋, 数理論理学, コロナ社 (平成8年)

[2] R. Hindley, The Basic Type Theory, Cambridge University Press (1996).

[3] D. Prawitz,Natural Deduction Almqvist and Wiksell (1965).

[4] 佐塚秀人、長沢武司、廣川左千男, 分散する証明推論エンジンのWEB上での結合について, マルチメディア と 分散処理 ワークショップ論文集 (平成8年) 341–348.

[5] M. Takahashi et. al., Normal Proofs and Their Grammar, Information and Computation 125 (1996) 144–153.