計算機による定理の自動証明

2001MM001 足立 大輔
指導教員　佐々木 克巳

1　はじめに

小野 [1] は，第 2 章で古典述語論理の体系 LK を導入し，第 3 章のはじめの部分で次のように述べている.『2 章の定理 2.5 で述べたように，与えられた式が (または論理式) が LK で証明可能であるか否かを判定するような有限の手続きは存在しないことがわかっている．しかしながら，与えられた式が証明可能であるときには必ず「証明可能である」ことを教えてくれるような部分アルゴリズムは存在する.』そして，部分アルゴリズムの一つの例として，しらみつぶしによる方法を述べてから，次のように続けている.『しかし，この方法はあまりにも非能率的である．そこでこの章ではより効率のよい部分アルゴリズムとして知られている導出原理 (resolution principle) について紹介する．現在，計算機による定理の自動証明の多くには，基本的にこの導出原理が用いられている.』本研究は，[1] で紹介されている導出原理の理解を目的とする．具体的には，[1] にしたがって，導出原理の考え方の基礎にあるエルブランの定理を理解し，次に導出原理を命題論理と述語論理の場合に分け，それぞれの導出計算 R_0 と R_1 の完全性を理解する．

2　エルブランの定理

この節では，エルブランの定理を [1] にしたがって説明する．

閉じた論理式

論理式 A が自由変数 (A において量化記号にともなって現れない出現がある変数) を一つも含まないとき，A を**閉じた** (closed) **論理式**という．

定義 2.1 存在冠頭論理式 (existential formula)

B が量化記号を一つも含まない論理式であるとき，

$$\exists x_1 \cdots \exists x_n B \quad (n \geqq 0)$$

の形の論理式を存在冠頭論理式という．

エルブラン領域

$H_{\mathcal{L}}$ は変数を含まないような $\mathcal{L}$ の項全体の集合とする。ただし，$\mathcal{L}$ が一つも定数記号を含まないときには，変数を含まないような項は一つも存在しないことになる．そこでこの場合には，まず定数記号を一つ $\mathcal{L}$ に付け加えておき，その上で変数を含まない項全体の集合を $H_{\mathcal{L}}$ と定義することにしておく．$H_{\mathcal{L}}$ を ($\mathcal{L}$ の定める) **エルブラン領域** (Herbrand universe) という．

定義 2.2 エルブラン構造

次の条件をみたす構造 $\mathfrak{A} =< U, J >$ を言語 $\mathcal{L}$ に対するエルブラン構造 (Herbrand structure) という．

1)　$U = H_{\mathcal{L}}$.

2)　c が $\mathcal{L}$ の対象定数のとき，$c^J = c$.

3)　f が $\mathcal{L}$ の n 変数関数記号のとき，
$f^J(t_1, \cdots, t_n) = f(t_1, \cdots, t_n)$
(ただし $t_1, \cdots, t_n \in H_{\mathcal{L}}$).

定理 2.1 (エルブランの定理) $\exists x_1 \cdots \exists x_n B$ を言語 $\mathcal{L}$ の閉じた存在冠頭論理式とする．ここで B は量化記号を一つも含まない論理式とする．このとき，$\exists x_1 \cdots \exists x_n B$ が恒真になるための必要十分条件は，ある自然数 $m(\geqq 1)$ と $H_{\mathcal{L}}$ の項 $t_{i1}, \cdots, t_{in} (i = 1, \cdots, m)$ が存在して

$$B[t_{11}/x_1, \cdots, t_{1n}/x_n] \vee \cdots\cdots \vee B[t_{m1}/x_1, \cdots, t_{mn}/x_n]$$

が任意の $\mathcal{L}$ に対するエルブラン構造で真になることである．

3　導出原理－命題論理の場合

この節では，命題論理の場合の導出計算 R_0 を [1] にしたがって導入する．そして，例として [1] の一つの問の解を示す.

一般に原子論理式または原子論理式の前に否定記号を一つ付けた論理式のことを**リテラル** (literal) という．命題論理の場合は，命題変数 (および命題定数) が原子論理式である．リテラル A に対し A^* を次のように定める．

$$A^* = \begin{cases} \neg p & A \text{ が } p \text{ のとき} \\ p & A \text{ が} \neg p \text{ のとき} \end{cases}$$

リテラルの有限集合を**節** (clause) という．空集合の場合には**空節**とよび，それを $\square$ で表す．節の有限集合を**節集合**という.

二つの節 C_1 と C_2 に対し，C_1 に属す一つのリテラル A に対して A^* が C_2 に属しているとする．このとき，節 $(C_1 - \{A\}) \cup (C_2 - \{A^*\})$ を C_1 と C_2 からの**導出節** (resolvent) という.

二つの節から導出節を作りだす操作のことを (命題論理の) **導出原理** (resolution principle) という.

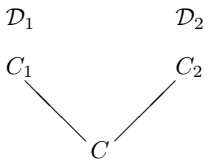
導出原理を繰り返し適用し，節集合から一つの節を導き出す過程を記述するために命題論理の**導出計算** R_0 およびその**導出図** (derivation) を導入する.

定義 3.1 R_0 の導出図

1)　節 C が節集合 S に属すときには，C だけからなる図は S から C に到る導出図である.

2)　S から節 C_1 に到る導出図 $\mathcal{D}_1$ と S から節 C_2 に到る導出図 $\mathcal{D}_2$ がすでに定義されているとする．さらに C_1 と C_2 から導出原理により節 C が得られるものとする．このとき，次のように与えられる図は

S から C に到る導出図である．



節集合 S から節 C に到る R_0 の導出図が存在するとき，R_0 で S から C は**導出可能である** (derivable) という．

節 C がリテラルの集合 $\{A_1, \cdots, A_k\}$ であるとき $\wedge C$ は論理式 $A_1 \wedge \cdots\cdots \wedge A_k$ を表すものとする．空でない節集合 $S = \{C_1, \cdots, C_m\}$ に対し S の論理和標準形表現を $d(S) = (\wedge C_1) \vee \cdots \vee (\wedge C_m)$ と定める．

定理 3.1 (命題論理の導出計算 R_0 の完全性) S を任意の空でない節集合とする．このとき，$d(S)$ がトートロジーになるための必要十分条件は R_0 で S から $\square$ が導出可能になることである．

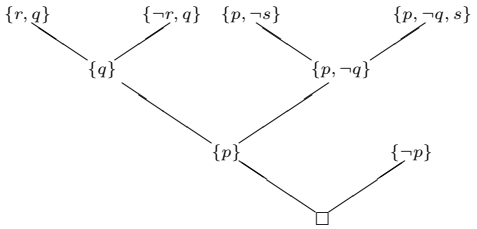
次の例は，[1] では問とされているものである．

例 3.1 定理 3.1 を用いて次の論理式がトートロジーになることを示す．

$(p \wedge \neg s) \vee \neg p \vee (r \wedge q) \vee (p \wedge \neg q \wedge s) \vee (\neg r \wedge q)$

この論理式は論理和標準形をしているので，これを $\{p, \neg s\}, \{\neg p\}, \{r, q\}, \{p, \neg q, s\}, \{\neg r, q\}$ からなる節集合 S に対する論理和標準形表現 $d(S)$ とする．

S に対し，下のように S から $\square$ に到る導出図を作ることができるので，定理 3.1 よりこの論理式はトートロジーになることがわかる．



4 導出原理－述語論理の場合

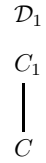
この節では，述語論理の導出計算 R_1 を [1] にしたがって導入し，[1] の章末問題にある論理式に対して R_1 を適用した結果を示す．

E を項または論理式とするとき，$E[s_1/x_1, \cdots, s_n/x_n]$ を，E における項 $s_1, \cdots, s_n$ の変数 $x_1, \cdots, x_n$ への**代入**という．

定義 4.1 R_1 **の導出図**

R_1 の導出図は R_0 の導出図の定義 1)，2) に次の 3) を付け加えることにより定義される．

3) S から節 C_1 に到る導出図 $\mathcal{D}_1$ が定義され，また代入 θ に対し $C_1\theta = C$ であるとする．このとき，次のように与えられる図は S から C に到る導出図である．



定理 4.1 (述語論理の導出計算 R_1 の完全性) S を空でない任意の節集合とする．また，$x_1, \cdots, x_n$ を S に現われる変数全体の集合とする．このとき，論理式 $\exists x_1 \cdots \exists x_n d(S)$ が恒真になるための必要十分条件は S から $\square$ が R_1 で導出可能になることである．

例 4.1 定理 4.1 を用いて次の論理式が恒真になることを示す (この論理式は [1] の章末問題で紹介されている)．

(1) $(\forall x \forall y (R(x,y) \supset R(y,x)) \wedge \forall x \forall y \forall z ((R(x,y) \wedge R(y,z)) \supset R(x,z)) \wedge \forall x \exists y R(x,y)) \supset \forall z R(z,z)$

まず，(1) の冠頭標準形を作る．

(2) $\forall u \forall y \exists x \exists v \exists w \exists z (((R(v,w) \supset R(w,v)) \wedge ((R(v,w) \wedge R(w,z)) \supset R(v,z)) \wedge R(x,y)) \supset R(u,u))$

次に，対象定数 a, b を導入し，(2) の存在冠頭論理式を作る．

(3) $\exists x \exists v \exists w \exists z (((R(v,w) \supset R(w,v)) \wedge ((R(v,w) \wedge R(w,z)) \supset R(v,z)) \wedge R(x,b)) \supset R(a,a))$

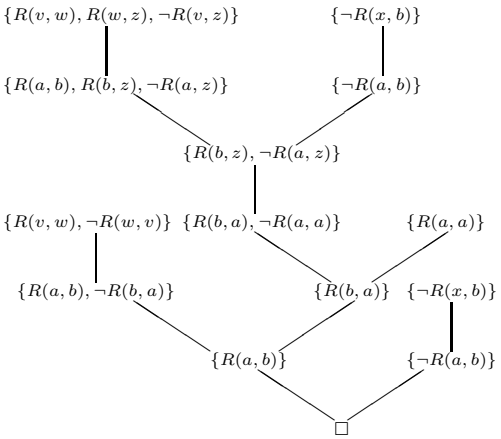
さらに (3) の量化記号を取り除いた部分を論理和標準形にする．

(4) $\exists x \exists v \exists w \exists z ((R(v,w) \wedge \neg R(w,v)) \vee (R(v,w) \wedge R(w,z) \wedge \neg R(v,z)) \vee \neg R(x,b) \vee R(a,a))$

ここで，(4) から節集合 S をつぎのように定める．

$\{R(v,w), \neg R(w,v)\}$, $\{R(v,w), R(w,z), \neg R(v,z)\}$, $\{\neg R(x,b)\}$, $\{R(a,a)\}$

このようにして定められた S に対し，下のような S から $\square$ に到る導出図を作ることができるので，定理 4.1 より (1) は恒真になることがわかる．



参考文献

[1] 小野寛晰:情報科学における論理, 日本評論社 (1994).