

論理学

第11回「エルブランの定理」

萩野 達也

hagino@sfc.keio.ac.jp

前回まで

- 命題論理
 - 論理結合子 (\wedge , \vee , \rightarrow , \neg)
 - 真理値表
 - トートロジー
 - 標準形
 - 公理と証明
 - LK体系とNK体系
 - 健全性と完全性
- 述語論理
 - 述語論理式 (言語, 項)
 - 量化記号 ($\forall x P(x)$, $\exists x P(x)$)
 - 閉じた論理式 (束縛変数, 自由変数)
 - 述語論理の意味 (構造)
 - 恒真な論理式
 - 冠頭論理式
 - 述語論理のLK体系
 - 健全性と完全性

述語論理で書いてみよう

- 述語 N, P, D を以下のようにする.
 - $N(x) =$ 「 x は自然数である ($1, 2, 3, 4, \dots$)」
 - $P(x) =$ 「 x は素数である」
 - $D(x, y) =$ 「自然数 x は自然数 y で割り切れる」=「 y は x の約数」
 - $x < y =$ 「自然数 x は自然数 y より小さい」
- 関数 g, l を以下のようにする.
 - $g(x, y) =$ 「自然数 x と自然数 y の最大公約数」
 - $l(x, y) =$ 「自然数 x と自然数 y の最小公倍数」

- 次の文章を述語論理式として書きなさい.

1. 素数は自然数である.

$$\forall x(P(x) \rightarrow N(x))$$

2. 素数は自らと1以外では割り切れない.

$$\forall x \forall y (P(x) \wedge D(x, y) \rightarrow (y = 1) \vee (y = x))$$

3. 素数は無限にある. (i.e. いくらでも大きな素数がある.)

$$\forall x \exists y (N(x) \rightarrow (x < y) \wedge P(y))$$

4. 2より大きな素数は奇数である. (奇数=2で割り切れない.)

$$\forall x (P(x) \wedge (2 < x) \rightarrow \neg D(x, 2))$$

つづき

5. 最大公約数 $g(x, y)$ は x および y の約数である.

$$\forall x \forall y (N(x) \wedge N(y) \rightarrow D(x, g(x, y)) \wedge D(y, g(x, y)))$$

6. 最大公約数 $g(x, y)$ は x および y の約数の中で最も大きい.

$$\forall x \forall y \forall z (N(x) \wedge N(y) \wedge N(z) \rightarrow (D(x, z) \wedge D(y, z) \rightarrow (z = g(x, y)) \vee (z < g(x, y))))$$

7. 最小公倍数 $l(x, y)$ は x および y の倍数である.

$$\forall x \forall y (N(x) \wedge N(y) \rightarrow D(l(x, y), x) \wedge D(y, l(x, y)))$$

8. 最小公倍数 $l(x, y)$ は x および y の倍数の中で最も小さい.

$$\forall x \forall y \forall z (N(x) \wedge N(y) \wedge N(z) \rightarrow (D(z, x) \wedge D(z, y) \rightarrow (z = l(x, y)) \vee (l(x, y) < z)))$$

述語論理における証明の問題

- 命題論理における証明

- 与えられた論理式が証明可能か否かを判定するアルゴリズムが存在する.
- アルゴリズムとは有限の手続き

- 述語論理における証明

- 与えられた論理式が証明可能か否かを判定するアルゴリズムは存在しない.

- 部分的なアルゴリズムの存在

- 与えられた論理式が証明可能である場合には, 証明可能であることを示すことができる.
- 証明可能でない場合には, どうなるか分からない.
- 証明可能でないものを, あると判断することはない.

スコールム化

冠頭標準形

- 任意の論理式を $Q_1x_1 \cdots Q_nx_n A$ の形にすることができる
 - Q_1 は \forall または \exists の量化記号
 - A は量化記号を含まない
- \forall 同士や \exists 同士を交換しても意味は変わらないが、 \forall と \exists は一般には交換できない。
 - $\forall x \exists y A \not\equiv \exists y \forall x A$

$$\forall x_1 \cdots \forall x_n \exists y A$$

x_1 から x_n に対して y が存在

スコールム化

- $\forall x_1 \cdots \forall x_n \exists y A$
- $\exists y$ の y は x_1, \dots, x_n にしたがって決まる
- 決まり方を新しい関数記号 f で表す(スコールム関数)
- $\forall x_1 \cdots \forall x_n A[f(x_1, \dots, x_n)/y]$

- 定理: $\forall x_1 \cdots \forall x_n \exists y A$ が充足可能であることと、
 $\forall x_1 \cdots \forall x_n A[f(x_1, \dots, x_n)/y]$ が充足可能なことであることは同値である。

- 注意: $\forall x_1 \cdots \forall x_n \exists y A \not\equiv \forall x_1 \cdots \forall x_n A[f(x_1, \dots, x_n)/y]$

スコールム化の例

- $L(x, y)$ = 「 x は y が好き」, $S(x)$ = 「 x はSFCの学生」としたとき, 次の論理式をスコールム化しなさい.

1. $\forall x \exists y L(x, y)$

$$\forall x L(x, f(x))$$

2. $\exists x \forall y L(x, y)$

$$\forall y L(c, y)$$

3. $\exists x \exists y L(x, y)$

$$L(c, d)$$

4. $\forall x (\forall y L(x, y) \rightarrow S(x))$

$$\forall x (L(x, f(x)) \rightarrow S(x))$$

全称冠頭論理式

- 冠頭論理式においてスコールム化を繰り返すと、全称記号だけからなる冠頭論理式を得ることができる。
 - $\forall x_1 \cdots \forall x_n A$
 - A は量化記号を一つも含まない論理式
 - もとの論理式と充足可能性については同値
 - 全称冠頭論理式**と呼ぶ
- さらに A を論理積標準形に変形すると
 - $\forall x_1 \cdots \forall x_n \left((L_{11} \vee \cdots \vee L_{1k_1}) \wedge \cdots \wedge (L_{m1} \vee \cdots \vee L_{mk_m}) \right)$
 - L_{ij} はリテラル(述語あるいはその否定)
- 双対性から次の形にも変形することができる
 - $\exists x_1 \cdots \exists x_n \left((L_{11} \wedge \cdots \wedge L_{1k_1}) \vee \cdots \vee (L_{m1} \wedge \cdots \wedge L_{mk_m}) \right)$

節

- **節** (clause)
 - リテラル(述語あるいはその否定)を論理和で結合したもの
 - $L_1 \vee \dots \vee L_n$
 - L_i は述語 P または $\neg P$
- 述語論理式の節への分解
 1. 冠頭論理式に変換する.
 2. スコーレム化し, 全称冠論理式にする.
 3. 論理積標準形へ変換する.
 4. 論理積ごとに分ける.
- 述語論理式の充足可能性の問題は, 節の集合の充足可能性の問題に還元することができる.

節への変換例

- $\forall x \left(\forall y (P(x, y) \vee Q(y)) \rightarrow R(x) \right)$ を節に変換しなさい。

1. 冠頭論理式に変換する。

$$\forall x \exists y (P(x, y) \vee Q(y) \rightarrow R(x))$$

$$\forall x B \rightarrow A \equiv \exists x (B \rightarrow A)$$

2. スコーレム化し, 全称冠頭論理式にする。

$$\forall x \left(P(x, f(x)) \vee Q(f(x)) \rightarrow R(x) \right)$$

3. 論理積標準形へ変換する。

$$\sim \forall x \left(\neg \left(P(x, f(x)) \vee Q(f(x)) \right) \vee R(x) \right)$$

$$A \rightarrow B \equiv \neg A \vee B$$

$$\sim \forall x \left(\left(\neg P(x, f(x)) \wedge \neg Q(f(x)) \right) \vee R(x) \right)$$

$$\neg(A \vee B) \equiv \neg A \wedge \neg B$$

$$\sim \forall x \left(\left(\neg P(x, f(x)) \vee R(x) \right) \wedge \left(\neg Q(f(x)) \vee R(x) \right) \right)$$

$$A \wedge (B \vee C) \equiv (A \wedge B) \vee (A \wedge C)$$

4. 論理積ごとに分ける。

$$\neg P(x, f(x)) \vee R(x)$$

$$\neg Q(f(x)) \vee R(x)$$

エルブラン解釈

- 言語 L のエルブラン領域 (Herbrand universe) H_L
 - L の変数を含まない項 (基礎項) の集合
 - L が定数を含まないときには H_L が空集合となるため, 定数記号を L に付け加えてからエルブラン領域を作る.

- 高さを使ったエルブラン領域の定義

- $H_0 = \{c \mid L \text{の定数}\}$
- $H_{k+1} = H_k \cup \{f(t_1, \dots, t_n) \mid f \text{は} L \text{の} n \text{変数の関数記号, } t_1, \dots, t_n \in H_k\}$
- $H_L = H_\infty$

- エルブラン基底 (Herbrand basis)

- エルブラン領域の要素を引数とした原始論理式全体
- $\{P(t_1, \dots, t_n) \mid P \text{は} L \text{の} n \text{変数の述語記号, } t_1, \dots, t_n \in H_L\}$

- エルブラン解釈 (Herbrand interpretation)

- エルブラン基底の部分集合 J
- この部分集合に含まれる原始論式を真と考える

エルブランの定理

- 言語 L のエルブラン構造 (Herbrand structure) $\mu = \langle H_L, J \rangle$
 - 定数 $c: c^J = c$
 - 関数記号 $f: f^J(t_1, \dots, t_n) = f(t_1, \dots, t_n)$
 - 述語記号 $P: \mu \models P(t_1, \dots, t_n) \iff P(t_1, \dots, t_n) \in J$

エルブランの定理

- $\forall x_1 \cdots \forall x_n A$ を言語 L の全称冠頭論理式とする.
 - A は量化記号を含まない.
- 次の2つは同値である.
 - $\forall x_1 \cdots \forall x_n A$ が充足不可能である.
 - ある自然数 m と H_L の項 t_{i1}, \dots, t_{in} ($i = 1, \dots, m$) が存在し,

$$A[t_{11}/x_1, \dots, t_{1n}/x_n] \wedge \cdots \wedge A[t_{m1}/x_1, \dots, t_{mn}/x_n]$$

がどのエルブラン構造 L においても充足可能でない.

エルブラン構造とは

- エルブラン構造

- 定数や関数記号に解釈を特に与えず, 記号のままあつかう.
- 述語記号だけの解釈を与える. 十分である.

- 特徴

- 定数や関数記号の解釈は述語の解釈に任せる.
- 任意の解釈(定数や関数記号の解釈を含む)に対応してエルブラン構造での解釈を作ることができる.
- 論理式の真偽に関してはエルブラン構造を考えるだけで十分である.

エルブランの定理の適用例

- $\forall x \exists y (P(x) \wedge \neg P(y))$ が充足不可能なことをエルブランの定理を使って示す.
 1. 全称冠頭論理式に変換する: $\forall x (P(x) \wedge \neg P(f(x)))$
 2. エルブラン領域: $H = \{c, f(c), f(f(c)), f(f(f(c))), \dots\}$
 3. $P(x) \wedge \neg P(f(x))$ の x に c を代入すると, $P(c) \wedge \neg P(f(c))$ であるが, これは充足可能である.
 4. $P(x) \wedge \neg P(f(x))$ の x に $f(c)$ を代入したものと, 3の論理式との論理積は

$$(P(c) \wedge \neg P(f(c))) \wedge (P(f(c)) \wedge \neg P(f(f(c))))$$

$\neg P(f(c))$ と $P(f(c))$ を同時に真とするエルブラン解釈は存在しないため充足不可能である.
 5. エルブランの定理から $\forall x \exists y (P(x) \wedge \neg P(y))$ は充足不可能である.
- この論理式が充足不可能なことから, この論理式の否定は恒真である.
 - $\neg \forall x \exists y (P(x) \wedge \neg P(y))$ は恒真, すなわち
 - $\exists x \forall y (P(x) \rightarrow P(y))$ は恒真

節のエルブランの定理

- **基礎例** (ground instance)
 - 変数を含まない論理式あるいは節
- **エルブランの定理(節の場合)**
 - S を節の集合とするとき, 以下の2つは同値である.
 - S が充足不可能である.
 - S から得られる基礎例の有限集合で充足不可能なものがある.
- 述語論理式 A が恒真であることを証明する部分アルゴリズム
 1. $\neg A$ を節の集合 S に変換する.
 2. エルブラン空間 H_0 の要素を代入してできた基礎例 S_0 が充足不可能か調べる (S_0 は有限集合).
 3. H_1 の要素を代入してできた基礎例 S_1 が充足不可能か調べる.
 4. H_2 の要素を代入してできた基礎例 S_2 が充足不可能か調べる.
 5. . . .
 6. これを繰り返し H_k の場合に充足不可能なことが分かれば, アルゴリズムを停止する.

エルブランの定理の双対形

- A が恒真であることと $\neg A$ が充足不可能なことが同値なので、エルブランの定理を双対的に言い直すことができる。

エルブランの定理 (双対系)

- $\exists x_1 \cdots \exists x_n A$ を言語 L の存在冠頭論理式とする.
 - A は量化記号を含まない.
- 次の2つは同値である.
 - $\exists x_1 \cdots \exists x_n A$ が恒真である.
 - ある自然数 m と H_L の項 t_{i1}, \dots, t_{in} ($i = 1, \dots, m$) が存在し,

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

がどのエルブラン構造 L においても真になる。

まとめ

- 証明
 - 命題論理の証明は自動的に行なうアルゴリズムがある
 - 述語論理には存在しない
- スコーレム化
 - 全称冠頭論理式
 - 節への変換
- エルブランの定理
 - エルブラン領域・解釈・構造
 - 全称冠頭論理式の充足不可能性を示す部分アルゴリズム