

『論理と形式化』試験問題と解答例

2014 年 6 月 27 日 (金)

問題 1. 以下の論理式のうち NK の定理であるものは証明し，そうでないものはその論理式を偽とする解釈を 1 つ与えなさい.

(a) $((A \supset B) \vee (A \supset C)) \supset (A \supset (B \wedge C))$

答. NK の定理でないので，偽とする解釈 (の 1 つ) を与える .

解釈 I のもとでの論理式 A の真偽値を $I[A]$ と書く . $I[A] = I[B] = \text{真}$, および , $I[C] = \text{偽}$ とすると , $I[((A \supset B) \vee (A \supset C)) \supset (A \supset (B \wedge C))]$ = 偽となる .

(b) $((A \supset B) \wedge (A \supset C)) \supset (A \supset (B \wedge C))$

答. NK の定理であるので，証明 (の 1 つ) を与える .

$$\frac{\frac{\frac{(A \supset B) \wedge (A \supset C)}{A \supset B} 1}{A \supset B} 2 \quad \frac{\frac{(A \supset B) \wedge (A \supset C)}{A \supset C} 1}{A \supset C} 2}{\frac{B \quad C}{B \wedge C} 2} 1$$

(c) $((A \supset B) \vee (A \supset C)) \supset (A \supset (B \vee C))$

答. NK の定理であるので，証明 (の 1 つ) を与える .

$$\frac{\frac{\frac{(A \supset B) \vee (A \supset C)}{A \supset B} 1 \quad \frac{\frac{A \supset B}{B} 3}{B \vee C} 2}{\frac{B \vee C}{A \supset (B \vee C)} 2} 3$$

(d) $(\forall x F(x)) \supset (\neg \forall x \neg F(x))$

答. NK の定理であるので，証明 (の 1 つ) を与える .

$$\frac{\frac{\frac{\forall x \neg F(x)}{\neg F(x)} 2}{\perp} 1}{\frac{\neg \forall x \neg F(x)}{(\forall x F(x)) \supset (\neg \forall x \neg F(x))} 2} 1$$

(e) $(\forall x F(x)) \supset (\neg \exists x \neg F(x))$

答. NK の定理であるので，証明 (の 1 つ) を与える .

$$\frac{\frac{\frac{\forall x F(x)}{F(a)} 1}{\neg F(a)} 3}{\frac{\exists x \neg F(x)}{\perp} 2} 3$$

問題 2. 以下の H1,H2,H3,H4 から構成される Prolog プログラムについて考える . X, Y, Z は変数、 0 は定数 , s は関数記号, p と r は述語記号である。

```
H1  r( 0,    Y).
H2  r(s(X), s(Y)) :- r(X, Y).
H3  p(X, Y, X)    :- r(X, Y).
H4  p(X, Y, Y)    :- r(Y, X).
```

(2-a) ホーン節 H1 は、 $\forall X(r(0, X))$ という論理式を表す。同様に、ホーン節 H2 が表す論理式を一階述語論理の論理式として書きなさい。

答. $\forall X \forall Y (r(X, Y) \supset r(s(X), s(Y)))$.

(2-b) 上記のプログラムに対して、以下のゴールを Prolog システムで実行した時、得られる解 (複数の解がある時はその全て) を示しなさい。

(2-b-1) ?- $r(s(s(0)), s(0))$.

答. false を返す .

補足. 導出を行なう . $\{r(s(s(0)), s(0))\} \rightarrow (H2) \rightarrow \{r(s(0), 0)\}$ となり、これ以上はマッチする Horn 節が 1 つもないので失敗する (false を返す) .

ここで、 $G1 \rightarrow (H2) \rightarrow G2$ は、ゴール $G1$ に対して Horn 節 H2 を使ってゴール $G2$ を得たことを表す .

(2-b-2) ?- $r(s(0), s(s(0)))$.

答. true を返す .

補足. 導出を行なうと、 $\{r(s(0), s(s(0)))\} \rightarrow (H2) \rightarrow \{r(0, s(0))\} \rightarrow (H1) \rightarrow \{\}$ となり、ゴールが空集合となるので成功する (true を返す) .

(2-b-3) ?- $p(s(s(0)), s(0), Z)$.

答. true で $Z=s(0)$ を返す .

補足. 導出を行なう .

$\{p(s(s(0)), s(0), Z)\} \rightarrow (H3; X=s(s(0)), Y=s(0), Z=X) \rightarrow \{r(s(s(0)), s(0))\} \rightarrow (H2) \rightarrow \{r(s(0), 0)\}$

となり、ここでは失敗する . 次の導出を行なうと、

$\{p(s(s(0)), s(0), Z)\} \rightarrow (H4; X=s(s(0)), Y=s(0), Z=Y) \rightarrow \{r(s(0), s(s(0)))\} \rightarrow (H2) \rightarrow \{r(0, s(0))\} \rightarrow (H1) \rightarrow \{\}$

となる . ここで最初のゴールに含まれる Z は $s(0)$ である . なお、これ以外に導出できるものはないので、上記の解以外にはない .

(2-b-4) ?- $p(s(s(0)), s(s(0)), Z)$.

答. true で $Z=s(s(0))$ という解を 2 回返す . (なお、問題文では「まったく同じ解を 2 回以上返すときに、どう書けばよいか」について曖昧であったので「2 回返す」ということを明示しない答案でも正解とした。「2 回返す」ところまで書いてある答案は加点した。)

補足. 導出を行なう .

$\{p(s(s(0)), s(s(0)), Z)\} \rightarrow (H3; X=s(s(0)), Y=s(s(0)), Z=X) \rightarrow \{r(s(s(0)), s(s(0)))\} \rightarrow (H2) \rightarrow \{r(s(0), s(0))\} \rightarrow (H2) \rightarrow \{r(0, 0)\} \rightarrow (H1) \rightarrow \{\}$

となり、ここで true と $Z=s(s(0))$ を返す . 次の導出を行なうと、

$\{p(s(s(0)), s(s(0)), Z)\} \rightarrow (H4; X=s(s(0)), Y=s(s(0)), Z=Y) \rightarrow \{r(s(s(0)), s(s(0)))\} \rightarrow (H2) \rightarrow \{r(s(0), s(0))\} \rightarrow (H2) \rightarrow \{r(0, 0)\} \rightarrow (H1) \rightarrow \{\}$

となり、再び true と $Z=s(s(0))$ を返す . 次の導出はない .

- (2-c) 上記のプログラム中の 0 は自然数の 0 で、 s は「1 を加える関数」であると考えた時、述語 r と p は、それぞれ、どういう関係を表すか言葉で簡潔に述べなさい。

答. 述語 r は第 1 引数が第 2 引数と同じか小さいことを表す. ($r(X,Y)$ は $X \leq Y$ を表す.)
 述語 p は第 3 引数が、第 1 引数と第 2 引数の最小値であることを表す. ($p(X,Y,Z)$ は $Z = \min(X,Y)$ を表す.)

- (2-d) 成功する解 (true を返す解) は、NK の証明に対応する。上記の (2-b) のゴールを走らせた時に成功する解の 1 つについて、対応する NK の証明を書きなさい。

答. (2-b-2) の解に対応する証明を以下に記載する .

$$\frac{\frac{H2 = \forall X \forall Y (r(X,Y) \supset r(s(X),s(Y)))}{\forall Y (r(0,Y) \supset r(s(0),s(Y)))} \quad \frac{H1 = \forall Y r(0,Y)}{r(0,s(0))}}{\frac{r(0,s(0)) \supset r(s(0),s(s(0)))}{r(s(0),s(s(0)))}}$$

- (2-e) 上記の (2-b-1),(2-b-2) のうち有限的に失敗する (成功する解が 1 つもない) ゴールを G とする。 $H1$, $H2$ に対応する論理式を真とし、 G に対応する論理式を偽とする解釈 I を示しなさい。(これらの論理式に述語 p は含まれないので、 p の解釈は与えなくてよい。)

答. (2-b-1) の解に対応する解釈 (それを偽とする解釈) を以下に記載する .

領域 D を自然数の集合 $\mathbb{N}$ とし、 $I[0] = 0$, $I[s]$ を $\mathbb{N}$ における「1 を加える関数」とする . $I[r]$ は、以下の関数 f とする .

$$f(m,n) = \begin{cases} \text{真} & \text{if } m \leq n \\ \text{偽} & \text{if } m > n \end{cases}$$

このように置くと、 $H1$ に対応する論理式 $\forall Y (r(0,Y))$ と、 $H2$ に対応する論理式 $\forall X \forall Y (r(X,Y) \supset r(s(X),s(Y)))$ が両方とも真になり、一方、 (2-b-1) に対応する論理式 $r(s(s(0)),s(0))$ が偽になることがわかる .

- (2-f) (ボーナス問題; 時間が余った人のみ) 自然数 X,Y の最大公約数 (greatest common divisor) が Z であるという関係 $\text{gcd}(X,Y,Z)$ を Prolog のプログラムとして実現せよ。

答. 一例は以下の通りである .

```
sub(X,0,X).
sub(s(X),s(Y),Z) :- sub(X,Y,Z).
gcd(0,X,X).
gcd(X,0,X).
gcd(s(X),s(Y),Z) :- r(X,Y), sub(Y,X,W), gcd(s(X), W, Z).
gcd(s(X),s(Y),Z) :- r(Y,X), sub(X,Y,W), gcd(W, s(Y), Z).
```

補足. $\text{sub}(X,Y,Z)$ は $X-Y=Z$ を表す述語である (授業で定義した add を使って定義することもできる。)

上記の gcd は「エラトステネスのふるい」のアルゴリズムをベースにした実装である . なお、上記の実装では、 $\text{gcd}(X,X,Z)$ というゴールに対して、5 行目と 6 行目の両方がマッチしてしまい、同じ計算を 2 回してしまう . これを避けるためには、 $X < Y$ を意味する $\text{lessthan}(X,Y)$ という述語を定義すればよい . (それでも $X < Y$ と $Y \leq X$ をそれぞれ計算しに行くので、効率が良いとは言いがたい . これを避けるため、「条件 C が成立する場合は、こちらを実行し、不成立の場合はあちらを実行する」という if-then-else のような

処理が欲しくなり、実際の Prolog 処理系は、そのような機能を持っている。しかし、このような機能をいれてしまうと、論理との対応が悪くなることも知られている。）