情報論理試験 2005 年 9 月 28 日 略解

1. P と Q を一引数の述語とする。

(1) A は一階述語論理の閉じた論理式で、関数記号を含まず述語記号としては P と Q のみを含むとする。A が充足可能であるとき、A を充足する解釈をもとにして、A を充足する解釈で領域が有限のものを与えよ。

(略解) A を充足する解釈 I の領域を D とする。D 上に同値関係 $\equiv$ を次のように定義する。

$$d_1 \equiv d_2 \ \ \textbf{iff} \ \ I(P)(d_1) = I(P)(d_2) \ \textbf{and} \ I(Q)(d_1) = I(Q)(d_2)$$

すると、$\equiv$ の同値類は高々4 個である。I をもとに $D/\equiv$ を領域とする解釈 $[I]$ を定義する。

$$\begin{aligned} [I](P)([d]) &= I(P)(d) \\ [I](Q)([d]) &= I(Q)(d) \end{aligned}$$

関数記号を含まず述語記号としては P と Q のみを含む論理式 B に対して、

$$[\![B]\!]_{I,J} = [\![B]\!]_{[I],[J]}$$

が成り立つ (論理式の構成に関する帰納法)。ただし、J は変数への D の要素の割り当てで、変数への $D/\equiv$ の要素の割り当て $[J]$ は、

$$[J](x) = [J(x)]$$

と定義される。

(2) A は一階述語論理の閉じた論理式で、関数記号を含まず述語記号としては P と Q と等号 $=$ のみを含むとする。等号 $=$ は、領域上の等しさによって解釈する。特に、A は $\forall x_1.\exists x_2.A'[x_1, x_2]$ という形とする。ただし、$A'[x_1, x_2]$ は $\forall$ も $\exists$ も含まず、変数は x_1, x_2 のみ。この場合も、A が充足可能であるときに、A を充足する解釈で領域が有限のものを与えよ。

(略解) (1) と同じく $\equiv$ を定義し $D/\equiv$ を求め、$D' = (D/\equiv) \times \{0, 1\}$ とおく。すると、D' の要素の数は高々8 である。D' 上の解釈 I' を、

$$\begin{aligned} I'(P)(\langle [d], i\rangle) &= I(P)(d) \\ I'(Q)(\langle [d], i\rangle) &= I(Q)(d) \end{aligned}$$

と定める。A は I によって充足されるので、任意の $d_1 \in D$ に対して $A'[d_1, d_2]$ を満たす $d_2 \in D$ が存在する。このとき、任意の $\langle [d_1], i \rangle \in D'$ に対して、$A'[\langle [d_1], i \rangle, \langle [d_2], j \rangle]$ が成り立つ。ただし、$d_1 = d_2$ ならば $j = i$ とし、$d_1 \neq d_2$ ならば $j = 1 - i$ とする。

2. 以下は一階述語論理のコンパクト性に関する文章である。途中の (1)(2)(3) が成り立つ理由を簡単に数行で説明せよ。

Γ を一階述語論理の閉じた論理式の集合とする。$\Gamma = \{A_i \mid i \in I\}$ とおく。Γ の任意の有限部分集合が充足可能であると仮定する。このとき、Γ が充足可能であることを示したい。

Γ の論理式 A_i を個別に Skolem 化した結果を、$\forall x_1. \cdots .\forall x_{n_i}.A'_i[x_1, \cdots, x_{n_i}]$ とする。($A'_i[x_1, \cdots, x_{n_i}]$ は $\forall$ も $\exists$ も含まず、変数は $x_1, \cdots, x_{n_i}$ のみ。Skolem 関数は A_i ごとに個別に用意する。) $A'_i[x_1, \cdots, x_{n_i}]$ を具体化して得られる閉じた論理式の全体 $\{A'_i[t_1, \cdots, t_{n_i}] \mid i \in I,\ t_1, \cdots, t_{n_i} :$ 閉じた項$\}$ を Γ_0 とおく。

(1) Γ_0 が充足可能ならば Γ は充足可能である。

> (解の例) Γ_0 に含まれる定数記号と関数記号から作られる Herbrand 領域の上で、Γ_0 を充足する解釈は Γ も充足する。

従って、Γ が充足不能ならば Γ_0 は充足不能である。

(2) Γ_0 が充足不能ならば、Γ_0 の有限部分集合 Δ_0 で充足不能なものが存在する。

> (解の例) Γ_0 が無矛盾 (任意の有限部分集合が充足可能) であるとすると、Γ_0 を含む無矛盾集合の全体は帰納的な順序集合となる。Zorn の補題により、Γ_0 を含む極大無矛盾集合が存在する。この極大無矛盾集合は、Γ_0 を充足する解釈を与える。

Δ_0 の各要素 $A'_i[t_1, \cdots, t_{n_i}]$ に $i \in I$ を一つずつ対応させ、そのような i の全体を J とおく。J は有限である。$\Delta = \{A_i \mid i \in J\}$ とおく。

(3) Δ_0 が充足不能なので Δ は充足不能である。

> (解の例) Δ が充足可能であるとすると、Δ を充足する解釈に Skolem 関数の解釈を追加することにより、Δ_0 を充足する解釈を得ることができる。

以上により、Γ が充足不能ならば、Γ の有限部分集合 Δ で充足不能なものが存在することがわかった。

3. 一階述語論理において、閉じた論理式 $\forall x.\exists y.A[x,y]$ を Skolem 化した結果を $\forall x.A[x,f(x)]$ とする。$A[x,y]$ は $\forall$ も $\exists$ も含まない。いま、$A[c,f(c)]\wedge A[f(c),f(f(c))]$ は充足不能であると仮定する。u と v を $A[x,y]$ に現れない新しい変数とする。

(1) $\neg A[c,u]\vee\neg A[u,v]$ がトートロジーである理由を簡単に述べよ。(ここでトートロジーとは、命題論理のトートロジーの各命題記号を論理式で置き換えたものをいう。)

> (略解) $\neg A[c,u]\vee\neg A[u,v]$ がトートロジーでないとすると、これを偽にする命題論理における解釈が存在する。この解釈をもとに、述語記号と関数記号の解釈および変数 u と v への割り当てを定めることにより、述語論理において $\neg A[c,u]\vee\neg A[u,v]$ を偽にする解釈と割り当てを得ることができる。(例えば、u と v を定数と見做して Herbrand 解釈を求め、変数 u の値は u 自身、変数 v の値は v 自身とすればよい。) さらに、$f(c)$ の解釈を u の値、$f(f(c))$ の解釈を v の値とすれば、$\neg A[c,f(c)]\vee\neg A[f(c),f(f(c))]$ を偽にする解釈が得られる。この解釈のもとで $A[c,f(c)]\wedge A[f(c),f(f(c))]$ は真になる。これは仮定に反する。

(2) 適当な演繹体系 (例えばシーケント計算、ヒルベルト流) のもとで、$\neg A[c,u]\vee\neg A[u,v]$ が証明できることを仮定して、論理式 $\exists x.\forall y.\neg A[x,y]$ が証明できることを説明せよ。(束縛変数の名前を付け替えて一致する論理式は同一視する。また、括弧の付け方に関して、例えば $(\forall x.A\vee B[x])\supset A\vee(\forall x.B[x])$ は $(\forall x.(A\vee B[x]))\supset(A\vee(\forall x.B[x]))$ に同じであることを注意しておく。)

シーケント計算による場合は、シーケント $\to\neg A[c,u],\neg A[u,v]$ が証明できると仮定して、シーケント $\to\exists x.\forall y.\neg A[x,y]$ を証明せよ。

> (略解 — シーケントの場合)

$$
\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\to\neg A[c,u],\neg A[u,v]}{\to\neg A[c,u],\forall v.\neg A[u,v]}}{\to\neg A[c,u],\exists u.\forall v.\neg A[u,v]}}{\to\forall u.\neg A[c,u],\exists u.\forall v.\neg A[u,v]}}{\to\exists z.\forall u.\neg A[z,u],\exists u.\forall v.\neg A[u,v]}}{\to\exists u.\forall v.\neg A[u,v]}
$$

ヒルベルト流による場合は、以下にあげる公理と推論規則を用いてよい。

公理:

- トートロジー
- $(\forall x.A\vee B[x])\supset A\vee(\forall x.B[x])$ という形の論理式 (A には x は自由に現れない)

- $(\forall x.A[x] \lor B) \supset (\forall x.A[x]) \lor B$ という形の論理式 (B には x は自由に現れない)
- $A[t] \supset (\exists x.A[x])$ という形の論理式 (t は任意の項)

推論規則:

- $A[x]$ から $\forall x.A[x]$ を導くことができる (汎化)。
- A と $A \supset B$ から B を導くことができる (MP)。

  (略解 — ヒルベルト流の場合) $\neg A[c,u] \lor \neg A[u,v]$ に対する汎化により、$\forall v.\neg A[c,u] \lor \neg A[u,v]$ が証明できる。公理と MP により、$\neg A[c,u] \lor (\forall v.\neg A[u,v])$ が得られる。これと、公理 $(\forall v.\neg A[u,v]) \supset (\exists u.\forall v.\neg A[u,v])$、および、トートロジー $(\neg A[c,u] \lor (\forall v.\neg A[u,v])) \supset (((\forall v.\neg A[u,v]) \supset (\exists u.\forall v.\neg A[u,v])) \supset (\neg A[c,u] \lor (\exists u.\forall v.\neg A[u,v])))$ より、MP を二回使って、$\neg A[c,u] \lor (\exists u.\forall v.\neg A[u,v])$ が得られる。ここで $\exists u.\forall v.\neg A[u,v]$ に u は自由に現れないので、同様にして、$(\exists w.\forall u.\neg A[w,u]) \lor (\exists u.\forall v.\neg A[u,v])$ が得られる。$(\exists w.\forall u.\neg A[w,u]) \lor (\exists u.\forall v.\neg A[u,v]) \supset (\exists u.\forall v.\neg A[u,v])$ はトートロジーであるから、MP より、$\exists u.\forall v.\neg A[u,v]$ が得られる。

4. 命題論理の導出原理において、否定の付かないリテラルを正リテラル、否定の付くリテラルを負リテラルと呼ぶ。正リテラルをちょうど一つ含む節を確定節という。節 $C \lor P$ と節 $D \lor \neg P$ から節 $C \lor D$ を得る導出を、節 $C \lor P$ の正リテラル P と節 $D \lor \neg P$ の負リテラル $\neg P$ に対する導出という。以下の問に答えよ。

(1) 確定節と確定節から導出によって得られる節も確定節であることを示せ。

> (略解) $\neg P_1 \lor \cdots \lor \neg P_m \lor P'$ と $\neg Q_1 \lor \cdots \lor \neg Q_n \lor Q'$ に対して導出が行えるとすると、P' がある Q_j に等しいか、Q' がある P_i に等しい。前者の場合、$\neg P_1 \lor \cdots \lor \neg P_m \lor \neg Q_1 \lor \cdots \lor \neg Q_{j-1} \lor \neg Q_{j+1} \lor \cdots \lor \neg Q_n \lor Q'$ が得られるが、これも確定節である。後者の場合も同様。

(2) S を確定節の集合とする。S に属する節を入力節と呼び、S の節から始まる導出を考える。入力節の正リテラルと (入力節とは限らない) 確定節の負リテラルに対する導出を正入力導出と呼ぶ。S の節から正入力導出のみを用いて確定節 D が得られるとき、D と同じ正リテラルを持つ入力節 D_0 と入力節 $C_0, \cdots, C_{n-1}$ が存在して、以下が成り立つことを示せ。C_i の正リテラルと D_i の負リテラルに対して正入力導出が行われ、D_{i+1} が得られる $(0 \leq i < n)$。そして、D_n は D に等しい。

(略解) Dが入力節ならばDをD_0とすればよい($n=0$)。そうでなければ、Dから正入力導出を逆に遡る。入力節Cの正リテラルと確定節D'の負リテラルに対して正入力導出が行われ、Dが得られたとする。D'とDは同じ正リテラルを持つ。D'が入力節ならばD'をD_0とすればよい($n=1$)。そうでなければ、同様にD'から正入力導出を逆に遡る。

(3) Sから確定節Dが導出されるとき、正入力導出のみを用いて確定節Dが得られることを示せ。(正確には、DもしくはDから負リテラルをいくつか除いた節が得られる。)

(略解) 導出の回数に関する帰納法。D'の正リテラルPとD''の負リテラル$\neg P$に対して導出が行われ、Dが得られたとする。帰納法の仮定により、D'とD''の正入力導出が存在する。D'の正入力導出において、前問により、Pを持つ入力節D_0と入力節$C_0, \cdots, C_{n-1}$が存在する。D_0の正リテラルPとD''の負リテラル$\neg P$に対して正入力導出を行った結果をD'''とおく。D'''と$C_0, \cdots, C_{n-1}$とを次々と導出すると、D(もしくはDから負リテラルをいくつか除いた節)を得ることができる。以上はすべて正入力導出である。

5. $T(e,x,y)$をKleeneの述語とする。すなわち、インデックスeのチューリング機械が入力xに対して停止する計算過程を符号化したものがyであるとき、$T(e,x,y)=0$となり、そうでないとき$T(e,x,y)=1$となる。なお、自然数xに対して、$\overline{x}$はsuccessor 関数Sをx個含む$S(\cdots(S(0))\cdots)$という形の項を表す。

いま、一階の算術において、論理式$A_T[e,x,y,z]$がTを表現すると仮定する。すなわち、以下が成り立つことを仮定する。

$T(e,x,y)=0$ならば$A_T[\overline{e},\overline{x},\overline{y},0]$が証明でき、$T(e,x,y)=1$ならば$A_T[\overline{e},\overline{x},\overline{y},S(0)]$が証明できる。さらに、$\forall e.\forall x.\forall y.\forall z_1.\forall z_2.\ A_T[e,x,y,z_1] \wedge A_T[e,x,y,z_2] \supset z_1=z_2$が証明できる。

(1) インデックスeのチューリング機械が入力xに対して停止するならば、一階の算術において$\exists y.A_T[\overline{e},\overline{x},y,0]$という論理式は証明可能であることを説明せよ。

(略解) インデックスeのチューリング機械が入力xに対して停止するならば、あるyが存在して、$T(e,x,y)=0$が成り立つ。従って、表現可能性より、$A_T[\overline{e},\overline{x},\overline{y},0]$が証明できる。従って、$\exists y.A_T[\overline{e},\overline{x},y,0]$が証明可能である。

(2) インデックスeのチューリング機械が入力xに対して停止しない場合、一階の算術において、必ずしも$\neg\exists y.A_T[\overline{e},\overline{x},y,0]$は証明可能であるとは限らないことを説明せよ。

(略解) $\neg\exists y.A_T[\overline{e},\overline{x},y,0]$ が証明可能であるとすると、論理式が証明可能かどうかは帰納的に可算であるので、インデックス e のチューリング機械が入力 x に対して停止しないような組 $\langle e,x\rangle$ の全体は帰納的に可算になる。ところが、インデックス e のチューリング機械が入力 x に対して停止するような組 $\langle e,x\rangle$ の全体も帰納的に可算であるので、どちらも帰納的になってしまう。これは、チューリング機械の停止性が判定できないことに矛盾する。

6. 様相論理の Kripke 構造 $\langle S,R,I\rangle$ において、S 上の二項関係 R は推移的であるとする。任意の論理式 A と任意の状態 s に対して、$s\models\Box A\supset\Box\Box A$ が成り立つことを示せ。

(略解) $s\models\Box A$ と仮定する。いま、sRs' かつ $s'Rs''$ とする。R は推移的なので sRs'' が成り立つ。従って、仮定より、$s''\models A$ が成り立つ。s'' は任意なので、$s'\models\Box A$ が成り立つ。s' も任意なので、$s\models\Box\Box A$ が成り立つ。従って、$s\models\Box A\supset\Box\Box A$ が成り立つ。