2007 年度 応用数学 XF レポート課題

自然数全体のなす半環を $(\mathbb{N}; +, \times)$ と書く. その中で正しい論理式の集合が決定不可能であることを示そう. すなわち, 自然数論に関する命題が与えられたとき, それが真であるかどうかを判定するのは不可能であるということを示す. 一応, 考えている論理式の範囲を明確にしておこう. 項として許されているのは, 変数と定数 $0, 1, 2, \ldots$ から演算子 $+, \times$ を組み合わせて作られるものだけである. それ以外の関数記号を使ってはいけない. 述語記号としては, $s = t$ と $s < t$ (ここで, s, t は任意の項) のみとする. これら二つの形の論理式を原始論理式という. 考えている論理式は, 原始論理式から初めて, 論理積 $\varphi \wedge \psi$, 論理和 $\varphi \vee \psi$, 否定 $\neg\varphi$, および 2 種類の量化子 $\forall x.\varphi$ と $\exists x.\varphi$ を組み合わせてできるものである.

決定不能性の証明は, Turing 機械の停止性問題を還元することで示す. すなわち, Turing 機械 M と入力文字列 w の組に対して, 論理式 $\varphi_{M,w}$ を対応させて, 「$M(w)$ が停止する」$\Leftrightarrow$ 「$\varphi_{M,w}$ が正しい」となるようにする. Turing 機械としては, $M = (Q, \Sigma, \delta, q_{init}, q_{acc})$ の形で, 遷移関数は $Q \times (\Sigma \cup \{\#\}) \xrightarrow{\delta} Q \times \Sigma \times \{L, R\}$ なるものを対象とする. まずは簡単な準備から始める.

(1) $\langle m, n\rangle := (m+n)(m+n+1)/2 + m$ で定義される関数は, $\mathbb{N} \times \mathbb{N}$ から $\mathbb{N}$ の上への全単射であることを示せ. 自然数 $\langle m, n\rangle$ の値が小さい順に並べると, どのような順序になるかを考えればよい.

ここで, 2 で割ることは論理式として許されていないが, $\langle m, n\rangle = x$ は $(m+n)(m+n+1) + 2m = 2x$ と同値なので, 必要に応じてこのように書き換えることで, 足し算とかけ算のみで表現できる. また, 射影関数 $\pi\langle m, n\rangle = m$ および $\pi'\langle m, n\rangle = n$ を考える. これらに関しても, たとえば, $\pi x = y$ のかわりに同値命題 $\exists n.\, x = \langle y, n\rangle$ で置き換えることで, 考えている論理式の範囲で記述できる.

まずは, Turing 機械の実行におけるコンフィギュレーションを自然数でコーディングする. アルファベット Σ は正の整数の有限集合 $\{1, 2, \ldots, r\}$ と同一視する. また, 空白記号 $\#$ は 0 と同一視する. Σ^* 内の文字列 $a_0 a_1 \cdots a_{n-1}$ は, $\langle a_0, \langle a_1, \ldots \langle a_{n-1}, 0\rangle \cdots\rangle\rangle$ でコーディングする. これを, $\langle a_0, a_1, \ldots, a_{n-1}\rangle$ と略記することにする. 空列は, 0 でコーディングされることになる. 射影関数 π と π' の組合せで, $\pi_0, \pi_1, \pi_2, \ldots$ を定義して, $\pi_i\langle a_0, a_1, \ldots, a_{n-1}\rangle = a_i$ が成り立つようにできる.

(2) アルファベットの元を正の整数に対応させた理由は何か. また, $i \geq n$ のとき, $\pi_i\langle a_0, a_1, \ldots, a_{n-1}\rangle$ の値はどうなるか.

状態集合 Q も適当に自然数の有限集合と同一視しておく. 標準的な手法

で, コンフィギュレーションを文字列で表しておくと都合がよい. 文字列 $a_0a_1\cdots qa_i\cdots a_{n-1}$ でもって, $(q,\, a_0a_1\cdots a_{n-1}, i) \in Q \times \Sigma^* \times \mathbb{N}$ を表現することにする. さらにこの文字列を, 自然数として $\langle u, q, a_i, v\rangle$ とコーディングする. ここで $u = \langle a_{i-1}, a_{i-2}, \ldots, a_0\rangle$ および $v = \langle a_{i+1}, a_{i+2}, \ldots, a_{n-1}\rangle$ である. u の方は, 逆順で並べていることに注意する.

(3) Turing 機械のヘッドは空白文字の上にくることもある. 遷移関数で空白文字は書き込めないことにしているので, このケースが起きるのは, テープの空白部分の一番左端にヘッドがくる場合である. このときのコンフィギュレーションの形と, それを表現する自然数はどのようになるか. そこからわかるように, コンフィギュレーションの表現 $\langle u, q, a_i, v\rangle$ においては成分が 0 になることがあるが, これは問題を引き起こさない. なぜか.

いよいよ, 論理式 $\varphi_{M,w}$ の設計を始める. まず, Turing 機械の実行 1 ステップ $\gamma \vdash \gamma'$ を表す論理式 $\varphi_{entail}(x, x')$ を定義する. これは, 有限論理和 $\bigvee_{(q,a)} E_{q,a}(x, x')$ として定義する. ここで, (q, a) は $Q \times (\Sigma \cup \{\#\})$ の上を走る. 論理式 $E_{q,a}(x, x')$ は以下のように, 場合分けで定義する. まず, $\delta(q, a) = (q', b, L)$ のときを扱う. 時刻 t でのコンフィギュレーションが,

$$\cdots\ u_2\ \ u_1\ \ u_0\ \ \ q\ \ \ a\ \ \ v_0\ \ v_1\ \ v_2\ \cdots$$

だとすると, 時刻 $t+1$ においては

$$\cdots\ u_2\ \ u_1\ \ \ q'\ \ u_0\ \ \ b\ \ \ v_0\ \ v_1\ \ v_2\ \cdots$$

となる. これらを自然数に対応させたとき, どのようになるか見てみると, $\langle u, q, a, v\rangle \rightsquigarrow \langle u', q', u_0, v'\rangle$ の形であり, u' は u の先頭の要素 u_0 を取り除いたもの, v' は v の先頭に b を付け足したものである. 論理式 $E_{q,a}(x, x')$ によって, $x = \langle u, q, a, v\rangle$ なおかつ $x' = \langle u', q', u_0, v'\rangle$ となっていることを表現したい. すなわち, $\pi_1 x = q$, $\pi_1 x' = q'$, $\pi_2 x = a$, $\pi_2 x' = \pi_0\pi_0 x$ ($\pi_0 x = u$ なので) がすべて成り立ち, さらに u と u' および v と v' の間に, 上に述べたような関係がある.

(4) これをヒントに, $E_{q,a}(x, x')$ を論理式として記述せよ. コンフィギュレーションのコーディング $\langle u, q, a, v\rangle$ で, u を逆順で並べたことの効果はどのようなことか.

(5) 次に, $\delta(q, a) = (q', b, R)$ のときを扱う. この場合に, 同様の考察を加えて, $E_{q,a}(x, x')$ を設計せよ.

次に, 論理式 $\varphi_{init}(x)$ を定義する. これは, x が初期コンフィギュレーションのコーディングであることを表す論理式である. 入力文字列 w が $a_0a_1\cdots a_{n-1}$ であるとすると, $\varphi_{init}(x)$ の定義は, $x = \langle 0, q_{init}, a_0, \langle a_1, a_2, \ldots, a_{n-1}\rangle\rangle$ とす

ればよい. 第一成分の 0 は空列のことである. また, 論理式 $\varphi_{acc}(x)$ を定義する. これは, x の表すコンフィギュレーションが受理状態 q_{acc} を含むことを表す論理式である. すなわち, $\varphi_{acc}(x)$ の定義は, $\pi_1 x = q_{acc}$ とすればよい.

定義からほぼ明らかなように,

$$\begin{array}{l}\varphi_{init}(\pi_0 z) \wedge \\ (\forall i < n.\, \varphi_{entail}(\pi_i z, \pi_{i+1} z)) \wedge \\ \varphi_{acc}(\pi_n z)\end{array}$$

が, ある自然数 n と z に対して成り立てば, $\pi_i z$ が表すコンフィギュレーション γ_i によって, 停止する実行 $\gamma_0 \vdash \gamma_1 \vdash \cdots \vdash \gamma_n$ が得られる.

(6) したがって,

$$\begin{array}{rcl}\varphi_{M,w} & = & \exists n \exists z.\, \varphi_{init}(\pi_0 z) \wedge \\ & & \quad (\forall i < n.\, \varphi_{entail}(\pi_i z, \pi_{i+1} z)) \wedge \\ & & \quad \varphi_{acc}(\pi_n z)\end{array}$$

と定義すればよいように思えるが, これは問題がある. どのようなことか.

したがって, π_i を使うことはあきらめて, 他の表現方法を考えないといけない. それが Gödel の β 関数を使う方法である. β 関数 $\beta(c, d, i)$ の定義はすぐ後で与えることにして, とにかく

$$\begin{array}{rcl}\varphi_{M,w} & = & \exists n \exists c \exists d.\, \varphi_{init}(\beta(c, d, 0)) \wedge \\ & & \quad (\forall i < n.\, \varphi_{entail}(\beta(c, d, i), \beta(c, d, i+1))) \wedge \\ & & \quad \varphi_{acc}(\beta(c, d, n))\end{array}$$

と定義する. β 関数 $\beta(c, d, i)$ は, 自然数 c を自然数 $1 + d \cdot (i + 1)$ で割った余りと定義する.

(7) $\beta(c, d, i) = x$ を論理式として記述せよ.

β 関数に関する重要な性質として示したいのは, 任意の n と任意の自然数列 $k_0, k_1, \ldots, k_n$ に対して,

$$\exists c \exists d.\, \forall i \leq n.\, \beta(c, d, i) = k_i$$

が成り立つことである. まず準備として,

(8) $1 + m! \cdot i$ $(i = 1, 2, \ldots, m + 1)$ が互いに素であることを示せ.

ここでは, m として $\max\{n, k_0, k_1, \ldots, k_n\}$ とする. また, $d = m!$ とする.

(9) このとき, $\exists c. \forall i \leq n.\, \beta(c, d, i) = k_i$ が成り立つことを示せ (ヒント: 中国人剰余定理). m を上のように取った理由は何か.

(10)　以上の考察を基に, $M(w)$ が停止することと, $\varphi_{M,w}$ が正しいことが同値であることを示せ.