アルゴリズム論 1

第 10 回: Turing 機械と計算可能な関数 (2)

関川 浩

2016/06/22

第 8 回から第 10 回の目標

計算可能性について, 正確な定義を与え, 基本的な性質を考察

第 8 回: 帰納的関数を導入

第 9 回: Turing 機械を導入し, 計算可能な関数を定義
帰納的関数は計算可能であることを証明

第 10 回: 計算可能な関数は帰納的であることを証明
万能 Turing 機械の紹介
Church の提唱の紹介

1. 計算の算術化
   - TM, 計算可能性の定義の変更
   - Goedel 数
   - 原始帰納的述語, 関数の準備
   - T_n は原始帰納的
2. 計算可能な関数は帰納的
   - 準備
   - 部分的に計算可能な関数は部分帰納的
   - 計算可能関数は帰納的
   - Kleene の標準形定理
   - 枚挙定理
3. 万能 Turing 機械
   - TM と万能 TM
   - 万能 TM の原理
   - アルゴリズムの定式化
   - Church の提唱

1. 計算の算術化
2. 計算可能な関数は帰納的
3. 万能 Turing 機械

TM, 計算可能性の定義の変更

議論を簡単にするため, TM および計算可能性の定義を変更

TM (K, Σ, Q, q_0, F) において, $F = \{q_h\}$ とする
(Q を $Q \cup \{qaaNq_h \mid q, q_h \in F, q \neq q_h\}$ で置き換え)

$(x_1, \ldots, x_n) = \mathbf{x}$ とする
関数 $f(\mathbf{x})$ が (部分的に) 計算可能であることの定義

$$\mathbf{x} \in \mathcal{D}(f) \iff (\overline{\mathbf{x}} q_0 B \overset{*}{\Rightarrow} \overline{(\mathbf{x}, f(\mathbf{x}))} q_h B)$$

の "$\overline{(\mathbf{x}, f(\mathbf{x}))}$" を "$\overline{f(\mathbf{x})}$" に変更
(今回は TM の結合や合成がないため, 入力 $\mathbf{x}$ の保存が不要)

古い定義における TM M に C (第 9 回で説明) を結合した TM MC を考えればよい

Gödel 数

- E: TM に関連した諸概念の表現 (記号, 記号列, . . .) の集合

  E の要素に自然数を対応させる

  $\Longrightarrow$ 帰納的関数や述語などに対応づけるため

- 以下の (1), (2), (3) を満たす対応づけ G を算術化または Gödel 数化といい, 数 $G(x)$ を Gödel 数という
  (1) $G : E \longrightarrow \mathbb{N}$ は 1 対 1 の関数
  (2) $G(x)$ を計算するアルゴリズムが具体的に与えられている
  (3) 任意の $y \in \mathbb{N}$ に対し, 以下が具体的に与えられている
    - $G(x) = y$ となる $x \in E$ が存在するか否かの判定法
    - x が存在するとき, それを求めるアルゴリズム

以下, Gödel 数化の具体例を一つ取り上げ, それを固定して議論

基本的記号

$M = (K, \Sigma, Q, q_0, \{q_h\})$: TM

基本的な記号: K, Σ の要素と, ヘッドの動きを規定する R, L, N

- K は以下の無限列のうちの最初の有限個

$$q_0,\ q_h,\ q_1,\ q_2, \ldots$$

- Σ は以下の無限列のうちの最初の有限個

$$B,\ 1,\ a_1,\ a_2, \ldots$$

基本的記号の Gödel 数

- 基本的記号を以下のように並べる

$$\underbrace{R,\ L,\ N,}_{\text{ヘッドの移動}}\quad \underbrace{q_0,\ B,\ q_h,\ 1,\ q_1,\ a_1,\ q_2,\ a_2,\ldots}_{K\ \text{と}\ \Sigma\ \text{の要素を交互に並べる}}$$

- これらの基本的記号に 3 以上の奇数を順次割り当てる

割り当てを "$\widehat{\ }$" で書けば,

$$\widehat{R}=3,\quad \widehat{L}=5,\quad \widehat{N}=7,\quad \widehat{q_0}=9,\quad \widehat{B}=11,$$
$$\widehat{q_h}=13,\quad \widehat{1}=15,\quad \widehat{q_1}=17,\quad \widehat{a_1}=19,\quad \widehat{q_2}=21,$$
$$\widehat{a_2}=23,\quad \ldots$$

記号列の Gödel 数

Q の要素である五つ組や様相などの記号列

$$\alpha = x_0 x_1 x_2 \dots x_n \qquad (x_i \in K \cup \Sigma \cup \{R, L, N\},\ n \geq 0)$$

に対して, 数 $gn(\alpha)$ を以下で定義

$$gn(\alpha) = \prod_{i \leq n} p_i^{\widehat{x_i}}$$

ただし, p_i は $i+1$ 番目の素数

例: $gn(q_0 B 1 R q_h) = 2^9 3^{11} 5^{15} 7^3 11^{13}$

記号列の列の Gödel 数

- TM に関する議論では，さらに計算や五つ組の集合 Q を扱う
- 集合を要素の適当な列とみなせば，これらは記号列の列
- 記号列の列 $\alpha_0, \alpha_1, \ldots, \alpha_m$ に対して，以下を対応させる

$$\prod_{i \leq m} p_i^{gn(\alpha_i)}$$

例

五つ組の列

$$q_0 B 1 R q_1, \quad q_0 1 B R q_h, \quad q_1 1 1 R q_1$$

に対しては，以下の数が対応

$$2^{2^9 3^{11} 5^{15} 7^3 11^{17}} 3^{2^9 3^{15} 5^{11} 7^3 11^{13}} 5^{2^{17} 3^{15} 5^{15} 7^3 11^{17}}$$

注: 巨大な数になるが，ここでは大きさは問題にしない

Gödel 数化となっていることの確認

割り当て状況:

- 基本的記号: 奇数
- 記号列: $2^n \cdot m$ (n, m は奇数) の形の偶数
- 記号列の列: $2^n \cdot m$ (n は偶数, m は奇数) の形の偶数

異なる記号, 記号列, 記号列の列には異なる数が割り当てられる
$\Longrightarrow$ 対応は 1 対 1 (条件 (1) が成立)

ただし, 一つの対象に対し, 見方によって複数の数が割り当て可能

例

基本的記号 R には 3 が対応
R は記号列, 記号列の列ともみなせ, それぞれ 2^3, 2^{2^3} が対応

条件 (2), (3) も成立
(たとえば, 2^2 が割り当てられる対象がないことが簡単に分かる)

当面の目標

以下の述語 T_n が原始帰納的であること (補題 1) を示すこと

$$T_n(z, x_1, \ldots, x_n, y) \leftrightarrow \begin{cases} y \text{ は, Gödel 数が } z \text{ の TM による計算} \\ \overline{(x_1, \ldots, x_n)} q_0 B \overset{*}{\Rightarrow} w q_h B \\ \text{の Gödel 数である } (w \in \Sigma^*) \end{cases}$$

TM $M = (K, \Sigma, Q, q_0, \{q_h\})$ の Gödel 数:
五つ組の有限集合 Q の要素を適当な順序で並べた列に対する Gödel 数のこと

注: M に対して $|Q|!$ 個の Gödel 数が存在するが, どれでもよい

原始帰納的述語, 関数の準備 (1/6)

- $D(x) \longleftrightarrow (x = 3) \vee (x = 5) \vee (x = 7)$
  (x はヘッドの動き R, L, N に対応する Gödel 数)
- $K(x) \longleftrightarrow (\exists y)_{<x}(x = 4y + 9)$
  (x は状態に対する Gödel 数)
- $\Sigma(x) \longleftrightarrow (\exists y)_{<x}(x = 4y + 11)$
  (x は Σ の要素に対する Gödel 数)

原始帰納的述語, 関数の準備 (2/6)

- *Gn*$(x) \longleftrightarrow \neg(\exists i)_{<L(x)}[((x)_i = 0) \wedge ((x)_{i'} \neq 0)]$
  (x は $\prod_{i \leq n} p_i^{\alpha_i}$, $\alpha_i > 0$ の形)
  ただし, $L(x)$, $(x)_i$ は以下で定義され, いずれも原始帰納的
  $L(x)$: $x = 0, 1$ のとき 0,
  $x \geq 2$ のとき x の最大の素因数を p_i として $i + 1$
  $(x)_i$: $x = 0, 1$ のとき 0,
  $x \geq 2$ のとき x の素因数分解における p_i の巾

注: *Gn*(x) が成り立つとき, $L(x)$ は x の相異なる素因数の数

- *Quin*$(x) \longleftrightarrow$ *Gn*$(x) \wedge (L(x) = 5) \wedge K((x)_0) \wedge \Sigma((x)_1)$
  $\wedge \Sigma((x)_2) \wedge D((x)_3) \wedge K((x)_4) \wedge ((x)_0 \neq 13)$
  (x は五つ組の Gödel 数)

原始帰納的述語, 関数の準備 (3/6)

- $\mathit{Ndet}(x, y) \leftrightarrow \mathit{Quin}(x) \wedge \mathit{Quin}(y) \wedge (x \neq y)$
  $\wedge((x)_0 = (y)_0) \wedge ((x)_1 = (y)_1)$
  (x, y は五つ組の Gödel 数で, $x \neq y$ かつ, 最初の二つの基本記号が相等しい)
- $\mathit{Tm}(x) \leftrightarrow \mathit{Gn}(x) \wedge (\forall i)_{<L(x)}[\mathit{Quin}((x)_i)$
  $\wedge(\forall j)_{<L(x)}(\neg \mathit{Ndet}((x)_i, (x)_j))]$
  (x は TM の一つの Gödel 数)
- $\mathit{Conf}(x)$
  $\leftrightarrow \mathit{Gn}(x) \wedge (\exists i)_{<L(x) \dot{-} 1}[K((x)_i) \wedge (\forall j)_{<L(x)}(i = j \vee \Sigma((x)_j))]$
  (x は様相の Gödel 数)
- $\mathit{Mem}(x, z) \leftrightarrow \mathit{Tm}(z) \wedge (\exists i)_{<L(x)}((z)_i = x)$
  (x は Gödel 数が z であるような TM の五つ組の一つに対する Gödel 数)

原始帰納的述語, 関数の準備 (4/6)

- $\mathit{Yield}_R(x,y,z) \leftrightarrow \mathit{Conf}(x) \wedge \mathit{Conf}(y) \wedge \mathit{Tm}(z)$
$$\wedge(\exists\varphi)_{<x}(\exists\psi)_{<x}(\exists a)_{<x}(\exists b)_{<y}(\exists p)_{<x}(\exists q)_{<y}$$
$$[(x=\varphi\circ 2^p3^a\circ\psi)\wedge(y=\varphi\circ 2^b3^q\circ\psi)$$
$$\wedge \mathit{Mem}(2^p3^a5^b7^3 11^q, z)]$$
(x, y はある様相 α, β の Gödel 数, z はある TM の Gödel 数, $pabRq \in Q$ の形の五つ組によって $\alpha \Rightarrow \beta$)

ただし, $x \circ y \stackrel{\text{def}}{=} x \cdot \prod_{i<L(y)} p_{L(x)+i}^{(y)_i}$ (原始帰納的関数)

例: $x = p_0^{x_0}\ldots p_{m-1}^{x_{m-1}}$, $y = p_0^{y_0}\ldots p_{n-1}^{y_{n-1}}$ のとき,

$$x\circ y = p_0^{x_0}\ldots p_{m-1}^{x_{m-1}} p_m^{y_0}\ldots p_{m+n-1}^{y_{n-1}}$$

原始帰納的述語, 関数の準備 (5/6)

- $\mathit{Yield}_L(x,y,z) \leftrightarrow \mathit{Conf}(x) \wedge \mathit{Conf}(y) \wedge \mathit{Tm}(z)$
$$\wedge(\exists\varphi)_{<x}(\exists\psi)_{<y}(\exists a)_{<x}(\exists b)_{<y}(\exists c)_{<x}(\exists p)_{<x}(\exists q)_{<y}$$
$$[(x=\varphi\circ 2^c3^p5^a\circ\psi)\wedge(y=\varphi\circ 2^q3^c5^b\circ\psi)$$
$$\wedge \mathit{Mem}(2^p3^a5^b7^5 11^q, z)]$$
$(pabLq \in Q$ の形の五つ組によって $\alpha \Rightarrow \beta)$

- $\mathit{Yield}_N(x,y,z) \leftrightarrow \mathit{Conf}(x) \wedge \mathit{Conf}(y) \wedge \mathit{Tm}(z)$
$$\wedge(\exists\varphi)_{<x}(\exists\psi)_{<y}(\exists a)_{<x}(\exists b)_{<y}(\exists p)_{<x}(\exists q)_{<y}$$
$$[(x=\varphi\circ 2^p3^a\circ\psi)\wedge(y=\varphi\circ 2^q3^b\circ\psi)$$
$$\wedge \mathit{Mem}(2^p3^a5^b7^7 11^q, z)]$$
$(pabNq \in Q$ の形の五つ組によって $\alpha \Rightarrow \beta)$

- $\mathit{Yield}(x,y,z) \leftrightarrow \mathit{Yield}_R(x,y,z) \vee \mathit{Yield}_L(x,y,z) \vee \mathit{Yield}_N(x,y,z)$.
(x, y は様相 α, β の Gödel 数, z は TM M の Gödel 数, M によって $\alpha \Rightarrow \beta$)

原始帰納的述語, 関数の準備 (6/6)

- $$\begin{cases} \mathit{Code}(0) = 2^{15}, \\ \mathit{Code}(x') = 2^{15} \circ \mathit{Code}(x) \quad (\mathit{Code}(x) = \mathit{gn}(\overline{x})) \end{cases}$$
- $\mathit{init}_n(x_1, \ldots, x_n)$
  $= \mathit{Code}(x_1) \circ 2^{11} \circ \mathit{Code}(x_2) \circ 2^{11} \circ \cdots \circ \mathit{Code}(x_n) \circ 2^9 3^{11}$
  $(\mathit{init}_n(x_1, \ldots, x_n) = \mathit{gn}(\overline{(x_1, \ldots, x_n)} q_0 B)$
  すなわち, n 変数関数の計算における開始時の様相に対する Gödel 数)
- $\mathit{Fin}(x) \longleftrightarrow \mathit{Conf}(x) \wedge (\exists y)_{\leq x}(x = \mathit{Code}(y) \circ 2^{13} 3^{11})$
  (x は $11 \cdots 1 q_h B$ の形の様相に対する Gödel 数)

T_n は原始帰納的

補題 1

述語 T_n は原始帰納的

証明

$$
\begin{aligned}
& T_n(z, x_1, \ldots, x_n, y) \\
& \qquad \longleftrightarrow \mathit{Tm}(z) \wedge \mathit{Gn}(y) \\
& \qquad\qquad \wedge (\forall i)_{<L(y) \dot{-} 1} [\mathit{Yield}((y)_i, (y)_{i'}, z) \\
& \qquad\qquad\qquad \wedge ((y)_0 = \mathit{init}_n(x_1, \ldots, x_n)) \\
& \qquad\qquad\qquad \wedge \mathit{Fin}((y)_{L(y) \dot{-} 1})]
\end{aligned}
$$

■

1. 計算の算術化
2. 計算可能な関数は帰納的
3. 万能 Turing 機械

原始帰納的関数の準備

- $\mathit{ck}(i, x) = \begin{cases} 1, & (x)_i = 15 \text{ のとき}, \\ 0, & (x)_i \neq 15 \text{ のとき} \end{cases}.$
  ($\mathit{ck}(i, x)$ は述語 $\neg((x)_i = 15)$ の特徴関数)
- $\mathit{decode}(x) = \left(\sum_{i<L(x)} \mathit{ck}(i, x)\right) \dot{-} 1$
  ($\mathit{decode}(x)$ は, Gödel 数が x である様相の中の 1 の個数を集計し, その総数から 1 を減じた数)
- $U(x) = \mathit{decode}((x)_{L(x) \dot{-} 1})$
  ($U(x)$ は, x が計算の Gödel 数であるとき, その最後の様相の Gödel 数に対して *decode* を適用し, 計算された関数値を取り出す)

部分的に計算可能な関数は部分帰納的 (1/2)

定理 1

部分的に計算可能な関数は部分帰納的

証明 (1/2)

$f(\mathbf{x})$: 部分的に計算可能な関数 ($\mathbf{x} = (x_1, \dots, x_n)$)
M: f を部分的に計算する TM (Gödel 数は k)

$\mathbf{x} \in \mathcal{D}(f)$ ならば, M による計算 $\alpha_0, \dots, \alpha_r$ が存在して,

$$\alpha_0 = \overline{\mathbf{x}} q_0 B, \qquad \alpha_r = \overline{f(\mathbf{x})} q_h B$$

y_0: 記号列の列 $\alpha_0, \dots, \alpha_r$ に対する Gödel 数
$\Longrightarrow T_n(k, \mathbf{x}, y_0)$ が成立

$k, x_1, \dots, x_n$ を固定すると $T_n(k, \mathbf{x}, y)$ が成立する y は高々一つ
$\Longrightarrow y_0 = \mu y T_n(k, \mathbf{x}, y)$

部分的に計算可能な関数は部分帰納的 (2/2)

証明 (2/2)

よって,

$$U(\mu y T_n(k, \mathbf{x}, y)) = U(y_0) = \mathit{decode}(\mathit{gn}(\alpha_r))$$
$$= \mathit{decode}(\mathit{gn}(\overline{f(\mathbf{x})} q_h B)) = f(\mathbf{x})$$

$\mathbf{x} \notin \mathcal{D}(f)$ ならば, α_0 に始まる M による計算は存在しない
$\Longrightarrow$ すべての y に対して $T_n(k, \mathbf{x}, y)$ は成立しない
$\Longrightarrow$ $U(\mu y T_n(k, \mathbf{x}, y))$ は無定義

以上より, $f(\mathbf{x}) \cong U(\mu y T_n(k, \mathbf{x}, y))$
(二つの部分関数 f, $g : A \to B$ に対し, $\mathcal{D}(f) = \mathcal{D}(g)$, かつ, $x \in \mathcal{D}(f)$ ならば $f(x) = g(x)$ であるとき, $f(x) \cong g(x)$ と書く)

よって, f は部分帰納的関数 ■

計算可能関数は帰納的

定理 1 の証明より，以下の二つの系が成り立つ

系 1

計算可能関数は帰納的

系 2

任意の部分的に計算可能な関数 $f(x_1, \ldots, x_n)$ に対して，

$$f(x_1, \ldots, x_n) \cong U(\mu y T_n(k, x_1, \ldots, x_n, y))$$

となるような数 k が存在する

Kleene の標準形定理

定理 2 (Kleene の標準形定理)

任意の部分帰納的関数 $f(x_1, \ldots, x_n)$ に対して,

$$f(x_1, \ldots, x_n) \cong U(\mu y T_n(k, x_1, \ldots, x_n, y))$$

となるような数 k が存在

証明 (1/2)

系 2 と, 第 9 回の系 4「部分帰納的関数は部分的に計算可能」より成立 ■

系 2, 定理 2 より, 任意の (部分的) 帰納的関数は,

原始帰納的な関数 U, 述語 T_n と μ 作用素を, それぞれ一回だけ使って表現可能

$\Longrightarrow$ 系 2, 定理 2 は強力な結果, 述語 T_n は重要

枚挙定理

定理 3 (枚挙定理)

任意の帰納的述語 $P(x_1, \ldots, x_n, y)$ に対して,

$$(\exists y)P(x_1, \ldots, x_n, y) \longleftrightarrow (\exists y)T_n(k, x_1, \ldots, x_n, y)$$

となるような数 k が存在

証明

M: P の特徴関数 $C_p(x_1, \ldots, x_n, y)$ を計算する TM

この M を使って $\mu y(C_p(x_1, \ldots, x_n, y) = 0)$ を部分的に計算する TM M_0 を作り, その Gödel 数を k とする

すると, 以下が成立

$$\begin{aligned}(\exists y)P(x_1, \ldots, x_n, y) &\leftrightarrow \mu y(C_p(x_1, \ldots, x_n, y) = 0) \text{ の値が確定} \\ &\leftrightarrow (\exists y)T_n(k, x_1, \ldots, x_n, y)\end{aligned}$$

■

1. 計算の算術化
2. 計算可能な関数は帰納的
3. 万能 Turing 機械

TM と万能 TM

これまでの TM:

- 一つの関数を計算するもの
- 計算機ではなくプログラムに相当

万能 Turing 機械 (万能 TM):

- 計算機に相当する, 任意の計算可能な関数を計算できる TM
- Turing が存在を示した

$\Longrightarrow$ von Neumann によるプログラム内蔵型計算機の開発に影響を与えた

万能 TM の原理 (1/2)

- f: 任意の 1 変数の部分的に計算可能な関数
  f に依存した定数 k を用いて，f は以下の通り表現可能

$$f(x) \cong U(\mu y T_1(k, x, y)) \tag{1}$$

- (1) の右辺の k も変数とみなして，

$$\varphi(z, x) \cong U(\mu y T_1(z, x, y))$$

  とすると，φ は部分帰納的

- A: φ を部分的に計算する TM

  引数 z の値を変えることによって，部分的に計算可能なすべての 1 変数関数を部分的に計算可能

万能 TM の原理 (2/2)

- M: f を部分的に計算する TM
  M の Gödel 数 k を z の値として A に与える

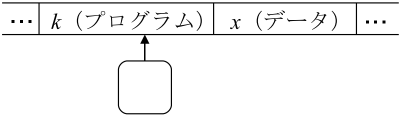
  $\Longrightarrow$ A は $\varphi(k,x)$ を部分的に計算

  $\Longrightarrow$ A は $f(x)$ を, $x \in \mathcal{D}(f)$ であるとき,
  またこのときに限り,

$$\overline{(k,x)}q_0B \overset{*}{\Rightarrow} \overline{f(x)}q_hB$$

  の形で計算

  $\Longrightarrow$ A は, k をプログラム, x を入力データとみなして,
  プログラム k にしたがって $f(x)$ を計算



n 変数関数の場合

- n 変数関数 $f(x_1, \ldots, x_n)$ は,
$$g(x) = f((x)_0, \ldots, (x)_{n-1})$$
によって 1 変数関数に置き換え可能
f が部分的に計算可能ならば, $g(x)$ は部分的に計算可能
- N: 任意の $(x_1, \ldots, x_n)$ に対して以下を計算する TM
$$x = \prod_{i<n} p_i^{x_i+1}$$
N と A を結合した TM は,
n 変数の部分的に計算可能な任意の関数を部分的に計算可能

アルゴリズムの定式化 (1/2)

アルゴリズムが存在すること:
　一定の規則にしたがって, 有限回の操作で機械的に解を求めることができる計算法を示せば十分

アルゴリズムが存在しないこと:
　アルゴリズムの正確な定義が必要

アルゴリズムの定式化 (2/2)

- 1930 年代, アルゴリズムの数学的定義となり得る概念の導入
  - K. Gödel による「帰納的」
  - A. Church による「λ 定義可能性」
  - A. M. Turing による「Turing 機械」
  - E. L. Post による「Post 機械」
- S. C. Kleene は, およそアルゴリズムを持つと考えられる関数はことごとく λ 定義可能であることを確認
- Kleene と Gödel は, 帰納的と λ 定義可能性の等価性を証明

Church の提唱

Church の提唱 (1936 年)

アルゴリズムを持つ関数 (述語) と帰納的関数 (述語) を同一視しよう

- Turing は Church や Kleene とは独立に TM を導入
  TM によって計算可能な関数族と λ 定義可能な関数族が一致することを証明
- Post も同じころ, 同様の定式化を行った

その後もさまざまなアルゴリズムの定式化があったが,
ことごとく上記の概念と等価であった

今日までの経験と合わせ, Church の提唱を疑う人はまずいない