現代の数学と数理解析・講義資料（2015年4月24日）

照井一成（京都大学数理解析研究所）

はじめに　本講義では「自然数」というとき0も含める。

$$\mathbb{N} := \{0, 1, 2, 3, \dots\}$$

$\mathbb{N}$ 上の関数 f を次のように定める。

$$\begin{aligned} f(n) &= n/2 \quad (n \text{ が偶数のとき}) \\ &= 3n+1 \quad (n \text{ が奇数のとき}) \end{aligned}$$

コラッツ・角谷予想： $\forall n \geq 1.\, \exists m.\, f^m(n) = 1.$

少なくとも $n < 2^{60}$ までは成り立つことが確認済み。全ての n について成り立つかは未解決。

初等数論の形式系　次の形の表現を**項**という。

$$\mathsf{0} \qquad \mathsf{S}(t) \qquad t + u \qquad t \cdot u \qquad x$$

ただし t, u はそれ自体項である（帰納的定義）。また x は変数を表す（y, z 等を用いてもよい）。

$$\mathsf{0}, \qquad \mathsf{S}(\mathsf{0}), \qquad \mathsf{S}(\mathsf{S}(\mathsf{0})), \qquad \dots$$

を $\mathsf{0}, \mathsf{S0}, \mathsf{SS0}, \dots$ または $\mathsf{0}, \mathsf{1}, \mathsf{2}, \dots$ と略記する。

次の形の表現を**論理式**という。

$$t = u \qquad \bot \qquad A \wedge B \qquad A \vee B \qquad A \to B \qquad \forall x.A \qquad \exists x.A$$

ただし t, u は項、A, B はそれ自体論理式であるとする。$\forall x$, $\exists x$ は A の中にある変数 x を束縛する。未束縛の変数を含まない論理式を**文**という。

等号の推論規則

$$\frac{}{t = t}\ (\mathsf{e1}) \qquad \frac{t = v \quad u = v}{t = u}\ (\mathsf{e2})$$

$$\frac{t_1 = t_2 \quad u_1 = u_2}{t_1 + u_1 = t_2 + u_2}\ (\mathsf{e3}) \qquad \frac{t_1 = t_2 \quad u_1 = u_2}{t_1 \cdot u_1 = t_2 \cdot u_2}\ (\mathsf{e4}) \qquad \frac{t = u}{\mathsf{S}(t) = \mathsf{S}(u)}\ (\mathsf{e5})$$

数論記号の推論規則

$$\frac{\mathsf{S}(t) = \mathsf{S}(u)}{t = u}\ (\mathsf{a1}) \qquad \frac{\mathsf{S}(t) = \mathsf{0}}{\bot}\ (\mathsf{a2})$$

$$\frac{}{t + \mathsf{0} = t}\ (\mathsf{a3}) \qquad \frac{}{t + \mathsf{S}(u) = \mathsf{S}(t + u)}\ (\mathsf{a4})$$

$$\frac{}{t \cdot \mathsf{0} = \mathsf{0}}\ (\mathsf{a5}) \qquad \frac{}{t \cdot \mathsf{S}(u) = t \cdot u + t}\ (\mathsf{a6})$$

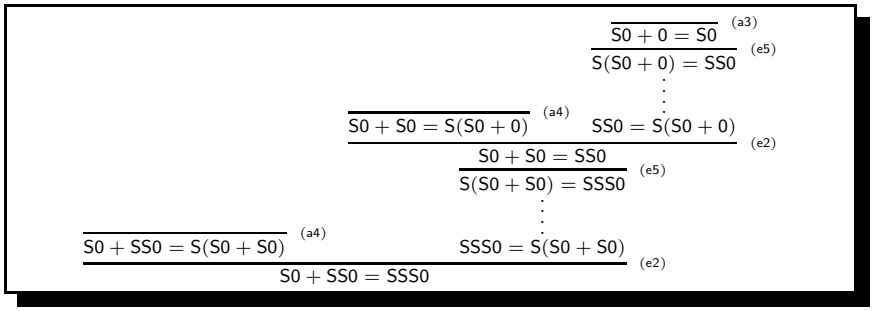


図 0.1: $1 + 2 = 3$ の証明図

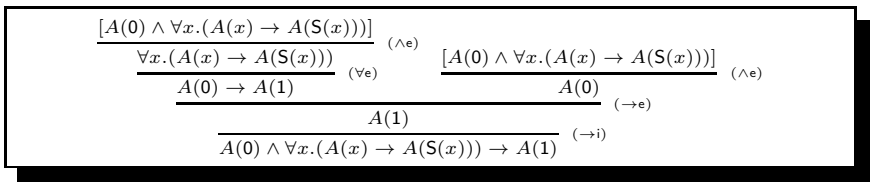


図 0.2: 証明図の例

論理記号の推論規則（例）

$$\frac{A \quad B}{A \wedge B}\ (\wedge\mathsf{i}) \qquad \frac{A \wedge B}{A}\ (\wedge\mathsf{e}) \qquad \frac{A \wedge B}{B}\ (\wedge\mathsf{e})$$

$$\frac{\begin{array}{c}[A] \\ \vdots \\ B\end{array}}{A \to B}\ (\to\mathsf{i}) \qquad \frac{A \to B \quad A}{B}\ (\to\mathsf{e})$$

$$\frac{A(y)}{\forall x.A(x)}\ (\forall\mathsf{i}) \qquad \frac{\forall x.A(x)}{A(t)}\ (\forall\mathsf{e})$$

$$\frac{\bot}{A}\ (\bot) \qquad \frac{\begin{array}{c}[\neg A] \\ \vdots \\ \bot\end{array}}{A}\ (\mathsf{abs})$$

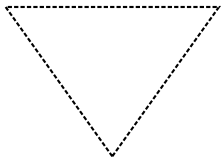
数学的帰納法の推論規則

$$\frac{A(0) \quad A(y) \to A(\mathsf{S}(y))}{A(t)}\ (\mathsf{ind})$$

ただし t は任意の項である。また (∀i) 規則と (ind) 規則については固有変数条件が必要である（説明略）。

ペアノ算術　上の規則により定められる形式系を**ペアノ算術 PA** という。

A を文とする。以上の推論規則を組み合わせて



A

の形の図が作図できるとき、これを A **の証明図**という（ただし仮定は含まないものとする）。A の証明図が存在するとき

$$\mathbf{PA} \vdash A$$

と書き、「**PA** は A を証明できる」と読む。

定理 1(計算可能性の壁（チューリング 1936）)

文 A が与えられたとき、「A は証明図を持つか」をイエス・ノーで判定できるコンピュータプログラムは存在しない。

定理 2(NP の壁)

文 A と自然数 n が与えられたとき、「A はサイズ n の証明図を持つか」は **NP** 完全問題である。

定理 3(証明可能性の壁（ゲーデル 1931）)

真なのに **PA** には証明できない文が存在する。例：

$$\begin{aligned} G_{\mathbf{PA}} &:= \text{“}\mathbf{PA} \text{ は文 } G_{\mathbf{PA}} \text{ を証明できない”} \quad \text{（第一不完全性）} \\ \mathsf{Con}_{\mathbf{PA}} &:= \text{“}\mathbf{PA} \text{ は無矛盾である（}\mathbf{PA} \nvdash \bot\text{）”} \quad \text{（第二不完全性）} \end{aligned}$$

なお、完全な形式系も存在する（例：実閉体の公理系）。その場合、証明可能性・計算可能性の壁は存在しない。

アッカーマン　自然数の有限列を $\langle 3,4,0,9\rangle$ のように表す。次の操作を考える。

$$\begin{aligned} \langle n,0,\ldots\rangle &\longrightarrow_{(\mathsf{a})} \langle n+1,\ldots\rangle \\ \langle 0,m+1,\ldots\rangle &\longrightarrow_{(\mathsf{b})} \langle 1,m,\ldots\rangle \\ \langle n+1,m+1,\ldots\rangle &\longrightarrow_{(\mathsf{c})} \langle n,m+1,m,\ldots\rangle \\ \langle n\rangle &\longrightarrow_{(\mathsf{d})} \mathsf{end} \end{aligned}$$

この操作はどんな列から始めても停止するだろうか？

$\mathbb{N}$ 上の関数列 $g_0, g_1, g_2, \ldots$ を次のように定義する。

$$\begin{aligned} g_0(n) &:= n+1 \\ g_{m+1}(n) &:= \underbrace{g_m(g_m(\cdots g_m}_{n+1}(1)\cdots)) \end{aligned}$$

定理 4

$g_m(n) = k \iff \langle n, m\rangle \longrightarrow^* \langle k\rangle.$

半順序・全順序・整列順序　X を集合、$\prec$ を X 上の関係とする。

- $(X, \prec)$ は**半順序**である　$\iff$　すべての $x, y, z \in X$ について

$$x \not\prec x, \qquad x \prec y \prec z \to x \prec z.$$

- $(X, \prec)$ は**全順序**である　$\iff$　半順序かつすべての $x, y \in X$ について

$$x \prec y \quad \text{または} \quad x = y \quad \text{または} \quad y \prec x.$$

- $(X, \prec)$ は**整列順序**である　$\iff$　全順序かつどんな $x_0 \in X$ から始めても

$$x_0 \succ x_1 \succ x_2 \succ x_3 \succ \cdots$$

なる無限下降列は存在しない。

定理 5(整列定理)

どんな集合 X についても、適当な関係 $\prec$ が存在し $(X, \prec)$ は整列順序となる。

ϵ_0 未満の順序数　集合 $\mathsf{ON}(\epsilon_0)$ を以下のように定義する（便宜上、少々変わった定義をする）。

1. $0 \in \mathsf{ON}(\epsilon_0)$.
2. $\alpha_1, \ldots, \alpha_n \in \mathsf{ON}(\epsilon_0)$ なら $\omega^{\alpha_1} + \cdots + \omega^{\alpha_n} \in \mathsf{ON}(\epsilon_0)$.

ただし 2 で $\omega^{\alpha_1}, \ldots, \omega^{\alpha_n}$ の順番を並べ変えたものは元の順序数と同一視する（$+$ は可換）。また $\omega^\alpha \cdot n := \underbrace{\omega^\alpha + \cdots + \omega^\alpha}_{n}$ と略記し、$n := \omega^0 \cdot n$ とする。順序関係は十進法とのアナロジーで自然に定義する。

- $\omega^6 \cdot 3 \succ \omega^6 \cdot 2 + \omega^5 \cdot 4 \succ \omega^5 \cdot 9$
  （順序数は最高桁の数が大きいほど大きい）
- $\omega^6 \cdot 3 + \omega^5 \cdot 4 \succ \omega^6 \cdot 3 + \omega^5 \cdot 3 + \omega^4 \cdot 9$
  （最高桁の数が同じならば次の桁を比べる）

定理 6

$(\mathsf{ON}(\epsilon_0), \prec)$ は整列順序である。

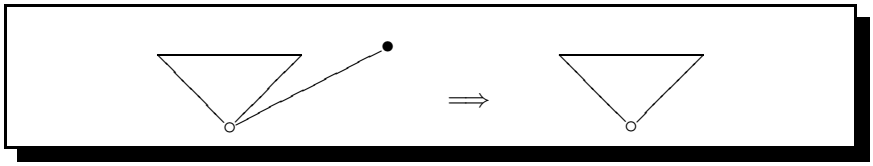


図 0.3: ヒドラの変形 1

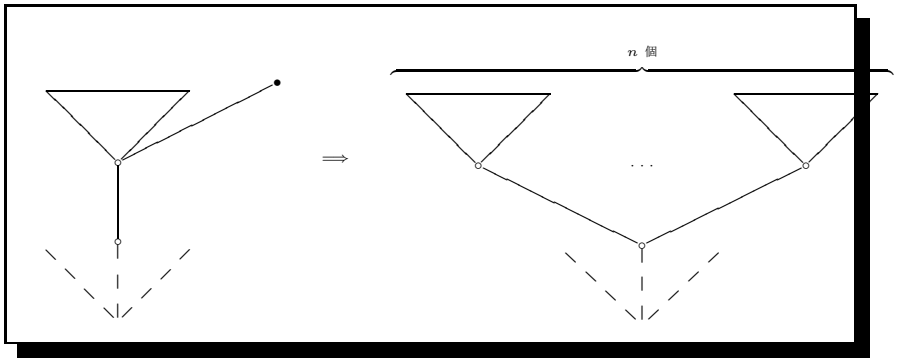


図 0.4: ヒドラの変形 2

アッカーマン再考　自然数の有限列に対して順序数を次のように割り当てる ($k \geq 0$)。

$$\begin{aligned} \langle n \rangle &\mapsto 0 \\ \langle n, m, l_1, \ldots, l_k \rangle &\mapsto \omega^m \cdot (2n+1) + \omega^{l_1+1} + \cdots + \omega^{l_k+1} \end{aligned}$$

定理 7

有限列にアッカーマンの操作を適用すると、対応する順序数は減少する。ゆえにどんな有限列から出発しても、アッカーマンの操作は必ず停止する。

ヒドラゲーム　有限木を**ヒドラ**と見なす。ヘラクレスがヒドラの首（葉）を切るたびにヒドラは身体の一部を増やしていく（図参照)。ヘラクレスの勝利条件はヒドラの全ての首を切ることである（胴体＝根を除く)。

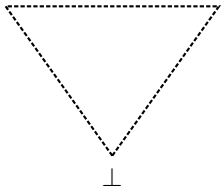
定理 8

どんな順序で首を切り落としていっても、ヘラクレスは常にヒドラに勝利する。

ヒドラゲームはオンラインでプレイできる (`http://math.andrej.com/2008/02/02/the-hydra-game`)。

ゲンツェンの無矛盾性証明　以下、ゲンツェンによる **PA** の無矛盾性証明のアイデアを述べる。

仮にもしも $\mathbf{PA} \vdash \bot$ となったら **PA** は矛盾していることになる。ゆえに **PA** の無矛盾性を示すには、**矛盾証明図**、すなわち



なる証明図（ただし仮定を含まない）が作図不可能であることを示せばよい。

1. **単純な矛盾証明図**、すなわち等式 $t = u$ のみを用いて $\bot$ に至るような証明図は存在しえない。
2. 単純でない矛盾証明図は、“もっと簡単な” 矛盾証明図に書き換えられる。
3. 証明図に適当に順序数 $\alpha \in \mathsf{ON}(\epsilon_0)$ を割り当てれば、書き換えによって順序数が減少するようにすることができる。
4. 仮に矛盾証明図が作図できたとしたら、それは 1 により単純でない。それゆえ 2 により別の矛盾証明図に書き換えることができる。この操作を繰り返せば順序数の矛盾下降列

$$\alpha_0 \succ \alpha_1 \succ \alpha_2 \succ \cdots$$

が作れるが、これは $\mathsf{ON}(\epsilon_0)$ の整列性に反する。

順序数 $\alpha \in \mathsf{ON}(\epsilon_0)$ または $\alpha = \epsilon_0$ について、「α 未満の順序数たちは整列している」ことを初等数論の文で（ほぼ）表した文（スキーマ）を $\mathsf{TI}(\alpha)$ とする。

定理 9(ゲンツェン 1936, 1938, 1943)

1. $\mathbf{PA} + \mathsf{TI}(\epsilon_0) \vdash \mathsf{Con}_{\mathbf{PA}}$.
2. $\alpha < \epsilon_0$ ならば $\mathbf{PA} \vdash \mathsf{TI}(\alpha)$.

よって

3. $\mathbf{PA} \nvdash \mathsf{TI}(\epsilon_0)$.
1. $\alpha < \epsilon_0$ ならば $\mathbf{PA} + \mathsf{TI}(\alpha) \nvdash \mathsf{Con}_{\mathbf{PA}}$.

定理 10

1. **PA** は「アッカーマンの操作は常に停止する」ことを証明できる。
2. **PA** は「ヘラクレスはヒドラに常に勝利する」ことを証明できない（カービィ・パリス 1982）。

レポート課題　以下から一題以上選んで答えよ（1 はやさしい問題。3,4 は普通の問題。2 は中間）。

1. 次の各対は半順序か？全順序か？無限下降列を持つか？

   - $(\mathbb{C}, \prec)$、ただし $\mathbb{C}$ は複素数全体の集合で $\alpha \prec \beta \Leftrightarrow |\alpha| < |\beta|$.
   - $(\mathbb{N}, \prec)$、ただし $n \prec m \Leftrightarrow n$ は m の約数で $n \neq m$.

2. $(\mathbb{N}^2, \prec)$ は整列順序であることを証明せよ。ただし $\mathbb{N}^2$ は自然数の対（つい）全体の集合で $(x_1, y_1) \prec (x_2, y_2) \Leftrightarrow x_1 < x_2$ または、$x_1 = x_2$ かつ $y_1 < y_2$. なお $\mathsf{ON}(\epsilon_0)$ が整列順序であることは自由に用いてよい。

3. 自然数の有限列全体の集合を $\mathbb{N}^*$ とする。

   $$\mathbb{N}^* := \{\langle n_1, \ldots, n_k \rangle : k, n_1, \ldots, n_k \in \mathbb{N}\}$$

   $\mathbb{N}^*$ 上に適当な関係 $\prec$ を定めて $(\mathbb{N}^*, \prec)$ を整列順序とせよ。

4. コンピュータプログラムを書いて、コラッツ・角谷の予想を 1 億まで確かめよ。その際、なるべく無駄を省いてプログラムを最適化せよ。わかりやすいコメントつきのソースコードを提出すること。言語は何を用いてもよい。