

数 学 入 門 公 開 講 座

平成14年8月5日(月)から平成14年8月8日(木)まで

京都大学数理解析研究所

講師及び内容

1. 自己言及の論理と計算 (5時間)

京都大学数理解析研究所・助教授 長谷川 真人

自分自身について述べることの難しさと面白さは、日常誰でも経験することだと思います。

この講座では、数理論理学と計算機科学の密接な関係を示す好例として、自己言及から生じる様々なパラドックスなどの数理論理学における問題、また自分自身を呼び出すような再帰的なプログラムやデータ構造に関する問題などについて、統一的な視点から考察します。

2. 積分の周期について (5時間)

京都大学数理解析研究所・教授 齋藤 恭司

円周率 $\pi=3,141592\dots$ (以下無限に続く)は円周の長さとして、積分

$$\frac{\pi}{2} = \int_0^1 \frac{dx}{\sqrt{1-x^2}}$$

で与えられます。 π の様に超越的な数が右辺の様に、高々根号の入る積分で表示されるのは非常に面白いと思います。積分を不定積分にすると

$$\sin^{-1}(t) = \int^t \frac{dx}{\sqrt{1-x^2}}$$

三角関数の逆関数(2π はその周期)となります。ガウスは更に、不定積分

$$\int^t \frac{dx}{\sqrt{1-x^4}}$$

を考察して、複素変数の2重の周期函数(楕円函数の特別な場合)を得ました。この講義では積分の周期、又その高次元化等について考えてみたいと思います。

3. トーリックの世界 (5時間)

京都大学数理解析研究所・助手 藤野 修

ユークリッド空間内の有限個のベクトルで張られた凸体を錐と呼びます。錐の集まりである扇が今回のお話の主人公です。扇から自然にトーリック多様体という代数多様体が構成できます。トーリック多様体の視点を導入することにより代数幾何の理論を扇の研究に用いることが出来ます。

一方、森理論は高次元代数幾何学の中心であり、現在も活発に研究されている大変難しい分野です。一般の代数多様体の世界ではまだまだ完成には程遠い状態です。しかしトーリック多様体の世界では森理論は扇の分割という非常に素朴な話になります。

講義では多面体や扇の分割という素朴なお話を題材にし、皆さんを広大なトーリック幾何学の世界の入口まで案内したいです。

時間割

時間 \ 日	8月 5日 (月)	6日 (火)	7日 (水)	8日 (木)
10:30~11:45	長谷川	長谷川	長谷川	長谷川
11:45~13:00	休憩			
13:00~14:15	齋藤 ^恭	齋藤 ^恭	齋藤 ^恭	齋藤 ^恭
14:15~14:45	休憩			
14:45~16:00	藤野	藤野	藤野	藤野

自己言及の理論と計算

京都大学数理解析研究所・助教授 長谷川 真人

2002, AUGUST 5, 6, 7, 8, 10:30～11:45

自己言及の論理と計算

長谷川真人

自分自身について述べることの難しさと面白さは、日常誰でも経験することだと思います。この講座では、数理論理学と計算機科学の密接な関係を示す好例として、自己言及から生じる様々なパラドックスなどの数理論理学における問題、また自分自身を呼び出すような再帰的なプログラムやデータ構造に関する問題などについて、統一的な視点から考察します。また、後半では、自己言及現象の自明でないモデルの例を、実際に構成します。

目次

I 自己言及と対角線論法	2
1 ラッセルの逆理	2
2 カントールの対角線論法	2
3 自己適用	3
4 停止性問題	5
5 対角線論法から不動点へ	7
6 不動点定理から具体例を見直す	7
II 矛盾したものを構成する	10
1 完備半順序集合と連続関数	10
2 最小不動点の発想	11
3 最初の試み	11
4 埋め込みと射影	13
5 なぜ失敗したか	14
6 正しい解の構成 — 逆極限法	15

Part I

自己言及と対角線論法

1 ラッセルの逆理

ラッセル (Russell, B.A.W., 1872-1970) は, 有名なパラドックスを指摘することにより, 安易な集合論の定式化が矛盾をひきおこすことを指摘した. ラッセルのパラドックス (のよく引用されるヴァージョン) とは以下のようなものである.

ラッセル集合とは, それ自身を要素として含むような集合のことであるとする. すなわち, $X \in X$ であるような集合 X のことをラッセル集合とよぶことにする. さて, M を, ラッセル集合でないような集合の集合であるとしよう¹. このとき, M 自身はラッセル集合だろうか? もし M がラッセル集合だとすると, ラッセル集合の定義より $M \in M$ である. しかし, これは M の元はラッセル集合ではないことと矛盾している. ところが, M をラッセル集合ではないと仮定してみても, M はラッセル集合でないような集合の集合だったから, $M \in M$ であり, したがって M はラッセル集合となる.

以下では, 導入として, この良く知られたパラドックスと, 数学基礎論や計算の理論などにおける関連した話題について解説する. その後, それらに共通する数学的構造を, 一種の不動点定理として定式化し, 一般的な視点から考察する. ところどころで数学基礎論, 直観主義論理, 圏論, プログラミング言語などの知識を要するところも出てくるが, 馴染みのない事柄については, とりあえずとばして頂いてかまわない.

2 カントールの対角線論法

やはり良く知られているカントール (Cantor, G., 1845-1918) の対角線論法は, はじめに述べたラッセルのパラドックスと大変良く似た構造を持っている.

定理 1 自分自身の巾集合を含むような集合は存在しない. より正確には, 任意の集合 X について, その巾集合 2^X から X への単射は存在しない. \square

証明はラッセルのパラドックスに用いられたのとほとんど同じ論法による. X を集合とし, $m: 2^X \rightarrow X$ を単射としよう. ここで, X の部分集合 R を,

$$R = \{m(A) \mid A \subseteq X, m(A) \notin A\}$$

と定義しよう. 問題は, $m(R)$ が R に属するかどうかである. まず, $m(R) \in R$ と仮定しよう. R の定義により, $m(A) \notin A$ なる $A \subseteq X$ が存在して $m(R) = m(A)$ となるはずである. m は単射だから, $R = A$. したがって $m(R) \notin R$ となり, 矛盾する. しかし, $m(R) \notin R$ と仮定すると, R の定義により $m(R) \in R$ となり, やはり矛盾する.

¹言葉の選択について: 歴史的には, この M のことをラッセル集合と呼ぶのが正統的であると思われる.

問題 1 定理 1 の証明と, 通常の (自然数と実数の濃度に関する) カントールの対角線論法とを比較してみよ.

3 自己適用

定理 1 の変形として, 以下のような結果も得られる. これは, 関数を「それ自身」に適用する, 自己適用現象に関するものである.

定理 2 任意の集合 X について, X がふたつ以上の相異なる要素を持つならば, X 上の関数全体の集合 X^X から X への単射は存在しない. \square

証明は定理 1 のそれとまったく同様である. X を集合とし, $m: X^X \rightarrow X$ を単射としよう. また, a, b を, X の相異なる要素と仮定しよう. ここで, X 上の関数 $f: X \rightarrow X$ を,

$$f(x) = \begin{cases} a & x = m(g) \text{ となる } g: X \rightarrow X \text{ が存在し } g(m(g)) = b \text{ であるとき} \\ b & \text{その他の場合} \end{cases}$$

と定義する. $f(m(f)) \in X$ を計算してみよう. f の定義から, $f(m(f))$ は a または b のどちらかである. まず, $f(m(f)) = a$ であると仮定する. f の定義より, $m(f) = m(g)$ となる $g: X \rightarrow X$ が存在して $g(m(g)) = b$ であるはずである. m は単射だから $f = g$, したがって $f(m(f)) = b$ となり, これは $f(m(f)) = a$ であると仮定したことに矛盾する. しかし, $f(m(f)) = b$ だと仮定しても, 今度は $f(m(f)) = a$ でなくてはならなくなるから, やはり矛盾する.

以前とそっくりな証明であるが, ここでは, 「 X がふたつ以上の相異なる要素を持つ」という前提条件が重要であることに注意して欲しい. この前提がなければ, X^X から X への単射をもつような集合 X は存在する — ただし一点集合だが (この証明は, X の任意の要素 a, b について $a = b$ であることを主張している).

上の例では, 関数 $f: X \rightarrow X$ を, それ自身 (の $m: X^X \rightarrow X$ による X での像) に適用することで矛盾を導いた. しかし, これは, あくまでも通常の集合と関数の世界での話である. それ以外の世界では, このような自己適用・自己言及現象は必ずしも矛盾を意味しない. たとえば, コンピュータ上で扱われるデータ全体の集合を X とすると, X の要素を入力して X の要素を出力するようなプログラムもデータとして扱うことができるので, そのようなプログラム全体 $[X \rightarrow X]$ は X の部分集合とみなすことができる.

そして, このことから, 自分自身を呼び出すようなプログラム (再帰プログラム) を, 自己適用現象を用いて得られる不動点として構成することができるのである. (似たことが直観主義論理の世界でも起こりうる: 以下のコラムを参照.)

対角線論法というと, 矛盾から否定的な結果を導くための道具, という印象を持っておられる方が少なくないであろうし, また, (すでに見てきたように) 実際そうなのであるが, 少し広い視野に立って, 一般化された対角線論法を考えると, 実は, 有用な (肯定的な) 結果を導く際にも対角線論法が現れていることがわかる.

ここで使われる数学は決して難解なものではないが、数学における具体例からの一般化、また一般化された見方からの具体例の分析、さらに否定的な見方から肯定的な見方への変化などの面白さが、端的に現れているものだと思う。そのあたりの楽しさを味わって頂ければ幸いである。

Advanced Topic

直観主義的抜け道について

実は、直観主義論理の世界(排中律が必ずしも成り立たない世界)では、 X^X から X への単射をもつような集合 X がつねに一点集合になるとはいえない場合がある。これは大変奇異な主張である。すこし丁寧に解説しよう。

まず、直観主義論理においても、 2^X から X への単射が存在するような集合 X は存在しないことがわかっている(証明は定理1のそれと基本的に同じである)。一方、 $2 = \{a, b\} \subseteq X$ だとすると、 2^X から X^X への単射が存在するから、もしも X^X から X への単射が存在するならば 2^X から X への単射が構成できてしまい、矛盾する。したがって、直観主義論理においても、 $2 = \{a, b\} \subseteq X$ かつ X^X から X への単射をもつような集合 X は存在しない。しかし、見方を変えると、この考察は、

定理 3 (直観主義的集合論においても) X^X から X への単射をもつような集合 X は、二点集合(より正確には真偽値の集合)を部分集合に持たない。□

ということを主張しているにすぎない。ここが直観主義論理の面白いところであるが、直観主義の立場では、真偽値の集合を部分集合に持たないけれども、一点集合とも異なる(同型でない)ような集合が存在しうるのである。そのような集合は、「真偽値の集合と直交している」ともいう(注:正確には、集合 S が集合 A と直交しているとは、 A から S への任意の関数が定数関数になるということをさす)。その中には、 X^X から X への単射を持つような集合 X も含まれている。

このような X が取れる例としては、たとえば、帰納的関数の世界のうえに構築された集合論が挙げられる。この集合論においては、集合も関数もなんらかの意味で計算できる(構成的である)もののみを対象とするのであるが、その世界においては X 上の(計算可能な)関数のあつまりが X 自身と同型になることがありえることは、容易に想像できることだろう。その一方、定理3により、 X は真偽値の集合と直交している。つまり、ちょっと不思議ではあるが、真偽値の集合から X への(計算可能な)関数は定数関数しか存在しない。

このようなアイデアをもとに、直観主義的集合論を基礎にして、集合論的にプログラミング言語の数学的モデルを構築する研究が1980年代に創始され、総合的領域理論(synthetic domain theory, ここでsyntheticはanalyticに対する語)として、独自の進歩を遂げている。これらの事柄はかなり専門的であり、今のところ研究論文以外に情報源はあまりないが、最近出た B. Jacobs: *Categorical Logic and Type Theory* (North-Holland, 1999)には、そのような直観主義集合論のモデルに関するくわしい解説が含まれている。

4 停止性問題

もうひとつだけ、やや手の込んだ例として、いわゆる停止性問題の決定不可能性、すなわち、与えられたプログラムが停止するかどうかを判定するプログラムが存在しないことを証明してみよう。本質的なアイデアは、これまでに考えてきた例と同じである(対角線論法/自己適用)。ただし、自己適用する関数の構成は、やや技巧的である。

チャーチ (Church, A., 1903-1995) の提唱によれば、自然数上の「計算可能」な部分関数は、帰納的関数 (**recursive function**) として特徴づけられる。帰納的関数は、有限の手続きの組み合わせで得られるので、その構成方法に適当に自然数を対応させて数え上げることができる(算術化またはゲーデル化と呼ばれる)。以下の定理は、その数え上げを遂行する帰納的関数が存在する(したがって計算可能である)ことを主張している。

定理 4 以下のような性質を満たす帰納的関数 $\varphi: \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ が存在する。

任意の帰納的関数 $f: \mathbb{N} \rightarrow \mathbb{N}$ について、ある自然数 i が存在して $f(x) = \varphi(i, x)$ が成り立つ。

□

$f(x) = \varphi(i, x)$ であるような i を、 f のインデックスとよぶ。また、 φ は、(1変数の帰納的関数に関する) 万能関数 (**universal function**) とよばれる。

決定不可能性について議論するために、若干の準備をする：

定義 1 \mathbb{N}^n の部分集合 A について、関数 $\chi_A: \mathbb{N}^n \rightarrow \mathbb{N}$ を

$$\chi_A(x_1, \dots, x_n) = \begin{cases} 0 & (x_1, \dots, x_n) \in A \\ 1 & (x_1, \dots, x_n) \notin A \end{cases}$$

で定義する。 χ_A を A の特性関数 (**characteristic function**) という。

□

定義 2 ● \mathbb{N}^n の部分集合 A の特性関数が全域帰納的関数であるとき、 A は帰納的集合 (**recursive set**) であるという。

● \mathbb{N}^n の部分集合 A がある帰納的関数の定義域になっているとき、 A は帰納的可算集合 (**recursively enumerable set**) であるという。

□

帰納的集合とは、要素であるかないかを機械的に判定することが可能(決定可能, **decidable**)な集合である。また、帰納的可算集合とは、要素である場合には停止するが、要素でない場合には停止しないような機械的な手続きが存在する集合である(半決定可能, **semidecidable** という)。

補題 1 帰納的集合の補集合は帰納的集合である。また、帰納的集合は帰納的可算集合である。

□

定理 5 $\mathbb{N} \times \mathbb{N}$ の部分集合 $\{(i, x) \in \mathbb{N}^2 \mid \varphi(i, x) \text{ が定義されている}\}$ は帰納的集合ではない(すなわち決定不可能である)。

□

[証明] 対角線論法を用いる. もしもこれが帰納的集合であるなら, 集合

$$A = \{x \in \mathbf{N} \mid \varphi(x, x) \text{が定義されている}\}$$

も帰納的集合であり, したがって補集合 $\mathbf{N} - A$ もまた帰納的集合である. しかし, 以下の議論から, 実際には, $\mathbf{N} - A$ は帰納的可算集合ではない (したがって帰納的集合ではない) ことがわかる.

$\mathbf{N} - A$ が帰納的可算集合だと仮定しよう. すなわち, ある帰納的関数 $f: \mathbf{N} \rightarrow \mathbf{N}$ が存在して, $\mathbf{N} - A$ は f の定義域になっているとする.

$$\mathbf{N} - A = \{x \in \mathbf{N} \mid f(x) \text{が定義されている}\}$$

そこで, i を f のインデックスとすると,

$$\begin{aligned} \mathbf{N} - A &= \{x \in \mathbf{N} \mid f(x) \text{が定義されている}\} \\ &= \{x \in \mathbf{N} \mid \varphi(i, x) \text{が定義されている}\} \end{aligned}$$

である. すなわち,

$$x \notin A \Leftrightarrow \varphi(i, x) \text{が定義されている}$$

が成り立つ. とくに, $x = i$ の場合,

$$i \notin A \Leftrightarrow \varphi(i, i) \text{が定義されている}$$

ところが, A の定義から,

$$i \in A \Leftrightarrow \varphi(i, i) \text{が定義されている}$$

である. したがって,

$$i \in A \Leftrightarrow i \notin A$$

となり, 矛盾する.

帰納的関数論については, 多くの良書があるが, たとえば

高橋正子 (1991) 計算論: 計算可能性とラムダ計算. コンピュータサイエンス大学講座 24, 近代科学社.

などを参照されたい (この本では, あとで言及するラムダ計算についても詳しく解説されている).

なお, ゲーデル (Gödel, K., 1906-1978) の第一不完全性定理も, この停止性問題とほぼ同様の方法により証明される. 停止性問題では, x をインデックスにもつような帰納的関数を入力 x に適用した結果が未定義のときにのみ $f(x)$ が定義されている, という, 風変わりな帰納的関数 f を想定してその自己適用から矛盾を導いた. 一方, 不完全性定理では, 「 x は $P(x)$ が証明可能であるような (一変数の) 論理式 P のインデックスではない」ということをあらわす (一変数の) 論理式を構成して, その自己適用 (いわゆるゲーデル文) を考える. すなわち, 停止性問題の場合と, 本質的に同じ論法が用いられているのである.

5 対角線論法から不動点へ

ここからは、より一般的な観点から、ラッセルの逆理やカントールの対角線論法などの背後に共通する数学的な仕組みについて考えてみよう。ここでは、一種の不動点定理を拠所にして、種々の同様な現象へのシステムティックなアプローチを試みる。

まず、ややインフォーマルな説明をしよう。 $\varphi: A \times A \rightarrow B$ について、以下のことが成り立っているものとする。

任意の $g: A \rightarrow B$ に対しある $a \in A$ が存在して $g(x) = \varphi(a, x)$ が成り立つ(このような a を g のインデックスと呼ぶ)。

このとき、任意の $f: B \rightarrow B$ は不動点を持つ。具体的には、 $g_0: A \rightarrow B$ を $g_0(x) = f(\varphi(x, x))$ で定義してやり、 $a_0 \in A$ を g_0 のインデックスとすると、 $\varphi(a_0, a_0)$ は f の不動点になっている。実際、 $f(\varphi(a_0, a_0)) = g_0(a_0) = \varphi(a_0, a_0)$ 。

ほとんど自明とも思われる結果だが、ここには、インデックス付けによる数え上げ、対角成分への着目(関数の自分自身のインデックスへの自己適用)による不動点の構成といった、数理論理学や計算の理論の基礎的なアイデアが、端的なかたちであらわれている。

より正確には、有限直積²をもつ任意の圏について、以下の結果が知られている(ローヴィル³の不動点定理)。圏論の言葉になじみのない人には、上記の説明で十分なので、とばしてもらってかまわない。

定理 6 (Lawvere) 対象 A, B と射 $\varphi: A \times A \rightarrow B$ について、以下の条件が成り立っているとす。

任意の $g: A \rightarrow B$ についてある $a: 1 \rightarrow A$ が存在して $g = \varphi \circ (a \times id_A): A \rightarrow B$ が成り立つ。

$$\begin{array}{ccc}
 A & & \\
 \vdots & \searrow \forall g & \\
 \exists a \times id_A \vdots & & \\
 \vdots & & \\
 A \times A & \xrightarrow{\varphi} & B
 \end{array}$$

このとき、任意の $f: B \rightarrow B$ は不動点を持つ。すなわち、ある $b: 1 \rightarrow B$ が存在して $f \circ b = b$ となる。 \square

証明はさきほどのインフォーマルな説明を圏論ふう丁寧にやりなおせばよい(これは圏論の知識のある方への練習問題とする)。

6 不動点定理から具体例を見直す

以下では、定理 6(のインフォーマルな説明)を用いて、お馴染の例を見直してみることにする。

²実はもう少し弱い条件でも成立する。

³Lawvere, W., 1937-

例 1 ラッセルのパラドックス. S を, すべての集合の集合としよう (もちろんこの仮定がまずいのだけれど, 矛盾を導くために, 少しのあいだ目をつぶろう). 関数 $\varphi: S \times S \rightarrow 2$ (ここで $2 = \{\text{true}, \text{false}\}$) を,

$$\varphi(x, y) = \begin{cases} \text{true} & y \in x \text{ であるとき} \\ \text{false} & y \notin x \text{ であるとき} \end{cases}$$

と定義する. 任意の $g: S \rightarrow 2$ について, $a = \{x \in S \mid g(x) = \text{true}\} \in S$ とおくと, 容易にわかるように $g(x) = \varphi(a, x)$ が成り立つ. つまり a は g のインデックスである. そこで, 定理 6 を用いて, 任意の $f: 2 \rightarrow 2$ の不動点を得ることができる. とくに, 否定演算子 $\neg: 2 \rightarrow 2$ (すなわち $\neg(\text{true}) = \text{false}$, $\neg(\text{false}) = \text{true}$) の不動点は以下のように構成される. まず,

$$g_0(x) = \neg(\varphi(x, x)) = \begin{cases} \text{true} & x \notin x \text{ であるとき} \\ \text{false} & x \in x \text{ であるとき} \end{cases}$$

で $g_0: S \rightarrow 2$ を定める. g_0 のインデックス a_0 は

$$a_0 = \{x \in S \mid g_0(x) = \text{true}\} = \{x \in S \mid x \notin x\}$$

で与えられる. そこで $\varphi(a_0, a_0)$ を計算すると

$$\begin{aligned} \varphi(a_0, a_0) &= \begin{cases} \text{true} & a_0 \in a_0 \text{ であるとき} \\ \text{false} & a_0 \notin a_0 \text{ であるとき} \end{cases} \\ &= \begin{cases} \text{true} & \varphi(a_0, a_0) = g_0(a_0) = \text{false} \text{ であるとき} \\ \text{false} & \varphi(a_0, a_0) = g_0(a_0) = \text{true} \text{ であるとき} \end{cases} \\ &= \neg(\varphi(a_0, a_0)) \end{aligned}$$

しかし, 明らかにこれは矛盾である. (正確には, ある体系が矛盾しているとは, その体系の中で $\text{true} = \text{false}$ が導かれてしまうことをいう. これは否定演算子が不動点を持つことと同値である.) \square

問題 2 この不動点定理を用いた証明を, はじめのラッセルのパラドックスのそれと比較せよ.

例 2 同様に, カントールの対角線論法 (定理 1) も定理 6 の一例になっている. 集合 X について, X 上の集合 2^X から X への単射が存在するとは, X から 2^X への全射が存在することと同値である (確かめよ). しかし, $\psi: X \rightarrow 2^X$ をそのような全射とすると, $\varphi(x, y) = \psi(x)(y)$ で定められる $\varphi: X \times X \rightarrow 2$ は定理 6 の仮定をみたす (任意の $g: X \rightarrow 2$ について $g = \varphi(a, -)$ をみたす $a \in X$ が存在する). したがって任意の $f: 2 \rightarrow 2$ は不動点をもつが, これはもちろん矛盾である (前の例と同様, 否定演算子の不動点を考えてみよ). \square

さらに, ゲーデルの不完全性定理や停止性問題なども, この不動点定理の一例と考えることができる. いずれも, 論理式や帰納的関数の数え上げ (ゲーデル化) をもとにして, その対角成分に着目することにより, 一見トリッキーな論理式や再帰関数が, 一種の不動点として得られる (あるいは存在が否定される) というものである.

興味をもたれた方へ: この不動点定理の出典は

Lawvere, F.W. (1969) Diagonal arguments and cartesian closed categories. *Category Theory, Homology Theory and their Applications II*, Springer Lecture Notes in Mathematics **92**, pp. 134–145.

である。幸い、以下のような平易な入門書で概要を知ることができる。

森 毅 (1976) 無限集合. 数学ワンポイント双書 4, 共立出版.

Advanced Topic

ラムダ計算とパラドキシカル結合子

ラムダ計算 (**lambda calculus**, λ -calculus) は, プログラムとデータの区別がまったくない, 理想化された計算体系である. 数学的には, ラムダ計算のモデル D は, $D \simeq D^D$ をみたすような D でなくてはならない. すでに述べたように, そのような D は, 集合と関数の世界では自明なもの (一点集合) しか存在しないが, 計算可能な関数 (帰納的関数) にだけ着目した世界や, 後で述べる CPO と連続関数の世界では, $D \simeq D^D$ をみたす自明でない D が存在する.

さて, D をそのようなラムダ計算のモデルとし, $\psi : D \xrightarrow{\sim} D^D$ とすると, $\varphi(x, y) = \psi(x)(y)$ で定まる $\varphi : D \times D \rightarrow D$ は, 定理 6 の仮定をみたす. すなわち, 任意の $g : D \rightarrow D$ について, $a = \psi^{-1}(g) \in D$ とすれば, $g(x) = \varphi(a, x)$ が成り立つ. したがって任意の $f : D \rightarrow D$ は不動点

$$\varphi(\psi^{-1}(g_0), \psi^{-1}(g_0)) = g_0(\psi^{-1}(g_0))$$

(ただし $g_0(x) = f(\varphi(x, x)) = f(\psi(x)(x))$) をもつ.
ラムダ計算の記法に即せば, この不動点は

$$(\lambda x. f(x x)) (\lambda x. f(x x))$$

と表現される. これはパラドキシカル結合子 (を f に適用したもの) $\mathbf{Y} f$ として知られているものである. ラムダ計算の規則から, $\mathbf{Y} f = f(\mathbf{Y} f)$ が成り立つことがわかる. パラドキシカル結合子は, 自分自身を呼び出すような (再帰的な) 計算のラムダ計算における解釈を与える際に重要な役割を果たす. ラムダ計算に馴染みがなくても,

$$\begin{array}{lll} \lambda x. \dots & \text{を} & \{x \mid \dots\} \quad (\dots \text{をみたす } x \text{ 全体}) \\ M N & \text{を} & N \in M \quad (N \text{ は } M \text{ の要素}) \\ f(\dots) & \text{を} & \neg(\dots) \quad (\dots \text{ の否定}) \end{array}$$

と読み替えれば, 実は $\mathbf{Y} f$ は以下のようなになる:

$$\{x \mid x \notin x\} \in \{x \mid x \notin x\}$$

したがって, $\mathbf{Y} f = f(\mathbf{Y} f)$ はラッセルの逆理に他ならない.

(だからといって, ラムダ計算が矛盾しているというわけではない. むしろ, ラムダ計算のようにすべてのものが不動点をもつ世界では, 否定「 \neg 」に相当するものを表現することはできない, と考えるのが妥当である.)

Part II

矛盾したものを構成する

Computer science contradicts mathematics.
*Peter Freyd*⁴

ここまで、 $2^X \simeq X$ となるような集合 X が存在しないことをカントールの対角線論法を用いて説明し、それが、より一般的な不動点定理の一例として理解できることを示した。

以下では、実際に、その一見矛盾しているように見える例を、完備半順序集合 (CPO) の世界で構成する方法を紹介する。具体的には、与えられた CPO A について、 $[X \rightarrow A] \simeq X$ をみたすような CPO X を構成する方法を考える。

1 完備半順序集合と連続関数

ここでは、必要最小限の事柄のみを解説する。より詳しくは、たとえば

田辺誠, 中島玲二, 長谷川真人 (1999) コンピュータサイエンス入門: 論理とプログラム意味論. 岩波書店.

の第5章を参照されたい。

定義 3 (CPO) 半順序集合 (D, \sqsubseteq) は、最小元をもち、また、任意の単調増加列 $d_0 \sqsubseteq d_1 \sqsubseteq d_2 \sqsubseteq \dots$ について上限 $\bigsqcup d_n$ が存在するとき、完備半順序集合 (Complete Partial Order, CPO) と呼ばれる。□

D が CPO であるとき、その最小元を \perp_D または単に \perp であらわす。

定義 4 (連続関数) CPO D, E について、関数 $f : D \rightarrow E$ は、以下の条件をみたすとき連続 (continuous) であるという。

- 単調性: $d \sqsubseteq d'$ ならば $f(d) \sqsubseteq f(d')$
- 連続性: 任意の単調列 $d_0 \sqsubseteq d_1 \sqsubseteq d_2 \sqsubseteq \dots$ について $f(\bigsqcup d_n) = \bigsqcup f(d_n)$

□

補題 2 (関数空間) CPO D, E について、 D から E への連続関数全体からなる集合 $[D \rightarrow E]$ は、以下のように定まる半順序 \sqsubseteq に関して CPO である。

$$f \sqsubseteq g \Leftrightarrow \text{任意の } d \in D \text{ について } f(d) \sqsubseteq g(d)$$

□

⁴Freyd, P. (1991) Algebraically complete categories. *Category Theory*, Springer Lecture Notes in Mathematics 1488, pp. 95–104. 計算機科学で必要となる数学構造が、常識的な数学の世界とは相容れないことについて言及して。Freyd (1935-) は、圏論など幅広い分野で仕事をしてきた数学者。

$[D \rightarrow E]$ の最小元 $\perp_{[D \rightarrow E]}$ は, 任意の $d \in D$ について $\perp_{[D \rightarrow E]}(d) = \perp_E$ である恒等関数である. また, $[D \rightarrow E]$ の単調列 $f_0 \sqsubseteq f_1 \sqsubseteq f_2 \sqsubseteq \dots$ の上限 $\bigsqcup f_n$ は, $(\bigsqcup f_n)(d) = \bigsqcup f_n(d)$ で与えられる.

命題 1 (最小不動点) $CPO D$ と連続関数 $f: D \rightarrow D$ について, $f(d) = d$ をみたす $d \in D$ で最小のものが存在し, それは $\bigsqcup f^n(\perp)$ で与えられる. \square

2 最小不動点の発想

以上の準備のもとで, $[X \rightarrow A] \simeq X$ をみたすような $CPO X$ を求める方法を考える. 計算を簡単にするため, 以下では, A が二点からなる $CPO \Omega = \{\perp \sqsubseteq \top\}$ である場合だけを扱う.

CPO 上の連続関数 $f: D \rightarrow D$ の最小不動点は, (加算無限の) 単調増加列

$$\perp, f(\perp), f^2(\perp), \dots, f^n(\perp), \dots$$

の上限として得られるのであった. 同じように, $[X \rightarrow \Omega] \simeq X$ をみたすような X も, $CPO D$ に $CPO [D \rightarrow \Omega]$ を対応させる関数の“最小不動点”, すなわち適当な $CPO X_0$ から始まる無限列

$$X_0, [X_0 \rightarrow \Omega], [[X_0 \rightarrow \Omega] \rightarrow \Omega], [[[X_0 \rightarrow \Omega] \rightarrow \Omega] \rightarrow \Omega], \dots$$

の“上限”として得られるのではないかと期待するのは自然な発想である. 以下では, この直感的なアイデアを, 実際に計算しながら検証していく.

準備として, 以後頻繁に用いる CPO 間の関係“ \simeq ”の正確な定義を確認しておこう.

定義 5 $CPO D$ と E について, D と E が同型であるとは, 連続関数 $f: D \rightarrow E$ および $g: E \rightarrow D$ が存在して $g \circ f = id_D$ と $f \circ g = id_E$ をみたすことをいう. このとき, f は D から E への同型な連続関数であるといい, g のことを f^{-1} と書く. また, D と E が同型であることを, $D \simeq E$ と書く. \square

補題 3 任意の $CPO D$ について, $D \simeq D$ がなりたつ. また, $D \simeq E$ ならば $E \simeq D$ である. さらに, $D \simeq E$ かつ $E \simeq F$ ならば, $D \simeq F$ である. \square

3 最初の試み

CPO の無限列 $\{X_0, X_1, X_2, \dots, X_n, \dots\}$ を, 以下のように定める.

$$\begin{aligned} X_0 &= \{0\} && (\text{一点 } 0 \text{ だけからなる } CPO) \\ X_{i+1} &= [X_i \rightarrow \Omega] && (X_i \text{ から } \Omega \text{ への連続関数からなる } CPO) \end{aligned}$$

明らかに X_0 は CPO である. また, CPO は関数空間の構成について閉じており, Ω も CPO であるから, (帰納法により) 任意の n について X_n が CPO であることがわかる.

補題 4 D_n ($n = 0, 1, 2, \dots$) を, $n + 1$ 個の要素からなる CPO

$$\{0 \sqsubseteq 1 \sqsubseteq 2 \sqsubseteq \dots \sqsubseteq n\}$$

とする. このとき, 任意の n について $X_n \simeq D_n$ がなりたつ. □

[証明] n に関する帰納法を用いる. $X_0 = D_0$ だから, 明らかに $X_0 \simeq D_0$ である. $X_n \simeq D_n$ と仮定して, $X_{n+1} \simeq D_{n+1}$ がなりたつことを示そう. $X_n \simeq D_n$ より, $X_{n+1} = [X_n \rightarrow \Omega] \simeq [D_n \rightarrow \Omega]$ である. $[D_n \rightarrow \Omega]$ の要素は D_n から Ω への連続関数であるが, それは, 連続関数の定義により, ある $0 \leq k \leq n + 1$ について

$$f_k^n(i) = \begin{cases} \perp & i + k \leq n \text{ のとき} \\ \top & i + k > n \text{ のとき} \end{cases}$$

というかたちになっていなくてはならない. とくに f_0^n はつねに \perp を返す定数関数, また f_{n+1}^n はつねに \top を返す定数関数である. したがって, $[D_n \rightarrow \Omega]$ は, $n + 2$ 個の要素 $f_0^n, f_1^n, \dots, f_n^n, f_{n+1}^n$ を持つことがわかる. また, これらは, 順序

$$f_0^n \sqsubseteq f_1^n \sqsubseteq \dots \sqsubseteq f_n^n \sqsubseteq f_{n+1}^n$$

をなすので, $[D_n \rightarrow \Omega] \simeq D_{n+1}$ である. $X_{n+1} \simeq [D_n \rightarrow \Omega]$ だったから, $X_{n+1} \simeq D_{n+1}$ がなりたつ.

この結果から, 我々が考察している無限列は (同型なもので置き換えると)

$$\{0\}, \{0 \sqsubseteq 1\}, \{0 \sqsubseteq 1 \sqsubseteq 2\}, \dots, \{0 \sqsubseteq 1 \sqsubseteq 2 \sqsubseteq \dots \sqsubseteq n\}, \dots$$

であることがわかった. 直感的には, これらは単調に増加していく CPO の列になっていると言ってよさそうである. では, その“上限”はなんだろうか? 単純にこれらを全部あわせた

$$\{0 \sqsubseteq 1 \sqsubseteq 2 \sqsubseteq \dots \sqsubseteq n \sqsubseteq \dots\}$$

だろうか? 一見これでよさそうだが, 問題がある. まず, 単純なことだが, この順序集合は CPO ではない. 単調列 $0 \sqsubseteq 1 \sqsubseteq \dots \sqsubseteq n \sqsubseteq \dots$ の上限が存在しないのである. さいわい, 簡単な解決法として, “無限大” ∞ を追加してやれば, CPO

$$\{0 \sqsubseteq 1 \sqsubseteq 2 \sqsubseteq \dots \sqsubseteq n \sqsubseteq \dots \sqsubseteq \infty\}$$

を得ることができる. この CPO を Θ とよぶことにしよう. では, $[\Theta \rightarrow \Omega] \simeq \Theta$ だろうか?

命題 2 $[\Theta \rightarrow \Omega] \simeq \Theta$ はなりたたない. □

[証明] 実際に $[\Theta \rightarrow \Omega]$ を計算してみればよい. Θ から Ω への連続関数は, ある $k \geq 0$ について

$$f_k(x) = \begin{cases} \top & k \sqsubseteq x \text{ のとき} \\ \perp & \text{その他のとき} \end{cases}$$

というかたちをしているか, または定数関数 $f_\infty(i) = \perp$ でなくてはならない. これらの間の順序は,

$$f_\infty \sqsubseteq \dots \sqsubseteq f_n \sqsubseteq \dots \sqsubseteq f_2 \sqsubseteq f_1 \sqsubseteq f_0$$

(いいかえれば $-\infty \sqsubseteq \dots \sqsubseteq -2 \sqsubseteq -1 \sqsubseteq 0$) となり, これは Θ と同型ではない(確かめよ). $[[\Theta \rightarrow \Omega] \rightarrow \Omega] \simeq \Theta$ がなりたつことは同様の計算によって確かめられる(これも練習問題とする).

問題 3 $[[\Theta \rightarrow \Omega] \rightarrow \Omega] \simeq \Theta$ もなりたたないことを確かめよ.

4 埋め込みと射影

以上の試みでは, なにがいけなかったのだろうか? 無限列

$$\{0\}, \{0 \subseteq 1\}, \{0 \subseteq 1 \subseteq 2\}, \dots, \{0 \subseteq 1 \subseteq 2 \subseteq \dots \subseteq n\}, \dots$$

を考えたところまでは問題がないのだが, それから安易に(和集合として)“上限” Θ を計算したのがどうもまずいようである.

実は, この無限列を“単調増加列”とみなす方法はひとつとおりにはきまらない. 正確に説明すると:

定義 6 CPO D と E について, $D \sqsubseteq E$ であるとは, 連続関数 $e: D \rightarrow E$ および $p: E \rightarrow D$ が存在して $p \circ e = id_D$ と $e \circ p \sqsubseteq id_E$ をみたすことをいう. e のことを埋め込み, また p のことを射影とよぶ. \square

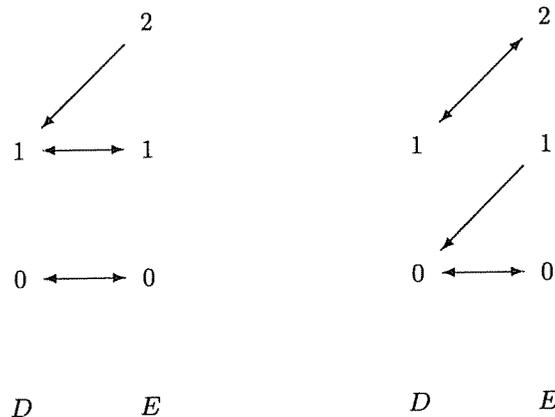
$D \sqsubseteq E$ となるための埋め込みと射影の取り方は, ひとつとおりとは限らない. たとえば, $D = \{0 \subseteq 1\}$, $E = \{0 \subseteq 1 \subseteq 2\}$ とすると, $D \sqsubseteq E$ とするための埋め込み e と射影 p は,

$$e(0) = 0, e(1) = 1, p(0) = 0, p(1) = p(2) = 1$$

とすることも, また

$$e(0) = 0, e(1) = 2, p(0) = p(1) = 0, p(2) = 1$$

とすることもでき, これらは D より E が“大きい”とみなす二通りの方法をあらわしている. 図示すると以下ようになる. 左から右への矢印は埋め込み e の作用を, また右から左への矢印は射影 p の作用をそれぞれあらわす.



なお, 埋め込みを定めると, 対応する射影はただひとつ定まり, また, 射影を定めると対応する埋め込みもただひとつに定まる. 証明は練習問題とする.

問題 4 $e: D \rightarrow E$, $p, p': E \rightarrow D$ について, e, p と e, p' がともに埋め込みと射影の組をなすならば, $p = p'$ であることを示せ. また, $e, e': D \rightarrow E$, $p: E \rightarrow D$ について, e, p と e', p がともに埋め込みと射影の組をなすならば, $e = e'$ であることを示せ.

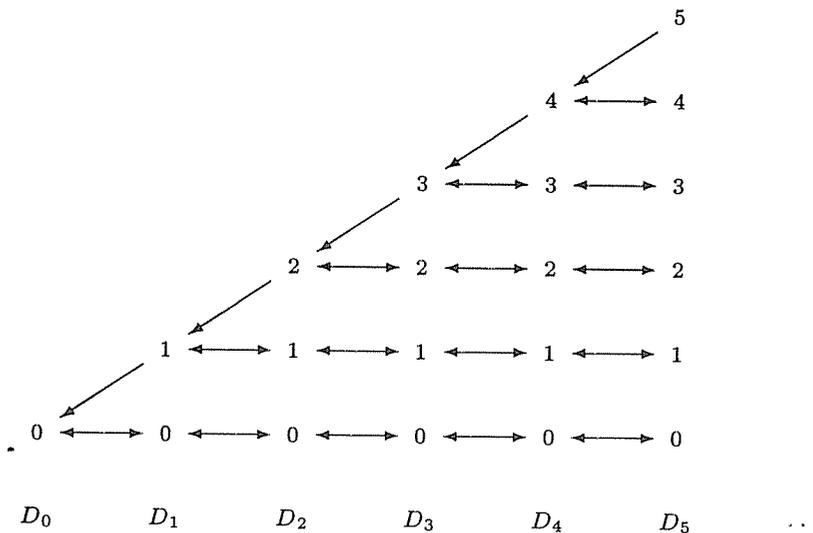
問題 5 $e: D \rightarrow E$ と $p: E \rightarrow D$ が埋め込みと射影になっているとき, e は D の最小元を E の最小元に写すことを示せ.

5 なぜ失敗したか

特に, Θ を得た発想は, 以下の図で理解することができる. ここでは, 単純に, 埋め込み $e_n : D_n \rightarrow D_{n+1}$ と射影 $p_n : D_{n+1} \rightarrow D_n$ を

$$e_n(x) = x, \quad p_n(x) = \begin{cases} x & x \leq n \text{ のとき} \\ n & x = n + 1 \text{ のとき} \end{cases}$$

と定めている.



この図で, 射影によりつながった無限列 $(0, 1, 2, \dots, n, n, n, \dots)$ を n と, また (無限に増加していく) 無限列 $(0, 1, 2, \dots, n, n+1, \dots)$ を ∞ と同一視して考えることにより, Θ が得られるのである.

ところが, この埋め込みと射影の定め方は, $[X \rightarrow \Omega] \simeq X$ をみたく X を見つけるためにはうまく働かない. 例として, D_0 から D_1 , また D_1 から D_2 への埋め込みおよび射影がどのようなになっているべきか考えよう.

まず, $D_0 = \{0\}, D_1 = \{0 \sqsubseteq 1\}$ であった. この場合には埋め込みと射影はひとつとおりにしか存在しない. その埋め込み $e_0 : D_0 \rightarrow D_1$ は 0 を 0 に写し, また射影 $p_0 : D_1 \rightarrow D_0$ は 0 も 1 も 0 に写す.

次に, $D_2 = \{0 \sqsubseteq 1 \sqsubseteq 2\}$ であった. しかし, D_1 は,

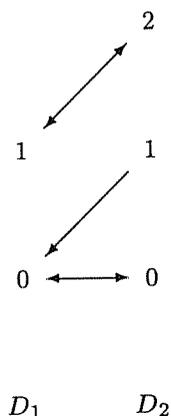
$$X_1 \simeq [D_0 \rightarrow \Omega] = \{f_0^0 \sqsubseteq f_1^0\}$$

また, D_2 は,

$$X_2 \simeq [D_1 \rightarrow \Omega] = \{f_0^1 \sqsubseteq f_1^1 \sqsubseteq f_2^1\}$$

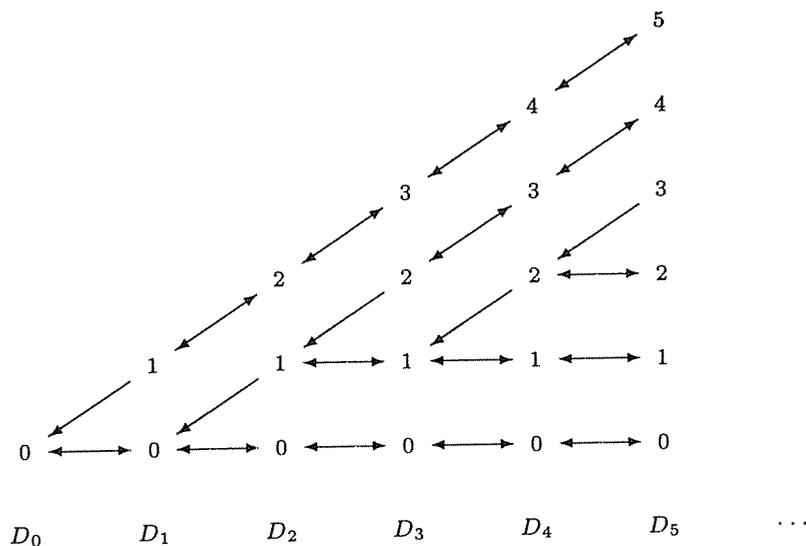
として得られたものであり, $D_1 \sqsubseteq D_2$ とするための正しい埋め込みは, $f_0^0 : D_0 \rightarrow \Omega$ をその自然な拡張である $f_0^0 \circ p_0 = f_1^0 : D_1 \rightarrow \Omega$ に, また $f_1^0 : D_0 \rightarrow \Omega$ をその拡張である $f_1^0 \circ p_0 = f_2^0 : D_1 \rightarrow \Omega$ に, それぞれ対応させるものでなくてはならない. D_1 と D_2 の要素について言い換えると, 埋め込み $e_1 : D_1 \rightarrow D_2$ は 0 を 0 に, また 1 を 2 に写さなくてはならない. 一方, 射影の方は, $f_1^0 : D_1 \rightarrow \Omega$ をその自然な制限である $f_1^0 \circ e_0 = f_1^0 : D_0 \rightarrow \Omega$ に, また f_1^1 を $f_1^1 \circ e_0 = f_0^1$ に, さらに f_2^1 を $f_2^1 \circ e_0 = f_1^1$ に, それぞれ対応させるものである. D_1 と D_2 について言い換

えると, 射影 $p_1 : D_2 \rightarrow D_1$ は, 0と1を0に, また2を1に写すものである. これを図示すると以下のようなになる.



6 正しい解の構成 — 逆極限法

同様に, D_2 から D_3 への埋め込みと射影, D_3 から D_4 への埋め込みと射影, ..., も, 関数が自然な拡張・制限に対応されるように定めていくことができる. その結果を途中まで示したのが以下の図である.



この埋め込み・射影の“上限”として得られるCPOが Θ ではないことは, 容易

に想像がつくだろう。実際,

- 0 を無限列 $(0, 0, 0, 0, \dots)$ と
- 1 を無限列 $(0, 0, 1, 1, 1, \dots)$ と
- ⋮
- n を無限列 $(0, 0, 1, 1, 2, 2, \dots, n, n, n, \dots)$ と
- ⋮
- ∞ を無限列 $(0, 0, 1, 1, 2, 2, \dots, m, m, m+1, m+1, \dots)$ と
- ⋮
- n' を無限列 $(0, 0, 1, 1, 2, 2, \dots, n, n+1, n+2, \dots)$ と
- ⋮
- $1'$ を無限列 $(0, 0, 1, 2, 3, \dots)$ と
- $0'$ を無限列 $(0, 1, 2, 3, \dots)$ と

同一視することにより, CPO

$$\Phi = \{0 \sqsubseteq 1 \sqsubseteq 2 \sqsubseteq \dots \sqsubseteq \infty \sqsubseteq \dots \sqsubseteq 2' \sqsubseteq 1' \sqsubseteq 0'\}$$

が得られる.

定理 7 $[\Phi \rightarrow \Omega] \simeq \Phi$ がなりたつ. □

[証明] $x \in \Phi$ に対し連続関数 $\psi_x : \Phi \rightarrow \Omega$ を以下の表で定める (ψ_x を y に適用した結果 $\psi_x(y)$ を, ψ_x 行の y 列に示す).

	0	1	...	$n-1$	n	...	∞	...	n'	$n-1'$...	$1'$	$0'$
ψ_0	⊥	⊥	...	⊥	⊥	...	⊥	...	⊥	⊥	...	⊥	⊥
ψ_1	⊥	⊥	...	⊥	⊥	...	⊥	...	⊥	⊥	...	⊥	⊥
⋮													
ψ_n	⊥	⊥	...	⊥	⊥	...	⊥	...	⊥	⊤	...	⊤	⊤
⋮													
ψ_∞	⊥	⊥	...	⊥	⊥	...	⊥	...	⊤	⊤	...	⊤	⊤
⋮													
$\psi_{n'}$	⊥	⊥	...	⊥	⊤	...	⊤	...	⊤	⊤	...	⊤	⊤
⋮													
$\psi_{1'}$	⊥	⊤	...	⊤	⊤	...	⊤	...	⊤	⊤	...	⊤	⊤
$\psi_{0'}$	⊤	⊤	...	⊤	⊤	...	⊤	...	⊤	⊤	...	⊤	⊤

写像 $\psi : x \mapsto \psi_x$ が Φ から $[\Phi \rightarrow \Omega]$ への同型な連続関数となっていることは容易に確認できる.

問題 6 $\psi : x \mapsto \psi_x$ が同型な連続関数であることを示せ.

一般に, CPO A について, $[X \rightarrow A] \simeq X$ をみたす X を求め, これに以前解説した不動点定理 (定理 6) を適用することにより, A 上の連続関数の不動点を構成することができる. このことを Ω と Φ にあてはめると, 以下のようなになる.

系 1 任意の連続関数 $g : \Omega \rightarrow \Omega$ について, $h : \Phi \rightarrow \Omega$ を $h(x) = g(\psi_x(x))$ と定め, $a = h(\psi^{-1}(h)) \in \Omega$ とすると, a は g の不動点である. □

[証明]

$$\begin{aligned}
 a &= h(\psi^{-1}(h)) \\
 &= g(\psi_{\psi^{-1}(h)}(\psi^{-1}(h))) \\
 &= g(h(\psi^{-1}(h))) \\
 &= g(a)
 \end{aligned}$$

問題 7 このようにして求めた a は, g の最小不動点と一致する. 確かめよ.

なお, $[X \rightarrow \Omega] \simeq X$ をみたす解は Φ だけではない (しかし Φ がもっとも自然なものであることは知られている). たとえば, Φ に新しい要素 ∞' を追加した CPO

$$\Phi' = \{0 \sqsubseteq 1 \sqsubseteq 2 \sqsubseteq \dots \sqsubseteq \infty \sqsubseteq \infty' \sqsubseteq \dots \sqsubseteq 2' \sqsubseteq 1' \sqsubseteq 0'\}$$

も解になる.

問題 8 Φ' が $[\Phi' \rightarrow \Omega] \simeq \Phi'$ をみたすことを確かめよ. また, この Φ' を用いて, 系と同様にして Ω 上の連続関数の不動点を構成し, それが最小不動点とは一致しないことを確かめよ.

ここで紹介した方法 (逆極限法とも呼ばれる) は, ラムダ計算やプログラミング言語のモデルを構成するための基本的な技法のひとつである. 1970 年頃にスコット (Scott, D., 1932-) によって (ラムダ計算の自明でないモデル $D_\infty \simeq [D_\infty \rightarrow D_\infty]$ の構成方法として) 発見されて以来, 多くの人によって研究・応用されている. 関心を持たれた方は, 以下のような文献を参照されたい.

中島玲二 (1982) 数理情報学入門—スコット・プログラム理論. 数理科学ライブラリー 3, 朝倉書店.

横内寛文 (1994) プログラム意味論. 情報科学講座 7, 共立出版.

Gunter, C.A. (1992) **Semantics of Programming Languages – Structures and Techniques**. MIT Press.

Advanced Topic

不動点としての再帰プログラム

ここで紹介した構成は, 自分自身を呼び出す再帰的な関数定義, たとえば

$$\text{factorial}(n) = \begin{cases} 1 & n = 0 \text{ のとき} \\ n \times \text{factorial}(n-1) & n \geq 1 \text{ のとき} \end{cases}$$

に対応するプログラムを与えるために用いることができる. この関数 $\text{factorial} : \mathbb{N} \rightarrow \mathbb{N}$ は,

$$F(f)(n) = \begin{cases} 1 & n = 0 \text{ のとき} \\ n \times f(n-1) & n \geq 1 \text{ のとき} \end{cases}$$

で定まる汎関数 $F : (\mathbb{N} \rightarrow \mathbb{N}) \rightarrow (\mathbb{N} \rightarrow \mathbb{N})$ の不動点であること, すなわち $F(\text{factorial}) = \text{factorial}$ が成り立つことに注意されたい.

一方, $X \simeq (X \rightarrow (\mathbb{N} \rightarrow \mathbb{N}))$ であるようなデータ型 X を用いて, $(\mathbb{N} \rightarrow \mathbb{N})$ 上の汎関数の不動点を得ることができる. 特に, factorial を F の不動点として得ることができる. このことを, プログラミング言語 ML^a で表現したのが, 以下のプログラム例である.

```
datatype X = psi_inv of X -> (int -> int);
fun psi (psi_inv (f)) = f;
(* psi: X -> (X -> (int -> int)),
   psi_inv: (X -> (int -> int)) -> X *)

fun fixpoint(g) =
  let fun h(f) = g(fn x => psi(f)(f)(x))
      in h(psi_inv(h))
  end;
(* fixpoint : ((int -> int) -> (int -> int)) -> (int -> int) *)

fun F(f)(n) = if n=0 then 1 else n * f(n-1);
(* F: (int -> int) -> (int -> int) *)

val factorial = fixpoint(F);
(* factorial: int -> int *)

factorial(10);
(* 10! = 3628800 *)
```

^aプログラミング言語MLについては, 以下の優れた解説書がある.

大堀淳 (2001) プログラミング言語 Standard ML 入門. 共立出版.