きょうの予定 Nelson による、数学的帰納法を使わない数学の再構築の紹介の続き。

- predicative coding
- 集合の表現
- 有限概念の分析

目 次

8 自然数列の不定性 (3)

8.1 集合論

8.1.1 Encoding

数の有限列を次のように coding する。その数を 2 進表示し、それらを並べて区切りとして 2 を入れる。得られた $0, 1, 2$ の列を 4 進数とみなす。

例) $3, 0, 11, 32$ という数列は、まず、2 進表示 $11, 0, 111, 100000$ に直し、最後に 21120211121000002 にする。

以下、もう少し詳しく述べる。

- $|x|_b = q \overset{def}{\iff} q$ は b のべき乗 $\wedge\ x \neq 0 \wedge q \leq x < q \cdot b$ otherwise $q = 1$.

  例えば $|12|_2 = 8$, $|30|_2 = 16$, $1101010011_4 = 4^9$. 数 x が $k > 0$ 桁の b 進数で表されるとき $|x|_b$ は b^{k-1} である。

- $Rm(b, Qt(q, x))$: 数 x の b 進展開の第 q 桁の数字。ここで、桁の呼称は、右から、$1, b, b^2, b^3, \cdots$ としている。

- 例 $x = 22 = 10110_2$ について：

桁の名前	16	8	4	2	1
その桁の数	1	0	1	1	0

$$\begin{aligned} Rm(2, Qt(16, 22)) &= 1 \\ Rm(2, Qt(8, 22)) &= 0 \\ Rm(2, Qt(4, 22)) &= 1 \\ Rm(2, Qt(2, 22)) &= 1 \\ Rm(2, Qt(1, 22)) &= 0 \end{aligned}$$

- $Enc\, x = z \overset{def}{\iff} \forall q(q \text{ is a power of two } \Rightarrow Rm(2, Qt(q, x)) = Rm(4, Qt(q \cdot q), z))$. 例えば $Enc\, 10110_2 = 10110_4$.

- $enc(q_1, q_2, x, a) \overset{def}{\iff} q_1, q_2$ は 4 のべき $\wedge\ Rm(4, Qt(q_1, a) = Rm(4, Qt(q_2, a)) = 2$ $\wedge\ q_2 = 4 \cdot |Enc\, x|_4 \cdots q_1 \wedge Rm(q_2/(q_1 \cdot 4), Qt(q_1 \cdot 4, a)) = Enc\, x$.

  例えば

$$\begin{aligned} enc(4^0, 4^5, 1011_2, 21011211012_4) &= 1101_2, \\ enc(4^5, 4^{10}, 1011_2, 21011211012_4) &= 1011_2. \end{aligned}$$

8.2 集合論

集合は重複のないリストとして表現する。

- $x \in a \overset{def}{\iff} \exists q_1\, \exists q_2\, enc(q_1, q_2, x, a)$. 例えば

$$11011_2 \in 211011211110210102_4.$$

- a is a set $\overset{def}{\iff} \forall b(b < a \Rightarrow \exists x\ (x \in a \wedge x \notin b))$.

- $\left\{ x \in y \;\middle|\; A \right\} = z \overset{def}{\iff} \min_z \forall x\ (\ x \in y \wedge A \Rightarrow x \in z)$.

- $\langle x, y \rangle = (x + y) \cdots (x + y) + y$.

- f is a function $\overset{def}{\iff}$ f is a set $\wedge \forall w\ (w \in f \Rightarrow \exists x\ \exists y \langle x, y \rangle = w\ ) \wedge \forall x \forall y_1 \forall y_2\ (\langle x, y_1 \rangle \in f \wedge \langle x, y_2 \rangle \in f \Rightarrow y_1 = y_2\ )$.

- $f(x) = y \overset{def}{\iff} f$ is a function $\wedge \langle x, y \rangle \in f$ otherwise $y = 0$.

8.3 べきの定義

- $exp(x,k,f) \overset{def}{\iff} f$ is a function $\wedge\ f(0)=1 \wedge \forall i(i \in Domf \Leftrightarrow i \leq k) \wedge \forall i(i < k \ \Rightarrow\ f(i+1) = x \cdot f(i))$.
- $\epsilon(k) \overset{def}{\iff} \forall x \exists f\ exp(x,k,f)$.
- ϵ は inductive だが bounded ではない。
- $x^{\uparrow k} = z \overset{def}{\iff} \epsilon^3(k) \wedge \exists f\ (exp(x,k,f)\ \wedge\ f(k) = z)$. これも bounded ではない。
- ϵ で相対化しても ϵ が成り立つかどうかわからない。

8.4 有限でない自然数

ここは、＜ふつうの＞数学で議論する。ペアノの公理系に、arity 1 の述語 ϕ と、公理

(Fin.) $\phi(0)\ \wedge\ (\phi(x)\ \Rightarrow\ \phi(Sx))$.

を添加する。このとき、$\phi(N)$ が証明できない数 N が以下のように構成できる (Simon Kochen)。

- ゲーデルの不完全定理の証明により、個々の閉項 n については $C[n]$ が証明できるが、$\forall n\ C[n]$ は証明できないような論理式 C がある。

  構成の概略は次の通り。

  - $\lceil P \rceil$ を論理式 P のゲーデル数とする。論理式の有限列も数で表し、それをゲーデル数という。
  - $ProofPair(x,y)$ は、x が論理式 P のゲーデル数であるとき,y はその証明のゲーデル数であることを表す論理式とする。
  - $P := \forall z \neg ProofPair(x,z)$ は x は証明できない論理式のゲーデル数であることを表す。このとき $P(\lceil P \rceil)$ がゲーデル文で、証明できないし反駁もできないことがわる。(実際これが証明されると P が証明できないことになり矛盾するので、これは証明できない。従って P は正しい。正しいので、反駁できるはずはない。)
  - $C[z] := \neg ProofPair(P(\lceil P \rceil), z)$ とおく。このとき、$P(\lceil P \rceil)$ が証明できないので、$C[n]$ はどの n についても証明できる（これは ProofPair が算術的述語であることによる)。しかし、$\forall n C[n]$ が証明できないことがわかっている。

- $C[n]$ を使って、$\exists n\ D[n]$ は示せるが、どの項 n についても $\neg D[n]$ であるような論理式 D が作れる。実際

$$D[n] := C[n]\ \Rightarrow\ \forall m C[m]$$

とおけばよい。なぜならば

- $\exists n\ D[n]$ は $\forall n C[n] \Rightarrow \forall m C[m]$ と同値。
- $D[n]$ となる n があれば、$C[n]$ であることがわかっているので、$\forall m\ C[m]$ となり、ゲーデルの定理の結論と矛盾する。

- さて、ペアノの理論に各閉項ごとに公理 $\neg D[n]$ を添加しさらに定数 N と公理

$$N = z \overset{def}{\iff} \min_z D[z]$$

を付け加える。これは無矛盾なので、モデルを持つ。その中に 0 と S で閉じた最小の集合 M をとると、これは、ペアノの理論のモデルであり、添加した公理 $\neg D[n]$ も当然満たす。さらに ϕ と公理 (Fin) とを加えた理論は ϕx を $x \in M$ と解釈することにより M をモデルとする。もしも $\phi(N)$ が証明されると、$\phi(N)$ は M で正しいことになり $N \in M$ となるが、これは $M \models D[N]$ となり、矛盾する。