4 集合と論理

4.1 集合の濃度

4.2 ブール代数

4.3 論理関数

4.1 集合の濃度

集合 A の濃度：

$$|A| = \begin{cases} \text{要素の数} \cdots \textbf{if } A \text{は有限集合} \\ \text{加算無限} \cdots \textbf{if } A \text{は自然数と対応がつく} \end{cases}$$

- 以下の集合は加算無限か？

自然数: 0, 1, 2, 3, 4, 5, 6, ···
偶数 : 0, 2, 4, 6, 8, 10, 12, ···
奇数 : 1, 3, 5, 7, 9, 11, 13, ···
素数 : 2, 3, 5, 7, 11, 13, 17, ···
整数 :
実数 :
有理数:

濃度の比較

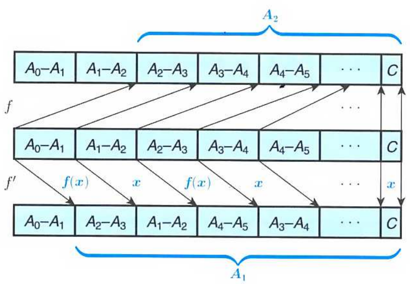
- $A =_C B$: 全単射 (1対1かつ上への写像) $f : A \to B$ が存在
- $A \leq_C B$: 単射 (1対1写像) $f : A \to B$ が存在
- $A <_C B$: $A \leq_C B$ かつ $A \neq_C B$
- 有限集合 $<_C$ 加算無限集合

問4.2 濃度の等しさ $=_C$ が同値関係であることを示せ

補題4.1： $A_0 \supseteq A_1 \supseteq A_2$ かつ $A_0 =_C A_2$ ならば、$A_0 =_C A_1$

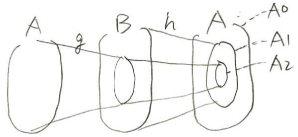
証明： $A_0 =_C A_2$ より全単射 $f : A_0 \to A_2$ が存在

- f から以下のように全単射 $f' : A_0 \to A_1$ が定義できる



定理4.1： $A =_C B \iff A \leq_C B \land B \leq_C A$

証明： 単射 $g : A \to B$, $h : B \to A$ が存在し



- $g \circ h : A \to A_2$ は全単射なので $A =_C A_2$
- 補題4.1より $A =_C A_1$
- ここで、$h : B \to A_1$ も全単射なので $B =_C A_1$
- よって問4.2より、$A =_C B$

問4.4： $\leq_C$ が反射律と推移律を満たすことを示せ

定理4.2： 任意の $A \subseteq \mathbb{N}$ に対して、

$$|A| \notin \mathbb{N} \iff A =_C \mathbb{N}$$

証明： (⇐) 明らか（全単射 $f : \mathbb{N} \to A$ を考えよ）

(⇒) $A \notin \mathbb{N}$ とする。$A \subseteq \mathbb{N}$ より、A の要素は小さい順に並べることができるため $A =_C \mathbb{N}$

問4.5： 任意の $A \subseteq \mathbb{N}$ に対して、

$$|A| \notin \mathbb{N} \iff \exists B (\subset A)\ B =_C A$$

略解 (⇒) 定理4.2より $A =_C \mathbb{N}$、全単射 $f : A \to \mathbb{N}$ 有。$A - f(0)$ で B を定めると、$g(x) = f(x+1)$ は全単射

(⇐) $|A| \in \mathbb{N}$ とすると、$B (\subset A)$ について $|B| < |A|$

加算無限より大きい濃度の集合

(注) $2^A = \{X \mid X \subseteq A\}$ **(教科書p.18の定義)**

定理4.3： 任意の集合Aに対して、$A <_C 2^A$

証明：

($A \leq_C 2^A$) $f(x) = \{x\}$で定まる$f : A \to 2^A$は単射

($A \neq_C 2^A$) $f : A \to 2^A$が全**(**単**)**射と仮定する

- $B = \{a \in A \mid a \notin f(a)\} \subseteq A$とおく
  すなわち、どんな$a \in A$にも、$a \in B \iff a \notin f(a)$
- $f(a) = B$を満たす$a \in A$は存在しない。なぜなら、$a \in f(a)$なら$a \notin B$。また、$a \notin f(a)$なら$a \in B$
- よって、fが全射であることに矛盾

問4.6： $A =_C B$ならば$2^A =_C 2^B$であることを示せ

略解　全単射$f : A \to B$から以下のように定まる$g : 2^A \to 2^B$が全単射であることを示せばよい

$$g(X) = \{f(a) \mid a \in X\}$$

例　$\mathbb{N} =_C \mathbb{Z} =_C \mathbb{Q} <_C \mathbb{R} =_C 2^{\mathbb{N}}$

教科書**p.114**から**p.117**を参照

定理4.5, 系**4.5.2：** $\mathbb{N} \times \mathbb{N} =_C \mathbb{N}$, $\mathbb{Q} = \mathbb{N}$

定理4.6： $\mathbb{N}^* = \bigcup_{n=0}^{\infty} \mathbb{N}^n$と書くとき、$\mathbb{N}^* =_C \mathbb{N}$

証明： $\mathbb{N}^*$を$G_0, G_1, \ldots$にグループ分けできる

$$G_m = \{(a_1, \ldots, a_n) \in \mathbb{N}^* \mid m = a_1 + \cdots + a_n\}$$

各G_mは有限集合なので、$\mathbb{N}^*$の要素を$G_0, G_1, \ldots$の順に並べられる

定理4.7： $\mathbb{R} =_C 2^{\mathbb{N}}$

証明： 系**4.5.2**、問**4.6**より$2^{\mathbb{N}} =_C 2^{\mathbb{Q}}$

($\mathbb{R} \leq_C 2^{\mathbb{Q}}$)： $H : \mathbb{R} \to 2^{\mathbb{Q}}$を以下のように定める

$$H(\alpha) = \{x \in \mathbb{Q} \mid x \leq \alpha\}$$

二つの実数の間には必ず有理数が存在するので、Hは単射

($2^{\mathbb{N}} \leq_C \mathbb{R}$)： $h : 2^{\mathbb{N}} \to \mathbb{R}$を以下のように定める

$$h(A) = \sum_{n \in A} 3^{-n}$$

問**4.9**よりhは単射

問4.9： $h(A) = \sum_{n \in A} 3^{-n}$で定まる$h : 2^{\mathbb{N}} \to \mathbb{R}$が単射であることを示せ

略解： $A \neq A'$とする。一方にだけ含まれる要素の最小をkとし、$k \in A, k \notin A'$とする

$$\begin{aligned} & h(A) - h(A') \\ & > 1/3^k - (1/3^{k+1} + 1/3^{k+2} + \cdots) \\ & > 1/3^k - 1/(2 \cdot 3^k) \\ & > 0 \end{aligned}$$

よって、$h(A) \neq h(A')$

4.2 ブール代数

代数： 集合とその上のいくつかの演算

ブール代数： 以下の公理を満たす代数$\langle A, \{0, 1, \vee, \wedge, \neg\}\rangle$

- 冪等則 $x \wedge x = x \vee x = x$
- 交換則 $x \wedge y = y \wedge x$, $x \vee y = y \vee x$
- 結合則 $(x \wedge y) \wedge z = x \wedge (y \wedge z)$, $(x \vee y) \vee z = x \vee (y \vee z)$
- 吸収則 $(x \wedge y) \vee x = x$, $(x \vee y) \wedge x = x$
- 分配則 $(x \vee y) \wedge z = (x \wedge z) \vee (y \wedge z)$, $(x \wedge y) \vee z = (x \vee z) \wedge (y \vee z)$
- 補元 $x \vee \neg x = 1$, $x \wedge \neg x = 0$

4.3 論理関数

論理関数： ブール領域$\mathbb{B}=\{0,1\}$上の関数

次の定理から、どの$f:\mathbb{B}^n\to\mathbb{B}$も、関数$\wedge,\vee,\neg$の合成で表せることが分かる

定理4.9： シャノンの展開定理

任意の$f:\mathbb{B}^n\to\mathbb{B}$に対して以下が成り立つ

$$\begin{aligned}&f(x_1,\ldots,x_{n-1},x_n)\\&=(f(x_1,\ldots,x_{n-1},0)\wedge\neg x_n)\\&\quad\vee(f(x_1,\ldots,x_{n-1},1)\wedge x_n)\end{aligned}$$

証明： $x_n=0$と$x_n=1$で場合分けすれば示せる

定理4.10： 和積標準系 (DNF)

$$f(x_1,\ldots,x_n)=\bigvee_{f(a_1,\ldots,a_n)=1}\bigwedge_{i=1}^{n}x_i^{a_i}$$

ここで、$x_i^1=x_i$，$x_i^0=\neg x_i$

例： 右の表で与えられる論理関数fの**DNF**は、$(\neg x\wedge y)\vee(x\wedge\neg y)$

x	y	$f(x,y)$
0	0	0
0	1	1
1	0	1
1	1	0

定理4.10'： 積和標準系 (CNF)

$$f(x_1,\ldots,x_n)=\bigwedge_{f(a_1,\ldots,a_n)=0}\bigvee_{i=1}^{n}x_i^{\neg a_i}$$

ここで、$x_i^1=x_i$，$x_i^0=\neg x_i$

例： 右の表で与えられる論理関数fの**CNF**は、$(x\vee y)\wedge(\neg x\vee\neg y)$

x	y	$f(x,y)$
0	0	0
0	1	1
1	0	1
1	1	0

- **CNF**サイズの爆発

問4.18： $\vee$と$\neg$で任意の論理関数を表せることを示せ

解： $x\wedge y=\neg(\neg x\vee\neg y)$より明らか

fが充足可能： $f(x_1,\ldots,x_n)=1$を満たす$x_1,\ldots,x_n\in\mathbb{B}$が存在する

Teistin変換： 新しい変数を導入するが、充足可能性を保存したまま**CNF**に変換する変換。

各関数$f\in\{\wedge,\vee,\neg,\ldots\}$に対して、

$$\begin{cases}T(x)=\langle x,1\rangle & x\text{が変数、}\mathbf{0}\text{、}\mathbf{1}\text{のいずれかのとき}\\ T(f(\phi_1,\ldots,\phi_n))=\langle z,\delta\wedge\psi_1\wedge\cdots\wedge\psi_n\rangle\end{cases}$$

ここで、zは新しい変数、$T(\phi_i)=\langle y_i,\psi_i\rangle$，$\delta$は$(z\Leftrightarrow f(y_1,\ldots,y_n))$と等価な**CNF**

補題： $T(\phi)=\langle z,\psi\rangle$とするとき、$\psi$は**CNF**

Teistin変換の例： $(x_1\wedge x_2)\vee(x_3\wedge x_4)$を**Teistin**変換する

$$\begin{aligned}&T(x_1\wedge x_2)\\&=\langle z_1,(\neg z_1\vee x_1)\wedge(\neg z_1\vee x_2)\wedge(z_1\vee\neg x_1\vee\neg x_2)\rangle\\&T(x_3\wedge x_4)\\&=\langle z_2,(\neg z_2\vee x_3)\wedge(\neg z_2\vee x_4)\wedge(z_2\vee\neg x_3\vee\neg x_4)\rangle\\&T(x_1\wedge x_2)\vee(x_3\wedge x_4))\\&=\langle z,(\neg z\vee z_1\vee z_2)\wedge(z\vee z_1)\wedge(z\vee z_3)\wedge\cdots\rangle\end{aligned}$$

ϕとψは充足可能性が等価： $\phi=1$とする変数の割当に対して、それにψだけに現れる変数を追加して定めることで$\psi=1$とできる。また逆も可能

定理： $T(\phi)=\langle z,\psi\rangle$に対して、$\phi$と$z\wedge\psi$は充足可能性が等価

略証： ϕの構造に関する帰納法。

- $\phi=\phi_1\wedge\phi_2$のとき、
  - $\phi=1$とすると、$\phi_i=1$と帰納法の仮定**(IH)**より$y_i=\psi_i=1$。$z=1$ととれば、$\delta=(z\Leftrightarrow y_1\wedge y_2)=1$。よって、$z\wedge\phi=1$
  - $z\wedge\phi=1$とすると、$\delta=1$より$y_1=y_2=1$。また、$\psi_1=\psi_2=1$と**IH**より$\phi_1=\phi_2=1$。よって、$\phi=1$。
- その他の場合も同様