

5.5 束とブール代数

ブール関数 (= 論理関数) とは真理値の集合 $\{0, 1\}$ から $\{0, 1\}$ への関数であるとして, その性質と応用についてすでに 5.3.1~5.3.2 項で学んだ. 特に, $\bar{x}, x \cdot y, x + y, x \oplus y$ といったブール関数を論理演算と見る世界は「スイッチング代数」と呼ばれることがあるが, それはこの項で述べる「ブール代数」の特別の場合である (すなわち, スwitching代数はブール代数の具体的な一例に過ぎない). この節では, 真理値 $0, 1$ が持つ性質を別の観点から考え, その性質を特徴付けることにより, そのことを学ぶ. すなわち, まず, 半順序集合^{そく}の上で束という代数系^{そく}*を考え, ある性質を満たす束をブール代数と呼ぶ. 真理値の世界はブール代数の特別な場合であることが証明される.

• 束とは 半順序集合 $(A, \leq)$ において, A の任意の 2 元 a, b に対して, それらの上限 $\sup\{a, b\}$ と下限 $\inf\{a, b\}$ がともに存在するとき A を束という[†]

- $\sup\{a, b\}$ を $a \vee b$ と書き, a と b の結びと呼び,
- $\inf\{a, b\}$ を $a \wedge b$ と書き, a と b の交わりと呼ぶ.

A が束ならば, $\vee, \wedge$ は A の上の 2 項演算であると考えてよい.

〔例 5.16〕 束の例

(1) 集合 X のべき集合 2^X は, 集合の包含関係 $\subseteq$ の下で半順序集合である. $A, B \in 2^X$ に対して, 半順序 $\subseteq$ に関する A, B の下限は $A \cap B$ (共通部分), また, A, B の上限は $A \cup B$ (和集合) であり, これらはいずれも 2^X の元なので, $(2^X, \subseteq)$ は束である. これをべき集合束という.

(2) 全順序集合 $(N, \leq)$ の 2 元 m, n に対して

$$m \vee n = \max\{m, n\}, \quad m \wedge n = \min\{m, n\}$$

であるから, $(N, \leq)$ は束である.

*代数系とは, いくつかの演算が定義された世界のことである. 数学的には, ある集合 X とその上で定義されたいくつかの演算 (例えば, 単項演算 $\neg$, 2 項演算 $\cdot$ と $+$) を考え, それが満たすべき基本的性質 (その代数系の公理) からその他にどんな性質が成り立つかを考える. その際, X の特定の元 (例えば, 0 と 1) が重要な役割を果たす場合, それらを明示して $(X, \neg, \cdot, +, 0, 1)$ のように表わす. $\neg, \cdot, +$ に関する公理として例えば定理 5.1' を仮定した代数系 $(X, \neg, \cdot, +, 0, 1)$ がスイッチング代数である.

[†]束: lattice (「格子」の意), 結び: join, 交わり: meet

(3) $m, n \in N$ に対して, m が n を割り切るとき $m \mid n$ と書く. $\mid$ は N の上の半順序である. この半順序の下で

$$m \vee n = \text{lcm}\{m, n\} \quad (m \text{ と } n \text{ の最小公倍数})$$

$$m \wedge n = \text{gcd}\{m, n\} \quad (m \text{ と } n \text{ の最大公約数})$$

が成り立ち, $(N, \mid)$ は束である.

(4) 真理値 T と F の間の大小関係 $<$ を $F < T$ で定義すると $(\{T, F\}, \leq)$ は束であり, $x \vee y$ は x と y の論理和, $x \wedge y$ は x と y の論理積である. $\square$

● 束における双対 $\overset{\text{そうつい}}{\leq}$ を集合 A 上の半順序とするとき,

$$a \leq^* b \stackrel{\text{def}}{\iff} b \leq a$$

によって定義される半順序 $\leq^*$ を $\leq$ の双対という. $(A, \leq)$ が束なら $(A, \leq^*)$ も束となることは明らかである. A における順序関係が全く逆になるだけで, $(A, \leq^*)$ における a, b の結びは $(A, \leq)$ における a, b の交わりに等しく, $(A, \leq^*)$ における a, b の交わりは $(A, \leq)$ における a, b の結びに等しい.

いま, どんな束 $\mathcal{A} = (A, \leq)$ においても成り立つ命題 P があったとしよう. P が $\mathcal{A}$ における結び $\vee$, 交わり $\wedge$, 半順序 $\leq$ に言及していることを $P(\vee, \wedge, \leq)$ と書くことにする. 仮定より, P は双対束 $\mathcal{A}^* := (A, \leq^*)$ においても成り立つ. つまり, $\mathcal{A}^*$ における $\leq^*$ の下での結び, 交わりをそれぞれ $\vee^*$, $\wedge^*$ と書くことにすれば $P(\vee^*, \wedge^*, \leq^*)$ が成り立つ. ところが任意の $a, b \in A$ に対し

$$a \vee^* b = a \wedge b, \quad a \wedge^* b = a \vee b,$$

$$\mathcal{A}^* \text{ において } a \leq^* b \iff \mathcal{A} \text{ において } b \leq a \text{ (すなわち } \mathcal{A} \text{ において } a \geq b)$$

が成り立っているから,

$$\mathcal{A}^* \text{ において } P(\vee^*, \wedge^*, \leq^*) \text{ が成立する}$$

$$\iff \mathcal{A} \text{ において } P(\wedge, \vee, \geq) \text{ が成立する}$$

が成り立つ. 命題 $P(\wedge, \vee, \geq)$ を命題 $P(\vee, \wedge, \leq)$ の双対という. 我々は次の定理を証明したことになる.

定理 5.5' (双対の原理) 束 $(A, \leq)$ において, 命題 $P(\vee, \wedge, \leq)$ が成り立つならば, その双対 $P(\wedge, \vee, \geq)$ も成り立つ.

束における 2 つの演算 $\vee, \wedge$ は次の性質を満たし, 半順序 $\leq$ とは次のような関係がある.

● 束の基本的性質

定理 5.11 束 $(A, \leq)$ の任意の元 a, b, c に対し, 次のことが成り立つ.

- | | |
|--|-----|
| (1) $a \vee a = a = a \wedge a$ | 巾等律 |
| (2) $a \vee b = b \vee a, \quad a \wedge b = b \wedge a$ | 可換律 |
| (3) $(a \vee b) \vee c = a \vee (b \vee c), \quad (a \wedge b) \wedge c = a \wedge (b \wedge c)$ | 結合律 |
| (4) $(a \vee b) \wedge a = a = (a \wedge b) \vee a$ | 吸収律 |
| (5) $a \vee b = b \iff a \leq b \iff a \wedge b = a$ | 整合律 |

証明 (1) (2) は結び, 交わりの定義より自明である.

(3) 結びの定義より,

$$(a \vee b) \vee c \geq a \vee b, \quad (a \vee b) \vee c \geq c, \quad a \vee b \geq a, \quad a \vee b \geq b$$

が成り立つ. $(a \vee b) \vee c \geq a \vee b \geq b, (a \vee b) \vee c \geq c$ より $(a \vee b) \vee c \geq b \vee c$ であり, また, $(a \vee b) \vee c \geq a \vee b \geq a$ でもあるから $(a \vee b) \vee c \geq a \vee (b \vee c)$ が示された. $(a \vee b) \vee c \leq a \vee (b \vee c)$ も同様に証明できるので, $(a \vee b) \vee c = a \vee (b \vee c)$. また, 双対の原理により, $(a \wedge b) \wedge c = a \wedge (b \wedge c)$ も成り立つ.

(4) 交わりの定義より $(a \vee b) \wedge a \leq a$. 次に, 結びの定義より $a \vee b \geq a$ であるから, $(a \vee b) \wedge a \geq a$. よって, $(a \vee b) \wedge a = a$.

$(a \wedge b) \vee a = a$ は双対の原理より導かれる.

$$\begin{aligned} (5) \quad a \vee b = b &\implies b = a \vee b \geq a && (\vee \text{ の定義}) \\ &\implies a \wedge b = a. && (\wedge \text{ の定義}) \end{aligned}$$

逆に,

$$\begin{aligned} a \wedge b = a &\implies a = a \wedge b \leq b && \wedge \text{ の定義} \\ &\implies a \vee b = b && \vee \text{ の定義} \quad \square \end{aligned}$$

実は，束の持つ性質のうち，定理 5.11(2)～(4)は束として本質的なものである．すなわち，束とは，演算 $\vee$ と $\wedge$ が定義されていて定理 5.11(2)～(4)が満たされているような代数系として特徴づけることができるのである．そのことを次の定理に述べる．

定理 5.12 集合 A の上で 2 つの 2 項演算 $\wedge$ と $\vee$ が定義されていて，定理 5.11(2)～(4)を満たしているとする．このとき，

- (1) $a \vee b = b \iff a \wedge b = a$.
- (2) $a \leq b \stackrel{\text{def}}{\iff} a \vee b = b$ により $\leq$ を定義すると，
 - (a) $\leq$ は半順序であり，
 - (b) $\leq$ の下で $\inf\{a, b\} = a \wedge b$, $\sup\{a, b\} = a \vee b$ が成り立つ．よって， $(A, \leq)$ は束である* .

*逆に，束とは定理 5.11(2)～(4)を満たす代数系 $(A, \vee, \wedge)$ のことであると定義し，その上で定理 5.12(2)のように半順序 $\leq$ が定義できるとも考える．

証明 (1) $a \vee b = b$ とすると， $(a \vee b) \wedge a = b \wedge a = a \wedge b$ である (最後の等号は可換律による) . 一方，吸収律により， $(a \vee b) \wedge a = b$ であるから， $(a \wedge b) = a$. 同様に， $a \wedge b = a \implies a \vee b = b$ を示すことができる .

(2)(a) $\leq$ が反射律，反対称律，推移律を満たすことを示す .

(i) 吸収律が成り立てはベキ等律が成り立つ (問 5.26) ので， $a \vee a = a$. これは $\leq$ の定義より $a \leq a$ を意味するので， $\leq$ は反射的である .

(ii) $a \leq b, b \leq a \implies a \vee b = b, b \vee a = a$ $\leq$ の定義
 $\implies a = b \vee a = a \vee b = b$ 可換律

よって， $\leq$ は反対称的である .

(iii) $a \leq b, b \leq c \implies a \vee b = b, b \vee c = c$ $\leq$ の定義
 $\implies a \vee c = a \vee (b \vee c)$ $b \vee c = c$
 $= (a \vee b) \vee c$ 結合律
 $= b \vee c = c$ $a \vee b = b$
 $\implies a \leq c$. $\leq$ の定義

よって, $\leq$ は推移的である.

(i), (ii), (iii)より, $\leq$ は半順序である.

(2)(a) まず $a \vee b$ が a, b の上界になること, すなわち $a \leq a \vee b$ かつ $b \leq a \vee b$ が成り立つことを示そう. $\leq$ の定義より, $a \vee (a \vee b) = a \vee b, b \vee (a \vee b) = a \vee b$ を示せばよい.

$$\begin{aligned} a \vee (a \vee b) &= (a \vee a) \vee b && \text{結合律} \\ &= a \vee b. && \text{ベキ等律 } a \vee a = a \end{aligned}$$

$b \vee (a \vee b) = a \vee b$ についても同様.

次に, c を a, b の任意の上界とすると $a \leq c$ かつ $b \leq c$, すなわち, $a \vee c = c, b \vee c = c$ が成り立つので,

$$\begin{aligned} (a \vee b) \vee c &= a \vee (b \vee c) && \text{結合律} \\ &= a \vee (c \vee b) && \text{可換律} \\ &= (a \vee c) \vee b && \text{結合律} \\ &= c \vee b && a \vee c = c \\ &= b \vee c && \text{可換律} \\ &= c. \end{aligned}$$

ゆえに, $a \vee b \leq c$ が成り立つことになり, $a \vee b$ は a, b の最小上界すなわち $\sup\{a, b\}$ に等しいことがわかる.

$a \vee b = \inf\{a, b\}$ も同様に示すことができる. □

● 分配束 束 $(A, \vee, \wedge)$ の任意の元 a, b, c に対して,

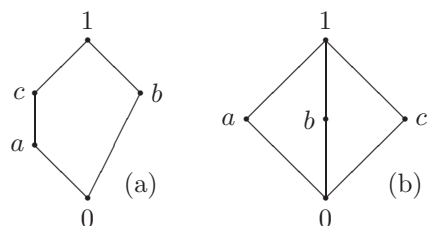
$$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c), \quad a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c) \quad \text{分配律}$$

が成り立つならば, $(A, \vee, \wedge)$ を分配束という.

[例 5.17] 分配束と非分配束

(1) 例 5.16(1) ~ (4)はいずれも分配束である.

(2) 次のハッセ図で示される半順序集合はいずれも分配束ではない.



例えば、図 (b) において $a \wedge (b \vee c) = a \neq 0 = (a \wedge b) \vee (a \wedge c)$ である。

● ブール代数 束において最大元，最小元が存在する場合，それらをそれぞれ $1, 0$ で表わす。以下では，最大元，最小元を持つような束を考える。

束 $(A, \vee, \wedge, 0, 1)$ の元 a, b が

$$a \vee b = 1, \quad a \wedge b = 0$$

を満たすとき， a は b の (b は a の) 補元であるという。任意の元 $a \in A$ が少なくとも 1 つ補元を持つような束 A は相補的であるという。相補的かつ分配的な束をブール束 (別称，ブール代数) という。ブール束においては，任意の元 a がちょうど 1 つの補元を持つので，それを $\bar{a}$ で表わす。

〔例 5.18〕 補元，ブール束

(1) 0 と 1 は互いに他の補元である。

(2) 上図 (a) のようなハッセ図を持つ束において， b は 2 つの補元 a, c を持っているが， b にも c にも補元がないので，この束は相補的でない。

(3) 上図 (b) のようなハッセ図を持つ束において， a, b, c は互いに他の補元である。この束は相補的であるが分配律が成り立たないのでブール束はない。

(4) ベキ集合束 $(2^{\{a,b,c\}}, \cup, \cap)$ において， $\{a, b\}$ の補元は $\{c\}$ であり， $\{b\}$ の補元は $\{a, c\}$ であり， $\{a, b, c\}$ の補元は $\emptyset$ である (例 3.15 (1) の図参照)。この束はブール束である。

一般に，ベキ集合束 $(2^X, \vee, \wedge)$ はブール束である。集合 $A \subseteq X$ の補元 $\bar{A}$ はその補集合 $X - A$ であり， $\emptyset$ が最小元 ($\vee$ の単位元)， X が最大元 ($\wedge$ の単位元) である。

(5) 真理値のなす束 $(\{T, F\}, \vee, \wedge)$ はブール束である。 $x \in \{T, F\}$ の補元はその否定 $\bar{x}$ である： $\bar{T} = F$ ， $\bar{F} = T$ 。 F が最小元， T が最大元。□

すでにそのことを述べ (定理 5.12), 適宜両方の使い方をしてるように, 束 $(A, \vee, \wedge)$ は

$$a \leq b \iff a \vee b = b \iff a \wedge b = a$$

$$a \vee b = \sup\{a, b\}, \quad a \wedge b = \inf\{a, b\}$$

という関係の下で半順序集合 $(A, \leq)$ でもある. さらに, ブール束の場合には, 2 つの 2 項演算 $\vee, \wedge$ の他に単項演算 $\neg$ (補元をとる演算) も定義されていて, 定理 5.11(1)~(4) の他に次の定理に示すような性質も成り立つ (定理 5.1'(6)~(9) も参照せよ).

定理 5.13 ブール代数 $(A, \vee, \wedge, \neg, 0, 1)$ の任意の元 a, b をに對して, 次のことが成り立つ.

- (1) $\bar{\bar{a}} = a$ 二重否定
- (2) $\bar{0} = 1, \quad \bar{1} = 0.$
- (3) $a \vee 0 = a, \quad a \wedge 0 = 0, \quad a \vee 1 = 1, \quad a \wedge 1 = a$
- (4) $\overline{a \vee b} = \bar{a} \wedge \bar{b}, \quad \overline{a \wedge b} = \bar{a} \vee \bar{b}$ ド・モルガンの法則
de Morgan の法則
- (5) $a \leq b \iff \bar{b} \leq \bar{a}$ □

そこで, A を 3 つの演算 $\wedge, \vee, \neg$ が定義されていて, ベキ等律, 可換律, 結合律, 吸収律, 整合律, 分配律 (以上, 定理 5.11), 補元に関する性質 (定理 5.13) が成り立つ代数系

$$(A, \vee, \wedge, \neg, 0, 1)$$

だと見て, ブール束のことをブール代数*ともいう. この名前は, 初めてこのような代数系を体系的に研究した (1854 年) フランスの数学者 G. Boole に因んでいる.

実は, ブール代数の公理としては, 今述べたものは冗長である. 集合 A の上で 2 つの 2 項演算 $\vee, \wedge$ と, 1 つの単項演算 $\neg$ とが定義されていて, 次の 4 つの公理 (E.V. Huntington, 1904) を満たすとき $(A, \vee, \wedge, \neg)$ をブール代数と言ってよいことが証明できるからである:

*ブール代数: Boolean algebra.

● ブール代数の公理 (Huntington の公理)

次の (1) ~ (4) が成り立つとき, $(A, \vee, \wedge, \neg)$ をブール代数という:

任意の $a, b, c \in A$ に対して次の (1), (2) が成り立つ:

$$(1) \quad a \vee b = b \vee a, \quad a \wedge b = b \wedge a. \quad \text{可換律}$$

$$(2) \quad \begin{aligned} a \vee (b \wedge c) &= (a \vee b) \wedge (a \vee c) \\ a \wedge (b \vee c) &= (a \wedge b) \vee (a \wedge c) \end{aligned} \quad \text{分配律}$$

A には異なる 2 元 $0, 1$ が存在し, 任意の $a \in A$ に対して次の (3), (4) が成り立つ:

$$(3) \quad a \vee 0 = a, \quad a \wedge 1 = a \quad \text{単位元}$$

$$(4) \quad a \vee \bar{a} = 1, \quad a \wedge \bar{a} = 0 \quad \text{相補律}$$

- 有限のブール代数は本質的にはベキ集合束である 半順序集合 $(A, \leq)$ と $(B, \leq)$ は, 全単射 $f: A \rightarrow B$ が存在して任意の $a, b \in A$ に対して

$$a \leq b \iff f(a) \leq f(b)$$

が成り立つとき同型(順序同型)であるという.

次の定理に示すように, 有限個の元からなるブール代数は, ある集合の部分集合の上で集合演算 $\cup, \cap, \neg$ を考えることと本質的に同じである.

定理 5.14 有限ブール代数 (から定理 5.12 によって定義される束) は, 適当な集合 X をとると, ベキ集合束 $(2^X, \subseteq)$ と同型である.

この定理の逆に相当すること (X を '任意の' 集合とするとき, ベキ集合束 $(2^X, \subseteq)$ における半順序 $\subseteq$ から定理 5.12 によって演算 $\cap, \cup, \neg$ を定義して得られる代数系 $(2^X, \cap, \cup, \neg, 0, 1)$ はブール代数である (例 5.18 (4) 参照)) も成り立つことに注意する.

系 5.15 有限ブール代数の元の個数は 2 のベキである.