平成 13 年 5 月 24 日

教科書 定理 2.6 の証明

新潟工科大学 情報電子工学科 竹野茂治

教科書 p.62 の定理 2.6 の証明はやや不親切で、省略されているものもあるのでここでそれを証明したものを紹介しておく。

公理 1 (ブール代数の公理)
$\oplus, *$ という 2 項演算と $'$ という単項演算が定義されていて、0,1 という名前の元を含む集合 B が次を満たすとき、それを **ブール代数** であるという。

(B_1) $a \oplus b = b \oplus a,\ a * b = b * a$ (交換則)

(B_2) $a \oplus (b * c) = (a \oplus b) * (a \oplus c),\ \ a * (b \oplus c) = (a * b) \oplus (a * c)$ (分配則)

(B_3) $a \oplus 0 = a,\ a * 1 = a$ (単位元)

(B_4) $a \oplus a' = 1,\ a * a' = 0$

例えば、集合演算は $\oplus = \cup, * = \cap, A' = \bar{A}, 0 =, 1 = U$ に関してブール代数となる。
任意のブール代数に対して次が成り立つ。

定理 2 (教科書 定理 2.6)

(T_1) $a \oplus a = a,\ a * a = a$

(T_2) $a \oplus 1 = 1,\ a * 0 = 0$

(T_3) $a \oplus (a * b) = a,\ a * (a \oplus b) = a$ (吸収則)

(T_4) $(a \oplus b) \oplus c = a \oplus (b \oplus c),\ \ (a * b) * c = a * (b * c)$ (結合則)

(T_5) $0' = 1,\ \ 1' = 0$

(T_6) $(a \oplus b)' = a' * b',\ \ (a * b)' = a' \oplus b'$ (ド・モルガンの法則)

証明
(T_1) $a \overset{(B_3)}{=} a \oplus 0 \overset{(B_4)}{=} a \oplus (a * a') \overset{(B_2)}{=} (a \oplus a) * (a \oplus a') \overset{(B_4)}{=} (a \oplus a) * 1 \overset{(B_3)}{=} a \oplus a$
$*$ の方は双対、つまり $\oplus$ と $*$, 0 と 1 を入れ換えて上と同様に行えばよい。以下の命題についても同様。
(T_2) $1 \overset{(B_4)}{=} a \oplus a' \overset{(B_3)}{=} a \oplus (a' * 1) \overset{(B_2)}{=} (a \oplus a') * (a \oplus 1) \overset{(B_4)}{=} 1 * (a \oplus 1) \overset{(B_3)}{=} a \oplus 1$
(T_3) $a \oplus (a * b) \overset{(B_3)}{=} (a * 1) \oplus (a * b) \overset{(B_2)}{=} a * (1 \oplus b) \overset{(T_2)}{=} a * 1 \overset{(B_3)}{=} a$
(T_4) 左辺 $= L$ とする。

$$L \overset{(B_3)}{=} L * 1 \overset{(B_4)}{=} L * (a \oplus a') \overset{(B_2)}{=} (L * a) \oplus (L * a')$$

ここで、

$$\begin{aligned} L*a &= \{(a\oplus b)\oplus c\}*a \overset{(B_2)}{=} \{(a\oplus b)*a\}\oplus(c*a) \overset{(T_3)}{=} a\oplus(c*a) \overset{(T_3)}{=} a, \\ L*a' &= \{(a\oplus b)\oplus c\}*a' \overset{(B_2)}{=} \{(a\oplus b)*a'\}\oplus(c*a'), \\ (a\oplus b)*a' &\overset{(B_2)}{=} (a*a')\oplus(b*a') \overset{(B_4)}{=} 0\oplus(b*a') \overset{(B_3)}{=} b*a' \end{aligned}$$

より、

$$L*a' = (b*a')\oplus(c*a') = (b\oplus c)*a'$$

ゆえに

$$\begin{aligned} L &= (L*a)\oplus(L*a') \\ &= a\oplus\{(b\oplus c)*a'\} \overset{(B_2)}{=} \{a\oplus(b\oplus c)\}*(a\oplus a') \overset{(B_4)}{=} \{a\oplus(b\oplus c)\}*1 \\ &\overset{(B_3)}{=} a\oplus(b\oplus c) \end{aligned}$$

(T_5) (B_4) で $a=0$ とすると $0\oplus 0'=1$ で、(B_3) より $0\oplus 0'=0'$
(T_6) これを示す前に、まず次を示す。

(T_7) $x\oplus a=1$ かつ $x*a=0$ ならば $x=a'$

$$\begin{aligned} x &\overset{(B_3)}{=} 1*x \overset{(B_4)}{=} (a\oplus a')*x \overset{(B_2)}{=} (a*x)\oplus(a'*x) = 0\oplus(a'*x) \\ &\overset{(B_3)}{=} a'*x \overset{(B_3)}{=} a'*(0\oplus x) \overset{(B_4)}{=} a'*\{(a*a')\oplus x)\} \\ &\overset{(B_2)}{=} a'*\{(a\oplus x)*(a'\oplus x)\} = a'*\{1*(a'\oplus x)\} \overset{(B_3)}{=} a'*(a'\oplus x) \\ &\overset{(T_3)}{=} a' \end{aligned}$$

これを用いると、$R=a'*b'$ に対して

$R\oplus(a\oplus b)=1$ かつ $R*(a\oplus b)=0$

を示せばよいことになる。

$$\begin{aligned} R\oplus(a\oplus b) &= (a'*b')\oplus(a\oplus b) \overset{(T_4)}{=} \{(a'*b')\oplus a\}\oplus b \overset{(B_2)}{=} \{(a'\oplus a)*(b'\oplus a)\}\oplus b \\ &\overset{(B_4)}{=} \{1*(b'\oplus a)\}\oplus b \overset{(B_3)}{=} (a\oplus b')\oplus b \overset{(T_4)}{=} a\oplus(b'\oplus b) \overset{(B_4)}{=} a\oplus 1 \overset{(T_2)}{=} 1, \\ R*(a\oplus b) &= (a'*b')*(a\oplus b) \overset{(T_4)}{=} \{a'*(a\oplus b)\}*b' \overset{(B_2)}{=} \{(a'*a)\oplus(a'*b)\}*b' \\ &\overset{(B_4)}{=} \{0\oplus(a'*b)\}*b' \overset{(B_3)}{=} (a'*b)*b' \overset{(T_4)}{=} a'*(b*b') \overset{(B_4)}{=} a*0 \overset{(T_2)}{=} 0 \end{aligned}$$

∎

この証明中でも使ったものも含むが、次が成り立つこともいえる。

定理 3

(T_7) $x\oplus a=1$ かつ $x*a=0$ ならば $x=a'$

(T_8) $a\oplus b=0$ ならば $a=b=0$, $a*b=1$ ならば $a=b=1$

証明
(T_7) は前証明中に示したので、(T_8) の前半のみ示す (後半は双対)。

$$a \overset{(T_3)}{=} a * (a \oplus b) = a * 0 \overset{(T_2)}{=} 0$$

b も同様。∎