符号理論･暗号理論

- No.6 ブール代数 -

渡辺　裕

Coding Theory / Cryptography

- No.6 Boolean Algebra -

Hiroshi Watanabe

演算子

- 2項演算子
  - 加法演算子　+
  - 乗法演算子　・
- 単項演算子
  - 補元演算子　–
- 変数
  - 0, 1
  - 代数系

Operations

- Two binary operations
  - addition　+
  - multiplication　・
- Single operation
  - negation　–
- Variables
  - 0, 1
  - Binary algebra

公理 (1)

- 交換法則
  - A+B=B+A
  - A･B=B･A
- 分配法則
  - A･(B+C)=(A･B)+(A･C)
  - A+(B･C)=(A+B)･(A+C)
- 単位元
  - A+0=A
  - A･1=A

Laws (1)

- Commutativity
  - A+B=B+A
  - A･B=B･A
- Associativity
  - A･(B+C)=(A･B)+(A･C)
  - A+(B･C)=(A+B)･(A+C)
- Identity
  - A+0=A
  - A･1=A

公理 (2)

- 補元
  - A+$\underline{A}$=1
  - A･$\underline{A}$=0

Laws (2)

- Complementation
  - A+$\underline{A}$=1
  - A･$\underline{A}$=0

公理 (3)

- 演算の特徴
  - 分配法則の2番目は通常の数の演算と異なる
  - 補元は逆元と異なる
  - 加法･乗法･補元の演算結果は{0,1}に閉じる
- 双対原理
  - 加法と乗法の演算子を入れ替えても結果は同じ
  - 0と1を入れ替えても結果は同じ

Laws (3)

- Characteristics of operation
  - Second law of associativity is not regular operation
  - Complementation is not inverse
  - Result of addition, multiplication, complementatoin is closed in {0,1}
- Duality principle
  - Result has similar form by exchanging addition and multiplication
  - Same result can be obtained by exchanging 0 and 1

双対定理

- 定理
  - ブール代数では, 元の式の+と･,0と1を交換してできる式を, 元の式の双対(dual)と呼ぶ
  - ブール代数において, ある定理が成り立てば, その双対も成り立つ
    - 注意:ブール代数において、加法と乗法は対等. 通常は乗法が加法に優先する.

Duality

- Theorem
  - In Boolean, an equation which exchange + and – as well as 0 and 1 of the original equation is called “dual” of the original
  - In Boolean, if one theorem holds, its dual also holds
    - Note: Addition and multiplication are on even ground where as multiplication is given priority over addition in the normal algebra.

真理値表 (1)

- ORの真理値表

A	B	A+B
0	0	0
0	1	1
1	0	1
1	1	1

- ANDの真理値表

A	B	A･B
0	0	0
0	1	0
1	0	0
1	1	1

Truth Table (1)

- Truth table of OR

A	B	A+B
0	0	0
0	1	1
1	0	1
1	1	1

- Truth table of AND

A	B	A･B
0	0	0
0	1	0
1	0	0
1	1	1

真理値表 (2)

- NOTの真理値表

A	$\overline{A}$
0	1
1	0

- NORの真理値表

A	B	$\overline{A+B}$
0	0	1
0	1	0
1	0	0
1	1	0

Truth Table (2)

- Truth table of NOT

A	$\overline{A}$
0	1
1	0

- Truth table of NOR

A	B	$\overline{A+B}$
0	0	1
0	1	0
1	0	0
1	1	0

真理値表 (3)

- NANDの真理値表

A	B	$\overline{A \cdot B}$
0	0	1
0	1	1
1	0	1
1	1	0

- XORの真理値表

A	B	$A \oplus B$
0	0	0
0	1	1
1	0	1
1	1	0

Truth Table (3)

- Truth table of NAND

A	B	$\overline{A \cdot B}$
0	0	1
0	1	1
1	0	1
1	1	0

- Truth table of XOR

A	B	$A \oplus B$
0	0	0
0	1	1
1	0	1
1	1	0

定理 (1)

- 結合則
  - $A+(B+C)=(A+B)+C$
  - $A\cdot(B\cdot C)=(A\cdot B)\cdot C$
- 吸収則
  - $A+(A\cdot B)=A$
  - $A\cdot(A+B)=A$
- べき等律
  - $A+A=A$
  - $A\cdot A=A$

Theorem (1)

- Associativity
  - $A+(B+C)=(A+B)+C$
  - $A\cdot(B\cdot C)=(A\cdot B)\cdot C$
- Absorption
  - $A+(A\cdot B)=A$
  - $A\cdot(A+B)=A$
- Idempotence
  - $A+A=A$
  - $A\cdot A=A$

定理 (2)

- 続き
  - $A+1=1$
  - $A\cdot 0=0$
  - $A+(\underline{A}+B)=1$
  - $A\cdot(\underline{A}\cdot B)=0$
  - $(A+\underline{B})\cdot(\underline{A}+B)=(A\cdot B)+(\underline{A}\cdot\underline{B})$
  - $(A\cdot\underline{B})+(\underline{A}\cdot B)=(A+B)\cdot(\underline{A}+\underline{B})$
- ド･モルガンの法則
  - $\underline{(A+B)}=\underline{A}\cdot\underline{B}$
  - $\underline{(A\cdot B)}=\underline{A}+\underline{B}$

Theorem (2)

- Contd.
  - $A+1=1$
  - $A\cdot 0=0$
  - $A+(\underline{A}+B)=1$
  - $A\cdot(\underline{A}\cdot B)=0$
  - $(A+\underline{B})\cdot(\underline{A}+B)=(A\cdot B)+(\underline{A}\cdot\underline{B})$
  - $(A\cdot\underline{B})+(\underline{A}\cdot B)=(A+B)\cdot(\underline{A}+\underline{B})$
- De Morgan Law
  - $\underline{(A+B)}=\underline{A}\cdot\underline{B}$
  - $\underline{(A\cdot B)}=\underline{A}+\underline{B}$

ド･モルガンの法則

- 例1
  - 「私の身長は170cm以上であり, 体重は60kg以上」である
    の論理否定は
    「私の身長は170cm以上であり, 体重は60kg以上」でない,
    ではなく,
    「私の身長は170cm未満であるか, 体重は60kg未満」である
- 例2
  - 「このボールは青いか, 赤い」
    の論理否定は
    「このボールは青くもないし, 赤くもない」

De Morgan Law

- Ex. 1
  - "My height is over 170cm and weight is over 60kg"
    its negative is not
    "My height is less than 170cm and weight is less than 60kg"
    but,
    "My height is less than 170cm or weight is less than 60kg"
- Ex. 2
  - "This ball is blue or red"
    its negative is
    "This ball is neither blue nor red"

定理 (3)

- モジュラー律
  - $A\cdot(B+(A\cdot C))=(A\cdot B)+(A\cdot C)$
  - $A+(B\cdot(A+C))=(A+B)\cdot(A+C)$
- 補元の吸収
  - $A+(\underline{A}\cdot B)=A+B$
  - $A\cdot(\underline{A}+B)=A\cdot B$

Theorem (3)

- Modular Law
  - $A\cdot(B+(A\cdot C))=(A\cdot B)+(A\cdot C)$
  - $A+(B\cdot(A+C))=(A+B)\cdot(A+C)$
- Absorption of complement
  - $A+(\underline{A}\cdot B)=A+B$
  - $A\cdot(\underline{A}+B)=A\cdot B$

関数の標準形 (1)

- ブール関数(3変数)の最小項と最大項
  - $f(x,y,z)=(x+y)\cdot z$

x	y	z	f(x,y,z)	最小項	最大項
0	0	0	0		$x+y+z$
0	0	1	0		$x+y+\underline{z}$
0	1	0	0		$x+\underline{y}+z$
0	1	1	1	$\underline{x}\cdot y\cdot z$	
1	0	0	0		$\underline{x}+y+z$
1	0	1	1	$x\cdot\underline{y}\cdot z$	
1	1	0	0		$\underline{x}+\underline{y}+z$
1	1	1	1	$x\cdot y\cdot z$	

Normal Form of Formula (1)

- Conjunctive Clause and Disjunctive Clause of Boolean algebra (3 variables)
  - $f(x,y,z)=(x+y)\cdot z$

x	y	z	f(x,y,z)	C.C.	D.C
0	0	0	0		$x+y+z$
0	0	1	0		$x+y+\underline{z}$
0	1	0	0		$x+\underline{y}+z$
0	1	1	1	$\underline{x}\cdot y\cdot z$	
1	0	0	0		$\underline{x}+y+z$
1	0	1	1	$x\cdot\underline{y}\cdot z$	
1	1	0	0		$\underline{x}+\underline{y}+z$
1	1	1	1	$x\cdot y\cdot z$	

関数の標準形 (2)

- 最小項と最大項
  - 最小項: ブール変数の積
  - 最大項: ブール変数の和
- 主加法標準形と主乗法標準形
  - 主加法標準形: 最小項の和で関数を表現
  - 主乗法標準形: 最大項の積で関数を表現
- 例
  - $f(x,y,z)=\underline{x}\cdot y\cdot z+ x\cdot\underline{y}\cdot z+ x\cdot y\cdot z$
    $=(x+y+z)\cdot(x+y+\underline{z})\cdot(x+\underline{y}+z)\cdot(\underline{x}+y+z)\cdot(\underline{x}+\underline{y}+z)$

Normal Form of Formula (2)

- Conjunctive Clause and Disjunctive Clause
  - Conjunctive Clause: Multiplication of Boolean variables
  - Disjunctive Clause: Addition of Boolean variables
- Disjunctive Normal Form and Conjunctive Normal Form
  - Disjunctive Normal Form: Logical formula is represented by additions of Conjunctive Clauses
  - Conjunctive Normal Form: Logical formula is represented by multiplication of Disjunctive Clauses
- Ex.
  - $f(x,y,z)=\underline{x}\cdot y\cdot z+ x\cdot\underline{y}\cdot z+ x\cdot y\cdot z$
    $=(x+y+z)\cdot(x+y+\underline{z})\cdot(x+\underline{y}+z)\cdot(\underline{x}+y+z)\cdot(\underline{x}+\underline{y}+z)$

関数の標準形 (3)

- 主加法標準形の変形
  - $f(x,y,z)=\underline{x}\cdot y\cdot z+x\cdot\underline{y}\cdot z+x\cdot y\cdot z$
    $=(\underline{x}\cdot y+x\cdot\underline{y}+x\cdot y)\cdot z$
    $=(\underline{x}\cdot y+x\cdot(\underline{y}+y))\cdot z$
    $=(\underline{x}\cdot y+x\cdot 1)\cdot z$
    $=(\underline{x}\cdot y+x)\cdot z$
    $=(x+y)\cdot z$

Normal From of Formula (3)

- Modification of Disjunctive Normal Form
  - $f(x,y,z)=\underline{x}\cdot y\cdot z+x\cdot\underline{y}\cdot z+x\cdot y\cdot z$
    $=(\underline{x}\cdot y+x\cdot\underline{y}+x\cdot y)\cdot z$
    $=(\underline{x}\cdot y+x\cdot(\underline{y}+y))\cdot z$
    $=(\underline{x}\cdot y+x\cdot 1)\cdot z$
    $=(\underline{x}\cdot y+x)\cdot z$
    $=(x+y)\cdot z$

問題

- 主乗法標準形から元の関数を導け
  - $f(x,y,z)=(x+y+z)\cdot(x+y+\underline{z})\cdot(x+\underline{y}+z)\cdot(\underline{x}+y+z)\cdot(\underline{x}+\underline{y}+z)$

Quiz

- Derive the original formula from the conjunctive normal form
  - $f(x,y,z)=(x+y+z)\cdot(x+y+\underline{z})\cdot(x+\underline{y}+z)\cdot(\underline{x}+y+z)\cdot(\underline{x}+\underline{y}+z)$

問題 (2)

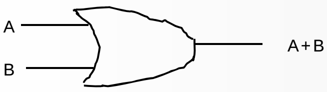
- $A+(\underline{A}\cdot B)=A+B$ を証明せよ

Quiz (2)

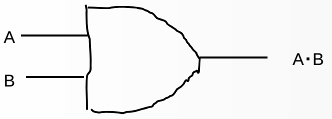
- Give a proof for $A+(\underline{A}\cdot B)=A+B$

論理回路

- OR

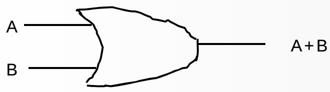


- AND

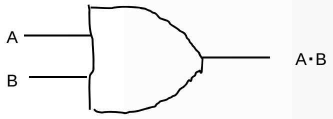


Logic Circuit

- OR



- AND



答え

- $A+(\underline{A}\cdot B)=A+B$
- $=A\cdot 1+\underline{A}\cdot B$
- $=A\cdot(B+\underline{B})+\underline{A}\cdot B$
- $=A\cdot B+A\cdot\underline{B}+\underline{A}\cdot B$
- $=A\cdot B+A\cdot B+A\cdot\underline{B}+\underline{A}\cdot B$
- $=(A\cdot B)+(A\cdot\underline{B})+(A\cdot B)+(\underline{A}\cdot B)$
- $=A\cdot(B+\underline{B})+(A+\underline{A})\cdot B$
- $=A\cdot 1+B\cdot 1$
- $=A+B$

Answer

- $A+(\underline{A}\cdot B)=A+B$
- $=A\cdot 1+\underline{A}\cdot B$
- $=A\cdot(B+\underline{B})+\underline{A}\cdot B$
- $=A\cdot B+A\cdot\underline{B}+\underline{A}\cdot B$
- $=A\cdot B+A\cdot B+A\cdot\underline{B}+\underline{A}\cdot B$
- $=(A\cdot B)+(A\cdot\underline{B})+(A\cdot B)+(\underline{A}\cdot B)$
- $=A\cdot(B+\underline{B})+(A+\underline{A})\cdot B$
- $=A\cdot 1+B\cdot 1$
- $=A+B$

問題

1. $A(A+B)+B=$
2. $A(A+B)+B(A+B)=$
3. $\underline{A}(A+\underline{B})=$
4. $\underline{A}(\underline{A}+\underline{B})=$
5. $(A+B)(A+\underline{B})=$
6. $(A+B)(\underline{A}+\underline{B})=$
7. $(\underline{A\cdot B})+\underline{B}=$
8. $(\underline{A+B})+\underline{B}=$
9. $(\underline{A\cdot B})\cdot\underline{A}=$
10. $(\underline{A\cdot B})(\underline{A+B})=$
11. $(A+B)(\underline{A}+B)+B(A+\underline{B})=$
12. $(\underline{A+B})+(\underline{A}+B)=$

Quiz

1. $A(A+B)+B=$
2. $A(A+B)+B(A+B)=$
3. $\underline{A}(A+\underline{B})=$
4. $\underline{A}(\underline{A}+\underline{B})=$
5. $(A+B)(A+\underline{B})=$
6. $(A+B)(\underline{A}+\underline{B})=$
7. $(\underline{A\cdot B})+\underline{B}=$
8. $(\underline{A+B})+\underline{B}=$
9. $(\underline{A\cdot B})\cdot\underline{A}=$
10. $(\underline{A\cdot B})(\underline{A+B})=$
11. $(A+B)(\underline{A}+B)+B(A+\underline{B})=$
12. $(\underline{A+B})+(\underline{A}+B)=$

答え

1. $A(A+B)+B=AA+AB+B=A+B(A+1)=A+B$
2. $A(A+B)+B(A+B)=(A+B)+(A+B)=A+B$
3. $\underline{A}(A+\underline{B})=\underline{A}A+\underline{A}\cdot\underline{B}=\underline{A}\cdot\underline{B}=\underline{A+B}$
4. $\underline{A}(\underline{A}+\underline{B})=\underline{A}\cdot\underline{A}+\underline{A}\cdot\underline{B}=\underline{A}+\underline{A}\cdot\underline{B}=\underline{A}(1+\underline{B})=\underline{A}$
5. ...

Answer

1. $A(A+B)+B=AA+AB+B=A+B(A+1)=A+B$
2. $A(A+B)+B(A+B)=(A+B)+(A+B)=A+B$
3. $\underline{A}(A+\underline{B})=\underline{A}A+\underline{A}\cdot\underline{B}=\underline{A}\cdot\underline{B}=\underline{A+B}$
4. $\underline{A}(\underline{A}+\underline{B})=\underline{A}\cdot\underline{A}+\underline{A}\cdot\underline{B}=\underline{A}+\underline{A}\cdot\underline{B}=\underline{A}(1+\underline{B})=\underline{A}$
5. ...