命題、述語、ブール代数

離散数学・オートマトン
2024 年後期
佐賀大学理工学部　只木進一

命題: Propositions

- 言明 (statements): ある事実を述べたもの
  - 真（true, 正しい)、偽（false, 正しくない)
- 命題 (propositions): 真偽が定まる言明
- 真理値/論理値 (truth/logical values)
  - T (true) または F (false)

例 1.1: 簡単な命題

- 7 は素数である: T
- 整数の積は整数である: T

$$\forall x \in Z, \forall y \in Z, \exists z \in Z \Rightarrow xy = z \tag{1.1}$$

- $2 + 3 = 6$: F
- 任意の自然数は、1 を除いて、一つまたはそれ以上の素数の積として一意に表すことができる (算術の基本定理): T

論理積と論理和

- 二つの命題 p と q
- 論理積 (conjunction): $p \wedge q$
  - 二つの命題がいずれも成り立つとき真
- 論理和 (disjunction): $p \vee q$
  - 二つの命題のいずれか一方が成り立つとき真
- 排他的論理和 (exclusive disjunction): $p \oplus q$
  - 二つの命題のいずれか一方だけが成り立つとき真

真理値表 (Truth Table)

p	q	$p \wedge q$	$p \vee q$	$p \oplus q$
T	T	T	T	F
T	F	F	T	T
F	T	F	T	T
F	F	F	F	F

Python で真理値表を作る

```
for p in [True, False]:
    for q in [True, False]:
        x = p and q
        y = p or q
        z = p ^ q
        m = f'{p}:{q}:{x}:{y}:{z}'
        print(m)
```

出力

```
True:True:True:True:False
True:False:False:True:True
False:True:False:True:True
False:False:False:False:False
```

p は q を含意する: p implies q

- p が成り立つならば、q が成り立つ

$$p \Rightarrow q \tag{2.1}$$

- p を前提（仮定)、q を結論という。
- 「p は q を含意する」(p implies q)
- imply: to suggest that something is true without saying so directly

p と q は論理的に等しい: Equivalent

- p が成り立つとき、かつその時に限って、q が成り立つ

$$p \Leftrightarrow q \tag{2.2}$$

$$(p \Rightarrow q) \wedge (q \Rightarrow p) \tag{2.3}$$

- p と q は同値 (logically equivalent)
- p と q は論理的に等しい

必要 (Necessary) と十分 (Sufficient)

- p は q の十分条件
  - p が成り立つときには、必ず q が成り立つ
  - p が成り立たないときにも、q が成り立つ場合があり得る
- q は p の必要条件
  - p が成り立つためには、q が必要
  - q が成り立っても、必ず p がなりたつとは限らない
- p は q の必要十分条件
  - p が成り立つことと、q が成り立つことは同値

命題の「逆(Opposite)」、「裏(Inverse)」、「対偶(Contrapositive)」

- 命題 $p \Rightarrow q$ の逆 (opposite): $q \Rightarrow p$
- 命題 $p \Rightarrow q$ の裏 (inverse):$\neg p \Rightarrow \neg q$
- 命題 $p \Rightarrow q$ の対偶 (contrapositive): $\neg q \Rightarrow \neg p$

p	q	$p \Rightarrow q$	$q \Rightarrow p$	$\neg p \Rightarrow \neg q$	$\neg q \Rightarrow \neg p$
T	T	T	T	T	T
T	F	F	T	T	F
F	T	T	F	F	T
F	F	T	T	T	T

$(p \Rightarrow q) \Leftrightarrow (\neg p \vee q)$

p	q	$p \Rightarrow q$	$\neg p \vee q$
T	T	T	T
T	F	F	F
F	T	T	T
F	F	T	T

Python で確認

```python
for p in [True, False]:
    for q in [True, False]:
        x = (not p) or q
        m = f'{p}:{q}:{x}'
        print(m)
```

結果

```
True:True:True
True:False:False
False:True:True
False:False:True
```

対偶証明法: Proof by contraposition

- 命題 $p \Rightarrow q$ をその対偶 $\neg q \Rightarrow \neg p$ を証明することで示す

例 2.1: 対偶証明法
m 及び n が奇数 $\Rightarrow p = mn$ は奇数

- 対偶: $p = mn$ が偶数のとき、m と n の少なくとも一方は偶数である
- 証明
  - $p = 2m'n'$ と書き直す
  - $m' = m$ ならば $n = 2n'$ となり偶数である
  - $n' = n$ ならば $m = 2m'$ となり偶数である

背理法: Proof by contradiction

- 結果を否定することにより、矛盾を導く

例 2.2: 背理法 合成数(1より大きい素数でない自然数)nは、$\sqrt{n}$以下の素因子を持つ

- n が $\sqrt{n}$ 以下の素因子を持たないと仮定。
- $n = pq \ \ (1 < p \leq q < n)$ と分解
- $n = pq \geq p^2 \Rightarrow \sqrt{n} \geq p$
- p が素数ならば、仮定と矛盾
- p が素数で無いならば、更に因数分解可能
    - $p = rs(r$ は素数) とすると $\sqrt{n} \geq p \geq r$ となり、r という素因子があり、仮定と矛盾

de Morgan の法則

$$\neg (p \vee q) \Leftrightarrow (\neg p) \wedge (\neg q) \tag{2.4}$$
$$\neg (p \wedge q) \Leftrightarrow (\neg p) \vee (\neg q) \tag{2.5}$$

p	q	$\neg (p \vee q)$	$\neg (p \wedge q)$	$(\neg p) \wedge (\neg q)$	$(\neg p) \vee (\neg q)$
T	T	F	F	F	F
T	F	F	T	F	T
F	T	F	T	F	T
F	F	T	T	T	T

述語: predicates

- T または F を値とする関数を述語という
  - 変数の値によって真偽が定まる
- 大文字の P、Q などで表記
- $P : X_0 \times X_1 \times \cdots \times X_{N-1} \to \{\mathsf{T}, \mathsf{F}\}$
  - $X_0 \times X_1 \times \cdots \times X_{N-1}$ 上の述語
- $Q : X^n \to \{\mathsf{T}, \mathsf{F}\}$
  - X 上の n 変数述語
- 命題: 変数の無い述語

例 3.1: 述語

二通りの記述方法を示す

$$P(x) = \begin{cases} \mathsf{T} & \text{if } x \geq 0 \\ \mathsf{F} & \text{otherwise} \end{cases} \tag{3.1}$$

$$P(x) : x \geq 0 \tag{3.2}$$

$$\begin{aligned} P(1) &= \mathsf{T} \\ P(0) &= \mathsf{T} \\ P(-1) &= \mathsf{F} \end{aligned}$$

例 3.2: 述語

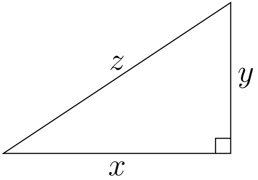
$$P(x, y, z) = \begin{cases} \mathsf{T} & \text{if } x^2 + y^2 = z^2 \\ \mathsf{F} & \text{otherwise} \end{cases} \tag{3.3}$$

$$P(x, y, z) : x^2 + y^2 = z^2 \tag{3.4}$$

$$\begin{aligned} P(3, 4, 5) &= \mathsf{T} \\ P(5, 12, 13) &= \mathsf{T} \\ P(3, 3, 3) &= \mathsf{F} \end{aligned}$$

命題から命題を導出

- $P(x, y, z) : x^2 + y^2 = z^2$
  - x と y が直角三角形の直角を挟む二辺の長さであり、z がその三角形の斜辺の長さである場合に T となる。



- $Q(x, z) : \exists y P(x, y, z)$
  - 組 (x, z) に対して、ある y が存在して、$P(x, y, z) = \mathrm{T}$ となるとき、$Q(x, z) = \mathrm{T}$ となる。
  - つまり、(x, z) が直角三角形の直角を挟む一辺と斜辺の長さであるときに $Q(x, z) = \mathrm{T}$ となる。

論理演算の標準形: Normal forms

- NAND: $A \uparrow B \equiv \neg(A \wedge B)$
- NOR: $A \downarrow B \equiv \neg(A \vee B)$
- 任意の論理式を以下の形式で表現可能
    - $\neg$ と $\wedge$ しか含まない
    - $\neg$ と $\vee$ しか含まない
    - $\neg$ と $\Rightarrow$ しか含まない
    - $\uparrow$ しか含まない
    - $\downarrow$ しか含まない

標準形: 証明

- 論理和が否定と論理積で表現可能: de Morgan

$$p \lor q \equiv \neg\left(\neg p \land \neg q\right)$$

- 論理積が否定と論理和で表現可能: de Morgan

$$p \land q \equiv \neg\left(\neg p \lor \neg q\right)$$

- 論理和、論理積を否定と $\Rightarrow$ で表現

$$p \land q \equiv \neg\left(\neg p \lor \neg q\right) \equiv \neg\left(p \Rightarrow \neg q\right)$$
$$p \lor q \equiv \left(\neg\neg p\right) \lor q \equiv \neg p \Rightarrow q$$

標準形: 証明

- NAND だけで表現できること

$$
\begin{aligned}
\neg p &\equiv \neg(p \wedge p) \equiv p \uparrow p \\
p \vee q &\equiv \neg(\neg p \wedge \neg q) \\
&\equiv \neg((p \uparrow p) \wedge (q \uparrow q)) \\
&\equiv (p \uparrow p) \uparrow (q \uparrow q) \\
p \wedge q &\equiv \neg(\neg p \vee \neg q) \equiv \neg((p \uparrow p) \uparrow (q \uparrow q)) \\
&\equiv \neg(((p \uparrow p) \uparrow (p \uparrow p)) \uparrow ((q \uparrow q) \uparrow (q \uparrow q))) \\
&\equiv \neg(p \uparrow q) \\
&\equiv (p \uparrow q) \uparrow (p \uparrow q)
\end{aligned}
$$

- 注意:

$$
(p \uparrow p) \uparrow (p \uparrow p) \equiv p
$$

Python で確認

```
def nand(p:bool, q:bool) -> bool:
    return not (p and q)

for p in [True, False]:
    for q in [True, False]:
        #and
        x = nand(nand(p,q), nand(p,q))
        #or
        y = nand(nand(p,p), nand(q,quit))
        print(f'{p}:{q}:{x}:{y}')

for p in [True, False]:
    x = nand(nand(p,p), nand(p,p))
    print(f'{p}:{x}')
```

標準形: 証明

- NOR だけで表現できること

$$
\begin{aligned}
\neg p &\equiv \neg(p \vee p) \equiv p \downarrow p \\
p \wedge q &\equiv \neg(\neg p \vee \neg q) \\
&\equiv (p \downarrow p) \downarrow (q \downarrow q) \\
p \vee q &\equiv \neg(\neg p \wedge \neg q) \equiv \neg((p \downarrow p) \downarrow (q \downarrow q)) \\
&\equiv \neg(((p \downarrow p) \downarrow (p \downarrow p)) \downarrow ((q \downarrow q) \downarrow (q \downarrow q))) \\
&\equiv \neg(p \downarrow q) \\
&\equiv (p \downarrow q) \downarrow (p \downarrow q)
\end{aligned}
$$

- 注意:

$$(p \downarrow p) \downarrow (p \downarrow p) \equiv p$$

Python で確認

```
def nor(p:bool, q:bool) -> bool:
    return not (p or q)

for p in [True, False]:
    for q in [True, False]:
        #and
        x = nor( nor(p,p), nor(q,q))
        #or
        y = nor( nor(p,q), nor(p,q))
        print(f'{p}:{q}:{x}:{y}')

for p in [True, False]:
    x = nor( nor(p,p), nor(p,p))
    print(f'{p}:{x}')
```

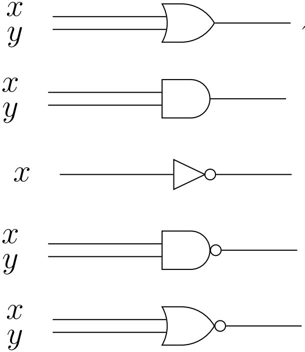
ブール代数

- 1 bit に対して $0 \to$ F、$1 \to$ T と対応付ける
- ブール変数:$\{0, 1\}$
- 演算の対応付け

論理演算	ブール演算
$p \vee q$	$p + q$
$p \wedge q$	$p \cdot q$
$\neg p$	$\bar{p}$

- 基本積: 同じ変数の一回のみ含む論理積

論理回路



$$z = x + y$$

$$z = x \cdot y$$

$$z = \overline{x}$$

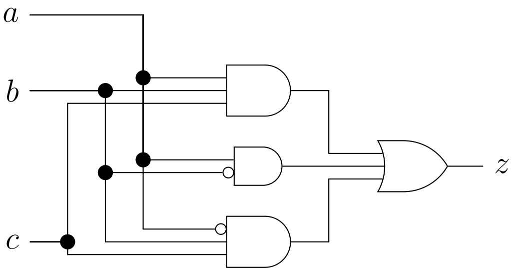
$$z = \overline{x \cdot y}$$

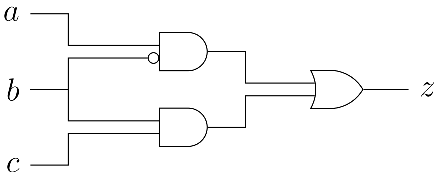
$$z = \overline{x + y}$$

JIS C 0617-2

例 5.1: より少数の基本積へ

$$
\begin{aligned}
z &= abc + a\bar{b} + \bar{a}bc \\
&= (a + \bar{a})\, bc + a\bar{b} \\
&= a\bar{b} + bc
\end{aligned}
$$




a
b
c
z

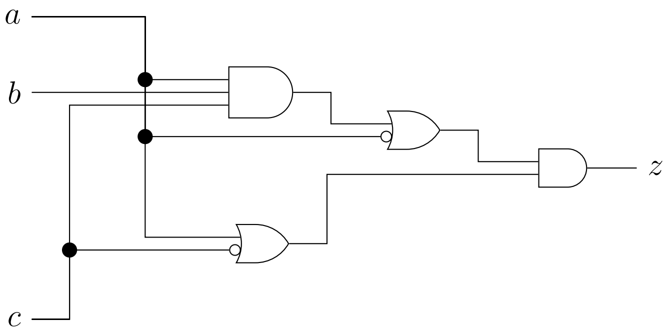
Python で確認

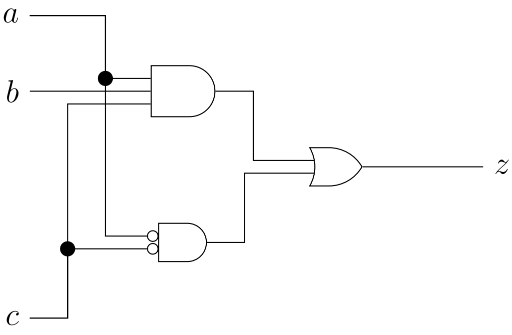
```python
for a in [True, False]:
    for b in [True, False]:
        for c in [True, False]:
            z0 = (a and b and c) or (a and (not b)) or ((not a) and b and c)
            z1 = (a and (not b)) or (b and c)
            m = f'({a},{b},{c})->({z0},{z1})'
            print(m)
```

```
(True,True,True)->(True,True)
(True,True,False)->(False,False)
(True,False,True)->(True,True)
(True,False,False)->(True,True)
(False,True,True)->(True,True)
(False,True,False)->(False,False)
(False,False,True)->(False,False)
(False,False,False)->(False,False)
```

例 5.2:

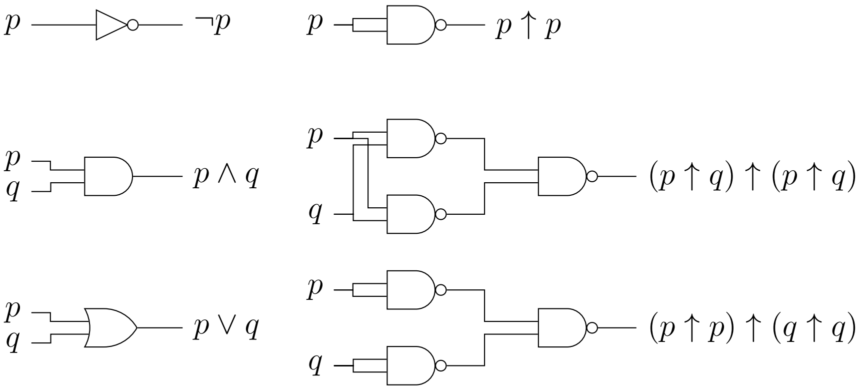
$$
\begin{aligned}
z &= (abc + \bar{a})(a + \bar{c}) \\
&= aabc + abc\bar{c} + a\bar{a} + \bar{a}\bar{c} \\
&= abc + 0 + 0 + \bar{a}\bar{c} \\
&= abc + \bar{a}\bar{c}
\end{aligned}
$$





a
b
c
z

例 5.3: Nand 標準形


p
$\neg p$
p
$p \uparrow p$
p
q
$p \wedge q$
p
q
$(p \uparrow q) \uparrow (p \uparrow q)$
p
q
$p \vee q$
p
q
$(p \uparrow p) \uparrow (q \uparrow q)$