离散数学

Discrete Mathematics

虞慧群

yhq@ecust.edu.cn

主讲老师：杨海

yanghai@ecust.edu.cn

合式公式(Well-Formed Formulas): 递归定义如下：

(1) 命题常元和变元符号是合式公式；

(2) 若A是合式公式，则(¬A)是合式公式，称为A的否定式；

(3) 若A，B是合式公式，则 (A∨B)， (A∧B)， (A→B)， (A↔B)是合式公式；

(4) 所有合式公式都是有限次使用(1)，(2)，(3)、(4)得到的符号串。

子公式 (subformulas): 如果X是合式公式**A**的一部分，且X本身也是一个合式公式，则称X为公式**A**的子公式。

公式举例：

(1) $(((\neg p) \vee q) \to p)$;

(2) $((p \vee q) \wedge ((\neg p) \vee q))$;

(3) $((p \to q) \wedge (q \to p))$;

(4) $(((\neg p) \to p) \leftrightarrow p)$;

(5) $(p \to (\bot \to r))$.

例、如下符号串不是公式：

(1) $((p \vee \top;$

(2) $\neg r;$

(3) $((r \vee X) \rightarrow q);$

约定： （1）最外层的括号可以省略；

（2）联结词运算的优先次序（由高到底）为：

$\neg$

$\wedge$

$\vee$

$\rightarrow$，　$\leftrightarrow$

目的为减少括号的数量。

例、 $\neg p \wedge \neg q$ 表示$((\neg p) \wedge (\neg q))$;

$\neg p \vee q$ 表示$((\neg p) \vee q)$;

- (A→B)不是合式公式，是一个公式模式，代表一类具体的公式

$$(p \longrightarrow q)$$

$$((p \longrightarrow q) \longrightarrow (s \longrightarrow r))$$

$$((p \vee r) \longrightarrow (\neg q))$$

2、 公式的真值

概念

赋值，公式求值函数，真值表，等值式，重言式，矛盾式，蕴含式

赋值（指派，解释）： 设Σ是命题变元集合，则称函数 $v: \Sigma \rightarrow \{1, 0\}$是一个真值赋值。

A是一个公式，v是一个赋值，则A在赋值v下的值，记为v(A),有：

1、若A为命题变元符号p，则v(A)= v(p);

2、若A为命题常元，则

$$v(A) = \begin{cases} 1 & 若A = \top \\ 0 & 若A = \bot \end{cases}$$

3、若A为否定式(¬B)，则

$$v(A)=\begin{cases}1 & 若\,v(B)=0\\0 & 若\,v(B)=1\end{cases}$$

4、若A为析取式(B∨C)，则

$$v(A)=\begin{cases}1 & 若\,v(B)=1或\,v(C)=1\\0 & else\end{cases}$$

5、若A为析取式(B ∧C)，则

$$v(A)=\begin{cases}1 & 若\,v(B)=1且\,v(C)=1\\0 & else\end{cases}$$

6、若A为蕴含式(B→C)，则

$$v(A)=\begin{cases}0 & 若\,v(B)=1且\,v(C)=0\\ 1 & else\end{cases}$$

7、若A为等价式(B ↔C)，则

$$v(A)=\begin{cases}1 & 若\,v(B)=v(C)\\ 0 & else\end{cases}$$

成真赋值：当$v(A)=1$时，称v满足A，记为$v \models A$

成假赋值：当$v(A)=0$时，称v不满足A，记为$v \not\models A$

例、$A=p \vee q$

$v(p)=1, v(q)=0, \quad v(A)=1$

$v(p)=0, v(q)=0, \quad v(A)=0$

真值表：公式A在其所有可能的赋值下所取真值的表，称为A的真值表。

➢ **若公式A中有n个不同变元$p_1, p_2, \ldots, p_n$，那么A共有2^n种不同的赋值。**

例、

公式 $(p \wedge q) \rightarrow r$

p	q	r	$(p \wedge q) \rightarrow r$
1	1	1	1
1	1	0	0
1	0	1	1
1	0	0	1
0	1	1	1
0	0	1	1
0	1	0	1
0	0	0	1

可满足的：公式A，若∃赋值v，使得v $\models$ A，则称A是可满足的。

不可满足的：若∀赋值v，使得v $\not\models$ A，则称A是不可满足的。

例、 $(p\wedge q)\rightarrow r$　可满足的

$(p\wedge \neg p)$　不可满足的

扩充到公式集U

v满足U：公式集U，若$\exists$赋值v，使得对$\forall$公式A$\in$U，有 v $\models$ A，则称v为U的成真赋值。
否则，U是不可满足的。

例、 $\{q \wedge \neg r, q \vee r\}$;

$\{p \rightarrow q, \neg q, p\}$;

重言式、矛盾式

重言式（永真式） 任意赋值v，有v $\models$ A

矛盾式（永假式） 任意赋值v，有v $\not\models$ A

例、$(p \wedge \neg p)$

$(p \vee \neg p)$

- A是永真的当且仅当$\neg$A是永假的。

- 若A是永真的，则A是可满足的；反之不对。

- 设A是公式，则A是矛盾式当且仅当A是不可满足的。

证明：

A是矛盾式$\Leftrightarrow$ $\forall$赋值v， 有v $\not\models$ A

$\Leftrightarrow$$\forall$赋值v， 有v(A)=0

$\Leftrightarrow$不存在赋值v，使得v(A)=1

$\Leftrightarrow$ A是不可满足的

等值式：若等价式$A \leftrightarrow B$是重言式，则称A与B等值，记作$A \Leftrightarrow B$。

注意：

- $\Leftrightarrow$与$\leftrightarrow$是两个完全不同的 符号
- 用真值表可检查两个公式是否等值
- 基本等值式（见课本pp.17-18）

置换规则（置换定理）

设X是公式A的子公式，X$\Leftrightarrow$ Y。将A中的X（可以是全部或部分X）用Y来置换，所得到的公式B，则 A$\Leftrightarrow$B。

判断下列各组公式是否等值:

(1) $p\to(q\to r)$ 与 $(p\wedge q)\to r$

$p\ \ q\ \ r$	$q\to r$	$p\to(q\to r)$	$p\wedge q$	$(p\wedge q)\to r$
0 0 0	1	1	0	1
0 0 1	1	1	0	1
0 1 0	0	1	0	1
0 1 1	1	1	0	1
1 0 0	1	1	0	1
1 0 1	1	1	0	1
1 1 0	0	0	1	0
1 1 1	1	1	1	1

结论: $p\to(q\to r)\Leftrightarrow(p\wedge q)\to r$

等值式例题

(2) $p\to(q\to r)$ 与 $(p\to q)\to r$

p q r	$q\to r$	$p\to(q\to r)$	$p\to q$	$(p\to q)\to r$
0 0 0	1	1	1	0
0 0 1	1	1	1	1
0 1 0	0	1	1	0
0 1 1	1	1	1	1
1 0 0	1	1	0	1
1 0 1	1	1	0	1
1 1 0	0	0	1	0
1 1 1	1	1	1	1

结论：$p\to(q\to r)$ 与 $(p\to q)\to r$ 不等值

基本等值式

双重否定律 $\neg\neg A \Leftrightarrow A$

幂等律 $A \vee A \Leftrightarrow A,\ A \wedge A \Leftrightarrow A$

交换律 $A \vee B \Leftrightarrow B \vee A,\ A \wedge B \Leftrightarrow B \wedge A$

结合律 $(A \vee B) \vee C \Leftrightarrow A \vee (B \vee C),\ (A \wedge B) \wedge C \Leftrightarrow A \wedge (B \wedge C)$

分配律 $A \vee (B \wedge C) \Leftrightarrow (A \vee B) \wedge (A \vee C),$

$A \wedge (B \vee C) \Leftrightarrow (A \wedge B) \vee (A \wedge C)$

德摩根律 $\neg(A \vee B) \Leftrightarrow \neg A \wedge \neg B$

$\neg(A \wedge B) \Leftrightarrow \neg A \vee \neg B$

吸收律 $A \vee (A \wedge B) \Leftrightarrow A,\ A \wedge (A \vee B) \Leftrightarrow A$

基本等值式

零律	$A\vee \top \Leftrightarrow \top$，$A\wedge \bot \Leftrightarrow \bot$
同一律	$A\vee \bot \Leftrightarrow A$. $A\wedge \top \Leftrightarrow A$
排中律	$A\vee\neg A \Leftrightarrow \top$
矛盾律	$A\wedge\neg A\Leftrightarrow \bot$
蕴涵等值式	$A\rightarrow B\Leftrightarrow\neg A\vee B$
等价等值式	$A\leftrightarrow B\Leftrightarrow(A\rightarrow B)\wedge(B\rightarrow A)$
假言易位	$A\rightarrow B\Leftrightarrow\neg B\rightarrow\neg A$
等价否定等值式	$A\leftrightarrow B\Leftrightarrow\neg A\leftrightarrow\neg B$
归谬论	$(A\rightarrow B)\wedge(A\rightarrow\neg B) \Leftrightarrow\neg A$

特别提示：必须牢记这16组等值式，这是继续学习的基础

等值演算——由已知的等值式推演出新的等值式的过程。

证明两个公式等值

例2 证明 $p \to (q \to r) \Leftrightarrow (p \wedge q) \to r$

证 $p \to (q \to r)$

$\Leftrightarrow \neg p \vee (\neg q \vee r)$ （蕴涵等值式，置换规则）

$\Leftrightarrow (\neg p \vee \neg q) \vee r$ （结合律，置换规则）

$\Leftrightarrow \neg (p \wedge q) \vee r$ （德摩根律，置换规则）

$\Leftrightarrow (p \wedge q) \to r$ （蕴涵等值式，置换规则）

3、范式

概念：

文字，析取范式，极小项，主析取范式，合取范式，极大项，主合取范式

文字 设A∈∑（命题变元集），则A和 ¬ A都称为命题符号A的文字，其中前者称为正文字，后者称为负文字。

析取范式

形如

$$A_1 \vee A_2 \vee \ldots \vee A_n \quad (n \geq 1)$$

的公式称为析取范式，其中$A_i(i=1,\ldots,n)$是由文字组成的合取范式。

例：求$\neg (P \vee Q) \leftrightarrow (P \wedge Q)$的析取范式。

极小项 文字的合取式称为极小项，其中公式中每个命题符号的文字都在该合取式中出现一次。

注：(1) n个命题符号共有2^n个极小项。

(2)极小项的编码与性质（p.25）。

主析取范式

给定的命题公式的主析取范式是一个与之等价的公式，后者由极小项的析取组成。

例：求公式$(P\rightarrow Q)\rightarrow R$的主析取范式

定理：公式的真值表中真值为1的指派所对应的极小项的析取，即为此公式的主析取范式。

例：求$P\rightarrow Q$的主析取范式

合取范式

形为

$$A_1 \wedge A_2 \wedge \ldots \wedge A_n \ (n \geq 1)$$

的公式称为合取范式，其中$A_1,\ldots,A_n$都是由文字组成的析取式。

例：求$(P \wedge (Q \rightarrow R)) \rightarrow S$的合取范式

极大项 文字的析取式称为极大项，其中公式中每个命题符号的文字都在该合取式中出现一次。

注：（1）n个命题符号共有2^n个极大项。

（2）极大项的编码等性质（p.25）。

主合取范式 给定的命题公式的主合取范式是一个与之等价的公式，后者由极大项的合取组成。

定理：公式的真值表中真值为0的指派所对应的极大项的合取，即为此公式的主合取范式。

例：求$(P \wedge Q) \vee (\neg P \wedge R)$的主析取范式与主合取范式。

4、联结词的完备集

概念：

真值函数，异或，条件否定，与非，或非，联结词完备集

真值函数： 称$F:\{0,1\}^n \to \{0,1\}$ 为n元真值函数.

$\{0,1\}^n=\{00\ldots0, 00\ldots1, \ldots, 11\ldots1\}$，包含 2^n 个长为n的0,1符号串.
共有 2^{2^n} 个n元真值函数.

1元真值函数

p	$F_0^{(1)}$	$F_1^{(1)}$	$F_2^{(1)}$	$F_3^{(1)}$
0	0	0	1	1
1	0	1	0	1

2元真值函数

p	q	$F_0^{(2)}$	$F_1^{(2)}$	$F_2^{(2)}$	$F_3^{(2)}$	$F_4^{(2)}$	$F_5^{(2)}$	$F_6^{(2)}$	$F_7^{(2)}$
0	0	0	0	0	0	0	0	0	0
0	1	0	0	0	0	1	1	1	1
1	0	0	0	1	1	0	0	1	1
1	1	0	1	0	1	0	1	0	1

p	q	$F_8^{(2)}$	$F_9^{(2)}$	$F_{10}^{(2)}$	$F_{11}^{(2)}$	$F_{12}^{(2)}$	$F_{13}^{(2)}$	$F_{14}^{(2)}$	$F_{15}^{(2)}$
0	0	1	1	1	1	1	1	1	1
0	1	0	0	0	0	1	1	1	1
1	0	0	0	1	1	0	0	1	1
1	1	0	1	0	1	0	1	0	1

异或　　$P \oplus Q \Leftrightarrow \neg(P \leftrightarrow Q)$

条件否定　$P \xrightarrow{c} Q \Leftrightarrow \neg(P \rightarrow Q)$

与非　　$P \uparrow Q \Leftrightarrow \neg(P \wedge Q)$

或非　　$P \downarrow Q \Leftrightarrow \neg(P \vee Q)$

注：能构造多少联结词呢？

11个（二元以内）

联结词的完备集(Adequate Set of Connectives)

设C是联结词的集合，若对于任意一个合式公式均存在一个与之等价的公式，而后者只含有C中的联结词，则称C是联结词的完备集。

例如：

（1）{¬，∧，∨，→，↔}，{ ¬，∧，∨ } 是联结词 的完备集。

（2） {¬， ∧}， {¬， ∨}，{⊥，→}是联结词 的完备集。

（3）{↑}是联结词的完备集。

（4）{ ¬ }，{ ∨ }，{ ∧ }，{ ∨ ,∧ }不是联结词的完备集。

5、推理理论

概念：

重言蕴含式，有效结论，P规则，T规则，CP规则，推理

重言蕴含式 当且仅当$P \rightarrow Q$是一个重言式时，称P重言蕴含Q，记为$P \Rightarrow Q$。

注意: (1) $\Rightarrow$ 和 $\rightarrow$ 含义的本质区别。

(2) 重言蕴含式也称为逻辑蕴含式。

证明$P \Rightarrow Q$的方法：任给赋值v

(1) 假设$v(P)=1$, 推出$v(Q)=1$，或者

(2) 假设$v(Q)=0$, 推出$v(P)=0$。

例：求证：$\neg Q \wedge (P \rightarrow Q) \Rightarrow \neg P$

常见的重言蕴含式(P.46)

推理定律——重言蕴涵式

1. $A \Rightarrow (A \vee B)$ 附加律
2. $(A \wedge B) \Rightarrow A$ 化简律
3. $(A \to B) \wedge A \Rightarrow B$ 假言推理
4. $(A \to B) \wedge \neg B \Rightarrow \neg A$ 拒取式
5. $(A \vee B) \wedge \neg B \Rightarrow A$ 析取三段论
6. $(A \to B) \wedge (B \to C) \Rightarrow (A \to C)$ 假言三段论
7. $(A \leftrightarrow B) \wedge (B \leftrightarrow C) \Rightarrow (A \leftrightarrow C)$ 等价三段论
8. $(A \to B) \wedge (C \to D) \wedge (A \vee C) \Rightarrow (B \vee D)$ 构造性二难

   $(A \to B) \wedge (\neg A \to B) \Rightarrow B$ 构造性二难(特殊形式)
9. $(A \to B) \wedge (C \to D) \wedge (\neg B \vee \neg D) \Rightarrow (\neg A \vee \neg C)$ 破坏性二难

每个等值式可产生两个推理定律

如, 由$A \Leftrightarrow \neg\neg A$可产生 $A \Rightarrow \neg\neg A$ 和 $\neg\neg A \Rightarrow A$