> 本笔记适用于对课上内容已有了解，但时间太久忘了（指考试前）的情况下复习用，不能作为初次学习的指导
> 本笔记基于《离散数学》任明明版ppt

第一章 命题逻辑

基本概念

p	q	$\neg p$	$p \wedge q$	$p \vee q$	$p \rightarrow q$	$p \leftrightarrow q$
0	0	1	0	0	1	1
0	1	1	0	1	1	0
1	0	0	0	1	0	0
1	1	0	1	1	1	1
运算优先级：$\neg > \wedge > \vee > \rightarrow > \leftrightarrow$						
含n个命题变元的公式共有2^n个不同的赋值，真值表有2^n行						

- 若A在它的各种赋值下取值均为真，则称A为**重言式（永真式）**
- 若A在它的各种赋值下取值均为假，则称A为**矛盾式（永假式）**，
- 若A不是矛盾式，则称A为**可满足式**

等值演算

若$A \leftrightarrow B$为重言式，则称A与B等值，记作$A \Leftrightarrow B$
基本等值式：

1. 双重否定律$A \Leftrightarrow \neg\neg A$
2. 幂等律$A \Leftrightarrow A \wedge A, A \Leftrightarrow A \vee A$
3. 交换律$A \wedge B \Leftrightarrow B \wedge A, A \vee B \Leftrightarrow B \vee A$
4. 结合律$A \wedge (B \wedge C) \Leftrightarrow (A \wedge B) \wedge C, A \vee (B \vee C) \Leftrightarrow (A \vee B) \vee C$
5. 分配律$A \wedge (B \vee C) \Leftrightarrow (A \wedge B) \vee (A \wedge C), A \vee (B \wedge C) \Leftrightarrow (A \vee B) \wedge (A \vee C)$
6. 德摩根律$\neg(A \wedge B) \Leftrightarrow \neg A \vee \neg B, \neg(A \vee B) \Leftrightarrow \neg A \wedge \neg B$
7. 吸收律$A \wedge (A \vee B) \Leftrightarrow A, A \vee (A \wedge B) \Leftrightarrow A$
8. 零律$A \wedge 0 \Leftrightarrow 0, A \vee 1 \Leftrightarrow A$
9. 同一律$A \wedge 1 \Leftrightarrow A, A \vee 0 \Leftrightarrow A$
10. 排中律$A \vee \neg A \Leftrightarrow 1$
11. 矛盾律$A \wedge \neg A \Leftrightarrow 0$
12. 蕴含等值式$A \rightarrow B \Leftrightarrow \neg A \vee B$
13. 等价等值式$A \leftrightarrow B \Leftrightarrow (A \rightarrow B) \wedge (B \rightarrow A)$
14. 假言易位$A \rightarrow B \Leftrightarrow \neg B \rightarrow \neg A$
15. 等价否定式$A \leftrightarrow B \Leftrightarrow \neg A \leftrightarrow \neg B$
16. 归谬论证$(A \rightarrow B) \wedge (A \rightarrow \neg B) \rightarrow \neg A$

对偶等值式： 将一个逻辑等值式的∧与∨互换，0与1互换，即可得到对偶等值式

置换规则： 若$A \Leftrightarrow B$，则$\Phi(A) \Leftrightarrow \Phi(B)$
主析取范式的所有简单合取式都是极小项，按成真赋值的二进制编号为$m_0, m_1 \cdots m_{2^n-1}$，记作$m_i \vee m_j \vee \cdots \vee m_k$
主合取范式的所有简单析取式都是极大项，按成假赋值的二进制编号为$M_0, M_1 \cdots M_{2^n-1}$，记作$M_i \wedge M_j \wedge \cdots \wedge M_k$
n个命题变项一共可以产生2^n个极大（小）项，可以产生$C_{2^n}^0 + C_{2^n}^1 + \cdots + C_{2^n}^{2^n} = 2^{2^n}$个主合取（析取）范式

命题逻辑的推理

设S是一个联结词集合，如果任何$n(n \geq 1)$元真值函数都可以由仅含S中的联结词构成的公式表示，则称S是**联结词全功能集**

- $\{\neg, \wedge, \vee\}, \{\neg, \wedge\}, \{\neg, \vee\}, \{\neg, \rightarrow\}$,与非$\{\uparrow\}$,或非$\{\downarrow\}$都是联结词全功能集

若$A \rightarrow B \Leftrightarrow 1$，则称$A \Rightarrow B$
基本蕴含关系

1. 化简律$A \wedge B \Rightarrow A, A \wedge B \Rightarrow B$
2. 附加律$A \Rightarrow A \vee B$
3. 假前键恒真$\neg A \Rightarrow A \rightarrow B$
4. 真后键恒真$B \Rightarrow A \rightarrow B$
5. 蕴涵等值式$\neg(A \rightarrow B) \Rightarrow A, \neg(A \rightarrow B) \Rightarrow \neg B$
6. 前真推后真（假言推理）$A \wedge (A \rightarrow B) \Rightarrow B$
7. 后假推前假（拒取式）$\neg B \wedge (A \rightarrow B) \Rightarrow \neg A$
8. 排除法（析取三段论）$\neg A \wedge (A \vee B) \Rightarrow B$
9. 传递性（假言三段论）$(A \rightarrow B) \wedge (B \rightarrow C) \Rightarrow (A \rightarrow C)$
10. 充分性$(A \vee B) \wedge (A \rightarrow C) \wedge (B \rightarrow C) \Rightarrow C$
11. 蕴含分配率（构造性二难）$(A \rightarrow B) \wedge (D \rightarrow C) \Rightarrow (A \wedge D) \rightarrow (B \wedge C)$
12. 等值传递性（等价三段论）$(A \leftrightarrow B) \wedge (B \leftrightarrow C) \Rightarrow (A \leftrightarrow C)$
13. 构造性二难$(A \rightarrow B) \wedge (\neg A \rightarrow B) \Rightarrow B$
14. 破坏性二难$(A \rightarrow B) \wedge (C \rightarrow D) \wedge (\neg B \vee \neg D) \Rightarrow (\neg A \vee \neg C)$

推理规则

- P（前提引入）
- T（结论）
- CP（附加前提引入）
- 归谬法P（结论否定作为前提引入）

第二章 谓词逻辑

谓词逻辑的基本概念

全称量词： $\forall x P(x)$，常与$\rightarrow$联结，如$\forall x(P(x) \rightarrow Q(x))$
存在量词： $\exists x P(x)$，常与$\wedge$联结，如$\exists x(P(x) \wedge Q(x))$

等值演算

1. 量词转换律
   $\neg(\forall x)P(x) \Leftrightarrow (\exists x)\neg P(x)$
   $\neg(\exists x)P(x) \Leftrightarrow (\forall x)\neg P(x)$
2. 量词辖域扩张及收缩律
   $(\forall x)A(x) \vee B \Leftrightarrow (\forall x)(A(x) \vee B)$
   $(\forall x)A(x) \wedge B \Leftrightarrow (\forall x)(A(x) \wedge B)$
   $(\exists x)A(x) \wedge B \Leftrightarrow (\exists x)(A(x) \wedge B)$
   $(\exists x)A(x) \vee B \Leftrightarrow (\exists x)(A(x) \vee B)$
   $(\forall x)A(x) \rightarrow B \Leftrightarrow (\exists x)(A(x) \rightarrow B)$ 后合并变号
   $(\exists x)A(x) \rightarrow B \Leftrightarrow (\forall x)(A(x) \rightarrow B)$
   $A \rightarrow (\forall x)B(x) \Leftrightarrow (\forall x)(A \rightarrow B(x))$ 前合并不变
   $A \rightarrow (\exists x)B(x) \Leftrightarrow (\exists x)(A \rightarrow B(x))$
3. 等值分配律
   $(\forall x)(A(x) \wedge B(x)) \Leftrightarrow ((\forall x)A(x)) \wedge ((\forall x)B(x))$
   $(\exists x)(A(x) \vee B(x)) \Leftrightarrow ((\exists x)A(x)) \vee ((\exists x)B(x))$
4. 蕴含分配律
   $(\forall x)(A(x) \vee B(x)) \Rightarrow ((\forall x)A(x)) \vee ((\forall x)B(x))$
   $(\exists x)(A(x) \wedge B(x)) \Rightarrow ((\exists x)A(x)) \wedge ((\exists x)B(x))$
5. 量词换序
   $(\forall x)(\forall y)P(x,y) \Leftrightarrow (\forall y)(\forall x)P(x,y) \Rightarrow (\exists y)(\forall x)P(x,y) \Rightarrow (\forall x)(\exists y)P(x,y) \Rightarrow$
   $(\exists x)(\exists y)P(x,y) \Leftrightarrow (\exists y)(\exists x)P(x,y)$

推理原则

1. 全称指定原则（US）$\forall x P(x) \Rightarrow P(u)$
2. 全称推广原则（UG）$P(u) \Rightarrow \forall x P(x)$
3. 存在指定原则（ES）$\exists x P(x) \Rightarrow P(c)$
4. 存在推广原则（EG）$P(c) \Rightarrow \exists x P(x)$

- 连续使用US可用相同变元，先用ES后用US可取相同变元。
- 先用US后用ES取不同变元，连续使用ES取不同变元。

第三章 集合论

集合论的基本概念

省略简单概念
幂集$P(A) = \{x \mid x \subseteq A\}$，如果$|A| = n$，则$|P(A)| = 2^n$
对称差$A \oplus B = (A \cup B) - (A \cap B) = (A - B) \cup (B - A)$，符合交换律和结合律
对称差与交可分配，$A \cap (B \oplus C) = (A \cap B) \oplus (A \cap C)$
差集的德摩根律，$(A - B) \cap (A - C) = A - (B \cup C), (A - B) \cup (A - C) = A - (B \cap C)$

容斥原理

$$|\bar{A}_1 \cap \bar{A}_2 \cap \cdots \cap \bar{A}_n| = |S| - \sum_{i=1}^{n} |A_i| + \sum_{1 \le i < j \le m} |A_i \cap A_j| - \sum_{1 \le i < j < k \le m} |A_i \cap A_j \cap A_k| + \cdots + (-1)^n |A$$

$$|A_1 \cup A_2 \cup \cdots \cup A_n| = \sum_{i=1}^{n} |A_i| - \sum_{1 \le i < j \le m} |A_i \cap A_j| + \sum_{1 \le i < j < k \le m} |A_i \cap A_j \cap A_k| - \cdots + (-1)^{n-1} |A_1 \cap$$

笛卡尔积与二元关系

笛卡尔积

设A, B为集合，$A \times B = \{\langle a, b \rangle \mid a \in A, b \in B\}$，称为$A$和$B$的**笛卡尔积**，记作$A \times B$
性质：

1. $A \times \varnothing = \varnothing \times A = \varnothing$
2. 不满足交换律，$A \times B \neq B \times A$
3. 不满足结合律，$A \times (B \times C) \neq (A \times B) \times C$
4. 对并和交分别满足分配律，$A \times (B \cup C) = A \times B \cup A \times C, A \times (B \cap C) = A \times B \cap A \times C$
5. 若$|A| = n, |B| = m$，则$|A \times B| = nm$

二元运算

如果一个非空集合，且它的元素都是有序对，则称它为**二元关系**，空集合也是二元关系，记作R，如$\langle x, y \rangle \in R$，可记作$xRy$
设A, B为集合，R为$A \times B$的子集，称R为**从A到B的（二元）关系**，当$A = B$时称为 **A上的（二元）关系**
空关系$\varnothing$，全域关系$E_A = A \times A$，恒等关系$I_A = \{\langle x, x \rangle \mid x \in A\}$
$|A| = n, |A \times A| = n^2, |E_A| = n^2, |I_A| = n, A$上的关系数为$2^{n^2}$

- **定义域**$dom(R) = \{x \mid \exists y(xRy)\}$
- **值域**$ran(R) = \{y \mid \exists x(xRy)\}$
- **域**$fld(R) = dom(R) \cup ran(R)$
- **逆关系**$R^{-1} = \{\langle y, x \rangle \mid \langle x, y \rangle \in R\}$
- **合成关系**$R \circ S = \{\langle x, z \rangle \mid \exists y(\langle x, y \rangle \in R \wedge \langle y, z \rangle \in S)\}$
- **R在A上的限制**$R|_A = \{\langle x, y \rangle \mid \langle x, y \rangle \in R \wedge x \in A\}$
- **A在R上的像**$R[A] = ran(R|_A)$
- **R的n次幂**$R^0 = I_A, R^n = R \circ R^{n-1}$

定理：

1. $R = (R^{-1})^{-1}$
2. $dom(R) = ran(R^{-1}), ran(R) = dom(R^{-1})$
3. $dom(R \cup S) = dom(R) \cup dom(S), ran(R \cup S) = ran(R) \cup ran(S)$
4. $dom(R \cap S) \subseteq dom(R) \cap dom(S), ran(R \cap S) \subseteq ran(R) \cap ran(S)$
5. $(R \cup S)^{-1} = R^{-1} \cup S^{-1}, (R \cap S)^{-1} = R^{-1} \cap S^{-1}$
6. $(R - S)^{-1} = R^{-1} - S^{-1}, (R \subseteq S)^{-1} \Rightarrow R^{-1} \subseteq S^{-1}$

7. $R \circ S = (S \circ R)^{-1}$
8. $(F \circ G) \circ H = F \circ (G \circ H)$
9. $F \circ (G \cup H) = (F \circ G) \cup (F \circ H), F \circ (G \cap H) \subseteq (F \circ G) \cap (F \circ H)$
10. 必存在s, t，使得$R^s = R^t$
11. $R^m \circ R^n = R^{m+n}$
12. $(R^m)^n = R^{mn}$

二元关系的性质

- 自反性，$\forall x(x \in A \to \langle x, x \rangle \in R)$
- 反自反性，$\forall x(x \in A \to \langle x, x \rangle \notin R)$
- 对称性，$\forall x \forall y(x, y \in A \land \langle x, y \rangle \in R \Rightarrow \langle y, x \rangle \in R)$
- 反对称性，$\forall x \forall y(x, y \in A \land \langle x, y \rangle \in R \land \langle y, x \rangle \in R \Rightarrow x = y)$
- 传递性，$\forall x \forall y \forall z(x, y \in A \land y, z \in A \land \langle x, y \rangle \in R \land \langle y, z \rangle \in R \Rightarrow \langle x, z \rangle \in R)$
- R是自反的 $I_A \subseteq R$
- R是反自反的 $R \cap I_A = \varnothing$
- R是对称的 $R = R^{-1}$
- R是反对称的 $R \cap R^{-1} \subseteq I_A$
- R是传递的 $R \circ R \subseteq R$

闭包：设R是A上的关系，R的自反（对称或传递）闭包记作是A上的关系R'，使得R'满足：

- $R \subseteq R'$
- R'是自反（对称或传递）的
- 对A上任何包含R的自反（对称或传递）关系S，有$R' \subseteq S$

自反闭包记作$r(R)$，对称闭包记作$s(R)$，传递闭包记作$t(R)$

- $r(R) = R \cup I_A$
- $s(R) = R \cup R^{-1}$
- $t(R) = R \cup R^2 \cup R^3 \cup \cdots$

性质：

1. 不动点定理：若$R \subseteq A \times A$，则
   R是自反的 $\iff r(R) = R$
   R是对称的 $\iff s(R) = R$
   R是传递的 $\iff t(R) = R$
2. 单调性：若$R, S \subseteq A \times A$，且$R \subseteq S$，则
   $r(R) \subseteq r(S)$
   $s(R) \subseteq s(S)$
   $t(R) \subseteq t(S)$
3. 交换性：若$R \subseteq A \times A$，则
   $rs(R) = sr(R)$
   $rt(R) = tr(R)$
   $st(R) \subseteq ts(R)$
4.

	自反性	**对称性**	**传递性**
r(R)	✔	✔	✔

	自反性	对称性	传递性
s(R)	✔	✔	✘
t(R)	✔	✔	✔

Warshell算法：给定一个关系矩阵R，

```
for k = 1 to n
    for i = 1 to n
        for j = 1 to n
            R[i][j] = R[i][j] | (R[i][k] & R[k][j])
```

等价关系

等价关系： 若R是A上的关系，且R是自反的、对称的和传递的，则称R是A上的等价关系。
等价类： 若R是A上的等价关系，$\forall x \in A$，$[x]_R = \{y \mid \langle x, y\rangle \in R\}$，则称$[x]_R$是$R$的等价类，简记为$[x]$。
商集： 若R是A上的等价关系，以R的所有等价类为元素的集合称为A上的R的商集，记作A/R，$A/R = \{[x]_R \mid x \in A\}$
集合的划分： 若A是一个集合，P的每个元素都是A的一个子集且不为空，且P中的任意两个子集都不相交，且P中所有元素的并等于A，则称P是A的一个划分。
等价关系与划分一一对应
若$|A| = n$，则A上的等价关系共有$\sum_{k=1}^{n} \left\{ n \atop k \right\}$个，其中$\left\{ n \atop k \right\}$表示$n$个不同元素恰好分为$k$个集合的方案数。

偏序关系

偏序关系： 若R是A上的关系，且R是自反的、反对称的和传递的，则称R是A上的偏序关系，记作$\preceq$，若$\langle x, y\rangle \in R$，则称$x \preceq y$，如小于等于关系。
x与y可比： 若$x \preceq y$或$y \preceq x$，则称x与y可比。
全序关系： 若R是A上的偏序关系，且$\forall x, y \in A$，$x \preceq y$或$y \preceq x$，则称R是A上的全序（或线序）关系。
覆盖： 若R是A上的偏序关系，$x, y \in A$，且$x \prec y$，且不存在$z \in A$，使得$x \prec z \prec y$，则称x覆盖y。
偏序集： 若A是一个集合，A和A上的偏序关系$\preceq$一起称为偏序集，记作$\langle A, \preceq\rangle$。
哈斯图：
设$\langle A, \preceq\rangle, B \subseteq A$，$y \in B$，

- 若$\forall x \in B, x \preceq y$，则称$y$是$B$的最大元
- 若$\forall x \in B, y \preceq x$，则称$y$是$B$的最小元
- 若$\neg\exists x \in B, x \preceq y$，则称$y$是$B$的极小元
- 若$\neg\exists x \in B, y \preceq x$，则称$y$是$B$的极大元
- 最元存在必唯一且是极元

设$\langle A, \preceq\rangle, B \subseteq A$，$y \in A$，

- 若$\forall x \in B, x \preceq y$，则称$y$是$B$的上界
- 若$\forall x \in B, y \preceq x$，则称$y$是$B$的下界
- 上界中的最小元称为B的最小上界或上确界
- 下界中的最大元称为B的最大下界或下确界
- 集合的最小元就是下确界，最大元就是上确界，反之不然

链： 若$\langle A, \preceq\rangle$是一个偏序集，$B \subseteq A$，且$B$中的任意两个元素$x, y$都可比，则称$B$是$A$的一条链，$|B|$称为链的长度。
反链： 若$\langle A, \preceq\rangle$是一个偏序集，$B \subseteq A$，如果$\forall x, y \in B, x \neq y$，$x$与$y$都是不可比的，则称$B$是$A$的一条反链，$|B|$称为反链的长度。

拟序关系

拟序关系： 若R是A上的关系，且R是反自反的、传递的（蕴含反对称），则称R是A上的拟序关系，记作$\prec$。
$\preceq - I_A \to \prec$，$\prec \cup I_A \to \preceq$。

代数系统

运算

运算性质：
略
幺元：

- 左幺元：$\exists e_l \in A, \forall x \in A, e_l \cdot x = x$
- 右幺元：$\exists e_r \in A, \forall x \in A, x \cdot e_r = x$
- 幺元：$\exists e \in A, \forall x \in A, e \cdot x = x = x \cdot e$
- 存在必唯一 $e_l = e_r = e$

零元：

- 左零元：$\exists \theta_l \in A, \forall x \in A, \theta_l \cdot x = \theta_l$
- 右零元：$\exists \theta_r \in A, \forall x \in A, x \cdot \theta_r = \theta_r$
- 零元：$\exists \theta \in A, \forall x \in A, \theta \cdot x = \theta = x \cdot \theta$
- 存在必唯一 $0_l = 0_r = 0$

逆元：

- 左逆元：$\exists x^{-1} \in A, \forall x \in A, x^{-1} \cdot x = e$
- 右逆元：$\exists x^{-1} \in A, \forall x \in A, x \cdot x^{-1} = e$
- 逆元：$\exists x^{-1} \in A, \forall x \in A, x^{-1} \cdot x = x \cdot x^{-1} = e$
- 左右逆元不一定相等且不一定唯一

若$\langle A, *\rangle$是一个代数系统，$|A| > 1$，且存在幺元和零元，则$\theta \neq e$
若$\langle A, *\rangle$是一个代数系统，$*$可结合，a关于$*$的左右逆元存在，则两者相等，且逆元唯一
若$\langle A, *\rangle$是一个代数系统，存在幺元e，且每个元素都有左逆元，则左右逆元相等，且逆元唯一

代数结构

$\langle G, *\rangle$

- 封闭，则为**广群**
- 加上$*$满足结合律，则为**半群**

- 加上含有幺元，则为**独异点（幺半群）**
- 加上可逆，则为**群**
- 可交换的群，则为**阿贝尔群**
- G是群，$\exists a \in G, \forall x \in G, x = a^n$，则为**循环群**，$a$为生成元

定理：

1. 半群的封闭子群也是半群，称为子半群
2. $\langle S, *\rangle$是半群，S为有限集，则必有$a \in S, a * a = a$（幂等元）
3. 幺半群的运算表中任何两行、列都不同
4. 独异点中含逆元的a, b有$(a^{-1})^{-1} = a$，$(a * b)^{-1} = b^{-1} * a^{-1}$
5. G是群，$|G|$称为群的阶
6. 阶数大于1的群中不存在零元
7. 存在唯一的元素$x \in G$，使$a * x = b$
8. 消去律成立：$a * b = a * c \Rightarrow b = c$
9. 有限群的运算表中的每一行或每一列都是G的元素的置换
10. 群中，除幺元e外，不可能有任何别的等幂元
11. G中的幺元e必定也是子群S中的幺元. 且元素在子群S中的逆元即为在群G中的逆元
12. $B \subseteq G$，B封闭，有限，非空，则B必是子群
13. $B(\neq \varnothing) \subseteq G, \forall a, b \in B, a * b^{-1} \in B \Leftrightarrow B$是$G$的子群
14. G是群，$\forall a, b \in G, (a * b) * (a * b) = (a * a) * (b * b) \Leftrightarrow G$是阿贝尔群
15. 循环群必是阿贝尔群
16. G是群，$a \in G, a^n = e, n$尽量小，则称a的阶为n
17. 有限循环群的阶为n，则$G = \{a, a^2, \cdots, a^{n-1}, a^n (= e)\}$，生成元的阶等于群的阶
18. 设$G = \langle a \rangle$是循环群：
    1. 若G是无限循环群，则G只有a和a^{-1}两个生成元
    2. 若G是n阶循环群，则a^r是生成元$\Leftrightarrow$ r是n的约数
    3. G的子群仍是循环群
    4. 若G是无限循环群，则G的子群除$\{e\}$都是无限循环群
    5. 若G是n阶循环群，则对n的每个正因子d，G的子群$\langle a^{n/d} \rangle$是d阶循环群