离散数学笔记

Kajih Du

数理逻辑

1 命题

命题: 有**确定真值**的**陈述句**为命题。真值，只有“真”（T）、“假”（F）两种，**不能既真又假**。（悖论不是命题！）
原子命题: 不能分解为更简单陈述句的命题。
复合命题: 由联结词、标点符号和原子命题复合构成的命题。
命题的标识符表示确定的命题，则称为*命题常量*，如果命题的标识符只表示任意命题的位置，则称为*命题变元*。命题变元不能确定真值，所以**命题变元不是命题**。命题变元如果表示原子命题时，变元称为*原子变元*。

2 联结词

2.1 否定（Negation）

若P为一命题，加上否定词得到一个新的命题，称为其否定。其否定记为$\neg P$。否定$\neg$是一元联结词。否定的真值表为

P	$\neg P$
T	F
F	T

2.2 合取（Conjunction）

若P和Q为命题，那么$P \wedge Q$表示的命题“P并且Q”只有当P和Q均为真的时候成真，否则为假。$P \wedge Q$称为P和Q的合取，其真值表为

P	Q	$P \wedge Q$
T	T	T
T	F	F
F	T	F
F	F	F

2.3 析取（Disjunction）

若P和Q为命题，那么$P \vee Q$表示的命题“P或者”只有当P和Q均为假的时候成假，否则为真。$P \vee Q$称为P和Q的析取，其真值表为

P	Q	$P \vee Q$
T	T	T
T	F	T
F	T	T
F	F	F

析取代表**可兼或**，即两者都可取真。有时候P和Q不能够同时成立，此时需要使用*异或*$\oplus$。

2.4 蕴含（Implication）

P和Q为命题，命题$P \to Q$表示命题“如果P为真，那么Q也为真”，只有当P为真而Q为假的时候命题$P \to Q$为假，否则为真。命题P称为前件（假设），命题Q称为后件（结论）。蕴含有时也被称为*条件语句*。蕴含的真值表为

P	Q	$P \to Q$
T	T	T
T	F	F
F	T	T
F	F	T

$P \to Q$体现了P不必是Q成立的必要条件，即P是Q的充分条件，Q是P的必要条件。
善意推定：当前件P为假时，不管Q的真假如何，都认为$P \to Q$为真。
$P \to Q$的陈述：P是Q的充分条件，Q是P的必要条件，若P则Q，Q每当P，P仅当Q，只有Q才P，除非Q才P，除非Q否则$\neg P$。

逆蕴含：$Q \to P$
倒置蕴含：$\neg Q \to \neg P$
反蕴含：$\neg P \to \neg Q$

$\neg Q \to \neg P$与$P \to Q$有相同的真值，即**一个蕴含与其倒置蕴含等价**。

2.5 双条件（Biconditional）

P，Q为两个命题，双条件$P \leftrightarrow Q$表示命题只有在P和Q具有相同的真值时为真，否则为假。双条件的真值表为

P	Q	$P \leftrightarrow Q$
T	T	T
T	F	F
F	T	F
F	F	T

即$P \leftrightarrow Q$只在$P \to Q$和$Q \to P$为真的时候为真，双条件通常可以表述为“P当且仅当Q”。双条件联结词也可以用“iff”代替。

$P \leftrightarrow Q$和$(P \to Q) \wedge (Q \to P)$有相同的真值。

3 合式公式

合式公式（wff）规定为：

1. 命题变元是合式公式；
2. 如果A为合式公式，那么$\neg A$也是合式公式；
3. 如果A, B为合式公式，那么$(A \wedge B), (A \vee B), (A \to B), (A \leftrightarrow B)$均为合式公式；
4. 当且仅当经过有限次地使用1, 2, 3所组成的符号串才是合式公式。

运算符的优先级：$\neg$、$\wedge$、$\vee$、$\to$、$\leftrightarrow$。

3.1 重言式与可满足式

一个公式（以下将合式公式均简称为公式）对于任意解释其值均为真，则其为*重言式*（永真式）。例如$P \vee \neg P$是一个重言式。
由$\wedge$、$\vee$、$\to$、$\leftrightarrow$联结的重言式仍然是重言式。
如果一个公式在某一解释下为真，则其为*可满足式*。显然重言式是可满足式。

3.2 矛盾式

一个公式对于任意解释其值均为假，则其为*矛盾式*（永假式）。例如$P \wedge \neg P$为一个矛盾式。

重言式、可满足式、矛盾式关系:

1. A永真，当且仅当$\neg A$永假;
2. A可满足，当且仅当$\neg A$非永真;
3. 非可满足的公式必永假;
4. 非永假的公式必可满足。

3.3 等值定理

对于两个命题公式A和B，$P_1 \cdots P_n$是出现在A, B中所有命题变元，那么公式A和B共有2^n种解释，对于任意解释，公式A和B的真值相同，那么A与B等价，即$A = B$。

等值定理: A, B为命题，$A = B$当且仅当$A \leftrightarrow B$为重言式。

$A = B$与$A \leftrightarrow B$不同，仅$A \leftrightarrow B$为真时有$A = B$；$A = B$不是合式公式而$A \leftrightarrow B$是合式公式。

3.3.1 基本等价关系

幂等律: $G \vee G = G; G \wedge G = G$
交换律: $G \vee G = H \vee G; G \wedge H = H \wedge G$
结合律: $G \vee (H \vee S) = (G \vee G) \vee S; G \wedge (H \wedge S) = (G \wedge H \wedge S)$
同一律: $G \vee F = G; G \wedge T = G$
支配律: $G \vee T = T; G \wedge F = F$
分配律: $G \vee (H \wedge S) = (G \vee H) \wedge (G \vee S); G \wedge (H \vee S) = (G \wedge H) \vee (G \wedge S)$
吸收律: $G \vee (G \wedge H) = G; G \wedge (G \vee H) = G$
矛盾律: $\neg G \vee G = F$
排中律: $\neg G \wedge G = T$
双非律: $\neg(\neg G) = G$
De Morgan律: $\neg(G \vee H) = \neg G \wedge \neg H; \neg(G \wedge H) = \neg G \vee \neg H$
蕴含式: $G \rightarrow H = \neg G \vee H$
假言易位: $G \rightarrow H = \neg H \rightarrow \neg G$

等价式：$G \leftrightarrow H = (G \to H) \wedge (H \to G) = (\neg G \vee H) \wedge (\neg H \vee G)$
等价否定：$G \leftrightarrow H = \neg G \leftrightarrow \neg H$
归谬：$(G \to H) \wedge (G \to \neg H) = \neg G$ （反证法之原理）

3.4 对偶式

在给定的命题公式A中，将联结词$\wedge$换成$\vee$，$\vee$换成$\wedge$，特殊变元F和T互换，得到的新的命题公式A^*称为A的*对偶式*。

性质：

1. 如果A和A^*互为对偶式，且$P_1, P_2, \cdots, P_n$为A与A^*中的原子变元，那么有
   - $\neg A(P_1, P_2, \cdots, P_n) \iff A^*(P_1, P_2, \cdots, P_n)$
   - $A(\neg P_1, \neg P_2, \cdots, \neg P_n) = \neg A^*(P_1, P_2, \cdots, P_n)$

   证明：利用De Morgan律，易证之。
2. 如果$A \iff B$，则$A^* \iff B^*$。

证明：$A \iff B$则$A(P_1, P_2, \cdots, P_n) \leftrightarrow B(P_1, P_2, \cdots, P_n)$为重言式，因此$P_1, P_2, \cdots, P_n$的真值不影响$A \leftrightarrow B$的真值，因而$A(\neg P_1, \neg P_2, \cdots, \neg P_n) \leftrightarrow B(\neg P_1, \neg P_2, \cdots, \neg P_n)$也是重言式。考虑对偶式的性质$A(\neg P_1, \neg P_2, \cdots, \neg P_n) = \neg A^*(P_1, P_2, \cdots, P_n)$，得到$\neg A^* \leftrightarrow \neg B^*$为重言式，即$A^* \leftrightarrow B^*$，命题得证。

3.5 范式

任何命题公式都存在与之等值的合取范式和析取范式。

合取范式：当一个命题具有$A_1 \wedge A_2 \wedge \cdots \wedge A_n$的形式，其中$A_1, A_2, \cdots, A_n$为命题变元及其否定组成的析取式。
析取范式：当一个命题具有$A_1 \vee A_2 \vee \cdots \vee A_n$的形式，其中$A_1, A_2, \cdots, A_n$为命题变元及其否定组成的合取式。

求取范式常用公式：

消去$\to$与$\leftrightarrow$：

$$
\begin{aligned}
A \to B &= \neg A \vee B \\
A \leftrightarrow B &= (\neg A \vee B) \wedge (\neg B \vee A) \quad \text{(用于求合取范式)} \\
&= (A \wedge B) \vee (\neg A \wedge \neg B) \quad \text{(用于求析取范式)}
\end{aligned}
$$

一般常用真值转写法。

对于简单命题P，P与$\neg P$统称为*文字*。

3.5.1 主析取范式

极小项：对有n个命题变元$P_1, \cdots, P_n$的命题，公式$Q_1 \wedge Q_2 \wedge \cdots \wedge Q_n$（$Q_i = P_i \text{ or } \neg P_i$）为极小项。极小项必须包含全部$n$个文字。

将P与1对应，$\neg P$与0对应，极小项可以如下表记

$$
\begin{gathered}
P_1 \wedge P_2 \wedge P_3 = m_7 \ \text{（对应111，即7）} \\
P_1 \wedge \neg P_2 \wedge P_3 = m_5 \ \text{（对应101，即5）} \\
\neg P_1 \wedge \neg P_2 \wedge \neg P_3 = m_0 \ \text{（对应000，即0）}
\end{gathered}
$$

仅由极小项构成的析取范式就是*主析取范式*。

极小项的性质：

1. 含有n个命题变元的公式，极小项的个数为2^n个。
2. 每个极小项只有一个解释成真。
3. 极小项两两不等值，且$m_i \wedge m_j = F \ (i \neq j)$。
4. 恰有2^n个极小项的析取构成的公式必为重言式，即

   $$\bigvee_{i=0}^{2^n-1} m_i = T$$

   如果命题P由k个极小项析取组成，那么剩下的$2^n - k$个极小项的析取为$\neg P$。

3.5.2 主合取范式

极大项：对有n个命题变元$P_1, \cdots, P_n$的命题，公式$Q_1 \vee Q_2 \vee \cdots \vee Q_n$（$Q_i = P_i \text{ or } \neg P_i$）为极大项。极大项必须包含全部$n$个文字。

将P与1对应，$\neg P$与0对应，极大项可以如下表记

$$
\begin{gathered}
P_1 \vee P_2 \vee P_3 = M_7 \ \text{（对应111，即7）} \\
P_1 \vee \neg P_2 \vee P_3 = M_5 \ \text{（对应101，即5）} \\
\neg P_1 \vee \neg P_2 \vee \neg P_3 = M_0 \ \text{（对应000，即0）}
\end{gathered}
$$

仅由极大项构成的析取范式就是*主合取范式*。

极大项的性质：

1. 含有n个命题变元的公式，极大项的个数为2^n个。
2. 每个极大项只有一个解释成假。
3. 极大项两两不等值，且$M_i \vee M_j = T \ (i \neq j)$。
4. 恰有2^n个极大项的合取构成的公式必为永假式，即

$$\bigwedge_{i=0}^{2^n-1} m_i = F$$

   如果命题P由k个极大项合取组成，那么剩下的$2^n - k$个极大项的合取为$\neg P$。

通过真值表可以书写命题的主析取范式和主合取范式。

3.5.3 析取范式和合取范式的转化

合取范式转化为析取范式

$$A = \bigwedge\nolimits_{\{i,j,\cdots\}}$$
$$\neg A = \bigwedge\nolimits_{\{0,1,\cdots,2^n-1\}-\{i,j,\cdots\}}$$
$$A = \neg\neg A = \neg \bigwedge\nolimits_{\{0,1,\cdots,2^n-1\}-\{i,j,\cdots\}} = \bigvee\nolimits_{(\{0,1,\cdots,2^n-1\}-\{i,j,\cdots\})_{补}}$$

析取范式转化为合取范式

$$A = \bigvee\nolimits_{\{i,j,\cdots\}}$$
$$\neg A = \bigvee\nolimits_{\{0,1,\cdots,2^n-1\}-\{i,j,\cdots\}}$$
$$A = \neg\neg A = \neg \bigvee\nolimits_{\{0,1,\cdots,2^n-1\}-\{i,j,\cdots\}} = \bigwedge\nolimits_{(\{0,1,\cdots,2^n-1\}-\{i,j,\cdots\})_{补}}$$

3.6 联结词的完备集

$\{\wedge, \neg\}$与$\{\vee, \neg\}$是联结词的完备集，且为一组基底（最小的完备集）。

与非$\uparrow$：$A \uparrow B = \neg(A \wedge B)$

或非$\downarrow$：$A \downarrow B = \neg(A \vee B)$

$\{\uparrow\}$是一个基底。（只需要证明其能表示$\{\wedge, \neg\}$或$\{\vee, \neg\}$即可）

$$\neg A = A \uparrow A \quad A \wedge B = \neg(A \uparrow B) = (A \uparrow B) \uparrow (A \uparrow B)$$

$\{\downarrow\}$也是一个基底。（只需要证明其能表示$\{\wedge, \neg\}$或$\{\vee, \neg\}$即可）

$$\neg A = A \downarrow A \quad A \vee B = \neg(A \downarrow B) = (A \downarrow B) \downarrow (A \downarrow B)$$

注意：$\{\wedge, \vee\}$和$\{\neg, \leftrightarrow\}$不是完备集。

任取四个一元或二元联结词，必不构成基底。

常见的基底：一个元素$\{\uparrow\}, \{\downarrow\}$；两个元素$\{\neg, \wedge\}, \{\neg, \vee\}, \{\neg, \rightarrow\}$

4 命题推理

4.1 重言蕴含

对于两个公式P, Q，在任何解释下P为真的时候Q也为真，那么P*重言蕴含*Q，记作$P \implies Q$。

$P \rightarrow Q$与$P \implies Q$的差异：$P \rightarrow Q$是合式公式而$P \implies Q$不是合式公式；$P \rightarrow Q$表示"P真则Q真"与"P假时Q可真可假"，而$P \implies Q$仅表示"P真则Q真"。

4.2 推理规则

1. 前提引入：推理过程中随时引入前提。
2. 结论引用：推理过程中得到的中间结论可以作为后续推理的前提。
3. 代入：**重言式**的命题变项可以进行代入（必须所有变项全部代入）。
4. 置换：命题公式中的任何部分公式可以用与之等值的命题公式置换。
5. 分离：已知$A \rightarrow B$和A，那么有命题公式B。
6. 条件证明规则：$A_1 \wedge A_2 \implies B$与$A_1 \implies A_2 \rightarrow B$等价。

常用的基本推理公式：

1. $P \wedge Q \implies P$
2. $P \implies P \vee Q$
3. $P \wedge (P \rightarrow Q) \implies Q$（**分离规则**）
4. $\neg Q \wedge (P \rightarrow Q) \implies \neg P$
5. $(P \rightarrow Q) \wedge (Q \rightarrow R) \implies P \rightarrow R$（**蕴含的传递**）

6. $(P \leftrightarrow Q) \wedge Q \leftrightarrow R \implies P \leftrightarrow R$（**等价的传递**）

4.3 归结推理

证明$A \to B$重言式等价于证明$A \wedge \neg B$是矛盾式。

1. 将$A \wedge \neg B$化为合取范式，建立子句集S，包含所有析取式。

   注意：子句集内只能出现析取！

2. 将S内子句双双归结，如$P \wedge R$和$\neg P \wedge Q$归结得到$R \wedge Q$，放回子句集S中。
3. 直到归结得到矛盾式$\square$。

5 量词

$p(x)$是包含变量x的语句，对于集合D中的每一个x，$p(x)$为命题，p是D中的命题函数，D是p的论域。

存在自由变量（没有被量词约束的变量）的语句不是命题。

5.1 全称量词

所有$x, p(x)$写作$\forall x, p(x)$。

证明$\forall x, p(x)$为假：只需$\exists x, p(x)$为假。

若D中元素有限可以一一列出为$x_1, x_2, \cdots, x_n$，则$\forall x, p(x)$与下式等价

$$p(x_1) \wedge p(x_2) \wedge \cdots \wedge p(x_n)$$

全称量词是合取$\wedge$的推广。

两个全称量词并列，可以交换位置。

5.2 存在量词

存在$x, p(x)$写作$\exists x, p(x)$。

若D中元素有限可以一一列出为$x_1, x_2, \cdots, x_n$，则$\exists x, p(x)$与下式等价

$$p(x_1) \vee p(x_2) \vee \cdots \vee p(x_n)$$

两个存在量词并列，可以交换位置。

存在量词是析取$\vee$的推广。

全称量词和存在量词并列，不能交换位置！

恰有量词$\exists !$表示只存在一个。

$$(\exists ! x)\alpha(x)=(\exists x)(\alpha(x)\wedge(\forall y)(y\neq x\rightarrow\neg\alpha(y)))$$

5.3 广义De Morgan律

$p(x)$为命题函数，则下列两组式子有相同的真值

1. $\neg(\forall x, p(x))$与$\exists x, \neg p(x)$
2. $\neg(\exists x, p(x))$与$\forall x, \neg p(x)$

5.4 量词分配等值式

5.4.1 对$\wedge$和$\vee$的分配

$$\begin{aligned}
(\forall x)(P(x)\wedge q)&=(\forall x)P(x)\wedge q\\
(\forall x)(P(x)\vee q)&=(\forall x)P(x)\vee q\\
(\exists x)(P(x)\wedge q)&=(\exists x)P(x)\wedge q\\
(\exists x)(P(x)\vee q)&=(\exists x)P(x)\vee q
\end{aligned}$$

只有一个含约束变量时，量词可以自由进出。

$$\begin{aligned}
(\forall x)(P(x)\wedge Q(x))&=(\forall x)P(x)\wedge(\forall x)Q(x)\\
(\exists x)(P(x)\vee Q(x))&=(\exists x)P(x)\vee(\exists x)Q(x)
\end{aligned}$$

存在两个约束变量时，全称量词对$\wedge$有分配律，存在量词对$\vee$有分配律。

$$\begin{aligned}
(\forall x)P(x)\vee(\forall x)Q(x)&\implies(\forall x)(P(x)\vee Q(x))\\
(\exists x)(P(x)\wedge Q(x))&\implies(\exists x)P(x)\wedge(\exists x)Q(x)
\end{aligned}$$

5.4.2 对$\rightarrow$的分配

$$\begin{aligned}
(\forall x)(P(x)\rightarrow q)&=(\exists x)P(x)\wedge q\\
(\exists x)(P(x)\rightarrow q)&=(\forall x)P(x)\wedge q\\
(\forall x)(p\rightarrow Q(x))&=(\forall x)p\rightarrow Q(x)\\
(\exists x)(p\rightarrow Q(x))&=(\exists x)p\rightarrow Q(x)
\end{aligned}$$

含一个约束变量时，如果约束变量在蕴含词前件，去括号后量词发生改变；如果约束变量在蕴含词后件，去括号后量词不发生改变。

$$\begin{aligned}(\forall x)(P(x) \to q) &= (\forall x)(\neg P(x) \vee q) \\ &= (\forall x)\neg P(x) \vee q \\ &= \neg(\forall x)\neg P(x) \vee q \\ &= (\exists x)P(x) \vee q\end{aligned}$$

5.5 变元易名的分配律

$$(\forall x)(\forall y)(P(x) \vee Q(y)) = (\forall x)P(x) \vee (\forall x)Q(x)$$
$$(\exists x)(\exists y)(P(x) \wedge Q(y)) = (\exists x)P(x) \wedge (\exists x)Q(x)$$

6 前束范式

前束范式：A中的一切量词都在公式的最左边（不含否定）且辖域都延伸到公式的末端。其中$Q_1, \cdots, Q_n$都是量词，M中不含有量词。

$$(Q_1 x_1) \cdots (Q_n x_n) M(x_1, \cdots, x_n)$$

6.1 Skolem标准形

此处只解释保留全称量词的Skolem标准形。

先将公式化为前束范式，然后对于存在量词管辖的变量以多元函数代替，多元函数的自变量为存在量词之前出现的全称量词管辖的变量，消去存在量词。

如将$(\exists x)(\forall y)(\forall z)(\exists u)(\forall v)(\exists w)P(x, y, z, u, v, w)$化成Skolem标准形：

$$\begin{aligned}&(\exists x)(\forall y)(\forall z)(\exists u)(\forall v)(\exists w)P(x, y, z, u, v, w) \\ &\quad = (\forall y)(\forall z)(\exists u)(\forall v)(\exists w)P(a, y, z, u, v, w) \\ &\quad = (\forall y)(\forall z)(\forall v)(\exists w)P(a, y, z, f(y, z), v, w) \\ &\quad = (\forall y)(\forall z)(\forall v)P(a, y, z, f(y, z), v, g(y, z, v))\end{aligned}$$

7 谓词推理

7.1 基本推理公式

1. $(\forall x)P(x) \vee (\forall x)Q(x) \implies (\forall x)(P(x) \vee Q(x))$
2. $(\exists x)(P(x) \wedge Q(x)) \implies (\exists x)P(x) \wedge (\exists x)Q(x)$
3. $(\forall x)(P(x) \to Q(x)) \implies (\forall x)P(x) \to (\forall x)Q(x)$
4. $(\forall x)(P(x) \to Q(x)) \implies (\exists x)P(x) \to (\exists x)Q(x)$

5. $(\forall x)(P(x) \leftrightarrow Q(x)) \implies (\forall x)P(x) \leftrightarrow (\forall x)Q(x)$
6. $(\forall x)(P(x) \leftrightarrow Q(x)) \implies (\exists x)P(x) \leftrightarrow (\exists x)Q(x)$
7. $(\forall x)(P(x) \to Q(x)) \wedge P(a) \implies Q(a)$（分离）
8. $(\forall x)(\forall y)P(x,y) \implies (\exists x)(\forall y)P(x,y)$
9. $(\exists x)(\forall y)P(x,y) \implies (\forall y)(\exists x)P(x,y)$

7.2 推理规则

7.2.1 $\forall$消去

$$(\forall x)P(x) \implies P(y)$$

其中y为论域中一个个体，且不能在$P(x)$的约束中出现。

7.2.2 $\forall$引入

$$P(y) \implies (\forall x)P(x)$$

y是论域中任何个体，且y不能自由出现在任何**假设**中。

7.2.3 $\exists$消去

$$(\exists x)P(x) \implies P(c)$$

c为论域中一个体常项。$(\exists x)P(x)$中不能有自由变元，$P(x)$中不含有c。得到的$P(c)$是一个**假设**。

7.2.4 $\exists$引入

$$P(c) \implies (\exists x)P(x)$$

c是论域中一个体常项，x不能出现在$P(c)$中。

集合论

1 集合

*集合*是一些对象的整体（**不考虑出现次数及出现次序**），可用枚举法描述也可以列出其元素性质描述。

记集合X为有限集合，则$|X|$即为集合X中元素的个数。没有元素的集合为空集$\varnothing$，$\varnothing = \{x \mid x \neq x\}$。

1.1 集合的关系

外延公理：若两个集合X和Y具有相同的元素，则两个集合相等，即$X = Y$。

若两个集合X和Y，X中的所有元素都是Y的元素，那么X为Y的*子集*，即$X \subseteq Y$当且仅当$\forall x(x \in X \rightarrow x \in Y)$。**空集是任何集合的子集**。

空集是唯一的：假设有两个空集$\varnothing, \varnothing'$，由于空集是任何集合的子集，于是$\varnothing \subseteq \varnothing', \varnothing' \subseteq \varnothing$，可以得出$\varnothing = \varnothing'$。

若两个集合X和Y，$X \neq Y, X \subseteq Y$，那么集合X是集合Y的*真子集*。

1.2 集合的运算

1.2.1 基本运算

集合的*并集* $X \cup Y = \{\, x \mid x \in X \vee x \in Y \,\}$
集合的*交集* $X \cap Y = \{\, x \mid x \in X \wedge x \in Y \,\}$
集合的*差集* $X - Y = \{\, x \mid x \in X \vee x \notin Y \,\}$
集合的*补集* 记全集为U，集合X是U的一个子集，则集合$\bar{X} = U - X$是集合X的补集。
集合的*对称差* $X \oplus Y = (X - Y) \cup (Y - X)$（类似于异或）

结合律：$(A \cup B) \cup C = A \cup (B \cup C) \quad (A \cap B) \cap C = A \cap (B \cap C)$
交换律：$A \cup B = B \cup A \quad A \cap B = B \cap A$
分配律：$A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \quad A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
同一律：$A \cup \varnothing = A \quad A \cap U = A$
互补律：$A \cup \bar{A} = U \quad A \cap \bar{A} = \varnothing$

吸收律: $A \cup (A \cap B) = A \quad A \cap (A \cup B) = A$
De Morgan律: $\overline{A \cup B} = \bar{A} \cap \bar{B} \quad \overline{A \cap B} = \bar{A} \cup \bar{B}$

1.2.2 幂集

集合X的所有子集的集合是集合X的*幂集*，记作$P(X)$，n个元素的集合的幂集有2^n个元素。

对于空集$\varnothing$，其幂集为$\{\varnothing\}$。

对任意集合A，$\varnothing \subseteq A, A \subseteq A$，于是$\varnothing \in P(A), A \in P(A)$.

幂集的性质：

1. $A \subseteq B \iff P(A) \subseteq P(B)$
2. $A = B \iff P(A) = P(B)$
3. $P(A) \cap P(B) = P(A \cap B)$
4. $P(A) \cup P(B) \subseteq P(A \cup B)$
5. $P(A - B) \subseteq P(A) - P(B) + \{\varnothing\}$
6. $P(A) \in P(B) \implies A \in B$（**逆定理不成立！**）

> **幂集相关性质的证明**
>
> 性质1：
> 若$A \subseteq B$成立，$x \in P(A) \iff x \subseteq A \implies x \subseteq B \iff x \in P(B)$，于是$P(A) \subseteq P(B)$.
> 若$P(A) \subseteq P(B)$成立，
> $x \in A \iff \{x\} \subseteq A \iff \{x\} \in P(A) \implies \{x\} \in P(B) \iff x \in B$，于是有$A \subseteq B$.
>
> 性质3：
>
> $$\begin{aligned} & x \in P(A) \cap P(B) \iff x \in P(A) \wedge x \in P(B) \\ & \iff x \subseteq A \wedge x \subseteq B \\ & \iff (\forall y)(y \in x \to y \in A) \wedge (\forall y)(y \in x \to y \in B) \\ & \iff (\forall y)((y \in x \to y \in A) \wedge (y \in x \to y \in B)) \\ & \iff (\forall y)(y \in x \to (y \in A \wedge y \in B)) \\ & \iff x \subseteq A \cap B \iff x \in P(A \cap B) \end{aligned}$$
>
> 性质4：

> $$\begin{aligned} x \in P(A) \cup P(B) &\iff x \in P(A) \vee x \in P(B) \\ &\iff x \subseteq A \vee x \subseteq B \\ &\iff (\forall y)(y \in x \to y \in A) \vee (\forall y)(y \in x \to y \in B) \\ &\implies (\forall y)((y \in x \to y \in A) \vee (y \in x \to y \in B)) \\ &\iff (\forall y)(y \in x \to (y \in A \vee y \in B)) \\ &\iff x \subseteq A \cup B \iff x \in P(A \cup B) \end{aligned}$$

1.3 划分

由集合X的*非空*子集的整体组成的S，如果X的每个元素都只属于S中的*某一个元素*，S就是X的一个**划分**。例如
$X = \{1, 2, 3, 4, 5, 6\}, S = \{\{1, 4, 5\}, \{2, 6\}, \{3\}\}$。

1.3.1 Descartes积

序偶：一个由两个元素组成的**有序**对(a, b)。
一种有序对的定义为$\langle x, y\rangle = \{\{x\}, \{x, y\}\}$

对于两个集合X, Y，它们的*Descartes积*定义为

$$X \times Y = \{\,(x, y) \mid x \in X \wedge y \in Y\,\}$$

Descartes积对$\cap, \cup$有分配律：

1. $A \times (B \cup C) = (A \times B) \cup (A \times C)$
2. $A \times (B \cap C) = (A \times B) \cap (A \times C)$
3. $(A \times B) \cup C = (A \cup C) \times (B \cup C)$
4. $(A \times B) \cap C = (A \cap C) \times (B \cap C)$

2 序列和串

*序列*是表示元素的**有序**表，若a是一个序列，一般a_n表示序列的第n项。

子序列：$\{s_n\}(n = m, m+1, \cdots)$是一个序列，$n_1, n_2, \cdots$是一个值在$m, m+1, \cdots$的**增序列**，则序列$\{s_{n_k}\}$是$\{s_n\}$的一个子序列。

串：由集合X中元素组成的**有限**序列为串，没有元素的串为空串λ。
X^*是集合X上所有串的集合。若α是一个串，那么$|\alpha|$是该串的长度。

3 有限集合的基数

常见有限集合的基数:

$|P(A)| = 2^{|A|}$
$|A \times B| = |A| \cdot |B|$
$|A \cup B| = |A| + |B| - |A \cap B| \leq |A| + |B|$
$|A \cap B| \leq \min\{|A|, |B|\}$
$|A - B| \geq |A| - |B|$
$|A \oplus B| = |A| + |B| - 2|A \cap B|$

容斥原理

$$\left|\bigcup_{i=1}^{n} A_i\right| = \sum_{1\leq i\leq n} |A_i| - \sum_{1\leq i<j\leq n} |A_i \cap A_j| + \sum_{1\leq i<j<k\leq n} |A_i \cap A_j \cap A_k| + \cdots$$
$$+(-1)^{n-1}|A_1 \cap A_2 \cap \cdots \cap A_n|$$

4 关系

集合X到集合Y的*关系*R是Descartes积$X \times Y$的一个子集，若$(x, y) \in R$，记作xRy。

自反关系：集合X上的关系R，$\forall x \in X$都有$(x, x) \in R$，那么R是自反的（仅考虑元素自身与自身之间的关系）。

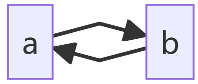
对称：集合X上的关系R，$\forall x, y \in X$，若$(x, y) \in R$则有$(y, x) \in R$，那么R是对称的。

反对称：集合X上的关系R，$\forall x, y \in X$，若$(x, y) \in R$且$x \neq y$，则一定有$(y, x) \notin R$，那么R是反对称的。

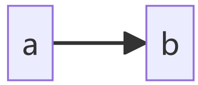
传递：集合X上的关系R，$\forall x, y, z \in X$，若$(x, y \in R)$且$(y, z) \in R$，一定有$(x, z) \in R$，那么关系R是传递的。

Example：关系$R = \{\,(a, a), (b, b), (c, c)\,\}$，显然$R$满足自反关系和对称关系，$R$是自反关系且对称的，关系$R$中没有两个不同元素存在关系，故$R$也是反对称关系，因而关系$R$既是对称关系也是反对称关系。

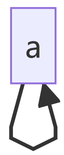
可以使用有向图来表示关系。下图表示对称关系，即a和b及b和a之间均存在关系。



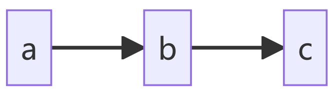
反对称关系可以表示为下图，表示仅存在a与b之间的关系，不存在b和a之间的关系。



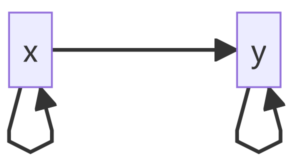
自反关系可以表示为下图，表示a与a自身存在关系。



传递关系可以表示为下图。



Example：



图中，x, y自身均存在自反关系；因为存在x到y的关系，不存在y到x的关系，所以x与y之间存在反对称关系；又因为存在x到y的关系，也存在y到y的关系（自反关系），因此x与y之间存在传递关系。

自反关系：$I_A = \{\langle x, x\rangle \mid x \in A\}$
全关系：$E_A = \{\langle x, y\rangle \mid x \in A \wedge y \in A\}$

偏序（partial order）：集合X上的关系R，如果是**自反**的，**反对称**的，**传递**的，则为偏序关系。

逆关系：R为集合X到集合Y的关系，其逆关系R^{-1}定义为

$$R^{-1} = \{ (y, x) \mid (x, y) \in R \}$$

复合：R_1为X到Y的关系，R_2为Y到Z的关系，R_1和R_2关系的复合记作$R_2 \circ R_1$，定义为

$$R_2 \circ R_1 = \{ (x, z) \mid \exists y \, (x, y) \in R_1 \wedge (y, z) \in R_2 \}$$

复合关系的性质：

1. $R_1 \circ (R_2 \cup R_3) = (R_1 \circ R_2) \cup (R_1 \circ R_3)$
2. $R_1 \circ (R_2 \cap R_3) \subseteq (R_1 \circ R_2) \cap (R_1 \circ R_3)$
3. $(R_1 \cup R_2) \circ R_3 = (R_1 \circ R_3) \cup (R_2 \circ R_3)$
4. $(R_1 \cap R_2) \circ R_3 \subseteq (R_1 \circ R_3) \cap (R_2 \circ R_3)$

等价关系：**自反**的、**对称**的、**传递**的关系。

等价类：R是集合X上的一个等价关系，定义等价类

$$[a] = \{ x \in X \mid xRa \}$$

此时，$S = \{ [a] | a \in x \}$是X的一个划分。

4.1 用矩阵表示关系

用0-1矩阵表示集合$A = \{ a_1, a_2, \cdots, a_n \}$和$B = \{ b_1, b_2, \cdots, b_n \}$之间的关系，以矩阵$M_R = [m_{ij}]$表示

$$m_{ij} = \begin{cases} 1 & , (a_i, b_j) \in R \\ 0 & , (a_i, b_j) \notin R \end{cases}$$

对于在集合A上的自反关系R，$\forall a_i \in A, (a_i, a_i) \in R$，于是其关系矩阵$M_R$的主对角线元素均为1，即

$$M_R = \begin{bmatrix} 1 & & & & \\ & 1 & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1 \end{bmatrix}$$

对于集合A上的对称关系R，对$\forall a_i, a_j \in A$，如果$(a_i, a_j) \in R$也有$(a_j, a_i) \in A$，于是有$m_{ij} = m_{ji} = 1$，其关系矩阵M_R为一个对称矩阵。

对于关系的复合，其矩阵为

$$M_{S\circ R} = M_R M_S$$