

# 问题求解 (一) 期末试卷

魏恒峰

hfwei@nju.edu.cn

2018 年 03 月 05 日



一分也是爱



试卷批改基本原则

## 1. “算一算” (Let us Calculate!)

(1) 某公司要从赵、钱、孙、李、吴 5 名员工中选派某些人出国考察。由于某些不可描述的原因, 选派要求如下:

- (1) 若赵去, 钱也去;
- (2) 李、吴两人中必有一人去;
- (3) 钱、孙两人中去且仅去一人;
- (4) 孙、李两人同去或同不去;
- (5) 若吴去, 则赵、钱也去;
- (6) 只有孙去, 赵才会去。

请使用形式化推理的方法帮该公司判断应选哪些人出国考察。

## 1. “算一算” (Let us Calculate!)

(1) 某公司要从赵、钱、孙、李、吴 5 名员工中选派某些人出国考察。由于某些不可描述的原因, 选派要求如下:

- (1) 若赵去, 钱也去;
- (2) 李、吴两人中必有一人去;
- (3) 钱、孙两人中去且仅去一人;
- (4) 孙、李两人同去或同不去;
- (5) 若吴去, 则赵、钱也去;
- (6) 只有孙去, 赵才会去。

请使用形式化推理的方法帮该公司判断应选哪些人出国考察。

$Z, Q, S, L, W$  vs.  $P, Q, R, S, T$

## 1. “算一算” (Let us Calculate!)

(1) 某公司要从赵、钱、孙、李、吴 5 名员工中选派某些人出国考察。由于某些不可描述的原因, 选派要求如下:

- |                   |  |
|-------------------|--|
| (1) 若赵去, 钱也去;     | (1) $Z \rightarrow Q$ ;                          |
| (2) 李、吴两人中必有一人去;  | (2) $L \vee W$ ;                                 |
| (3) 钱、孙两人中去且仅去一人; | (3) $(Q \wedge \neg S) \vee (S \wedge \neg Q)$ ; |
| (4) 孙、李两人同去或同不去;  | (4) $(S \wedge L) \vee (\neg S \wedge \neg L)$ ; |
| (5) 若吴去, 则赵、钱也去;  | (5) $W \rightarrow Z \wedge Q$ ;                 |
| (6) 只有孙去, 赵才会去。   | (6) $Z \rightarrow S$ 。                          |

请使用形式化推理的方法帮该公司判断应选哪些人出国考察。

$Z, Q, S, L, W$  vs.  $P, Q, R, S, T$

$$(1) \wedge (2) \wedge (3) \wedge (4) \wedge (5) \wedge (6)$$

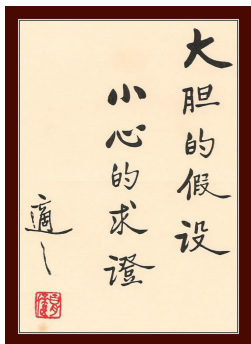
$$= \dots$$

$$= \text{ONE PAGE HERE } \dots$$

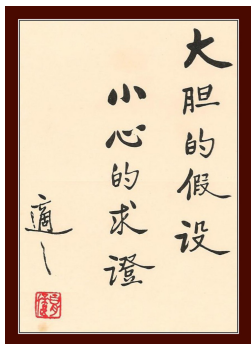
$$= \neg Z \wedge \neg Q \wedge S \wedge L \wedge \neg W$$

$$\begin{aligned} & (1) \wedge (2) \wedge (3) \wedge (4) \wedge (5) \wedge (6) \\ & = \dots \\ & = \text{ONE PAGE HERE} \dots \\ & = \neg Z \wedge \neg Q \wedge S \wedge L \wedge \neg W \end{aligned}$$









## 1. “算一算” (Let us Calculate!)

(2) 给定如下“前提”，请判断“结论”是否有效，并说明理由。

前提如下：

- (1) 每个人或者喜欢美剧，或者喜欢韩剧（可以同时喜欢二者）；
- (2) 任何人如果他喜欢抗日神剧，他就不喜欢美剧；
- (3) 有的人不喜欢韩剧。

结论：有的人不喜欢抗日神剧。

## 1. “算一算” (Let us Calculate!)

(2) 给定如下“前提”，请判断“结论”是否有效，并说明理由。

前提如下：

- (1) 每个人或者喜欢美剧，或者喜欢韩剧（可以同时喜欢二者）；
- (2) 任何人如果他喜欢抗日神剧，他就不喜欢美剧；
- (3) 有的人不喜欢韩剧。

结论：有的人不喜欢抗日神剧。

$x$ : Human

$A(x), \quad K(x), \quad J(x)$

# 1. “算一算” (Let us Calculate!)

(2) 给定如下“前提”，请判断“结论”是否有效，并说明理由。  
前提如下：

(1) 每个人或者喜欢美剧，或者喜欢韩剧（可以同时喜欢二者）；  
 $\forall x : A(x) \vee K(x)$

(2) 任何人如果他喜欢抗日神剧，他就不喜欢美剧；  
 $\forall x : J(x) \rightarrow \neg A(x)$

(3) 有的人不喜欢韩剧。  
 $\exists x : \neg K(x)$

结论：有的人不喜欢抗日神剧。  $\exists x : \neg J(x)$

$x$ : Human

$A(x), \quad K(x), \quad J(x)$

# 1. “算一算” (Let us Calculate!)

(2) 给定如下“前提”，请判断“结论”是否有效，并说明理由。  
前提如下：

(1) 每个人或者喜欢美剧，或者喜欢韩剧（可以同时喜欢二者）；  
 $\forall x : A(x) \vee K(x)$

(2) 任何人如果他喜欢抗日神剧，他就不喜欢美剧；  
 $\forall x : J(x) \rightarrow \neg A(x)$

(3) 有的人不喜欢韩剧。  
 $\exists x : \neg K(x)$

结论：有的人不喜欢抗日神剧。  $\exists x : \neg J(x)$

$x$ : Human       $Q : H(x)?$

$A(x), \quad K(x), \quad J(x)$

$$A, \quad K, \quad J$$

$$\forall x : A \vee K$$

$$\forall x : J \rightarrow \neg A$$

$$\exists x : \neg K$$

$$\exists x : \neg J$$

## 2. 常用证明方法

证明: 从  $\{1, 2, 3, \dots, 3n\}$  ( $n \in \mathbb{Z}^+$ ) 中任选  $n+1$  个数, 则总存在两个数, 它们的差不超过 2。

## 2. 常用证明方法

证明: 从  $\{1, 2, 3, \dots, 3n\}$  ( $n \in \mathbb{Z}^+$ ) 中任选  $n + 1$  个数, 则总存在两个数, 它们的差不超过 2。

Proof by the pigeonhole principle:



## 2. 常用证明方法

证明: 从  $\{1, 2, 3, \dots, 3n\}$  ( $n \in \mathbb{Z}^+$ ) 中任选  $n+1$  个数, 则总存在两个数, 它们的差不超过 2。

Proof by the pigeonhole principle:

$$\{1, 2, 3\}, \quad \{4, 5, 6\}, \quad \dots, \quad \{3n-2, 3n-1, 3n\}$$



## 2. 常用证明方法

证明: 从  $\{1, 2, 3, \dots, 3n\}$  ( $n \in \mathbb{Z}^+$ ) 中任选  $n+1$  个数, 则总存在两个数, 它们的差不超过 2。

Proof by the pigeonhole principle:

$$\{1, 2, 3\}, \quad \{4, 5, 6\}, \quad \dots, \quad \{3n-2, 3n-1, 3n\}$$



Proof by contradiction:

## 2. 常用证明方法

证明: 从  $\{1, 2, 3, \dots, 3n\}$  ( $n \in \mathbb{Z}^+$ ) 中任选  $n+1$  个数, 则总存在两个数, 它们的差不超过 2。

Proof by the pigeonhole principle:

$$\{1, 2, 3\}, \quad \{4, 5, 6\}, \quad \dots, \quad \{3n-2, 3n-1, 3n\}$$



Proof by contradiction:

$$1, 4, 7, \dots, 3n+1$$



## 常用证明方法

令  $S \subseteq \{x \mid 1 \leq x \leq 50, x \in \mathbb{N}\}$  且  $|S| = 10$ 。

证明: 存在两个大小均为 4 的不同集合  $A, B \subseteq S$  ( $A, B$  可相交), 它们的元素之和相等。

## 常用证明方法

令  $S \subseteq \{x \mid 1 \leq x \leq 50, x \in \mathbb{N}\}$  且  $|S| = 10$ 。

证明: 存在两个大小均为 4 的不同集合  $A, B \subseteq S$  ( $A, B$  可相交), 它们的元素之和相等。

Proof by the pigeonhole principle:

## 常用证明方法

令  $S \subseteq \{x \mid 1 \leq x \leq 50, x \in \mathbb{N}\}$  且  $|S| = 10$ 。

证明: 存在两个大小均为 4 的不同集合  $A, B \subseteq S$  ( $A, B$  可相交), 它们的元素之和相等。

Proof by the pigeonhole principle:

$$\binom{10}{4} = 210$$

VS.

$$\left| \{1 + 2 + 3 + 4 = 10 \leq x \leq 47 + 48 + 49 + 50 = 194\} \right|$$



### 3. 集合的势 (Cardinality)

$A$  是由所有半径为有理数、圆心在  $x$  轴 (实数轴) 上的圆组成的集合。  
请问  $A$  的势是什么, 并给出证明。

### 3. 集合的势 (Cardinality)

$A$  是由所有半径为有理数、圆心在  $x$  轴 (实数轴) 上的圆组成的集合。  
请问  $A$  的势是什么, 并给出证明。

$$|\mathbb{R}| \leq |\mathbb{Q} \times \mathbb{R}| \leq |\mathbb{R} \times \mathbb{R}| = |\mathbb{R}|$$



## Theorem (Cantor-(Dedekind)-Schröder–Bernstein (1887))

$$|X| \leq |Y| \wedge |Y| \leq |X| \implies |X| = |Y|$$

Definition ( $|A| \leq |B|$ )

$|A| \leq |B|$  if there exists an *one-to-one* function  $f$  from  $A$  into  $B$ .

Theorem (Cantor-(Dedekind)-Schröder-Bernstein (1887))

$$|X| \leq |Y| \wedge |Y| \leq |X| \implies |X| = |Y|$$

Definition ( $|A| \leq |B|$ )

$|A| \leq |B|$  if there exists an *one-to-one* function  $f$  from  $A$  into  $B$ .

*Q : Is " $\leq$ " a partial order?*

Theorem (Cantor-(Dedekind)-Schröder-Bernstein (1887))

$$|X| \leq |Y| \wedge |Y| \leq |X| \implies |X| = |Y|$$

Definition ( $|A| \leq |B|$ )

$|A| \leq |B|$  if there exists an *one-to-one* function  $f$  from  $A$  into  $B$ .

*$Q : Is \leq a partial order?$*

Theorem (Cantor-(Dedekind)-Schröder-Bernstein (1887))

$$|X| \leq |Y| \wedge |Y| \leq |X| \implies |X| = |Y|$$

$$\exists f : A \xrightarrow{1-1} B \wedge g : B \xrightarrow{1-1} A \implies \exists h : A \xleftrightarrow[onto]{1-1} B$$

By Julius König (1906).

$$A \uplus B$$

By Julius König (1906).

$$A \uplus B$$

$$a \in A : \cdots \rightarrow f^{-1}(g^{-1}(a) \rightarrow g^{-1}(a) \rightarrow \textcolor{red}{a} \rightarrow f(a) \rightarrow g(f(a)) \rightarrow \cdots$$

By Julius König (1906).

$$A \uplus B$$

$$a \in A : \cdots \rightarrow f^{-1}(g^{-1}(a) \rightarrow g^{-1}(a) \rightarrow \textcolor{red}{a} \rightarrow f(a) \rightarrow g(f(a)) \rightarrow \cdots$$

- (i)  $\cdots \rightsquigarrow \cdots$
- (ii)  $a \in A \rightsquigarrow \cdots$
- (iii)  $b \in B \rightsquigarrow \cdots$
- (iv)  $\cdots \rightsquigarrow a \in A$
- (v)  $\cdots \rightsquigarrow b \in B$

By Julius König (1906).

$$A \uplus B$$

$$a \in A : \cdots \rightarrow f^{-1}(g^{-1}(a) \rightarrow g^{-1}(a) \rightarrow \textcolor{red}{a} \rightarrow f(a) \rightarrow g(f(a)) \rightarrow \cdots$$

- (i)  $\cdots \rightsquigarrow \cdots$
- (ii)  $a \in A \rightsquigarrow \cdots$
- (iii)  $b \in B \rightsquigarrow \cdots$
- (iv)  $\cdots \rightsquigarrow a \in A$
- (v)  $\cdots \rightsquigarrow b \in B$

Partition of  $A \uplus B$





#### 4. 关系与序 (Order)

一个自反 (reflexive) 且传递 (transitive) 的二元关系  $R \subseteq X \times X$  称为  $X$  上的拟序 (preorder/quasiorder)。

令  $\leq \subseteq X \times X$  为拟序, 请证明:

(1) 如果定义  $X$  上的关系  $\sim$  为

$$x \sim y \triangleq x \leq y \wedge y \leq x,$$

则  $\sim$  是  $X$  上的等价关系 (equivalence relation)。

#### 4. 关系与序 (Order)

一个自反 (reflexive) 且传递 (transitive) 的二元关系  $R \subseteq X \times X$  称为  $X$  上的拟序 (preorder/quasiorder)。

令  $\leq \subseteq X \times X$  为拟序, 请证明:

(1) 如果定义  $X$  上的关系  $\sim$  为

$$x \sim y \triangleq x \leq y \wedge y \leq x,$$

则  $\sim$  是  $X$  上的等价关系 (equivalence relation)。

reflexive + symmetric + transitive

#### 4. 关系与序 (Order)

一个自反 (reflexive) 且传递 (transitive) 的二元关系  $R \subseteq X \times X$  称为  $X$  上的拟序 (preorder/quasiorder)。

令  $\leq \subseteq X \times X$  为拟序, 请证明:

(2) 如果定义商集 (quotient set)  $X/\sim$  上的关系  $\preceq$  为

$$[x]_{\sim} \preceq [y]_{\sim} \triangleq x \leq y,$$

则  $\preceq$  是偏序关系 (partial order)。

#### 4. 关系与序 (Order)

一个自反 (reflexive) 且传递 (transitive) 的二元关系  $R \subseteq X \times X$  称为  $X$  上的拟序 (preorder/quasiorder)。

令  $\leq \subseteq X \times X$  为拟序, 请证明:

(2) 如果定义商集 (quotient set)  $X/\sim$  上的关系  $\preceq$  为

$$[x]_{\sim} \preceq [y]_{\sim} \triangleq x \leq y,$$

则  $\preceq$  是偏序关系 (partial order)。

reflexive + antisymmetric + transitive

#### 4. 关系与序 (Order)

一个自反 (reflexive) 且传递 (transitive) 的二元关系  $R \subseteq X \times X$  称为  $X$  上的拟序 (preorder/quasiorder)。

令  $\leq \subseteq X \times X$  为拟序, 请证明:

(2) 如果定义商集 (quotient set)  $X/\sim$  上的关系  $\preceq$  为

$$[x]_{\sim} \preceq [y]_{\sim} \triangleq x \leq y,$$

则  $\preceq$  是偏序关系 (partial order)。

reflexive + antisymmetric + transitive

Well-definedness!!!

Well-definedness: Independence of Representative

Well-definedness: Independence of Representative

$$[x_1] = [x_2] \wedge [y_1] = [y_2]$$



$$[x_1] \preceq [y_1] \iff [x_2] \preceq [y_2]$$

$$[a]_n + [b]_n = [a + b]_n$$

$$[a]_n \times [b]_n = [ab]_n$$



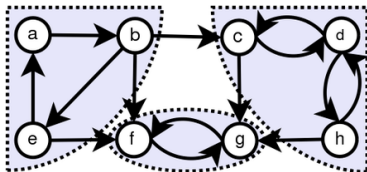
$$[a]_n + [b]_n = [a + b]_n$$

$$[a]_n \times [b]_n = [ab]_n$$

$$Q : [a]_n^{[b]_n} = [a^b]_n$$

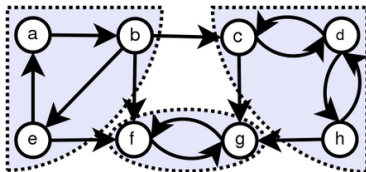


$\leq$ : ??? relationship in a directed graph



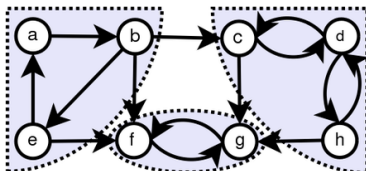


$\leq$ : Reachability relationship in a directed graph





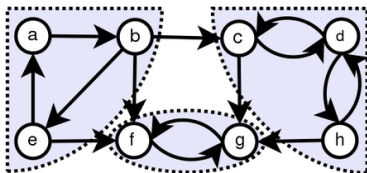
$\leq$ : Reachability relationship in a directed graph



$\sim, [x]_{\sim}$ :



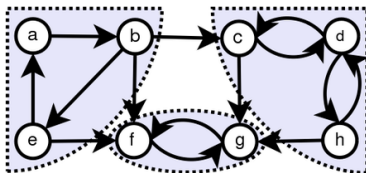
$\leq$ : Reachability relationship in a directed graph



$\sim, [x]_{\sim}$ : Strongly Connected Component (SCC)



$\leq$ : Reachability relationship in a directed graph

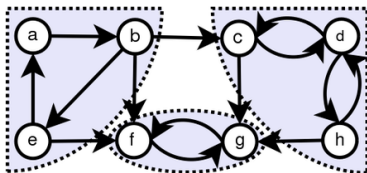


$\sim, [x]_{\sim}$ : Strongly Connected Component (SCC)

$\preceq$ :



$\leq$ : Reachability relationship in a directed graph



$\sim, [x]_{\sim}$ : Strongly Connected Component (SCC)

$\preceq$ : Reachability relationship in a condensed directed acyclic graph

## 5. 格 (Lattice)

假设  $(L, \leq)$  是格。

如果以下模律 (modular law) 成立, 则称  $L$  是模格 (modular lattice):

$$\forall x \in L : a \leq b \implies a \vee (x \wedge b) = (a \vee x) \wedge b.$$

以下均假设  $L$  是模格。



## 5. 格 (Lattice)

假设  $(L, \leq)$  是格。

如果以下模律 (modular law) 成立, 则称  $L$  是模格 (modular lattice):

$$\forall x \in L : a \leq b \implies a \vee (x \wedge b) = (a \vee x) \wedge b.$$

以下均假设  $L$  是模格。

$$\text{vs. } a \vee (x \wedge b) = (a \vee x) \wedge (a \vee b)$$

## 5. 格 (Lattice)

假设  $(L, \leq)$  是格。

如果以下模律 (modular law) 成立, 则称  $L$  是模格 (modular lattice):

$$\forall x \in L : a \leq b \implies a \vee (x \wedge b) = (a \vee x) \wedge b.$$

以下均假设  $L$  是模格。

$$\text{vs. } a \vee (x \wedge b) = (a \vee x) \wedge (a \vee b)$$

The stronger distributivity property is *not* available.

## 5. 格 (Lattice)

$$\forall x \in L : a \leq b \implies a \vee (x \wedge b) = (a \vee x) \wedge b.$$

(1) 请证明模律与以下条件等价:

$$\forall x \in L : a \leq b \implies a \vee (x \wedge b) \geq (a \vee x) \wedge b.$$

## 5. 格 (Lattice)

$$\forall x \in L : a \leq b \implies a \vee (x \wedge b) = (a \vee x) \wedge b.$$

(1) 请证明模律与以下条件等价:

$$\forall x \in L : a \leq b \implies a \vee (x \wedge b) \geq (a \vee x) \wedge b.$$

$$\forall x \in L : a \leq b$$

$$\implies$$

$$\left( (a \vee (x \wedge b) = (a \vee x) \wedge b) \right.$$

$$\iff$$

$$\left. (a \vee (x \wedge b) \geq (a \vee x) \wedge b) \right).$$

## 5. 格 (Lattice)

$$\forall x \in L : a \leq b \implies a \vee (x \wedge b) = (a \vee x) \wedge b.$$

(1) 请证明模律与以下条件等价:

$$\forall x \in L : a \leq b \implies a \vee (x \wedge b) \geq (a \vee x) \wedge b.$$

$$\begin{aligned} \forall x \in L : a \leq b & \qquad a \leq b \implies a \vee (x \wedge b) \leq (a \vee x) \wedge b \\ \implies & \\ \left( (a \vee (x \wedge b) = (a \vee x) \wedge b) \right. & \\ \iff & \\ \left. (a \vee (x \wedge b) \geq (a \vee x) \wedge b) \right) & \end{aligned}$$

## 5. 格 (Lattice)

$$\forall x \in L : a \leq b \implies a \vee (x \wedge b) = (a \vee x) \wedge b.$$

(1) 请证明模律与以下条件等价:

$$\forall x \in L : a \leq b \implies a \vee (x \wedge b) \geq (a \vee x) \wedge b.$$

$$\forall x \in L : a \leq b$$

$$\implies$$

$$\left( (a \vee (x \wedge b) = (a \vee x) \wedge b) \right.$$

$$\iff$$

$$\left. (a \vee (x \wedge b) \geq (a \vee x) \wedge b) \right).$$

$$a \leq b \implies a \vee (x \wedge b) \leq (a \vee x) \wedge b$$

$$a \leq a \vee x, a \leq b \implies a \leq (a \vee x) \wedge b$$

## 5. 格 (Lattice)

$$\forall x \in L : a \leq b \implies a \vee (x \wedge b) = (a \vee x) \wedge b.$$

(1) 请证明模律与以下条件等价:

$$\forall x \in L : a \leq b \implies a \vee (x \wedge b) \geq (a \vee x) \wedge b.$$

$$\forall x \in L : a \leq b$$

$$\implies$$

$$\left( (a \vee (x \wedge b) = (a \vee x) \wedge b) \right.$$

$$\iff$$

$$\left. (a \vee (x \wedge b) \geq (a \vee x) \wedge b) \right).$$

$$a \leq b \implies a \vee (x \wedge b) \leq (a \vee x) \wedge b$$

$$a \leq a \vee x, a \leq b \implies a \leq (a \vee x) \wedge b$$

$$x \wedge b \leq (a \vee x) \wedge b$$

## 5. 格 (Lattice)

$$\forall x \in L : a \leq b \implies a \vee (x \wedge b) = (a \vee x) \wedge b.$$

(2) 请证明:  $\forall a, b, c \in L$ ,

如果  $c \leq a$ ,  $a \wedge b = c \wedge b$ ,  $a \vee b = c \vee b$  成立, 则  $a = c$ .



## 5. 格 (Lattice)

$$\forall x \in L : a \leq b \implies a \vee (x \wedge b) = (a \vee x) \wedge b.$$

(2) 请证明:  $\forall a, b, c \in L$ ,

如果  $c \leq a$ ,  $a \wedge b = c \wedge b$ ,  $a \vee b = c \vee b$  成立, 则  $a = c$ .

$$[a \leftarrow c] \quad [b \leftarrow a]$$

$$\forall x \in L : c \leq a \implies c \vee (x \wedge a) = (c \vee x) \wedge a.$$

## 5. 格 (Lattice)

$$\forall x \in L : a \leq b \implies a \vee (x \wedge b) = (a \vee x) \wedge b.$$

(2) 请证明:  $\forall a, b, c \in L$ ,

如果  $c \leq a$ ,  $a \wedge b = c \wedge b$ ,  $a \vee b = c \vee b$  成立, 则  $a = c$ .

$$[a \leftarrow c] \quad [b \leftarrow a]$$

$$\forall x \in L : c \leq a \implies c \vee (x \wedge a) = (c \vee x) \wedge a.$$

$$[x := b]$$

$$c \leq a \implies c \vee (b \wedge a) = (c \vee b) \wedge a.$$

## 5. 格 (Lattice)

$$\forall x \in L : a \leq b \implies a \vee (x \wedge b) = (a \vee x) \wedge b.$$

(3) 给定任意元素  $s, t \in L$ , 且  $s \leq t$ , 构造集合 (称为区间 (interval)):

$$[s, t] \triangleq \{x \in L \mid s \leq x \leq t\}.$$

请证明  $([s, t], \leq)$  是  $L$  的子格 (sublattice)。

## 5. 格 (Lattice)

$$\forall x \in L : a \leq b \implies a \vee (x \wedge b) = (a \vee x) \wedge b.$$

(3) 给定任意元素  $s, t \in L$ , 且  $s \leq t$ , 构造集合 (称为区间 (interval)):

$$[s, t] \triangleq \{x \in L \mid s \leq x \leq t\}.$$

请证明  $([s, t], \leq)$  是  $L$  的子格 (sublattice)。



## 5. 格 (Lattice)

$$\forall x \in L : a \leq b \implies a \vee (x \wedge b) = (a \vee x) \wedge b.$$

(3) 给定任意元素  $s, t \in L$ , 且  $s \leq t$ , 构造集合 (称为区间 (interval)):

$$[s, t] \triangleq \{x \in L \mid s \leq x \leq t\}.$$

请证明  $([s, t], \leq)$  是  $L$  的子格 (sublattice)。



$$a, b \in [s, t] \implies a \vee b, a \wedge b \in [s, t]$$

## 5. 格 (Lattice)

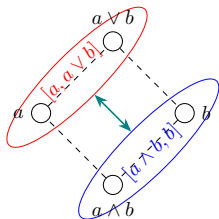
$$\forall x \in L : a \leq b \implies a \vee (x \wedge b) = (a \vee x) \wedge b.$$

(4) 给定任意元素  $a, b \in L$ , 定义函数

$$\varphi : [a \wedge b, b] \rightarrow [a, a \vee b] \quad \varphi(x) = x \vee a$$

$$\psi : [a, a \vee b] \rightarrow [a \wedge b, b] \quad \psi(y) = y \wedge b$$

请证明  $\varphi$  (类似地,  $\psi$ ) 是从  $[a \wedge b, b]$  到  $[a, a \vee b]$  的同构。



## Definition (Lattice Isomorphism)

$$(L, \vee_L, \wedge_L) \quad (M, \vee_M, \wedge_M)$$

A *lattice isomorphism* from  $L$  to  $M$  is a bijection

$$f : L \xrightarrow[\text{onto}]{1-1} M$$

such that  $\forall a, b \in L$ :

$$f(a \vee_L b) = f(a) \vee_M f(b)$$

$$f(a \wedge_L b) = f(a) \wedge_M f(b)$$

## Definition (Lattice Isomorphism)

$$(L, \vee_L, \wedge_L) \quad (M, \vee_M, \wedge_M)$$

A *lattice isomorphism* from  $L$  to  $M$  is a bijection

$$f : L \xleftrightarrow[\text{onto}]{1-1} M$$

such that  $\forall a, b \in L$ :

$$f(a \vee_L b) = f(a) \vee_M f(b)$$

$$f(a \wedge_L b) = f(a) \wedge_M f(b)$$

$f$  preserving  $\vee$  and  $\wedge$ .



$\varphi$  preserving  $\vee$  and  $\wedge$ .

$$\varphi : [a \wedge b, b] \rightarrow [a, a \vee b] \quad \varphi(x) = x \vee a$$

$\varphi$  preserving  $\vee$  and  $\wedge$ .

$$\varphi : [a \wedge b, b] \rightarrow [a, a \vee b] \quad \varphi(x) = x \vee a$$

$$\varphi(x_1 \wedge x_2) = \varphi(x_1) \wedge \varphi(x_2)$$

$\varphi$  preserving  $\vee$  and  $\wedge$ .

$$\varphi : [a \wedge b, b] \rightarrow [a, a \vee b] \quad \varphi(x) = x \vee a$$

$$\varphi(x_1 \wedge x_2) = \varphi(x_1) \wedge \varphi(x_2)$$

$$\varphi(x_1 \wedge x_2) = (x_1 \wedge x_2) \vee a$$

$$\begin{aligned} \varphi(x_1) \wedge \varphi(x_2) &= (x_1 \vee a) \wedge (x_2 \vee a) \\ &= (a \vee x_1) \wedge (x_2 \vee a) \\ &=_{\text{modular law}} a \vee (x_1 \wedge (x_2 \vee a)) \\ &= \dots \end{aligned}$$



$$\varphi : [a \wedge b, b] \rightarrow [a, a \vee b] \quad \varphi(x) = x \vee a$$

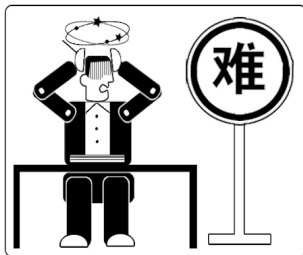
$$\psi : [a, a \vee b] \rightarrow [a \wedge b, b] \quad \psi(y) = y \wedge b$$

$\varphi$  is bijective.

$$\varphi : [a \wedge b, b] \rightarrow [a, a \vee b] \quad \varphi(x) = x \vee a$$

$$\psi : [a, a \vee b] \rightarrow [a \wedge b, b] \quad \psi(y) = y \wedge b$$

$\varphi$  is bijective.



Theorem (UD Theorem 15.8 (iii))

$$f : A \rightarrow B$$

$$\exists g : B \rightarrow A \left( g \circ f = i_A \wedge f \circ g = i_B \right)$$

$$\implies$$

$$f : A \rightarrow B \text{ is bijective} \wedge g = f^{-1}$$

$$\psi \circ \varphi = id_{[a, a \vee b]} \quad \varphi \circ \psi = id_{[a \wedge b, b]}$$



$$\psi \circ \varphi = id_{[a, a \vee b]} \quad \varphi \circ \psi = id_{[a \wedge b, b]}$$

$$(\psi \circ \varphi)(y) = \psi(\varphi(y)) = (y \wedge b) \vee a = a \vee (b \wedge y) = (a \vee b) \wedge y = y$$

$$\psi \circ \varphi = id_{[a, a \vee b]} \quad \varphi \circ \psi = id_{[a \wedge b, b]}$$

$$(\psi \circ \varphi)(y) = \psi(\varphi(y)) = (y \wedge b) \vee a = a \vee (b \wedge y) = (a \vee b) \wedge y = y$$

$$(\varphi \circ \psi)(x) = \varphi(\psi(x)) = (x \vee a) \wedge b = x \vee (b \wedge a) = x$$

Back to  $\varphi$  preserving  $\vee$  and  $\wedge$ .

Back to  $\varphi$  preserving  $\vee$  and  $\wedge$ .

$\psi$  preserving  $\wedge$ :

$$\psi(y_1 \wedge y_2) = y_1 \wedge y_2 \wedge b = (y_1 \wedge b) \wedge (y_2 \wedge b) = \psi(y_1) \wedge \psi(y_2)$$

Back to  $\varphi$  preserving  $\vee$  and  $\wedge$ .

$\psi$  preserving  $\wedge$ :

$$\psi(y_1 \wedge y_2) = y_1 \wedge y_2 \wedge b = (y_1 \wedge b) \wedge (y_2 \wedge b) = \psi(y_1) \wedge \psi(y_2)$$

$$\psi(\varphi(x_1) \wedge \varphi(x_2)) = \psi(\varphi(x_1)) \wedge \psi(\varphi(x_2)) = x_1 \wedge x_2$$

Back to  $\varphi$  preserving  $\vee$  and  $\wedge$ .

$\psi$  preserving  $\wedge$ :

$$\psi(y_1 \wedge y_2) = y_1 \wedge y_2 \wedge b = (y_1 \wedge b) \wedge (y_2 \wedge b) = \psi(y_1) \wedge \psi(y_2)$$

$$\psi(\varphi(x_1) \wedge \varphi(x_2)) = \psi(\varphi(x_1)) \wedge \psi(\varphi(x_2)) = x_1 \wedge x_2$$

$$\varphi(x_1 \wedge x_2) = \varphi(\psi(\varphi(x_1) \wedge \varphi(x_2))) = \varphi(x_1) \wedge \varphi(x_2)$$

## 6. 布尔代数 (Boolean Algebra)

给定某布尔表达式  $E = xy' + xyz' + x'yz'$ , 请证明:

(1)  $xz' + E = E$

(2)  $x + E \neq E$

## 6. 布尔代数 (Boolean Algebra)

给定某布尔表达式  $E = xy' + xyz' + x'yz'$ , 请证明:

(1)  $xz' + E = E$

(2)  $x + E \neq E$





## 6. 布尔代数 (Boolean Algebra)

给定某布尔表达式  $E = xy' + xyz' + x'yz'$ , 请证明:

(1)  $xz' + E = E$

(2)  $x + E \neq E$



$$E = xy'z + xy'z' + xyz' + x'yz'$$

## 6. 布尔代数 (Boolean Algebra)

给定某布尔表达式  $E = xy' + xyz' + x'yz'$ , 请证明:

(1)  $xz' + E = E$

(2)  $x + E \neq E$



$$E = xy'z + xy'z' + xyz' + x'yz'$$

$$xz' = x\textcolor{red}{y}z' + x\textcolor{red}{y}'z'$$

## 6. 布尔代数 (Boolean Algebra)

给定某布尔表达式  $E = xy' + xyz' + x'y z'$ , 请证明:

(1)  $xz' + E = E$

(2)  $x + E \neq E$



$$E = xy'z + xy'z' + xyz' + x'y z'$$

$$xz' = xyz' + xy'z'$$

$$x = xyz + xyz' + xy'z + xy'z'$$

## 7. 算法设计与正确性证明

在“掼蛋”游戏中, 5 张大小连续的扑克牌构成一个顺子 (如  $A\ 2\ 3\ 4\ 5$  和  $10\ J\ Q\ K\ A$  都是顺子; 不考虑花色)。

任给 13 张从小到大的牌 (允许不同花色重复, 如  $A\ 3\ 3\ 4\ 5\ 7\ 8\ 9\ 10\ J\ J\ Q\ K$ ):

- (1) 请设计算法, 找到所有的顺子。
- (2) 请使用“循环不变式” (loop invariants) 证明你设计的算法的正确性。
- (3) 数学归纳法的正确性也是需要证明的。请证明第一数学归纳法的正确性。(不允许使用第二数学归纳法证明。)

## 7. 算法设计与正确性证明

(1) 任给 13 张从小到大的牌, 请设计算法, 找到所有的顺子。

Preprocessing:

## 7. 算法设计与正确性证明

(1) 任给 13 张从小到大的牌, 请设计算法, 找到所有的顺子。

Preprocessing:

$A\ 3\ 3\ 4\ 5\ 7\ 8\ 9\ 10\ J\ J\ Q\ K$

## 7. 算法设计与正确性证明

(1) 任给 13 张从小到大的牌, 请设计算法, 找到所有的顺子。

Preprocessing:

$A\ 3\ 3\ 4\ 5\ 7\ 8\ 9\ 10\ J\ J\ Q\ K$

$A\ 3\ 4\ 5\ 7\ 8\ 9\ 10\ J\ Q\ K$

## 7. 算法设计与正确性证明

(1) 任给 13 张从小到大的牌, 请设计算法, 找到所有的顺子。

Preprocessing:

$A\ 3\ 3\ 4\ 5\ 7\ 8\ 9\ 10\ J\ J\ Q\ K$

$A\ 3\ 4\ 5\ 7\ 8\ 9\ 10\ J\ Q\ K$

$A\ 3\ 4\ 5\ 7\ 8\ 9\ 10\ J\ Q\ K\ A$



## “Sliding Window” Algorithm:

```
i ← 1 // starting index of the sliding window
cnt ← 1
while (i ≤ n - 4) // n: # of cards
    while (cnt ≠ 5)
        if (P[i + cnt] == P[i + cnt - 1] + 1)
            cnt++
        else // fail: skip cnt
            i ← i + cnt
            cnt ← 1
            break
    if (cnt == 5) // succeed: slid by one
        print P[i] ... P[i + cnt - 1]
        i++
        cnt ← 4 // only need to check the new card
```



## 7. 算法设计与正确性证明

(2) 请使用“循环不变式” (loop invariants) 证明你设计的算法的正确性。

## 7. 算法设计与正确性证明

(2) 请使用“循环不变式” (loop invariants) 证明你设计的算法的正确性。



## 7. 算法设计与正确性证明

(2) 请使用“循环不变式” (loop invariants) 证明你设计的算法的正确性。



`while ( $i \leq n - 4$ ) :`

## 7. 算法设计与正确性证明

(2) 请使用“循环不变式” (loop invariants) 证明你设计的算法的正确性。



**while** ( $i \leq n - 4$ ) : the **straight** starting at  $P[k]$  ( $k < i$ ) has been found

## 7. 算法设计与正确性证明

(2) 请使用“循环不变式” (loop invariants) 证明你设计的算法的正确性。



**while**  $(i \leq n - 4)$  : the **straight** starting at  $P[k]$  ( $k < i$ ) has been found

**OR** does not exist

## 7. 算法设计与正确性证明

- (3) 数学归纳法的正确性也是需要证明的。请证明第一数学归纳法的正确性。(不允许使用第二数学归纳法证明。)

## 7. 算法设计与正确性证明

- (3) 数学归纳法的正确性也是需要证明的。请证明第一数学归纳法的正确性。(不允许使用第二数学归纳法证明。)

Well-ordering Principle  $\implies$  Principle of Mathematical Induction



## Definition (Well-ordering Principle)

Every non-empty subset of  $\mathbb{N}$  contains a least element.

## Definition (Well-ordering Principle)

Every non-empty subset of  $\mathbb{N}$  contains a least element.

## Definition (Principle of Mathematical Induction)

$$\left[ P(1) \wedge \forall n \in \mathbb{N}^+ (P(n) \rightarrow P(n+1)) \right] \rightarrow \forall n \in \mathbb{N}^+ P(n).$$

## Definition (Well-ordering Principle)

Every non-empty subset of  $\mathbb{N}$  contains a least element.

## Definition (Principle of Mathematical Induction)

$$\left[ P(1) \wedge \forall n \in \mathbb{N}^+ (P(n) \rightarrow P(n+1)) \right] \rightarrow \forall n \in \mathbb{N}^+ P(n).$$

WOP  $\implies$  PMI.

By contradiction.

## Definition (Well-ordering Principle)

Every non-empty subset of  $\mathbb{N}$  contains a least element.

## Definition (Principle of Mathematical Induction)

$$\left[ P(1) \wedge \forall n \in \mathbb{N}^+ (P(n) \rightarrow P(n+1)) \right] \rightarrow \forall n \in \mathbb{N}^+ P(n).$$

WOP  $\implies$  PMI.

By contradiction.

$$Q = \{k \in \mathbb{N} \mid \neg P(k)\} \neq \emptyset$$

## Definition (Well-ordering Principle)

Every non-empty subset of  $\mathbb{N}$  contains a least element.

## Definition (Principle of Mathematical Induction)

$$\left[ P(1) \wedge \forall n \in \mathbb{N}^+ (P(n) \rightarrow P(n+1)) \right] \rightarrow \forall n \in \mathbb{N}^+ P(n).$$

WOP  $\implies$  PMI.

By contradiction.

$$Q = \{k \in \mathbb{N} \mid \neg P(k)\} \neq \emptyset$$

$$k = \min Q$$

## Definition (Well-ordering Principle)

Every non-empty subset of  $\mathbb{N}$  contains a least element.

## Definition (Principle of Mathematical Induction)

$$\left[ P(1) \wedge \forall n \in \mathbb{N}^+ (P(n) \rightarrow P(n+1)) \right] \rightarrow \forall n \in \mathbb{N}^+ P(n).$$

WOP  $\implies$  PMI.

By contradiction.

$$Q = \{k \in \mathbb{N} \mid \neg P(k)\} \neq \emptyset$$

$$k = \min Q$$

$$k \neq 1 \implies k > 1$$

## Definition (Well-ordering Principle)

Every non-empty subset of  $\mathbb{N}$  contains a least element.

## Definition (Principle of Mathematical Induction)

$$\left[ P(1) \wedge \forall n \in \mathbb{N}^+ (P(n) \rightarrow P(n+1)) \right] \rightarrow \forall n \in \mathbb{N}^+ P(n).$$

WOP  $\implies$  PMI.

By contradiction.

$$Q = \{k \in \mathbb{N} \mid \neg P(k)\} \neq \emptyset$$

$$k = \min Q$$

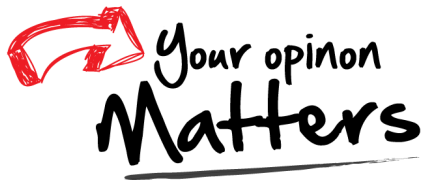
$$k \neq 1 \implies k > 1$$

$$k-1 \notin Q \implies P(k-1) \implies P(k)$$



Thank  
You!





Office 302

Mailbox: H016

hfwei@nju.edu.cn