# VE203 Lecture Note 1 (18 SUMMER)

## 1. Operations on sets

1. $\bigcup X=\{x \in A|(\exists y \in X)(x \in y)\}$ 是至少一个X的元素（集合）含有的元素
2. $\bigcap X=\{x \in A|(\forall y \in X)(x \in y)\}$ 是每个X的元素（集合）含有的元素

## 2. Relations

### 2 .1 Definition

1. dom $R=\{x|\exists y((x,y) \in R)\}$
2. ran $R=\{y|\exists x((x,y) \in R)\}$
3. Field: Ran $R$=ran$R \cup$ dom $R$

### 2.2 Attributes of Relations

1. reflexive $\forall a \in M((a,a) \in R)$
2. symmetric $\forall a,b \in M((a,b) \in R \Rightarrow (b,a) \in R)$
3. antisymmetric $\forall a,b \in M((a,b) \in R \wedge (b,a) \in R \Rightarrow a=b)$
4. asymmetric $\forall a,b \in M((a,b) \in R \Rightarrow (b,a) \notin R)$
5. transitive $\forall a,b,c \in M((a,b) \in R \wedge (b,c) \in R \Rightarrow (a,c) \in R)$

### 2.3 Equivalence Relations

#### 2.3.1 Definition

- reflexive, symmetric and transitive

#### 2.3.2 Equivalence class

1. $a \in M \Rightarrow [a]_R=\{b \in M|(a,b) \in R\}$
2. either $[a]_R=[b]_R$ or $[a]_R \cap [b]_R=\emptyset$
3. Suppose $c \in [a]_R \cap [b]_R$, $x \in [a]_R$ then $(x,a) \in R$ and $(c,a) \in R$, then $(a,x) \in R$ (symmetric) and $(c,x),(x,c) \in R$ (transitive), Also $(b,c),(c,b) \in R$, then $(x,b),(b,x) \in R$. Then $x \in [b]_R$ Hence $[a]_R \subseteq [b]_R$
4. 同理证明$[b]_R \subseteq [a]_R$，则$[a]_R=[b]_R$

## 3.Orders

### 3.1 Partial order ($\geq$)

#### 3.1.1 Definition

- reflexive, antisymmetric, transitive

#### 3.1.2 Partially ordered set (poset)

偏序集 $(M, R)$

## 3.2 Strictly partial order ($>$)

- asymmetric, transitive

## 3.3 Linear (total) order

- partial order
- $\forall x, y \in M((x, y) \in R \vee (y, x) \in R)$
- 就是每两个元素都要有relation($\geq$任意两个都可以比较)

## 3.4 Well order

- linear order
- $(\forall A \neq \emptyset \subseteq M)(\exists x \in A)(\forall y \in A)((y, x) \in R \Rightarrow y = x)$.
- 就是存在一个“最小”的x，只有x自己≤x

# 4. Lattices

格是一种特殊的poset

## 4.1 Definition

$(L, \preceq)$ a poset, $S \subseteq L$

- $x \in L$ is an upper bound on S $\Leftrightarrow (\forall y \in S)(y \preceq x)$
- $x \in L$ is an lower bound on S $\Leftrightarrow (\forall y \in S)(x \preceq y)$ x是在全集$L$里的
- $x \in L$ is a least upper bound on S $\Leftrightarrow (x \text{ is an u.b.}) \wedge (\forall y \text{ is an u.b.})(y \preceq x)$
- $x \in L$ is an greatest lower bound on S $\Leftrightarrow (x \text{ is a l.b.}) \wedge (\forall y \text{ is a l.b.})(y \preceq x)$

> $S = \{2, 3\} \subseteq (\mathbb{N}, |), 1 \text{ is g.l.b}, 6 \text{ is l.u.b}$

$(L, \preceq)$ a poset, $S \subseteq L$

- $(\forall x, y \in L)(\{x, y\} \text{ has l.u.b } x \vee y \text{ and g.l.b } x \wedge y)$

## 4.2 Example

1. $(\mathbb{N}, |)$, gcd(x,y) is g.l.b., lcm(x,y) is l.u.b.
2. Linearly ordered poset $(M, \preceq)$ is a lattice
3. If $A = \{1, 2, 3, 4\}$ and $R = \{(1, 1), (2, 2), (3, 3), (4, 4), (1, 2), (2, 4), (3, 4), (1, 4)\}$, then $(A, R)$ is not a lattice because $\{2, 3\}$ has no lower bound (l.u.b. is 4).
4. $(\mathcal{P}(A), \subseteq)$

## 4.3 Complete Lattices

$L$的任意子集都有l.u.b.和g.l.b.

- 非空有限格是complete lattices
- $(\mathbb{R}, \leq)$ 不是complete lattice

If $(L, \preceq)$ is complete lattice, max element is $\bigvee L$ If $(L, \preceq)$ is complete lattice, min element is $\bigwedge L$

> $(\mathbb{Z}^*, \leq^*)$ $(\mathbb{N}, |)$, $\bigvee L = 0$, $\bigwedge L = 1$

### 4.4 Chain Complete Posets

#### 4.4.1 Chain

$(L, \preceq)$ is partial order, $X \subseteq L$ is a linear order $\Rightarrow X$ is a chain

> 子序是个全序

$(L, \preceq)$ is a linear order $\Rightarrow \forall X \subseteq L$ is a chain

#### 4.4.2 Chain Complete

$(L, \preceq)$ is partial order, every chain $X$ has l.u.b.

> 有最小元素，否则空链的l.g.b.确定不下来

# 5. Functions

## 5.1 Definition

$f \subseteq A \times B, f : A \to B$

> $(\forall x \in A)(\forall y, z \in B)((x, y) \in f \wedge (x, z) \in f \Rightarrow y = z)$ 只有一个像

$f\text{''}\, C = \{y | \exists x(x \in C \wedge (x, y) \in f)\} = \{f(x) | x \in C\}$, 值域 $f \restriction C = \{(x, y) | (x, y) \in f \wedge x \in C\}$

## 5.2 Injective

### 5.2.1 Definition

$(\forall x, y \in A)(\forall z \in B)((x, z) \in f \wedge (y, z) \in f) \Rightarrow x = y$

## 5.3 Composing Functions

### 5.3.1 Defintion

$\mathrm{ran} f \subseteq \mathrm{dom} g$, $g \circ f = \{(x, y) | \exists z((x, z) \in f \wedge (z, y) \in g)\}$

> $\mathrm{ran} f \subseteq \mathrm{dom} g$, 那么$g \circ f$是一个函数（可用来证明函数）

## 5.4 Inverse

### 5.4.1 Definition

$f^{-1} = \{(x, y) \in B \times A | (y, x) \in f\}$

### 5.4.2 Identity function

$id_A = \{(x, y) \in A \times A | x = y\}$

## 5.4.3 Lemma

$f^{-1}$ is a function with $\mathrm{dom} f^{-1} = \mathrm{ran} f$ and $\mathrm{ran} f^{-1} = A$ iff $f$ is injective.

$f \circ f^{-1} = f^{-1} \circ f = id_A$

## 5.5 Surjective functions

$(\forall x \in B)(\exists y \in A)((y,x) \in f)$is surjective.

## 5.6 Bijection

Both injective and surjective.

### 5.6.1 Lemma

$f : A \to B$ and $g : B \to C$ are bijections, then $g \circ f$ is a bijection.

### 5.6.2 Definition

A and B has the same cardinality if there exists a bijection $f : A \to B$

> $|A| = |B|$ 无限集也可以对应相等cardinality

$|A| \leq |B|$ if there exists a injection $f : A \to B$

> $|A| = |\mathrm{ran} f|$, $\mathrm{ran} f \subseteq B$

### 5.6.3 Examples

$f((-1)^k n) = \begin{cases} 0 & ,n=0 \\ 2n+k & ,n \neq 0 \end{cases}$, $|\mathbb{Z}| = |\mathbb{N} \backslash \{1\}|$

### 5.6.4 Theorem

$|\mathbb{Z}| = |\mathbb{N}|$

# 6. Countable Sets

## 6.1 Definition

A is countable if $|A| \leq |\mathbb{N}|$. A is countably infinite if A is countable and A is infinite.

## 6.2 Infinite

$A \to A$ is an injection but not a surjection.

- Dedekind infinite

## 6.3 Cantor's Pairing Function

1. If B is countable and $A \subseteq B$ then A is countable.
2. $|\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$
3. $\pi(x,y) = \frac{1}{2}(x+y)(x+y+1)+y$
4. $\mathbb{Q} \to \mathbb{N} \times \mathbb{N}$ 互质整数相除 is an injection.
5. $|A| < |B|$ if there exists a bijection $f : A \to B$ and no bijection.

## 6.4 Cantor's Theorem

1. There's no injection $\mathcal{P}(A) \to A$.

> Contradiction:
>
> 1. $f^{-1}: \mathrm{ran} f \to \mathcal{P}(A)$ is a bijection 一一对应
> 2. $Z = \{x \in \mathrm{ran} f | x \notin f^{-1}(x)\} \subseteq A$ x不在$f^{-1}(x)$这个集合里的集合
> 3. $z = f(Z)$，如果$z \in f^{-1}(z) = Z$，那$z$就不应该在$Z$这个集合里；如果$z \notin Z$，那按照$Z$的定义，$z$应该被放进$Z$里去 $Z = \{\cdots, z, \cdots\} \to z$不成立

2. $|A| < |\mathcal{P}(A)|$

> $f = \{(x, \{x\}) \in A \times \mathcal{P}(A) | x \in A\}$ is an injection + $\mathcal{P}(A) \not\preceq A$

3. $|\mathbb{N}| < |\mathcal{P}(\mathbb{N})| < |\mathcal{P}(\mathcal{P}(\mathbb{N}))| < \cdots$
4. $\mathcal{P}(V) \subseteq V$ -> $f: \mathcal{P}(V) \to V$, $f(x) = x$ is a injection -> $|\mathcal{P}(V)| \le |V|$ -> Contradictive to Cantor's

-> No largest set -> Inconsistency in Naive Set Theory -> (ZFC)

# 7. Morphisms and Isomorphisms

(A,R) and (B,S) and bijection $f: A \to B$, $\forall x, y \in A$, $(x, y) \in R \Leftrightarrow (f(x), f(y)) \in S$

(A,R) and (B,S) have the same structure. f是 $\mathcal{R}$ 和 $\mathcal{S}$的domain之间的bijection

## 7.1 Isomorphism 同构

f is an isomorphism

> 1. $x|y$, $ax|ay$

2. $n \le m, n-1 \le m-1$

## 7.2 Homomorphism 同态

f is not necessarily a bijection

# 8. Order-preserving Functions 保序函数

$(P_1, \preceq_1), (P_2, \preceq_2)$ are partial orders, $\forall x, y \in P_1$, $(x \preceq_1 y) \Rightarrow (f(x) \preceq_2 f(y))$. $f: (P_1, \preceq_1) \to (P_2, \preceq_2)$.

# 9. Fixed points

$x \in A$, $f(x) = x$.

# 10. Tarski-Knaster Theorem

## 10.1 Definition

Let $(L, \preceq)$ be a complete lattice. $f: (L, \preceq) \to (L, \preceq)$ is an order-preserving function $\Rightarrow$ f has a fixed point.

## 10.2 Proof

> $X = \{x \in L | f(x) \preceq x\}$ and $a = \bigwedge X$

> 1. Claim I: if $x \in X$, then $f(x) \in X$. $f(x) \preceq x \Rightarrow f(f(x)) \preceq f(x)$. Then $f(x) \in X$.

> 2. Claim II: f(a) is a lower bound on X. $a \preceq x$, $f(a) \preceq f(x) \preceq x$. 既然$f(a)$是lower bound, a是g.l.b, 那么 $f(a) \preceq a$

- Q：a一定在X中吗？
- A: 在的 因为 $f(a) \preceq a$

> a在X中所以f(a)也在X中 所以$a \preceq f(x)$ 所以 $a = f(a)$，即不动点

### 10.3 Corollary

f has a least fixed point

## 11. SB Theorem

### 11.1 Definition

If exists injections $f : A \to B$ and $g : B \to A$, then exists a bijection $h : A \to B$

### 11.2 Proof

We know that $(\mathcal{P}(A), \subseteq)$ is a complete lattice.

Define $F : \mathcal{P}(A) \to \mathcal{P}(A)$, $F(X) = A \backslash g\text{ " }(B \backslash f\text{ " }X)$ Step 1. 证明F是O-P function

> Let $Y \subseteq Z \subseteq A$, then $f\text{ " }Y \subseteq f\text{ " }Z$ and $B \backslash f\text{ " }Z \subseteq B \backslash f\text{ " }Y$ and $g\text{ " }(B \backslash f\text{ " }Z) \subseteq g\text{ " }(B \backslash f\text{ " }Y)$ then $F(Y) \subseteq F(Z)$

Step 2. T-K Theorem，let $F(X) = X, X \subseteq A$

Step 3. Let $C = \mathbf{ran} g$. 理论上来说，这时候我们还认为C是A的子集 $g^{-1} : C \to B$ is an injection （实际上已经是bijection了

- $A \backslash X \subseteq C$ ?
- 因为 $A \backslash X = A \backslash F(X) = g\text{ " }(B \backslash f\text{ " }X)$，是通过$g$映射出来的，是ran$g$的一部分

$h = (f \restriction X) \cup (g^{-1} \restriction (A \backslash X))$

dom h=A （X并上A去掉X的部分） ran h=B （$f\text{ " }X \cup B \backslash f\text{ " }X$）

## 12. A flawed definition of $\mathbb{N}$

1. $L = \{x \in V | \emptyset \in x\}$, 有空集的集合
2. $(L, \subseteq)$ is a complete lattice
3. Successor operation: $S : V \to V$, $S(x) = x \cup \{x\}$ for all $x \in V$.
4. $F : L \to L$, $F(A) = A \cup S\text{ " }A$, for all $A \in L$

- $S\text{ " }A = \{S(x) | x \in A\}$
- F is order-preserving
- F has a least fixed point
- $F(\mathbb{N}_{def}) = \mathbb{N}_{def}$
- $0 := \emptyset, 1 := S(\emptyset) = \{\emptyset\}, 2 := S(S(\emptyset)) = \{\emptyset, \{\emptyset\}\}$

5. $\mathbb{N}_{def} = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \cdots\}$

- $F(\mathbb{N}_{def}) = \mathbb{N}_{def} \cup S\text{ " }\mathbb{N}_{def} = \mathbb{N}_{def} \cup \{S(x) | x \in \mathbb{N}_{def}\}$

- $S(1) = S(\{\emptyset\}) = \{\emptyset\} \cup \{\{\emptyset\}\} = \{\emptyset, \{\emptyset\}\} =: 2$
- $S(n) = n + 1$

6. $\leq$ is a well-ordering of $\mathbb{N}_{def}$?
7. 如果归纳法不成立，$\mathbb{N}_{def}$ 就不是least fixed point

## 13. Example of induction

1. Theorem

- $(L, \preceq)$ is a lattice, if $X \subseteq L$ is finite with $|X| \geq 2$, then $X$ has a least upper bound.
- Proof:

> Suppose $X = \{x_1, \cdots, x_m\}$ has no l.u.b., m is the least We can prove $y \vee x_m = \bigvee\{x_1, \cdots, x_{m-1}\} \vee x_m$ is an upper bound of $X$. Any other upper bound $u$ of $X$ can lead to $y \vee x_m \preceq u$, which means $y \vee x_m$ is a l.u.b..

## 14. Strong induction

> $P(n) \Leftrightarrow \forall k(n_0 \leq k \leq n)A(k)$ 推出A(n+1)要用到不止A(n)

## 15. Recursive definition

1. $G(n, f(n)) = (n + 1, f(n + 1))$
2. $X = \{R \in \mathcal{P}(\mathbb{N} \times \mathbb{N}) | (0, n_0) \in R\}$

> $\forall A \subseteq X, (0, n_0) \in \bigcap A \subseteq \bigcup A \in \mathcal{P}(\mathbb{N} \times \mathbb{N})$

3. $(X, \subseteq)$ is a complete lattice, $\bigwedge A = \bigcap A$至少包含$(0, n_0)$, $\bigvee A = \bigcup A$
4. $F : X \to X$ by $F(R) = R \cup G\text{"}\ R$
5. F is order preserving

> $R \subseteq T \Rightarrow F(R) \subseteq F(T)$

6. There exists a least f in X s.t. $F(f) = f$.
7. $F(f) = f \cup G\text{"}\ f = f, G\text{"}\ f \subseteq f$

## 16. More general recursive functions

1. $\mathbb{N}_{def}$ is the $\subseteq -$least set (least fixed point of the successor operation)?

## 17. Principle of Structural Induction

### 17.1 Principle of Structural Induction

A is $\subseteq$-least, $B \subseteq A$, $A$ is closed under $C_1, \cdots, C_n$.

1. For all $b \in B$, P(b) holds
2. For all $a_1, \cdots, a_m$ and $c$ and $1 \leq i \leq n$, if $P(a_1), \cdots, P(a_m)$ all hold and $c$ is obtained from $a_1, \cdots, a_m$ by a single application of $C_i$, then $P(c)$ holds

> 每次挑出一个$C_i$算出c就行

### 17.2 $\subseteq$-least Property of Recursively Defined Sets:

X 满足$C_i$运算封闭，则$A \subseteq X$

# 18. Recursively Defined Sets

1. Example

> S is the $\subseteq$-least set s.t. $3 \in S$, if $x, y \in S$, then $x + y \in S$, $S = \{n \in \mathbb{N} | 3 | n\}$.

# 19. A question from assignment 1

## 19.1 Theorem

1. $B = \{\oplus_1, \oplus_2 \cdots\}$ is a set of atomic propositions. Every well-formed compound propositional expression formed from atomic propositions in $B$ is logically equivalent to a compound expression that only involves atomic propositions from $B = \{\vee, \neg\}$.