

# 逻辑推导和数学归纳

赵建华

南京大学计算机系

# 证明的过程

- 根据已知的事实，经过逻辑推导得到结论
  - 事实通常是论域中的定理等，通常也使用逻辑公式表示。
  - 逻辑推导必须遵循一阶逻辑的要求。但是写法有所改变
- 实际推导时，不可能每次都根据最基本的事实进行推导。
  - 可能需要使用定理；
  - 可能需要考虑概念的定义；
  - 也可能使用一些模式来简化证明过程

# 例子 (1)

- 给定  $S_n$  中两个轮换：

$$\sigma = (i_1 \ i_2 \ \dots \ i_k), \tau = (j_1 \ j_2 \ \dots \ j_s),$$

若  $\{i_1, i_2, \dots, i_k\} \cap \{j_1, j_2, \dots, j_s\} = \emptyset$ , 则  $\sigma\tau = \tau\sigma$

- 证明：

– 对任意  $x \in S$ , 分三种情况讨论：

–  $x \in \{i_1, i_2, \dots, i_k\}$ ;

–  $x \in \{j_1, j_2, \dots, j_s\}$ ;

–  $x \in S - (\{i_1, i_2, \dots, i_k\} \cup \{j_1, j_2, \dots, j_s\})$ ,

均有  $\sigma\tau(x) = \tau\sigma(x)$

# 分解

- $\sigma\tau = \tau\sigma$ 等价于

$$\forall x(x \in S \Rightarrow (\tau(\sigma(x)) = \sigma(\tau(x))))$$

- $\sigma$ 的定义为

$$\sigma(x) = \begin{cases} i_{(j \bmod k)+1} & \text{if } x = i_j \text{ for some } j \\ x & \text{other wise} \end{cases}$$

- $\tau$ 也可以类似地定义。
- 所以，前面的例子可以分解为

$$\begin{aligned} \forall x(\sigma(x) = \dots \wedge \tau(x) = \dots) \wedge \\ \{i_1, i_2, \dots, i_k\} \cap \{j_1, j_2, \dots, j_s\} = \emptyset \\ \Rightarrow \forall x(\tau(\sigma(x)) = \sigma(\tau(x))) \end{aligned}$$

# 证明

- 令  $S_1 = \{i_1, i_2, \dots, i_k\}$ ,  $S_2 = \{j_1, j_2, \dots, j_s\}$
- 任取一个元素  $x \in S$ ,
  - (1)  $S_1 \cap S_2 = \emptyset$  (条件)
  - (2)  $x \in S \Rightarrow (x \in S_1) \vee (x \in S_2) \vee (x \in S - S_1 - S_2)$  (集合论)
  - (3)  $(x \in S_1) \Rightarrow \tau(x) = x$  (定义, 1)
  - (4)  $(x \in S_1) \Rightarrow \sigma(x) \in S_1 \Rightarrow \tau(\sigma(x)) = \sigma(x)$  (定义, 1)
  - (5)  $(x \in S_1) \Rightarrow \tau(\sigma(x)) = \sigma(\tau(x))$  (3, 4)
  - (6)  $(x \in S_2) \Rightarrow \sigma(x) = x$  (定义, 1)
  - (7)  $(x \in S_2) \Rightarrow \tau(x) \in S_2 \Rightarrow \sigma(\tau(x)) = \tau(x)$  (定义, 1)
  - (8)  $(x \in S_2) \Rightarrow \tau(\sigma(x)) = \sigma(\tau(x))$  (6, 7)
  - (9)  $(x \in S - S_1 - S_2) \Rightarrow \sigma(x) = \tau(x) = x$  (集合论, 定义)
  - (10)  $(x \in S - S_1 - S_2) \Rightarrow \tau(\sigma(x)) = \sigma(\tau(x))$  (9)
  - (11)  $x \in S \Rightarrow \tau(\sigma(x)) = \sigma(\tau(x))$  (2, 5, 8, 10)
  - (12)  $\forall x(x \in S \Rightarrow (\tau(\sigma(x)) = \sigma(\tau(x))))$  (逻辑证明规则)

# 证明的格式化

- 证明由一系列命题组成；这些命题应该编号。
- 这一系列中最后一个命题是要证明的命题。
- 每个命题应该注明推导的依据，即
  - 由哪些命题推导得到，
  - 以及按照何种规则进行推导。