

开场白

# Prologue and Notation

Xiaofeng Gao

Department of Computer Science and Engineering  
Shanghai Jiao Tong University, P.R.China

# Outline

## 1 Preliminary 初步的

- Set 集合
- Function
- Logical Notation

## 2 Proof

- Definition
- Categories 类别
- Peano Axioms

# Outline

## 1 Preliminary

- Set
- Function
- Logical Notation

## 2 Proof

- Definition
- Categories
- Peano Axioms

# Definition

- A **set** is an unordered collection of elements.  $\rightarrow$  No duplications.
- Examples and notations:
  - $\{a, b, c\}$
  - $\{x \mid x \text{ is an even integer}\} \rightarrow \{0, 2, 4, 6, \dots\}$
  - $\phi$ : empty set
  - $\mathbb{N} = \{0, 1, 2, \dots\}$ : natural numbers (nonnegative integers)
  - $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ : integers
  - $\mathbb{R}$ : real numbers
  - $\mathbb{E}$ : even numbers
  - $\mathbb{O}$ : odd numbers

# Definition (2)

## 基数

- **Cardinality** of a set:  $|S| \rightarrow$  number of distinct elements
- **Set Equality**:  $S = T \rightarrow x \in S$  iff  $x \in T$
- **Subset**: A set  $S$  is a subset of  $T$ ,  $S \subseteq T$ , if every element of  $S$  is an element of  $T$
- **Proper subset**: a subset of  $T$  is a subset other than the empty set  $\emptyset$  or  $T$  itself (Use of word proper, proper subsequence or proper substring)
- **Strict Subset**:  $S$  is a strict subset,  $S \subset T$ , if not equal to  $T$

非空真子集

真子集

$\cup, \cap, \rightarrow, \bar{S}$ 

- **Union:**  $S \cup T \rightarrow$  the set of elements that are either in  $S$  or in  $T$ .
  - $S \cup T = \{s | s \in S \text{ or } s \in T\}$
  - $\{a, b, c\} \cup \{c, d, e\} = \{a, b, c, d, e\}$
  - $|S \cup T| \leq |S| + |T|$
- **Intersection:**  $S \cap T$ 
  - $S \cap T = \{s | s \in S \text{ and } s \in T\}$
  - $\{a, b, c\} \cap \{c, d, e\} = \{c\}$
- **Difference:**  $S - T \rightarrow$  set of all elements in  $S$  not in  $T$ 
  - $S - T = \{s | s \in S \text{ but not in } T\} = S \cap \bar{T}$
  - $\{1, 2, 3\} - \{1, 4, 5\} = \{2, 3\}$
- **Complement:**
  - Need universal set  $U$
  - $\bar{S} = \{s | s \in U \text{ but not in } S\}$

$\times, 2^S$ 

- Cartesian Product 笛卡尔乘积

- $S \times T = \{(s, t) \mid s \in S, t \in T\}$

- In a graph  $G = (V, E)$ , the edge set  $E$  is the subset of Cartesian product of vertex set  $V$ .  $E \subseteq V \times V$ .

- Power Set 幂集

- $2^S$  set of all subsets of  $S$

- Note: notation  $|2^S| = 2^{|S|}$ , meaning  $2^S$  is a good representation for power set.

- $S = \{a, b, c\}$ , then 所有子集

$$2^S = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$$

- Indicator Vector: We can use a zero/one vector to represent the elements in power set.

|               | $a$ | $b$ | $c$ |
|---------------|-----|-----|-----|
| $\emptyset$   | 0   | 0   | 0   |
| $\{a\}$       | 1   | 0   | 0   |
| $\{b\}$       | 0   | 1   | 0   |
| $\{a, b, c\}$ | 1   | 1   | 1   |

# Ordered Pair

- $(x, y)$ : ordered pair of elements  $x$  and  $y$ ;  $(x, y) \neq (y, x)$ .
- $(x_1, \dots, x_n)$ : ordered  $n$ -tuple  $\rightarrow$  boldfaced  $\mathbf{x}$ .
- $A_1 \times A_2 \times \dots \times A_n = \{(x_1, \dots, x_n) \mid x_1 \in A_1, \dots, x_n \in A_n\}$ .
- $A \times A \times \dots \times A = A^n$ .
- $A^1 = A$ .



# Outline

## 1 Preliminary

- Set
- **Function**
- Logical Notation

## 2 Proof

- Definition
- Categories
- Peano Axioms

# Definition

- $f$  is a set of ordered pairs s.t. if  $(x, y) \in f$  and  $(x, z) \in f$ , then  $y = z$ , and  $f(x) = y$ .
- $Dom(f)$ : Domain of  $f$ ,  $\{x \mid f(x) \text{ is defined}\}$ . 定义域
- $f(x)$  is undefined if  $x \notin Dom(f)$ .
- $Ran(f)$ : Range of  $f$ ,  $\{f(x) \mid x \in Dom(f)\}$ .
- $f$  is a function from  $A$  to  $B$ :  $Dom(f) \subseteq A$  and  $Ran(f) \subseteq B$ .
- $f : A \rightarrow B$ :  $f$  is a function from  $A$  to  $B$  with  $Dom(f) = A$ .

# Mapping and Operation

## 单射

- **Injective (one-to-one)**: if  $x, y \in \text{Dom}(f)$ ,  $x \neq y$ , then  $f(x) \neq f(y)$ .
- **Inverse  $f^{-1}$** : the unique function  $g$  s.t.  $\text{Dom}(g) = \text{Ran}(f)$ , and  $g(f(x)) = x$ .
- **Surjective (onto)**: if  $\text{Ran}(f) = B$ . **满射**
- **Bijjective**: both injective and surjective.
- **Composition**:  $f \circ g$ , domain  $\{x \mid x \in \text{Dom}(g) \wedge g(x) \in \text{Dom}(f)\}$ , value  $f(g(x))$ .  
?

# Polynomial

A polynomial  $p$  is an expression of finite length constructed from variables and constants, using only the operations of addition, subtraction, multiplication, and non-negative integer exponents.

# Polynomial

A polynomial  $p$  is an expression of finite length constructed from variables and constants, using only the operations of addition, subtraction, multiplication, and non-negative integer exponents.

- $4x^2y + 3x - 5$  is a polynomial.
- $-6y^2 - \frac{7}{9}x$  is a polynomial.
- $\frac{1}{x} + x^{\frac{3}{4}}$  is not a polynomial.
- $3xy^{-2}$  is not a polynomial.

# Outline

## 1 Preliminary

- Set
- Function
- Logical Notation

## 2 Proof

- Definition
- Categories
- Peano Axioms

# Hand Writing

- Small letters for **elements** and **functions**.
  - $a, b, c$  for elements,
  - $f, g$  for functions,
  - $i, j, k$  for integer indices,
  - $x, y, z$  for variables,
- Capital letters for **sets**.  $A, B, S$ .  $A = \{a_1, \dots, a_n\}$
- Bold small letters for **vectors**.  $\mathbf{x}, \mathbf{y}$ .  $\mathbf{v} = \{v_1, \dots, v_m\}$
- Bold capital letters for **collections**.  $\mathbf{A}, \mathbf{B}$ .  $\mathbf{S} = \{S_1, \dots, S_n\}$  ?
- Blackboard bold capitals for **domains** (standard symbols).  $\mathbb{N}, \mathbb{R}, \mathbb{Z}$  (in memory of German mathematician Zahlen).
- German script for **collection of functions**.  $\mathcal{C}, \mathcal{I}, \mathcal{J}$ . ?
- Greek letters for **parameters** or **coefficients**.  $\alpha, \beta, \gamma$ . 参数系数
- Double strike handwriting for bold letters.

# Reviews

- Graph
  - Basic concepts: directed/undirected graph;
  - Path; Cycle; Tree;
  - Handshaking Theorem
- Data Structure
  - Table; Link-list;
  - Stack; Queue; Heap;
  - Other basic concepts.



# Outline

## 1 Preliminary

- Set
- Function
- Logical Notation

## 2 Proof

- Definition
- Categories
- Peano Axioms

# What is proof?

A **proof** of a statement is essentially a convincing argument that the statement is true. A typical step in a proof is to derive statements from

- assumptions or hypotheses. 假设
- statements that have already been derived.
- other generally accepted facts, using general principles of logical reasoning.

# Outline

## 1 Preliminary

- Set
- Function
- Logical Notation

## 2 Proof

- Definition
- **Categories**
- Peano Axioms

# Types of Proof

- Proof by Construction 解释
- Proof by Contrapositive 反命题 逆否?
  - Proof by Contradiction 矛盾
  - Proof by Counterexample 反例
- Proof by Cases
- Proof by Mathematical Induction 数学归纳法
  - The Principle of Mathematical Induction
  - Minimal Counterexample Principle 最小反例原理
  - The Strong Principle of Mathematical Induction

# Proof by Construction ( $\forall x, P(x)$ holds)

**Example:** For any integers  $a$  and  $b$ , if  $a$  and  $b$  are odd, then  $ab$  is odd.

# Proof by Construction ( $\forall x, P(x)$ holds)

**Example:** For any integers  $a$  and  $b$ , if  $a$  and  $b$  are odd, then  $ab$  is odd.

**Proof:** Since  $a$  and  $b$  are odd, there exist integers  $x$  and  $y$  such that  $a = 2x + 1$ ,  $b = 2y + 1$ .

# Proof by Construction ( $\forall x, P(x)$ holds)

**Example:** For any integers  $a$  and  $b$ , if  $a$  and  $b$  are odd, then  $ab$  is odd.

**Proof:** Since  $a$  and  $b$  are odd, there exist integers  $x$  and  $y$  such that  $a = 2x + 1$ ,  $b = 2y + 1$ . We wish to show that there is an integer  $z$  so that  $ab = 2z + 1$ . Let us therefore consider  $ab$ .

# Proof by Construction ( $\forall x, P(x)$ holds)

**Example:** For any integers  $a$  and  $b$ , if  $a$  and  $b$  are odd, then  $ab$  is odd.

**Proof:** Since  $a$  and  $b$  are odd, there exist integers  $x$  and  $y$  such that  $a = 2x + 1$ ,  $b = 2y + 1$ . We wish to show that there is an integer  $z$  so that  $ab = 2z + 1$ . Let us therefore consider  $ab$ .

$$\begin{aligned} ab &= (2x + 1)(2y + 1) \\ &= 4xy + 2x + 2y + 1 \\ &= 2(2xy + x + y) + 1 \end{aligned}$$



# Proof by Construction ( $\forall x, P(x)$ holds)

**Example:** For any integers  $a$  and  $b$ , if  $a$  and  $b$  are odd, then  $ab$  is odd.

**Proof:** Since  $a$  and  $b$  are odd, there exist integers  $x$  and  $y$  such that  $a = 2x + 1$ ,  $b = 2y + 1$ . We wish to show that there is an integer  $z$  so that  $ab = 2z + 1$ . Let us therefore consider  $ab$ .

$$\begin{aligned} ab &= (2x + 1)(2y + 1) \\ &= 4xy + 2x + 2y + 1 \\ &= 2(2xy + x + y) + 1 \end{aligned}$$

Thus if we let  $z = 2xy + x + y$ , then  $ab = 2z + 1$ , which implies that  $ab$  is odd.  $\square$

# Proof by Contrapositive ( $p \rightarrow q \Leftrightarrow \neg q \rightarrow \neg p$ )

**Example:**  $\forall i, j, n \in \mathbb{N}$ , if  $i \times j = n$ , then either  $i \leq \sqrt{n}$  or  $j \leq \sqrt{n}$ .

# Proof by Contrapositive ( $p \rightarrow q \Leftrightarrow \neg q \rightarrow \neg p$ )

**Example:**  $\forall i, j, n \in \mathbb{N}$ , if  $i \times j = n$ , then either  $i \leq \sqrt{n}$  or  $j \leq \sqrt{n}$ .

**Proof:** We change this statement by its logically equivalence:

$\forall i, j, n \in \mathbb{N}$ , if it is not the case that  $i \leq \sqrt{n}$  or  $j \leq \sqrt{n}$ , then  $i \times j \neq n$ .

# Proof by Contrapositive ( $p \rightarrow q \Leftrightarrow \neg q \rightarrow \neg p$ )

**Example:**  $\forall i, j, n \in \mathbb{N}$ , if  $i \times j = n$ , then either  $i \leq \sqrt{n}$  or  $j \leq \sqrt{n}$ .

**Proof:** We change this statement by its logically equivalence:

$\forall i, j, n \in \mathbb{N}$ , if it is not the case that  $i \leq \sqrt{n}$  or  $j \leq \sqrt{n}$ , then  $i \times j \neq n$ .

If it is not true that  $i \leq \sqrt{n}$  or  $j \leq \sqrt{n}$ , then  $i > \sqrt{n}$  and  $j > \sqrt{n}$ .

# Proof by Contrapositive ( $p \rightarrow q \Leftrightarrow \neg q \rightarrow \neg p$ )

**Example:**  $\forall i, j, n \in \mathbb{N}$ , if  $i \times j = n$ , then either  $i \leq \sqrt{n}$  or  $j \leq \sqrt{n}$ .

**Proof:** We change this statement by its logically equivalence:

$\forall i, j, n \in \mathbb{N}$ , if it is not the case that  $i \leq \sqrt{n}$  or  $j \leq \sqrt{n}$ , then  $i \times j \neq n$ .

If it is not true that  $i \leq \sqrt{n}$  or  $j \leq \sqrt{n}$ , then  $i > \sqrt{n}$  and  $j > \sqrt{n}$ .

Since  $j > \sqrt{n} \geq 0$ , we have

$$i > \sqrt{n} \Rightarrow i \times j > \sqrt{n} \times j > \sqrt{n} \times \sqrt{n} = n.$$

It follows that  $i \times j \neq n$ . The original statement is true.  $\square$

# Proof by Contradiction ( $p$ is true $\Leftrightarrow \neg p \rightarrow \text{false}$ is true)

**Example:** For any sets  $A$ ,  $B$ , and  $C$ , if  $A \cap B = \emptyset$  and  $C \subseteq B$ , then  $A \cap C = \emptyset$ .

# Proof by Contradiction ( $p$ is true $\Leftrightarrow \neg p \rightarrow \text{false}$ is true)

**Example:** For any sets  $A$ ,  $B$ , and  $C$ , if  $A \cap B = \emptyset$  and  $C \subseteq B$ , then  $A \cap C = \emptyset$ .

**Proof:** Assume  $A \cap B = \emptyset$ ,  $C \subseteq B$ , and  $A \cap C \neq \emptyset$ .

# Proof by Contradiction ( $p$ is true $\Leftrightarrow \neg p \rightarrow \text{false}$ is true)

**Example:** For any sets  $A$ ,  $B$ , and  $C$ , if  $A \cap B = \emptyset$  and  $C \subseteq B$ , then  $A \cap C = \emptyset$ .

**Proof:** Assume  $A \cap B = \emptyset$ ,  $C \subseteq B$ , and  $A \cap C \neq \emptyset$ .

Then there exists  $x$  with  $x \in A \cap C$ , so that  $x \in A$  and  $x \in C$ .



# Proof by Contradiction ( $p$ is true $\Leftrightarrow \neg p \rightarrow \text{false}$ is true)

**Example:** For any sets  $A$ ,  $B$ , and  $C$ , if  $A \cap B = \emptyset$  and  $C \subseteq B$ , then  $A \cap C = \emptyset$ .

**Proof:** Assume  $A \cap B = \emptyset$ ,  $C \subseteq B$ , and  $A \cap C \neq \emptyset$ .

Then there exists  $x$  with  $x \in A \cap C$ , so that  $x \in A$  and  $x \in C$ .

Since  $C \subseteq B$  and  $x \in C$ , it follows that  $x \in B$ .

# Proof by Contradiction ( $p$ is true $\Leftrightarrow \neg p \rightarrow \text{false}$ is true)

## 反证法 非 $p$ 推出矛盾

**Example:** For any sets  $A$ ,  $B$ , and  $C$ , if  $A \cap B = \emptyset$  and  $C \subseteq B$ , then  $A \cap C = \emptyset$ .

**Proof:** Assume  $A \cap B = \emptyset$ ,  $C \subseteq B$ , and  $A \cap C \neq \emptyset$ .

Then there exists  $x$  with  $x \in A \cap C$ , so that  $x \in A$  and  $x \in C$ .

Since  $C \subseteq B$  and  $x \in C$ , it follows that  $x \in B$ .

Therefore  $x \in A \cap B$ , which contradicts the assumption that  $A \cap B = \emptyset$ . □

# Proof by Cases (Divide domain into distinct subsets)

**Example:** Prove that if  $n \in \mathbb{N}$ , then  $3n^2 + n + 14$  is even.

# Proof by Cases (Divide domain into distinct subsets)

**Example:** Prove that if  $n \in \mathbb{N}$ , then  $3n^2 + n + 14$  is even.

**Proof:** Let  $n \in \mathbb{N}$ . We can consider two cases:  $n$  is even and  $n$  is odd.

分类讨论

# Proof by Cases (Divide domain into distinct subsets)

**Example:** Prove that if  $n \in \mathbb{N}$ , then  $3n^2 + n + 14$  is even.

**Proof:** Let  $n \in \mathbb{N}$ . We can consider two cases:  $n$  is even and  $n$  is odd.

**Case 1.**  $n$  is even. Let  $n = 2k$ , where  $k \in \mathbb{N}$ . Then

$$\begin{aligned} 3n^2 + n + 14 &= 3(2k)^2 + 2k + 14 \\ &= 12k^2 + 2k + 14 \\ &= 2(6k^2 + k + 7) \end{aligned}$$

Since  $6k^2 + k + 7$  is an integer,  $3n^2 + n + 14$  is even if  $n$  is even.

# Proof by Cases (Cont.)

**Case 2.**  $n$  is odd. Let  $n = 2k + 1$ , where  $k \in \mathbb{N}$ . Then

$$\begin{aligned} 3n^2 + n + 14 &= 3(2k + 1)^2 + (2k + 1) + 14 \\ &= 3(4k^2 + 4k + 1) + (2k + 1) + 14 \\ &= 12k^2 + 12k + 3 + 2k + 1 + 14 \\ &= 12k^2 + 14k + 18 \\ &= 2(6k^2 + 7k + 9) \end{aligned}$$

Since  $6k^2 + 7k + 9$  is an integer,  $3n^2 + n + 14$  is even if  $n$  is odd.

# Proof by Cases (Cont.)

**Case 2.**  $n$  is odd. Let  $n = 2k + 1$ , where  $k \in \mathbb{N}$ . Then

$$\begin{aligned} 3n^2 + n + 14 &= 3(2k + 1)^2 + (2k + 1) + 14 \\ &= 3(4k^2 + 4k + 1) + (2k + 1) + 14 \\ &= 12k^2 + 12k + 3 + 2k + 1 + 14 \\ &= 12k^2 + 14k + 18 \\ &= 2(6k^2 + 7k + 9) \end{aligned}$$

Since  $6k^2 + 7k + 9$  is an integer,  $3n^2 + n + 14$  is even if  $n$  is odd.

Since in both cases  $3n^2 + n + 14$  is even, it follows that if  $n \in \mathbb{N}$ , then  $3n^2 + n + 14$  is even.  $\square$

# The Principle of Mathematical Induction

Suppose  $P(n)$  is a statement involving an integer  $n$ . Then to prove that  $P(n)$  is true for every  $n \geq n_0$ , it is sufficient to show these two things:

- $P(n_0)$  is true.
- For any  $k \geq n_0$ , if  $P(k)$  is true, then  $P(k + 1)$  is true.



# An Example for Mathematical Induction

**Example:** Let  $P(n)$  be the statement  $\sum_{i=0}^n i = n(n+1)/2$ . Prove that  $P(n)$  is true for every  $n \geq 0$ .

# An Example for Mathematical Induction

**Example:** Let  $P(n)$  be the statement  $\sum_{i=0}^n i = n(n+1)/2$ . Prove that  $P(n)$  is true for every  $n \geq 0$ .

**Proof:** We prove  $P(n)$  is true for  $n \geq 0$  by induction.

# An Example for Mathematical Induction

**Example:** Let  $P(n)$  be the statement  $\sum_{i=0}^n i = n(n+1)/2$ . Prove that  $P(n)$  is true for every  $n \geq 0$ .

**Proof:** We prove  $P(n)$  is true for  $n \geq 0$  by induction.

**Basis step.**  $P(0)$  is  $0 = 0(0+1)/2$ , and it is obviously true.

# An Example for Mathematical Induction

**Example:** Let  $P(n)$  be the statement  $\sum_{i=0}^n i = n(n+1)/2$ . Prove that  $P(n)$  is true for every  $n \geq 0$ .

**Proof:** We prove  $P(n)$  is true for  $n \geq 0$  by induction.

**Basis step.**  $P(0)$  is  $0 = 0(0+1)/2$ , and it is obviously true.

**Induction Hypothesis.** Assume  $P(k)$  is true for some  $k \geq 0$ . Then  $0 + 1 + 2 + \cdots + k = k(k+1)/2$ .

# An Example for Mathematical Induction

**Example:** Let  $P(n)$  be the statement  $\sum_{i=0}^n i = n(n+1)/2$ . Prove that  $P(n)$  is true for every  $n \geq 0$ .

**Proof:** We prove  $P(n)$  is true for  $n \geq 0$  by induction.

**Basis step.**  $P(0)$  is  $0 = 0(0+1)/2$ , and it is obviously true.

**Induction Hypothesis.** Assume  $P(k)$  is true for some  $k \geq 0$ . Then  $0 + 1 + 2 + \cdots + k = k(k+1)/2$ .

**Proof of Induction Step.** Now let us prove that  $P(k+1)$  is true.

$$\begin{aligned} 0 + 1 + 2 + \cdots + k + (k+1) &= k(k+1)/2 + (k+1) \\ &= (k+1)(k/2 + 1) \\ &= (k+1)(k+2)/2 \end{aligned} \quad \square$$

# The Minimal Counterexample Principle

**Example:** Prove  $\forall n \in \mathbb{N}, 5^n - 2^n$  is divisible by 3.

# The Minimal Counterexample Principle

**Example:** Prove  $\forall n \in \mathbb{N}, 5^n - 2^n$  is divisible by 3.

**Proof:** If  $P(n) = 5^n - 2^n$  is not true for every  $n \geq 0$ , then there are values of  $n$  for which  $P(n)$  is false, and there must be a smallest such value, say  $n = k$ .

Since  $P(0) = 5^0 - 2^0 = 0$ , which is divisible by 3, we have  $k \geq 1$ , and  $k - 1 \geq 0$ .

Since  $k$  is the smallest value for which  $P(k)$  false,  $P(k - 1)$  is true. Thus  $5^{k-1} - 2^{k-1}$  is a multiple of 3, say  $3j$ .

假设小于k时都成立，大于等于k时不成立，  
结果证得大于等于k时也成立，原假设错误

# The Minimal Counterexample Principle (Cont.)

However, we have

$$\begin{aligned}5^k - 2^k &= 5 \times 5^{k-1} - 2 \times 2^{k-1} \\&= 5 \times (5^{k-1} - 2^{k-1}) + 3 \times 2^{k-1} \\&= 5 \times 3j + 3 \times 2^{k-1}\end{aligned}$$

This expression is divisible by 3. We have derived a contradiction, which allows us to conclude that our original assumption is false.  $\square$



# An Example for the Weakness of Mathematical Induction

**Example:** Prove that  $\forall n \in \mathbb{N}$  with  $n \geq 2$ , it has prime factorizations.

# An Example for the Weakness of Mathematical Induction

**Example:** Prove that  $\forall n \in \mathbb{N}$  with  $n \geq 2$ , it has prime factorizations.

**Proof:** Define  $P(n)$  be the statement that “ $n$  is either prime or the product of two or more primes”. We will try to prove that  $P(n)$  is true for every  $n \geq 2$ .

# An Example for the Weakness of Mathematical Induction

**Example:** Prove that  $\forall n \in \mathbb{N}$  with  $n \geq 2$ , it has prime factorizations.

**Proof:** Define  $P(n)$  be the statement that “ $n$  is either prime or the product of two or more primes”. We will try to prove that  $P(n)$  is true for every  $n \geq 2$ .

**Basis step.**  $P(2)$  is true, since 2 is a prime. ✓

# An Example for the Weakness of Mathematical Induction

**Example:** Prove that  $\forall n \in \mathbb{N}$  with  $n \geq 2$ , it has prime factorizations.

**Proof:** Define  $P(n)$  be the statement that “ $n$  is either prime or the product of two or more primes”. We will try to prove that  $P(n)$  is true for every  $n \geq 2$ .

**Basis step.**  $P(2)$  is true, since 2 is a prime. ✓

**Induction hypothesis.**  $P(k)$  for  $k \geq 2$ . (as usual process)

# An Example for the Weakness of Mathematical Induction

**Example:** Prove that  $\forall n \in \mathbb{N}$  with  $n \geq 2$ , it has prime factorizations.

**Proof:** Define  $P(n)$  be the statement that “ $n$  is either prime or the product of two or more primes”. We will try to prove that  $P(n)$  is true for every  $n \geq 2$ .

**Basis step.**  $P(2)$  is true, since 2 is a prime. ✓

**Induction hypothesis.**  $P(k)$  for  $k \geq 2$ . (as usual process)

**Proof of induction step.** Let's prove  $P(k + 1)$ .

If  $P(k + 1)$  is prime, ✓

If  $P(k + 1)$  is not a prime, then we should prove that  $k + 1 = r \times s$ , where  $r$  and  $s$  are positive integers greater than 1 and less than  $k + 1$ .

# An Example for the Weakness of Mathematical Induction

**Example:** Prove that  $\forall n \in \mathbb{N}$  with  $n \geq 2$ , it has prime factorizations.

**Proof:** Define  $P(n)$  be the statement that “ $n$  is either prime or the product of two or more primes”. We will try to prove that  $P(n)$  is true for every  $n \geq 2$ .

**Basis step.**  $P(2)$  is true, since 2 is a prime. ✓

**Induction hypothesis.**  $P(k)$  for  $k \geq 2$ . (as usual process)

**Proof of induction step.** Let's prove  $P(k+1)$ .

If  $P(k+1)$  is prime, ✓

If  $P(k+1)$  is not a prime, then we should prove that  $k+1 = r \times s$ , where  $r$  and  $s$  are positive integers greater than 1 and less than  $k+1$ .

However, from  $P(k)$  we know nothing about  $r$  and  $s \longrightarrow ???$

# The Strong Principle of Mathematical Induction

Suppose  $P(n)$  is a statement involving an integer  $n$ . Then to prove that  $P(n)$  is true for every  $n \geq n_0$ , it is sufficient to show these two things:

- $P(n_0)$  is true.
- For any  $k \geq n_0$ , if  $P(n)$  is true for every  $n$  satisfying  $n_0 \leq n \leq k$ , then  $P(k+1)$  is true.

Also called **the principle of complete induction**, or **course-of-values induction**.

? 完全归纳法

# To Complete the Example

**Example:** Prove that  $\forall n \in \mathbb{N}$  with  $n \geq 2$ , it has prime factorizations.



# To Complete the Example

**Example:** Prove that  $\forall n \in \mathbb{N}$  with  $n \geq 2$ , it has prime factorizations.

**Continue the Proof:**

**Induction hypothesis.** For  $k \geq 2$  and  $2 \leq n \leq k$ ,  $P(n)$  is true. (Strong Principle)

# To Complete the Example

**Example:** Prove that  $\forall n \in \mathbb{N}$  with  $n \geq 2$ , it has prime factorizations.

**Continue the Proof:**

**Induction hypothesis.** For  $k \geq 2$  and  $2 \leq n \leq k$ ,  $P(n)$  is true. (Strong Principle)

**Proof of induction step.** Let's prove  $P(k+1)$ .

If  $P(k+1)$  is prime,  $\checkmark$

If  $P(k+1)$  is not a prime, by definition of a prime,  $k+1 = r \times s$ , where  $r$  and  $s$  are positive integers greater than 1 and less than  $k+1$ .

# To Complete the Example

**Example:** Prove that  $\forall n \in \mathbb{N}$  with  $n \geq 2$ , it has prime factorizations.

**Continue the Proof:**

**Induction hypothesis.** For  $k \geq 2$  and  $2 \leq n \leq k$ ,  $P(n)$  is true. (Strong Principle)

**Proof of induction step.** Let's prove  $P(k+1)$ .

If  $P(k+1)$  is prime,  $\checkmark$

If  $P(k+1)$  is not a prime, by definition of a prime,  $k+1 = r \times s$ , where  $r$  and  $s$  are positive integers greater than 1 and less than  $k+1$ .

It follows that  $2 \leq r \leq k$  and  $2 \leq s \leq k$ . Thus by induction hypothesis, both  $r$  and  $s$  are either prime or the product of two or more primes. Then their product  $k+1$  is the product of two or more primes.  $P(k+1)$  is true.

# Outline

## 1 Preliminary

- Set
- Function
- Logical Notation

## 2 Proof

- Definition
- Categories
- Peano Axioms

# Giuseppe Peano (1858-1932)

- In 1889, Peano published the first set of axioms.
- Build a rigorous system of arithmetic, number theory, and algebra. 严格的
- A simple but solid foundation to construct the edifice of modern mathematics. 知识结构
- The fifth axiom deserves special comment. It is the first formal statement of what we now call the “induction axiom” or “the principle of mathematical induction”.

# Peano Five Axioms

- Axiom 1. 0 is a number.
- Axiom 2. The successor of any number is a number.
- Axiom 3. If  $a$  and  $b$  are numbers and if their successors are equal, then  $a$  and  $b$  are equal.
- Axiom 4. 0 is not the successor of any number.
- Axiom 5. If  $S$  is a set of numbers containing 0 and if the successor of any number in  $S$  is also in  $S$ , then  $S$  contains all the numbers.