1-3 常用的证明方法

魏恒峰

hfwei@nju.edu.cn

2017 年 10 月 23 日

习题选讲

UD (第五章)	反证法 (Contradiction)
UD (第十七章)	数学归纳法 (Mathematical Induction)
ES (第二十四章)	鸽笼原理 (Pigeonhole Principle)

习题选讲

UD (第五章)	反证法 (Contradiction)
UD (第十七章)	数学归纳法 (Mathematical Induction)
ES (第二十四章)	鸽笼原理 (Pigeonhole Principle)

UD 题目 17.14：第二数学归纳法

使用 (第一) 数学归纳法证明第二数学归纳法。

Theorem (Cantor Theorem)

Let A be a set.
If $f : A \to 2^A$, then f is not onto.

UD 题目 17.14：第二数学归纳法

使用 (第一) 数学归纳法证明第二数学归纳法。

Theorem (Cantor Theorem)

Let A be a set.
If $f : A \to 2^A$, then f is not onto.

UD 题目 17.14：第二数学归纳法

使用 (第一) 数学归纳法证明：

Theorem (Second Principle of Mathematical Induction)

For an integer n, let $Q(n)$ denote an assertion. Suppose that

(i) *$Q(1)$ is true and*

(ii) *for all positive integers n, if $Q(1), \cdots, Q(n)$ are true, then $Q(n+1)$ is true.*

Then $Q(n)$ holds for all positive integers n.

Theorem (第二数学归纳法)

$$\Big[Q(1) \land \forall n \in \mathbb{N}^+ \Big((Q(1) \land \cdots \land Q(n)) \to Q(n+1) \Big) \Big] \to \forall n \in \mathbb{N}^+ Q(n).$$

Theorem (第二数学归纳法)

$$\Big[Q(1) \wedge \forall n \in \mathbb{N}^+ \Big((Q(1) \wedge \cdots \wedge Q(n)) \to Q(n+1) \Big) \Big] \to \forall n \in \mathbb{N}^+ Q(n).$$

Theorem ((第一) 数学归纳法)

$$\Big[P(1) \wedge \forall n \in \mathbb{N}^+ (P(n) \to P(n+1)) \Big] \to \forall n \in \mathbb{N}^+ P(n).$$

"标准" 证明示例。

$$P(n) \triangleq Q(1) \wedge \cdots \wedge Q(n)$$

用(第一) 数学归纳法证明 $P(n)$ 对一切正整数都成立。

"标准" 证明示例。

$$P(n) \triangleq Q(1) \wedge \cdots \wedge Q(n)$$

用(第一) 数学归纳法证明 $P(n)$ 对一切正整数都成立。

Proof.

By mathematical induction on $\mathbb{N}^{+}$.

Basis $P(1)$

Inductive Step $P(n) \rightarrow P(n+1)$

Therefore, $P(n)$ holds for all positive integers. □

"标准" 证明示例。

$$P(n) \triangleq Q(1) \land \cdots \land Q(n)$$

用(第一) 数学归纳法证明 $P(n)$ 对一切正整数都成立。

Proof.

By mathematical induction on $\mathbb{N}^+$.

Basis $P(1)$

Inductive Hypothesis $P(n)$

Inductive Step $P(n) \to P(n+1)$

Therefore, $P(n)$ holds for all positive integers. □

Proof.

能不能“算一算”呢?

$$P(n) \triangleq Q(1) \land \cdots \land Q(n)$$

$\square$

Let us calculate [calculemus].

数学归纳法

(第一) 数学归纳法与第二数学归纳法等价。

数学归纳法

(第一) 数学归纳法与第二数学归纳法等价。

Q : 为什么第二数学归纳法也被称为“强” (strong) 数学归纳法?

Theorem (Cantor Theorem (1891))

Let A be a set.
If $f : A \to 2^A$, then f is not onto.

Georg Cantor (1845 – 1918)

Theorem (Cantor Theorem)

Let A be a set.
If $f : A \to 2^A$, then f is not onto.

Theorem (Cantor Theorem)

Let A be a set.
If $f : A \to 2^A$, then f is not onto.

Theorem (Cantor Theorem)

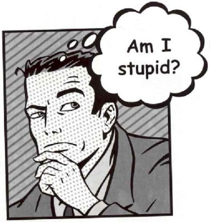
Let A be a set.
If $f : A \to 2^A$, then f is not onto.

Theorem (Cantor Theorem)

Let A be a set.
If $f : A \to 2^A$, then f is not onto.

Theorem (Cantor Theorem)

Let A be a set.
If $f : A \to 2^A$, then f is not onto.



Theorem (Cantor Theorem)

Let A be a set.
If $f : A \to 2^A$, then f is not onto.

Understanding this problem:

Theorem (Cantor Theorem)

Let A be a set.
If $f : A \to 2^A$, then f is not onto.

Understanding this problem:

2^A $A = \{1, 2, 3\}$,

$$2^A = \Big\{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\Big\}$$

Theorem (Cantor Theorem)

Let A be a set.
If $f : A \to 2^A$, then f is not onto.

Understanding this problem:

2^A $A = \{1, 2, 3\}$,

$$2^A = \Big\{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\Big\}$$

Onto

$$\forall B \in 2^A \, \exists a \in A \, (f(a) = B).$$

Theorem (Cantor Theorem)

Let A be a set.
If $f : A \to 2^A$, then f is not onto.

Understanding this problem:

2^A $A = \{1, 2, 3\}$,

$$2^A = \Big\{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\Big\}$$

Onto

$$\forall B \in 2^A \; \exists a \in A \; (f(a) = B).$$

Not Onto

$$\exists B \in 2^A \; \neg\Big(\exists a \in A \; (f(a) = B)\Big).$$

Theorem (Cantor Theorem)

Let A be a set.
If $f : A \to 2^A$, then f is not onto.

Proof. $\square$

Theorem (Cantor Theorem)

Let A be a set.
If $f : A \to 2^A$, then f is not onto.

Proof.

- Constructive proof:

$$B = \{x \in A \mid x \notin f(x)\}.$$

$\square$

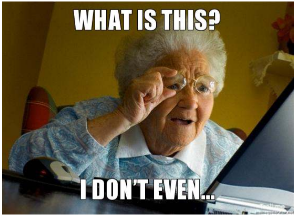
Theorem (Cantor Theorem)

Let A be a set.
If $f : A \to 2^A$, then f is not onto.

Proof.

- Constructive proof:

$$B = \{x \in A \mid x \notin f(x)\}.$$



□

Theorem (Cantor Theorem)

Let A be a set.
If $f : A \to 2^A$, then f is not onto.

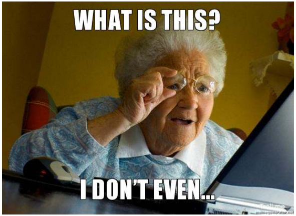
Proof.

- Constructive proof:

$$B = \{x \in A \mid x \notin f(x)\}.$$

- By contradiction:

$$\exists a \in A : f(a) = B.$$



□

Theorem (Cantor Theorem)

Let A be a set.
If $f : A \to 2^A$, then f is not onto.

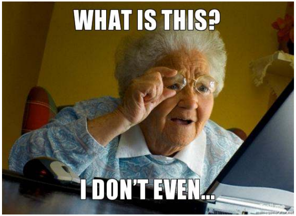
Proof.

- Constructive proof:

$$B = \{x \in A \mid x \notin f(x)\}.$$

- By contradiction:

$$\exists a \in A : f(a) = B.$$



$$Q : a \in B \ (= f(a))?$$

□

Theorem (Cantor Theorem)

Let A be a set.
If $f : A \to 2^A$, then f is not onto.

对角线论证 (Cantor's diagonal argument) (以下仅适用于可数集合 A).

a	$f(a)$					
	1	2	3	4	5	$\cdots$
1	1	1	0	0	1	$\cdots$
2	0	0	0	0	0	$\cdots$
3	1	0	0	1	0	$\cdots$
4	1	1	1	1	1	$\cdots$
5	0	1	0	1	0	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ldots$

$\square$

Theorem (Cantor Theorem)

Let A be a set.
If $f : A \to 2^A$, then f is not onto.

对角线论证 (Cantor's diagonal argument) (以下仅适用于可数集合 A).

a	$f(a)$					
	1	2	3	4	5	$\cdots$
1	1	1	0	0	1	$\cdots$
2	0	0	0	0	0	$\cdots$
3	1	0	0	1	0	$\cdots$
4	1	1	1	1	1	$\cdots$
5	0	1	0	1	0	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ldots$

$\square$

Theorem (Cantor Theorem)

Let A be a set.
If $f : A \to 2^A$, then f is not onto.

对角线论证 (Cantor's diagonal argument) (以下仅适用于可数集合 A).

a	$f(a)$					
	1	2	3	4	5	$\cdots$
1	1	1	0	0	1	$\cdots$
2	0	0	0	0	0	$\cdots$
3	1	0	0	1	0	$\cdots$
4	1	1	1	1	1	$\cdots$
5	0	1	0	1	0	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\cdots$

$$B = \{0, 1, 1, 0, 1\}$$

补充题目

存在性证明 (Existence Proof)

1. 构造性证明 (Constructive proof)
2. 反证法 (By contradiction)
3. 概率法 (Probabilistic Method)

Theorem (Dov Jarden (1953))

$$\exists a, b \in \mathbb{R} \setminus \mathbb{Q} : a^b \in \mathbb{Q}.$$

Theorem (Dov Jarden (1953))

$$\exists a, b \in \mathbb{R} \setminus \mathbb{Q} : a^b \in \mathbb{Q}.$$

$$\sqrt{2} \in \mathbb{R} \setminus \mathbb{Q} \qquad \text{(Theorem 5.2)}$$

Theorem (Dov Jarden (1953))

$$\exists a, b \in \mathbb{R} \setminus \mathbb{Q} : a^b \in \mathbb{Q}.$$

$$\sqrt{2} \in \mathbb{R} \setminus \mathbb{Q} \qquad \text{(Theorem 5.2)}$$

Proof.

$$\sqrt{2}^{\sqrt{2}}$$

Theorem (Dov Jarden (1953))

$$\exists a, b \in \mathbb{R} \setminus \mathbb{Q} : a^b \in \mathbb{Q}.$$

$$\sqrt{2} \in \mathbb{R} \setminus \mathbb{Q} \qquad \text{(Theorem 5.2)}$$

Proof.

$$\sqrt{2}^{\sqrt{2}}$$

$$(\sqrt{2}^{\sqrt{2}})^{\sqrt{2}}$$

□

Theorem (Dov Jarden (1953))

$$\exists a, b \in \mathbb{R} \setminus \mathbb{Q} : a^b \in \mathbb{Q}.$$

$$\sqrt{2} \in \mathbb{R} \setminus \mathbb{Q} \qquad \text{(Theorem 5.2)}$$

Proof.

$$\sqrt{2}^{\sqrt{2}}$$

$$(\sqrt{2}^{\sqrt{2}})^{\sqrt{2}}$$

□

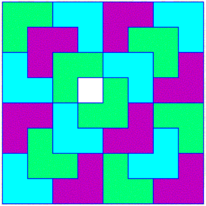
Q: 这是构造性证明吗？这是反证法吗？

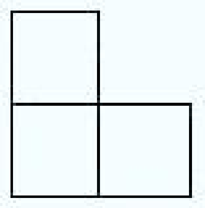
Lossless Compression

补充思考题

Theorem (Tiling Theorem)

For any positive integer k, a $2^k \times 2^k$ checkerboard with any one square removed can be tiled using right triominoes.






Thank
You!