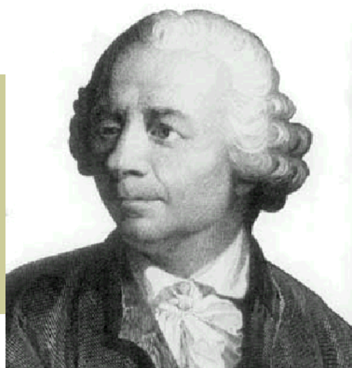
NANJING UNIVERSITY



离 散 数 学
Discrete Mathematics

第五讲：集合论导引

史颖欢

南京大学计算机科学与技术系

2016 年9 月 8 日

前 情 提 要

- 证明的本质
- 逻辑推理的形式结构
- 常用的证明方法与证明策略
  - 直接证明法，间接证明法
  - 归谬法（反证法），穷举法
  - 空证明法，平凡证明法
  - 构造性证明法，反例证明法

本讲主要内容

- 引子：数学基础的几次危机
- 集合的概念
- 子集、空集与幂集
- 集合的运算与集合代数
- 集合公式的几种基本证明方式

引子：数学基础的几次危机

- 19世纪早期，发现数学存在缺陷
  - **Н.И. Лобаче́вский，G. Riemann：非欧几何**
  - **A. Cauthy等：分析(微积分及其扩展)的基础**
- 19世纪后期的公理化运动：去除基于直觉或经验的朴素概念的模糊之处，使数学严密化
  - **G. Peano，D. Hilbert：算术与几何的公理化**

数学基础的几次危机（续）

- 1900年国际数学大会
  - H. Poincare:“借助集合论…可以建造数学大厦…今天我们可以宣称绝对的严密已经实现了!”
- 随后发现了Cantor集合论中的一些悖论：如1901年的罗素悖论
- G. Frege评论：当大厦竣工时基础却动摇了

数学基础的几次危机（续）

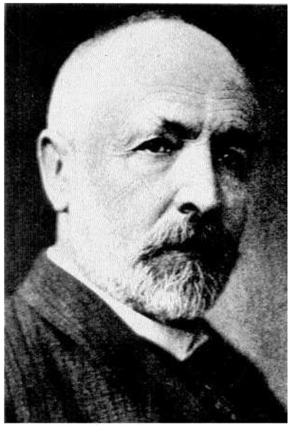
危机的解决：

公 理 化 集 合 论

集合的概念

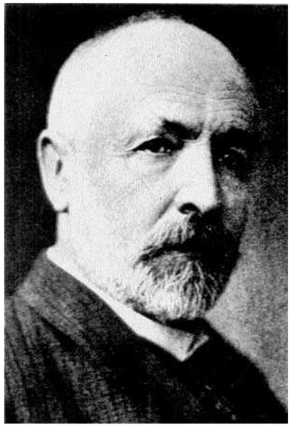
- 集合没有明确的定义，G. Cantor给出了一种刻划：

> “吾人直观或思维之对象，如为相异而确定之物，其总括之全体即谓之集合，其组成此集合之物谓之集合之元素。通常用大写字母表示集合，如A、B、C等，用小写字母表示元素，如a、b、c 等。若集合A系由a、b、c等诸元素所组成，则表如$A=\{a,b,c,\cdots\}$，而a为A之元素，亦常用$a \in A$之记号表之者， a非A之元素，则记如$a \notin A$。”
>
> （肖文灿译于1939年，《集合论初步》，商务印书馆）



集合的概念（续）

- 例：{1,2,3}为集合，“自然数之全体”为集合；但诸如“甚大之数”或“与P点接近之点”则不能为集合，因其界限不清
- 集合中的元素互异，我们把元素的重复看作一次出现，如$\{2,2,3,3\} = \{2,3\}$
- Cantor提到的“总括之全体”之“总括”，可由集合的外延公理和概括原则来描述



集合的外延公理与概括原则

- **(ZF.1)** 外延公理：集合由其元素完全决定

$$A = B \leftrightarrow \forall x(x \in A \leftrightarrow x \in B)$$

故证明集合$A = B$只需证明$\forall x(x \in A \leftrightarrow x \in B)$

- 概括原则：对于人们直观或者思维之对象x的任一性质$P(x)$，存在集合S的元素恰为具有性质P的那些对象，记为$S = \{x|P(x)\}$。从而对任何a，$a \in S \leftrightarrow P(a)$，例如$\{1,2,3\} = \{x|x = 1 \vee x = 2 \vee x = 3\}$

罗素悖论与公理集合论

- $\{x|P(x)\}$未必产生集合，B. Russell在1901年给出反例，即著名的罗素悖论：令$R=\{x|x\notin x\}$，则若R为集合则$R\in R\leftrightarrow R\notin R$矛盾，故$R$不为集合。

罗素悖论与公理化集合论

- 罗素悖论是集合论迄今为止最著名的悖论，因其形式简单而意义深远。由罗素悖论人们重新审视集合论，修改概括原理，用形式化方法讨论集合论，最终导致公理集合论的诞生。
- ☞进一步阅读：公理化集合论

  http://zh.wikipedia.org/wiki/公理化集合论

子 集

- A为B之**子集**（记为$A \subseteq B$）指$\forall x(x \in A \to x \in B)$，
  A为B之**真子集**（记为$A \subset B$）指$A \subseteq B$且$A \neq B$。
  $A \not\subseteq B$是指$\exists x(x \in A \land x \notin B)$
- **例**：$\{1,2\} \subseteq \{1,2,3\}$，$A \subseteq A$，$\mathbb{N} \subseteq \mathbb{R}$
- **命题**：

$$\boldsymbol{A = B \leftrightarrow (A \subseteq B \land B \subseteq A)}$$

该命题也常被用来证明集合相等

空 集

- 集合论系统有二种：一种承认有原子（即本身不含元素但能作为别的集合的元素），另一种不承认有原子，认为一切皆为集合。本课程采用后者，这样便导致最初之元素为没有任何元素的集合，从这种集合出发构成集合世界，因此它是任何集合的子集
- **(ZF.3*)** 空集公理：*存在一个集合其没有任何元素，称这种集合为空集（null set），记作∅，其为任何集合（包含空集本身）之子集*

空 集（续）

- 命题：空集是唯一的
  - 证明：设$\emptyset_1, \emptyset_2$皆为空集，则根据空集的定义，有$\emptyset_1 \subseteq \emptyset_2 \wedge \emptyset_2 \subseteq \emptyset_1$，根据集合相等的定义有$\emptyset_1 = \emptyset_2$
- 空集本身是一个集合，也可以做为另一个集合的元素或子集，故：$\emptyset \in \{\emptyset\}$，$\emptyset \subseteq \{\emptyset\}$；但因为空集不含任何元素，故$\emptyset \notin \emptyset$，$\emptyset \neq \{\emptyset\}$
- 定义：若集合A含有n个元素，则称A为n元集，记为$|A| = n$；易见，$\emptyset$是0元集，$\{\emptyset\}$是1元集

由集合定义自然数

- 在公理集合论中，集合是自然数的基础
  - **定义：设a为集合，称$a\cup\{a\}$为a的后继，记作a^+**
  - **定义 (von Neumann)：**

$$令\ 0=\emptyset, 1=0^+, 2=0^{++}, \cdots, n=0^{\overbrace{+\cdots+}^{n}}$$

  - **定义：设A是集合，称A为归纳集 (inductive set)指：**

$$\emptyset\in \boldsymbol{A}\land(\forall \boldsymbol{x}\in \boldsymbol{A})(\boldsymbol{x}^+\in \boldsymbol{A})$$

归纳集是否存在？

- 若存在归纳集A，则$\emptyset \in A, \emptyset^{+} \in A, \emptyset^{++\cdots+} \in A$，从而$A$是无穷集
- Russell说：“事实上，在这个世界中是否有无穷集合，我们还不能确定。”
- 据此，还不能确定归纳集是否存在。大多数人认为宇宙是无穷的（Hilbert 则否），为了保证归纳集的存在，引入无穷公理

无穷公理

- **(ZF.7)** 无穷公理（Axiom of Infinity）：

$$\exists A\big(\emptyset \in A \land (\forall x \in A)(x^+ \in A)\big)$$

- 以往按照von Neumann的定义，$0=\emptyset$，$n+1=n^+$，从而可以定义出单个的自然数，但不能说明全体自然数集合$\mathbb{N}$的存在性，而由无穷公理可以定义$\mathbb{N}$

- 定义：$\mathbb{N} \stackrel{\text{def}}{=} \cap\{A|A\text{为归纳集}\} =$

$$\Big\{\emptyset,\{\emptyset\},\{\emptyset,\{\emptyset\}\},\big\{\emptyset,\{\emptyset\},\{\emptyset,\{\emptyset\}\}\big\},\cdots\Big\}$$

幂 集

- **(ZF.8)** **幂集公理**：集合A的幂集$P(A)=\{x|x\subseteq A\}$

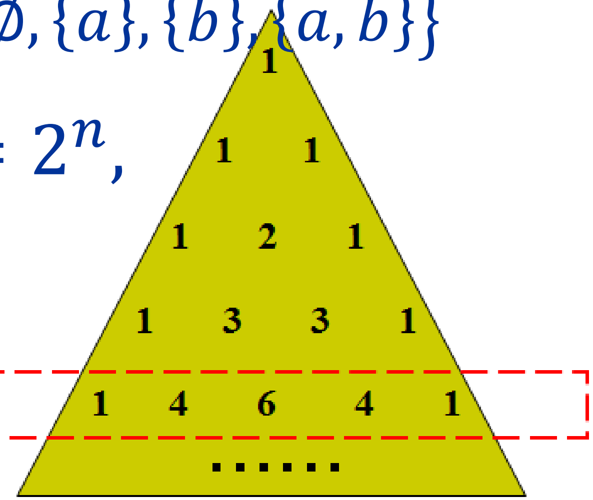
  即由集合A的全体子集构成的集合

  - 例：$P(\emptyset)=\{\emptyset\}$，$PP(\emptyset)=\{\emptyset,\{\emptyset\}\}$，$PPP(\emptyset)=\{\emptyset,\{\emptyset\},\{\{\emptyset\}\},\{\emptyset,\{\emptyset\}\}\}$，$P(\{a,b\})=\{\emptyset,\{a\},\{b\},\{a,b\}\}$

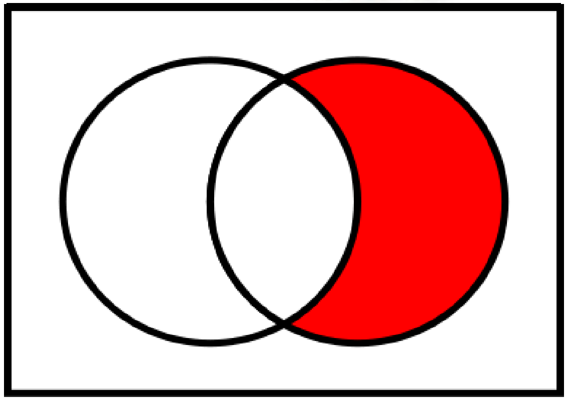
- 若$|A|=n$，则$|P(A)|=\sum_{k=0}^{n}\binom{n}{k}=2^n$，

  故集合A的幂集的另一种记法为$\mathbf{2^A}$

- 若$P(A)\in P(B)$，则$A\in B$



集合运算

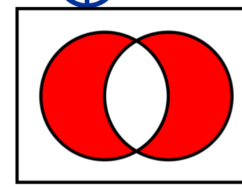


- 为了由已有集合产生新的集合，引入一些集合上的运算：
- 定义：
  - **(ZF.5)**集合的并：$A \cup B = \{x | x \in A \vee x \in B\}$
  - 集合的交：$A \cap B = \{x | x \in A \wedge x \in B\}$
  - 集合的相对补：$A - B = \{x | x \in A \wedge x \notin B\}$
  - 集合的对称差：

$$A \oplus B = \{x | (x \in A \wedge x \notin B) \vee (x \in B \wedge x \notin A)\}$$
$$= (A - B) \cup (B - A)$$

集合运算（续）

- 例：观察文氏图，试证明对称差$A \oplus B = (A \cup B) - (A \cap B)$



证明：根据对称差定义，$\boldsymbol{A \oplus B = (A - B) \cup (B - A)}$，任取$\boldsymbol{x \in A \oplus B}$，即$\boldsymbol{x \in (A - B)}$或$\boldsymbol{x \in (B - A)}$.

- 1. 假设$\boldsymbol{x \in (A - B)}$，根据相对补定义，有$\boldsymbol{x \in A}$且$\boldsymbol{x \notin B}$，故而$\boldsymbol{x \in (A \cup B)}$但$\boldsymbol{x \notin (A \cap B)}$，根据相对补定义，有$\boldsymbol{x \in (A \cup B) - (A \cap B)}$;
- 2. 假设$\boldsymbol{x \in (B - A)}$，根据相对补定义，有$\boldsymbol{x \in B}$且$\boldsymbol{x \notin A}$，故而$\boldsymbol{x \in (A \cup B)}$但$\boldsymbol{x \notin (A \cap B)}$，根据相对补定义，亦有$\boldsymbol{x \in (A \cup B) - (A \cap B)}$.

综上，对于任意$\boldsymbol{x \in A \oplus B}$，皆有$\boldsymbol{x \in (A \cup B) - (A \cap B)}$，反之亦然（需要加入证明内容）。由集合相等定义，$\boldsymbol{A \oplus B = (A \cup B) - (A \cap B)}$. □

广义交与广义并

- 上面介绍的是两个集合的交与并，现将其推广：
- 定义（广义交与广义并）：
  - 集合的广义并：设A为集合，A的所有元素的并称为集合A的广义并，记为：$\cup A=\{x|(\exists y\in A)(x\in y)\}$
  - 集合的广义交：设A为非空集合，A的所有元素的交称为集合A的广义交，记为：$\cap A=\{x|\forall y\in A\rightarrow x\in y)\}$
  - 思考：为什么规定广义交的对象不能为$\emptyset$?

集合代数

- 在集合的运算中，满足以下规律：
- 定理：设A, B, C为任意集合
  - 交换律：$A \cup B = B \cup A$，$A \cap B = B \cap A$
  - 结合律：$A \cup (B \cup C) = (A \cup B) \cup C$

    $A \cap (B \cap C) = (A \cap B) \cap C$
  - 分配律：$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

    $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
  - 幂等律：$A \cap A = A \cup A = A$
  - 空集性质：$A \cap \emptyset = \emptyset$，$A \cup \emptyset = A$

集合代数（续）

- 在集合的运算中，满足以下规律（续）：
- 定理（续）：设A, B, C为任意集合
  - De Morgan 律：$A - (B \cup C) = (A - B) \cap (A - C)$

    $$A - (B \cap C) = (A - B) \cup (A - C)$$
  - 幂集性质：$P(A \cap B) = P(A) \cap P(B)$

    $$P(A \cup B) \supseteq P(A) \cup P(B)$$

集合公式的基本证明方式

- 方法一：直接使用集合包含或相等的定义
  - 例：$A \cup B = B \Rightarrow A \subseteq B$
  - 分析：待证结论为$A \subseteq B$，即$\forall x(x \in A \rightarrow x \in B)$，因此，证明框架如下：

    对任意x，假设$x \in A$，{⋯**适当内容**⋯}
    因此，$x \in B$，故$A \subseteq B$. □

  - 证明：

    对任意x，假设$x \in A$，根据集合并的定义有$x \in A \cup B$，由已知条件$A \cup B = B$，因此$x \in B$，故$A \subseteq B$. □

集合公式的基本证明方式（续）

- 方法二：利用运算定义作逻辑等值式推演
  - 例：试证 $\boldsymbol{A-(B\cup C)=(A-B)\cap(A-C)}$

另一种等价的描述方式：

$$
\begin{aligned}
x\in A-(B\cup C) &\Leftrightarrow (x\in A)\wedge\big(x\notin(B\cup C)\big)\\
&\Leftrightarrow x\in A\wedge x\notin B\wedge x\notin C\\
&\Leftrightarrow (x\in A\wedge x\notin B)\wedge(x\in A\wedge x\notin C)\\
&\Leftrightarrow \big(x\in(A-B)\big)\wedge\big(x\in(A-C)\big)\\
&\Leftrightarrow x\in\big((A-B)\cap(A-C)\big)
\end{aligned}
$$

集合公式的基本证明方式（续）

- 方法三：利用已知恒等式或等式作集合代数推演
  - 例1：$A \cap B = A \Leftrightarrow A - B = \emptyset$
  - 例2：$A \cup (A \cap B) = A$
  - 例3：已知$A \oplus B = A \oplus C$，证明$B = C$

$$A - B = A \cap \sim B$$
$$= (A \cap \sim B) \cup (A \cap \sim A)$$
$$= A \cap (\sim B \cup \sim A)$$
$$= A \cap \sim(A \cap B)$$
$$= A \cap \sim A = \emptyset$$

$$A \cup (A \cap B)$$
$$= (A \cap E) \cup (A \cap B)$$
$$= A \cap (E \cup B) = A \cap E = A$$

$$B = \emptyset \oplus B = (A \oplus A) \oplus B$$
$$= A \oplus (A \oplus B) = A \oplus (A \oplus C)$$
$$= (A \oplus A) \oplus C = \emptyset \oplus C = C$$

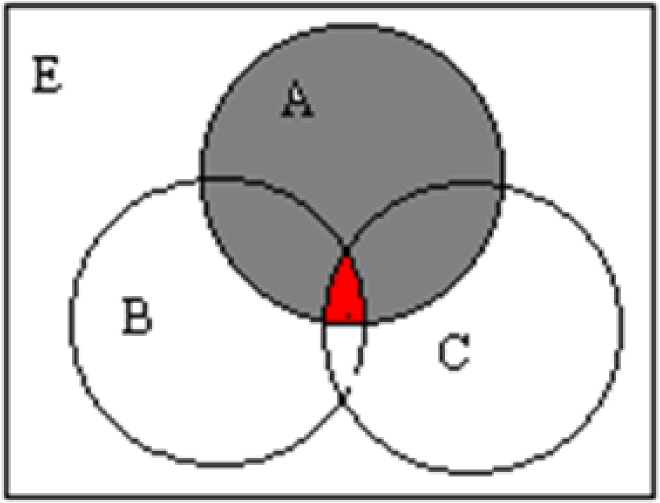
集合公式的基本证明方式（续）

- 方法四：循环证明一系列逻辑等值式
  - 例：试证$A\cup B=B \Leftrightarrow A\subseteq B \Leftrightarrow A\cap B=A \Leftrightarrow A-B=\emptyset$
  - 证明路径：(1)➞(2)➞(3)➞(4)➞(1)
  - 只要完成上述证明，由循环关系就证明了上述诸多充分必要关系
  - 在以上例子的基础上，只要再证明$A-B=\emptyset \Rightarrow A\cup B=B$
    - $A\cup B=(A\cup B)\cap E=(A\cup B)\cap(\sim B\cup B)=(A\cap$

集合公式的基本证明方式（续）

- 其它证明方法：文氏图也可帮助推测结论（但不能代替证明的过程）
- 例：$(A-B)\cup(A-C)=A$ 成立的充分必要条件？

充要条件：$A\cap B\cap C=\emptyset$



Georg Cantor

- 23岁获数学博士学位
- 集合论“公认为全部数学的基础”
- 关于无限的若干论断：
  - 集合论是一种“疾病”
  - “雾中之雾”、“疯子”
- 可能是这个时代所能夸耀的最巨大的工作。 ——罗素

本次课后作业

- 教材内容：[Rosen] 2.1 – 2.2 节
- 课后习题：
  - p. 107-108（英文教材 pp. 120 – 121）: 24, 41
  - pp. 116 -117（英文教材 pp. 131 – 132）: 18, 40, 50, 59

ZFC公理化集合系统*

- Ax. 1 外延公理
- Ax. 2 正则公理
- Ax. 3 分类公理
- Ax. 4 配对公理
- Ax. 5 并集公理
- Ax. 6 替代公理
- Ax. 7 无穷公理
- Ax. 8 幂集公理
- Ax. 9 选择公理（AC，或良序公理）

Tip：ZFC 系统

ZFC公理化集合系统*（续）

- 外延公理（Axiom of extensionality）
  - 如果两个集合含有同样的元素，则它们是相等的.

$$\forall x \forall y [\forall z (z \in x \Leftrightarrow z \in y) \Rightarrow x = y].$$

- 正则公理（Axiom of regularity/foundation）
  - 任意非空集*x*包含一个成员*y*，*x*与集合*y*是不相交的

$$\forall x [\exists a (a \in x) \Rightarrow \exists y (y \in x \wedge \neg \exists z (z \in y \wedge z \in x))].$$

Tip：ZFC 系统

ZFC公理化集合系统*（续）

- 分类公理（Axiom schema of separation）
  - 对任意集合z和任意对z的元素x有定义的逻辑谓词$\phi(x)$，存在z的子集y，使$x \in y$当且仅当$x \in z$且$\phi(x)$为真.

$$\forall z \forall w_1 \ldots w_n \exists y \forall x [x \in y \Leftrightarrow (x \in z \wedge \phi)].$$

- 配对公理（Axiom of pairing）

$$\forall x \forall y \exists z (x \in z \wedge y \in z).$$

- 并集公理（Axiom of union ）

$$\forall \mathcal{F} \exists A \forall Y \forall x [(x \in Y \wedge Y \in \mathcal{F}) \Rightarrow x \in A].$$

ZFC公理化集合系统*（续）

- 替代公理（Axiom schema of replacement）

$$\forall A \forall w_1, \ldots, w_n \big[\forall x(x \in A \Rightarrow \exists! y\, \phi) \Rightarrow \exists B \forall x\big(x \in A \Rightarrow \exists y(y \in B \wedge \phi)\big)\big].$$

- 无穷公理（Axiom of infinity ）
  - $S(y)$是指y^+

$$\exists X \left[\varnothing \in X \wedge \forall y(y \in X \Rightarrow S(y) \in X)\right].$$

- 幂集公理（Axiom of power set）

$$\forall x \exists y \forall z [z \subseteq x \Rightarrow z \in y].$$

Tip：ZFC 系统

ZFC公理化集合系统*（续）

- 选择公理（Axiom of choice）
  - 任一非空集合族$(S_i)_{i\in I}$均存在元素族$(s_i)_{i\in I}, \forall i \in I. s_i \in S_i$
- 或良序定理（Well-ordering theorem）

$$\forall X \exists R (R \text{ well-orders } X).$$

Tip：ZFC 系统