集合及其运算

离散数学－集合论

南京大学计算机学院

回顾

- 证明方法
  - 直接证明
  - 反证法
  - 分情形证明
  - 等价性证明
  - 存在性证明
  - 唯一性证明
  - 寻找反例

提要

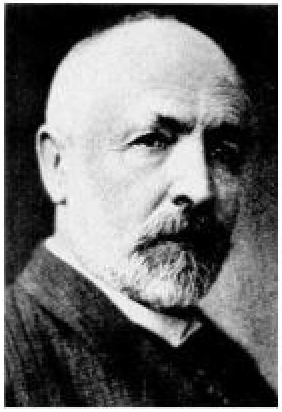
- 基本概念
  - 集合及其描述
  - 集合相等、子集关系
  - 幂集、笛卡尔乘积
- 集合运算
  - 交并补、广义交、广义并
  - 集合恒等式
  - 集合相关命题的证明方式
- 自然数的构造

集合的定义

- 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）



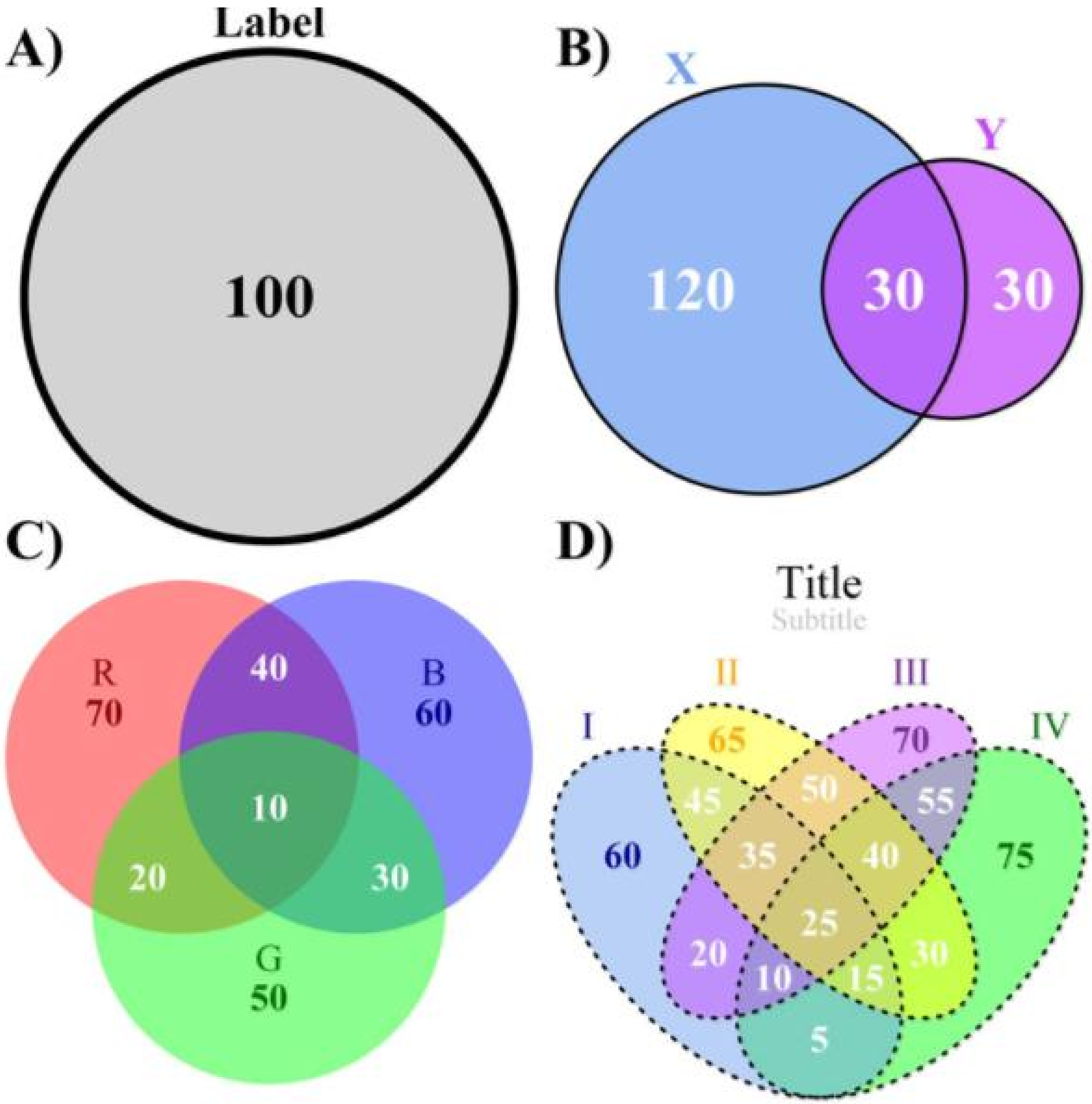
Naïve set theory，朴素集合论

集合的描述

- 外延法：罗列、枚举
  - V={a, e, i, o, u}
  - {1, 3, 5, 7, 9}
- 概括法：
  - {x | P(x)}, P： 某种思维、观察中总结出的对象性质
    - $a\in\{x \mid P(x)\} \leftrightarrow P(a)$
  - 例：$Z^{+}=\{x\in Z \mid x>0\}$， $Q=\{p/q \mid p\in Z, q\in Z, q\neq 0\}$，
    - $[a, b]=\{x\in R \mid a\leq x\leq b\}$

集合的

- 文氏图



A)
Label
100
B)
X
Y
120
30
30
C)
R
70
40
B
60
10
20
30
G
50
D)
Title
Subtitle
I
II
III
IV
65
70
45
50
55
60
35
40
75
25
20
30
10
15
5

集合相等、子集关系

- 定义：集合相等当且仅当它们有同样的元素
  - A=B 当且仅当 $\forall x(x\in A \leftrightarrow x\in B)$ //外延原则
- 定义：集合A称为集合B的子集，记作$A\subseteq B$
  - $\forall x\ (x\in A \rightarrow x\in B\ )$
  - 如果$A\subseteq B$, 但$A\neq B$，则A是B的真子集，记作$A\subset B$
- 定理：对任意集合A和B, A=B 当且仅当:
  - $A\subseteq B$, 且$B\subseteq A$

子集关系的一个性质

- 证明：如果$X\subseteq Y$且$Y\subseteq Z$, 则$X\subseteq Z$
- 要证明：“对任意的 a, 如果 $a\in X$, 则 $a\in Z$”
- 证明：
  - 对任意的 $a\in X$
  - 根据已知的“$X\subseteq Y$”，可得：$a\in Y$
  - 根据已知的“$Y\subseteq Z$”，可得：$a\in Z$
  - 所以，$\forall a\,(a\in X \rightarrow a\in Z)$, 即$X\subseteq Z$

集合的大小

- 有限集合及其基数
  - 若S恰有n个不同的元素，n是自然数，就说S是有限集合，而n是S的基数，记作$|S|=n$。
- 无限集合
  - 如果一个集合不是有限的，就说它是无限的。

空集

- 存在一个没有任何元素的集合：空集∅
- 关于空集的一些性质：
  - 空集是任何集合的子集。
    - $\varnothing \subseteq A$，即 $\forall x(x \in \varnothing \rightarrow x \in A)$
  - 空集是唯一的，可以用 ∅表示
    - 如果 $\varnothing_1, \varnothing_2$都是空集，则 $\varnothing_1 \subseteq \varnothing_2$ 和 $\varnothing_2 \subseteq \varnothing_1$ 均为真

关于空集的讨论

- 空集本身可以是一个对象，可以是某个集合的元素
  - $\varnothing \in \{\varnothing\}, \varnothing \subseteq \{\varnothing\}$
- 事实上，我们从空集开始构造整个集合世界!
  - 自然数
  - 有理数
  - 实数（幂集运算）
  - …

幂集

- S是一个集合，S的幂集是S的所有子集的集合
  - $\rho(S)=\{x|\ x \subseteq S\}$
- 举例
  - $\rho(\{a, b\}) = \{\varnothing,\{a\},\{b\},\{a, b\}\}$
  - $\rho(\varnothing) = \{\varnothing\}$

If $\rho(A) \subseteq \rho(B)$, then $A \subseteq B$

$\mathcal{P}(X)$

$\mathcal{P}(X)$

$\mathscr{P}(X)$

$\wp(X)$

$\mathbb{P}(X)$

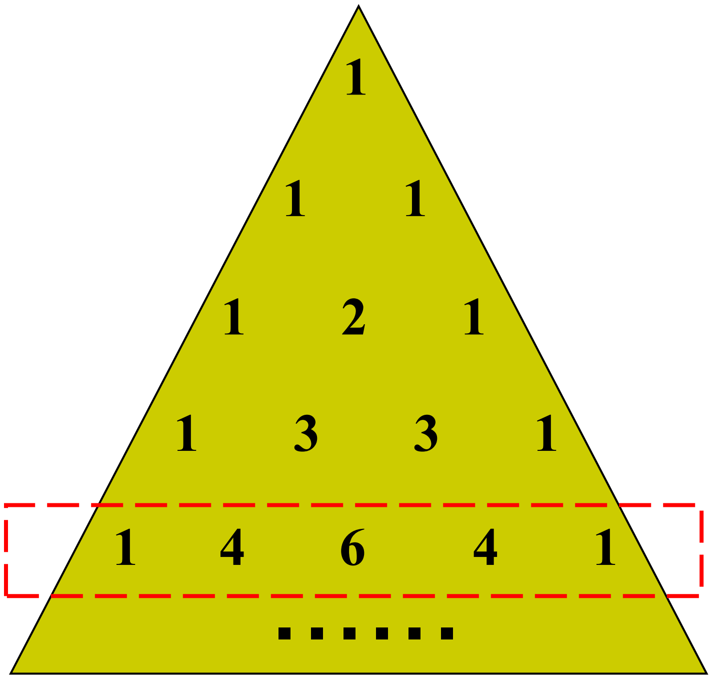
$\mathrm{P}(X)$

If $\rho(A) \subseteq \rho(B)$, then $A \subseteq B$

有限集合的所有子集

如果 $|A|=n$, 则 $|\rho(A)|=2^n$

幂集的另一种记法: 2^A



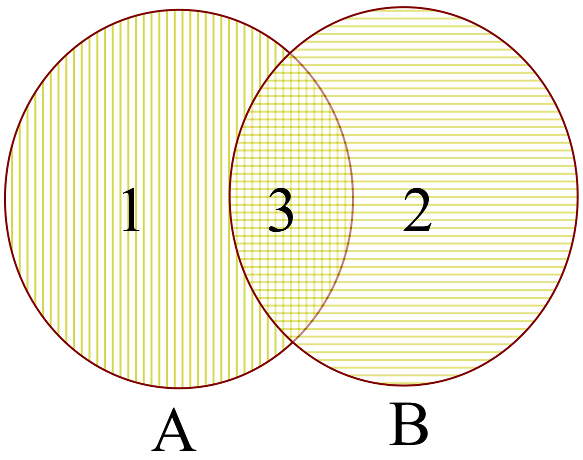
$C(4, 0)+ C(4, 1)+ C(4, 2)+ C(4, 3)+ C(4, 4) =2^4$

$A=\{1, .., n\}$

$\sum_{k=0\ldots n} C(n, k) =2^n$

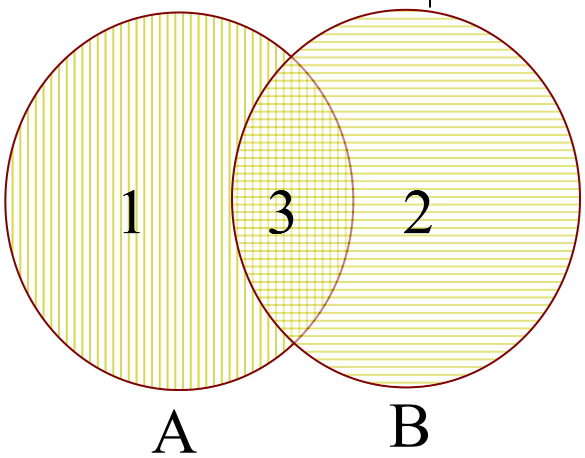
集合运算的定义

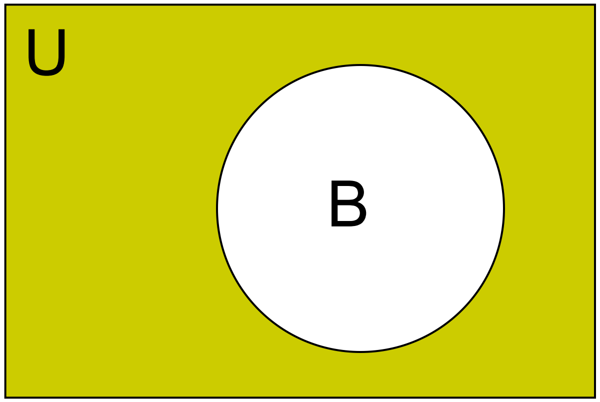
- **运算定义的基本方式：将结果定义为一个新的集合**
  - 并： $A\cup B=\{ x \mid x\in A \vee x\in B \}$
    - 并集: {1, 2 , 3}
  - 交： $A\cap B=\{ x \mid x\in A \wedge x\in B \}$
    - 交集: {3}



相对补（差）

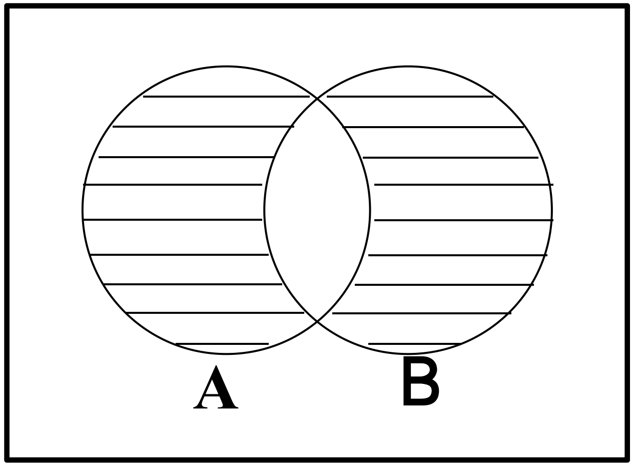
- B对于A的补集
  - A-B={ x | x∈A ∧ x∉B }
- 举例，A-B={1}
- 若有一个我们关心的“所有”对象的集合，称为全集，常用U表示，U-B称为B的“补集”，记为~B
  - x∈~B ↔ x∉B





对称差

- 对称差
  - $A \oplus B = (A-B) \cup (B-A)$
- 证明: $A \oplus B = (A \cup B) - (A \cap B)$
  - $(A-B) \cup (B-A) \subseteq (A \cup B) - (A \cap B)$
  - $(A \cup B) - (A \cap B) \subseteq (A-B) \cup (B-A)$



证明: $A \oplus B = (A \cup B) - (A \cap B)$

$$(A-B) \cup (B-A) \subseteq (A \cup B) - (A \cap B)$$

$$(A \cup B) - (A \cap B) \subseteq (A-B) \cup (B-A)$$

广义并和广义交

- 广义并
  - 设A为集合， A的所有元素的并，记为$\bigcup A$; 定义为 $\bigcup A=\{x|\exists y(y\in A\land x\in y)\}$
- 广义交
  - 设A为非空集合， A的所有元素的交，记为$\bigcap A$, 定义为： $\bigcap A=\{x|\forall y(y\in A\to x\in y)\}$
    - 注意：限制条件为A非空， $\bigcap\emptyset$无意义

运算的重要性质

- **包含关系下两个集合的最小上界和最大下界**
  - 最小上界:
    - $A \subseteq A \cup B$, $B \subseteq A \cup B$ ----A和B的上界
    - 对任意X， 若$A \subseteq X$, $B \subseteq X$,则$A \cup B \subseteq X$ ----最小上界
  - 最大下界:
    - $A \cap B \subseteq A$, $A \cap B \subseteq B$ ----A和B的下界
    - 对任意X， 若$X \subseteq A$, $X \subseteq B$,则$X \subseteq A \cap B$ ----最大下界

集合与谓词逻辑

- 在量化逻辑表达式中使用集合符号
  - $\forall x \in S(P(x))$代表$\forall x(x \in S \to P(x))$
  - $\exists x \in S(P(x))$代表$\exists x(x \in S \wedge P(x))$
  - 举例
    - $\forall x \in R(x^2 \geq 0)$: $\forall x(x \in R \to (x^2 \geq 0))$
    - $\exists x \in Z(x^2 = 1)$: $\exists x(x \in Z \wedge x^2 = 1)$

$$\forall_{x \in S} P(x)$$

$$\exists_{x \in S} P(x)$$

- 逻辑表达式的真值集合，$\{x \in D \mid P(x)\}$
  - 举例：$\{x \in Z \mid |x| = x\}$，$\{x \in Z \mid x^2 = 2\}$，$\{x \mid x \in Z \wedge x^2 = 2\}$

皮亚诺公理
(Peano axioms for natural numbers)

- 零是个自然数.
- 每个自然数都有一个后继（也是个自然数）.
- 零不是任何自然数的后继.
- 不同的自然数有不同的后继.
- （归纳公理）设由自然数组成的某个集合含有零，且每当该集合含有某个自然数时便也同时含有这个数的后继，那么该集合定含有全部自然数.

- 备注：另有4个与自然数相等有关的公理

皮亚诺公理
(Peano axioms for natural numbers)

戴德金-皮亚诺结构可以描述为满足所有以下条件的三元组 (S, f, e)

- $e \in S$
- $\forall a \in S\,(f(a) \in S)$
- $\forall b \in S\,\forall c \in S\,((f(b) = f(c)) \to (b = c))$
- $\forall a \in S\,(f(a) \neq e)$
- $\forall A \subseteq S\,(((e \in A) \wedge (\forall a \in A(f(a) \in A))) \to (A = S))$

用集合定义自然数

- 设a为集合, 称$a\cup\{a\}$为a的**后继**, 记为$s(a)$， 或a^+。
- 设A是集合， 若A满足下列条件， 称A为**归纳集**：
  - $\varnothing\in A$
  - $\forall a(a\in A\rightarrow s(a)\in A\}$
- 自然数集合N ($\mathbb{N}$) :是所有归纳集的交集。
  - 因此： $N = \{ \varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}, \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\}, \ldots \}$
  - N的每一个元素称为一个自然数。
  - Ø记为0， s(0)记为1， s(1)记为2， s(2)记为3， 以此类推

再具体一点

- 记号0表示：$\varnothing$
- 记号1表示0^+：$\varnothing \cup \{\varnothing\} = \{\varnothing\}$
- 记号2表示1^+：$\{\varnothing\} \cup \{\{\varnothing\}\} = \{\varnothing, \{\varnothing\}\}$
- 记号3表示2^+: $\{\varnothing, \{\varnothing\}\} \cup \{\{\varnothing, \{\varnothing\}\}\} = \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\}$
- $3 \cup 2 = ?$　$3 \cap 2 = ?$
- $2 \in 3?$　$1 \in 3?$
- $1 \subseteq 2?$　$2 \subseteq 5?$

自然数上的小于关系？

自然数上的运算

- 加法（递归定义）
  - $m+0=m$
  - $m+n^{+}=(m+n)^{+}$
- 乘法（递归定义）
  - $m*0=0$
  - $m*n^{+}=m + m*n$
- 序关系
  - $a \leq b$ iff $\exists c \in N.\ a+c=b$

集合悖论

- A=$\{x \mid P(x)\}$, 实际上不能保证：对任意的性质 P，这样的定义都有意义。
- 例如：
  - 1)存在不以自己为元素的集合，称它们为“平凡集”
    - 性质：年收入大于50万、教室里的同学
  - 2)定义包含所有“平凡集”的集合
    - A = $\{x|x\notin x\}$
- Russell 悖论：

定义 $R=\{x \mid x\notin x\}$。则如果R存在，定有: $R\in R$ iff. $R\notin R$

- 理发师悖论：“我给所有不给自己理发的人理发”

重新考察广义交

- **广义交**
  - 设A为非空集合， A的所有元素的交， 记为$\bigcap A$, 定义为： $\bigcap A = \{x \mid \forall y (y \in A \to x \in y)\}$
    - 注意：限制条件为A非空， $\bigcap \emptyset$无意义
    - – but why?

重新考察广义交

- 广义并和交的另一种记法

$$x \in \bigcup_{X \in \mathcal{C}} X \iff \exists_{X \in \mathcal{C}} \; x \in X$$

$$x \in \bigcap_{X \in \mathcal{C}} X \iff \forall_{X \in \mathcal{C}} \; x \in X$$

- 试证明：

Let $\mathcal{C} = \{A, B\}$. Show that

$$\bigcup_{X \in \mathcal{C}} X = A \cup B, \quad \bigcap_{X \in \mathcal{C}} X = A \cap B$$

Show that $\bigcup_{X \in \emptyset} X = \emptyset$

试证明：

Given a collection of sets $\mathcal{C} \neq \emptyset$ show that, for any $A \in \mathcal{C}$,

$$\bigcap_{X \in \mathcal{C}} X = \left\{ x \in A \,\middle|\, \forall_{X \in \mathcal{C}}\ x \in X \right\}$$

命题：对于任意集合x，都有 $x \notin x$ 成立。

先说一点，ZFC中有一条正则公理：$\forall x\,(x \neq \phi \rightarrow \exists y \in x(\forall z \in y(\neg z \in x)))$ 意思是说对于所有不空的集合x，存在x中的元素y，y中的所有元素都不属于x。这条公理可以排除很多奇异集合，比如：

命题：对于任意集合x，都有 $x \notin x$ 成立。

证明：假设命题不成立，即存在一集合，满足 $x \in x$。构造集合 $\{x\}$，易见 $\{x\}$ 不空且有唯一元素 x，因此 $\{x\} \cap x = x$。因为 $\{x\}$ 只有元素 x，因此 $\{x\}$ 中不存在元素 y，y 所有的元素都不属于 $\{x\}$。这与正则公理矛盾，因此假设不成立，原命题成立。（证毕）

空集的广义交不是一个集合

Theorem (Russell's paradox). $\bigcap\limits_{X \in \emptyset} X$ *is not a set.*

Proof. We will prove by contradiction. This method consists in assuming the result we want to prove is false and arriving at a contradiction. The contradiction shows that our assumption was wrong, hence the result is true. So assume $A = \bigcap_{X \in \emptyset} X$ is a set. By axiom 2 we can build the set

$$B = \{Y \in A \mid Y \notin Y\}$$

Then, by definition of B, the following is a true sentence:

$$B \in B \Longleftrightarrow (B \in A \text{ and } B \notin B)$$

It follows that both sentences $B \notin A$ and $B \notin B$ must be true. Then, by definition of A,

$$B \notin A \Leftrightarrow \text{not} \left(\forall_{X \in \emptyset} B \in X \right) \Leftrightarrow \exists_{X \in \emptyset} B \notin X$$

But this last sentence is false so we have reached a contradiction. We conclude A is not a set. $\square$

公理集合论（Axiomatic set theory）

- 用公理来约束集合世界，以摆脱悖论
  - 集合相等（=）和元素属于集合的关系（∈）
  - 某种集合存在性，亦即给定合法集合构造原则
- Zermelo–Fraenkel set theory with the axiom of Choice（ZFC集合论）参见附录

外延公理 正则公理 分离公理模式 配对公理 并集公理	替代公理模式 无穷公理 幂集公理 选择公理

笛卡尔乘积

- 有序偶:
  - 有序偶(a,b)=(x,y) 当且仅当 a=x, b=y
    - 实际上：(a,b)={{a},{a,b}}（后续课程介绍）
- 集合A和B的笛卡尔乘积
  - $A \times B = \{(a, b) \mid a \in A \wedge b \in B\}$
- 何种情形下，A×B=B×A
- 集合$A_1, A_2, \ldots, A_n$的笛卡尔乘积
  - $A_1 \times A_2 \times \ldots \times A_n = \{(a_1, a_2, \ldots, a_n) \mid a_i \in A_i, i=1,2,\ldots n\}$

集合相关命题的基本证明方式

- 直接使用集合包含、相等定义
  - $A \cup B = B \Rightarrow A \subseteq B$
  - 证明:
  - 对任何x, 假设$x \in A$
  - 由集合并定义：$x \in A \cup B$
  - 由已知条件：$A \cup B = B$
  - $\therefore x \in B$
  - 因此：$A \subseteq B$

基本证明方式

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

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

等价的描述方式：

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

基本证明方式

- 利用已知恒等式或等式作集合代数推演
  - 例： $A\cap B=A \Leftrightarrow A-B=\varnothing$

$A\cap B=A\Rightarrow A-B=\varnothing$:

$A-B=\varnothing \Rightarrow A\cap B=A$:

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

$$=A\cap(B\cup\sim B)=A\cap U=A$$

基本证明方式

- 利用已知恒等式或等式作集合代数推演
  - 例： 已知$A\oplus B=A\oplus C$, 证明$B=C$

$$
\begin{aligned}
B&=\varnothing\oplus B\\
&=(A\oplus A)\oplus B\\
&=A\oplus(A\oplus B)\\
&=A\oplus(A\oplus C)\\
&=C
\end{aligned}
$$

集合恒等式（1）

等 式	名 称
$A\cup\varnothing=A$ $A\cap U=A$	恒等律
$A\cup U=U$ $A\cap\varnothing=\varnothing$	支配律
$A\cup A=A$ $A\cap A=A$	幂等律
$\sim(\sim A)=A$	补集律
$A\cup B=B\cup A$ $A\cap B=B\cap A$	交换律

集合恒等式（2）

等 式	名 称
$A\cup(B\cup C)=(A\cup B)\cup C$ $A\cap(B\cap C)=(A\cap B)\cap C$	结合律
$A\cap(B\cup C)=(A\cap B)\cup(A\cap C)$ $A\cup(B\cap C)=(A\cup B)\cap(A\cup C)$	分配律
$\sim(A\cup B)=\sim A\cap\sim B$ $\sim(A\cap B)=\sim A\cup\sim B$	德摩根定律
$A\cup(A\cap B)=A$ $A\cap(A\cup B)=A$	吸收律
$A\cup\sim A=U$ $A\cap\sim A=\varnothing$	补律

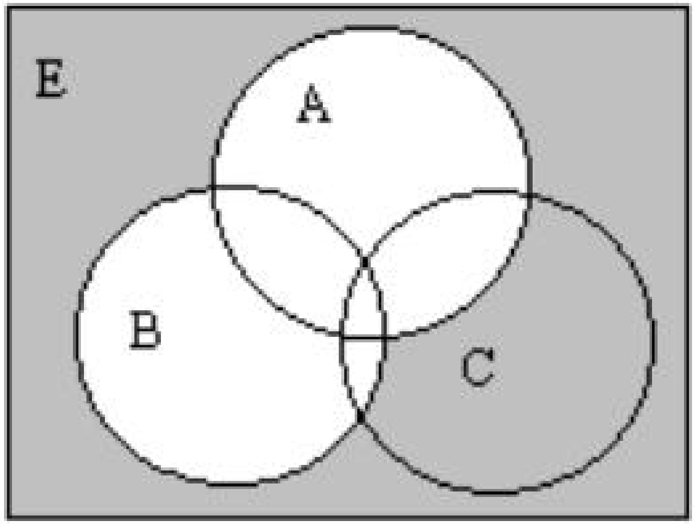
基本证明方式

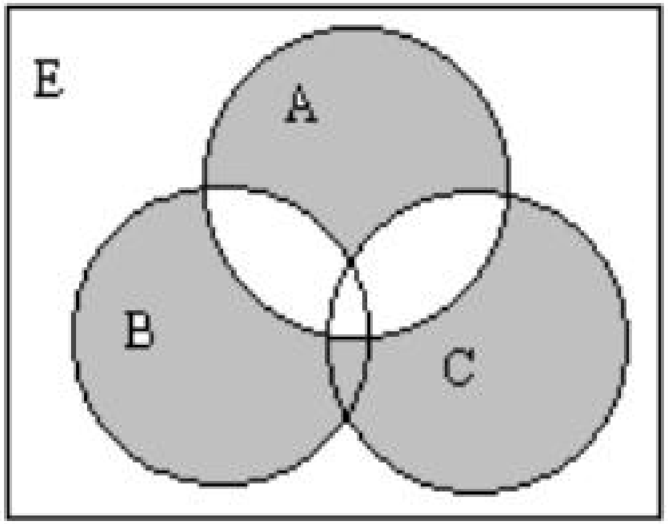
- 利用成员表证明集合恒等式
  - $A\cup(A\cap B)=A$

A	B	$A\cap B$	$A\cup(A\cap B)$
1	1	1	1
1	0	0	1
0	1	0	0
0	0	0	0

文氏图的更多例子

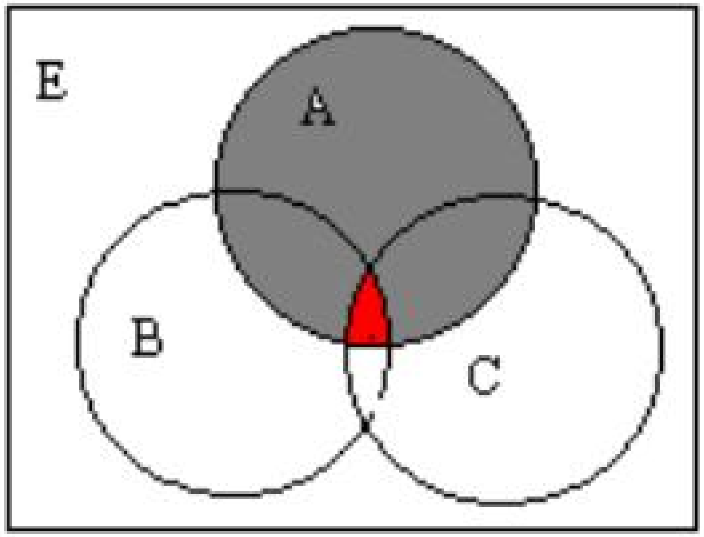
- $\sim A \cap \sim B$
- $(A-(B \cup C)) \cup ((B \cup C)-A)$





文氏图与数学证明

- 文氏图不能代替数学证明, 但可以帮助推测结论
- 例子:
  - $(A-B)\cup(A-C)=A$?



充要条件: $A\cap B\cap C=\varnothing$

作业

- 教材内容：[Rosen] 2.1—2.2 节
- 课后习题：
  - 见课程主页。

Zermelo–Fraenkel set theory with the axiom of choice

- 外延公理
- 正则公理
- 分离公理模式
- 配对公理
- 并集公理
- 替代公理模式
- 无穷公理
- 幂集公理
- 选择公理（或，良序定理）

ZFC公理

- **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/基础公理（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

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

ZFC公理

- **分离公理模式**（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ϕ(x), 存在z的子集y，使x∈y当且仅当x∈z而且ϕ(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

- 替代公理模式（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∪{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）

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

ZFC公理

- 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）

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

参考： Zermelo–Fraenkel set theory @Wiki