集合代数

李修成 lixiucheng@hit.edu.cn

计算机科学与技术学院

Outline

集合的基本概念

集合的基本运算

集合恒等式

集合计数

作业

集合的基本概念

集合的定义与表示法

1. 集合的定义

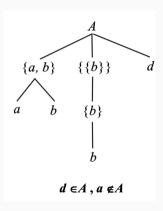
- 集合 (set) 是由一系列对象 (object) 构成的整体,这些对象被称为集合的元素.
- 通常通大写字母 A, B, \ldots 表示集合,用小写字母 a, b, \ldots 表示集合的元素.
- 如果元素 a 属于集合 A, 则记为 $a \in A$; 若不属于,则记为 $a \notin A$.
- 集合 A 中所包含的元素个数称为其基(cardinality),记为 |A|.
- 数学中常见的集合: $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ 分别表示自然数、整数、有理数、实数、复数集合.

2. 集合表示法

- 枚举法:通过枚举出全体元素来表示集合.
- 谓词表示法: 通过谓词概括出集合元素的性质.
- $\mathbb{N} = \{0, 1, 2, 3, \ldots\}.$
- $S = \{x \mid x \in \mathbb{R}, \ x^2 1 = 0\}.$

元素与集合

- 集合元素的性质
 - 无序性: 不关心集合中元素的顺序.
 - 相异性:集合中每个元素只计数一次.
 - 确定性: 给定任意元素都可以确定是否属于 一个给定集合.
 - 任意性:集合的元素也可以是集合.
- **例子:** $A = \{\{a, b\}, \{\{b\}\}, d\}.$



集合与集合

集合与集合之间的关系: \subseteq ,=, \neq , \nsubseteq , \subset , $\not\subset$

- 定义 1.1. $A \subseteq B \Leftrightarrow \forall x(x \in A \to x \in B)$.
- 定义 1.2. $A \nsubseteq B \Leftrightarrow \exists x (x \in A \land x \notin B)$.
- 定义 1.3. $A = B \Leftrightarrow \forall x(x \in A \to x \in B) \land \forall x(x \in B \to x \in A)$.
- 定义 1.4. $A \neq B \Leftrightarrow \exists x(x \in A \land x \notin B) \lor \exists x(x \in B \land x \notin A)$.
- 定义 1.5. $A \subset B \Leftrightarrow \forall x(x \in A \to x \in B) \land \exists x(x \in B \land x \notin A)$.
- **定义 1.6.** A ⊄ B ⇔?

空集、全集与幂集

定义 1.7 (空集). 空集是不含有任何元素的集合,记为 \emptyset .

定理 1.1. 空集是任何集合的子集.

证明. 给定任意集合 A, 有 $\emptyset \subseteq A \Leftrightarrow \forall x(x \in \emptyset \to x \in A)$, (根据空集定义) 恒为真.

推论 1.1. Ø 具有唯一性.

定义 1.8 (全集). 全集 (universal set) 是包含所有研究对象的集合 1 , 默认记为 U.

定义 1.9 (幂集). 幂集 (power set): $\mathcal{P}(A) = \{B \mid B \subseteq A\}$.

例子 1.1. $\mathcal{P}(\emptyset) = \{\emptyset\}, \mathcal{P}(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}, \mathcal{P}(\{a, b\}) = ?, \mathcal{P}(\{a, b, c\}) = ?.$

思考: 给定有穷集合 A,其幂集的大小 $|\mathcal{P}(A)| = 2^{|A|}$ 是否成立,幂集与二进制表示有何关联?

¹注意: 全集具有相对性, 是否为全集取决于问题设定.

集合的基本运算

初级运算

定义 2.1 (基本运算).

- 并 (union) $A \cup B = \{x \mid x \in A \lor x \in B\}.$
- $\bullet \ \ \ \ \, \hbox{$\stackrel{}{\raisebox{1.5ex}{$\scriptstyle \frown}}$} \ \ \ \, \hbox{$\stackrel{}{\raisebox{1.5ex}{$\scriptstyle \frown}}$} \ \ (\text{intersection}) \quad \ \ \, A \cap B = \{x \, | \, x \in A \wedge x \in B\}.$
- 差 (difference) $A B = \{x \mid x \in A \land x \notin B\}.$
- 补 (complement) $\overline{A} = U A$, 其中 U 为全集.
- 对称差(symmetric difference) $A \oplus B = (A-B) \cup (B-A)$.

其中,并和交运算可以推广至n个集合上,

广义并与交

定义 2.2 (广义并与交). 令 A 为一个集合的集合(其每个元素 $A \in A$ 均为集合),A 中元素的广义并(generalized union)和广义交(generalized intersection)分别被定义

- $\bigcup_{A \in \mathcal{A}} A = \{x \mid x \in A \text{ for at least one } A \in \mathcal{A}\},$ 也记为 $\cup \mathcal{A}$,
- $\bigcap_{A \in \mathcal{A}} A = \{x \mid x \in A \text{ for every } A \in \mathcal{A}\},$ 也记为 $\cap \mathcal{A}$.

例子 2.1 (广义并与交).

- $\mathcal{A} = \{\{1\}, \{1, 2\}, \{1, 2, 3\}\}, \cup \mathcal{A} = \{1, 2, 3\}, \cup \mathcal{A} = \{1\}.$
- $\mathcal{A} = \{\{a\}\}, \cup \mathcal{A} = \{a\}, \cap \mathcal{A} = \{a\}.$
- $\mathcal{A} = \{a\}, \cup \mathcal{A} = a, \cap \mathcal{A} = a.$

广义并与交的性质

- 广义并与广义交减少集合的层次 (大括号减少一层);
- 单元集 {a} 的广义并与广义交都等于 a;
- ∪∅ = ∅, ∩∅ 无定义;
- 广义并与广义交通常情况下可以转化成初级运算

例子 2.2 (广义并交运算). $A = \{\{a\}, \{a, b\}\}, \text{ 计算 } \cap \cup A \cup (\cup \cup A - \cup \cap A).$

解. 先计算 $\cup A = \{a\} \cup \{a,b\} = \{a,b\}, \cap A = \{a\} \cap \{a,b\} = \{a\}.$ 故,

广义并与交(选学)

为什么要定义广义并与交运算?

- 广义并与交在点集拓扑(point set topology)中有着广泛运用.
- 点集拓扑是研究微分流形、微分几何(黎曼几何)、李群与李代数、代数拓扑等的基础.
- 其基本研究对象是拓扑空间(topology space),我们所熟知的度量空间(metric space)的推广.
- 拓扑可以直观理解为所研究对象的组织和邻近关系,度量空间的拓扑由 metric 指定.
- 在更一般的拓扑空间中,空间的拓扑则由其上定义的开集(open set)指定.
- 一个拓扑空间的开集数量可能是(大部分情况下)无穷个,因此需要<u>广义的并和交</u>来构造其他拓扑(如子空间拓扑,乘积拓扑)结构.

广义并与交(选学)

为什么要定义广义并与交运算?

- 在前期的数学学习中,我们熟知欧式空间中开集和闭集的概念.
- n 个闭集的并集依然是闭集, n 个开集的交依然是开集.

•
$$\bigcup_{n=2}^{\infty} [1/n, 1-1/n] = ?,$$
 $\bigcap_{n=2}^{\infty} (-1/n, 1+1/n) = ?$

集合恒等式

集合恒等式

Identity	Name	
$A \cap U = A$	ldentity laws 同一律	
$A \cup \emptyset = A$		
$A \cup U = U$	Domination laws 支配律(零律)	
$A\cap\emptyset=\emptyset$		
$A \cup A = A$	Idempotent laws 幂等律	
$A \cap A = A$	idempotent laws 番号件	
$\overline{(\overline{A})} = A$	Complementation law 双重否定	
$A \cup \overline{A} = U$	Complement laws 五本律	
$A \cap \overline{A} = \emptyset$	Complement laws 互补律	

集合恒等式

Identity	Name	
$A \cup B = B \cup A$	Commutative laws 交換律 Associative laws 结合律	
$A \cap B = B \cap A$		
$A \cup (B \cup C) = (A \cup B) \cup C$		
$A \cap (B \cap C) = (A \cap B) \cap C$		
$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$	Distributive laws 分配律	
$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$	Distributive laws 为配件	
$\overline{A \cap B} = \overline{A} \cup \overline{B}$	De Mergen Javes	
$\overline{A \cup B} = \overline{A} \cap \overline{B}$	De Morgan laws	
$A \cup (A \cap B) = A$	Absorption laws 吸收律	
$A \cap (A \cup B) = A$		

集合恒等式的证明

例子 3.1 (De Morgan's laws). 证明 $\overline{A \cap B} = \overline{A} \cup \overline{B}$.

证明 *(*证明 *1)*. 首先,证明 $\overline{A \cap B} \subseteq \overline{A} \cup \overline{B}$,我们通过对任意 $x \in \overline{A \cap B}$ 则必有 $x \in \overline{A} \cup \overline{B}$ 来证明这一结论. 假设 $x \in \overline{A \cap B}$,根据集合补的定义有, $x \notin A \cap B$,即 $x \in A \land x \in B$ 为 假,亦即 $\neg (x \in A \land x \in B)$ 为真. 使用命题的 De Morgan's law,有 $\neg (x \in A)$ or $\neg (x \in B)$. 即 $x \notin A$ or $x \notin B$,亦即 $x \in \overline{A}$ or $x \in \overline{B}$. 根据集合并集的定义,有 $x \in \overline{A} \cup \overline{B}$.

然后,使用同样思路证明, $\overline{A} \cup \overline{B} \subseteq \overline{A \cap B}$. 假设 $x \in \overline{A} \cup \overline{B}$,根据集合并的定义有, $x \in \overline{A}$ or $x \in \overline{B}$,即 $x \notin A$ or $x \notin B$. 故, $\neg(x \in A) \vee \neg(x \in B)$ 为真. 使用命题的 De Morgan's law,有 $\neg(x \in A \land x \in B)$ 为真. 根据集合交的定义有, $\neg(x \in A \cap B)$ 为真,即 $x \notin A \cap B$. 根据集合补的定义有, $x \in \overline{A \cap B}$.

证毕.

集合恒等式的证明

证明 (证明 2).

$$\overline{A \cap B} = \{x \mid x \notin A \cap B\} \qquad \text{by definition of complement}$$

$$= \{x \mid \neg(x \in (A \cap B))\} \qquad \text{by definition of does not belong symbol}$$

$$= \{x \mid \neg(x \in A \land x \in B)\} \qquad \text{by definition of intersection}$$

$$= \{x \mid \neg(x \in A) \lor \neg(x \in B)\} \qquad \text{by the first De Morgan law for propositions}$$

$$= \{x \mid x \notin A \lor x \notin B\} \qquad \text{by definition of does not belong symbol}$$

$$= \{x \mid x \in \overline{A} \lor x \in \overline{B}\} \qquad \text{by definition of complement}$$

$$= \{x \mid x \in \overline{A} \cup \overline{B}\} \qquad \text{by definition of union}$$

$$= \overline{A} \cup \overline{B} \qquad \text{by meaning of set builder notation}$$

集合恒等式的证明

例子 3.2 (Distributive laws). 证明 $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$. 证明.

$$A \cup (B \cap C) = \{x \mid (x \in A) \lor (x \in B \cap C)\}$$
 by definiti
$$= \{x \mid (x \in A) \lor (x \in B \land x \in C)\}$$
 by definiti
$$= \{x \mid (x \in A \lor x \in B) \land (x \in A \lor x \in C)\}$$
 by the dis
$$= \{x \mid (x \in A \cup B) \land (x \in A \cup C)\}$$
 by definiti
$$= \{x \mid x \in (A \cup B) \cap (A \cup C)\}$$
 by definiti

by definition of union by definition of intersection by the distributive law for prop. by definition of union by definition of intersection

使用集合恒等式进行证明

在下面的例子,我们使用已经建立的集合恒等式证明或化简更一般的集合等式. **例子 3.3.** 令 A,B,C 为集合,证明 $\overline{A \cup (B \cap C)} = (\overline{C} \cup \overline{B}) \cap \overline{A}$. 证明.

$$\overline{A \cup (B \cap C)} = \overline{A} \cap (\overline{B \cap C}) \qquad \text{by the first De Morgan law}$$

$$= \overline{A} \cap (\overline{B} \cup \overline{C}) \qquad \text{by the second De Morgan law}$$

$$= (\overline{B} \cup \overline{C}) \cap \overline{A} \qquad \text{by the commutative law}$$

$$= (\overline{C} \cup \overline{B}) \cap \overline{A} \qquad \text{by the commutative law}$$

使用集合恒等式进行证明

例子 3.4. 化简 $((A \cup B \cup C) \cap (A \cup B)) - ((A \cup (B - C)) \cap A)$.

根据吸收律有,

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

= $(A \cup B) - A,$
= $B - A.$

其他集合等式

定义 3.1. 特征函数 (indicator function) $\chi: U \mapsto \{0,1\}, \ \diamondsuit \ A \subseteq U$,

$$\chi_A(x) = \begin{cases} 1, & x \in A, \\ 0, & x \notin A. \end{cases}$$

- $\chi_A = \chi_B$ 当且仅当 A = B.
- $\bullet \quad \chi_{A \cap B} = \chi_A \chi_B.$
- χ_{A⊕B} = χ_A +₂ χ_B, 其中 +₂ 定义为模 2 加法运算².

²即 a+2 $b \triangleq (a+b) \pmod{2}$.

其他集合等式

例子 3.5. 集合的对称差运算满足结合律: $(A \oplus B) \oplus C = A \oplus (B \oplus C)$.

证明. 由于 $A = B \iff \chi_A = \chi_B$,故只需证明 $\chi_{(A \oplus B) \oplus C} = \chi_{A \oplus (B \oplus C)}$.

$$\chi_{(A \oplus B) \oplus C} = \chi_{(A \oplus B)} +_2 \chi_C$$

$$= \chi_A +_2 \chi_B +_2 \chi_C$$

$$= \chi_A +_2 (\chi_B +_2 \chi_C)$$

$$= \chi_A +_2 \chi_{B \oplus C}$$

$$= \chi_{A \oplus (B \oplus C)}.$$

其中, 我们使用了模 2 加法运算的结合律.

其他集合等式

例子 3.6. 已知: $A \oplus B = A \oplus C$, 求证 B = C.

证明. 由于
$$A \oplus B = A \oplus C$$
, 故 $A \oplus (A \oplus B) = A \oplus (A \oplus C)$.

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

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

$$(A \oplus A) \oplus C$$

$$\Rightarrow \emptyset \oplus B = \emptyset \oplus C$$

$$\Rightarrow B = C$$
.

associativity of set \oplus

definition of set \oplus

容斥原理(inclusion-exclusion principle)

1. 令 A_1, A_2 为集合,从 Venn 图可以观察到如下结论:

$$|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|.$$

2. 对于三个集合 A_1, A_2, A_3 , 可以的到:

$$|A_1 \cup A_2 \cup A_2| = |A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_1 \cap A_3| - |A_2 \cap A_3| + |A_1 \cap A_2 \cap A_3|.$$

3. 该结论可以推广至 n 个集合,

$$\bigcup_{i=1}^{n} A_{i} = \sum_{i_{1}} |A_{i_{1}}| - \sum_{i_{1} < i_{2}} |A_{i_{1}} \cap A_{i_{2}}| + \sum_{i_{1} < i_{2} < i_{3}} |A_{i_{1}} \cap A_{i_{2}} \cap A_{i_{3}}| \dots
+ (-1)^{n-1} |A_{1} \cap A_{2} \cap \dots \cap A_{n}|,$$

$$= \sum_{k=1}^{n} (-1)^{k-1} \sum_{1 \le i_{1} < i_{2} < \dots < i_{k} \le n} |A_{i_{1}} \cap A_{i_{2}} \cap \dots \cap A_{i_{k}}|.$$

容斥原理(inclusion-exclusion principle)

定理 4.1 (容斥原理). 令 U 为全集, A_1, A_2, \ldots, A_n 为其子集, 则

$$\bigcup_{i=1}^{n} A_i = \sum_{k=1}^{n} (-1)^{k-1} \sum_{1 \le i_1 < i_2 < \dots < i_k \le n} |A_{i_1} \cap A_{i_2} \cap \dots \cap A_{i_k}|,$$

推论 4.1. 令 U 为全集, $A_1, A_2, ..., A_n$ 为其子集, 则

$$|\overline{A}_1 \cap \overline{A}_2 \cap \ldots \cap \overline{A}_n| = |U| + \sum_{k=1}^n (-1)^k \sum_{1 \le i_1 < i_2 < \ldots < i_k \le n} |A_{i_1} \cap A_{i_2} \cap \ldots \cap A_{i_k}|, \quad 1 \le i_1, i_k \le n.$$

证明. 使用定理证明, 留作练习.

例子 4.1. 求 1 到 1000 (包含 1 和 1000) 不能同时被 5, 6, 8 整除的整数个数. 定义如下集合.

$$U = \{x \mid x \in \mathbb{Z}, 1 \le x \le 1000\},\$$

$$A_1 = \{x \mid x \in U, x \equiv 0 \pmod{5}\},\$$

$$A_2 = \{x \mid x \in U, x \equiv 0 \pmod{6}\},\$$

$$A_3 = \{x \mid x \in U, x \equiv 0 \pmod{8}\}.$$

问题所求数即为 $|\overline{A}_1 \cap \overline{A}_2 \cap \overline{A}_3|$.

$$|A_1| = \lfloor 1000/5 \rfloor = 200, \ |A_2| = \lfloor 1000/6 \rfloor = 166, \ |A_3| = \lfloor 1000/8 \rfloor = 125,$$
 $|A_1 \cap A_2| = \lfloor 1000/ \operatorname{lcm}(5,6) \rfloor = 33, \ |A_1 \cap A_3| = \lfloor 1000/ \operatorname{lcm}(5,8) \rfloor = 25,$ $|A_2 \cap A_3| = \lfloor 1000/ \operatorname{lcm}(6,8) \rfloor = 41, \ |A_1 \cap A_2 \cap A_3| = \lfloor 1000/ \operatorname{lcm}(5,6,8) \rfloor = 8.$ 根据推论4.1, $|\overline{A}_1 \cap \overline{A}_2 \cap \overline{A}_3| = 1000 - (200 + 166 + 125) + (33 + 25 + 41) - 8 = 600.$

例子 4.2. 欧拉函数 $\phi(n)$ 表示 $1,2,\ldots,n-1$ 中与 n 互素数的个数,定义 $\phi(1)=1$. 由于与 12 互素的数有 1,5,7,11,故 $\phi(12)=4$;同理, $\phi(13)=12$. 假定整数有如下素因子分解

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k},$$

试计算 $\phi(n)$ 的通项公式.

定义如下集合,

$$U = [n-1],$$

$$A_i = \{x \mid x \in U, x \equiv 0 \pmod{p_i}\}$$

则
$$\phi(n) = |\overline{A}_1 \cap \overline{A}_2 \cap \ldots \cap \overline{A}_k|$$
.

$$|A_i| = \frac{n}{p_i}, \quad i = 1 \le i \le k.$$

$$|A_i \cap A_j| = \frac{n}{p_i p_i}, \quad 1 \le i \le n.$$

. . .

根据推论4.1,

$$\phi(n) = n - \left(\frac{n}{p_1} + \frac{n}{p_2} + \dots + \frac{n}{p_k}\right) + \left(\frac{n}{p_1 p_2} + \frac{n}{p_1 p_3} + \dots + \frac{n}{p_{k-1} p_k}\right) \dots + (-1)^k \frac{n}{p_1 p_2 \dots p_k}$$

$$= n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_k}\right).$$

实例:

- $\phi(60) = 60 \left(1 \frac{1}{2}\right) \left(1 \frac{1}{3}\right) \left(1 \frac{1}{5}\right) = 60 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} = 16.$
- 与 60 互素的正整数有: 1,7,11,13,17,19,23,29,31,37,41,43,47,49,53,59.

组合计数 (选学)

• 在计算机的算法设计与分析中,我们经常会碰到递推关系(recurrence relations),

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \ldots + c_k a_{n-k}, \quad c_k \in \mathbb{R}, c_k \neq 0.$$

- 被称为线性齐次递推(linear homogeneous recurrence)关系.
- Fibonacci 序列 $f_n = f_{n-1} + f_{n-2}$, $f_0 = 0, f_1 = 1$, 如何计算其通项 f_n ?

组合计数 (选学)

线性齐次递推关系可以转化为矩阵表示,以 Fibonacci 序列为例,

$$\begin{bmatrix} f_{n+1} \\ f_n \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} f_n \\ f_{n-1} \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^2 \begin{bmatrix} f_{n-1} \\ f_{n-2} \end{bmatrix} = \dots = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^n \begin{bmatrix} f_1 \\ f_0 \end{bmatrix}$$

- 令变换矩阵为 A,则我们仅需计算出 A^n ,如何快速计算 A^n ?
- 回忆矩阵 eigenvector 和 eigenvalue 的定义, Av = λv.
- 如果矩阵 **A** 存在两个线性独立的 eigenvectors $\mathbf{v}_1, \mathbf{v}_2$,则矩阵可以对角化.

$$\mathbf{A}[\mathbf{v}_1 \, \mathbf{v}_2] = [\mathbf{v}_1 \, \mathbf{v}_2] egin{bmatrix} \lambda_1 & & \\ & \lambda_2 \end{bmatrix} \quad \text{or} \quad \mathbf{AP} = \mathbf{PD}$$

 $A^n = \mathbf{P} \mathbf{D}^n \mathbf{P}^{-1}.$

组合计数 (选学)

■ 求解特征方程(characteristic equation). $\diamondsuit f_n = r^n$,带入 Fibonacii 递推关系,

$$r^n = r^{n-1} + r^{n-2}.$$

假设 r≠0,则有

$$r^2 = r + 1 \iff r^2 - r - 1 = 0.$$

• 特征方程存在根 $r_1 = (1 + \sqrt{5})/2$, $r_2 = (1 - \sqrt{5})/2$. 由递推关系的线性可知,

$$f_n = \alpha_1 \left(\frac{1+\sqrt{5}}{2}\right)^n + \alpha_2 \left(\frac{1-\sqrt{5}}{2}\right)^n$$

■ 使用初始条件 $f_0 = 0, f_1 = 1$ 计算出系数 α_1, α_2 .

组合计数(选学)

- 生成函数 (generating function) 是复杂组合计数问题的有效求解工具(通用、简洁).
- 阅读推荐教材第8章, Advanced Counting Techniques.
- 生成函数与复数,
 - Find the number of subsets of $\{1, 2, \dots, 2000\}$, the sum of whose elements is divisible by 5.
 - 3Blue1Brown Olympiad level counting.
- 生成函数专著 generatingfunctionology.

作业

指定教材习题 6.

- **4**
- **8**-(4), 8-(5), 8-(6)
- **9**-(5)
- **15-(2)**
- **18-(4)**
- **2**1
- **30-(3)**, 30-(4)
- **3**5