Discrete Mathematics

Lecture 1

Lets Count!

史灵生
清华数学系

math

- Continuous (infinite)
  - Analysis
  - Real analysis
  - Complex analysis
  - Functional analysis
  - Math physics …
- Discrete (finite)
  - Algebra
  - Combinatorics
  - Graph theory
  - Number theory
  - Set theory …

序言

- 离散数学是一个迷人的数学分支，它起源于古代的游戏和美学鉴赏.
- 在现代科学技术的发展中，人们会面临各种各样的离散数学问题.
- 离散数学在计算机科学中发挥着极为重要的作用.

- 离散数学的发展道路是坎坷不平的，主要是受连续数学的传统影响.
- 现在离散数学这个领域无论广度、深度，还是成果的重要性上都急剧的增长，使得那些“纯”数学家大为震惊.
- 计算机科学是研究算法的一门科学，在算法的研究中，必须要对算法所需要的计算量和存储单元做出估计，这就是计算的时间复杂性和空间复杂性分析，这些计算都离不开离散数学.

- 目前， 离散数学已经被广泛应用于计算机科学、管理科学、信息科学、电子工程、人工智能、生命科学等诸多领域中.
- 这一讲我们先介绍集合，以后再深入讨论学习离散数学.
- 学习建议：预习！

1.2 集

一、集合的基本概念

- **集合**是一些确定的、作为整体识别的、互相区别的对象的总体。
- 组成集合的对象称为集合的**成员**（*member*）或**元素**（*element*）。
- 一般用大写字母表示集合，用小写字母表示元素。
- 例如：A表示一个集合，a表示元素，

Really?

Let's see the Russell Paradox:

- **集合**是一些确定的、作为整体识别的、互相区别的对象的总体。

Let $A = \{a \mid a \notin a\}$.

Clearly, $A \in A \Leftrightarrow A \notin A$.

What should we do?

"Easy", just rule out $x \in x$!

- 如果*a*是*A*的元素，记为：$a \in A$，读作“*a*属于*A*”、“*a*是*A*的元素”、“*a*是*A*的成员”、“*a*在*A*之中”、“*A*包含*a*”。
- 如果*a*不是*A*的元素，记为：$a \notin A$，读作“*a*不属于*A*”。
- 空集∅和只含有有限多个元素的集合称为**有限集**（*finite sets*），否则称为**无限集**（*infinite sets*）。有限集合中元素的个数称为集合的**基数**（*cardinality*）
- 集合*A*的基数表示为 $|A|$。

二、集合的表示方式有三种：

1. 列举法

将集合的元素列举出来。

2. 描述法

利用一项规则（一个公式），描述集合中的元素的共同性质，以便决定某一物体是否属于该集合。

3. 归纳法

用递归方法定义集合。

一、列举法：将集合的元素列举出来

例：$A = \{a，b，c，d\}$，

$Odd = \{1，3，5，7，9，\ldots\}$

使用列举法，须列出足够多的元素以反映集合中成员的特征。如：

$B = \{2，4，8，\ldots\}$

若$x = 2^n$，则

$B=\{2，4，8，16，32，\ldots\}$

若$x = 2 + n(n-1)$，则

$B=\{2，4，8，14，22，\ldots\}$

二、描述法：$A=\{x: P(x)\}$或$A=\{x \mid P(x)\}$

例： $C=\{x\in\mathbb{R} \mid 1\le x\le 5\}$,

$D=\{(x, y) \mid x^2+y^2\le 1, x, y\in\mathbb{R}\}$,

$F=\{x \mid x$是中国的一个省$\}$,

$\mathbb{N}=\{n\in\mathbb{Z}: n>0\}$,

$\mathbb{Z}_+=\{n\in\mathbb{Z}: n\ge 0\}$，…

说明：

1、$C = \{x\in\mathbb{R} \mid 1 \le x \le 5\} = \{y\in\mathbb{R} \mid 1\le y\le 5\}$

表示同一个集合。

2、集合中元素是无序的：

$\{a，b，c\}=\{b，c，a\}=\{c，a，b\}$。

3、集合中的元素可能也是集合，例：

$A=\{1, 2, \{1\}, \{1，2，3\}\}$，$1\in A$，$\{1\}\in A$。

三、集合的关系

相等(外延性公理)：两个集合是相等的，当且仅当它们有相同的元素。

两个集合A和B相等，记作$A = B$，两个集合不相等，记作$A \neq B$。

$\{0，1\} = \{x \mid x(x^2 - 2x + 1) = 0\}$

$\{0，1\} \neq \{1，2\}$

注：$A = B \Leftrightarrow \forall x(x \in A \Leftrightarrow x \in B)$

定义 设A、B是任意两个集合，如果A的每一个元素都是B的元素，则称集合A是集合B的**子集合**（或**子集**，*subset*），或称A包含在B内，记为$A \subseteq B$；或称B包含A，记为$B \supseteq A$，

即$A \subseteq B \Leftrightarrow \forall x(x \in A \Rightarrow x \in B)$; 若还有$A \neq B$，则称$A$是$B$的**真子集**，记为$A \subset B$。

设A，B，C为任意集合，包含关系具有：

- 自反性：$A \subseteq A$;
- 传递性：若$A \subseteq B$且$B \subseteq C$，则$A \subseteq C$;
- 反对称性：$A = B \Leftrightarrow A \subseteq B$且$B \subseteq A$。

满足这三条性质的关系被称为偏序关系。

注：可能$A \subseteq B$或$B \subseteq A$，也可能两者均不成立，不是两者必居其一。

数集：$\varnothing \subset \mathbb{N} \subset \mathbb{Z}_{+} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$.

四、特殊的集合

空集(empty sets)

定义：不含任何元素的集合称为空集，

记作$\varnothing$。

例如：$\{x \in \mathbb{R}：x^2+1=0\} = \varnothing$。

注意：$\varnothing \in \{\varnothing\}$，$\varnothing \neq \{\varnothing\}$。

定理：对于任意一个集合A，$\varnothing \subseteq A$。

证明：反证法，假设存在一个集合A，使得$\varnothing \subseteq A$为假。则存在$x \in \varnothing$且$x \notin A$，这与空集的定义矛盾，所以$\varnothing \subseteq A$，空集是任意集合的子集。

推论：空集是唯一的。

证明：设$\varnothing_1$，$\varnothing_2$是两个空集，则$\varnothing_1 \subseteq \varnothing_2$，$\varnothing_2 \subseteq \varnothing_1$，得$\varnothing_1=\varnothing_2$，所以空集是唯一的。

例：$A=\{a, \varnothing\}$，判断下列结论是否正确。

1）$\varnothing \in A$，　2）$\varnothing \subseteq A$，　3）$\{\varnothing\} \subseteq A$，
4）$\{\varnothing\} \in A$，5）$a \in A$，　6）$a \subseteq A$，
7）$\{a\} \in A$，　8）$\{a\} \subseteq A$。

结论（1）、（2）、（3）、（5）、（8）正确。

集合的运算及其性质

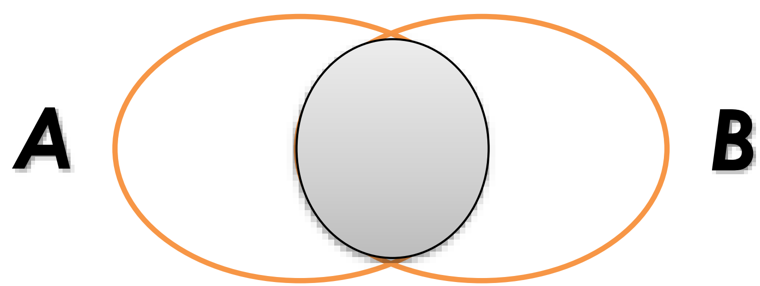
1、交（intersection）：∩
2、并（union）：∪
3、差（difference）：\
4、补（complement）：c
5、对称差（symmetric difference）△

1、交（intersection）

定义：设任意两个集合*A*和*B*，由*A*和*B*的所有共同元素组成的集合，称为*A*和*B*的**交集**，记为$A \cap B$，

$$A \cap B = \{x \mid x \in A \land x \in B\}。$$

The Venn diagram:



例1：设A是平面上所有矩形的集合，B是平面上所有菱形的集合，则$A \cap B$是所有正方形的集合。

例2：设A是所有能被k整除的整数的集合，B是所有能被l整除的整数的集合，则$A \cap B$是所有能被k与l最小公倍数整除的整数的集合。

性质：

a) $A \cap A = A$

b) $A \cap \varnothing = \varnothing$

c) $A \cap B = B \cap A$

d) $(A \cap B) \cap C = A \cap (B \cap C)$

e) $A \cap B \subseteq A$， $A \cap B \subseteq B$

例3 设$A \subseteq B$，求证$A \cap C \subseteq B \cap C$。

思路：对任一$x \in A \cap C$，有$x \in A$且$x \in C$，

因为若$x \in A$，则$x \in B$，

所以$x \in B$且$x \in C$，故$x \in B \cap C$。

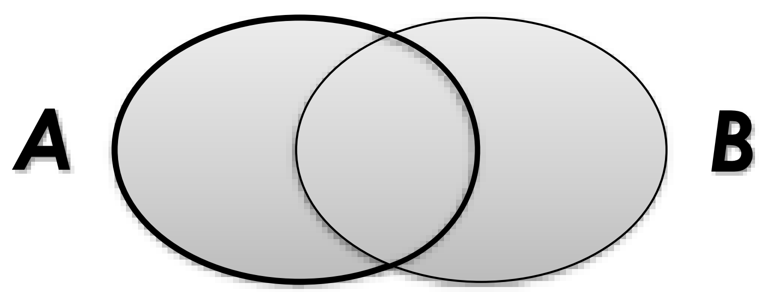
因此$A \cap C \subseteq B \cap C$。

2、并集（union）

定义：设任意两个集合*A*和*B*，所有属于*A*或属于*B*的元素组成的集合，称为*A*和*B*的并集，记作$A \cup B$。

$$A \cup B = \{x \mid x \in A \lor x \in B\}$$

The Venn diagram:



例1 设A是奇数集合，B是偶数集合，则 $A \cup B = \mathbb{Z}$，$A \cap B = \varnothing$。

性质：

a) $A \cup A = A$

b) $A \cup \varnothing = A$

c) $A \cup B = B \cup A$

d) $(A \cup B) \cup C = A \cup (B \cup C)$

e) $A \subseteq A \cup B$，$B \subseteq A \cup B$

例2 设$A \subseteq B$，$C \subseteq D$，求证$A \cup C \subseteq B \cup D$。

思路：对任一$x \in A \cup C$，则$x \in A$或$x \in C$，

若$x \in A$，则$x \in B$，故$x \in B \cup D$；

若$x \in C$，则$x \in D$，故$x \in B \cup D$。

因此$A \cup C \subseteq B \cup D$。

定理 设A，B，C为三个集合，则下列分配律成立。

a) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

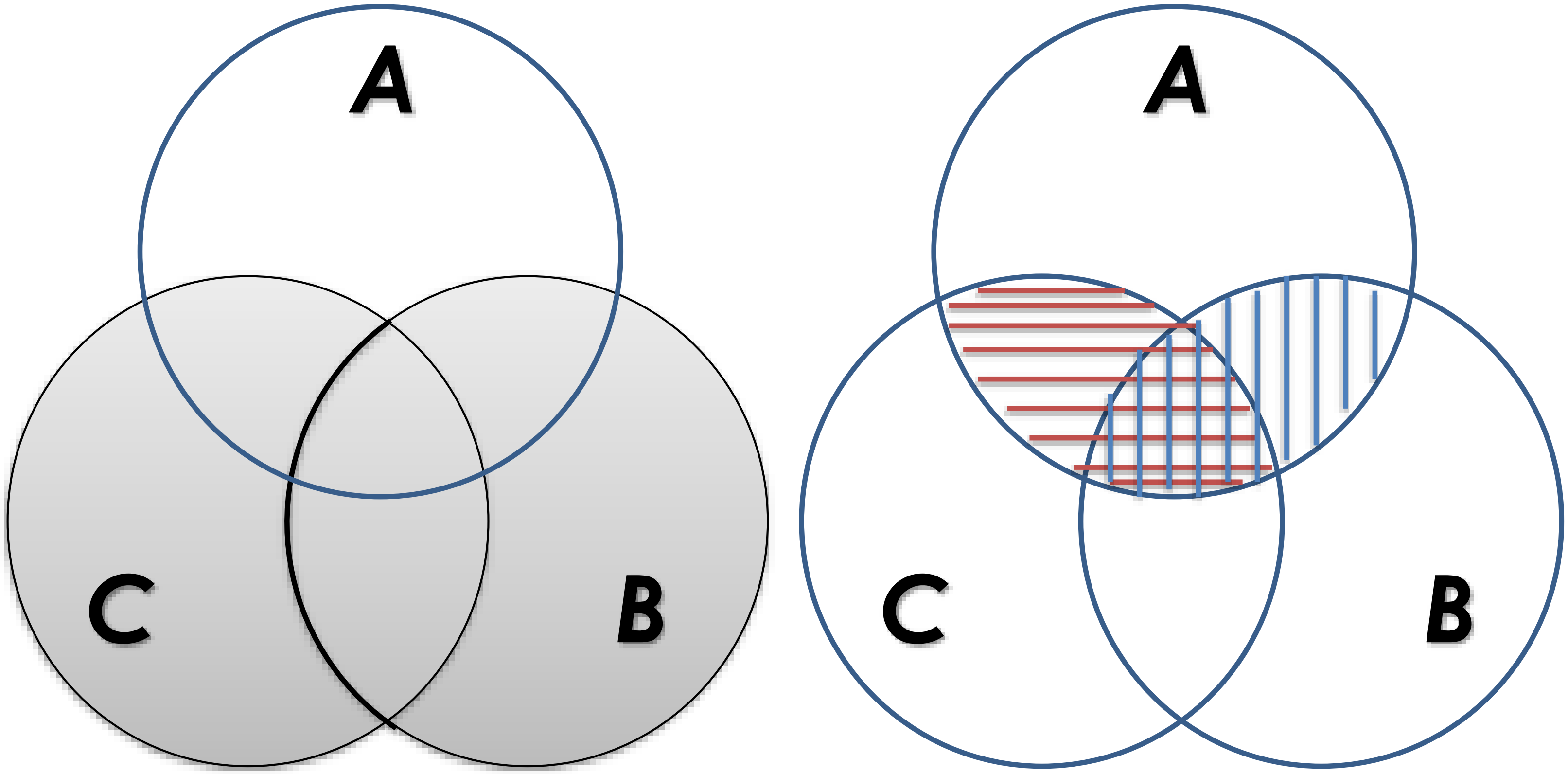
b) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

a) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

思路：设$S = A \cap (B \cup C)$，$T=(A \cap B) \cup (A \cap C)$，
若$x \in S$，则$x \in A$且$x \in B \cup C$，即$x \in A$且 $x \in B$或 $x \in A$且 $x \in C$，
$x \in A \cap B$或$x \in A \cap C$即$x \in T$，所以$S \subseteq T$。
反之，若$x \in T$，则$x \in A \cap B$或$x \in A \cap C$， $x \in A$且 $x \in B$或 $x \in A$且 $x \in C$，即$x \in A$且$x \in B \cup C$，于是$x \in S$，所以$T \subseteq S$。
因此，$S = T$。

b)证明完全与a)类似。

a) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$



The Venn diagram of three sets

定理 设A，B为任意两个集合，则下列吸收律成立。

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

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

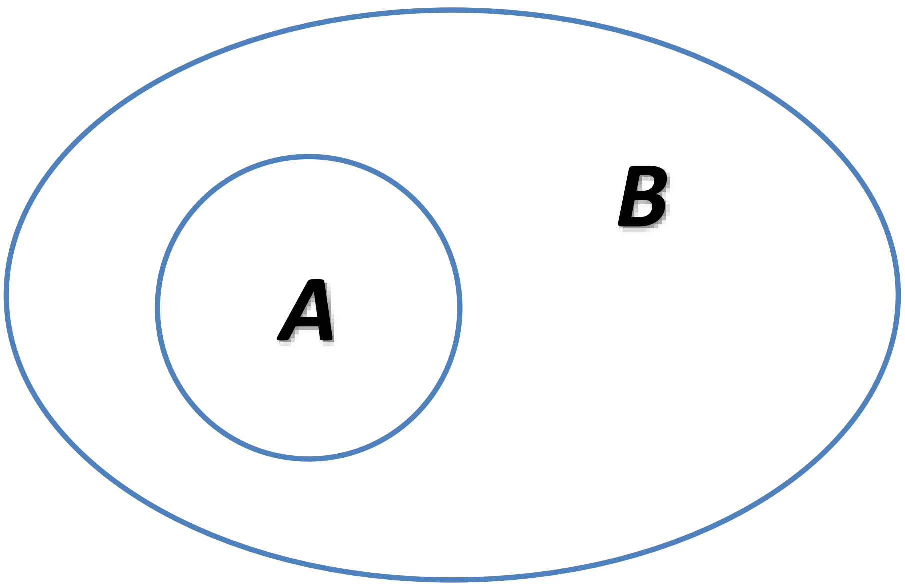
证明思路：

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

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

定理 $A\subseteq B \Leftrightarrow A\cup B = B \Leftrightarrow A\cap B = A$。

思路：若$A\subseteq B$，则$A\cup B\subseteq B\subseteq A\cup B$。
反之，若$A\cup B = B$，则$A\subseteq A\cup B = B$。
同理可证得$A\cap B = A$。

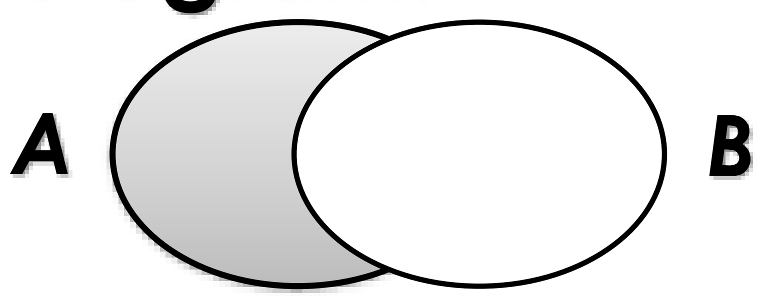


3、差集（difference）

定义：设*A*、*B*是任意两个集合，所有属于*A*而不属于*B*的元素组成的集合称为*A*和*B*差集，(或*B*对*A*的补集，或相对补)记作$A \setminus B$。

$$A \setminus B = \{x \mid x \in A \wedge x \notin B\}$$

The Venn diagram:

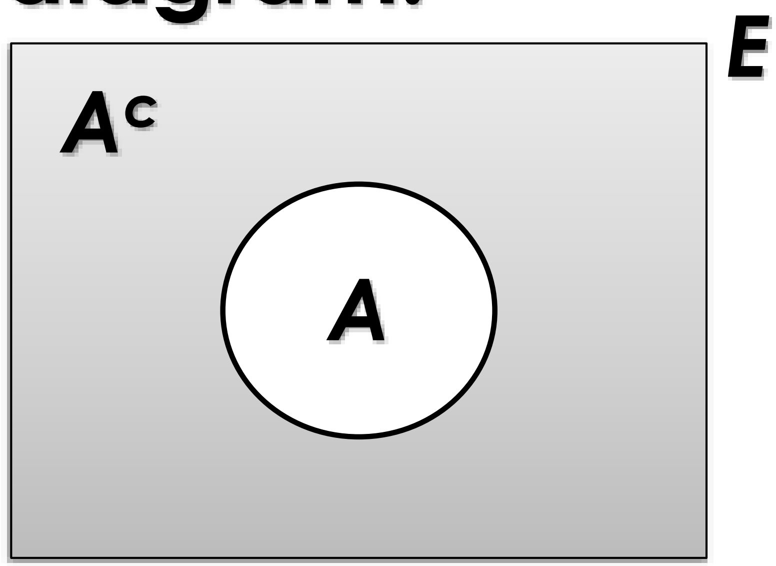


4、补集(complement)

定义：设E为全集，任一集合A对E的补，称为A的绝对**补**，记作A^c。

$$A^c = E \setminus A = \{x \mid x \in E \wedge x \notin A\}$$

The Venn diagram:



性质：

a) $(A^c)^c = A$

b) $E^c = \varnothing$

c) $\varnothing^c = E$

d) $A \cup A^c = E$

e) $A \cap A^c = \varnothing$

定理 设A，B为任意两个集合，则下列关系式成立。

a) $(A\cup B)^c = A^c \cap B^c$

b) $(A\cap B)^c = A^c \cup B^c$

c) $A\setminus B = A\cap B^c$

d) $A\setminus B = A\setminus(A\cap B)$

定理 设A，B，C为三个集合，则

$A\cap(B\setminus C) = (A\cap B)\setminus(A\cap C)$.

定理 设A，B为任意两个集合，若$A\subseteq B$，则

a) $B^c \subseteq A^c$

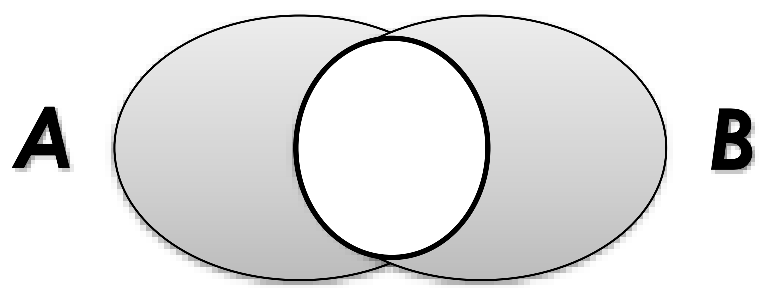
b) $(B\setminus A)\cup A = B$.

5、对称差(symmetric difference)

定义：设*A*、*B*是任意两个集合，集合*A*和*B*的对称差，其元素或属于*A*，或属于*B*，但不能既属于*A*又属于*B*，记作$A \triangle B$。

$$A \triangle B = (A \setminus B) \cup (B \setminus A)$$

The Venn diagram:



性质：

a) $A \triangle B = B \triangle A$

b) $A \triangle \varnothing = A$

c) $A \triangle A = \varnothing$

d) $A \triangle B = (A \cap B^c) \cup (A^c \cap B)$

e) $(A \triangle B) \triangle C = A \triangle (B \triangle C)$

1.3 幂集的基数

定义：给定集合A，由A的所有子集为元素组成的集合称为A的**幂集**，记作$\wp(A)$或2^A。

$$\wp(A) = \{S \mid S \subseteq A\}$$

例：$2^{\varnothing} = \{\varnothing\}$，$|2^{\varnothing}| = 1$；

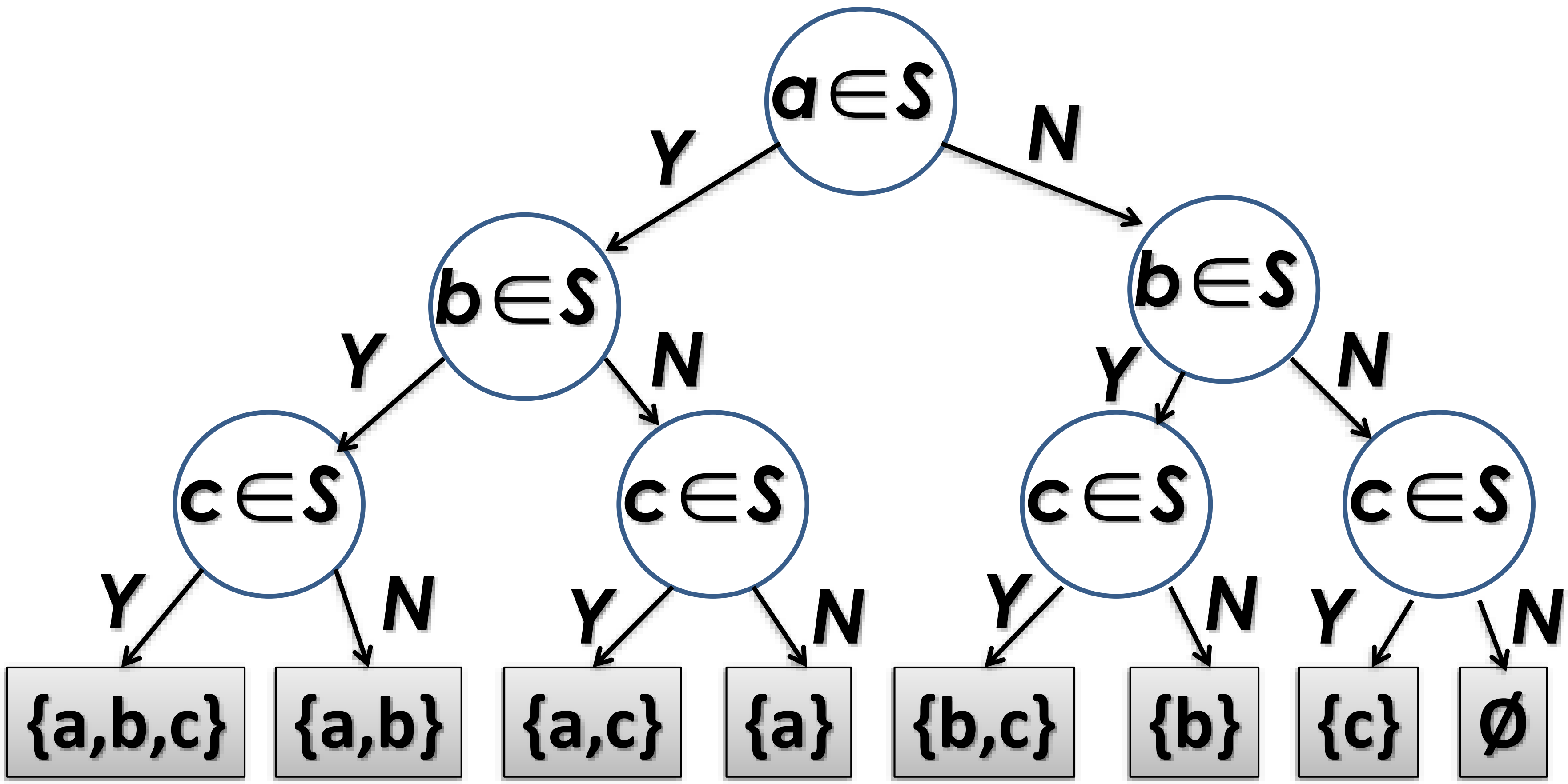
$2^{\{a\}} = \{\varnothing，\{a\}\}$，$|2^{\{a\}}| = 2$；

$2^{\{a,b\}} = \{\varnothing，\{a\}，\{b\}，\{a,b\}\}$，$|2^{\{a,b\}}| = 2^2$；

设$A = \{a，b，c\}$，则A的幂集：

$2^A = \{\varnothing，\{a\}，\{b\}，\{c\}，\{a，b\}，\{a，c\}，\{b，c\}，\{a，b，c\}\}$，$|2^A| = 2^{|A|} = 2^3 = 8.$

定理1.3.1 如果有限集*A*有*n*个元素，则其幂集有2^n个元素。



Encoding

$0 \Leftrightarrow 000 \Leftrightarrow \varnothing$

$1 \Leftrightarrow 001 \Leftrightarrow \{\ ,\ ,c\}$

$2 \Leftrightarrow 010 \Leftrightarrow \{\ ,b,\ \}$

$3 \Leftrightarrow 011 \Leftrightarrow \{\ ,b,c\}$

$4 \Leftrightarrow 100 \Leftrightarrow \{a,\ ,\ \}$

$5 \Leftrightarrow 101 \Leftrightarrow \{a,\ ,c\}$

$6 \Leftrightarrow 110 \Leftrightarrow \{a,b,\ \}$

$7 \Leftrightarrow 111 \Leftrightarrow \{a,b,c\}$

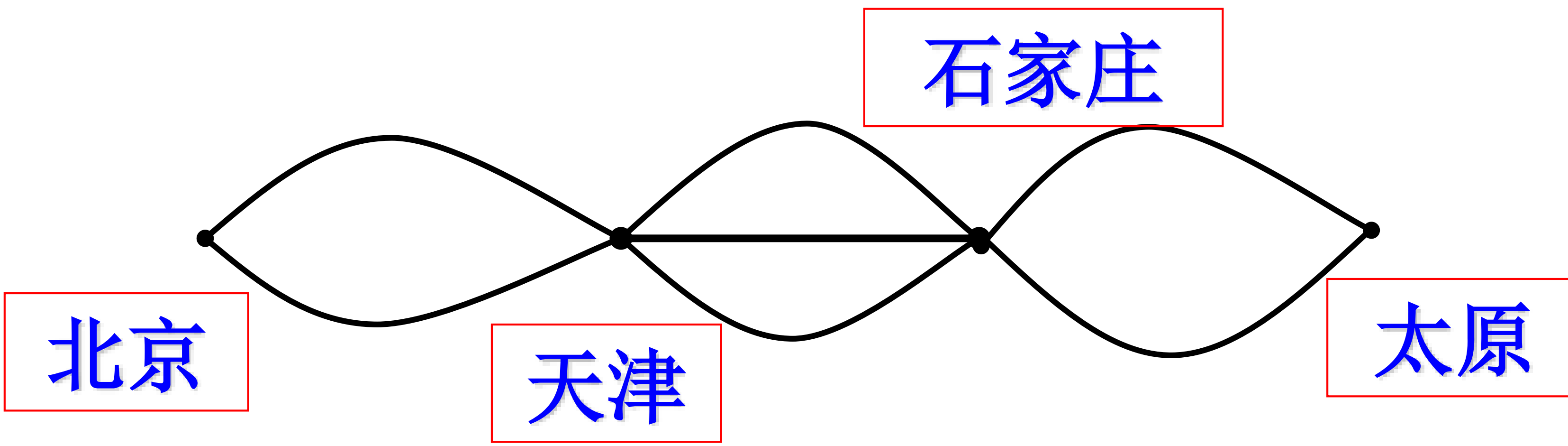
1.5 Sequences

Theorem 1.5.1 The number of strings of length n composed of k given elements is k^n.

定理1.5.2（乘法原理） 设事件A_1有k_1种产生方式, 事件A_2有k_2种产生方式, …, 事件A_n有k_n种产生方式，则事件$A_1,A_2,\ldots,A_n$依次接连产生共有$k_1k_2\cdots k_n$种不同方式.

注意: 这里的事件$A_1,A_2,\ldots,A_n$必须是互相独立的.

例 如果从北京到天津有2条道路可供选择, 从天津到石家庄有3条道路可供选择, 从石家庄到太原有2条道路可供选择, 问从北京经天津、石家庄到太原有多少条道路可供选择?



例 从1000到9999的整数中, 问(1)含有5的数有多少个? (2)含有多少个百位和十位数均为奇数的偶数? (3)各位数都不相同的奇数有多少个?

解 设有数字集合{0,1,2,3,4,5,6,7,8,9}.

(1) 先求不含5的整数的个数. 这时候个位数字, 十位数字和百位数字各有9种选择, 而千位数字只有8种选择, 所以不含5的整数的个数 $=8\times9\times9\times9=5832$, 从1000到9999共有9000个整数, 所以含有5的整数 $=9000-5832=3168$ 个.

例 从1000到9999的整数中, 问(1)含有5的数有多少个? (2)含有多少个百位和十位数均为奇数的偶数? (3)各位数都不相同的奇数有多少个?

解 设有数字集合{0,1,2,3,4,5,6,7,8,9}.

(2) 当个位数字为0,2,4,6,8的时候对应的该整数为偶数, 因此个位数有5种选择, 十位数字和百位数字各有5种选择,而千位数字有9种选择, 故含有百位和十位数均为奇数的偶数 $= 9\times5\times5\times5 = 1125$个.

例 从1000到9999的整数中, 问(1)含有5的数有多少个? (2)含有多少个百位和十位数均为奇数的偶数? (3)各位数都不相同的奇数有多少个?

(3)当个位数为1,3,5,7,9的时候对应整数为奇数. 如果要求各位数都不相同, 则个位数有5种选择, 当个位数选定之后, 千位数只有8种选择, 而当千位数选择之后, 百位数可以有8种选择, 以上三位数都选定之后,剩下的十位数就只有7种选择了. 所以, 各位数字都不相同的奇数 $= 8\times8\times7\times5 = 2240$个.

1.6-8 排列与组合

定义1.1 从n个不同的元素中，取k个并按次序排列，称为从n中取k个的一个**排列**，全部这样的排列数记为$P(n, k)$.

若$k = n$，则称为n个元素的一个**置换**(permutation)，且$P(n, n) = n!$。

定义1.2 从n个不同的元素中, 取k个但是不考虑次序时候, 称为从n中取k个的一个**组合**, 全部这样的组合总数记为$C(n, k)$.

Theorem 1.7.1 $P(n, k) = n!/(n - k)!$.

Theorem 1.8.1 $C(n, k) = n!/[k!(n - k)!]$.

Theorem 1.8.2

(1) $C(n, k) = C(n, n - k)$;

(2) $C(n-1,k-1)+C(n-1,k)=C(n,k)$ for $n>k>0$;

(3) $C(n, 0) + C(n, 1) + \cdots + C(n, n) = 2^n$.

证明 (3):

一般地，如果$|A| = n$，则A的〇元子集有$C(n, 0) = 1$个，即空集$\varnothing$,

1元子集有$C(n, 1)$个,

2元子集有$C(n, 2)$个，…,

$n - 1$元子集有$C(n, n - 1)$个,

n元子集有$C(n, n)$个。

所以A的子集个数为:

$C(n, 0) + C(n, 1) + \cdots + C(n, n) = 2^n$。

例 由字母a, b, c, d, e, f所组成4个字母的“单词”, 问: (1) 如果每个字母在“单词”中至多出现一次, 这样的单词个数有多少? (2)如果字母允许重复可组成多少个单词?

解 (1) 每个字母在单词中至多出现一次, 其单词个数 $= P(6, 4) = 6!/(6-4)! = 360$.

(2) 如果字母允许重复可组成的单词个数为$6^4 = 1296$.

例 从{1, 2, 3, 4, 5, 6, 7, 8, 9}中选取不同的数字且使4, 5, 6不相邻的7位数有多少个？（这里不相邻是指不出现4, 5, 6的任意一个排列）

解 先算4, 5, 6相邻的7位数的个数。7位数中的7位数字，除4, 5, 6外还有4位数字，应该从{1, 2, 3, 7, 8, 9}中选取，可以有P(6, 4)种选取方式。若用“♥”来表示这4位数字，而4, 5, 6相邻则用“♣”来表示，则♣共有下列5种可能的位置：♣♥♥♥♥，♥♣♥♥♥，♥♥♣♥♥，♥♥♥♣♥，♥♥♥♥♣。

由于4, 5, 6的全排列数 = 3! = 6, 因此4, 5, 6相邻的7位数的个数=$6\times5\times P(6, 4)$=10800.
这样4, 5, 6不相邻的7位数的个数为:

$$P(9, 7) - 6\times5\times P(6, 4)$$

$$=181440 - 10800 = 170640.$$