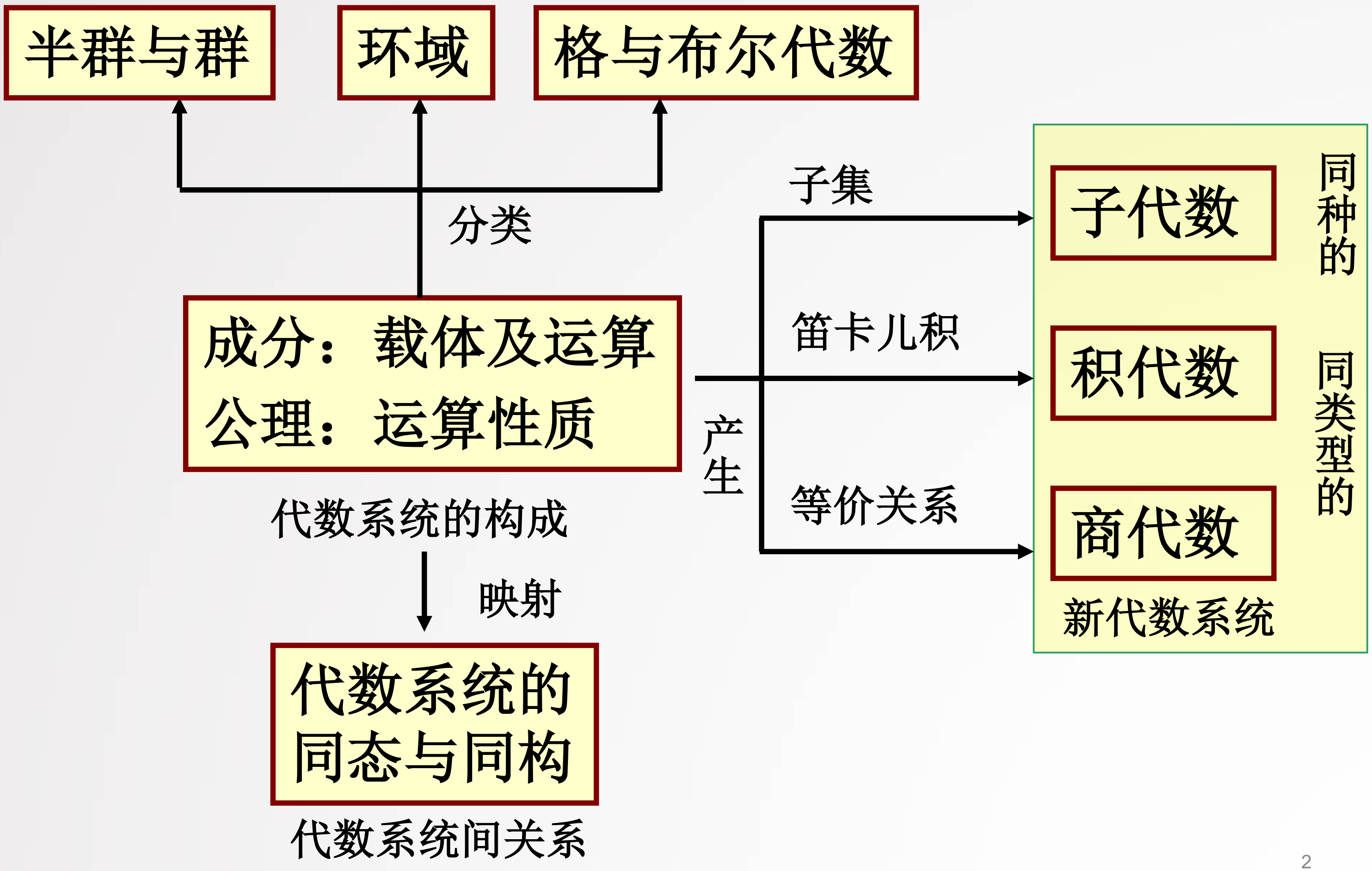
课程小结

代数结构与组合数学

代数系统的知识点

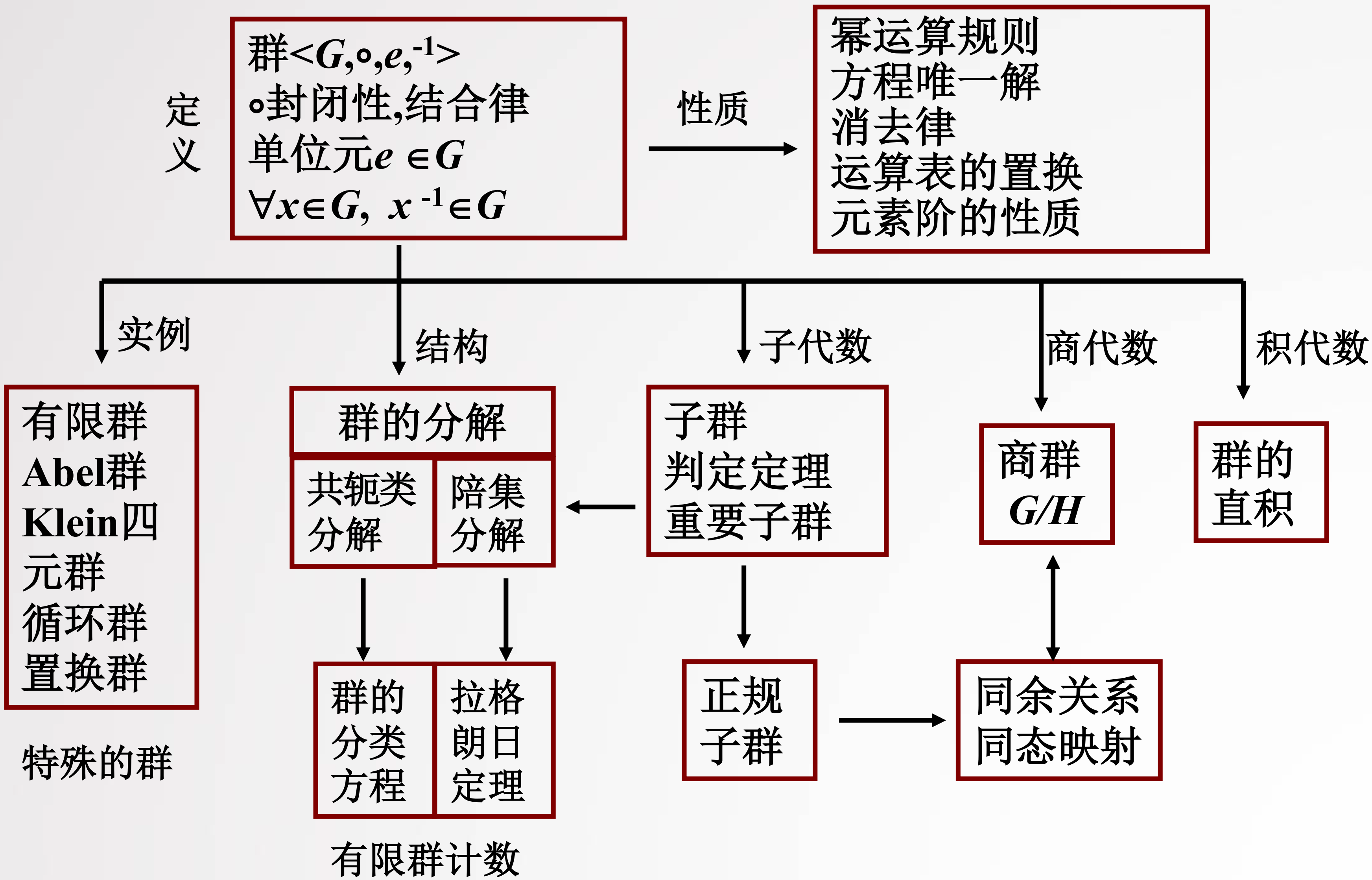


半群与群
环域
格与布尔代数
分类
成分：载体及运算
公理：运算性质
代数系统的构成
映射
代数系统的同态与同构
代数系统间关系
产生
子集
笛卡儿积
等价关系
子代数
积代数
商代数
同种的
同类型的
新代数系统

要求

1. 给定集合和运算，判断代数系统的构成
2. 判断运算的性质——算律及特异元素
3. 求子代数、积代数、商代数
4. 同态与同构映射的概念、性质及构造、几种典型的同态或同构的定义、同态基本定理

群的知识点



定义
群$<G,\circ,e,^{-1}>$
$\circ$封闭性,结合律
单位元$e\in G$
$\forall x\in G,\ x^{-1}\in G$
性质
幂运算规则
方程唯一解
消去律
运算表的置换
元素阶的性质
实例
结构
子代数
商代数
积代数
有限群
Abel群
Klein四元群
循环群
置换群
特殊的群
群的分解
共轭类分解
陪集分解
群的分类方程
拉格朗日定理
有限群计数
子群
判定定理
重要子群
正规子群
商群
G/H
同余关系
同态映射
群的直积

证明群或者子群

证明群: 验证下述条件之一

(1) 封闭性、结合律、单位元、每个元素有逆

(2) 封闭性、结合律、右单位元、每个元素有右逆

(3) 封闭性、结合律、方程有解

(4) 封闭性、结合律、有限、无零元、消去律

证明 H 是 G 的子群: 判定定理

前提：H 是 G 的非空子集 (进行验证)

验证下述条件之一

(1) $\forall x, y \in H,\ xy \in H, x^{-1} \in H.$

(2) $\forall x, y \in H,\ xy^{-1} \in H$

(3) H 有限，$\forall x, y \in H,\ xy \in H$

证明正规性或者同态

证明子群 N 的正规性

验证下述条件之一：

(1) $\forall g \in G,\ n \in N,\ gng^{-1} \in N$

(2) $\forall g \in G,\ gNg^{-1} = N$

(3) $|N| = t,\ N$ 是 G 的唯一的 t 阶子群

(4) $[G : N] = 2$

证明 f 是 G_1 到 G_2 的同态

(1) 验证 $f: G_1 \to G_2$（注意良定义性的验证）

(2) 验证 $\forall x, y \in G_1,\ f(x\,y) = f(x)\,f(y)$

证明同构或不同构

证明同构的方法

1. 定义：证明 $f: G_1 \to G_2$是同态，证明 f 为双射
2. 同态基本定理，其中一个群是商群

证明不存在同构的方法

1. 通常用反证法

与有限群相关的数量结果

(1) $|G|=[G:H]\ |H|$

$|G|=|G/H||H|$

$|a|\,||G|,\quad a\in G$

(2) $f: G\to G'$是满同态 $\Rightarrow |G'|\,|\,|G|$ 且 $|G'| = |G/\ker f|$

(3) $|G| = n$, p为素数，$p\,|\,n$, G 为 Abel 群

$\Rightarrow G$ 中含 p 阶元

$$|AB|=\frac{|A||B|}{|A\cap B|}$$

(4) $|\bar{a}|=[G:N(a)]$

(5) A, B是G 的子群，A,B有限，则

要求

1. 群的定义、实例与术语（有限群、无限群、平凡群、交换群或Abel群、群的阶、元素的幂、元素的阶）
2. 群的基本性质：幂运算规则、消去律、群方程有解、元素阶的性质
3. 子群及正规子群的判别定理和方法
4. 陪集的定义及其性质
5. 拉格朗日定理及其应用
6. 商群的定义和实例
7. 群同态映射的定义及其性质
8. 循环群的生成元和子群
9. 置换群

组合数学知识点

组合计数

- 计数定理：容斥原理；Polya定理
- 计数方法：递推方程；生成函数；指数生成函数
- 计数模型：选取方案；不定方程解；非降路径；拆分方案；放球方案

组合存在

- 鸽巢原理；Ramsey定理

组合存在性定理

- 鸽巢原理的简单形式

  n+1个物体放到 n个盒子里，则存在一个盒子至少含有2个或者2个以上的物体.

- 应用关键
  - 选择鸽子——所有的配置
  - 构造鸽巢——配置的所有可能的模式
  - 模式数比配置数至少小1

选取问题的公式

$$P(n,r)=\frac{n!}{(n-r)!}$$

$$C(n,r)=\frac{n!}{r!(n-r)!}$$

多重集 $S=\{n_1\cdot a_1,n_2\cdot a_2,\ldots,n_k\cdot a_k\}$

排列 $\begin{cases}\dfrac{n!}{n_1!n_2!\cdots n_k!} & r=n=n_1+n_2+\ldots+n_k\\ k^r & r\le n_i,i=1,2,\ldots,k\end{cases}$

组合 $C(k+r-1,r)\qquad r\le n_i,i=1,2,\ldots,k$

非降路径问题

- 从(0,0)到(m,n)点的非降路径数 $\binom{m+n}{n}$
- 从(a,b)到(m,n)点的非降路径数 $\binom{m-a+n-b}{n-b}$
- 从(0,0)经过(a,b)点到(m,n)点的非降路径数

$$\binom{a+b}{b}\binom{m-a+n-b}{n-b}$$

- 从(0,0)到(m,n)点的有约束条件的非降路径数

  ——一一对应方法

不定方程的解

方程	对应的生成函数
$x_1 + x_2 + \dots + x_k = r$ $x_i \in \mathrm{N}$	$(1 + y + y^2 + \dots)^k = \dfrac{1}{(1-y)^k}$ $\boxed{N = \binom{r+k-1}{r}}$
$x_1 + x_2 + \dots + x_k = r$ $x_i \in \mathrm{N}$ $l_i \le x_i \le n_i$	$(y^{l_1} + y^{l_1+1} + \dots + y^{n_1})$ $(y^{l_2} + y^{l_2+1} + \dots + y^{n_2})\dots$ $(y^{l_k} + y^{l_k+1} + \dots + y^{n_k})$
$p_1 x_1 + p_2 x_2 + \dots + p_k x_k = r$ $p_i \in \mathrm{Z}^+$ $x_i \in \mathrm{N},\ l_i \le x_i \le n_i$	$(y^{l_1 p_1} + y^{(l_1+1)p_1} + \dots + y^{n_1 p_1})$ $(y^{l_2 p_2} + y^{(l_2+1)p_2} + \dots + y^{n_2 p_2})\dots$ $(y^{l_k p_k} + y^{(l_k+1)p_k} + \dots + y^{n_k p_k})$

正整数的拆分问题

- 无序拆分基本模型
  - 将N无序拆分成正整数$\alpha_1, \alpha_2, \ldots,\alpha_n$,不允重复

$$\alpha_1 x_1 + \alpha_2 x_2 + \ldots + \alpha_n x_n = N$$

$$0 \le x_i \le 1$$

  - 将N无序拆分成正整数$\alpha_1, \alpha_2, \ldots,\alpha_n$,允许重复

$$\alpha_1 x_1 + \alpha_2 x_2 + \ldots + \alpha_n x_n = N$$

$$0 \le x_i$$

- 有序拆分
  - 把N有序拆分成r个部分且允许重复的方案数，不定方程$x_1+x_2+\ldots x_r=N$的正整数解：$C(N-1,r-1)$

放球：n个球, m个盒子

球号	盒号	空否	方法数	组合问题
N	N	N		n 恰好拆分成 m 个部分
N	N	Y		n 拆分成 t 个部分($t \le m$)
N	Y	N	$\binom{n-1}{m-1}$	$x_1+x_2+\ldots+x_m=n$ 正整数解
N	Y	Y	$\binom{n+m-1}{n-1}$	$x_1+x_2+\ldots+x_m=n$ 非负整数解
Y	N	N	$\left\{ n \atop m \right\}$	n 个不同的球恰好放到 m 个相同盒子
Y	N	Y	$\sum_{k=1}^{m}\left\{ n \atop k \right\}$	n 个不同的球放到 m 个相同盒子
Y	Y	N	$m!\left\{ n \atop m \right\}$	n 个不同的球恰好放到 m 个不同盒子
Y	Y	Y	m^n	n 个不同的球放到 m 个不同盒子

组合计数方法

- 递推方程
  - 通过依赖关系导出递推方程、确定初值
  - 求解方法：公式法、换元法、迭代归纳法、递归树法、尝试法、生成函数法
- 生成函数与指数生成函数
  - 分别对应于无序与有序计数问题
  - 如何根据问题得到生成函数和指数生成函数
  - 如何展开生成函数与指数生成函数得到a_n

组合计数定理

- 容斥原理

$$|\overline{A_1}\cap\overline{A_2}\cap\ldots\cap\overline{A_m}|=|S|-\sum_{i=1}^{m}|A_i|+\sum_{1\le i<j\le m}|A_i\cap A_j|$$

$$-\sum_{1\le i<j<k\le m}|A_i\cap A_j\cap A_k|+\ldots+(-1)^m|A_1\cap A_2\cap\ldots\cap A_m|$$

- 应用
  - 欧拉函数
  - 错位排列

$$\varphi(n)=n(1-\frac{1}{p_1})(1-\frac{1}{p_2})\ldots(1-\frac{1}{p_k})$$

$$D_n=n![1-\frac{1}{1!}+\frac{1}{2!}-\ldots+(-1)^n\frac{1}{n!}]$$

Polya定理

设$N=\{1, 2, \ldots, n\}$，$G=\{\sigma_1, \sigma_2, \ldots, \sigma_g\}$是$N$上置换群, 用$m$中颜色涂色$N$中元素，$C(\sigma_k)$是$\sigma_k$中的轮换（含1—轮换在内）个数，则在$G$的作用下不同的涂色方案数是

$$M=\frac{1}{|G|}\sum_{k=1}^{g} m^{C(\sigma_k)}$$

实例：

各种对称图形的旋转、翻转，每个动作看做一个置换

注意置换的复合运算必须封闭

组合计数符号

- 排列数 $P(n,m)= m!\ C(n,m)$
- 组合数（二项式系数）$C(n, m)$, $\binom{n}{m} = \frac{n!}{m!(n-m)!}$
- 多项式系数 $\binom{n}{n_1 n_2 \dots n_t} = \frac{n!}{n_1!\ n_2! \dots n_t!}$
- 错位排列数 $D_n = n![1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \dots + (-1)^n \frac{1}{n!}]$
- Fibonacci数 $f_n = f_{n-1} + f_{n-2}$ 1, 1, 2, 3, 5, 8, 11, …
- Catalan数（多边形三角划分） $h_n = \frac{1}{n}\binom{2n-2}{n-1}$
- 第一类Stirling数（多项式系数） $\left[{n \atop k} \right]$
- 第二类Stirling数（放球） $\left\{ {n \atop k} \right\}$

Catalan数与第二类Stirling数

- Catalan数

  凸n边形划分成三角形的方式数

$$h_n = \sum_{k=1}^{n-1} h_k h_{n-k}, n \ge 2, \quad h_1 = 1 \qquad h_n = \frac{1}{n}\binom{2n-2}{n-1}$$

- 第二类Stirling数

  n个不同的球放到 r 个相同的盒子里方法数

$$\begin{Bmatrix} n \\ r \end{Bmatrix} = r\begin{Bmatrix} n-1 \\ r \end{Bmatrix} + \begin{Bmatrix} n-1 \\ r-1 \end{Bmatrix}, \quad n > r \ge 1,$$

$$\begin{Bmatrix} n \\ n \end{Bmatrix} = 1, \quad \begin{Bmatrix} n \\ 2 \end{Bmatrix} = 2^{n-1} - 1, \quad \begin{Bmatrix} n \\ n-1 \end{Bmatrix} = \binom{n}{2}$$

基本组合恒等式

1. $\binom{n}{r} = \binom{n}{n-r}$

2. $\binom{n}{r} = \binom{n-1}{r} + \binom{n-1}{r-1}$

3. $\binom{n+r+1}{r} = \binom{n+r}{r} + \binom{n+r-1}{r-1} + \ldots + \binom{n+1}{1} + \binom{n}{0}$

4. $\binom{n}{r}\binom{l}{r} = \binom{n}{r}\binom{n-r}{l-r}$

5. $\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \ldots + \binom{n}{n} = 2^n$

6. $\binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \ldots \pm \binom{n}{n} = 0$

7. $\binom{m+n}{r} = \binom{m}{0}\binom{n}{r} + \binom{m}{1}\binom{n}{r-1} + \ldots + \binom{m}{r}\binom{n}{0}$

要求

- 鸽巢原理简单形式及其应用
- 熟悉组合数、排列数、多项式系数、错位排列数、Fibonacci数、Catalan数、第二类Stirling数的定义及性质
- 恒等式证明、组合数序列求和
- 求解实际的组合计数问题

离散数学在计算机科学中的应用实例

- 建模
  - 集合、关系、函数
  - 图
  - 代数系统
  - 离散概率
- 分析
  - 组合
  - 图论
  - 概率
  - 数理逻辑

问题1: 单链聚类

- 网络最小费用的连通

  网络路由算法

- 单链聚类——数据分析

  有一组离散的数据，任何两个数据i,j 之间有对称的相似度函数$d(i,j)$，求对这组数据的k-划分，使得存在k个聚类$C_1,C_2,\ldots,C_k$，两个聚类C_s,C_t之间的距离

$$D(C_s,C_t)=\min \{ d(i,j) \mid i\in C_s, j\in C_t \}$$

  k-聚类的最小间隔

$$D=\min\{ D(C_s,C_t) \mid 1 \le s < t \le k \}$$

  求使得D最大的k 聚类.

一个3-聚类的实例

结点集合：

{1,2,3,4,5,6,7,8,9,10}

最大间隔3-聚类：

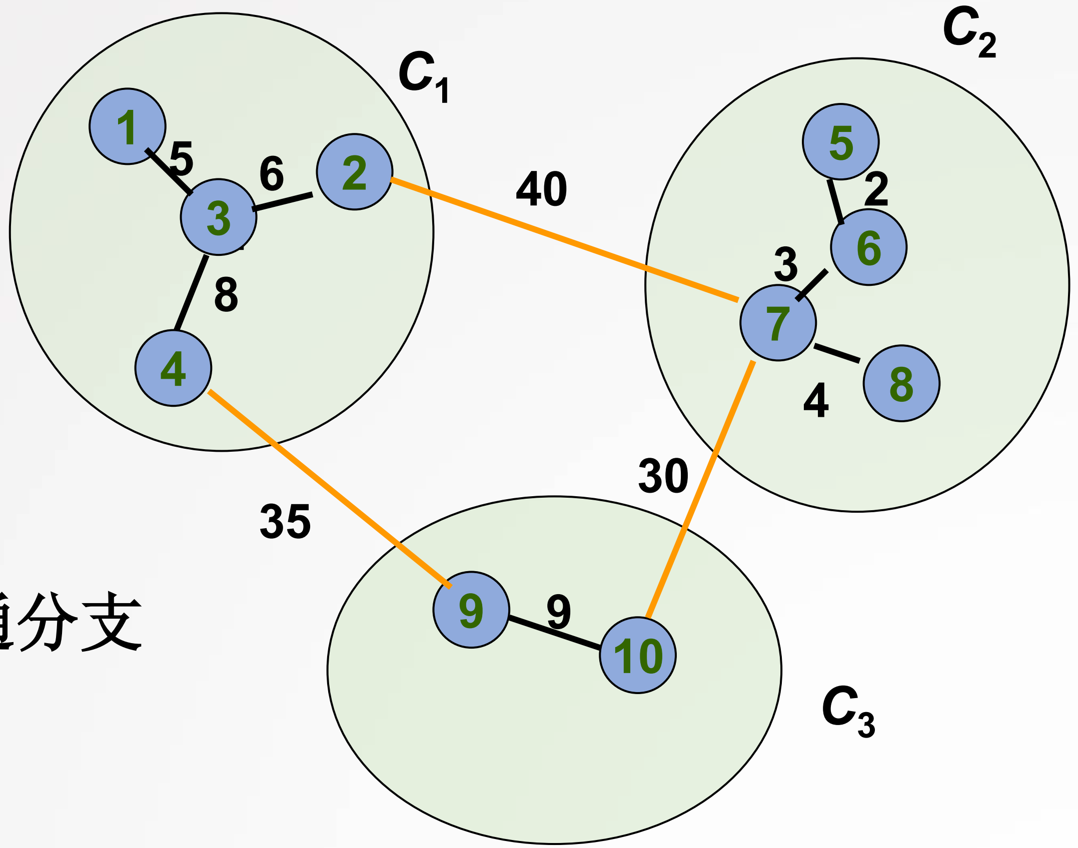
$\{C_1,C_2,C_3\}$

最大间隔：

$D=\min\{30,35,40\}=30$

Kruskal算法：

加边直到构成 k 个连通分支



聚类问题的背景

- 根据测试数据的相似性做出分类分析
  - 数据挖掘
  - 图像处理
- 系统划分
  - 电路设计
- 根据不同优化目标形成不同类型的聚类问题，其中某些单链聚类问题可以使用最小生成树的模型

问题2 网络优化

- 背景
  - 树状连通网络，每条线路有传输延迟，只能改进K条线路，以降低传输延迟，如何选择？
- 实例
  - 节点集 $V=\{1,2,\ldots, n\}$，$E=\{e_1,e_2,\ldots,e_{n-1}\}$，$K\leq n-1$
  - w_t 是边 e_t 的传输延迟，$t=1,2,\ldots, n-1$，$W(i,j)$是 i 到 j 的延迟 (从 i 到 j 路径上所有边延迟之和)
  - 对e_i 改进后，边上的延迟减少了pw_i，$p<1$为常数
- 问题
  - 选 $A\subseteq E$, $|A|=K$, 使得

$$W_A = \min\left(\sum_{1\leq i<j\leq n} W(i,j)\right)$$

贪心法设计与分析

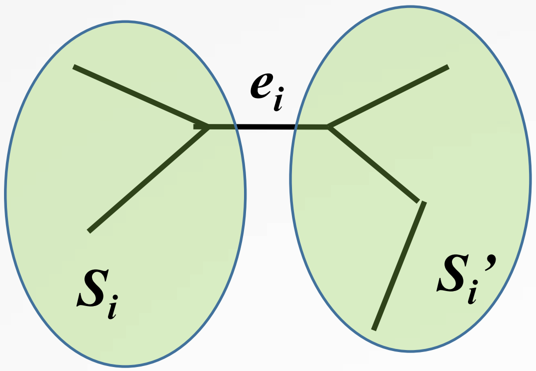
- 改进e_i之后总延迟减少了

$$c_i = |S_i| \times |S_i'| \times pw_i$$

- 选择A后总延迟是

$$W_A = W - \max\{\sum_{e_i \in A} c_i\}$$

- 贪心法
  - 计算c_i， i=1,2,…,n-1
  - 排序e_i使得 $c_1 \geq c_2 \geq \ldots \geq c_{n-1}$
  - $A=\{ e_1, e_2, \ldots , e_K \}$
  - 可以证明得到最优解



问题3：Slepian译码表

k 维线性码 C—— $[n, k]$码：

$F_2^n = \{v \mid v = a_1 a_2 \ldots a_n, a_i \in \{0,1\}\}$ 的 k 维子空间

$v = x_1 v_1 + x_2 v_2 + \ldots + x_k v_k$，$v_1, v_2, \ldots, v_k$ 为一组基

实例：[7,4]码，红色码是一组基

C={ 0000000, 0001011, 0010101, 0011110, 0100110, 0101101,
0110011, 0111000, 1000111, 1001100, 1010010, 1011001,
1100001, 1101010, 1110100, 1111111}

C构成群

- C关于向量加法封闭，加法满足结合律，单位元是 n 维0向量，码 v 的逆元就是 v 自己
- C是 F_2^n 的子群
- C的陪集 $C+a$，其中$a\in F_2^n$

实例：[4, 2]码 $C = \{ 0000, 0110, 1001, 1111 \}$

	错误向量			
C	0000	0110	1001	1111
C+0001	0001	0111	1000	1110
C+0010	0010	0100	1011	1101
C+0011	0011	0101	1010	1100

纠错——Slepian译码表

- 发送 $v\in C$，接收到的可能是 $u\notin C$，需要将u译成C中与u最接近（不同的位数最少）的代码v——最近距离译码原则

- Slepian译码表：由全体向量构成，第一行是C，第二行是陪集$C+a_1$，a_1是剩余向量中1个数最少且数值最小的向量；类似选取$a_2, a_3, \ldots$作为陪集的代表元素.

- 译码： 若接收到 $u=v+a_j\in C+a_j$，那么$v=u+a_j$，即译作u与所在陪集代表元素之和

网上资源

- 哈佛大学
  http://lib.harvard.edu/eresources/details/d/descmath.html
- 普林斯顿大学
  http://www.math.princeton.edu/~bsudakov/seminar.html
- 伯克利大学
  http://www-inst.eecs.berkeley.edu/~cs70/
- 肯塔基大学
  http://www.ms.uky.edu/~math/Research/Margot/DM/DiscreteMath.html

网上资源（续）

- 离散数学论坛网址
  http://mathforum.org/discrete
- 布朗大学
  http://www.cs.brown.edu/courses/cs022/
- 科罗拉多大学
  http://www.colorado.edu/education/DMP/
- 数学世界网址
  http://mathworld.wolfram.com/topics/DiscreteMathematics.html

祝大家取得好成绩！

谢　谢！