

信息安全数学基础

韩 琦

计算机科学与技术学院

Detailed overview

1 组合数学

- 概述
- 先修课程知识点回顾
 - 排列与组合
 - 鸽巢原理
 - 容斥原理
 - 母函数
- 递推关系
- 区组设计

拉丁方

先来看一个例子：

例

在一块实验田里试种4种小麦品种A、B、C、D，以便比较品种的优劣。为了消除土地纵向和横向肥脊不均的影响，将实验田分为16块，种法如下：

A	B	C	D
D	A	B	C
C	D	A	B
B	C	D	A

每个品种在每行每列都出现一次，这样就可以通过比较各品种的平均产量来比较各品种的优劣了。

拉丁方、正交拉丁方

定义

设 \mathbf{A} 是一个 $n \times n$ 的矩阵, 若 \mathbf{A} 的每行、每列都是 $\{1, 2, \dots, n\}$ 的全排列, 则称 \mathbf{A} 是一个 n 阶拉丁方。

定义

设 $\mathbf{A} = (a_{ij})$, $\mathbf{B} = (b_{ij})$ 是两个 n 阶拉丁方, 若 n^2 个有序对 (a_{ij}, b_{ij}) ($i, j = 1, 2, \dots, n$)互不相同, 则称 \mathbf{A} 与 \mathbf{B} 是一对正交的 n 阶拉丁方。

是否为正交拉丁方的判别其实很简单, 将两个矩阵重叠起来组成一个以有序对为元素的矩阵, 如果所有元素互不相同, 则两个拉丁方正交。

定理

若 $\mathbf{A}_1, \mathbf{A}_2, \dots, \mathbf{A}_r$ 是一组正交 n 阶拉丁方, 则 $r \leq n - 1$ 。

定理

设 $n = p^a$ 且 $n \geq 3$, 其中 p 是一个质数, a 是一个整数, 则存在 $n - 1$ 个相互正交的 n 阶拉丁方。

定理

若存在 r 个 n 阶拉丁方正交组和 r 个 m 阶拉丁方正交组, 则存在 r 个 nm 阶拉丁方正交组。

定理

设 $n = p_1^{a_1} p_2^{a_2} \cdots p_t^{a_t}$ 是正整数 $n (n > 1)$ 的素数幂分解, $r = \min_j \{p_j^{a_j} - 1\}$, 则存在 r 个 n 阶正交拉丁方组。

区组

定义

设 $\mathbf{X} = \{x_1, x_2, \dots, x_v\}$ 是一个具有 v 个元素的集合, B_1, B_2, \dots, B_b 是 \mathbf{X} 的 b 个 k -子集, 若集族 $\{B_1, B_2, \dots, B_b\}$ 满足以下条件:

- 1 \mathbf{X} 中的任何一个元素恰好在 b 个子集的 r 个中出现;
- 2 \mathbf{X} 中的任一对元素恰好在 b 个子集的 λ 个中出现;
- 3 $k < v$ 。

则称 $\{B_1, B_2, \dots, B_b\}$ 为 \mathbf{X} 的一个平衡不完全区组设计, 记为 (b, v, r, k, λ) -BIBD, B_1, B_2, \dots, B_b 称为该设计的区组。

BIBD举例

$X = \{x_1, x_2, \dots, x_9\}$ 的 $(12, 9, 4, 3, 1)$ -BIBD 为 $\{B_1, B_2, \dots, B_{12}\}$

$$B_1 = \{x_1, x_2, x_3\}, \quad B_2 = \{x_4, x_5, x_6\}, \quad B_3 = \{x_7, x_8, x_9\}$$

$$B_4 = \{x_1, x_4, x_7\}, \quad B_5 = \{x_2, x_5, x_8\}, \quad B_6 = \{x_3, x_6, x_9\}$$

$$B_7 = \{x_1, x_5, x_9\}, \quad B_8 = \{x_2, x_6, x_7\}, \quad B_9 = \{x_3, x_4, x_8\}$$

$$B_{10} = \{x_1, x_6, x_8\}, \quad B_{11} = \{x_2, x_4, x_9\}, \quad B_{12} = \{x_3, x_5, x_7\}$$

区组、关联矩阵

定理

对于一个 (b, v, r, k, λ) -BIBD, 有

$$bk = vr, \quad r(k - 1) = \lambda(v - 1)$$

定义

设 $\{B_1, B_2, \dots, B_b\}$ 为集合 $\mathbf{X} = \{x_1, x_2, \dots, x_v\}$ 的一个 (b, v, r, k, λ) -BIBD, 该区组设计的关联矩阵是一个 $v \times b$ 矩阵 $\mathbf{A} = (a_{ij})$, 其中

$$a_{ij} = \begin{cases} 1, & \text{if } x_i \in B_j \\ 0, & \text{if } x_i \notin B_j \end{cases}$$

区组、关联矩阵

定理

设 \mathbf{A} 是 $\mathbf{X} = \{x_1, x_2, \dots, x_v\}$ 的一个 (b, v, r, k, λ) -BIBD的关联矩阵, 那么有

$$\mathbf{A}\mathbf{A}^T = (r - \lambda)\mathbf{I} + \lambda\mathbf{J}$$

其中 \mathbf{I} 为 v 阶单位矩阵, \mathbf{J} 为所有元素均为1的 v 阶方阵。

定理

对任 (b, v, r, k, λ) -BIBD, 有 $b \geq v$ 。

区组设计的构造

定义

在 (b, v, r, k, λ) - $BIBD$ 中, 若 $b = v, r = k$, 则称该设计为对称平衡不完全区组设计, 记为 (v, k, λ) - $SBIBD$ 。

引理

(v, k, λ) - $SBIBD$ 的任何两个区组恰有 λ 个公共元素。

区组设计的构造

定理

若 B_1, B_2, \dots, B_v 是集合 $\mathbf{X} = \{x_1, x_2, \dots, x_v\}$ 的一个 (v, k, λ) -SBIBD, 则对任 $B_i \in \{B_1, B_2, \dots, B_v\}$, $\{B_1 - B_i, \dots, B_{i-1} - B_i, B_{i+1} - B_i, \dots, B_v - B_i\}$ 是 $\mathbf{X} - B_i$ 的 $(v-1, v-k, k, k-\lambda, \lambda)$ -BIBD。

定理

若 B_1, B_2, \dots, B_v 是集合 $\mathbf{X} = \{x_1, x_2, \dots, x_v\}$ 的一个 (v, k, λ) -SBIBD, 则对任 $B_i \in \{B_1, B_2, \dots, B_v\}$,

$$B_1 \cap B_i, \dots, B_{i-1} \cap B_i, B_{i+1} \cap B_i, \dots, B_v \cap B_i$$

是 B_i 的 $(v-1, k, k-1, \lambda, \lambda-1)$ -BIBD。

作业

① 求解下列递推关系：

① $a_n - 5a_{n-1} + 6a_{n-2} = 0, a_0 = 1, a_1 = -2$

② $a_n - a_{n-1} - 9a_{n-2} + 9a_{n-3} = 0, a_0 = 0, a_1 = 1, a_2 = 2$

② 下列区组是否为BIBD？若是则确定其参数 (b, v, r, k, λ)

① $B_1 = \{1, 2, 3\}, B_2 = \{2, 3, 4\}, B_3 = \{3, 4, 5\}, B_4 = \{1, 4, 5\}, B_5 = \{1, 2, 5\}$

② $B_1 = \{1, 2, 3, 4\}, B_2 = \{1, 3, 4, 5\}, B_3 = \{1, 2, 4, 5\}, B_4 = \{1, 2, 3, 5\}, B_5 = \{2, 3, 4, 5\}$

谢谢！

hanqi_xf@hit.edu.cn