



上海大学
Shanghai University

课程教学大纲

（专业基础课、专业选修课、高年级研讨课适用）

| | | | |
|------|----------|------|-------------------|
| 课程编号 | 08305093 | 课程名称 | （中文）编码理论 |
| | | | （英文）Coding Theory |
| 学分 | 3 | 课程性质 | 专业选修课 |

一、指导思想

课程内容与课程设计要以习近平新时代中国特色社会主义思想为指导，落实立德树人根本任务，深入挖掘各类课程和教学方式中蕴含的思想政治教育元素，建设适应新时代要求的一流本科课程。

二、诚信要求

学生在学习过程中要恪守道德规范，实事求是，不欺骗他人，不弄虚作假。

三、教材与参考资料

| | |
|------|-----------------------------------|
| 教材 | 刘爱莲编著，《纠错编码原理及 MATLAB 实现》，清华大学出版社 |
| 参考书 | 万哲先编著，《代数和编码》第三版，高等教育出版社 |
| 参考网站 | |

四、课程目标

| | |
|--------|---|
| 课程目标 1 | 掌握纠错编码所需要用到的代数知识，包括抽象代数基本概念，有限域的结构及有限域上的因式分解等基本理论和方法。 |
| 课程目标 2 | 掌握纠错编码的基本原理，掌握线性分组码、循环码的构造方法、它们的编码译码方法以及他们的性质和纠错能力。 |

（注：课程目标要兼顾“知识传授、能力培养、价值引导”三方面的目标）

五、本课程支撑的毕业要求

| 毕业要求 | 支撑的具体指标点 | 对应的课程目标 |
|--------------|-----------------------|----------|
| 1.工程知识 | 系统地掌握本学科的基本理论、基本技能与方法 | 课程目标 1、2 |
| 2.问题分析 | 系统地掌握本学科的基本理论、基本技能与方法 | 课程目标 1、2 |
| 3. 设计/开发解决方案 | 能够从事智能科学与技术相关的研发等工作 | 课程目标 2 |
| 4.研究 | 能够从事智能科学与技术相关的研发等工作 | 课程目标 1、2 |

（注：“毕业要求”从本专业培养方案中学生毕业要求中选取；“支撑的具体指标点”从学生毕业要求中细化的指标点中选取）

六、课程教学环节

| | | |
|-------------------|------|--|
| 第 1-5 周 15 学时 | 支撑关系 | 课程目标 1 中“掌握纠错编码所需要用到的代数知识，包括抽象代数基本概念，有限域的结构及有限域上的因式分解等基本理论和方法。” |
| | 教学内容 | <p>第 2 章纠错编码的代数基础</p> <p>2.1 整数的有关概念（3 学时） 总结整数的下列相关概念并推广到多项式：素数、公因子、带余除法、辗转相除法、同余、剩余类、剩余类的加法和乘法。</p> <p>2.2 群的基本概念（2.2.1 群的定义）（3 学时） 群的基本概念，会判断一个代数系统是否构成群，单位元和逆元的求法； 整数剩余类集合关于模 m 的加法和乘法在什么情况下构成群；多项式剩余类集合关于模多项式的加法和乘法在什么情况下构成群。</p> <p>2.2 群的基本概念（2.2.2 循环群，2.2.3 子群和陪集）2.3 环的基本概念（3 学时） 循环群及其生成元，子群和陪集； 环的定义，整数与多项式的剩余类环，子环。</p> <p>2.4 域的基本概念（2.4.1 域的定义，2.4.2 有限域（部分））（3 学时） 域的定义；有限域的定义；有限域的本原元；有限域的特征；有限域的加法和乘法结构；有限域的共轭根组。</p> <p>2.4 域的基本概念（2.4.2 有限域（部分）2.4.3 二元域的运算）（3 学时） 有限域的最小多项式、即约多项式和本原多项式；有限域中元素的四种表示；有限域上的因式分解。</p> |
| | 教学方式 | 以教师课堂讲授为主，配合课堂练习、课后作业讲解。 |
| 第 6 周 3 学时 | 支撑关系 | 课程目标 2 中“掌握纠错编码的基本原理”。 |
| | 教学内容 | <p>第 1 章纠错编码的基本概念（3 学时） 数字通信和信道信源编码基本原理； 检错编码和纠错编码概念； 极大似然译码方法； 码的检错和纠错能力。</p> |
| | 教学方式 | 以教师课堂讲授为主，配合课堂练习。 |
| 第 7-10 周 12 学时 | 支撑关系 | 课程目标 2 中“掌握线性分组码、循环码的构造方法、它们的编码译码方法以及他们的性质和纠错能力。” |
| | 教学内容 | <p>第 3 章线性分组码 3.1 线性分组码的定义，3.2 生成矩阵和校验矩阵（3 学时） 线性分组码的定义，线性子空间及其生成基，生成矩阵和校验矩阵。</p> |

| | | |
|------------|---|--|
| | | <p>第3章线性分组码 3.3 系统线性分组码, 3.4 对偶码 (3 学时) 将生成矩阵化为阶梯形矩阵, 系统矩阵及系统码; 线性子空间的对偶子空间定义, 线性码及其对偶码的关系; 生成矩阵和校验矩阵之间的关系。</p> <p>第3章线性分组码 3.5 编码的实现, 3.6 线性分组码的译码 (3 学时) 根据生成矩阵进行编码; 由一致校验矩阵求出校验子、陪集首及其对应关系; 给定码字的译码及判断译码是否为确定性译码。</p> <p>第4章循环码 (3 学时, 如果提前考, 本部分内容删除) 循环码的定义, 循环码的多项式描述; 循环码的生成矩阵、生成多项式和监督矩阵; 循环码的编码与译码。</p> |
| | 教学方式 | 以教师课堂讲授为主, 配合课堂练习、课后作业讲解。 |
| 课外作业/问题/项目 | <p>每周布置 1-3 题, 第 5 周代数部分学完和第 9 周代数部分学完后各布置一个研讨项目。</p> <p>第一周作业: 1、用辗转相除法求 $\mathbf{Z}_2[x]$ 中多项式 $a(x) = x^4 + x + 1$ 和 $b(x) = x^3 + x + 1$ 的最高公因式 $\gcd(a(x), b(x))$; 并将 $\gcd(a(x), b(x))$ 表示成 $c(x)a(x) + d(x)b(x)$ 的形式。</p> <p>2、将题 1 中的 $\mathbf{Z}_2[x]$, 改为 $\mathbf{Z}_3[x]$。</p> <p>第二周作业: 3、考察 $\mathbf{Z}_2[x]$ 中多项式 $f_1(x) = x^3 + x + 1$ 和 $f_2(x) = x^3 + 1$, (1) 判断 $f_1(x)$ 和 $f_2(x)$ 哪个是 $\mathbf{Z}_2[x]$ 上的不可约多项式; (2) 将找出的不可约多项式记为 $f(x)$, 写出 $\mathbf{Z}_2[x]$ 关于模 $f(x)$ 的剩余类的集合 $\mathbf{Z}_2[x]_{f(x)}$ 的全部元素; (3) 在集合 $\mathbf{Z}_2[x]_{f(x)}$ 上定义加法运算 \oplus 和乘法运算 \otimes 分别为: $a(x) \oplus b(x) = a(x) + b(x)$ $a(x) \otimes b(x) = (a(x)b(x))_{f(x)}$ 请求出 $(x+1) \oplus (x^2 + x + 1)$ 和 $(x+1) \otimes (x^2 + x + 1)$ 的值; (4) 求出 $x+1$ 关于乘法运算 \otimes 的逆元。</p> <p>第三周作业: 4、设 $p = 7$, 用 \mathbf{Z}_7 来记所有整数集合 \mathbf{Z} 模 7 的等价类的集合, 在 \mathbf{Z}_7 上定义加法运算 \oplus 和乘法运算 \otimes 分别为: $a \oplus b = (a + b)_7$</p> | |

$$a \otimes b = (ab)_7$$

- (1) 写出模 7 的等价类的集合 \mathbf{Z}_7 的全部元素;
- (2) 请列出 \mathbf{Z}_7 关于 \oplus 和 \otimes 这两种运算的运算表;
- (3) 试从域的定义出发验证 $\langle \mathbf{Z}_7, \oplus, \otimes \rangle$ 是一个有限域。

- 5、用 \mathbf{Z}_8 来记模 8 的等价类的集合, 在 \mathbf{Z}_8 上定义加法运算 \oplus 和乘法运算 \otimes 分别为:

$$a \oplus b = (a + b)_8$$

$$a \otimes b = (ab)_8$$

- (1) 写出模 8 的等价类的集合 \mathbf{Z}_8 的全部元素;
 - (2) 请列出 \mathbf{Z}_8 关于 \oplus 和 \otimes 这两种运算的运算表;
 - (3) 试从域的定义出发说明 $\langle \mathbf{Z}_8, \oplus, \otimes \rangle$ 不是一个有限域;
6. 比较第 4 题和第 5 题, 想一想为什么第 2 题的 8 个元素不能构成有限域而第 5 题的 8 个元素能构成有限域。他们的运算有什么不同。(该题重在理解, 可不写成书面作业)

第四周作业:

- 7、设 $p = 5$, 考察 $\mathbf{Z}_5[x]$ 中多项式

$$p(x) = x^2 + 2,$$

- (1) 试说明 $p(x)$ 是 $\mathbf{Z}_5[x]$ 上的不可约多项式;
- (2) $\mathbf{Z}_5[x]_{p(x)}$ 是含有 $5^2=25$ 个元素的集合, 写出 $\mathbf{Z}_5[x]_{p(x)}$ 的全部元素;
- (3) 在 $\mathbf{Z}_5[x]_{p(x)}$ 上定义加法运算 \oplus 和乘法运算 \otimes 分别为:

$$a(x) \oplus b(x) = a(x) + b(x)$$

$$a(x) \otimes b(x) = (a(x)b(x))_{p(x)}$$

请求出 $(x+2) \oplus (3x+4)$ 和 $(x+2) \otimes (3x+4)$ 的值。

- 8、设 $p = 2$, 考察 $\mathbf{Z}_2[x]$ 中多项式

$$p(x) = x^3 + x + 1,$$

- (1) 试说明 $p(x)$ 是 $\mathbf{Z}_2[x]$ 上的不可约多项式;
- (2) $\mathbf{Z}_2[x]_{p(x)}$ 是含有 $2^3=8$ 个元素的集合, 写出 $\mathbf{Z}_2[x]_{p(x)}$ 的全部元素;
- (3) 在 $\mathbf{Z}_2[x]_{p(x)}$ 上定义加法运算 \oplus 和乘法运算 \otimes 分别为:

$$a(x) \oplus b(x) = a(x) + b(x)$$

$$a(x) \otimes b(x) = (a(x)b(x))_{p(x)}$$

请列出 $\mathbf{Z}_2[x]_{p(x)}$ 关于 \oplus 和 \otimes 这两种运算的运算表;

第五周研讨项目：

研讨项目 1（代数部分）---认识有限域 $GF(p^n)$

目的：掌握有限域 $GF(p^n)$ 的结构，以及有限域 $GF(p^n)$ 上的运算。

要求：讨论有限域 $GF(p^n)$ 的构造方法，有限域 $GF(p^n)$ 加法结构和乘法结构，讨论有限域 $GF(p^n)$ 上的运算。

提交时间：第 6 周

提交方式：报告，因为涉及较多的数学公式，所以直接写作业本上，拍照上传。

参考提纲：

在 $GF(2)=\{0,1\}$ 的系数域上，以 $p(x)=x^4+x^3+1$ 为模构成有限域 $GF(2^4)$ ，

- (1) 有限域 $GF(2^4)$ 的特征；
- (2) 设 α 为 $p(x)$ 的根，并写出有限域 $GF(2^4)$ 中元素的四种表示；
- (3) 找出所有的共轭根组，并构成相应的最小多项式；
- (4) 将所有的最小多项式化简；
- (5) 将 $x^{16}-x$ 因式分解；
- (6) 求出所有的本原元和本原多项式。

第六周作业：

9. 将域 F_3 上的 4×4 矩阵 A 化为与之行等价的阶梯形矩阵 A_0 ，

$$A = \begin{pmatrix} 1 & 2 & 0 & 2 \\ 2 & 1 & 1 & 0 \\ 2 & 2 & 1 & 1 \\ 0 & 1 & 2 & 2 \end{pmatrix}.$$

并求出矩阵 A 的秩。

10. 将域 F_2 上的 8×8 矩阵 A 化为与之行等价的阶梯形矩阵 A_0 ，

$$A = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 \end{pmatrix}.$$

并求出矩阵 A 的秩。

第七周作业：

11. 求出齐次线性方程组 $Ax' = 0'$ 的解空间的一组基。

$$A = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 \end{pmatrix}$$

12. 设码 $C = \{(10100), (01010), (01101), (10011)\}$ ，

- (1) 计算 C 中所有码字的两两 Hamming 距离；

(2) 指出 C 是可以检几错的检错码, 并且指出 C 是可以纠几错的纠错码;

13. 设 C 是一个二元 (6, 3) 线性码, 其生成矩阵为

$$G = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

(1) 求出 C 的全部码字;

(2) 求出 C 的校验矩阵 H。

第八周作业:

14. 设 C 是一个二元 (6, 3) 线性码, 其生成矩阵为

$$G = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

(1) 求出所有的校验子 Hx' 和与之相对应的陪集首 e ;

(2) 求出以 $e = (000100)$ 为陪集首的 C 的陪集;

(3) 设收到的字为 $r = (011011)$, 计算 r 的校验子 Hr' , 并确定 r 的译码。

第九周研讨项目:

研讨项目 2 (编码部分) ---关于线性分组码的讨论

目的: 掌握线性分组码的编码问题、译码问题、纠错能力和检错能力。

要求: 构造一个 (n, k) 线性分组码, 讨论它的生成矩阵、校验矩阵、译码表的构造、译码方法、纠错能力和检错能力。

提交时间: 第 10 周

提交方式: 报告, 因为涉及较多的数学公式, 所以直接写作业本上, 拍照上传。

参考提纲:

以二元 (6, 3) 线性码为例:

(1) 写出一个二元 (6, 3) 线性码 C 的生成矩阵 G, 例如:

$$G = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

(2) 求出 C 的全部码字;

(3) 求出 C 的校验矩阵 H; (讨论生成矩阵 G 与校验矩阵 H 的关系)

(4) 求出所有的校验子 Hx' 和与之相对应的陪集首 e ;

(5) 求出以 $e = (000100)$ 为陪集首的 C 的陪集; (讨论译码表的构造)

(6) 设收到的字为 $r = (011011)$, 计算 r 的校验子 Hr' , 并确定 r 的译码。(讨论译码方法)

| | |
|--|---|
| | (7) 简述判断线性分组码的纠错能力和检错能力的方法； (8) 判断该线性码 C 是可以检几错的检错码和可以纠几错的纠错码。 |
|--|---|

(注：教学方式要能体现课前自学、课中研讨互动、课后作业的内容安排；课外作业/问题/项目要描述问题或项目的内容、组织方式、评价方法等)

七、课程目标评价方法

| 课程 目标 | 考核来源 | | | | | | 合 计 |
|---------------|-------------------|--------------------------------|-------------|-------------|------|---------|--------|
| | 平时成绩 | | | | 期末成绩 | | |
| | 出勤及 课堂学 习态度 | 课堂练 习和课 后小作 业完成 情况 | 研讨项 目（一） | 研讨项 目（二） | 第二章 | 第一、三、四章 | |
| 课程 目标 1 | 5 | 5 | 5 | | 35 | | 50 |
| 课程 目标 2 | 5 | 5 | | 5 | | 35 | 50 |
| 合计 | 10 | 10 | 5 | 5 | 35 | 35 | 100 |

(注：请选择若干考核来源，并在对应的课程目标中填上分数，考核来源可以由随堂测验、期中考试、课堂讨论、课堂报告、文献阅读、小组作业在线学习、在线讨论、实验项目、期末考试等中的若干种组成)

八、审核意见

| | |
|-----------------|--|
| 课程负责人/专业负责人审核意见 | <div style="text-align: right;"> <u>牛志华</u> (签名) 2022 年 3 月 20 日 </div> |
| 系 审核意见 | <div style="text-align: right;"> _____ (系) _____ (签名) 年 月 日 </div> |

| | |
|--------------------|---|
| <p>学院 审核意见</p> | <p>_____（签名） _____（公章） 年 月 日</p> |
|--------------------|---|