

平成 26 年度 情報工学科 教授細目

【講義名】 代数系と符号理論 (Algebraic Systems and Coding Theory)

【科目区分】 理工系科目 理工系広域科目 コア科目 (○印)

【開講学期】 5 学期

【単位数】 2-1-0

【担当教員】 (E クラス) 笠井 健太 准教授 南 3 棟 4 階 418 号室 内線 3902:
(O クラス) 植松 友彦 教授 南 3 棟 3 階 304 号室 内線:3243

【講義の目的】 符号理論の数学的基礎をなす群, 環, 体の代数構造とガロア体上のベクトル空間の部分空間である線形符号について講義する.

【知識ユニット】

- － 符号理論の基礎概念
- － 群, 環, 体
- － ガロア体の構成法と算法
- － 線形符号
- － 巡回符号
- － 代数的符号

【関連科目】 情報基礎学 (2 学期, ○,2-0-0), 通信理論 (4 学期, ●,2-0-0) デジタル通信 (5 学期, ◇,2-0-0), 情報ネットワーク設計論 (6 学期, ◇,2-0-0) 情報通信理論 (大学院: 集積システム), 符号理論特論 (大学院: 集積システム: 計算工学)

【教科書】 (E クラス)・代数系と符号理論入門、坂庭好一、渋谷智治著、コロナ社、2010 年
(O クラス)・代数系と符号理論、植松友彦、オーム社、2010 年

【参考書】

- － 符号理論入門, 岩垂 好裕 著, 昭晃堂, 1992 年
- － 符号理論入門, Vera Pless 著, 伊藤 昇 訳, 啓学出版, 1985 年
- － 情報数学入門, 榎本 彦衛 著, 新曜社, 1987 年
- － 符号理論, 今井 秀樹 著, コロナ社, 1990 年

【講義計画】

1. 基礎概念 1 : 符号化と復号, 受信空間と復号領域
2. 基礎概念 2 : 誤りと距離, 最尤復号, 誤り制御
3. 代数構造 1 : 群, 環, 体
4. 代数構造 2 : 整数環, イデアル
5. 代数構造 3 : 多項式環, 多項式環のイデアル

6. ガロア体 1 : ガロア体の構成法と表現
7. ガロア体 2 : 共役元と最小多項式, ガロア体の算法
8. 線形符号 1 : 基礎概念, 生成行列と検査行列
9. 線形符号 2 : 線形符号の復号, 部分符号と修正
10. 線形符号 3 : ハミング符号, 重み分布
11. 巡回符号 1 : 巡回符号の表現, 巡回符号の符号化
12. 巡回符号 2 : 巡回符号の根とフーリエ変換, BCH 限界
13. BCH 符号 1 : BCH 符号, リードソロモン符号
14. BCH 符号 2 : BCH 符号の復号 (1)
15. BCH 符号 3 : BCH 符号の復号 (2)

- 【実際の講義】
1. 基礎概念, ブロック符号
 2. 生成行列と組織符号, 双対符号とパリティ検査行列, 符号の最小距離
 3. 通信路のモデル, 符号の誤り訂正能力, 誤り制御, ハミング符号
 4. シンドローム, 線形符号の復号, 誤り訂正能力の限界式
 5. 群, 巡回群, 部分群による類別, 同型写像と群の同型
 6. 環, 準同型写像とイデアル, 整数環, 素因数分解の一意性
 7. 体, 多項式環, 多項式環を基礎とした有限体, 位数と原始元
 8. 有限体の構造, 有限体の表現, 有限体の構造のまとめ
 9. リード・ソロモン (RS) 符号, RS 符号の復号の原理
 10. Vandermonde 行列とその性質, RS 符号の生成行列とパリティ検査行列, Peterson のアルゴリズム
 11. 巡回符号と生成多項式, 巡回符号の生成行列とパリティ検査行列
 12. 巡回符号の双対符号, 最小多項式の性質, 巡回符号の最小距離, 巡回 RS 符号, BCH 符号と構成例
 13. BCH 符号と RS 符号の関係, BCH 符号と RS 符号の相違点

【成績評価】 第 1 回板書プリント参照のこと。