情報数理科学概論 (4)・情報数理科学特論 レポート課題
2015 年 1 月 15 日配布

注意

- **以下の問題のうち 1 問以上に解答すること.**
- 1 月 28 日（水）までに担当教員に直接提出するか，1 月 29 日（木）の講義の際に提出すること.
- 1 枚目に学修番号・氏名を書くこと.
- レポートが複数枚にわたるときは，左上をホッチキス等で綴じること.
- A4 レポート用紙を使用すること.

問題

以下の問題では，関数体はすべて 1 変数代数関数体を表すものとし，関数体 F/K において K は完全定数体であるとする．すなわち，K 上代数的な F の元は K の元に限るものとする.

1. $\mathbb{F}_3$ 係数多項式 $f(X) = X^3 + 2X + 1$ を考える．以下の問いに答えよ.
   （a）$f(X)$ は $\mathbb{F}_3[X]$ において既約であることを示せ.
   （b）$\mathbb{F}_3[X]/(f(X))$ は位数 27 の有限体であることを示せ.
   （c）$\mathbb{F}_3[X]/(f(X))$ において，X が属する剰余類を α で表す.（すなわち，$\alpha = X + (f(X))$ である.）このとき，$(\alpha+1)^{-1}$ を α の 2 次以下の多項式として表せ.
2. $\mathbb{F}_2$ 上の線形符号 C が次のパリティ検査行列を持つとして，以下の問いに答えよ.
$$H = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}.$$
   （a）C の生成行列を 1 つ求めよ.
   （b）C の長さ n，次元 k，最小距離 d を求めよ.
3. F/K を種数 0 の関数体とし，D を F/K の因子とする．このとき，$\deg D = 0$ ならば，D は主因子であることを示せ.
4. F/K を種数 1 の関数体とし，次数 1 の座 $P \in \mathbb{P}_F$ が存在するとする．以下の問いに答えよ.
   (a) 整数 $n \geq 0$ に対し，$\ell(nP)$ を求めよ.
   (b) $x \in \mathscr{L}(2P) \setminus \mathscr{L}(P)$, $y \in \mathscr{L}(3P) \setminus \mathscr{L}(2P)$ とする．体の拡大次数 $[F : K(x)]$, $[F : K(y)]$ をそれぞれ求めよ.（このような x, y の存在は (a) から分かる.）
   (c) 任意の $x \in \mathscr{L}(2P) \setminus \mathscr{L}(P)$, $y \in \mathscr{L}(3P) \setminus \mathscr{L}(2P)$ に対し，$F = K(x, y)$ が成り立つことを示せ.
   (d) $x \in \mathscr{L}(2P) \setminus \mathscr{L}(P)$, $y \in \mathscr{L}(3P) \setminus \mathscr{L}(2P)$ と定数 $a_1, a_2, a_3, a_4, a_6 \in K$ が存在して，
$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$
   が成り立つことを示せ.
5. q を素数の冪，m を 1 以上の整数，n を $q^m - 1$ の正の約数とする．$\beta \in \mathbb{F}_{q^m}$ を 1 の原始 n 乗根とする．l を整数，δ を 2 以上の整数とする．$f(X) \in \mathbb{F}_q[X]$ を，$f(\beta^l) = f(\beta^{l+1}) = \cdots = f(\beta^{l+\delta-2}) = 0$ を満たす $\mathbb{F}_q$ 係数モニック多項式の中で次数最小のものとして，$t = \deg f$ とする．$\mathbb{F}_q$ 上の符号 C を
$$C = \{(a_0, a_1, \ldots, a_{n-1}) \mid f(X)g(X) = a_0 + a_1X + \cdots + a_{n-1}X^{n-1}, g \in \mathbb{F}_q[X], \deg g \leq n - t - 1\}$$
   で定義する．このとき，C が講義で説明した意味（裏面参照）で BCH 符号であることを示せ.

注意

講義で説明した BCH 符号の定義は次の通りである．

q を素数の冪，m を 1 以上の整数，n を $q^m - 1$ の正の約数とする．l を整数，δ を 2 以上の整数とする．$\beta \in \mathbb{F}_{q^m}$ を 1 の原始 n 乗根とする．$\mathbb{F}_{q^m}$ 上の線形符号 $C(n, l, \delta)$ を次の生成行列で定義する．

$$H = \begin{pmatrix} 1 & \beta^{l} & \beta^{2l} & \dots & \beta^{(n-1)l} \\ 1 & \beta^{l+1} & \beta^{2(l+1)} & \dots & \beta^{(n-1)(l+1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \beta^{l+\delta-2} & \beta^{2(l+\delta-2)} & \dots & \beta^{(n-1)(l+\delta-2)} \end{pmatrix}.$$

このとき，符号 $C = C(n, l, \delta)^{\perp}|_{\mathbb{F}_q}$ を，設計距離を δ とする **BCH 符号**という．言い換えれば，符号 C は次の式で定まる．

$$C = \{c \in \mathbb{F}_q \mid H \cdot {}^t c = 0\}.$$

通常，BCH 符号はこの定義ではなく，問題 5 のように定義することが多い．