ProblemSet 4 – Finite fields and codes

George McNinch

due 2024-03-29

1. Let q be a power of a prime $p \neq 3$, let $k = \mathbb{F}_q$ and let $\ell = \mathbb{F}_{q^3}$ be the degree 3 extension.

   Suppose that $3 \mid q - 1$.

   (Examples: $q = 7, 13, 16, 19, 25, \ldots$)

   a. Show that there are elements $\alpha \in k$ for which $T^3 - \alpha \in k[T]$ is *irreducible*.

   b. Choose $\alpha \in k$ as in (a), explain why $\ell = k[\beta] \simeq k[T]/\langle T^3 - \alpha\rangle$ where $\beta^3 = \alpha$. Explain why $1, \beta, \beta^2$ is a k-basis for ℓ.

   View ℓ as a k-vector space; for any $\gamma \in \ell$, multiplication by γ defines a k-linear map

   $$\lambda_\gamma : \ell \to \ell \quad \text{defined by } \lambda_\gamma(x) = \gamma \cdot x$$

   The *trace* $\mathrm{tr} = \mathrm{tr}_{\ell/k} : \ell \to k$ is defined by $\mathrm{tr}(\gamma) = \mathrm{tr}(\lambda_\gamma)$.

   c. Compute the matrix of the linear mapping $\lambda_\beta : \ell = k[\beta] \to \ell = k[\beta]$ in the basis $1, \beta, \beta^2$.

   d. Prove that $\mathrm{tr}(1) = 3$ and $\mathrm{tr}(\beta) = \mathrm{tr}(\beta^2) = 0$. Conclude that $\mathrm{tr} : \ell \to k$ is a non-zero linear mapping.

   e. Compute the *matrix* of the bilinear form
   $$\langle -, - \rangle = \ell \times \ell \to k$$
   defined for $x, y \in \ell$ by $\langle x, y\rangle = \mathrm{tr}(xy)$ in the basis $e_0 = 1, e_1 = \beta, e_2 = \beta^2$. In other words, compute the 3×3 matrix
   $$M = (\langle e_i, e_j\rangle)_{ij} = (\mathrm{tr}(e_i e_j))_{ij} \in \mathrm{Mat}_{3\times 3}(k).$$

   f. Show that $\det M \neq 0$ so that $\langle x, y\rangle = \mathrm{tr}(xy)$ is a non-degenerate symmetric bilinear form on ℓ.

   g. Let X, Y, Z be polynomial variables, let
   $$v = X + Y\beta + Z\beta^2 = Xe_0 + Ye_1 + Ze_2 \in \ell[X, Y, Z]_1$$
   and compute [1]
   $$Q(X, Y, Z) := \langle v, v\rangle \in k[X, Y, Z]_2.$$
   Note that
   $$Q(X, Y, Z) = \begin{bmatrix} X & Y & Z \end{bmatrix} \cdot M \cdot \begin{bmatrix} X \\ Y \\ Z \end{bmatrix},$$
   and that Q is a homogeneous polynomial of degree 2.

   h. For any $P = (x : y : z) \in \mathbb{P}^2_k$, prove that $Q(P) \neq 0$.

2. Let $f = T^{11} - 1 \in \mathbb{F}_4[T]$.

   a. Show that $T^{11} - 1$ has a root in $\mathbb{F}_{4^5}$.

[1] We are extending the bilinear form linearly; to compute for example the quantity $\langle Xv + Yw, Zu\rangle$ for vectors $v, w, u \in \ell$, we must take
$$\langle Xv + Yw, Zu\rangle = XZ\langle v, u\rangle + YZ\langle w, u\rangle.$$

b. If $\alpha \in F_{4^5}$ is a primitive element – i.e. an element of order $4^5 - 1$, find an element $a = \alpha^i \in \mathbb{F}_{4^5}$ of order 11, for a suitable i.

c. Show that the minimal polynomial g of a over $\mathbb{F}_4$ has degree 5, and that the roots of g are powers of a. Which powers?

d. Show that $f = g \cdot h \cdot (T - 1)$ for another irreducible polynomial $h \in \mathbb{F}_4[T]$ of degree 5. The roots of h are again powers of a. Which powers?

e. Show that $\langle f \rangle$ is a $[11, 6, d]_4$ code for which $d \geq 4$.

3. Consider the following variant of a Reed-Solomon code: let $\mathcal{P} \subset \mathbb{F}_q$ be a subset with $n = |\mathcal{P}|$ and write $\mathcal{P} = \{a_1, \cdots, a_n\}$.

Let $1 \leq k \leq n$ and write $\mathbb{F}_q[T]_{<k}$ for the space of polynomial of degree $\leq k$, and let

$C \subset \mathbb{F}_q^n$ be given by

$$C = \{(p(a_1), \cdots, p(a_n)) \mid p \in \mathbb{F}_q[T]_{<k}.$$

a. Prove that C is a $[n, k, n-k]_q$-code.

b. If $P = \mathbb{F}_q^\times$, prove that C is a *cyclic code*.

c. If $q = p$ is *prime* and if $P = \mathbb{F}_p$, prove that C is a *cyclic code*.