ProblemSet 4 – Finite fields and codes

George McNinch

due 2024-03-01

1. Find the irreducible factors of the polynomial $T^9 - 1$ in $\mathbb{F}_7[T]$.

   (You should include proofs that the factors you describe are irreducible).

2. Let $0 < k, m \in \mathbb{N}$, put $n = mk$, and consider the subspace $C \subset \mathbb{F}_q^n$ defined by

   $$C = \{(v, v, \cdots, v) \mid v \in \mathbb{F}_q^k\} \subset \mathbb{F}_q^n.$$

   Find the *minimal distance* d of this code.

   For example, if $n = 6$, $k = 3$ and $m = 2$ then

   $$C = \{(a_1, a_2, a_3, a_1, a_2, a_3) \mid a_i \in \mathbb{F}_q\} \subset \mathbb{F}_q^6.$$

   (Corrected)

3. By an $[n, k, d]_q$-system we mean a pair $(V, \mathcal{P})$, where V is a finite dimensional vector space over $\mathbb{F}_q$ and $\mathcal{P}$ is an ordered finite family

   $$\mathcal{P} = (P_1, P_2, \cdots, P_n)$$

   of points in V (in general, points of $\mathcal{P}$ need not be distinct – you should view $\mathcal{P}$ as a *list* of points which may contain repetitions) such that $\mathcal{P}$ spans V as a vector space. Evidently $|\mathcal{P}| \geq \dim V$.

   The parameters $[n, k, d]$ are defined by

   $$n = |\mathcal{P}|, \quad k = \dim V, \quad d = n - \max_H |\mathcal{P} \cap H|.$$

   where the maximum defining d is taken over all linear hyperplanes $H \subset V$ and where points are counted with their multiplicity – i.e. $|\mathcal{P} \cap H| = |\{i \mid P_i \in H\}|$.

   Gjven a $[n, k, d]_q$-system $(V, \mathcal{P})$, let V^* denote the dual space to V and consider the linear mapping

   $$\Phi : V^* \to \mathbb{F}_q^n$$

   defined by

   $$\Phi(\psi) = (\psi(P_1), \cdots, \psi(P_n)).$$

   a. Show that Φ is injective.

   b. Write $C = \Phi(V^*)$ for the image of Φ, so that C is an $[n, k]_q$-code. Show that the minimal distance of the code C is given by d.

   c. Conversely, let $C \subset \mathbb{F}_q^n$ be an $[n, k, d]_q$-code, and put $V = C^*$. Let $e^1, \cdots, e^n \in (\mathbb{F}_q^n)^*$ be the dual basis to the standard basis. The restriction of e^i to the subspace C determines an element P_i of $C^* = V$. Write $\mathcal{P} = (P_1, P_2, \cdots, P_n)$ for the resulting list of vectors in V..

      Prove that the minimum distance d of the code C satisfies

      $$d = n - \max_H |\mathcal{P} \cap H|.$$

4. Let C be the linear code over $\mathbb{F}_5$ generated by the matrix

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

   a. Find a *check matrix* H for C.

   b. Find the minimum distance of C.

   c. Decode the received vectors $(0, 2, 3, 4, 3, 2)$ and $(0, 1, 2, 0, 4, 0)$ using syndrome decoding.

Bibliography