Assignment 1. Codes Over Finite Fields

Data Transmission and Cryptography

March 2025

A Constructing the finite field of size 9: $\mathbb{F}_9$

1. Prove that the polynomial $m(x) = x^2 + x + 2 \in \mathbb{Z}_3[x]$ is irreducible.

Consider the quotient ring $R = \mathbb{Z}_3[x]/(m(x))$. Since $m(x)$ is an irreducible primitive polynomial, the ring R is actually a field. In fact, there is only one finite field of this size, we will denote it by $\mathbb{F}_9$.

2. Let α be a root of $m(x)$ in $\mathbb{F}_9$. Show that α is a primitive element in $\mathbb{F}_9$. Give all elements of $\mathbb{F}_9 = \{0, 1, \alpha, \alpha^2, \ldots, \alpha^7\}$ in the form $u_1\alpha + u_0$, where $u_1, u_0 \in \mathbb{Z}_3$. For example, $\alpha^2 = 2\alpha + 1$.

3. Find the inverse of all nonzero elements in $\mathbb{F}_9$ (e.g., $(\alpha^2)^{-1} = \alpha^6 = \alpha + 2$).

B A linear code over the finite field $\mathbb{F}_9$

Consider the linear code C over the finite field $\mathbb{F}_9$ defined by the following generator matrix:

$$G = \begin{pmatrix} 1 & 0 & 2 & \alpha & 2 \\ \alpha & 1 & 0 & \alpha + 1 & \alpha + 2 \end{pmatrix} \tag{1}$$

1. Determine the length n and dimension k of C.

2. Determine $|C|$, that is, the number of codewords.

3. Encode the information vector $(1, 1)$ using the generator matrix G.

4. Is G in standard form? If not, find a generator matrix G_s in standard form (no need to make any column permutation).

5. Find a parity-check matrix H for C.

6. Show that $u = (\alpha + 2, 1, 1, 1, \alpha)$ is a codeword of C.

7. Give the syndrome of $v = (\alpha + 2, 1, 1, 2, \alpha)$ using H. Is it a codeword of C? Note that $v = u + (0, 0, 0, 1, 0)$. Compute the syndrome of $(0, 0, 0, 1, 0)$.

8. Determine the minimum distance and error correcting capability of C. Hint: Find the minimum number of linearly dependent columns in H.