Error-Correcting Codes: Assignment #2

Alfred Menezes (cryptography101.ca)

NOTE: You can attempt a question after watching all video lectures up to and including the one listed in the question title.

1. **Finite fields** (V2e)
   The polynomial $f(x) = x^4 + 3x^3 + 5$ is irreducible over $\mathbb{Z}_7$.
   (a) What is the order of the field $F = \mathbb{Z}_7[x]/(f(x))$?
   (b) Describe the elements of F.
   (c) What is the characteristic of F?
   (d) Perform the following computation in F: $(5x^3 + 3x^2 + 6) + (6x^2 + 6)$.
   (e) Perform the following computation in F: $(x + 1)^7 \cdot (4x^3 + 5x^2 + 6x + 4)^{2400}$.

2. **Irreducible polynomials** (V2e)
   Determine the irreducibility of the following polynomials.
   (You should do this question by hand, without the aid of a computer.)
   (a) $f(x) = 2x^4 + 2x^3 + 2x + 1$ over $\mathbb{Z}_3$.
   (b) $g(x) = 2x^4 + 2x^2 + x + 2$ over $\mathbb{Z}_3$.

3. **Generators** (V2e)
   Consider the field $F = GF(2^6) = \mathbb{Z}_2[x]/(x^6 + x + 1)$. Elements of this field are represented by polynomials $a_0 + a_1x + a_2x^2 + \cdots + a_5x^5$ where $a_i \in \{0, 1\}$. Show that $\alpha = x$ is a generator of $GF(2^6)^*$.
   (You should do this question by hand, without the aid of a computer.)

4. **Orders of field elements** (V2e)
   Let $\alpha \in GF(q)^*$. The *order* of α, denoted $\text{ord}(\alpha)$, is the smallest positive integer t such that $\alpha^t = 1$. Suppose that $\text{ord}(\alpha) = t$.
   (a) Prove that the elements $\alpha^0, \alpha^1, \ldots, \alpha^{t-1}$ are distinct.
   (b) Prove that $\text{ord}(\alpha) = \text{ord}(\alpha^{-1})$.

5. **Linear codes** (V3c)
   Consider the following generator matrix for a binary linear code C:

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

   (a) What are the length and dimension of C?
   (b) Encode the source message $m = (1101)$ with respect to the given G.
   (c) What are the length and dimension of $C^\perp$.
   (d) Find a parity-check matrix for C.

(e) Find a parity-check matrix for $C^{\perp}$.

(f) What is the distance of C? (Justify your answer.)

(g) What is the error-correcting capability of C?

(h) What is the error-detecting capability of C?