Chapter 9

Exercises to Chapter 9 (answers at end)

Version 2022-11-16. To accessible online version of these exercises

Exercise 9.1. Find all cyclic codes of weight 1 in $\mathbb{F}_q^n$.

Exercise 9.2. Let $C \subseteq \mathbb{F}_2^n$ be a binary cyclic code with generator polynomial $g(x)$. Prove that the following are equivalent: (i) $g(1) = 0$; (ii) the vector $\underline{g} \in \mathbb{F}_2^n$ has even weight; (iii) $C \subseteq E_n$.

Exercise 9.3. A *burst* of length $\leq l$ is defined as a vector in $\mathbb{F}_q^n$ with chosen l consecutive symbols such that all non-zeros occur only within the chosen l symbols.

(a) Explain why a burst of length $\leq l$ has weight at most l, but not every vector of weight l or less is a burst of length $\leq l$.

(b) Let $C \subseteq \mathbb{F}_q^n$ be a cyclic code with generator polynomial of degree r. Show that C can detect all burst errors of length $\leq r$. (*That is, a burst of length $\leq r$ is not a codeword.*) *Hint*: if a burst $\underline{b} \neq \underline{0}$ is a codeword, then all vectors obtained from $\underline{b}$ by cyclic shifts are also codewords. Shift $\underline{b}$ to positions $0, 1, \ldots, r-1$ so that the polynomial $b(x)$ is of degree $\leq r-1$. Show that a polynomial of degree $\leq r-1$ cannot be a codeword.

(*Informally: this means that burst error detection by cyclic codes is better than "generic" error detection. Cyclic codes are used for encoding information stored on CDs and memory cards and transmitted via Ethernet networks where the errors that occur are likely to be burst errors — scratches, electrical noise etc.*)

Exercise 9.4. Data read from an SD memory card is encoded by CRC-16-CCITT which is a binary cyclic code C with generator polynomial $g(x) = x^{16} + x^{12} + x^5 + 1$. The smallest n for which $g(x)$ divides the polynomial $x^n - 1$ in $\mathbb{F}_2[x]$ is $n = 32767$; accordingly, C is of length 32767.

(a) What is the number of rows and columns in the generator matrix of C? In the check matrix of C? What is the degree of the parity check polynomial of C?

(b) What is the rate of C?

(c) Show that C detects all burst errors of length up to 16.

(d) Explain why $d(C)$ is not greater than 4. Show that $d(C)$ is even. Prove that $d(C) = 4$.