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 $d(C) = 4$.

Chapter 10

Exercises to Chapter 10 (answers at end)

Version 2022-11-24. To accessible online version of these exercises

Exercise 10.1 (the extended binary Golay code)**.** The code G_{24} is defined as $\widehat{G}_{23}$, that is, by *extending* the binary Golay code defined earlier.

(a) Determine the parameters $[n, k, d]_q$ of G_{24}. State how many bit errors per codevector is the code guaranteed to *detect*. Same for *correct*. Find the rate of G_{24}.

(b) A codevector of G_{24} is transmitted, and thirteen bit errors occur. Will an error be detected?

(c) Prove that G_{24} is a self-dual code. The proof may involve calculations, but they should not be computer-aided — it should be possible to do them by hand in a reasonable amount of time.

Exercise 10.2 (*This exercise is discussed in the review sessions*)**.** Find all possible binary cyclic codes of length 7. For each such code, find its minimum distance, determine whether the code is perfect. Determine which codes that you obtain are linearly equivalent.

Exercise 10.3. (i) Show that a perfect ternary code of length 11 and minimum distance 5 must contain 729 codewords.

(ii) A football match can end in a Win (2), Draw (1) or Loss (0) for your club. You buy a *football pool* ticket which contains 11 boxes. You fill in the boxes trying to predict the result of each of the 11 matches your club will play in a forthcoming tournament. If, at the end of the tournament, it turns out that your ticket contained 9 or more correct guesses (out of 11), you win a prize.

(a) Assuming that the outcomes of the 11 matches are completely independent and random, show that one ticket wins a prize with a probability $\frac{1}{729}$. [*Of course, this does not mean that just by completing 729 tickets you are guaranteed a prize!*]

(b) Explain how one can use a code from (i) to buy and complete 729 football pool tickets and to *guarantee* that one of them wins a prize.