Homework #8

Due Sun, March 29th by 23:59pm in filedrop

Reading and plan for the next week:

1. For this homework assignment read 3.2, 3.3 and 7.1.

2. Plan for next week: We will continue talking about cyclic codes. I plan to cover 7.2 and 7.3 in detail and then briefly go over 7.4 and 7.5. If time left (unlikely, but possible), we will start talking about generalized Reed-Solomon codes. For this topic I will not be following the book; instead, we will probably follow the presentation in Chapter 6 of Yehuda Lindell's notes (see a link on the course webpage).

Problems:

1. Problem 3.7 (a)(b)(d) (part (c) was essentially done in class during Lecture 15)

2. Problem 3.10.

3. Problem 3.13. For a brief discussion of primitive elements see online notes from Lecture 15 (we did not get to that part in class). Note that to answer the question for $\mathbb{F}_8$ and $\mathbb{F}_9$ you first have to realize $\mathbb{F}_8$ and $\mathbb{F}_9$ in the form $\mathbb{F}_p[x]/(f(x))$ for appropriate p and irreducible $f(x) \in \mathbb{F}_p[x]$ (you have to choose specific $f(x)$ for your computation).

4. Problem 7.1. Make sure to prove your answer.

5. Problem 7.2.

6. Let A be an alphabet and $n \in \mathbb{N}$. Let us say that a code $C \subseteq A^n$ is **shift-invariant** if $(a_1 \dots a_n \in C \Rightarrow a_2 \dots a_n a_1 \in C)$. Thus, cyclic codes are precisely shift-invariant **linear** codes.

Now define a relation $\sim$ on A^n by $w \sim v \iff v$ can be obtained from w by a cyclic shift (by some number of positions). It is not hard to show that $\sim$ is an equivalence relation. One can reformulate the definition of a shift-invariant code in terms of $\sim$: a code $C \subseteq A^n$ is shift-invariant if and only if C is a union of (some) equivalence classes with respect to $\sim$.

(a) Describe the equivalence classes on $\mathbb{F}_2^3$ with respect to $\sim$

(b) Use (a) to determine the number of binary shift-invariant codes of length 3

(c) Now describe all binary cyclic codes of length 3 (and prove there are no other such codes).

7. Let F be a field and $n \in \mathbb{N}$.

(a) Let $C \subseteq F^n$ be a linear code. Suppose that C has a generator matrix G whose set of rows is invariant under cyclic shifts. Prove that C is a cyclic code.

(b) Give an example of a cyclic code which does NOT have a generator matrix G satisfying the condition in (a).