Homework #8

Due Sat, March 30th by 11:59pm on Canvas

Reading and plan for the next week:

1. For this homework assignment read 3.2, 3.3, 7.1 and beginning of 7.2 + online lectures 15 and 16 from Spring 20.

2. Plan for next week: We will continue talking about cyclic codes. Right now we are in the middle of online Lecture 16 from Spring 20. The current plan is to cover the rest of 16, 17 and at least the first half of 18. The corresponding sections in the book are 7.2 and 7.3.

Problems:

1. Problem 3.7 (b)(d). Note: we did part (a) in Lecture 16 in class on Tue, March 19th (but it is not included in the posted notes from Lecture 16). Part (c) is solved in the online Lecture 15 from Spring 20, but you should try to do it yourself first (either way you probably need to solve (c) as preparation for (d)).

2. Problem 3.10.

3. Problem 3.13. For a brief discussion of primitive elements see online notes from Lecture 15 from Spring 20 (we have not discussed primitive elements in class so far). 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.(a) Problem 3.9. The existence of $u(x)$ and $v(x)$ satisfying the condition of 3.9 (including the degree restrictions) follows from a general theorem stated in part (b) below.

(b) (bonus) Let F be a field, let $f(x), g(x) \in F[x]$ be nonzero polynomials, $h(x) = gcd(f(x), g(x))$, $n = \deg f(x)$, $m = \deg g(x)$ and $d = \deg h(x)$. Prove that the exist UNIQUE polynomials $u(x), v(x) \in F[x]$ such that

(i) $h(x) = f(x)u(x) + g(x)v(x)$ and

(ii) $\deg u(x) < n - d$ and $\deg v(x) < m - d$.

Moreover, prove that one can construct such $u(x)$ and $v(x)$ by applying part 2 of the Euclidean algorithm in $F[x]$. **Hint:** First prove the result in the special case where $h(x) = 1$. Then deduce the general case from this special case.

5. Problem 7.2.

6. Problem 7.3. Make sure to prove your answer.

7. Let A be an alphabet and $n \in \mathbb{N}$. Recall that a code $C \subseteq A^n$ is **shift-invariant** if $(a_1 \ldots a_n \in C \Rightarrow a_n a_1 \ldots a_{n-1} \in C)$.

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).

8. 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).