Homework #9

Due Sun, April 5th by 23:59pm in filedrop

Reading and plan for the next week:

1. For this homework assignment read 7.2 and 7.3.

2. Plan for next week: We will talk about some of the material in Chapter 8, but I am not yet sure about the order and whether we will follow the book or not. For instance, for the discussion of Reed-Solomon codes I currently plan to follow the presentation in Chapter 6 of Yehuda Lindell's notes (see a link on the course webpage).

Problems:

1. Let F be a field and $R_n(F) = F[x]/(x^n - 1)$.

(a) Prove (rigorously) that for any $u(x), v(x) \in R_n(F)$, their product in $R_n(F)$ (which we denote by $u(x) \odot v(x)$) is obtained from $u(x)v(x)$ (the product in the regular polynomial ring $F[x]$) by replacing x^k by $x^{k \bmod n}$ for each k (as usual, $k \bmod n$ is the principal remainder of dividing k by n).

(b) Let $g(x) = \sum_{i=0}^{n-1} x^i$. Use (a) to prove that $\langle g(x) \rangle$, the principal ideal of $R_n(F)$ generated by $g(x)$, is equal to $\{a \cdot g(x) : a \in F\}$, the set of scalar multiples of $g(x)$.

2. Problem 3.23(b)(d)(e). **Hint:** For two of the three parts you can use a suitable theorem from Lecture 18. For the third part you can perform factorization by "brute force" (keep doing natural factorizations as long as you can and then try to show that the factors are irreducible).

3. Problem 7.6. Make sure to include all your work.

4. Let F be a field, $n \in \mathbb{N}$, let $C \subseteq F^n$ be a cyclic code and let $g(x)$ be the generator polynomial for C. Let $k = \deg g(x)$, and write $g(x) = \sum_{i=0}^{k} g_i x^i$. Recall that the **reciprocal polynomial** $\bar{g}(x)$ is defined by

$$\overline{g}(x) = x^k g\left(\frac{1}{x}\right) = \sum_{i=0}^{k} g_{k-i} x^i.$$

Let $g'(x) = \frac{\overline{g}(x)}{g_0}$ (note that $g'(x)$ is monic).

(a) Prove that $\overline{g}(x)$ divides $x^n - 1$ (in $F[x]$) and hence $g'(x)$ divides $x^n - 1$ as well.

(b) By (a) and the correspondence between cyclic codes and monic divisors of $x^n - 1$, there exists a unique cyclic code C' whose generator polynomial is $g'(x)$. Prove that C' is equivalent to C. **Hint:** Use Theorem 7.3.1. It may be useful to start with the case $g_0 = 1$ (so that $g' = \overline{g}$). The proof in the general case is not that different from this special case.

5. Problem 7.11. Also find (with proof) all monic divisors of $x^{15} - 1$ such that the corresponding cyclic code is equivalent to the Hamming code $Ham(4, 2)$.

6. Problem 7.15.

7. Problem 7.22. **Hint:** There is a problem from Chapter 4 (which was previously assigned as a homework problem) that is very relevant.