Homework #11

Due Tue, April 28th by 11:59pm in filedrop

Reading and plan for the last class:

1. For this homework assignment read 5.2.2 in the book, 4.2 and Chapter 7 in Lindell's notes and class notes from Lectures 22-24.

2. Plan for the last class: We will start by introducing concatenation of codes (6.3.1 in the book and 7.2 in Lindell's notes). Then I plan to go back to Lecture 24 and present a corrected construction of asymptotically good sequences of codes that can be constructed in polynomial time. There should be time left after that, so we may be able to briefly discuss another topic.

Problems:

1. Let us recall the restriction of scalars construction introduced in Lecture 22. Let p be a prime, $m \in \mathbb{N}$ and $q = p^m$. As usual, we can identify the field $\mathbb{F}_q$ with the set

$$Pol_k(\mathbb{F}_p) = \left\{ \sum_{i=0}^{m-1} a_i x^i : a_i \in \mathbb{F}_p \right\}$$

consisting of polynomials over $\mathbb{F}_p$ of degree $\leq k-1$. To describe the multiplication in $Pol_k(\mathbb{F}_p)$ under this identification we need to choose an irreducible polynomial of degree k over $\mathbb{F}_p$, but this will not be necessary here.

Define the map $\rho : \mathbb{F}_q \to \mathbb{F}_p^m$ which sends each polynomial to the sequence of its coefficients:

$$\rho\left(\sum_{i=0}^{m-1} a_i x^i\right) = (a_0, a_1, \ldots, a_{m-1})$$

(ρ is the inverse of the map that we always denoted by π in our discussion of cyclic codes).

For any $n \in \mathbb{N}$ we can extend ρ to a map $\rho_n : \mathbb{F}_q^n \to (\mathbb{F}_p^m)^n = \mathbb{F}_p^{mn}$ which applies ρ to each coordinate:

$$\rho_n((f_1(x), \ldots, f_n(x))) = (\rho(f_1(x)), \ldots, \rho(f_n(x))),$$

or, more explicitly,

$$\rho_n(\sum_{i=0}^{m-1} a_{i1}x^i, \sum_{i=0}^{m-1} a_{i2}x^i, \ldots, \sum_{i=0}^{m-1} a_{in}x^i) \\ = (a_{01}, a_{11}, \ldots, a_{m-1,1}, a_{02}, \ldots, a_{m-1,2}, \ldots, a_{0n}, \ldots, a_{m-1,n}).$$

It is straightforward to check that ρ_n is an isomorphism of vector spaces over $\mathbb{F}_p$.

Now let C be a linear code over $\mathbb{F}_q$ of length n, and define $C_{\mathbb{F}_p} = \rho_n(C)$. We say that the code $C_{\mathbb{F}_p}$ is obtained from C by *restriction of scalars*. Finally, we formulate the actual problem:

(a) Let C be the zero-sum code of length 3 over $\mathbb{F}_4$, that is, $C = \{(x_1, x_2, x_3) \in \mathbb{F}_4^3 : x_1 + x_2 + x_3 = 0\}$. Describe the code $C_{\mathbb{F}_2}$ as the set of solutions to (an explicit) system of linear equations over $\mathbb{F}_2$.

(b) Let C be any $[n, k, d]$-linear code over $\mathbb{F}_{p^m}$. Prove that $C_{\mathbb{F}_p}$ is an $[nm, km, d']$-linear code over $\mathbb{F}_p$ with $d' \geq d$ (this is the first part of Theorem 22.2 from class).

2.

(a) Deduce from the binary Plotkin bound that for any $n, d \in \mathbb{N}$ with $n \leq 2d$ we have $A_2(n, d) \leq 4d$.

(b) Now assume that $n > 2d$. Prove that $B_2(n, d) \leq 2^{n-2d+2} \cdot d$, that is, for any binary linear code C of length n and distance d we have $|C| \leq 2^{n-2d+2} \cdot d$.

Hint: Given $m \leq n$, let us think of $\mathbb{F}_2^m$ as the subspace of $\mathbb{F}_2^n$ consisting of all vectors whose last $n - m$ coordinates are zero. Now consider the code $C' = C \cap \mathbb{F}_2^{2d}$. Show that the size of C' can be bounded above using the Plotkin bound. Then use the fact that $\dim(U \cap W) = \dim(U) + \dim(W) - \dim(U + W)$ for any vector subspaces U and W of a finite-dimensional vector space V, deduce the desired bound on $|C|$.

(c) Now let $\mathcal{C} = \{C_m\}_{m=1}^{\infty}$ be a sequence of binary linear codes. Assume that C_m is $[n_m, k_m, d_m]$-linear where $n_m \to \infty$ as $m \to \infty$. Also assume that the asymptotic relative distance $\delta(\mathcal{C}) = \liminf_{m\to\infty} \delta(C_m) = \liminf_{m\to\infty} \frac{d_m - 1}{n_m}$ satisfies $\delta(\mathcal{C}) \geq \frac{1}{2}$. Use (a) and (b) to prove that $R(\mathcal{C}) = 0$.

Recall that $R(\mathcal{C}) = \liminf_{m\to\infty} R(C_m) = \liminf_{m\to\infty} \frac{k_m}{n_m}$. If you are not comfortable with liminf, you may assume that the limit in the definition of $\delta(\mathcal{C})$ exists.

3. Prove Lemma 24.1 from class.

4. Prove that an $[n, k, d]$-linear code over $\mathbb{F}_q$ satisfying the Gilbert-Varshamov bound can be constructed using at most $q^{n-k} \cdot k(n-k)$ additions in $\mathbb{F}_q$.

5. Let $B = PCC_3$, the parity-check code of length 3, and let A be the zero-sum code of length 4 over $\mathbb{F}_4$. Verify that the concatenated code $B \circ A$ is defined and compute its length, dimension, distance AND a generator matrix. **Note:** For the definition of the concatenated code see Theorem 6.3.1 in the book or 7.2 in Lindell's notes; I recommend the latter. The concatenated code is defined as the image of a certain injective linear map. Whenever the code is defined in this way, there is a simple general way to find its GM – if you are not sure what it is, recall the definition of GM.