Homework #10, due Tue, April 26th by 11:59pm in filedrop

Reading and plan for the next week:

1. For this homework assignment read 7.5, 6.1 and 6.2 in Lindell's notes and online notes from Lectures 19-22.

2. Plan for the next 3 classes. On Tue, April 19, we will continue talking about burst error correction (online lectures 21 and 22 and Section 7.5 in the book). On Thu, April 21 and Tue, April 26 we will talk about Asymptotically good codes (online lectures 23 and 24). This topic is not in our main book. It is discussed in Lindell's notes (see 4.1, 4.2 and Chapter 7), although these sections contain considerably more material than what we will cover in class.

Problems:

1. Let C be a narrow-sense RS (Reed-Solomon) code over $\mathbb{F}_7$ (as defined in online Lecture 20) of dimension $k = 4$ (such a code is unique up to the choice of primitive element α). Write down explicitly a GM for C, a PCM for C and the generator polynomial for C (all matrix entries and coefficients of the polynomial in your answer should be explicit elements of $\mathbb{F}_7$).

2. Let F be a finite field, $q = |F|$ and $n = q - 1$.

(a) Given $\beta \in F$, let $\Sigma(\beta) = \sum_{j=0}^{n-1} \beta^j$. Prove that $\Sigma(0) = 1$, $\Sigma(1) = -1$ and $\Sigma(\beta) = 0$ for $\beta \neq 0, 1$. **Hint:** Consider the cases $\beta = 0, 1$ separately. For all other β recall how to find the sum of a finite geometric progression. **Warning:** $F \ncong \mathbb{Z}_q$ unless q is prime.

(b) Let us recall the definition of GRS codes (below we are using notation from class which is a bit different from online notes). Fix an integer $1 \leq k \leq n-1$, and let $\vec{\alpha} = (\alpha_1, \ldots, \alpha_n)$ and $\vec{v} = (v_1, \ldots, v_n)$ where $\alpha_i, v_i \in F \setminus \{0\}$ for all i and $\{\alpha_i\}$ are distinct. Define $H_k(\vec{\alpha}, \vec{v}) \in Mat_{(n-k)\times n}(F)$ by

$$H_k(\vec{\alpha}, \vec{v}) = \begin{pmatrix} v_1 & v_2 & \ldots & v_n \\ v_1\alpha_1 & v_2\alpha_2 & \ldots & v_n\alpha_n \\ v_1\alpha_1^2 & v_2\alpha_2^2 & \ldots & v_n\alpha_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ v_1\alpha_1^{n-k-1} & v_2\alpha_2^{n-k-1} & \ldots & v_n\alpha_n^{n-k-1} \end{pmatrix}$$

Recall that $GRS_k(\vec{\alpha}, \vec{v}, PCM)$ is the linear code over F whose PCM is $H_k(\vec{\alpha}, \vec{v})$ and $GRS_k(\vec{\alpha}, \vec{v}, GM)$ is the linear code over F whose GM is $H_{n-k}(\vec{\alpha}, \vec{v})$. Note that $GRS_k(\vec{\alpha}, \vec{v}, PCM)$ and $GRS_k(\vec{\alpha}, \vec{v}, GM)$ are both $[n, k]$-linear codes.

Now assume that the locator sequence $\vec{\alpha}$ is *primitive*, that is, there exists a primitive element $\alpha \in F$ such that $\alpha_i = \alpha^{i-1}$ for $1 \leq i \leq n$. Define the vector $\vec{w} = (w_1, \ldots, w_n)$ by $\vec{w} = \frac{\vec{\alpha}}{\vec{v}}$, that is, set $w_i = \frac{\alpha_i}{v_i} = \frac{\alpha^{i-1}}{v_i}$ for all i. Prove that

$$GRS_k(\vec{\alpha}, \vec{w}, GM) = GRS_k(\vec{\alpha}, \vec{v}, PCM) \qquad (***)$$

Hint: Prove by direct computation that $H_k(\vec{\alpha}, \vec{v}) \cdot H_{n-k}(\vec{\alpha}, \vec{w})^T = 0$ and then deduce (***) from this equality arguing similarly to the proof of Theorem 19.4 from online notes (in class this theorem was proved at the beginning of Lecture 20 on Thu, April 6th).

3. Give a new proof of the fact that GRS codes are MDS using polynomial representation of GRS codes (see the section "Explicit description of elements of $GRS_k(\vec{\alpha}, \vec{v})$" at the end of Lecture 19). You only need to use the description obtained in this section, not the original definition. **Hint:** use the fact that for any field F, a nonzero polynomial of degree m over F cannot have more than m roots.

4. Prove Lemma 21.2 from online notes (=Lemma 23.2 from class). In the proof make sure to use the definition given in online Lecture 21. **Hint:** for the second part of Lemma 21.2 (dealing with burst error correction) it may be convenient to "negate the definition of an E-error correcting code", that is, to rewrite the definition in the form "A code C is NOT E-error correcting $\iff$ ..."

5. Prove Theorem 22.1 from online notes. I plan to prove the analogue of this result for burst error detection in class on Tue, April 19.