Homework #10, due Thu, April 25th by 11:59pm on Canvas

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 (Lectures 20-23 from this semester and Lectures 19-22 from Spring 20 – content is mostly the same, but there are some differences).

2. Plan for the next week. Asymptotically good codes and concatenated codes (lectures 23-25 from Spring 20). These topics are not in our main book. They are 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. Prove Lemma 22.2 from class (=Lemma 21.2 from Spring 20 notes). In the proof make sure to use the formal definition given in class. **Hint:** for the second part (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 $\iff$ ..."

2. Prove the error detection part of Theorem 23.2 restated below. Let C be an $[n, k, d]$-linear code over $\mathbb{F}_{p^r}$, and let $C_{\mathbb{F}_p}$ be the code over $\mathbb{F}_p$ obtained from C by restriction of scalars (see Lecture 23 for the definition).

(a) Prove that $C_{\mathbb{F}_p}$ is $[nr, kr, d']$-linear for some $d' \geq d$.

(b) Assume that C is m-burst error detecting for some m. Prove that $C_{\mathbb{F}_p}$ is $m(r-1)+1$-burst error detecting. You should also think how you would prove the analogous statement for burst error correction, but it is optional to write down the latter proof.

3. Let $n \geq 2$ be an integer and let C be a BINARY MDS code of length n. Prove that C is a trivial MDS code, that is, C is equal to the full code $\mathbb{F}_2^n$, PCC_n or the simple repetition code $Rep(1, n)$.

Hint: Let $k = \dim(C)$. Assuming that $C \neq F^n$, we get that $k < n$, so that PCM of C is non-empty. After replacing C by an equivalent code, we can assume that C has a PCM H in the standard form, so that the last $n-k$ columns of H form the identity matrix. Now use a suitable theorem to show that there are very few choices for the remaining

columns of H and eventually deduce that $k = n - 1$ or $k = 1$, and in each case H is unique, with the corresponding codes being PCC_n and $Rep(1, n)$. Note that this would only prove that C is equivalent to PCC_n or $Rep(1, n)$. You still have to explain why C is EQUAL to one of those codes.

4. Let C be a narrow-sense RS (Reed-Solomon) code over $\mathbb{F}_7$ (as defined near the end of Lecture 21) of dimension $k = 4$ (such a code is unique up to the choice of primitive element α). Write down explicitly a GM for C (for your choice of α), 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 $\mathbb{F}_7$).

5. Give a new proof of the fact that GRS codes are MDS using polynomial representation of GRS codes (see the section "Encoding and explicit description of elements of $GRS_k(\vec{\alpha}, \vec{v})$" in Lecture 21). 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.