Homework #7. Due Saturday, March 23rd, by 11:59pm on Canvas

All reading assignments and references to exercises, definitions etc. are from our main book 'Coding Theory: A First Course' by Ling and Xing

Reading and plan for the next week:

1. For this homework assignment read 5.2, 5.3, 5.5 and 5.6.

2. Plan for next week: Finish polynomial rings and basic theory of finite fields (3.2 and parts of 3.3; see also online lecture 15 from Spring 2020). Cyclic codes (7.1 and start 7.2; see also online lectures 16 and 17 from Spring 2020).

Problems:

1. Let $r \geq 2$ be an integer.

(a) Assume that $d \geq 3$. Prove that there is no binary $[2^r, 2^r - r, d]$-linear code.
(b) Given an example of a binary $[2^r, 2^r - r - 1, 4]$-linear code.

2. Problem 5.14.

3. Prove the first part of the **binary** Plotkin bound (part (i) of Theorem 5.5.3 in the case $n < 2d$). **Note:** In class we proved a slightly weaker bound, namely, $A_2(n,d) \leq \lfloor \frac{2d}{2d-n} \rfloor$ instead of $A_2(n,d) \leq 2\lfloor \frac{d}{2d-n} \rfloor$. You may look up the proof on wikipedia,
`https://en.wikipedia.org/wiki/Plotkin_bound`
but note that there is an unjustified statement in that proof.

4. Combining the sphere-packing bound with the first inequality of Corollary 5.2.7 (which is essentially a reformulation of the Gilbert-Varshamov bound), we get that for any prime power q and any integers $1 \leq d \leq n$ we have

$$q^{n - \lceil \log_q(V_q^{n-1}(d-2)+1) \rceil} \leq B_q(n,d) \leq A_q(n,d) \leq \frac{q^n}{V_q^n(\lfloor \frac{d-1}{2} \rfloor)}. \qquad (***)$$

Verify that in the case $n = \frac{q^r - 1}{q-1}$ and $d = 3$ (these are the length and the distance of the Hamming code $Ham(r,q)$), the expressions on the left-hand and the right-hand side of (***) are equal. **Note:** This a rare case when a lower bound and an upper bound (on the size of a code) obtained from very general considerations coincide with each other.

5. Use the Gilbert-Varshamov bound to show that there exists a $[8, 3, 4]$-linear binary code. Then use the algorithm from the proof of the Gilbert-Varshamov bound to explicitly construct an $[8, 3, 4]$-linear binary code. The point of this problem is to construct such a code using a specific algorithm; just defining a code in some other way and proving it is an $[8, 3, 4]$-linear code will not be an acceptable solution.

6. Problem 5.37 (see Problem 5.36 for the relevant definitions).

7. The Hadamard codes $\{\text{Hdr}(k)\}_{k=0}^{\infty}$ are binary codes defined inductively by $\text{Hdr}(0) = \{0, 1\}$ and

$$\text{Hdr}(k) = \{ww, w\overline{w} : w \in \text{Hdr}(k-1)\} \text{ for } k \geq 1$$

where $\overline{w}$ is the word obtained from w by flipping every symbol, and ww and $w\overline{w}$ are concatenations. For instance, $\text{Hdr}(1) = \{00, 01, 11, 10\}$, $\text{Hdr}(2) = \{0000, 0011, 0101, 0110, 1111, 1100, 1010, 1001\}$ (note that $\text{Hdr}(0)$ and $\text{Hdr}(1)$ are full codes of length 1 and 2, respectively, but $\text{Hdr}(k)$ is not full for $k \geq 2$)

(a) List all the elements of $\text{Hdr}(k)$ for $k = 3$ and $k = 4$.

(b) Prove that $\text{Hdr}(k)$ is a $(2^k, 2^{k+1}, 2^{k-1})$-code for $k \geq 1$.

Note: The statements about the length and size of $\text{Hdr}(k)$ follow easily from the definition, but you should still explain why they hold. For the statement about the distance it is convenient to prove the following stronger result by induction: $d(\text{Hdr}(k)) = 2^{k-1}$ AND $\text{Hdr}(k)$ is closed under inversion, that is, $(w \in Hdr(k) \Rightarrow \overline{w} \in \text{Hdr}(k))$.