Homework #7

Due Thu, March 19th by 23:59pm in my mailbox or collab filedrop

Reading and plan for the next week:

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

2. Plan for next week: Polynomial rings and basic theory of finite fields (3.2 and parts of 3.3). Start talking about cyclic codes (7.1 and maybe 7.2).

Problems:

1. Redo problem 4 on the midterm (=Problem 5.6 in the book). No need to submit if you got full credit on the midterm.

2. Use the result of Problem 5.19 to show that the simplex codes $S(r,q)$ attain the Griesmer bound.

3.

(a) Read (and understand) the proof of the Gilbert-Varshamov bound (5.2.2)

(b) Combining the sphere-packing bound with the first inequality of Corollary 5.2.7, we get that for any prime power q and any integers $1 \le d \le n$ we have

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

Verify that in the case $n = \frac{q^r-1}{q-1}$ and $d = 3$ (these are length and 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.

4. Recall from Lecture 14 that the Hadamard codes $\{\mathrm{Hdr}(k)\}_{k=0}^{\infty}$ are binary codes defined inductively by $\mathrm{Hdr}(0) = \{0,1\}$ and

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

(here $\overline{w}$ is the word obtained from w by flipping every symbol, and ww and $w\overline{w}$ are concatenations).

(a) List all the elements of $\mathrm{Hdr}(k)$ for $k = 3$ and $k = 4$ (we did the same in class for $k \le 2$).

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

Note: The statements about the length and size of $\mathrm{Hdr}(k)$ 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: $d(\mathrm{Hdr}(k)) = 2^{k-1}$ AND $\mathrm{Hdr}(k)$ is closed under inversion, that is, $(w \in Hdr(k) \Rightarrow \overline{w} \in \mathrm{Hdr}(k))$.

5. 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 $A_2(n,d) \leq 2\lfloor \frac{d}{2d-n} \rfloor$. Explain how you use the assumption that d is even in your proof. You may look up the proof on wikipedia, but note that there is an unjustified statement in that proof.

6. Problem 5.14.

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