Error Correcting Codes: Combinatorics, Algorithms and Applications Spring 2010

HOMEWORK 2
Due Friday February 26, 2010 in class

You can collaborate in groups of up to 3. However, the write-ups must be done individually, that is, your group might have arrived at the solution of a problem together but everyone in the group has to write up the solution in their own words. Further, you **must** state at the beginning of your homework solution the names of your collaborators. Just to be sure that there is no confusion, the group that you pick has to be for all problems [i.e. you cannot pick different groups for different problems :-)]

If you are not typesetting your homework, please make sure that your handwriting is legible. Illegible handwriting will most probably lose you points.

Unless stated otherwise, for all homeworks, you are **only** allowed to use notes from the course: this includes any notes that you might have taken in class or any scribed notes from Fall 07 or Spring 09 version or the current version of the course. Doing otherwise will be considered cheating. Note that if your collaborator cheats and you use his/her solution, then you have cheated too (ignorance is not a valid excuse).

Please use the comments section of the post on HW 2 on the blog if you have any questions and/or you need any clarification.

For this homework, you are limited to **six pages** in total.

This homework has more problems and is harder than the previous one, so I encourage you to start thinking on the problems **early**.

---

1. (**Operations on Codes**) $(1 + 2 + 1 + 1 = 5$ points) In class we have seen some examples of how one can modify one code to get another code with interesting properties (for example, the construction of the Hadamard code from the Simplex code and the construction of codes with smaller block lengths in the proof of the Singleton bound). In this problem you will need to come up with various ways of constructing new codes from existing ones.

   Prove the following statements (recall that the notation $(n, k, d)_q$ code is used for general codes with q^k codewords where k need not be an integer, whereas the notation $[n, k, d]_q$ code stands for a *linear code* of dimension k):

   (a) If there exists an $(n, k, d)_q$ code, then there also exists an $(n - 1, k, d' \geq d - 1)_q$ code.

   (b) If there exists an $(n, k, d)_2$ code with d odd, then there also exists an $(n + 1, k, d + 1)_2$ code.

   (c) If there exists an $(n, k, d)_{2^m}$ code, then there also exists an $(nm, km, d' \geq d)_2$ code.

   (d) If there exists an $[n, k, d]_{2^m}$ code, then there also exists an $[nm, km, d' \geq d]_2$ code.

Note: In all the parts, the only things that you can assume about the original code are only the parameters given by its definition– nothing else! The proofs for each part should not take more than a few sentences.

2. (**Distance of General Random Codes**) (5 points) In class, we saw Varshamov's proof that random *linear* code meets the GV bound. It is natural to as the question for general random codes. (By a random $(n,k)_q$ code, I mean the following: for each of the q^k messages, pick a random vector from $[q]^n$. Further, the choices for each codeword is independent.) We will do so in this problem.

   (a) Prove that a random binary code with rate $R > 0$ with high probability has relative distance $\delta \geq H^{-1}(1-2R-\epsilon)$.[1] Note that this is worse than the bound we proved in class for random linear codes.

   (*Hint:* Proceed with the proof as in the random linear case: what events do you now need to take care of in the union bound?)

   (b) (*For your cognitive pleasure only; no need to turn this part in in*)
   Prove that with high probability the relative distance of a random code of rate R is at most $H^{-1}(1-2R)+\epsilon$. In other words, general random codes are worse than random linear codes in terms of their distance.

3. (**Toeplitz Matrix**) ($1+10+2+2=15$ points) In class we saw that the Gilbert construction can compute an $(n,k)_q$ code in time $q^{O(n)}$. Now the Varshamov construction is a randomized construction and it is natural to ask how quickly can we compute an $[n,k]_q$ code that meets the GV bound. In this problem, we will see that this can also be done in $q^{O(n)}$ deterministic time, though the deterministic algorithm is not that straight-forward anymore.

   (a) (*A warmup*) Argue that Varshamov's proof gives a $q^{O(kn)}$ time algorithm that constructs an $[n,k]_q$ code on the GV bound. (Thus, the goal of this problem is to "shave" off a factor of k from the exponent.)

   (b) A $k \times n$ *Toeplitz Matrix* $A = \{A_{i,j}\}_{i=1,\,j=1}^{k,\,n}$ satisfies the property that $A_{i,j} = A_{i-1,j-1}$. In other words, any diagonal has the same value. For example, the following is a 4×6 Toeplitz matrix:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 7 & 1 & 2 & 3 & 4 & 5 \\ 8 & 7 & 1 & 2 & 3 & 4 \\ 9 & 8 & 7 & 1 & 2 & 3 \end{pmatrix}$$

   A *random* $k \times n$ Toeplitz matrix $T \in \mathbb{F}_q^{k \times n}$ is chosen by picking the entries in the first row and column uniformly (and independently) at random.

   Prove the following claim: For any non-zero $\mathbf{m} \in \mathbb{F}_q^k$, the vector $\mathbf{m} \cdot T$ is uniformly distributed over $\mathbb{F}_q^n$, that is for every $\mathbf{y} \in \mathbb{F}_q^n$, $\Pr[\mathbf{m} \cdot T = \mathbf{y}] = q^{-n}$.

   (*Hint:* Write down the expression for the value at each of the n positions in the vector $\mathbf{m} \cdot T$ in terms of the values in the first row and column of T. Think of the values in the first row and column as variables. Then divide these variables into two sets (this

[1] I forgot to mention this in class but generally $H(\cdot)$ is used to denote $H_2(\cdot)$. Further the "inverse" function $H^{-1}(\cdot)$ is defined as follows. For every $y \in [0,1]$, $H^{-1}(y) = x$ iff $H(x) = y$ and $x \in [0, 1/2]$.

"division" will depend on $\mathbf{m}$) say S and $\overline{S}$. Then argue the following: for every fixed $\mathbf{y} \in \mathbb{F}_q^n$ and for every fixed assignment to variables in S, there is a unique assignment to variables in $\overline{S}$ such that $\mathbf{m}T = \mathbf{y}$.)

(c) Briefly argue why the claim in part (b) implies that a random code defined by picking its generator matrix as a random Toeplitz matrix with high probability lies on the GV bound.

(d) Conclude that an $[n, k]_q$ code on the GV bound can be constructed in time $q^{O(k+n)}$.

Note: Even if you cannot prove part (b) you can still use its statement as given for parts (c) and (d).