Error Correcting Codes: Combinatorics, Algorithms and Applications Spring 2011

Homework 1

Due Monday, February 21, 2011 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, Spring 09, Spring 10 version or the current version of the course. Doing otherwise will be considered cheating. Note that if your collaborator cheats and you use his solution, then you have cheated too (ignorance is not a valid excuse).

Please use the comment section of the post on HW 1 on the blog if you have any questions and/or you need any clarification.

You might find the Problem 1 in HW 0 useful for this homework. You can use any statement from HW 0 without proof.

All the problems in the homework should be simple. Also the solutions are short, so you are allowed to use only one page per problem (part). Anything that follows after the first page (for any problem) will not be graded. Note that in total you can use **three** pages for this homework.

---

1. (**Systematic Codes**) ($4 + 6 = 10$ points) In the class we did not talk about how to obtain the parity check matrix of a linear code from its generator matrix. In this problem, we will look at this "conversion" procedure.

   (a) Prove that any generator matrix $\mathbf{G}$ of an $[n, k]_q$ code C (recall that $\mathbf{G}$ is a $k \times n$ matrix) can be converted into another equivalent generator matrix of the form $\mathbf{G}' = [\mathbf{I}_k|\mathbf{A}]$, where $\mathbf{I}_k$ is the $k \times k$ identity matrix and $\mathbf{A}$ is some $k \times (n-k)$ matrix. By "equivalent," I mean that the code generated by $\mathbf{G}'$ has a linear bijective map to C.

   Note that the code generated by $\mathbf{G}'$ has the message symbols as its first k symbols in the corresponding codeword. Such codes are called *systematic codes*. In other words, every linear code can be converted into a systematic code.

   (b) Given an $k \times n$ generator matrix of the form $[\mathbf{I}_k|\mathbf{A}]$, give a corresponding $(n-k) \times n$ parity check matrix. Briefly justify why your construction of the parity check matrix is correct.

(*Hint*: Try to think of a parity check matrix that can be decomposed into two submatrices: one will be closely related to $\mathbf{A}$ and the other will be an identity matrix, though the latter might not be a $k \times k$ matrix).

2. (**Correcting erasures for linear codes**) (5 points) A nice property of linear codes that we did not cover in class is that one can correct erasures in polynomial time. In this problem you will prove this fact.

   Let C be an $[n, k, d]_q$ code. Let $\mathbf{y} = (y_1, \ldots, y_n) \in (\mathbb{F}_q \cup \{?\})^n$ be a received word[1] such that $y_i =?$ for at most $d-1$ values of i. Present an $O(n^3)$ time algorithm that outputs a codeword $\mathbf{c} = (c_1, \ldots, c_n) \in C$ that agrees with y in all un-erased positions (i.e., $c_i = y_i$ if $y_i \neq ?$) or states that no such $\mathbf{c}$ exists. (Recall that if such a $\mathbf{c}$ exists then it is unique.)

[1] A ? denotes an erasure.