ENEE626. Final examination, due on 12/17/09, 1:30pm **Instructor:** A. Barg

1. *This is a take-home exam.* If you cannot submit the paper on 12/17, please make sure to submit it *before* that date. No late papers will be accepted. Papers are to be submitted to my office (AVW 2361). If I am not there, slide the paper under the office door.

2. Any sources, such as books, course notes, and WWW can be consulted. However you must work on your own, not turning to anyone for advice.

3. *Complete* proofs are required. Intermediate calculations should be shown. If applicable, clearly identify the answer to the problem. Give a succinct (this means short) proof of the claim with no side remarks or examples. A complete solution of each question is worth **20** points.

4. On the first page of the exam paper, write the following:

"*I certify that I completed this assignment myself* (sign your name)"

Questions.

1. Let G be a binary (0-1) matrix of dimensions $k \times n$ in which every element is a Bernoulli $(1/2, 1/2)$ random bit. Let A_w be the random number of codewords of weight w in the code generated by G. Find $\mathbb{E}A_w, \text{Var}(A_w)$ for $w = 0, 1, \dots, n$.

2. Let $\Phi = \{C_i, i = 1, 2, \dots\}$ be a family of linear codes over a finite field $\mathbb{F}_q$ in which every code C_i has length n and dimension k. Suppose that every vector $\boldsymbol{x} \in \mathbb{F}_q^n$ is contained in the same number of codes from Φ.

(a) Prove that if

$$\sum_{i=0}^{d-1} \binom{n}{i} (q-1)^i < \frac{q^n - 1}{q^k - 1},$$

then Φ contains a code with distance d.

(b) Let $q = 2$. Show that for $n \to \infty$ the family Φ contains codes that meet the asymptotic GV bound.

3. Consider a $[n, m+1]$ linear code C over $\mathbb{F}_q$ with generator matrix formed of $n = q^m$ columns of the form $(1, \boldsymbol{x})^t$, where $\boldsymbol{x}$ runs over all the vectors in $(\mathbb{F}_q)^k$. (For $q = 2$ this is the $RM(1, m)$ code).

(a) Prove that the distance of the code equals $d = q^{m-1}(q-1)$ and that $A_d = q(q^m - 1)$. What are the weights of the other q code vectors?

(b) Prove that no $[q^m, q^{m+1}]$ linear q-ary code can have distance $d > q^{m-1}(q-1)$. (For that, derive a q-ary version of the Plotkin bound for linear codes following our argument in Theorem 6.3.)

4. Consider a code $\mathscr{P} = B \otimes B$ where B is a binary $[n = k+1, k, 2]$ single parity-check code, $k \geq 2$. We assume systematic encoding with the message symbols occupying the first k columns in the first k rows.

(a) Let

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1k} & a_{1,k+1} \\ \vdots & \vdots & & \vdots & \vdots \\ a_{k1} & a_{k2} & \cdots & a_{kk} & a_{k,k+1} \\ a_{k+1,1} & a_{k+1,2} & \cdots & a_{k+1,k} & a_{k+1,k+1} \end{pmatrix}$$

be a codeword of $\mathscr{P}$. Prove directly that $a_{k+1,k+1} = \sum_{i=1}^{k} a_{k+1,i} = \sum_{i=1}^{k} a_{i,k+1}$.

(b) Give an explicit procedure that corrects one error (answers such as "finding the closest codeword" or "the min-sum algorithm will correct one error" are not acceptable).

(c) Prove directly (without appealing to the minimum distance) that the code $\mathscr{P}$ detects two errors. Are there combinations of two errors that the code will correct?