ENEE626. Final examination, 12/20/2008 (max 70pt) **Instructor:** A. Barg

1. Let G be a matrix over $\mathbb{F}_2$ given by $G = \begin{bmatrix} 0&1&1&1&1&0&0&0&0&0\\ 1&0&0&0&1&1&0&0&0&1\\ 0&0&0&1&1&1&1&0&0&0\\ 0&0&1&0&1&1&0&1&0&0\\ 0&0&0&0&0&1&1&1&1&0 \end{bmatrix}$.

(a) (3pt) Find the parameters $[n, k, d]$ of the binary linear code $\mathscr{C}$ generated by G. Find k coordinates that form an information set. Find k coordinates that do not form an information set.

(b) (5pt) How was this code constructed? (Hint: Relate it to some familiar code).

(c) (5pt) Relying on the values n, k, d found in part (a) prove that $\mathscr{C}$ is optimal (i.e., that there is no $[n, k, d+1]$ code).

(d) (5pt) Consider the $(2^{n-k} \times n)$ matrix M formed by the codewords of the code $\mathscr{C}^\perp$. Let M' be the matrix formed by columns $2, 3, 5$ of M. How many times does the vector 001 appear as a row of M'? The same question for the vector 011.

(e) (7pt) Generalize the result of part (d) for an arbitrary $[n, k]$ linear code $\mathscr{D}$ over $\mathbb{F}_q$ such that $\mathrm{d}(\mathscr{D}^\perp) = d^\perp$. (Give a precise statement and a proof.)

2. (5pt) Factorize the polynomial $x^{20} + x^{12} + x^4 + 1$ over $\mathbb{F}_2$.

3. (5pt) Consider a binary cyclic code $\mathscr{T}$ of length $n = 17$ with zero α, a primitive root of unity mod n. Find the BCH designed distance of the code $\mathscr{T}$.

4. Consider a linear code $\mathscr{R}$ whose $(n-k) \times n$ parity-check matrix H is selected randomly from $\mathbb{F}_q$ (every element of H is chosen from $\mathbb{F}_q$ with uniform probability, and the elements are independent). Let X_w be the random number of vectors of weight w in $\mathscr{R}$.

(a) (7pt) Compute $\mathbb{E}X_w, \mathrm{Var}(X_w)$.

(b) (5pt) Based on part (a), show that there exist linear q-ary codes with weight distribution

$$A_w \le n^2 \binom{n}{w} (q-1)^w q^{k-n}.$$

(c) (5pt) Derive an asymptotic version of the GV bound for the q-ary case relying on the estimate in part (b)

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

(a) (3pt) 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) (5pt) 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) (5pt) 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?

6. (5pt) Let $\mathscr{R}$ be a 16-ary cyclic RS code of length $n = 15$ with generator polynomial

$$g(x) = (x + \alpha^7)(x + \alpha^8)(x + \alpha^9)$$

where α is a primitive element of $\mathbb{F}_{16}$. Write out a generator matrix and a parity-check matrix of $\mathscr{R}$.