ENEE626. Final examination, 12/14/2006 **Instructor:** A. Barg

All answers should be accompanied with proofs or sufficient explanation. Intermediate calculations should be shown. *The absence of proof or credible explanation will result in no points given for the problem.*

(1) (i) [10 pts.] Which of the polynomials $f_n(x) = \sum_{i=0}^n x^i, n = 1, 2, ..., 10$ are irreducible over $\mathbb{F}_2$?

(ii) [5] What is the necessary condition on n for $f_n(x) = \sum_{i=0}^n x^i$ to be irreducible over $\mathbb{F}_2$?

(2) [15] Find the generator polynomial of a BCH code of dimension 9 with designed BCH distance 5 over $\mathbb{F}_4$.

(3) [15] Prove that the Krawtchouk numbers satisfy

$$K_k(i) = (-1)^k K_k(n-i); \quad \binom{n}{i} K_k(i) = \binom{n}{k} K_i(k); \quad K_k(i) = (-1)^i K_{n-k}(i)$$

(4) Let C be an $[n = 2^m - 1, k = n - m]$ binary cyclic code with zero $\alpha^j, (j, n) = 1$. ([5] points each)

(i) What is the parity check matrix of C? What is the distance of C?

(ii) Is it true that C is equivalent to the Hamming code?

(iii) What is the generator polynomial of C?

(iv) Consider the code C' formed of all the vectors of *even* weight in C. What is the parity-check matrix of C'?

(v) What is the distance of C'?

(vi) What is the generator polynomial of C'?

(vii) Prove that C' can correct double errors of the form $e(x) = x^i + x^{i+1},\ i = 1, 2, \dots, n-1$.

(viii) Is the claim on the previous line true for the code C?

(5) [15] Let S, T be sets of binary vectors, $|S|T| \triangleq \{|\boldsymbol{s}|\boldsymbol{t}| : \boldsymbol{s} \in S, \boldsymbol{t} \in T\}$. Prove that

$$RM(r+1, m+1) = \cup |S|S|$$

where S runs through those cosets of $RM(r, m)$ that are contained in $RM(r+1, m)$.

(6) [10] Let C be a linear q-ary code with parity-check matrix H and let $\boldsymbol{c} \in C$ be a codeword, $\text{supp}(\boldsymbol{c}) = E$. We say that $\boldsymbol{c}$ is minimal if, for any codeword $\boldsymbol{c}' \in C$,

$$\text{supp}(\boldsymbol{c}') \subseteq E$$

implies that either $\boldsymbol{c}' = 0$ or $\boldsymbol{c}' = \delta \boldsymbol{c}$ for some $\delta \in \mathbb{F}_q$. Prove that $\boldsymbol{c}$ is minimal if and only if $\text{rk}(H(E)) = |E| - 1$.

(7) [10] Consider binary codes decoded up to half their minimum distance, used for transmission over BSC(p). Using the best codes, is it possible to reach capacity of the channel with this transmission protocol?