**ENEE626. Final examination, 12/15/2005** **Instructor:** A. Barg

**All answers should be accompanied with proofs.**

**Problem 1.**(14 pts., 2pts each) Let $C$ be the 3-ary Hamming code of length $n = 13$.

(a) Write out a parity-check matrix $H$ of $C$.

(b) Determine the dimension and the distance of $C$.

(c) What are the parameters $[n, k, d]$ of the dual code of $C$?

(d) Let $f(x) = x^3 + 2x + 1$. Prove that this polynomial is primitive over $\mathbb{F}_3$.

(e) Using the polynomial from part (d), construct a table representing the field $\mathbb{F}_{3^3}$.

(f) Let $B$ be the cyclic ternary Hamming code of length 13. Write out a parity-check matrix of $B$.

(g) What is the generator polynomial of $B$?

**Problem 2.** (8pts., 2pts. each) Let $q$ be a power of a prime number $p$. Consider the ensemble $\mathcal{L}_q(n, k)$ of linear codes defined by random $(n-k) \times n$ parity-check matrices $H$ whose elements are chosen independently of each other with probability $(1/q)$ from the finite field $\mathbb{F}_q$.

(a) Let $\mathbf{x} \in \mathbb{F}_q$ be a given vector and let $H$ be a random matrix. What is the probability $P(H\mathbf{x}^T = 0)$?

(b) What is the mathematical expectation of the number of codewords of Hamming weight $w$ in codes from the ensemble $\mathcal{L}_q$?

(c)[1] Prove that there exists a code $\mathcal{C} \in \mathcal{L}_q$ whose weight distribution is bounded above as follows:

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

for all $w = 1, 2, \dots, n$.

(d)[2] Let $n \to \infty, \omega = \frac{w}{n}$. Prove that the code $\mathcal{C}$ from part (c) satisfies

$$A_{\omega n} \le q^{n(R-1+h_q(\omega))(1+o(1))}$$

where $h_q(\omega) = -\log_q \frac{\omega}{q-1} - (1-\omega)\log_q(1-\omega)$.

**Problem 3.** (8pts., 1pt. each) True or false (explain your answer):

(a) The minimum distance of a linear code code equals the rank of its parity-check matrix.

(b) The covering radius of a linear code code equals the largest weight of the coset leader.

(c) If a linear code is perfect then every coset leader is a unique vector of the minimum weight in its coset.

(d) It is not possible to achieve capacity of the binary symmetric channel if we transmit using linear codes.

(e) Suppose a linear code can correct 4 errors under some decoding algorithm. Suppose that this code is used to correct 3 errors (i.e., the decoder outputs a codeword only if it is found to be distance $\le 3$ to the received word and outputs erasure otherwise). Then the probability of decoding error for the first algorithm will be smaller than for the second algorithm.

(f) Let $\alpha$ be a root of a primitive polynomial of degree $m$ over $\mathbb{F}_p$ and let $i \ge 1$ be an integer. The cyclotomic coset that contains $\alpha^i$ can be of size $1, 2, 3, \dots, m-1, m$.

(g) Typical random binary linear codes under *maximum likelihood decoding* achieve capacity of the binary symmetric channel (i.e., for any $R < 1 - h_2(p)$ typical codes in the ensemble $\mathcal{L}(n, Rn)$ have vanishing error probability).

(h) The code in Problem 1(c) of this exam is Maximum Distance Separable (MDS).

---

[1] The Markov inequality states that a random variable $\xi$ satisfies $P(\xi \ge a) \le \mathbb{E}[\xi]/a$.

[2] Recall that $\binom{n}{\omega n} \le 2^{-n(\omega \log_2 \omega + (1-\omega)\log_2(1-\omega))}$.