ENEE626. Final examination, 12/13/2007 **Instructor:** A. Barg

1. (1.5 points each question; 20 total). Give a complete and precise definition of the following concepts (no examples or explanation, just the definition):

(a). coset of a linear code
(b). coset leader
(c). parity-check matrix of a linear code
(d). information set of a linear code
(e). correctable error
(f). shortening of a linear code
(g). characteristic of a finite field
(h). Reed-Solomon code
(i). error locator polynomial
(j). correction of r errors under decoding into a list of size t
(k). minimal polynomial of an element of a finite field
(l). cyclic code
(m). the ensemble of random linear binary codes
(n). product code
(o). regular (j, k) LDPC code.

2. (5 points each question, 10 total). Let $C = RM(1,3)$ be the first-order RM code.

(a) Write out a generator and a parity-check matrix of C.

(b) Let t be the minimum weight of a noncorrectable error for the code C. Give an example of a correctable and an uncorrectable error vector of weight t

3. (5 points each question, 30 total). Consider $F = \mathbb{F}_{17}$.

(a). How many primitive elements are there in F?
(b). What is the sum of all elements of F?
(c). What is the product of all nonzero elements of F?
(d). For each possible multiplicative order of elements in F, give the number of elements.
(e). Is the polynomial $x^2 + x - 6$ irreducible over F?
(f). If F is a general finite field, what is the product of its nonzero elements?

4. (5 points). Factorize $x^{18} - 1$ over $\mathbb{F}_2$.

5. (20 total). Consider an $[n, k = Rn]$ binary linear code C with the weight distribution

$$A_0 = 1, \quad A_w \le n\binom{n}{w}2^{n(R-1)}. \qquad (\S)$$

(a) (5 points) Let d be the distance of C. What is $\lim_{n\to\infty} \frac{d}{n}$?

(b) (5 points) Suppose C is used for transmission over a BSC(p) with error detection (if the received vector is a codeword, decode to this codeword, otherwise declare an error). What is the probability of undetected error $P_{\text{ue}}(C)$ (use Equation (§) above to write an upper bound).

(c) (10 points) Use the result of (b) to find (estimate from above) the exponential asymptotics of $P_{\text{ue}}(C)$, i.e., the quantity

$$\lim_{n\to\infty} \frac{1}{n} \log_2 P_{\text{ue}}(C).$$

Consider separately the cases $p < \delta_{\text{GV}}(R)$ and $p > \delta_{\text{GV}}(R)$ where $\delta_{\text{GV}}(R) = h_2^{-1}(1 - R)$ is the Gilbert-Varshamov distance for the rate R.