ENEE626. Final examination, Spring 2014 **Instructor:** A. Barg

Submit by **Monday May 19, 12:30 pm**. Please submit a paper version of the exam to my office AVW 2361. If I am not there, please slide your paper under the door.

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

(b) The polynomial $x^{15} + 1$ factors over F_2 as follows:

$$x^{15} + 1 = (x + 1)(x^2 + x + 1)(x^4 + x + 1)(x^4 + x^3 + 1)(x^4 + x^3 + x^2 + x + 1)$$

Let C be a $[15, k, d]$ binary cyclic code of length 15 generated by $g = (x + 1)(x^4 + x + 1)$.

(c)

(b.1) What are k and d_{BCH} (the designed distance)? What about the true distance?

(b.2) Is $x^{14} + x^{12} + x^8 + x^4 + x + 1$ a codeword in C?

(b.3) List all $[15, 8]$ binary cyclic codes with their generator polynomials.

2. The Sudan algorithm sometimes outputs more than one decoding result (i.e., a true list of codewords). Give an example of such an outcome. In other words, take some finite field, choose the parameters of the RS code C, construct a vector $x \in \mathbb{F}_q^n$, and use the Sudan algorithm to decode this vector. The algorithm should output at least 2 distinct codewords of the code C. You can use the computer, but your calculations and claims should be verifiable (e.g., I should be able to check that your decoding results are indeed codewords in the RS code, and that you obtained them by actually applying the Sudan algorithm).

Hints: (i) The algorithm is presented on p.43,p.45 of the slides (pt. 2); (ii) To make life simpler, you can take a prime field; (iii) The last step of the algorithm calls for finding the roots of $Q(x, y)$, but since you have created the problem yourself, you already know the roots, and it remains just to check that the $Q(x, y)$ you found is correct.

3. In this problem you are asked to generalize the results proved in class and home assignment 3 for binary codes to the case codes over a finite field of size q, where q is any prime power.

1. The volume of the ball of radius $r = \rho n$ in the binary Hamming space is given by $2^{nh(\rho)(1+o(1))}$. Derive the asymptotic volume of the ball of radius $r = \rho n$ in the q-ary Hamming space.

2. Derive the Gilbert bound on the cardinality of q-ary codes with a given distance d. Derive the Varshamov bound on the cardinality of q-ary linear codes in the q-ary Hamming space. Give the asymptotic expression of each of bounds in terms of the code rate and relative distance in the regime $n \to \infty, d = \delta n$.

3. Consider the ensemble of linear codes given by random parity check matrices in which every entry is selected independently with probability $1/q$. Find the EA_w =expected number of code vectors of weight w in the random code from this ensemble. Compute the variance $\operatorname{Var} A_w$.