ENEE626. Midterm examination, due on 10/28/2008 **Instructor:** A. Barg

Instructions.

1. *This is a take-home exam.* If you are not coming to class on 10/28, please make sure to submit the paper *before* class. No late papers will be accepted.

2.Any sources, such as books, course notes, and WWW can be consulted. However you must work on your own, not turning to anyone for advice.

3. *Complete* proofs are required. Intermediate calculations should be shown. If applicable, clearly identify the answer to the problem.

4. On the first page of the exam paper, write the following:

"*I certify that I completed this assignment myself* (sign your name)"

Questions.

(1) (20pts) Prove that the polynomial $x^6 + x^5 + x^2 + x + 1$ is primitive over $\mathbb{F}_2$.

(2) (40 pts) Give an example of a received vector $\boldsymbol{r}$ for an RS code for which Sudan's algorithm outputs more than one codeword. Show all the steps of the decoding algorithm with intermediate results. The choice of the field $\mathbb{F}_q$ and the code's parameters $[n, k]$ is up to you; however you must choose $n \geq 11, n-4 \geq k \geq 4$ (in other words, do not take a code of length $n = 1$ or a code with the parameters $[n, n, 1]$).

(3) (30 pts) How many primitive elements are there in the field $\mathbb{F}_q, q = 17^{12}$? Prove your answer (not by computer).

(4) (50 pts) Design a code of length 10 over $\mathbb{F}_{11}$ that corrects single transposition errors. These are errors in which exactly one pair (c_i, c_j) of digits in a codeword $\boldsymbol{c} = (c_1, ..., c_{10})$ gets interchanged; for example, the codeword $(1, 2, 3, 4, 5, 6, 7, 8, 9, 10)$ may get transformed to $(1, 2, 6, 4, 5, 3, 7, 8, 9, 10)$. We don't care about other kinds of errors.

You may give more than one code design. Your design(s) must include an explicit specification of a parity-check matrix or generator matrix of the code, a description of the decoding algorithm, and a proof of the correctness of your construction. Your design(s) will be judged based on correctness, and coding rate achieved.