Applied Modern Algebra (MATH 4383/5383) Spring 2009
Exam 1

Due: March 13, 2009

Instructions: For this exam you may use your class text, homeworks and notes, but you may not consult with any other sources (other books, people, internet, etc.). You are free however to ask me any questions about your old homeworks, lecture material or material in the text which may be related to the problems below. Also, if you do not understand the statement of a question, please ask. You may not use a calculator or computer, except where stated explicitly.

Explain your solutions as best you can. Staple your papers together and turn your exam either into me in person, or put it in an envelope and slide it under my office door (PHSC 922) by the end of the day Friday March 13.

Problem A (Quadratic Residue Codes). (25 points) Let p be an odd prime. We say $r \in \mathbb{Z}/p$ is a *quadratic residue* mod p if $x^2 = r$ for some $x \in \mathbb{Z}/p$. Otherwise, r is a *quadratic non-residue*. For example the quadratic residues mod 5 are $0, 1, 4$.

(i) Compute the quadratic residues mod 11.

(ii) Let $V = \mathbb{F}_2^p$. Let $v_0 = (a_0, a_1, \ldots, a_{p-1}) \in V$ be given by $a_j = 1$ if j is a **non-zero** quadratic residue mod p and $a_j = 0$ if j is 0 or a quadratic non-residue mod p. Let v_i be the *right cyclic shift* of v_{i-1}, i.e.,

$$v_1 = (a_{p-1}, a_0, a_1, \ldots, a_{p-2}),$$

$$v_2 = (a_{p-2}, a_{p-1}, a_0, a_1, \ldots, a_{p-3}),$$

and so on. (Note when we get to v_p they start repeating, so we only consider v_0 through v_{p-1}.) For example, v_0 and its cyclic shifts v_1 through v_4 are given by

$$v_0 = 01001$$
$$v_1 = 10100$$
$$v_2 = 01010$$
$$v_3 = 00101$$
$$v_4 = 10010.$$

Write down v_0 through v_{p-1} for $p = 11$.

(iii) Let $\mathcal{Q}_p \subseteq V$ be the linear code generated (spanned) by $v_0, \ldots, v_{p-1}$. (I do not claim they are linearly independent—if they were, we would have $\mathcal{Q}_p = V$!). Codes generated by the cyclic shifts of some vector are called *cyclic codes*, though $\mathcal{Q}_p$ in particular is called a quadratic residue code. Note that $\mathcal{Q}_7$ is (equivalent to) the [7,4,3] binary Hamming code and $\mathcal{Q}_{23}$ is the binary [23,12,7] Golay code, both of which are perfect. The [24, 12, 8] extended binary Golay code was used in NASA's Voyager mission. Determine the parameters $[n, k, d]$ of $\mathcal{Q}$ when $p = 11$. Is it perfect? (You may use a calculator to check if it is perfect.)

Problem B (Reed-Solomon and related codes). (50 points)

(i) Let $f(X) = X^3 + X^2 + 1$ as a polynomial over $\mathbb{F}_2$. Prove that $f(X)$ is irreducible.

(ii) Construct $\mathbb{F}_8 = \mathbb{F}_2[X]/(f(X))$ with the polynomial $f(X)$ above. Write out the multiplication table.

(iii) Find a *primitive element* $\alpha \in \mathbb{F}_8$, i.e., an α such that $\mathbb{F}_8 = \{0, \alpha^0 = 1, \alpha, \alpha_2, \ldots, \alpha^6\}$. (Note that $\alpha^7 = 1$.) Make a table expressing each α^j as a polynomial mod $f(X)$.

(iv) Using the ordering of $\mathbb{F}_8$ as $\{0, 1, \alpha, \ldots, \alpha^6\}$, write down a generator matrix G for a $\mathcal{RS}(4, 8)$ code. What are its $[n, k, d]$ parameters?

(v) Define the *trace map* $tr : \mathbb{F}_8 \to \mathbb{F}_2$ by $tr(x) = x + x^2 + x^4$. Compute $tr(x)$ for each element of $\mathbb{F}_8$. (To compute the $tr(\alpha^j)$, use your table from (iii) and do the computation as polynomials. Your computations should show you always get 0 or 1.)

(vi) If $A = (a_{ij})$ is an $m \times n$ matrix over $\mathbb{F}_8$, we can form the $m \times n$ matrix $tr(A) = (tr(a_{ij}))$ over $\mathbb{F}_2$ just by taking the trace of each entry. Let $\mathcal{C}$ be the binary linear code with generator matrix $tr(G)$. Determine its $[n, k, d]$ parameters.

(vii) The trace was one way to get a binary code from an 8-ary code. A more obvious way is to write each element of $\mathbb{F}_8$ as 3 binary digits. Specifically, take any bijection $\iota : \mathbb{F}_8 \to F_2^3$. Define a code of length 24 by

$$\mathcal{C}' = \{(\iota(x_0), \iota(x_1), \ldots, \iota(x_7)) \in \mathbb{F}_2^{24} | (x_0, \ldots, x_7) \in \mathcal{RS}(4, 8).\}$$

What can you say about the $[n, k, d]$ parameters for $\mathcal{C}'$? (Caution: If you just apply ι to the vectors in the generating matrix, this will not generate $\mathcal{C}'$! You could of course consider a code generated this way (like we did for the trace map), but in this situation it is much better to apply ι to every codeword. To see this, just think how many codewords you would get by doing it each way.)

Problem C (Code Design). (25 points) You are working on a project involving communication via new high-speed optical cables. Assume that the cables provide a binary symmetric channel with bit error probability of $p = 10^{-4} = .0001$, i.e., you expect about 1 bit error for every 10000 sent., i.e., about 1000 errors in every megabyte. You want to design a code to accurately send large amounts of data. For engineering and speed purposes, the code should have information rate no less than 1/2 (though something closer to 3/4 would be preferable) and the length should be a multiple of 8. (In practice one also needs to worry about the speed of the decoding algorithm, but do not worry about that here.) For this problem you may use a calculator/computer. Note that Python is a pretty accurate calculator—perhaps the only thing you should know is the exponentiation syntax: if you want to calculate x^y in Python, type

```
x**y
```

(i) Calculate the probability of at most one error in a given byte (1 byte = 8 bits).

(ii) Design a code for the situation described above so that with your error correcting code, the probability of an error in 1 byte is less than 10^{-6}. (This should mean you can expect about one bit error in every megabyte of of data sent.) Compute the probability of an error in one byte for this code. What is the information rate? Try to make this as large as you can with the constraints given.