Question 4:

Let p(x) be a primitive polynomial of degree m with coefficients from GF(q). Prove that the roots of p(x) have order (q^m-1).

See proof in book or class

Question 1: Consider an (n,k) code. Assume that during transmission at most 3% of all transmitted bits are received in error..

+10 a) For each lengths n=100, 200, 1000 what is the minimum possible redundancy r such that all errors might be correctible ?

+10 b) For each lengths n=100, 200, 1000 what is the maximum possible code rate R such that all errors might be correctible ?

$d_{min} \leq n-k+1$

a) $r = n-k$

$t \leq \frac{d_{min}-1}{2} \leq \frac{n-k}{2}$

$3 \leq \frac{d_{min}-1}{2} \leq \frac{n-k}{2}$

$\Rightarrow r = n-k \geq 6$

b) $r = n-k \geq 12$

c) $r = n-k \geq 60$

b) $R = \frac{k}{n} = 1 - \frac{n-k}{n}$

$\rightarrow \frac{n}{n} - \frac{n-k}{n} =$

$n=100$: $R = 1 - \frac{n-k}{n} \leq 1 - \frac{6}{100} = .94$

$n=200$ $R \leq 1 - \frac{12}{200} = .94$

$n=100$ $R \leq 1 - \frac{60}{1000} = .94$

Question 2:

a) Show that $p_1(x) = x^3 + x + 1$ and $p_2(x) = x^3 + x^2 + 1$ are both primitive polynomials in GF(2)[x].

b) Let α be a root of $p_1(x)$ and β a root of $p_2(x)$. Give 2 different constructions of GF(8), one using (α, $p_1(x)$) and the other using (β, $p_2(x)$)

c) Is α also a root of $p_2(x)$? (recall that α is a root of $p_1(x)$) Explain

d) Express α in terms of β

a)

$$x^3+x+1 \overline{)\,x^7+1}\quad x^4+x^2+x+1$$
$$x^7+x^5+x^4$$
$$x^5+x^4+1$$
$$x^5+x^3+x^2$$
$$x^4+x^3+x^2+1$$
$$x^4+x^2+x$$
$$x^3+x+1$$

minimal

$$x^3+x+1 \overline{)\,x^6+1}\quad x^3$$
$$x^6+x^4+x^3$$
$$x^4+x^3+1$$
$$x^4+x^2+x$$
$$x^3+x^2+x+1$$

$$x^3+x^2+1 \overline{)\,x^5+1}\quad x^2$$
$$x^5+x^3+x^2$$
$$x^3+x^2+1$$
$$x^3+x^2+x$$
$$x^2+x+1$$

$$x^3+x^2+1 \overline{)\,x^7+1}\quad x^4+x^3+x^2+1$$
$$x^7+x^6+x^4$$
$$x^6+x^4+1$$
$$x^6+x^5+x^3$$
$$x^5+x^4+x^3+1$$
$$x^5+x^4+x^2$$
$$x^3+x^2+1$$

maximal

$$x^3+x^2+1 \overline{)\,x^6+1}\quad x^3+x^2+x$$
$$x^6+x^5+x^3$$
$$x^5+x^3+1$$
$$x^5+x^4+x^2$$
$$x^4+x^3+x^2+1$$
$$x^4+x^3+x$$
$$x^2+x+1$$

$$x^3+x^2+1 \overline{)\,x^5+1}\quad x^2+x$$
$$x^5+x^4+x^2$$
$$x^4+x^2+1$$
$$x^4+x^3+x$$
$$x^3+x^2+x+1$$

$$x^3+x^2+1 \overline{)\,x^4+1}\quad x$$
$$x^4+x^3+x$$
$$x^3+x+1$$

Both are irreducible because neither is $\div$ by x^2+x+1

b)

p_1

	$\alpha^2\ \alpha^1\ \alpha^0$
0	0 0 0
1	0 0 1
α	0 1 0
α^2	1 0 0
$\alpha^3 = \alpha + 1$	0 1 1
$\alpha^4 = \alpha^2 + \alpha$	1 1 0
$\alpha^5 = \alpha + 1 + \alpha^2$	1 1 1
$\alpha^6 = \alpha + 1 + \alpha^2 + \alpha = \alpha^2 + 1$	1 0 1

p_2

	$\beta^2\ \beta^1\ \beta^0$
0	0 0 0
1	0 0 1
β	0 1 0
β^2	1 0 0
$\beta^3 = \beta^2 + 1$	1 0 1
$\beta^4 = \beta^2 + 1 + \beta$	1 1 1
$\beta^5 = \beta^2 + 1 + \beta + \beta^2 = 1 + \beta$	0 1 1
$\beta^6 = \beta + \beta^2$	1 1 0

$\beta = \alpha^4$

c) $p_2(x) = x^3 + x^2 + 1$

$p_2(\alpha) = \alpha^3 + \alpha^2 + 1$

$= \alpha + 1 + \alpha^2 + 1$

$\neq 0$ Also !!

d) Note: α^3 is a root

$\alpha, \alpha^2, \alpha^4$ are roots of $p_1(x)$

$\alpha^3, \alpha^5, \alpha^6$ are roots of $p_2(x)$

so are β, β^2, β^4

Question 3:

Consider any linear block code C with parity check matrix H:

a) Let H' be H with the first two columns switched. Let C' be the code associated with H'. Does C = C'? Namely are the set of codewords in C and C' the same? Why or why not? What is the relationship between C and C'?

No, not true for all $\underline{c} \in C$, $\underline{c}' = (c_1, c_0, c_2, \ldots c_{n-1}) \in C'$

b) Consider the following parity check matrix for code C:

$$H = \begin{bmatrix} 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{bmatrix}$$

i) give the length, dimension and rate of the code
ii) Find a valid G for C, using the result from part a)
iii) Find the minimum distance of the code. How many errors does it correct and detect?

a) Not, $\underline{c}' \in C'$, $\underline{c}' = (c_1, c_0, c_2, \ldots, c_{n-1}) \notin C$ in general.

b) i) $n-k = 3$, $n = 6 \Rightarrow k = 3$

ii) Let $H' = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{bmatrix} \in H$ with 1st & 2 columns switched

$$G' = \left[\begin{array}{ccc|ccc} 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{array}\right]$$

$$G = \left[\begin{array}{ccc|ccc} 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{array}\right]$$

iii) $d_{min} = 3$ (either from G or H)

corrects 1 error, detects 2

Question 5:

Consider a matrix H and let column *i* of H be the binary expansion of *i*, for i=1,2...,15

a) Confirm that this is the parity check matrix of a Hamming code. What is (n,k)?
b) Give the syndrome decoder for this code, namely list all possible syndromes and give the corresponding error pattern
c) Give a simple (one line) decoding algorithm that does not require a lookup table for implementing the decoder

+5 a) $H = \begin{bmatrix} 0&0&0&0&0&0&0&1&1&1&1&1&1&1&1 \\ 0&0&0&1&1&1&1&0&0&0&0&1&1&1&1 \\ 0&1&1&0&0&1&1&0&0&1&1&0&0&1&1 \\ 1&0&1&0&1&0&1&0&1&0&1&0&1&0&1 \end{bmatrix}$ $n=15,\ k=15-4=11$

$\Rightarrow$ satisfies defn of Hamming code

+7 b) $\Rightarrow$ # possible syndromes $= 2^{n-k} = 16 \Rightarrow$ corresponds to 15 cols of H plus 0000

e	s
$1 0 \ldots 0$	0001
$0^1 1 0^{13}$	0010
$0^2 1 0^{12}$	0011
⋮	
$0^{14} 1$	1111

+8 c) Take decimal equivalent of s, this gives location of error.