Math 437 – Homework 4

Due 10:15am on Thursday, February 9, 2017

Please indicate any sources you used for a given problem on the solution to that problem. For example, if you worked with another student to get the solution to a problem, please indicate who. You are welcome to work together in small groups, but please try the problems on your own first and write up your own solutions.

Problem 1. Let $p(x) = x^3 + x + 1 \in \mathbb{Z}_2[x]$, as in Example 4.2 from the book.

(a) Give a 3×7 matrix H (with entries in $\mathbb{Z}_2$) that satisfies

$$\begin{pmatrix} 1 & a & a^2 \end{pmatrix} H = \begin{pmatrix} 1 & a & a^2 & a^3 & a^4 & a^5 & a^6 \end{pmatrix}$$

in the field $\mathbb{Z}_2[a]/(p(a))$.

(b) Explain why H is a parity check matrix for the BCH code resulting from the first power of a in $\mathbb{Z}_2[a]/(p(a))$.

(c) Explain why the BCH code from part (b) is a Hamming code.

Problem 2. Let $p \in \mathbb{Z}_2[x]$ be a primitive polynomial of degree n and take $F = \mathbb{Z}_2[a]/(p(a))$. Show that every element of F^* is a root of the polynomial $f(x) = x^N - 1$ where $N = 2^n - 1$. (This implies that the minimal polynomial of any element of F^* divides $x^N - 1$.)

Problem 3. Consider the field $F = \mathbb{Z}_2[a]/(p(a))$ where $p(x) = x^4 + x^3 + 1 \in \mathbb{Z}_2[x]$. We see that p is primitive by looking at the powers a^k in F:

a^k	rep. in F	a^k	rep. in F	a^k	rep. in F	a^k	rep. in F
a^0	1	a^4	$1+a^3$	a^8	$a+a^2+a^3$	a^{12}	$1+a$
a^1	a	a^5	$1+a+a^3$	a^9	$1+a^2$	a^{13}	$a+a^2$
a^2	a^2	a^6	$1+a+a^2+a^3$	a^{10}	$a+a^3$	a^{14}	a^2+a^3
a^3	a^3	a^7	$1+a+a^2$	a^{11}	$1+a^2+a^3$	a^{15}	1

(a) Find the minimal polynomial of each element in F^*.
(Using that b and b^2 have the same minimal polynomial will save on computations!)

(b) For each value of $2t$, give the following data for the BCH code resulting from the first $2t$ powers of a in F :

$2t$	# Correctable Errors	Degree of generator polynomial	Linear code parameters	# Codewords
2				
4				
6				
8				
14				