Math 437 – Homework 5

Due 10:15am on Thursday, February 16, 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 $p \in \mathbb{Z}_2[x]$ be a primitive polynomial of degree n and take $F = \mathbb{Z}_2[a]/(p(a))$. Suppose $e(x) \in \mathbb{Z}_2[x]$ has syndromes $s_1 = e(a), s_2 = e(a^2), s_3 = e(a^3)$ and let

$$S = \begin{pmatrix} s_1 & s_2 \\ s_2 & s_3 \end{pmatrix}.$$

Show the following:

(a) If $e(x)$ has one term (say $e(x) = x^d$), then the matrix S has rank one.
(b) If $e(x)$ has two terms (say $e(x) = x^{d_1} + x^{d_2}$), then S has rank two.

Problem 2. Let C be the BCH code generated by the first 4 powers of a in $\mathbb{Z}_2[a]/(a^4+a+1)$ (see page 97). Correct each of polynomials $r(x)$ to a polynomial in C:

(a) $r(x) = 1 + x^7 + x^{11} + x^{14}$
(b) $r(x) = x^6 + x^7 + x^8 + x^{11}$

Problem 3. Ch. 5 #6 on page 169
(The table from Homework 4 #3 may be helpful.)