Name : Spring 2009

**MATH 291T** **Homework 6** Due on Tuesday 05/12/09

---

**1.** This exercise, you are asked to construct BCH-codes of length 15 and designed distance 5 over certain fields. Try to find an example with maximal dimension. For each code, you must identify $b$ and the dimension.

(a) over $GF(4)$.

(c) over $GF(16)$.

**2.** Construct a BCH-code of length 17 and dimension 9 over $GF(4)$ that can correct at least three errors.

**3.** Construct a binary BCH-code of length 31 of designed distance 5 with minimum distance at least 11.

**4.** Put $\beta = \alpha$ where $\alpha$ is a primitive element of $GF(16)$ as defined in the table for $GF(16)$ in the notes. Consider the binary BCH-code of length 15 with generator polynomial

$$\text{lcm}(m_\beta(x), m_{\beta^2}(x), m_{\beta^3}(x), m_{\beta^4}(x))$$

(a) What is the dimension of this code?

(b) What is the designed distance of this code?

(c) Use the Peterson-Gorenstein-Zierler decoding algorithm to decode the following word:

$$\mathbf{y} = 111000000000000$$

**5.** Put $\beta = \alpha$ where $\alpha$ is a primitive element of $GF(8)$ as defined in the table for $GF(8)$ in the notes. Consider the binary BCH-code of length 7 with generator polynomial $\text{lcm}(m_\beta(x), m_{\beta^2}(x))$. Use the Peterson-Gorenstein-Zierler decoding algorithm to decode the following words:

(a) 1000110

(b) 1000001

**6.** Put $\beta = \alpha^3$ where $\alpha$ is a primitive element of $GF(16)$ as defined in the table for $GF(16)$ in the notes. Then $GF(4) = \{0, 1, \alpha^5, \alpha^{10}\}$ is a subfield of $GF(16)$. Consider the BCH-code of length 5 over $GF(4)$ with generator polynomial $\text{lcm}(m_{\beta^2}(x), m_{\beta^3}(x))$. So $b = 2$.

(a) What is the dimension of this code?

(b) What is the designed distance of this code?

(c) Use the Peterson-Gorenstein-Zierler decoding algorithm to decode the word $\mathbf{y} = 1\alpha^5 100$

---

---