**UNIVERSITY OF CALIFORNIA, DAVIS**
**Error Correcting Codes I**

**PROBLEM SET 5**

Reading Assignment: Lecture Notes: 6. Textbook: Sections 7.1–7.4.

Solve problems by hand, i.e., do not use symbolic and/or numerical mathematics software package to solve the problems. However, you can use them, if you want, to check your answers.

**Remark** You have to solve the problems in order since each problem depends on the previous problems.

**Problem 1** In this problem we construct addition and multiplication tables for GF(4) which we will use later to define a BCH code over this field.

1. Construct a table for $GF(2^2)$ based on the primitive polynomial $X^2 + X + 1$. Display the power, polynomial, and vector representations of each of the four elements, similar to Table 2.8 in textbook. However, use $\omega$ instead of $\alpha$ (which will be used later in another context).
2. GF(4) is composed of four elements, $0, 1, \omega$, and $\omega^2$. Construct addition and multiplication tables for GF(4).

**Problem 2** In this problem, we will construct $GF(4^2)$ as an extension field of GF(4) constructed in Problem 1 with elements $0, 1, \omega$, and $\omega^2$.

1. The polynomial $p(X) = X^2 + X + \omega$ is a primitive polynomial over GF(4), i.e., $p(X)$ is irreducible (does not factor as a product of polynomials of degree less than two) and the minimal positive integer $n$ such that $X^n - 1$ is divisible by $p(X)$ is $n = 4^2 - 1$. Just check that it is irreducible.
2. Construct a table for $GF(4^2)$ based on the primitive polynomial $p(X) = X^2 + X + \omega$ as an extension field of GF(4) rather than GF(2) as in Table 2.8 in textbook. Display the power (i.e., 0, 1, $\alpha^i$ for $i = 1, 2, \ldots, 14$ where $\alpha$ is a root of $p(X)$), polynomial (i.e., $a + b\alpha$ where $a, b$ are in $GF(4) = \{0, 1, \omega, \omega^2\}$), and vector (i.e., $(a, b)$ where $a, b$ are in GF(4)$= \{0, 1, \omega, \omega^2\}$) representations of each of the sixteen elements. To check your solution, $\alpha^8 = \omega^2 + \alpha$ which is represented

by the vector $(\omega^2, 1)$. (The fact that all powers of $\alpha^i$, $i = 1, 2, \ldots, 14$ have distinct nonzero polynomial representations and $\alpha^{15}$ has the same polynomial representation as 1 proves that the minimal positive integer $n$ such that $X^n - 1$ is divisible by $p(X)$ is $n = 4^2 - 1$, which completes the proof that $p(X)$ is a primitive polynomial.)

3. Find the minimal polynomial over GF(4) of each nonzero element in GF($4^2$). To do this, you need to determine the exponent of each nonzero element $\beta$ in GF($4^2$) with respect to GF(4). This is the least positive integer $e$ such that $\beta^{4^e} = \beta$. Then, the minimal polynomial of $\beta$ is $\prod_{i=0}^{e-1}(X - \beta^{4^i})$. The minimal polynomial should have coefficients in GF(4)= $\{0, 1, \omega, \omega^2\}$. To check your solution, the minimal polynomial of $\alpha^3$ is $(X + \alpha^3)(X + \alpha^{12}) = X^2 + \omega^2 X + 1$.

**Problem 3**

1. Find the generator polynomial of a double error correcting primitive BCH code over GF(4) of length 15.

2. Determine the dimension and the number of codewords in this BCH code.

**Problem 4** Decode the polynomial $r(X) = \omega^2 X^9 + \omega X^8 + X^3 + X$ with respect to the BCH code of Problem 3 using the Berlekmap-Massey algorithm.