Math 406
Assignment 4

Due 13 November 2014

Note: Problems marked with an asterisk (*) are only for graduate students.

1. Consider the double-error-correcting binary linear code defined by the parity check matrix
   \[ H = \begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \alpha^7 & \alpha^8 & \alpha^9 & \alpha^{10} & \alpha^{11} & \alpha^{12} & \alpha^{13} & \alpha^{14} \\ 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} \end{pmatrix}, \]
   where \( \alpha = x \) is the primitive element \((0100)\) in \( \mathbb{F}_{16} = \mathbb{F}_2[x]/(x^4 + x^3 + 1) \).
   Decode each of the following received words (if possible) using the decoding algorithm derived in class:
   (i) \((0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)\)
   (ii) \((1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0)\)
   (iii) \((1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0)\)

   Remark: You might want to use MAPLE for some of the computations. If you do, then submit your MAPLE output.

2. Let \( \mathbb{F} \) be field of order \(|\mathbb{F}| = p^n\), and let \( \mathbb{P}(\mathbb{F}) \) be its prime subfield. For \( \alpha \in \mathbb{F} \), put
   \[ \text{tr}(\alpha) = \sum_{k=0}^{n-1} \alpha^{p^k} \quad \text{and} \quad N(\alpha) = \prod_{k=0}^{n-1} \alpha^{p^k}. \]
   (a) Show that \( \text{tr}(\alpha) \in \mathbb{P}(\mathbb{F}) \), for all \( \alpha \in \mathbb{F} \), and conclude that \( \text{tr} : \mathbb{F} \to \mathbb{P}(\mathbb{F}) \) is an \( \mathbb{P}(\mathbb{F}) \)-linear map (called the trace map).
   (b) Show that \( N(\alpha) \in \mathbb{P}(\mathbb{F}) \), for all \( \alpha \in \mathbb{F} \). (The map \( N : \mathbb{F} \to \mathbb{P}(\mathbb{F}) \) is called the norm map.) Prove that if \( \alpha \) is a generator of \( \mathbb{F} \), then \( N(\alpha) \) is a generator of \( \mathbb{P}(\mathbb{F}) \).
   (c) Show that \( \text{tr}(\alpha^p) = \text{tr}(\alpha) \) and \( N(\alpha^p) = N(\alpha) \), for all \( \alpha \in \mathbb{F} \).

3. The polynomial \( x^6 + x + 1 \) can be verified to be irreducible over \( \mathbb{F}_2 \). By a class result (cf. Proposition 7.9 in the Roth textbook), \( x^6 + x + 1 \) is the minimal polynomial of some element \( \alpha \) in \( \mathbb{F}_{64} \).
   In the following, the degree of an element in \( \mathbb{F}_{64} \) always refers to its degree over \( \mathbb{F}_2 \).
   (a) Show that \( \alpha \) is a generator of \( \mathbb{F}_{64} \).
   (b) Find the order (in \( \mathbb{F}_{64} \)) of \( \alpha^9 \), and also its degree.
(c) Find the minimal polynomial over $\mathbb{F}_2$ of $\alpha^9$.

(d) Find an element in $\mathbb{F}_{64}$ of order 3, and determine its degree.

(e) Find the minimal polynomial over $\mathbb{F}_2$ of the element found in part (d).

(f) Find the minimal polynomial over $\mathbb{F}_2$ of $\alpha^3$.

**Note:** To solve this problem, there is no need to compute the entire table of $\mathbb{F}_{64}$, or even to assume a particular construction of this field. Try to make use of the various properties known for order, degree, minimal polynomials and so on. (Remember to justify your assertions.)

[5*] 4*. Let $F$ be a finite field of order $p^n$.

(a) Prove that the trace $\text{tr} : F \to P(F)$ and norm $N : F \to P(F)$ maps are surjective. [Hint (for the trace): Consider the roots of the polynomial $X^{p^n} + \ldots + X^p + X$.]

(b) Let $f(X) \in F[X]$ be an irreducible polynomial, and let $A_f = F[X]/(f)$ be the extension field defined by $f$. Prove that the polynomial $f$ splits into distinct linear factors over $A_f$.

[5] 5. MAPLE problem (refer to the MAPLE instruction sheet):

(a) Let $F = \mathbb{F}_q$ be a finite field with $q = p^n$ elements, and let $\alpha \in F^\times$ be a generator. For an integer $k$, let $C_{\alpha^k} = \{\alpha^k, \alpha^{pk}, \ldots\}$ denote the conjugacy class of $\alpha^k$.

Write a program $\text{conjcl}(k, p, n)$ which computes the list of exponents of $\alpha$ of the elements which appear in $C_{\alpha^k}$.

(b) Use your program to find the exponents of all the conjugacy classes of $\mathbb{F}_{24}$.

(c) Let $F = \mathbb{F}_p[x]/(g)$, where $g(x)$ is irreducible over $\mathbb{F}_p$, and let $\alpha \in F = \mathbb{F}_p[x]$ be an explicit generator. Write a program $\text{minpoly}(\alpha, k, p, g)$ which computes the minimal polynomial $M_{\alpha^k}(X)$ of $\alpha^k$ (over $\mathbb{F}_p$). (Use your program $\text{conjcl}$ of part (a).)

(d) Now consider the case that $g(x) = x^4 + x + 1 \in \mathbb{F}_2[x]$, and $\alpha = x$. Find the minimal polynomials corresponding to the conjugacy classes of part (b). Multiply these together and compare the resulting product to $X^{15} - 1$. 