EE 605: Error Correcting Codes

Instructor: Saravanan Vijayakumaran
Indian Institute of Technology Bombay
Autumn 2010

120 minutes
Midsemester Exam: **30 points** September 12, 2010

Instructions:

- Answer **five** out of the **first seven** questions. Each of the first seven questions is worth 4 points. If you answer more than five questions, the five lowest scoring answers will be considered.
- **Question 8 is compulsory**. It has 10 parts worth one point each for a total of 10 points.

1. Lagrange's theorem states that if a group G has order n and H is a subgroup of G of order m, then m divides n. Prove the following two statements and use them to prove Lagrange's theorem.
   (a) No two elements in a coset of H are identical.
   (b) No two elements in two different cosets of H are identical.
2. In a field of F_q of q elements where q is not necessarily a prime, prove that that all the elements of F_q are roots of $x^q - x \in F_q[x]$.
3. Let $g(x)$ be an irreducible polynomial in $\mathbb{F}_p[x]$ where $\mathbb{F}_p$ is a field with number of elements equal to a prime p. Prove that the set of polynomials in $\mathbb{F}_p[x]$ with degrees less than the degree of $g(x)$ form a field under polynomial addition and multiplication modulo $g(x)$.
4. Let F be a field. Euclid's lemma for polynomials states that if a prime polynomial $g(x)$ divides $r(x)s(x)$ where $g(x)$, $r(x)$ and $s(x)$ belong to $F[x]$, then $g(x)$ divides $r(x)$ or $g(x)$ divides $s(x)$. Prove this statement.
5. In a field $\mathbb{F}$ of characteristic p, prove that any $f(x) \in \mathbb{F}[x]$ satisfies $f^p(x) = f(x^p)$ if and only if $f(x) \in \mathbb{F}_p[x]$, i.e. the coefficients of $f(x)$ are in the prime subfield $\mathbb{F}_p$.
6. The minimal polynomial $g(x)$ of an element β in a finite field $\mathbb{F}$ having characteristic p is the monic polynomial of least degree in $\mathbb{F}_p[x]$ such that $g(\beta) = 0$. For any $f(x) \in \mathbb{F}_p[x]$, prove that $f(\beta) = 0$ if and only if $g(x)$ divides $f(x)$.
7. Let α and β be elements in a field F. If α has order m, β has order n and $\gcd(m, n) = 1$, prove that $\alpha\beta$ has order mn.
8. Answer the following questions and give a one line justification for each question which has a **Yes** or **No** answer. An answer without justification will not be awarded any points.

(a) Does a field of order 85,683 exist?

(b) Does a cyclic abelian group of order 85,683 exist?

(c) Is $X^{3^n} + X^{3^n-1} + X^{3^n-2} + \cdots + X + 1$ a prime polynomial in $\mathbb{F}_2[x]$ for all positive integers n?

(d) Is $2^{p-1} = 1 \bmod p$ for every prime $p > 2$?

(e) Let $a, b, c \in F$ where F is a field of characteristic p. Simplify $\left[(a+b)^{p^2} + c\right]^{p^3}$ as much as possible.

(f) Let F be a field with p^3 elements where p is a prime and let $\alpha \in F$. Simplify $\alpha^{p^{13}}$ as much as possible.

(g) List all the elements in the set $R_{\mathbb{F}_3,2}$.

(h) Consider the group $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$ under addition modulo n where n is a positive integer. Suppose there exist $i, j \in \mathbb{Z}_n$ which have no factors in common. What is the smallest subgroup of $\mathbb{Z}_n$ which contains both i and j?

(i) Let $\mathbb{F}$ be a field of characteristic 2. Let $x^2 + x + 1$ be the minimal polynomial of $\beta \in \mathbb{F}$. List all the elements in the set $G_\beta = \{f(\beta) \mid f(x) \in \mathbb{F}_2[x]\}$.

(j) Using Euclidean algorithm, find the greatest common divisor of $x^4 + 1$ and $x^6 + x^5 + x^4 + x^3 + x^2 + 1$ in $\mathbb{F}_2[x]$.