6.451 Principles of Digital Communication II — Wednesday, March 2, 2005
MIT, Spring 2005 — Handout #11
Due: Wednesday, March 9, 2005

Problem Set 5

Problem 5.1 (Euclidean division algorithm).

(a) For the set $\mathbb{F}[x]$ of polynomials over any field $\mathbb{F}$, show that the distributive law holds: $(f_1(x) + f_2(x))h(x) = f_1(x)h(x) + f_2(x)h(x)$.

(b) Use the distributive law to show that for any given $f(x)$ and $g(x)$ in $\mathbb{F}[x]$, there is a unique $q(x)$ and $r(x)$ with $\deg r(x) < \deg g(x)$ such that $f(x) = q(x)g(x) + r(x)$.

Problem 5.2 (unique factorization of the integers).

Following the proof of Theorem 7.7, prove unique factorization for the integers $\mathbb{Z}$.

Problem 5.3 (finding irreducible polynomials).

(a) Find all prime polynomials in $\mathbb{F}_2[x]$ of degrees 4 and 5. [Hint: There are three prime polynomials in $\mathbb{F}_2[x]$ of degree 4 and six of degree 5.]

(b) Show that $x^{16} + x$ factors into the product of the prime polynomials whose degrees divide 4, and $x^{32} + x$ factors into the product of the prime polynomials whose degrees divide 5.

Problem 5.4 (The nonzero elements of $\mathbb{F}_{g(x)}$ form an abelian group under multiplication).

Let $g(x)$ be a prime polynomial of degree m, and $r(x), s(x), t(x)$ polynomials in $\mathbb{F}_{g(x)}$.

(a) Prove the distributive law, *i.e.,* $(r(x) + s(x)) * t(x) = r(x) * t(x) + s(x) * t(x)$. [Hint: Express each product as a remainder using the Euclidean division algorithm.]

(b) For $r(x) \neq 0$, show that $r(x) * s(x) \neq r(x) * t(x)$ if $s(x) \neq t(x)$.

(c) For $r(x) \neq 0$, show that as $s(x)$ runs through all nonzero polynomials in $\mathbb{F}_{g(x)}$, the product $r(x) * s(x)$ also runs through all nonzero polynomials in $\mathbb{F}_{g(x)}$.

(d) Show from this that $r(x) \neq 0$ has a mod-$g(x)$ multiplicative inverse in $\mathbb{F}_{g(x)}$; *i.e.,* that $r(x) * s(x) = 1$ for some $s(x) \in \mathbb{F}_{g(x)}$.

Problem 5.5 (Construction of $\mathbb{F}_{32}$).

(a) Using an irreducible polynomial of degree 5 (see Problem 5.3), construct a finite field $\mathbb{F}_{32}$ with 32 elements.

(b) Show that addition in $\mathbb{F}_{32}$ can be performed by vector addition of 5-tuples over $\mathbb{F}_2$.

(c) Find a primitive element $\alpha \in \mathbb{F}_{32}$. Express every nonzero element of $\mathbb{F}_{32}$ as a distinct power of α. Show how to perform multiplication and division of nonzero elements in $\mathbb{F}_{32}$ using this "log table."

(d) Discuss the rules for multiplication and division in $\mathbb{F}_{32}$ when one of the field elements involved is the zero element, $0 \in \mathbb{F}_{32}$.

Problem 5.6 (Second nonzero weight of an MDS code)

Show that the number of codewords of weight $d+1$ in an (n, k, d) linear MDS code over $\mathbb{F}_q$ is

$$N_{d+1} = \binom{n}{d+1}\left((q^2-1) - \binom{d+1}{d}(q-1)\right),$$

where the first term in parentheses represents the number of codewords with weight $\geq d$ in any subset of $d+1$ coordinates, and the second term represents the number of codewords with weight equal to d.

Problem 5.7 (N_d and N_{d+1} for certain MDS codes)

(a) Compute the number of codewords of weights 2 and 3 in an $(n, n-1, 2)$ SPC code over $\mathbb{F}_2$.

(b) Compute the number of codewords of weights 2 and 3 in an $(n, n-1, 2)$ linear code over $\mathbb{F}_3$.

(c) Compute the number of codewords of weights 3 and 4 in a $(4, 2, 3)$ linear code over $\mathbb{F}_3$.

Problem 5.8 ("Doubly" extended RS codes)

(a) Consider the following mapping from $(\mathbb{F}_q)^k$ to $(\mathbb{F}_q)^{q+1}$. Let $(f_0, f_1, \ldots, f_{k-1})$ be any k-tuple over $\mathbb{F}_q$, and define the polynomial $f(z) = f_0 + f_1 z + \cdots + f_{k_1} z^{k-1}$ of degree less than k. Map $(f_0, f_1, \ldots, f_{k-1})$ to the $(q+1)$-tuple $(\{f(\beta_j), \beta_j \in \mathbb{F}_q\}, f_{k-1})$— *i.e.*, , to the RS codeword corresponding to $f(z)$, plus an additional component equal to f_{k-1}.

Show that the q^k $(q+1)$-tuples generated by this mapping as the polynomial $f(z)$ ranges over all q^k polynomials over $\mathbb{F}_q$ of degree less than k form a linear $(n = q+1, k, d = n-k+1)$ MDS code over $\mathbb{F}_q$. [Hint: $f(z)$ has degree less than $k-1$ if and only if $f_{k-1} = 0$.]

(b) Construct a $(4, 2, 3)$ linear code over $\mathbb{F}_3$. Verify that all nonzero words have weight 3.