Error Correcting Codes: Combinatorics, Algorithms and Applications **(Spring 2011)**

Lecture N: Intro to Polynomial Fields

2/23/2011

Lecturer: Atri Rudra *Scribe: Dan Padgett*

1 Polynomials

Definition 1.1. *Let $\mathbb{F}_q$ be a finite field of order q. Then a function $P(x) = \sum_{i=0}^{\infty} p_i x^i, p_i \in \mathbb{F}_q$ is called a (univariate) polynomial.*

For our purposes, we will only consider the finite case; that is, $P(x) = \sum_{i=0}^{d} p_i x^i, p_i \in \mathbb{F}_q$ for some integer $d > 0$ and $p_d \neq 0$.

Definition 1.2. *In this case, we call d the degree of $P(x)$. We notate this by* $\deg(P)$.

Let $\mathbb{F}_q[x]$ be the set of polynomials over $\mathbb{F}_q$, that is, with coefficients from $\mathbb{F}_q$. Let $P(x), Q(x) \in \mathbb{F}_q[x]$ be polynomials. Then $\mathbb{F}_q[x]$ is a ring with the following operations:

Addition: $P(x) + Q(x) = \sum_{i=0}^{\max(\deg(P),\deg(Q))} (p_i + q_i)x^i$

Multiplication: $P(x) \cdot Q(x)$
i.e. $x(1 + x) = x + x^2$; $(1 + x)^2 = 1 + 2x + x^2 = 1 + x^2$ with $q = 2$.

Definition 1.3. *$\alpha \in \mathbb{F}_q$ is a root of a polynomial $P(x)$ if $P(\alpha) = 0$.*

For instance, 1 is a root of $1 + x^2$ over $\mathbb{F}_2$.

Definition 1.4. *A polynomial $P(x)$ is irreducible if $\forall Q_1(x), Q_2(x)$ such that $P(x) = Q_1(x)Q_2(x)$,* $\min(\deg(Q_1), \deg(Q_2)) = 0$

E.g. $1 + x^2$ is not irreducible over $\mathbb{F}_2$, as $(1 + x)(1 + x) = 1 + x^2$. However, $1 + x + x^2$ is irreducible, since the only possible linear terms are x and $x + 1$.

Theorem 1.5. *Let $E(x)$ be an irreducible polynomial with degree ≥ 2 over $\mathbb{F}_p$, p prime. Then the quotient ring $\mathbb{F}_p[x]/E(x)$ is a field.*

- elements are polynomials in $\mathbb{F}_p[x]$ of degree $\leq s - 1$ - there are p^s such polynomials.
- addition: $P(x) + Q(x) \mod E(x) = P(x) + Q(x)$

- multiplication: $P(x) \cdot Q(x) \mod E(x)$ = the unique polynomial $R(x)$ with degree $< s$ such that for some $A(x)$, $R(x) + A(x)E(x) = P(x) \cdot Q(x)$

Example: $\mathbb{F}_2[x]/(1 + x + x^2) \to \{0, 1, x, 1 + x\}$.

Theorem 1.6. *For all $s \geq 2$ and $\mathbb{F}_q$, $\exists$ an irreducible polynomial of degree s over $\mathbb{F}_q$. In fact, the number of such irreducible polynomials = $\theta\left(\frac{q^s}{s}\right)$.*

Corollary 1.7. *One can use a Las Vegas algorithm to efficiently generate an irreducible polynomial of degree s.*

Corollary 1.8. *Now recall that for every prime power p^s, $\exists$ a unique field $\mathbb{F}_{p^s}$. This along with theorems 1.5 and 1.6 $\implies$ The field $\mathbb{F}_{p^s}$ is $\mathbb{F}_p[x]/E(x)$, where $E(x)$ is an irreducible polynomial of degree s.*

2 Reed-Solomon Codes

Reed-Solomon codes are $(n, k)_q$ codes, where q is a prime power. They are defined by

$$RS_S : \mathbb{F}_q^k \to \mathbb{F}_q^n$$

where $S = \{\alpha_1, \ldots, \alpha_n\} \subseteq \mathbb{F}_q$. (Note that this implies $q \geq n$).

In a Reed-Solomon code, each codeword $\overline{m} = (m_0, \ldots, m_{k-1})$ is transformed into a polynomial $P_{\overline{m}}(x) = m_0 + m_1 x + \cdots + m_{k-1}x^{k-1}$. The corresponding codeword $RS_S(\overline{m})$ is then computed by

$$RS_S(\overline{m}) = (P_{\overline{m}}(\alpha_1), P_{\overline{m}}(\alpha_2), \ldots, P_{\overline{m}}(\alpha_n))$$

We claim that every Reed-Solomon code is a linear code. To verify this, it suffices to find the generator matrix G. Define G by:

$$RS_S(\overline{m}) = (m_0, \ldots, m_{k-1}) \underbrace{\begin{pmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & & \alpha_n^2 \\ \vdots & \vdots & & \vdots \\ \alpha_1^{k-1} & \alpha_2^{k-1} & \cdots & \alpha_n^{k-1} \end{pmatrix}}_{G}$$

Then G is a Vandermonde matrix, and hence has full rank if all α_i, $1 \leq i \leq n$ are distinct.