Coding Theory

(Mathematical Background II)

Lector: Nikolai L. Manev

Institute of Mathematics and Informatics, Sofia, Bulgaria

Quotient polynomial ring

Let $\mathbb{F}$ be a field and $m(x) \in \mathbb{F}[x]$. Any two polynomials $a(x)$ and $b(x)$ in $\mathbb{F}[x]$ of degree less than $m = \deg m(x)$ are non-congruent, $a(x) \not\equiv b(x) \pmod{m(x)}$, since the degree of $a(x) - b(x)$ is less than m, that is, $m(x)$ cannot divide the difference. Also, any polynomial, $a(x)$, of degree less than m is the unique polynomial of the lowest degree in the set

$$\{a(x) + f(x)m(x) \mid f(x) \in \mathbb{F}[x]\}$$

of all congruent to $a(x)$ modulo $m(x)$ polynomials.

Quotient polynomial ring

Let $\mathbb{F}$ be a field and $m(x) \in \mathbb{F}[x]$. Any two polynomials $a(x)$ and $b(x)$ in $\mathbb{F}[x]$ of degree less than $m = \deg m(x)$ are non-congruent, $a(x) \not\equiv b(x) \pmod{m(x)}$, since the degree of $a(x) - b(x)$ is less than m, that is, $m(x)$ cannot divide the difference. Also, any polynomial, $a(x)$, of degree less than m is the unique polynomial of the lowest degree in the set

$$\{a(x) + f(x)m(x) \mid f(x) \in \mathbb{F}[x]\}$$

of all congruent to $a(x)$ modulo $m(x)$ polynomials.

Definition. The set of all polynomials of degree less than $m = \deg m(x)$ which is denoted $\mathbb{F}[x]/(m(x))$, is called *ring of polynomials modulo* $m(x)$, or just *quotient ring modulo* $m(x)$.

Quotient polynomial ring

Define addition $a(x) \oplus b(x)$ and multiplication $a(x) \circ b(x)$ in $\mathbb{K} = \mathbb{F}[x]/(m(x))$ by:

$$a(x) \oplus b(x) \stackrel{\text{def}}{=} a(x) + b(x) \pmod{m(x)}$$

$$a(x) \circ b(x) \stackrel{\text{def}}{=} a(x)b(x) \pmod{m(x)}$$

It is easy to check that $\mathbb{K}$ meets all axioms of a ring. If $m(x)$ is reducible over $\mathbb{F}$, that is, $m(x) = a(x)b(x)$, then the elements of $\mathbb{K}$, $\alpha = a(x)$ and $\beta = b(x)$, satisfy $\alpha \circ \beta = 0$. Thus, a quotient polynomial ring needs not to be a field.

$\mathbb{K} = \mathbb{F}[x]/(m(x))$ is a field if and only if $m(x)$ is irreducible over $\mathbb{F}$.

Indeed, for any nonzero element $\alpha = a(x)$ of $\mathbb{K}$ there exist $u(x), v(x) \in \mathbb{F}[x]$ such that $u(x)a(x) + v(x)m(x) = 1$. Hence, for $\beta = u(x) \pmod{m(x)}$ we have $\alpha \circ \beta = 1$, i.e., $\beta = \alpha^{-1}$.

Examples.

1) $\mathbb{K} = \mathbb{Z}_2[x]/(x^2+x+1) = \{0, 1, x, x+1\} =$
$= \{0, 1, \alpha,\ \alpha^2 = \alpha + 1\}.$ $\alpha^3 = 1$ and $\alpha^{-1} = \alpha + 1.$
$|\mathbb{K}| = 4.$

2) $\mathbb{K} = \mathbb{R}[x]/(x^2+1) = \{a + bx \mid a, b \in \mathbb{R}\} \cong \mathbb{C}$. If we denote $i = x$, then $i^2 = -1$ in $\mathbb{K}$. $|\mathbb{K}| = \infty.$

3) $\mathbb{K} = \mathbb{Z}_3[x]/(x^2+1) = \{0, 1, 2, x, x+1, x+2, 2x, 2x+1, 2x+2\}.$
$|\mathbb{K}| = 9.$ $(x-1)^{-1} = x + 1.$

4) $\mathbb{K} = \mathbb{Z}_2[x]/(x^3+x+1) =$
$\{0, 1, \alpha,\ \alpha+1, \alpha^2, \alpha^2+1, \alpha^2+\alpha, \alpha^2+\alpha+1\}.$
$1, \alpha, \alpha^2$ form a basis of $\mathbb{K}$ over $\mathbb{Z}_2$. Thus, there exists one-to-one correspondence between elements of $\mathbb{K}$ and binary vectors of length 3.

Finite fields

Theorem. Any finite field $\mathbb{F}$ has a finite characteristic $p > 0$ and $q = |\mathbb{F}| = p^n$ for a suitable positive integer n. $\mathbb{F}$ coincides with the set of all roots of $x^q = x$.

Finite fields 1

Theorem. Any finite field $\mathbb{F}$ has a finite characteristic $p > 0$ and $q = |\mathbb{F}| = p^n$ for a suitable positive integer n. $\mathbb{F}$ coincides with the set of all roots of $x^q = x$.

Let $\mathbb{F}^*$ denote the subset of all nonzero elements of $\mathbb{F}$. Thus $|\mathbb{F}^*| = q - 1$ and $\mathbb{F}^*$ is the set of all roots of $x^{q-1} - 1 = 0$. $\mathbb{F}^*$ is called the *multiplicative group* of the field $\mathbb{F}$.

Definition. The *order* of an element $\beta \in \mathbb{F}^*$, written ord β, is the smallest positive integer m such that $\beta^m = 1$.

The ordβ divides any integer n for which $\beta^n = 1$.

Finite fields

Theorem. Any finite field $\mathbb{F}$ has a finite characteristic $p > 0$ and $q = |\mathbb{F}| = p^n$ for a suitable positive integer n. $\mathbb{F}$ coincides with the set of all roots of $x^q = x$.

Let $\mathbb{F}^*$ denote the subset of all nonzero elements of $\mathbb{F}$. Thus $|\mathbb{F}^*| = q - 1$ and $\mathbb{F}^*$ is the set of all roots of $x^{q-1} - 1 = 0$. $\mathbb{F}^*$ is called the *multiplicative group* of the field $\mathbb{F}$.

Definition. The *order* of an element $\beta \in \mathbb{F}^*$, written ord β, is the smallest positive integer m such that $\beta^m = 1$.

The ordβ divides any integer n for which $\beta^n = 1$.

Theorem. There exists an element $\alpha \in \mathbb{F}^*$ such that

$$\mathbb{F}^* = \{1, \alpha, \alpha^2, \alpha^3, \ldots, \alpha^{q-2}\} \text{ and } \alpha^{q-1} = 1.$$

Definition. Any element of $\mathbb{F}^*$ with order $q - 1$ is called a *primitive element of the field.*

Theorem. Any finite field $\mathbb{F}$ with $|\mathbb{F}| = p^n$ is $\mathbb{F} \cong \mathbb{Z}_p[x]/(m(x))$, where $m(x)$ is irreducible over $\mathbb{F}$ polynomial with degree $\deg f(x) = n$ and $m(x)$ divides $x^{p^n} - x$.

Definition. Two fields $\mathbb{F}_1$ and $\mathbb{F}_2$ are *isomorphic, written* $\mathbb{F}_1 \cong \mathbb{F}_2$, if there exists a bijection $\varphi : \mathbb{F}_1 \to \mathbb{F}_2$, such that

$$\varphi(a+b) = \varphi(a) + \varphi(b) \text{ and } \varphi(ab) = \varphi(a)\varphi(b), \quad \forall a, b \in \mathbb{F}_1.$$

Theorem. Any finite field $\mathbb{F}$ with $|\mathbb{F}| = p^n$ is $\mathbb{F} \cong \mathbb{Z}_p[x]/(m(x))$, where $m(x)$ is irreducible over $\mathbb{F}$ polynomial with degree $\deg f(x) = n$ and $m(x)$ divides $x^{p^n} - x$.

Definition. Two fields $\mathbb{F}_1$ and $\mathbb{F}_2$ are *isomorphic, written* $\mathbb{F}_1 \cong \mathbb{F}_2$, if there exists a bijection $\varphi : \mathbb{F}_1 \to \mathbb{F}_2$, such that

$$\varphi(a+b) = \varphi(a) + \varphi(b) \text{ and } \varphi(ab) = \varphi(a)\varphi(b), \quad \forall a, b \in \mathbb{F}_1.$$

Theorem. For any prime p and any positive integer n there exists an unique up to isomorphism finite field with p^n elements.

The unique field with p^n elements is denoted $GF(p^n)$ and called *Galois field* after Evariste Galois.

Theorem. The finite field $GF(p^m)$ is a subfield of $GF(p^n)$ if and only if $m|n$.

For example, $GF(4) \not\subset GF(8)$, but $GF(4) \subset GF(16)$.

Theorem. The finite field $GF(p^m)$ is a subfield of $GF(p^n)$ if and only if $m|n$.

For example, $GF(4) \not\subset GF(8)$, but $GF(4) \subset GF(16)$.

Theorem. Let $f(x)$ be an irreducible polynomial over $GF(q),\ q = p^n$, with degree $m = \deg f(x)$. The set of its root consists of

$$\alpha, \alpha^q, \ldots, \alpha^{q^{m-1}},$$

where α is someone of its root.

All roots of $f(x)$ are called *conjugates to α with respect to, or over, $\mathbb{F}$*, and form the *conjugacy class of α*.

Theorem. The finite field $GF(p^m)$ is a subfield of $GF(p^n)$ if and only if $m|n$.

For example, $GF(4) \not\subset GF(8)$, but $GF(4) \subset GF(16)$.

Theorem. Let $f(x)$ be an irreducible polynomial over $GF(q),\ q = p^n$, with degree $m = \deg f(x)$. The set of its root consists of

$$\alpha, \alpha^q, \ldots, \alpha^{q^{m-1}},$$

where α is someone of its root.

All roots of $f(x)$ are called *conjugates to α with respect to, or over, $\mathbb{F}$*, and form the *conjugacy class of α*.

Definition. Let $\mathbb{F} = GF(q)$, $\mathbb{K} \supseteq \mathbb{F}$, and $\alpha \in \mathbb{K}$. The *minimal polynomial of α over $\mathbb{F}$* is the smallest-degree monic polynomial $m(x) \in \mathbb{F}[x]$ such that $m(\alpha) = 0$. We denote $m(x) = \mathrm{irr}_F \alpha$. The minimal polynomial is irreducible.

Definition. A polynomial $m(x)$ of degree m over $GF(q)$ is said to be a *primitive polynomial*, if it is irreducible and the smallest positive integer n for which $m(x)$ divides $x^n - 1$ is $n = q^m - 1$.

Definition. The *period, or order*, of a polynomial $f(x)$ is defined as the smallest positive integer n for which $f(x)$ divides $x^n - 1$.

Hence, the primitive polynomials are ones with period $n = q^m - 1$.

Definition. A polynomial $m(x)$ of degree m over $GF(q)$ is said to be a *primitive polynomial*, if it is irreducible and the smallest positive integer n for which $m(x)$ divides $x^n - 1$ is $n = q^m - 1$.

Definition. The *period, or order*, of a polynomial $f(x)$ is defined as the smallest positive integer n for which $f(x)$ divides $x^n - 1$.

Hence, the primitive polynomials are ones with period $n = q^m - 1$.

Theorem. Let $\mathbb{F} = GF(q)$. The splitting field of any irreducible over $\mathbb{F}$ polynomial $m(x) \in \mathbb{F}[x]$ of degree $\deg m(x) = m$ is the field $GF(q^m)$. A root of $m(x)$ is a primitive element of $GF(q^m)$ if and only if $m(x)$ is a primitive polynomial.

Example. Consider $x^8 - 1$ as a polynomial over $\mathbb{Z}_3$. In the ring $\mathbb{Z}_3[x]$ we have

$$x^8-1 = (x^4-1)(x^4+1) = (x^2-1)(x^2+1)(x^2+x-1)(x^2-x-1).$$

Therefore $x^2 + x - 1$ and $x^2 - x - 1$ are primitive, while $x^2 + 1$ is not a primitive polynomial. The period of $x^2 + 1$ is 4.

What is the difference in constructing a finite field by a primitive and non-primitive polynomial?

The quotient rings $\mathbb{Z}_3[x]/(x^2 + 1)$ and $\mathbb{Z}_3[x]/(x^2 + x - 1)$ are both isomorphic to $GF(3^2)$, that is, they are two representations of $GF(3^2)$. Let α and β be the residue class of x modulo $(x^2 + 1)$ and $(x^2 + x - 1)$, respectively. Hence

$$GF(9) = \{0, 1, 2, \alpha, \alpha+1, \alpha+2, 2\alpha, 2\alpha+1, 2\alpha+2\},\ \alpha^2+1=0$$

$$GF(9) = \{0, 1, 2, \beta, \beta+1, \beta+2, 2\beta, 2\beta+1, 2\beta+2\},\ \beta^2+\beta-1=0.$$

The difference is in that $\beta^4 = -1,\ \beta^8 = 1$, that is, β is a primitive element of the field, while $\alpha^4 = 1$ and α is not a primitive element of $GF(9)$ (only $1, \alpha, \alpha^2$ and α^3 are different). In the former case we can represent the elements of $GF(9)$ as powers of β, that is, $GF(9) = \{0, 1, \beta, \beta^2, \ldots, \beta^7\}$.

This representation is often called *multiplicative*. It allows the nonzero elements of $GF(9)$ to be indexed by the numbers $0, 1, 2, \ldots, 7$ (Zech's logarithms).

Ideals in rings

Definition. Let R be a ring. A nonempty subset $I \subseteq R$ is said to be an *ideal, written* $I \lhd R$, if it satisfies the following:

(1) If $a, b \in I$, then $a - b \in I$;

(2) $r \cdot a \in I$ for all $a \in I$ and for all $r \in R$.

An ideal $I \lhd R$ is called *principle*, if there exists $g \in R$ such that any element of I can be expressed as the product rg for some $r \in R$. It is denoted $I = (g)$. The element g is called the *generator element* of I.

Theorem. Let $\mathbb{F}$ be a field and $f(x) \in \mathbb{F}[x]$. If I is an ideal in $R_n = \mathbb{F}[x]/(f(x))$, then there exists an unique monic polynomial $g(x) \in R_n$ such that $I = (g(x))$ and $g(x)$ divides $f(x)$ in $\mathbb{F}[x]$. The generator polynomial $g(x)$ has minimal degree among the polynomials in I.

Examples.

1. In $\mathbb{Z}$ all ideals are principle and have the form $(n) = n\mathbb{Z} = \{na \mid a = 0, \pm 1, \pm 2, \ldots\}$.
2. In $\mathbb{F}[x]$, $\mathbb{F}$ is a field, all ideals are principle and have the form $(f(x))$, where $f(x) \in \mathbb{F}[x]$.
3. In $\mathbb{F}[x]/(x^n - 1)$ all ideals are also principle and have the form $(g(x))$, where $g(x) \in \mathbb{F}[x]$ is uniquely determined and $g(x)$ divides $x^n - 1$.