Finite Fields: Part I

Cunsheng Ding

HKUST, Hong Kong

November 20, 2015

Contents

The Objectives of this Lecture

The finite fields we learnt so far

Prime fields $(\mathbb{Z}_p, \oplus_p, \otimes_p)$, where p is any prime. In the future, we will use $+$ and $\cdot$ to mean $\oplus_p$ and $\otimes_p$, respectively.

Throughout this lecture, $\mathrm{GF}(p)$ denotes the finite field $(\mathbb{Z}_p, \oplus_p, \otimes_p)$, where p is any prime. We define $\mathrm{GF}(p)^* = \mathrm{GF}(p) \setminus \{0\}$.

Our objectives

Our major objectives in this lecture and the next ones are to treat finite fields $\mathrm{GF}(p^m)$ with p^m elements. Our approach will be **constructive**, so that it will be easy to understand. To this end, we need to employ irreducible polynomials over $\mathrm{GF}(p)$.

Irreducible Polynomials in $\mathrm{GF}(p)[x]$

Recall of definition

A polynomial $f \in \mathrm{GF}(p)[x]$ with positive degree is called irreducible over $\mathrm{GF}(p)$ if f has only constant divisors a and divisors of the form af, where $a \in \mathrm{GF}(p)^*$.

Question 1

- *Is there any irreducible polynomial over $\mathrm{GF}(p)$ of degree d for any given positive integer m and prime p?*
- *What is the total number of irreducible polynomials over $\mathrm{GF}(p)$ of degree m?*
- *How to find out an irreducible polynomial over $\mathrm{GF}(p)$ of degree m, if it exists?*

The Möbius Function $\mu(n)$

Definition 1

The Möbius function μ is the function on $\mathbb{N}$ defined by

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1, \\ (-1)^k & \text{if } n \text{ is the product of } k \text{ distinct primes,} \\ 0 & \text{if } n \text{ is divisible by the square of a prime.} \end{cases}$$

Example 2

Some initial terms of the Möbius sequence $(\mu(i))_{i=1}^{\infty}$ is given by

$$(1, -1, -1, 0, -1, 1, -1, 0, 0, 1, \ldots,).$$

The Number of Irreducible Polynomials over $\mathrm{GF}(p)$

Theorem 3

The number $N_p(m)$ of monic irreducible polynomials in $\mathrm{GF}(p)[x]$ of degree m is given by

$$N_p(m) = \frac{1}{m}\sum_{d|m}\mu(m/d)p^d = \frac{1}{m}\sum_{d|m}\mu(d)p^{m/d}.$$

Remarks

- For a proof, see Chapter 3 of Lidl and Niederreiter.
- $N_p(m) \geq \frac{1}{m}(p^m - p^{m-1} - p^{m-2} - \cdots - p) = \frac{1}{m}\left(p^m - \frac{p^m - p}{p-1}\right) > 0.$
- For the construction of irreducible polynomials in $\mathrm{GF}(p)[x]$ of any degree, see Section 3.3 of Lidl and Niederreiter.
- Tables of monic irreducible polynomials of certain degrees in $\mathrm{GF}(p)[x]$ are given in the Appendix of Lidl and Niederreiter.

Examples of Irreducible Polynomials in $\mathrm{GF}(p)[x]$

Example 4

All monic irreducible polynomials of degree 4 in $\mathrm{GF}(2)[x]$ are given by

$$x^4+x^3+1,\ x^4+x^3+x^2+x+1,\ x^4+x+1.$$

Example 5

All monic irreducible polynomials of degree 3 in $\mathrm{GF}(3)[x]$ are given by

$$x^3+2x+1,\ x^3+2x^2+2x+2,\ x^3+x^2+x+2,\ x^3+2x+2,$$
$$x^3+x^2+2,\ x^3+2x^2+x+1,\ x^3+x^2+2x+1,\ x^3+2x^2+1$$

Remark

These are computed with the Magma software package using the command AllIrreduciblePolynomials(F, m)

Finite Fields $\mathrm{GF}(p^m)$

Existence of an irreducible polynomial of degree m over $\mathrm{GF}(p)$

For any prime p and positive integer m, we are now ready to construct the finite field $\mathrm{GF}(p^m)$ with p^m elements.
By Theorem 3, we see that the number $N_p(m)$ of irreducible polynomials of degree m over $\mathrm{GF}(p)$ is at least one.

Building materials

p, m and a monic irreducible polynomial $p(x)$ of degree m over $\mathrm{GF}(p)$.

The set $\mathrm{GF}(p^m)$

$\mathrm{GF}(p^m)$ consists of all polynomials of degree at most $m-1$ over $\mathrm{GF}(p)$.

The Set $\mathrm{GF}(2^3)$

Example 6

Let $p = 2$ and $m = 3$. Then the set $\mathrm{GF}(2^3)$ is composed of the following 8 polynomials:

$$\begin{array}{llll} f_0 = 0, & f_1 = 1, & f_2 = x, & f_3 = 1 + x, \\ f_4 = x^2, & f_5 = 1 + x^2, & f_6 = x + x^2, & f_7 = 1 + x + x^2. \end{array}$$

Addition of the Finite Fields $\mathrm{GF}(p^m)$

Definition 7

Let

$$f(x) = \sum_{i=0}^{m-1} a_i x^i \in \mathrm{GF}(p)[x] \text{ and } g(x) = \sum_{i=0}^{m-1} b_i x^i \in \mathrm{GF}(p)[x].$$

Then the addition of f and g is defined by

$$f(x) + g(x) = \sum_{i=0}^{m-1} (a_i + b_i) x^i \in \mathrm{GF}(p)[x].$$

Theorem 8

$(\mathrm{GF}(p^m), +)$ is a finite abelian group with the identity 0, i.e., the zero polynomial.

Proof.

It is straightforward and left as an exercise. $\square$

Multiplication of the Finite Fields $\mathrm{GF}(p^m)$

Definition 9

Let $\pi(x) \in \mathrm{GF}(p)[x]$ be a monic irreducible polynomial of degree m over $\mathrm{GF}(p)$, and let

$$f(x) = \sum_{i=0}^{m-1} a_i x^i \in \mathrm{GF}(p)[x] \text{ and } g(x) = \sum_{i=0}^{m-1} b_i x^i \in \mathrm{GF}(p)[x].$$

Then the multiplication of f and g is defined by

$$f(x) \cdot g(x) = f(x)g(x) \bmod \pi(x),$$

where $f(x)g(x)$ is the ordinary multiplication of two polynomials.

Remark

The multiplication $\cdot$ depends on the irreducible polynomial $\pi(x)$.

Multiplication of the Finite Fields $\mathrm{GF}(p^m)$

Example 10

Let $p = 2$ and $m = 3$, and let the monic irreducible polynomial $\pi(x) = x^3 + x + 1 \in \mathrm{GF}(2)[x]$. Then the set $\mathrm{GF}(2^3)$ is composed of the following 8 polynomials:

$$
\begin{array}{llll}
f_0 = 0, & f_1 = 1, & f_2 = x, & f_3 = 1 + x, \\
f_4 = x^2, & f_5 = 1 + x^2, & f_6 = x + x^2, & f_7 = 1 + x + x^2.
\end{array}
$$

By definition

$$
\begin{aligned}
f_6 \cdot f_7 &= f_6 f_7 \bmod \pi(x) = (x^4 + x) \bmod x^3 + x + 1 = x^2, \\
f_7 \cdot f_7 &= f_7 f_7 \bmod \pi(x) = (x^4 + x + 1) \bmod x^3 + x + 1 = 1 + x.
\end{aligned}
$$

Multiplication of the Finite Fields $\mathrm{GF}(p^m)$

Proposition 11

Let $\pi(x)$ be a monic irreducible polynomial over $\mathrm{GF}(p)$ of degree m. Let $f \in \mathrm{GF}(p^m)$ and $f \neq 0$. Then there is an element $g \in \mathrm{GF}(p^m)$ such that $f \cdot g = 1$. This polynomial g is called the *multiplicative inverse* *of f modulo π.*

Proof.

Since $\pi(x)$ is irreducible and $f \neq 0$ with degree at most $m-1$, $\gcd(f, \pi) = 1$. By Theorem 21 in the previous lecture and with the Extended Eulidean Algorithm, one can find two polynomials $u(x) \in \mathrm{GF}(p)[x]$ and $v(x) \in \mathrm{GF}(p)[x]$ such that

$$1 = \gcd(f, \pi) = uf + v\pi.$$

It then follows that $uf \bmod \pi = 1$. Hence, $g = u \bmod \pi$ is the desired polynomial. $\square$

Multiplication of the Finite Fields $\mathrm{GF}(p^m)$

Theorem 12

Let $\mathrm{GF}(p^m)^* = \mathrm{GF}(p^m) \setminus \{0\}$. *Then* $(\mathrm{GF}(p^m)^*, \cdot)$ *is a finite abelian group with identity* 1.

Proof.

Since $\pi(x)$ is irreducible, $\mathrm{GF}(p^m)^*$ is closed under the binary operation $\cdot$. It is obvious that 1 is the identity. By Proposition 11, every element $f \in \mathrm{GF}(p^m)^*$ has its inverse. The binary operation $\cdot$ is commutative, as the ordinary multiplication for polynomials over $\mathrm{GF}(p)$ is so. The desired conclusion then follows. $\square$

Finite Field $(\mathrm{GF}(p^m), +, \cdot)$

Theorem 13

Let $\pi(x) \in \mathrm{GF}(p)[x]$ *be any irreducible polynomial over* $\mathrm{GF}(p)$ *with degree m. Then* $(\mathrm{GF}(p^m), +, \cdot)$ *is a finite field with* p^m *elements.*

Proof.

By the definitions of the binary operations $+$ and $\cdot$, the distribution laws hold. It then follows from Theorems 8 and 12 that $(\mathrm{GF}(p^m), +, \cdot)$ is a finite field with p^m elements. $\square$

Characteristics of Fields

Definition 14

Let $\mathbb{F}$ be a field. If there exists a positive integer n such that $na = 0$ for all $a \in \mathbb{F}$, such least n is called the characteristic of $\mathbb{F}$. If there is no such n, we say that $\mathbb{F}$ has characteristic 0.

Example 15

- The field $(\mathbb{Q}, +, \cdot)$ of rational numbers has characteristic 0.
- The field $(\mathbb{R}, +, \cdot)$ of real numbers has characteristic 0.
- The field $(\mathbb{C}, +, \cdot)$ of complex numbers has characteristic 0.

Characteristics of Fields

Theorem 16

The finite field $\mathrm{GF}(p^m)$ *has characteristic* p*.*

Proof.

By definition, $\mathrm{GF}(p) \subseteq \mathrm{GF}(p^m)$. The smallest positive integer n such that $na = 0$ for all $a \in \mathrm{GF}(p)$ is equal to p, as $(\mathrm{GF}(p), \oplus_p)$ is cyclic. On the other hand, by definition, $pf = 0$ for all $f \in \mathrm{GF}(p^m)$. The desired conclusion then follows. □

Properties of Finite Fields

Theorem 17

Let $\mathbb{F}$ be any field with characteristic p. Then $(a+b)^{p^n} = a^{p^n} + b^{p^n}$ for all $a, b \in \mathbb{F}$ and $n \in \mathbb{N}$.

Proof.

For all integers i with $1 \leq i \leq p-1$, we have

$$\binom{p}{i} = \frac{p(p-1)\cdots(p-i+1)}{1 \cdot 2 \cdot \cdots \cdot i} \equiv 0 \pmod{p}.$$

Then by the binomial theorem,

$$(a+b)^p = a^p + \binom{p}{1} a^{p-1} b + \cdots + \binom{p}{p-1} a b^{p-1} + b^p = a^p + b^p.$$

The desired conclusion follows the induction on n. $\square$