A Basics of Finite Fields

A.1 Constructions and Computations

The following theorem could be called the fundamental theorem of finite fields.

**Theorem A.1.** For every prime power \( q \), there is a field of size \( q \), and it is unique up to isomorphism. There are no other finite fields.

The field with \( q \) elements can be denoted by \( \mathbb{F}_q \). The following theorem states how finite fields can be constructed.

**Theorem A.2.** If \( p \) is a prime, then integers modulo \( p \) form a finite field of size \( p \).

If \( q \) is a prime power, \( n \geq 2 \) an integer, and \( f(x) \in \mathbb{F}_q[x] \) an irreducible polynomial of degree \( n \), then the polynomials in \( \mathbb{F}_q[x] \) modulo \( f(x) \) form a finite field of size \( q^n \).

Note that if \( q \) is not a prime, then integers modulo \( q \) do not form a field. The second part of Theorem A.2 is most often used with a prime \( q \); this is sufficient for constructing all finite fields. However, if we already have constructed the field \( \mathbb{F}_p^k \), we can use the theorem with \( q = p^k \) to construct the field \( \mathbb{F}_{p^k} \).

Using the notation of Theorem A.2, we can write

\[
\mathbb{F}_{q^n} = \{ a_0 x^0 + \cdots + a_{n-1} x^{n-1} \mid a_0, \ldots, a_{n-1} \in \mathbb{F}_q, f(x) = 0 \}.
\]

We can also say that this is the field \( \mathbb{F}_{q^n} \) defined by \( f(x) \). If the elements of a finite field are written like this, they can be added like polynomials:

\[
\sum_{i=0}^{n-1} a_i x^i + \sum_{i=0}^{n-1} b_i x^i = \sum_{i=0}^{n-1} (a_i + b_i) x^i.
\]

They can also be multiplied like polynomials, except that we must use the relation \( f(x) = 0 \) to get rid of powers \( x^k \) with \( k \geq n \).

**Example A.3.** For a prime \( p \), we will always use the notation \( \mathbb{F}_p = \{ 0, \ldots, p-1 \} \) with the understanding that the elements are integers modulo \( p \).

We will use the field \( \mathbb{F}_2 = \{ 0, 1 \} \) particularly often, because its elements can be interpreted as bits, addition as XOR, and multiplication as AND. Remember that \( 1 = -1 \) in this field, and in every field \( \mathbb{F}_{2^n} \), so addition and subtraction are the same thing.

Bytes (sequences of eight bits) can be interpreted as elements of \( \mathbb{F}_{2^8} \) so that addition is bitwise XOR. Multiplication does not have any simple interpretation, but it can be implemented efficiently. This is used in AES, for example.

**Example A.4.** The polynomial \( x^3 + x + 1 \in \mathbb{F}_2[x] \) is irreducible, so we can let

\[
\mathbb{F}_8 = \{ a + bx + cx^2 \mid a, b, c \in \mathbb{F}_2, \ x^3 = 1 + x \}.
\]

Let us compute the sum and product of \( 1 + x^2 \) and \( 1 + x + x^2 \) in this field. We have \((1 + x^2) + (1 + x + x^2) = x \) and

\[
(1 + x^2)(1 + x + x^2) = 1 + x + x^2 + x^2 + x^3 + x^4 = 1 + x + x^3 + x^4 = x(1 + x) = x + x^2.
\]
We could also use the irreducible polynomial \( x^3 + x^2 + 1 \in \mathbb{F}_2[x] \) and let 
\[ \mathbb{F}_8 = \{ a + bx + cx^2 \mid a, b, c \in \mathbb{F}_2, \; x^3 = 1 + x^2 \}. \]
Let us compute the sum and product \( 1 + x^2 \) and \( 1 + x + x^2 \) in this field. We have 
\[ (1 + x^2) + (1 + x + x^2) = x \]
and 
\[ (1 + x^2)(1 + x + x^2) = 1 + x + x^2 + x^2 + x^3 + x^4 = 1 + x + x^3 + x^4 = 1 + x + x^3 + x(1 + x^2) = 1. \]
This construction of \( \mathbb{F}_8 \) looks different, but it is isomorphic to the first one.

It is often useful to remember that \((a + b)p = a^p + b^p\) for all \(a, b \in \mathbb{F}_{p^n}\).

**Example A.5.** The polynomial \( x^2 + 1 \in \mathbb{F}_3[x] \) is irreducible, so we can let 
\[ \mathbb{F}_9 = \{ a + bx \mid a, b \in \mathbb{F}_3, \; x^2 = -1 \}. \]
Let us compute the square and cube of \( 1 + 2x \) in this field. We have 
\[ (1 + 2x)^2 = 1 + 4x + 4x^2 = 1 + x + x^2 = x. \]
Here are two ways two compute the cube:
\[ (1 + 2x)^3 = (1 + 2x)(1 + 2x)^2 = (1 + 2x)x = x + 2x^2 = 1 + x, \]
\[ (1 + 2x)^3 = 1^3 + (2x)^3 = 1 + 8x^3 = 1 + 2x^3 = 1 + x. \]

The next lemma gives the irreducible polynomials that can be used to construct the fields \( \mathbb{F}_4, \mathbb{F}_8, \mathbb{F}_{16}, \) and \( \mathbb{F}_{32} \).

**Lemma A.6.** The irreducible polynomials of degrees 2, 3, 4 and 5 in \( \mathbb{F}_2[x] \) are given below.

- **Degree 2:** \( 1 + x + x^2 \).
- **Degree 3:** \( 1 + x + x^3, 1 + x^2 + x^3 \).
- **Degree 4:** \( 1 + x + x^4, 1 + x^3 + x^4, 1 + x + x^2 + x^3 + x^4 \).
- **Degree 5:** \( 1 + x^2 + x^5, 1 + x^3 + x^5, 1 + x + x^2 + x^3 + x^5, 1 + x + x^2 + x^4 + x^5, 1 + x + x^3 + x^4 + x^5, 1 + x^2 + x^3 + x^4 + x^5 \).

**Proof.** We will prove the cases of degrees 2 and 4; degrees 3 and 5 are left as an exercise.

A polynomial \( a + bx + x^2 \in \mathbb{F}_2[x] \) is reducible iff it has a root in \( \mathbb{F}_2 \). It has a root 0 iff \( a = 0 \), and a root 1 iff \( a + b + 1 = 0 \). Thus it is irreducible iff \( a = b = 1 \).

A polynomial \( a + bx + cx^2 + dx^3 + x^4 \) is reducible iff it has a root in \( \mathbb{F}_2 \) or is a product of irreducible polynomials of degree 2. It has a root iff \( a = 0 \) or \( a + b + c + d + 1 = 0 \), and it is a product of irreducible polynomials of degree 2 iff it is \( (1 + x + x^2)^2 = 1 + x^2 + x^4 \). This specifies the required three irreducible polynomials. \( \square \)
A.2 Order of an element

The order of an element $a$ in a group is the smallest positive integer $n$ such that $a^n = 1$. It is denoted by $\text{ord}(a)$. The order of an element divides the size of the group. To determine $\text{ord}(a)$ in a group of size $m$, it is sufficient to calculate $a^d$ for every $d|m$, $d < m$.

We will mostly use order in the multiplicative group $\mathbb{F}_q^*$ of a finite field $\mathbb{F}_q$. The size of $\mathbb{F}_q^*$ is $q-1$.

Example A.7. Every element of $\mathbb{F}_8^*$ has order either 1 or 7. The only element with order 1 is the identity element 1.

Every element of $\mathbb{F}_{16}^*$ has order either 1, 3, 5, or 15. The order of $a \neq 1$ can be determined as follows: If $a^3 = 1$, then $\text{ord}(a) = 3$. If $a^5 = 1$, then $\text{ord}(a) = 5$. If $a^3 \neq a^5$, then $\text{ord}(a) = 15$.

Example A.8. Let $a \in \mathbb{F}_q^*$. If $n$ is a large integer, then computing $a^n$ can be made easier by reducing $n$ modulo $\text{ord}(a)$, or modulo $q-1$ if $\text{ord}(a)$ is not known. For example, if $\text{ord}(a) = 10$, then $a^{205} = a^{200 \cdot 5} = (a^{10})^{20 \cdot 5} = 1^{20} \cdot a^5 = a^5$.

The inverse $a^{-1}$ can be computed as $a^{\text{ord}(a)-1}$ or as $a^{q-2}$. However, sometimes there are easier ways. In particular, if the field is defined by $a_0 x^0 + \cdots + a_n x^n$, then the inverse of $x$ is

$$x^{-1} = -a_0^{-1}(a_1 x^0 + \cdots + a_n x^{n-1}).$$

An irreducible polynomial $f(x) \in \mathbb{F}_q[x]$ of degree $n \geq 2$ is primitive if the order of $x$ modulo $f(x)$ is $q^n - 1$. In other words, $f(x)$ is primitive if and only if the multiplicative group of the field

$$\mathbb{F}_{q^n} = \{ a_0 x^0 + \cdots + a_{n-1} x^{n-1} \mid a_0, \ldots, a_{n-1} \in \mathbb{F}_q, f(x) = 0 \}$$

is generated by $x$, that is,

$$\mathbb{F}_{q^n}^* = \{ x^0, \ldots, x^{q^n-2} \}.$$ 

If $q^n - 1$ is prime, then every irreducible polynomial is primitive.

Example A.9. Let us find out which polynomials in Lemma A.6 are primitive. Because $2^n - 1$ is prime for $n \in \{2, 3, 5\}$, all of these polynomials of degrees 2, 3 and 5 are primitive. For degree 4, we can follow example A.7 to see when the order is 15. Clearly, $x^3 \neq 1$ modulo every polynomial of degree 4, and

$$x^5 = x(1 + x) = x + x^2 \neq 1 \quad \text{(mod } 1 + x + x^4),$$

$$x^5 = x(x + x^3) = x + x^4 = x + 1 + x^3 \neq 1 \quad \text{(mod } 1 + x^3 + x^4),$$

$$x^5 = x(1 + x + x^2 + x^3) = x + x^2 + x^3 + x^4 = 1 \quad \text{(mod } 1 + x + x^2 + x^3 + x^4),$$

so only $1 + x + x^2 + x^3 + x^4$ is not primitive.

Often it is useful to construct finite fields with primitive polynomials. Luckily, this is always possible by the following theorem.
Theorem A.10. For every prime power $q$ and integer $n \geq 2$, there exists a primitive polynomial of degree $n$ in $\mathbb{F}_q[x]$.

The following theorem is occasionally useful.

Theorem A.11. Let $a \in \mathbb{F}_{q^n}$. Then $a \in \mathbb{F}_q$ if and only if $a^q = a$.

Proof. If $a \in \mathbb{F}_{q^n}^*$, then $\text{ord}(a)|(q - 1)$, so $a^{q-1} = 1$. Thus $a^q = a$, and of course $0^q = 0$.

If $a \in \mathbb{F}_{q^n}$ and $a^q = a$, then $a$ is a root of the polynomial $x^q - x$. Every element of $\mathbb{F}_q$ is a root of this polynomial, and it cannot have more than $q$ roots, so $a \in \mathbb{F}_q$. \qed