Finite Fields: Part III

Cunsheng Ding

HKUST, Hong Kong

November 21, 2015

Contents

Our Objectives

- Treat $\mathrm{GF}(q^n)$ as a vector space over $\mathrm{GF}(q)$.
- Introduce normal bases of $\mathrm{GF}(q^n)$ over $\mathrm{GF}(q)$.
- Study the trace and norm functions on finite fields.
- Introduce some applications of finite fields.

Vector Spaces V over a Fielf $\mathbb{F}$

Definition 1

A vector space V over $\mathbb{F}$ has a binary operation "$+$" on V and a scalar multiplication on $\mathbb{F} \times V$ such that

1. $(V, +)$ is an abelian group with identity 0;
2. $av \in V$ for all $a \in \mathbb{F}$ and all $v \in V$;
3. $a(bv) = (ab)v$ for all $a, b \in \mathbb{F}$ and all $v \in V$;
4. $(a+b)v = av + bv$ for all $a, b \in \mathbb{F}$ and all $v \in V$;
5. $a(v_1 + v_2) = av_1 + av_2 \in V$ for all $a \in \mathbb{F}$ and all $v_1, v_2 \in V$; and
6. $1v = v$ for all $v \in V$.

Vector Spaces V over a Fielf $\mathbb{F}$

Definition 2

Let V be a vector space over a field $\mathbb{F}$. A set $\{v_1, v_2, \cdots, v_n\}$ of elements in V is called a basis of V over $\mathbb{F}$ if

- $v_1, v_2, \cdots, v_n$ are linearly independent over $\mathbb{F}$, i.e., $\sum_{i=1}^n a_i v_i = 0$, where all $a_i \in \mathbb{F}$, if and only if all $a_i = 0$; and
- every element $v \in V$ can be expressed as $v = \sum_{i=1}^n a_i v_i$, where all $a_i \in \mathbb{F}$.

In this case, we say that V has dimension n or V is an n-dimensional vector space over $\mathbb{F}$.

Example 3

$\mathbb{Q}^n = \mathbb{Q} \times \mathbb{Q} \times \cdots \times \mathbb{Q}$ is an n-dimensional vector space over the field $\mathbb{Q}$ of rational numbers.

$\mathrm{GF}(q^n)$ as an n-Dimensional Vector Space over $\mathrm{GF}(q)$

Theorem 4

$\mathrm{GF}(q^n)$ is an n-dimensional vector space over $\mathrm{GF}(q)$ with respect to the addition and multiplication of the finite field $\mathrm{GF}(q^n)$.

Proof.

$\mathrm{GF}(q^n)$ is a vector space over $\mathrm{GF}(q)$ due to the following:

1. $(\mathrm{GF}(q^n), +)$ is an abelian group with identity 0;
2. $av \in \mathrm{GF}(q^n)$ for all $a \in \mathrm{GF}(q)$ and all $v \in \mathrm{GF}(q^n)$;
3. $a(bv) = (ab)v$ for all $a, b \in \mathrm{GF}(q)$ and all $v \in \mathrm{GF}(q^n)$;
4. $(a+b)v = av + bv$ for all $a, b \in \mathrm{GF}(q)$ and all $v \in \mathrm{GF}(q^n)$;
5. $a(v_1 + v_2) = av_1 + av_2 \in \mathrm{GF}(q^n)$ for all $a \in \mathrm{GF}(q)$ and all $v_1, v_2 \in \mathrm{GF}(q^n)$; and
6. $1v = v$ for all $v \in \mathrm{GF}(q^n)$.

□

$\mathrm{GF}(q^n)$ as an n-Dimensional Vector Space over $\mathrm{GF}(q)$

Proof of the dimension of $\mathrm{GF}(q^n)$ over $\mathrm{GF}(q)$.

Let α be a generator of $\mathrm{GF}(q^n)^*$. It was demonstrated in the previous lecture that the minimal polynomial $P_\alpha(x)$ over $\mathrm{GF}(q)$ of α has degree n. We now claim that $\{1, \alpha, \alpha^2, \cdots, \alpha^{n-1}\}$ is a basis of $\mathrm{GF}(q^n)$ over $\mathrm{GF}(q)$.
First of all, $1, \alpha, \alpha^2, \cdots, \alpha^{n-1}$ are linearly independent over $\mathrm{GF}(q)$, otherwise, the minimal polynomial of α over $\mathrm{GF}(q)$ would have degree less than n.
Second, the set $\{\sum_{i=0}^{n-1} a_i \alpha^i \mid a_i \in \mathrm{GF}(q)\}$ has cardinality q^n, as $1, \alpha, \alpha^2, \cdots, \alpha^{n-1}$ are linearly independent over $\mathrm{GF}(q)$.
Hence $\{1, \alpha, \alpha^2, \cdots, \alpha^{n-1}\}$ is a basis of $\mathrm{GF}(q^n)$ over $\mathrm{GF}(q)$, and is referred to as a polynomial basis.

□

The Dimension of $\mathbb{F}$ as a Vector Space over $\mathbb{K}$

Definition 5

Let $\mathbb{K}$ be a subfield of $\mathbb{F}$. We use $[\mathbb{F} : \mathbb{K}]$ to denote the dimension of $\mathbb{F}$ when $\mathbb{F}$ is viewed as a vector space over $\mathbb{K}$.

Example 6

$[\mathrm{GF}(q^n) : \mathrm{GF}(q)] = n$.

Normal Bases of $\mathrm{GF}(q^n)$ over $\mathrm{GF}(q)$

Definition 7

A basis of $\mathrm{GF}(q^n)$ over $\mathrm{GF}(q)$ of the form $\{\alpha, \alpha^q, \cdots, \alpha^{q^{n-1}}\}$ is called a <u>normal basis</u> of $\mathrm{GF}(q^n)$ over $\mathrm{GF}(q)$, where $\alpha \in \mathrm{GF}(q^n)$.

Example 8

Let α be a generator of $\mathrm{GF}(2^3)^*$ with minimal polynomial $x^3 + x^2 + 1$ over $\mathrm{GF}(2)$. Then $\{\alpha, \alpha^2, \alpha^4\}$ is a normal basis of $\mathrm{GF}(2^3)$ over $\mathrm{GF}(2)$. Note that $\alpha^4 = 1 + \alpha + \alpha^2$.

Normal Bases of $\mathrm{GF}(q^n)$ over $\mathrm{GF}(q)$

The existence of a normal basis is guaranteed by the following theorem whose proof can be found in p. 60 of Lidl and Niederreiter.

Theorem 9 (Normal Basis Theorem)

For any finite field $\mathbb{K}$ and any finite extension $\mathbb{F}$ of $\mathbb{K}$, there exists a normal basis of $\mathbb{F}$ over $\mathbb{K}$.

Remark

Normal bases are sometimes more convenient to use than polynomial bases.

Trace Function $\mathrm{Tr}_{\mathbb{F}/\mathbb{K}}(x)$

Definition 10

For $a \in \mathbb{F} = \mathrm{GF}(q^n)$ and $\mathbb{K} = \mathrm{GF}(q)$, the trace $\mathrm{Tr}_{\mathbb{F}/\mathbb{K}}(a)$ of a over $\mathbb{K}$ is defined by

$$\mathrm{Tr}_{\mathbb{F}/\mathbb{K}}(a) = a + a^q + \cdots + a^{q^{n-1}}.$$

If $\mathbb{K}$ is the prime subfield of $\mathbb{F}$, then $\mathrm{Tr}_{\mathbb{F}/\mathbb{K}}(a)$ is called the absolute trace of a and simply denoted by $\mathrm{Tr}_{\mathbb{F}}(a)$.

Remarks

The trace function $\mathrm{Tr}_{\mathbb{F}/\mathbb{K}}(x)$ from $\mathbb{F}$ to $\mathbb{K}$ is a **linear** function, and has many applications in engineering areas.

Trace Function $\mathrm{Tr}_{\mathbb{F}/\mathbb{K}}(x)$

The following theorem describes important properties of the trace function $\mathrm{Tr}_{\mathbb{F}/\mathbb{K}}(x)$ from $\mathbb{F}$ to $\mathbb{K}$.

Theorem 11

Let $\mathbb{F} = \mathrm{GF}(q^n)$ and $\mathbb{K} = \mathrm{GF}(q)$. Then the trace function $\mathrm{Tr}_{\mathbb{F}/\mathbb{K}}(x)$ from $\mathbb{F}$ to $\mathbb{K}$ has the following properties:

1. $\mathrm{Tr}_{\mathbb{F}/\mathbb{K}}(a+b) = \mathrm{Tr}_{\mathbb{F}/\mathbb{K}}(a) + \mathrm{Tr}_{\mathbb{F}/\mathbb{K}}(b)$ *for all* $a, b \in \mathbb{F}$.
2. $\mathrm{Tr}_{\mathbb{F}/\mathbb{K}}(ca) = c\mathrm{Tr}_{\mathbb{F}/\mathbb{K}}(a)$ *for all* $a \in \mathbb{F}$ *and* $c \in \mathbb{K}$.
3. $\mathrm{Tr}_{\mathbb{F}/\mathbb{K}}(c) = m\mathrm{Tr}_{\mathbb{F}/\mathbb{K}}(c)$ *for all* $c \in \mathbb{K}$.
4. $\mathrm{Tr}_{\mathbb{F}/\mathbb{K}}(a^q) = \mathrm{Tr}_{\mathbb{F}/\mathbb{K}}(a)$.

Proof.

The proof of these conclusions is trivial and left as an exercise. □

Trace Function $\mathrm{Tr}_{\mathbb{F}/\mathbb{K}}(x)$

Another important property of the trace function is its transitivity, which is depicted in the following.

Theorem 12

Let $\mathbb{K}$ be a finite field, let $\mathbb{F}$ be a finite extension of $\mathbb{K}$, and $\mathbb{E}$ a finite extension of $\mathbb{F}$. Then

$$\mathrm{Tr}_{\mathbb{E}/\mathbb{K}}(a) = \mathrm{Tr}_{\mathbb{F}/\mathbb{K}}(\mathrm{Tr}_{\mathbb{E}/\mathbb{F}}(a))$$

for all $a \in \mathbb{E}$.

Trace Function $\mathrm{Tr}_{\mathbb{F}/\mathbb{K}}(x)$

Proof of Theorem 12.

Let $\mathbb{K} = \mathrm{GF}(q)$, let $[\mathbb{F} : \mathbb{K}] = \ell$ and $[\mathbb{E} : \mathbb{F}] = n$. Then $[\mathbb{E} : \mathbb{K}] = n\ell$ and

$$|\mathbb{F}| = q^{\ell}, \ |\mathbb{E}| = q^{\ell n}.$$

Then for any $a \in \mathbb{E}$ we have

$$\begin{aligned}
\mathrm{Tr}_{\mathbb{F}/\mathbb{K}}(\mathrm{Tr}_{\mathbb{E}/\mathbb{F}}(a)) &= \sum_{i=0}^{\ell-1} \mathrm{Tr}_{\mathbb{E}/\mathbb{F}}(a)^{q^i} = \sum_{i=0}^{\ell-1} \left(\sum_{j=0}^{n-1} a^{q^{\ell j}} \right)^{q^i} \\
&= \sum_{i=0}^{\ell-1} \sum_{j=0}^{n-1} a^{q^{\ell j+i}} = \sum_{k=0}^{n\ell-1} a^{q^k} \\
&= \mathrm{Tr}_{\mathbb{E}/\mathbb{K}}(a).
\end{aligned}$$

$\square$

Norm Function $\mathrm{N}_{\mathbb{F}/\mathbb{K}}(x)$

Another interesting function from $\mathbb{F}$ to its subfield $\mathbb{K}$ is the norm function defined below.

Definition 13

For $a \in \mathbb{F} = \mathrm{GF}(q^n)$ and $\mathbb{K} = \mathrm{GF}(q)$, the norm $\mathrm{N}_{\mathbb{F}/\mathbb{K}}(a)$ of a over $\mathbb{K}$ is defined by

$$\mathrm{N}_{\mathbb{F}/\mathbb{K}}(a) = a \cdot a^q \cdots \cdot a^{q^{n-1}} = a^{\frac{q^n-1}{q-1}}.$$

Remark

Note that $\mathrm{N}_{\mathbb{F}/\mathbb{K}}(a)^q = \mathrm{N}_{\mathbb{F}/\mathbb{K}}(a)$ for all $a \in \mathbb{F}$. we have $\mathrm{N}_{\mathbb{F}/\mathbb{K}}(a) \in \mathbb{K}$ for all $a \in \mathbb{F}$.

Norm Function $\mathrm{N}_{\mathbb{F}/\mathbb{K}}(x)$

The following theorem describes basic properties of the norm function whose proofs are straightforward and left as exercises.

Theorem 14

Let $\mathbb{K} = \mathrm{GF}(q)$ and $\mathbb{F} = \mathrm{GF}(q^n)$. Then the norm function $\mathrm{N}_{\mathbb{F}/\mathbb{K}}(x)$ has the following properties:

1. $\mathrm{N}_{\mathbb{F}/\mathbb{K}}(ab) = \mathrm{N}_{\mathbb{F}/\mathbb{K}}(a)\mathrm{N}_{\mathbb{F}/\mathbb{K}}(b)$ *for all* $a, b \in \mathbb{F}$.
2. $\mathrm{N}_{\mathbb{F}/\mathbb{K}}$ *maps* $\mathbb{F}$ *onto* $\mathbb{K}$ *and* $\mathbb{F}^*$ *onto* $\mathbb{K}^*$.
3. $\mathrm{N}_{\mathbb{F}/\mathbb{K}}(a) = a^n$ *for all* $a \in \mathbb{K}$.
4. $\mathrm{N}_{\mathbb{F}/\mathbb{K}}(a^q) = \mathrm{N}_{\mathbb{F}/\mathbb{K}}(a)$ *for all* $a \in \mathbb{F}$.

Norm Function $\mathrm{N}_{\mathbb{F}/\mathbb{K}}(x)$

The norm function has also the following transitivity.

Theorem 15

Let $\mathbb{K}$ be a finite field, let $\mathbb{F}$ be a finite extension of $\mathbb{K}$, and $\mathbb{E}$ a finite extension of $\mathbb{F}$. Then

$$\mathrm{N}_{\mathbb{E}/\mathbb{K}}(a) = \mathrm{N}_{\mathbb{F}/\mathbb{K}}(\mathrm{N}_{\mathbb{E}/\mathbb{F}}(a))$$

for all $a \in \mathbb{E}$.

Proof.

It is straightforward and left as an exercise. □

Applications of Finite Fields

Finite fields have a lot of applications in science and engineering. Below is a list of some applications.

- Mathematics (finite geometry, combinatorial designs, algebraic geometry, number theory).
- Computer science (cryptography and coding theory, computer algorithms, data storage systems, simulation, software testing).
- Electrical engineering (CDMA communications, error detection and correction, signal processing, signal designs).