A very brief introduction to finite fields

Olivia Di Matteo

December 10, 2015

1 What are they and how do I make one?

Definition 1 (Finite fields)**.** Let p be a prime number, and $n \geq 1$ an integer. A *finite field* of order p^n, denoted by $\mathbb{F}_{p^n}$ or $\mathrm{GF}(p^n)$, is a collection of p^n objects and two binary operations, addition and multiplication, such that the following properties hold:

1. The elements are closed under addition modulo p,
2. The elements are closed under multiplication modulo p,
3. For all non-zero elements, there exists a multiplicative inverse.

1.1 Prime dimensions

Nothing much to see here. In prime dimension p, the finite field $\mathbb{F}_p$ is very simple:

$$\mathbb{F}_p = \mathbb{Z}_p = \{0, 1, \ldots, p-1\}. \tag{1}$$

1.2 Power of prime dimensions and field extensions

Fields of prime-power dimension are constructed by extending a field of smaller order using a primitive polynomial. See section 2.1.2 in [1].

1.2.1 Primitive polynomials

Definition 2. Consider a polynomial

$$q(x) = a_0 + a_1 x + \cdots + a_n x^n, \tag{2}$$

having degree n and coefficients $a_i \in \mathbb{F}_q$. Such a polynomial is called *monic* if $a_n = 1$.

Definition 3. A polynomial

$$q(x) = a_0 + a_1 x + \cdots + a_n x^n, \qquad a_i \in \mathbb{F}_q \tag{3}$$

is called *irreducible* if $q(x)$ has positive degree, and

$$q(x) = u(x)v(x), \tag{4}$$

and either $u(x)$ or $v(x)$ a constant polynomial. In other words, the equation

$$q(x) = a_0 + a_1 x + \cdots + a_n x^n = 0 \tag{5}$$

has no solutions in the field $\mathbb{F}_q$.

Example 1 (Irreducible polynomial)**.** Consider the field $\mathbb{F}_2$ and the polynomial

$$q(x) = x^2 + x + 1. \tag{6}$$

One can easily check that neither element of $\mathbb{F}_2$ will satisfy the equation $q(x) = 0$, and thus the polynomial is irreducible.

To construct a finite field, it is not sufficient that a polynomial is merely irreducible. The polynomial must also be *primitive*, in the sense that all roots of the polynomial are *primitive elements* of the field.

Definition 4. A *primitive element* of $\mathbb{F}_q$ is an element which multiplicatively generates the entire field $\mathbb{F}_q \backslash \{0\} = \mathbb{F}_q^*$.

Definition 5. A *primitive polynomial* is a monic polynomial whose roots are all primitive elements of a field.

I usually find the primitive polynomials I need by looking them up in tables online [2, 3].

1.2.2 Extending a prime field

To construct a field $\mathbb{F}_{p^n}$, we *extend* the prime field $\mathbb{F}_p$ using a primitive polynomial of degree n. Take the irreducible polynomial, and let σ denote a solution. As the polynomial is primitive, this σ is a *primitive element* of the field, and thus generates the entire field:

$$\mathbb{F}_{p^n} = \{0, \sigma, \sigma^2, \ldots, \sigma^{p^n - 1}\}, \tag{7}$$

where successive powers of σ can be expanded using relations derived from the polynomial. It is a general property that a field extension will contain a copy of its base field, namely $\mathbb{F}_p \subseteq \mathbb{F}_{p^n}$.

Example 2 ($\mathbb{F}_4$)**.** The degree 2 polynomial $q(x) = x^2 + x + 1$ used in the above example is primitive, so let us construct the field $\mathbb{F}_{2^2} = \mathbb{F}_4$. We call σ the primitive element, and let

$$\mathbb{F}_4 = \{0, \sigma, \sigma^2, \sigma^3\}. \tag{8}$$

As we claimed σ is the solution to $x^2 + x + 1 = 0$, we can rearrange this to obtain

$$\begin{aligned} \sigma^2 &= -\sigma - 1 (\text{mod } 2) && (9) \\ &= \sigma + 1 && (10) \end{aligned}$$

Similary we can compute $\sigma^3 = 1$. Thus,

$$\mathbb{F}_4 = \{0, \sigma, \sigma + 1, 1\}. \tag{11}$$

Observe that as expected, $\mathbb{F}_2$ is contained within $\mathbb{F}_4$. In addition to this, all elements of $\mathbb{F}_4$ are linear combinations of 1 and σ with coefficients in $\mathbb{F}_2$.

1.2.3 Extending a non-prime field

It is possible to extend a non-prime field in a similar way using a primitive polynomial with coefficients over the base field.

Example 3 ($\mathbb{F}_{16}/\mathbb{F}_4$)**.** It is easier to grasp this kind of field extension by using an example. As $16 = 2^4 = 4^2$, we can consider $\mathbb{F}_{16}$ as not only a degree 4 extension of $\mathbb{F}_2$ (denoted $\mathbb{F}_{16}/\mathbb{F}_2$), but also a degree 2 extension of $\mathbb{F}_4$ ($\mathbb{F}_{16}/\mathbb{F}_4$). Let σ be the primitive element of $\mathbb{F}_4$. A primitive polynomial of degree 2 with coefficients in $\mathbb{F}_4$ is

$$q(x) = x^2 + x + \sigma. \tag{12}$$

Denote the primitive element of $\mathbb{F}_{16}$ as ξ. Once again using the irreducible polynomial to expand higher powers of ξ, we find that

$$\mathbb{F}_{16}/\mathbb{F}_4 = \{0, \xi, \xi^2, \ldots, \xi^{15}\} \tag{13}$$

$$= \{ \begin{array}{cccc} 0, & \xi, & \xi+\sigma, & (\sigma+1)\xi+\sigma, \\ \xi+1, & \sigma, & \sigma\xi, & \sigma\xi+(\sigma+1), \\ \xi+(\sigma+1), & \sigma\xi+\sigma, & \sigma+1, & (\sigma+1)\xi, \\ (\sigma+1)\xi+1, & \sigma\xi+1, & (\sigma+1)\xi+(\sigma+1), & 1 \end{array} \}. \tag{14}$$

As expected we can see a copy of $\mathbb{F}_4$ contained in $\mathbb{F}_{16}$, and all the elements are linear combinations of 1 and ξ, with coefficients in $\mathbb{F}_4$.

2 What are some interesting properties and operations?

2.1 Miscellaneous properties

- Finite fields in every dimension are unique (up to an isomorphism).
- The highest power of the primitive element will always be 1, leading us to an easy formula for computing multiplicative inverses: for any field element α, $\alpha^{-1} = \alpha^{p^n-2}$.
- The non-zero elements of a prime-power field form a cyclic group under multiplication.
- The sum of all elements of a finite field is 0, except for $\mathbb{F}_2$.
- If there exists a positive integer n such that $n\alpha = 0$ for all $\alpha \in \mathbb{F}_{p^n}$, then the smallest such n is the *characteristic* of the field. A finite field has prime characteristic.

2.2 Some functions on field elements

Definition 6 (Conjugates)**.** Let $\mathbb{F}_q$, and $\mathbb{F}_{q^n}$ be an extension field of F. The *conjugates* of a field element α over $\mathbb{F}_q$ are the set $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{n-1}}$.

Definition 7 (Trace)**.** Let $G = \mathbb{F}_q$, and $F = \mathbb{F}_{q^n}$ be an extension field of F, with q not necessarily prime. The *trace* of a field element $\alpha \in \mathbb{F}_{q^n}$ is the linear map

$$\mathrm{tr}_{F/G}(\alpha) = \alpha + \alpha^q + \alpha^{q^2} + \cdots + \alpha^{q^{n-1}}. \tag{15}$$

In other words, the trace of a field element is the sum of its conjugates. The trace is strictly defined with respect to the subfield on which the field extension is built. In the case where we have a subset of F, say, $H = \mathbb{F}_p$, where $p^m = q$ such that $H \subseteq G \subseteq F$, then the trace of $\alpha \in \mathbb{F}_{q^n}$ over $\mathbb{F}_p$ is given by

$$\mathrm{tr}_{F/H} = \mathrm{tr}_{G/H}(\mathrm{tr}_{F/G}(\alpha)). \tag{16}$$

Definition 8 (Norm)**.** Let $G = \mathbb{F}_q$, and $F = \mathbb{F}_{q^n}$ be an extension field of F, with q not necessarily prime. The *norm* of a field element $\alpha \in \mathbb{F}_{q^n}$ is the product of its conjugates,

$$\mathrm{norm}_{F/G}(\alpha) = \alpha\alpha^q\alpha^{q^2}\cdots\alpha^{q^{n-1}}. \tag{17}$$

The trace and the norm of a field element are a little more intuitive to think about when considering the matrix representation of the field (see Section 2.4). The trace of an element is the matrix trace of its matrix representation, and the norm is the determinant.

2.3 Field bases

In the previous examples, we noted that all field elements were a linear combination of 1 and the primitive element. This is an example of a *basis* for the field, specifically the *polynomial basis*. In general, a degree n field extension $\mathbb{F}_{q^n}$ will have n basis elements $\{\theta_1, \ldots \theta_n\}$, orthogonal with respect to the trace, such that each field element α can be written as

$$\alpha = \sum_{i=1}^{n} a_i\theta_i, \tag{18}$$

for coefficients $a_i = \mathrm{tr}(\alpha\theta_i) \in \mathbb{F}_q$.

Definition 9 (Polynomial basis)**.** Let σ be the primitive element of a field $\mathbb{F}_{q^n}$. The set

$$\{1, \sigma, \sigma^2, \ldots, \sigma^{n-1}\} \tag{19}$$

is the *polynomial basis* of $\mathbb{F}_{q^n}$.

Examining a field in terms of its basis elements allows us to make a correspondence between finite fields and vector spaces.

Example 4 (Basis of $\mathbb{F}_4$)**.** Consider the version of $\mathbb{F}_4$ we computed in Example 2. Let us write each field element as vectors in the polynomial basis $\{\sigma^3 = 1, \sigma\}$:

$$\vec{s}_0 = \begin{pmatrix} 0 \\ 0 \end{pmatrix}, \quad \vec{s}_\sigma = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \quad \vec{s}_{\sigma^2} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \quad \vec{s}_{\sigma^3} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}. \tag{20}$$

We see immediately that this forms a 2-dimensional vector space, and we can add the field elements as we do vectors. In general, an extension field with dimension q^n forms an n-dimensional vector space.

2.3.1 Normal bases

Definition 10 (Normal basis)**.** Consider some $\alpha \in \mathbb{F}_{q^n}$. If the set of conjugates of α, $\{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\}$ is a basis for $\mathbb{F}_{q^n}$, this basis is termed a *normal* basis, and α is termed a *normal element*.

Example 5. In $\mathbb{F}_4$, the set of conjugates of σ, $\{\sigma, \sigma^2\}$ form a normal basis.

2.3.2 Dual and self-dual bases

Definition 11. Consider two basis of $\mathbb{F}_{q^n}/\mathbb{F}_q$, $\{\theta_i\}$ and $\{\nu_i\}$ for $i = 1, \ldots, n$. These two bases are *dual* if $\mathrm{tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\theta_i \nu_j) = \delta_{ij}$.

Definition 12. A basis is *self-dual* if it is dual to itself.

Example 6. In $\mathbb{F}_4$, one can check that $\{\sigma, \sigma^2\}$ is in fact a self-dual, normal basis.

2.4 Matrix representation

We previously mentioned that the non-zero elements of an extension field are a cyclic group; one can thus compute a representation of this group as linear matrices. This is done using something called the *companion matrix* of the primitive polynomial.

Definition 13. Let

$$q(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} + x^n. \tag{21}$$

The *companion matrix* of $q(x)$ is

$$C_{q(x)} = \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & 0 & \vdots & -a_2 \\ \vdots & 0 & \ddots & 0 & \vdots \\ 0 & 0 & \cdots & 1 & -a_{n-1} \end{pmatrix}, \tag{22}$$

where operations on the coefficients are considered modulo p.

A representation ρ of the field is

$$\rho(\mathbb{F}_{p^n}) = \{0, C_{q(x)}, C_{q(x)}^2, \ldots, C_{q(x)}^{n-1} = \mathbb{1}\} \tag{23}$$

Example 7. Let us consider $\mathbb{F}_8$, constructed using the primitive polynomial

$$q(x) = x^3 + x + 1. \tag{24}$$

We compute

$$C_{q(x)} = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}. \tag{25}$$

Then, the representation ρ of $\mathbb{F}_8$ is given as

$$\begin{aligned} \rho(0) &= \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} & \rho(\sigma) &= \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} & \rho(\sigma^2) &= \begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix} & \rho(\sigma^3) &= \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix} \\ \rho(\sigma^4) &= \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix} & \rho(\sigma^5) &= \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{pmatrix} & \rho(\sigma^6) &= \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} & \rho(\sigma^7) &= \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \end{aligned} \tag{26}$$

One interesting question that came up in discussion, and that I have not been able to find an answer to yet, is whether or not the matrix representation of each field is an irreducible representation.

3 Where can I use them?

Finite fields find application in many different areas; here we show two examples, the construction of Latin squares, and of mutually unbiased bases.

3.1 Latin squares

Definition 14 (Permutation polynomial)**.** A polynomial over $\mathbb{F}_{q^n}$ is called a *permutation polynomial* if it induces a permutation on the elements of $\mathbb{F}_{q^n}$.

There are a number of known classes of permutation polynomials over finite fields, categorized in chapter 8 of [1]. Permutation polynomials over finite fields are useful, as they allow us to construct Latin squares.

Definition 15 (Latin square)**.** A *Latin square* of order d is a $d \times d$ array of d unique symbols, such that every row and column contains each symbol exactly once. Every Latin square is associated to a permutation polynomial.

Example 8 (Latin square of order 4)**.** Consider the polynomial on field elements $\beta = \sigma\alpha$. This permutes the field elements as follows:

$$0 \leftrightarrow 0, \quad \sigma \to \sigma^2 \to \sigma^3 \to \sigma. \tag{27}$$

We can create a 4×4 Latin square as follows, displayed in Figure 1. To create a Latin square, begin with a grid, and label the two axes, one with the field in standard ordering, and the other the result of the permutation polynomial acting on the field elements in this ordering. Then in each square, sum up the values on the corresponding axis.

	0	σ	σ^2	σ^3
0				
σ^2				
σ^3				
σ				

	0	σ	σ^2	σ^3
0	0	σ	σ^2	σ^3
σ^2	σ^2	σ^3	0	σ
σ^3	σ^3	σ^2	σ	0
σ	σ	0	σ^3	σ^2

Figure 1: Latin square produced in dimension 4 using the permutation polynomial $\beta = \sigma\alpha$.

One can see that only polynomials which are permutation polynomials can produce Latin squares. Permutation polynomials are 1-1, meaning that each value on the axis will be unique; consequently, each sum of two field elements is unique neglecting ordering, so across a single row or column, all values will be unique.

3.2 Mutually unbiased bases

The Wootters construction of MUBs is built entirely on finite fields. The bases are constructed element by element using equations over the field element (see [7]). A second construction exists, based on sets of commuting operators. Some of the same permutation polynomials which produce

Latin squares can be used to construct sets of mutually unbiased bases in this way (see [5, 6] for more details). We present here the general idea.

Let $\mathcal{Z}$ and $\mathcal{X}$ represent the generalized Pauli Z and X operators in dimension p, and consider a generalized Pauli operation in dimension p^n. All possible operators can be written using a pair of field elements α, β like so:

$$Z_\alpha X_\beta = \mathcal{Z}^{a_1}\mathcal{X}^{b_1} \otimes \cdots \otimes \mathcal{Z}^{a_n}\mathcal{X}^{b_n} \tag{28}$$

where the a_i and b_i represent the expansion coefficients of α and β in a self-dual basis $\{\theta_1, \ldots, \theta_n\}$:

$$\alpha = \sum_{i=1}^{n} a_i\theta_i, \qquad \beta = \sum_{i=1}^{n} b_i\theta_i. \tag{29}$$

Consider the set of permutation polynomials of the form $\beta = \lambda\alpha$, for $\lambda \in \mathbb{F}_{p^n}$. One can define sets of monomials $\{Z_\alpha X_{\lambda\alpha}\}$; these sets will be disjoint and all monomials within each set will commute, leading to a set of mutually unbiased bases (the curve $\alpha = 0$ must be added to the mix to create a complete set).

Example 9 (MUBs in dimension 4)**.** We choose the self-dual basis $\{\sigma, \sigma^2\}$. The generalized Pauli operators are the normal 2-dimensional Pauli operators, σ_z and σ_x. Using expansions of field elements in the self-dual basis and the 5 curves ($\beta = \lambda\alpha, \alpha = 0$) we can compute the sets of monomials (neglecting phases):

Curve	Monomials	Paulis
$\alpha = 0$	$X_\sigma, X_{\sigma^2}, X_{\sigma^3}$	$\sigma_x \otimes \mathbb{1}, \mathbb{1} \otimes \sigma_x, \sigma_x \otimes \sigma_x$
$\beta = 0$	$Z_\sigma, Z_{\sigma^2}, Z_{\sigma^3}$	$\sigma_z \otimes \mathbb{1}, \mathbb{1} \otimes \sigma_z, \sigma_z \otimes \sigma_z$
$\beta = \sigma\alpha$	$Z_\sigma X_{\sigma^2}, Z_{\sigma^2} X_{\sigma^3}, Z_{\sigma^3} X_\sigma$	$\sigma_z \otimes \sigma_x, \sigma_x \otimes \sigma_y, \sigma_y \otimes \sigma_z$
$\beta = \sigma^2\alpha$	$Z_\sigma X_{\sigma^3}, Z_{\sigma^2} X_\sigma, Z_{\sigma^3} X_{\sigma^2}$	$\sigma_y \otimes \sigma_x, \sigma_x \otimes \sigma_z, \sigma_z \otimes \sigma_y$
$\beta = \sigma^3\alpha = \alpha$	$Z_\sigma X_\sigma, Z_\sigma X_{\sigma^2}, Z_{\sigma^3} X_{\sigma^3}$	$\sigma_y \otimes \mathbb{1}, \mathbb{1} \otimes \sigma_y, \sigma_y \otimes \sigma_y$

Table 1: Table of disjoint, mutually commuting sets of operators creating using curves over the finite field $\mathbb{F}_4$. The mutual eigenvectors of each row of the table are pair-wise unbiased with any other row; the collection of all eigenvectors forms a complete set of mutually-unbiased bases.

References

[1] G. L. Mullen and D. Panario, *Handbook of Finite Fields*, (CRC Press, 2013)

[2] http://theory.cs.uvic.ca/gen/poly.html

[3] http://fchabaud.free.fr/English/default.php?COUNT=1&FILE0=Poly

[4] A. B. Klimov, L. L. Sánchez-Soto and H. de Guise (2005) J. Phys. A: Math. Gen. **38** 2747

[5] A. B. Klimov, J. L. Romero, G. Björk, L. L. Sánchez-Soto (2009) Ann. Phys. **324** 53-72

[6] M. Gaeta, O. Di Matteo, A. B. Klimov, H. de Guise (2014) J. Phys. A: Math. Theor. **47** 435303

[7] W. K. Wootters and B. D. Fields (1989) Ann. Phys. **191** 363