1 Sequences and the One-Dimensional Fourier Transform

An *alphabet* is a set of symbols. Some alphabets are infinite, such as the set of real numbers or the set of complex numbers. Usually, we will be interested in finite alphabets. A *sequence* is a string of symbols from a given alphabet. A sequence may be of infinite length. An infinite sequence may be *periodic* or *aperiodic*; infinite aperiodic sequences may become periodic after some initial segment. Any infinite sequence that we will consider has a fixed beginning, but is unending. It is possible, however, that an infinite sequence has neither a beginning nor an end.

A *finite sequence* is a string of symbols of finite length from the given alphabet. The *blocklength* of the sequence, denoted n, is the number of symbols in the sequence. Sometimes the blocklength is not explicitly specified, but is known implicitly only by counting the number of symbols in the sequence after that specific sequence is given. In other situations, the blocklength n is explicitly specified, and only sequences of blocklength n are under consideration.

There are a great many aspects to the study of sequences. One may study the structure and repetition of various subpatterns within a given sequence of symbols. Such studies do not need to presuppose any algebraic or arithmetic structure on the alphabet of the sequence. This, however, is not the aspect of the study of sequences that we shall pursue. We are interested mainly in sequences – usually of finite blocklength – over alphabets that have a special arithmetic structure, the structure known as an *algebraic field*. In such a case, a sequence of a fixed finite blocklength will also be called a *vector*.

We can treat sequences over fields by using algebraic methods. We shall study such sequences by using the ideas of the linear recursion, the cyclic convolution, and the Fourier transform. We shall study here only the structure of individual sequences (and only those whose symbol alphabet is an algebraic field – usually a *finite field*), sets of sequences of finite blocklength n (called *codes*), and the componentwise difference of pairs of sequences (now called *codewords*) from a given code.

An important property of an individual vector over a field is its *Hamming weight* (or *weight*), which is defined as the number of components at which the vector is nonzero. An important property of a pair of vectors over a field is the *Hamming distance* (or *distance*) between them, which is defined as the number of coordinates in which the two vectors differ. We shall devote much effort to determining the weights of vectors and the distances between pairs of vectors.

1.1 Fields

Loosely, an algebraic field is any arithmetic system in which one can add, subtract, multiply, or divide such that the usual arithmetic properties of *associativity*, *commutativity*, and *distributivity* are satisfied. The fields familiar to most of us are: the *rational field*, which is denoted $\boldsymbol{Q}$ and consists of all numbers of the form a/b where a and b are integers, b not equal to zero; the *real field*, which is denoted $\boldsymbol{R}$ and consists of all finite or infinite decimals; and the *complex field*, which is denoted $\boldsymbol{C}$ and consists of all numbers of the form $a + \mathrm{i}b$ where a and b are real numbers. The rules of addition, subtraction, multiplication, and division are well known in each of these fields.

Some familiar arithmetic systems are not fields. The set of integers $\{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$, which is denoted $\boldsymbol{Z}$, is not a field under ordinary addition and multiplication. Likewise, the set of natural numbers $\{0, 1, 2, \ldots\}$, which is denoted $\boldsymbol{N}$, is not a field.

There are many other examples of fields, some with an infinite number of elements and some with a finite number of elements. Fields with a finite number of elements are called *finite fields* or *Galois fields*. The Galois field with q elements is denoted $GF(q)$, or F_q. The set of nonzero elements of a finite field is denoted $GF(q)^*$. "The" Galois field $GF(q)$ exists only if q equals a prime p or a prime power p^m, with m an integer larger than one. For other values of the integer q, no definition of addition and multiplication will satisfy the formal axioms of a field.

We may define the field F as a set that has two operations defined on pairs of elements of F; these operations are called "addition" and "multiplication," and the following properties must be satisfied.

(1) Addition axioms. The field F is closed under addition, and addition is associative and commutative,

$$a + (b + c) = (a + b) + c,$$
$$a + b = b + a.$$

There is a unique element called *zero*, denoted 0, such that $a + 0 = a$, and for every element a there is a unique element called the *negative* of a and denoted $-a$ such that $a + (-a) = 0$. *Subtraction* $a - b$ is defined as $a + (-b)$.

(2) Multiplication axioms. The field F is closed under multiplication, and multiplication is associative and commutative

$$a(bc) = (ab)c,$$
$$ab = ba.$$

There is a unique element not equal to zero called *one*, denoted 1, such that $1a = a$, and for every element a except zero, there is a unique element called the *inverse* of a and denoted a^{-1} such that $aa^{-1} = 1$. *Division* $a \div b$ (or a/b) is defined as ab^{-1}.

(3) Joint axiom. The *distributive law*

$$(a + b)c = ac + bc$$

holds for all elements a, b, and c in the field F.

The structure of the finite field $GF(q)$ is simple to describe if q is equal to a prime p. Then

$$GF(p) = \{0, 1, 2, \ldots, p - 1\},$$

and addition and multiplication are modulo-p addition and modulo-p multiplication. This is all the specification needed to determine $GF(p)$ completely; all of the field axioms can be verified to hold under this definition. Any other attempt to define a field with p elements may produce a structure that appears to be different, but is actually this same structure defined from a different point of view or with a different notation. Thus for every prime p, the finite field $GF(p)$ is unique but for notation. In this sense, only one field exists with p elements. A similar remark could be made for the field $GF(p^m)$ for any prime p and integer m larger than 1.

We can easily write down addition and multiplication tables for $GF(2)$, $GF(3)$, and $GF(5)$; see Table 1.1.

The field $GF(4)$ can *not* have this modulo-p structure because $2 \times 2 = 0$ modulo 4, and 2 does not have an inverse under multiplication modulo 4. We will construct $GF(4)$ in a different way as an *extension* of $GF(2)$. In general, any field that contains the field F is called an *extension field* of F. In such a discussion, F itself is sometimes called the *ground field*. A field of the form $GF(p^m)$ is formed as an extension of $GF(p)$ by means of a simple polynomial construction akin to the procedure used to construct the complex field from the real field. Eventually, we want to describe the general form of this construction, but first we shall construct the complex field $\boldsymbol{C}$ as an extension of the real field $\boldsymbol{R}$ in the manner of the general construction.

The extension field will consist of pairs of real numbers to which we attach a definition of addition and of multiplication. We will temporarily refer to this extension field using the notation $\boldsymbol{R}^{(2)} = \{(a, b) \mid a \in \boldsymbol{R}, b \in \boldsymbol{R}\}$. The extension field $\boldsymbol{R}^{(2)}$ must not be confused with the vector space $\boldsymbol{R}^2$. We also remark that there may be more than one way of defining addition and multiplication on $\boldsymbol{R}^{(2)}$. To define the arithmetic for the extension field $\boldsymbol{R}^{(2)}$, we represent the elements of the extension field by polynomials. We will use the symbol z to construct polynomials for such purposes, leaving the symbol

Table 1.1. *Arithmetic tables for some small fields*

GF(2)

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

GF(3)

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

·	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

GF(5)

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

·	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

x for other things. Thus redefine the extension field as follows:

$$\boldsymbol{R}^{(2)} = \{a + bz \mid a \in \boldsymbol{R}, b \in \boldsymbol{R}\},$$

where $a + bz$ is a new and useful name for (a, b). Next, find a polynomial of degree 2 over $\boldsymbol{R}$ that cannot be factored over $\boldsymbol{R}$. The polynomial

$$p(z) = z^2 + 1$$

cannot be factored over $\boldsymbol{R}$. Although there are many other polynomials of degree 2 that also cannot be factored over $\boldsymbol{R}$ (e.g., $z^2 + z + 1$), this $p(z)$ is the usual choice because of its extreme simplicity. Define the extension field as the set of polynomials with degrees smaller than the degree of $p(z)$ and with coefficients in $\boldsymbol{R}$. Addition and multiplication in $\boldsymbol{R}^{(2)}$ are defined as addition and multiplication of polynomials modulo[1] the polynomial $p(z)$. Thus

$$(a + bz) + (c + dz) = (a + c) + (b + d)z$$

and

$$\begin{aligned}(a + bz)(c + dz) &= ac + (ad + bc)z + bdz^2 \pmod{z^2 + 1} \\ &= (ac - bd) + (ad + bc)z.\end{aligned}$$

[1] The phrase "modulo $p(z)$," abbreviated (mod $p(z)$), means to take the remainder resulting from the usual polynomial division operation with $p(z)$ as the divisor.

This is exactly the form of the usual multiplication of complex numbers if the conventional symbol $\mathrm{i} = \sqrt{-1}$ is used in place of z because dividing by $z^2 + 1$ and keeping the remainder is equivalent to replacing z^2 by -1. The extension field that we have constructed is actually the complex field $\boldsymbol{C}$. Moreover, it can be shown that any other construction that forms such an extension field $\boldsymbol{R}^{(2)}$ also gives an alternative representation of the complex field $\boldsymbol{C}$, but for notation.

Similarly, to extend the field $GF(2)$ to the field $GF(4)$, choose the polynomial

$$p(z) = z^2 + z + 1.$$

This polynomial cannot be factored over $GF(2)$, as can be verified by noting that z and $z + 1$ are the only polynomials of degree 1 over $GF(2)$ and neither is a factor of $z^2 + z + 1$. Then

$$GF(4) = \{a + bz \mid a \in GF(2), b \in GF(2)\}.$$

The field $GF(4)$ has four elements. Addition and multiplication in $GF(4)$ are defined as addition and multiplication of polynomials modulo $p(z)$. Thus

$$(a + bz) + (c + dz) = (a + c) + (b + d)z$$

and

$$\begin{aligned}(a + bz)(c + dz) &= ac + (ad + bc)z + bdz^2 \pmod{z^2 + z + 1} \\ &= (ac + bd) + (ad + bc + bd)z\end{aligned}$$

(using the fact that "$-$" and "$+$" are the same operation in $GF(2)$). Denoting the four elements $0, 1, z$, and $z + 1$ of $GF(4)$ by 0, 1, 2, and 3, the addition and multiplication tables of $GF(4)$ now can be written as in Table 1.2.

The notation used here may cause confusion because, for example, with this notation $1 + 1 = 0$ and $2 + 3 = 1$ in this field. It is a commonly used notation, however, in engineering applications.

To extend any field F to a field $F^{(m)}$, first find any polynomial $p(z)$ of degree m over F that cannot be factored in F. Such a polynomial is called an *irreducible polynomial* over F. An irreducible polynomial $p(z)$ of degree m need not exist over the field F (e.g., there is no irreducible cubic polynomial over $\boldsymbol{R}$). Then $F^{(m)}$ does not exist. For a finite field $GF(q)$, however, an irreducible polynomial of degree m does exist for every positive integer m. If more than one such irreducible polynomial of degree m exists, then there may be more than one such extension field. Over finite fields, all such extension fields formed from irreducible polynomials of degree m are the same, except for notation. They are said to be *isomorphic* copies of the same field.

Table 1.2. *Arithmetic table for GF (4)*

	+	0	1	2	3	·	0	1	2	3
	0	0	1	2	3	0	0	0	0	0
GF(4)	1	1	0	3	2	1	0	1	2	3
	2	2	3	0	1	2	0	2	3	1
	3	3	2	1	0	3	0	3	1	2

Write the set of polynomials of degree smaller than m as

$$F^{(m)} = \{a_{m-1}z^{m-1} + a_{m-2}z^{m-2} + \cdots + a_1 z + a_0 \mid a_i \in F\}.$$

The symbol z can be thought of as a kind of place marker that is useful to facilitate the definition of multiplication. Addition in $F^{(m)}$ is defined as addition of polynomials. Multiplication in $F^{(m)}$ is defined as multiplication of polynomials modulo $p(z)$.

The construction makes it evident that if F is $GF(q)$, the finite field with q elements, then the extension field is also a finite field and has q^m elements. Thus it is the field $GF(q^m)$, which is unique up to notation. Every finite field $GF(q)$ can be constructed in this way as $GF(p^\ell)$ for some prime p and some positive integer ℓ. The prime p is called the *characteristic* of $GF(q)$.

For example, to construct $GF(16)$ as an extension of $GF(2)$, choose[2] $p(z) = z^4 + z + 1$. This polynomial is an irreducible polynomial over $GF(2)$, and it has an even more important property as follows. If $p(z)$ is used to construct $GF(16)$, then the polynomial z represents a field element that has order 15 under the multiplication operation. (The *order* of an element γ is the smallest positive integer n such that $\gamma^n = 1$.) Because the order of the polynomial z is equal to the number of nonzero elements of $GF(16)$, every nonzero element of $GF(16)$ must be a power of z.

Any polynomial $p(z)$ over the ground field $GF(q)$ for which the order of z modulo $p(z)$ is equal to $q^m - 1$ is called a *primitive polynomial* over $GF(q)$, and the element z is called a *primitive element* of the extension field $GF(q^m)$. The reason for using a primitive polynomial to construct $GF(q)$ can be seen by writing the fifteen nonzero field elements of $GF(16)$, $\{1, z, z+1, z^2, z^2+1, z^2+z, z^2+z+1, z^3, z^3+1, z^3+z, z^3+z+1, z^3+z^2, z^3+z^2+1, z^3+z^2+z, z^3+z^2+z+1\}$, as powers of the field element z. In this role, a primitive element z *generates* the field because all fifteen nonzero field elements are powers of z. When we wish to emphasize its role as a primitive element, we shall denote z by α. We may regard α as the abstract field element, and z as the polynomial representation of α. In $GF(16)$, the nonzero field elements are expressed as powers of α (or of z) as follows:

$$\alpha^1 = z,$$
$$\alpha^2 = z^2,$$

[2] The use of p both for a prime and to designate a polynomial should not cause confusion.

$$
\begin{aligned}
\alpha^3 &= z^3, \\
\alpha^4 &= z+1, && \text{(because } z^4 = z+1 \text{ (mod } z^4+z+1)\text{)}, \\
\alpha^5 &= z^2+z, \\
\alpha^6 &= z^3+z^2, \\
\alpha^7 &= z^3+z+1, \\
\alpha^8 &= z^2+1, \\
\alpha^9 &= z^3+z, \\
\alpha^{10} &= z^2+z+1, \\
\alpha^{11} &= z^3+z^2+z, \\
\alpha^{12} &= z^3+z^2+z+1, \\
\alpha^{13} &= z^3+z^2+1, \\
\alpha^{14} &= z^3+1, \\
\alpha^{15} &= 1 \;=\; \alpha^0.
\end{aligned}
$$

The field arithmetic of $GF(16)$ works as follows. To add the field elements z^3+z^2 and z^2+z+1, add them as polynomials with coefficients added modulo 2. (Writing only the coefficients, this can be expressed as $1100+0111=1011$.) To multiply 1100 by 0111 (here 1100 and 0111 are abbreviations for the field elements denoted previously as z^3+z^2 and z^2+z+1), write

$$
\begin{aligned}
(1100)(0111) = (z^3+z^2)(z^2+z+1) &= \alpha^6 \cdot \alpha^{10} = \alpha^{16} = \alpha \cdot \alpha^{15} \\
&= \alpha \cdot 1 = \alpha = z \\
&= (0010).
\end{aligned}
$$

To divide 1100 by 0111, write

$$
\begin{aligned}
(1100)/(0111) = (z^3+z^2)/(z^2+z+1) &= \alpha^6/\alpha^{10} = \alpha^6\alpha^5 \\
&= \alpha^{11} = z^3+z^2+z \\
&= (1110)
\end{aligned}
$$

(using the fact that $1/\alpha^{10} = \alpha^5$ because $\alpha^5 \cdot \alpha^{10} = 1$).

The field $GF(256)$ is constructed in the same way, now using the irreducible polynomial

$$p(z) = z^8+z^4+z^3+z^2+1$$

(which, in fact, is a primitive polynomial) or any other irreducible polynomial over $GF(2)$ of degree 8.

In any field, most of the methods of elementary algebra, including matrix algebra and the theory of vector spaces, are valid. In particular, the Fourier transform of blocklength n is defined in any field F, providing that F contains an element of order n. The finite field $GF(q)$ contains an element of order n for every n that divides $q-1$, because $GF(q)$ always has a primitive element α, which has order $q-1$. Every nonzero element of the field is a power of α, so there is always a power of α that has order n if n divides $q-1$. If n does not divide $q-1$, there is no element of order n.

One reason for using a finite field (rather than the real field) in an engineering problem is to eliminate problems of round-off error and overflow from computations. However, the arithmetic of a finite field is not well matched to everyday computations. This is why finite fields are most frequently found in those engineering applications in which the computations are introduced artificially as a way of manipulating bits for some purpose such as error control or cryptography.

1.2 The Fourier transform

The (*discrete*) *Fourier transform*, when defined in the complex field, is a fundamental tool in the subject of signal processing; its rich set of properties is part of the engineer's workaday intuition. The Fourier transform exists in any field. Since most of the properties of the Fourier transform follow from the abstract properties of a field, but not from the specific structure of a particular field, most of the familiar properties of the Fourier transform hold in any field.

The Fourier transform is defined on the vector space of n-tuples, denoted F^n. A *vector* $\boldsymbol{v}$ in the *vector space* F^n consists of a block of n elements of the field F, written as

$$\boldsymbol{v} = [v_0, v_1, \ldots, v_{n-1}].$$

The vector $\boldsymbol{v}$ is multiplied by the element γ of the field F by multiplying each component of $\boldsymbol{v}$ by γ. Thus

$$\gamma \boldsymbol{v} = [\gamma v_0, \gamma v_1, \ldots, \gamma v_{n-1}].$$

Here the field element γ is called a *scalar*. Two vectors $\boldsymbol{v}$ and $\boldsymbol{u}$ are added by adding components

$$\boldsymbol{v} + \boldsymbol{u} = [v_0 + u_0, v_1 + u_1, \ldots, v_{n-1} + u_{n-1}].$$

Definition 1.2.1 *Let $\boldsymbol{v}$ be a vector of blocklength n over the field F. Let ω be an element of F of order n. The Fourier transform of $\boldsymbol{v}$ is another vector $\boldsymbol{V}$ of blocklength*

n over the field F whose components are given by

$$V_j = \sum_{i=0}^{n-1} \omega^{ij} v_i \qquad j = 0, \ldots, n-1.$$

The vector $\boldsymbol{V}$ is also called the *spectrum* of $\boldsymbol{v}$, and the components of $\boldsymbol{V}$ are called *spectral components*. The components of the Fourier transform of a vector will always be indexed by j, whereas the components of the original vector $\boldsymbol{v}$ will be indexed by i. Of course, $\boldsymbol{V}$ is itself a vector so this indexing convention presumes that it is clear which vector is the original vector and which is the spectrum. The Fourier transform relationship is sometimes denoted by $\boldsymbol{v} \leftrightarrow \boldsymbol{V}$.

The Fourier transform can also be understood as the evaluation of a polynomial. The *polynomial representation* of the vector $\boldsymbol{v} = [v_i \mid i = 0, \ldots, n-1]$ is the polynomial

$$v(x) = \sum_{i=0}^{n-1} v_i x^i.$$

The *evaluation* of the polynomial $v(x)$ at β is the field element $v(\beta)$, where

$$v(\beta) = \sum_{i=0}^{n-1} v_i \beta^i.$$

The Fourier transform, then, is the evaluation of the polynomial $v(x)$ on the n powers of ω, an element of order n. Thus component V_j equals $v(\omega^j)$ for $j = 0, \ldots, n-1$. If F is the finite field $GF(q)$ and ω is a primitive element, then the Fourier transform evaluates $v(x)$ at all $q-1$ nonzero elements of the field.

The Fourier transform has a number of useful properties, making it one of the strongest tools in our toolbox. Its many properties are summarized in Section 1, 3. We conclude this section with a lengthy list of examples of the Fourier transform.

(1) $\boldsymbol{Q}$ or $\boldsymbol{R}$: $\omega = +1$ has order 1, and $\omega = -1$ has order 2. For no other n is there an ω in $\boldsymbol{Q}$ or $\boldsymbol{R}$ of order n. Hence only trivial Fourier transforms exist in $\boldsymbol{Q}$ or $\boldsymbol{R}$. To obtain a Fourier transform over $\boldsymbol{R}$ of blocklength larger than 2, one must regard $\boldsymbol{R}$ as embedded into $\boldsymbol{C}$.

There is, however, a *multidimensional Fourier transform* over $\boldsymbol{Q}$ or $\boldsymbol{R}$ with 2^m elements. It uses $\omega = -1$ and a Fourier transform of length 2 on each dimension of a two by two by ... by two m-dimensional array, and it is a nontrivial example of a multidimensional Fourier transform in the fields $\boldsymbol{Q}$ and $\boldsymbol{R}$. (This transform is more commonly expressed in a form known as the (one-dimensional) *Walsh–Hadamard transform* by viewing any vector of length 2^m over $\boldsymbol{R}$ as an m-dimensional two by two by $\cdots$ by two array.)

(2) $\boldsymbol{C}$: $\omega = e^{-i2\pi/n}$ has order n, where $i = \sqrt{-1}$. A Fourier transform exists in $\boldsymbol{C}$ for any blocklength n. There are unconventional choices for ω that work also. For example, $\omega = (e^{-i2\pi/n})^3$ works if n is not a multiple of 3.

(3) $GF(5)$: $\omega = 2$ has order 4. Therefore

$$V_j = \sum_{i=0}^{3} 2^{ij} v_i \quad j = 0, \ldots, 3$$

is a Fourier transform of blocklength 4 in $GF(5)$.

(4) $GF(31)$: $\omega = 2$ has order 5. Therefore

$$V_j = \sum_{i=0}^{4} 2^{ij} v_i \quad j = 0, \ldots, 4$$

is a Fourier transform of blocklength 5 in $GF(31)$. Also $\omega = 3$ has order 30 in $GF(31)$. Therefore

$$V_j = \sum_{i=0}^{29} 3^{ij} v_i \quad j = 0, \ldots, 29$$

is a Fourier transform of blocklength 30 in $GF(31)$.

(5) $GF(2^{16} + 1)$. Because $2^{16} + 1$ is prime, an element ω of order n exists if n divides $2^{16} + 1 - 1$. Thus elements of order 2^ℓ exist for $\ell = 1, \ldots, 16$. Hence for each power of 2 up to 2^{16}, $GF(2^{16} + 1)$ contains a Fourier transform of blocklength n equal to that power of 2.

(6) $GF((2^{17} - 1)^2)$. This field is constructed as an extension of $GF(2^{17} - 1)$, using a polynomial of degree 2 that is irreducible over $GF(2^{17} - 1)$. An element ω of order n exists in the extension field if n divides $(2^{17} - 1)^2 - 1 = 2^{18}(2^{16} - 1)$. In particular, for each power of 2 up to 2^{18}, $GF((2^{17} - 1)^2)$ contains a Fourier transform of blocklength equal to that power of 2.

(7) $GF(16)$. If $GF(16)$ is constructed with the primitive polynomial $p(z) = z^4 + z + 1$, then z has order 15. Thus $\omega = z$ is an element of order 15, so we have the 15-point Fourier transform

$$V_j = \sum_{i=0}^{14} z^{ij} v_i \quad j = 0, \ldots, 14.$$

The components v_i (and V_j), as elements of $GF(16)$, can be represented as polynomials of degree at most 3 over $GF(2)$, with polynomial multiplication reduced by $z^4 = z + 1$.