Matrix Representation of Finite Fields

W. P. Wardlaw

Identification Systems Branch
Radar Division

March 12, 1992

Approved for public release; distribution unlimited
Matrix Representation of Finite Fields

W. P. Wardlaw

Naval Research Laboratory
4555 Overlook Avenue
Washington, DC 20375-5000

Naval Air Systems Command
Washington, DC 20361-1213

Approved for public release; distribution unlimited.

Finite fields (also called Galois Fields) have been studied since their introduction by Evariste Galois in 1832 and the publication of his work in 1846. In the last few decades, finite fields have become important to information theory, coding theory, and cryptography.

This report presents a simple method for representing a finite field in terms of powers of a single matrix over the integers modulo the characteristic of the field. The addition and multiplication in the field are immediately obtained as the results of ordinary matrix addition and multiplication. This representation called the canonical cyclic representation, makes it easy to understand the field structure and to carry out computations in the field.

**Subject Terms**
- Finite fields
- Matrix representation
- Canonical cyclic representation
- Cyclotomic polynomials

**Security Classification**
- Unclassified

**Number of Pages**
14

**Price Code**

---

13. ABSTRACT (Maximum 200 words)

Finite fields (also called Galois Fields) have been studied since their introduction by Evariste Galois in 1832 and the publication of his work in 1846. In the last few decades, finite fields have become important to information theory, coding theory, and cryptography.

This report presents a simple method for representing a finite field in terms of powers of a single matrix over the integers modulo the characteristic of the field. The addition and multiplication in the field are immediately obtained as the results of ordinary matrix addition and multiplication. This representation called the canonical cyclic representation, makes it easy to understand the field structure and to carry out computations in the field.
INTRODUCTION

Finite fields have many applications to coding theory, information theory, and cryptography. For this reason, it is important to have understandable and efficient methods of representing finite fields.

Most undergraduate texts in abstract algebra show how to represent a finite field \( \mathbb{F}_q \) over its prime field \( \mathbb{F}_p \) by clearly specifying its additive structure as a vector space or a quotient ring of polynomials over \( \mathbb{F}_p \) while leaving the multiplicative structure hard to determine, or they explicitly illustrate the cyclic structure of its multiplicative group without clearly connecting it to the additive structure. In this note we suggest a matrix representation which naturally and simply displays both the multiplicative and the additive structures of the field \( \mathbb{F}_q \) (with \( q = p^d \)) over its prime field \( \mathbb{F}_p \). Although this representation is known (See [3, p. 65], for example.), it does not appear to be widely used in abstract algebra texts.

REPRESENTATIONS OF FINITE FIELDS

To illustrate these ideas, let us first consider the field \( \mathbb{F}_8 \) of eight elements over its prime field \( \mathbb{F}_2 \). The additive structure of \( \mathbb{F}_8 \) is that of the three dimensional vector space \( V \).
= \{(0 0 0), (1 0 0), (0 1 0), (0 0 1), (1 1 0), (1 0 1), (0 1 1), (1 1 1)\} over \(\mathbb{F}_2\). However, it is not at all clear how to define products of these vectors to get the multiplicative structure of \(\mathbb{F}_8\). It can be shown that extending the multiplication table

\[
\begin{array}{ccc}
(1 0 0) & (0 1 0) & (0 0 1) \\
(1 0 0) & (1 0 0) & (0 1 0) & (0 0 1) \\
(0 1 0) & (0 1 0) & (0 0 1) & (1 1 0) \\
(0 0 1) & (0 0 1) & (1 1 0) & (0 1 1) \\
\end{array}
\]

for the basis \(\mathcal{B} = \{(1 0 0), (0 1 0), (0 0 1)\}\) of \(V\) by bilinearity gives the multiplicative structure of \(\mathbb{F}_8\), although a direct proof would be tedious.

A more usual, as well as more useful, treatment (See [1, p. 171] or [3, p. 25, Thm. 1.6.1].) is to represent

\[
(2) \quad \mathbb{F}_8 \cong \mathbb{F}_2[x]/(x^3 + x + 1)
\]

as the ring of all polynomials over \(\mathbb{F}_2\) modulo the third degree irreducible polynomial \(x^3 + x + 1\). If we let \(a \in \mathbb{F}_8\) denote the residue class of \(x\) modulo \(x^3 + x + 1\), we have \(a^3 + a + 1 = 0\). Then it is easy to see (Recall that the characteristic is 2!) that \(a^3 = a + 1\), \(a^4 = a^2 + a\), \(a^5 = a^2 + a + 1\), \(a^6 = a^2 + 1\), and \(a^7 = 1\), so

\[
\begin{align*}
\mathbb{F}_8 &= \{0, 1, a, a^2, a^3, a^4, a^5, a^6\} \\
(3) &= \{0, 1, a, a^2, a + 1, a^2 + a, \varepsilon^2 + a + 1, a^2 + 1\}.
\end{align*}
\]
Thus, the multiplicative group $F_8^* = \langle a \rangle$ of $F_8$ is simply the cyclic group of order 7 generated by $a$. The second formulation in (3) makes the additive structure easy to see, although it obscures the multiplicative structure a little. One can use the abbreviated multiplication table

\[
\begin{array}{ccc}
1 & a & a^2 \\
1 & 1 & a & a^2 \\
a & a & a^2 & a + 1 \\
a^2 & a^2 & a + 1 & a^2 + a \\
\end{array}
\]

(4)

along with the distributive law to multiply elements of $F_8$. (Comparing tables (1) and (4) is one fairly easy way to prove that the multiplication given by table (1) satisfies the field axioms.) Alternatively, one can use the relation $a^3 + a + 1 = 0$ to multiply the elements given in the second formulation in (3). This is the standard representation of a finite field, and it is reasonably satisfactory. However, the transition from addition to multiplication still leaves something to be desired.

**MATRIX REPRESENTATIONS**

If we pick any element $b$ of the field $F_8$, left multiplication by $b$ is a linear transformation $L_b$ on the vector space $V = F_8$ over $F_2$. If we choose any basis $B'$ of $V = F_8$ over $F_2$, we can find the matrix $[L_b] = [L_b]_{B'}$ of $L_b$ with respect to that basis. If we fix the basis $B'$ and find the matrix of each element of $F_8$ in this way, it is clear that the resulting set of matrices form a field isomorphic to $F_8$!
Thus, each choice of basis gives a different matrix representation of $F_8$. It appears at first glance that we must have a multiplication table for the field before we can get the matrix representation. But there is a way to get around this difficulty.

Let

$$A = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$$

be the companion matrix (See [1, p. 264], [2, pp. 229-230], or [5, p. 201, Definition 5.2.16].) of the irreducible third degree polynomial $f(x) = x^3 + x + 1$ over the field $F_2$. Then $f(A) = 0$, so the powers of $A$ satisfy the relations satisfied by $A$ above; in particular, the matrix $A$ generates the cyclic group $<A>$ of order 7 isomorphic to $F_8^*$, and the ring of matrices

$$F_2[A] = \{0, I, A, A^2, A^3, A^4, A^5, A^6\}$$

is isomorphic to the field $F_8$. That was easy, wasn't it?

Indeed, a bit too easy, as we shall see. Consider now the irreducible polynomial $g(x) = x^2 + 1$ over the three element field $F_3$. We see that its companion matrix $B$ has multiplicative order 4:

$$B = \begin{bmatrix} 0 & 2 \\ 1 & 0 \end{bmatrix}, \quad B^2 = \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}, \quad B^3 = \begin{bmatrix} 0 & 1 \\ 2 & 0 \end{bmatrix}, \quad B^4 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I.$$

Not enough elements for $F_9$! And the powers of $B$ are not closed under addition. Fortunately, there is a fairly simple
cure: Adjoin the matrices 0, I + B, I + B^3, B + B^2, and B^2 + B^3 to the set of powers of B to obtain the ring \( F_2[B] \) of matrices generated by B. Since \( g(B) = B^2 + I = 0 \), it is clear that the ring \( F_2[B] \) is isomorphic to the field \( F_9 \). Thus, B provides a matrix representation \( F_2[B] \) of the nine element field, and we say that B is a generator of the field \( F_9 \).

**CANONICAL CYCLIC REPRESENTATION**

But we would like to have a cyclic generator of \( F_9 \); that is, a matrix M such that the multiplicative group \( F_9^* \) of \( F_9 \) is isomorphic to the cyclic group \(<M>\) generated by M. This, too, is not terribly difficult. An eight element cyclic group has exactly \( \varphi(8) = 4 \) generators, none of which is a power of an element of order 4. Thus, the multiplicative group \( F_3[B]^* \cong F_9^* \) is cyclically generated by any of the four nonzero matrices in \( F_3[B] \) which are not powers of B. The reader can easily verify that the matrix \( M = I + B = \begin{bmatrix} 1 & 2 \\ 1 & 1 \end{bmatrix} \) is a cyclic generator of \( F_9 \).

Note that the set \( F_3[B] \) is spanned (over \( F_3 \)) by the matrices I and B, and also by I and M. That is, \( F_3[B] = L(I, B) = L(I, M) \). If B and M are the ordered bases \((I, B)\) and \((I, M)\), respectively, we see that

\[
L_B : \begin{align*}
I & \rightarrow B = 0 \cdot I + 1 \cdot B \\
B & \rightarrow B^2 = 2 \cdot I + 0 \cdot B
\end{align*}
so \( [L_B]_B = \begin{bmatrix} 0 & 2 \\ 1 & 0 \end{bmatrix} = B, \\
L_M : \begin{align*}
I & \rightarrow M = 1 \cdot I + 1 \cdot B \\
B & \rightarrow MB = 2 \cdot I + 1 \cdot B
\end{align*}
so \( [L_M]_B = \begin{bmatrix} 1 & 2 \\ 1 & 1 \end{bmatrix} = M, \\
and
\]
\[ L_M : \begin{align*} I &\mapsto M = 0 \cdot I + 1 \cdot M \\ M &\mapsto M^2 = 1 \cdot I + 2 \cdot M \end{align*} \text{ so } [L_M]M = \begin{bmatrix} 0 & 1 \\ 1 & 2 \end{bmatrix} = A. \]

Since \( A \) is similar to \( M \), it follows that \( A \) is another cyclic generator of \( \mathbb{F}_9 \). Moreover, \( A \) is the companion matrix of its characteristic polynomial \( f_A(x) = x^2 + x + 2 \). We call \( A \) a canonical cyclic generator of \( \mathbb{F}_9 \), and call the representation

\[ \mathbb{F}_9[A] = \{0, 1, A, A^2, A^3, A^4, A^5, A^6, A^7\} \]

a canonical cyclic representation of \( \mathbb{F}_9 \).

**THE GENERAL CASE**

Of course, all of these ideas generalize for arbitrary finite fields. (Indeed, they generalize to finite extensions of any field, but we restrict the treatment here to finite extensions of fields \( \mathbb{F}_p \) with \( p \) prime.) Let \( p \) be a prime number and let \( q = p^e \) be the \( e \)th power of \( p \). Then \( \mathbb{F}_q \) is a \( q \) element field containing \( \mathbb{F}_p = \mathbb{Z}_p = \mathbb{Z}/(p) \) (the integers modulo \( p \)) as its prime field. Let \( m(x) \) be any irreducible polynomial of degree \( e \) over \( \mathbb{F}_p \), and let \( B \) be the companion matrix of \( m(x) \). The ring \( \mathbb{F}_p[B] \) of sums of powers of \( B \) is isomorphic to the field \( \mathbb{F}_q \), and is thus a matrix representation of \( \mathbb{F}_q \). Locate a matrix \( M \) in \( \mathbb{F}_p[B] \) which has period (multiplicative order) \( q - 1 \). \( M \) is necessarily a cyclic generator of \( \mathbb{F}_q \). The companion matrix \( A \) of the minimum polynomial \( m_M(x) = m_A(x) \) is a canonical cyclic generator of

\[ \mathbb{F}_p[A] = \{0, 1, A, A^2, \ldots, A^{q-2}\} \cong \mathbb{F}_q. \]
Note that if $C$ is any $e \times e$ matrix over $\mathbb{F}_p$, then the ring $\mathbb{F}_p[C]$ generated by $C$ is isomorphic to $\mathbb{F}_q$ if and only if the sequence $C = (I, C, C^2, \ldots, C^{e-1})$ of powers of $C$ is independent if and only if the characteristic polynomial $f_C(x)$ of $C$ is irreducible. In this case, the matrix $[L_C]_C$ of left multiplication by $C$, with respect to the basis $C$, is the companion matrix of $f_C(x)$. $C$ is a cyclic generator of $\mathbb{F}_q$ if and only if $C$ is a primitive $(q - 1)^{st}$ root of unity in $\mathbb{F}_p[C]$.

**Cyclotomic Polynomials**

There is another, possibly easier, method of getting a canonical cyclic generator of $\mathbb{F}_q$. Recall that the $n^{th}$ cyclotomic polynomial $c_n(x)$ is defined to be the product

\[(5)\quad c_n(x) = \prod (x - a)\]

taken over all $\varphi(n)$ primitive $n^{th}$ roots $a$ of unity. Since every root of $x^n - 1 = 0$ is a primitive $d^{th}$ root of unity for some divisor $d$ of $n$, it follows from (5) that

\[(6)\quad x^n - 1 = \prod_{d|n} c_d(x).\]

One can use (6) to obtain the recursive formula

\[(7)\quad c_n(x) = (x^n - 1) / \prod_{d|n\&d|n} c_d(x).\]

It follows inductively from (7) that $c_n(x)$ is a monic
polynomial with integer coefficients of degree (from (5)) \( \varphi(n) \).
The cyclotomic polynomials are all irreducible over the rational
number field (See [3, p. 61, Thm. 2.4.7], [4, p. 162], or [5,
p. 289, Thm. 6.3.13],..), but they usually factor over finite
fields. It will be useful later to note that if \( n = r^d \) is a
power of a prime \( r \), then it follows inductively from (7) that

\[
\text{(8)} \quad c_n(x) = (x^n - 1)/(x^{n/r} - 1), \quad (n = r^d, r \text{ prime}).
\]

Every element of \( F_q \) (\( p \) prime and \( q = p^e \)) is a root of

\[
\text{(9)} \quad x^q - x = x(x^{q-1} - 1) = 0,
\]
since \( F_q \) is the splitting field of \( x^q - x \), and every nonzero
element is a \((q - 1)\)st root of unity. If \( m(x) \) is a monic
irreducible factor of \( c_{q-1}(x) \), and \( a \) is a root of \( m(x) \), then
\( a \) is a primitive \((q - 1)\)st root of unity. (Note that \( m(x) \) is
necessarily of degree \( e \).) It follows that if \( A \) is the \( e \times e \)
companion matrix of \( m(x) \), then \( A \) is a canonical cyclic
generator of \( F_q \).

Conversely, if \( A \) is a canonical cyclic generator of \( F_q \)
over \( F_p \), then its minimum polynomial \( m_A(x) \) is an irreducible
factor of the cyclotomic polynomial \( c_{q-1}(x) \) in \( F_p[x] \). This
observation can lead to a method of factoring cyclotomic polyno-
mials. This is a related but different topic which we will not
pursue here.

**EXAMPLES REVISITED**

Let us conclude with two examples that use the method of
factoring cyclotomic polynomials to obtain canonical cyclic representations of $F_8$ over $F_2$, and of $F_9$ over $F_3$. (We have treated these cases more naively above.)

For $F_8$ over $F_2$, $e = [F_8:F_2] = 3$, so the factors of $c_7(x)$ are cubic.

$$c_7(x) = \frac{(x^7 - 1)}{(x - 1)} = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 = (x^3 + x + 1)(x^3 + x^2 + 1).$$

(The factorization of $c_7(x)$ was particularly easy, since it factors are the only irreducible polynomials of degree three over $F_2$!) Since $x^3 + x + 1$ and $x^3 + x^2 + 1$ are irreducible factors of $c_7(x)$, it follows that their companion matrices

$$A = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} \quad \text{and} \quad B = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{bmatrix}$$

are canonical cyclic generators of $F_8$ over $F_2$.

For $F_9$ over $F_3$, we would like to factor

$$c_8(x) = \frac{(x^8 - 1)}{(x^4 - 1)} = x^4 + 1.$$

Since $e = [F_9:F_3] = 2$, the factors are quadratic. It is not hard to see that the monic irreducible quadratics over $F_3$ are $x^2 + 1$, $x^2 - x - 1$, and $x^2 + x - 1$. The desired factorization is

$$c_8(x) = x^4 + 1 = (x^2 + x - 1)(x^2 - x - 1),$$

so the canonical cyclic generators of $F_9$ over $F_3$ are the
corresponding companion matrices,

\[ A = \begin{bmatrix} 0 & 1 \\ 1 & 2 \end{bmatrix} \quad \text{and} \quad B = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}. \]

CONCLUSION

As mentioned in the introduction, finite fields have many applications to coding theory, information theory, and cryptography. The canonical cyclic matrix representation of finite fields described in this report gives an easily understandable and convenient computational method of dealing with finite fields that can simplify their use in these applications.

REFERENCES