Abstract

Finite Fields can be represented in various ways. Generally, they are most easily understood when represented as matrices. This representation poses serious computational issues when considering the multiplicative operation. Several methods have been devised to deal with the problem. Holger Schellwat presented a simpler slide rule, and William Wardlaw circumvented the problem of dealing with vectors by modeling finite fields using square matrices.

Finite fields are deceptively complex objects. Since any finite field can be viewed as a vector space over another (smaller) finite field and all have a characteristic which must be prime, all finite fields have order (size) $p^n$ where $p$ is a prime number and $n$ is a positive integer. Additionally, for any $p$ and $n$ as above, there is a finite field of order $p^n$ [4]. Although, it is somewhat easy to prove facts regarding finite fields, great difficulty arises in the actual representation and manipulation of these objects. Defining the multiplicative operation on these fields is extremely challenging. Here we describe a method for obtaining a new representation of finite fields that has the additional benefit of making the multiplicative operation somewhat transparent. Additional consequences include answering some classic questions regarding the length of Fibonacci-like cycles of a certain type. To see the various results on this topic, see (for example) Catlan [1], Vella and Vella [6], and Freyd and Brown [3]. Before getting started, it is important to note that we will be using the phrase “Fibonacci sequence” to describe sequences that are not, strictly speaking, the sequences that Fibonacci originally had in mind. In particular, we will be allowed to multiply terms of the sequence before adding them together. Technically, these are known as recursively defined additive sequences. Our convention will to be to refer to them as Fibonacci sequences.

Definition 1. Let $(G,+)$ be an abelian group. Define $\cdot$ as another binary operation on G. Then $(G,+,\cdot)$ is a ring if and only if $\cdot$ is associative and left and right distributive over $+$. 

Definition 2. If there is a two-sided $\cdot$ identity, we say that $(G,+,\cdot)$ is ring with unity.

Definition 3. A finite field is a field that contains a finite number of elements, is a commutative ring with unity, and has the additional property that if $a\cdot b=0$ then $a=0$ or $b=0$. 

---

This Project received funding as part of an ASU Faculty Mentored Grant.
Definition 4. Given a finite field $F$, we define $G(F)$ to be the group that is obtained by removing 0 from the set, and considering the remaining elements as a group with the operation $\cdot$.

In many texts $G(F)$ is referred to as the multiplicative group or Galois group.

Theorem 1. The multiplicative group $G(F)$ associated to a finite field $F$ is cyclic. This proof follows from an easily proven fact that any polynomial of degree $n$ has at most $n$ roots in the finite field $F$. For a more thorough explanation, see Herstein [4] or any reasonable text in abstract algebra.

Definition 5. A polynomial $f$ of degree $n$ is said to be primitive irreducible if its roots can be used to generate the entire multiplicative group for a finite field $F$.

The motivation for definition 2 comes from fact that the $G(F)$ is cyclic, so there is a generator for this group. It is reasonably easy to show that this generator may be obtained by first finding a primitive irreducible polynomial and then letting the object represent one of the roots. Here it is important to note that the other elements of $G(F)$ become extremely complicated, as they are constructed using the original polynomial and the element $a$. For example, one method of constructing fields of greater size is to fix a prime $p$ and consider the basic field $[p]$ which is the field of integers modulo the prime $p$. This field is easy to handle since multiplication and addition work in exactly the way expected modulo $p$. To then extend this to a field containing $p^n$ many elements, one need only find a primitive irreducible polynomial over $[p]$ and use a root for that polynomial to generate the entire field. The root will not be an element of $[p]$ but it will suffice to generate the entire field $F$ of order $p^n$. For example, suppose we wish to construct a finite field of order $8 = 2^3$. To find the seven elements which make up $G(F)$, we start with the polynomial $x^3+x+1$, which is primitive irreducible over the field of order 2. Let $a$ be a root for this polynomial, then $a^3+a+1=0$. Since this field has characteristic 2, it is reasonably easy to see that

$$a^3 = a+1,$$
$$a^4 = a\cdot a^3 = a\cdot(a+1) = a^2+a,$$
$$a^5 = a\cdot a^4 = a\cdot(a^2+a) = a^3+a^2 = a^2+a+1,$$
$$a^6 = a^3\cdot a^3 = (a+1)\cdot(a+1) = a^2+2a+1 = a^2+1$$ (recall, $2a = 0$),
$$a^7 = a\cdot a^6 = a\cdot(a^2+1) = a^3+a = a+1+a = 2a+1 = 1.$$

So this finite field can be represented by $\{0,1,a,a^2,a+1,a^2+a, a^2+a+1, a^2+1\}$.

Although this representation is adequate, it is cumbersome. The water becomes murkier when dealing with even greater sized finite fields.
A better approach is to use the work done by Wardlaw [7] to first represent a field \( F \) of order \( p^n \) using \( n \times n \) matrices with entries which come from the field of integers modulo \( p \). If the matrices have a particular form, then they may be used to generate a recursively defined sequence. Such a sequence may be immediately used to represent the finite field. In this case, both the multiplication and addition are obvious, but the objects are a bit ungainly. So the final distillation will come by extracting pieces of the sequence as vectors, and then using the sequence itself to describe the multiplication by creating a slide rule for that operation. The notion of such a slide rule is not new to this paper; see the work of Schellwat [5]. However, it is much easier to obtain the slide rule using this approach. The following will explain in detail how such a representation may be obtained. We will restrict our attention to Fibonacci-like sequences (that is, the cases where \( n=2 \)) but all of the material may be easily applied to other recursively defined sequences, and a few comments will be made to emphasize this point.

To understand the approach, one must first be acquainted with the idea of the characteristic matrix associated to a particular polynomial. The idea is that to each polynomial of degree \( n \), there is an \( n \times n \) matrix (many, actually) that satisfy that polynomial. In other words, when that matrix is plugged into the polynomial, the result is the \( n \times n \) zero matrix. For a more detailed description, see Finkbeiner [2].

**Definition 6.** A 2×2 matrix is said to be a Canonical Fibonacci Matrix (CFM) if it is the characteristic matrix for a primitive irreducible quadratic equation over a field \( F \) of order \( p^n \), and it is of the form
\[
\begin{bmatrix}
0 & a \\
1 & b
\end{bmatrix}
\]
where \( a \) and \( b \) are elements of \([p]\).

*Note:* This definition can be extended to a \( n \times n \) matrix for any \( n \). In this case, the CFM would be of the form
\[
\begin{bmatrix}
0 & 0 & \ldots & a_1 \\
1 & 0 & \ldots & a_2 \\
\vdots & \ddots & \ddots & \vdots \\
0 & \ldots & 1 & a_n
\end{bmatrix}
\begin{bmatrix}
0 & -d \\
1 & -c
\end{bmatrix}
\]
Theorem 2. Suppose \( x^2 + cx + d \) is a primitive irreducible polynomial. Then is a CFM.

**Proof.**

The matrix \[
\begin{pmatrix}
0 & -d \\
1 & -c
\end{pmatrix}
\] is of the correct form. We need only show that substituting this matrix into the polynomial results in the zero matrix. Notice that
\[
\begin{pmatrix}
0 & -d \\
1 & -c
\end{pmatrix}^2 + c \begin{pmatrix}
0 & -d \\
1 & -c
\end{pmatrix} + d \begin{pmatrix}
1 & 0 \\
0 & 1
\end{pmatrix}
\]
\[
= \begin{pmatrix}
-d & cd \\
c^2 - d
\end{pmatrix} + \begin{pmatrix}
0 & -cd \\
c & -c^2
\end{pmatrix} + \begin{pmatrix}
d & 0 \\
0 & d
\end{pmatrix} = \begin{pmatrix}
0 & 0 \\
0 & 0
\end{pmatrix}.
\]

We will now use a CFM to produce a Fibonacci cycle. There is nothing particularly new about using a matrix of the form \[
\begin{pmatrix}
0 & a \\
b & 0
\end{pmatrix}
\] to generate a Fibonacci sequence. We will show that by using a CFM, a maximal length Fibonacci cycle is obtained. This cycle may then be exploited as a slide rule.

**Example 1.** To illustrate the procedure, we consider the finite field \( F \) of order \( p = 3 \), and we let \( n = 2 \) (as per our convention). Then the polynomial \( x^2 + 2x + 2 \) is, in fact, primitive irreducible over \( F \). By theorem 2, we have that \[
\begin{pmatrix}
0 & -2 \\
1 & -1
\end{pmatrix}
\] is a CFM. Notice that in \( F \), \(-2 \ (mod \ 3) \equiv 1\). We express the matrix as \[
\begin{pmatrix}
0 & 1 \\
1 & 1
\end{pmatrix}.
\]

To create the Fibonacci sequence, we will start with \(0, 1\). Then
\[
\begin{align*}
[0 & 1] \begin{pmatrix}
0 & 1 \\
1 & 1
\end{pmatrix} = [1 & 1], \\
[1 & 1] \begin{pmatrix}
0 & 1 \\
1 & 1
\end{pmatrix} = [1 & 2], \\
[1 & 2] \begin{pmatrix}
0 & 1 \\
1 & 1
\end{pmatrix} = [2 & 3] \equiv_3 [2 \ 0] \ (in \ F, \ 3 \ (mod \ 3) \equiv 0), \\
[2 & 0] \begin{pmatrix}
0 & 1 \\
1 & 1
\end{pmatrix} = [0 & 2], \\
[0 & 2] \begin{pmatrix}
0 & 1 \\
1 & 1
\end{pmatrix} = [2 & 2], \\
[2 & 2] \begin{pmatrix}
0 & 1 \\
1 & 1
\end{pmatrix} = [2 & 4] \equiv_3 [2 \ 1], \\
[2 & 1] \begin{pmatrix}
0 & 1 \\
1 & 1
\end{pmatrix} = [1 \ 0], \\
[1 & 0] \begin{pmatrix}
0 & 1 \\
1 & 1
\end{pmatrix} = [0 \ 1].
\end{align*}
\]
Since we have returned to our starting point, we may assume that the pattern simply repeats itself. Now, gluing this together, the following sequence is obtained:
0, 1, 1, 2, 0, 2, 2, 1, 0, 1, 1, 2, 0, 2, 2, 1, ...

Then the finite field of order 9 can be represented using the following nine sequences:

\[
\begin{align*}
0 &= 0, 0, 0, 0, 0, \ldots \\
\alpha &= 0, 0, 1, 1, 2, 0, 2, 2, 1, 0, 1, \ldots \\
\alpha^2 &= 1, 1, 2, 0, 2, 2, 1, 0, 1, 0, \ldots \\
\alpha^3 &= 1, 2, 0, 2, 2, 1, 0, 1, 0, 1, \ldots \\
\end{align*}
\]
Etc.

Evidently, the elements of the field are obtained by merely shifting the starting point of the original sequence. To simplify the representative notation, one may represent the individual sequence elements using a vector containing the first two terms of the sequence, since \(n=2\). The dimensions of the vector change with different values of \(nn\). For example, \(\alpha^3 = 1, 2, 0, 2, 2, 1, 0, 1, 0, 1, \ldots\) would be abbreviated \(\alpha^3 = [1 2]\).

**Theorem 3.** The Fibonacci cycles generated using the CFM will be of maximal length.

**Proof.**

Let \(M\) be a CFM for this field, and let \(a = [0 1]\). Then \(a^2=aM, a^3=aMM=aM^2\), and in general, for any integer \(k\), \(a^k = aM^{k-1}\). If the Fibonacci cycle were not of maximal length, then there is some \(n\) less than the order of \(G(F)\) so that \(a^n = a\). That says that \(a = aM^{n-1}\) which, in turn, tells us that \(M^{n-1}\) is the identity matrix. Thus, the CFM does not generate the entire multiplicative group. This contradicts the fact that the CFM was a root to a primitive irreducible polynomial, and so it must generate the entire group. Therefore, the Fibonacci cycle must be of maximal length.

Addition between elements in the field works like basic vector addition, as expected. A simple example using a finite field of order 9: \([2 2]+[1 1]=[3 3](mod 3)\equiv[0 0]\).

The multiplication as stated earlier, is more difficult to achieve. An approach to multiplication may be taken directly from the cycles themselves. This approach operates in the manner of a slide rule. Suppose, you wish to multiply \([1 2]\) and \([2 2]\). You will use two copies of the extended Fibonacci cycles to do this. The second copy will slide beneath the first in order to perform the multiplication. That is, locate the first vector to be multiplied and begin the second cycle directly beneath the second term of that first vector. Locate the second vector on the second cycle. The product will be the vector directly above the second vector. The figure below will illustrate this procedure.

| Cycle 1: | 0 1 [1 2] 0 2 2 1 [0 1] 1 2 0 2 2 ⋯ |
| Cycle 2: | 0 1 1 2 0 [2 2] 1 0 1 1 2 ⋯ |

So, evidently, \([1 2]×[2 2]=[0 1]\).
A simpler method can be found as a consequence of our research to multiply elements between one another in the field. As above, using a finite field of order $9$ ($p = 3$ and $n = 2$) can be reassigned using the abbreviated sequence:

\[
\begin{align*}
0 &= [0 0] \\
\alpha^1 &= [0 1] \\
\alpha^2 &= [1 1] \\
\alpha^3 &= [1 2] \\
\alpha^4 &= [2 0] \\
\alpha^5 &= [0 2] \\
\alpha^6 &= [2 2] \\
\alpha^7 &= [2 1] \\
\alpha^8 &= [1 0] \equiv \alpha^0.
\end{align*}
\]

*Note:* For commutative multiplication to be closed, we perform modular arithmetic by the maximal length order minus one. In this case, modulo 8.

By assigning the elements of the finite field with a new exponential notation, multiplication now can be performed using algebraic methods. For example, $[1 2] \times [2 2] = \alpha^3 \alpha^6 = \alpha^9 (\text{mod } 8) \equiv \alpha^1 = [0 1]$. From this, we confirm this method will give the same results as the slide rule above.

---

**References**


