

PERIOD SETS OF LINEAR RECURRENCES OVER FINITE FIELDS AND RELATED COMMUTATIVE RINGS

MICHAEL R. BUSH AND DAN JOSEPH QUIJADA

ABSTRACT. After giving an overview of the existing theory regarding the periods of sequences defined by linear recurrences over finite fields, we give explicit descriptions of the sets of periods that arise if one considers all sequences over \mathbb{F}_q generated by linear recurrences for a fixed choice of the degree k in the range $1 \leq k \leq 4$. We also investigate the periods of sequences generated by linear recurrences over rings of the form $\mathbb{F}_{q_1} \oplus \dots \oplus \mathbb{F}_{q_r}$.

1. INTRODUCTION

We begin by fixing some notation and recalling some definitions and basic results concerning linear recurrence sequences. Let R be a commutative ring with unity $1 \neq 0$. Let $\mathbf{a} = (a_n)_{n=0}^\infty$ be a sequence with $a_n \in R$ for all $n \geq 0$. If there exist $c_i \in R$ for $0 \leq i \leq k-1$ such that the terms in the sequence satisfy the following equation

$$(1) \quad a_{n+k} = \sum_{i=0}^{k-1} c_i a_{n+i}$$

for all $n \geq 0$, then we say that \mathbf{a} is a *linear recurrence sequence over R* . The equation is called a *linear recurrence* and the quantity k is called the *degree* of the recurrence. Formally, the linear recurrence is specified by a tuple of coefficients $(c_0, \dots, c_{k-1}) \in R^k$ and zero entries are allowed in any position including c_0 , thus the degree is not required to be minimal in any sense.

Example 1.1. *The well-known Fibonacci sequence*

$$0, 1, 1, 2, 3, 5, 8, 13, \dots$$

Date: 8 May 2018.

2010 Mathematics Subject Classification. 11B50 (11B37, 11B39, 94A55).

Key words and phrases. sequence, linear recurrence, period, characteristic polynomial, finite field, finite commutative ring, cyclic group algebra.

This work began as a summer project while the second author was an undergraduate student at Washington and Lee University. It subsequently became part of an Honors thesis [8] completed in 2015. The second author would like to thank the university for providing summer research scholar funding. The first author was also partially supported by an internal Lenfest grant.

is a linear recurrence sequence over \mathbb{Z} satisfying the degree 2 recurrence

$$a_{n+2} = a_{n+1} + a_n$$

for all $n \geq 0$ with coefficients $c_0 = c_1 = 1$.

It is clear from the form of equation (1) that each term in the sequence depends on the previous k terms. As a result, it is natural to consider the tuple $s_n = (a_n, \dots, a_{n+k-1}) \in R^k$ ($n \geq 0$), which we refer to as the n -th state vector of the sequence. Any linear recurrence sequence of degree k is completely determined by specifying the recurrence equation and initial state $s_0 = (a_0, \dots, a_{k-1})$.

If R is a finite ring, then there are a finite number of possible states $|R^k| = |R|^k$ and an argument using the pigeonhole principle shows that the sequence must be ultimately periodic, ie. there exist positive $N, m \in \mathbb{Z}$ such that $a_{n+m} = a_n$ for all $n \geq N$. In this situation, we will say the sequence \mathbf{a} is m -periodic. The smallest positive value of m with this property is called the *period* of the sequence and it will be denoted by $\rho(\mathbf{a})$. We note that some authors use the term *least period* for $\rho(\mathbf{a})$, but we will not. It is straightforward to verify using a Division Algorithm argument that for any positive integer m , the sequence \mathbf{a} is m -periodic if and only if $\rho(\mathbf{a})$ divides m .

Important examples of finite commutative rings include the integers modulo n which we denote \mathbb{Z}_n and also finite fields. We use the notation \mathbb{F}_q to denote the finite field of order q where $q = p^e$ with $e \geq 1$ and p a prime integer. Recall that when $n = q = p$ these notions coincide and we have $\mathbb{Z}_p \cong \mathbb{F}_p$.

Example 1.2. Consider the Fibonacci recurrence $a_{n+2} = a_{n+1} + a_n$ over $\mathbb{F}_2 = \{0, 1\}$. Starting from the initial state $s_0 = (a_0, a_1) = (0, 1)$, we obtain the sequence

$$\underline{0}, \underline{1}, 1, \underline{0}, \underline{1}, 1, 0, 1, \dots$$

and so clearly we have $\rho(\mathbf{a}) = 3$ in this case.

In general, if the coefficient $c_0 \in R$ is a unit, then one can invert the recurrence equation (1) and observe that any state s_n uniquely determines the preceding term a_{n-1} and hence the state s_{n-1} . In this situation, the periodicity begins right from the initial term. ie. $a_{n+m} = a_n$ for all $n \geq 0$. Throughout this paper we will restrict attention to sequences defined by recurrence equations satisfying this condition.

It is natural to ask about the set of all possible periods of linear recurrence sequences defined over a finite ring R and how this depends on the choice of ring. One easy observation is that for a given degree k , the period is always bounded above by $|R|^k - 1$. This follows from the pigeonhole principle argument above. Since there are $|R|^k$ state vectors, any list of $|R|^k + 1$ consecutive states must include the repetition of at least two states. This gives a bound of $|R|^k$ on the period. One can decrease this slightly because the zero state vector $(0, \dots, 0)$ clearly generates the zero sequence of period 1. Hence any sequence containing infinitely many non-zero terms cannot involve this state and so the maximum number of allowed states in a repeating cycle is reduced to $|R|^k - 1$.

In the case where $R = \mathbb{F}_q$, there is a well-developed theory describing the behavior of these periods. In particular, it can be shown (see Corollary 2.10) that for each $k \geq 1$, there exist linear recurrence sequences of degree k with period equal to the upper bound $q^k - 1$. In Section 2, we give an overview of some of this theory. In Section 3, we apply it to obtain our main result (Theorem 3.5) giving explicit descriptions of the sets of periods that can be achieved for small values of the degree k over an arbitrary finite field. In Section 4, we investigate the periods of sequences defined over a slightly broader class of finite commutative rings.

Throughout we will assume that the reader is familiar with the basic facts about finite fields and polynomial rings defined over fields as can be found in many introductory books on abstract algebra. See for instance [2, 5].

2. LINEAR RECURRENCES OVER FINITE FIELDS

In this section, we review some material concerning orders of polynomials and then explain how this is connected with determining the periods of linear recurrence sequences defined over finite fields. We follow the treatment in [6, Chapters 3 and 8] and further discussion and additional results can be found there. See also [1, Section 6.2] although we note that the latter uses slightly different terminology.

Definition 2.1. *Let $f(x) \in \mathbb{F}_q[x]$ and suppose $f(x) = x^r g(x)$ with $r \geq 0$ and $\gcd(g(x), x) = 1$. Observe that r and $g(x)$ are uniquely determined by $f(x)$. The order of $f(x)$ (denoted $\text{ord}(f(x))$) is defined to be the smallest integer $n > 0$ such that $g(x)$ divides $x^n - 1$. Equivalently, this quantity is the multiplicative order of $x + \langle g(x) \rangle$ in the group of units of the quotient ring $\mathbb{F}_q[x]/\langle g(x) \rangle$.*

Remark 2.2. *The fact that such an n exists follows since the quotient ring $\mathbb{F}_q[x]/\langle g(x) \rangle$ is finite and so has a finite multiplicative group of units. The condition $\gcd(g(x), x) = 1$ ensures that $\alpha = x + \langle g(x) \rangle$ is an element of the unit group.*

If the polynomial $f(x)$ (or $g(x)$) is irreducible in $\mathbb{F}_q[x]$, then we have an isomorphism $\mathbb{F}_q[x]/\langle g(x) \rangle \cong \mathbb{F}_{q^d}$ where $d = \deg g(x)$. In this situation, $\alpha \neq 0$ is a root of $g(x)$ in the larger field \mathbb{F}_{q^d} and the order of the polynomial is simply the multiplicative order of α in $\mathbb{F}_{q^d}^\times = \mathbb{F}_{q^d} - \{0\}$. It follows by Lagrange's theorem that $\text{ord}(f(x))$ must divide $q^d - 1$ in this situation.

The problem of computing $\text{ord}(f(x))$ can be reduced to the irreducible case using the following two results. For proofs, see [6, Theorems 3.8, 3.9 and 3.11].

Theorem 2.3. *Let $g(x)$ be irreducible over \mathbb{F}_q with $g(0) \neq 0$ and $\text{ord}(g(x)) = e$, and let $f(x) = g(x)^b$ with $b \in \mathbb{Z}_{>0}$. Let t be the smallest integer with $p^t \geq b$ where p is the characteristic of \mathbb{F}_q . Then $\text{ord}(f(x)) = ep^t$.*

Theorem 2.4. *Let $g_1(x), \dots, g_k(x) \in \mathbb{F}_q[x]$ be pairwise relatively prime nonzero polynomials, and let $f(x) = g_1(x) \dots g_k(x)$. Then $\text{ord}(f(x))$ is equal to the least common multiple of $\text{ord}(g_1(x)), \dots, \text{ord}(g_k(x))$.*

In order to establish the connection between the periods of linear recurrence sequences and the orders of certain polynomials, we must first introduce the following matrix. Using the coefficients in Equation (1), we define a $k \times k$ matrix C over \mathbb{F}_q by

$$(2) \quad C = \begin{pmatrix} 0 & 0 & \dots & 0 & c_0 \\ 1 & 0 & \dots & 0 & c_1 \\ 0 & 1 & \dots & 0 & c_2 \\ \vdots & \vdots & \ddots & \vdots & \\ 0 & 0 & \dots & 1 & c_{k-1} \end{pmatrix}.$$

This matrix is called the *companion matrix* of the linear recurrence. It is straightforward to verify that $s_n C = s_{n+1}$ for all $n \geq 0$ where s_n is the n th state vector of a sequence satisfying the recurrence and we view s_n as a row vector. By induction, it follows that $s_n = s_0 C^n$ for all $n \geq 0$. From this point onwards, we will assume that $\det C = (-1)^{k-1} c_0 \neq 0$ and hence that C is an element of the general linear group $GL_k(\mathbb{F}_q)$. Recall from Section 1 that under this assumption on c_0 , all sequences associated with the recurrence are periodic starting from the initial state.

There is an important relationship between the periods of sequences defined by a given linear recurrence and the order of the corresponding companion matrix C in the multiplicative group $GL_k(\mathbb{F}_q)$. Recall that the order of a matrix C is the smallest positive integer n such that $C^n = I_k$ where $I_k \in GL_k(\mathbb{F}_q)$ is the $k \times k$ identity matrix. We will denote this quantity by $\text{ord}(C)$.

Theorem 2.5. *Let \mathbf{a} be a sequence satisfying a linear recurrence and let C be the companion matrix, then $\rho(\mathbf{a})$ divides $\text{ord}(C)$. Furthermore, for any given companion matrix C , there exists a sequence \mathbf{b} satisfying the associated recurrence with $\rho(\mathbf{b}) = \text{ord}(C)$.*

Proof. This result appears in [6, Theorems 8.13 and 8.17]. Since the proof is fairly short and contains some important ideas, we recall it here.

Let \mathbf{a} be an arbitrary sequence satisfying the given recurrence. We first show that $\rho(\mathbf{a})$ divides $\rho(\mathbf{b})$ for a special sequence \mathbf{b} which we now introduce. Let \mathbf{b} be the sequence satisfying the same recurrence with initial state $t_0 = (0, \dots, 0, 1)$ – so the first $k - 1$ entries equal 0 and the k th entry is 1. Then the n th state t_n satisfies $t_n = t_0 C^n$ for all $n \geq 0$. The first k states then have the following special form

$$\begin{aligned} t_0 &= (0, \dots, 0, 0, 1) \\ t_1 &= (0, \dots, 0, 1, *) \\ t_2 &= (0, \dots, 1, *, *) \\ &\vdots \\ t_{k-1} &= (1, *, \dots, *, *, *) \end{aligned}$$

where $*$ denotes some element in \mathbb{F}_q that we do not specify exactly. Clearly, $\mathcal{B} = \{t_i \mid 0 \leq i \leq k-1\}$ is a basis for \mathbb{F}_q^k since the matrix formed by these vectors has full rank k . It follows that the initial state s_0 of \mathbf{a} can be expressed as a linear combination of the vectors in \mathcal{B} . Using the linearity of the recurrence, one can then see that the sequence \mathbf{a} is a linear combination of the sequences with initial states in \mathcal{B} . These sequences consist of \mathbf{b} together with its cyclic shifts and so all have the same period $\rho(\mathbf{b})$. Any linear combination of m -periodic sequences is m -periodic, so the sequence \mathbf{a} must be $\rho(\mathbf{b})$ -periodic. It follows that $\rho(\mathbf{a})$ divides $\rho(\mathbf{b})$.

To finish, we now show that $\rho(\mathbf{b}) = \text{ord}(C)$. Let $m = \rho(\mathbf{b})$ and $n = \text{ord}(C)$. Since $C^n = I_k$, we see that $t_n = t_0 C^n = t_0$. It follows that \mathbf{b} is n -periodic and so m must divide n . We note that this part of the argument does not make use of the special nature of \mathbf{b} and could be applied to an arbitrary sequence \mathbf{a} , thus establishing directly that $\rho(\mathbf{a})$ always divides $\text{ord}(C)$. Now observe that since \mathbf{b} is m -periodic, the sequence of state vectors must also be m -periodic and so we have $t_{m+i} = t_i$ for all $i \geq 0$. But $t_{m+i} = t_i C^m$, thus $t_i C^m = t_i I_k$ for all $i \geq 0$ and, in particular, this holds for all of the state vectors in the basis \mathcal{B} . It follows that $C^m = I_k$ and so the order n must divide m . Since $m = \rho(\mathbf{b})$ and $n = \text{ord}(C)$ are positive integers that divide each other, we conclude that $\rho(\mathbf{b}) = \text{ord}(C)$ as desired. \square

Remark 2.6. *Theorem 2.5 shows that the maximum period for a given recurrence with associated matrix C is $\text{ord}(C)$. The sequence \mathbf{b} with initial sequence $t_0 = (0, \dots, 0, 1)$ which is shown to attain this maximum in the proof is called the impulse response sequence for the given recurrence. If one examines the argument used at the end of the proof, one sees that any sequence \mathbf{a} , for which the first k state vectors $\{s_i \mid 0 \leq i \leq k-1\}$ form a basis for \mathbb{F}_q^k , will also have the property that $\rho(\mathbf{a}) = \text{ord}(C)$.*

There is an important polynomial associated to the matrix C and so also the recurrence (1).

Definition 2.7. *The characteristic polynomial of $C \in GL_k(\mathbb{F}_q)$ is the polynomial*

$$f(x) = \det(xI_k - C) \in \mathbb{F}_q[x].$$

Observe that if C is a $k \times k$ matrix, then we have $\deg f(x) = k$.

For matrices C of the special form (2) above, it is a straightforward exercise using properties of determinants to show that

$$f(x) = \det(xI_k - C) = x^k - \sum_{i=0}^{k-1} c_i x^i.$$

The latter polynomial is very closely related to the original recurrence equation. Indeed, if one sets $n = 0$ and formerly substitutes x^i for a_i in Equation (1), then this polynomial appears after moving all of the terms to one side.

We now show that there is a direct connection between the order of this polynomial (as defined at the beginning of the section) and the order of the matrix C .

Theorem 2.8. *Let $C \in GL_k(\mathbb{F}_q)$ and let $f(x)$ be the associated characteristic polynomial. Then $\text{ord}(C) = \text{ord}(f(x))$.*

Proof. This result appears in [6, Lemma 8.26]. The proof there assumes some familiarity with advanced linear algebra so we give a self-contained proof here.

Consider the following set of polynomials

$$J = \{g(x) \in \mathbb{F}_q[x] \mid g(C) = 0\}$$

where the expression $g(C)$ is evaluated in the natural way (treating the constant term as a scalar multiple of the identity matrix) and the equation $g(C) = 0$ means $g(C)$ is the zero matrix. It is a consequence of the Cayley-Hamilton Theorem, that $f(C) = 0$ and so $f(x) \in J$. For matrices C of the special form (2) above, this can also be seen directly as follows. If we consider the impulse response sequence \mathbf{b} with n th state vector t_n , then since the state vectors also satisfy the recurrence (1), we have

$$\begin{aligned} 0 = t_{n+k} - \sum_{i=0}^{k-1} c_i t_{n+i} &= t_n C^k - \sum_{i=0}^{k-1} c_i (t_n C^i) \\ &= t_n \left(C^k - \sum_{i=0}^{k-1} c_i C^i \right) \\ &= t_n f(C) \end{aligned}$$

for all $n \geq 0$. In particular, this holds for all of the vectors in the basis $\mathcal{B} = \{t_i \mid 0 \leq i \leq k-1\}$ and so we must have $f(C) = 0$ as desired.

Having shown that $f(x) \in J$, we now observe that J is an ideal and so $\langle f(x) \rangle \subseteq J$ where $\langle f(x) \rangle$ is the principal ideal generated by $f(x)$. In fact, equality must hold. This can be seen using the standard fact that $\mathbb{F}_q[x]$ is a principal ideal domain and verifying that J does not contain any nonzero polynomials of smaller degree. Suppose that this were not the case and $g(x) \in J$ with $\deg g(x) < \deg f(x) = k$. Then since $g(C) = 0$, we would have $t_n g(C) = 0$ for all $n \geq 0$. Expanding the left-hand side when $n = 0$ would then give a dependence relation among the vectors in \mathcal{B} which is a contradiction since these vectors are linearly independent.

Having established that $J = \langle f(x) \rangle$, we finish by noting that $C^n = I_k$ holds if and only if $x^n - 1 \in J$ which in turn holds if and only if $f(x)$ divides $x^n - 1$. It follows from the definitions that $\text{ord}(C) = \text{ord}(f(x))$. Note that $f(0) = -c_0 \neq 0$, so $\text{gcd}(x, f(x)) = 1$. \square

Combining Theorem 2.5 and Theorem 2.8, we have

Corollary 2.9. *Let $f(x)$ be the characteristic polynomial of a linear recurrence and let \mathbf{a} be any sequence satisfying the recurrence, then $\rho(\mathbf{a})$ divides $\text{ord}(f(x))$. Moreover, there exist sequences with $\rho(\mathbf{a}) = \text{ord}(f(x))$.*

Corollary 2.10. *For each prime power q and $k \in \mathbb{Z}_{>0}$, there exists a linear recurrence sequence \mathbf{a} over \mathbb{F}_q of degree k achieving the maximum possible period $\rho(\mathbf{a}) = q^k - 1$.*

Proof. The multiplicative group of the finite field \mathbb{F}_{q^k} is cyclic of order $q^k - 1$. Let $f(x)$ be the minimum polynomial of a generator for this group. (Such an irreducible polynomial is said to be *primitive*). Then we have $\text{ord}(f(x)) = q^k - 1$ by Remark 2.2 and so the statement now follows by Corollary 2.9. \square

More can be said about the possible values of $\rho(\mathbf{a})$. Observe that every periodic sequence \mathbf{a} satisfies a linear recurrence. For instance, if \mathbf{a} is m -periodic then it automatically satisfies the degree m recurrence $a_{n+m} = a_n$ for all $n \geq 0$. Among the set of all such recurrences, we single out the one of smallest degree. This is uniquely determined since if there were two distinct recurrences of this degree, we could subtract, cancel and divide by the non-zero coefficient on the largest index term remaining to obtain a recurrence of even smaller degree satisfied by the sequence which would be a contradiction.

Definition 2.11. *Let \mathbf{a} be a nonzero periodic sequence. We define the minimal polynomial $m(x)$ to be the characteristic polynomial of the (unique) linear recurrence of smallest degree satisfied by \mathbf{a} . For the zero sequence $\mathbf{a} = (0)_{n=0}^\infty$, we set $m(x) = 1$.*

From the definition and preceding observations, we clearly have $\deg m(x) \leq \rho(\mathbf{a})$ and $\deg m(x) \leq \deg f(x)$ for all characteristic polynomials $f(x)$ of linear recurrences satisfied by \mathbf{a} . In fact, a much stronger statement holds.

Theorem 2.12. *Let \mathbf{a} be a periodic sequence and let $m(x)$ be the minimal polynomial of \mathbf{a} . Then $f(x)$ is the characteristic polynomial of a linear recurrence satisfied by \mathbf{a} if and only if $m(x)$ divides $f(x)$. We also have $\rho(\mathbf{a}) = \text{ord}(m(x))$.*

Proof. For a proof of the divisibility statement, which we will not need in our subsequent work, see [6, Section 8.4]. Note that in [6], the minimal polynomial is defined via a divisibility condition. After existence and uniqueness have been demonstrated, it is straightforward to see that this is equivalent to the definition used here.

For the second statement, observe that $\rho(\mathbf{a})$ divides $\text{ord}(m(x))$ by Corollary 2.9 and, as noted above, we have $\text{ord}(m(x)) \leq \rho(\mathbf{a})$. Equality follows immediately. Alternatively, one can see directly that if $\deg(m(x)) = k$, then the first k state vectors of \mathbf{a} must be linearly independent since a dependence relation would give rise to a recurrence of smaller degree satisfied by the full sequence of state vectors and hence also \mathbf{a} . It follows that the first k state vectors form a basis of \mathbb{F}_q^k since the dimension is k , and so we can apply Remark 2.6 to see that $\rho(\mathbf{a}) = \text{ord}(m(x))$. \square

We conclude by showing how the results in this section provide information about the periods of sequences in the case of the Fibonacci recurrence.

Example 2.13. *The Fibonacci recurrence $a_{n+2} = a_{n-1} + a_n$ has been extensively studied over both \mathbb{Z}_n and finite fields. Recent work includes [3, 4] and additional*

references can be found in these papers. For this recurrence, the companion matrix is

$$C = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$$

and the characteristic polynomial is $f(x) = x^2 - x - 1$. The sequence \mathbf{a} defined by this recurrence with initial state $s_0 = (0, 1)$ is the impulse response sequence and so attains the maximum possible period $\rho(\mathbf{a}) = \text{ord}(f(x))$. Other initial states will give rise to sequences whose periods divide this maximum. Since the recurrence and initial state for \mathbf{a} are both defined over the prime subfield $\mathbb{F}_p \subseteq \mathbb{F}_q$, the entire sequence will also lie in \mathbb{F}_p and so it suffices to consider the case $q = p$ prime.

Determining the value of $\text{ord}(f(x))$ involves first factoring $f(x)$ in $\mathbb{F}_p[x]$. We now consider various cases. If $p = 2$, then one observes that $f(x) = x^2 + x + 1$ is irreducible. Since $\alpha = x + \langle f(x) \rangle$ must have nontrivial multiplicative order in $\mathbb{F}_2[x]/\langle f(x) \rangle \cong \mathbb{F}_4$, we see that $\text{ord}(f(x)) = 3$. Alternatively, one can simply generate the sequence and observe that the period is 3 as we did in Example 1.2.

If p is odd, then 2 is invertible in \mathbb{F}_p and we can complete the square to write $f(x) = (x - 2^{-1})^2 - \Delta/2^{-2}$ where $\Delta = 5$ is the discriminant of $f(x)$. It follows that $f(x)$ will be irreducible over \mathbb{F}_p if and only if 5 is not a square in \mathbb{F}_p . By the law of quadratic reciprocity, we see that 5 is not a square in \mathbb{F}_p if and only if $p \equiv 2, 3 \pmod{5}$, and 5 is a square if and only if $p \equiv 1, 4 \pmod{5}$ or $p = 5$.

- If $p \equiv 2, 3 \pmod{5}$, then $f(x)$ is irreducible over \mathbb{F}_p and the order and hence period of the sequence will be the multiplicative order of $\alpha = x + \langle f(x) \rangle$ in $\mathbb{F}_p[x]/\langle f(x) \rangle \cong \mathbb{F}_{p^2}$. It follows that the order will be a divisor of $p^2 - 1$ that does not divide $p - 1$. (The second condition is forced since α cannot belong to the prime field \mathbb{F}_p in this case.)
- If $p \equiv 1, 4 \pmod{5}$, then $f(x)$ factors as a product of distinct linear factors over \mathbb{F}_p and applying Theorem 2.4 we see that the period will divide $p - 1$.
- Finally, if $p = 5$, then we have a repeated linear factor $f(x) = (x - 3)^2$. Since 3 has order 4 in \mathbb{F}_5 , we can apply Theorem 2.3 to see that $\text{ord}(f(x)) = 20$. Alternatively, one can simply generate the sequence and observe that the period is 20.

In fact, more can be said in the case where $f(x)$ is irreducible as shown in [4, Theorem 5]. Given one root α of $f(x)$, the other root can be obtained by applying the Frobenius automorphism and is simply α^p . Since the product of the roots of a quadratic is the constant coefficient, we obtain the relation $\alpha \cdot \alpha^p = \alpha^{p+1} = -c_0 = -1$. It follows that $\alpha^{2(p+1)} = 1$ and thus the order of α must divide $2(p+1)$ which is strictly smaller than $p^2 - 1$ for $p > 3$.

3. PERIOD SETS OF SMALL DEGREE RECURRENCES

In this section, we use the results from the previous section to determine the period sets for recurrences of small degree over finite fields.

Definition 3.1. Let $k \in \mathbb{Z}_{>0}$ and let q be a prime power. We define the period set of degree k over \mathbb{F}_q by

$$P(k, \mathbb{F}_q) = \{\rho(\mathbf{a}) \mid \mathbf{a} \text{ satisfies a linear recurrence of degree } k \text{ over } \mathbb{F}_q\}$$

and the order set of degree k over \mathbb{F}_q by

$$O(k, \mathbb{F}_q) = \{\text{ord}(f(x)) \mid f(x) \in \mathbb{F}_q[x] \text{ and } \deg f(x) = k\}.$$

A simple inductive argument, in which the inductive step involves adding together two copies of the recurrence equation for consecutive values of the leading index, shows that every sequence satisfying a recurrence of degree j satisfies a recurrence of degree k for all $k \geq j$. Hence, we have $P(j, \mathbb{F}_q) \subseteq P(k, \mathbb{F}_q)$ for all $j \leq k$. Similarly, from the definition, we have $\text{ord}(f(x)) = \text{ord}(g(x))$ for $f(x) = x^d g(x)$ with $d \geq 0$, so then $O(j, \mathbb{F}_q) \subseteq O(k, \mathbb{F}_q)$ for all $j \leq k$.

The next lemma shows that if we want to compute the period set of a given degree, then it suffices to compute the corresponding order set.

Lemma 3.2. For all $k \in \mathbb{Z}_{>0}$ and prime powers q , we have $P(k, \mathbb{F}_q) = O(k, \mathbb{F}_q)$.

Proof. We check containment in both directions. Let $n \in P(k, \mathbb{F}_q)$. Then $n = \rho(\mathbf{a})$ for some sequence \mathbf{a} defined by a linear recurrence of degree k over \mathbb{F}_q . Let $f(x)$ be the associated characteristic polynomial and let $m(x)$ be the minimal polynomial of \mathbf{a} . Let $d = \deg m(x)$. Then $d \leq k$ by definition of the minimal polynomial. It follows from Theorem 2.12 that

$$n = \rho(\mathbf{a}) = \text{ord}(m(x)) \in O(d, \mathbb{F}_q) \subseteq O(k, \mathbb{F}_q).$$

Thus $P(k, \mathbb{F}_q) \subseteq O(k, \mathbb{F}_q)$.

Now suppose $n \in O(k, \mathbb{F}_q)$. Then $n = \text{ord}(f(x))$ for some $f(x) \in \mathbb{F}_q[x]$ with $\deg f(x) = k$. By Corollary 2.9, there exists a sequence \mathbf{a} satisfying the linear recurrence associated to $f(x)$ with $\rho(\mathbf{a}) = \text{ord}(f(x)) = n$, and so $n \in P(k, \mathbb{F}_q)$. Thus $O(k, \mathbb{F}_q) \subseteq P(k, \mathbb{F}_q)$. The desired set equality now follows. \square

Before using Lemma 3.2 to give an explicit description of $P(k, \mathbb{F}_q)$ for small values of k , we introduce some more notation. Given $n \in \mathbb{Z}_{>0}$, we let $D(n)$ denote the set of all positive integer divisors of n . For example, $D(6) = \{1, 2, 3, 6\}$. Given an integer a and subsets $S_1, S_2 \subseteq \mathbb{Z}$, we define $aS_1 = \{ax \mid x \in S_1\}$ and $S_1S_2 = \{xy \mid x \in S_1, y \in S_2\}$. For example, $5D(6) = \{5, 10, 15, 30\}$ and $D(2)D(6) = \{1, 2, 3, 4, 6, 12\}$.

Theorem 3.3. Let \mathbb{F}_q have prime characteristic p . For all $k \in \mathbb{Z}_{>0}$, we have

$$\bigcup_{i=1}^k \{p^j \mid 0 \leq j \leq t_i\} D(q^i - 1) \subseteq P(k, \mathbb{F}_q)$$

where $t_i = \lceil \log_p \lfloor k/i \rfloor \rceil = \min\{t \in \mathbb{Z} \mid p^t \geq \lfloor k/i \rfloor\}$ for $1 \leq i \leq k$.

Proof. To prove the containment, let $1 \leq i \leq k$ and consider $n = p^j d$ with $0 \leq j \leq t_i$ and $d \in D(q^i - 1)$. We show that $n \in P(k, \mathbb{F}_q)$ by constructing an appropriate polynomial $f(x)$ with $\text{ord}(f(x)) = n$.

Since the multiplicative group of $K = \mathbb{F}_{q^i}$ is cyclic of order $q^i - 1$ and d divides $q^i - 1$, we can find an element $\alpha \in K$ of order d . Let $g(x) \in \mathbb{F}_q[x]$ be the minimal polynomial of α over \mathbb{F}_q . Then $g(x)$ is irreducible with $\deg g(x) \leq i$ and $\text{ord}(g(x)) = d$ by Remark 2.2. Now set $f(x) = g(x)^b$ with $b = 1$ if $j = 0$ and $b = p^{j-1} + 1$ if $j \geq 1$. Note that in both cases, j is the smallest integer such that $p^j \geq b$. Then $\text{ord}(f(x)) = \text{ord}(g(x))p^j = dp^j = n$ by Theorem 2.3, and

$$\deg f(x) = b \deg g(x) \leq (p^{j-1} + 1)i \leq (p^{t_i-1} + 1)i \leq \lfloor k/i \rfloor i \leq k.$$

The inequality $p^{t_i-1} + 1 \leq \lfloor k/i \rfloor$ used in the second-last step above follows directly from the definition of t_i . We conclude that $n \in O(k, \mathbb{F}_q) = P(k, \mathbb{F}_q)$ by Lemma 3.2. \square

Remark 3.4. *The exponent bounds t_i and corresponding sets of prime powers appearing in Theorem 3.3 are often small. Observe that $t_i \geq 0$ for $1 \leq i \leq k$ and $t_i = 0$ occurs for $\lfloor k/2 \rfloor + 1 \leq i \leq k$. Since the largest value of the floor function $\lfloor k/i \rfloor$ occurs when $i = 1$, it follows that for $p > k$, we have $\{p^j \mid 0 \leq j \leq t_i\} = \{1, p\}$ for $1 \leq i \leq \lfloor k/2 \rfloor$. Larger sets of prime powers can occur when k is large relative to p .*

We now come to our main result.

Theorem 3.5. *Let \mathbb{F}_q have prime characteristic p . For $1 \leq k \leq 4$, the set containment in Theorem 3.3 is actually an equality. In particular, we have*

$$\begin{aligned} \text{(i)} \quad & P(1, \mathbb{F}_q) = D(q - 1). \\ \text{(ii)} \quad & P(2, \mathbb{F}_q) = D(q^2 - 1) \cup pD(q - 1). \\ \text{(iii)} \quad & P(3, \mathbb{F}_q) = \begin{cases} D(q^3 - 1) \cup D(q^2 - 1) \cup pD(q - 1), & \text{if } p \geq 3. \\ D(q^3 - 1) \cup D(q^2 - 1) \cup \{2, 4\}D(q - 1), & \text{if } p = 2. \end{cases} \\ \text{(iv)} \quad & P(4, \mathbb{F}_q) = \begin{cases} D(q^4 - 1) \cup D(q^3 - 1) \cup pD(q^2 - 1), & \text{if } p \geq 5. \\ D(q^4 - 1) \cup D(q^3 - 1) \cup pD(q^2 - 1) \cup p^2D(q - 1), & \text{if } p = 2, 3. \end{cases} \end{aligned}$$

Proof. It is straightforward to verify that the set expressions appearing on the right above match the one appearing in Theorem 3.3 for $1 \leq k \leq 4$. Note that some simplification has been carried out. For instance, if i divides j , then $q^i - 1$ divides $q^j - 1$ and one then has $D(q^i - 1) \subseteq D(q^j - 1)$. It follows that if both of these occur in a set union then the first is redundant and can be omitted. In particular, $D(q - 1)$ has been omitted from most of the expressions above. $D(q^2 - 1)$ has also been omitted when $D(q^4 - 1)$ occurs.

Since Theorem 3.3 shows containment in one direction, we will establish equality by checking the reverse containment for each value $1 \leq k \leq 4$. We have $P(k, \mathbb{F}_q) =$

$O(k, \mathbb{F}_q)$ by Lemma 3.2, so it will suffice to verify that $\text{ord}(f(x))$ belongs to the given set union for all $f(x)$ with $\deg f(x) = k$. We will make frequent use of the fact that if $g(x) \in \mathbb{F}_q[x]$ is irreducible and $\deg g(x) = d$, then $\text{ord}(g(x)) \in D(q^d - 1)$ which follows from Remark 2.2. We also note that the order of a polynomial is invariant under multiplication by nonzero scalars. Thus we can restrict our attention to monic polynomials and will also assume, without loss of generality, that all factors are monic when working with factorizations of such polynomials.

If $\deg f(x) = 1$, then $f(x)$ must be irreducible so $\text{ord}(f(x)) \in D(q - 1)$ as noted above. This establishes part (i).

If $\deg f(x) = 2$, then either $f(x)$ is irreducible, in which case we have $\text{ord}(f(x)) \in D(q^2 - 1)$, or we have a factorization $f(x) = g_1(x)g_2(x)$ with $\deg g_1(x) = \deg g_2(x) = 1$. There are then two cases to consider. If the factors are distinct (not associates), then we see that $\text{ord}(f(x))$ is the least common multiple of $\text{ord}(g_1(x))$ and $\text{ord}(g_2(x))$ by Theorem 2.4. Since both orders divide $q - 1$, it follows that $\text{ord}(f(x)) \in D(q - 1)$. On the other hand, if $g_1(x)$ and $g_2(x)$ are associates, then they must be equal since we are assuming all factors are monic. Thus we have $f(x) = g_1(x)^2$. Applying Theorem 2.3, we see that $\text{ord}(f(x)) = p \text{ord}(g_1(x)) \in pD(q - 1)$ since $p = p^1 \geq 2$ for all p . Combining the above cases, we have thus established that if $\deg f(x) = 2$, then

$$\text{ord}(f(x)) \in D(q^2 - 1) \cup D(q - 1) \cup pD(q - 1) = D(q^2 - 1) \cup pD(q - 1).$$

This establishes part (ii).

The same sort of arguments are used to handle the remaining values $k = 3, 4$ and we now outline the main subcases. If $\deg f(x) = 3$, then one of the following must hold:

- $f(x)$ is irreducible. In this case, we have $\text{ord}(f(x)) \in D(q^3 - 1)$.
- $f(x) = g(x)h(x)$ with $g(x), h(x) \in \mathbb{F}_q[x]$ irreducible and $\deg g(x) = 2$ and $\deg h(x) = 1$. Then $\text{ord}(g(x)) \in D(q^2 - 1)$ and $\text{ord}(h(x)) \in D(q - 1)$. Since $q - 1$ divides $q^2 - 1$, we see that $\text{ord}(f(x)) \in D(q^2 - 1)$.
- $f(x) = g_1(x)g_2(x)g_3(x)$ with $\deg g_1(x) = \deg g_2(x) = \deg g_3(x) = 1$ and the factors pairwise distinct. We see that $\text{ord}(g_i(x)) \in D(q - 1)$ for $i = 1, 2, 3$. Since $D(q - 1)$ is closed under least common multiples, we have $\text{ord}(f(x)) \in D(q - 1)$.
- $f(x) = g_1(x)^2g_2(x)$ with $\deg g_1(x) = \deg g_2(x) = 1$ and $g_1(x)$ distinct from $g_2(x)$. We see that $\text{ord}(g_1(x)^2) \in pD(q - 1)$ and $\text{ord}(g_2(x)) \in D(q - 1)$. Since $D(q - 1)$ is closed under least common multiples, we have $\text{ord}(f(x)) \in pD(q - 1)$.
- $f(x) = g(x)^3$ with $\deg g(x) = 1$. We have $\text{ord}(g(x)) \in D(q - 1)$. The smallest value of t such that $p^t \geq 3$ is $t = 1$ if $p \geq 3$ and $t = 2$ if $p = 2$. It follows that $\text{ord}(f(x)) \in pD(q - 1)$ if $p \geq 3$, and $\text{ord}(f(x)) \in 4D(q - 1)$ if $p = 2$.

Combining the above, we see that if $\deg f(x) = 3$ and $p \geq 3$, then

$$\begin{aligned} \text{ord}(f(x)) &\in D(q^3 - 1) \cup D(q^2 - 1) \cup D(q - 1) \cup pD(q - 1) \\ &= D(q^3 - 1) \cup D(q^2 - 1) \cup pD(q - 1) \end{aligned}$$

If $p = 2$, then $4D(q - 1)$ must also be included in the union. This establishes part (iii).

Finally, if $\deg f(x) = 4$, then one of the following must hold:

- $f(x)$ is irreducible. Then $\text{ord}(f(x)) \in D(q^4 - 1)$.
- $f(x)$ is the product of degree 3 and degree 1 irreducible polynomials. Since $q - 1$ divides $q^3 - 1$, we see that $\text{ord}(f(x)) \in D(q^3 - 1)$.
- $f(x)$ is the product of two irreducible quadratics. One must consider both the case where the quadratic factors are distinct and also the case where one is repeated. Combining, one sees that $\text{ord}(f(x)) \in \{1, p\}D(q^2 - 1)$.
- $f(x)$ is the product of an irreducible quadratic and two degree 1 polynomials (where the latter might be repeated). Then $\text{ord}(f(x)) \in \{1, p\}D(q^2 - 1)$. In deriving this statement, note that the least common multiple of an element in $D(q^2 - 1)$ and $pD(q - 1)$ will lie in $pD(q^2 - 1)$.
- $f(x)$ is the product of 4 linear factors. These could all be distinct or there could be some repetition. The cases where $f(x)$ includes a repeated factor $g(x)^3$ or $g(x)^4$ are the ones where the behavior is slightly different for small p . In particular, the smallest value of t such that $p^t \geq 4$ is $t = 1$ for $p \geq 5$ and $t = 2$ for $p = 2, 3$. Analyzing all the cases, we see that if $p \geq 5$, then $\text{ord}(f(x)) \in \{1, p\}D(q - 1)$, and if $p = 2, 3$, then $\text{ord}(f(x)) \in \{1, p, p^2\}D(q - 1)$.

Combining the above, we see that if $\deg f(x) = 4$ and $p \geq 5$, then

$$\begin{aligned} \text{ord}(f(x)) &\in D(q^4 - 1) \cup D(q^3 - 1) \cup \{1, p\}D(q^2 - 1) \cup \{1, p\}D(q - 1) \\ &= D(q^4 - 1) \cup D(q^3 - 1) \cup pD(q^2 - 1). \end{aligned}$$

If $p = 2, 3$, then $p^2D(q - 1)$ must also be included in the union. This establishes part (iv) and completes the proof. \square

Example 3.6. Consider the field \mathbb{F}_2 so $q = p = 2$. Using Theorem 3.5, we can easily compute all possible periods for linear recurrence sequences of degree $k \leq 4$ over this field. We have:

$$P(1, \mathbb{F}_2) = D(1) = \{1\}.$$

$$P(2, \mathbb{F}_2) = D(3) \cup 2D(1) = \{1, 2, 3\}.$$

$$P(3, \mathbb{F}_2) = D(7) \cup D(3) \cup \{2, 4\}D(1) = \{1, 2, 3, 4, 7\}.$$

$$P(4, \mathbb{F}_2) = D(15) \cup D(7) \cup 2D(3) \cup 4D(1) = \{1, 2, 3, 4, 5, 6, 7, 15\}.$$

Remark 3.7. It is relatively easy to find examples showing that the containment in Theorem 3.3 can be strict once $k \geq 5$. For example, the polynomials $g(x) = x^2 + x + 1$ and $h(x) = x^3 + x + 1$ are primitive over \mathbb{F}_2 and so achieve the maximum possible order $2^k - 1$ relative to their degree k as discussed in Corollary 2.10. If we set $f(x) =$

$g(x)h(x) = x^5 + x^4 + 1 = x^5 - x^4 - 1$, then $\text{ord}(f(x)) = \text{lcm}(\text{ord}(g(x)), \text{ord}(h(x))) = \text{lcm}(3, 7) = 21$. It follows that the impulse response sequence defined by the corresponding linear recurrence

$$a_5 = a_4 + a_0$$

has period 21. This can also be verified directly by computing the sequence

$$0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, \dots$$

Observe that $21 \notin D(2^k - 1)$ for $1 \leq k \leq 5$ which demonstrates that the containment in Theorem 3.3 is strict when $k = 5$ and $q = p = 2$.

4. LINEAR RECURRENCES AND PERIOD SETS OVER OTHER FINITE RINGS

Let q be a power of the prime p . The finite field \mathbb{F}_q can be constructed as a quotient $\mathbb{F}_p[t]/\langle f(t) \rangle$ where $f(t) \in \mathbb{F}_p[t]$ is irreducible. In this section, we consider sequences defined by linear recurrences over a broader class of finite commutative rings, some of which arise by weakening this assumption on $f(t)$.

Let $f(t) = \prod_{i=1}^r f_i(t)$ with $f_i(t) \in \mathbb{F}_p[t]$ monic and irreducible for $1 \leq i \leq r$. Define $\mathcal{R} = \mathbb{F}_p[t]/\langle f(t) \rangle$. If we assume that the factors $f_i(t)$ are pairwise distinct (hence relatively prime), then we can apply the Chinese Remainder Theorem to obtain a ring isomorphism

$$\mathcal{R} \cong \mathbb{F}_p/\langle f_1(t) \rangle \oplus \dots \oplus \mathbb{F}_p/\langle f_r(t) \rangle \cong \mathbb{F}_{p^{d_1}} \oplus \dots \oplus \mathbb{F}_{p^{d_r}}$$

where $d_i = \deg f_i(t)$ for $1 \leq i \leq r$. The induced projection π_i from \mathcal{R} onto the i th component $\mathbb{F}_p/\langle f_i(t) \rangle \cong \mathbb{F}_{p^{d_i}}$ is given explicitly by

$$g(t) + \langle f(t) \rangle \mapsto g(t) + \langle f_i(t) \rangle.$$

More generally, we will consider rings of the form $\mathcal{R} = \mathbb{F}_{q_1} \oplus \dots \oplus \mathbb{F}_{q_r}$ in which the finite fields in different components are not required to have the same characteristic.

Suppose we have a sequence $\mathbf{a} = (a_j)_{j=1}^{\infty}$ defined over such a ring \mathcal{R} . Applying the projection maps $\pi_i : \mathcal{R} \rightarrow \mathbb{F}_{q_i}$, we obtain r sequences $\pi_i(\mathbf{a}) := (\pi_i(a_j))_{j=1}^{\infty}$, each one defined over the corresponding component field \mathbb{F}_{q_i} . Conversely, given sequences $(a_j^{(i)})_{j=1}^{\infty}$ defined over \mathbb{F}_{q_i} for $1 \leq i \leq r$, we can form r -tuples to obtain a sequence $\mathbf{a} = (a_j^{(1)}, \dots, a_j^{(r)})_{j=1}^{\infty}$ defined over \mathcal{R} . The following lemma is easily verified.

Lemma 4.1. *The sequence \mathbf{a} is periodic if and only if $\pi_i(\mathbf{a})$ is periodic for all $1 \leq i \leq r$. When \mathbf{a} is periodic, we have*

$$\rho(\mathbf{a}) = \text{lcm}(\rho(\pi_1(\mathbf{a})), \dots, \rho(\pi_r(\mathbf{a}))).$$

Some straightforward algebraic manipulations show that the sequence \mathbf{a} is defined by a linear recurrence of degree k over \mathcal{R} if and only if this holds for all of the component sequences $\pi_i(\mathbf{a})$. The recurrence equations for the latter are obtained by simply applying the projection maps to the coefficients of the recurrence equation for \mathbf{a} .

We will continue to restrict attention to linear recurrence equations in which the lowest indexed coefficient c_0 is a unit. This condition holds for $c_0 \in \mathcal{R}$ if and only if $\pi_i(c_0)$ is a unit in \mathbb{F}_{q_i} for all i , equivalently $\pi_i(c_0) \neq 0$ for all i . Recall from Section 1 that sequences defined by such a linear recurrence of degree k over \mathcal{R} will be periodic with $\rho(\mathbf{a})$ bounded above by $|\mathcal{R}|^k - 1$. As we will see shortly, this upper bound on the period is not always attained.

Extending the period set notation introduced in the previous section and using the lemma and other observations above, we have the following result.

Lemma 4.2. *Let $\mathcal{R} = \mathbb{F}_{q_1} \oplus \dots \oplus \mathbb{F}_{q_r}$ and $k \geq 1$. Then*

$$P(k, \mathcal{R}) = \{\text{lcm}(\omega_1, \dots, \omega_r) \mid \omega_i \in P(k, \mathbb{F}_{q_i}) \text{ for } 1 \leq i \leq r\}.$$

Example 4.3. *Let $\mathcal{R} = \mathbb{F}_2 \oplus \mathbb{F}_3 \oplus \mathbb{F}_5$. First consider $k = 1$. Using Theorem 3.5, we see that:*

$$\begin{aligned} P(1, \mathbb{F}_2) &= D(1) = \{1\}. \\ P(1, \mathbb{F}_3) &= D(2) = \{1, 2\}. \\ P(1, \mathbb{F}_5) &= D(4) = \{1, 2, 4\}. \end{aligned}$$

It follows by Lemma 4.2 that

$$\begin{aligned} P(1, \mathcal{R}) &= \{\text{lcm}(\omega_1, \omega_2, \omega_3) \mid \omega_1 \in P(1, \mathbb{F}_2), \omega_2 \in P(1, \mathbb{F}_3), \omega_3 \in P(1, \mathbb{F}_5)\} \\ &= \{1, 2, 4\}. \end{aligned}$$

When $k = 2$,

$$\begin{aligned} P(2, \mathbb{F}_2) &= D(3) \cup 2D(1) = \{1, 2, 3\}. \\ P(2, \mathbb{F}_3) &= D(8) \cup 3D(2) = \{1, 2, 3, 4, 6, 8\}. \\ P(2, \mathbb{F}_5) &= D(24) \cup 5D(4) = \{1, 2, 3, 4, 5, 6, 8, 10, 12, 20, 24\}. \end{aligned}$$

By Lemma 4.2, we then have

$$\begin{aligned} P(2, \mathcal{R}) &= \{\text{lcm}(\omega_1, \omega_2, \omega_3) \mid \omega_1 \in P(2, \mathbb{F}_2), \omega_2 \in P(2, \mathbb{F}_3), \omega_3 \in P(2, \mathbb{F}_5)\} \\ &= \{1, 2, 3, 4, 5, 6, 8, 10, 12, 15, 20, 24, 30, 40, 60, 120\}. \end{aligned}$$

We will skip over $k = 3$ and $k = 4$ since our main point is to demonstrate how easily one can obtain the full period sets without doing a brute force enumeration of all possible combinations of linear recurrence equations and initial states. Even for $k = 2$, there are $8 \cdot 30 = 240$ choices for the coefficients (c_0, c_1) with c_0 a unit, and each of these can be paired with $30^2 = 900$ different initial states $s_0 = (a_0, a_1)$.

Remark 4.4. *By the Chinese Remainder Theorem, we have $\mathbb{F}_2 \oplus \mathbb{F}_3 \oplus \mathbb{F}_5 \cong \mathbb{Z}_{30}$ so the calculations in the preceding example can be viewed as determining the period sets for linear recurrences of small degree defined over \mathbb{Z}_{30} . More generally, the methods in this paper can be applied to find period sets of linear recurrences defined over \mathbb{Z}_n for any n that decomposes as a product of distinct prime numbers. The periods of sequences*

in the case where n includes nontrivial prime powers have also been investigated. We refer the reader to [7, 10] for more details.

We have the following upper bound on the periods of sequences defined over such rings.

Lemma 4.5. *Let $\mathcal{R} = \mathbb{F}_{q_1} \oplus \dots \oplus \mathbb{F}_{q_r}$ and $k \geq 1$. Let \mathbf{a} be a sequence defined by a linear recurrence of degree k over \mathcal{R} . Then*

$$\rho(\mathbf{a}) \leq \prod_{i=1}^r (q_i^k - 1).$$

Proof. We have $\rho(\mathbf{a}) = \text{lcm}(\omega_1, \dots, \omega_r) \leq \prod_{i=1}^r \omega_i$ with $\omega_i \in P(k, \mathbb{F}_{q_i})$ for $1 \leq i \leq r$. Since $\omega_i \leq q_i^k - 1$ for all i , the result follows. \square

One easy consequence of this upper bound is the following characterization of the fields among such rings. Note that $\mathcal{R} = \mathbb{F}_{q_1} \oplus \dots \oplus \mathbb{F}_{q_r}$ is not a field if $r > 1$ due to the presence of zero divisors.

Theorem 4.6. *Let $\mathcal{R} = \mathbb{F}_{q_1} \oplus \dots \oplus \mathbb{F}_{q_r}$ and $k \geq 1$. Among all sequences \mathbf{a} defined by linear recurrences of degree k over \mathcal{R} , the maximum period $|\mathcal{R}|^k - 1$ is achieved if and only if \mathcal{R} is a field ($r = 1$).*

Proof. By Corollary 2.10, the maximum can be achieved when \mathcal{R} is a field so the reverse implication holds. The forward implication follows from the preceding lemma by observing that if $r > 1$, then

$$\rho(\mathbf{a}) \leq \prod_{i=1}^r (q_i^k - 1) < \left(\prod_{i=1}^r q_i^k \right) - 1 = |\mathcal{R}|^k - 1$$

for all sequences \mathbf{a} defined by a linear recurrence of degree k over \mathcal{R} . \square

We have investigated the maximum periods for some families of rings that are not fields. One particularly simple family are those of the form $\mathcal{A}_n = \mathbb{F}_p[t]/\langle t^n - 1 \rangle$ for $n > 1$. These are also called *cyclic group algebras* since the elements of \mathcal{A}_n can be identified with formal linear combinations of the elements of a cyclic group of order n with coefficients in \mathbb{F}_p . The multiplication operation can then be viewed as arising by extending the group multiplication to such linear expressions in a natural way.

The factorization $t^n - 1 = (t - 1)(t^{n-1} + \dots + t + 1)$ immediately implies that \mathcal{A}_n is not a field for $n > 1$ and the maximum period for a linear recurrence sequence of degree k over \mathcal{A}_n must be strictly smaller than $|\mathcal{A}_n|^k - 1 = p^{nk} - 1$. (Note that the latter assertion holds even when $f(t)$ has repeated irreducible factors which occurs when p divides n .) Computer experiments show that there is a lot of variation in the maximum period. This is not surprising since it depends on the structure of \mathcal{A}_n which in turn depends on the factorization of $t^n - 1$ into irreducibles over \mathbb{F}_p as p varies. In general, it seems that the larger the number of factors of $t^n - 1$, the smaller

the maximum period, although we have not formulated a precise statement regarding this relationship.

We conclude with one general observation about the family $\{\mathcal{A}_n\}_{n=1}^\infty$. It is well known that if $n = \ell$ is a prime integer, then the cyclotomic polynomial $\Phi_\ell(t) = t^{\ell-1} + \dots + t + 1$ is irreducible over \mathbb{Q} . It follows from the Frobenius Density Theorem (see [9, pg 32] for more details on the latter), that $\Phi_\ell(t)$ remains irreducible when reduced modulo p for infinitely many primes p . For such p , we have $\mathcal{A}_\ell \cong \mathbb{F}_p \oplus \mathbb{F}_{p^{\ell-1}}$ and so the maximum period of linear recurrence sequences of degree k over \mathcal{A}_ℓ is at least $p^{(\ell-1)k} - 1 \approx \frac{1}{p^k}(|\mathcal{A}_\ell|^k - 1)$ in this case. This follows since there are sequences defined over the field $\mathbb{F}_{p^{\ell-1}}$ in the second component with period $p^{(\ell-1)k} - 1$ by Corollary 2.10.

REFERENCES

- [1] E. Berlekamp, *Algebraic Coding Theory*, revised edition, World Scientific Publishing, Singapore, 2015.
- [2] J. Gallian, *Contemporary Abstract Algebra*, 7th edition, Brooks Cole, 2009.
- [3] C. Guo, A. Koch, *Bounds for Fibonacci period growth*, *Involve*, Vol. 2, No. 2 (2009), 195–210.
- [4] S. Gupta, P. Rockstroh, F. E. Su, *Splitting Fields and Periods of Fibonacci Sequences Modulo Primes*, *Math. Magazine*, Vol. 85, No. 2, (2012), 130–135.
- [5] T. Judson, *Abstract Algebra: Theory and Applications*, 2017. Available online: <http://abstract.ups.edu>.
- [6] R. Lidl, H. Niederreiter, *Finite Fields*, *Encyclopedia of Mathematics and Its Applications*, Vol. 20, Cambridge University Press, 1997.
- [7] R. G. E. Pinch, *Recurrent sequences modulo prime powers*, in: M. Ganley (ed.), *Cryptography and Coding III*, *Proceedings 3rd IMA conference on cryptography and coding*, Cirencester, December 1991, IMA Conference Series, vol. 45, Oxford University Press, 1993.
- [8] D. Quijada, *Periods of Linearly Recurring Sequences*, Honors Thesis, Washington and Lee University, 2015. Available at: <https://repository.wlu.edu/handle/11021/32172>
- [9] P. Stevenhagen, H. W. Lenstra, Jr., *Chebotarëv and his Density Theorem*, *Math. Intelligencer* **18** (1996), 26–37.
- [10] M. Ward, *The Arithmetical Theory of Linear Recurring Series*, *Trans. Amer. Math. Soc.* **35** (1933), 600–628.

DEPARTMENT OF MATHEMATICS, WASHINGTON AND LEE UNIVERSITY, 204 W. WASHINGTON ST., LEXINGTON, VA 24450, USA.

E-mail address: bushm@wlu.edu

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF SOUTHERN CALIFORNIA, 3620 S. VERMONT AVE., KAP 104, LOS ANGELES, CA 90089-2532, USA.

E-mail address: dquijada@usc.edu