PURELY PERIODIC SECOND ORDER LINEAR RECURRENCES

THOMAS MCKENZIE AND SHANNON OVERBAY

Abstract. Second order linear homogeneous recurrence relations with coefficients in a finite field or in the integers modulo of an ideal have been the subject of much study (see for example [1, 2, 4, 5, 6, 7, 8, 9]). This paper extends many of these results to finite rings. In the first part of this paper we develop polynomials which generate purely periodic sequences over any finite ring, R. We then use these polynomials with coefficients in R to establish bounds on the period of these sequences.

1. Introduction

Throughout this paper R is a finite commutative ring with identity. We assume that a ring and its subrings share the same identity. Let $\mathbb{Z}$ denote the integers, $\mathbb{N}$ denote the nonnegative integers, and $\mathbb{Z}^+$ denote the positive integers.

A sequence $\mathbf{s} = \{s_0, s_1, \ldots\}$ of elements in R is purely periodic with period $n \in \mathbb{Z}^+$, if n is the smallest positive integer with $s_{n+i} = s_i$ for all $i \in \mathbb{N}$. If $\mathbf{s}$ is purely periodic with period n then $\mathbf{s}$ is said to be uniformly distributed if for every $r \in R$, the cardinality of $\{i \in \mathbb{N} | s_i = r, 0 \leq i \leq n-1\}$ equals n divided by the order of R.

For $n \in \mathbb{Z}^+$ we call $\mathbf{s}$ an nth order linear homogeneous recurrence relation if there exist $a_1, \ldots, a_n \in R$ with $a_n \neq 0$ such that

$$s_{i+n} = a_n s_i + a_{n-1} s_{i+1} + \cdots + a_1 s_{i+n-1}$$

for all $i \in \mathbb{N}$.

The aim of this section is to establish a relationship between purely periodic nth order linear homogeneous recurrence relations and the coefficients of certain polynomials. In the next theorem we use the division algorithm to create an nth order linear recurrence.

Theorem 1.1. *Let $f(x) = a_n x^n + \cdots + a_1 x - 1 \in R[x]$ where $n \in \mathbb{Z}^+$ and $a_n \neq 0$. Suppose that there exists $h(x) \in R[x]$ with degree at most $n-1$ and $m \in \mathbb{Z}^+$ such that $m \geq n$ and $f(x)$ divides $h(x) \cdot (x^m - 1)$ in $R[x]$. Now let $\sum_{j=0}^{m-1} c_j x^j \in R[x]$ such that $h(x) \cdot (x^m - 1) = (\sum_{j=0}^{m-1} c_j x^j) \cdot f(x)$ and define $\mathbf{s} = \{s_0, s_1, \ldots\}$ as the sequence given by $s_i = c_j$ where $i \cong j$ modulo m. Then $\mathbf{s}$ is a purely periodic nth order linear recurrence given by*

$$s_{i+n} = a_n s_i + a_{n-1} s_{i+1} + \cdots + a_1 s_{i+n-1}$$

for all $i \in \mathbb{N}$.

Proof. Let $i \in \mathbb{N}$ and let $g(x) = \sum_{j=0}^{m-1} c_j x^j$. Note that $f(x) \cdot g(x) = h(x) \cdot (x^m - 1)$ and $g(x) x^{mk} = s_{mk} x^{mk} + \cdots + s_{m(k+1)-1} x^{m(k+1)-1}$. Use the division algorithm to write $i + n$ as $mq + r$ where $q, r \in \mathbb{Z}$ and $0 \leq r < m$.

Now

$$\begin{aligned}
&f(x)\cdot(s_{qm}x^{qm}+s_{qm-1}x^{qm-1}+\cdots+s_1x+s_0)\\
&=f(x)\cdot(x^{qm}g(x)+x^{(q-1)m}g(x)+\cdots+g(x))\\
&=x^{qm}f(x)g(x)+x^{(q-1)m}f(x)g(x)+\cdots+f(x)g(x)\\
&=x^{qm}h(x)(x^m-1)+x^{(q-1)m}h(x)(x^m-1)+\cdots+h(x)(x^m-1)\\
&=x^{(q+1)m}h(x)-x^{qm}h(x)+x^{qm}h(x)-\cdots-h(x)\\
&=x^{(q+1)m}h(x)-h(x).
\end{aligned}$$

Since $0\le n-1<i+n<(q+1)m$, the coefficient of x^{i+n} in the expansion above equals zero. In other words,

$$(a_ns_i+a_{n-1}s_{i+1}+\cdots+a_1s_{i+n-1}-s_{i+n})x^{i+n}=0.$$

Hence, $s_{i+n}=a_ns_i+a_{n-1}s_{i+1}+\cdots+a_1s_{i+n-1}$ for all $i\in\mathbb{N}$. This completes the proof. □

Example 1.2. *Assume for the moment that $R=\mathbb{Z}/(5\mathbb{Z})$. Let $f(x)=x^2+4x-1$ and $h(x)=x$. Note that $f(x)$ divides $x(x^{20}-1)$ and*

$$\begin{aligned}
\frac{h(x)\cdot(x^{20}-1)}{f(x)}&=\sum_{j=0}^{20-1}c_jx^j\\
&=0+1x+4x^2+2x^3+2x^4+0x^5+2x^6+3x^7\\
&\quad+4x^8+4x^9+0x^{10}+4x^{11}+1x^{12}+3x^{13}+3x^{14}\\
&\quad+0x^{15}+3x^{16}+2x^{17}+1x^{18}+1x^{19}.
\end{aligned}$$

If we let $s_0=0,s_1=1$, and $s_{i+2}=s_i+4s_{i+1}$, then for all $i\in\mathbb{N},s_i=c_j$ where i is congruent to j modulo 20. Note that this purely periodic sequence is uniformly distributed.

In Theorem 1.1 we took polynomials and produced a purely periodic sequence. In the next theorem we reverse that process. The reader should note the similarity between this next theorem and Theorem 6.25 on page 197 of Lidl and Niederreiter [4]. Although this result in Lidl and Niederreiter is stated for finite fields, the proof actually works over more general rings.

Theorem 1.3. *Suppose $\mathbf{s}=\{s_0,s_1,\ldots\}$ is a purely periodic nth order recurrence in R with period $m\ge n$. That is, there exist $a_1,\ldots,a_n\in R$ with $a_n\neq0$ such that, for all $i\in\mathbb{N}$,*

$$s_{i+n}=a_ns_i+a_{n-1}s_{i+1}+\cdots+a_1s_{i+n-1}.$$

Let

$$f(x)=a_nx^n+\cdots+a_1x-1$$

and

$$h(x)=\sum_{j=0}^{n-1}-(a_js_0+a_{j-1}s_1+\cdots+a_2s_{j-2}+a_1s_{j-1}-s_j)x^j.$$

Then $h(x)\cdot(x^m-1)=(\sum_{j=0}^{m-1}s_jx^j)\cdot f(x)$.

Proof. Clearly the polynomials $f(x)\cdot\sum_{j=0}^{m-1} s_j x^j$ and $h(x)\cdot(x^m-1)$ both have degree $m+n-1$. It suffices to check that these polynomials are equal term by term. Let $i \in \{0,\ldots,m+n-1\}$.

Case 1 ($i < n$): In this case the coefficient of x^i in $f(x)\cdot\sum_{j=0}^{m-1} s_j x^j$ equals $a_i s_0 + a_{i-1}s_1 + \cdots + a_2 s_{i-2} + a_1 s_{i-1} - s_i$ which equals the coefficient of x^i in $-h(x)$. Since $i < n < m$, the coefficient of x^i in $h(x)\cdot(x^m-1)$ is equal to the coefficient of x^i in $-h(x)$.

Case 2 ($n \le i \le m-1$): In this case the coefficient of x^i in $h(x)\cdot(x^m-1)$ is equal to zero, since the degree of $h(x)$ is $n-1$. The coefficient of x^i in $f(x)\cdot\sum_{j=0}^{m-1} s_j x^j$ equals $a_n s_{i-1} + a_{n-1}s_{i-n+1} + a_{n-2}s_{i-n+2} + \cdots + a_1 s_{i-1} - s_i$. This is also equal to zero by the recurrence relation.

Case 3 ($m \le i \le m+n-1$): In this case the coefficient of x^i in $f(x)\cdot\sum_{j=0}^{m-1} s_j x^j$ equals $a_n s_{i-n} + a_{n-1}s_{i-n+1} + a_{n-2}s_{i-n+2} + \cdots + a_{i-m+1}s_{m-1}$ equals $-(a_{i-m}s_m + a_{i-m-1}s_{m+1} + \cdots + a_1 s_{i-1} - s_i)$ (by the recurrence relation) equals $-(a_{i-m}s_0 + a_{i-m-1}s_1 + \cdots + a_1 s_{i-1-m} - s_{i-m})$ (since $\mathbf{s}$ is periodic) equals the coefficient of x^i in $x^m\cdot h(x)$ equals the coefficient of x^i in $(x^m-1)\cdot h(x)$ (since $n-1 \le m \le i$). □

2. Purely Periodic Second Order Linear Recurrences

Throughout this section let $\mathbf{s} = \{s_0, s_1, \ldots\}$ be the sequence in R generated by second order linear recurrence relation $s_{i+2} = a_2 s_i + a_1 s_{i+1}$ for all $i \in \mathbb{N}$ where $a_1 \in R$ and a_2 is a unit in R. The polynomial $g(x) = x^2 - a_1 x - a_2$ is the characteristic polynomial associated to this recurrence.

In this section we establish a formula for s_n in terms of the roots of the characteristic polynomial. We then use this formula to give an upper bound for the period of $\mathbf{s}$.

Theorem 2.1. *There exists a ring S which contains R as a subring, an element $r_1 \in S$, and an element $r_2 \in R[r_1]$ such that*

$$g(x) = x^2 - a_1 x - a_2 = (x - r_1)(x - r_2).$$

Proof. Let $S = R[x]/(g(x))$ and let r_1 be the element $x + (g(x)), \in S$. Note that R is a subring of S and $g(r_1) = 0$. By the division algorithm on page 158 of [3], there exists a polynomial $h(x)$ with coefficients in $R[r_1]$ and element c in $R[r_1]$ such that

$$g(x) = (x - r_1)h(x) + c$$

in $R[r_1][x]$. Plugging r_1 into both sides of this equation and recalling that $g(r_1) = 0$ yields $c = 0$ and $g(x) = (x - r_1)h(x)$. Since $g(x)$ is a monic polynomial of degree two and $(x - r_1)$ is a monic polynomial of degree one, it follows that there exists $r_2 \in R[r_1]$ such that $h(x) = (x - r_2)$ and $g(x) = (x - r_1)(x - r_2)$. □

Consider a ring S which contains R as a subring with elements $r_1, r_2 \in S$ such that $g(x) = x^2 - a_1 x - a_2 = (x - r_1)(x - r_2)$. Since $r_1 r_2 = -a_2$, and a_2 was assumed to be a unit in R, it follows that r_1 and r_2 are units in S. Now r_1 is integral over R and thus by Theorem 5.3 on page 395 of [3], $R[r_1]$ is a finitely generated R module. This, along with the fact that R is a finite ring, implies that the units of $R[r_1]$ form a finite group. We use $|r_1|, |r_2| \in \mathbb{Z}^+$ to denote the orders of r_1 and r_2 in this group. Hence, $r_1^{|r_1|} = r_2^{|r_2|} = 1_R$.

Recall that $g(x) = x^2 - a_1 x - a_2$ is the characteristic polynomial corresponding to the recurrence $s_{i+2} = a_2 s_i + a_1 s_{i+1}$.

Theorem 2.2. *Let S be a ring which contains R as a subring and let $r_1, r_2 \in S$ such that $g(x) = (x - r_1)(x - r_2)$. Then for $n \geq 1$,*

$$s_n = s_0 r_1^n + (s_1 - s_0 r_1) \sum_{j=0}^{n-1} r_1^j r_2^{n-j-1}.$$

Proof. We proceed by induction on n. If $n = 1$ then

$$s_0 r_1^1 + (s_1 - s_0 r_1) \sum_{j=0}^{0} r_1^j r_2^{n-j-1} = s_0 r_1^1 + (s_1 - s_0 r_1) = s_1.$$

When $n = 2$ we have

$$\begin{aligned} s_0 r_1^2 + (s_1 - s_0 r_1) \sum_{j=0}^{2-1} r_1^j r_2^{2-j-1} &= s_0 r_1^2 + (s_1 - s_0 r_1)(r_1 + r_2) \\ &= (r_1 + r_2) s_1 + s_0(-r_1 r_2) \\ &= a_1 s_1 + a_2 s_0 \\ &= s_2. \end{aligned}$$

Now let k be an integer greater than 2 and assume that the equality holds for all integers n greater than zero and less than k. We show the equality holds for $n = k$. Note that

$$\begin{aligned} s_k &= a_1 s_{k-1} + a_2 s_{k-2} \\ &= a_1 \Big(s_0 r_1^{k-1} + (s_1 - s_0 r_1) \sum_{j=0}^{k-1-1} r_1^j r_2^{k-1-j-1} \Big) \\ &\quad + a_2 \Big(s_0 r_1^{k-2} + (s_1 - s_0 r_1) \sum_{j=0}^{k-2-1} r_1^j r_2^{k-2-j-1} \Big) \\ &= (r_1 + r_2) \Big(s_0 r_1^{k-1} + (s_1 - s_0 r_1) \sum_{j=0}^{k-1-1} r_1^j r_2^{k-1-j-1} \Big) \\ &\quad + (-r_1 r_2) \Big(s_0 r_1^{k-2} + (s_1 - s_0 r_1) \sum_{j=0}^{k-2-1} r_1^j r_2^{k-2-j-1} \Big) \\ &= r_1 \Big(s_0 r_1^{k-1} + (s_1 - s_0 r_1) \sum_{j=0}^{k-1-1} r_1^j r_2^{k-1-j-1} \Big) \\ &\quad + r_2 \Big(s_0 r_1^{k-1} + (s_1 - s_0 r_1) \sum_{j=0}^{k-1-1} r_1^j r_2^{k-1-j-1} \Big) \\ &\quad + (-r_1 r_2) \Big(s_0 r_1^{k-2} + (s_1 - s_0 r_1) \sum_{j=0}^{k-2-1} r_1^j r_2^{k-2-j-1} \Big) \end{aligned}$$

$$
\begin{aligned}
&= s_0 r_1^k + (s_1 - s_0 r_1) \sum_{j=0}^{k-1-1} r_1^{j+1} r_2^{k-1-j-1} \\
&\quad + s_0 r_1^{k-1} r_2 + (s_1 - s_0 r_1) \sum_{j=0}^{k-1-1} r_1^j r_2^{k-j-1} \\
&\quad - s_0 r_1^{k-1} r_2 - (s_1 - s_0 r_1) \sum_{j=0}^{k-2-1} r_1^{j+1} r_2^{k-j-2} \\
&= s_0 r_1^k + (s_1 - s_0 r_1)\Big(r_1^{k-1} + \sum_{j=0}^{k-2} r_1^j r_2^{k-j-1}\Big) \\
&= s_0 r_1^k + (s_1 - s_0 r_1) \sum_{j=0}^{k-1} r_1^j r_2^{k-j-1}.
\end{aligned}
$$

□

We did not use the fact that R is finite or the fact that a_2 is a unit in the proof of the last theorem. The result even holds when $r_1 - r_2$ is a zero divisor. If we set r_1 equal to r_2 in the last theorem we get our next result.

Corollary 2.3. *Let S be a ring which contains R as a subring and let $r \in S$ such that $g(x) = (x - r)^2$. Then for $k \geq 1$,*

$$s_k = s_0(1 - k)r^k + s_1 k r^{k-1}.$$

Write n_R for the characteristic of the finite ring R.

Theorem 2.4. *Let S be a ring which contains R as a subring and let $r_1, r_2 \in S$ such that $g(x) = (x - r_1)(x - r_2)$. Let λ be the least common multiple or $|r_1|$ and $|r_2|$. Then* **s** *is purely periodic with period dividing $\lambda \cdot n_R$.*

Proof. Let $m = \lambda \cdot n_R$ and let $k \in \mathbb{N}$. Then

$$
\begin{aligned}
s_{m+k} &= s_0 r_1^{m+k} + (s_1 - s_0 r_1) \sum_{j=0}^{m+k-1} r_1^j r_2^{m+k-j-1} \\
&= s_0 r_1^{m+k} + (s_1 - s_0 r_1) \sum_{j=0}^{m-1} r_1^j r_2^{m+k-j-1} \\
&\quad + (s_1 - s_0 r_1) \sum_{j=m}^{m+k-1} r_1^j r_2^{m+k-j-1} \\
&\quad \Big(\text{where } \sum_{j=m}^{m+k-1} r_1^j r_2^{m+k-j-1} = 0 \text{ if } k = 0\Big) \\
&= s_0 r_1^m r_1^k + (s_1 - s_0 r_1) r_1^m \sum_{j=0}^{k-1} r_1^j r_2^{k-j-1}
\end{aligned}
$$

$$
\begin{aligned}
&+ (s_1 - s_0 r_1) \sum_{j=0}^{m-1} r_1^j r_2^{m+k-j-1} \\
&= s_0 r_1^k + (s_1 - s_0 r_1) \sum_{j=0}^{k-1} r_1^j r_2^{k-j-1} \\
&\quad + (s_1 - s_0 r_1) \sum_{j=0}^{m-1} r_1^j r_2^{m+k-j-1} (\text{ since } r_1^\lambda = 1) \\
&= s_0 r_1^k + (s_1 - s_0 r_1) \sum_{j=0}^{k-1} r_1^j r_2^{k-j-1} + (s_1 - s_0 r_1) \Big(\sum_{j=0}^{\lambda-1} r_1^j r_2^{m+k-j-1} \\
&\quad + \sum_{j=\lambda}^{2\lambda-1} r_1^j r_2^{m+k-j-1} + \ldots + \sum_{j=\lambda(n_R-1)}^{m-1} r_1^j r_2^{m+k-j-1} \Big) \\
&= s_0 r_1^k + (s_1 - s_0 r_1) \sum_{j=0}^{k-1} r_1^j r_2^{k-j-1} \\
&\quad + (s_1 - s_0 r_1) \Big(n_R \cdot \sum_{j=0}^{\lambda-1} r_1^j r_2^{m+k-j-1} \Big) \quad (\text{since } r_1^\lambda = r_2^\lambda = 1) \\
&= s_0 r_1^k + (s_1 - s_0 r_1) \sum_{j=0}^{k-1} r_1^j r_2^{k-j-1} = s_k.
\end{aligned}
$$

□

Acknowledgment

We would like to thank the referee for a very careful reading of this paper and for many valuable suggestions.

References

[1] R. T. Bumby, *A Distribution Property for Linear Recurrences of the Second Order*, Proc. American Mathematical Society, **50** (1975), 101–106.
[2] J. R. Burke, *Some Remarks on the Distribution of Second Order Recurrences and a Related Group Structure*, Applications of Fibonacci Numbers, **6** (1996), 47–52.
[3] T. Hungerford, *Algebra*, Springer, New York, 1974.
[4] R. Lidl and H. Niederreiter, *Introduction to Finite Fields and Their Applications*, Cambridge University Press, Cambridge, 1986.
[5] W. Narkiewicz, *Uniform Distribution of Sequences of Integers in Residue Classes*, Lecture Notes in Math. 1087, Springer, Berlin, 1984.
[6] M. Nathanson, *Linear Recurrences and Uniform Distribution*, Proc. American Mathematical Society, **48** (1975), 289–291.
[7] H. Niederreiter and J.-S. Shiue, *Equidistribution of Linear Recurring Sequences in Finite Fields*, Indag. Math., **80** (1977), 397–405.
[8] W. Valez, *Uniform Distribution of Two-Term Recurrence Sequences*, Trans. American Mathematical Society, **301** (1987), 37–45.
[9] W. A. Webb and C. T. Long, *Distribution Modulo p of the General Second Order Recurrence*, Atti Accad. Lincei, **58** (1975), 92–100.

MSC2000: 11B37, 11B50

Department of Mathematics, Gonzaga University, Spokane, WA 99258
E-mail address: mckenzie@gonzaga.edu

Department of Mathematics, Gonzaga University, Spokane, WA 99258
E-mail address: overbay@gonzaga.edu