THE RANK AND PERIOD OF A LINEAR RECURRENT SEQUENCE OVER A RING

DONALD W. ROBINSON
Brigham Young University, Provo, Utah 84602

INTRODUCTION

Two problems from the theory of linear recurrent sequences are considered in this paper. The first is to establish the existence of the rank of the Lucas sequence over an arbitrary ring with an identity. In particular, a theorem of Wyler [10, Theorem 1], for second-order sequences over a commutative ring, is generalized to sequences of arbitrary order over an arbitrary (not necessarily commutative) ring. The second problem is to determine the period of a purely periodic Lucas sequence as a function of its rank. Solutions to this problem have previously been given in special cases: Vinson [7, Theorem 3] and Barner [1, Theorem 2] for the modular Fibonacci sequence; Ward [9] for modular integral sequences of arbitrary order in case the characteristic polynomial of the recurrence has distinct roots; and Wyler [10, Theorem 4] for second-order sequences over a commutative ring with odd prime power characteristic. A solution is given in the present paper for linear recurrent sequences of arbitrary order over an arbitrary commutative ring with an identity.

1. PERIODIC LINEAR RECURRENT SEQUENCES

Let R be an associative ring with an identity 1, and let $a_1, \cdots, a_k$ be elements of R. A sequence (w): $w_0, w_1, \cdots$ of elements in R that satisfy the recurrence

$$w_{n+k} = w_{n+k-1}a_1 + \cdots + w_n a_k$$

for $n \geq 0$ is said to be a (right) linear recurrent sequence associated with the list $(a_1, \cdots, a_k)$. Let $S(a_1, \cdots, a_k)$ be the collection of all linear recurrent sequences over R associated with $(a_1, \cdots, a_k)$ and let

$$A = \begin{pmatrix} 0 & 0 & \cdots & 0 & a_k \\ 1 & 0 & \cdots & 0 & a_{k-1} \\ & & \cdots & & \\ 0 & 0 & \cdots & 1 & a_1 \end{pmatrix} \in R^{k\times k}$$

be the companion matrix of $(a_1, \cdots, a_k)$.

The *Lucas sequence* of $S(a_1, \cdots, a_k)$ is the sequence (u): $u_0, u_1, \cdots$ associated with the list $(a_1, \cdots a_k)$ such that $u_0 = 0, \cdots, u_{k-2} = 0, u_{k-1} = 1$. (In case $k = 1$, then $u_0 = 1$). For n a non-negative integer and $\epsilon_k = (0, \cdots, 0, 1) \in R^k$, let $U_n \in R^{k\times k}$ be the matrix with $\epsilon_k A^{i-1+n}$ as its i^{th} row, $i = 1, \cdots, k$. Since the rows of U_0 are of the form $\epsilon_k = 0, \cdots, 0, 1)$, $\epsilon_k A = (0, \cdots, 1, *), \cdots, \epsilon_k A^{k-1} = (1, *, \cdots, *)$, then U_0 is invertible in $R^{k\times k}$.

Lemma 1. Let $(w) \in S(a_1, \cdots, a_k)$. Then for $n \geq 0$,

$$(w_n, \cdots, w_{n+k-1}) = (w_0, \cdots, w_{k-1})A^n = (w_0, \cdots, w_{k-1})U_0^{-1}U_n.$$

Proof. By finite induction on n, both the first equality and $U_n = U_0A^n$ are valid. Thus, since U_0 is invertible, then $A^n = U_0^{-1}U_n$, and the second equality holds.

Let $(w) \in S(a_1, \cdots, a_k)$. If there is a list of k consecutive elements of (w) that is equal to a preceding list of k consecutive elements of (w), then the sequence is said to be of finite period. Specifically, if

$$(w_{\alpha+\nu}, \cdots, w_{\alpha+\nu+k-1}) = (w_\alpha, \cdots, w_{\alpha+k-1}),$$

with $\alpha + \nu > \alpha \geq 0$, is the first such list, then $w_\alpha, w_{\alpha+1}, \cdots$ is periodic of period ν. In this case (w) is said to be periodic of index α and period ν. If the index $\alpha = 0$, then (w) is said to be purely periodic.

Similarly, the matrix A is said to be periodic if some term of the sequence $I, A, A^2, \cdots$ is equal to a preceding term.

If $A^{\alpha+\nu} = A^{\alpha}$, $\alpha+\nu > \alpha \geqslant 0$, is the first such term, then A is said to be periodic of index α and period ν.

Lemma 2. The following statements are equivalent:

(i) Every sequence of $S(a_1, \cdots, a_k)$ is periodic.

(ii) The Lucas sequence of $S(a_1, \cdots, a_k)$ is periodic.

(iii) A is periodic.

Proof. (i) $\Rightarrow$ (ii) is trivial.

(ii) $\Rightarrow$ (iii). Let (u) be periodic. Then

$$U_{\alpha+\nu} = U_{\alpha}, \qquad \alpha+\nu > \alpha \geqslant 0.$$

Hence,

$$U_0 A^{\alpha+\nu} = U_0 A^{\alpha} \qquad \text{and} \qquad A^{\alpha+\nu} = A^{\alpha}.$$

That is, A is periodic.

(iii) $\Rightarrow$ (i). Let

$$A^{\alpha+\nu} = A^{\alpha}, \qquad \alpha+\nu > \alpha \geqslant 0.$$

Then

$$(w_{\alpha+\nu}, \cdots, w_{\alpha+\nu+k-1}) = (w_{\alpha}, \cdots, w_{\alpha+k-1}),$$

and (w) is periodic.

It is clear that the index of (w) is at most the index of A and that the period of (w) divides the period of A. Moreover, the index and period of the Lucas sequence are, respectively, the index and period of A.

Lemma 3. Let the Lucas sequence of $S(a_1, \cdots, a_k)$ be periodic. Then the following statements are equivalent:

(i) Every sequence of $S(a_1, \cdots, a_k)$ is purely periodic.

(ii) The Lucas sequence of $S(a_1, \cdots, a_k)$ is purely periodic.

(iii) a_k is right invertible in R.

(iv) a_k is not a right zero divisor in R.

Proof. (i) $\Rightarrow$ (ii) and (iii) $\Rightarrow$ (iv) are trivial.

(ii) $\Rightarrow$ (iii). Let the Lucas sequence $(u) \in S(a_1, \cdots, a_k)$ be purely periodic. Then $U_{\nu} = U_0$ for $\nu > 0$. That is,

$$A^{\nu} = U_0^{-1} U_{\nu} = I.$$

If $[c_{ij}] = A^{\nu-1}$, then by direct calculation, $a_k c_{k,1} = 1$, and a_k is right invertible.

(iv) $\Rightarrow$ (i). Since (u) is periodic, then by Lemma 2, every $(w) \in S(a_1, \cdots, a_k)$ is periodic. Let

$$(w_0, \cdots, w_{k-1}) A^{\alpha+\nu} = (w_0, \cdots, w_{k-1}) A^{\alpha}, \qquad \alpha+\nu > \alpha \geqslant 0.$$

Also since a_k is not a right zero divisor, then A is right cancellable. Indeed, suppose $BA = 0$. Since

$$A^k = Ia_k + Aa_{k-1} + \cdots + A^{k-1} a_1,$$

then $Ba_k = 0$ and $B = 0$. Therefore,

$$(w_0, \cdots, w_{k-1}) A^{\nu} = (w_0, \cdots, w_{k-1})$$

and (w) is purely periodic.

Reference is made at this point to DeCarli [4]; the main result given there follows immediately from Lemma 3.

2. THE RANK OF THE LUCAS SEQUENCE

A result of Wyler [8, Theorem 1], for second-order recurrences over a commutative ring, is now extended.

Theorem 1. Let $(u) \in S(a_1, \cdots, a_k)$ be the Lucas sequence, and suppose a_k is not a right zero divisor in R. Then there exists a unique non-negative integer ρ such that $u_n = 0, \cdots, u_{n+k-2} = 0$ if and only if n is a multiple of ρ. If $\rho = 0$, then (u) is not periodic. If $\rho > 0$, then (u) is periodic if and only if $u_{\rho+k-1}$ is of finite order in the unit group of R.

Proof. First, a matrix characterization of the condition $u_n = 0, \cdots, u_{n+k-2} = 0$ is provided. Specifically, suppose $u_n = 0, \cdots, u_{n+k-2} = 0$. Then

$$u_{n+k-1}\epsilon_k = (0, \cdots, 0, u_{n+k-1}) = \epsilon_k A^n, \quad \text{and} \quad u_{n+k-1}\epsilon_k A^i = \epsilon_k A^n A^i = \epsilon_k A^i A^n$$

for $i = 0, \cdots, k-1$. Therefore, $u_{n+k-1}U_0 = U_0A^n$. On the other hand, if $tU_0 = U_0A^n$ for some $t \in R$, then by checking the first row of this matrix, $u_n = 0, \cdots, u_{n+k-2} = 0$ and $u_{n+k-1} = t$. Consequently, $u_n = 0, \cdots, u_{n+k-2} = 0$ if and only if $A^n = U_0^{-1}tU_0$ for some $t \in R$; and in this case $t = u_{n+k-1}$.

Second, if $A^n = U_0^{-1}tU_0$, then t is not a right zero divisor in R. Indeed, suppose $vt = 0$ for $v \in R$. Then

$$vU_0A^n = vtU_0 = 0.$$

Since a_k is not a right zero divisor in R, then as in the proof of Lemma 3, A is right cancellable, $vU_0 = 0$ and $v = 0$.

The existence of ρ is now demonstrated. If $u_n = 0, \cdots, u_{n+k-2} = 0$ implies $n = 0$, then choose $\rho = 0$. In this case, by Lemma 3, the Lucas sequence (u) is not periodic. Thus, suppose $u_n = 0, \cdots, u_{n+k-2} = 0$ for some $n > 0$, and let ρ be the least such n. (If $k = 1$, then the condition is satisfied vacuously for every positive n and $\rho = 1$.) We show that every such n is a multiple of ρ. Indeed, let $A^\rho = U_0^{-1}sU_0$ with $s = u_{\rho+k-1}$. Then

$$A^{\rho q} = U_0^{-1}s^qU_0 \qquad \text{and} \qquad u_{\rho q} = 0, \cdots, u_{\rho q+k-2} = 0.$$

On the other hand, suppose

$$A^n = U_0^{-1}tU_0, \quad t \in R, \quad n = \rho q + \lambda, \quad 0 \leqslant \lambda < \rho.$$

Then

$$U_0^{-1}tU_0 = A^n = A^\lambda A^{\rho q} = A^\lambda U_0^{-1}s^qU_0,$$

where s^q is not a right zero divisor. Define

$$[d_{ij}] = D = U_0A^\lambda U_0^{-1}.$$

Then $Ds^q = It$. Since $d_{ij}s^q = 0$ for $i \neq j$, then $d_{ij} = 0$ for $i \neq j$. Also since

$$d_{ii}s^q = t = d_{11}s^q,$$

then $d_{ii} = d_{11} = d$, say, $i = 1, \cdots, k$. That is, $D = Id$ and $A^\lambda = U_0^{-1}dU_0$. Hence, by definition of ρ, it follows that $\lambda = 0$ and $n = \rho q$. That is, the desired ρ exists and is unique.

Finally, the last statement of the theorem is demonstrated. Indeed, if $s^q = 1$, then $A^{\rho q} = U_0^{-1}s^qU_0 = I$ and, by Lemma 2, (u) is periodic. Conversely, if (u) is periodic, then it is purely periodic and $A^\nu = I, \nu > 0$. Therefore, $A^\nu = U_0^{-1}IU_0$ and $\nu = \rho q$ for some q. Consequently,

$$I = A^{\rho q} = U_0^{-1}s^qU_0, \qquad Is^q = I,$$

$s^q = 1$, and $s = u_{\rho+k-1}$ is of finite order in the unit group of R.

The non-negative integer ρ of Theorem 1 is called the *rank* of the Lucas sequence associated with $(a_1, \cdots, a_k)$.

Corollary 1. Suppose a_k is not a right zero divisor in R. Let ρ be the rank of the Lucas sequence $(u) \in S(a_1, \cdots, a_k)$, and let $(w) \in S(a_1, \cdots, a_k)$. If $w_0 = 0$, then $w_\rho = 0$.

Proof. Let $\epsilon_1 = (1, 0, \cdots, 0) \in R^k$ and $\epsilon_k = (0, \cdots, 0, 1) \in R^k$. Since $\epsilon_k' = U_0\epsilon_1'$, where the prime denotes transpose, then $U_0^{-1}\epsilon_k' = \epsilon_1'$. Therefore,

$$A^\rho\epsilon_1' = U_0^{-1}u_{\rho+k-1}U_0\epsilon_1' = U_0^{-1}u_{\rho+k-1}\epsilon_k' = U_0^{-1}\epsilon_k'u_{\rho+k-1} = \epsilon_1'u_{\rho+k-1},$$

and

$$w_\rho = (w_\rho, \cdots, w_{\rho+k-1})\epsilon_1' = (w_0, \cdots, w_{k-1})A^\rho\epsilon_1' = (w_0, \cdots, w_{k-1})\epsilon_1'u_{\rho+k-1} = w_0u_{\rho+k-1}.$$

Consequently, if $w_0 = 0$, then $w_\rho = 0$. (Compare [3, Theorem 1].)

3. RELATIONS BETWEEN THE RANK AND PERIOD

In this section R is a *commutative* ring with identity 1. Also, (x,y) and $[x,y]$ denote the greatest common divisor and least common multiple of the positive integers x and y.

Theorem 2. Suppose a_k is not a zero divisor in R. Let the Lucas sequence $(u) \in S(a_1, \cdots, a_k)$ be of rank $\rho > 0$. Then (u) is periodic if and only if a_k is of finite order in the unit group of R. In this case, let ν be the period of (u), and let δ and β be the orders of $(-1)^{k-1}$ and $u_{\rho+k-1}$, respectively, in the unit group of R. Then

(i) $\nu = \rho\beta = (k, \beta)[\delta, \rho]$.

(ii) (k,β) is the order of $u_{\rho+k-1}^{[\delta,\rho]/\rho}$.

Proof. Since R is commutative, then

$$A^{\rho} = U_0^{-1}u_{\rho+k-1}U_0 = u_{\rho+k-1}I \qquad \text{and} \qquad ((-1)^{k-1}a_k)^{\rho} = \det A^{\rho} = (u_{\rho+k-1})^k .$$

Therefore, a_k is of finite order if and only if $u_{\rho+k-1}$ is of finite order. Consequently, by Theorem 1, (u) is periodic if and only if a_k is of finite order.

Now, suppose (u) is periodic of period ν, and let δ and β be the orders of $(-1)^{k-1}a_k$ and $u_{\rho+k-1}$, respectively, in the unit group of R. Since

$$I = A^{\nu} = (A^{\rho})^{\nu/\rho} = (u_{\rho+k-1}I)^{\nu/\rho},$$

then $\beta \mid \nu/\rho$. On the other hand since

$$A^{\rho\beta} = (u_{\rho+k-1}I)^{\beta} = I,$$

then $\nu \mid \rho\beta$. Therefore, $\nu = \rho\beta$. Moreover, the order of

$$((-1)^{k-1}a_k)^{\rho} = (u_{\rho+k-1})^k$$

is $\delta/(\delta,\rho) = \beta/(k,\beta)$. Since $\delta/(\delta,\rho) = [\delta,\rho]/\rho$, then

$$\rho\beta = (k,\beta)[\delta,\rho] .$$

Finally, since $\beta/(k,\beta) = [\delta,\rho]/\rho$, then (k,β) is the order of $u_{\rho+k-1}^{[\delta,\rho]/\rho}$.

The first part of (i) in Theorem 2 is due to Carmichael [2]. The second part of (i) is an extension of a result of Ward [9] for modular integral sequences. (See also Robinson [6].)

Corollary 2. Let the conditions be as in Theorem 2. Then

(i) $\delta \mid \nu$.

(ii) $\beta \mid k\delta$.

(iii) $\beta \mid k$ if and only if $\delta \mid \rho$.

This corollary includes several facts that have been previously observed for some special sequences. For example, let 0, 1, 1, 2, 3, 5, $\cdots$ be the sequence of Fibonacci numbers reduced modulo $m > 2$. In this case, $k = 2$, $a_1 = a_2 = 1$, and $\delta = 2$. In particular $2 \mid \nu$. (See for example Wall [8, Theorem 4].) Also, $\beta \mid 4$, and $\beta \mid 2$ if and only if $2 \mid \rho$. In other words, $\beta \mid 2$ if $2 \mid \rho$ and $\beta = 4$ if $2 \nmid \rho$. (See Vinson [7, Theorem 3].)

Corollary 3. Let the conditions be as in Theorem 2, and suppose k is a prime. Then

(i) $\nu = k[\delta,\rho]$ if $u_{\rho+k-1}^{[\delta,\rho]/\rho} \neq 1$.

(ii) $\nu = [\delta,\rho]$ if $u_{\rho+k-1}^{[\delta,\rho]/\rho} = 1$.

In particular, the relation between the rank and period of the Fibonacci sequence modulo a prime may now be given. (See Barner [1, Theorem 2] or Herrick [5, Theorem 3].)

Corollary 4. Let the Fibonacci sequence reduced modulo an odd prime be of rank ρ and period ν. Then

(i) $\nu = 4\rho$ if $2 \nmid \rho$.

(ii) $\nu = 2\rho$ if $2 \mid \rho$, $2 \mid \rho/2$.

(iii) $\nu = \rho$ if $2 \mid \rho$, $2 \nmid \rho/2$.

Proof. Let R be the ring of integers modulo an odd prime; in particular, $k = 2$ and $\delta = 2$. If ρ is odd, then $\beta = 4$ and, by Theorem 2(i), $\nu = 4\rho$. Thus, suppose ρ is even and let A be the companion matrix associated with $a_1 = 1$, $a_2 = 1$. Clearly

$$(-1)^{\rho/2}A^{\rho/2} = (\det A^{\rho/2})A^{\rho/2} = ((\operatorname{adj} A^{\rho/2})A^{\rho/2})A^{\rho/2} = (\operatorname{adj} A^{\rho/2})A^{\rho} = (\operatorname{adj} A^{\rho/2})u_{\rho+1} .$$

Since the off diagonal elements of $A^{\rho/2}$ are not zero and are the negatives of the off diagonal elements of adj $A^{\rho/2}$, then it follows that $u_{\rho+1} = -(-1)^{\rho/2}$. Therefore, since $[2,\rho]/\rho = 1$,

$$u_{\rho+1}^{[2,\rho]/\rho} = u_{\rho+1} = -(-1)^{\rho/2} = \begin{cases} -1 & \text{if } 2 \mid \rho/2 \\ 1 & \text{if } 2 \nmid \rho/2 . \end{cases}$$

Consequently, by Corollary 3, $\nu = 2\rho$ if $2 \mid \rho/2$ and $\nu = \rho$ if $2 \nmid \rho/2$.

A slight extension of the foregoing argument provides another proof of the main theorem of Wyler [10]. In fact, Wyler [10, Theorem 4] is valid for every purely periodic second-order Lucas sequence over a commutative ring with 1 satisfying the following two properties: $1 + 1$ is not a zero divisor, and $u^2 = 1$ implies either $u = 1$ or $u = -1$.

REFERENCES

1. K. Barner, "Zur Fibonacci-Folge modulo p," *Monatsh. Math.,* 69 (1965), pp. 97–104.
2. R. D. Carmichael, "On Sequences of Integers Defined by Recurrence Relations," *Quart. J. Math.,* 48 (1920), pp. 343–372.
3. E. C. Dade, D. W. Robinson, O. Taussky, and M. Ward, "Divisors of Recurrent Sequences," *J. Reine Angew. Math.,* 214/215 (1964), pp. 180–183.
4. R. J. DeCarli, "Periodicity Over the Ring of Matrices," *The Fibonacci Quarterly,* Vol. 11, No. 5 (Dec. 1973), pp. 466–468.
5. D. L. Herrick, "On the Periodicity of the Terminal Digits in the Fibonacci Sequence," *The Fibonacci Quarterly,* Vol. 11, No. 5 (Dec. 1973), pp. 535–538.
6. D. W. Robinson, "The Fibonacci Matrix Modulo m," *The Fibonacci Quarterly,* Vol. 1, No. 1 (Feb. 1963), pp. 29–36.
7. J. Vinson, "The Relation of the Period Modulo m to the Rank of Apparition of m in the Fibonacci Sequence," *The Fibonacci Quarterly,* Vol. 1, No. 1 (Feb. 1963), pp. 37–45.
8. D. D. Wall, "Fibonacci Series Modulo m," *Amer. Math. Monthly,* 67 (1960), pp. 525–532.
9. M. Ward, "The Modular Period of a Linear Integral Recurrence," unpublished manuscript dated Europe; July–October, 1962.
10. O. Wyler, "On Second-Order Recurrences," *Amer. Math. Monthly,* 72 (1965), pp. 500–506.

★★★★★★★

LETTER TO THE EDITOR

GENERALIZED FIBONACCI NUMBERS AND UNIFORM DISTRIBUTION MOD 1

L. KUIPERS
Mollens, Valais, Switzerland

In the following I want to comment on a paper by William Webb concerning the distribution of the first digits of Fibonacci numbers [1] and to give a partial answer to some questions raised by the author. In fact, restriction to Fibonacci-related sequences makes it possible to obtain a number of results. (F_n) or 1, 1, 2, 3, 5, ⋯ stands for the sequence of Fibonacci numbers.

Theorem 1. Let k be an integer different from 0. Then the sequence $(\log F_n^{1/k})$ is uniformly distributed mod 1 (abbreviated u.d. mod 1).

Proof. We apply a classic result of J. G. van der Corput: Let (u_n) be a sequence of real numbers. If

$$\lim_{n \to \infty} (u_{n+1} - u_n)$$

exists and is irrational, then the sequence (u_n) is u.d. mod 1. See [2], p. 28.

Now set $u_n = \log F_n^{1/k}$. Then

$$u_{n+1} - u_n = \log F_{n+1}^{1/k} - \log F_n^{1/k} = \frac{1}{k} \log \frac{F_{n+1}}{F_n},$$

which tends to

[Continued on page 253.]