

Matrices, Recurrent Sequences and Arithmetic

U.Cerruti and F.Vaccarino

Introduction

The aim of this paper is to give a method, based on linear algebra techniques, thanks to which, the authors are also able to generalize older results on recurrent sequences to commutative rings with identity, often giving proofs essentially different to the ones previously given. In paragraph 2, is also proved a theorem which tells us, in a precise manner, how an impulse response sequence determines all the others having the same characteristic polynomial. In the third paragraph, among the other results, two theorems are proved: the former allows to prove (in an immediate way) a result on decimated sequences, which was given in [6], the latter gives rise to two really surprising arithmetical applications, which are explained in the fourth paragraph. The results here obtained are all proved in an elementary way, notwithstanding their generality.

1.Preliminaries

Let R be a commutative ring with unity 1. Let B be a $n \times n$ square matrix with entries in R : $B \in Mat(n, R)$. The elements of B will be denoted by B_{ij} with $0 \leq i, j \leq n - 1$. The (i, j) entry of B^m , the $m - th$ power of B , shall be denoted by B_{ij}^m . The matrix B^m is defined for $m < 0$ iff $det(B) \in R^*$ (the multiplicative group of the invertible elements of R).

In virtue of the following theorem there exists at least one polynomial $g(x) \in R[x]$ such that $g(B) = 0$.

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$ - $\mathcal{T}\mathcal{E}\mathcal{X}$

Theorem 1.1. *If $c_B(x) = \det(xI_n - B)$ then $c_B(B) = 0$. ([1],page 70,Th.7.23). \square*

A monic polynomial $g(x) \in R[x]$ of degree k shall be written as:

$$g(x) = x^k - \sum_{h=1}^k g_h x^{k-h} \quad (1.2)$$

Given a vector $\vec{s} = (s_0, s_1, \dots, s_{k-1}) \in R^k$ we denote by $W(\vec{s}; g) = W(s_0, s_1, \dots, s_{k-1}; g)$ the homogeneous linear recurrent sequence with characteristic polynomial $g(x)$ and initial values s_0, s_1, \dots, s_{k-1} :

$$W_n(\vec{s}; g) = \begin{cases} s_n & \text{for } 0 \leq n \leq k-1 \\ \sum_{h=1}^k g_h W_{n-h}(\vec{s}; g) & \text{for } n \geq k \end{cases} \quad (1.3)$$

Given any integer i , with $0 \leq i \leq k-1$, we pose

$$W(i; g) := W(\vec{e}_i; g) \quad (1.4)$$

where $\vec{e}_i = (0, \dots, 0, 1, 0, \dots, 0)$, with 1 at the i -th place.

Furthermore we set:

$$\begin{cases} U_m(g) := W_m(k-1; g) \\ T_m(g) := W_m(0; g) \\ V_m(g) := \sum_{h=0}^{k-1} W_{m+h}(h; g) \end{cases} \quad (1.5)$$

Theorem 1.6. *For every matrix $B \in \text{Mat}(n, R)$ and every $g(x)$ as in (1.2), if $g(B) = 0$, then:*

$$B_{ij}^m = W_m([B]_{ij}; g), \quad \forall m \geq 0 \quad \text{and} \quad 0 \leq i, j \leq n-1.$$

Where $[B]_{ij} = (B_{ij}^0, B_{ij}^1, \dots, B_{ij}^{k-1})$.

Furthermore, if $\det(B) \in R^*$, then the above equality is true $\forall m \in \mathbb{Z}$.

Proof. Since $g(B) = 0$ we have $B^k = \sum_{h=1}^k g_h B^{k-h}$. Thus $B_{ij}^m = \sum_{h=1}^k g_h B_{ij}^{m-h}$, $\forall m \geq k$. The result then follows from definition 1.3 with initial condition $\vec{s} = [B]_{ij}$. If $B^{-1} \in \text{Mat}(n, R)$, then the sequence can be extended to negative values. \square

Corollary 1.7. *In the same hypotheses of 1.6:*

$$B^m = W_m(0; g)I_n + W_m(1; g)B + \cdots + W_m(k-1; g)B^{k-1}, \quad \forall m \geq 0. \quad (1.8)$$

Proof. Indeed 1.6 may be written $B_{ij}^m = \sum_{h=0}^{k-1} W_m(h; g)B_{ij}^h$. \square

Let now A be the companion matrix of $g(x)$:

$$A = \begin{pmatrix} 0 & 0 & \cdots & 0 & g_k \\ 1 & 0 & \cdots & 0 & g_{k-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & g_1 \end{pmatrix} \quad (1.9)$$

so that $g(A) = 0$.

Theorem 1.10.

$$A_{ij}^m = W_{m+j}(i; g), \quad \forall m \geq 0 \quad \text{and} \quad 0 \leq i, j \leq k-1. \quad (1.11)$$

If $g_k \in R^*$, then 1.11 is true $\forall m \in \mathbb{Z}$. furthermore:

$$\begin{cases} U_m(g) = A_{k-1,0}^m \\ T_m(g) = A_{00}^m \\ V_m(g) = \text{Tr}(A^m) \end{cases} \quad (1.12)$$

Proof. The 1.11 is true for $m = 0$. The result follows by induction on m , computing

$$A^m A = A^{m+1}:$$

$$\begin{pmatrix} W_m(0; g) & W_{m+1}(0; g) & \cdots & W_{m+k-1}(0; g) \\ W_m(1; g) & W_{m+1}(1; g) & \cdots & W_{m+k-1}(1; g) \\ \vdots & \vdots & \vdots & \vdots \\ W_m(k-1; g) & W_{m+1}(k-1; g) & \cdots & W_{m+k-1}(k-1; g) \end{pmatrix} \times \begin{pmatrix} 0 & 0 & \cdots & 0 & g_k \\ 1 & 0 & \cdots & 0 & g_{k-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & g_1 \end{pmatrix}. \quad \square$$

We remark that 1.11 was used without proof in [5].

Corollary 1.13. *Let us suppose $g(B) = 0$ and A be the companion matrix of $g(x)$.*

Then:

$$B_{ij}^m = \sum_{h=0}^{k-1} B_{ij}^h A_{ht}^{m-t}, \quad \forall m \geq k, 0 \leq i, j \leq n-1 \quad \text{and} \quad 0 \leq t \leq k-1.$$

Proof. By 1.6 and 1.10. \square

$$2. \quad A^m A^n = A^{m+n}$$

Theorem 2.1. *If $W(i; g)$ is defined as in 1.4, then:*

$$W_{n+m}(i; g) = \sum_{j=0}^{k-1} W_{n+j-h}(i; g) W_{m+h}(j; g), \quad (2.2)$$

$\forall n, m \geq 0$, with $0 \leq i \leq k-1$ and $0 \leq h \leq n$. furthermore if $\det(A) \in R^*$, then 2.2 is true for any $n, m \in \mathbb{Z}$.

Proof.

Let A be the companion matrix of $g(x)$ as in 1.9. If we recall 1.10, then the thesis follows since $A^{m+n} = A^m A^n$, $\forall n, m \geq 0$ ($\forall n, m \in \mathbb{Z}$, when A^{-1} is defined). \square

Corollary 2.3. *With the same hypotheses of 2.1:*

$$\begin{cases} T_m(g) = g_k U_{m-1}(g) & \forall m \geq 1 \\ W_m(i; g) = W_{m-1}(i-1; g) + g_{k-i} U_{m-1}(g) & \forall m \geq 1 \quad \text{with } 1 \leq i \leq k-1. \end{cases} \quad (2.4)$$

Proof. To prove 2.4 apply 2.2 to $A^m = AA^{m-1}$. \square

Corollary 2.5. *With the same hypotheses of 2.1:*

$$W_m(i; g) = \sum_{j=0}^i g_{k-i+j} U_{m-j-1}(g), \quad \forall m \geq k. \quad (2.6)$$

Proof. The equality 2.5 is obtained applying 2.4 iteratively until one of the decreasing indices becomes zero. \square

Corollary 2.7. *If $W(\vec{s}; g)$ is defined as in 1.3, with the same hypotheses of 2.1, then:*

$$W_m(\vec{s}; g) = \sum_{h=1}^k g_h(\vec{s}) U_{m-h}(g), \quad \forall m \geq k \quad (2.8)$$

where

$$g_h(\vec{s}) := \sum_{j=0}^{k-h} s_{j+h-1} g_{k-j}, \quad \text{with } 1 \leq h \leq k. \quad (2.9)$$

furthermore:

$$g_k W_m(\vec{s}; g) = \sum_{h=1}^k g_h(\vec{s}) T_{m-h+1}(g), \quad \forall m \geq k. \quad (2.10)$$

Proof. Since

$$W_m(\vec{s}; g) = \sum_{i=0}^{k-1} W_m(i; g) W_i(\vec{s}; g), \quad \forall m \geq 0, \quad (\text{recall 2.2})$$

then, $\forall m \geq k$:

$$W_m(\vec{s}; g) = \sum_{i=0}^{k-1} s_i \left(\sum_{j=0}^i g_{k-i+j} U_{m-j-1}(g) \right) = \sum_{h=1}^k \left(\sum_{j=0}^{k-h} s_{j+h-1} g_{k-j} \right) U_{m-h}(g).$$

To prove 2.10 is enough to recall 2.4 and to substitute in 2.8. \square

Equations 2.6 and 2.8 show that every recurrence with characteristic polynomial $g(x)$ is completely determined by the impulse response sequence $U(g(x))$.

REMARK 2.11 If we pose $k = d$ and $g_i = r_{i-1}$, with $1 \leq i \leq k$, then the sequence $\{U_n\}$ introduced by Waddill in his quoted paper (see [7]) at page 602, before (3), is related to our $\{U_n(g)\}$, given in 1.5, by means of $U_n = U_{n+1}(g)$, $\forall n \geq 0$.

Thus (3) of Waddill becomes:

$$U_n^{(j)} = \sum_{i=0}^{j-1} r_{d-i-1} U_{n-j+1+i} = \sum_{h=0}^{j-1} g_{k-j+h+1} U_{n-h+1}(g) = W_{n+2}(j-1; g).$$

This agrees with the fact that, under the above assumptions, $A = \rho R^t \rho$, where R^t is the transposed of R and ρ is the $k \times k$ matrix

$$\begin{pmatrix} 0 & 0 & \dots & 0 & 1 \\ 0 & 0 & \dots & 1 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & 0 & \dots & 0 & 0 \end{pmatrix}. \square$$

REMARK 2.12 Note that:

$$\begin{cases} g_1(\vec{s}) = W_k(\vec{s}; g) \\ g_{j+1}(\vec{s}) = W_{k+j}(\vec{s}; g) - \sum_{l=1}^j g_l W_{k+j-l}(\vec{s}; g) \end{cases} \quad \text{for } 1 \leq j \leq k-1. \square \quad (2.13)$$

Corollary 2.14. *If $[B]_{ij}$ is defined as in 1.6, then*

$$B_{ij}^m = \sum_{h=1}^k g_h([B]_{ij})U_{m-h}(g), \quad \forall m \geq k. \square \quad (2.15)$$

$$3. \quad (A^n)^m = A^{mn}$$

We shall use now the matrix identity $(A^n)^m = A^{mn}$. Let A be the companion matrix of $g(x) = x^k - \sum_{i=1}^k g_i x^{k-i}$.

Theorem 3.1. *If $B = A^m$, then, $\forall n \geq 0$ with $0 \leq i, j \leq k-1$:*

$$W_{mn+j}(i; g) = W_n([B]_{ij}; c_B) = \sum_{h=0}^{k-1} W_{hm+j}(i; g)W_n(h; c_B) \quad (3.2)$$

where $c_B(x)$ is the characteristic polynomial of B .

Proof. Observe that

$$\begin{aligned} W_{mn+j}(i; g) &= A_{ij}^{mn} \quad (\text{by 1.11}) \\ &= (A^m)_{ij}^n = B_{ij}^n = W_n([B]_{ij}; c_B). \quad (\text{by 1.6}) \end{aligned}$$

Furthermore

$$\begin{aligned} W_n([B]_{ij}; c_B) &= W_n(A_{ij}^0, A_{ij}^m, \dots, A_{ij}^{m(k-1)}; c_B) = \sum_{h=0}^{k-1} A_{ij}^{hm} W_n(h; c_B) \\ &= \sum_{h=0}^{k-1} W_{hm+j}(i; g)W_n(h; c_B). \quad \square \end{aligned}$$

The foregoing theorem generalizes the following well known fact about usual generalized Fibonacci numbers: if $\deg(g(x)) = 2$, then, $\forall m, n \geq 0$, $U_n(g)$ divides $U_{mn}(g)$. Note that 3.1 tell us which is the quotient $U_{mn}(g)/U_n(g)$ as it is shown in the following corollary.

Corollary 3.3. *Let $g(x) = x^2 - ax + b$, then*

$$U_{mn}(g) = U_m(g)U_n(h)$$

where $h(x) = x^2 - V_m(g)x + b^m$.

Proof. In this case $A = \begin{pmatrix} 0 & -b \\ 1 & a \end{pmatrix}$ and $c_B(x) = x^2 - \text{Tr}(A^m)x + \det(A^m)$. Thus the result follows immediately by 3.2, applied with $j = 0$ and $i = 1$. \square

We denote by greek letters the sequences in R , i.e. the elements of $R^{\mathbb{N}}$. Thus $\sigma = (\sigma_n)_{n \geq 0}$ with $\sigma_n \in R$. We say that σ is a linear recurrent sequence in R if there exists a monic polynomial $g(x) \in R[x]$, $g(x) = x^k - \sum_{i=1}^k g_i x^{k-i}$, such that

$$\sigma_n = W_n(\sigma_0, \sigma_1, \dots, \sigma_{k-1}; g), \quad \forall n \geq 0.$$

In this case we say that $g(x)$ is a characteristic polynomial of σ . Now, let $\sigma = (\sigma_n)_{n \geq 0}$ be any linear recurrent sequence in R with characteristic polynomial $g(x)$. If we fix $m \geq 1$, then the sequence $\sigma^{(m)} = (\sigma_n^{(m)})_{n \geq 0} = (\sigma_{mn})_{n \geq 0}$ is called *decimated sequence* ([3]). The decimated sequence is again recurrent with a different characteristic polynomial. The problem of finding a characteristic polynomial of $\sigma^{(m)}$ has been considered in [2] in the case of fields. We can now give a quick way to find such a polynomial over any commutative ring R .

Corollary 3.4. *If $\sigma, g(x)$ and $\sigma^{(m)}$ are defined as before, then a characteristic polynomial of $\sigma^{(m)}$ is $c_B(x)$: the characteristic polynomial of $B = A^m$, where A is the companion matrix of $g(x)$.*

Proof. It follows immediately by 3.2 with $j = 0$. \square

The same result of 3.4 has been found in [6] in different way.

Note that we could obtain decimated sequence with prescribed characteristic polynomial $g(x)$ from a sequence to be determinate, if we are able to compute the m -th root of the companion matrix A of $g(x)$. Indeed, if $B^m = A$, then we obtain $A^n = B^{mn}$; thus the sequence $W_n(i; g)$ is obtained by decimation from a sequence of characteristic polynomial $c_B(x)$.

EXAMPLE 3.5 Let $A = \begin{pmatrix} 0 & -1 \\ 1 & 3 \end{pmatrix}$ be the companion matrix of $g(x) = x^2 - 3x + 1$. If $B = \begin{pmatrix} -1 & -1 \\ 1 & 2 \end{pmatrix} = -I + A$, then $B^2 = A$ and $c_B(x) = x^2 - x - 1$. It follows that: $\forall n \geq 0, U_n(g) = U_{2n}(c_B) = F_{2n}$. \square

If two matrices M, N commute, then the identity

$$(MN)^n = M^n N^n \quad (*)$$

gives interesting relations between recurrences with different characteristic polynomials.

Theorem 3.6. *If $M, S \in Mat(k, R)$ with $MS = SM$ and $T := MS$, then*

$$W_n([T]_{ij}; h) = \sum_{l=0}^{k-1} W_n([M]_{il}; g_1) W_n([S]_{lj}; g_2), \quad \forall n \geq 0$$

where $h(x), g_1(x), g_2(x) \in R[x]$ are monic polynomials such that $h(T) = g_1(M) = g_2(S) = 0$.

Proof. It follows immediately from (*). \square

We shall give a noteworthy application of 3.6. in the second part of 4.

4. Two Arithmetical Applications

Application I

Here we shall apply formula 2.8. We prove the following Theorem.

Theorem 4.1. *Given $k \geq 1$, then there exist $k + 1$ easily computable integers $v_h^{(k)}$, $1 \leq h \leq k + 1$, such that:*

$$n^k = \sum_{h=1}^{k+1} v_h^{(k)} \binom{n-h}{k}, \quad \forall n \in \mathbb{Z}. \quad (4.2)$$

Proof. Let us consider the impulse response sequences $U(g^{(k)}(x))$, where $g^{(k)}(x) := (x-1)^k = x^k - \sum_{h=1}^k g_h^{(k)} x^{k-h}$. Then $g_h^{(k)} = (-1)^{h-1} \binom{k}{h}$. It is easy to prove that

$$U_n((x-1)^k) = \binom{n}{k-1}, \quad \forall n \in \mathbb{Z}, \quad \forall k \geq 1. \quad (*)$$

Let $\vec{p}^{(k)}$ be the vector $(0, 1, 2^k, \dots, k^k)$.

Then it is clear that $n^k = W_n(\vec{p}^{(k)}; (x-1)^{k+1})$. Hence, by 2.8 and (*):

$$n^k = \sum_{h=1}^{k+1} g_h^{(k+1)} \vec{p}^{(k)} \binom{n-h}{k}, \quad \forall n \in \mathbb{Z}, \quad (**)$$

where $g_h^{(k+1)}(\vec{p}^{(k)})$ depends only by k . Indeed:

$$g_h^{(k+1)}(\vec{p}^{(k)}) = \sum_{j=0}^{k-h+1} (j+h-1)^k (-1)^{k-j} \binom{k+1}{j}, \quad \text{with } 1 \leq h \leq k+1. \quad \square (***)$$

EXAMPLE 4.3 If $k = 3$, then equations (**) and (***) give:

$$n^3 = 64 \binom{n-1}{3} - 131 \binom{n-2}{3} + 100 \binom{n-3}{3} - 27 \binom{n-4}{3}, \quad \forall n \in \mathbb{Z}. \square$$

REMARK 4.4 For fixed k the equation 4.2 can be reduced to a linear system. For example, if $k = 3$, then we obtain:

$$\begin{cases} v_1^{(3)} + v_2^{(3)} + v_3^{(3)} + v_4^{(3)} = 6 \\ 2v_1^{(3)} + 3v_2^{(3)} + 4v_3^{(3)} + 5v_4^{(3)} = 0 \\ 11v_1^{(3)} + 26v_2^{(3)} + 47v_3^{(3)} + 74v_4^{(3)} = 0 \\ v_1^{(3)} + 4v_2^{(3)} + 10v_3^{(3)} + 20v_4^{(3)} = 0 \end{cases} \quad (***)$$

whose solutions are, of course, $(64, -131, 100, -27)$. It is quite not obvious the fact that a system like (***) have solutions and that these are integral. \square

Application II

Now we shall apply Theorem 3.6.

We use $circ(a, b, c)$ to denote the left circulant matrix with first row (a, b, c) .

Theorem 4.5. *Let us pose:*

$$h(x) := x^3 - 3(a^2 + b^2 + c^2)x^2 + 3[a^4 + a^2(b-c)^2 - 2ab(b+c) + b^4 + b^2c^2 + c^4]x + a^6 - 6a^4bc + (2a^3 - 6abc)(b+c)(b^3 - bc + c^2) + 9a^2b^2c^2 + b^6 + 2b^3c^3 + c^6;$$

$$g(x) := x^3 - 3ax^2 + 3(bc - a^2)x + a^3 - 3abc + b^3 + c^3;$$

$$\vec{s}_0 := (1, a^2 + b^2 + c^2, (a^2 + 2bc)^2 + (b^2 + 2ac)^2 + (c^2 + 2ab)^2);$$

$$\vec{s}_1 := (1, a, a^2 + 2bc);$$

$$\vec{s}_2 := (0, b, c^2 + 2ab);$$

$$\vec{s}_3 := (0, c, b^2 + 2ac);$$

with $a, b, c \in \mathbb{Z}$.

Then:

$$W_n(\vec{s}_0; h) = W_n(\vec{s}_1; g)^2 + W_n(\vec{s}_2; g)^2 + W_n(\vec{s}_3; g)^2, \quad \forall n \geq 0.$$

Proof. Let us pose $M := \text{circ}(a, b, c)$, $S := \text{circ}(a, c, b)$, $T := MS$. We have $MS = SM$ and $M^n = \text{circ}(W_n(\vec{s}_1; g), W_n(\vec{s}_2; g), W_n(\vec{s}_3; g))$, $S^n = (M^n)^T$, the transpose of M^n . Now, $h(x) = c_T(x)$, $g(x) = c_M(x) = c_S(x)$, and the result follows by 3.6, computing $W_n([T]_{00}; h)$. \square

Hence, every element of the sequence $W_n(\vec{s}_0; h)$ is the sum of three squares.

In some cases the numbers $W_n(\vec{s}_0; h)$ can be given in closed form, as we see now.

Let $r, s \in \mathbb{Z}$ and let we pose $A(r, s) := r^2 + rs + s^2$. The following Lemma is easily proved by induction.

Lemma 4.6.

$$W_{n-1}(2A(r, s), 6A(r, s)^2; (x-3A(r, s))^2) = 2 \cdot 3^{n-1} \cdot A(r, s)^n, \quad \forall r, s \in \mathbb{Z} \quad \text{and} \quad \forall n \geq 1. \quad \square$$

Theorem 4.7. *Let us pose:*

$$u(x) := x^2 - 3rx + 3A(r, s);$$

$$\vec{t}_0 := (r, r^2 - 2rs - 2s^2);$$

$$\vec{t}_1 := (s, r^2 + 4rs + s^2);$$

$$\vec{t}_2 := (-r - s, -2r^2 - 2rs + s^2);$$

then:

$$2 \cdot 3^{n-1} \cdot A(r, s)^n = W_n(\vec{t}_0; u)^2 + W_n(\vec{t}_1; u)^2 + W_n(\vec{t}_2; u)^2, \quad \forall n \geq 1.$$

Proof. We pose in Theorem 4.3 the values: $a = r, b = s, c = -r - s$. Then: $h(x) = x(x - 3A(r, s))^2$ and $g(x) = x(x^2 - 3rx + 3A(r, s))$. Hence it is enough to use second order recurrences, starting a step later. Finally, we use 4.6 and the result follows by 4.5. \square

REMARK 4.8 It is well known that every number M not of the form $4^n(8m + 7)$ can be expressed as a sum of three squares. It is in general quite difficult (see [4]) to find an explicit expression of M as a sum $x^2 + y^2 + z^2$. Thus, results as 4.5 and 4.7 are really interesting. Furthermore we do not know any other example of a second order recurrent sequence, such that every element is a sum of three squares. \square

REFERENCES

- [1.] W.C.Brown, *Matrices over Commutative Rings*, Marcel Dekker, New York, 1993.
- [2.] P.F.Duvall, J.C.Mortick, *Decimation of Periodic Sequences*, SIAM J.Appl.Math. **21, No.3** (1971), 367-372.
- [3.] S.Golomb, *Shift Register Sequences*, Holden-Day, San Francisco, Calif., 1967.
- [4.] E.Grosswald, *Representations of Integers as Sums of Squares*, Springer-Verlag, New York, 1985.
- [5.] N.S.Mendelsohn, *Congruence Relationships for Integral Recurrences*, Canad.Math.Bull. **5, no.3** (1962), 281-284.
- [6.] H.Niederreiter, *A simple and general approach to the decimation of feedback shift-register sequences*, Problems Control Inform.Theory **17, no.5** (1988), 327-331.
- [7.] M.Waddil, *Using Matrix Techniques to establish properties of k-order Linear Recursive Sequences*, Applications of Fibonacci Numbers. Vol.5. Edited by G.E.Bergum, A.N.Philippou and A.F.Horadam, Kluwer Academic Publ., Dordrecht, The Netherlands (1993), 601-615.