

Vector Linear Recurrence Sequences in Commutative Rings

*Umberto Cerruti and Francesco Vaccarino**

Introduction

Let R be a commutative ring with identity. Let X be a vector sequence in $\mathfrak{M} := R^t$, such that $X^{(m)} := \sum_{h=1}^k X^{(m-h)} G_h$, with $G_h \in \text{Mat}(t, R)$. The main result of this paper is to show that X can be computed as linear recurrent sequence (in \mathfrak{M}) with scalar coefficients.

We also prove that the set $S = S(G_1, G_2, \dots, G_k)$ of all sequences in \mathfrak{M} that are recurrent with coefficients G_1, G_2, \dots, G_k , is a free R -module. A basis for this R -module is computed in a really efficient way. This problem has been discussed in [2] with R being a finite field.

At the end of this paper, two examples are given: the first example shows how the main result can be used to compute linear recurrent sequences in any finite, even non commutative, R -algebra; the second example gives rise to a surprising application of the usual Fibonacci numbers. For the notation, we refer the reader to [1].

Vector Sequences

Let R be a commutative ring with identity 1. Let B be a $n \times n$ square matrix with entries in R , $B \in \text{Mat}(n, R)$. 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 invertible elements of R).

We need the next two result, which can be found in [1].

*The authors were partially supported by the Italian M.U.R.S.T.

Theorem 1. For every matrix $B \in \text{Mat}(n, R)$ and every $g(x) = x^k - \sum_{h=1}^k g_h x^{k-h} \in R[x]$, if $g(B) = 0$, we have

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

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 $\forall m \in \mathbb{Z}$. \square

Now, let A be the companion matrix of $g(x)$. That is,

$$A = \begin{pmatrix} 0 & 0 & \dots & 0 & g_k \\ 1 & 0 & \dots & 0 & g_{k-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & g_1 \end{pmatrix}$$

so that $g(A) = 0$. We then have the following.

Theorem 2.

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

If $\vec{z} \in R^n$, $\vec{z} = (z_0, z_1, \dots, z_{n-1})$, we can define the sequence $\{\vec{z}^{(m)}\}_{m \geq 0}$, where $\vec{z}^{(m)} = (z_0^{(m)}, z_1^{(m)}, \dots, z_{n-1}^{(m)}) = \vec{z}B^m$, $\forall m \geq 0$, with $B \in \text{Mat}(n, R)$. Note that $\vec{z}^{(0)} = \vec{z}I_n = \vec{z}$.

Theorem 3. If $g(x) = x^k - \sum_{h=1}^k g_h x^{k-h} \in R[x]$ and $g(B) = 0$, then, for $j = 0, 1, \dots, n-1$,

$$z_j^{(m)} = W_m(z_j^{(0)}, z_j^{(1)}, \dots, z_j^{(k-1)}; g), \quad (4)$$

and

$$z_j^{(m)} = \sum_{h=0}^{n-1} z_h^{(0)} W_m([B]_{hj}; g). \quad (5)$$

Proof. To show (4), it is enough to observe that

$$\vec{z}^{(m)} = \vec{z}^{(0)} B^m = \vec{z}^{(0)} \sum_{h=1}^k g_h B^{m-h} = \sum_{h=1}^k g_h \vec{z}^{(m-h)}.$$

On the other hand

$$\vec{z}^{(m)} = \vec{z}^{(0)} B^m \Rightarrow z_j^{(m)} = \sum_{h=0}^{m-1} z_h^{(0)} B_{hj}^m,$$

so that (5) follows from Theorem 1. \square

Theorem 6. *If A is the companion matrix of $g(x)$, $\vec{z}^{(0)} \in M^k$, and $\vec{z}^{(m)} = \vec{z}^{(0)} A^m$, then*

$$\vec{z}^{(m)} = (W_m(\vec{z}^{(0)}; g), W_{m+1}(\vec{z}^{(0)}; g), \dots, W_{m+k-1}(\vec{z}^{(0)}; g)).$$

Proof. The proof follows immediately from Theorem 2. \square

Let us now use $\mathfrak{M} = R^t$ and $G_1, G_2, \dots, G_k \in \text{Mat}(t, R)$, with $t, k \geq 1$. Given the initial vector values $X^{(0)}, X^{(1)}, \dots, X^{(k-1)} \in \mathfrak{M}$ (considered as row vectors), we shall construct the sequence $X = (X^{(m)})_{m \geq 0}$ in \mathfrak{M} by means of

$$X^{(m)} := \sum_{h=1}^k X^{(m-h)} G_h, \quad \forall m \geq k. \quad (7)$$

In the following theorem, we prove that X can always be computed as a linear recurrence sequence with coefficients in R .

Theorem 8. *If the sequence X is given by (7), then there exists $g(x) \in R[x]$, with $\deg(g(x)) = n = kt$, such that $g(x) = x^n - \sum_{h=1}^n g_h x^{n-h}$ and*

$$X^{(m)} := \sum_{h=1}^n g_h X^{(m-h)}, \quad \forall m \geq n.$$

Proof. Let $B = B(G_1, G_2, \dots, G_k)$ be the following matrix

$$B = \begin{pmatrix} 0_t & 0_t & \dots & 0_t & G_k \\ I_t & 0_t & \dots & 0_t & G_{k-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0_t & 0_t & \dots & I_t & G_1 \end{pmatrix},$$

where O_t, I_t are respectively the zero and the identity of $\text{Mat}(t, R)$. We can think of B as an element from $\text{Mat}(n, R)$.

Let us consider the vector

$$\vec{z}^{(0)} = (X_0^{(0)}, X_1^{(0)}, \dots, X_{t-1}^{(0)}, X_0^{(1)}, \dots, X_{t-1}^{(1)}, \dots, X_0^{(k-1)}, \dots, X_{t-1}^{(k-1)})$$

so that $\vec{z}^{(0)} \in \mathfrak{M}^k = R^n$.

By induction on m , it is clear that if $\vec{z}^{(m)} := \vec{z}^{(0)} B^m, \forall m \geq 0$, then

$$\vec{z}^{(m)} = (X_0^{(m)}, X_1^{(m)}, \dots, X_{t-1}^{(m)}, X_0^{(m+1)}, \dots, X_{t-1}^{(m+1)}, \dots, X_0^{(m+k-1)}, \dots, X_{t-1}^{(m+k-1)}).$$

If $g(x) = c_B(x)$ then by (4) we have

$$z_j^{(m)} = W_m(z_j^{(0)}, z_j^{(1)}, \dots, z_j^{(k-1)}; g), \quad 0 \leq j \leq n-1,$$

which implies

$$X^{(m)} = W_m(X^{(0)}, X^{(1)}, \dots, X^{(n-1)}; g), \quad \forall m \geq 0.$$

The result now follows. \square

REMARK 1: We observe that if \mathfrak{A} is any R -algebra of finite dimension over R , even non commutative, then Theorem 8 permits one to reduce the recurrence $s_n = \sum_{h=1}^k g_h s_{n-h}, g_h \in \mathfrak{A}$, to a linear recurrence with coefficients in R . Indeed, if $t = \dim_R(\mathfrak{A})$, then $s_n = (X_0^{(n)}, X_1^{(n)}, \dots, X_{t-1}^{(n)}) \in \mathbb{F}^t$, and g_h can be represented as a matrix $G_h \in \text{Mat}(t, R)$ by using the transpose of the right regular representation. \square

We now use $S(G_1, G_2, \dots, G_k)$ to denote the set of all the vector sequences X which satisfy (7).

Theorem 9. $S = S(G_1, G_2, \dots, G_k)$ is a free R -module of rank $n = kt$.

An R -basis of S can be read explicitly from the columns of the powers of $B := B(G_1, G_2, \dots, G_k)$.

Proof. Let $\vec{e}_i \in R^t$ be the vector with 1 in the i -th place and 0 elsewhere, $0 \leq i \leq t-1$. Let δ_{ab} be the Kronecker delta. We denote by $Y_{ij} \in S$ the sequence determined by the

initial vector conditions

$$Y_{ij}^{(h)} = \delta_{hj} \vec{e}_i, \quad \text{with } 0 \leq j, h \leq k-1 \quad \text{and} \quad 0 \leq i \leq t-1.$$

It is clear that the n sequences Y_{ij} in S are R -independent. If $X \in S$, for $0 \leq h \leq k-1$, we can write

$$X^{(h)} = \sum_{i,j} X_i^{(j)} Y_{ij}^{(h)}.$$

Looking at the proof of Theorem 8, we see that:

$$(X^{(m)}, X^{(m+1)}, \dots, X^{(m+k-1)}) = (X^{(0)}, X^{(1)}, \dots, X^{(k-1)}) B^m.$$

Thus

$$\begin{aligned} (X^{(m)}, X^{(m+1)}, \dots, X^{(m+k-1)}) &= (\sum_{i,j} X_i^{(j)} (Y_{ij}^{(0)}, Y_{ij}^{(1)}, \dots, Y_{ij}^{(k-1)})) B^m = \\ &= \sum_{i,j} X_i^{(j)} (Y_{ij}^{(m)}, Y_{ij}^{(m+1)}, \dots, Y_{ij}^{(m+k-1)}). \end{aligned}$$

$$\text{Hence: } X^{(m)} = \sum_{i,j} X_i^{(j)} Y_{ij}^{(m)}, \quad \forall m \geq k, \quad \text{and} \quad X = \sum_{i,j} X_i^{(j)} Y_{ij}.$$

It is now clear that the Y_{ij} form an R -basis of S .

Next, we divide each row of B^m into a sequence of k vectors where each one belongs to R^t . We call $B_{(u,v)}^m$ the vector at place v , ($0 \leq v \leq k-1$), in the row u , ($0 \leq u \leq n-1$).

That is

$$B_{(u,v)}^m = (B_{u,tv}^m, B_{u,tv+1}^m, \dots, B_{u,tv+t-1}^m)$$

and

$$B^m = \begin{pmatrix} B_{(0,0)}^m & B_{(0,1)}^m & \cdots & B_{(0,k-1)}^m \\ B_{(1,0)}^m & B_{(1,1)}^m & \cdots & B_{(1,k-1)}^m \\ \vdots & \vdots & \vdots & \vdots \\ B_{(n-1,0)}^m & B_{(n-1,1)}^m & \cdots & B_{(n-1,k-1)}^m \end{pmatrix}.$$

It is easy to prove by induction that

$$Y_{ij}^{(m+h)} = B_{(tj+i,h)}^m, \quad \forall m \geq 0 \quad \text{with} \quad 0 \leq j, h \leq k-1 \quad \text{and} \quad 0 \leq i \leq t-1$$

which proves the second part of the theorem. \square

We note that the single "bit" of place d , ($0 \leq d \leq t-1$), of $X^{(m)}$, can be computed directly as

$$X_d^{(m)} = \sum_{i,j} X_i^{(j)} B_{tj+i,d}^m.$$

We explain by giving an example of Remark 1.

EXAMPLE:1 Let \mathbb{H} be the quaternion ring. That is

$$\mathbb{H} = \{a_0 + a_1\vec{i} + a_2\vec{j} + a_3\vec{k} : a_i \in \mathbb{R}, \forall i\}$$

with multiplication rules

$$\vec{i}^2 = \vec{j}^2 = \vec{k}^2 = -1, \quad \vec{i}\vec{j} = \vec{k} = -\vec{j}\vec{i}, \quad \vec{j}\vec{k} = \vec{i} = -\vec{k}\vec{j}, \quad \vec{i}\vec{k} = \vec{j} = -\vec{i}\vec{k}.$$

We consider the sequence

$$s_n = (\vec{i} + \vec{j})s_{n-1} + (\vec{i} + \vec{k})s_{n-2}, \quad \forall n \geq 2 \quad (10)$$

with arbitrary initial values $s_0, s_1 \in \mathbb{H}$.

If we represent $(\vec{i} + \vec{j})$, by right multiplication, as a matrix in $Mat(4, \mathbb{R})$ and we transpose it, then we obtain

$$G_1 = \begin{pmatrix} 0 & 1 & 1 & 0 \\ -1 & 0 & 0 & 1 \\ -1 & 0 & 0 & -1 \\ 0 & -1 & 1 & 0 \end{pmatrix}.$$

In the same way, the matrix associated with $(\vec{i} + \vec{k})$ is

$$G_2 = \begin{pmatrix} 0 & 1 & 0 & 1 \\ -1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \\ -1 & 0 & 1 & 0 \end{pmatrix}.$$

Then (10) is equivalent to the vectorial recurrence

$$X^{(n)} = X^{(n-1)}G_1 + X^{(n-2)}G_2,$$

where $X^{(m)} \in \mathbb{R}^4$ represents s_m as a real vector.

Now, the characteristic polynomial of $B = B(G_1, G_2)$, is $(x^4 + 2x^2 + 2x + 2)^2$. Furthermore, the minimum polynomial of B is $x^4 + 2x^2 + 2x + 2$. Thus

$$X^{(m)} = -2(X^{(m-2)} + X^{(m-3)} + X^{(m-4)}), \quad \forall m \geq 4.$$

If, for example, $s_0 = 1$ and $s_1 = 0$, then $X^{(m)}$ and $X^{(m+1)}$ can be read directly from the first row of B . \square

EXAMPLE: 2 We now give an example of an application of Theorem 10, with $k = 2, t = 3$ and $G_1, G_2 \in \text{Mat}(3, \mathbb{Z})$.

Let G_1 be the matrix representing the permutation (012) or

$$G_1 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

Let $G_2 := G_1^{-1}$ so that

$$G_2 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}.$$

Doing this, the space $S = S(G_1, G_2)$ is formed by all of the vector sequences X such that

$$X^{(m)} = X^{(m-1)}G_1 + X^{(m-2)}G_2, \quad \forall m \geq 2$$

with the given initial values $X^{(0)}, X^{(1)} \in \mathbb{Z}^3$. The matrix $B = B(G_1, G_2)$ is then

$$B = \begin{pmatrix} 0_3 & G_2 \\ I_3 & G_1 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \end{pmatrix}.$$

Let $F_n, n \geq 0$ be the usual Fibonacci numbers. It is then easy to see that

$$B^m = \begin{cases} \begin{pmatrix} F_{n-1}I_3 & F_nG_1 \\ F_nG_2 & F_{n+1}I_3 \end{pmatrix} & \text{if } m \equiv 0 \pmod{3} \\ \begin{pmatrix} F_{n-1}G_1 & F_nG_2 \\ F_nI_3 & F_{n+1}G_1 \end{pmatrix} & \text{if } m \equiv 1 \pmod{3} \\ \begin{pmatrix} F_{n-1}G_2 & F_nI_3 \\ F_nG_1 & F_{n+1}G_2 \end{pmatrix} & \text{if } m \equiv 2 \pmod{3}. \end{cases}$$

Since $X^{(m)} = (X^{(0)}, X^{(1)})B^m$, we obtain

$$X^{(m)} = \begin{cases} (F_{m-1}X_0^{(0)} + F_mX_2^{(1)}, F_{m-1}X_0^{(1)} + F_mX_0^{(1)}, F_{m-1}X_2^{(0)} + F_mX_1^{(1)}) & \text{if } m \equiv 0 \pmod{3} \\ (F_{m-1}X_1^{(0)} + F_mX_0^{(1)}, F_{m-1}X_2^{(0)} + F_mX_1^{(1)}, F_{m-1}X_0^{(0)} + F_mX_2^{(1)}) & \text{if } m \equiv 1 \pmod{3} \\ (F_{m-1}X_2^{(0)} + F_mX_1^{(1)}, F_{m-1}X_0^{(0)} + F_mX_2^{(1)}, F_{m-1}X_1^{(0)} + F_mX_0^{(1)}) & \text{if } m \equiv 2 \pmod{3}. \end{cases} \quad (a)$$

But $c_B(x) = x^6 - 4x^3 - 1$, so we know by Theorem 8, that

$$X^{(m)} = 4X^{(m-3)} + X^{(m-6)}, \quad \forall m \geq 6.$$

That is

$$X_h^{(m)} = 4X_h^{(m-3)} + X_h^{(m-6)}, \quad \forall m \geq 6 \quad \text{with} \quad 0 \leq h \leq 2.$$

Now, we compute $\{X_0^{(m)}\}_{m \geq 0}$ by using this recurrence. We choose the two initial vectors $X^{(0)}, X^{(1)}$ and obtain

$$(X_0^{(m)}, X_0^{(m+1)}, \dots, X_0^{(m+5)}) = (X_0^{(0)}, X_0^{(1)}, \dots, X_0^{(5)})C^m, \quad \forall m \geq 6, \quad (b)$$

where C is the companion matrix of $c_B(x)$, $X_0^{(0)}$ and $X_0^{(1)}$ are given by the initial conditions, and, by (a),

$$X_0^{(2)} = X_2^{(0)} + X_1^{(1)}$$

$$X_0^{(3)} = X_0^{(0)} + 2X_2^{(1)}$$

$$X_0^{(4)} = 2X_1^{(0)} + 3X_0^{(1)}$$

$$X_0^{(5)} = 3X_2^{(0)} + 5X_1^{(1)}.$$

We now consider the second order recurrent sequence $T_k := W_k(1, 0; x^2 - 4x - 1)$, $\forall k \geq 0$, where $m := 3k + j$, $0 \leq j \leq 2$.

Using these definitions it is easy to see that

$$C^m = \begin{cases} \begin{pmatrix} T_k I_3 & T_{k+1} I_3 \\ T_{k+1} I_3 & T_{k+2} I_3 \end{pmatrix} & \text{if } m \equiv 0 \pmod{3} \\ \begin{pmatrix} 0 & 0 & T_{k+1} & 0 & 0 & T_{k+2} \\ T_k & 0 & 0 & T_{k+1} & 0 & 0 \\ 0 & T_k & 0 & 0 & T_{k+1} & 0 \\ 0 & 0 & T_{k+2} & 0 & 0 & T_{k+3} \\ T_{k+1} & 0 & 0 & T_{k+2} & 0 & 0 \\ 0 & T_{k+1} & 0 & 0 & T_{k+2} & 0 \end{pmatrix} & \text{if } m \equiv 1 \pmod{3} \\ \begin{pmatrix} 0 & T_{k+1} & 0 & 0 & T_{k+2} & 0 \\ 0 & 0 & T_{k+1} & 0 & 0 & T_{k+2} \\ T_k & 0 & 0 & T_{k+1} & 0 & 0 \\ 0 & T_{k+2} & 0 & 0 & T_{k+3} & 0 \\ 0 & 0 & T_{k+2} & 0 & 0 & T_{k+3} \\ T_{k+1} & 0 & 0 & T_{k+2} & 0 & 0 \end{pmatrix} & \text{if } m \equiv 2 \pmod{3}. \end{cases}$$

Hence, the computation of $X^{(m)}$ may be easily accomplished. Let us consider the case $m \equiv 0 \pmod{3}$, $m = 3k$. Then, by the preceding results, we have

$$X_0^{(m)} = X_0^{(0)} T_k + X_0^{(3)} T_{k+1} = X_0^{(0)} T_k + (X_0^{(0)} + 2X_2^{(1)}) T_{k+1}$$

and

$$X^{(m)} = X_0^{(0)} F_{m-1} + X_2^{(1)} F_m.$$

Equating this results, we have

$$X_0^{(0)} (T_k + T_{k+1} - F_{m-1}) + X_2^{(1)} (2T_{k+1} - F_m).$$

However, this must be true for all $X_0^{(0)}, X_2^{(1)}$, which are chosen freely in the initial conditions. Hence,

$$\begin{cases} F_{3k-1} = T_k + T_{k+1} \\ F_{3k} = 2T_{k+1} \end{cases}, \forall k \geq 0. \square$$

ACKNOWLEDGEMENT

The authors would like to thank the Referee for his valuable comments.

REFERENCES

- [[1]] U.Cerruti, F.Vaccarino, *Matrices, Recurrent Sequences and Arithmetic*, Preprint.
- [[2]] S.Singh, *Recurring Sequences over Vector Spaces*, *Lin.Alg.Appl.* **131** (1990), 93-106.

A.M.S. classification numbers:11B37,15A33,11B39..