

R-Algebras of Linear Recurrent Sequences

*Umberto Cerruti and Francesco Vaccarino**

Introduction

Given any commutative ring R , with identity, we prove that the set of all the linear recurrent sequences in R is an R -algebra with respect the usual termwise sum and two different products, namely the Hadamard product and the convolution product. This generalizes, to commutative rings with identity, the results obtained by several authors in the case of sequences in a field (see [1],[6],[7],[9],[11],[12]). We also prove that the resulting rings are never isomorphic, as R -algebras, for any commutative ring R . For further results about these algebraic structure see [1],[7] and [10], where, however, the sequences are taken in fields. Furthermore we will give explicitly characteristic polynomials of the sum, the Hadamard product and the convolution product of any two, or more, linear recurrent sequences in R . This generalizes to any commutative ring with identity the results of [11],[9],[12] and [6] respectively. In spite of the generality of the results obtained, the methods are elementary.

1. Preliminaries

Let R be any commutative ring with identity 1. A monic polynomial $g(x) \in R[x]$ of degree k shall be written as:

$$g(x) = x^k - \sum_{h=1}^k g_h x^{k-h} \quad (1.1)$$

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} , that is:

$$W_n(\vec{s}; g) = \begin{cases} s_n & \text{for } 0 \leq n \leq k-1 \\ \sum_{h=1}^k g_h W_{n-h}(\vec{s}; g) & \text{for } n \geq k \end{cases} \quad (1.2)$$

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

$$W(i; g) := W(\vec{e}_i; g) \quad (1.3)$$

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

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

It is well known that:

$$W_n(\vec{s}; g) = \sum_{h=0}^{k-1} s_h W_n(h; g), \quad \forall n \geq 0. \quad (1.4)$$

Let $R^{\mathbb{N}}$ be the set of all the sequences in R . $R^{\mathbb{N}}$, endowed with componentwise sum and product, is an R -algebra. The componentwise product is often called the Hadamard product and we follow this custom. We denote by Greek letters the elements of $R^{\mathbb{N}}$. Thus $\sigma = (\sigma_n)_{n \geq 0}$ with $\sigma_n \in R$. For any $a \in R$ we denote by \tilde{a} the constant sequence with $\tilde{a}_n = a$.

We say that σ is a linear recurrent sequence in R , if there exists a monic polynomial $g(x) \in R[x]$, such that

$$\sigma_n = W_n(\sigma_0, \sigma_1, \dots, \sigma_{k-1}; g), \quad \forall n \geq 0. \quad (1.5)$$

In this case we say that $g(x)$ is a characteristic polynomial of σ .

2. The Hadamard ring of Linear Recurrent Sequences

For any monic polynomial $g(x) \in R[x]$ let us denote by $\mathcal{H}_R(g)$ the set of all linear recurrent sequences in R having $g(x)$ as a characteristic polynomial.

As was done in [5], we define an action of $R[x]$ on $R^{\mathbb{N}}$ by:

$$(x^k \sigma)_n = \sigma_{n+k} \quad (2.1)$$

extended by linearity. The following theorem is evident.

Theorem 2.2.

- a) $\sigma \in \mathcal{H}_R(g)$ iff $g(x)\sigma = \tilde{0}$.
- b) $O(\sigma) = \{h(x) \in R[x] : h(x)\sigma = \tilde{0}\}$ is an ideal of $R[x]$. \square

REMARK 2.3 If R is a field, then $R[x]$ is a principal ideal domain and $O(\sigma)$ is a principal ideal. So we can find a minimal characteristic polynomial of σ . In general, of course, this is not the case. If, for example, $a \neq 0, 1$ is an idempotent of R , then the sequence \tilde{a} has characteristic polynomials both $x - 1$ and $x - a$, hence it has no minimal characteristic polynomial. \square

We call \mathcal{H}_R the set of all linear recurrent sequences in R .

Now, we shall prove that \mathcal{H}_R is a *sub - R - algebra* of $R^{\mathbb{N}}$. In doing this, we shall give an effective (and easy to be implemented) algorithm to compute a characteristic polynomial of $\alpha\beta$, given any $\alpha, \beta \in \mathcal{H}_R$. In order to prove what we have just said, we need the next two results. Before, some notation.

Let B be a $n \times n$ square matrix with entries in R : $B \in \text{Mat}(n, R)$. The entries 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 $(B^m)_{ij}$. The matrix B^m is defined for $m < 0$ iff $\det(B) \in R^*$ (the multiplicative group of the invertible elements of R).

Theorem 2.4. ([2],page 70,Th.7.23).

If $c_B(x) = \det(xI_n - B)$ then $c_B(B) = 0$. \square

The following theorem is very easy to prove and very rich of consequences,(see[3]).

Theorem 2.5. For every matrix $B \in \text{Mat}(n, R)$ and every $g(x)$ as in (1.1), if $g(B) = 0$, then:

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

Where $[B]_{ij} = ((B^0)_{ij}, (B^1)_{ij}, \dots, (B^{k-1})_{ij})$. Furthermore, if $\det(B) \in R^*$, then the above equality is true $\forall m \in \mathbb{Z}$. \square

Note that 2.4 ensures us that 2.5 is never an empty statement.

Now, we can state explicitly and prove what we have asserted before.

Theorem 2.6. \mathcal{H}_R is a *sub - R - algebra* of $R^{\mathbb{N}}$.

Proof. It should be clear that \mathcal{H}_R is closed under the product by scalars defined above. If $\sigma, \rho \in \mathcal{H}_R$ have characteristic polynomials $f(x), g(x) \in R[x]$ respectively, then

$$(f(x)g(x))(\sigma + \rho) = (g(x)(f(x)\sigma) + f(x)(g(x)\rho)) = f(x)\tilde{0} + g(x)\tilde{0} = \tilde{0}.$$

Hence $(\sigma + \rho)$ is recurrent with characteristic polynomial $f(x)g(x)$.

If $\alpha = W(\alpha_0, \alpha_1, \dots, \alpha_{d-1}; f)$, $\beta = W(\beta_0, \beta_1, \dots, \beta_{e-1}; g)$ with $\deg(f(x)) = d$ and $\deg(g(x)) = e$, then, by 1.4,

$$\gamma_n := \alpha_n \beta_n = \sum_{l=0}^{d-1} \sum_{t=0}^{e-1} \alpha_l \beta_t W_n(l; f) W_n(t; g).$$

We have just seen that any R -linear combination of elements of \mathcal{H}_R belongs to \mathcal{H}_R . Thus, in order to prove that \mathcal{H}_R is closed with respect the product defined above, it is enough to show that $W(l; f)W(t; g) \in \mathcal{H}_R, \forall l, t$ with $0 \leq l \leq d-1$ and $0 \leq t \leq e-1$. Let A, B be the companion matrices of $f(x), g(x)$ respectively. If we pose $C := A \otimes B$ then it follows immediately from the definition of tensor product and from $(A \otimes B)^n = A^n \otimes B^n$, that

$$C_{ij}^n = A_{rs}^n B_{uv}^n \quad (*),$$

where $r = [i/e], s = [j/e]$ and $u = i \bmod e, v = j \bmod e$, with $0 \leq i, j \leq de - 1$. ($[a]$ denotes as usual the greatest non negative integer less or equal to a).

By 2.4 and 2.5, if we pose $h(x) = c_C(x)$, then $(*)$ implies:

$$W_n([C]_{ij}; h) = W_n([A]_{rs}; f)W_n([B]_{uv}; g).$$

Theorem 1.10 in [3] shows that, if D is that companion matrix of $p(x) = x^k - \sum_{i=1}^k p_i x^{k-i}$, i.e.

$$D = \begin{pmatrix} 0 & 0 & \dots & 0 & p_k \\ 1 & 0 & \dots & 0 & p_{k-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & p_1 \end{pmatrix},$$

then

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

Hence:

$$W_n([C]_{ij}; h) = W_{n+s}(r; f)W_{n+v}(u; g) \quad \text{and} \quad W_n(l; f)W_n(t; g) = W_n([C]_{le+t,0}; h). \quad \square$$

We state explicitly a fact which emerge from the foregoing proof.

Corollary 2.7. *For any monic $f(x), g(x) \in R[x]$, it holds*

$$\mathcal{H}_R(f)\mathcal{H}_R(g) \subset \mathcal{H}_R(h)$$

where $h(x) \in R[x]$ is the characteristic polynomial of the tensor product of the companion matrices of $g(x)$ and $f(x)$ respectively. \square

The closure of \mathcal{H}_R under the Hadamard product is proved in [1] and in [7], where the proofs work only if R is a field. A result similar to Corollary 2.7 is proved in [9] in a really different way, which is heavily based on the assumption that R is a finite field.

EXAMPLE 2.8 Let R be a commutative ring with identity 1 and $\sigma_n = W_n(\sigma_0, \sigma_1; g)$, $\tau_n = W_n(\tau_0, \tau_1; h)$ two linear recurrent sequences of degree 2 in R , with characteristic polynomials $g(x) = x^2 - ax - b$ and $h(x) = x^2 - cx - d$ respectively.

Then, by Th.2.6, the sequence $\sigma\tau = (\sigma_n\tau_n)_{n \geq 0}$ has characteristic polynomial:

$$x^4 - acx^3 - (a^2d + b(c^2 + 2d))x^2 - abcdx + b^2d^2. \square$$

EXAMPLE 2.9 Let a be the matrix $a = \begin{pmatrix} 1 & i \\ -i & 1 \end{pmatrix} \in Mat(2, \mathbb{C})$ and $R = \mathbb{Z}[a]$. We consider $c = 2I_2 - a = \begin{pmatrix} 1 & -i \\ i & 1 \end{pmatrix} \in \mathbb{Z}[a]$ and the polynomials $g(x) = x^2 - ax - I_2$, $h(x) = x^2 - cx - I_2$ in $R[x]$. We pose $\sigma_n = W_n(0_2, I_2; g)$, $\tau_n = W_n(0_2, I_2; h)$.

Since $\mathbb{Z}[a]$ cannot be embedded in a field, no previously existing method could give a characteristic polynomial $z(x)$ of $\sigma\tau$. On the contrary, from the foregoing example, we immediately get that: $z(x) = x^4 - 6I_2x + I_2$.

With a simple calculation (using $ac = 0$), we obtain:

$$\sigma_n\tau_n = \begin{cases} 0 & \text{if } n \text{ is even} \\ W_n(1, 5; x^2 - 6x + 1)I_2 & \text{otherwise} \end{cases}. \square$$

3. The Convolution Ring

We denote by $R[[x]]$ the ring of the formal power series with coefficient in R . That is $R[[x]] = \{\sigma(x) = \sum_{n=0}^{\infty} \sigma_n x^n : \sigma_n \in R, \forall n \in \mathbb{N}\}$ with the usual product and sum.

$R^{\mathbb{N}}$ and $R[[x]]$ are naturally isomorphic as R -modules, by means of

$$\sigma = (\sigma_n)_{n \geq 0} \leftrightarrow \sum_{n=0}^{\infty} \sigma_n x^n, \quad \forall \sigma \in R^{\mathbb{N}}. \quad (3.1)$$

We call this correspondence the natural one.

We say that $\sigma(x) \in R[[x]]$ is recurrent, if the sequence $\sigma \in R^{\mathbb{N}}$, naturally corresponding to it, is recurrent. In this case we say that $g(x)$ is a characteristic polynomial of $\sigma(x)$.

Let us pose $\mathcal{C}_R := \{\sigma(x) \in R[[x]] : \sigma(x) \text{ is recurrent}\}$.

For any monic polynomial $g(x) \in R[x]$ we denote by $\mathcal{C}_R(g)$ the set of all the $\sigma(x) \in \mathcal{C}_R$ with characteristic polynomial $g(x)$.

We denote by $g^*(x)$ the reciprocal polynomial of $g(x)$.

Lemma 3.2.

$\sigma(x) \in \mathcal{C}_R(g) \Leftrightarrow g^*(x)\sigma(x) = t(x)$ with $t(x) \in R[x]$ and $\deg(t(x)) < \deg(g(x))$.

Proof. Let k be the degree of $g(x)$. Since: $g^*(x)\sigma(x) = \sigma_0 + (\sigma_1 - g_1\sigma_0)x + (\sigma_2 - g_1\sigma_1 - g_2\sigma_0)x^2 + \cdots + (\sigma_{k-1} - g_1\sigma_{k-2} - \cdots - g_{k-1}\sigma_0)x^{k-1} + \sum_{j=k}^{\infty} (\sigma_j - g_1\sigma_{j-1} - \cdots - g_k\sigma_{j-k})x^j$, the result is clear \square

For a similar result, in the case $R = GF(q)$, see [8], Th.8.40 at page 416.

Theorem 3.3. \mathcal{C}_R is a sub- R -algebra of $R[[x]]$.

In particular:

$$(i) \mathcal{C}_R(g) + \mathcal{C}_R(h) \subseteq \mathcal{C}_R(gh);$$

$$(ii) \mathcal{C}_R(g)\mathcal{C}_R(h) \subseteq \mathcal{C}_R(gh);$$

for all monic polynomials $g(x), h(x) \in R[x]$.

Proof. (i) follows directly from 3.1 and 2.6. If $\sigma(x) \in \mathcal{C}_R(g), \tau(x) \in \mathcal{C}_R(h)$, with $\deg(g(x)) = d$ and $\deg(h(x)) = e$, then $g^*(x)\sigma(x) = t(x) \in R[x]$, with $\deg(t(x)) \leq d-1$, and $h^*(x)\tau(x) = u(x) \in R[x]$, with $\deg(u(x)) \leq e-1$. Hence:

$$g^*(x)h^*(x)(\sigma(x)\tau(x)) = (g^*(x)\sigma(x))(h^*(x)\tau(x)) = t(x)u(x),$$

with $\deg(t(x)u(x)) \leq d+e-2 < d+e$, and the result follows by 3.2. \square

REMARK 3.4 If we recall the correspondence 3.1, then is evident that, to the product of two formal series, say $\sigma(x)$ and $\tau(x)$, it corresponds the product of convolution $\sigma \star \tau$, as it is defined in [6]. That is

$$(\sigma \star \tau)_n = \sum_{i+j=n} \sigma_i \tau_j, \quad \forall n \geq 0. \quad (3.5)$$

It follows that we have also found a generalization to any commutative ring of the result presented in [6]. \square

Of course \mathcal{H}_R and \mathcal{C}_R are isomorphic as R -modules. But we can prove that does not exist any R -algebra isomorphism between \mathcal{H}_R and any subalgebra of \mathcal{C}_R .

Theorem 3.6. If $\psi : \mathcal{H}_R \longrightarrow \mathcal{C}_R$ is an R -algebra morphism, then ψ is not injective.

Proof. Let us suppose that $\psi : \mathcal{H}_R \longrightarrow \mathcal{C}_R$ is an injective morphism. Let us consider $a := (1, 0, 0, \dots)$ and $b := (0, 1, 0, \dots)$ in \mathcal{H}_R , and pose $\alpha(x) := \psi(a)$, $\beta(x) := \psi(b)$.

Then $\alpha(x)\beta(x) = 0$ in \mathcal{C}_R and, by hypothesis, $\alpha(x), \beta(x) \neq 0$. Now, there exist a monic polynomial $g(x) \in R[x]$, with $\deg(g(x)) = k$, such that $\alpha(x) \in \mathcal{C}_R(g)$. Hence, by 3.2, we know that $g^*(x)\alpha(x) = t(x) \in R[x]$, with $\deg(t(x)) \leq k - 1$. If we remember the proof of 3.2, then we see that: $t(x) = 0$ iff $\alpha_0 = \alpha_1 = \dots = \alpha_{k-1} = 0$. Thus, in this case, $t(x) = 0$ implies $\alpha(x) = 0$, by the recursivity of $\alpha(x)$, which is not the case. From $\alpha(x)\beta(x) = 0$, we get, multiplying by $g^*(x)$, $t(x)\beta(x) = 0$. This implies, by (2.9) of [4], that there is a nonzero element $r \in R$, such that $r\beta(x) = 0$. Thus, again by injectivity, $rb = 0$ in \mathcal{H}_R , which is absurd. \square

ACKNOWLEDGMENT

The authors thank the Referee for his useful remarks and suggestions.

REFERENCES

- [1.] B.Benzaghou, *Algebres de Hadamard*, Bull.Soc.math. France **98** (1970), 209-252.
- [2.] W.C.Brown, *Matrices over Commutative Rings*, Marcel Dekker, New York, 1993.
- [3.] U.Cerruti, F.Vaccarino, *Matrices, Recurrent Sequences and Arithmetic*, Preprint (1994).
- [4.] R.Gilmer, *On polynomial and power series rings over a commutative ring*, Rocky Mt.J.Math. **5** (1975), 157-175.
- [5.] M.Hall, Jr., *An Isomorphism between linear recurring sequences and algebraic rings*, Trans.Amer.Math.Soc. **44** (1938), 196-218.
- [6.] P.Haukkanen, *On a Convolution of Linear Recurring Sequences over Finite Fields*, J. Algebra **149** (1992), 179-182.
- [7.] R.G.Larson, E.J.Taft, *The algebraic structure of linearly recursive sequences under Hadamard product*, Israel J. Math. **72** (1990), 118-132.
- [8.] R.Lidl, H.Niederreiter, *Introduction to Finite Fields and Their Applications*, Cambridge Univ.Press, London, 1986.
- [9.] L.Peizhong, S.Guowen, *Feasible Calculation of the Generator of Combined LFSR Sequences*, Lecture Notes in Comput.Sci.(Springer Verlag, Berlin) **508** (1991), 86-95.
- [10.] B.Peterson, E.J.Taft, *The Hopf algebra of linearly recursive sequences*, Aequationes Math. **20** (1980), 1-17.
- [11.] N.Zierler, *Linear recurring sequences*, J.Soc.Indus.Appl.Math. **7** (1959), 31-48.
- [12.] N.Zierler, W.H.Mills, *Products of Linear Recurring sequences*, J.Algebra **27** (1973), 147-157.