DECOMPOSITION OF LINEAR AUTOMATA OVER RESIDUE RINGS INTO SHIFT-REGISTERS *

Arnold SCHEUING

Institut für Informatik und Angewandte Mathematik, Universität Bern, CH-3012 Bern, Switzerland

Communicated by M. Nivat
Received November 1984
Revised September 1985

Abstract. A linear automaton \( \mathcal{A} \) over a residue ring \( \mathbb{Z}_n \), \( n \in \mathbb{N} \), is in general not decomposable into a parallel connection of shift-registers. We are able to formulate necessary and sufficient conditions for such a decomposition, by using the theory of artin local rings \( R \) and the \( R[x] \)-module-structure of \( \mathcal{A} \).

1. Introduction

The structure of a finite, deterministic, linear automaton (fa) is of interest not only in computer science but also in system theory. Applications of fa's—also called linear sequential circuits LCS—include error detection and correction, random number generator, and cryptology (the author's motivation), and the discrete and continuous-time, finite-dimensional constant linear systems. As long as the coefficients of such automata or systems are elements of a field \( F \), the structure is well known and has extensively been studied in the past twenty years [4] by means of linear algebra: The state space \( E \) of a fa \( \mathcal{A} \) is a finite-dimensional vectorspace \( E \) over \( F \) and the transition function can be seen as an endomorphism in \( E \), or as a matrix \( A \) over \( F \) if a basis in \( E \) is fixed.

To find a 'simplest' fa equivalent to \( \mathcal{A} \), one uses the 1-1-correspondence between fa's equivalent to \( \mathcal{A} \) and matrices similar to \( A \). And there are good reasons to choose the rational canonical form of \( A \) as 'simplest' form, because it corresponds to the decomposition of \( A \) into parallel shift-registers.

In Fig. 1 we show three corresponding presentations of an fa in respect of a given basis \( B \) in \( E \). Fig. 1(a) shows (the technical realisation of) a shift register with 3-dimensional state space, each state with components \( (s_1, s_2, s_3) \). In system theory the \( s_i \) are called delay- and the \( a_i \) multiplication-elements. Each time-cycle brings the element stored in \( s_3 \) to \( s_2 \), the contents of \( s_2 \) to \( s_1 \), and the sum \( a_0s_1 + a_1s_2 + a_2s_3 \) (formed in \( F \)) in \( s_3 \). Fig. 1(b) is the representation of the linear transition function

* The results reported here formed part of the author's Ph.D. Dissertation, which was supervised by Professor Urs Würgler at the University of Bern.
Fig. 1. Corresponding presentations \((a_0, a_1, a_2, a_3) \in F\). (a) Shift-register. (b) Companion matrix. (c) Cyclic \(F[x]\)-module of rank 3.

\[
\begin{pmatrix}
0 & 1 & 0 \\
0 & 0 & 1 \\
a_0 & a_1 & a_2
\end{pmatrix}
\]

\(F[x]/(x^3 - a_2x^2 - a_1x - a_0)\)

\(f\) in form of a 3 x 3-matrix. This special form is called a companion matrix. If the polynomial \(x^3 - a_2x^2 - a_1x - a_0\) is irreducible in \(F[x]\), then the \(f\) is not decomposable. Fig. 1(c) names a cyclic \(F[x]\)-module of rank 3, e.g., the basis \(B\) has three elements \(e, f(e), f^2(e)\), and

\[f^3(e) = a_0e + a_1f(e) + a_2f^2(e)\]

The 1-1-correspondence of these three structures is used throughout this paper: diagrams of \(f\)'s and shift-registers to visualise the technical realisation, matrices to calculate the examples, and modules to develop the theory.

It is well known that an \(f\) with coefficients over a field can always be realised by a parallel connection of shift-registers [9]. But in the applications mentioned above we are also interested in systems over rings \(\mathbb{Z} \mod 2^r (r \in \mathbb{N})\). As an example in cryptology, the process of computer-aided enciphering and deciphering is closely related to the value range \(2^r\) of a register with \(r\) binary digits.

A very good survey of the extension of the theory of linear systems from fields to rings in the last ten years can be found in [12]. The duality principle for linear systems over residue class rings is discussed in [2, 8]. Matrix fraction representation for linear systems over commutative rings has also been studied in [5].

In Section 5 we give an example of an \(f\) over \(\mathbb{Z}_4\), which is neither a shift-register nor decomposable into shift-registers. Therefore, the question arises under what conditions an \(f\) over \(\mathbb{Z}_n\) can be realised by a parallel connection of shift-registers. A similar problem was studied in [6, 7] by using a bijection \(\beta : \mathbb{Z}_{p^r} \approx \prod \mathbb{Z}_p\) to decompose an \(f\) \(\mathbb{A}\) over \(\mathbb{Z}_{p^r}\) into a cascade connection of \(r\) \(f\)'s \(\mathbb{A}_i\) over \(\mathbb{Z}_p\). But because \(\beta\) is not a ringhomomorphism, the \(\mathbb{A}_i\)'s are connected by a nonlinear, delay-free logic, which limits a further analysis by means of commutative algebra.

This paper is divided as follows: In Section 2 we shall show that the appropriate mathematical objects to study the structure of \(f\)'s over \(\mathbb{Z}_n\) are \(\mathbb{Z}_n\)-free \(\mathbb{Z}_n[x]\)-modules (Fig. 1). In Section 3 we shall prove that the problem can be reduced without loss
of generality to fa's over \( \mathbb{Z}_p \); on the other hand, the recursive criterion in the last section suggests not to restrict our attention to the finite and local rings \( \mathbb{Z}_p \), but to consider more general (commutative) artin local rings \( R \) (with 1). Therefore, we shall summarise in Section 3 the necessary statements for artin local rings and modules over such rings. In Section 4 we shall show that our \( R[x] \)-module always has a primary decomposition. The main results are in Sections 5 and 6, where we give necessary and sufficient conditions for a cyclic decomposition of the state space; in other words, conditions for the fa to be equivalent to a direct sum of shift-registers. We discuss the general case in Section 5 and a special case with principal ideal ring \( R \) in Section 6.

2. The module-structure of an fa

We start with a more precise description of an fa.

**Definition 2.1.** A finite, deterministic, linear automaton (fa) (without input- or output-functions) over a ring \( R \) is a pair \((E,f)\), where the state space \( E \) is a free \( R \)-module of finite dimension (say \( n \)) and the transition function \( f \) is a linear mapping from \( E \) into \( E \). Each \( e \in E \) is a state of the fa, the transition function maps a state \( e \) onto a new state \( f(e) \). We can use this simple notation without initial state because we are only interested in the whole structure of the fa.

The set of all transition functions over \( E \) is the endomorphism ring \( \text{End}_R(E) = \{ f : E \rightarrow E \mid f \text{ linear} \} \). \( \text{End}_R(E) \) is also an \( R \)-module. This fact can be expressed by the ringhomomorphism in the following commutative diagram.

\[
\begin{array}{ccc}
R & \xrightarrow{\psi} & \text{End}_R(E) \\
\downarrow & & \downarrow \hat{\psi} \\
R[x] & \xrightarrow{\hat{\psi}} & \text{End}_R(E) \\
\end{array}
\]

For \( r \in R \), \( \psi(r) \) is the scalar multiplication with \( r \) in \( E \). Because \( f \) operates linearly on \( E \), we can extend \( \psi \) as ringhomomorphism to \( R[x] \) by setting \( \hat{\psi}(x) := f \). Now \( E \) becomes a \( R[x] \)-module.

By parallel connection of different fa's over the same ring we can build larger automata. Of even more interest is the possibility to decompose a given (complex) automaton into smallest, irreducible parts, the shift registers.

**Definition 2.2.** An fa \((E,f)\) over a ring \( R \) is a shift-register if \( E \) is cyclic as \( R[x] \)-module. In other words, if there exists an initial state \( e \in E \) such that its orbit

\[ e, f(e), f^2(e), \ldots, f^{n-1}(e) \]

spans \( E \).
By the term ‘parallel connection of fa’s \( (E_i, f_i) \)’ we have the technical realisation
in mind (see Fig. 2(b)), but it simply means the direct sum sum \( \bigoplus E_i, \bigoplus f_i \). To say
that an \( f \) is ‘a realisation by parallel connection of shift registers’ is an intuitive
way to express that \( E \) is the direct sum of \( R[x] \)-cyclic \( R \)-free submodules.

To formulate a first theorem, we need the following notation:

- \( M_n(R) \): the set of all \( n \times n \) matrices over \( R \),
- \( \text{GL}_n(R) \): the subset of \( M_n(R) \) of all regular matrices,
- \( M_n(R)/\text{GL}_n(R) \): the set of all similarity-classes of matrices \( A \in M_n(R) \) is similar
to \( T^{-1}AT \) for all \( T \in \text{GL}_n(R) \),
- \( \text{Mod}_n(R[x]) \): the class of all \( R \)-free \( R[x] \)-modules \( E \) of rank \( n \) (that is \( \dim_R(E) = n \)),
- \( \text{Iso}(\text{Mod}_n(R[x])) \): the set of all isomorphism-classes of such modules.

**Theorem 2.3.** There is a 1-1-correspondence

\[ \chi : M_n(R)/\text{GL}_n(R) \to \text{Iso}(\text{Mod}_n(R[x])). \]

**Proof.** Definition of \( \chi \): Let \([A] \in M_n(R)/\text{GL}_n(R) \) and \( A \in M_n(R) \) be a representant.
Further, let \( E \) be a free \( R \)-module of rank \( n \). Choose a basis in \( E \) and then define
\( x \cdot e := A \cdot e \quad (\forall e \in E) \). In this way, \( E \) becomes an \( R[x] \)-module \( E_A \). We define
\( \chi[A] := [E_A] \), the isomorphism-class of \( E_A \). We define \( \chi[A] := [E_A] \), the isomorphism-class of \( E_A \). \( \chi \) is well-defined, because, for similar matrices \( A \sim A' \), the modules
are isomorphic: \( E_A \cong E_{A'} \), hence, \([E_A] = [E_A]\).

Definition of \( \chi' \): Let \([F] \in \text{Iso}(\text{Mod}_n(R[x])) \) and \( F \in \text{Mod}_n(R[x]) \) be a representant.
Choose in \( F \) an \( R \)-basis, then the (linear) action of \( x \) can be expressed by a
matrix \( A \). If we set \( \chi'[F] := [A] \), then this is also well-defined and obviously the
inverse function of \( \chi \). \( \square \)

3. Artin local rings and finitely generated modules

In the first part of this section, we apply the ‘Chinese Reminder Theorem’ to
simplify the problem of fa’s over \( Z_n \) to fa’s over \( Z_p \) \( (p \) prime, \( r \in \mathbb{N}) \). We remember
that—because \( n \) has a unique decomposition into prime factors \( n = p_1^{e_1}p_2^{e_2} \cdots p_m^{e_m} \)—the ring \( Z_n \) is isomorphic to the ring product \( \prod_{i=1}^m Z_{p_i^{e_i}} \). This isomorphism
induces the following theorem.

**Theorem 3.1.** Let \( R_1, R_2, \ldots, R_m \) be (commutative) rings (with 1), \( R := \prod_{i=1}^m R_i \), \( E \)
an \( R \)-module and define \( E_i := E \otimes R_i \). Then the ring \( \text{End}_R(E) \) is isomorphic to
\( \bigoplus_{i=1}^m \text{End}_{R_i}(E_i) \).

**Proof.** Let \( f_i := f \otimes 1_{E_i} \in \text{End}_{R_i}(E_i) \). We can define the ringhomomorphism
\( \varphi : \text{End}_R(E) \to \bigoplus_{i=1}^m \text{End}_{R_i}(E_i) \) by \( \varphi(f) := (f_1, f_2, \ldots, f_m) \).
\( \varphi \) is mono: for \( f \in \ker(\varphi) \Rightarrow f_i = f \otimes 1_{E_i} = 0 \quad (\forall i) \Rightarrow f(E) \cong \prod_{i=1}^m (f(E) \otimes R_i) = 0 \Rightarrow f = \ldots \)
\( \varphi \) is epi: we take an arbitrary \( f_i \in \text{End}_R(E_i) \). Consider the diagram

\[
\begin{array}{ccc}
E & \xrightarrow{\prod_i f_i(1_E \otimes \pi_i)} & \prod_i E_i = \prod_i (E \otimes R_i) \cong E \otimes \prod_i R_i \cong E, \\
& \downarrow 1_E \otimes \pi_i & \downarrow \pi_i \\
E_i & \xrightarrow{f_i} & E_i \\
\end{array}
\]

thus, \( \varphi(\prod_i f_i(1_E \otimes \pi_i)) = (f_1, f_2, \ldots, f_m). \) \( \square \)

**Conclusion 3.2.** An fa over \( \mathbb{Z}_n \) can always be realised by a parallel connection of fa's over \( \mathbb{Z}_{p^r} \).

**Example 3.3.** The fa in Fig. 2(a) over \( \mathbb{Z}_6 \) is isomorphic to the fa in Fig. 2(b). The corresponding module is

\[
E \cong \mathbb{Z}_6[x]/(x^3 - 2x^2 - 3x - 4) \cong \mathbb{Z}_2[x]/(x^3 + x) \oplus \mathbb{Z}_3[x]/(x^3 + x^2 - 1).
\]

In the second part of this section, we want to summarise the needed facts about artin local rings and modules over such rings.

**Definition 3.4.** A ring \( R \) is *artin* if \( R \) is noetherian and has dimension 0 (every prime ideal is maximal, see [1]).

---

![Diagram](attachment:image.png)

Fig. 2. Equivalent fa's over \( \mathbb{Z}_6 \) (with input and output).
A ring \( R \) is local if \( R \) is noetherian and has exactly one maximal ideal \( M \). Notation: \((R, M)\).

**Example 3.5.** \((\mathbb{Z}_p^\ast, (p))\) and \((\mathbb{Z}_p[x]/(x^r), (p, x))\) are artin local rings.

**Lemma 3.6.** Some properties of artin local rings \((R, M)\) are:

(a) \( M \) is the only prime ideal;
(b) the nilradical \( \text{Rad}(R) \) coincides with \( M \) and is nilpotent itself; the smallest \( z \in \mathbb{N} \) with \( M^z = (0) \) is called the nilpotency of \( M \);
(c) each element of \( R \) is either a unit or nilpotent.

Snapper [11] calls these rings 'completely primary rings'.

Because the canonical projection \( \pi: R \to R/\text{Rad}(R) \) is important, we shall use the following notation throughout the paper: \( \bar{R} = R/\text{Rad}(R) \), the residue field, \( \bar{r} = \pi(r) (\forall r \in R) \), \( \bar{M}[x] = \pi(M[x]) = 0 \).

**Remark 3.7.** We shall only consider finitely generated modules in this paper without repeating this fact every time.

The reason why we fail to follow the same decomposition as fa’s over a field \( F \)—that is, as modules over the principal ideal domain \( F[x] \)—is the fact that a submodule of a free module need not be free. But we have the following fundamental theorem.

**Theorem 3.8.** (a) In a local ring \((S, M)\) all finitely generated projective modules are free.
(b) Let \((S, M)\) be an artin local ring, \( F \subset E \) both finitely generated, free \( S \)-modules. Then \( E \cong F \oplus E/F \).
(c) Let \((S, M)\) be an artin local ring, \( F, G \subset E \) three finitely generated, free \( S \)-modules. Then \( F \cap G \) and \( F + G \) are free.

**Proof.** (a) See [10].
(b) Let \( \{e_1, \ldots, e_n\} \) and \( \{f_1, \ldots, f_m\} \) be bases for \( E \) and \( F \), respectively. Because \( F \subset E \Rightarrow f_i = \sum \varphi_i e_i \) and because \( \{f_1, \ldots, f_m\} \) is linearly independent, at least one of the \( \varphi_i \)'s must be a unit (see Lemma 3.6). Without loss of generality, \( \varphi_1 \) is a unit implies \( e_1 = (\varphi_1^{-1})(f_1 - \sum_{i>1} \varphi_i e_i) \). So \( \{f_1, e_2, \ldots, e_n\} \) is a basis for \( E \). With induction we see that \( \{f_1, f_2, \ldots, f_m, e_{m+1}, \ldots, e_n\} \) is a basis for \( E \), hence, \( E \cong F \oplus L_R(e_{m+1}, \ldots, e_n) \).
(c) \( G \to F \oplus E/F \) and both summands are free (part (b)). Let \( \{g_1, \ldots, g_p\} \) be a basis of \( G \) and \( \{f_1, \ldots, f_m, e_{m+1}, \ldots, e_n\} \) a basis of \( E = F \oplus E/F \). Because \( g_1 \in E \), we can conclude analogously to part (b), that \( \{g_1, \ldots, g_q, f_{q+1}, \ldots, f_m, g_{q+1}, \ldots, g_p, e_{n-m-p+q}, \ldots, e_n\} \) is a basis of \( E \). Hence, \( F \cap G = L_S(g_1, \ldots, g_q) \) and \( F + G = L_S(g_1, \ldots, g_p, f_{q+1}, \ldots, f_m) \) are both free. ☐
We recall that for an irreducible polynomial \( \alpha \in \mathbb{R}[x] \), the projection \( \bar{\alpha} \in \bar{\mathbb{R}}[x] \) is not necessarily irreducible. If it is, then we call \( \alpha \) fundamental irreducible.

**Lemma 3.9.** Some important types of ideals in \( \mathbb{R}[x] \) for artin local \((\mathbb{R}, M)\) are:

(a) \( M[x] := \{ \sum r_i x^i \in \mathbb{R}[x] | r_i \in M \} \subset \mathbb{R}[x] \) is the only nil prime ideal of \( \mathbb{R}[x] \);

(b) All non-nil prime ideals are of the form \( M[x] + (\alpha) \), with \( \alpha \in \mathbb{R}[x] \) monic and fundamental irreducible. Because \( \bar{\mathbb{R}} \) is a field, these ideals are also maximal;

(c) A non-nil ideal of \( \mathbb{R}[x] \) is of the form \( N + (\beta) \), where \( \beta \) is a monic polynomial and \( N \subset M[x] \). The generators of \( N \) can always be chosen of a smaller degree than \( \beta \).

The proof is straightforward; for more details, see [11].

### 4. Primary decomposition

First we prepare some facts and definitions about ideals. Let \( J \) be an ideal of a ring \( S \). The radical of \( J \) is \( \text{Rad}(J) = \{ s \in S | \exists n \in \mathbb{N}: s^n \in J \} \). Recall that \( \text{Rad}(R) := \text{Rad}(0) \). \( J \) is called primary, if, for \( st \in J \), \( t \in J \Rightarrow s \in \text{Rad}(J) \).

Let \( E \) be an \( S \)-module, then the annihilator ideal of \( E \) is defined by \( \text{Ann}_S(E) := \{ s \in S | se = 0 (\forall e \in E) \} \).

**Definition 4.1.** An \( S \)-module \( E \) is called primary if \( (0) \) is a primary submodule of \( E \). That is, for \( s \in S \), \( 0 \neq e \in E \) with \( se = 0 \) implies \( s \in \text{Rad}(\text{Ann}_S(E)) \). (If an element \( s \) kills one element of \( E \), then a potency of \( s \) kills all of \( E \).) Ideals \( J \) and \( I \) of \( S \) are called coprime, if \( I + J = S \).

**Lemma 4.2.** Let \( (\mathbb{R}, M) \) be an artin local ring and \( I, J \) be primary ideals of \( \mathbb{R}[x] \). Then:

(a) \( J, I \) coprime \( \iff \text{Rad}(J), \text{Rad}(I) \) coprime;

(b) let \( J \) and \( I \) be non-nil: \( \text{Rad}(J) = \text{Rad}(I) \Rightarrow J, I \) coprime.

**Proof.** (a) \((\iff)\): This is obvious because \( \text{Rad}(J) \subset J \) and \( \text{Rad}(I) \subset I \).

\((\Rightarrow)\): We choose \( p \in \text{Rad}(J) \), \( q \in \text{Rad}(I) \) such that \( p + q = 1 \). Now there exist \( n, m \in \mathbb{N} \) with \( p^m \in J \) and \( q^n \in I \) such that
\[
1 = 1^{m+n-1} = (p + q)^{m+n-1} = \sum_{k=1}^{m+n-1} \binom{m+n-1}{k} p^k q^{m+n-1-k} = p^m(\ldots) + q^n(\ldots) \in J + I,
\]
which implies \( 1 \in J + I \).

(b) We know from Lemma 3.9 that \( \text{Rad}(J) = M[x] + (\alpha) \), \( \text{Rad}(I) = M[x] + (\beta) \) with suitable \( \alpha, \beta \in \mathbb{R}[x] \) monic and \( \bar{\alpha}, \bar{\beta} \in \bar{\mathbb{R}}[x] \) coprime. Hence, \( 1 \in \bar{\alpha} + \bar{\beta} \), so \( 1 + \nu \in (\alpha) + (\beta) \) with some \( \nu \in M[x] \). Thus, \( \text{Rad}(J) \) and \( \text{Rad}(I) \) are coprime and, with part (a), \( J \) and \( I \) are coprime. \( \square \)
Lemma 4.3. Let $R$ be a noetherian ring and $E$ be an $R$-free $R[x]$-module. $E$ primary $\iff$ $\text{Ann}_{R[x]}(E)$ primary.

Proof. Let $A := \text{Ann}_{R[x]}(E)$.

($\Rightarrow$): Let $\alpha \beta \in A$, $\beta \not\in A$ implying that there is $0 \neq e \in E$ with $\beta e \neq 0$. But $(\alpha \beta)e = 0 = \alpha(\beta e)$ and $E$ is primary, hence, $\alpha \in \text{Rad}(A)$.

($\Leftarrow$) Let $0 \neq e \in E$, $ae = 0$. We know that

$$((\alpha) + A) \cdot ((\alpha) \cap A) \subseteq (\alpha) \cap A.$$ 

Case 1: $(\alpha) \cdot A = (\alpha) \cap A$. For noetherian rings this means that $(\alpha) + A = R[x]$. Hence, there exist $\beta \in R[x]$, $\gamma \in A$ with $\beta \alpha + \gamma = 1$. $1 \cdot e = \beta(\alpha e) + \gamma e = \beta 0 + 0$, a contradiction.

Case 2: $(\alpha) \cdot A \neq (\alpha) \cap A$. There exists a $\beta \in (\alpha) \cap A$, $\beta \not\in (\alpha) \cdot A$ such that $\beta = \alpha \gamma \in A$, $\gamma \not\in A$, hence, $\alpha \in \text{Rad}(A)$.

We are interested in artin local rings, but these are noetherian by definition, so we can apply the following important theorem.

Theorem 4.4. In a noetherian ring $R$ every ideal $J$ has a primary decomposition into primary ideals $Q_i$ (unique up to order)

$$J = \bigcap_{i=1}^{m} Q_i, \quad Q_i \not\subseteq \bigcap_{j \neq i} Q_j \quad (i = 1, \ldots, m)$$

and all $\text{Rad}(Q_i)$ are different.

If all the $Q_i$ are mutually coprime, then even

$$J \cong \prod_{i=1}^{m} Q_i.$$ 

For the proof of the first part see [3]. For the second part, we refer to [13].

Theorem 4.5 (Primary decomposition of modules). Let $(R, M)$ be an artin local ring, $E \in \text{Mod}_n(R[x])$. Then there exist $L_i \in \text{Mod}_n(R[x])$, $L_i \subset E$, primary and endomorphisms $f_i = f|_{L_i}$, such that

$$E \cong \bigoplus_{i=1}^{m} L_i \quad \text{and} \quad \text{Ann}_{R[x]}(E) \cong \prod_{i=1}^{m} \text{Ann}_{R[x]}(L_i).$$

Proof. Applying Theorem 4.4 we have a primary decomposition of $\text{Ann}_{R[x]}(E) = \bigcap_i Q_i$, each $Q_i$ primary. Because $E$ has finite rank, all $Q_i$'s are nonnil. Lemma 4.2 then assures us that all $Q_i$ are mutually coprime, hence, $\text{Ann}_{R[x]}(E) \cong \prod_i Q_i$. 
Let $L_i := \prod_{j \neq i} Q_j \cdot E$, $K_i := \prod_{j=1}^i Q_j \cdot E$. We wish to show that $E = L_1 \oplus L_2 \oplus \cdots \oplus L_i \oplus K_i$ for $i = 0, \ldots, m$ by induction. Surely, $L_0 = \text{Ann}(E)E = 0$, $K_0 = E$, and $K_m = 0$. We show, that $K_{i-1} = L_i \oplus K_i$:

$$L_i + K_i = \left( \prod_{j \neq i} Q_j + \prod_{j=1}^i Q_j \right) E = \prod_{j=1}^{i-1} Q_j \left( \prod_{j=i+1}^m Q_j \right) E = \prod_{j=i+1}^m (Q_j + Q_i) K_{i-1} = K_{i-1},$$

because all $Q_j$'s are coprime. And in the same way, $L_i \cap K_i = \prod_{j=1}^m Q_j E = \text{Ann}(E)E = 0$.

Each $L_i$ is $R$-free, because it is $R$-projective (as direct summand of an $R$-free module), hence, $R$-free by Theorem 3.8. Each $L_i$ is primary, because $\text{Ann}(L_i) = Q_i$ and by Lemma 4.3. □

Example 4.6. Let $R = \mathbb{Z}_4$, $E = e_1 R \oplus e_2 R$. The fa of Fig. 3(a) corresponds to the transition matrix

$$A = \begin{pmatrix} 3 & 3 \\ 0 & 0 \end{pmatrix}.$$ 

$A^2 + A = 0$ implies $\text{Ann}(E) = (x^2 + x)$ with primary decomposition $(x)(x + 1)$. Hence,

$L_1 = (x) E = (3e_1 + 3e_2) \mathbb{Z}_4$, $f_1 = f \mid L_1 = (3)$,

$L_2 = (x + 1) E = (e_2) \mathbb{Z}_4$, $f_2 = f \mid L_2 = (0)$.

In relation to the new basis $\{3e_1 + 3e_2, e_2\}$, we have the transition matrix

$$A^* = \begin{pmatrix} 3 & 0 \\ 0 & 0 \end{pmatrix}$$

and the fa in Fig. 3(b).

5. Cyclic decomposition

Due to Theorem 4.5 we can assume without loss of generality to start with a local artin ring $(R, M)$ and a primary $E \in \text{Mod}_R(R[x])$. In general, a decomposition of $E$ into cyclic $R[x]$-modules is not possible. We give the following example.
Example 5.1. Let \( R = \mathbb{Z}_4 \), \( E = e_1 \mathbb{R} \oplus e_2 \mathbb{R} \). The two fa's in Fig. 4 are equivalent. They correspond to the matrices

\[
A = \begin{pmatrix} 1 & 2 \\ 2 & 3 \end{pmatrix}, \quad A' = \begin{pmatrix} 3 & 2 \\ 2 & 1 \end{pmatrix}.
\]

By trying all transformations of \( GL_2(\mathbb{Z}_4) \), we see that \( \{A, A'\} \) is the similarity-class of \( A \). And neither \( A \) nor \( A' \) are representations of cyclic modules.

That's why we define a weaker condition than the direct sum. Let \( L_i \) be \( R[x] \)-submodules of \( E \) (\( i = 1, \ldots, k \)) with \( \sum_{i=1}^{k} L_i = E \).

Definition 5.2. The sum \( E = \sum_{i=1}^{k} L_i \) is called direct sum modulo \( M \) if \( \overline{E} = \bigoplus_{i=1}^{k} \overline{L}_i \), denoted by \( M \sum_{i=1}^{k} L_i \).

It is easy to see that \( E = M \sum_{i} L_i \) iff \( (L_i + ME) \cap \sum_{j \neq i} L_j \subseteq ME \). We recall that an \( R[x] \)-module \( E \) is called cyclic if \( E \) can be generated by one element; we then have \( E \cong R[x]/\text{Ann}(E) \).

Lemma 5.3. With \( (R, M) \) and \( E \) as above, there exist monic and irreducible \( \alpha_i \in \overline{R}[x] \) and \( s_i \in \mathbb{N} \) \( (i = 1, \ldots, k) \), such that \( \overline{E} = \bigoplus_{i=1}^{k} L'_i \) and \( L'_i \cong \overline{R}[x]/(\alpha_i^{s_i}) \).

Proof. Because \( e \) is an \( R[x] \)-module, we can apply the structure-theorem for finitely generated modules over the principal ideal domain \( \overline{R}[x] = R[x]/M[x] = (R/M)[x] \) (e.g., [3]). Because \( e \) is primary, so is \( \overline{E} \), hence, all submodules \( L'_i \). A primary ideal in \( \overline{R}[x] \) is a potency of a prime ideal \( (\alpha_i)^{s_i} \). ∎

These \( \overline{R}[x] \)-submodules \( L'_i \subseteq \overline{E} \) can be lifted to \( R[x] \)-submodules \( L_i \) in the following way: Let \( e'_i \in L'_i \) be a generator of \( L'_i \) and choose \( e_i \in \pi^{-1}(e'_i) \subseteq E \) arbitrary: then \( L_i := R[x] \cdot e_i \) \( (i = 1, \ldots, k) \). Each \( L_i \) is cyclic by definition but in general not \( R \)-free. Because \( \pi((L_i + ME) \cap \sum_{j \neq i} L_j) = L'_i \cap \sum_{j \neq i} L_j = 0 \) we have proved the following theorem.

Theorem 5.4. Let \( (R, M) \) be an artin local ring and \( E \in \text{Mod}_n(R[x]) \) be primary. Then there exist cyclic \( R[x] \)-modules \( L_i \subseteq E \) \( (i = 1, \ldots, k) \) such that \( E = M \sum_{i=1}^{k} L_i \) (sum modulo \( M \)).

![Fig. 4. Counterexample: an fa over \( \mathbb{Z}_4 \) which is not decomposable into shift-registers.](image)
Theorem 5.5. With \((R, M)\) and \(E\) as above:

\[
E \equiv \bigoplus_{i=1}^{k} L_i \iff L_i \text{ is } \text{R-free} \quad (i = 1, \ldots, k)
\]

\[
\iff \text{Ann}_{R[x]}(L_1) \text{ is a principal ideal} \quad (i = 1, \ldots, k).
\]

Proof. (a) \((\Rightarrow)\): \(E\) is \(R\)-free and \(L_i\) a direct summand of \(E\), hence, \(L_i\) is \(R\)-projective; then use Theorem 3.8.

\((\Leftarrow)\): From Theorem 3.8 we can conclude that \(L_1 \cap \sum_{i>1} L_i\) is \(R\)-free and from the definition of the sum mod \(M\), we know that

\[
(L_1 + ME) \cap \sum_{i>1} L_i < ME \Rightarrow L_1 \cap \sum_{i>1} L_i = 0.
\]

Now continue with \(\sum_{i>1} L_i\) by induction.

(b) Let \(i = 1, \ldots, k\) arbitrary, \(e\) a generator of \(L_i\) and \(d := d_i\), then \(B := \{e, xe, \ldots, x^{d-1}e\}\) is an \(R\)-basis for \(L_i\).

\((\Rightarrow)\): \(x^d e = \sum_{j=0}^{d-1} a_j x^j e \in L\) implying \(\alpha := x^d - \sum_{j=0}^{d-1} a_j x^j \in \text{Ann}(L)\) and \(\alpha\) has degree \(d\). According to Lemma 3.9, \(\text{Ann}(L) = (\alpha) + N\) with \(N \subseteq M[x]\). If \(N \neq 0\), then \(\exists \neq \beta \in N\), \(\deg(\beta) < d\) (Lemma 3.9), but this leads to a contradiction with the fact that the basis \(B\) is linearly independent.

\((\Leftarrow)\): Without loss of generality, \(\text{Ann}(L_i)\) is generated by an \(\alpha \in R[x]\) with a non-nil leading coefficient. Obviously, \(\deg(\alpha) = d\). Because \(\text{Ann}(L_i)\) contains no polynomials of smaller degree, there are no relations of the elements of \(B\) possible, hence, \(B\) is a basis.

Example 5.6. Let \(R = \mathbb{Z}_4\), \(E = \bigoplus_{i=1}^{4} e_i \mathbb{Z}_4\). The \(fa\) in Fig. 5(a) corresponds to the transition matrix

\[
A = \begin{pmatrix}
0 & 1 & 0 & 2 \\
1 & 2 & 0 & 0 \\
0 & 0 & 1 & 0 \\
4 & 0 & 1 & 0
\end{pmatrix}.
\]

\(\text{Ann}(E) = ((x^2 - 1)(x^2 - 2x - 1), 4(x^2 - 1))\).

Following the derivation and notation of Theorem 5.4, we get \(\bar{R}[x] = \mathbb{Z}_2[x]\), \(\bar{E} = \bigoplus_{i=1}^{4} \bar{e}_i \mathbb{Z}_2\) and \(\text{Ann}_{\mathbb{Z}_2[x]}(\bar{E}) = (x^2 + 1)\). \(L_1 = L_{\mathbb{Z}_2}(\bar{e}_1, \bar{e}_2)\), analogously, \(L_2 = L_{\mathbb{Z}_2}(\bar{e}_3, \bar{e}_4)\). Now we choose \(\hat{e}_1 := e_1 + 2e_3\), \(\hat{e}_2 := 3e_3\) and find

\[
L_1 = L_{\mathbb{Z}_2[x]}(\hat{e}_1) = L_{\mathbb{Z}_2}(\hat{e}_1, x \hat{e}_1, (4x + 4) \hat{e}_2),
\]

\[
L_2 = L_{\mathbb{Z}_2}(\hat{e}_2, x \hat{e}_2, (4x + 4) \hat{e}_1),
\]

both are not \(\mathbb{Z}_2\)-free.
Fig. 5. Three equivalent fa's: simplification by cyclic decomposition.

With the new basis \{\hat{e}_i\}, we get a new transition matrix \( A^* \)
\[
A^* = \begin{pmatrix}
0 & 1 & 0 & 0 \\
1 & 2 & 4 & 0 \\
0 & 0 & 0 & 1 \\
4 & 0 & 1 & 0
\end{pmatrix} = \begin{pmatrix}
0 & 1 & 0 & 0 \\
1 & 2 & 0 & 0 \\
0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1
\end{pmatrix} + \begin{pmatrix}
0 & 0 & 0 & 0 \\
0 & 0 & 4 & 0 \\
0 & 0 & 0 & 0 \\
4 & 0 & 0 & 0
\end{pmatrix}.
\]

Because \( L_1 \) and \( L_2 \) are not \( \mathbb{Z}_8 \)-free, the two shift-registers are connected, but with the following restrictions to the connections:

1. they are only connected by elements of the nilradical (the components of the 'twist-matrix');
2. they end only in the first delay element (highest index) of each shift-register.

**Definition 5.7.** A primary \( R \)-free \( R[x] \)-module is called **twisted** if it is not isomorphic to a direct sum of cyclic \( R[x] \)-modules.

**Theorem 5.4** gives us necessary and sufficient conditions whether a module is twisted or not. But we have the unpleasant situation in that the submodules \( L_i \) are not independent of the choice of \( e_i \in \pi^{-1}(e'_i) \). For one choice of \( e_i \), \( L_i \) can be cyclic and for another choice is not. In the following corollary we give an ‘algorithmic’ approach to the problem of the missing independency.
Corollary 5.8. With \((R, M)\) and \(E\) as above, \(E = \bigoplus_{i=1}^{m} L_i\), let \(\alpha_i \in R[x]\) be monic with \((\alpha_i) = \text{Ann}(L_i) \subset \tilde{R}[x]\). Then \(E\) is not twisted iff there exist \(\nu_i \in M[x]\) \((i = 1, \ldots, k)\) such that \((\alpha_i + \nu_i)L_i \subset (\alpha_i + \nu_i)M E\). If \(E\) is not twisted, then \(\text{Ann}(E) = \bigcap_{i=1}^{k} (\alpha_i + \nu_i)\).

Proof. \((\Rightarrow)\): This is obvious from Theorem 5.5: we set \(\nu_i := 0\).

\((\Leftarrow)\): There exists an \(m_i \in ME\) such that \((\alpha_i + \nu_i)e_i = (\alpha_i + \nu_i)m_i\) for the \(L_i\)-generators \(e_i\) implying \((\alpha_i + \nu_i)(e_i - m_i) = 0\). Define \(L_0^0 := R[x](e_i - m_i); L_0^0\) is \(R\)-free, and \(L_i = L_i\) implies \(E = \bigoplus_{i=1}^{k} L_i^0\) and Theorem 5.4 finishes the proof:

\[
\text{Ann}(E) = \text{Ann} \left( \bigoplus_{i} L_i \right) = \bigcap_{i} \text{Ann}(L_i) = \bigcap_{i} (\alpha_i + \nu_i). \quad \square
\]

Example 5.6. (Continued). We set \(\alpha_1 = x^2 + 1 \in \mathbb{Z}_8[x]\), \(\nu_1 = nx + m\) \((n, m \in (2) \subset \mathbb{Z}_8)\).

\((x^2 + nx + m + 1)\tilde{e}_1 = \tilde{e}_1((m + 2) + x(n + 2)) + 4\tilde{e}_2\) and, for \(n = m = 6\), we find \((x^2 - 2x - 1)\tilde{e}_1 = (x^2 - 2x - 1)2x\tilde{e}_2 + 4\tilde{e}_2\). Hence, with a new choice of \(\tilde{e}_1 := \tilde{e}_1 - 2x\tilde{e}_2 = e_1 + 2e_4 + 2e_4, L_2^0\) is \(\mathbb{Z}_8\)-free, \(\text{Ann}(L_2^0) = (x^2 - 2x - 1)\). In an analogous way we choose \(\tilde{e}_2 := \tilde{e}_2 - 2x\tilde{e}_1 = e_3 + 2e_2\) and \(L_2^2\) becomes \(\mathbb{Z}_8\)-free too, \(\text{Ann}(L_2^2) = (x^2 - 1)\). The transition matrix \(A^*\) becomes

\[
A^* = \begin{pmatrix}
0 & 1 & 0 & 0 \\
1 & 2 & 0 & 0 \\
0 & 0 & 0 & 1 \\
0 & 0 & 1 & 0
\end{pmatrix},
\]
corresponding to the fa in fig. 5(c).

\[
E\text{ is not twisted } \Rightarrow \text{Ann}(E) = (x^2 - 2x - 1) \cap (x^2 - 1) = (((x^2 - 2x - 1)(x^2 - 1), 4(x^2 - 1)).
\]

6. A special case with a recursive criterion

We continue the problem of the last section, where \((R, M)\) is an artin local ring and \(E \in \text{Mod}_n(R[x])\) is primary. To formulate the special case of interest, we need a definition first. We keep in mind that according to Theorem 5.4 \(E = \bigoplus_{i=1}^{k} L_i\), with cyclic \(R[x]\)-modules \(L_i \subset E\) \((i = 1, \ldots, k)\).

Definition 6.1. A primary module \(E = \bigoplus_{i=1}^{k} L_i \in \text{Mod}_n(R[x])\) is called full of degree \(d\) if all \(L_i\) have \(d\) linear independent generators.

In other terms, \(\dim_R(L_i) = d\) \((i = 1, \ldots, k)\). The fa corresponding to a full module of degree \(d\) is characterised by a constant number of \(d\) delay-elements in each shift-register.
Let \( A := R[x]/\text{Ann}(E) \). Surely, \( E \) is an \( A \)-module.

This section has the following motivation: An \( fa \) corresponding to a full module consists of shift-registers \( \mathcal{S}_i \) \((i = 1, \ldots, k)\) and of connections between these shift-registers described by the 'twist-matrix'. We now want to consider a shift-register as a 'vector-delay-element', as a delay-element \( \mathcal{S}_i \) over \( A \) and the multiplication elements in the connections of the \( \mathcal{S}_i \)'s as elements of \( A \) (Fig. 6).

![Diagram](a)

![Diagram](b)

Fig. 6. (a) A diagram of an \( fa \) over \( (R, M) \) corresponding to a full module of degree 3. (b) A diagram of an equivalent \( fa \) over \( A = R[x]/\text{Ann}(E) \).

We choose a minimal set of \( A \)-generators \( \{e_1, \ldots, e_k\} \) of \( E \). Because every module is the image of a free module, we have the projection \( \rho : F \to E \) for the free \( A \)-module \( F \) with basis \( \{b_1, \ldots, b_k\} \), \( \rho(b_i) = e_i \) \((i = 1, \ldots, k)\). We get the short exact sequence

\[
0 \to \ker(\rho) \to F \xrightarrow{\rho} E \to 0.
\]

**Lemma 6.2.** Let \( E = \bigoplus_{i=1}^k L_i \) be a full \( A \)-module of degree \( d \). Then there exists \( \alpha \in A \) monic of degree \( d \) such that \( \text{im}(\alpha) \subset ME \). \( \alpha \) is unique up to polynomials in \( MA \) of degree \( d - 1 \).

**Proof.** For a full module, we can always choose \( \alpha \in A \) monic with \( \tilde{\alpha} = \text{Ann}(L_i) \) \((i = 1, \ldots, k)\). \( \deg(\alpha) = \deg(\tilde{\alpha}) = \dim_k(L_i) = d \). For all \( e \in E \), \( \tau(\alpha e) = \tilde{\alpha} \bar{e} = 0 \), hence, \( e \in ME \). \( \Box \)

The generators of \( \ker(\rho) \) are determined by the relations in \( E \). They are of the form \( \alpha b_i = \sum_{j=1}^k \beta_{ij} b_j \) \((i = 1, \ldots, k)\), \( \alpha \in A \) monic, \( \beta_{ij} \in MA \). We choose \( \alpha \) according
to Lemma 6.2. Now we define $h \in \text{End}(F)$ by $h(b_i) := \alpha b_i - \sum_{j=1}^{k} \beta_j b_j \ (i = 1, \ldots, k)$ and have thus found the exact sequence

$$F \xrightarrow{h} F \xrightarrow{\rho} E \to 0.$$  

Notice that $E \cong \text{coker}(h)$. Now, define $f_{\alpha} := \alpha - h$.

**Theorem 6.3.** Let $E \in \text{Mod}_n(A)$ be full of degree $d$. Then the following properties are equivalent:

1. $E$ is not twisted with cyclic submodules of rank $d \ (i = 1, \ldots, k)$;
2. $h$ is diagonalisable with monic eigenvalue-polynomials of degree $d \ (i = 1, \ldots, k)$;
3. $f_{\alpha} \in \text{Hom}(F, MF)$ is diagonalisable with eigenvalue-polynomials in $\text{MA}$ of degree $< d \ (i = 1, \ldots, k)$.

**Proof.** (1) $\Rightarrow$ (2): In Lemma 3.9 and in the proof of Theorem 5.5 we used the fact that $x^d \cdot e_i = \beta_i e_i$, $\deg(\beta_i) < d \Rightarrow h(b_i) = (x^d - \beta_i) b_i$, hence, $h$ is diagonal in relation to the basis $\{b_i\}$ and $\deg (x^d - \beta_i) = d$.

(2) $\Leftarrow$ (1): Let $h$ be diagonalisable. Then there is a basis-transformation $t \in \text{Aut}(F)$ such that $t^{-1} \cdot h \cdot t$ is diagonal.

$$
\begin{array}{cccc}
F & \xrightarrow{h} & F & \xrightarrow{\rho} & E & \to 0 \\
\downarrow t & & \downarrow t & & \downarrow t & \\
F & \xrightarrow{th^{-1}} & F & \xrightarrow{\rho} & E & \to 0 \\
\end{array}
$$

In general it is not possible to extend $t$ to $E$ as $A$-homomorphism because $t(\ker(\rho)) \not\subset \ker(\rho)$. But it is sufficient to treat $E$ as a (free) $R$-module. Then there exists a $\hat{t} \in \text{Aut}_R(E)$ with $\rho t = \hat{t} \rho$. Starting with $h(b_i) = \alpha b_i - \sum_{j} \beta_j b_i$ we then get $(\hat{t}h^{-1})(tb_i) = \alpha (tb_i) - \sum \beta_j (tb_i)$, because $h$ diagonalisable. $\deg(\gamma_i) < d$. With $e_i := \rho(tb_i)$, we get $\gamma_i(e_i) = \gamma \rho(tb_i) = \rho \gamma_i(tb_i) = \rho (\hat{t} h^{-1})(tb_i) = \hat{t}(\rho h) t^{-1}(tb_i) = 0$, because $\rho h = 0$.

(2) $\iff$ (3): This immediately follows from the equivalence of (1) and (2) and from the definition of $f_{\alpha}$. $\square$

**Notation.** $E' := F/M^{z-1}F, \ R' := R[x]/(\text{Ann}(E) + M^{z-1})$.

**Theorem 6.4.** Let $(R, M)$ be a local artin principal ideal ring, $M = (m)$, $z$ the nilpotency of $M$ and $E \in \text{Mod}_n(R[x])$. Then there exist $R$-module isomorphisms

- (a) $\phi: \text{Hom}_R(F, MF) \to \text{End}_R(E')$;
- (b) $\psi: \text{Aut}_R(F)/(1 + \text{Hom}(F, M^{z-1}F)) \to \text{Aut}_R(E')$;
- (c) $\phi$ and $\psi$ commute with the action of the automorphism-group on the endomorphism-ring, especially,

$$\bar{\phi}: \text{Hom}_R(E, ME)/\text{Aut}_R(E) \cong \text{End}_R(E')/\text{Aut}_R(E').$$
Proof. For this proof, let $H := \text{Hom}(F, M_{r^{-1}} F)$.

(a) Let $m : F \to (m)E$ (multiplication by $m$). Then $\ker(m) = M_{r^{-1}} E$. In an analogous way, we can associate $f : E \to (m)E$ with $\bar{f} : E' \to (m)E$ and thus define $f' := \varphi(f) := \bar{m}^{-1} \cdot \bar{f} \in \text{End}(E')$, with $f' \pi = \pi f$.

$\varphi$ is mono, because $\ker(\varphi) = \{f \in \text{Hom}(E, ME) | \bar{f} = 0\} = 0$.

$\varphi$ is epi: Let $f' \in \text{End}(E')$ be arbitrary:

$$
\begin{array}{ccc}
E & \xrightarrow{m} & (m)E \\
\pi & \downarrow & \bar{m} \\
E' & \xrightarrow{f'} & E'
\end{array}
$$

Because $E$ is free, $f'$ can be lifted along $\pi$ to get $mf \in \text{End}(E)$. $\varphi^{-1}(f') := mf$ implies $\varphi(mf) = \bar{m}^{-1} \cdot (mf) = \pi \bar{f} = f'$.

(b) Define $\psi' : \text{Aut}(E) \to \text{Aut}(E')$ by $\psi(g) := g'$, with $\pi g = g' \pi$ for $g \in \text{Aut}(E)$. $\psi'$ is well-defined and epi (like part (a)).

$$
\begin{array}{ccc}
E & \xrightarrow{g} & E \\
\pi & \downarrow & \pi \\
E' & \xrightarrow{g'} & E'
\end{array}
$$

$\psi'(g) = 1_E \leftrightarrow \pi = \pi g \leftrightarrow 1_E - g \in \ker(\pi) \leftrightarrow 1_E - g \in H$. Hence, $\ker(\psi') = 1 + H$ and $\psi$ is mono.

(c) $\alpha$ is the action of $g \in \text{Aut}(E)$ on $f \in \text{End}(E)$, $\alpha(g)f := g^{-1}fg \in \text{End}(E)$. Let $\bar{g} \in \text{Aut}(E)/(1 + H)$ and $mf \in \text{Hom}(E, ME)$. Then $\varphi^* \alpha(\bar{g})(mf) = \varphi^*(\bar{g}^{-1}mf\bar{g}) = (\bar{g}^{-1}f\bar{g})'$ and $\alpha\psi(\bar{g})(f') = (\bar{g}')^{-1}f'\bar{g}'$. Because of the linearity of $f$, $\bar{g}$, and $\pi$, $(\bar{g}^{-1}f\bar{g})' = (\bar{g}')^{-1}f'\bar{g}'$. □

**Theorem 6.5.** Let $(R, M)$ be an artin local, principal ideal ring and $E \in \text{Mod}_n(R[x])$ be full of degree $d$. Then $E$ not twisted is equivalent to $f' := \varphi(f) \in \text{End}_R(E')$ diagonalisable.

**Proof.** According to Theorem 6.3, we have to show that $\varphi : \text{Hom}(F, MF) \to \text{End}(E')$
Compact Linear Automata

Let $B := \{b_1, \ldots, b_k\}$ be a basis for $F$, $\pi : F \rightarrow E' = F/M^{2-1}F$ the canonical projection and $\pi(B)$ a basis in $E'$.

\[
\begin{array}{cccc}
A & F & \xrightarrow{f_\alpha} & MF \\
\downarrow \pi & \downarrow \pi & \uparrow = m \\
R' & E' & \xrightarrow{f} & E'
\end{array}
\]

The theorem is an immediate consequence of the fact that $\pi$ and $m$ are diagonal in relation to $B$. □

Example 6.6. Let $R = \mathbb{Z}_9$, $E = \bigoplus_{i=1}^{6} e_i \cdot \mathbb{Z}_9$. We want to apply the theorems of this section to the $\mathbb{F}$ given in Fig. 7(a). The transition matrix is given in relation to the basis $\{e_1, \ldots, e_6\}$ by

\[
\begin{pmatrix}
0 & 1 & 0 & 0 & 0 & 0 \\
5 & 6 & 0 & 0 & 3 & 3 \\
0 & 0 & 0 & 1 & 0 & 0 \\
3 & 6 & 2 & 0 & 6 & 3 \\
0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 8 & 0
\end{pmatrix}
\]

Ann($E$) = $((x^2 + 1), 3(x^2 + 1))$. We choose $\alpha = x^2 - 2$. Over $R' = \mathbb{Z}_3[x]/(x^2 + 1)$ we have the $\mathbb{F}$ of Fig. 7(b) with the transition matrix

\[
\begin{pmatrix}
1 + 2x & 0 & 1 + x \\
1 + 2x & 0 & 2 + x \\
0 & 0 & 2
\end{pmatrix}
\]

$f' \in \text{End}(E')$ suggests to define an $R'[y]$-module-structure on $E'$ by $y \cdot e := f' \cdot e$ ($\forall e \in E'$). The primary decomposition of $E' \in \text{Mod}_3(R'[y])$ shows that $f'$ is diagonalisable by a $t \in \text{Aut}(E')$; we get $f'^*$ and the $\mathbb{F}$ of Fig. 7(c).

\[
\begin{pmatrix}
1 + 2x & 0 & 0 \\
0 & 0 & 0 \\
0 & 0 & 2
\end{pmatrix}
\]

The action of $\psi^{-1}(t)$ on $f$ gives $f^*$ corresponding to the $\mathbb{F}$ of Fig. 7(d), a parallel connection of shift-registers.

\[
\begin{pmatrix}
0 & 1 & 0 & 0 & 0 & 0 \\
5 & 6 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 2 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 8 & 0
\end{pmatrix}
\]
Let $(R, M)$ be a local Artin ring and $E \in \text{Mod}_n(R[x])$ primary. Then $R'$ is local Artin and $\text{Rad}(R) = \text{Rad}(\text{Ann}(E))/(\text{Ann}(E) + M^{z-1})$.

**Proof.** Because every prime ideal contains the nilradical, it is sufficient to show, that $\text{Rad}(R')$ is a maximal ideal.

\[
\text{Rad}(R') = (\text{Rad}(R[x]) + \text{Rad}(\text{Ann}(E) + M^{z-1}))/\text{Ann}(E) + M^{z-1})
= \text{Rad}(\text{Ann}(E))/(\text{Ann}(E) + M^{z-1}).
\]
Thus,
\[ R'/\text{Rad}(R') = R[x]/\text{Rad}(\text{Ann}(E) + M^{x-1}) \cong R[x]/(M[x] + (\alpha)), \]
according to Lemma 3.9, with \( \alpha \) a monic and fundamental irreducible polynomial. Hence, \( R'/\text{Rad}(R') = \bar{R}[x]/(\bar{\alpha}) \) which is a field. \( \square \)

We remember having started with a local artin principal ideal ring \( R \), a free \( R \)-module \( E \), and an \( f \in \text{End}_R(E) \) in such a way that the \( R[x] \)-module-structure induced by \( f \) gives a full module of degree \( d \). We have transferred the problem of the 'twist-matrix' to a new local artin ring \( R' \) (Lemma 6.7), a free \( R' \)-module \( E' \) of dimension \( \dim_R(E)/d \), and a \( f' \in \text{End}_{R'}(E') \) (Theorem 6.4) with the property '\( E \) not twisted \( \Leftrightarrow f' \) diagonalisable' (Theorem 6.5). The notation should suggest the recursive criterion: we start with \( R' \), \( E' \), and \( f' \) all over again: primary decomposition, cyclic decomposition and so on (see Example 6.6).

7. Final remarks

To end, we would like to give some words concerning generalisations which we have in mind.

(1) We could start with an artin ring \( R \) instead of \( \mathbb{Z}_n (n \in \mathbb{N}) \), because \( R \) is always isomorphic to a product of local artin rings, and we could apply Theorem 3.1.

(2) The restriction to principal ideal rings \((R, M)\) in Section 6 made the notation easier, but is a little too restricting. It would be enough to ask that \( f(E) \subseteq (m)E \) for some suitable \( m \in M \) to prove Theorem 6.4.

(3) Let \( E \) be a module that is not full. Then it is possible to define an embedding \( E \subseteq E' \) into a full module \( E' \). But it is not always possible to restrict basis-transformations of \( E' \) to \( E \).

(4) The thoughts presented in this paper suggest to look for a recursive definition of a 'canonical form' for square matrices over artin rings; but we should generalise Section 6 to do so.

Acknowledgment

The author wishes to thank Prof. U. Würgler for many helpful suggestions throughout the project.

References


