ASPECTS ON ANALYSIS AND SYNTHESIS OF LINEAR DISCRETE SYSTEMS OVER THE FINITE FIELD $\mathbb{F}_q$

J. Reger[†] **and K. Schmidt**[‡]

Lehrstuhl für Regelungstechnik, Universität Erlangen-Nürnberg
Cauerstraße 7, D–91058 Erlangen, Germany

[†]phone: +49(0)9131/85-27134
e-mail: reger@ieee.org

[‡]phone: +49(0)9131/85-27133
e-mail: klaus.schmidt@rt.eei.uni-erlangen.de

Keywords: Linear Modular Systems, Finite Fields, Polynomial Approach, Feedback Shift Registers.

Abstract

This note presents a method for synthesizing a static state feedback controller for multiple-input linear systems over discrete sets. The method allows of a complete setting of the cyclic subspaces of the closed loop system by specifying invariant polynomials of the closed loop system. To this end, fundamentals of finite field theory and basic elements of the polynomial approach are developed towards a means of analysis of the cyclic behavior of the system, which, with regard to synthesis issues, results in an algorithm for setting the invariant polynomials of the system dynamics in the closed loop system. The basic ideas are illustrated in an example.

1 Introduction

Modeling finite state automata in a discrete state space, we address some theoretical issues of analysis and synthesis of linear automata. Within the scope of analyzing the transient behavior of finite state automata it is a well-known fact that the finite state space splits into cyclic and acyclic subspaces [2]. However, even in the linear case it remained unclear which structural, algebraic properties are to represent this cyclic behavior, due to a lack of sufficient criteria. Based on a particular state space model over finite fields [3] another state space approach, first of all for the linear case, was made recently [7]. In this approach, drawing benefit from some results of feedback shift register theory [4] a complete analysis of the cyclic subspace by means of invariant polynomials was presented. Thus, a straightforward step is to extend the setting by specifying a state feedback so as to determine the cyclic structure of the closed loop system, which is the focus of the paper. In addition to this, the underlying discrete system theory is prepared in a manner such that the reader who is familiar with the continuous system theory is enabled to understand the main concepts.

This note is organized as follows: In Section 2 basic algebraic concepts are recalled. Section 3 characterizes the notion of invariant polynomials. In Section 4 essential properties of Linear Modular Systems are discussed. The analysis for cyclic subspaces is described in Section 5. Section 6 deals with the synthesis of a static state feedback controller. The example in Section 7 exposes the main steps of the method before conclusions are drawn in Section 8.

2 Algebraic Preliminaries

For the purpose of a better understanding of the basic ideas some unalterable algebraic fundamentals have to be developed. A concise introduction to finite fields is given by [6].

2.1 Basic Properties of Finite Fields

Since a special type of field is dealt with some terminology is recalled.

Definition 2.1 (Groups) *A group is a set $\mathcal{G}$ together with a binary operation $*$ such that*

1. *for all $a, b \in \mathcal{G}$, $a * b \in \mathcal{G}$.*
2. *$*$ is associative, i. e. $a*(b*c) = (a*b)*c$ for any $a, b, c \in \mathcal{G}$.*
3. *There exists an identity element e such that for all $a \in \mathcal{G}$, $a * e = e * a = a$.*
4. *There exists an inverse element $a^{-1} \in \mathcal{G}$ for each $a \in \mathcal{G}$ such that $a * a^{-1} = a^{-1} * a = e$.*

Moreover, a group is commutative (or abelian) if for all $a, b \in \mathcal{G}$, $a * b = b * a$. A group is called finite if the set $\mathcal{G}$ contains finitely many elements.

Definition 2.2 (Field) *A set $\mathbb{F}$ with the operations addition and multiplication, $+$ and $\cdot$, is a field if*

1. *$\mathbb{F}$ is a commutative group wrt. addition.*
2. *$\mathbb{F} \setminus \{0\}$ is a commutative group wrt. multiplication.*
3. *$\mathbb{F}$ is distributive wrt. addition and multiplication.*

A field $\mathbb{F}$ with q elements, denoted by $\mathbb{F}_q$, is called finite if it contains finitely many elements.

Definition 2.3 (Galois-Field) *The set of integral numbers* $\{0,1,\ldots,q-1\}$*, where q prime, with operations addition and multiplication mod q, is a finite field called Galois-Field* $\mathbb{F}_q$*.*

The primality of q is decisive for the existence of a multiplicative inverse element in general (otherwise zero divisors occur), e. g. $2\cdot 3 \bmod 6 = 0$. In the sequel we will concentrate on Galois-Fields only. Consequently, addition and multiplication in $\mathbb{F}_q$ implicitly are understood modulo q.

Theorem 2.1 (Fermat's Little Theorem) *Let* $q\in\mathbb{Z}$ *be prime. Then for all integers* λ *not divisible by q, q divides* $\lambda^{q-1}-1$*.*

Corrolary 2.1 *Every* $\lambda\in\mathbb{F}_q$ *satisfies* $\lambda^q=\lambda$*.*

Hence, a polynomial $p\in\mathbb{F}_q[\lambda]$ over a finite field $\mathbb{F}_q$, where $\mathbb{F}_q[\lambda]$ denotes the ring of polynomials with coefficients in $\mathbb{F}_q$, can be identical to zero for arbitrary $\lambda\in\mathbb{F}_q$, whereas for a polynomial $p\in\mathbb{R}[\lambda]$ over the field of real numbers $\mathbb{R}$ this holds if and only if all coefficients are zero.

2.2 Polynomials over Finite Fields

2.2.1 Reducible and Irreducible Polynomials

Polynomials over the field of real numbers $\mathbb{R}$ generally can be factorized (reduced) quadratically over $\mathbb{R}$. This need not be the case for finite fields $\mathbb{F}_q$, which will be shown in the following.

Definition 2.4 (Monic Polynomial) *A polynomial* $p(\lambda)=\sum_{i=0}^{d}a_i\lambda^i$ *with degree d is called monic if* $a_d=1$*.*

Definition 2.5 (Irreducibe Polynomial) *A non-constant polynomial* $p\in\mathbb{F}[\lambda]$ *is called irreducible over* $\mathbb{F}$ *if whenever* $p(\lambda)=g(\lambda)h(\lambda)$ *in* $\mathbb{F}[\lambda]$ *then either* $g(\lambda)$ *or* $h(\lambda)$ *is a constant.*

Theorem 2.2 (Unique Factorization Theorem) *Any polynomial* $p\in\mathbb{F}[\lambda]$ *can be written in the form*

$$p = a\,{p_1}^{e_1}\cdots{p_k}^{e_k}\,, \tag{1}$$

where $a\in\mathbb{F}$*,* $p_1,\ldots,p_k$ *are distinct monic irreducible polynomials in* $\mathbb{F}[\lambda]$*, and* $e_1,\ldots,e_k$ *are positive integers. Moreover, this factorization is unique apart from the order of the factors.*

Example: $p(\lambda)=\lambda^5+\lambda^2+\lambda+1=(\lambda^3+\lambda+1)(\lambda+1)^2$, $p\in\mathbb{F}_2[\lambda]$, because $\lambda^3+\lambda+1$ and $\lambda+1$ are irreducible over $\mathbb{F}_2$.

2.2.2 Period of Polynomials

Definition 2.6 (Period of a Polynomial) *Let* $p\in\mathbb{F}_q[\lambda]$ *be a nonzero polynomial. If* $p(0)\neq 0$*, then the least positive integer e for which* $p(\lambda)$ *divides* λ^e-1 *is called the period* τ_p *of the polynomial p. If* $p(0)=0$*, then* $p(\lambda)=\lambda^h g(\lambda)$*, where* $h\in\mathbb{N}$ *and* $g\in\mathbb{F}_q[\lambda]$ *with* $g(0)\neq 0$*, and* τ_p *is defined as* τ_g*.*

In practice periods of polynomials do not have to be calculated. They can be found in tabulars [6], or are internally tabulated in computer algebra software like Maple or Mathematica.

3 Structural Properties of Matrices over $\mathbb{F}_q$

3.1 Similarity of Matrices

The major properties of a matrix reside in structural invariants. These are preserved under so-called similarity transforms. We recall some basic terminology.

Definition 3.1 (Similarity of a Matrix) *Matrices* $\mathbf{A}_1,\ \mathbf{A}_2\in\mathbb{F}^{n\times n}$ *are similar if for some invertible matrix* $\mathbf{T}\in\mathbb{F}^{n\times n}$

$$\mathbf{A}_1=\mathbf{T}^{-1}\mathbf{A}_2\mathbf{T}\,. \tag{2}$$

Definition 3.2 (Rational Matrix) *A matrix* $\mathbf{R}(\lambda)$*, the elements of which are fractions of polynomials over* $\mathbb{F}[\lambda]$ *is called a rational matrix. If the denominator polynomial of each element of* $\mathbf{R}(\lambda)$ *is equal to one the matrix is a polynomial matrix.*

Definition 3.3 (Unimodular Matrix) *If the determinant of a polynomial matrix is a scalar in the underlying field* $\mathbb{F}$*, the matrix is called unimodular.*

Theorem 3.1 (Smith Form of a Matrix) *For any* $\mathbf{A}\in\mathbb{F}^{n\times n}$ *there exist unimodular matrices* $\mathbf{U}(\lambda)$ *and* $\mathbf{V}(\lambda)$ *such that*

$$\mathbf{U}(\lambda)(\lambda\mathbf{I}-\mathbf{A})\mathbf{V}(\lambda)=\mathbf{S}(\lambda) \tag{3}$$

with

$$\mathbf{S}(\lambda)=\begin{bmatrix} c_1(\lambda) & 0 & \cdots & 0\\ 0 & c_2(\lambda) & & \vdots\\ \vdots & & \ddots & 0\\ 0 & \cdots & 0 & c_n(\lambda)\end{bmatrix}, \tag{4}$$

where the monic polynomials $c_{i+1}|c_i,\ i=1,\ldots,n-1$*.*

Matrices $\mathbf{A}_1$ and $\mathbf{A}_2$ are similar iff they have the same Smith form. Since the polynomials $c_i(\lambda)$ are preserved under similarity transforms this gives rise to a further definition.

3.2 Invariant Polynomials

Definition 3.4 (Similarity Invariants) *The monic polynomials* $c_i(\lambda)$*,* $i=1,\ldots,n$ *referring to a* $\mathbf{S}(\lambda)$ *are the similarity invariants of* $\mathbf{A}$*.*

Note that the uppermost polynomial $c_1(\lambda)$ is the minimal polynomial of the dynamics $\mathbf{A}$. The product of all similarity invariants is the characteristical polynomial $\det(\lambda\mathbf{I}-\mathbf{A})$ of $\mathbf{A}$.

Definition 3.5 (Elementary Divisor Polynomials) *The unique irreducible factor polynomials* $p_j(\lambda)$ *of all the* $c_i(\lambda)$*,* $i=1,\ldots,n$ *referring to the Smith Form* $\mathbf{S}(\lambda)$ *of* $\mathbf{A}$ *are called elementary divisor polynomials of* $\mathbf{A}$*.*

3.3 Remark

In order to facilitate the synthesis procedure the Jordan Normal Form of a matrix is not introduced here. This would have meant to define eigenvalues, thus to calculate the eigenvalues of $\mathbf{A}$ in some extension field $\mathbb{F}_{q^k}, k=1,2,\ldots$ of $\mathbb{F}_q$, which is much more cumbersome than for real numbers.

4 Linear Modular Systems over $\mathbb{F}_q$

In the preceding chapters basic properties of finite fields have been recapitulated and the relevance of polynomials over finite fields has been demonstrated. In this chapter the notion of Linear Modular Systems is introduced as a representation of a class of systems over finite fields and analogies to linear continuous systems (over the field of real numbers $\mathbb{R}$) are shown.

Linear Modular Systems over $\mathbb{F}_q$ (LMS(q)) can be expressed in terms of the following matrix equation [4]

$$\mathbf{x}[k+1] = \mathbf{A}\mathbf{x}[k] + \mathbf{B}\mathbf{u}[k]\,. \tag{5}$$

The matrix $\mathbf{A} \in \mathbb{F}_q^{n\times n}$ is the dynamics of the system and $\mathbf{B} \in \mathbb{F}_q^{n\times m}$ is the input matrix, $\mathbf{u}[k]$ is the input vector and $\mathbf{x}[k]$ is the state vector of the LMS(q).

4.1 $\mathcal{A}$-Transform

As for linear continuous systems an image domain can be introduced for the LMS(q).

Definition 4.1 *The $\mathcal{A}$-Transform for causal, discrete functions $f[k]$ over $\mathbb{F}_q$ is:*

$$F(a) := \mathcal{A}(f[k]) := \sum_{k=0}^{\infty} f[k]\cdot a^{-k}. \tag{6}$$

For completeness, relevant relations are shown in Table 1.

time function	$\mathcal{A}$-transformed function
$\sum_\nu \alpha_\nu \cdot f_\nu[k]$	$\sum_\nu \alpha_\nu \cdot F_\nu(a)$
$f[k+1]$	$a\cdot F(a) - a\,f[0]$

Table 1: $\mathcal{A}$ - Transform for causal functions f[k]

Using (6) the state equation (5) can be transformed into the $\mathcal{A}$-Domain and a solution for the system state can be verified.

4.2 Solution of the State Equation

With Table 1 the $\mathcal{A}$-Transform of (5) reads[1]

$$a\mathbf{X}(a) = \mathbf{A}\mathbf{X}(a) + \mathbf{B}\mathbf{U}(a) + a\mathbf{x}[0]\,. \tag{7}$$

This representation directly leads to the computation of the $\mathcal{A}$-Transform of the system state

$$\mathbf{X}(a) = (a\mathbf{I} - \mathbf{A})^{-1}(\mathbf{B}\mathbf{U}(a) + a\mathbf{x}[0])\,. \tag{8}$$

The result can readily be used to determine the well-known solution of the difference equation [1, 4]:

$$\mathbf{x}[k] = \mathbf{A}^k\mathbf{x}[0] + \sum_{i=0}^{k-1}\mathbf{A}^{k-1-i}\mathbf{B}\mathbf{u}[i], \tag{9}$$

where the system state depends on the initial state $\mathbf{x}[0]$ and on the history of the input vector $\mathbf{u}[k]$. One more important property of the system representation (8) is used in Section 6 to prove one main result of this paper.

4.3 l-controllability

In analogy to linear continuous systems an equivalent definition of controllability can be given in the framework of LMS(q).

Definition 4.2 *An LMS(q) of order n is l-controllable if for all ordered pairs $(\mathbf{x}_1, \mathbf{x}_2)$ the system can be driven from state $\mathbf{x}_1$ to state $\mathbf{x}_2$ in exactly l steps. An LMS(q) is controllable iff it is l-controllable for some l.*

In combination with (9) the following theorem emerges [1].

Theorem 4.1 *An LMS(q) of order n is l-controllable iff $[\mathbf{B}\ \mathbf{A}\mathbf{B}\ \ldots\ \mathbf{A}^{l-1}\mathbf{B}]$ has full rank n.*

4.4 Controllability Companion Form

Using Theorem 4.1 the *reduced controllability matrix* $\mathbf{L}$ of an LMS(q) is attainable by choosing n linearly independent columns from $[\mathbf{B}\ \mathbf{A}\mathbf{B}\ \ldots\ \mathbf{A}^{l-1}\mathbf{B}]$ with minimal powers of $\mathbf{A}$ [8][2]

$$\mathbf{L} = [\mathbf{b}_1, \ldots, \mathbf{A}^{c_1-1}\mathbf{b}_1, \ldots, \mathbf{b}_m, \ldots, \mathbf{A}^{c_m-1}\mathbf{b}_m]\,. \tag{10}$$

The set of integers c_i, $i = 1, \ldots, m$ is called the set of controllability indices of the LMS(q). The following properties hold:

- the set of c_i is unique,
- the set of c_i is invariant wrt. similarity transformations,
- $\sum_{i=1}^m c_i = n$,
- the list $\sigma_i = \sum_{j=1}^i c_j$, $i = 1, \ldots, m$, decomposes the system representation into structural subunits.

Given a controllable LMS(q) a characteristic companion form of the state equations (5) can be found by executing similarity transformations, using (10) and the set of c_i. It is called the controllability companion form (CCF) [8] and shall be marked with the superscript c in the following sections:

$$\mathbf{x}^c[k+1] = \underbrace{\begin{bmatrix} \mathbf{A}^c_{1,1} & \cdots & \mathbf{A}^c_{1,m} \\ \mathbf{A}^c_{2,1} & \cdots & \mathbf{A}^c_{2,m} \\ \vdots & \ddots & \vdots \\ \mathbf{A}^c_{m,1} & \cdots & \mathbf{A}^c_{m,m} \end{bmatrix}}_{\mathbf{A}^c} \mathbf{x}^c[k] + \underbrace{\begin{bmatrix} 0 & 0 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & x & x & \cdots & x & x \\ 0 & 0 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 1 & x & \cdots & x & x \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 1 \end{bmatrix}}_{\mathbf{B}^c} \mathbf{u}[k],$$

$$\mathbf{A}^c_{i,i} = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & 1 \\ x & x & x & x & x \end{bmatrix} \quad \text{and} \quad \mathbf{A}^c_{i,j,i\neq j} = \begin{bmatrix} 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ x & x & x & x & x \end{bmatrix}.$$

For separating structural and informal properties of the system in CCF the rows with undetermined entries x are represented in two matrices:

$$\mathbf{A}^c_{\sigma_i} = \begin{bmatrix} \text{row } \sigma_1 \text{ of } \mathbf{A}^c \\ \text{row } \sigma_2 \text{ of } \mathbf{A}^c \\ \vdots \\ \text{row } \sigma_m \text{ of } \mathbf{A}^c \end{bmatrix}, \ \mathbf{B}^c_{\sigma_i} = \begin{bmatrix} \text{row } \sigma_1 \text{ of } \mathbf{B}^c \\ \text{row } \sigma_2 \text{ of } \mathbf{B}^c \\ \vdots \\ \text{row } \sigma_m \text{ of } \mathbf{B}^c \end{bmatrix} = \begin{bmatrix} 1 & x & x & \cdots & x \\ 0 & 1 & x & \cdots & x \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{bmatrix}.$$

These matrices will be needed in Section 6.4.2.

[1] Capital letters denote functions in the $\mathcal{A}$-Domain.

[2] The vectors $\mathbf{b}_i$, $i = 1, \ldots, m$ are the column vectors of the input matrix $\mathbf{B}$.

5 Cycle Sum of a Linear Modular System

Linear Modular systems typically show cyclic behavior. In the autonomous case $\mathbf{B}=\mathbf{0}$ any information needed to analyze for cyclic subspaces is included in structural invariants of the dynamics $\mathbf{A}$. For brevity the main theorem is recalled from [4, 7].

The state space decomposes in periodic and aperiodic subspaces, which are constituted by the following definition.

Definition 5.1 (Period of States) *The period of a state $\mathbf{x}[k] \in \mathbb{F}_q^n$ is the least $\tau \in \mathbb{N}$ such that $\mathbf{x}[k+\tau]=\mathbf{x}[k]$.*

Generally, state spaces decompose in more than one cyclic subspace. Let their number be N. All occurring subspace cyclicities can be written in a more convenient form by

Definition 5.2 (Cycle Sum) *The cycle sum Σ is the formal sum of cycle terms*

$$\Sigma = \nu_1[\tau_1] \dotplus \nu_2[\tau_2] \dotplus \ldots \dotplus \nu_N[\tau_N]\,, \tag{11}$$

where ν_i is the number of cycles of length τ_i and the relation $\nu_i[\tau] \dotplus \nu_j[\tau] = (\nu_i+\nu_j)[\tau]$ is satisfied.

Definition 5.3 (Product of Cycle Terms) *The product*

$$\nu_1[\tau_1]\nu_2[\tau_2] = \nu_1\nu_2 \gcd(\tau_1,\tau_2)[\operatorname{lcm}(\tau_1,\tau_2)] \tag{12}$$

is called cycle term product. The expressions $\gcd(\tau_1,\tau_2)$ and $\operatorname{lcm}(\tau_1,\tau_2)$ are greatest common divisor and least common multiple of τ_1, τ_2 respectively.

Theorem 5.1 (Superposition) *The cycle sum Σ superposing e cycle sums Σ_i can be calculated distributively by the product*

$$\Sigma = \Sigma_1\Sigma_2\cdots\Sigma_e\,. \tag{13}$$

An adapted version of a theorem in [4, 7] can now be stated:

Theorem 5.2 (Cycle Sum of an autonomous LMS) *Let $\mathbf{S}(\lambda)$ be the Smith Form of the dynamics of an autonomous LMS(q), $\mathcal{P}$ the set of factorized elementary divisor polynomials $p_i = (p_{i,\mathrm{irr}})^{e_i} \in \mathbb{F}_q[\lambda]$, where $p_{i,\mathrm{irr}}$ is an irreducible basis polynomial with $p_{i,\mathrm{irr}}(0) \neq 0$. Then each $p_i \in \mathcal{P}$ contributes the cycle sum*

$$\Sigma_i = 1[1] + \frac{q^{d_i}-1}{\tau_1^{(i)}}[\tau_1^{(i)}] + \frac{q^{2d_i}-q^{d_i}}{\tau_2^{(i)}}[\tau_2^{(i)}] + \ldots + \frac{q^{e_i d_i}-q^{(e_i-1)d_i}}{\tau_{e_i}^{(i)}}[\tau_{e_i}^{(i)}]\,, \tag{14}$$

where d_i marks the degree of $p_{i,\mathrm{irr}}$ and $\tau_j^{(i)}$ denotes the period of $(p_{i,\mathrm{irr}})^j$. For the entire LMS(q) the cycle sum Σ follows by superposition of all $|\mathcal{P}|$ cycle sums Σ_i.

Remark: As the stress is put on the synthesis of the cyclic structure of the state space, the periodic states $\mathbf{x}_\tau$ themselves are of minor relevance. Therefore their calculation is not considered here.

6 Synthesis

6.1 Main Objectives

In the previous section the cyclic properties of LMS(q) have been examined. Now the question arises, if and how these properties can be changed. Thus, the main objective of this section is to find a constructive synthesis procedure for changing the cyclic properties of an LMS(q).

6.2 State Feedback

In Section 5 we have seen that the cyclic properties of LMS(q) are directly related to the invariant polynomials[3] of the dynamics $\mathbf{A}$. Furthermore, it is clear from the theory of linear continuous systems that the invariant polynomials of an LMS(q) can be changed by linear state feedback

$$\mathbf{u}[k] = -\mathbf{K}\mathbf{x}[k] + \mathbf{w}[k] \tag{15}$$

with the corresponding state equation

$$\mathbf{x}[k+1] = (\mathbf{A}-\mathbf{B}\mathbf{K})\,\mathbf{x}[k] + \mathbf{B}\mathbf{w}[k]. \tag{16}$$

In this context it is decisive that we must actually consider the invariant polynomials, which is more restrictive than regarding the characteristic polynomial of $\mathbf{A}-\mathbf{B}\mathbf{K}$.

6.3 Structural Theorem

The following important theorem shows in which range the invariant polynomials of an LMS(q) can be changed.

Theorem 6.1 (Structural Theorem) *Given a controllable LMS(q) with controllability indices $c_1 \geq \ldots \geq c_m$ and desired invariant polynomials $c_{i,\mathbf{K}}(a)$, $\deg(c_{1,\mathbf{K}}(a)) \geq \ldots \geq \deg(c_{m,\mathbf{K}}(a))$, there exists a constant matrix $\mathbf{K}$ with $\mathbf{A}-\mathbf{B}\mathbf{K}$ with invariant polynomials $c_{i,\mathbf{K}}(a)$ iff*

$$\sum_{i=1}^{k} \deg(c_{i,\mathbf{K}}(a)) \geq \sum_{i=1}^{k} c_i \quad \forall k = 1,2,\ldots,m. \tag{17}$$

Since the synthesis of linear state feedback in the "Time Domain" in general is not straight forward a new approach using polynomial matrices shall be introduced.

6.4 A Frequency Domain for Finite Fields?

6.4.1 Transfer Function

Comparing (8) and (3) it is obvious that the cyclic properties of the system state are described by the expression $(a\mathbf{I}-\mathbf{A})^{-1}$, which is also contained in the system "transfer function"

$$\mathbf{X}(a)|_{\mathbf{x}[0]=0} = \mathbf{F}(a)\,\mathbf{U}(a) = (a\mathbf{I}-\mathbf{A})^{-1}\mathbf{B}\mathbf{U}(a). \tag{18}$$

Thus in the next sections we concentrate on computing a linear state feedback by using equation (18).

[3] Elementary divisor polynomials and invariant polynomials are equivalent.

6.4.2 Polynomial Matrix Fraction

At first some denotation, which will be used in the sequel, shall be defined and two important theorems are recalled.

Definition 6.1 (Right Polynomial Matrix Fraction) *A right polynomial matrix fraction (RPMF) of a rational matrix* $\mathbf{R}(a)$ *is an expression of the following form*

$$\mathbf{R}(a) = \mathbf{N}(a)\,\mathbf{D}^{-1}(a) \qquad (19)$$

with denominator matrix $\mathbf{D}(a)$ *and numerator matrix* $\mathbf{N}(a)$*.*

Theorem 6.2 (Conservation) *The product of an arbitrary polynomial matrix* $\mathbf{R}(a)$ *and an unimodular polynomial matrix* $\mathbf{U}(a)$ *has the same invariant polynomials as* $\mathbf{R}(a)$*.*

As the transfer matrix in (18) is a rational matrix the known results on rational matrices can be applied.

Theorem 6.3 (Existence) *For each rational matrix* $\mathbf{R}(a)$ *there is a right-prime polynomial matrix fraction.*

This means that each transfer matrix can be represented like in (19). In accordance with [8] a closed expression for the polynomial matrix fraction for a system representation in CCF is

$$\mathbf{F}(a) = \mathbf{S}(a)\,[(\mathbf{B}^c_{\sigma_i})^{-1}(\boldsymbol{\gamma}(a) - \mathbf{A}^c_{\sigma_i}\,\mathbf{S}^c(a))]^{-1}, \qquad (20)$$

with

$$\mathbf{S}(a) = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ a & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ a^{c_1-1} & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & a^{c_2-1} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & a^{c_p-1} \end{bmatrix}, \; \boldsymbol{\gamma}(a) = \begin{bmatrix} a^{c_1} & 0 & \cdots & 0 \\ 0 & a^{c_2} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & a^{c_p} \end{bmatrix}. \qquad (21)$$

This means that if the LMS(q) is given in CCF it is straight forward to find a closed expression for the polynomial matrix fraction of the system transfer matrix (18).

The same is valid for the system with state feedback matrix **K** in (16). In this case the polynomial matrix fraction reads

$$\mathbf{F}(a) = \mathbf{S}(a)\,[\underbrace{(\mathbf{B}^c_{\sigma_i})^{-1}(\boldsymbol{\gamma}(a) - \overbrace{(\mathbf{A}^c_{\sigma_i} - \mathbf{B}^c_{\sigma_i}\,\mathbf{K}^c)}^{\mathbf{A}^c_{\sigma_i,\mathbf{K}}}\,\mathbf{S}(a))}_{\mathbf{D_K}(a)}]^{-1}. \qquad (22)$$

This RPMF shows the following important properties:

- the numerator matrix $\mathbf{S}(a)$ of the RPMF is not changed by linear state feedback.
- the denominator matrix $\mathbf{D_K}(a)$ and the corresponding system matrix have the same invariant polynomials.
- the controllability indices c_i coincide with the column degrees[4] of the denominator matrix.

As the feedback matrix **K** can be uniquely determined if $\mathbf{D_K}(a)$ in (22) is known, it is evident that the problem of finding an adequate state feedback to fit the given LMS(q) with desired invariant polynomials reduces to determining a denominator matrix $\mathbf{D_K}(a)$ with the following properties:

(i) the invariant polynomials of $\mathbf{D_K}(a)$ must coincide with the desired invariant polynomials $c_{i,\mathbf{K}}(a)$.

(ii) the column degrees $\deg(col_i)$ of $\mathbf{D_K}(a)$ must coincide with the controllability indices c_i of the LMS(q) [5].

Since $\mathbf{D_K}(a) = (\mathbf{B}^c_{\sigma_i})^{-1}\mathbf{D}^*_{\mathbf{K}}(a)$, it suffices to consider the matrix $\mathbf{D}^*_{\mathbf{K}}(a)$ because $(\mathbf{B}^c_{\sigma_i})^{-1}$ is unimodular and triangular and thus $\mathbf{D_K}(a)$ has the same invariant polynomials and the same column degrees as $\mathbf{D_K}(a)$.

6.5 Main Theorem

With the results from the previous sections the main theorem for the synthesis of linear state feedback can be specified.

Theorem 6.4 *Let a controllable LMS(q) be given in CCF, let* c_i*,* $i = 1, \cdots, m$ *be the controllability indices, let* $c_{i,\mathbf{K}}(a)$*,* $i = 1, \ldots, m$ *be desired invariant polynomials and let* $\mathbf{D}^*(a) = \mathrm{diag}(c_{i,\mathbf{K}}(a))$*,* $i = 1, \ldots, m$*, let* $\deg(c_{1,\mathbf{K}}(a)) \geq \cdots \geq \deg(c_{m,\mathbf{K}}(a))$ *and* $\sum_{i=1}^{m} \deg(c_{i,\mathbf{K}}(a)) = \sum_{i=1}^{m} c_i = n$*. An algorithm which admits to determine a feedback matrix* **K***, if any, is as follows:*

1. *Verify the structural theorem 6.1 for* c_i *and* $c_{i,\mathbf{K}}(a)$*. If (17) holds* **go to** *2, else the algorithm fails.*

2. *Examine* $\mathbf{D}^*(a)$*.*
   - **if** *the column degrees of* $\mathbf{D}^*(a)$ *coincide with the ordered list of controllability indices* **go to** *step 5.*
   - **else** *detect the first column of* $\mathbf{D}^*(a)$ *which differs from the ordered list of controllability indices, starting with column* 1*. Denote this column* col_u*. (*$\deg(col_u) > c_u$*)*
   - *Do the same beginning with column m. Denote the specified column* col_d*. (*$\deg(col_d) < c_d$*)*

3. *Adapt the column degrees of* $\mathbf{D}^*(a)$ *by applying elementary operations*[6]
   - *Multiply* row_d *by "a" and add the result to* row_u
$\Rightarrow \mathbf{D}^*(a) \rightarrow \mathbf{D}^+(a)$
   - **if** $\deg(col_u^+) = \deg(col_u) - 1$
     - $\mathbf{D}^+(a) \rightarrow \mathbf{D}^{++}(a)$ *and* **go to** *step 4.*
   - **else**
     - *Define:* $r := \deg(col_u) - \deg(col_d) - 1$

[4] This is the highest polynomial degree in the corresponding column.

[5] For abbreviation, the i-th matrix columns and rows are denoted by col_i and row_i, $i = 1, \ldots, m$, respectively. The controllability indices c_i are not changed by linear state feedback.

[6] These are operations that are equivalent to multiplications with unimodular matrices. As a consequence, doing this way the invariant polynomials of the considered matrix are not changed.

- *Multiply* col_u^+ *with* a^r *and subtract the result from* col_d^+. $\Rightarrow \mathbf{D}^+(a) \rightarrow \mathbf{D}^{++}(a)$

4. *Generate the column pointer matrix* Γ^{++} *of* $\mathbf{D}^{++}(a)$[7] $\Rightarrow \mathbf{D}^*(a) = (\Gamma^{++})^{-1}\,\mathbf{D}^{++}(a)$ *and* **go to** *step 2*

5. $\mathbf{D}^*_{\mathbf{K}}(a) := \mathbf{D}^*(a)$
   return $\mathbf{D}^*_{\mathbf{K}}(a)$

If the conditions from above are fulfilled, and $\mathbf{D}^*_{\mathbf{K}}(a)$ *is returned by the algorithm, then* $\mathbf{D}^*_{\mathbf{K}}(a)$ *can be generated by linear state feedback.*

In Section 6.4.2 it was argued that if the matrix $\mathbf{D}_{\mathbf{K}}(a)$ is known it is straight forward to compute $\mathbf{K}$. This is shown now:

$$\begin{aligned}\mathbf{D}_{\mathbf{K}}(a) &= (\mathbf{B}^c_{\sigma_i})^{-1}\mathbf{D}^*_{\mathbf{K}}(a)\\ &= (\mathbf{B}^c_{\sigma_i})^{-1}(\boldsymbol{\gamma}(a) - \mathbf{A}^c_{\sigma_i,\mathbf{K}}\mathbf{S}^c(a))\,.\end{aligned}$$

This leads to

$$\mathbf{A}^c_{\sigma_i,\mathbf{K}}\mathbf{S}^c(a) = \boldsymbol{\gamma}(a) - \mathbf{B}^c_{\sigma_i}\,\mathbf{D}_{\mathbf{K}}(a) \tag{23}$$

and by comparison of coefficients the matrix $\mathbf{A}^c_{\sigma_i,\mathbf{K}}$ can be determined. By equation (22) this directly provides

$$\mathbf{K}^c = (\mathbf{B}^c_{\sigma_i})^{-1}(\mathbf{A}^c_{\sigma_i} - \mathbf{A}^c_{\sigma_i,\mathbf{K}})\,. \tag{24}$$

7 Example

For a short example consider the following LMS(2) in CCF

$$\mathbf{A}^c = \begin{bmatrix} 0&1&0&0&0\\ 0&0&1&0&0\\ 0&0&0&0&0\\ 0&0&0&0&1\\ 1&0&0&1&0 \end{bmatrix},\ \mathbf{B}^c = \begin{bmatrix} 0&0\\ 0&0\\ 1&0\\ 0&0\\ 0&1 \end{bmatrix} \quad \rightarrow \quad \begin{aligned} \mathbf{A}^c_{\sigma_i} &= \begin{bmatrix} 0&0&0&0&0\\ 1&0&0&1&0 \end{bmatrix}\\ \mathbf{B}^c_{\sigma_i} &= \begin{bmatrix} 1&0\\ 0&1 \end{bmatrix} \end{aligned}$$

For analysis wrt. the autonomous case, $\mathbf{u}[k] = \mathbf{0}$, first, the Smith Form of the system dynamics $\mathbf{A}^c$ is determined, which yields one system invariant $\neq 1$, that is $c_1(\lambda) = \lambda^3(\lambda+1)^2$. Hence, the only elementary divisor polynomial $p_{i,\mathrm{irr}}(0) \neq 0$ is the elementary divisor polynomial $p_1(\lambda) = (\lambda+1)^2 = \lambda^2+1$, the period of which is $\tau_1 = 2$ (see Definition 2.6). Finally, by equations (14), (11) the cycle sum for the autonomous system reads

$$\Sigma = 1[1] \dot{+} \frac{2^1-1}{1}[1] \dot{+} \frac{2^2-2^1}{2}[2] = 2[1] \dot{+} 1[2]\,.$$

For a synthesis the controlled system shall have the invariant polynomials $c_{1,\mathbf{K}}(a) = (a^2+a+1)(a+1)^2$ and $c_{2,\mathbf{K}}(a) = a+1$ (control objective: $4[1] \dot{+} 2[2] \dot{+} 4[3] \dot{+} 2[6]$). The controllability indices are $c_1 = 3$ and $c_2 = 2$. By Theorem 6.4 we compute

$$\begin{aligned}
&\xrightarrow{1}\ \textstyle\sum_{i=1}^{1}\deg(c_{i,\mathbf{K}}(a)) = 4 \ \geq\ \sum_{i=1}^{1} c_i = 3 \quad \surd\\
&\phantom{\xrightarrow{1}}\ \textstyle\sum_{i=1}^{2}\deg(c_{i,\mathbf{K}}(a)) = 5 \ \geq\ \sum_{i=1}^{2} c_i = 5 \quad \surd\\
&\xrightarrow{2}\ \mathbf{D}^*(a) = \begin{bmatrix} a^4+a^3+a+1 & 0\\ 0 & a+1 \end{bmatrix}\\
&\xrightarrow{3}\ \mathbf{D}^+(a) = \begin{bmatrix} a^4+a^3+a+1 & a^2+a\\ 0 & a+1 \end{bmatrix} \longrightarrow \mathbf{D}^{++}(a) = \begin{bmatrix} a+1 & a^2+a\\ a^3+a^2 & a+1 \end{bmatrix}\\
&\xrightarrow{4}\ \mathbf{D}^*(a) = \begin{bmatrix} a^3+a^2 & a+1\\ a+1 & a^2+a \end{bmatrix} \quad \xrightarrow{2,5}\ \mathbf{D}^*_{\mathbf{K}}(a) = \begin{bmatrix} a^3+a^2 & a+1\\ a+1 & a^2+a \end{bmatrix}
\end{aligned}$$

Now $\mathbf{K}^c$ can be computed. With equation (23) we have

$$\mathbf{A}^c_{\sigma_i,\mathbf{K}}\begin{bmatrix} 1&0\\ a&0\\ a^2&0\\ 0&1\\ 0&a \end{bmatrix} = \underbrace{\begin{bmatrix} a^3&0\\ 0&a^2 \end{bmatrix}}_{\boldsymbol{\gamma}(a)} - \underbrace{\begin{bmatrix} 1&0\\ 0&1 \end{bmatrix}}_{\mathbf{B}^C_{\sigma_i}}\underbrace{\begin{bmatrix} a^3+a^2 & a+1\\ a+1 & a^2+a \end{bmatrix}}_{\mathbf{D}^*_{\mathbf{K}}(a)} = \begin{bmatrix} a^2 & a+1\\ a+1 & a \end{bmatrix}$$

and with (24) the feedback matrix $\mathbf{K}^C$, which fits the given system with the desired invariant polynomials, can be calculated

$$\mathbf{K}^c = \begin{bmatrix} 1&0\\ 0&1 \end{bmatrix}^{-1}\left(\begin{bmatrix} 0&0&0&0&0\\ 1&0&0&1&0 \end{bmatrix} - \begin{bmatrix} 0&0&1&1&1\\ 1&1&0&0&1 \end{bmatrix}\right) = \begin{bmatrix} 0&0&1&1&1\\ 0&1&0&1&1 \end{bmatrix}.$$

8 Conclusion

In this paper we have considered Linear Modular Systems over the Galois Field $\mathbb{F}_q$. In the analytic part it has been shown that the cyclic properties of this class of systems depend on the invariant polynomials of the system dynamics. Beyond this, an algorithm has been introduced that decides if there exists a linear feedback which fits the system with desired invariant polynomials and, if the decision is positive, computes an appropriate feedback matrix.[8] Further research will involve the nonlinear case and the computation of the cyclic state vectors.

Acknowledgments

This research was partially supported by Studienstiftung des deutschen Volkes and by Deutsche Forschungsgemeinschaft (DFG) under Grant No. RO 2262/3-1.

References

[1] M. Cohn. “Controllability in Linear Sequential Networks”, *IEEE Transactions on circuit theory*, **9**, pp. 74–78, (1962).

[2] D. Franke. “Sequentielle Systeme”, Vieweg, Braunschweig, (1994).

[3] R. Germundsson. “Symbolic Systems — Theory, Computation and Applications”, PhD thesis, Linköping, (1995).

[4] A. Gill. “Linear Modular Systems”. In: Zadeh L.A., Polak E., “System Theory”, McGraw-Hill, New York, (1969).

[5] V. Kučera. “Analysis and Design of Discrete Linear Control Systems”, Prentice Hall, Englewood Cliffs, (1995).

[6] R. Lidl, H. Niederreiter. “Introduction to Finite Fields and their Applications”, Cambridge Univ. Press, New York, (1994).

[7] J. Reger. “Cycle Analysis for Deterministic Finite State Automata”, *Proc. of 15th IFAC World-Congress*, Barcelona, (2002).

[8] W. A. Wolovich. “Linear Multivariable Systems”, Springer, New York, (1974).

[7] The scalar column pointer matrix consists of elements in $\mathbb{F}_q$ that are the coefficients of the highest degree monomials in a in each column of $\mathbf{D}^{++}(a)$.

[8] In general there does not exist an unique solution.