SYNTHESIS OF STATE FEEDBACK FOR LINEAR AUTOMATA IN THE FINITE FIELD $\mathbb{F}_2$ [1]

K. Schmidt and J. Reger, University of Erlangen-Nuremberg, Germany
Corresponding Author: K. Schmidt
Universitt Erlangen Nrnberg
Lehrstuhl fr Regelungstechnik
Cauerstrasse 7, 91058 Erlangen, Germany
Phone: +49 (0)9131/85-27133, Fax: +49 (0)9131/85-28715
email: schmidt@rt.eei.uni-erlangen.de

Abstract. Discrete event systems can be modelled by multilinear state equations over the finite field $\mathbb{F}_2$. This paper treats the synthesis of state feedback for the subclass of linear discrete systems over $\mathbb{F}_2$ with the aim of generating a closed-loop system with specified properties. In our approach the desired properties are related to system invariants. The computation of an appropriate state feedback is achieved by introducing a frequency domain and adopting the polynomial matrix method to linear discrete systems over $\mathbb{F}_2$.

1. Introduction

In the first paper of this series we motivate the description of discrete event systems via state space models in the finite field $\mathbb{F}_2$. It is shown that in general, multilinear state equations are obtained. Further on, the problem of determining the cyclic states is solved for the subclass of linear automata. In the paper on hand, linear automata described as linear discrete systems over the finite field $\mathbb{F}_2$ are under concern. The state equation is as follows [1]:

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

In this case, the matrix $\mathbf{A}$ is the system dynamics, $\mathbf{B}$ is the input matrix, $\mathbf{x}[k]$ is the current state and $\mathbf{x}[k+1]$ is the next state, whereby all vector and matrix entries are binary.

The most important property of this class of systems is the cyclicity of states[2], which uniquely corresponds to the elementary divisor polynomials of the system dynamics and can be directly related to the smith normal form of $\mathbf{A}$ [1], which has been shown in the first paper of this series.

Based on this knowledge the synthesis of linear state feedback for imposing properties on the controlled system (concerning the cyclicity of states) is performed. By imposing these properties, the elementary divisor polynomials of the closed loop dynamics are set.

In the scope of continuous systems this problem usually is solved by performing the parametric approach [2]. By means of this approach the synthesis of linear state feedback for linear multivariate systems can be carried out easily. To this end a closed-loop system with specified eigenvalues is established and the remaining degrees of freedom are used for adjusting the eigenspaces of the closed-loop system.

Dealing with discrete systems in $\mathbb{F}_2$ this approach would involve specifying the zeros of the elementary divisor polynomials and determining the desired eigenspaces of the closed-loop system. As this idea emerges to be inappropriate another method for synthesizing a linear state feedback has to be employed.

For linear continuous systems the polynomial matrix method in the frequency domain is used to compute a state feedback for achieving specified eigenvalues of the closed loop system by solving a diophantine equation [3]. This method is adapted to linear discrete systems over $\mathbb{F}_2$. At first the *$\mathcal{A}$-Transform* is introduced for generating a frequency domain-like representation of the given linear automaton [1]. Next a transfer function is defined for the linear automaton and a right polynomial matrix fraction description of this transfer function is obtained. The denominator matrix of this polynomial matrix fraction contains the similarity invariants and thus the cyclic properties of the original linear system. Due to this the synthesis problem reduces to specifying similarity invariants of the denominator matrix in the *$\mathcal{A}$-Domain* and computing the appropriate state feedback. This can easily be done by first evaluating an algorithm suggested by Kučera [3] and then utilizing the structure of a special normal form, the so-called controllability normal form. The latter is a major advantage in contrast to the usual method of solving a diophantine equation.

[1] This paper is part two of three papers dealing with the finite field description of finite state automata.
[2] This topic is treated in the first paper of this series.

By means of these results an algorithm is developed for generating a linear state feedback which fits a given linear automaton with specified cyclicity properties. Additionally the structural constraints for linear state feedback given by the structure theorem of Rosenbrock [3] are fulfilled automatically by the presented construction algorithm.
In the following section Linear Modular Systems over $\mathbb{F}_2$ are introduced. In Section 3 linear state feedback is introduced and the Rosenbrock Structure Theorem is related to our work. Section 4 defines a frequency domain for finite fields and determines a polynomial matrix fraction of the system transfer function. The main theorem is given in Section 5 and in Section 6 a detailed example illustrates the suggested method.

2. Linear Modular Systems over $\mathbb{F}_2$

In the first paper of this series the basic properties of finite fields are introduced. For completeness the most important terms which will be needed in the sequel are recapitulated.

2.1 The Finite Field $\mathbb{F}_2$

At first the definition of a galois field $\mathbb{F}_q$ shall be given and with this definition the galois field $\mathbb{F}_2$, which will be used throughout this paper, is introduced.

Definition 1 *(Galois Field) Let $\{0,1,\ldots,q-1\}$ be the set of integers smaller than a prime integer q. Let further be $\Phi : \mathbb{Z} \bmod q \to \mathbb{F}_q$ the map which is defined by $\Phi([a]) = a$ whereby $a = \{0,1,\ldots,q-1\}$ and $\mathbb{Z}$ is the set of integers. Then $\mathbb{F}_q$ is a finite field called the Galois Field $\mathbb{F}_q$ of order q.*
In our framework we set $q = 2$ and thus define the addition and multiplication in $\mathbb{F}_2$ as[3]

$$\begin{aligned} a+b &:= a+b \bmod 2 \\ a\cdot b &:= a\cdot b \bmod 2 \end{aligned}$$

2.2 The State Equations

Over the finite field $\mathbb{F}_2$ the vector space of n-dimensional column vectors with entries in $\mathbb{F}_2$ shall be defined. Over this vector space the state equation of the so called Linear Modular Systems over $\mathbb{F}_2$[4], which are the common representation for linear discrete systems over $\mathbb{F}_2$, can be expressed in terms of the following matrix equation [1]:

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

whereby $\mathbf{A} \in \mathbb{F}_2^{n\times n}$ is the systems dynamics and $\mathbf{B} \in \mathbb{F}_2^{n\times m}$ is the input matrix, $\mathbf{u}[k]$ is the input vector and $\mathbf{x}[k]$ is the state vector of the LMS(2). All matrix and vector entries lie in $\mathbb{F}_2$.

2.3 Controllability

As the main goal of this paper involves the synthesis of a control for linear discrete systems over $\mathbb{F}_2$ the notion of controllability must be examined for the LMS(2). Thus at first the well-known solution of the state equation (1) is given.

$$\mathbf{x}[k] = \mathbf{A}^{k-1}\mathbf{x}[0] + \sum_{i=0}^{k-1} \mathbf{A}^{k-1-i}\mathbf{B}\,\mathbf{u}[i]. \tag{2}$$

Corresponding to this result controllability can now be defined for LMS(2) and a theorem can be stated [4].

Definition 2 (Controllability) *A nth-order LMS(2) is l-controllable iff for all ordered state 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. A LMS(2) is controllable iff it is l-controllable for some l.*

Theorem 1 (Controllability) *A nth-order LMS(2) is l-controllable iff $[\mathbf{B}\ \mathbf{AB}\ \ldots\ \mathbf{A}^{l-1}\mathbf{B}]$ has full rank n .*

This theorem will be used to establish a very usefull standard form, the controllability companion form, which can be determined by applying linear transformations to the state equation.

2.4 Controllability Companion Form

Using Theorem 1 the reduced controllability matrix $\mathbf{L}$ of an LMS(2) can be determined by choosing n linearly independent columns from $[\mathbf{B}\ \mathbf{AB}\ \ldots\ \mathbf{A}^{l-1}\mathbf{B}]$ with minimum multiples of $\mathbf{A}$ [5] [5].

$$\mathbf{L} = [\mathbf{b}_1, \ldots, \mathbf{A}^{c_1-1}\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{A}^{c_2-1}\mathbf{b}_2, \ldots, \mathbf{b}_m, \ldots, \mathbf{A}^{c_m-1}\mathbf{b}_m] \tag{3}$$

[3] In this galois fi eld the minus and the plus operation are equivalent, so only the plus operation will be used
[4] The abbreviation LMS(2) will be used in the sequel
[5] The $\mathbf{b}_i$, $1 \le i \le m$ are the column vectors of the input matrix $\mathbf{B}$.

The set of integers c_i, $i = 1, \ldots, m$ is called the set of controllability indices of the LMS(2) and holds the following properties:

- the set of c_i is unique,
- the set of c_i is invariant w.r.t. similarity transformations,
- $\sum_1^m c_i = n$,
- the list $\sigma_i = \sum_{j=1}^{i} c_j$, $j = 1, \ldots, m$, divides the system representation into structural subunits.

Given a controllable LMS(2) a characteristic companion form of the state equations (1) can be found by executing similarity transformations, using (3) and the set of c_i. It is called the controllability companion form (CCF) [5] and shall be considered with the superscript c in the following sections. The representation in CCF is

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

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

In this representation $\mathbf{A}^c_{i,i}$ is a matrix of dimension $c_i \times c_i$. For separating structural and informal properties of the system in CCF the rows with undetermined entries x are summarized 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 4.4. Considering the definitions from above we can now define the aims of our approach and we can cite a fundamental theorem which will provide a solution to the problem.

3. Structural Theorem

3.1 State Feedback

As was shown in the first paper of this series, a certain class of discrete event systems can be modelled as LMS(2). Further on it is proved that one important property of LMS(2) is the existence of cyclic states which are closely related to the elementary divisor polynomials of the system dynamics $\mathbf{A}$[6]. For the control synthesis of discrete event systems at first it is interesting to detect cyclic states and then to introduce a control which influences the cyclic properties of the given system.

Changing the elementary divisor polynomials, which is equivalent to changing the system invariants of a LMS(2), is closely related to changing the eigenvalues of the system dynamics $\mathbf{A}$. Form the framework of linear continuous systems (over the field $\mathbb{R}$) it is well-known that changing the eigenvalues of $\mathbf{A}$ can be done by introducing a linear state feedback $\mathbf{K}$ of the following form: $\mathbf{u}[k] = -\mathbf{K}\mathbf{x}[k] + \mathbf{w}[k]$. Reffering to this it is reasonable to introduce such a linear state feedback for LMS(2) which leeds to the following state representation:

$$\begin{aligned} \mathbf{u}[k] &= \mathbf{K}\mathbf{x}[k] + \mathbf{w}[k] \\ \mathbf{x}[k+1] &= (\mathbf{A} + \mathbf{B}\mathbf{K})\mathbf{x}[k] + \mathbf{B}\mathbf{w}[k] \end{aligned} \tag{4}$$

[6] and thus to the invariant polynomials of $\mathbf{A}$

For this structure the following important theorem can be stated.

3.2 Structural Constraints

Theorem 2 (Rosenbrock Structure Theorem) *Given a controllable LMS(2) with controllability indices* $c_1 \geq \ldots \geq c_m$ *and desired invariant polynomials* $c_{i,\mathbf{K}}(a)$, $\deg(c_{1,\mathbf{K}}(a)) \geq \ldots \geq \deg(c_{m,\mathbf{K}}(a))$, $c_{i+1,\mathbf{K}}|c_{i,\mathbf{K}}$. *There exists a constant matrix* $\mathbf{K}$ *with* $\mathbf{A}+\mathbf{BK}$ *having the invariant polynomials* $c_{i,\mathbf{K}}(a)$ *iff*

$$\sum_{i=1}^{k} \deg(c_{i,\mathbf{K}}(a)) \geq \sum_{i=1}^{k} c_i \quad \forall k = 1,2,\ldots,m \tag{5}$$

There are different methods to compute linear state feedback in the ”Time Domain” by specifying desired eigenvalues. At first one could think of pole placing methods. But it is obvious that specifying desired invariant polynomials is a stronger requirement than specifying desired eigenvalues. As a consequence standard pole placing methods are not relevant.
Further on one could think of the parametric approach, which enables the modification of the eigenstructure of the given system. But in this approach different problems evolve:

- in this approach the open-loop and the closed-loop eigenvalues should be distinct, which is not a general assumption in the framework of LMS(2).
- the problem of assigning multiple eigenvalues, which is common in the framework of LMS(2) becomes cumbersome as the computation of generalized eigenvectors is required in the parametric approach.
- the notion of eigenvalues is difficult in the framework of LMS(2) as the eigenvalues of a polynomial in $\mathbb{F}_2[\lambda]$[7] lie in the extension field of $\mathbb{F}_2$, which in opposite to the field of real numbers $\mathbb{R}$ has no unique defining element [6].
  As each polynomial in $\mathbb{R}[\lambda]$ can be quadratic factorized, the zeros of each polynomial in $\mathbb{R}[\lambda]$ lie in the extension field of complex numbers $\mathbb{C}$ with the unique defining element $i = \sqrt{-1}$. In the first paper of this series it has been shown that polynomials in $\mathbb{F}_2[\lambda]$ cannot be quadratic factorized in general. As a consequence the computation of eigenvalues in the extension field of $\mathbb{F}_2$ is not straight forward.
- as the structural theorem imposes constraints on the invariant polynomials of the system this turns out to be more feasible in the frequency domain even for continuous systems.

Regarding the issues from above, we will define a frequency domain for LMS(2) in the next section.

4. A Frequency Domain for LMS(2)

4.1 The $\mathcal{A}$-Transform

As for linear continuous systems an image domain can be introduced for the LMS(2).

Definition 3 ($\mathcal{A}$-Transform) *The* $\mathcal{A}$*-Transform for causal, discrete functions* $f[k]$ *over* $\mathbb{F}_2$ *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]

[7] $\mathbb{F}[\lambda]$ shall denote the ring of polynomials over the fi eld $\mathbb{F}$.

With (6), the state equation (1) can be transformed into the $\mathcal{A}$-Domain and as a first interesting feature the solution of the state equation can be verified.

4.2 Solution of the State Equation

With Table 1 the $\mathcal{A}$-Transform of (1) is[8]

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

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 former result can readily be used to determine the well-known solution of the difference equation by using the state representation in the $\mathcal{A}-Domain$ given by (8). To do this the inverse of the $\mathcal{A}-Transform$ shall be defined:

Definition 4 (Inverse of the $\mathcal{A}-Transform$) *The inverse of the $\mathcal{A}$-transform is given by*[9]

$$\begin{array}{rcl} \mathcal{A}^{-1}(\mathbf{F}(a)) & := & \mathrm{sequ}(\mathbf{f}[k]), k = 1, \dots, \infty \\ \mathbf{f}[k] & := & [a^k \mathbf{F}(a)]_{\mathrm{scal}}, \end{array} \tag{9}$$

whereby the operator $[a^k\mathbf{F}(a)]_{\mathrm{scal}}$ provides the scalar addend of the rational function $a^k\mathbf{F}(a)$.

Using this definition, the state vector $\mathbf{x}[k]$ in the time domain can be computed[10].

$$\begin{array}{rcl} \mathbf{x}[k] & = & [a^k\,\mathbf{X}(a)]_{\mathrm{scal}} = [a^k\,(a\,\mathbf{I} + \mathbf{A})^{-1}(\mathbf{B}\,\mathbf{U}(a) + a\,\mathbf{x}[0])]_{\mathrm{scal}} \\ & = & [a^k \frac{1}{a} \sum_{i=0}^{\infty} (\frac{\mathbf{A}}{a})^i (\mathbf{B} \sum_{j=0}^{\infty} \mathbf{u}[j] a^{-j} + a\,\mathbf{x}[0])]_{\mathrm{scal}} \\ & = & \mathbf{x}[0]\,\mathbf{A}^{k-1} + \mathbf{B}\mathbf{u}[k-1] + \mathbf{A}\,\mathbf{B}\mathbf{u}[k-2] + \cdots + \mathbf{A}^{k-1}\,\mathbf{B}\mathbf{u}[0], \end{array}$$

which equals (2). The system representation in the $\mathcal{A}-Domain$ cannot only be used to solve the state equation. As the most important feature this representation is useful for assigning the cyclic properties of the system.

4.3 Transfer Matrix

In the first paper of this series it has become clear that the cyclic properties of the system state are described by the term $(a\,\mathbf{I} + \mathbf{A})^{-1}$. If we look at (8) we can define the system "transfer matrix" $\mathbf{F}(a)$ by the following equation:

$$\mathbf{X}(a)|_{\mathbf{x}[0]=0} = \mathbf{F}(a)\,\mathbf{U}(a) = (a\,\mathbf{I} + \mathbf{A})^{-1}\mathbf{B}\,\mathbf{U}(a). \tag{10}$$

It is obvious that the cyclic properties of the system are contained in $\mathbf{F}(a)$. Thus in the next sections we concentrate on computing a linear state feedback by using (10) and by working with the polynomial matrix approach.

4.4 Polynomial Matrix Fraction

For completeness at first the most important notions and concepts which evolve in the polynomial matrix approach must be defined.

Definition 5 (Rational Matrix) *A rational matrix over a field $\mathbb{F}[a]$ is a matrix whose entries are rational functions $r \in \mathbb{F}[a]$. If all matrix entries are polynomial, the matrix is called polynomial matrix.*

Definition 6 (Unimodular Matrix) *If the inverse of a polynomial matrix is again a polynomial matrix, this matrix is called unimodular.*

Definition 7 (Polynomial Matrix Fraction) *A right (left) polynomial matrix fraction RPMF (LPMF) of a rational matrix $\mathbf{R}(a)$ is an expression of the following form*

$$\mathbf{R}(a) = \mathbf{N}(a)\,\mathbf{D}^{-1}(a) \quad (\mathbf{R}(a) = \mathbf{D}^{-1}(a)\,\mathbf{N}(a)) \tag{11}$$

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

[8] Uppercase parameter names denote functions in the $\mathcal{A}$-Domain.

[9] sequ $(\mathbf{f}[k])$ denotes the sequence $\mathbf{f}[0], \mathbf{f}[1], \dots$

[10] The following equation is used: $(a\mathbf{I} + \mathbf{A})^{-1} = \frac{1}{a}(\mathbf{I} + \frac{\mathbf{A}}{a})^{-1} = \frac{1}{a}\sum_{i=0}^{\infty}(\frac{\mathbf{A}}{a})^i$

With these definitions the following theorem can be stated.

Theorem 3 (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 (10) is a rational matrix the known results on rational matrices can be applied.

Theorem 4 (Existence) *For each rational matrix* $\mathbf{R}(a)$ *there is a right (left)-prime polynomial matrix fraction.*

Theorem 5 (Invariant Polynomials) *Let* $\mathbf{R}(a)$ *be a rational matrix.*

- *the numerator matrices of arbitrary right- or left-prime polynomial matrix fractions of* $\mathbf{R}(a)$ *have the same invariant polynomials*
- *the denominator matrices of arbitrary right- or left-prime polynomial matrix fractions of* $\mathbf{R}(a)$ *have the same invariant polynomials*

As the transfer matrix representation in (10) is a left-prime polynomial matrix fraction, Theorem 5 states that the invariant polynomials of the denominator matrix of each polynomial matrix fraction of $\mathbf{F}(a)$ are equal to the invariant polynomials of the system dynamics $\mathbf{A}$. For system representation in CCF, a closed expression for a right-prime polynomial matrix fraction can be determined [5], that is

$$\mathbf{F}(a) = \mathbf{S}(a)\,[(\mathbf{B}^c_{\sigma_i})^{-1}(\gamma(a) - \mathbf{A}^c_{\sigma_i}\,\mathbf{S}^c(a))]^{-1}, \tag{12}$$

where the matrices $\mathbf{S}(a)$ and $\gamma(a)$ show the structure

$$\mathbf{S}(a) = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ a & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ a^{c_1-1} & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & a^{c_2-1} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & a^{c_p-1} \end{bmatrix}, \ \gamma(a) = \begin{bmatrix} a^{c_1} & 0 & \cdots & 0 \\ 0 & a^{c_2} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & a^{c_p} \end{bmatrix}. \tag{13}$$

This means that if the LMS(2) is given in CCF, it is straight forward to find a closed expression for the polynomial matrix fraction of the system transfer matrix (10).
The same is valid for the system with state feedback $\mathbf{K}$ in (4). In this case the polynomial matrix fraction is

$$\mathbf{F}(a) = \mathbf{S}(a)\,\underbrace{[(\mathbf{B}^c_{\sigma_i})^{-1}(\gamma(a) - \overbrace{(\mathbf{A}^c_m - \mathbf{B}^c_{\sigma_i}\,\mathbf{K}^c)}^{\mathbf{A}^c_{\sigma_i,\mathbf{K}}}\,\mathbf{S}(a))]}_{\mathbf{D}_\mathbf{K}(a)}{}^{-1}, \tag{14}$$

For this RPMF some interesting properties hold:

- the numerator matrix $\mathbf{S}(a)$ of the RPMF is not changed by linear state feedback.
- the denominator $\mathbf{D}_\mathbf{K}(a)$ and the corresponding system matrix $\mathbf{A}+\mathbf{BK}$ have the same invariant polynomials.
- the controllability indices coincide with the column degrees[11] of the denominator matrix.

As the feedback matrix $\mathbf{K}$ can be uniquely determined, if $\mathbf{D}_\mathbf{K}(a)$ in (14) is known it is clear that the problem of finding an adequate state feedback to fit the given LMS(2) with desired invariant polynomials reduces to determining a denominator matrix $\mathbf{D}_\mathbf{K}(a)$ with the following properties:

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

(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 of $\mathbf{D_K}(a)$ must coincide with the controllability indices c_i of the LMS(2).[12]

Since $\mathbf{D_K}(a) = (\mathbf{B}^c_{\sigma_i})^{-1}\mathbf{D}^*_\mathbf{K}(a)$, it suffices to consider the matrix $\mathbf{D}^*_\mathbf{K}(a)$ as $(\mathbf{B}^c_{\sigma_i})^{-1}$ is unimodular and thus $\mathbf{D}^*_\mathbf{K}(a)$ has the same invariant polynomials as $\mathbf{D_K}(a)$ (Theorem 3).

5. Main Theorem

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

Theorem 6 (Syntheses Algorithm) *Let a controllable LMS(2) 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 $\mathbf{D}^*(a) = \mathrm{diag}(c_{i,\mathbf{K}}(a))$, $i = 1,\ldots,m$, while $\deg(c_{1,\mathbf{K}}(a)) \geq \cdots \geq \deg(c_{m,\mathbf{K}}(a))$ and $\sum_{i=1}^m \deg(c_{i,\mathbf{K}}(a)) = \sum_{i=1}^m c_i = n$. The following algorithm is given:*[13]

1. *prove the structural theorem for c_i and $c_{i,\mathbf{K}}(a)$. If (5) 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*[14]*:*

   - *multiply row_d with a and add the result to row_u*
     $\Rightarrow \mathbf{D}^*(a) \to \mathbf{D}^+(a)$
   - **if** $\deg(col_u^+) = \deg(col_u) - 1$
     - $\mathbf{D}^+(a) \to \mathbf{D}^{++}(a)$ *and* **go to** *step 3.*
   - **else**
     - *define:* $r := \deg(col_u) - \deg(col_d) - 1$
     - *multiply col_u^+ with a^r and subtract the result from col_d^+.* $\Rightarrow \mathbf{D}^+(a) \to \mathbf{D}^{++}(a)$

4. *generate the column pointer matrix Γ^{++} of $\mathbf{D}^{++}(a)$*[15] $\Rightarrow \mathbf{D}^*(a) = (\Gamma^{++})^{-1} \cdot \mathbf{D}^{++}(a)$ *and* **go to** *step 2*

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

   return $\mathbf{D}^*_\mathbf{K}(a)$

If the above conditions 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 4.4 it was argued that if $\mathbf{D_K}(a)$ is known, it is straight forward to compute $\mathbf{K}$. This is shown now:

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

[12] The controllability indices c_i are not changed by linear state feedback.

[13] For abbreviation, the i-th matrix columns and rows are denoted by col_i and row_i, $i = 1,\ldots,m$, respectively.

[14] These are operations that are equivalent to multiplications with unimodular matrices. As a consequence, by executing these operations, the the invariant polynomials of the considered matrix are not changed.

[15] The scalar column pointer matrix is a matrix with elements in $\mathbb{F}_2$ consisting of the coeffi cients of the highest degree a terms in each column of $\mathbf{D}^{++}(a)$.

This leads to

$$\mathbf{A}^c_{\sigma_i,\mathbf{K}}\mathbf{S}^c(a) = \gamma(a) + \mathbf{B}^c_{\sigma_i}\,\mathbf{D}_{\mathbf{K}}(a) \tag{15}$$

and by comparison of the coefficients the matrix

$$\mathbf{A}^c_{\sigma_i,\mathbf{K}} = \mathbf{A}^c_{\sigma_i} + \mathbf{B}^c_{\sigma_i}\,\mathbf{K}^c \tag{16}$$

can be determined which directly provides $\mathbf{K}^c$ and thus we have found a feedback matrix $\mathbf{K}^c$, which fits the given LMS(2) with the desired invariant polynomials $c_{i,\mathbf{K}}$, $k = 1,\ldots,m$.

6. Example

For a short example the following LMS(2) in CCF is given:

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

The controllability indices of the system from above are $c_1 = 3$ and $c_2 = 2$. For synthesis the controlled system shall have the invariant polynomials $c_{1,\mathbf{K}}(a) = (a^2+a+1)(a+1)^2$ and $c_{2,\mathbf{K}}(a) = a+1$. Thus the algorithm from above can be applied.

$$\begin{array}{ll}
\stackrel{1}{\rightarrow} & \sum_1^1 \deg(c_{i,\mathbf{K}}(a)) = 4 \geq \sum_1^1 c_i = 3 \ \surd \\
& \sum_1^2 \deg(c_{i,\mathbf{K}}w(a)) = 5 \geq \sum_1^2 c_i = 5 \ \surd \\
\stackrel{2}{\rightarrow} & \mathbf{D}^*(a) = \begin{bmatrix} a^4+a^3+a+1 & 0\\ 0 & a+1 \end{bmatrix} \\
\stackrel{3}{\rightarrow} & \mathbf{D}^+(a) = \begin{bmatrix} a^4+a^3+a+1 & a^2+a\\ 0 & a+1 \end{bmatrix} \rightarrow \mathbf{D}^{++}(a) = \begin{bmatrix} a+1 & a^2+a\\ a^3+a^2 & a+1 \end{bmatrix} \\
\stackrel{4}{\rightarrow} & \Gamma^{++}(a) = \begin{bmatrix} 0&1\\ 1&0 \end{bmatrix} \rightarrow \mathbf{D}^*(a) = \begin{bmatrix} a^3+a^2 & a+1\\ a+1 & a^2+a \end{bmatrix} \stackrel{2,5}{\longrightarrow} \mathbf{D}^*_{\mathbf{K}}(a) = \begin{bmatrix} a^3+a^2 & a+1\\ a+1 & a^2+a \end{bmatrix}
\end{array}$$

Now $\mathbf{K}^c$ can be computed. With (15) we have

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

and with (16) the feedback matrix $\mathbf{K}^c$, which fits the given system with the desired invariant polynomials is

$$\mathbf{K}^c = \underbrace{\begin{bmatrix} 1&0\\ 0&1 \end{bmatrix}^{-1}}_{\mathbf{B}^c_{\sigma_i}} \left(\underbrace{\begin{bmatrix} 0&0&1&1&1\\ 1&1&0&0&1 \end{bmatrix}}_{\mathbf{A}_{\sigma_i,\mathbf{K}^c}} + \underbrace{\begin{bmatrix} 0&0&0&0&0\\ 1&0&0&1&0 \end{bmatrix}}_{\mathbf{A}^c_{\sigma_i}} \right) = \begin{bmatrix} 0&0&1&1&1\\ 0&1&0&1&1 \end{bmatrix}.$$

7. Conclusion

In this paper we have considered Linear Modular Systems over the Galois Field $\mathbb{F}_2$. Referring to a paper, which is closely related to this paper we have stated that the invariant polynomials of the system dynamics determine the cyclic properties of a LMS(2). We have obtained a structured representation of the given system by introducing the controllability companion form and the polynomial matrix fraction of the system transfer function. Based on the Rosenbrock structure theorem we have presented an algorithm which decides if there exists a linear feedback which fits the system whith desired invariant polynomials and, if the decision is positive, computes an appropriate feedback matrix.[16] Further research will involve the nonlinear case and the computation of the cyclic state vectors.

8. References

1. Gill A., Linear modular systems. In: Zadeh L.A., Polak E., System Theory; McGraw-Hill; New York,1969.
2. Roppenecker G., On parametric state feedback design. International Journal of Control, 43, 793-804, 1986.
3. Kucera V., Analysis and Design of discret Linear Control Systems. Prentice Hall International (UK) Ltd, 5. ed. 1995.
4. Cohn M., Controllability in Linear Sequential Networks. IEEE Transactions on circuit theory 9, 1962, S.74 - 78.
5. Wolovich W.A., Linear Multivariable Systems. Springer-Verlag, New York 1974.
6. Lidl R. und Niederreiter H., Introduction to finite fields and their applications. Cambridge University Press, 1997.

[16] In general there does not exist a unique solution.