Linear Systems over Finite Fields —

Modeling, Analysis, and Synthesis

Der Technischen Fakultät der

Universität Erlangen-Nürnberg

zur Erlangung des Grades

DOKTOR-INGENIEUR

vorgelegt von

Johann Reger

Erlangen 2004

Als Dissertation genehmigt von
der Technischen Fakultät der
Universität Erlangen-Nürnberg

Tag der Einreichung:	01. 06. 2004
Tag der Promotion:	15. 07. 2004
Dekan:	Prof. Dr. rer. nat. A. Winnacker
Berichterstatter:	Prof. Dr.-Ing. T. Moor
	Prof. Dr.-Ing. D. Abel

Vorwort

Die vorliegende Arbeit entstand während meiner Tätigkeit als Promotionsstipendiat und wissenschaftlicher Assistent am Lehrstuhl für Regelungstechnik der Friedrich-Alexander-Universität Erlangen-Nürnberg. Die Inspiration zur Arbeit gaben im wesentlichen die Vorarbeiten von Herrn Prof. Dr.-Ing. Dieter Franke, dem das Verdienst gebührt, die Steuerungstechnik wieder in der Regelungstechnik verankert zu haben. Auf Herrn Prof. Arthur Gill geht ein reichhaltiger Fundus an Ergebnissen zur Theorie linearer Schieberegister zurück, auf die ein Gutteil des Kapitels zur Analyse gründet. Zahlreiche Anregungen zog ich auch aus den Arbeiten von Herrn Prof. Dr. Dieter Bochmann zum Booleschen Differentialkalkül und von Herrn Prof. William Wolovich zur Polynommatrixmethode; sie finden sich in den Kapiteln zur Modellbildung und Synthese wieder.

An erster Stelle bedanke ich mich bei Herrn Prof. Dr.-Ing. Thomas Moor für die Übernahme des Referats, ebenso herzlich bei Herrn Prof. Dr.-Ing. Dirk Abel für die Übernahme des Korreferats. Herrn Prof. Dr.-Ing. Günter Roppenecker gilt mein Dank für die Übernahme des Prüfungsvorsitzes, meine besondere Wertschätzung aber für die Gewährung des nötigen Freiraums wie auch für die großzügige Bereitstellung von Mitteln zur Förderung des wissenschaftlichen Austauschs. Herrn Prof. Dr. Hans Kurzweil danke ich für seine Hilfestellung in Fragen der Algebra, nicht zuletzt aber für sein Mitwirken im Prüfungskollegium. Hervorheben möchte ich auch die gute Zusammenarbeit mit meinen Kollegen am Lehrstuhl, dabei insbesondere mit den Herren Dipl.-Ing. Klaus Schmidt, Dr.-Ing. Joachim Deutscher und Dr.-Ing. Armin Schleußinger. Ferner danke ich allen Studenten, die mit ihren Arbeiten einen Beitrag zum Gelingen dieser Arbeit geleistet haben. Herrn Dipl.-Ing. Klaus Schmidt danke ich für die sorgfältige und kritische Durchsicht der Arbeit. Not at least, warm thanks to Dr. Jonathan Magee in Galway for polishing what was supposed to be English.

Ein Dankeschön geht auch an die Studienstiftung des deutschen Volkes und die Deutsche Forschungsgemeinschaft, ohne deren Unterstützung, ideell wie finanziell, die Arbeit in dieser Form nicht möglich gewesen wäre.

Erlangen, im Juni 2004 Johann Reger

You're a well paid scientist
You only talk in facts
You know you're always right
'Cause you know how to prove it
Step by step
A PhD to show you're smart
With textbook formulas
But you're used up
Just like a factory hand

The Dead Kennedys "Well Paid Scientist"

Table of Contents

Zusammenfassung

Im Mittelpunkt der Untersuchungen stehen dynamische Systeme, welche sich in einem diskreten Zustandsraummodell über einem endlichen Körper abbilden lassen. Dazu werden Methoden zur algebraischen Modellierung und, speziell für den linearen Fall, strukturelle Verfahren zur Analyse und Synthese herausgearbeitet.

Ausgangspunkt der Modellbildung ist eine Tabelle, in der in Abhängigkeit jedes Zustands und Eingangs entsprechende Nachfolgezustände verzeichnet sind. Auf dieser Grundlage werden zwei Verfahren aus der Booleschen Algebra bzw. Kodierungstheorie vorgestellt, welche die Berechnung einer Zustandsübergangsfunktion gestatten, die ausschließlich auf den Operationen Konjunktion und exklusive Disjunktion beruht. Wie in der Arbeit gezeigt, ist diese Darstellung einer Darstellung über einem endlichen Körper mit zwei Elementen äquivalent, so daß damit auf einfache Weise eine Zustandsübergangsfunktion über einem endlichen Körper gewonnen wird. Diese schließt auch den nicht-deterministischen Fall mehrerer Folgezustände ein und ermöglicht die algebraische Darstellung jedes endlichen Automaten. Als besonders einfach erweist sich dabei die Berechnung mit der Methode, welche auf der Verwendung einer sogenannten Reed-Muller-Generator-Matrix fußt.

Der Analyseteil der Arbeit stellt eine detaillierte Untersuchung des Zustandsübergangsverhaltens autonomer linearer Systeme über einem beliebigen endlichen Körper dar. Dabei wird auf die reichhaltige Theorie linearer Schaltkreise der sechziger Jahre zurückgegriffen, im Gegensatz dazu aber wird die Herleitung nicht auf tiefergehende Erkenntnisse über endliche Ringe gegründet, sondern auf fortgeschrittenen Kapiteln der linearen Algebra. Auf diesem Weg wird gezeigt, wie strukturelle algebraische Eigenschaften der Systemdynamikmatrix, genauer die Perioden ihrer Elementarteilerpolynome, das Übergangsverhalten von Zuständen bestimmen, womit ein notwendiges wie hinreichendes Kriterium zur Zerfällung des Zustandsraums in zyklische und nicht-zyklische Unterräume hergeleitet wird. Ist ein endlicher Automat als ein solches lineares System darstellbar, so wird damit zum ersten Mal ein Kriterium vorgestellt, welches alle Automatenzyklen in Länge und Anzahl liefert sowie das nicht-zyklische Übergangsverhalten beschreibt. Es ergibt sich also eine Methode, mit Hilfe derer sich der zugehörige Automatengraph alleine unter Verwendung der Systemdynamikmatrix eindeutig bestimmen läßt. Wie am Ende des Analyseteils ausgeführt, erhält man ein dem entsprechendes Ergebnis auch für affin-lineare autonome Systeme über einem endlichen Körper.

Mit dem Wissen um den Einfluß der Elementarteilerpolynome auf das zyklische Verhalten eines autonomen linearen Systems über einem endlichen Körper gelingt im letzten Teil der Arbeit erstmalig die Herleitung eines Verfahrens zur gezielten Vorgabe des zyklischen Verhaltens eines linearen Systems über einem endlichen Körper. Dazu eignen sich statische lineare Zustandsrückführungen, die aber, will man im Mehrgrößenfall alle Elementarteilerpolynome vorgeben und nicht nur das charakteristische Polynom im geschlossenen Regelkreis, nicht mit klassischen Zeitbereichsverfahren wie z. B. der vollständigen modalen Synthese ermittelt werden können. Ein dem $\mathcal{Z}$-Bereich entsprechender Bildbereich über einem endlichen Körper, $\mathcal{A}$-Bereich genannt, erweist sich hierbei als Schlüssel zur Lösung des Problems: die im $\mathcal{A}$-Bereich erklärte Polynommatrixmethode gestattet gerade die Lösung dieses Vorgabeproblems. Die Lösung erfolgt in zwei Schritten: Mit Hilfe des Rosenbrockschen Kontrollstrukturtheorems wird die Frage der Existenz einer Zustandsrückführung, welche die gewünschten Elementarteilerpolynome im geschlossenen Kreis realisiert, geklärt. Die Synthese der Rückführung selbst geschieht durch Umformung der Nennermatrix einer rechtsprimen Polynommatrixzerlegung der Übertragungsmatrix bzgl. einer Zustandsdarstellung in Steuerbarkeitsnormalform. Die dazu nötigen Schritte beschreibt ein Algorithmus, der eine derartige Nennermatrix für den geschlossenen Regelkreis liefert. Eine einfache Rechnung ergibt dann die gesuchte Matrix der Zustandsrückführung. Eine Diophantische Gleichung muß hierzu nicht gelöst werden. Der zweite Abschnitt erweitert das Verfahren auf lineare Systeme mit nichtsteuerbarem Anteil. Hierzu wird eine an die Steuerbarkeitsnormalform angelehnte Darstellung abgeleitet, die den steuerbaren und nicht-steuerbaren Systemanteil offenlegt. Zur Unterbindung des Einflusses seitens des Anfangszustands des nicht-steuerbaren Systemanteils werden steuerbarer und nicht-steuerbarer Systemanteil voneinander entkoppelt, was sich für beliebige lineare Systeme mit nicht-steuerbarem Anteil als immer möglich herausstellt. Des weiteren wird ein neuartiges Kriterium vorgestellt, mit Hilfe dessen sich genau entscheiden läßt, wann eine solche Entkoppelung die Elementarteilerpolynome der Systemdynamikmatrix beeinflußt — dies in Erweiterung des bekannten Ergebnisses, daß eine derartige Entkoppelung das charakteristische Polynom der Systemdynamikmatrix des geschlossenen Kreises nicht zu verändern vermag. Am Ende dieser Untersuchungen steht eine Methode, welche die Anwendung des zuvor für steuerbare Systeme ermittelten Algorithmus auf das steuerbare Teilsystem erlaubt, dabei aber das charakteristische Polynom des nicht-steuerbaren Teilsystems unberührt läßt.

Chapter 1

Introduction

Discrete event systems are characterized by a discrete state transition behavior which is driven by an asynchronous occurrence of discrete events rather than by the propagation of continuous time. To some extent, this behavior can be reconciled with the state transition behavior of a discrete time continuous system if one is content with giving up equidistant time ticks in favor of just counter instants that indicate the occurrence of an event. In this respect, it seems promising to formulate a state space model for discrete event systems.

State space models are the dominant and successful paradigm for representing continuous dynamic systems. For the most part, this is due to the profound knowledge about linear algebra that captures many real world system properties in appropriate algebraic properties. This may explain why considerable effort has been made to setup a link between linear algebra and discrete event systems.

1.1 Motivation

Discrete space models using so-called *arithmetical polynomials* have been introduced for representing a class of discrete event systems with a finite number of states, i. e. finite state automata [Fra94, Fra96]. An other method employs *Walsh functions* for modeling deterministic finite state automata as autonomous linear systems [Son99, Son00]. There are major drawbacks in both approaches. In order to point out some of them, consider an example system in the framework of arithmetical polynomials[1] with, for simplicity, an autonomous state equation of n-th order

$$\mathbf{x}(k+1) = \mathbf{A}\mathbf{x}(k)\,. \tag{1.1}$$

In this regard, $\mathbf{A} \in \mathbb{Z}^{n\times n}$ is the dynamics matrix, $k \in \mathbb{N}_0$ is a counter, and for k fixed, $\mathbf{x}(k) \in \mathbb{B}^n$ is a state vector with boolean entries, 1 and 0 only. The algebraic operations addition and multiplication are understood in the usual sense.

[1] Similar arguments apply for the Walsh-function approach.

Problem 1 Assume that the task is to calculate a state $\mathbf{x}_t \in \mathbb{B}^n$ which "returns" after $t \in \mathbb{N}$ counter instances, i. e. a so-called periodic state with $\mathbf{A}^t \mathbf{x}_t = \mathbf{x}_t$ shall be calculated. Consequently, the equation

$$(\mathbf{I} - \mathbf{A}^t)\,\mathbf{x}_t = \mathbf{0}\,, \tag{1.2}$$

has to be solved, which as long as the matrix $(\mathbf{I} - \mathbf{A}^t) \in \mathbb{Z}^{n\times n}$ shows some rank deficiency has a solution $\mathbf{x}_t \in \mathbb{Q}^n$. This solution obviously does not need to be boolean. Conversely, let $\mathbf{x}_{t,1}, \mathbf{x}_{t,2} \in \mathbb{B}^n$ be two boolean solutions of equation (1.2). Then in the presupposed sense of addition, generally,

$$\mathbf{x}_{t,1} + \mathbf{x}_{t,2} \notin \mathbb{B}^n,$$

that is, superposition does not apply for these systems. Consequently, though on the face of it the example system appears to be linear, it is non-linear in nature.

Problem 2 Let $r \leq n$ be the rank deficiency of the matrix $\mathbf{I} - \mathbf{A}^t$. Then the general solution of equation (1.2) takes the form

$$\mathbf{x}_t = \sum_{i=1}^{r} c_i\, \mathbf{x}_t^i \tag{1.3}$$

with $\mathbf{x}_t^i \in \mathbb{Q}^n$ specific, but coefficients $c_i \in \mathbb{Q}$ arbitrary. If solutions $\mathbf{x}_t$ are admissible only if $\mathbf{x}_t \in \mathbb{B}^n$ then the coefficients c_i have to be suitably selected for rendering $\mathbf{x}_t$ boolean. The entailed calculations can be very cumbersome. The reason is that the general problem of solving

$$\mathbf{A}\,\mathbf{x} = \mathbf{b}$$

with $\mathbf{A} \in \mathbb{Z}^{n\times n}$ and $\mathbf{b} \in \mathbb{Z}^n$ for $\mathbf{x} \in \mathbb{B}^n$ is a non-polynomial complete (NP-complete) problem, which for the purposes here, shall mean that this problem cannot be solved in less than n^m calculations, whatever $m \in \mathbb{N}$ may be chosen [CLR90]. Hence, the calculations for solving such problems can be considered tractable for small numbers n only, which is strongly opposed to the rational case $\mathbf{x}_t \in \mathbb{Q}^n$ in which one were already done with the solution in (1.3), having an effort of less than n^2 calculations with the Gauß-algorithm for example.

These outlined shortcomings obviously originate from the model which admits integral numbers for the parameters in the state equation but claims to keep the states and inputs boolean.

In the author's opinion, the solution of both problems demands for a change in the algebraic setting:

- Operations should map numbers into the same set of numbers,
- The set of numbers should include the inverse elements for addition and multiplication,[2]
- The cardinality of the set of numbers should be finite.

An algebraic system which takes into account all these issues is the concept of a finite field. It is this notion that governs the development of theory to be exposed in the following chapters.

[2] Except for the zero element.

An other motivation of this work was to obtain a system model over a finite field that is general enough for encompassing the description of any deterministic or non-deterministic finite state automaton. In the approaches from above, basically, models for deterministic automata (arithmetical polynomials) or even without inputs (Walsh-functions) were derived. That is why, in this work, the modeling was started from the scratch by employing standard methods from boolean algebra and coding theory.

1.2 Contribution of this Dissertation

Based on a discrete state space model over a finite field, the first main contribution of this work is to provide a sufficient and necessary criterion for a complete algebraic locating of the periodic and aperiodic state transition behavior of linearly modeled finite state automata. This criterion is an essential enhancement compared to former results within the approaches of arithmetical polynomials and Walsh-functions, which both offered necessary criteria only [Fra94, Son00]. For an application of the criterion, the set of elementary divisor polynomials with respect to the system dynamics matrix has to be calculated. It turns out that this set can be divided into a set of periodic and aperiodic elementary divisor polynomials, where the former part is related to cycles in the state graph representation, and the latter part reflects the tree-like structures. Finally, the theory is extended to cover the case of affine-linear systems over finite fields as well.

A further important novelty presented in this work is a method for synthesizing linear state feedback which, under the assumption of controllability, imposes a desired state transition structure on these linear systems in the closed-loop, i. e. a set of desired periodic and aperiodic elementary divisor polynomials. To this end, an image domain for functions over finite fields is presented and connected to methods from the polynomial approach, which is a well-established image domain method for the controller synthesis of linear continuous systems [Wol74, Ant98]. The outcome is an algorithm, which first checks whether the requirements burdened by the structural constraints from Rosenbrock's control structure theorem are met. If the answer is positive, a desired set of elementary divisor polynomials can be realized by static state feedback. In a second step, an appropriate feedback matrix is derived by manipulating a denominator matrix of a right-prime polynomial matrix fraction, which results from the transfer matrix of the system representation in controllability companion form. This approach has the advantage that the solution of a Diophantine equation is not required, and that, opposed to continuous systems where controllability matrices tend to be ill-conditioned, linear systems over finite fields are not subject to this numerical problem. Thus, for linear systems over finite fields this approach of feedback design allows to fully benefit from its advantages without incurring its drawbacks. In the closing part of the work, the methods formerly derived for a controllable system are extended to the case with an uncontrollable subsystem. This is done by decoupling the uncontrollable subsystem from the controllable subsystem, for the latter of which an appropriate feedback is designed by resorting to the methods from before. In this

regard, a criterion of when a decoupling has an influence on the closed-loop elementary divisor polynomials is derived, which completes the known result that such a decoupling does not alter the characteristic polynomial of the system dynamics matrix. Moreover, it is worth mentioning that any linear system of equations occurring in this context can be solved with algorithms of just polynomial complexity.

1.3 Dissertation Overview

The algebraic foundation of this work, consisting particularly of basics from group theory, polynomials over finite fields, and linear algebra, is given in Chapter 2. This chapter also presents an image domain for functions over finite fields. In an exemplary manner, Chapter 3 exposes two methods from boolean algebra and coding theory for deriving the general non-linear state space model over a finite field with characteristic 2, for deterministic and non-deterministic systems. The analysis of linear and affine-linear systems over finite fields is dealt with in Chapter 4. It comprises the development of a criterion for a complete state space decompositon into periodic and aperiodic subspaces. In Chapter 5, the cycle sum synthesis problem is solved for controllable and partially uncontrollable linear systems over finite fields by adapting image domain feedback design methods on an image domain over a finite field. In Chapter 6 the main points are summarized and directions for future research are suggested.

Chapter 2

Mathematical Preliminaries

In engineering sciences, and particularly in control engineering, it is common practice to take the field on which the calculations are carried out for granted. Usually this field is the field of real (or complex) numbers, and since this field is a well-established paradigm, all the calculation rules and theorems, e. g. for the zeroes of polynomials, are used and understood in a rather all-embracing manner. Nevertheless, an infinite set of numbers is always assumed, at least implicitly.

On the contrary, an awareness of the algebraic fundamentals of discrete mathematics is of crucial importance when state space representations are used to model finite state automata. As the number of states is finite for finite state automata, this limitation naturally demands a finite state space because the automaton states have to be mapped somehow into a corresponding algebraic domain. Conversely, all states in this state space have to have their counterpart in the automaton, which means that a bijection must exist between each other. When automaton states are related by a next state function, an appropriate function must exist on the algebraic domain as well — that is for constructing those functions, on the algebraic domain some algebraic operations have to be given, as for instance addition and multiplication. All this indicates that the algebraic domain needs to be closed under these algebraic operations. Thus, the nature of the problem can be characterized by the notion of a group, in this case a finite group, and under stronger assumptions, the character of the problem is close to the concept of a finite field. Having established the field property within the mathematical model of description, the typical standard propositions for (general) fields can be applied. Next to them, those propositions must be taken into consideration which originate from the finiteness of the field. The latter propositions cause many differences in everyday calculations.

For all these reasons, the indispensable terminology from finite field theory which is the prerequisite for an easier understanding of the automaton model in Chapter 3 shall be prearranged. Yet, this review can only be far from complete. In the main, it refers to the comprehensive and thorough introduction to finite fields from Lidl and Niederreiter [LN94]. The train of thought, especially the introduction to vector spaces and matrices, follows the style presented in [DH78]. Reference

is made as well to [McE87, Sel66] where polynomials over finite fields are the focus of attention. Additionally, the reader may refer to [Lan84, BM77] wherein most of the algebraic fundamentals that are introduced here can be found in detail. All these stress the development and exposition of the mathematical background, whereas [Boo67] serves automata theory from a more practical point of view.

The chapter is organized as follows: in Section 2.1 fundamental concepts and basic terminology of group theory are recalled. Using the result of Fermat's little theorem some important properties of polynomials over finite fields, in particular the concepts of irreducibility and periodicity, are introduced in Section 2.2. Provided with this knowledge, vector spaces, linear transformations and matrices are introduced in Section 2.3. Special attention is directed to matrices in standardized (canonical) forms because the properties of a matrix become visible right away by inspecting the corresponding matrix in certain canonical forms. Since difference equations prospectively become algebraic in an image domain, an operational calculus for finite fields is presented in Section 2.4. This operational calculus prepares the way for an algebraic examination and synthesis of linear modular systems in Chapter 5. Some remarks demonstrate the differences between finite and infinite fields.

2.1 Fundamental Concepts of Group Theory

In algebraic systems, elements of a set are connected by applying operations on them. If an operation relates two elements of the set, then the operation is called a binary operation. The first and most general algebraic system is a semigroup.

Definition 2.1 (Semigroup)
A semigroup $(\mathcal{S}, *)$ is a nonempty set $\mathcal{S}$ together with a binary operation $*$ such that

1. For all $a, b \in \mathcal{S}$, $a * b \in \mathcal{S}$.
2. The operation $*$ is associative, i. e. $a * (b * c) = (a * b) * c$ for any $a, b, c \in \mathcal{S}$. □

An example of a semigroup is $(\mathbb{N}, +)$, the set of positive integers $\mathbb{N}$ together with the binary operation $+$ defined as addition. Note that in this case there is no positive integer $e \in \mathbb{N}$ such that for some positive integer $a \in \mathbb{N}$, $a + e = a$. That is an identity element is missed here, which would be $e = 0$ if the set of positive integers were enlarged by the number 0. On that account one more assumption can be added.

Definition 2.2 (Monoid)
A semigroup $(\mathcal{M}, *)$ with set $\mathcal{M}$ and binary operation $*$ is a monoid if an identity element $e \in \mathcal{M}$ exists such that for all $a \in \mathcal{M}$, $a * e = e * a = a$. □

In other words: a monoid is a set that is closed under an operation and has an identity element by means of which the operation maps elements onto itself. If the task is to solve for an element in the operation, monoids have to be enhanced by one more property. An inverse element must exist for each element of the set, i. e. the more powerful concept of a group is necessary.

Definition 2.3 (Group)
A group $(\mathcal{G}, *)$ 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. The operation $*$ is associative, i. e. $a * (b * c) = (a * b) * c$ for any $a, b, c \in \mathcal{G}$.
3. An identity element, $e \in \mathcal{G}$, exists such that for all $a \in \mathcal{G}$, $a * e = e * a = a$.
4. For all $a \in \mathcal{G}$ exists an inverse element $a^{-1} \in \mathcal{G}$ 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. □

By virtue of the last part of this definition, systems of equations can be solved for variables.[1] An example for a group is $(\mathbb{R}, +)$, the set of real numbers $\mathbb{R}$ with respect to addition; the identity element is $e = 0$, the inverse element is the corresponding negative element. The set of rational numbers $\mathbb{Q}\backslash\{0\}$ together with multiplication is another simple example of a group; the identity element of this group, $(\mathbb{Q}\backslash\{0\}, \cdot)$, is $e = 1$, the inverse element is the corresponding quotient of the element.

The next step is to extend the basic theory by adding a second operation.

Definition 2.4 (Ring)
A ring $(\mathcal{R}, +, \cdot)$ is a set $\mathcal{R}$ together with two binary operations, addition $+$, and multiplication $\cdot$, such that

1. $\mathcal{R}$ is a commutative group with respect to addition.
2. $\mathcal{R}$ is a semigroup with respect to multiplication.
3. $\mathcal{R}$ is distributive with respect to these operations, that is
   $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(b + c) \cdot a = b \cdot a + c \cdot a$ for all $a, b, c \in \mathcal{R}$.

[1] This is the main obstacle when using dioids like the (max,+)-algebra, where inverses do not exist in general.

A ring is called commutative if its multiplication is commutative. In a ring $(\mathcal{R},+,\cdot)$ the identity element with respect to $+$ is denoted by 0, the identity with respect to $\cdot$ is denoted by 1.[2] □

It is essential for a ring that an inverse operation for the multiplication need not exist. If, however, a multiplicative inverse is required – for example when solving for multiplicatively bound indeterminates — the concept of a field becomes important.

Definition 2.5 (Field)
A ring $(\mathcal{F},+,\cdot)$ is a field $\mathbb{F}=(\mathcal{F},+,\cdot)$ if the subset $\mathcal{F}\setminus\{0\}$ is a commutative group with respect to the multiplication $\cdot$. A field $\mathbb{F}$ with q elements, denoted by $\mathbb{F}_q$, is called finite if q is finite.[3] □

According to common notational practice the symbol "$\cdot$", indicating multiplication, will be omitted, unless it is necessary. In the further chapters a special type of finite field is utilized that is based on the division remainder operation *modulo*. The following theorem is shown by simply checking the field property.

Theorem 2.1 (Galois-Field)
The set of integral numbers $\{0,1,\ldots,q-1\}$, where q is a prime number, together with the binary operations addition and multiplication modulo q, is a finite field, called a Galois-Field $\mathbb{F}_q$. □

To spot the need for the primality of q consider the nonempty set $\{0,1,\ldots,q-1\}$ with cardinality q, endowed with the operations addition and multiplication modulo q, respectively. The interesting case is when $q>1$. Assume that $q>1$ were not a prime such that a factorization is $q=p_1\,p_2$ with $p_i\neq 1$ and obtain $p_1\,p_2=0 \mod q$. If a field $\mathbb{F}_q$ existed then an inverse element p_1^{-1} such that $p_1^{-1}p_1=1 \mod q$ must also exist since 1 is the identity element of multiplication. As a consequence, the conclusion would be $p_2=0 \mod q$ or equivalently that $q\,|\,p_2$, a contradiction. Therefore, such a field does not exist.

Remark 2.1
The property that $a\,b=0$ iff $a=0\vee b=0$ for $a,b\in\mathbb{F}$ often is referred to that fields are devoid of zero divisors. □

It can be shown that any finite field is equivalent to some Galois-Field or at least to one of its extension fields[4]; for a proof see [LN94]. Hence, as the field property is required in finite automata

[2] Note that in this definition addition and multiplication, denoted by the symbols "+" and "$\cdot$", represent a generalization of the ordinary concept of addition and multiplication. They are not to be confused with the ordinary concept, since the above-given definition of a ring applies to arbitrary operations, which have the stated properties of commutativity, associativity and distributivity.

[3] The symbol $\mathbb{F}$ is used to emphasize the field character. For example $\mathbb{F}$ denotes a field, whereas $\mathcal{F}$ would mark a set, which would not necessarily be equipped with any operations. Subscripts indicate the cardinality of the underlying (finite) set. Without a subscript no further assumptions on the field, whether finite or infinite, are made.

[4] An example which bases on the notion of extension fields is considered in Appendix C.

models over a finite set, any of those models can be described by means of some suitable Galois-Field. For this reason, the main attention is paid to Galois-Fields, and for simplicity, if a finite field is in question then always a respective Galois-Field is assumed.

Theorem 2.2 (Fermat's Little Theorem)
Let an integral number q be a prime number. Then for all integers λ, q divides $\lambda^q - \lambda$. In cases where the integer λ is not divisible by the prime q, q divides $\lambda^{q-1} - 1$. □

Proof In order to explain this, the first part of the theorem to be proven is rephrased by $\lambda^q \equiv \lambda \mod q$, expressing the equivalence modulo q of λ^q and λ. An induction argument will be used. To start with, the first integer $\lambda = 1$ is checked, which obviously verifies this part of the theorem. From the binomial theorem $(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^{n-i} b^i$ it follows

$$\begin{aligned} (\lambda+1)^q &= \sum_{i=0}^{q} \binom{q}{i} \lambda^{q-i} = \lambda^q + q\lambda^{q-1} + \frac{q(q-1)}{2}\lambda^{q-2} + \cdots + q\lambda + 1 \\ &= \lambda^q + 1 + q\,(\lambda^{q-1} + \frac{q-1}{2}\lambda^{q-2} + \cdots + \lambda) \\ \Longrightarrow \quad (\lambda+1)^q &\equiv \lambda^q + 1 \mod q\,. \end{aligned}$$

Applying the induction hypothesis $\lambda^q \equiv \lambda \mod q$ yields

$$(\lambda+1)^q \equiv \lambda + 1 \mod q\,,$$

and since the statement already holds for $\lambda = 1$ the first part of the theorem has been shown. Concerning the second part, it is clear that with

$$\lambda^q \equiv \lambda \mod q \quad \Longleftrightarrow \quad \lambda(\lambda^{q-1} - 1) \equiv 0 \mod q\,,$$

the first part of the theorem implies that either λ or $\lambda^{q-1} - 1$ is divisible by q. Due to the assumption that q does not divide λ, finally the second part of the theorem is obtained. □

Remark 2.2
Fermat's little theorem is important whenever polynomials over a finite field $\mathbb{F}_q$ are concerned. The theorem implies that many polynomials over a finite field $\mathbb{F}_q$ can be identical to zero for arbitrary $\lambda \in \mathbb{F}_q$, because these polynomials may contain polynomial factors $\lambda^q - \lambda$, which are zero modulo q. In contrast, a polynomial over the infinite field of real numbers $\mathbb{R}$ is identical to zero iff all coefficients are zero. □

2.2 Polynomials over Finite Fields

A fundamental property of polynomials, which is according to Gauß' fundamental theorem of algebra, is that all polynomials over the field of real numbers $\mathbb{R}$ can be factored (reduced) in

quadratical factors, or over the extension field $\mathbb{C}$ in linear factors. As will be demonstrated in this section, for finite fields $\mathbb{F}_q$ in general this is not the case.

It can easily be verified that the set of polynomials together with customary polynomial addition and polynomial multiplication is a ring.

Theorem 2.3 (Ring of Polynomials)
The set of all polynomials $p(\lambda) = \sum_i a_i \lambda^i$ with indeterminate λ and $i = 0, 1, 2, \ldots$ coefficients a_i in a field $\mathbb{F}$ together with polynomial addition and polynomial multiplication is a ring, called the ring of polynomials over the field $\mathbb{F}$. It is denoted by $\mathbb{F}[\lambda]$. □

Remark 2.3
In the ring of polynomials, the 0-element (identity element wrt. polynomial addition) is the polynomial 0 in which all coefficients a_i are zero. The respective 1-element (identity element wrt. polynomial multiplication) is the polynomial 1 in which the coefficient $a_0 = 1$ and all other coefficients are zero. □

For convenience some fundamentals are recalled.

Definition 2.6 (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 2.7 (Irreducible Polynomial)
A non-constant polynomial $p \in \mathbb{F}[\lambda]$ is called irreducible over $\mathbb{F}$, whenever $p(\lambda) = g(\lambda)h(\lambda)$ in $\mathbb{F}[\lambda]$, then either $g(\lambda)$ or $h(\lambda)$ is a constant. □

In view of irreducibility, Gauß' fundamental theorem of algebra can be rephrased.

Theorem 2.4 (Unique Factorization Theorem)
Any polynomial $p \in \mathbb{F}[\lambda]$ can be written in the form

$$p = a\, {p_1}^{e_1} \cdots {p_k}^{e_k}, \tag{2.1}$$

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 sequence of the factors. □

For the infinite field $\mathbb{R}$ it is a well-known fact that all factor polynomials are at most of second degree over $\mathbb{R}$, that is $e_i \leq 2$ in Theorem 2.4. This does not apply for finite fields $\mathbb{F}_q$. For example: $p(\lambda) = \lambda^5 + \lambda^2 + \lambda + 1 = (\lambda^3 + \lambda + 1)(\lambda + 1)^2$ for $p \in \mathbb{F}_2[\lambda]$, because $\lambda^3 + \lambda + 1$ and $\lambda + 1$ are irreducible over $\mathbb{F}_2$. However, with $q \in \mathbb{F}_3[\lambda]$ the case is a different one, as shows $q(\lambda) = \lambda^3 + \lambda + 1 = (\lambda^2 + \lambda + 2)(\lambda + 2)$. Consequently, reducibility of a polynomial depends on the field.

The latter concepts apply for fields in general. The following concepts apply only if the fields under concern are finite. Besides the degree of a polynomial, it can be shown that for any non-zero polynomial over a finite field, another characteristic integer exists.

Definition 2.8 (Period of a Polynomial)
Let $p \in \mathbb{F}_q[\lambda]$ be a non-zero polynomial over the finite field $\mathbb{F}_q$. If $p(0) \neq 0$, then the least positive integer τ for which $p(\lambda)$ divides $\lambda^\tau - 1$ is called the period (or order) 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 the period τ of the polynomial p is defined as the period of g. □

As a consequence, all polynomials with period τ represent factors of the polynomial $\lambda^\tau - 1$. For polynomials which are powers of irreducible polynomials, so-called powered polynomials, the following theorem is taken from [LN94].

Theorem 2.5 (Period of a Powered Polynomial)
Let $p \in \mathbb{F}_q[\lambda]$ be an irreducible polynomial over the finite field $\mathbb{F}_q$ with $p(0) \neq 0$ and period τ. Let $f \in \mathbb{F}_q[\lambda]$ be $f = p^e$ with $e \in \mathbb{N}$. Let l be the least integer such that $q^l \geq e$. Then the powered polynomial f has the period $q^l\tau$. □

Example 2.1
The period of the polynomial $f(\lambda) = \lambda^4 + \lambda^2 + 1 \in \mathbb{F}_2[\lambda]$ is to be calculated. From the sequence

$$\lambda^4 + \lambda^2 + 1 \;\rightarrow\; \lambda^6 + \lambda^4 + \lambda^2 \;\rightarrow\; \lambda^6 + 1\,,$$

that is from,

$$\lambda^2 f(\lambda) + f(\lambda) = (\lambda^2 + 1) f(\lambda) = \lambda^6 + 1 \quad \Rightarrow \quad f(\lambda) | \lambda^6 + 1$$

it follows $\tau_f = 6$. Using the factorization $f = p^2$ with $p(\lambda) = \lambda^2 + \lambda + 1 \in \mathbb{F}_2[\lambda]$ the sequence

$$\lambda^2 + \lambda + 1 \;\rightarrow\; \lambda^3 + \lambda^2 + \lambda \;\rightarrow\; \lambda^3 + 1$$

or in other words,

$$\lambda\, p(\lambda) + p(\lambda) = (\lambda + 1) p(\lambda) = \lambda^3 + 1 \quad \Rightarrow \quad p(\lambda) | \lambda^3 + 1$$

shows that $\tau_p = 3$. Thus, observing $e = 2$ and Theorem 2.5 results in $l = 1$, in the first place, and therefore with $\tau_p = 3$ finally the period $\tau_f = 2^1 \cdot 3 = 6$ is obtained.[5] □

In practice, periods of polynomials need not be calculated manually. For finite fields $\mathbb{F}_q$ starting from characteristic $q = 2$ up to $q = 7$ the respective periods of irreducible polynomials can be found in tabulars such as in [LN94], in [PW72] for polynomials over $\mathbb{F}_2$ up to degree 34, or are internally tabulated and calculated in computer algebra software.[6]

Remark 2.4
Nilpotent polynomials $p \in \mathbb{F}_q[\lambda]$, i. e. polynomials of the form $p = \lambda^k$ for some positive integer k, are not periodic by definition (see Definition 2.8). With the fact that in a factorization of a polynomial apart from nilpotent polynomial factors only irreducible polynomials and their powers may occur, polynomials over finite fields are either periodic or nilpotent. This implies some important consequences to be discussed in Chapter 4. □

[5] The introductory proof of Theorem 4.4 in Chapter 4 gives more insight to the above-used algorithm.
[6] Typical such software are for instance the packages Maple® or Mathematica®.

2.3 Linear Transformations and Matrices

2.3.1 Vector Spaces

Having developed the basis of algebraic systems as groups and rings of polynomials over finite sets one may then define a vector space.

Definition 2.9 (Linear Space, Vector Space)
A (linear vector) space over a field $\mathbb{F}$, denoted by $V = (\mathcal{V}, +, \mathbb{F})$, is a set $\mathcal{V}$ which is a commutative group with respect to addition $+$ together with a field $\mathbb{F}$ such that

1. The operations on the field $\mathbb{F}$ are addition and multiplication.
2. For any $\mathbf{v} \in \mathcal{V}$ and any $a \in \mathbb{F}$, $a\mathbf{v} = \mathbf{v}a \in \mathcal{V}$. (closedness)
3. For arbitrary $\mathbf{u}, \mathbf{v} \in \mathcal{V}$ and arbitrary $a, b \in \mathbb{F}$,
   (a) $a(\mathbf{u}+\mathbf{v}) = a\mathbf{u} + a\mathbf{v}$ (distributivity 1)
   (b) $(a+b)\mathbf{u} = a\mathbf{u} + b\mathbf{u}$ (distributivity 2)
   (c) $(ab)\mathbf{u} = a(b\mathbf{u}) = b(a\mathbf{u}) = (ba)\mathbf{u}$ (associativity)
   (d) $1_{\mathbb{F}}\,\mathbf{u} = \mathbf{u}$ ($1_{\mathbb{F}}$ is the identity element wrt. multiplication in $\mathbb{F}$)

The elements of $\mathcal{V}$ are called vectors, the elements of $\mathbb{F}$ are called scalars. The identity element of the group $(\mathcal{V}, +)$ is given by the zero vector $\mathbf{0}$, the inverse element of an element $\mathbf{v} \in \mathcal{V}$ is its corresponding negative element $-\mathbf{v}$. □

Definition 2.10 (Subspaces)
Let $V = (\mathcal{V}, +, \mathbb{F})$ and $\overline{V} = (\overline{\mathcal{V}}, +, \mathbb{F})$ with $\mathcal{V} \subseteq \overline{\mathcal{V}}$ be two vector spaces associated to the same operations defined over the same field $\mathbb{F}$. Then V is called a subspace of $\overline{V}$. □

In a vector space $V = (\mathcal{V}, +, \mathbb{F})$, vectors $\mathbf{v}_i \in \mathcal{V}$, $i = 1, \ldots, n$, can be combined such that with $a_i \in \mathbb{F}$ the vector

$$\mathbf{v} = a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \cdots + a_n\mathbf{v}_n$$

is a so-called linear combination of the vectors $\mathbf{v}_i$.

Definition 2.11 (Linear Independence)
Vectors $\mathbf{v}_i \in \mathcal{V}$, $i = 1, \ldots, n$, of a vector space $V = (\mathcal{V}, +, \mathbb{F})$ are said to be linearly independent iff for $a_i \in \mathbb{F}$, $i = 1, \ldots, n$

$$a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \cdots + a_n\mathbf{v}_n = \mathbf{0}$$

implies that $a_i = 0$ for all $i = 1, \ldots, n$. Otherwise the vectors are called linearly dependent. □

With the notion of linear independence a set of vectors may be defined which can be used to represent a vector space.

Definition 2.12 (Basis of a Vector Space)
A set of vectors $\mathcal{B} = \{\mathbf{b}_1, \mathbf{b}_2, \ldots\}$ is a basis of the vector space $V = (\mathcal{V}, +, \mathbb{F})$ if

1. $\mathcal{B} \subseteq \mathcal{V}$,
2. $\mathcal{B}$ spans V, i. e. all $\mathbf{v} \in \mathcal{V}$ are linear combinations of the vectors $\mathbf{b}_i$ with respective coordinates $v_i \in \mathbb{F}$, hence
$$\mathbf{v} = \sum_i v_i \mathbf{b}_i \,.$$
3. The vectors in $\mathcal{B}$ are linearly independent.

The cardinality of $\mathcal{B}$ is called the dimension $\dim(V)$ of the vector space V.[7] Any $\mathbf{v} \in \mathcal{V}$ can be represented by a tuple $(v_1, v_2, \ldots)$, a so-called vector of coordinates, with respect to a basis $\mathcal{B}$. □

Remark 2.5
Finite dimensional vector spaces over finite fields are point spaces consisting of a finite number of vectors — in a sense, the vector space is void between any two points. Moreover, the common notion of a scalar product does not yield an expressive notion of distance. For these reasons, a definition of convergence is not straight-forward for finite fields.[8] □

Remark 2.6
According to common practice, $\mathbb{F}^n$ denotes the n-dimensional column vector space over $\mathbb{F}$. Any vector $\mathbf{v} \in \mathbb{F}^n$ can be termed by a column vector of coordinates

$$\mathbf{v} = \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix},$$

instead of which, for convenience, often the transpose $\mathbf{v}^{\mathrm{T}} = (v_1, v_2, \ldots, v_n)$ will be used. □

Example 2.2
The set $\mathcal{V} = \{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3\}$ of column vectors $\mathbf{v}_1^{\mathrm{T}} = (1,1,2,0)$, $\mathbf{v}_2^{\mathrm{T}} = (0,1,1,1)$ and $\mathbf{v}_3^{\mathrm{T}} = (1,0,1,2)$ over the finite field $\mathbb{F}_3$ with addition and multiplication modulo 3, respectively, generates a subspace $V \in \mathbb{F}_3^4$. Observing that

$$\mathbf{v}_3 = \mathbf{v}_1 + 2\mathbf{v}_2 \,,$$

[7] If $\mathcal{B}$ contains infinitely many elements then V is called a vector space of infinite dimension.
[8] This imposes strong restrictions on the existence of approximation models.

the vector $\mathbf{v}_3$ is a linear combination of the linearly independent vectors $\mathbf{v}_1$ and $\mathbf{v}_2$. Then a basis of V is $\{\mathbf{v}_1, \mathbf{v}_2\}$ and $\bar{\mathbf{v}}_3$, the column vector of coordinates for $\mathbf{v}_3$ with respect to that basis of V, is $\bar{\mathbf{v}}_3^{\mathrm{T}} = (1,2)$. The dimension of this space is $\dim(V) = 2$. □

Now, one is in the position to define transformation maps on vector spaces.

Definition 2.13 (Linear Transformations)
Let $V = (\mathcal{V}, +, \mathbb{F})$ and $\bar{V} = (\bar{\mathcal{V}}, +, \mathbb{F})$ be vector spaces over the field $\mathbb{F}$. The mapping $t : \mathcal{V} \to \bar{\mathcal{V}}$ is called a linear transformation (mapping) or homomorphism if for all $\mathbf{v}_1, \mathbf{v}_2 \in \mathcal{V}$ and for all $a, b \in \mathbb{F}$

$$t(a\mathbf{v}_1 + b\mathbf{v}_2) = at(\mathbf{v}_1) + bt(\mathbf{v}_2) = a\bar{\mathbf{v}}_1 + b\bar{\mathbf{v}}_2$$

where $\bar{\mathbf{v}}_i = t(\mathbf{v}_i) \in \bar{\mathcal{V}}$ is the image of $\mathbf{v}_i \in \mathcal{V}$ in the vector space $\bar{V}$ under the mapping t. If the mapping t is a one-to-one mapping of $\mathcal{V}$ onto $\bar{\mathcal{V}}$ then the linear transformation t is called nonsingular and V and $\bar{V}$ are termed isomorphic. Otherwise the linear transformation t is called singular. □

As per Definition 2.12, any vector $\mathbf{v}$ of an n-dimensional vector space V can be expressed by use of a basis $\mathcal{B} = \{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$. If $t : \mathcal{V} \to \bar{\mathcal{V}}$, that is $\mathbf{v}$ is subject to a linear transformation into an $\bar{n}$-dimensional vector space $\bar{V}$, then first by linearity

$$t(\mathbf{v}) = t\left(\sum_{j=1}^{n} a_j \mathbf{b}_j\right) = \sum_{j=1}^{n} a_j t(\mathbf{b}_j) \tag{2.2}$$

with the result that linear transformations can be expressed by transformations of the basis. Secondly, all $t(\mathbf{b}_j)$, $j = 1, \ldots, n$, and $t(\mathbf{v})$ are vectors of the vector space $\bar{V}$ with a base, say $\bar{\mathcal{B}} = \{\bar{\mathbf{b}}_1, \ldots, \bar{\mathbf{b}}_{\bar{n}}\}$, hence

$$t(\mathbf{v}) = \sum_{j=1}^{n} a_j \sum_{i=1}^{\bar{n}} t_{ij} \bar{\mathbf{b}}_i, \tag{2.3}$$

$$t(\mathbf{v}) = \sum_{i=1}^{\bar{n}} \bar{a}_i \bar{\mathbf{b}}_i. \tag{2.4}$$

Swapping the sums in equation (2.3) and equating it with (2.4) yields

$$\sum_{i=1}^{\bar{n}} \bar{\mathbf{b}}_i \left(\bar{a}_i - \sum_{j=1}^{n} a_j t_{ij}\right) = 0. \tag{2.5}$$

Since $\bar{\mathcal{B}} = \{\bar{\mathbf{b}}_1, \ldots, \bar{\mathbf{b}}_{\bar{n}}\}$ is a basis, all vectors $\bar{\mathbf{b}}_i$ are linearly independent, thus, the expression in parentheses is zero, that is

$$\bar{a}_i = \sum_{i=0}^{n} t_{ij} a_j. \tag{2.6}$$

Using a matrix $\mathbf{T}$ the entries of which are t_{ij}, $i = 1,\ldots,\bar{n}$, $j = 1,\ldots,n$, and column vectors for the coordinates $\mathbf{a}^{\mathrm{T}} = (a_1,\ldots,a_n)$ and $\bar{\mathbf{a}}^{\mathrm{T}} = (\bar{a_1},\ldots,\bar{a_{\bar{n}}})$ linear transformations can be computed by the matrix-vector product

$$\bar{\mathbf{a}} = \mathbf{T}\,\mathbf{a}, \quad \mathbf{a} \in \mathbb{F}^n, \bar{\mathbf{a}} \in \mathbb{F}^{\bar{n}}, \mathbf{T} \in \mathbb{F}^{\bar{n}\times n} \tag{2.7}$$

employing the coordinates with respect to the corresponding bases only. Moreover, in equation (2.7) the vector spaces are indicated by making use of the typical symbolic notation.

2.3.2 Matrices

The subsequent concepts are intensively used and understood for infinite fields. At a first glance, however, it might be not so clear how to calculate, for instance, the rank or nullspace of a matrix over a finite field. Therefore, some well-known terminology shall be re-exposed and exemplified.

Definition 2.14 (Elementary Column and Row Operations on Matrices)
Let $\mathrm{col}_i(\mathbf{A})$ be the i-th column vector ($\mathrm{row}_i(\mathbf{A})$ the i-th row vector) of a matrix $\mathbf{A} \in \mathbb{F}^{m\times n}$ and $a \neq 0 \in \mathbb{F}$. Then elementary column (row) operations on $\mathbf{A}$ are:

1. replacing $\mathrm{col}_i(\mathbf{A})$ by $a \cdot \mathrm{col}_i(\mathbf{A})$ $\big(\mathrm{row}_i(\mathbf{A})$ by $a \cdot \mathrm{row}_i(\mathbf{A})\big)$,
2. interchanging $\mathrm{col}_i(\mathbf{A})$ and $\mathrm{col}_j(\mathbf{A})$ $\big(\mathrm{row}_i(\mathbf{A})$ and $\mathrm{row}_j(\mathbf{A})\big)$,
3. replacing $\mathrm{col}_i(\mathbf{A})$ by $\mathrm{col}_i(\mathbf{A}) + a \cdot \mathrm{col}_j(\mathbf{A})$ $\big(\mathrm{row}_i(\mathbf{A})$ by $\mathrm{row}_i(\mathbf{A}) + a \cdot \mathrm{row}_j(\mathbf{A})\big)$, $j \neq i$. □

Elementary column (row) operations are performed by right and left multiplication with so-called elementary matrices, which assure scaling, interchanging and replacing of rows (columns).

Example 2.3
By elementary row operations the following system of equations $\mathbf{A}\,\mathbf{x} = \mathbf{b}$ with

$$\mathbf{A} = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}, \; \mathbf{b} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$$

can be solved for $\mathbf{x}$. First, assume the case of a field of rational numbers $\mathbb{Q}$, hence, $\mathbf{A} \in \mathbb{Q}^{3\times 3}$ and $\mathbf{b} \in \mathbb{Q}^3$, and it shall be solved for $\mathbf{x} \in \mathbb{Q}^3$. By elementary row operations

$$\left(\begin{array}{ccc|c} 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \end{array}\right) \rightarrow \left(\begin{array}{ccc|c} 1 & 0 & 1 & 1 \\ 0 & 1 & -1 & -1 \\ 0 & 1 & 1 & 0 \end{array}\right) \rightarrow \left(\begin{array}{ccc|c} 1 & 0 & 1 & 1 \\ 0 & 1 & -1 & -1 \\ 0 & 0 & 2 & 1 \end{array}\right) \rightarrow \left(\begin{array}{ccc|c} 1 & 0 & 1 & 1 \\ 0 & 1 & -1 & -1 \\ 0 & 0 & 1 & 1/2 \end{array}\right)$$

a system of equations is obtained which easily is solved recursively. The unique solution is $\mathbf{x}^{\mathrm{T}} = (1/2, -1/2, 1/2)$.

If the case of a finite field $\mathbb{F}_2$ is assumed then $\mathbf{A} \in \mathbb{F}_2^{3\times 3}$ and $\mathbf{b} \in \mathbb{F}_2^3$ and the task is to solve for $\mathbf{x} \in \mathbb{F}_2^3$, now all operations taken modulo 2. Hence it follows,

$$\left(\begin{array}{ccc|c} 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \end{array}\right) \rightarrow \left(\begin{array}{ccc|c} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{array}\right) \rightarrow \left(\begin{array}{ccc|c} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{array}\right)$$

and from the last row it is obvious that there is no solution $\mathbf{x} \in \mathbb{F}_2^3$. □

Definition 2.15 (Rank of a Matrix)
The column (row) rank of a matrix $\mathbf{A} \in \mathbb{F}^{m\times n}$ is the number of linearly independent column (row) vectors of $\mathbf{A}$. If the column (row) rank is n (m) then the matrix $\mathbf{A}$ is said to have full column (row) rank. □

It can be seen that for square matrices column and row rank are the same. In this regard they simply have *a rank*.

Remark 2.7 (Column and Row Space)
The column (row) vectors of a matrix $\mathbf{A} \in \mathbb{F}^{m\times n}$ generate or span the so-called column (row) space of the matrix $\mathbf{A}$. The associated dimension of the column (row) space of a matrix $\mathbf{A}$ equals its column (row) rank. Moreover, the column space of a matrix is a subspace of $\mathbb{F}^m$. □

Since scaling and interchanging of vectors in a basis does not vary the vector space, elementary row operations on matrices do not change the row space of a matrix. This will be made use of by recourse to the example above. The rank of the square matrix $\mathbf{A} \in \mathbb{Q}^{3\times 3}$ is to be determined. The last transformation comprises three linearly independent row vectors, $(1,0,1)$, $(0,1,-1)$, $(0,0,1)$, hence, the dimension of the associated row vector space is three and as $\mathbf{A}$ is square, $\text{rank}(\mathbf{A}) = 3$ assuming $\mathbf{A} \in \mathbb{Q}^{3\times 3}$. For $\mathbf{A} \in \mathbb{F}_2^{3\times 3}$ there are two linearly independent row vectors, $(1,0,1)$, $(0,1,1)$, alternatively, there is only a choice of two linearly independent column vectors, which results in $\text{rank}(\mathbf{A}) = 2$ in the case $\mathbf{A} \in \mathbb{F}_2^{3\times 3}$.

Linear equations as $\mathbf{A}\mathbf{x} = \mathbf{b}$ with $\mathbf{A}$ square are always uniquely solvable if $\mathbf{A}$ is of full (maximal) rank. In these cases a linear left transformation to be applied on $\mathbf{A}$ which maps $\mathbf{A}$ to the identity matrix $\mathbf{I}$ exists. This leads to the following theorem.

Theorem 2.6 (Inverse of a Matrix)
Iff a matrix $\mathbf{A} \in \mathbb{F}^{n\times n}$ is of full rank then a unique inverse matrix denoted by $\mathbf{A}^{-1} \in \mathbb{F}^{n\times n}$ exists such that

$$\mathbf{A}^{-1}\mathbf{A} = \mathbf{I}.$$

In this case $\mathbf{A}$ is termed invertible. □

With the inverse matrix $\mathbf{A}^{-1}$ the unique solution of a system of equations $\mathbf{A}\mathbf{x} = \mathbf{b}$ reads $\mathbf{x} = \mathbf{A}^{-1}\mathbf{b}$.

Remark 2.8
If a linear transformation t on a vector space $V = (\mathcal{V}, +, \mathbb{F})$ maps $\mathcal{V}$ onto $\mathcal{V}$, that is $t : \mathcal{V} \to \mathcal{V}$, then the corresponding matrix $\mathbf{T}$ is square and has full rank, thus the matrix $\mathbf{T}$ is invertible. In addition to that, such linear transformations are called nonsingular, see Definition 2.13. For this reason invertible matrices are said to be nonsingular. □

Many major properties of a matrix are invariant by its structure and are preserved under elementary row and column operations, so-called similarity transformations.

Definition 2.16 (Similarity of Matrices)
Matrices $\mathbf{A}_1, \mathbf{A}_2 \in \mathbb{F}^{n\times n}$ are similar if

$$\mathbf{A}_2 = \mathbf{T}\mathbf{A}_1\mathbf{T}^{-1} \tag{2.8}$$

for some invertible matrix $\mathbf{T} \in \mathbb{F}^{n\times n}$. □

An interpretation of similarity is given by a change of coordinates. Consider a linear transformation $a : \mathcal{V} \to \mathcal{V}$ on a vector space $V = (\mathcal{V}, +, \mathbb{F})$ represented by $\mathbf{x}' = \mathbf{A}\mathbf{x}$ with a square matrix $\mathbf{A}$ that is not necessarily nonsingular. According to equation (2.7) let the coordinates $\mathbf{x}$ be subject to a coordinate transformation $t : \mathcal{V} \to \mathcal{V}$ with $\bar{\mathbf{x}} = \mathbf{T}\mathbf{x}$ and a nonsingular square matrix $\mathbf{T}$. Then the question arises: how can the linear transformation a be translated into the new coordinates? Some simple calculation steps give the answer

$$\bar{\mathbf{x}}' = \mathbf{T}\mathbf{A}\mathbf{T}^{-1}\,\bar{\mathbf{x}}. \tag{2.9}$$

Consequently, $\bar{\mathbf{A}} = \mathbf{T}\mathbf{A}\mathbf{T}^{-1}$ represents the matrix of the linear transformation a with regard to the new coordinates.

Definition 2.17 (Kernel and Image of a Matrix)
Let the matrix $\mathbf{A} \in \mathbb{F}^{m\times n}$ represent the mapping $a : \mathbb{F}^n \to \mathbb{F}^m$. Then the set

$$\mathrm{Ker}(\mathbf{A}) := \{\mathbf{x} \in \mathbb{F}^n \,|\, \mathbf{A}\mathbf{x} = \mathbf{0}\}$$

is termed kernel or nullspace of the matrix $\mathbf{A}$ and the set

$$\mathrm{Im}(\mathbf{A}) := \{\mathbf{b} \in \mathbb{F}^m \,|\, \exists \mathbf{x} \in \mathbb{F}^n : \mathbf{A}\mathbf{x} = \mathbf{b}\}$$

is referred to as the image of the matrix $\mathbf{A}$. □

In order to simplify the terminology, any vectors will implicitly mean column vectors unless explicitly specified in a different way.

Example 2.4
As an example recall the linear transformation with the matrix $\mathbf{A} \in \mathbb{F}_2^{3\times 3}$ from above. Then the kernel and image of $\mathbf{A}$ can be calculated by

$$\left(\begin{array}{ccc|c} 1 & 0 & 1 & b_1 \\ 1 & 1 & 0 & b_2 \\ 0 & 1 & 1 & b_3 \end{array}\right) \rightarrow \left(\begin{array}{ccc|c} 1 & 0 & 1 & b_1 \\ 0 & 1 & 1 & b_1+b_2 \\ 0 & 1 & 1 & b_3 \end{array}\right) \rightarrow \left(\begin{array}{ccc|c} 1 & 0 & 1 & b_1 \\ 0 & 1 & 1 & b_1+b_2 \\ 0 & 0 & 0 & b_1+b_2+b_3 \end{array}\right)$$

Therefore, the kernel is

$$\mathrm{Ker}(\mathbf{A}) = \left\{ \begin{pmatrix} x_3 \\ x_3 \\ x_3 \end{pmatrix}, x_3 \in \mathbb{F}_2 \right\} = \left\{ x_3 \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, x_3 \in \mathbb{F}_2 \right\}$$

and the image

$$\begin{aligned} \mathrm{Im}(\mathbf{A}) &= \left\{ \mathbf{b} \in \mathbb{F}^3 \,|\, b_1+b_2+b_3 = 0 \right\} = \left\{ \begin{pmatrix} b_2+b_3 \\ b_2 \\ b_3 \end{pmatrix}, b_2, b_3 \in \mathbb{F}_2 \right\} \\ &= \left\{ b_2 \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} + b_3 \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}, b_2, b_3 \in \mathbb{F}_2 \right\}. \end{aligned}$$ □

Remark 2.9
The complement to the concept of rank is the concept of nullity. The nullity of a matrix $\mathbf{A} \in \mathbb{F}^{m\times n}$, or equivalently, of its linear mapping $a : \mathbb{F}^n \rightarrow \mathbb{F}^m$ is the dimension of the nullspace of the matrix $\mathbf{A}$, $\mathrm{nullity}(\mathbf{A}) = \dim(\mathrm{Ker}(\mathbf{A}))$, whereas the rank is the dimension of the image concerning $\mathbf{A}$, $\mathrm{rank}(\mathbf{A}) = \dim(\mathrm{Im}(\mathbf{A}))$. Connecting both, an important theorem states that

$$\mathrm{nullity}(\mathbf{A}) + \mathrm{rank}(\mathbf{A}) = n = \dim(\mathbb{F}^n). \qquad \square$$

The subsequent definitions prepare the introduction of the Smith canonical form of a matrix. To this end, matrices with variant coefficients need to be considered.

Definition 2.18 (Rational and Polynomial Matrix)
A matrix $\mathbf{R}(\lambda)$, the elements of which are fractions of polynomials in $\mathbb{F}[\lambda]$ is called a rational matrix. If the denominator polynomial of each element of $\mathbf{R}(\lambda)$ is equal to one then the matrix is a polynomial matrix.[9] □

[9] Let $\mathbb{F}[\lambda]^{n\times m}$ denote the set of $n \times m$ polynomial matrices with entries that are polynomials in the ring $\mathbb{F}[\lambda]$, i. e. with coefficients in the field $\mathbb{F}$. Accordingly, $\mathbb{F}_q[\lambda]^{n\times m}$ denotes the respective finite field version.

Elementary column and row operations can be extended to row and column multiplications with polynomial factors using matrices, which are a generalization to elementary matrices: unimodular matrices.

Definition 2.19 (Unimodular Matrix)
A polynomial matrix whose inverse matrix is a polynomial matrix is called unimodular. □

It is easy to show that the determinant of an unimodular (polynomial) matrix is a nonzero scalar in the underlying field $\mathbb{F}$. Unimodular matrices are the main ingredient for stating the following important theorem.

Theorem 2.7 (Smith Form of the Characteristic Matrix)
For any matrix $\mathbf{A} \in \mathbb{F}^{n\times n}$ unimodular matrices $\mathbf{U}(\lambda), \mathbf{V}(\lambda) \in \mathbb{F}[\lambda]^{n\times n}$ exist such that

$$\mathbf{U}(\lambda)(\lambda\mathbf{I} - \mathbf{A})\mathbf{V}(\lambda) = \mathbf{S}(\lambda) \tag{2.10}$$

with the characteristic matrix $(\lambda\mathbf{I} - \mathbf{A})$ corresponding to $\mathbf{A}$ and the unique polynomial matrix

$$\mathbf{S}(\lambda) = \begin{pmatrix} c_1(\lambda) & 0 & \cdots & 0 \\ 0 & c_2(\lambda) & & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \cdots & 0 & c_n(\lambda) \end{pmatrix}, \tag{2.11}$$

in which the monic polynomials $c_{i+1} \,|\, c_i$, $i = 1, \ldots, n-1$. The polynomial matrix $\mathbf{S}(\lambda) \in \mathbb{F}[\lambda]^{n\times n}$ is called the Smith canonical form of (the characteristic matrix wrt.) $\mathbf{A}$.[10] □

The calculation of the unimodular matrices $\mathbf{U}(\lambda)$ and $\mathbf{V}(\lambda)$ is most efficiently carried out by employing symbolic procedures which are offered by computer algebra packages such as Maple® and Mathematica®. For an algorithm see [Boo67, p. 268 ff.], [Gil69, p. 222 ff.] or [LT85].

By equating the Smith canonical forms of two matrices $\mathbf{A}_1$ and $\mathbf{A}_2$ and employing Definition 2.19 for unimodular matrices finally leads the following important result[11]

Theorem 2.8 (Smith Form Similarity Criterion)
Two square matrices $\mathbf{A}_1$ and $\mathbf{A}_2$ are similar iff they have the same Smith form. □

Since the polynomials $c_i(\lambda)$, $i = 1, \ldots, n$, in the Smith canonical form are preserved under similarity transformations this gives rise to define invariants.

[10] In general, respective Smith canonical forms exists for arbitrary non-square polynomial matrices.
[11] Showing that the corresponding transformation matrices are constant matrices is more involved [Kai80].

2.3.3 Invariants of Matrices

Definition 2.20 (Invariant Polynomials)
The unique (non-constant) monic polynomials $c_i(\lambda), i = 1,\ldots,n$, referring to the Smith form $\mathbf{S}(\lambda) \in \mathbb{F}[\lambda]^{n\times n}$ of a matrix $\mathbf{A} \in \mathbb{F}^{n\times n}$ are the invariant polynomials (similarity invariants) of $\mathbf{A}$. □

Note that the product of all invariant polynomials equals the characteristic polynomial, that is $\mathrm{cp}_{\mathbf{A}}(\lambda) = \det(\lambda\mathbf{I} - \mathbf{A}) = \prod_i c_i(\lambda)$. The uppermost polynomial $c_1(\lambda)$ in the Smith form can be identified with the minimal polynomial $\mathrm{mp}_{\mathbf{A}}(\lambda)$ of the matrix $\mathbf{A}$, which is the polynomial of least degree such that the associated matrix polynomial holds identically zero, that is $\mathrm{mp}_{\mathbf{A}}(\mathbf{A}) \equiv \mathbf{0}$. From the divisibility property of the invariant polynomials it is clear that $\mathrm{mp}_{\mathbf{A}} | \mathrm{cp}_{\mathbf{A}}$.

With Theorem 2.4 the invariant polynomials can be decomposed into factors.

Definition 2.21 (Elementary Divisor Polynomials, Elementary Divisors)
Let $c_i \in \mathbb{F}[\lambda]$, $i = 1,\ldots,n$, be the invariant polynomials of a matrix $\mathbf{A} \in \mathbb{F}^{n\times n}$ and $c_i = p_{i,1}^{e_{i,1}} \cdots p_{i,N_i}^{e_{i,N_i}}$ be the unique factorization of c_i into N_i factors due to Theorem 2.4. Then, the $N = \sum_{i=1}^{n} N_i$ non-constant monic factor polynomials $p_{i,j}^{e_{i,j}}$, $i = 1,\ldots,n$ and $j = 1,\ldots,N_i$, are termed elementary divisor polynomials of $\mathbf{A}$. The set of (integral) powers e_j, $j = 1,\ldots,N$, is referred to as the set of elementary divisors of $\mathbf{A}$. □

2.3.4 The Rational Canonical Form

In addition to the Smith form (2.11), another canonical form referring to the elementary divisor polynomials will be used. This involves the notion of a companion matrix.

Definition 2.22 (Companion Matrix)
Let $p_{\mathbf{C}}(\lambda) = \lambda^d + \sum_{i=0}^{d-1} a_i \lambda^i \in \mathbb{F}[\lambda]$ be a monic polynomial of degree d. Then the $(d \times d)$-matrix[12]

$$\mathbf{C} = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & 0 & \cdots & 0 & -a_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & -a_{d-2} \\ 0 & 0 & 0 & \cdots & 1 & -a_{d-1} \end{pmatrix} \tag{2.12}$$

over $\mathbb{F}$ is called the companion matrix with respect to the polynomial $p_{\mathbf{C}}(\lambda)$. □

By transforming the characteristic matrix of a companion matrix on its Smith form [LT85] the following useful property of a companion matrix can be shown [BM77, p. 339].

[12] in literature, sometimes the transpose of this matrix

Theorem 2.9 (Characteristic and Minimal Polynomial of a Companion Matrix)
Let $p_{\mathbf{C}}(\lambda)$ be the defining polynomial, $\mathrm{cp}_{\mathbf{C}}(\lambda)$ the characteristic polynomial, and $\mathrm{mp}_{\mathbf{C}}(\lambda)$ the minimal polynomial, all with respect to a companion matrix $\mathbf{C}$. Then the following property holds:

$$\mathrm{cp}_{\mathbf{C}}(\lambda) \equiv \mathrm{mp}_{\mathbf{C}}(\lambda) \equiv p_{\mathbf{C}}(\lambda)\,, \tag{2.13}$$

that is, companion matrices are so-called non-derogatory matrices. □

Definition 2.23 (Rational Canonical Form)
The block diagonal matrix $\mathbf{A}_{\mathrm{rat}} \in \mathbb{F}^{n\times n}$ with

$$\mathbf{A}_{\mathrm{rat}} = \mathrm{diag}(\mathbf{C}_1, \ldots, \mathbf{C}_N)\,, \tag{2.14}$$

where $\mathbf{C}_i$, $i = 1, \ldots, N$ are companion matrices, is called a rational canonical form. □

Theorem 2.10 (Uniqueness of the (Classical) Rational Canonical Form of a Matrix)
For any matrix $\mathbf{A} \in \mathbb{F}^{n\times n}$ exists a similarity transformation

$$\mathbf{A}_{\mathrm{rat}} = \mathbf{T}\mathbf{A}\mathbf{T}^{-1} \tag{2.15}$$

by virtue of an invertible constant matrix $\mathbf{T}$ such that $\mathbf{A}_{\mathrm{rat}}$ is a rational canonical form, which comprises the $i = 1, \ldots, N$ companion matrices $\mathbf{C}_i$ with respect to the elementary divisor polynomials p_i of the matrix $\mathbf{A}$.

Apart from the ordering of the companion matrices $\mathbf{C}_i$ the matrix $\mathbf{A}_{\mathrm{rat}}$ is unique and the number N is maximal regarding $\mathbf{A}$. □

The matrix $\mathbf{A}_{\mathrm{rat}}$ often will be referred to, simply, as the rational canonical form of $\mathbf{A}$. An algorithm for computing the transformation matrix $\mathbf{T}$ is given in [Gil69, p. 225 ff.]. An alternative is presented in Appendix B.

Example 2.5
The following Smith form of a matrix $\mathbf{A} \in \mathbb{F}_2^{6\times 6}$

$$\mathbf{S}(\lambda) = \begin{pmatrix} \lambda^5+\lambda^4+\lambda^2+\lambda & 0 & 0 & 0 & 0 & 0 \\ 0 & \lambda+1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} (\lambda^2+\lambda+1)(\lambda+1)^2\lambda & 0 & 0 & 0 & 0 & 0 \\ 0 & \lambda+1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

apparently has the elementary divisor polynomials

$$p_1(\lambda) = \lambda^2+\lambda+1, \quad p_2(\lambda) = (\lambda+1)^2, \quad p_3(\lambda) = \lambda, \quad p_4(\lambda) = \lambda+1\,.$$

Then the corresponding companion matrices and the rational canonical form of **A** are

$$\mathbf{C}_1 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \quad \mathbf{C}_3 = \begin{pmatrix} 0 \end{pmatrix}, \qquad \mathbf{C}_2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \mathbf{C}_4 = \begin{pmatrix} 1 \end{pmatrix}, \qquad \longrightarrow \quad \mathbf{A}_{\text{rat}} = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}. \qquad \square$$

Remark 2.10
The Jordan canonical form of a matrix, which would follow from diagonalizing the rational canonical form, is omitted here because the Jordan canonical form is accompanied by the notion of an extension field $\mathbb{F}_{q^k}$, $k = 1, 2, \ldots$, associated to $\mathbb{F}_q$. As will be shown in Appendix C, for finite fields the calculation of roots in this extension field $\mathbb{F}_{q^k}$ is much more cumbersome than it is in the extension field associated to the field of real numbers $\mathbb{R}$, which is $\mathbb{C}$, the field of complex numbers. $\square$

2.4 An Image Domain for Finite Fields

In this section discrete functions $f : \mathbb{N}_0 \to \mathbb{F}_q$ are dealt with. These functions can be interpreted as an infinite sequence of function values $f(0), f(1), f(2), \ldots \in \mathbb{F}_q$. Similar to discrete functions over the infinite field of real numbers, for which the so-called $\mathcal{Z}$-transform applies, a counterpart exists for the finite field $\mathbb{F}_q$. This will be referred to as the $\mathcal{A}$-transform. The basic idea of this transform, an operational calculus for finite fields, was introduced for feedback shift register synthesis at the end of the fifties [Huf56, Fri59] and widely used for linear coding, linear sequential switching circuits and networks in the sixties of the past century; see [Kau65] which is a compilation of the most important contributions in that field. Though it was made use of frequently, a formal derivation of the calculus was performed quite late [Boo62, Ric65, Boo67]. After a decade this transform was rediscovered for the use within the analysis of linear automata [Wun75, Gös91]. Recently, it was applied for establishing a binary system theory [Wen00].

2.4.1 The $\mathcal{A}$-Transform

The application of the $\mathcal{A}$-transform in Chapter 5 will have the very narrow focus of transforming a first order linear recurring sequence into an algebraic expression with respect to an image domain. Therefore, the mathematical theory shall be exposed only briefly.[13]

[13] During the years the image domain representation was defined and redefined in several other ways. Huffmann [Huf56] originally defined the $\mathcal{D}$-transform by $\mathcal{D}\{f(k)\} = F(D) = \sum_{k=0}^{\infty} f(k) D^k$, thus $D = 1/a$. In the same manner

Definition 2.24 ($\mathcal{A}$-Transform)
The $\mathcal{A}$-transform for a discrete function $f(k)$ over $\mathbb{F}_q$ with $f(k) = 0, \forall k < 0$ is

$$\mathcal{A}\{f(k)\} = F(a) := \sum_{k=0}^{\infty} f(k)\, a^{-k},$$

in which addition and multiplication are taken modulo q. □

In this sense, the original domain is the domain on which the discrete function $f(k)$ resides and the image domain is the domain where $F(a)$, the $\mathcal{A}$-transform of $f(k)$, is defined.[14] To any value of $f(k)$ in the k-domain corresponds exactly one monomial in the $\mathcal{A}$-domain (it can be shown that the converse is true as well). Both domains are related by a bijection of transform and inverse transform. As a consequence, any calculation can be carried out, alternatively, on either of the both domains.

In view of Definition 2.24 the inverse transform can be determined according to the following theorem.

Theorem 2.11 (Inverse of the $\mathcal{A}$-Transform)
The inverse transform of the $\mathcal{A}$-transform is given by

$$\begin{aligned} \mathcal{A}^{-1}\{F(a)\} &= f(0),\, f(1),\, f(2), \ldots \\ f(k) &= [a^k F(a)]_{\text{ind}}, \end{aligned} \tag{2.16}$$

in which the operation $[a^k F(a)]_{\text{ind}}$ provides the addend of the rational expression $a^k F(a)$ which is independent of a.[15] □

The inverse operation $\mathcal{A}^{-1}$ precisely transforms image domain functions into corresponding infinite sequences of function values in the original domain.

2.4.2 Table of Correspondences

If the transform of linear systems of equations is taken into account then only a few rather obvious transformation rules are relevant (see Table 2.1).

Wunsch [Wun75] and Gössel [Gös91] used the symbols ζ and d, respectively, instead of the parameter D whereas Richalet [Ric65] defined an operational calculus as per $F(p) = \sum_{k=0}^{\infty} f(k)\, p^{-(k+1)}$ with parameter p, as a consequence $F(p) = F(a)/p$. In general, causality of $f(k)$, i. e. $f(k) = 0, \forall k < 0$, is an assumption common to all the definitions used. The definition presented here is taken from [Wen00] and its laws are in wide accordance with those from the $\mathcal{Z}$-transform. This clue, at least to the author, is reason enough to use the $\mathcal{A}$-transform. Whatever may be preferred, the transform tables are easily rephrased.

[14] Clearly, $F(a)$ is an operator, but for the purposes here it can simply be considered as a quotient of polynomials.

[15] As an alternative to equation (2.16) the rational function $F(a)$ can be written in partial fraction form (after a polynomial division if necessary) and then some correspondences may be used for the backward transform by means of which sequences of function values are obtained, typically. To obtain functional expressions for $f(k)$ involves more computational effort. The reader may refer to [Boo62] for the details.

original domain (function of k)	**image domain** (function of a)
$\alpha_i \in \mathbb{F}_q : \; g(k) := \sum_{i=1}^{n} \alpha_i \, f_i(k)$	$\alpha_i \in \mathbb{F}_q : \; G(a) = \sum_{i=1}^{n} \alpha_i F_i(a)$
$g(k) := \sum_{i=0}^{k} f(i)$	$G(a) = \frac{a}{a-1} F(a)$
$g(k) := \sum_{i=0}^{k} f_1(i) \, f_2(k-i)$	$G(a) = F_1(a) F_2(a)$
$g(k) := f(k+1)$	$G(a) = aF(a) + a \, f(0)$

Table 2.1: $\mathcal{A}$-transform for functions $f(k)$ with $f(k) = 0, \forall k < 0$

Applications are part of Chapter 5.

Chapter 3

Finite State Automata in the State Space

The study of dynamic systems presupposes a system model. There are many models for discrete event systems, and each model has pros and cons depending its purpose. Established models are graphical representations like Petri nets or automaton graphs, set-oriented representations invoking formal languages, or algebraic models as the (max,+)-algebra. This chapter presents two methods for determining a particular algebraic model with respect to a subclass of discrete event systems, finite state automata. The result is a discrete state space model over a finite field.

In order not to loose oneself in too much technicalities, consider the following illustration (Figure 3.1) which reflects a deterministic automaton model of a simple conveyor belt and its interpretation as a discrete state space model over a finite field — Table 3.1 depicts the meaning of the used symbols, Figure 3.2 illustrates the conveyor belt states.

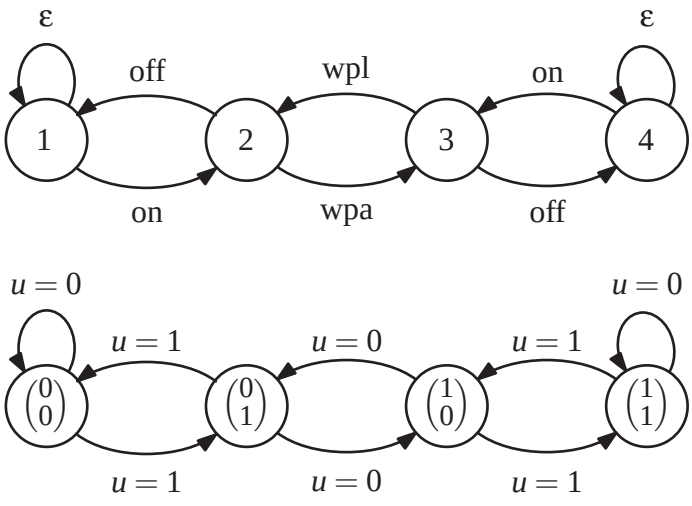


Figure 3.1: Simple conveyor belt — automaton graph (top), state space model interpretation (bottom)

Symbol	Type	Meaning
on	Event	motor of the conveyor belt switched on
off	Event	motor of the conveyor belt switched off
wpa	Event	workpiece arrives at sensor of conveyor belt
wpl	Event	workpiece leaves sensor of conveyor belt
ε	Event	empty string (no event taking place)
1	State (initial)	conveyor belt at rest, without workpiece
2	State	moving conveyor belt, without workpiece
3	State	moving conveyor belt, workpiece detected at sensor
4	State	conveyor belt at rest, workpiece detected at sensor

Table 3.1: Meaning of the symbols in the automaton graph used in Figure 3.1

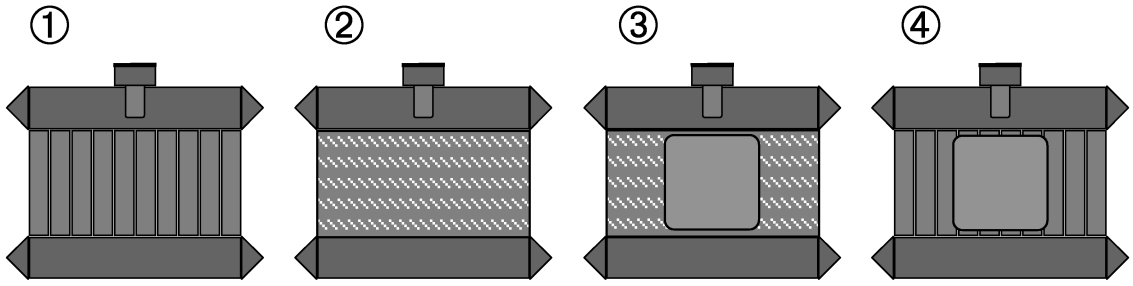


Figure 3.2: Conveyor belt states in the automaton graph of Figure 3.1

In the state space model, u is to be understood as an input variable that takes on values $u \in \{0,1\}$. Setting $u = 1$ results in switching the conveyor belt motor into the corresponding other mode — from on to off and from off to on — and $u = 0$ means to stay in the respective mode. For practical purposes, $u = 1$ is the actual control action, $u = 0$ corresponds to doing nothing. The states $\mathbf{x}$ of the automaton graph are coded in binary vectors with values in $\{0,1\} \times \{0,1\}$. In light of the mathematical preliminaries from Chapter 2, for a fixed counter instant $k \in \mathbb{N}_0$ the respective state vector $\mathbf{x}(k)$ and input vector $u(k)$ can be interpreted as elements of a vector space over a finite field with characteristic 2, i. e. for $k \in \mathbb{N}_0$ fixed $\mathbf{x}(k) \in \mathbb{F}_2^2$ and $u(k) \in \mathbb{F}_2$.

Additionally, the input $u(k)$ can be considered as a necessary condition that has to be met in instant k for enabling a state transition from state $\mathbf{x}(k)$ to state $\mathbf{x}(k+1)$. For instance in the example

problem from above, if the input $u(k) = 0$ for all $k \in \mathbb{N}_0$ then beginning in some instant, two of the states show a 2-periodic transient behavior

$$\cdots \begin{pmatrix} 0 \\ 1 \end{pmatrix} \rightarrow \begin{pmatrix} 1 \\ 0 \end{pmatrix} \rightarrow \begin{pmatrix} 0 \\ 1 \end{pmatrix} \cdots$$

and the remaining two states are mapped onto itself.

Considerations like those lead to the central question of this chapter:

> How to determine an algebraic relation that represents the state evolution depending on the input?

On the basis of an algebraic relation, a behavior as in the above-sketched example problem can be related to a corresponding algebraic property, which for the case of linear models will be examined in detail in Chapter 4 and Chapter 5 where the focus is on the analysis and synthesis of linear systems over finite fields, whereas this chapter is to demonstrate how such discrete models can be derived by referring to methods that base on an elementary level of boolean algebra — see Remark 3.1. From this boolean algebra point of view, discrete models over a finite field $\mathbb{F}_q$ are natural just for $q = 2$. For this reason, the development of the discrete state space models will concentrate on the case of $\mathbb{F}_2$ as well as the examples in the subsequent Chapters 4 and 5, though the examinations in these later chapters encompass the general case $\mathbb{F}_q$ for q an arbitrary prime.

The chapter continues with a review of the minimum necessary basics from boolean algebra in Section 3.1. Besides the standard boolean operations, in particular the isomorphism of boolean algebra with the finite field $\mathbb{F}_2$ is stressed. Utilizing the disjunctive normal form and the Reed-Muller form, two methods for deriving a finite field model over $\mathbb{F}_2$ out of a state transition table or an automaton graph are presented in Section 3.2. Final remarks comment on how these methods can be applied for modeling deterministic systems.

Remark 3.1
From a more general point of view, discrete state space model can be defined as polynomial dynamic systems over an arbitrary finite field $\mathbb{F}_q$, for which it is essential that the respective transition function is a partial, polynomial function over $\mathbb{F}_q$. In order to develop methods for such systems that are rich in content, one is bound to make considerable enlargements within “algebraic toolbox”, that means, it is necessary to introduce basics from algebraic geometry and elimination theory [CLO98], for example ideals, varieties and Gröbner-bases. For the scope of analysis and synthesis of only linear systems as it is the goal in the Chapters 4 and 5 this would much mean overdoing it. The reader may refer to the excellent works from Hervé Marchand and Michel Le Borgne at the Institut National de Recherche en Informatique et Automatique (INRIA) and the Institut de Recherche en Informatique et Système Aléatoires (IRISA), both in Rennes (France) — for a short overview see [LBL89, LBL91, BLL91], deeper insight offers the thesis [Mar97] and the technical reports [ML97, ML99, PML99]. □

3.1 The Relation of Boolean Algebra with the Finite Field $\mathbb{F}_2$

Some basics from boolean algebra are required for determining the discrete system model over a finite field [BP81, Tha88].

Definition 3.1 (Boolean Operations)
Given the set $\mathbb{B} = \{0,1\}$. The boolean operations AND "$\wedge$" (conjunction), OR "$\vee$" (disjunction), XOR "$\oplus$" (exclusive disjunction) and NOT "$\bar{}$" (negation) are defined on $\mathbb{B}$ as follows:

x_1	x_2	$x_1 \wedge x_2$
0	0	0
0	1	0
1	0	0
1	1	1

x_1	x_2	$x_1 \vee x_2$
0	0	0
0	1	1
1	0	1
1	1	1

x_1	x_2	$x_1 \oplus x_2$
0	0	0
0	1	1
1	0	1
1	1	0

x	$\bar{x}$
0	1
1	0

□

Boolean operations allow to construct boolean functions, which usually are expressed in normal form representations. In practice, special types of normal forms help to reduce the logic complexity by diminishing the number of logical devices and admit an easier decomposition into logical subfunctions in order to improve modularity. The next normal form is standard.

Definition 3.2 (Disjunctive Normal Form (DNF))
A boolean function $f : \mathbb{B}^n \to \mathbb{B}$ with indeterminates $\mathbf{x}^{\mathrm{T}} = (x_1, \ldots, x_n) \in \mathbb{B}^n$ is given in disjunctive normal form (DNF) if with $\mathbf{c}^{\mathrm{T}} = (c_1, \ldots, c_n) \in \mathbb{B}^n$

$$f(\mathbf{x}) = \bigvee_{\mathbf{c} \in \mathbb{B}^n} \Big(f(\mathbf{c}) \wedge \bigwedge_{i=1}^{n} (x_i \oplus c_i) \Big). \qquad \square$$

As already suggested by the denotation "normal form", the following holds true.

Theorem 3.1 (Uniqueness of the DNF of a Boolean Function)
For any boolean function $f : \mathbb{B}^n \to \mathbb{B}$ a representation in a disjunctive normal form exists. Except for ordering this representation is unique. □

Example 3.1
The disjunctive normal form of the boolean function $f : \mathbb{B}^2 \to \mathbb{B}$ with $f(x_1, x_2) = x_1 \oplus x_2$ is

$$\begin{aligned} f(x_1,x_2) \;=\; & \big(f(0,0) \wedge (x_1 \oplus 0) \wedge (x_2 \oplus 0)\big) \vee \big(f(0,1) \wedge (x_1 \oplus 0) \wedge (x_2 \oplus 1)\big) \vee \\ & \big(f(1,0) \wedge (x_1 \oplus 1) \wedge (x_2 \oplus 0)\big) \vee \big(f(1,1) \wedge (x_1 \oplus 1) \wedge (x_2 \oplus 1)\big) = \\ & \big((x_1 \wedge (x_2 \oplus 1)\big) \vee \big((x_1 \oplus 1) \wedge x_2\big) = (x_1 \wedge \bar{x_2}) \vee (\bar{x_1} \wedge x_2), \quad x_1, x_2 \in \mathbb{B}. \end{aligned}$$

Hence, the XOR-operation can be eliminated by means of the operations AND, OR and NOT. □

An other important normal form is based on XOR and AND [Zhe27, Mul54, Ree54, HHL$^+$00].[1]

Definition 3.3 (Zhegalkin Form (Reed-Muller Form))
A boolean function $f : \mathbb{B}^n \to \mathbb{B}$ with indeterminates $\mathbf{x}^{\mathrm{T}} = (x_1, \ldots, x_n) \in \mathbb{B}^n$ is given in Zhegalkin form (Reed-Muller form) if

$$f(\mathbf{x}) = \bigoplus_{\mathcal{S} \in 2^{\mathcal{J}}} \left(\delta^{\mathcal{S}} \wedge \bigwedge_{i \in \mathcal{S}} x_i \right)$$

in which $2^{\mathcal{J}}$ is the power set of the index set $\mathcal{J} = \{1, 2, \ldots, n\}$ and $\delta^{\mathcal{S}} \in \mathbb{B}$ are constants. □

Theorem 3.2 (Uniqueness of the Zhegalkin Form of a Boolean Function)
For any boolean function $f : \mathbb{B}^n \to \mathbb{B}$ a representation in a Zhegalkin form (Reed-Muller form) exists. Except for ordering this representation is unique. □

Example 3.2
The Zhegalkin form of an arbitrary boolean function $f : \mathbb{B}^2 \to \mathbb{B}$ with indeterminates x_1, x_2 reads

$$f(x_1, x_2) = \delta^{\emptyset} \oplus (\delta^1 \wedge x_1) \oplus (\delta^2 \wedge x_2) \oplus (\delta^{1,2} \wedge x_1 \wedge x_2)$$

in which $\delta^{\emptyset}, \delta^1, \delta^2, \delta^{1,2} \in \mathbb{B}$ are constants. □

Any boolean operation in Definition 3.1 can be expressed by XOR and AND only. To this end, observe that

$$\overline{x} = 1 \oplus x, \quad x \in \mathbb{B}, \tag{3.1}$$

which applying DeMorgan's Law results in

$$x_1 \vee x_2 = \overline{x_1 \wedge x_2} = 1 \oplus ((1 \oplus x_1) \wedge (1 \oplus x_2)) = x_1 \oplus x_2 \oplus (x_1 \wedge x_2), \quad x_1, x_2 \in \mathbb{B}. \tag{3.2}$$

The underlying algebraic system with the operations XOR and AND is a ring with respect to $(\mathbb{B}, \oplus, \wedge)$, the so-called boolean ring, and by deeper inspection it can be inferred that $\mathbb{B} \backslash \{0\}$ is a commutative group with respect to $\wedge$, see the Definitions 2.3 and 2.5. As a consequence, $(\mathbb{B}, \oplus, \wedge)$ is a field. Even further, the operations XOR and AND on the set $\mathbb{B} = \{0, 1\}$ can be identified with addition modulo 2 and multiplication modulo 2 on the field $\mathbb{F}_2$, that is the following important theorem can be stated.

Theorem 3.3 (Isomorphism of $\mathbb{F}_2$ and $\mathbb{B}$)
The set $\mathbb{B} = \{0, 1\}$ together with the operations $+ := \oplus$ and $\cdot := \wedge$ is a finite field. The finite field $\mathbb{B}$ is isomorphic to the Galois-Field $\mathbb{F}_2$. □

[1] In the year 1927, Zhegalkin was the first to discover that such a normal form exists for any boolean function. Reed and Muller, to whom these forms now are attributed, 1954 reinvented this normal form and extended the notion to arbitrary rings over finite fields $\mathbb{F}_q$. Currently, many different Reed-Muller forms circulate in the literature. Exactly speaking, the Reed-Muller form presented here is the so-called positive polarity Reed-Muller expansion, a denotation that refers to the positive exponents regarding the indeterminates (all equal 1 for the case $\mathbb{F}_2$).

Since any boolean function f can be manipulated so as to obtain its Zhegalkin form which comprises the operations $\oplus$ and $\wedge$ only, the calculation of the finite field representation of f over $\mathbb{F}_2$ amounts to a simple interchange of $\oplus$ by $+\bmod 2$ and $\wedge$ by $\cdot \bmod 2$, respectively (starting from here addition and multiplication understood modulo 2). Then for $x_1, x_2 \in \mathbb{B}$ the following equivalences to $\mathbb{F}_2$ apply:

$$x_1 \wedge x_2 \iff x_1 x_2 \tag{3.3}$$
$$x_1 \vee x_2 \iff x_1 + x_2 + x_1 x_2 \tag{3.4}$$
$$x_1 \oplus x_2 \iff x_1 + x_2 \tag{3.5}$$
$$\bar{x} \iff 1 + x \tag{3.6}$$

These equivalences indicate how to transform an arbitrary boolean function into its respective counterpart over the finite field $\mathbb{F}_2$.

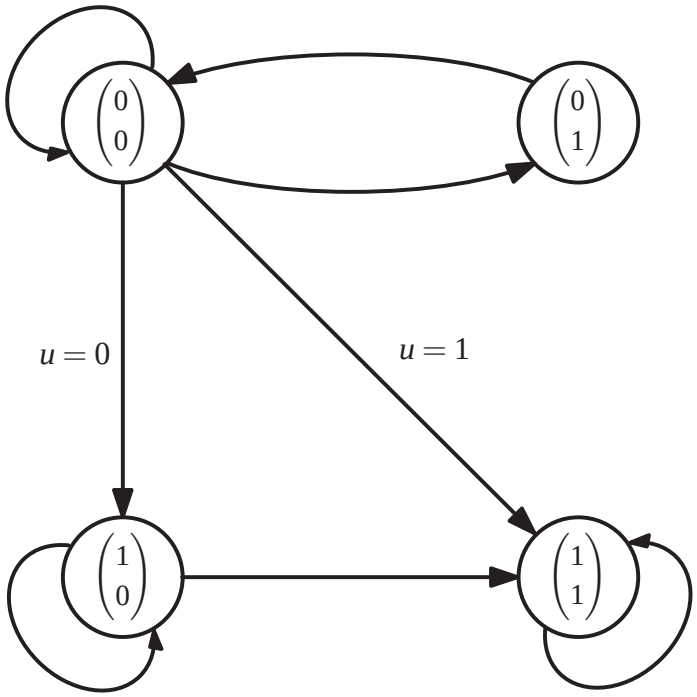
3.2 Methods for Determining the State Space Model

Considering the concepts from boolean algebra presented above, this section exposes two methods for determining a discrete system model over the finite field $\mathbb{F}_2$. The outcome of these methods is an implicit multilinear transition function $f : \mathbb{F}_2^n \times \mathbb{F}_2^n \times \mathbb{F}_2^m \to \mathbb{F}_2$ according to

$$f(\mathbf{x}(k+1), \mathbf{x}(k), \mathbf{u}(k)) = 0 = \sum_{\mathcal{S}_1 \in 2^{\mathcal{J}_n}} \sum_{\mathcal{S}_2 \in 2^{\mathcal{J}_n}} \sum_{\mathcal{S}_3 \in 2^{\mathcal{J}_m}} \delta^{\mathcal{S}_1, \mathcal{S}_2, \mathcal{S}_3} \Big(\prod_{i \in \mathcal{S}_1} x_i(k+1) \Big) \Big(\prod_{j \in \mathcal{S}_2} x_j(k) \Big) \Big(\prod_{l \in \mathcal{S}_3} u_l(k) \Big), \tag{3.7}$$

in which $k \in \mathbb{N}_0$ is a counter, $\mathbf{x}(k) \in \mathbb{F}_2^n$ and $\mathbf{u}(k) \in \mathbb{F}_2^m$ are the state and input vector of the system at instant k, respectively. The sets $\mathcal{J}_n = \{1, 2, \ldots, n\}$, $\mathcal{J}_m = \{1, 2, \ldots, m\}$ are index sets, $2^{\mathcal{J}_n}$ denotes the (possibly empty) power set of $\mathcal{J}_n$ and $\delta^{\mathcal{S}_1, \mathcal{S}_2, \mathcal{S}_3} \in \mathbb{F}_2$ are constants. The function f takes on the value 0 at a fixed instant k if $\mathbf{x}(k)$, $\mathbf{x}(k+1)$, $\mathbf{u}(k)$ represents an admissible evolution of state $\mathbf{x}(k)$ into $\mathbf{x}(k+1)$ under the input $\mathbf{u}(k)$ in the underlying system, otherwise the value of f is 1.[2] Inspecting the next state $\mathbf{x}(k+1)$ for fixed k, multiple successors $\mathbf{x}(k+1)$ may be observed since f is an implicit function for the next state $\mathbf{x}(k+1)$ — strictly speaking a relation. This indicates that the finite field representation (3.7) is capable of modeling non-deterministic finite state automata as well.

[2] It is a peculiarity of discrete models over finite fields $\mathbb{F}_q$ that one single function f is sufficient for representing the state transition behavior even for $n > 1$ states. For the finite field $\mathbb{F}_2$ this can easily be seen when considering $i = 1, \ldots, n$ equations $f_i(\mathbf{x}) = 0$ in which only those $\mathbf{x} = \mathbf{x}^\star$ are considered admissible that solve all n equations. As a consequence, $f(\mathbf{x}) := 1 + \prod_{i=1}^{n} (1 + f_i(\mathbf{x})) = 0$. A similar result can be shown for the general case $\mathbb{F}_q$.



u	x_2'	x_1'	x_2	x_1	f_c
0	0	0	0	0	1
0	0	0	0	1	0
0	0	0	1	0	1
0	0	0	1	1	0
0	0	1	0	0	1
0	0	1	0	1	1
0	0	1	1	0	0
0	0	1	1	1	0
0	1	0	0	0	1
0	1	0	0	1	0
0	1	0	1	0	0
0	1	0	1	1	0
0	1	1	0	0	0
0	1	1	0	1	1
0	1	1	1	0	0
0	1	1	1	1	1
1	0	0	0	0	1
1	0	0	0	1	0
1	0	0	1	0	1
1	0	0	1	1	0
1	0	1	0	0	0
1	0	1	0	1	1
1	0	1	1	0	0
1	0	1	1	1	0
1	1	0	0	0	1
1	1	0	0	1	0
1	1	0	1	0	0
1	1	0	1	1	0
1	1	1	0	0	1
1	1	1	0	1	1
1	1	1	1	0	0
1	1	1	1	1	1

Figure 3.3: Graph of an example automaton (above) and its state table (to the right). The column marked f_c signifies whether a transition from $(x_1,x_2)^T$ to $(x_1',x_2')^T$ under input u is admissible and vice versa.

3.2.1 The Disjunctive Normal Form Method

In what follows, a single input example is used to introduce the main steps for obtaining the discrete transition function over the finite field $\mathbb{F}_2$ for a non-deterministic automaton. The underlying algorithm can be generalized easily and is omitted for clearness.

Consider the automaton depicted in Figure 3.3. The nodes are coded by binary vectors, which represent the states $\mathbf{x}^T = (x_1,x_2) \in \mathbb{F}_2^2$. Arcs connect the states and indicate admissible transitions between the states. Marked arcs denote that the transition is admissible only if a certain condition imposed on the input variables u is satisfied, that is if $u = 1$. If no marking is specified on an arc then a transition is admissible under any choice of inputs. Obviously, there are arcs with the same marking that lead to different successor states, i. e. the automaton is non-deterministic.

For abbreviation, let the symbol k be omitted within the denotation of $x_i(k)$ and $u(k)$ and let $x_i(k+1)$ be abbreviated by x_i' instead. In order to work out the state transition function, the logical interconnection of the state $\mathbf{x}$ and input u and successor state $\mathbf{x}'$ is translated into a state table (right

hand side of Figure 3.3). Clearly, each row in the state table corresponds to a function value $f_c = 1$ if a transition in the automaton graph is admissible, $f_c = 0$ if it is not.

Therefore, in view of the DNF, Definition 3.2, and along the lines of Example 3.1 the DNF of the function f represented in the state table of Figure 3.3 reads

$$\begin{aligned} f(x_1', x_2', x_1, x_2, u) \;=\; & \overline{u}x_2'\overline{x}_1'\overline{x}_2\overline{x}_1 \vee \overline{u}\overline{x}_2'\overline{x}_1'x_2\overline{x}_1 \vee \overline{u}x_2'\overline{x}_1'\overline{x}_2\overline{x}_1 \vee \overline{u}\overline{x}_2'x_1'\overline{x}_2x_1 \vee \overline{u}x_2'\overline{x}_1'\overline{x}_2\overline{x}_1 \vee \\ & \overline{u}x_2'x_1'\overline{x}_2x_1 \vee \overline{u}x_2'x_1'x_2x_1 \vee u\overline{x}_2'\overline{x}_1'\overline{x}_2\overline{x}_1 \vee u\overline{x}_2'\overline{x}_1'x_2\overline{x}_1 \vee u\overline{x}_2'x_1'\overline{x}_2x_1 \vee \\ & ux_2'\overline{x}_1'\overline{x}_2\overline{x}_1 \vee ux_2'x_1'\overline{x}_2\overline{x}_1 \vee ux_2'x_1'\overline{x}_2x_1 \vee ux_2'x_1'x_2x_1 = 1\,, \end{aligned} \tag{3.8}$$

$$\begin{aligned} \Longleftrightarrow\; f(x_1', x_2', x_1, x_2, u) \;=\; & \overline{x}_2'\overline{x}_1'\overline{x}_2\overline{x}_1 \vee \overline{x}_2'\overline{x}_1'x_2\overline{x}_1 \vee \overline{u}\overline{x}_2'x_1'\overline{x}_2\overline{x}_1 \vee \overline{x}_2'x_1'\overline{x}_2x_1 \vee x_2'\overline{x}_1'\overline{x}_2\overline{x}_1 \vee \\ & x_2'x_1'\overline{x}_2x_1 \vee x_2'x_1'x_2x_1 \vee ux_2'x_1'\overline{x}_2\overline{x}_1 = 1\,, \end{aligned} \tag{3.9}$$

in which the abbreviation $a \wedge b = a\,b$ is used. Observe that by applying DeMorgan's law

$$a_1 \vee a_2 \vee \ldots \vee a_k = 1 \quad \Longleftrightarrow \quad (1 \oplus a_1) \wedge (1 \oplus a_2) \wedge \ldots \wedge (1 \oplus a_k) = 0\,, \tag{3.10}$$

all disjunctions can be eliminated. The remaining negations in (3.9) vanish by setting $\overline{a} = a \oplus 1$, thus, a function that comprises $\wedge$ and $\oplus$ only is obtained. Therefore, with (3.3) and (3.5), the representation of the transition function in the finite field $\mathbb{F}_2$ is

$$\begin{aligned} f(x_1'x_2', x_1, x_2, u) \;=\; & \big(1 + (1 + x_2')(1 + x_1')(1 + x_2)(1 + x_1)\big) \cdots \\ & \big(1 + x_2'x_1'x_2x_1\big)\big(1 + ux_2'x_1'(1 + x_2)(1 + x_1)\big) = 0\,, \end{aligned} \tag{3.11}$$

$$\begin{aligned} \Longleftrightarrow\; f(x_1'x_2', x_1, x_2, u) \;=\; & x_1 + x_1x_1' + x_2x_1' + x_2x_2' + x_1x_2x_2' + x_1'x_2' + x_1x_1'x_2' + \\ & x_1x_2x_1'x_2' + x_1'u + x_1x_1'u + x_2x_1'u + x_1x_2x_1'u = 0\,. \end{aligned} \tag{3.12}$$

3.2.2 The Reed-Muller Generator Matrix Method

The regular tabulation of the state table in Figure 3.3 — which originates from binary counting, row by row — gives a hint for determining the transition function f more efficiently. So-called Reed-Muller codes, well-known in linear coding theory, exploit this property [HHL$^+$00].

Consider the Reed-Muller generator matrix $\mathbf{G}_i \in \mathbb{F}_2^{2^i \times 2^i}$, $i \in \mathbb{N}_0$, which is defined recursively as per

$$\mathbf{G}_i := \begin{pmatrix} \mathbf{G}_{i-1} & \mathbf{0} \\ \mathbf{G}_{i-1} & \mathbf{G}_{i-1} \end{pmatrix}, \quad \mathbf{G}_0 := 1\,. \tag{3.13}$$

Using this Reed-Muller generator matrix the demanded transition function reads [Ree54, HHL$^+$00]

$$f(x_1', x_2', \ldots, x_n', x_1, x_2, \ldots, x_n, u_1, u_2, \ldots, u_m) = (\mathbf{G}_{2n+m}\mathbf{f}_c)^{\mathrm{T}}\boldsymbol{\varphi}_{2n+m} + 1 = 0\,. \tag{3.14}$$

In equation (3.14), the vector $\boldsymbol{\varphi}_{2n+m}$ with $\dim(\boldsymbol{\varphi}_{2n+m}) = 2^{2n+m}$ is a vector of those monomials that can be combined from the variable sets $\{x_1,\ldots,x_n\}$, $\{u_1,\ldots,u_m\}$, and $\{x'_1,\ldots,x'_n\}$, which are the entries of the state vector $\mathbf{x}$, the input vector $\mathbf{u}$ and the next state vector $\mathbf{x}'$, respectively. The vector $\mathbf{f}_c$ with $\dim(\mathbf{f}_c) = 2^{2n+m}$ is made up of the rightmost column entries in the state table of Figure 3.3.

It remains to explain how to tabulate the monomials in $\boldsymbol{\varphi}_{2n+m}$. This will become clear by resorting to the example of Figure 3.3, in which

$$\mathbf{G}_5 = \begin{pmatrix}
1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
1&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
1&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
1&1&0&0&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
1&0&1&0&1&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
1&1&1&1&1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
1&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
1&1&0&0&0&0&0&0&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
1&0&1&0&0&0&0&0&1&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
1&1&1&1&0&0&0&0&1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
1&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
1&1&0&0&1&1&0&0&1&1&0&0&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
1&0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
1&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0\\
1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0\\
1&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0\\
1&1&0&0&1&1&0&0&0&0&0&0&0&0&0&0&1&1&0&0&1&1&0&0&0&0&0&0&0&0&0&0\\
1&0&1&0&1&0&1&0&0&0&0&0&0&0&0&0&1&0&1&0&1&0&1&0&0&0&0&0&0&0&0&0\\
1&1&1&1&1&1&1&1&0&0&0&0&0&0&0&0&1&1&1&1&1&1&1&1&0&0&0&0&0&0&0&0\\
1&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0\\
1&1&0&0&0&0&0&0&1&1&0&0&0&0&0&0&1&1&0&0&0&0&0&0&1&1&0&0&0&0&0&0\\
1&0&1&0&0&0&0&0&1&0&1&0&0&0&0&0&1&0&1&0&0&0&0&0&1&0&1&0&0&0&0&0\\
1&1&1&1&0&0&0&0&1&1&1&1&0&0&0&0&1&1&1&1&0&0&0&0&1&1&1&1&0&0&0&0\\
1&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0\\
1&1&0&0&1&1&0&0&1&1&0&0&1&1&0&0&1&1&0&0&1&1&0&0&1&1&0&0&1&1&0&0\\
1&0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1&0\\
1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1
\end{pmatrix}, \quad \boldsymbol{\varphi}_5 = \begin{pmatrix}
1\\ x_1\\ x_2\\ x_1x_2\\ x'_1\\ x_1x'_1\\ x_2x'_1\\ x_1x_2x'_1\\ x'_2\\ x_1x'_2\\ x_2x'_2\\ x_1x_2x'_2\\ x'_1x'_2\\ x_1x'_1x'_2\\ x_2x'_1x'_2\\ x_1x_2x'_1x'_2\\ u\\ x_1u\\ x_2u\\ x_1x_2u\\ x'_1u\\ x_1x'_1u\\ x_2x'_1u\\ x_1x_2x'_1u\\ x'_2u\\ x_1x'_2u\\ x_2x'_2u\\ x_1x_2x'_2u\\ x'_1x'_2u\\ x_1x'_1x'_2u\\ x_2x'_1x'_2u\\ x_1x_2x'_1x'_2u
\end{pmatrix} \tag{3.15}$$

are the Reed-Muller generator matrix and the respective vector of monomials. The tabulation regarding the elements of $\boldsymbol{\varphi}_5$ obeys a recursion: if starting the inspection from the top of the vector then any added new variable becomes a right factor of a copy of the former part of the vector, and so on. A substitution of $\mathbf{G}_5$ and $\boldsymbol{\varphi}_5$ from (3.15) in (3.14) verifies the result from (3.12).

3.2.3 Deterministic State Space Model

The following is to comment on how an explicit deterministic model can be generated for a deterministic finite state automaton. In this case, the state tables can be reshaped as illustrated in Table 3.2. Thus, by employing the methods from Section 3.2.1 and 3.2.2 a transition function can be determined in which the next state becomes explicit, that is

$$\mathbf{x}(k+1) = \mathbf{f}(\mathbf{x}(k), \mathbf{u}(k)) \tag{3.16}$$

u_m	$\cdots$	u_2	u_1	x_n	$\cdots$	x_2	x_1	x_n'	$\cdots$	x_2'	x_1'
0	$\cdots$	0	0	0	$\cdots$	0	0	$f_{n,1}$	$\cdots$	$f_{2,1}$	$f_{1,1}$
0	$\cdots$	0	0	0	$\cdots$	0	1	$f_{n,2}$	$\cdots$	$f_{2,2}$	$f_{1,2}$
0	$\cdots$	0	0	0	$\cdots$	1	0	$f_{n,3}$	$\cdots$	$f_{2,3}$	$f_{1,3}$
$\vdots$	$\cdots$	$\vdots$	$\vdots$	$\vdots$	$\cdots$	$\vdots$	$\vdots$	$\vdots$	$\cdots$	$\vdots$	$\vdots$
1	$\cdots$	1	1	1	$\cdots$	1	1	$f_{n,2^{n+m}}$	$\cdots$	$f_{2,2^{n+m}}$	$f_{1,2^{n+m}}$

Table 3.2: Typical shape of a state table regarding a deterministic system

with $k \in \mathbb{N}_0$, $\mathbf{x}(k) \in \mathbb{F}_2^n$, and $\mathbf{u}(k) \in \mathbb{F}_2^m$, which except for the field reminds of the standard form of a non-linear discrete time continuous system.

Since the further examinations in the next chapters are restricted to the deterministic case, the example from the introductory part of this chapter shall be reconsidered, for convenience. Concerning this example, the respective state table, Reed-Muller generator matrix and appendant vector of monomials are

u	x_2	x_1	x_2'	x_1'
0	0	0	0	0
0	0	1	1	0
0	1	0	0	1
0	1	1	1	1
1	0	0	1	0
1	0	1	1	1
1	1	0	0	0
1	1	1	0	1

$$\mathbf{G}_3 = \begin{pmatrix} 1&0&0&0&0&0&0&0 \\ 1&1&0&0&0&0&0&0 \\ 1&0&1&0&0&0&0&0 \\ 1&1&1&1&0&0&0&0 \\ 1&0&0&0&1&0&0&0 \\ 1&1&0&0&1&1&0&0 \\ 1&0&1&0&1&0&1&0 \\ 1&1&1&1&1&1&1&1 \end{pmatrix}, \quad \boldsymbol{\varphi}_3 = \begin{pmatrix} 1 \\ x_1 \\ x_2 \\ x_1x_2 \\ u \\ x_1u \\ x_2u \\ x_1x_2u \end{pmatrix}.$$

Denoting the columns regarding the next state entries x_2' and x_1' in the state table by $\mathbf{f}_{\mathrm{c},2}$ and $\mathbf{f}_{\mathrm{c},1}$, respectively, the application of equation (3.14) results in the state equations

$$\begin{aligned} x_1(k+1) &= (\mathbf{G}_3\mathbf{f}_{\mathrm{c},1})^{\mathrm{T}}\boldsymbol{\varphi}_3(k)+1 = x_2(k)+\big(x_1(k)+x_2(k)\big)\,u(k)\,, \\ x_2(k+1) &= (\mathbf{G}_3\mathbf{f}_{\mathrm{c},2})^{\mathrm{T}}\boldsymbol{\varphi}_3(k)+1 = x_1(k)+u(k)+\big(x_1(k)+x_2(k)\big)\,u(k)\,, \end{aligned}$$

which are non-linear in this case. Observe that by applying a state feedback

$$u(k) = 1+x_1(k)+x_2(k)$$

which avoids that the conveyor belt gets at rest, an affine linear system

$$\mathbf{x}(k+1) = \begin{pmatrix} 0&1 \\ 0&1 \end{pmatrix}\mathbf{x}(k) + \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

can be obtained that can readily be analyzed with the methods to be derived in the next chapter.

Conclusion

In this chapter, an algebraic model for the transient behavior of finite state automata is exposed. On the face of it, this algebraic model appears to be similar to a discrete time system in the world of continuous systems. However, the discrete state space model established here resides on a finite field. For simplicity, it is shown in an exemplary manner that the determination of a state space model over a finite field $\mathbb{F}_2$ involves basics from boolean algebra only. By invoking the disjunctive normal form and the Reed-Muller form of a boolean function, two methods are proposed that allow to derive non-deterministic discrete state space models over the finite field $\mathbb{F}_2$ for such systems. In both methods it is assumed that any state transitions are tabulated in a state table, which does not incur much a restriction as such tables can easily be obtained from other system representations, as for example automaton graphs.

The first procedure is the common boolean algebra method for determining a boolean function out of a set of its function values. The respective disjunctive normal form (DNF) of such a function can be simply read off the state table. In order to obtain a function that depends on the operations XOR and AND only, all disjunctions and negations are eliminated in the DNF, which results in the Reed-Muller form of this function. Employing the isomorphism of boolean algebra and of finite fields over $\mathbb{F}_2$, the outcome is an implicit function that typically represents a non-deterministic state transition behavior, as demonstrated in an example.

In the second procedure the Reed-Muller form of the transition function is determined directly. This methods turns out to entail much less calculation effort as just a matrix multiplication with a generic matrix, the so-called Reed-Muller generator matrix, is required for calculating the Reed-Muller form. For this reason, this method is pursued in the remark on deterministic systems, in which the impressive simplicity is illustrated by means of deriving the discrete state equation over $\mathbb{F}_2$ for the deterministic example problem in the introductory part of this chapter.

Chapter 4

Analysis of Linear Systems over Finite Fields

The main goal of the study in Chapter 3 was to obtain a state space model over finite fields for a rather broad class of discrete event systems. Throughout the next two chapters these models shall be restricted to the deterministic linear case; the technical term *linear modular system* became established for systems, in which the expression *modular* indicates the premise of a finite field.

Even though the scope of linearity seems far from any practical interest, the consideration of linear state space models for finite state automata is worthwhile since their study reveals important insight into the state transition behavior of automata in general. In addition to that, the class of linear discrete systems over finite fields naturally entails a multitude of far-reaching propositions. Not at least, the resulting algorithms are mainly of tractable computational complexity.

When a vector space is endowed with a relation, the type of this relation imposes a particular structure on the underlying vector space. Accordingly, linear state equations impose a somewhat particular structure, a linear structure on the respective state space. Thus, the notion itself suggests that this linear structure of the state space can be exploited for an examination of the interconnection structure of the states in the corresponding automaton. This is the basic idea behind the linear state space models for automata recalled in Section 1.1 of the introductory chapter. Common to all of them is the attempt to determine periodicity properties of states in terms of specific system invariants; for instance eigenvalues of the system dynamics. Yet, using eigenvalues only necessary criteria for periodicity properties have been stated, and without calling for a periodicity test which utilizes the system equations with respect to each considered state [Son00], that is enumerating the state space, no sufficient statements have been derived so far. This lack of sufficient criteria is due to the absence of the field property in these state space models, and as a consequence field-dependent concepts as are for example eigenvalues cannot be employed, which highlights the decisive constructional flaw within these approaches.

Assuming a linear state space model over finite fields, it is the main objective of this chapter to develop and present a necessary and sufficient criterion for determining the entire structural state space decomposition into periodic/aperiodic subspaces comprising the associated periodic/aperiodic states. As a result, the periodic and aperiodic properties of any automaton state can be determined by an effective method which is dependent on a similarity transformation and divisions of polynomials only, whilst at the same time refraining from any state space enumeration technique (exhaustive search algorithms or testing), known to be intractable for large system dimensions. The key concept is the notion of a linear modular system (LMS).

Primarily, the theory of LMS was developed by Huffmann under the technical term *linear sequential coding networks* to the end of generating quasi-random binary digital numbers by employing shift registers with feedback logic [Huf56, Huf59]. The major application was in the field of error-correcting codes [PW72]. Many of the results to be presented in this chapter can be traced back to Elspas and Friedland [Els59, Fri59], who worked out the essential properties of *linear sequential (switching) circuits* under an algebraic perspective using finite fields. A collection of these contributions[1] is given with [Kau65]. Later developments focused on how periodic states could be related to invariants of the characteristic matrix of a linear sequential circuit; the main part of the contributions originate to Gill [Gil64, Gil66b, Gil66a, Gil69] whose results are particularly important within the analysis of LMS.

The first objective of this chapter is to present the basic concept of a linear modular system. On this basis, autonomous and the subclasses of homogeneous and inhomogeneous linear modular systems are introduced in Section 4.1. At the beginning of Section 4.2 the period of a state is defined. The subsequent paragraphs of this section are concerned with the structure of the state space of homogeneous linear modular systems in order to develop a method by means of which a brute force calculation of periodic states is rendered unnecessary. To this end, the block structure of the rational canonical form of the system dynamics matrix is shown to be in strong relation to the structure of the state space. Since these blocks consist of cyclic and nilpotent dynamics matrices only, their influence on the state space is considered, and by linearity these results are superposed amounting to a statement for the case of arbitrary linear dynamics. The main objective is to state a necessary and sufficient criterion of how to decompose the entire state space into subspaces of certain period and cardinality. Resorting to this decomposition the actual states with specified periodic property are calculated in an efficient manner. Section 4.3 presents a generalization of the results to those inhomogeneous linear modular systems for which a translation of state allows to render the state equations linear. For the case in which such a linearization is not possible a solution is given as well. The section closes with the composition of the afore-obtained results. The final part of this chapter summarizes the main steps of the analysis developed so far (Section 4.3.3) and exposes an illustrative example (Section 4.3.4).

[1] the journals of which are rarely available in libraries

4.1 Linear Modular Systems

A Linear Modular System (LMS) is a discrete state space system over a finite field for which the deterministic state transition function f given in relation (3.16) is linear. Furthermore, LMS include a linear output function relating state and input with an output. An LMS represents a discrete dynamic system over finite fields which, owing to the field property, shows analogies to linear discrete time systems over the field of real numbers $\mathbb{R}$. Due to the fact that the state space of an LMS is finite and the transition functions are discrete, LMS are an adequate model for an algebraic examination of simple automata. In view of equation (3.16) a possible definition of an LMS in terms of matrices is as follows

Definition 4.1 (Linear Modular System)
A linear modular (k-invariant) system over $\mathbb{F}_q$, denoted by LMS(q), is given by an evolution equation of the form

$$\mathbf{x}(k+1) = \mathbf{A}\mathbf{x}(k) + \mathbf{B}\mathbf{u}(k), \quad k \in \mathbb{N}_0\,, \tag{4.1}$$

called state equation, in which addition and multiplication are taken modulo q. Furthermore,

- the vector $\mathbf{x}(k)$ is called state vector or state, the vector $\mathbf{u}(k)$ is called input. The set $\mathcal{X} = \mathbb{F}_q^n$ of states and the set $\mathcal{U} = \mathbb{F}_q^m$ of inputs are vector spaces, termed state space and input space, respectively.[2]
- the dimension n of the state space, that is $n = \dim(\mathcal{X})$, is the order or dimension of an LMS,
- the matrix $\mathbf{A} \in \mathbb{F}_q^{n\times n}$ is called the (system) dynamics matrix, the matrix $\mathbf{B} \in \mathbb{F}_q^{n\times m}$ is the input matrix (all matrices independent from k). □

For simplicity, the term LMS will be used any time when it is clear that the prime q is not yet specified. A system is said to be autonomous if the input has no influence on the evolution of state. For an LMS according to equation (4.1) this amounts to $\mathbf{B} = \mathbf{0}$. Moreover, such an autonomous LMS is called homogeneous. If otherwise for all instants k the vector $\mathbf{B}\mathbf{u}(k) = \text{const.} =: \mathbf{b}$ is non-zero then the autonomous LMS is called inhomogeneous.

Obviously, LMS are based on all the concepts from algebra that have been developed so far in Chapter 2 and Chapter 3. For LMS(2) the latter chapter, Chapter 3, introduced methods from Boolean algebra for deriving the respective state space model over the finite field $\mathbb{F}_2$. That is why most of the examples will be confined to the case of $\mathbb{F}_2$ though the results are formulated for $\mathbb{F}_q$ with q an arbitrary prime.

[2] More precisely, $\mathbf{x}(k)$ is the vector-valued mapping $\mathbf{x}: \mathbb{N} \to \mathbb{F}_q^n$ and $\mathbf{u}(k)$ is the vector-valued mapping $\mathbf{u}: \mathbb{N} \to \mathbb{F}_q^m$, both mapping an instant k to a column vector in $\mathcal{X}$ and $\mathcal{U}$, respectively. In order to keep the denotation simple this will not be stressed unless necessary.

4.2 Homogeneous LMS

Firstly, linear homogeneous LMS according to the simplest version of the state space representation in equation (4.1), that is equations of the form

$$\mathbf{x}(k+1) = \mathbf{A}\,\mathbf{x}(k) \tag{4.2}$$

with $\mathbf{x}(k) \in \mathbb{F}_q^n$ and $\mathbf{u}(k) \in \mathbb{F}_q^m$, $k \in \mathbb{N}_0$, shall be dealt with. In the autonomous case, evidently, any information must be included in the structure of the dynamics matrix $\mathbf{A}$. The transition of state $\mathbf{x}(k)$ to $\mathbf{x}(k+1)$ is determined by the linear mapping which corresponds to the matrix $\mathbf{A}$. By applying this mapping κ times the state $\mathbf{x}(k)$ is mapped to the state $\mathbf{x}(k+\kappa)$. Consider the sequence of states $\mathbf{x}(k), \mathbf{x}(k+1), \ldots, \mathbf{x}(k+\kappa)$ which originates from a κ-fold sequence of these mappings. It is easy to see that beginning from an instant i, when some state $\mathbf{x}(i)$ occurs again at instant $i+t$, $t \in \mathbb{N}$, all $t-1$ states in between these identical states show the same characteristic t-periodic behavior for increasing instances $\kappa > i+t$. This idea is characterized in the following definition.[3]

Definition 4.2 (Period of a State)
A state $\mathbf{x}_t$ of an LMS is called t-periodic if

$$\mathbf{x}_t \in \mathcal{X}_t, \quad \mathcal{X}_t := \left\{ \boldsymbol{\xi} \in \mathbb{F}_q^n \,|\, \exists t \in \mathbb{N}, \boldsymbol{\xi} = \mathbf{A}^t \boldsymbol{\xi} \wedge \forall i \in \mathbb{N}, i < t, \boldsymbol{\xi} \neq \mathbf{A}^i \boldsymbol{\xi} \right\}.$$

$\mathcal{X}_t$ is the set of t-periodic states. □

A particular periodic state is the zero state $\mathbf{x}_t = \mathbf{0}$ (null state). In fact, any autonomous LMS comprises a zero state with period $t = 1$. Apart from the zero state there need not exist another periodic state in the state space of an LMS. If only the zero state is periodic all state transitions terminate finally in the zero state. If there is at least one other periodic state (besides the zero state) then some of the state transitions terminate in the periodic structure/s associated to this other periodic state/s with some period. Such periodic structures will be referred to as cycles, a denotation which becomes perspicuous in the state graph, see Figure 4.1.

Apparently, for a linear modular system (4.2) the t-periodic states $\mathbf{x}_t \in \mathbb{F}_q^n$ can be determined from the linear system of equations

$$(\mathbf{I} - \mathbf{A}^t)\,\mathbf{x}_t = \mathbf{0}, \tag{4.3}$$

which for example by employing Gauß' algorithm can be solved for $\mathbf{x}_t$ concerning all conceivable periods t; see the previous Example 2.3.

However, doing that way is by no means an efficient procedure for determining all periodic states in the state space $\mathbb{F}_q^n$ with respect to an autonomous LMS. The most crucial problem is the typically

[3] A similar argument is valid for autonomous non-linear deterministic discrete state space systems over finite fields.

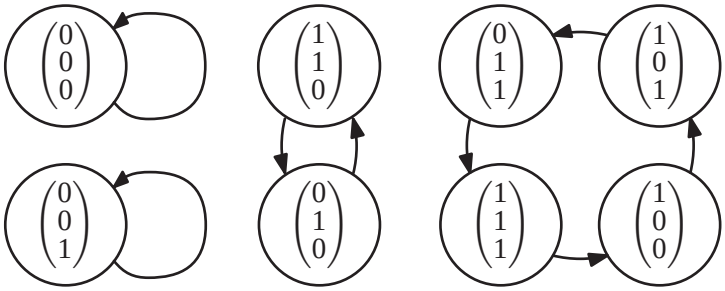


Figure 4.1: Typical example for a state graph with cycles in an LMS of order 3

huge number of q^n states such that after subtracting the 1-periodic zero state, periodic states up to the maximal possible period of $t_{\max} = q^n - 1$ (all but one state in the same cycle) may occur.

In the worst case the calculation of all periodic states $\mathbf{x}_t$, $t = 1, 2, \ldots q^n - 1$, entails the effort of

- $(q^n - 2)$-fold multiplication of the matrix $\mathbf{A}$ for calculating the matrix $\mathbf{A}^t$,
- $q^n - 1$ times solving the linear system of equation (4.3).

A remaining problem is that these calculations still do not yield the sets of states sorted by its period. The reason is that all solutions $\mathbf{x}_{t_\mathrm{d}}$ of

$$(\mathbf{I} - \mathbf{A}^{t_\mathrm{d}})\,\mathbf{x}_{t_\mathrm{d}} = \mathbf{0}$$

for any integer t_d such that $t_\mathrm{d} | t$, that are any divisors t_d which divide t, are solutions of (4.3) as well. Hence, ordinary evaluations of (4.3) as the method proposed in [Son99] bear the risk of enormous computational expenses.

Here on the contrary, the proposal is to benefit from algebraic properties within the structure of the dynamics matrix $\mathbf{A}$. The interconnection of the states is given by the linear modular system (4.2), which relates the state $\mathbf{x}(k)$ in instant k with the next state $\mathbf{x}(k+1)$. It is obvious that a (bijective) change of coordinates on the states, which just amounts to a relabeling of states, does not affect the state graph, hence the state interconnection structure. Concerning linear systems (4.2) a linear change of coordinates on the state $\mathbf{x}$ results in a similarity transformation of the dynamics matrix $\mathbf{A}$. Among others, the most revealing similarity transformation of $\mathbf{A}$ is the transformation into the rational canonical form $\mathbf{A}_\mathrm{rat} = \mathbf{T}\mathbf{A}\mathbf{T}^{-1}$, introduced in equation (2.14). The matrix $\mathbf{A}_\mathrm{rat}$ is transformed into a maximal number of diagonal blocks, each of which is entirely specified by one of the elementary divisor polynomials of $\mathbf{A}$, which are invariant under similarity transformations. As these invariants of $\mathbf{A}$ and $\mathbf{A}_\mathrm{rat}$, respectively, cannot be altered by a coordinate change, these invariants must express the interconnection structure of the states. For this reason, the elementary divisor polynomials have to express the periodicity properties of all states in the respective state space.

As a consequence, when analyzing for periodic states, one is justified in examining the periodicity properties by means of the structurally simpler rational canonical form $\mathbf{A}_{\text{rat}} = \text{diag}(\mathbf{C}_1, \mathbf{C}_2, \ldots, \mathbf{C}_N)$ of the dynamics matrix $\mathbf{A}$. Thus, by transforming $\overline{\mathbf{x}} = \mathbf{T}\mathbf{x}$ with the invertible matrix $\mathbf{T} \in \mathbb{F}_q^{n\times n}$, which only renumbers the state vectors, equation (4.3) can be turned into

$$(\mathbf{I} - \text{diag}(\mathbf{C}_1^t, \mathbf{C}_2^t, \ldots, \mathbf{C}_N^t))\,\overline{\mathbf{x}}_t = \mathbf{0}\,. \tag{4.4}$$

Recall that the companion matrices $\mathbf{C}_i$, $i = 1, \ldots, N$ are determined by the elementary divisor polynomials of $\mathbf{A}$ each of which is a power of an irreducible polynomial. Since the matrix in (4.4) is of block-diagonal type the system of equations can be partitioned into N subproblems to be superposed finally. With regard to the solution of equation (4.4) two disjoint sets with cardinality N_c and N_n yielding $N = N_\text{c} + N_\text{n}$ can be distinguished due to the finiteness of the underlying field[4]

1. the set of all N_c cyclic companion matrices, i. e. all $\mathbf{C}_i$ such that $\mathbf{C}_i^{t_i} = \mathbf{I}$ for some $t_i \in \mathbb{N}$,
2. the set of all N_n nilpotent companion matrices, i. e. all $\mathbf{C}_i$ such that $\mathbf{C}_i^{t_i} = \mathbf{0}$ for some $t_i \in \mathbb{N}$.

Remark 4.1
If the dynamics matrix $\mathbf{A}$ is not singular then all companion matrices $\mathbf{C}_i$ in $\mathbf{A}_{\text{rat}}$ are cyclic. Furthermore, the rightmost column entries of nilpotent companion matrices are all zero. Therefore, for finding out whether a companion matrix is nilpotent it is not necessary to calculate any matrix power. □

Remark 4.2
In Section 4.2.2 nilpotent companion matrices referring to elementary divisor polynomials of the form $p_\mathbf{C}(\lambda) = \lambda^h$ with $h \in \mathbb{N}$ will be concerned separately as these are not related to periodic subspaces. □

It remains to introduce some notation in order to facilitate references in the subsequent sections.

As the rational canonical form $\mathbf{A}_{\text{rat}}$ is determined except for the ordering of its block-diagonal companion matrices, its companion matrices can be reordered such that

$$\hat{\mathbf{A}}_{\text{rat}} = \text{diag}(\mathbf{A}_\text{c}, \mathbf{A}_\text{n})\,, \tag{4.5}$$

in which $\mathbf{A}_\text{c}$ and $\mathbf{A}_\text{n}$ collect the cyclic and nilpotent companion matrices within $\mathbf{A}_{\text{rat}}$, respectively. Thus, the system is decomposable into a cyclic and a nilpotent subsystem

$$\hat{\mathbf{x}}_\text{c}(k+1) \;=\; \mathbf{A}_\text{c}\,\hat{\mathbf{x}}_\text{c}(k)\,, \tag{4.6}$$

$$\hat{\mathbf{x}}_\text{n}(k+1) \;=\; \mathbf{A}_\text{n}\,\hat{\mathbf{x}}_\text{n}(k) \tag{4.7}$$

[4]Note that companion matrices over the infinite field of real numbers can be neither cyclic nor nilpotent.

with $k \in \mathbb{N}_0$ and $\hat{\mathbf{x}}^{\mathrm{T}}(k) =: (\hat{\mathbf{x}}_{\mathrm{c}}^{\mathrm{T}}(k), \hat{\mathbf{x}}_{\mathrm{n}}^{\mathrm{T}}(k))$ such that $\hat{\mathbf{x}}_{\mathrm{c}}(k) \in \mathbb{F}_q^{n_{\mathrm{c}}}$, $\hat{\mathbf{x}}_{\mathrm{n}}(k) \in \mathbb{F}_q^{n_{\mathrm{n}}}$ and $\mathbb{F}_q^{n_{\mathrm{c}}} \times \mathbb{F}_q^{n_{\mathrm{n}}} = \mathbb{F}_q^{n}$, that is $n = n_{\mathrm{c}} + n_{\mathrm{n}}$. Furthermore, N_{c} cyclic and N_{n} nilpotent companion matrices compose $\mathbf{A}_{\mathrm{c}}$ and $\mathbf{A}_{\mathrm{n}}$, respectively. Results regarding any of these subsystems can be superposed due to linearity. The associated original states $\mathbf{x}$ are given by the inverse coordinate transformation[5]

$$\mathbf{x} = \hat{\mathbf{T}}^{-1}\,\hat{\mathbf{x}}. \tag{4.8}$$

In what follows, if not specified any dynamics matrix $\mathbf{A}$ of an LMS shall be assumed in its re-ordered rational canonical form $\hat{\mathbf{A}}_{\mathrm{rat}}$ — since resorting to the appropriate transformation matrix $\hat{\mathbf{T}}$ any dynamics matrix can be transformed into its appropriate rational canonical form and vice versa, which therefore incurs no loss in generality.

4.2.1 Cyclic Dynamics

First of all, by referring to equation (4.6) the cyclic system part $\mathbf{A}_{\mathrm{c}}$ and its respective state space $\mathbb{F}_q^{n_{\mathrm{c}}}$ shall be examined. This amounts to the case as if a cyclic dynamics matrix $\mathbf{A}$ were under concern. An adaption of condition (4.4) to the cyclic system part (4.6) allows to calculate a t-periodic state $\hat{\mathbf{x}}_{\mathrm{c},t} \in \mathbb{F}_q^{n_{\mathrm{c}}}$ by means of the following N_{c} equations

$$(\mathbf{I} - \mathbf{C}_i^t)\,\hat{\mathbf{x}}_{\mathrm{c},t}^{(i)} = \mathbf{0}, \quad i = 1, \ldots, N_{\mathrm{c}}, \tag{4.9}$$

to be fulfilled all at once. In the latter relation the N_{c}-fold composition

$$\hat{\mathbf{x}}_{\mathrm{c},t} = \begin{pmatrix} \hat{\mathbf{x}}_{\mathrm{c},t}^{(1)} \\ \hat{\mathbf{x}}_{\mathrm{c},t}^{(2)} \\ \vdots \\ \hat{\mathbf{x}}_{\mathrm{c},t}^{(N_{\mathrm{c}})} \end{pmatrix}, \quad \hat{\mathbf{x}}_{\mathrm{c},t}^{(i)} \in \mathbb{F}_q^{d_i},\ i = 1, \ldots, N_{\mathrm{c}} \tag{4.10}$$

indicates the N_{c} disjoint subspaces satisfying $\mathbb{F}_q^{d_1} \times \cdots \times \mathbb{F}_q^{d_{N_{\mathrm{c}}}} = \mathbb{F}_q^{n_{\mathrm{c}}}$.

On the other hand, each of these $i = 1, \ldots, N_{\mathrm{c}}$ subspaces has its own t_i-periodic vectors $\hat{\mathbf{x}}_{\mathrm{c},t_i}^{(i)}$ which are determined by

$$(\mathbf{I} - \mathbf{C}_i^{t_i})\,\hat{\mathbf{x}}_{\mathrm{c},t_i}^{(i)} = \mathbf{0}. \tag{4.11}$$

Consequently, each of these $i = 1, \ldots, N_{\mathrm{c}}$ subspaces has its own periodic properties, to be examined with equation (4.11). As the problem is linear, the periodic properties of the entire state space $\mathbb{F}_q^{n_{\mathrm{c}}} = \mathbb{F}_q^{d_1} \times \cdots \times \mathbb{F}_q^{d_{N_{\mathrm{c}}}}$ are determined by the periodic properties of its parts (Section 4.2.1.1). In the next step, the superposition yields all periodic states $\hat{\mathbf{x}}_{\mathrm{c},t}$ with regard to equation (4.10), that is for the cyclic part $\mathbf{A}_{\mathrm{c}}$, which is block-diagonally composed of cyclic companion matrices only (Section 4.2.1.2).

[5] The transformation matrix $\hat{\mathbf{T}}$ transforming $\mathbf{A}$ into $\hat{\mathbf{A}}_{\mathrm{rat}} = \hat{\mathbf{T}}\mathbf{A}\hat{\mathbf{T}}^{-1}$ results in $\hat{\mathbf{T}} = \mathbf{\Pi}\mathbf{T}$, where $\mathbf{T}$ is the transformation matrix such that $\mathbf{A}_{\mathrm{rat}} = \mathbf{T}\mathbf{A}\mathbf{T}^{-1}$ and the matrix $\mathbf{\Pi}$ is the orthogonal permutation matrix that provides the exchanges of companion matrices in $\mathbf{A}_{\mathrm{rat}}$ according to $\hat{\mathbf{A}}_{\mathrm{rat}} = \mathbf{\Pi}\mathbf{A}_{\mathrm{rat}}\mathbf{\Pi}^{\mathrm{T}}$. For details see Chapter A of the Appendix.

4.2.1.1 Periodic States of an LMS with Cyclic Companion Matrix as Dynamics

Thus, the first task is to determine the period t_i which corresponds to a state $\hat{\mathbf{x}}_{\mathrm{c},t_i}^{(i)}$ in the subsystem $\hat{\mathbf{x}}_{\mathrm{c}}^{(i)}(k+1) = \mathbf{C}_i \hat{\mathbf{x}}_{\mathrm{c}}^{(i)}(k)$.[6] The key to the solution of the problem is to take advantage from the notion of annihilating polynomials of matrices and their properties [LT85].

Definition 4.3 (Annihilating Polynomial)
Let $\mathbf{M} \in \mathbb{F}^{n\times n}$ be a matrix. Then any polynomial $p \in \mathbb{F}[\lambda]$ for which

$$p(\mathbf{M}) \equiv \mathbf{0}$$

is called annihilating polynomial of $\mathbf{M}$. □

The standard examples for annihilating polynomials of a matrix $\mathbf{M}$ are its minimal polynomial $\mathrm{mp}_{\mathbf{M}}(\lambda)$ and its characteristic polynomial $\mathrm{cp}_{\mathbf{M}}(\lambda)$, the latter of which is characterized in the well-known theorem of Cayleigh-Hamilton.

Theorem 4.1 (Cayleigh-Hamilton Theorem)
Let $\mathbf{M} \in \mathbb{F}^{n\times n}$ be a matrix. Then the respective characteristic polynomial $\mathrm{cp}_{\mathbf{M}}(\lambda) := \det(\lambda\mathbf{I} - \mathbf{M})$ is one of its annihilating polynomials:

$$\mathrm{cp}_{\mathbf{M}}(\mathbf{M}) \equiv \mathbf{0}\,.$$ □

A simple consequence on companion matrices is due to Theorem 2.9.

Corollary 4.1 (Cayleigh-Hamilton Theorem for Companion Matrices)
Let $p_{\mathbf{C}} \in \mathbb{F}[\lambda]$ be the defining polynomial of the companion matrix $\mathbf{C}$. Then

$$p_{\mathbf{C}}(\mathbf{C}) \equiv \mathrm{cp}_{\mathbf{C}}(\mathbf{C}) \equiv \mathrm{mp}_{\mathbf{C}}(\mathbf{C}) \equiv \mathbf{0}\,.$$ □

The following theorems provides a link between divisibility of polynomials and singularity of matrices, which will be exploited in the proofs of the remaining part of this section.

Theorem 4.2 (Minimal Polynomials Divide Annihilating Polynomials)
Let $\mathbf{M} \in \mathbb{F}^{n\times n}$ be a matrix, $\mathrm{mp}_{\mathbf{M}}(\lambda)$ its minimal polynomial and $f \in \mathbb{F}[\lambda]$. Then f is an annihilating polynomial of $\mathbf{M}$ iff $\mathrm{mp}_{\mathbf{M}}$ divides f, that is

$$f(\mathbf{M}) \equiv \mathbf{0} \quad \Longleftrightarrow \quad \mathrm{mp}_{\mathbf{M}}(\lambda) \,|\, f(\lambda)\,.$$ □

[6] Throughout Section 4.2.1.1 the notation $\mathbf{x}$ and $\mathbf{C}$ will be used instead of the more involved $\hat{\mathbf{x}}_{\mathrm{c},t_i}^{(i)}$ and $\mathbf{C}_i$, respectively.

Theorem 4.3 (Singularity of a Matrix Polynomial)
Let $\mathbf{M} \in \mathbb{F}^{n\times n}$ be a matrix, $\mathrm{mp}_{\mathbf{M}}(\lambda)$ its minimal polynomial and $f \in \mathbb{F}[\lambda]$. Then the matrix $f(\mathbf{M})$ is singular iff $\mathrm{mp}_{\mathbf{M}}(\lambda)$ and $f(\lambda)$ have at least one common factor, that is[7]

$$\det(f(\mathbf{M})) = 0 \quad \Longleftrightarrow \quad \gcd\big(\mathrm{mp}_{\mathbf{M}}(\lambda), f(\lambda)\big) \neq 1\,. \qquad \square$$

Recall, that each companion matrix $\mathbf{C}_i$, $i = 1,\ldots,N_\mathrm{c}$ is already of particular type — $\mathbf{C}_i$ corresponds to the i-th elementary divisor polynomial of $\mathbf{A}_\mathrm{c}$, each of which is a power of one single irreducible polynomial only (and not of more of them). Thus, a promising guideline for the subsequent examination is the following: Firstly, the perspective is confined to a cyclic companion matrix defined by an irreducible polynomial. Secondly, a cyclic companion matrix that is defined by a power of an irreducible polynomial is dealt with, resorting to the results of stage one.

Companion Matrices of an Irreducible Polynomial

In this part of the section the periodic properties of the state space with respect to a cyclic companion matrix of an irreducible polynomial shall be derived. To this end, the following lemma will be helpful.

Lemma 4.1 (Least Exponent of Unipotency of a Matrix)
Let $\mathrm{mp}_{\mathbf{M}} \in \mathbb{F}_q[\lambda]$ be the minimal polynomial with respect to a cyclic matrix $\mathbf{M} \in \mathbb{F}_q^{d\times d}$. Let τ denote the period of $\mathrm{mp}_{\mathbf{M}}(\lambda)$. Then the least $t \in \mathbb{N}$ such that

$$\mathbf{M}^t - \mathbf{I} \equiv \mathbf{0}$$

is $t = \tau$. $\square$

Proof According to Definition 2.8 and since for cyclic $\mathbf{M}$, $p_{\mathbf{M}}(0) \neq 0$, a period τ of $\mathrm{mp}_{\mathbf{M}}(\lambda)$ exists, this period is the least τ such that $\mathrm{mp}_{\mathbf{M}}(\lambda) | \lambda^\tau - 1$, or equivalently

$$g(\lambda)\mathrm{mp}_{\mathbf{M}}(\lambda) = \lambda^\tau - 1$$

for some polynomial $g(\lambda)$; where the degree of $p_{\mathbf{M}}$ is minimal (minimal polynomial), the degree of $\lambda^\tau - 1$ is minimal (period of a polynomial), hence the degree of $g(\lambda)$ is minimal. But then with

$$g(\mathbf{M})\,\mathrm{mp}_{\mathbf{M}}(\mathbf{M}) = \mathbf{M}^\tau - \mathbf{I}\,,$$

and with the annihilating polynomial of least degree, that is $\mathrm{mp}_{\mathbf{M}}(\mathbf{M}) \equiv \mathbf{0}$, immediately follows the result. $\square$

Equipped with this result the central theorem of this paragraph can be proven.

[7] The expression $\gcd(a,b)$ is the greatest common divisor of a and b.

Theorem 4.4 (Periodic State Space wrt. a Companion Matrix of an Irreducible Polynomial) Given an LMS whose dynamics matrix is a cyclic companion matrix $\mathbf{C} \in \mathbb{F}_q^{d\times d}$ that corresponds to an irreducible polynomial $p_{\mathbf{C}} \in \mathbb{F}_q[\lambda]$ of period τ. Then in the LMS

- all non-zero state vectors $\mathbf{x} \in \mathbb{F}_q^d$ are τ-periodic,
- the states form $\nu = (q^d-1)/\tau$ disjoint cycles with period τ (called cycles of length τ),
- the remaining zero-vector has period 1. □

Proof By Corollary 4.1 the defining polynomial $p_{\mathbf{C}}$ of the companion matrix $\mathbf{C}$ is its annihilating polynomial of least degree. Then since $\mathbf{C}$ is cyclic Lemma 4.1 implies that the period τ of $p_{\mathbf{C}}$ is the least number such that

$$\mathbf{C}^\tau - \mathbf{I} \equiv \mathbf{0}\,.$$

Therefore, for arbitrary $\mathbf{x} \in \mathbb{F}_q^d$

$$(\mathbf{C}^\tau - \mathbf{I})\,\mathbf{x} \equiv \mathbf{0}\,,$$

which expresses that any non-zero state $\mathbf{x}$ is periodic of period at most $t = \tau$.

It remains to show that any of these states $\mathbf{x}$ cannot be periodic with $t < \tau$. Assume $t \in \mathbb{N}$ is the period of a state $\mathbf{x}$. Then

$$(\mathbf{C}^t - \mathbf{I})\,\mathbf{x} = \mathbf{0}\,,$$

where t is the least such number. Excluding the trivial case $\mathbf{x} = \mathbf{0}$, which is 1-periodic, the matrix $\mathbf{C}^t - \mathbf{I}$ has to be singular. Consequently, by Theorem 4.3 the minimal polynomial $\mathrm{mp}_{\mathbf{C}}(\lambda)$ and the polynomial $\lambda^t - 1$ must have a common factor. Since by assumption $p_{\mathbf{C}}(\lambda) = \mathrm{mp}_{\mathbf{C}}(\lambda)$ is irreducible[8], the polynomial $\lambda^t - 1$ can only be power of $\mathrm{mp}_{\mathbf{C}}(\lambda)$, which by Theorem 4.2 entails that

$$(\mathbf{C}^t - \mathbf{I})\,\mathbf{x} \equiv \mathbf{0}\,.$$

Hence, by Lemma 4.1 the conclusion is $t = \tau$ and any non-zero state vector $\mathbf{x}$ in the corresponding state space $\mathbb{F}_q^d$ is τ-periodic. Leaving aside the zero state, the remaining $q^d - 1$ states in $\mathbb{F}_q^d$ form $\nu = (q^d-1)/\tau$ cycles of length τ. □

Remark 4.3
The minimally possible period of a d-th degree polynomial over $\mathbb{F}_q$ is its degree d, its maximally possible period is $q^d - 1$, which yields the inequality

$$d \le \tau \le q^d - 1\,.$$

The left inequality is clear from the divisibility of $\lambda^\tau - 1$ by the respective polynomial. The right inequality concerns the period of a so-called primitive polynomial. The result is in accordance with the fact that in any LMS maximally all but the zero state of the q^d states in $\mathbb{F}_q^d$ can make up together one single cycle. □

[8] It is here where the distinction into irreducible polynomials gets its justification.

Example 4.1
Given a companion matrix $\mathbf{C} \in \mathbb{F}_2^{3\times 3}$ together with its irreducible (characteristic and minimal) polynomial $p_{\mathbf{C}} \in \mathbb{F}[\lambda]$,

$$\mathbf{C} = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}, \quad p_{\mathbf{C}}(\lambda) = \lambda^3 + \lambda + 1 = 0,$$

the coefficients of which represent the third column of $\mathbf{C}$. Multiplying $p_{\mathbf{C}}(\mathbf{C})$ by $\mathbf{C}$ yields the following

$$\begin{aligned} \mathbf{C}^5 + \mathbf{C}^3 + \mathbf{C}^2 &\equiv 0 \quad | + \mathbf{C}^3 + \mathbf{C} + \mathbf{I} \equiv 0 \\ \mathbf{C}^5 + \mathbf{C}^2 + \mathbf{C} + \mathbf{I} &\equiv 0 \\ \mathbf{C}^6 + \mathbf{C}^3 + \mathbf{C}^2 + \mathbf{C} &\equiv 0 \quad | + \mathbf{C}^3 + \mathbf{C} + \mathbf{I} \equiv 0 \\ \mathbf{C}^6 + \mathbf{C}^2 + \mathbf{I} &\equiv 0 \\ \mathbf{C}^7 + \mathbf{C}^3 + \mathbf{C} &\equiv 0 \quad | + \mathbf{C}^3 + \mathbf{C} + \mathbf{I} \equiv 0 \\ \mathbf{C}^7 + \mathbf{I} &\equiv 0 \end{aligned}$$

where by construction the minimal number $t = 7$ is obtained (see Lemma 4.1). Consequently, the period of $p_{\mathbf{C}}(\lambda)$ is $\tau = 7$, which implies that $\lambda^3 + \lambda + 1 | \lambda^7 + 1$, i. e. $p_{\mathbf{C}}(\lambda)$ divides $\lambda^7 + 1$.[9] By Theorem 4.4 all non-zero state vectors $\mathbf{x} \in \mathbb{F}_2^3$ are 7-periodic and with $\nu = (2^3 - 1)/7 = 1$ there is exactly one cycle of length $\tau = 7$. □

Companion Matrices of Powered Irreducible Polynomials

It remains to examine the periodic property of the state space regarding a cyclic companion matrix $\mathbf{C} \in \mathbb{F}_q^{d\times d}$ of a powered irreducible polynomial

$$p_{\mathbf{C}}(\lambda) = \mathrm{mp}_{\mathbf{C}}(\lambda) = (p_{\mathrm{irr},\mathbf{C}}(\lambda))^e.$$

This examination is held separate from the past paragraph because in this case, in contrast to the former, the state space $\mathbb{F}_q^d$ can be decomposed further. It will be organized in three steps: firstly, it will be shown that the kernel of the matrix $p_{\mathbf{C}}(\mathbf{C})$ can be decomposed into e nested linear subspaces. Its dimensions shall be determined in a second step. With the knowledge of the dimensions, the number of states in the respective space is clear and the period of these states will be derived, leading to the main theorem of this section.

First, consider the $j = 0, 1 \ldots, e$ sets of vectors

$$\mathcal{N}_j := \mathrm{Ker}\Big((p_{\mathrm{irr},\mathbf{C}}(\mathbf{C}))^j\Big), \quad \mathcal{N}_0 := \{\mathbf{0}\} \tag{4.12}$$

[9] In light of Remark 4.3 this period is maximal and the irreducible polynomial $\lambda^3 + \lambda + 1$ is a primitive polynomial.

which are linear spaces and the $j = 1, \ldots, e$ sets of vectors

$$\mathcal{D}_j := \left\{ \mathbf{x} \in \mathbb{F}_q^d \,|\, (p_{\mathrm{irr},\mathbf{C}}(\mathbf{C}))^j \mathbf{x} = \mathbf{0} \wedge (p_{\mathrm{irr},\mathbf{C}}(\mathbf{C}))^{j-1} \mathbf{x} \neq \mathbf{0} \right\}, \tag{4.13}$$

for which obviously holds

$$\mathcal{D}_j = \mathcal{N}_j - \mathcal{N}_{j-1}, \quad j = 1, \ldots, e. \tag{4.14}$$

Furthermore, note that with this notation and with

$$(p_{\mathrm{irr},\mathbf{C}}(\mathbf{C}))^j \mathbf{x} \neq \mathbf{0} \quad \Longrightarrow \quad (p_{\mathrm{irr},\mathbf{C}}(\mathbf{C}))^\kappa \mathbf{x} \neq \mathbf{0}, \quad \forall \kappa < j \tag{4.15}$$

and for the minimal polynomial

$$(p_{\mathrm{irr},\mathbf{C}}(\mathbf{C}))^e \equiv \mathbf{0} \quad \Longrightarrow \quad (p_{\mathrm{irr},\mathbf{C}}(\mathbf{C}))^e \mathbf{x} = \mathbf{0}, \quad \forall \mathbf{x} \in \mathbb{F}_q^d \tag{4.16}$$

one obtains the following property.

Lemma 4.2 (Nesting Property of Nullspaces)
Let $p_{\mathbf{C}}(\lambda) = (p_{\mathrm{irr},\mathbf{C}}(\lambda))^e$, $e \in \mathbb{N}$, be the d-th degree defining polynomial in $\mathbb{F}_q[\lambda]$ of a companion matrix $\mathbf{C} \in \mathbb{F}_q^{d \times d}$. Assume the basis polynomial $p_{\mathbf{C},\mathrm{irr}}(\lambda)$ to be irreducible over $\mathbb{F}_q$. Then the strict inclusion property (nesting) applies[10]

$$\mathcal{N}_0 \subset \mathcal{N}_1 \subset \mathcal{N}_2 \subset \ldots \subset \mathcal{N}_e = \mathbb{F}_q^d, \tag{4.17}$$

where the $\mathcal{N}_j$ are nullspaces, $\mathcal{N}_0 := \{\mathbf{0}\}$ and $\mathcal{N}_j := \mathrm{Ker}\big((p_{\mathrm{irr},\mathbf{C}}(\mathbf{C}))^j\big)$, $j = 1, \ldots, e$. □

Remark 4.4
With equation (4.13) Lemma 4.2 can be expressed equivalently by

$$\mathbb{F}_q^d = \bigcup_{j=0}^{e} \mathcal{D}_j, \quad \mathcal{D}_0 := \{\mathbf{0}\}, \tag{4.18}$$

in which $\mathcal{D}_i \cap \mathcal{D}_j = \emptyset$ for $i \neq j$. □

For deriving the dimension of the spaces $\mathcal{N}_j$, $j = 1, \ldots, e$ the following lemma will be employed.

[10] On account of the intention to derive the periodicity properties of linear systems over finite fields, the statement of the theorem is restricted to finite fields, though the nesting property of course holds as well for infinite fields for which an analog is given, for example, by generalized eigenvectors $\mathbf{v}_k$ of k-th order defined by

$$(\lambda \mathbf{I} - \mathbf{A})^k \mathbf{v}_k = \mathbf{0} \ \wedge \ (\lambda \mathbf{I} - \mathbf{A})^{k-1} \mathbf{v}_k \neq \mathbf{0}.$$

Here the nesting property shows that the k-th order generalized eigenvector space, spanned by the generalized eigenvectors of k-th order $\mathbf{v}_k$, contains the $(k-1)$-th order generalized eigenvector space spanned by $\mathbf{v}_{k-1}$ and so forth.

Lemma 4.3 (Invariance of Nullspaces)
Let $(p_{\text{irr},\mathbf{C}})^j \in \mathbb{F}_q[\lambda]$ be the defining polynomial of the cyclic companion matrix $\mathbf{C} \in \mathbb{F}_q^{d\times d}$ in which the polynomial $p_{\text{irr},\mathbf{C}}(\lambda)$ is irreducible over $\mathbb{F}_q$. Then the $j = 1,\ldots,e$ nullspaces of the matrices $(p_{\text{irr},\mathbf{C}}(\mathbf{C}))^j$ are invariant under the transformation $\mathbf{C}$, i. e. on any $\mathbf{x}_j \in \text{Ker}\big((p_{\text{irr},\mathbf{C}}(\mathbf{C}))^j\big)$. □

Proof By virtue of the non-singularity of cyclic companion matrices $\mathbf{C}$ and by commutativity of matrix multiplication with regard to matrix polynomials of the same matrix, it follows

$$(p_{\text{irr},\mathbf{C}}(\mathbf{C}))^j\mathbf{x}_j = \mathbf{0} \iff \mathbf{C}\,(p_{\text{irr},\mathbf{C}}(\mathbf{C}))^j\mathbf{x}_j = \mathbf{0} \iff (p_{\text{irr},\mathbf{C}}(\mathbf{C}))^j\,\mathbf{C}\,\mathbf{x}_j = \mathbf{0}$$

for any $\mathbf{x}_j \in \text{Ker}\big((p_{\text{irr},\mathbf{C}}(\mathbf{C}))^j\big)$, $j = 1,\ldots,e$. This implies the invariance of $\mathcal{N}_j := \text{Ker}\big((p_{\text{irr},\mathbf{C}}(\mathbf{C}))^j\big)$ under the mapping $\mathbf{C}$. □

In view of Lemma 4.3, for $j = 1,\ldots,e$ define the map $\mathbf{C}|_{\mathcal{N}_j} : \mathcal{N}_j \to \mathcal{N}_j$ such that

$$\mathbf{C}|_{\mathcal{N}_j}\mathbf{x}_j = \mathbf{C}\,\mathbf{x}_j, \quad \forall \mathbf{x}_j \in \mathcal{N}_j \tag{4.19}$$

describes the portion of the linear transform $\mathbf{C}$ acting on the subspace $\mathcal{N}_j$ only. As a consequence,

$$(p_{\text{irr},\mathbf{C}}(\mathbf{C}|_{\mathcal{N}_j}))^j\mathbf{x}_j = (p_{\text{irr},\mathbf{C}}(\mathbf{C}))^j\mathbf{x}_j, \quad \forall \mathbf{x}_j \in \mathcal{N}_j$$

which with equation (4.12) reads

$$(p_{\text{irr},\mathbf{C}}(\mathbf{C}|_{\mathcal{N}_j}))^j\mathbf{x}_j = \mathbf{0}, \quad \forall \mathbf{x}_j \in \mathcal{N}_j\,.$$

Thus, the polynomial $(p_{\text{irr},\mathbf{C}}(\lambda))^j$ is an annihilating polynomial of $\mathbf{C}|_{\mathcal{N}_j}$ in the space $\mathcal{N}_j$, hence, it is a multiple of the minimal polynomial $\text{mp}_{\mathbf{C}|_{\mathcal{N}_j}}(\lambda)$ — see Theorem 4.2 — and since $(p_{\text{irr},\mathbf{C}}(\lambda))^j$ is power of an irreducible polynomial the minimal polynomial that corresponds to matrix $\mathbf{C}|_{\mathcal{N}_j}$ can only comply with

$$\text{mp}_{\mathbf{C}|_{\mathcal{N}_j}}(\lambda) = (p_{\text{irr},\mathbf{C}}(\lambda))^\kappa$$

for some $\kappa = 1,\ldots,j$.

For a contradiction argument assume $\kappa < j$. Using the fact that the minimal polynomial is the least degree annihilating polynomial of matrix $\mathbf{C}|_{\mathcal{N}_j}$ in the respective space, that is $\text{mp}_{\mathbf{C}|_{\mathcal{N}_j}}(\mathbf{C}|_{\mathcal{N}_j}) \equiv \mathbf{0}$, it follows

$$(p_{\text{irr},\mathbf{C}}(\mathbf{C}|_{\mathcal{N}_j}))^\kappa\mathbf{x}_j = \mathbf{0}, \quad \forall \mathbf{x}_j \in \mathcal{N}_j\,.$$

But on the contrary, for $\kappa < j$ vectors $\mathbf{x}_j^\star \in \mathcal{N}_j$ exist such that

$$(p_{\text{irr},\mathbf{C}}(\mathbf{C}|_{\mathcal{N}_j}))^j\mathbf{x}_j^\star = \mathbf{0} \;\wedge\; (p_{\text{irr},\mathbf{C}}(\mathbf{C}|_{\mathcal{N}_j}))^\kappa\mathbf{x}_j^\star \neq \mathbf{0}$$

as stated by the strict inclusion within the nesting property — see Lemma 4.2. By contradiction, the minimal polynomial of $\mathbf{C}|_{\mathcal{N}_j}$ in $\mathcal{N}_j$ is

$$\text{mp}_{\mathbf{C}|_{\mathcal{N}_j}}(\lambda) = (p_{\text{irr},\mathbf{C}}(\lambda))^j \tag{4.20}$$

and since to any minimal polynomial corresponds a companion matrix the dimension of which is the degree of its minimal polynomial, the subsequent lemma has been proven.

Lemma 4.4 (Dimension of Nullspaces)
Let $(p_{\mathrm{irr},\mathbf{C}})^j \in \mathbb{F}_q[\lambda]$ be the defining polynomial of the cyclic companion matrix $\mathbf{C} \in \mathbb{F}_q^{d\times d}$ with polynomial $p_{\mathrm{irr},\mathbf{C}}$ of degree δ and irreducible over $\mathbb{F}_q$. Let the $j = 1,\ldots,e$ nullspaces $\mathcal{N}_j$ be defined by $\mathcal{N}_j := \mathrm{Ker}\big((p_{\mathrm{irr},\mathbf{C}}(\mathbf{C}))^j\big)$. Then the dimension of each nullspace $\mathcal{N}_j$ is

$$\dim(\mathcal{N}_j) = \deg\big((p_{\mathrm{irr},\mathbf{C}})^j\big) = \delta\, j\,. \qquad \square$$

An other consequence of $(p_{\mathrm{irr},\mathbf{C}}(\lambda))^j$ being minimal polynomial of the matrix $\mathbf{C}|_{\mathcal{N}_j}$ in the space $\mathcal{N}_j$ is that by Lemma 4.1 the least number t such that

$$(\mathbf{C}|_{\mathcal{N}_j})^t - \mathbf{I} \equiv \mathbf{0}$$

is $t = \tau_j$, with τ_j denoting the period of the (powered) polynomial $(p_{\mathrm{irr},\mathbf{C}}(\lambda))^j$ — see Definition 2.5 for the period of a powered polynomial over $\mathbb{F}_q$. Hence all $\mathbf{x}_j \in \mathcal{N}_j$ are at most τ_j-periodic.

In order to see whether there are states with period $t \in \mathbb{N}$ with $t < \tau_j$, assume that $\mathbf{x}_j \in \mathcal{N}_j$ is t-periodic, i. e.

$$\big((\mathbf{C}|_{\mathcal{N}_j})^t - \mathbf{I}\big)\,\mathbf{x}_j = \mathbf{0}\,.$$

Then, excluding the trivial case $\mathbf{x}_j = \mathbf{0}$, the matrix $(\mathbf{C}|_{\mathcal{N}_j})^t - \mathbf{I}$ is singular which per Theorem 4.3 implies that the minimal polynomial $\mathrm{mp}_{\mathbf{C}|_{\mathcal{N}_j}}(\lambda)$ has a factor in common with $\lambda^t - 1$. For reason that the only factors of this minimal polynomial are powers of $p_{\mathrm{irr},\mathbf{C}}(\lambda)$ this means that $\lambda^t - 1$ is divided by $(p_{\mathrm{irr},\mathbf{C}}(\lambda))^\kappa$ for some $\kappa \le j$, analogously

$$g(\lambda)(p_{\mathrm{irr},\mathbf{C}}(\lambda))^\kappa = \lambda^t - 1$$

for some polynomial $g(\lambda)$. Therefore,

$$g(\mathbf{C}|_{\mathcal{N}_j})(p_{\mathrm{irr},\mathbf{C}}(\mathbf{C}|_{\mathcal{N}_j}))^\kappa = (\mathbf{C}|_{\mathcal{N}_j})^t - \mathbf{I} \tag{4.21}$$

In light of Remark 4.4 right-multiplication by an arbitrary state $\mathbf{x}_j \in \mathcal{N}_j$ yields

$$g(\mathbf{C}|_{\mathcal{N}_j})(p_{\mathrm{irr},\mathbf{C}}(\mathbf{C}|_{\mathcal{N}_j}))^\kappa \mathbf{x}_j = ((\mathbf{C}|_{\mathcal{N}_j})^t - \mathbf{I})\,\mathbf{x}_j \tag{4.22}$$

which implies that $\mathbf{x}_j$ is t-periodic if

$$(p_{\mathrm{irr},\mathbf{C}}(\mathbf{C}|_{\mathcal{N}_j}))^\kappa \mathbf{x}_j = \mathbf{0}\,. \tag{4.23}$$

According to the definitions of $\mathcal{N}_j$ and $\mathcal{D}_j$ and under assumption of $\kappa < j$ this equation can only be solved if $\mathbf{x}_j \in \mathcal{N}_\kappa$. But then the states in $\mathcal{D}_j$ are exactly those which are τ_j-periodic.

Lemma 4.5 (Period of the States in $\mathcal{D}_j$)
Let the dynamics matrix of an LMS be given by a cyclic companion matrix $\mathbf{C} \in \mathbb{F}_q^{d\times d}$ the defining polynomial of which is $(p_{\mathrm{irr},\mathbf{C}})^e \in \mathbb{F}_q[\lambda]$. Moreover, let the $j = 1,\ldots,e$ sets $\mathcal{D}_j$ be defined as in equation (4.13). Then any state vector in the set $\mathcal{D}_j$ is τ_j-periodic, where τ_j is the period of the polynomial $(p_{\mathrm{irr},\mathbf{C}}(\lambda))^j$. $\square$

Collecting the past results, referring to a cyclic companion matrix $\mathbf{C}$ and for $j = 0, \ldots, e$ the j-th nested subspace $\mathcal{N}_j := \mathrm{Ker}\big((p_{\mathrm{irr},\mathbf{C}}(\mathbf{C}))^j\big)$ contains exactly $q^{j\delta}$ states of the space $\mathbb{F}_q^d$. To sum it up, this leads to

- 1 state in $\mathcal{N}_0 := \{0\}$, the zero state,
- $q^\delta - 1$ states in the difference set $\mathcal{D}_1 = \mathcal{N}_1 - \mathcal{N}_0$,
- $q^{2\delta} - q^\delta$ states in the difference set $\mathcal{D}_2 = \mathcal{N}_2 - \mathcal{N}_1$,

  .....

- $q^{e\delta} - q^{(e-1)\delta}$ states in the difference set $\mathcal{D}_e = \mathcal{N}_e - \mathcal{N}_{e-1}$ with $\mathcal{N}_e = \mathbb{F}_q^d$ and $d = e\,\delta$.

All $q^{j\delta} - q^{(j-1)\delta}$ states in $\mathcal{D}_j$ have period τ_j such that $\nu_j = \big(q^{j\delta} - q^{(j-1)\delta}\big)/\tau_j$ cycles of τ_j-periodic states lie in the space $\mathcal{D}_j$. Adding up the number of all states in $\mathcal{D}_j$ from $j = 1, \ldots, e$ plus the zero state results in

$$1 + \sum_{j=1}^{e} q^{j\delta} - q^{(j-1)\delta} = q^{e\delta} = q^d$$

which shows that the entire space $\mathbb{F}_q^d$ is composed of those cycles. Accordingly, the following important theorem has been deduced.

Theorem 4.5 (Periodic Nullspace Decomposition of a Companion Matrix)
Given a cyclic companion matrix $\mathbf{C} \in \mathbb{F}_q^{d\times d}$ with respect to the d-th degree polynomial $p_{\mathbf{C}}(\lambda) = (p_{\mathrm{irr},\mathbf{C}}(\lambda))^e$, where $p_{\mathrm{irr},\mathbf{C}}(\lambda)$ is an irreducible polynomial over $\mathbb{F}_q$ of degree δ such that $d = e\,\delta$. Then

1. the associated state space $\mathbb{F}_q^d$ is entirely composed of periodic states as per

$$\begin{array}{lll}
\nu_0 = 1 & \text{cycles of length} & \tau_0 = 1 \\
\nu_1 = \big(q^\delta - 1\big)/\tau_1 & \text{"} & \tau_1 = \tau \\
\nu_2 = \big(q^{2\delta} - q^\delta\big)/\tau_2 & \text{"} & \tau_2 = q\tau \\
\cdots\cdots & \cdots\cdots & \cdots\cdots \\
\nu_j = \big(q^{j\delta} - q^{(j-1)\delta}\big)/\tau_j & \text{"} & \tau_j = q^{l_j}\tau \\
\cdots\cdots & \cdots\cdots & \cdots\cdots \\
\nu_e = \big(q^{e\delta} - q^{(e-1)\delta}\big)/\tau_e & \text{"} & \tau_e = q^{l_e}\tau
\end{array}$$

   where each l_j, $j = 1, \ldots, e$, is the least integer such that $q^{l_j} \geq j$,

2. the τ_j-periodic states $\mathbf{x}_{\tau_j} \in \mathbb{F}_q^d$ that build these cycles follow from the system of equations

$$(p_{\mathrm{irr},\mathbf{C}}(\mathbf{C}))^j \mathbf{x}_{\tau_j} = \mathbf{0} \;\wedge\; (p_{\mathrm{irr},\mathbf{C}}(\mathbf{C}))^{j-1} \mathbf{x}_{\tau_j} \neq \mathbf{0}, \quad j = 1, \ldots, e$$

   where $\mathbf{x}_{\tau_0} = \mathbf{0}$ and $(p_{\mathrm{irr},\mathbf{C}}(\mathbf{C}))^0 = \mathbf{I}$. □

The periodic decomposition can be written in a more convenient form by applying

Definition 4.4 (Cycle Sum)
The cycle sum Σ is the formal sum of cycle terms

$$\Sigma = \nu_1[\tau_1] \dot{+} \nu_2[\tau_2] \dot{+} \ldots \dot{+} \nu_\kappa[\tau_{N_\Sigma}], \tag{4.24}$$

in which the cycle term $\nu_i[\tau_i]$ denotes ν_i cycles of length τ_i and the binary operation $\dot{+}$ satisfies $\nu_i[\tau] \dot{+} \nu_j[\tau] = (\nu_i + \nu_j)[\tau]$. The number of different-length cycles in Σ is denoted by N_Σ. □

Using this definition the result of Theorem 4.5 can be rewritten as

$$\Sigma = 1[1] \dot{+} \frac{q^\delta - 1}{\tau_1}[\tau_1] \dot{+} \frac{q^{2\delta} - q^\delta}{\tau_2}[\tau_2] \dot{+} \ldots \dot{+} \frac{q^{e\delta} - q^{(e-1)\delta}}{\tau_e}[\tau_e], \tag{4.25}$$

in which τ_j, $j = 1, \ldots, e$, marks the periods of the polynomial $(p_{\mathrm{irr},\mathbf{C}}(\lambda))^j$ to be computed most simply via Theorem 2.5 by means of the period τ of its respective basis polynomial $p_{\mathrm{irr},\mathbf{C}}(\lambda)$.

Some examples for cycle sums with regard to powers of irreducible polynomials over $\mathbb{F}_2$ can be taken from Tabular 4.1.

4.2.1.2 Periodic States of an LMS Composed of Cyclic Companion Matrices

The knowledge of how the periodic states of an LMS with a dynamics matrix which is a cyclic companion matrix $\mathbf{C}_i$ of an elementary divisor polynomial can be calculated allows the generalization of the obtained result by benefiting from the linearity of LMS. Linearity grants the possibility of superposing the results for all $i = 1, \ldots, N_\mathrm{c}$ subspaces referring to the N_c elementary divisor polynomials of $\mathbf{A}_\mathrm{c}$.

Recall from equation (4.9) that the following $i = 1, \ldots, N_\mathrm{c}$ equations[11]

$$(\mathbf{I} - \mathbf{C}_i^t)\, \hat{\mathbf{x}}_{\mathrm{c},t}^{(i)} = \mathbf{0}$$

have to be fulfilled all at once in order to yield a t-periodic state $\hat{\mathbf{x}}_{\mathrm{c},t}^{\mathrm{T}} = \left(\hat{\mathbf{x}}_{\mathrm{c},t}^{(1)\mathrm{T}}, \ldots, \hat{\mathbf{x}}_{\mathrm{c},t}^{(N_\mathrm{c})\mathrm{T}}\right)$ in the overall N_c-fold composed cyclic part of the state space $\mathbb{F}_q^{d_1} \times \cdots \times \mathbb{F}_q^{d_{N_\mathrm{c}}} = \mathbb{F}_q^{n_c}$. Each of these $i = 1, \ldots, N_\mathrm{c}$ subspaces can be decomposed completely into cycles with an associated cycle sum according to equation (4.25).

The subsequent lemma provides a means for determining the period of a composed state.

[11] Beginning from here, the exact notation $\hat{\mathbf{x}}_{\mathrm{c},t_i}^{(i)}$ and $\mathbf{C}_i$ instead of, loosely, $\mathbf{x}$ and $\mathbf{C}$ becomes important again.

Polynomial	e	CycleSum $\nu_i[\tau_i]$
$(x+1)^e$	1	$1[1]$
	2	$2[1] \dot{+} 1[2]$
	3	$2[1] \dot{+} 1[2] \dot{+} 1[4]$
	4	$2[1] \dot{+} 1[2] \dot{+} 3[4]$
	5	$2[1] \dot{+} 1[2] \dot{+} 3[4] \dot{+} 2[8]$
$(x^2+x+1)^e$	1	$1[1] \dot{+} 1[3]$
	2	$1[1] \dot{+} 1[3] \dot{+} 2[6]$
	3	$1[1] \dot{+} 1[3] \dot{+} 2[6] \dot{+} 4[12]$
$(x^3+x+1)^e,\ (x^3+x^2+1)^e$	1	$1[1] \dot{+} 1[7]$
	2	$1[1] \dot{+} 1[7] \dot{+} 4[14]$
	3	$1[1] \dot{+} 1[7] \dot{+} 4[14] \dot{+} 16[28]$
$(x^4+x+1)^e,\ (x^4+x^3+1)^e$	1	$1[1] \dot{+} 1[15]$
	2	$1[1] \dot{+} 1[15] \dot{+} 8[30]$
	3	$1[1] \dot{+} 1[15] \dot{+} 8[30] \dot{+} 64[60]$
$(x^4+x^3+x^2+x+1)^e$	1	$1[1] \dot{+} 3[5]$
	2	$1[1] \dot{+} 3[5] \dot{+} 25[10]$
$(x^5+x^2+1)^e,\ \ldots$	1	$1[1] \dot{+} 1[31]$
	2	$1[1] \dot{+} 1[31] \dot{+} 16[62]$

Table 4.1: Cycle sums of irreducible polynomials over $\mathbb{F}_2$ risen to the power of e — taken from [Els59]

Lemma 4.6 (Period of Two Composed States)
Let $\mathbf{x}^{(1)}$ be a t_1-periodic substate in $\mathbb{F}_q^{d_1}$ and $\mathbf{x}^{(2)}$ be a t_2-periodic substate in $\mathbb{F}_q^{d_2}$ with respect to the linear modular systems induced by the matrices $\mathbf{A}_1$ and $\mathbf{A}_2$, respectively. Then the composed state $\mathbf{x}^{\mathrm{T}} = (\mathbf{x}^{(1)\mathrm{T}}, \mathbf{x}^{(2)\mathrm{T}})$ in $\mathbb{F}_q^{d_1+d_2} = \mathbb{F}_q^{d_1} \times \mathbb{F}_q^{d_2}$ with respect to the composed linear modular system induced by the matrix $\mathbf{A} := \mathrm{diag}(\mathbf{A}_1, \mathbf{A}_2)$ is periodic with period $t = \mathrm{lcm}(t_1, t_2)$, denoting the least common multiple of t_1 and t_2. □

Proof The period of $\mathbf{x}$ is the least integer t such that $\mathbf{x} = \mathbf{A}^t \mathbf{x}$. This implies $\mathbf{x}^{(1)} = \mathbf{A}_1^t \mathbf{x}^{(1)}$ and $\mathbf{x}^{(2)} = \mathbf{A}_2^t \mathbf{x}^{(2)}$, hence, t is a common multiple of t_1 and t_2, which are the periods of $\mathbf{x}^{(1)}$ and $\mathbf{x}^{(2)}$, respectively. Since t_1, t_2 and t are the least such integers, t has to be the least product of all factors of t_1 and t_2, that is the least common multiple of t_1 and t_2, $t = \mathrm{lcm}(t_1, t_2)$. □

An immediate generalization of this lemma owing to induction is the following

Theorem 4.6 (Period of Multiple Composed States)
Let $\mathcal{T} = \{\tau_1, \ldots, \tau_{N_c}\}$ denote a set of periods regarding the periodic substates $\hat{\mathbf{x}}_c^{(i)}$ in the $i = 1, \ldots, N_c$ linear modular subsystems $\hat{\mathbf{x}}_c^{(i)}(k+1) = \mathbf{A}_{c,i}\,\hat{\mathbf{x}}_c^{(i)}(k)$ with cyclic dynamics matrices $\mathbf{A}_{c,i}$. Let the overall LMS be composed according to $\mathbf{A}_c = \mathrm{diag}(\mathbf{A}_{c,1}, \ldots, \mathbf{A}_{c,N_c})$ such that $\hat{\mathbf{x}}_c(k+1) = \mathbf{A}_c\,\hat{\mathbf{x}}_c(k)$ with $\hat{\mathbf{x}}_c^{\mathrm{T}} = (\hat{\mathbf{x}}_c^{(1)\mathrm{T}}, \ldots, \hat{\mathbf{x}}_c^{(N_c)\mathrm{T}})$. Let $\mathcal{P} = \{\mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_{2^{N_c}}\}$ denote the power set of $\mathcal{T}$. Then the respective state space $\mathbb{F}_q^d$, $d = \dim(\hat{\mathbf{x}}_c)$, of the composed cyclic LMS is made up of states with periods $t_i = \mathrm{lcm}(\mathcal{P}_i)$, $i = 1, 2, \ldots, 2^{N_c}$. □

Remark 4.5
In general the periods t_i, $i = 1, 2, \ldots, 2^{N_c}$ of the states in the composed system are not distinct and can be summed up as described in Definition 4.4. □

Theorem 4.6 gives evidence about the periods, i. e. about the cycle lengths, that occur in an LMS. The next step is to deal with the numbers of theses cycles. For clearness, consider again an LMS the dynamics $\mathbf{A}_c$ of which consists of two cyclic companion matrices $\mathbf{C}_1$ and $\mathbf{C}_2$, one for each of the two elementary divisor polynomials,

$$\mathbf{A}_c = \begin{pmatrix} \mathbf{C}_1 & \mathbf{0} \\ \mathbf{0} & \mathbf{C}_2 \end{pmatrix}, \quad \mathbf{C}_1 \in \mathbb{F}_q^{d_1 \times d_1}, \mathbf{C}_2 \in \mathbb{F}_q^{d_2 \times d_2} \tag{4.26}$$

with corresponding cycle sums

$$\Sigma_1 = 1[1] \dot{+} \nu_1^{(1)}[\tau_1^{(1)}] \dot{+} \nu_2^{(1)}[\tau_2^{(1)}] \dot{+} \ldots \dot{+} \nu_{e_1}^{(1)}[\tau_{e_1}^{(1)}], \tag{4.27}$$

$$\Sigma_2 = 1[1] \dot{+} \nu_1^{(2)}[\tau_1^{(2)}] \dot{+} \nu_2^{(2)}[\tau_2^{(2)}] \dot{+} \ldots \dot{+} \nu_{e_2}^{(2)}[\tau_{e_2}^{(2)}]. \tag{4.28}$$

Hence q^{d_i}, the number of states in the respective subsystems $i = 1, 2$, is

$$q^{d_i} = 1 + \sum_{j=1}^{e_i} \nu_j^{(i)} \tau_j^{(i)},$$

which furthermore implies the number of states in the overall system

$$\begin{aligned} q^{d_1+d_2} &= \left(1 + \sum_{j=1}^{e_1} \nu_j^{(1)} \tau_j^{(1)}\right)\left(1 + \sum_{k=1}^{e_2} \nu_k^{(2)} \tau_k^{(2)}\right) = \\ &= 1 + \sum_{j=1}^{e_1} \underbrace{\nu_j^{(1)} \tau_j^{(1)}}_{a_j} + \sum_{k=1}^{e_2} \underbrace{\nu_k^{(2)} \tau_k^{(2)}}_{a_k} + \sum_{j=1}^{e_1} \sum_{k=1}^{e_2} \underbrace{\nu_j^{(1)} \nu_k^{(2)} \tau_j^{(1)} \tau_k^{(2)}}_{a_{jk}}. \end{aligned} \tag{4.29}$$

The addends 1, a_j, a_k, a_{jk} in the overall summation of state numbers in equation (4.29) are due to the following subsystem state combinations:

1: zero state referring to subsystem 1 combined with the zero state referring to subsystem 2

$\Rightarrow$ There results 1 state of period 1 in $\mathbb{F}_q^{d_1+d_2}$.

a_j: zero state referring to subsystem 2 combined with each $j = 1,\ldots,e_1$ of the $\nu_j^{(1)}$ states of period $\tau_j^{(1)}$ in subsystem 1

$\Rightarrow$ For each $j = 1,\ldots,e_1$ result $\nu_j^{(1)}\tau_j^{(1)}$ states of period $\tau_j^{(1)}$ in $\mathbb{F}_q^{d_1+d_2}$.

a_k: zero state referring to subsystem 1 combined with each $k = 1,\ldots,e_2$ of the $\nu_k^{(2)}$ states of period $\tau_k^{(2)}$ in subsystem 2

$\Rightarrow$ For each $k = 1,\ldots,e_2$ result $\nu_k^{(2)}\tau_k^{(2)}$ states of period $\tau_k^{(2)}$ in $\mathbb{F}_q^{d_1+d_2}$.

a_{jk}: combination of each $j = 1,\ldots,e_1$ of the $\nu_j^{(1)}$ states of period $\tau_j^{(1)}$ referring to subsystem 1 with each $k = 1,\ldots,e_2$ of the $\nu_k^{(2)}$ states of period $\tau_k^{(2)}$ referring to subsystem 2

$\Rightarrow$ For each pair $j = 1,\ldots,e_1$ and $k = 1,\ldots,e_2$ result $\nu_j^{(1)}\nu_k^{(2)}\tau_j^{(1)}\tau_k^{(2)}$ states of period $\operatorname{lcm}\left(\tau_j^{(1)},\tau_k^{(2)}\right)$ in $\mathbb{F}_q^{d_1+d_2}$.

As a consequence of the last item, the number

$$\nu_{jk} = \frac{\nu_j^{(1)}\nu_k^{(2)}\tau_j^{(1)}\tau_k^{(2)}}{\operatorname{lcm}\left(\tau_j^{(1)},\tau_k^{(2)}\right)} = \nu_j^{(1)}\nu_k^{(2)}\gcd\left(\tau_j^{(1)},\tau_k^{(2)}\right)$$

is the number of cycles consisting of states the period of which is $\tau_{jk} = \operatorname{lcm}\left(\tau_j^{(1)},\tau_k^{(2)}\right)$ and the expression $\gcd\left(\tau_j^{(1)},\tau_k^{(2)}\right)$ denotes the greatest common divisor of $\tau_j^{(1)}$ and $\tau_k^{(2)}$. Hence, a product of cycle terms may be defined.

Definition 4.5 (Product of Cycle Terms)
The product

$$\nu_1[\tau_1]\nu_2[\tau_2] = \nu_1\nu_2\gcd(\tau_1,\tau_2)[\operatorname{lcm}(\tau_1,\tau_2)] \tag{4.30}$$

is called the cycle term product. □

By means of the denotation of sum and product of cycle terms, according to Definition 4.4 and 4.5, the setting can be extended to the superposition of cycle sums. Reverting to the equations (4.27)

and (4.28) the product

$$\Sigma = \Sigma_1 \Sigma_2 =$$

$$= \left(1[1] \dot{+} \nu_1^{(1)}[\tau_1^{(1)}] \dot{+} \nu_2^{(1)}[\tau_2^{(1)}] \dot{+} \ldots \dot{+} \nu_{e_1}^{(1)}[\tau_{e_1}^{(1)}]\right) \left(1[1] \dot{+} \nu_1^{(2)}[\tau_1^{(2)}] \dot{+} \nu_2^{(2)}[\tau_2^{(2)}] \dot{+} \ldots \dot{+} \nu_{e_2}^{(2)}[\tau_{e_2}^{(2)}]\right)$$

$$= 1[1] \dot{+}_{j=1}^{e_1} \nu_j^{(1)}[\tau_j^{(1)}] \dot{+}_{k=1}^{e_2} \nu_k^{(2)}[\tau_k^{(2)}] \dot{+}_{j=1}^{e_1} \dot{+}_{k=1}^{e_2} \nu_j^{(1)} \nu_k^{(2)} \gcd\left(\tau_j^{(1)}, \tau_k^{(2)}\right) \left[\operatorname{lcm}\left(\tau_j^{(1)}, \tau_k^{(2)}\right)\right] \tag{4.31}$$

represents the cycle sum Σ of the composed LMS with respect to matrix $\mathbf{A}_\mathrm{c}$ in equation (4.26). The next theorem is an obvious generalization of this result.

Theorem 4.7 (Superposition of Cycle Sums)
The cycle sums $\Sigma_i, i = 1, \ldots, N_\mathrm{c}$ corresponding to N_c disjoint cyclic linear subspaces of an LMS superpose distributively in accordance with the product

$$\Sigma = \Sigma_1 \Sigma_2 \cdots \Sigma_{N_\mathrm{c}} . \qquad \square$$

Remark 4.6
In order to calculate the product in Theorem 4.7 in a simple fashion, the result from equation (4.31) can be extended to addends consisting of more than two factors by allowing for the definitions

$$\nu_{\mathbf{j}}^{(\mathbf{i})} := \nu_{j_1}^{(i_1)} \cdots \nu_{j_\eta}^{(i_\eta)} \gcd\left(\tau_{j_1}^{(i_1)}, \ldots, \tau_{j_\eta}^{(i_\eta)}\right), \tag{4.32}$$

$$\tau_{\mathbf{j}}^{(\mathbf{i})} := \operatorname{lcm}\left(\tau_{j_1}^{(i_1)}, \ldots, \tau_{j_\eta}^{(i_\eta)}\right) \tag{4.33}$$

with the abbreviations $\mathbf{i} = (i_1, \ldots, i_\eta)$, $\mathbf{j} = (j_1, \ldots, j_\eta)$ and $\eta \leq N_\mathrm{c}$ such that the cycle sum Σ consists of addends of the form $\nu_{\mathbf{j}}^{(\mathbf{i})}\left[\tau_{\mathbf{j}}^{(\mathbf{i})}\right]$ only. $\square$

All these results from above are combined in the main theorem of this section, Section 4.2.1.

Theorem 4.8 (Cycle Sum of an Autonomous LMS with Cyclic Dynamics)
Let the dynamics matrix $\mathbf{A}_\mathrm{c} = \operatorname{diag}(\mathbf{C}_1, \ldots, \mathbf{C}_{N_\mathrm{c}}) \in \mathbb{F}_q^{n_\mathrm{c} \times n_\mathrm{c}}$ of an autonomous LMS(q) be block-diagonally composed of $i = 1, \ldots, N_\mathrm{c}$ cyclic companion matrices $\mathbf{C}_i$, each with respect to one of the $i = 1, \ldots, N_\mathrm{c}$ elementary divisor polynomials $p_{\mathbf{C}_i} \in \mathbb{F}_q[\lambda]$ of degree d_i. Let each elementary divisor polynomial $p_{\mathbf{C}_i}$ be given in fully factored form $p_{\mathbf{C}_i} = (p_{\mathrm{irr},\mathbf{C}_i})^{e_i}$ subject to its irreducible factor polynomial $p_{\mathrm{irr},\mathbf{C}_i}$ of degree δ_i such that $d_i = e_i \delta_i$. Then

1. each elementary divisor polynomial $p_{\mathbf{C}_i}$ contributes the cycle sum

$$\Sigma_i = 1[1] \dot{+} \frac{q^{\delta_i} - 1}{\tau_1^{(i)}}\left[\tau_1^{(i)}\right] \dot{+} \frac{q^{2\delta_i} - q^{\delta_i}}{\tau_2^{(i)}}\left[\tau_2^{(i)}\right] \dot{+} \ldots \dot{+} \frac{q^{e_i\delta_i} - q^{(e_i-1)\delta_i}}{\tau_{e_i}^{(i)}}\left[\tau_{e_i}^{(i)}\right], \tag{4.34}$$

where $\tau_j^{(i)}$ denotes the period of the polynomial $(p_{\mathrm{irr},\mathbf{C}_i})^j$. For the entire autonomous LMS(q) the cycle sum Σ follows by superposition of all cycle sums Σ_i as per $\Sigma = \Sigma_1\Sigma_2\cdots\Sigma_{N_\mathrm{c}}$.

2. The $\tau_j^{(i)}$-periodic states $\hat{\mathbf{x}}_{\mathrm{c},j}^{(i)} \in \mathbb{F}_q^{d_i}$ that build the i-th cycle sum Σ_i are the solutions of the system of equations

$$(p_{\mathrm{irr},\mathbf{C}_i}(\mathbf{C}_i))^j\,\hat{\mathbf{x}}_{\mathrm{c},j}^{(i)} = \mathbf{0} \;\wedge\; (p_{\mathrm{irr},\mathbf{C}_i}(\mathbf{C}_i))^{j-1}\,\hat{\mathbf{x}}_{\mathrm{c},j}^{(i)} \neq \mathbf{0}\,, \quad j = 1,\ldots,e_i\,, \tag{4.35}$$

where $\hat{\mathbf{x}}_{\mathrm{c},0}^{(i)} = \mathbf{0}$ and $(p_{\mathrm{irr},\mathbf{C}_i}(\mathbf{C}_i))^0 = \mathbf{I}$. Abbreviate $\mathbf{i} = (i_1,\ldots,i_\eta)$, $\mathbf{j} = (j_1,\ldots,j_\eta)$ for which holds $i_1 \leq \ldots \leq i_\eta$, $j_1 \leq \ldots \leq j_\eta$ with $\eta \leq N_\mathrm{c}$. With a slight abuse of notation, let $\hat{\mathbf{x}}_{\mathrm{c},\mathbf{j}}^{(\mathbf{i})\,\mathrm{T}} = \left(\hat{\mathbf{x}}_{\mathrm{c},j_1}^{(i_1)\,\mathrm{T}},\ldots,\hat{\mathbf{x}}_{\mathrm{c},j_\eta}^{(i_\eta)\,\mathrm{T}}\right)$ denote a vector $\hat{\mathbf{x}}_{\mathrm{c},\mathbf{j}}^{(\mathbf{i})} \in \mathbb{F}_q^{n_\mathrm{c}}$ that results from the composition of η subvectors $\hat{\mathbf{x}}_{\mathrm{c},j_1}^{(i_1)},\ldots,\hat{\mathbf{x}}_{\mathrm{c},j_\eta}^{(i_\eta)}$, where non-specified vectors are zero vectors of corresponding dimension.[12] Then any state $\hat{\mathbf{x}}_{\mathrm{c},\mathbf{j}}^{(\mathbf{i})} \in \mathbb{F}_q^{n_\mathrm{c}}$ which is composable of arbitrary solutions $\hat{\mathbf{x}}_{\mathrm{c},j_1}^{(i_1)},\ldots,\hat{\mathbf{x}}_{\mathrm{c},j_\eta}^{(i_\eta)}$ of equation (4.35) for some fixed $\mathbf{i}$ and $\mathbf{j}$ has period $\tau_{\mathbf{j}}^{(\mathbf{i})} = \mathrm{lcm}\left(\tau_{j_1}^{(i_1)},\ldots,\tau_{j_\eta}^{(i_\eta)}\right)$. □

Remark 4.7
With respect to an elementary divisor polynomial $p_{\mathbf{C}_i}(\lambda)$ of degree d_i that is irreducible, obviously there are $\delta_i = d_i$ and $j = 1$, hence, from equation (4.34) it follows $\Sigma_i = 1[1] \dotplus (q^{d_i}-1)/\tau_1^{(i)}[\tau_1^{(i)}]$ and all non-zero substate vectors in $\mathbb{F}_q^{d_i}$ are $\tau_1^{(i)}$-periodic, that is all of them are solutions of equation (4.35). □

Recapitulating the past results, the determination of the cycle sum of an autonomous LMS(q) with dynamics matrix $\mathbf{A}$ takes the following steps:

i. Calculate the $i = 1,\ldots,N_\mathrm{c}$ periodic elementary divisor polynomials $p_{\mathbf{C}_i}(\lambda)$ of the dynamics matrix $\mathbf{A}$ by dint of deriving either

   - the factor polynomials $p_{\mathbf{C}_i}(\lambda)$ of the invariant polynomials using the Smith normal form $\mathbf{S}(\lambda)$ of $\mathbf{A}$,
   - or the rational canonical form $\mathbf{A}_\mathrm{rat}$ of $\mathbf{A}$. The polynomials with respect to each companion matrix in the rational canonical form are the elementary divisor polynomials.

   The nilpotent elementary divisor polynomials $p_{\mathbf{C}_i}(\lambda) = \lambda^{h_i}$, $i = 1,\ldots,N_\mathrm{n}$, do not contribute here due to Remark 4.2 — see Section 4.2.2 for the corresponding discussion.

[12] For an illustration, let $\mathbf{A}_\mathrm{c} = \mathrm{diag}(\mathbf{C}_1,\mathbf{C}_2,\mathbf{C}_3,\mathbf{C}_4)$ be a cyclic dynamics matrix in $\mathbb{F}_2^{9\times 9}$ with $p_{\mathbf{C}_1}(\lambda) = p_{\mathbf{C}_2}(\lambda) = \lambda^3+\lambda+1$, $p_{\mathbf{C}_3}(\lambda) = \lambda^2+\lambda+1$, $p_{\mathbf{C}_4}(\lambda) = 1$ irreducible defining polynomials of the companion matrices $\mathbf{C}_1 = \mathbf{C}_2$, $\mathbf{C}_3$, $\mathbf{C}_4$ such that the periods of the polynomials are $\tau_1^{(1)} = \tau_1^{(2)} = 7$, $\tau_1^{(3)} = 3$ and $\tau_1^{(4)} = 1$. Then the state vector $\hat{\mathbf{x}}_{\mathrm{c},\mathbf{j}}^{(\mathbf{i})\,\mathrm{T}} = (\hat{\mathbf{x}}_{\mathrm{c},j_1}^{(i_1)\,\mathrm{T}},\hat{\mathbf{x}}_{\mathrm{c},j_2}^{(i_2)\,\mathrm{T}})$ with $\mathbf{i} = (i_1,i_2) = (1,3)$ and $\mathbf{j} = (j_1,j_2) = (1,1)$ is a short cut denotation for any 21-periodic state vector $(\hat{\mathbf{x}}_{\mathrm{c},1}^{(1)\,\mathrm{T}},\mathbf{0}^\mathrm{T},\hat{\mathbf{x}}_{\mathrm{c},1}^{(3)\,\mathrm{T}},0)$ one of which is for example $((1,0,1),(0,0,0),(1,0),0)$.

ii. Determine the irreducible factor polynomials $p_{\mathrm{irr},\mathbf{C}_i}(\lambda)$ for each $i = 1,\ldots,N_\mathrm{c}$ periodic elementary divisor polynomial such that $p_{\mathbf{C}_i} = (p_{\mathrm{irr},\mathbf{C}_i})^{e_i}$.

iii. To each periodic polynomial $(p_{\mathrm{irr},\mathbf{C}_i})^j$, $i = 1,\ldots,N_\mathrm{c}$, $j = 1,\ldots,e_i$, assign the periods $\tau_j^{(i)}$.

iv. Compute the cycle sum Σ_i regarding each $i = 1,\ldots,N_\mathrm{c}$ periodic elementary divisor polynomial $p_{\mathbf{C}_i}(\lambda)$.

v. The cycle sum Σ of the entire autonomous LMS(q) then follows by distributively superposing all cycle sets Σ_i, $i = 1,\ldots,N_\mathrm{c}$.

vi. Simplify the cycle sum Σ by collecting cycle terms of the same period using Definition 4.4.

Remark 4.8 (Comment on the Complexity of the Method)
The first three steps within the above-stated method, the calculation of the Smith form of the dynamics matrix, the factorization of the invariant polynomials into elementary divisor polynomials, and the determination of its basis polynomial periods deserve some deeper examination of its computational complexity.[13,14]

For determining the Smith normal form of an n by n matrix Iliopoulus [Ili89] derived a polynomial complexity bound of $O(n^4)$, which was decreased down to $O(n^3)$ by Storjohann [Sto00].

The best known algorithm for factoring polynomials over finite fields is the algorithm of Berlekamp and von zur Gathen [Ber70, Gat87], for a review see [Sho90]. According to [Sho90], factoring an d-th degree polynomial over a finite field $\mathbb{F}_q$ entails a complexity less than $O(M(d) + q\,d^{2+\varepsilon})$, where $M(d)$ denotes the complexity of multiplying two d by d matrices — the least known upper bound for this is about $O(d^{2.4})$. The expression $O(d^\varepsilon)$ denotes a polynomial of finite degree in $\log d$. Consequently, for q fixed, factoring of polynomials over finite fields is of polynomial complexity.

The periods of the irreducible basis polynomials of the elementary divisor polynomials can be found in numerous tables, for example in [LN94]. For polynomial periods which are not tabulated, say due to the magnitude of its degree, there is a very severe obstacle: Though on the face of it, determining periods seems to be a simple task it turns out that it is as complex as determining the order of an element of a group or a discrete logarithm [BJT97]. This problem has been addressed by Meijer in [Mei96] and shown to be at least as complex as factoring integers. Unfortunately, at the moment, there is no polynomial time algorithm for factoring integers into primes.

Thus, an important consequence is that the presented method for solving the problem of determining the cycle set of an LMS allows to computationally benefit only in the case of rather small

[13] It is sufficient here to consider just the computational time complexity.

[14] Besides multiplication, step v comprises the calculation of greatest common divisors and least common multiples. For this task algorithms of polynomial complexity exist, for example the Euclidian Algorithm.

degrees of the basis polynomials; tabulars are available about up to degree $\delta = 100$. In this regard, it can be expected that the greater the number of invariant polynomials of the dynamics matrix and the more these polynomials factor into elementary divisor polynomials the less likely the latter practical bound may be exceeded. □

To the structural information expressed in the cycle sum corresponds the calculation of the respective periodic states of the autonomous LMS(q). Provided that all information after item v from above is at hand the following procedure will serve this purpose:

1. Calculate the $\tau_j^{(i)}$-periodic substates $\hat{\mathbf{x}}_{\mathrm{c},j}^{(i)}$ for all cycle sums Σ_i, $i = 1, \ldots, N_\mathrm{c}$ by making use of equation (4.35) in view of Remark 4.7.

2. For all periods $\tau_{\mathbf{j}}^{(\mathbf{i})}$ which occur in the unsimplified cycle sum Σ of the superposition (step v from above) determine the $\tau_{\mathbf{j}}^{(\mathbf{i})}$-periodic states $\hat{\mathbf{x}}_{\mathrm{c},\mathbf{j}}^{(\mathbf{i})} \in \mathbb{F}_q^{n_\mathrm{c}}$ by part 2 of Theorem 4.8.

3. In the overall state space $\mathbb{F}_q^n = \mathbb{F}_q^{n_\mathrm{c}+n_\mathrm{n}}$ the $\tau_{\mathbf{j}}^{(\mathbf{i})}$-periodic states $\hat{\mathbf{x}}_{\mathbf{j}}^{(\mathbf{i})} \in \mathbb{F}_q^n$ follow by composing $\hat{\mathbf{x}}_{\mathrm{c},\mathbf{j}}^{(\mathbf{i})}$ with the 1-periodic zero state of $\mathbb{F}_q^{n_\mathrm{n}}$ such that $\hat{\mathbf{x}}_{\mathbf{j}}^{(\mathbf{i})\,\mathrm{T}} = \left(\hat{\mathbf{x}}_{\mathrm{c},\mathbf{j}}^{(\mathbf{i})\,\mathrm{T}}, \mathbf{0}^\mathrm{T}\right)$ is $\tau_{\mathbf{j}}^{(\mathbf{i})}$-periodic.

4. The $\tau_{\mathbf{j}}^{(\mathbf{i})}$-periodic state vectors are given in original coordinates by $\mathbf{x}_{\mathbf{j}}^{(\mathbf{i})} = \hat{\mathbf{T}}^{-1}\hat{\mathbf{x}}_{\mathbf{j}}^{(\mathbf{i})} = \mathbf{\Pi}\mathbf{T}^{-1}\hat{\mathbf{x}}_{\mathbf{j}}^{(\mathbf{i})}$ as per equation (4.8).

4.2.1.3 Example: an LMS with Cyclic Dynamics Matrix

Consider a dynamics matrix $\mathbf{A} \in \mathbb{F}_2^{5\times 5}$ of an LMS(2) and its appendant Smith normal form $\mathbf{S}(\lambda) \in \mathbb{F}_2[\lambda]^{5\times 5}$ with $\mathbf{S}(\lambda) = \mathbf{U}(\lambda)(\lambda\mathbf{I} + \mathbf{A})\mathbf{V}(\lambda)$,

$$\mathbf{A} = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 \end{pmatrix}, \quad \mathbf{S}(\lambda) = \begin{pmatrix} (\lambda^2+\lambda+1)(\lambda+1)^2 & 0 & 0 & 0 & 0 \\ 0 & \lambda+1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

with unimodular matrices

$$\mathbf{U}(\lambda) = \begin{pmatrix} \lambda & \lambda^3+1 & \lambda^4+\lambda^3+\lambda+1 & 1 & \lambda^3+\lambda^2+\lambda+1 \\ 0 & 1 & \lambda & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix}$$

and

$$\mathbf{V}(\lambda) = \begin{pmatrix} \lambda^2+1 & \lambda^2+1 & \lambda+1 & 1 & 0 \\ \lambda & \lambda+1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ \lambda^3+\lambda^2 & \lambda^3+\lambda^2 & \lambda^2 & \lambda+1 & 1 \\ \lambda+1 & \lambda+1 & 1 & 0 & 0 \end{pmatrix}.$$

Here the only invariant polynomials $\neq 1$ of the matrix $\mathbf{A}$ are

$$c_1(\lambda) = (\lambda^2+\lambda+1)(\lambda+1)^2, \quad c_2(\lambda) = \lambda+1$$

as indicated by the Smith normal form. Thus, $\mathbf{A}$ has the elementary divisor polynomials

$$p_{\mathbf{C}_1}(\lambda) = \lambda^2+\lambda+1, \quad p_{\mathbf{C}_2}(\lambda) = (\lambda+1)^2, \quad p_{\mathbf{C}_3}(\lambda) = \lambda+1\,,$$

none of which are of the form λ^h for some integer h, hence, all elementary divisor polynomials are periodic in accordance with the assumption of a cyclic dynamics matrix $\mathbf{A}$. The corresponding base polynomial degrees are $\delta_1 = 2$, $\delta_2 = 1$ and $\delta_3 = 1$, respectively. Consequently, the corresponding rational canonical form $\mathbf{A}_{\text{rat}} = \mathbf{T}\mathbf{A}\mathbf{T}^{-1}$ together with its transformation matrix $\mathbf{T}$ reads[15]

$$\mathbf{A}_{\text{rat}} = \text{diag}(\mathbf{C}_1, \mathbf{C}_2, \mathbf{C}_3) = \begin{pmatrix} 0&1&0&0&0 \\ 1&1&0&0&0 \\ 0&0&0&1&0 \\ 0&0&1&0&0 \\ 0&0&0&0&1 \end{pmatrix}, \mathbf{T} = \begin{pmatrix} 1&0&0&1&1 \\ 0&0&0&1&1 \\ 1&0&1&0&1 \\ 0&0&1&1&1 \\ 0&1&1&0&1 \end{pmatrix}, \mathbf{T}^{-1} = \begin{pmatrix} 1&1&0&0&0 \\ 1&1&1&0&1 \\ 0&1&0&1&0 \\ 1&1&1&1&0 \\ 1&0&1&1&0 \end{pmatrix}.$$

In view of Definition 2.8 and Theorem 2.5 the corresponding periods are

$$\begin{aligned} p_{\text{irr},\mathbf{C}_1}(\lambda) = \lambda^2+\lambda+1 | \lambda^3+1 \quad &\Longrightarrow \quad \tau_1^{(1)}=3 \\ p_{\text{irr},\mathbf{C}_2}(\lambda) = \lambda+1 \quad &\Longrightarrow \quad \tau_1^{(2)}=1 \\ \big(p_{\text{irr},\mathbf{C}_2}(\lambda)\big)^2 = (\lambda+1)^2 = \lambda^2+1 \quad &\Longrightarrow \quad \tau_2^{(2)}=2 \\ p_{\text{irr},\mathbf{C}_3}(\lambda) = \lambda+1 \quad &\Longrightarrow \quad \tau_1^{(3)}=1 \end{aligned}$$

Theorem 4.8 yields

$$\Sigma_1 = 1[1] \dot{+} 1[3], \quad \Sigma_2 = 2[1] \dot{+} 1[2], \quad \Sigma_3 = 2[1]$$

and by superposition according to Theorem 4.7 it follows

$$\begin{aligned} \Sigma \;&=\; \Sigma_1\Sigma_2\Sigma_3 = \big(1[1] \dot{+} 1[3]\big)\big(2[1] \dot{+} 1[2]\big)\big(2[1]\big) = \big(2[1] \dot{+} 1[2] \dot{+} 2[3] \dot{+} 1[6]\big)\big(2[1]\big) = \\ &=\; 4[1] \dot{+} 2[2] \dot{+} 4[3] \dot{+} 2[6]\,. \end{aligned}$$

[15] A simple method for obtaining the transformation matrix $\mathbf{T}$ which transforms $\mathbf{A}$ into $\mathbf{A}_{\text{rat}}$ employing Maple® is presented in Chapter B of the Appendix.

Alternatively, Σ can be calculated in view of Remark 4.6 via

$$\begin{aligned}\Sigma &= \Sigma_1\Sigma_2\Sigma_3 = \big(1[1]\dot{+}1[3]\big)\big(2[1]\dot{+}1[2]\big)\big(2[1]\big)\\ &= 1\cdot 2\cdot 2\,\mathrm{gdc}(1,1,1)\,[\mathrm{lcm}(1,1,1)]\dot{+}1\cdot 1\cdot 2\,\mathrm{gdc}(1,2,1)\,[\mathrm{lcm}(1,2,1)]\dot{+}\\ &\quad 1\cdot 2\cdot 2\,\mathrm{gdc}(3,1,1)\,[\mathrm{lcm}(3,1,1)]\dot{+}1\cdot 1\cdot 2\,\mathrm{gdc}(3,2,1)\,[\mathrm{lcm}(3,2,1)]\\ &= 4[1]\dot{+}2[2]\dot{+}4[3]\dot{+}2[6]\,.\end{aligned}$$

Therefore, the LMS(2) represented by the dynamics matrix $\mathbf{A}$ comprises 4 cycles of length 1, 2 cycles of length 2, 4 cycles of length 3 and 2 cycles of length 6.

The respective periodic states $\hat{\mathbf{x}}_{\mathrm{c},1}^{(1)}$ and $\hat{\mathbf{x}}_{\mathrm{c},1}^{(3)}$ for the irreducible elementary divisor polynomials $p_{\mathbf{C}_1}(\lambda)$ and $p_{\mathbf{C}_3}(\lambda)$ immediately result from Remark 4.7, that is

$$\hat{\mathbf{x}}_{\mathrm{c},1}^{(1)} \in \left\{\begin{pmatrix}1\\0\end{pmatrix},\begin{pmatrix}0\\1\end{pmatrix},\begin{pmatrix}1\\1\end{pmatrix}\right\}, \quad \hat{\mathbf{x}}_{\mathrm{c},1}^{(3)} \in \{(1)\}$$

whereas for the reducible elementary divisor polynomial $p_{\mathbf{C}_2}(\lambda)$ equation (4.35) yields

$$\begin{aligned}&(p_{\mathrm{irr},\mathbf{C}_2}(\mathbf{C}_2))^1\,\hat{\mathbf{x}}_{\mathrm{c},1}^{(2)} = \mathbf{0} \;\wedge\; (p_{\mathrm{irr},\mathbf{C}_2}(\mathbf{C}_2))^0\,\hat{\mathbf{x}}_{\mathrm{c},1}^{(2)} \neq \mathbf{0}\\ \Longleftrightarrow\quad &(\mathbf{C}_2+\mathbf{I})\,\hat{\mathbf{x}}_{\mathrm{c},1}^{(2)} = \mathbf{0} \quad\wedge\quad \mathbf{I}\,\hat{\mathbf{x}}_{\mathrm{c},1}^{(2)} \neq \mathbf{0}\\ \Longleftrightarrow\quad &\begin{pmatrix}1&1\\1&1\end{pmatrix}\hat{\mathbf{x}}_{\mathrm{c},1}^{(2)} = \mathbf{0} \quad\wedge\quad \hat{\mathbf{x}}_{\mathrm{c},1}^{(2)} \neq \mathbf{0} \quad\Longrightarrow\; \hat{\mathbf{x}}_{\mathrm{c},1}^{(2)} \in \left\{\begin{pmatrix}1\\1\end{pmatrix}\right\}\\ &(p_{\mathrm{irr},\mathbf{C}_2}(\mathbf{C}_2))^2\,\hat{\mathbf{x}}_{\mathrm{c},2}^{(2)} = \mathbf{0} \;\wedge\; (p_{\mathrm{irr},\mathbf{C}_2}(\mathbf{C}_2))^1\,\hat{\mathbf{x}}_{\mathrm{c},2}^{(2)} \neq \mathbf{0}\\ \Longleftrightarrow\quad &(\mathbf{C}_2+\mathbf{I})^2\,\hat{\mathbf{x}}_{\mathrm{c},2}^{(2)} = \mathbf{0} \quad\wedge\quad (\mathbf{C}_2+\mathbf{I})\,\hat{\mathbf{x}}_{\mathrm{c},2}^{(2)} \neq \mathbf{0}\\ \Longleftrightarrow\quad &\begin{pmatrix}0&0\\0&0\end{pmatrix}\hat{\mathbf{x}}_{\mathrm{c},2}^{(2)} = \mathbf{0} \quad\wedge\quad \begin{pmatrix}1&1\\1&1\end{pmatrix}\hat{\mathbf{x}}_{\mathrm{c},2}^{(2)} \neq \mathbf{0} \quad\Longrightarrow\; \hat{\mathbf{x}}_{\mathrm{c},2}^{(2)} \in \left\{\begin{pmatrix}1\\0\end{pmatrix},\begin{pmatrix}0\\1\end{pmatrix}\right\}\end{aligned}$$

Now the overall periods $\tau_{\mathbf{j}}^{(\mathbf{i})}$ of the associated states $\hat{\mathbf{x}}_{\mathrm{c},\mathbf{j}}^{(\mathbf{i})}$ can be determined from all possible compositions which are vectors in the transformed coordinates (Figure 4.2). For instance, take the vector

$$\hat{\mathbf{x}}_1^{\mathrm{T}} = (0,0,1,0,0)$$

which was determined to be 2-periodic. Its counterpart in the original coordinates is given by the inverse transformation $\mathbf{x}_1 = \mathbf{T}^{-1}\hat{\mathbf{x}}_1$ with

$$\mathbf{x}_1^{\mathrm{T}} = (0,1,0,1,1)$$

The simple calculation

$$\mathbf{A}^2\mathbf{x}_1 = \mathbf{x}_1$$

$\tau = 1$	$\tau = 2$	$\tau = 3$	$\tau = 6$
$\hat{\mathbf{x}} \in \left\{ \begin{pmatrix} 0\\0\\0\\0\\0 \end{pmatrix} \right\}$	$\hat{\mathbf{x}}^{(2)}_{\mathrm{c},(2)} \in \left\{ \begin{pmatrix} 0\\0\\1\\0\\0 \end{pmatrix}, \begin{pmatrix} 0\\0\\0\\1\\0 \end{pmatrix} \right\}$	$\hat{\mathbf{x}}^{(1)}_{\mathrm{c},(1)} \in \left\{ \begin{pmatrix} 1\\0\\0\\0\\0 \end{pmatrix}, \begin{pmatrix} 0\\1\\0\\0\\0 \end{pmatrix}, \begin{pmatrix} 1\\1\\0\\0\\0 \end{pmatrix} \right\}$	$\hat{\mathbf{x}}^{(1,2)}_{\mathrm{c},(1,2)} \in \left\{ \begin{pmatrix} 1\\0\\1\\0\\0 \end{pmatrix}, \begin{pmatrix} 0\\1\\1\\0\\0 \end{pmatrix}, \begin{pmatrix} 1\\1\\1\\0\\0 \end{pmatrix}, \right.$
$\hat{\mathbf{x}}^{(2)}_{\mathrm{c},(1)} \in \left\{ \begin{pmatrix} 0\\0\\1\\1\\0 \end{pmatrix} \right\}$	$\hat{\mathbf{x}}^{(2,3)}_{\mathrm{c},(2,1)} \in \left\{ \begin{pmatrix} 0\\0\\1\\0\\1 \end{pmatrix}, \begin{pmatrix} 0\\0\\0\\1\\1 \end{pmatrix} \right\}$	$\hat{\mathbf{x}}^{(1,2)}_{\mathrm{c},(1,1)} \in \left\{ \begin{pmatrix} 1\\0\\1\\1\\0 \end{pmatrix}, \begin{pmatrix} 0\\1\\1\\1\\0 \end{pmatrix}, \begin{pmatrix} 1\\1\\1\\1\\0 \end{pmatrix} \right\}$	$\left. \begin{pmatrix} 1\\0\\0\\1\\0 \end{pmatrix}, \begin{pmatrix} 0\\1\\0\\1\\0 \end{pmatrix}, \begin{pmatrix} 1\\1\\0\\1\\0 \end{pmatrix} \right\}$
$\hat{\mathbf{x}}^{(3)}_{\mathrm{c},(1)} \in \left\{ \begin{pmatrix} 0\\0\\0\\0\\1 \end{pmatrix} \right\}$		$\hat{\mathbf{x}}^{(1,3)}_{\mathrm{c},(1,1)} \in \left\{ \begin{pmatrix} 1\\0\\0\\0\\1 \end{pmatrix}, \begin{pmatrix} 0\\1\\0\\0\\1 \end{pmatrix}, \begin{pmatrix} 1\\1\\0\\0\\1 \end{pmatrix} \right\}$	$\hat{\mathbf{x}}^{(1,2,3)}_{\mathrm{c},(1,2,1)} \in \left\{ \begin{pmatrix} 1\\0\\1\\0\\1 \end{pmatrix}, \begin{pmatrix} 0\\1\\1\\0\\1 \end{pmatrix}, \begin{pmatrix} 1\\1\\1\\0\\1 \end{pmatrix}, \right.$
$\hat{\mathbf{x}}^{(2,3)}_{\mathrm{c},(1,1)} \in \left\{ \begin{pmatrix} 0\\0\\1\\1\\1 \end{pmatrix} \right\}$		$\hat{\mathbf{x}}^{(1,2,3)}_{\mathrm{c},(1,1,1)} \in \left\{ \begin{pmatrix} 1\\0\\1\\1\\1 \end{pmatrix}, \begin{pmatrix} 0\\1\\1\\1\\1 \end{pmatrix}, \begin{pmatrix} 1\\1\\1\\1\\1 \end{pmatrix} \right\}$	$\left. \begin{pmatrix} 1\\0\\0\\1\\1 \end{pmatrix}, \begin{pmatrix} 0\\1\\0\\1\\1 \end{pmatrix}, \begin{pmatrix} 1\\1\\0\\1\\1 \end{pmatrix} \right\}$

Figure 4.2: Periodic states in transformed coordinates referring to Example 4.2.1.3

verifies that $\mathbf{x}_1$ is 2-periodic. Furthermore, deriving

$$\mathbf{A}\mathbf{x}_1 = \mathbf{x}_2, \quad \mathbf{x}_2^{\mathrm{T}} = (0,0,1,1,1)$$

is in accordance with the result of

$$\mathbf{x}_2 = \mathbf{T}^{-1}\hat{\mathbf{x}}_2, \quad \hat{\mathbf{x}}_2^{\mathrm{T}} = (0,0,0,1,0),$$

in which $\mathbf{x}_2$ is the remaining 2-periodic state vector $\hat{\mathbf{x}}_2$ expressed in original coordinates.

The entire state graph with states represented in transformed coordinates is depicted in Figure 4.3.

4.2.2 Nilpotent Dynamics

This section presents an investigation of the nilpotent part $\mathbf{A}_{\mathrm{n}}$ within the rational canonical form $\hat{\mathbf{A}}_{\mathrm{rat}}$ of the dynamics matrix $\mathbf{A}$ in the decomposition according to equation (4.5). The focus will lie again on the interconnection structure of the states, this time concerning the substates $\hat{\mathbf{x}}_{\mathrm{n}} \in \mathbb{F}_q^{n_{\mathrm{n}}}$. With this regard reconsider equation (4.7)

$$\hat{\mathbf{x}}_{\mathrm{n}}(k+1) = \mathbf{A}_{\mathrm{n}}\hat{\mathbf{x}}_{\mathrm{n}}(k), \quad k \in \mathbb{N}_0, \quad \mathbf{A}_{\mathrm{n}} = \mathrm{diag}(\mathbf{C}_1, \ldots, \mathbf{C}_{N_{\mathrm{n}}}) \tag{4.36}$$

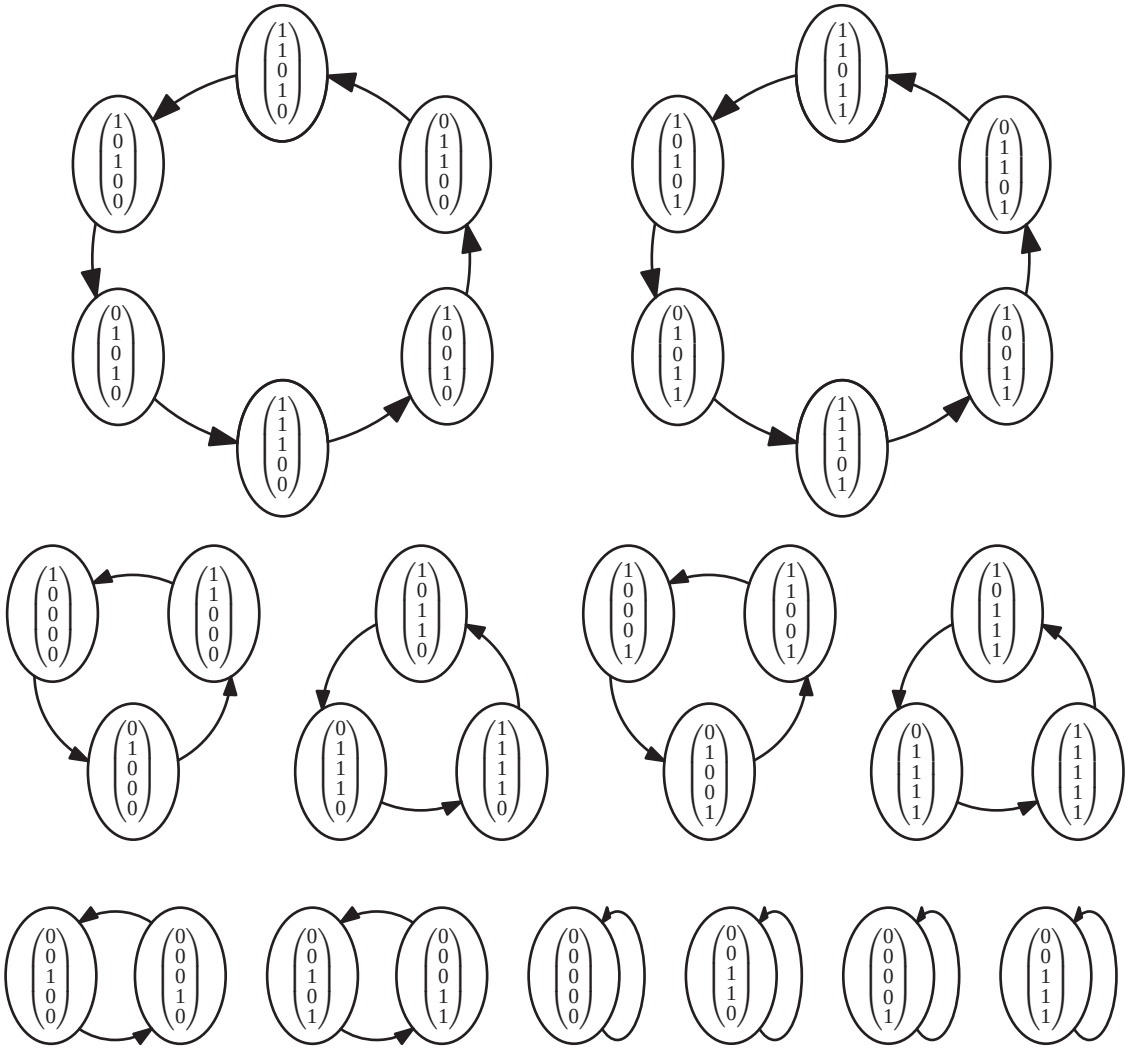


Figure 4.3: State graph of the LMS discussed in Example 4.2.1.3; states given in transformed coordinates

where $\hat{\mathbf{x}}_{\mathrm{n}}(k) \in \mathbb{F}_q^{n_{\mathrm{n}}}$ and all $i = 1, \ldots, N_{\mathrm{n}}$ matrices $\mathbf{C}_i$ are nilpotent companion matrices with respect to the elementary divisor polynomials $p_{\mathbf{C}_i}(\lambda) = \lambda^{h_i}$, $h_i \in \mathbb{N}$, implying $\mathbf{C}_i^{h_i} \equiv \mathbf{0}$. Note that with Remark 4.1 any $h \times h$ nilpotent companion matrix $\mathbf{C}$ uniquely reads

$$\mathbf{C} = \begin{pmatrix} 0 & 0 & \cdots & 0 & 0 \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix}, \quad \dim(\mathbf{C}) = h\,. \tag{4.37}$$

Collecting all nilpotent companion matrices in $\mathbf{A}_{\mathrm{n}}$ yields $n_{\mathrm{n}} = \sum_{i=1}^{N_{\mathrm{n}}} h_i$.

Definition 4.6 (Levels of a State Graph)
Let an LMS be given by a nilpotent dynamics matrix $\mathbf{A}_\mathrm{n}$. Then the associated states which reach the zero state $\hat{\mathbf{x}}_\mathrm{n} = \mathbf{0}$ in l steps are called states of level l (in the state graph). The set of states in level l is termed level l. □

4.2.2.1 State Graph of an LMS with a Nilpotent Companion Matrix as Dynamics Matrix

In the special case when the dynamics matrix of an LMS is a nilpotent companion matrix the following applies.

Theorem 4.9 (State Graph of an LMS with Minimal Polynomial λ^h)
In an LMS the dynamics matrix of which is a nilpotent companion matrix $\mathbf{C} \in \mathbb{F}_q^{h\times h}$ the following statements hold:

- the state graph consists of h levels,
- the level $l = 1,2\ldots,h$ comprises $(q-1)q^{l-1}$ states, $q^0 := 1$,
- any non-zero, non-terminal state has q confluent states,
- the zero state has $q-1$ confluent states (in level 1). □

Proof Any state $\mathbf{x}_h^\mathrm{T} = (x_1, x_2, \ldots, x_h) \in \mathbb{F}_q^h$ with $x_1 \in \mathbb{F}_q - \{0\}$ and arbitrary $x_{i\neq 1} \in \mathbb{F}_q$ has no predecessors since $\mathbf{x}_h \notin \mathrm{Im}(\mathbf{C})$. The number of states in this partition is $(q-1)q^{h-1}$. The mapping of $\mathbf{x}_h \in \mathbb{F}_q$ by means of matrix $\mathbf{C}$ results in $\mathbf{x}_{h-1}^\mathrm{T} = (0, x_1, x_2, \ldots, x_{h-1})$. Thus, the next partition is made up of all such states $\mathbf{x}_{h-1}$. These all have q confluent states, which is due to the number of values corresponding to the "omitted" x_h in the last shift. The number of states in this partition is $(q-1)q^{h-2}$. Proceeding in the same manner, finally, leeds to $\mathbf{x}_1^\mathrm{T} = (0,\ldots,0,x_1)$ which with $x_1 \in \mathbb{F}_q - \{0\}$ are $q-1$ states in this partition all of which again have q confluent states and terminate in the remaining zero state in a last step. Counting the states of all partitions yields

$$(q-1)q^{h-1} + (q-1)q^{h-2} + \cdots + (q-1) + 1 = 1 + (q-1)\sum_{i=0}^{h-1} q^i = 1 + (q-1)\frac{q^h - 1}{q-1} = q^h,$$

which is the total number of states in $\mathbb{F}_q^h$. As a consequence, all these states form h levels in the state graph. □

Example 4.2
For an LMS with nilpotent dynamics $\mathbf{A} = \mathbf{A}_\mathrm{n} = \mathbf{C} \in \mathbb{F}_2^{3\times 3}$ with

$$\mathbf{C} = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

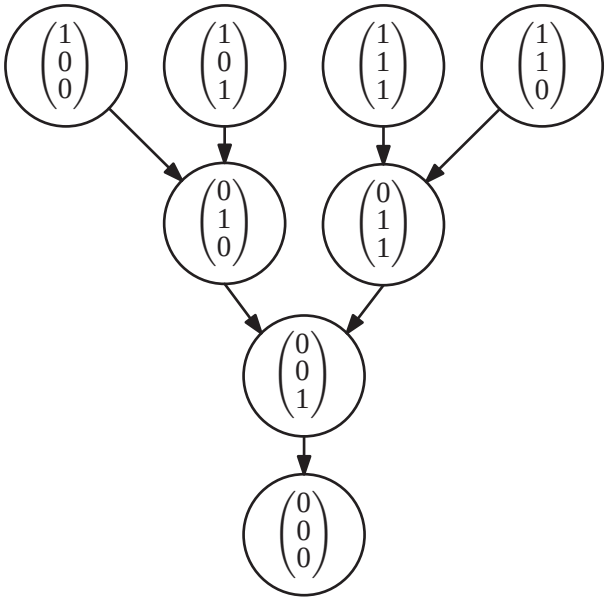


Figure 4.4: State graph of a 3-rd order LMS with nilpotent companion matrix as dynamics (Example 4.2)

Theorem 4.9 implies a graph as shown in Figure 4.4. □

4.2.2.2 State Graph of an LMS with Arbitrary Nilpotent Dynamics Matrix

The structural examination of the state graph of an LMS with arbitrary nilpotent dynamics matrix $\mathbf{A}_\mathrm{n}$ entails more effort. Let a companion matrix (of dimension h_i) referring to an elementary divisor polynomial λ^{h_i} be denoted by $\mathbf{C}_{\lambda^{h_i}}$, for simplicity, and consider the ordered recollection

$$\mathrm{diag}(\underbrace{\mathbf{C}_\lambda,\ldots,\mathbf{C}_\lambda}_{\mu_1 \text{ blocks}},\underbrace{\mathbf{C}_{\lambda^2},\ldots,\mathbf{C}_{\lambda^2}}_{\mu_2 \text{ blocks}},\ldots,\underbrace{\mathbf{C}_{\lambda^{h_\mathrm{max}}},\ldots,\mathbf{C}_{\lambda^{h_\mathrm{max}}}}_{\mu_{h_\mathrm{max}} \text{ blocks}}),\quad \sum_{j=1}^{h_\mathrm{max}}\mu_j = N_\mathrm{n}\,, \tag{4.38}$$

of the diagonal blocks of matrix $\mathbf{A}_\mathrm{n}$, which is a recollection by ascending block dimensions h_i. In the sequel, since this form can be obtained from $\mathbf{A}_\mathrm{n}$ by simple permutations[16], without loss of generality $\mathbf{A}_\mathrm{n}$ will be assumed in the form (4.38).

With (4.37) an immediate result is the following.

Theorem 4.10 (Termination into the Zero State)
Any state $\hat{\mathbf{x}}_\mathrm{n} \in \mathbb{F}_q^{n_\mathrm{n}}$ of an LMS with nilpotent dynamics matrix $\mathbf{A}_\mathrm{n} \in \mathbb{F}_q^{n_\mathrm{n}\times n_\mathrm{n}}$, which consists of $i = 1,\ldots,N_\mathrm{n}$ nilpotent companion matrices $\mathbf{C}_i$ of dimension h_i, terminates in at most $h_\mathrm{max} = \max(h_1,\ldots,h_{N_\mathrm{n}})$ steps into the zero vector. □

[16] See Chapter A of the Appendix for the details.

Proof The mapping of an arbitrary vector by virtue of a nilpotent companion matrix $\mathbf{C}_i$ shifts the vector entries one digit down and sets the first entry to zero. Hence, after h_i such mappings with $\mathbf{C}_i$ the zero vector is obtained. In the overall system with respect to $\mathbf{A}_\mathrm{n}$, consequently, $\max(h_1,\ldots,h_{N_\mathrm{n}})$ mappings of $\hat{\mathbf{x}}_\mathrm{n}$ by means of $\mathbf{A}_\mathrm{n}$ yield the zero vector for the first time which then persists for any further mappings using $\mathbf{A}_\mathrm{n}$. □

Thus, the subsequent consequence of Theorem 4.10 becomes obvious.

Corollary 4.2 (Number of Levels)
The state graph of an LMS with nilpotent dynamics matrix $\mathbf{A}_\mathrm{n}$ consisting of $i = 1,\ldots,N_\mathrm{n}$ nilpotent companion matrices $\mathbf{C}_i$ of dimension h_i consists of $h_\mathrm{max} = \max(h_1,\ldots,h_{N_\mathrm{n}})$ levels. □

In contrast to cyclic dynamics matrices, which in its rational canonical form comprise specific coefficients of its elementary divisor polynomials still (rightmost columns in the respective companion matrices), nilpotent dynamics matrices depend on the numbers h_i only. For this reason, it is worthwhile to interpret equation (4.7) as a linear system of equations for $\hat{\mathbf{x}}_\mathrm{n}(k)$. To this end, consider the κ-fold mapping from $\hat{\mathbf{x}}_\mathrm{n}(k)$ to $\hat{\mathbf{x}}_\mathrm{n}(k+\kappa)$ by means of $\mathbf{A}_\mathrm{n}$, amounting to the linear system of equations

$$\mathbf{A}_\mathrm{n}^\kappa \hat{\mathbf{x}}_\mathrm{n}(k) = \hat{\mathbf{x}}_\mathrm{n}(k+\kappa)\,. \tag{4.39}$$

Similar to (4.9), equation (4.39) comprises all information about the interconnection structure of the states.

Since the matrix $\mathbf{A}_\mathrm{n}$ is singular a more general concept of an inverse is requested for solving (4.39). So-called singular inverses (g-Inverses) grant this facility. Taking this into account, a solution of equation (4.39) exists iff $\hat{\mathbf{x}}_\mathrm{n}(k+\kappa) \in \mathrm{Im}(\mathbf{A}_\mathrm{n}^\kappa)$, which, referring to Chapter D of the Appendix, is equivalent to

$$(\mathbf{A}_\mathrm{n}^\kappa (\mathbf{A}_\mathrm{n}^\mathrm{T})^\kappa - \mathbf{I})\,\hat{\mathbf{x}}_\mathrm{n}(k+\kappa) = \mathbf{0}\,. \tag{4.40}$$

Given existence, a general solution of equation (4.39) is

$$\hat{\mathbf{x}}_\mathrm{n}(k) = (\mathbf{A}_\mathrm{n}^\mathrm{T})^\kappa \hat{\mathbf{x}}_\mathrm{n}(k+\kappa) + \left(\mathbf{I} - (\mathbf{A}_\mathrm{n}^\mathrm{T})^\kappa \mathbf{A}_\mathrm{n}^\kappa\right)\mathbf{z}, \quad \forall \mathbf{z} \in \mathbb{F}_q^{n_\mathrm{n}} \tag{4.41}$$

where the first addend marks the particular solution and the second addend the homogeneous solution, respectively.

Under the assumption that the state $\hat{\mathbf{x}}_\mathrm{n}(k+\kappa)$ meets the solvability condition (4.40) the number of different solutions is expressed by

$$\left(\mathbf{I} - (\mathbf{A}_\mathrm{n}^\mathrm{T})^\kappa \mathbf{A}_\mathrm{n}^\kappa\right)\mathbf{z}\,.$$

The matrix $(\mathbf{A}_\mathrm{n}^\mathrm{T})^\kappa \mathbf{A}_\mathrm{n}^\kappa$ is a diagonal matrix and its zero rows incur components from $\mathbf{z}$, which is an arbitrary vector in $\mathbb{F}_q^{n_\mathrm{n}}$. Thus, counting these zero rows allows to calculate the number of states that reach an arbitrary given state, if possible, in at most κ steps.

In light of the fact that $\mathbf{A}_\mathrm{n}$ is a block-diagonal matrix and that for nilpotent companion matrices

$$(\mathbf{C}^\mathrm{T})^\kappa \mathbf{C}^\kappa = \begin{cases} \mathbf{0}_h, & 1 \leq h \leq \kappa \\ \mathrm{diag}(\mathbf{I}_{h-\kappa}, \mathbf{0}_\kappa), & \kappa < h \leq h_\mathrm{max} \end{cases} \tag{4.42}$$

the number of zero rows $r(\kappa)$ in matrix $(\mathbf{A}_\mathrm{n}^\mathrm{T})^\kappa \mathbf{A}_\mathrm{n}^\kappa$ is

$$r(\kappa) = \sum_{j=1}^{\kappa} \mu_j \, j + \sum_{j=\kappa+1}^{h_\mathrm{max}} \mu_j \, \kappa, \quad \kappa = 1, \ldots, h_\mathrm{max} \tag{4.43}$$

in which the denotation introduced in equation (4.38) is applied. Finally, simple combinatorics imply the following theorem.

Theorem 4.11 (Number of States Reaching an Arbitrary State)
Let $\mathbf{A}_\mathrm{n}$ be a nilpotent dynamics matrix of an LMS in recollected form as per equation (4.38) and let $\hat{\mathbf{x}}_\mathrm{n} \in \mathbb{F}_q^{n_\mathrm{n}}$ be an arbitrary state with $(\mathbf{A}_\mathrm{n}^\kappa (\mathbf{A}_\mathrm{n}^\mathrm{T})^\kappa - \mathbf{I})\, \hat{\mathbf{x}}_\mathrm{n} = \mathbf{0}$ and $\kappa = 1, \ldots, h_\mathrm{max}$. Then the number of states which reach $\hat{\mathbf{x}}_\mathrm{n}$ in κ steps is $q^{r(\kappa)}$, $r(\kappa) = \sum_{j=1}^{\kappa} \mu_j \, j + \sum_{j=\kappa+1}^{h_\mathrm{max}} \mu_j \, \kappa$. □

Remark 4.9
The condition $(\mathbf{A}_\mathrm{n}^\kappa (\mathbf{A}_\mathrm{n}^\mathrm{T})^\kappa - \mathbf{I})\, \hat{\mathbf{x}}_\mathrm{n} = \mathbf{0}$ in Theorem 4.11 is fulfilled trivially if $\hat{\mathbf{x}}_\mathrm{n} = \mathbf{0}$. Consequently, the zero state $\hat{\mathbf{x}}_\mathrm{n} = \mathbf{0}$ is reachable from arbitrary states. □

On this account the number of states in level l can be calculated.

Corollary 4.3 (Number of States in each Level)
Let $\mathbf{A}_\mathrm{n}$ be a nilpotent dynamics matrix of an LMS in recollected form as per equation (4.38). Then the number of states in level l is given by

$$\eta(l) = q^{r(l)} - q^{r(l-1)}, \qquad r(l) = \sum_{j=1}^{l} \mu_j \, j + \sum_{j=l+1}^{h_\mathrm{max}} \mu_j \, l, \qquad r(0) := 0\,. \tag{□}$$

Theorem 4.11 and Corollary 4.3 are sufficient to construct the state graph of a nilpotent LMS. If the task is to determine particular states then equation (4.41) serves this purpose.

4.2.2.3 Example: an LMS with Nilpotent Dynamics Matrix

For simplicity the following nilpotent dynamics matrix $\mathbf{A}_\mathrm{n} \in \mathbb{F}_2^{7\times 7}$ of an LMS shall be given in the recollected rational canonical form according to equation (4.38), that is

$$\mathbf{A}_\mathrm{n} = \mathrm{diag}(\mathbf{C}_{\lambda^2}, \mathbf{C}_{\lambda^2}, \mathbf{C}_{\lambda^3})$$

with $N_\mathrm{n} = 3$ nilpotent companion matrices. From a comparison with equation (4.38) it follows that $\mu_1 = 0$, $\mu_2 = 2$, $\mu_3 = 1$ and $h_\mathrm{max} = 3$, where the latter with Definition 4.6 indicates a state graph with 3 levels. Corollary 4.3 yields

$$r(0) := 0\,, \qquad r(1) = \sum_{j=1}^{1} \mu_j\, j + \sum_{j=2}^{3} \mu_j = 3\,,$$
$$r(2) = \sum_{j=1}^{2} \mu_j\, j + \sum_{j=3}^{3} \mu_j\, 2 = 6\,, \qquad r(3) = \sum_{j=1}^{3} \mu_j\, j = 7$$

by means of which follow the number of states per level

$$\begin{aligned} \eta(1) &= 2^{r(1)} - 2^{r(0)} = 7\,, \\ \eta(2) &= 2^{r(2)} - 2^{r(1)} = 56\,, \\ \eta(3) &= 2^{r(3)} - 2^{r(2)} = 64\,. \end{aligned}$$

Hence, by Theorem 4.11 the number of states that reach any given state

- in 1 step is either 0 or $2^{r(1)} = 8$,
- in 2 steps is either 0 or $2^{r(2)} = 64$,
- in 3 steps is either 0 or $2^{r(3)} = 128$.

In this regard, 0 means that this given state cannot be reached because the solvability condition in equation (4.40) is not met. Figure 4.5 depicts the resulting state graph.

4.2.3 Arbitrary Dynamics

The general statement follows by superposition of the cyclic and nilpotent subsystem. As has been shown in equation (4.5) a similarity transformation can be used to decompose the dynamics matrix $\mathbf{A}$ into $\hat{\mathbf{A}}_\mathrm{rat} = \mathrm{diag}(\mathbf{A}_\mathrm{c}, \mathbf{A}_\mathrm{n})$ which comprises a cyclic matrix $\mathbf{A}_\mathrm{c}$ and a nilpotent matrix $\mathbf{A}_\mathrm{n}$, provided that either of both parts, cyclic and nilpotent, exists. Collecting equations (4.6) and (4.7) together in one equation and defining $\hat{\mathbf{x}}^\mathrm{T} = (\hat{\mathbf{x}}_\mathrm{c}^\mathrm{T}, \hat{\mathbf{x}}_\mathrm{n}^\mathrm{T}) \in \mathbb{F}_q^{n_\mathrm{c}+n_\mathrm{n}} = \mathbb{F}_q^n$ the t-fold mapping of $\hat{\mathbf{x}}$ with $\hat{\mathbf{A}}_\mathrm{rat}$ obviously results in

$$\hat{\mathbf{A}}_\mathrm{rat}^t \begin{pmatrix} \hat{\mathbf{x}}_\mathrm{c} \\ \hat{\mathbf{x}}_\mathrm{n} \end{pmatrix} = \begin{pmatrix} \mathbf{A}_\mathrm{c}^t\, \hat{\mathbf{x}}_\mathrm{c} \\ \mathbf{A}_\mathrm{n}^t\, \hat{\mathbf{x}}_\mathrm{n} \end{pmatrix}$$

which makes clear how the results of the cyclic and nilpotent subsystem can be superposed: composed states $\hat{\mathbf{x}}^\mathrm{T} = (\hat{\mathbf{x}}_\mathrm{c}^\mathrm{T}, \hat{\mathbf{x}}_\mathrm{n}^\mathrm{T})$ of the form $\hat{\mathbf{x}}_\mathrm{c} \neq \mathbf{0}$ and $\hat{\mathbf{x}}_\mathrm{n} = \mathbf{0}$ constitute a cyclic state graph according to Theorem 4.8, whereas states of the form $\hat{\mathbf{x}}_\mathrm{c} = \mathbf{0}$ and $\hat{\mathbf{x}}_\mathrm{n} \neq \mathbf{0}$ constitute a so-called null tree, a

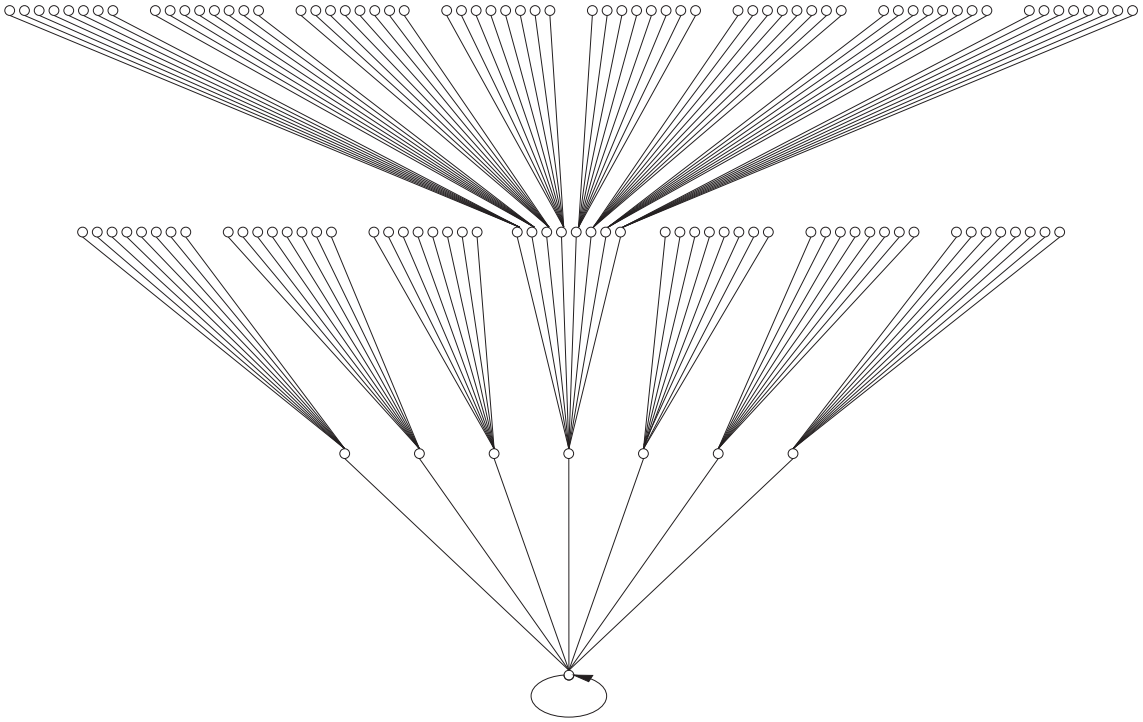


Figure 4.5: State graph of the 7-th order LMS with nilpotent dynamics matrix (Example 4.2.2.3)

state graph, all states of which incrementally approach the zero vector (null state) according to Theorem 4.11 and Corollary 4.3. For the remaining composed states with $\hat{\mathbf{x}}_c \neq \mathbf{0}$ and $\hat{\mathbf{x}}_n \neq \mathbf{0}$ — due to invertibility of matrix $\mathbf{A}_c$ the cyclic subsystem is characterized by unique predecessor and successor states — the overall state interconnection structure is governed by the nilpotent matrix $\mathbf{A}_n$ only. Hence, these structures are made up of trees with the shape of the null tree and all these trees incrementally approach and terminate in a periodic state $\hat{\mathbf{x}}_n = \mathbf{0}$. For this reason, the construction of the overall state graph amounts to simply attaching a null tree (to be determined by $\mathbf{A}_n$) to each periodic state (following from $\mathbf{A}_c$).

The following theorem completes the results that have been derived so far such that the entire state graph of the overall LMS can be determined completely.

Theorem 4.12 (State Graph of an LMS with Arbitrary Dynamics)
Let $\hat{\mathbf{A}}_{\text{rat}} = \text{diag}(\mathbf{A}_c, \mathbf{A}_n)$ be the (reordered) rational canonical form of the dynamics matrix $\mathbf{A}$ of an LMS, where $\mathbf{A}_c$ and $\mathbf{A}_n$ are cyclic and nilpotent matrices, given with its associated cycle sum and null tree, respectively. Let the corresponding composed state be expressed in transformed coordinates, i. e. $\hat{\mathbf{x}}^T = (\hat{\mathbf{x}}_c^T, \hat{\mathbf{x}}_n^T)$. Then any periodic state of the form $\hat{\mathbf{x}}_c \neq \mathbf{0}$ and $\hat{\mathbf{x}}_n = \mathbf{0}$ represents the root of a tree which has the structure of the null tree associated to $\mathbf{A}_n$ and the remaining states with $\hat{\mathbf{x}}_c = \mathbf{0}$ are the respective non-periodic tree states. □

4.2.3.1 Example: an LMS with Arbitrary Dynamics Matrix

For an illustration of how to construct the state graph of an LMS the dynamics matrix of which comprises both, a cyclic and a nilpotent subsystem, consider the dynamics matrix

$$\mathbf{A} = \operatorname{diag}(\mathbf{A}_\mathrm{c}, \mathbf{A}_\mathrm{n}), \quad \mathbf{A}_\mathrm{c} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \in \mathbb{F}_2^{2\times 2}, \quad \mathbf{A}_\mathrm{n} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \in \mathbb{F}_2^{2\times 2}$$

which is given already in (reordered) rational canonical form. To matrix $\mathbf{A}_\mathrm{c}$ corresponds the single elementary divisor polynomial $\lambda^2+\lambda+1$ which is irreducible and of period $\tau = 3$. By Theorem 4.8 the cycle sum of the respective LMS results in $\Sigma = 1[1] \dot{+} 1[3]$.

The single nilpotent submatrix $\mathbf{A}_\mathrm{n}$ is associated to the the single elementary divisor (and minimal) polynomial λ^2, by Theorem 4.9 the corresponding null tree consists of $h = 2$ levels and the level number $l = 0,1,2$ comprises 1, 1 and 2 states, respectively. The single state in level $l = 1$ has 2 confluent states, whereas the zero state has only one confluent state. Due to Theorem 4.12 this means to attach this null tree to any of the 4 cyclic states (see Figure 4.6).

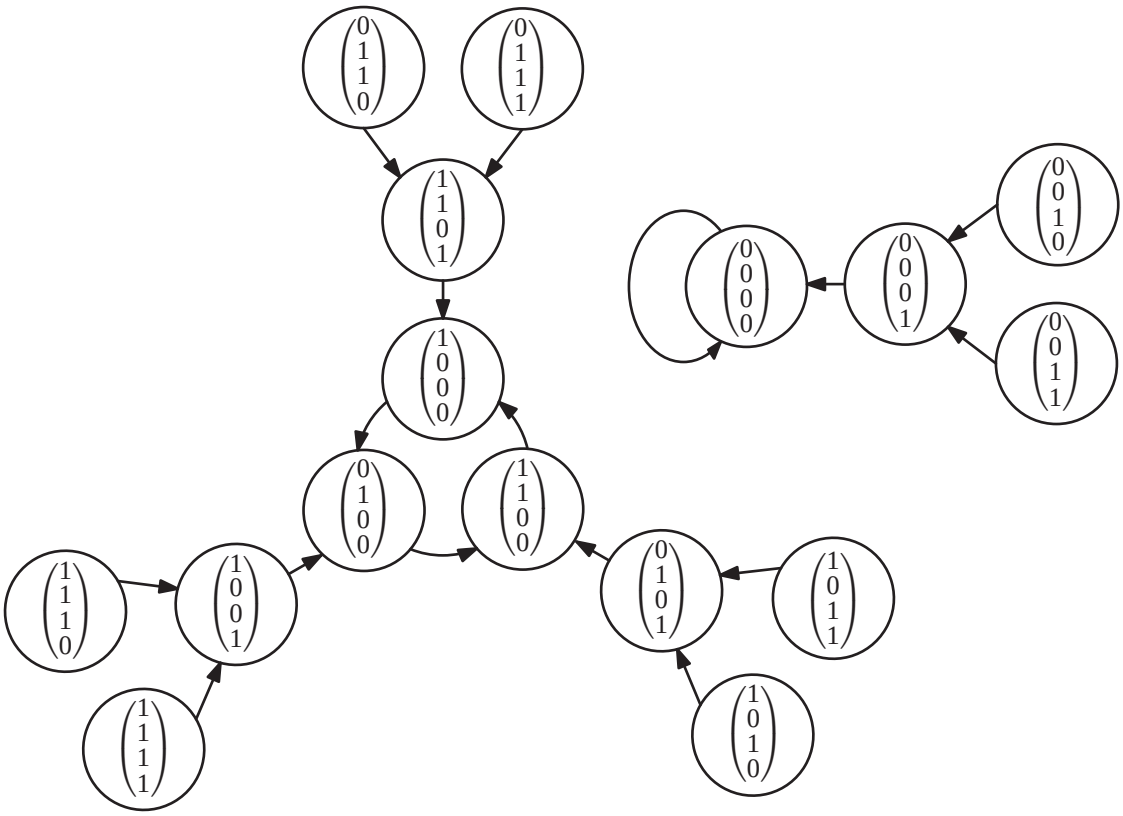


Figure 4.6: State graph of the 4-th order LMS discussed in Example 4.2.3.1

4.3 Inhomogeneous LMS

In this section, systems are in the focus which comply with

$$\mathbf{x}(k+1) = \mathbf{A}\,\mathbf{x}(k) + \mathbf{b}\,, \tag{4.44}$$

where $\mathbf{x}(k) \in \mathbb{F}_q^n$ is the state at instant $k \in \mathbb{N}_0$ and the additional constant vector $\mathbf{b} \in \mathbb{F}_q^n$, the affine part, enlarges the former homogeneous LMS by an inhomogeneous expression. Hence, these systems are termed inhomogeneous LMS. Based on the theory derived so far, it is promising to make efforts in reducing these systems to the homogenous case. Hence, one is left with the question under which conditions such a transform is possible, for example by a suitable change of coordinates. If these conditions cannot be met then an exact borderline should drawn, which renders the investigation of such an inhomogeneous LMS easier. This will be the guideline in what follows.

4.3.1 Linearization by Translation

The bijective mapping $\tilde{\mathbf{x}} = \mathbf{x} - \mathbf{x}_0$ represents a translation of the state vector $\mathbf{x}$ by the shift $\mathbf{x}_0$. The following Lemma points out when this translation can be used for transforming an inhomogeneous LMS according to (4.44) into a linear one.

Lemma 4.7 (First Condition for Transformability into a Homogeneous LMS)
An inhomogeneous LMS given in accordance with equation (4.44) can be transformed into an homogeneous LMS with dynamics matrix $\mathbf{A}$ iff $\mathbf{b} \in \mathrm{Im}(\mathbf{I} - \mathbf{A})$. □

Proof Assume an LMS with $\tilde{\mathbf{x}}' = \mathbf{A}\tilde{\mathbf{x}}$, which expresses the linear mapping of a state $\tilde{\mathbf{x}}$ to its successor $\tilde{\mathbf{x}}'$ in some transformed coordinates. Then, the respective (bijective) coordinate transform $\tilde{\mathbf{x}} = \phi(\mathbf{x})$ assures the existence of a vector $\mathbf{0} = \phi(\mathbf{x}_0)$ for one unique $\mathbf{x}_0$ in the original coordinates. Since $\tilde{\mathbf{x}} = \mathbf{0}$ is a fixpoint under the mapping $\mathbf{A}$, the vector $\mathbf{x}_0$ is this fixpoint expressed in the original coordinates, hence in the inhomogeneous LMS holds

$$\begin{aligned} & \mathbf{x}_0 = \mathbf{A}\,\mathbf{x}_0 + \mathbf{b} \\ \iff \quad & (\mathbf{I} - \mathbf{A})\,\mathbf{x}_0 = \mathbf{b} \end{aligned} \tag{4.45}$$

and to require solvability for $\mathbf{x}_0$ is to require $\mathbf{b} \in \mathrm{Im}(\mathbf{I} - \mathbf{A})$.

Conversely, if $\mathbf{b} \in \mathrm{Im}(\mathbf{I} - \mathbf{A})$ then a $\mathbf{x}_0$ exists for which $(\mathbf{I} - \mathbf{A})\,\mathbf{x}_0 = \mathbf{b}$ applies. Specify a coordinate transform $\tilde{\mathbf{x}} = \phi(\mathbf{x})$ such that $\phi(\mathbf{x}_0) = \mathbf{0}$. For example, choose the bijective mapping $\tilde{\mathbf{x}} = \mathbf{x} - \mathbf{x}_0$ and let $\tilde{\mathbf{x}}' = \mathbf{x}' - \mathbf{x}_0$ be the successor state of $\tilde{\mathbf{x}}$. Then by use of the inverse transform in the state

equation, i. e.

$$\begin{aligned} \tilde{\mathbf{x}}' + \mathbf{x}_0 &= \mathbf{A}(\tilde{\mathbf{x}} + \mathbf{x}_0) + \mathbf{b} = \mathbf{A}\tilde{\mathbf{x}} + \mathbf{A}\mathbf{x}_0 + (\mathbf{I} - \mathbf{A})\mathbf{x}_0 \\ &= \mathbf{A}\tilde{\mathbf{x}} + \mathbf{x}_0 \\ \iff \qquad \tilde{\mathbf{x}}' &= \mathbf{A}\tilde{\mathbf{x}}, \end{aligned}$$

an LMS in the transformed coordinates is obtained, as was the other part of the claim. □

Hence the question is: which are the requirements on $\mathbf{A}$ and on $\mathbf{b}$ such that $\mathbf{b} \in \mathrm{Im}(\mathbf{I} - \mathbf{A})$?

To this end, the state $\mathbf{x}$ is transformed using equation (4.8), which transforms the dynamics matrix $\mathbf{A}$ of an LMS into its respective rational canonical form $\mathbf{A}_{\mathrm{rat}}$. Consequently, the transformed form of equation (4.45) is

$$(\mathbf{I} - \mathbf{A}_{\mathrm{rat}})\,\hat{\mathbf{x}}_0 = \hat{\mathbf{b}}$$

with the denotation $\hat{\mathbf{b}} = \hat{\mathbf{T}}\mathbf{b}$. In more detail, this equation can be written by resorting to the companion matrices with respect to the N elementary divisor polynomials of $\mathbf{A}$, accordingly

$$(\mathbf{I} - \mathbf{C}_i)\,\hat{\mathbf{x}}_0^{(i)} = \hat{\mathbf{b}}_i, \quad i = 1, \ldots, N. \tag{4.46}$$

Equation (4.46) is always solvable if $\mathbf{A}$ does not contain elementary divisor polynomials $p_{\mathbf{C}_i}(\lambda) = (\lambda - 1)^{l_i}$, for some $l_i \in \mathbb{N}$. In this case all matrices $(\mathbf{I} - \mathbf{C}_i)$ are non-singular, hence invertible, as implied by Theorem 4.3.

On the contrary, if for some i the defining polynomial of the companion matrix $\mathbf{C}_i \in \mathbb{F}_q^{d_i \times d_i}$ is $p_{\mathbf{C}_i}(\lambda) = (\lambda - 1)^{l_i}$, $l_i \in \mathbb{N}$, then

$$\mathbf{I} - \mathbf{C}_i = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 & a_{0,i} \\ -1 & 1 & 0 & \cdots & 0 & a_{1,i} \\ 0 & -1 & 1 & \cdots & 0 & a_{2,i} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & -1 & 1 + a_{d_i - 1,i} \end{pmatrix}$$

and with the non-singular transformation matrix

$$\mathbf{L} = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 1 & 1 & 0 & \cdots & 0 \\ 1 & 1 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & 1 & \cdots & 1 \end{pmatrix} \tag{4.47}$$

equation (4.46) becomes

$$\mathbf{L}(\mathbf{I} - \mathbf{C}_i) = \begin{pmatrix} 1 & 0 & 0 & \cdots & a_{0,i} \\ 0 & 1 & 0 & \cdots & a_{0,i} + a_{1,i} \\ 0 & 0 & 1 & \cdots & a_{0,i} + a_{1,i} + a_{2,i} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 + \sum_{j=0}^{d_i - 1} a_{j,i} \end{pmatrix} \hat{\mathbf{x}}_0^{(i)} = \begin{pmatrix} \hat{b}_{1,i} \\ \hat{b}_{1,i} + \hat{b}_{2,i} \\ \hat{b}_{1,i} + \hat{b}_{2,i} + \hat{b}_{3,i} \\ \vdots \\ \sum_{j=1}^{d_i} \hat{b}_{j,i} \end{pmatrix} \tag{4.48}$$

Note that

$$1+\sum_{j=0}^{d_i-1} a_{j,i} = p_{\mathbf{C}_i}(1) \tag{4.49}$$

with regard to the polynomial $p_{\mathbf{C}_i}(\lambda) = (\lambda-1)^{l_i}$. But $p_{\mathbf{C}_i}(1) = 0$ which in consequence means that for assuring $\hat{\mathbf{b}}_i \in \mathrm{Im}(\mathbf{I}-\mathbf{C}_i)$ the relation

$$\sum_{j=1}^{d_i} \hat{b}_{j,i} = 0\,. \tag{4.50}$$

has to be satisfied with respect to all numbers i which refer to elementary divisor polynomials of the form $p_{\mathbf{C}_i}(\lambda) = (\lambda-1)^{l_i}$. With Lemma 4.7 this yields a proof of

Theorem 4.13 (General Condition for Transformability into a Homogeneous LMS)
Let an inhomogeneous LMS be given by its state equation in rational canonical form

$$\hat{\mathbf{x}}(k+1) = \mathbf{A}_{\mathrm{rat}}\,\hat{\mathbf{x}}(k) + \hat{\mathbf{b}} = \mathrm{diag}(\mathbf{C}_1,\ldots,\mathbf{C}_N) \begin{pmatrix} \hat{\mathbf{x}}^{(1)}(k) \\ \vdots \\ \hat{\mathbf{x}}^{(N)}(k) \end{pmatrix} + \begin{pmatrix} \hat{\mathbf{b}}_1 \\ \vdots \\ \hat{\mathbf{b}}_N \end{pmatrix}$$

with $i = 1,\ldots,N$ companion matrices $\mathbf{C}_i$ associated to the elementary divisor polynomials of the respective dynamics matrix $\mathbf{A}$. Then the inhomogeneous LMS can be transformed into an equivalent LMS by a change of coordinates iff the sum of vector entries is zero for those vectors $\hat{\mathbf{b}}_i$ which correspond to elementary divisor polynomials of the form $p_{\mathbf{C}_i}(\lambda) = (\lambda-1)^{l_i}$, if any. If no elementary divisor polynomial is of this form then the inhomogeneous LMS is equivalent to an LMS without any further restriction. □

If this transformability condition is satisfied then the respective shift vector $\hat{\mathbf{x}}_0^{(i)}$ concerning the partial coordinate transform $\tilde{\mathbf{x}}^{(i)} = \hat{\mathbf{x}}^{(i)} - \hat{\mathbf{x}}_0^{(i)}$ can be determined. To this end, observe that with equation (4.48), with the relation $1+\sum_{j=0}^{d_i-1} a_{j,i} = 0$ and with the kernel

$$\begin{aligned} \mathrm{Ker}(\mathbf{I}-\mathbf{C}_i) &= \mathrm{Ker}\big(\mathbf{L}\,(\mathbf{I}-\mathbf{C}_i)\big) \\ &= \mathrm{span}\big\{(-\alpha_{0,i}, -\alpha_{0,i}-\alpha_{1,i}, \ldots, -\alpha_{0,i}-\alpha_{1,i}\ldots-\alpha_{d_i-2,i}, 1)^{\mathrm{T}}\big\} \\ &= \mathrm{span}\big\{(1+\alpha_{1,i}+\cdots+\alpha_{d_i-1,i}, 1+\alpha_{2,i}+\cdots+\alpha_{d_i-1,i}, \ldots, 1+\alpha_{d_i-1,i}, 1)^{\mathrm{T}}\big\} \end{aligned} \tag{4.51}$$

the homogeneous solution can be obtained. A particular solution of equation (4.48) is given by setting the last entry of the solution vector equal to zero. Both ideas are summarized within the following theorem.

Theorem 4.14 (Translation into a Homogeneous LMS)
Assume that for an inhomogeneous LMS in rational canonical form the transformability condition of Theorem 4.13 is fulfilled. Then each subsystem $i = 1,\ldots,N$ of the inhomogeneous LMS can be transformed into an LMS by use of a translation of the substate $\hat{\mathbf{x}}^{(i)}$, that is $\tilde{\mathbf{x}}^{(i)} = \hat{\mathbf{x}}^{(i)} - \hat{\mathbf{x}}_0^{(i)}$, where

1. for elementary divisor polynomials $p_{\mathbf{C}_i}(\lambda) \neq (\lambda-1)^{l_i}$,

$$\hat{\mathbf{x}}_0^{(i)} = (\mathbf{I}-\mathbf{C}_i)^{-1}\hat{\mathbf{b}}_i\,,$$

2. for elementary divisor polynomials $p_{\mathbf{C}_i}(\lambda) = (\lambda-1)^{l_i}$,

$$\mathbf{x}_0^{(i)} = \begin{pmatrix} b_{1,i} \\ b_{1,i}+b_{2,i} \\ \vdots \\ \sum_{j=1}^{d_i-1} b_{j,i} \\ 0 \end{pmatrix} + \begin{pmatrix} 1+a_{d_i-1,i}+\cdots+a_{1,i} \\ 1+a_{d_i-1,i}+\cdots+a_{2,i} \\ \vdots \\ 1+a_{d_i-1,i} \\ 1 \end{pmatrix} z_i\,, \quad \forall z_i \in \mathbb{F}_q\,.$$

With these results, in the overall system the respective translation of state is

$$\tilde{\mathbf{x}} = \hat{\mathbf{x}} - \left(\hat{\mathbf{x}}_0^{(1)\mathrm{T}}, \ldots, \hat{\mathbf{x}}_0^{(N)\mathrm{T}}\right)^{\mathrm{T}}$$

that transforms the inhomogeneous LMS into a linear one. □

Remark 4.10
All free parameters z_i in part 2 of Theorem 4.14 can be chosen $z_i = 0$, for simplicity. □

4.3.2 Non-linearizable Parts

In order to complete the result, subsystems

$$\hat{\mathbf{x}}^{(i)}(k+1) = \mathbf{C}_i\,\hat{\mathbf{x}}^{(i)}(k) + \hat{\mathbf{b}}_i \tag{4.52}$$

of an inhomogeneous LMS have to be concerned which do not suffice the transformability condition of Theorem 4.13.

Theorem 4.15 (Cycle Sum of the Non-linearizable Subsystem of an Inhomogeneous LMS)
Assume that for an inhomogeneous LMS in rational canonical form the transformability condition of Theorem 4.13 is not fulfilled by N_u subsystems associated to $i = 1, \ldots, N_\mathrm{u}$ elementary divisor polynomials $p_{\mathbf{C}_i}(\lambda)$ of degree d_i. Then all q^{d_i} states of subsystem i are t_i-periodic with

$$t_i = \begin{cases} q^{l_i} & \text{if} \quad \exists l_i \in \mathbb{N} : q^{l_i} > d_i > q^{l_i-1} \\ q^{l_i+1} & \text{otherwise} \quad (\exists l_i \in \mathbb{N} : q^{l_i} = d_i) \end{cases} \tag{4.53}$$

and the subsystem i contributes the cycle sum

$$\Sigma_i = \frac{q^{d_i}}{t_i}[t_i]\,. \tag{4.54}$$

to the cycle sum

$$\Sigma_\mathrm{u} = \frac{q^{d_1+\cdots+d_{N_\mathrm{u}}}}{\mathrm{lcm}(t_1,\ldots,t_{N_\mathrm{u}})}[\mathrm{lcm}(t_1,\ldots,t_{N_\mathrm{u}})] \tag{4.55}$$

of all N_u non-linearizable subsystems. □

Proof The following statements are to be proven:

1) any state in the i-th subspace has a unique predecessor, thus is periodic,

2) all states have period t_i as in equation (4.53),

3) the cycle sum of N_{u} non-linearizable subsystems is given by equation (4.55).

In order to facilitate the notation, the system index i will be omitted.

ad 1) Rewrite equation (4.52) as per

$$\mathbf{C}\,\hat{\mathbf{x}}(k) = \hat{\mathbf{x}}(k+1) - \hat{\mathbf{b}}$$

Since with $p_{\mathbf{C}} = (\lambda - 1)^d$ the companion matrix $\mathbf{C}$ is invertible any state $\hat{\mathbf{x}}(k+1)$ has a unique predecessor state $\hat{\mathbf{x}}(k) = \mathbf{C}^{-1}(\hat{\mathbf{x}}(k+1) - \hat{\mathbf{b}})$, hence, the state graph cannot show tree structure, and due to the assumption that a vector $\hat{\mathbf{x}}_0$ solving $(\mathbf{I} - \mathbf{C})\,\hat{\mathbf{x}}_0 = \hat{\mathbf{b}}$ does not exist there is no state $\hat{\mathbf{x}}(k+1) = \hat{\mathbf{x}}(k)$. As a consequence, all states have to be periodic with $t > 1$.

ad 2) Starting with equation (4.52), the existence of a t-periodic state $\hat{\mathbf{x}}(k+t) = \hat{\mathbf{x}}(k) =: \hat{\mathbf{x}}_t$ means that

$$(\mathbf{I} - \mathbf{C}^t)\,\hat{\mathbf{x}}_t = \left(\sum_{i=0}^{t-1} \mathbf{C}^i\right) \hat{\mathbf{b}} \tag{4.56}$$

holds for a least integer t. The left hand side of this equation comprises a geometric series, which results in

$$\begin{aligned} &\left(\sum_{i=0}^{t-1} \mathbf{C}^i\right)(\mathbf{I} - \mathbf{C})\,\hat{\mathbf{x}}_t = \left(\sum_{i=0}^{t-1} \mathbf{C}^i\right)\hat{\mathbf{b}} \\ \Longleftrightarrow\ &\left(\sum_{i=0}^{t-1} \mathbf{C}^i\right)\Big((\mathbf{I} - \mathbf{C})\,\hat{\mathbf{x}}_t - \hat{\mathbf{b}}\Big) = \mathbf{0} \end{aligned} \tag{4.57}$$

There are three conceivable ways of solving equation (4.57):

a) a trivial solution $(\mathbf{I} - \mathbf{C})\,\hat{\mathbf{x}}_t - \hat{\mathbf{b}} = \mathbf{0}$ exists,

b) there are vectors $\hat{\mathbf{x}}^\star \in \mathrm{Ker}(\sum_{i=0}^{t-1} \mathbf{C}^i)$ with $\hat{\mathbf{x}}^\star := (\mathbf{I} - \mathbf{C})\,\hat{\mathbf{x}}_t - \hat{\mathbf{b}}$,

c) $\sum_{i=0}^{t-1} \mathbf{C}^i \equiv \mathbf{0}$.

ad a) By assumption the inhomogeneous LMS is not linearizable, therefore, such a trivial solution does not exist as per Lemma 4.7.

ad b) Equation (4.57) can be solved non-trivially iff the determinant $\det(\sum_{i=0}^{t-1}\mathbf{C}^i) = 0$. Then some $\hat{\mathbf{x}}^\star$ might be found in $\mathrm{Ker}(\sum_{i=0}^{t-1}\mathbf{C}^i)$. As by Theorem 4.3 the polynomials $p_{\mathbf{C}}(\lambda) = (\lambda-1)^l$ and $\sum_{i=0}^{t-1}\lambda^i$ must have a common factor, it results that the matrix $(\mathbf{I}-\mathbf{C})$ has a rank deficiency and the vector $\hat{\mathbf{x}}^\star$ is a solution of

$$(\mathbf{I}-\mathbf{C})\,\hat{\mathbf{x}}^\star = \mathbf{0} \tag{4.58}$$

by means of which $\hat{\mathbf{x}}_t$ can be determined with

$$(\mathbf{I}-\mathbf{C})\,\hat{\mathbf{x}}_t = \hat{\mathbf{x}}^\star + \hat{\mathbf{b}}\,. \tag{4.59}$$

By use of the kernel in equation (4.51) the solution of equation (4.58) is

$$(\hat{\mathbf{x}}^\star)^{\mathrm{T}} = z\,(1+a_{d-1}+\cdots+a_1, 1+a_{d-1}+\cdots+a_2, \ldots, 1+a_{d-1}, 1) \quad \forall z \in \mathbb{F}_q\,. \tag{4.60}$$

With this result and by applying the solvability condition (4.50), equation (4.59) is solvable iff

$$\sum_{i=1}^{d} \hat{x}_i^\star + \hat{b}_i = 0\,. \tag{4.61}$$

For testing this, first, calculate the coefficients in (4.60) by recalling that

$$(\lambda-1)^d = \sum_{i=0}^{d} \binom{d}{i} (-1)^{d-i}\lambda^i\,, \tag{4.62}$$

hence,

$$a_i = \binom{d}{i}(-1)^{d-i}, \quad i = 0,\ldots,d \tag{4.63}$$

and by equation (4.60) the sum of entries in vector $\hat{\mathbf{x}}^\star$ reads

$$\begin{aligned}\sum_{i=1}^{d} \hat{x}_i^\star &= z\,(d+(d-1)a_{d-1}+(d-2)a_{d-2}+\cdots+a_1) = z\sum_{i=1}^{d} i\,a_i \\ &= z\sum_{i=1}^{d} i\binom{d}{i}(-1)^{d-i}\,.\end{aligned} \tag{4.64}$$

The only interesting cases are vector-valued, thus, assume $d > 1$ in the evaluation of

$$\begin{aligned}\sum_{i=1}^{d} \hat{x}_i^\star &= z\sum_{i=1}^{d} i\binom{d}{i}(-1)^{d-i} = z\sum_{i=1}^{d}\frac{d!}{(d-i+1-1)!(i-1)!}(-1)^{d-i} \\ &= z\,d\sum_{i=1}^{d}\frac{(d-1)!}{((d-1)-(i-1))!(i-1)!}(-1)^{d-i} = z\,d\sum_{i=1}^{d}\binom{d-1}{i-1}(-1)^{d-i} \\ &= z\,d\sum_{j=0}^{d-1}\binom{d-1}{j}(-1)^{d-1-j} = z\,d\,(\lambda-1)^{d-1}\Big|_{\lambda=1} = 0\end{aligned} \tag{4.65}$$

and consequently

$$\sum_{i=1}^{d} \hat{x}_i^{\star} + \hat{b}_i = \sum_{i=1}^{d} \hat{b}_i \,. \tag{4.66}$$

But then by condition (4.61) equation (4.59) is solvable iff

$$\sum_{i=1}^{d} \hat{b}_i = 0 \tag{4.67}$$

which contradicts the assumption that the inhomogeneous LMS is non-linearizable; see Theorem 4.13.

ad c) Since there are periodic states it remains only that

$$\sum_{i=0}^{t-1} \mathbf{C}^i \equiv \mathbf{0} \tag{4.68}$$

is satisfied for some least integer t. With $p_{\mathbf{C}}(\lambda) = \mathrm{mp}_{\mathbf{C}}(\lambda) = (\lambda-1)^d$ Theorem 4.2 implies that

$$g(\lambda)(\lambda-1)^d = \sum_{i=0}^{t-1} \lambda^i \tag{4.69}$$

for some polynomial $g(\lambda)$. Multiplication by $(\lambda-1)$ yields

$$g(\lambda)(\lambda-1)^{d+1} = \lambda^t - 1 \tag{4.70}$$

for a least integer t. But then equation (4.70) implies that t is the period of the polynomial $(\lambda-1)^{d+1}$. This period t results from Theorem 2.5, accordingly

$$t = \tau_{(\lambda-1)^{d+1}} = \begin{cases} \tau_{(\lambda-1)^d} &= q^l \quad \text{if} \quad q^l > d > q^{l-1}, \, l \in \mathbb{N} \\ q\,\tau_{(\lambda-1)^d} &= q^{l+1} \quad \text{if} \quad q^l = d, \qquad\quad l \in \mathbb{N} \end{cases} \tag{4.71}$$

In part 1 it has been shown that all states in the respective state space are periodic. Observe, that equation (4.68) is state-independent. Hence, all states are periodic of the same period t and altogether they constitute q^d/t cycles of length t

ad 3) Using Theorem 4.7 for the superposition of $i = 1, \ldots, N_{\mathrm{u}}$ such subsystems yields

$$\begin{aligned} \Sigma_{N_{\mathrm{u}}} &= \left(\frac{q^{d_1}}{t_1}[t_1]\right) \cdots \left(\frac{q^{d_{N_{\mathrm{u}}}}}{t_{N_{\mathrm{u}}}}[t_{N_{\mathrm{u}}}]\right) = \frac{q^{d_1}\cdots q^{d_{N_{\mathrm{u}}}}}{t_1 \cdots t_{N_{\mathrm{u}}}} \gcd(t_1, \ldots, t_{N_{\mathrm{u}}}) \, [\mathrm{lcm}(t_1, \ldots, t_{N_{\mathrm{u}}})] \\ &= \frac{q^{d_1+\cdots+d_{N_{\mathrm{u}}}}}{\mathrm{lcm}(t_1, \ldots, t_{N_{\mathrm{u}}})} [\mathrm{lcm}(t_1, \ldots, t_{N_{\mathrm{u}}})] \end{aligned}$$

in accordance with equation (4.55); which completes the proof. □

Remark 4.11
In the subspace with regard to an elementary divisor polynomial $(\lambda-1)^d$ of a homogeneous LMS, the maximal possible period of the subspace states is $\tau_{\max} = q^l$ with $q^l \geq d > q^{l-1}$. If this subsystem is a non-linearizable inhomogeneous LMS with dimension $d = q^l$ then the maximal possible period of the subspace states is $\tau_{\max} = q^{l+1}$, that is q-times the maximal period of an homogenous LMS. □

4.3.3 General Inhomogeneous LMS

Summing up the results of the past sections, an inhomogeneous LMS as in equation (4.44) can be split into three uncoupled subsystems

$$\hat{\mathbf{x}}_{\mathrm{c,u}}(k+1) = \mathbf{A}_{\mathrm{c,u}}\hat{\mathbf{x}}_{\mathrm{c,u}}(k) + \hat{\mathbf{b}}_{\mathrm{u}} \tag{4.72}$$

$$\tilde{\mathbf{x}}_{\mathrm{c,s}}(k+1) = \mathbf{A}_{\mathrm{c,s}}\tilde{\mathbf{x}}_{\mathrm{c,s}}(k) \tag{4.73}$$

$$\tilde{\mathbf{x}}_{\mathrm{n}}(k+1) = \mathbf{A}_{\mathrm{n}}\tilde{\mathbf{x}}_{\mathrm{n}}(k) \tag{4.74}$$

First, the system with cyclic dynamics matrix $\mathbf{A}_{\mathrm{c,u}}$ represents the non-linearizable subsystem regarding $\mathbf{A}_{\mathrm{c}}$; all elementary divisor polynomials of $\mathbf{A}_{\mathrm{c,u}}$ are of the form $p_{\mathbf{C}_i}(\lambda) = (\lambda-1)^{l_i}$ and the corresponding sum of coefficients is $\sum_i \hat{b}_i \neq 0$. The second system with cyclic dynamics matrix $\mathbf{A}_{\mathrm{c,s}}$ represents the linearizable subsystem regarding $\mathbf{A}_{\mathrm{c}}$; any elementary divisor polynomial of $\mathbf{A}_{\mathrm{c,s}}$ that is of the form $p_{\mathbf{C}_i}(\lambda) = (\lambda-1)^{l_i}$ is associated to $\sum_i \hat{b}_i = 0$. Finally the third system, the nilpotent subsystem with dynamics matrix $\mathbf{A}_{\mathrm{n}}$, is always linearizable by a shift of state.

Finally, a possible combination of the main results developed in Section 4.2 and in Section 4.3 for calculating the cycle sum and the state graph of an inhomogeneous LMS is the following:

1. Transform the coordinates of the states in the inhomogeneous LMS such that with
$$\mathbf{x}(k+1) = \mathbf{A}\,\mathbf{x}(k) + \mathbf{b} \quad \Longleftrightarrow \quad \hat{\mathbf{x}}(k+1) = \hat{\mathbf{A}}_{\mathrm{rat}}\,\hat{\mathbf{x}}(k) + \hat{\mathbf{b}}$$
the dynamics matrix $\hat{\mathbf{A}}_{\mathrm{rat}}$ is in ordered rational canonical form $\hat{\mathbf{A}}_{\mathrm{rat}} = \mathrm{diag}(\mathbf{A}_{\mathrm{c}}, \mathbf{A}_{\mathrm{n}})$, which contains the dynamics matrices of the cyclic and nilpotent subsystems.

2. Check the linearizability condition of Theorem 4.13 for any cyclic subsystem (4.52) concerning $\mathbf{A}_{\mathrm{c}}$ and split this inhomogeneous LMS into a linearizable subsystem with dynamics matrix $\mathbf{A}_{\mathrm{c,s}}$ and a non-linearizable subsystem with dynamics matrix $\mathbf{A}_{\mathrm{c,u}}$.

3. Determine the cycle sum Σ_{s} of the subsystem concerning $\mathbf{A}_{\mathrm{c,s}}$ by use of Theorem 4.8.

4. Determine the cycle sum Σ_{u} of the subsystem concerning $\mathbf{A}_{\mathrm{c,u}}$ by use Theorem 4.15.

5. Superpose the cycle sums referring to Theorem 4.7 according to $\Sigma = \Sigma_{\mathrm{s}}\Sigma_{\mathrm{u}}$ to obtain the cycle sum Σ of the overall inhomogeneous LMS.

6. Calculate the null tree with respect to the nilpotent subsystem $\mathbf{A}_\mathrm{n}$ by means of Theorem 4.11 and Corollary 4.3.

7. For obtaining the state graph of the entire inhomogeneous LMS attach the above-derived null tree to any periodic state with regard to the cycle sum Σ; as per Theorem 4.12.

4.3.4 Example

For a demonstration of the results consider an inhomogeneous LMS(2) of order $n = 6$ with a dynamics matrix $\mathbf{A}$ that is given in ordered rational canonical form according to

$$\mathbf{x}(k+1) = \mathbf{A}\,\mathbf{x}(k) + \mathbf{b}, \qquad \mathbf{A} = \mathrm{diag}(\mathbf{C}_{(\lambda+1)^2}, \mathbf{C}_{(\lambda+1)^3}, \mathbf{C}_\lambda), \qquad \mathbf{b}^\mathrm{T} = (\mathbf{b}_1^\mathrm{T}, \mathbf{b}_2^\mathrm{T}, \mathbf{b}_3^\mathrm{T}),$$

$$\mathbf{C}_{(\lambda+1)^2} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \mathbf{C}_{(\lambda+1)^3} = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}, \quad \mathbf{C}_\lambda = 0, \quad \mathbf{b}_1 = \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \quad \mathbf{b}_2 = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \quad \mathbf{b}_3 = 1,$$

hence, the dynamics matrix $\mathbf{A} = \mathrm{diag}(\mathbf{A}_\mathrm{c}, \mathbf{A}_\mathrm{n})$ is (already) decomposed into a cyclic block-diagonal matrix $\mathbf{A}_\mathrm{c} = \mathrm{diag}(\mathbf{C}_{(\lambda+1)^2}, \mathbf{C}_{(\lambda+1)^3})$ and a nilpotent block-diagonal matrix $\mathbf{A}_\mathrm{n} = \mathbf{C}_\lambda$.

If the task is to determine the cycle sum of this inhomogeneous LMS, one is left with two companion matrices in the blocks of $\mathbf{A}$, these are $\mathbf{C}_{(\lambda+1)^2}$ and $\mathbf{C}_{(\lambda+1)^3}$ with defining polynomial $(\lambda-1)^2$ and $(\lambda-1)^3$, respectively, which both are candidates for representing non-linearizable subsystems. Thus, examine the mod2-sum of coefficients of $\mathbf{b}_1$

$$\sum_{j=1}^{d_1} b_{j,1} = 1 + 1 = 0$$

and of $\mathbf{b}_2$

$$\sum_{j=1}^{d_2} b_{j,2} = 1 + 1 + 1 = 1 \neq 0\,.$$

These signify that the subsystem corresponding to $\mathbf{A}_\mathrm{c,s} = \mathbf{C}_{(\lambda+1)^2}$ can be linearized as per

$$\tilde{\mathbf{x}}_\mathrm{c,s}(k+1) = \mathbf{A}_\mathrm{c,s}\,\tilde{\mathbf{x}}_\mathrm{c,s}(k) \tag{4.75}$$

using the translated state $\tilde{\mathbf{x}}_\mathrm{c,s} = \mathbf{x}_1 - \mathbf{x}_0^{(1)}$ with a shift vector $\mathbf{x}_0^{(1)}$, which by Theorem 4.13 is guaranteed to exist and via Theorem 4.14 together with Remark 4.10 can be chosen as $\mathbf{x}_0^{(1)} = (1,0)^\mathrm{T}$. In addition to that, the subsystem corresponding to $\mathbf{A}_\mathrm{c,u} = \mathbf{C}_{(\lambda+1)^3}$ and $\mathbf{b}_\mathrm{u} = \mathbf{b}_2$ cannot be linearized, hence

$$\mathbf{x}_\mathrm{c,u}(k+1) = \mathbf{A}_\mathrm{c,u}\,\mathbf{x}_\mathrm{c,u}(k) + \mathbf{b}_\mathrm{u}\,. \tag{4.76}$$

Moreover, it is clear that the nilpotent subsystem associated to $\mathbf{A}_\mathrm{n}$ is linearizable by the shift of state $\tilde{\mathbf{x}}_\mathrm{n} = \mathbf{x}_\mathrm{n} - 1$, that is

$$\tilde{\mathbf{x}}_\mathrm{n}(k+1) = \mathbf{A}_\mathrm{n}\,\tilde{\mathbf{x}}_\mathrm{n}(k)\,.$$

Then with Theorem 4.7, the cycle sum Σ of the entire inhomogeneous LMS can be determined by the superposition of the cycle sum Σ_s and Σ_u of the systems (4.75) and (4.76), respectively.

Concerning Σ_s, recall Theorem 4.8, which with $\mathbf{A}_\mathrm{c,s} = \mathbf{C}_{(\lambda+1)^2}$ means to calculate the cycle sum with respect to $\mathbf{C}_{(\lambda+1)^2}$ only, i. e.

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

Regarding Σ_u, recall Theorem 4.15, which with $\mathbf{A}_\mathrm{c,u} = \mathbf{C}_{(\lambda+1)^3}$ amounts to determine the cycle sum regarding $\mathbf{C}_{(\lambda+1)^3}$ only. As with the degree $d_2 = 3$ and for some least $l \in \mathbb{N}$

$$2^l > d_2 > 2^{l-1} \quad \Longrightarrow \quad 4 > 3 > 2$$

it follows that the period of $(\lambda+1)^3$ is $t_3 = 4$ and

$$\Sigma_\mathrm{u} = \frac{2^3}{4}[4] = 2[4]\,.$$

Superposition of the cycle sums Σ_s and Σ_u yields the cycle sum of the overall inhomogeneous LMS

$$\begin{aligned}\Sigma \;&=\; \Sigma_\mathrm{u}\Sigma_\mathrm{s} = 2[4]\big(2[1] \dot{+} 1[2]\big) = \big(2[4]2[1] \dot{+} 2[4]1[2]\big) \\ &=\; 2\cdot 2\,\gcd(1,4)\,[\mathrm{lcm}(1,4)] \dot{+} 1\cdot 2\,\gcd(2,4)\,[\mathrm{lcm}(2,4)] = 4[4] \dot{+} 4[4] = 8[4]\,.\end{aligned}$$

Finally, the nilpotent subsystem $\mathbf{A}_\mathrm{n} = 0$ implies a null tree, which attached to each state in these 8 cycles of length 4, results in the state graph given in Figure 4.7.

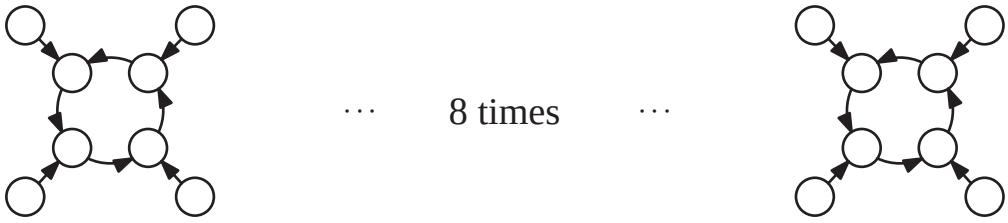


Figure 4.7: State graph of the inhomogeneous LMS of order 4 analyzed in Example 4.3.4

Conclusion

In this chapter, a method for analyzing the state interconnection structure within state spaces of autonomous linear dynamic systems over finite fields, so-called linear modular system (LMS), is

developed. The analysis method is based on the inspection of the elementary divisor polynomials, which are invariant under similarity transforms. When examining how the state space decomposes into subspaces, in particular into subspaces with periodic states, the period of these polynomials, which is a characteristic integral number common to all polynomials over a finite field, is shown to be decisive. Refraining from finite ring theory and setting up the theoretical development on a fundamental level of linear algebra and simple combinatorics only, the main theorem on the decomposition of the state space of a linear dynamic system into periodic subspaces is derived. The main outcome is a new criterion which allows to determine all cycles in length and number, and further, its respective periodic states, a result that can be applied in a straight-forward manner on automata modeled as LMS. It turns out that periodic transition behavior occurs already in the case of linear automata, hence, it is a linear phenomenon and is not to be confused with limit cycles as are encountered within non-linear continuous time systems.

A further result refers to the non-periodic elementary divisor polynomials, which correspond to nilpotent companion matrices. Again, these polynomials comprise the information necessary for determining the state interconnection structure within the associated non-periodic subspaces the state graph of which is a tree. Employing particular singular inverses a constructive procedure for deriving this state graph is presented, which is as before based on fundamental linear algebra only. By connecting the former results the structural analysis of autonomous LMS is rendered possible and verified in examples.

In an extension of the theory derived so far, affine-linear autonomous dynamic systems over finite fields (called inhomogeneous LMS) are concerned. Two conditions are deduced which state whether an inhomogeneous LMS can be reduced to a linear one by a coordinate transform in form of a state translation. If these conditions are fulfilled then the state graph can be constructed by resorting to the methods from above. If these conditions cannot be met, however, a theorem is proven that connects the periodicity of the states in the respective subspace with the period of the corresponding elementary divisor polynomial of the dynamics matrix of the inhomogeneous LMS. The combination of all results grants efficient means for a structural analysis of autonomous inhomogeneous LMS in general, as is illustrated in the closing part of this chapter.

Chapter 5

Synthesis of Linear Systems over Finite Fields

In the last chapter, for state space models that are autonomous linear dynamic systems over a finite field, conditions were presented by means of which the state space can be decomposed into subspaces whose states, typically, are periodic or correspond to tree states; both indicating a respective structure in the state graph.

Regarding non-autonomous systems, inputs are at one's disposal which can be used for controlling the state evolution. Further equipped with knowledge about the current state — provided by measurement, for example — the input can be related to an appropriate function of the state, a so-called (static) control law, in order to synthesize desired system properties in a feedback control loop. By virtue of a control law the closed-loop system is rendered autonomous. As a linear system remains linear under linear state feedback, consequently, the resulting autonomous closed-loop system again can be analyzed with the methods presented in Chapter 4. If the initial point is a certain closed-loop behavior then a usual task is to design a control that ensures this desired behavior. Thus naturally, the notion of controllability comes to the fore.

If the purpose of control is to guarantee certain closed-loop properties then a natural question is to ask for criteria about the existence of a suitable state feedback, and subsequently, how this suitable control law can be chosen. For linear continuous systems Rosenbrock's control structure theorem addresses the existence problem by relating the (desired) closed-loop invariant polynomials with the (control-invariant) controllability indices [Wol74, Kuč91]. Thus, Rosenbrock's control structure theorem is of particular value when the goal of feedback synthesis is to fit the closed-loop system with desired elementary divisor polynomials, which has already been shown sufficient for imposing a specific cycle sum on an LMS in Chapter 4. Since the outcome is an existence statement, the actual feedback law still has to be derived. For specifying invariant polynomials, image domain methods are well-known to be the suitable tool in the continuous world [Kuč91, Ant98, DH01]. To

this end, the $\mathcal{A}$-transform introduced in Chapter 2 is worked out for an adaption of the polynomial approach onto systems over finite fields for the first time. The result is an algorithm that allows to synthesize a state linear feedback for imposing a set of desired elementary divisor polynomials on the closed-loop system so as to obtain a closed-loop state graph comprising desired structural elements (i. e. states of certain periods, particular null tree). Expressed in a more formal way, this algorithm solves the following control problem:

Definition 5.1 (Cycle Sum Synthesis Problem (CSSP))
Given an LMS as in Definition 4.1 with measurable state. Design a linear state feedback such that the closed-loop LMS shows a specified cycle sum. □

The chapter is organized as follows: Basic notions as controllability of an LMS, controllability indices, and the controllability companion form (CCF) are presented in Section 5.1. The main contribution of this chapter is represented by Section 5.2 which develops a method for synthesizing a state feedback controller in an image domain. By invoking basics from the polynomial approach, a polynomial matrix fraction representation of the closed-loop transfer matrix is derived that ensures a specified periodic behavior. The result is a synthesis algorithm yielding the respective state feedback matrix. The chapter ends with an outlook of how to integrate a non-controllable part of the system and gives an illustration of the presented method in an example.

5.1 Controllability of an LMS

The property of controllability is a key prerequisite when considering control systems.

Definition 5.2 (Controllability)
An LMS of order n is l-controllable iff for all ordered pairs of states $(\mathbf{x}_1, \mathbf{x}_2)$, $\mathbf{x}_1, \mathbf{x}_2 \in \mathbb{F}_q^n$, the system can be driven (steered) from state $\mathbf{x}_1$ to state $\mathbf{x}_2$ in l steps. An LMS is controllable iff it is l-controllable for some l. □

In order to establish an easy criterion for checking controllability, resolve the recursion within the state equation (4.1) of an LMS according to Definition 4.1 so as to obtain its solution

$$\mathbf{x}(k) = \mathbf{A}^k \mathbf{x}(0) + \sum_{i=0}^{k-1} \mathbf{A}^{k-1-i} \mathbf{B} \mathbf{u}(i)\,. \tag{5.1}$$

In light of Definition 5.2 rewrite equation (5.1) in the form

$$\left(\mathbf{B}, \mathbf{AB}, \ldots, \mathbf{A}^{k-1}\mathbf{B}\right)\left(\mathbf{u}^{\mathrm{T}}(0), \ldots, \mathbf{u}^{\mathrm{T}}(k-1)\right)^{\mathrm{T}} = \mathbf{x}(k) - \mathbf{A}^k \mathbf{x}(0) \tag{5.2}$$

which indicates that an input sequence $\mathbf{u}(0),\ldots,\mathbf{u}(k-1)$ that drives an arbitrary state $\mathbf{x}(0)$ to an other arbitrary state $\mathbf{x}(k)$ in k steps (steering problem) can only be found if[1]

$$\mathrm{Im}(\mathbf{B},\mathbf{AB},\ldots,\mathbf{A}^{k-1}\mathbf{B}) = \mathbb{F}_q^n\,.$$

Furthermore, applying the theorem of Cayleigh-Hamilton, Theorem 4.1, on $\mathbf{A}$ yields that any column vector of some matrix $\mathbf{A}^k$ for $k \geq n$ can be expressed as some linear combination of corresponding column vectors of matrices $\mathbf{A}^i$ with $i < n$. Hence, any state can be reached in at most n steps, and a controllability criterion can be stated which is in full accordance with the well-known result in the continuous case.

Theorem 5.1 (Controllability Criterion)
An LMS of order n is l-controllable iff the matrix $(\mathbf{B},\mathbf{AB},\ldots,\mathbf{A}^{l-1}\mathbf{B}) \in \mathbb{F}_q^{n\times lm}$ has (full) rank n. □

Definition 5.3 (Controllability Matrix)
Given an LMS of order n. The matrix $(\mathbf{B},\mathbf{AB},\ldots,\mathbf{A}^{n-1}\mathbf{B}) \in \mathbb{F}_q^{n\times nm}$ is called controllability matrix of the LMS. □

Under assumption of controllability and by choosing new coordinates, the state equation (4.1) of an LMS can be transformed into the so-called controllability companion form.

5.1.1 Controllability Matrix and Controllability Indices

Given controllability, as per Theorem 5.1, a reduced controllability matrix $\mathbf{L} \in \mathbb{F}_q^{n\times n}$ of an LMS can be determined by choosing n linearly independent column vectors from the controllability matrix in Definition 5.3. These linearly independent column vectors are chosen in a way such that the appendant powers of $\mathbf{A}$ are minimal, see [Wol74]. This procedure yields the invertible matrix

$$\mathbf{L} = \left(\mathbf{b}_1,\ldots,\mathbf{A}^{c_1-1}\mathbf{b}_1,\mathbf{b}_2,\ldots,\mathbf{A}^{c_2-1}\mathbf{b}_2,\ldots,\mathbf{b}_m,\ldots\ \mathbf{A}^{c_m-1}\mathbf{b}_m\right), \tag{5.3}$$

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

Definition 5.4 (Controllability Indices)
Let the reduced controllability matrix $\mathbf{L} \in \mathbb{F}_q^{n\times n}$ of an LMS be given as in equation (5.3). The $i = 1,\ldots,m$ numbers $c_i \in \mathbb{N}$ are called controllability indices. □

[1] Given solvability, an appropriate generalized inverse matrix according to Appendix D is given by a matrix whose column space is the orthogonal complement space of $(\mathbf{B},\mathbf{AB},\ldots,\mathbf{A}^{k-1}\mathbf{B})$ — see the discussion in Section 5.2.6. For a method that employs a deadbeat-like feedback for solving the steering problem refer to the example in Appendix E.

[2] Without loss of generality, the column vectors of the input matrix $\mathbf{B}$ can be assumed linearly independent since, otherwise, the inputs would depend on each other which contradicts liberality in input choice.

Referring to [Wol74] again, some important properties of controllability indices shall be listed in the following theorem.

Theorem 5.2 (Properties of Controllability Indices)
Let c_i, $i = 1,\ldots,m$, be the controllability indices with respect to an LMS of order n. Then the following properties hold:

- the set of controllability indices is unique,
- the set of controllability indices is invariant with respect to a change of state coordinates,
- the LMS is controllable iff $\sum_{i=1}^{m} c_i = n$. □

5.1.2 The Controllability Companion Form

For controllable LMS, the state equation (4.1) can be transformed into a particular form by a change of state coordinates $\mathbf{x}$ using other characteristic coordinates $\mathbf{x}^{\mathrm{c}} = \mathbf{Q}\mathbf{x}$. The calculation of the transformation matrix $\mathbf{Q} \in \mathbb{F}_q^{n\times n}$ is based on the reduced controllability matrix $\mathbf{L}$ from (5.3) and its associated $i = 1,\ldots,m$ controllability indices c_i. The resulting state equation is called controllability companion form (CCF) [Wol74, Ant98].

Definition 5.5 (Controllability Companion Form (CCF))
An LMS of order n with m inputs is represented in controllability companion form (CCF) iff its state equation reads

$$\mathbf{x}^{\mathrm{c}}(k+1) = \mathbf{A}^{\mathrm{c}}\mathbf{x}^{\mathrm{c}}(k) + \mathbf{B}^{\mathrm{c}}\mathbf{u}(k), \quad \mathbf{A}^{\mathrm{c}} \in \mathbb{F}_q^{n\times n}, \mathbf{B}^{\mathrm{c}} \in \mathbb{F}_q^{n\times m}, \tag{5.4}$$

$$\mathbf{A}^{\mathrm{c}} = \begin{pmatrix} \mathbf{A}^{\mathrm{c}}_{11} & \mathbf{A}^{\mathrm{c}}_{12} & \cdots & \mathbf{A}^{\mathrm{c}}_{1m} \\ \mathbf{A}^{\mathrm{c}}_{21} & \mathbf{A}^{\mathrm{c}}_{22} & \cdots & \mathbf{A}^{\mathrm{c}}_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{A}^{\mathrm{c}}_{m1} & \mathbf{A}^{\mathrm{c}}_{m2} & \cdots & \mathbf{A}^{\mathrm{c}}_{mm} \end{pmatrix}, \quad \mathbf{A}^{\mathrm{c}}_{ii} = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ x & x & x & \cdots & x \end{pmatrix}, \quad \mathbf{A}^{\mathrm{c}}_{ij,i\neq j} = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 0 \\ x & x & x & \cdots & x \end{pmatrix},$$

$$\mathbf{B}^{\mathrm{c}} = \begin{pmatrix} \mathbf{B}^{\mathrm{c}}_1 \\ \mathbf{B}^{\mathrm{c}}_2 \\ \vdots \\ \mathbf{B}^{\mathrm{c}}_m \end{pmatrix}, \quad \mathbf{B}^{\mathrm{c}}_i = \begin{pmatrix} 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & \cdots & b^{\mathrm{c}}_{c_i i} & x & \cdots & x \end{pmatrix}, \quad b^{\mathrm{c}}_{c_i i} = 1$$

where $\mathbf{A}^{\mathrm{c}}_{ij} \in \mathbb{F}_q^{c_i\times c_j}$, $\mathbf{B}^{\mathrm{c}}_i \in \mathbb{F}_q^{c_i\times m}$ and $b^{\mathrm{c}}_{c_i i}$ is the element in the c_i-th row and i-th column of each matrix $\mathbf{B}^{\mathrm{c}}_i$, $i, j = 1,\ldots,m$. Moreover, any symbol "x" represents an arbitrary number in $\mathbb{F}_q$. □

The non-determined rows within the system in CCF can be concentrated in two matrices,

$$\mathbf{A}_\sigma^{\mathrm{c}} := \begin{pmatrix} \mathrm{row}_{\sigma_1}(\mathbf{A}^{\mathrm{c}}) \\ \mathrm{row}_{\sigma_2}(\mathbf{A}^{\mathrm{c}}) \\ \vdots \\ \mathrm{row}_{\sigma_m}(\mathbf{A}^{\mathrm{c}}) \end{pmatrix}, \quad \mathbf{B}_\sigma^{\mathrm{c}} := \begin{pmatrix} \mathrm{row}_{\sigma_1}(\mathbf{B}^{\mathrm{c}}) \\ \mathrm{row}_{\sigma_2}(\mathbf{B}^{\mathrm{c}}) \\ \vdots \\ \mathrm{row}_{\sigma_m}(\mathbf{B}^{\mathrm{c}}) \end{pmatrix} = \begin{pmatrix} 1 & x & x & \cdots & x \\ 0 & 1 & x & \cdots & x \\ 0 & 0 & 1 & \cdots & x \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix}, \tag{5.5}$$

in which $\sigma_i := \sum_{j=1}^{i} c_j$, $i = 1, \ldots, m$ and the expression $\mathrm{row}_i(.)$ denotes the i-th row of a matrix. Both matrices will be needed in Section 5.2.3.

The question of which matrix to choose for transforming an arbitrary controllable system into the representation in CCF is answered in the next theorem.

Theorem 5.3 (CCF Transformation Matrix)
Let an LMS of order n with m inputs be controllable with $i = 1, \ldots, m$ controllability indices c_i and $\sigma_i := \sum_{j=1}^{i} c_j$, $i = 1, \ldots, m$. Furthermore, let $\mathbf{L}^{-1} \in \mathbb{F}_q^{n \times n}$ denote the inverse of the respective reduced controllability matrix. Then a change of state coordinates $\mathbf{x}^{\mathrm{c}} = \mathbf{Q}\,\mathbf{x}$ by virtue of the matrix

$$\mathbf{Q} = \begin{pmatrix} \mathbf{q}_1^{\mathrm{T}} \\ \mathbf{q}_1^{\mathrm{T}}\mathbf{A} \\ \vdots \\ \mathbf{q}_1^{\mathrm{T}}\mathbf{A}^{c_1-1} \\ \mathbf{q}_2^{\mathrm{T}} \\ \mathbf{q}_2^{\mathrm{T}}\mathbf{A} \\ \vdots \\ \mathbf{q}_2^{\mathrm{T}}\mathbf{A}^{c_2-1} \\ \vdots \\ \mathbf{q}_m^{\mathrm{T}}\mathbf{A}^{c_m-1} \end{pmatrix}, \quad \mathbf{q}_i^{\mathrm{T}} = \mathrm{row}_{\sigma_i}(\mathbf{L}^{-1}), \quad i = 1, \ldots, m \tag{5.6}$$

transforms the state equation into CCF with dynamics matrix $\mathbf{A}^{\mathrm{c}}$ and input matrix $\mathbf{B}^{\mathrm{c}}$ as per

$$\mathbf{A}^{\mathrm{c}} = \mathbf{Q}\,\mathbf{A}\,\mathbf{Q}^{-1}, \quad \mathbf{B}^{\mathrm{c}} = \mathbf{Q}\,\mathbf{B}, \tag{5.7}$$

respectively.[3] □

Remark 5.1 (Ordered Controllability Companion Form)
For facilitating the algorithm in Section 5.2.4 that solves the cycle sum synthesis problem in Definition 5.1 it is advisable to have the controllability indices in decreasing order. Without loss of

[3] For continuous systems, the matrix $\mathbf{L}$ often is ill-conditioned. Due to the numerical problems incurred, the calculation of $\mathbf{L}^{-1}$ usually is avoided. For matrices over finite fields such problems cannot arise.

generality, this property can easily be obtained by renaming the input vector entries in a manner such that the powers of $\mathbf{A}$ in the reduced controllability matrix (5.3) obey $c_1 \geq \ldots \geq c_m$.

Without renumbering of the inputs, the block matrices $\mathbf{A}^{\mathrm{c}}_{ij} \in \mathbb{F}_q^{c_i \times c_j}$ in $\mathbf{A}^{\mathrm{c}}$ can be reordered with respect to decreasing controllability indices by a respective permutation matrix $\mathbf{\Pi}$, as described in Appendix A. Note that a consequence of this procedure is that the input matrix transforms as well, that is, the new input matrix becomes $\mathbf{\Pi}\mathbf{B}^{\mathrm{c}}$. Hence, the matrix that corresponds to $\mathbf{B}^{\mathrm{c}}_{\sigma}$ is in general not upper triangular anymore. □

In light of this conceptual framework, a synthesis method for imposing a specific cycle sum on an LMS can be developed.

5.2 Synthesis in the Image Domain

Changing the elementary divisor polynomials, which is equivalent to changing the invariant polynomials of an LMS, is closely related to changing the eigenvalues of the system dynamics. From the theory of linear discrete time systems over the field of real numbers it is well-known that a change of eigenvalues of the system dynamics can be achieved by introducing a (static) linear state feedback.

5.2.1 Linear State Feedback and its Structural Constraints

In view of the controllability companion form and by linearity of the system to be controlled a first simple state feedback is a linear form[4]

$$\mathbf{u}(k) = \mathbf{K}\mathbf{x}(k)\,. \tag{5.8}$$

This leeds to the closed-loop state representation

$$\mathbf{x}(k+1) = (\mathbf{A}+\mathbf{B}\mathbf{K})\,\mathbf{x}(k) \tag{5.9}$$

in which the matrix $\mathbf{A}+\mathbf{B}\mathbf{K}$ is the closed-loop dynamics.

Remark 5.2
The influence of state feedback can be studied easily by considering the state space representation in CCF because any controllable LMS can be transformed into CCF. For this purpose, note that $\mathbf{B}^{\mathrm{c}}_{\sigma}$ is invertible, thus $\mathbf{B}^{\mathrm{c}}$ generally can be altered by right-multiplication with $(\mathbf{B}^{\mathrm{c}}_{\sigma})^{-1}$ such that the resulting product matrix chooses the i-th rows, $i = 1,\ldots,m$, from any feedback matrix to the right. Thus, the corresponding σ_i-th rows of the closed-loop dynamics matrix can be changed completely at choice. □

[4] which can be extended by an additional new input, of course

Therefore, the question arises whether or at least to which extent the closed-loop invariant polynomials can be chosen freely. This major question is answered by Rosenbrock's control structure theorem [Kai80, Ros70], which can be shown to apply to systems over finite fields as well.[5]

Theorem 5.4 (Rosenbrock's Control Structure Theorem)
Given a controllable LMS of order n with controllability indices $c_1 \geq \ldots \geq c_m$ and desired monic invariant polynomials $c_{i,\mathbf{K}} \in \mathbb{F}_q[\lambda]$ with $c_{i+1,\mathbf{K}} | c_{i,\mathbf{K}}$, $i = 1, \ldots, m-1$, and $\sum_{i=1}^{m} \deg(c_{i,\mathbf{K}}) = n$. Then a matrix $\mathbf{K} \in \mathbb{F}_q^{m \times n}$ exists such that $\mathbf{A} + \mathbf{BK}$ has the desired invariant polynomials $c_{i,\mathbf{K}}$ iff the inequalities

$$\sum_{i=1}^{k} \deg(c_{i,\mathbf{K}}) \geq \sum_{i=1}^{k} c_i, \quad k = 1, 2, \ldots, m \tag{5.10}$$

are satisfied. □

Rosenbrock's control structure theorem is of particular importance for the controller problem on hand because it entails a limit when focusing on maximal liberality in the choice of closed-loop invariant polynomials, that is, in the choice of a desired cycle sum. If the inequalities in (5.10) can be verified for a desired set of closed-loop invariant polynomials then an appropriate feedback matrix exists, which can be determined by a method, one is still free to choose.

5.2.2 Controller Design in the Image Domain — why?

On the face of it, pole placing methods cannot be applied since specifying invariant polynomials, generally, is a stronger requirement than specifying eigenvalues. Consequently, standard pole placing methods do not meet the requirements and some specific method for synthesizing a state feedback for MIMO-systems is necessary. A well-established method for systems over the field of real numbers is the parametric approach [Rop86, DH01]. In this approach, besides the closed-loop eigenvalues, the remaining degrees of freedom are used for specifying a linear combination of closed-loop eigenvectors, the so-called parameter vectors, with the purpose of achieving a particular closed-loop behavior.

However, parametric approach techniques turn out to be inapplicable if the control objective is to design a state feedback that fits an LMS with a set of invariant polynomials. This is due to the following peculiar reasons:

- In the parametric approach it is fundamental that the open-loop and closed-loop eigenvalues are distinct. Applying this approach to LMS would incur that the invariant polynomials in the open and the closed loop have to be different, which is a restrictive assumption in the framework of LMS.

[5] See remark in [Kai80, p. 517].

- The assignment of multiple eigenvalues, which would be indispensable for the realization of rather standard cycle sums (e. g. cycles of even length for a model over $\mathbb{F}_2$), proves to be cumbersome because the computation of chains of generalized eigenvectors is required.

- As eigenvalues of matrices over a finite field $\mathbb{F}_q$ are roots of some polynomial the notion of zeroes becomes important. These zeroes typically lie in some extension field of $\mathbb{F}_q$, the size of which deeply depends on the degree of the polynomial and of its factors. Moreover, these extension fields have no defining element in common [LN94]. This is a severe difference to the field of real numbers in which any polynomial in $\mathbb{R}[\lambda]$ can be factored into quadratic irreducible polynomials over $\mathbb{R}$ (see Definition 2.7). Hence, any zero of a polynomial in $\mathbb{R}[\lambda]$ lies in the corresponding extension field, which is the field of complex numbers $\mathbb{C}$ with unique defining element $i = \sqrt{-1}$. Conversely, such a uniform factorization is not possible for polynomials in $\mathbb{F}_q[\lambda]$ with the consequence that the computation of eigenvalues in the extension field of $\mathbb{F}_q$ entails enormous symbolical computation effort.[6]

- The structural theorem imposes realizability constraints on the invariant polynomials in the closed-loop system. Thus, observing these constraints via some suitable set of closed-loop invariant polynomials immediately yields the respective Smith form of the closed-loop dynamics. Once given the Smith form of the closed-loop dynamics, an appropriate image domain framework provides simple straight-forward methods for determining the suitable state feedback matrix.[7]

In view of these issues, image domain design techniques as in particular the polynomial approach, will be adapted for the state feedback synthesis of LMS.

5.2.3 The Polynomial Matrix Fraction of the Transfer Matrix

An image domain representation of an LMS can be obtained by resorting to the $\mathcal{A}$-transform introduced in Definition 2.24. In the image domain, the counterpart of the state equation (4.1) reads

$$a\mathbf{X}(a) = \mathbf{A}\mathbf{X}(a) + \mathbf{B}\mathbf{U}(a) + a\mathbf{x}(0) \tag{5.11}$$

in which capital letters in bold face with argument denote the respective $\mathcal{A}$-transformed variables. This representation directly leads to the $\mathcal{A}$-transform of the system state[8]

$$\mathbf{X}(a) = (a\mathbf{I} - \mathbf{A})^{-1}\big(\mathbf{B}\mathbf{U}(a) + a\mathbf{x}(0)\big)\,. \tag{5.12}$$

[6] Refer to Appendix C for an example.

[7] In the same manner, this statement holds true for the frequency domain with respect to continuous systems.

[8] Appendix F exposes how the inverse $\mathcal{A}$-transform can be used for determining the solution of the state equation.

The rational matrix $\mathbf{F}(a) = (a\mathbf{I} - \mathbf{A})^{-1}\mathbf{B}$ in equation (5.12) can be identified with the customary form of a transfer matrix since

$$\mathbf{X}(a)\Big|_{\mathbf{x}(0)=0} = \mathbf{F}(a)\,\mathbf{U}(a) = (a\mathbf{I} - \mathbf{A})^{-1}\mathbf{B}\mathbf{U}(a)\,. \tag{5.13}$$

Nevertheless, the interpretation of $\mathbf{F}(a)$ as a transfer matrix is of minor importance here. In the following, just a particular decomposition of the transfer matrix will be used since it prepares the ground for a simple method of setting the invariant polynomials of $\mathbf{A}+\mathbf{B}\mathbf{K}$, i. e. in the closed loop.

5.2.3.1 Fundamentals

The polynomial matrix method is based on a particular decomposition of the transfer matrix in (5.13). To this end, those notions and concepts of the polynomial matrix approach which are significant for the purpose here are recalled from [Wol74, Kuč91, Ant98], for convenience.

First the concepts of factors and primeness of polynomial matrices shall be introduced.

Definition 5.6 (Right Divisor and Left Divisor of a Polynomial Matrix)
Let $\mathbf{P}(a)$, $\mathbf{L}(a)$ and $\mathbf{R}(a)$ be polynomial matrices. If

$$\mathbf{P}(a) = \mathbf{L}(a)\,\mathbf{R}(a)$$

then $\mathbf{R}(a)$ and $\mathbf{L}(a)$ are called right divisor and left divisor of $\mathbf{P}(a)$, respectively. □

Definition 5.7 (Greatest Common Right (Left) Divisor of Polynomial Matrices)
Let $\mathbf{P}(a)$ and $\mathbf{Q}(a)$ be polynomial matrices. A greatest common right (left) divisor of the polynomial matrices $\mathbf{P}(a)$ and $\mathbf{Q}(a)$ is a common right (left) divisor which is a left (right) multiple of every common right (left) divisor of $\mathbf{P}(a)$ and $\mathbf{Q}(a)$. □

Definition 5.8 (Right-prime and Left-prime Polynomial Matrices)
Polynomial matrices with the same number of columns (rows) are termed right-prime (left-prime) if their greatest common right divisors (greatest common left divisors) are unimodular matrices. □

In order to state a less involved criterion for testing primality of polynomial matrices, a Bézout dentity can be derived for polynomial matrices over finite fields as well. The proof can be kept to the lines in [Kai80, p. 379].

Lemma 5.1 (Bézout Identity)
Let $\mathbf{P}(a)$ and $\mathbf{Q}(a)$ be polynomial matrices. Then $\mathbf{P}(a)$ and $\mathbf{Q}(a)$ are right-prime (left-prime) iff polynomial matrices $\mathbf{X}(a)$, $\mathbf{Y}(a)$ $\left(\overline{\mathbf{X}}(a),\, \overline{\mathbf{Y}}(a)\right)$ exist such that the equations

$$\mathbf{X}(a)\,\mathbf{P}(a) + \mathbf{Y}(a)\,\mathbf{Q}(a) = \mathbf{I} \quad \left(\mathbf{P}(a)\,\overline{\mathbf{X}}(a) + \mathbf{Q}(a)\,\overline{\mathbf{Y}}(a) = \mathbf{I}\right) \tag{5.14}$$

hold. □

Lemma 5.1 is the basis for deriving a controllability criterion that is based on the primality of polynomial matrices only, and renders the calculation of eigenvalues in some field extension unnecessary — the proof in [Ros70] applies also to the finite field case.

Theorem 5.5 (Controllability Criterion)
Let $\mathbf{A}$ be the dynamics matrix and $\mathbf{B}$ be the input matrix of an LMS. The LMS is controllable iff the polynomial matrices $(a\mathbf{I}-\mathbf{A})$ and $\mathbf{B}$ are left-prime. □

Definition 5.9 (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

$$\mathbf{R}(a)=\mathbf{N}(a)\,\mathbf{D}^{-1}(a)\quad\left(\mathbf{R}(a)=\bar{\mathbf{D}}^{-1}(a)\,\bar{\mathbf{N}}(a)\right) \tag{5.15}$$

in which the denominator matrices $\mathbf{D}(a)$, $\bar{\mathbf{D}}(a)$ and the numerator matrices $\mathbf{N}(a)$, $\bar{\mathbf{N}}(a)$ are polynomial matrices. □

Lemma 5.2 (Existence of a Polynomial Matrix Fraction)
For any rational matrix $\mathbf{R}(a)$ there exists a right-prime RPMF (left-prime LPMF). □

Consequently, any transfer matrix can be represented by some polynomial matrix fraction. In particular, the transfer matrix representation in (5.13) is a LPMF. Moreover, it is a left-prime LPMF iff the LMS is controllable. The proof of the following theorem, taken from [Kai80, p. 410], applies right away to the finite field case.

Lemma 5.3 (Generalized Bézout Identity)
Let a rational matrix $\mathbf{R}(a)$ be given in a right-prime RPMF and left-prime LPMF as per

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

Then polynomial matrices $\mathbf{X}(a)$, $\mathbf{Y}(a)$, $\tilde{\mathbf{X}}(a)$, and $\tilde{\mathbf{Y}}(a)$ exist such that

$$\begin{pmatrix}\bar{\mathbf{D}}(a) & \bar{\mathbf{N}}(a)\\ -\tilde{\mathbf{X}}(a) & \tilde{\mathbf{Y}}(a)\end{pmatrix}\begin{pmatrix}\bar{\mathbf{X}}(a) & -\mathbf{N}(a)\\ \bar{\mathbf{Y}}(a) & \mathbf{D}(a)\end{pmatrix}=\begin{pmatrix}\mathbf{I} & \mathbf{0}\\ \mathbf{0} & \mathbf{I}\end{pmatrix}. \tag{5.16}$$

Moreover, all block matrices in equation (5.16) are unimodular. □

Under the assumptions in Lemma 5.3 it follows that

$$\begin{pmatrix}\bar{\mathbf{D}}(a) & \bar{\mathbf{N}}(a)\\ \mathbf{0} & \mathbf{I}\end{pmatrix}\begin{pmatrix}\bar{\mathbf{X}}(a) & -\mathbf{N}(a)\\ \bar{\mathbf{Y}}(a) & \mathbf{D}(a)\end{pmatrix}=\begin{pmatrix}\mathbf{I} & \mathbf{0}\\ \bar{\mathbf{Y}}(a) & \mathbf{D}(a)\end{pmatrix} \tag{5.17}$$

which, with unimodularity of the matrix in the middle, implies similarity of

$$\begin{pmatrix} \bar{\mathbf{D}}(a) & \bar{\mathbf{N}}(a) \\ \mathbf{0} & \mathbf{I} \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} \mathbf{I} & \mathbf{0} \\ \bar{\mathbf{Y}}(a) & \mathbf{D}(a) \end{pmatrix}.$$

In view of the identity matrices comprised, the matrices from above again can be converted unimodularly. Hence, the matrices

$$\begin{pmatrix} \bar{\mathbf{D}}(a) & \mathbf{0} \\ \mathbf{0} & \mathbf{I} \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} \mathbf{I} & \mathbf{0} \\ \mathbf{0} & \mathbf{D}(a) \end{pmatrix}$$

are similar and the following theorem has been shown.

Theorem 5.6 (Invariant Polynomials of Denominator Matrices)
Let a rational matrix $\mathbf{R}(a)$ be given in right-prime RPMF and a left-prime LPMF. Then both denominator matrices have the same nonunity invariant polynomials. □

As a result, if the LPMF in equation (5.13) is left-prime then the corresponding right-prime RPMF have the same nonunity invariant polynomials. The next section presents a suchlike right-prime RPMF.

5.2.3.2 Polynomial Matrix Fraction for Systems in CCF

For LMS in controllability companion form (CCF), see equations (5.4) and (5.5), a right-prime RPMF can be determined in a closed analytical expression[9].

Theorem 5.7 (RPMF of the Transfer Matrix for a System in CCF)
Let the state equation of a controllable LMS of order n with m inputs and controllability indices $c_1, \ldots, c_m$ be given in controllability companion form according to equations (5.4) and (5.5). Then a right-prime RPMF of the transfer matrix $\mathbf{F}(a) = (a\mathbf{I} - \mathbf{A})^{-1}\mathbf{B} \in \mathbb{F}_q(a)^{n\times m}$ is

$$\mathbf{F}(a) = \mathbf{P}(a)\,\mathbf{D}^{-1}(a) \tag{5.18}$$

with the denominator matrix $\mathbf{D}(a) \in \mathbb{F}_q[a]^{m\times m}$ as per

$$\mathbf{D}(a) = (\mathbf{B}^{\mathrm{c}}_{\sigma})^{-1}\left(\mathbf{\Lambda}(a) - \mathbf{A}^{\mathrm{c}}_{\sigma}\mathbf{P}(a)\right), \tag{5.19}$$

[9] referring to the *structure theorem* in [Wol74, p. 196],[Ant98, p. 291]

the numerator matrix $\mathbf{P}(a) \in \mathbb{F}_q[a]^{n\times m}$ and the diagonal matrix $\mathbf{\Lambda}(a) \in \mathbb{F}_q[a]^{m\times m}$ given as

$$\mathbf{P}(a) = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ a & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ a^{c_1-1} & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & a^{c_2-1} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & a^{c_m-1} \end{pmatrix}, \quad \mathbf{\Lambda}(a) = \begin{pmatrix} a^{c_1} & 0 & \cdots & 0 \\ 0 & a^{c_2} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & a^{c_m} \end{pmatrix}, \tag{5.20}$$

all operations to be understood over $\mathbb{F}_q$. □

Proof The correctness of equality (5.19) can be checked easily by multiplying with the respective denominator matrices and appealing to the shifting property of the nilpotent blocks in $\mathbf{A}_\sigma^{\mathrm{c}}$ — the rest is straight-forward. The matrices $\mathbf{P}(a)$ and $\mathbf{D}(a)$ are right-prime since Theorem 5.1 is fulfilled with the choice of

$$\mathbf{X}(a) = \begin{pmatrix} 1 & 0 & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & \cdots & 0 & 1 & 0 & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & \cdots & \cdots & 0 & 1 & 0 & \cdots \end{pmatrix}, \quad \mathbf{Y}(a) = \mathbf{0},$$

where the $i = 1,\ldots,m$ unity entries in the matrix $\mathbf{X}(a)$ are in the i-th row and ρ_i-th column, $\rho_i := 1 + \sum_{j=0}^{i-1} c_j$. □

In light of Remark 5.2, for an LMS in CCF which is subject to an extended linear state feedback of the form

$$\mathbf{u}(k) = \mathbf{K}\,\mathbf{x}(k) + \mathbf{w}(k) \tag{5.21}$$

it is obvious that the CCF-structure is preserved. This leads to

Corollary 5.1 (RPMF of the Closed-Loop Transfer Matrix for a System in CCF)
Let the transfer matrix of an n-th order controllable LMS with m inputs regarding the controllability companion form be given as per Theorem 5.7. Furthermore, assume that this LMS is subject to an (extended) state feedback law in CCF

$$\mathbf{u}(k) = \mathbf{K}^{\mathrm{c}}\,\mathbf{x}^{\mathrm{c}}(k) + \mathbf{w}(k)\,, \tag{5.22}$$

where $\mathbf{K}^{\mathrm{c}} = \mathbf{K}\,\mathbf{Q}^{-1} \in \mathbb{F}_q^{m\times n}$ is the feedback matrix with respect to the transform $\mathbf{x}^{\mathrm{c}} = \mathbf{Q}\,\mathbf{x}$ into CCF. Then with the denotation in (5.20) a right-prime RPMF of the closed-loop transfer matrix reads

$$\mathbf{F}_{\mathbf{K}}(a) = \mathbf{P}(a)\,\mathbf{D}_{\mathbf{K}}^{-1}(a) \tag{5.23}$$

with denominator matrix $\mathbf{D}_{\mathbf{K}}(a) \in \mathbb{F}_q^{m\times m}$ according to

$$\mathbf{D}_{\mathbf{K}}(a) = (\mathbf{B}_\sigma^{\mathrm{c}})^{-1}\big(\mathbf{\Lambda}(a) - \mathbf{A}_{\sigma,\mathbf{K}}^{\mathrm{c}}\mathbf{P}(a)\big), \quad \mathbf{A}_{\sigma,\mathbf{K}}^{\mathrm{c}} = \mathbf{A}_\sigma^{\mathrm{c}} + \mathbf{B}_\sigma^{\mathrm{c}}\mathbf{K}^{\mathrm{c}}, \tag{5.24}$$

in which $\mathbf{A}_{\sigma,\mathbf{K}}^{\mathrm{c}} \in \mathbb{F}_q^{m\times n}$ can be altered arbitrarily by the feedback matrix $\mathbf{K}^{\mathrm{c}}$. □

5.2.3.3 Properties

The main property of the right-prime RPMF for the system in the closed loop as given in Corollary 5.1 follows from Theorem 5.6 and is summarized in the following theorem.

Theorem 5.8 (Nonunity Invariant Polynomials of $a\mathbf{I}-(\mathbf{A}+\mathbf{BK})$ and $\mathbf{D}_{\mathbf{K}}(a)$ Coincide)
Let the state equation of a controllable LMS be given in controllability companion form according to equations (5.4) and (5.5). Moreover, let $\mathbf{D}_{\mathbf{K}}(a)$ denote the denominator matrix of the closed-loop transfer matrix in the right-prime RPMF as per Corollary 5.1. Then the polynomial matrices $a\mathbf{I}-(\mathbf{A}+\mathbf{BK})$ and $\mathbf{D}_{\mathbf{K}}(a)$ have the same nonunity invariant polynomials. □

As a result, desired closed-loop invariant polynomials can be synthesized by means of $\mathbf{D}_{\mathbf{K}}(a)$ which determines the feedback matrix $\mathbf{K}$ uniquely. Thus, by finding an adequate $\mathbf{D}_{\mathbf{K}}(a)$ the cycle sum synthesis problem (CSSP) as stated in Definition 5.1 can be solved.

In order to be in accordance with the notation in the literature, the column degree and the highest column degree coefficient matrix shall be defined [Wol74, Ant98].

Definition 5.10 (Column Degree of a Polynomial Matrix)
Let $\mathbf{M}(a) \in \mathbb{F}_q[a]^{n\times m}$ be an arbitrary polynomial matrix. The degree of the highest degree monomial in the indeterminate a regarding the i-th column vector of $\mathbf{M}(a)$ is termed the i-th column degree of $\mathbf{M}(a)$. The $i = 1,\ldots,m$ column degrees are denoted by $\partial_{\mathrm{c},i}(\mathbf{M})$.[10] □

Definition 5.11 (Highest Column Degree Coefficient Matrix)
Let $\mathbf{M}(a) \in \mathbb{F}_q[a]^{n\times m}$ be an arbitrary polynomial matrix. The highest column degree coefficient matrix $\mathbf{\Gamma}_{\mathrm{c}}(\mathbf{M}) \in \mathbb{F}_q^{n\times m}$ is the matrix made up of coefficients with respect to the highest degree a terms in each column of $\mathbf{M}$. □

In equation (5.23) the structure of the denominator matrix $\mathbf{D}_{\mathbf{K}}(a)$ of the closed-loop system transfer matrix $\mathbf{F}(a) = \mathbf{P}(a)\,\mathbf{D}_{\mathbf{K}}^{-1}(a)$ in RPMF reveals that the following properties are invariant under linear state feedback [Wol74].

[10] The subscript "c" is to emphasize column degrees, in contrast to row degrees.

Theorem 5.9 (Invariants under Linear State Feedback)
Let an LMS of order n with m inputs be subject to linear state feedback according to (5.21). Resorting to the denotation introduced in Corollary 5.1 and equation (5.24) the following terms are invariant under linear state feedback:

1. the numerator matrix $\mathbf{P}(a)$,
2. the $i = 1, \ldots, m$ column degrees of $\mathbf{D}(a)$, i. e. $\partial_{\mathrm{c},i}(\mathbf{D}_\mathbf{K}) = \partial_{\mathrm{c},i}(\mathbf{D})$,
3. the highest column degree coefficient matrix of $\mathbf{D}(a)$, i. e. $\mathbf{\Gamma}_\mathrm{c}(\mathbf{D}_\mathbf{K}) = \mathbf{\Gamma}_\mathrm{c}(\mathbf{D})$. □

Remark 5.3
By simple inspection, the $i = 1, \ldots, m$ controllability indices c_i can be identified with the control invariant column degrees $\partial_{\mathrm{c},i}(\mathbf{D})$, accordingly

$$\partial_{\mathrm{c},i}(\mathbf{D}) = c_i, \quad i = 1, \ldots, m \tag{5.25}$$

and for an LMS in CCF the matrix

$$\mathbf{\Gamma}_\mathrm{c}(\mathbf{D}) = (\mathbf{B}_\sigma^\mathrm{c})^{-1} \tag{5.26}$$

is the invariant highest column degree coefficient matrix.[11] □

5.2.4 Synthesis Algorithm

Solving the CSSP, see Definition 5.1, means to find an adequate state feedback matrix $\mathbf{K}$ for fitting the respective LMS with $i = 1, \ldots, m$ desired invariant polynomials $c_{i,\mathbf{K}}(a)$ in the closed loop. This amounts to determine a denominator matrix $\mathbf{D}_\mathbf{K}(a)$ that meets the following conditions:

C1) The $i = 1, \ldots, m$ invariant polynomials of $\mathbf{D}_\mathbf{K}(a)$ coincide with the desired closed-loop invariant polynomials $c_{i,\mathbf{K}}(a)$.

C2) The column degrees of $\mathbf{D}_\mathbf{K}(a)$ equal the controllability indices c_i of the LMS.

C3) The highest column degree coefficient matrix regarding $\mathbf{D}_\mathbf{K}(a)$ equals $(\mathbf{B}_\sigma^\mathrm{c})^{-1}$.

[11] The reader who is familiar with the polynomial approach recognizes by invertibility of $\mathbf{\Gamma}_\mathrm{c}(\mathbf{D})$ that the denominator matrix $\mathbf{D}(a)$ is column reduced.

5.2.4.1 Comments on the Algorithm

The following algorithm extends an algorithm presented in [Kuč91, p. 123]. However, the following algorithm does not depend on the solution of a Diophantine equation. Instead, it employs Corollary 5.1, that is a transform of the state equation into CCF.[12] In order to keep the algorithm simple, an LMS in ordered controllability companion form according to Remark 5.1 will be assumed, i. e. the controllability indices are arranged in decreasing order $c_1 \geq \ldots \geq c_m$.

The algorithm begins with checking realizability first, which means that the inequalities (5.10) in Rosenbrock's control structure theorem, Theorem 5.4, have to be verified for the $i = 1,\ldots,m$ desired closed-loop invariant polynomials $c_{i,\mathbf{K}}(a)$. As these are invariant polynomials, the choice of polynomials is restricted to $c_{i+1,\mathbf{K}}(a)|c_{i,\mathbf{K}}(a)$ for $i = 1,\ldots,m-1$ and $\sum_{i=1}^{m} \deg(c_{i,\mathbf{K}}(a)) = n$.

Given realizability, a denominator matrix of the form

$$\mathbf{D}^{\star}(a) = \operatorname{diag}(c_{1,\mathbf{K}}(a),\ldots,c_{m,\mathbf{K}}(a)) \tag{5.27}$$

appears to be a promising start because this matrix already covers the conditions C1 and C3 — obviously, condition C1 is satisfied. Condition C3 is fulfilled since the polynomials $c_{i,\mathbf{K}}(a)$ are monic which implies $\mathbf{\Gamma}_{\mathrm{c}}(\mathbf{D}^{\star}) = \mathbf{I}_m$. The latter property turns out sufficient for covering condition C3 as with the unimodular matrix $(\mathbf{B}_{\sigma}^{\mathrm{c}})^{-1}$ the inspection of the polynomial matrix

$$\mathbf{D}_{\mathbf{K}}^{\star}(a) := \mathbf{\Lambda}(a) - (\mathbf{A}_{\sigma}^{\mathrm{c}} + \mathbf{B}_{\sigma}^{\mathrm{c}}\mathbf{K}^{\mathrm{c}})\,\mathbf{P}(a) \tag{5.28}$$

in lieu of $\mathbf{D}_{\mathbf{K}}(a)$ is equivalent because $\mathbf{D}_{\mathbf{K}}^{\star}(a)$ and $\mathbf{D}_{\mathbf{K}}(a) = (\mathbf{B}_{\sigma}^{\mathrm{c}})^{-1}\mathbf{D}_{\mathbf{K}}^{\star}(a)$ have the same invariant polynomials. Consequently, the task with respect to condition C3 turns into generating $\mathbf{D}_{\mathbf{K}}^{\star}(a)$ in place of $\mathbf{D}_{\mathbf{K}}(a)$, and now the goal is to achieve a highest column degree coefficient matrix

$$\mathbf{\Gamma}_{\mathrm{c}}(\mathbf{D}_{\mathbf{K}}^{\star}) = \mathbf{I}_m\,, \tag{5.29}$$

which is in accordance with the matrix from the start as $\mathbf{\Gamma}_{\mathrm{c}}(\mathbf{D}^{\star}) = \mathbf{I}_m$.

In order to fulfill condition C2, the column degrees in $\mathbf{D}^{\star}(a)$ are adapted by performing suitable elementary row and column operations on $\mathbf{D}^{\star}(a)$; being unimodular operations they do not change the invariant polynomials. By construction of $\mathbf{D}^{\star}(a)$ in virtue of decreasing polynomial degrees it is clear that column degrees $\partial_i(\mathbf{D}^{\star}(a)) > c_i$ for some increasing number $i = 1,2,\ldots$ can be reduced by raising the column degrees $\partial_j(\mathbf{D}^{\star}(a)) < c_j$ for some decreasing number $j = m, m-1,\ldots$, the possibility of which is ensured by Rosenbrock's control structure theorem.

In the course of these unimodular transforms the resulting polynomial matrix $\mathbf{D}^{++}(a)$ may finally have a highest column degree coefficient matrix $\mathbf{\Gamma}_{\mathrm{c}}(\mathbf{D}^{++}) \neq \mathbf{I}_m$. Therefore, a multiplication with $(\mathbf{\Gamma}_{\mathrm{c}}(\mathbf{D}^{++}))^{-1}$ may be necessary so as to be conform to equation (5.29), expressing the adapted version of condition C3.

[12] The calculation of the transformation matrix $\mathbf{Q} \in \mathbb{F}_q^{n\times n}$ by inversion of $\mathbf{L} \in \mathbb{F}_q^{n\times n}$, see Theorem 5.3, does not incur numerical problems — unlike in the real case $\mathbf{L} \in \mathbb{R}^{n\times n}$, where $\mathbf{L}$ often emerges to be ill-conditioned.

5.2.4.2 The Algorithm

The last section accounted for the following algorithm for solving the CSSP [RS03, Sch02]

Theorem 5.10 (Synthesis Algorithm for Solving CSSP)
Let a controllable LMS be given in ordered CCF with controllability indices c_i, $i = 1,\ldots,m$. Let $c_{i,\mathbf{K}} \in \mathbb{F}_q[a]$, $i = 1,\ldots,m$, be desired invariant polynomials with $c_{j+1,\mathbf{K}} | c_{j,\mathbf{K}}$, $j = 1,\ldots,m-1$ and $\sum_{i=1}^{m} \deg(c_{i,\mathbf{K}}) = n$.

If possible, the following steps yield a denominator matrix $\mathbf{D_K}(a)$ for solving the CSSP:

1. Check Rosenbrock's control structure theorem, Theorem 5.4, for c_i and $c_{i,\mathbf{K}}(a)$.
   - **if** the inequalities (5.10) are fulfilled **then**
     goto step 2,
   - **else**
     - **return** "A suitable denominator matrix $\mathbf{D_K}(a)$ does not exist."
2. Define $\mathbf{D}^\star(a) := \mathrm{diag}(c_{1,\mathbf{K}},\ldots,c_{m,\mathbf{K}})$.
3. Examine the column degrees of $\mathbf{D}^\star(a)$.
   - **if** the column degrees of $\mathbf{D}^\star(a)$ equal the ordered list of controllability indices **then goto** step 6.
   - **else**
     - Detect the first column of $\mathbf{D}^\star(a)$ which differs from the ordered list of controllability indices, starting with column 1. Denote this column $\mathrm{col}_u(\mathbf{D}^\star)$. $(\deg(\mathrm{col}_u(\mathbf{D}^\star)) > c_u)$
     - Detect the first column of $\mathbf{D}^\star(a)$ which differs from the ordered list of controllability indices, starting with column m. Denote this column $\mathrm{col}_d(\mathbf{D}^\star)$. $(\deg(\mathrm{col}_d(\mathbf{D}^\star)) < c_d)$
4. Adapt the column degrees of $\mathbf{D}^\star(a)$ by unimodular transformations.
   - Multiply $\mathrm{row}_d(\mathbf{D}^\star)$ by a and add the result to $\mathrm{row}_u(\mathbf{D}^\star)$ in $\mathbf{D}^\star(a) \rightarrow \mathbf{D}^+(a)$.
   - **if** $\deg(\mathrm{col}_u(\mathbf{D}^+)) = \deg(\mathrm{col}_u(\mathbf{D}^\star)) - 1$ **then**
     - $\mathbf{D}^+(a) \rightarrow \mathbf{D}^{++}(a)$ and **goto** step 5.
   - **else**
     - Define $r := \deg(\mathrm{col}_u(\mathbf{D}^\star)) - \deg(\mathrm{col}_d(\mathbf{D}^\star)) - 1$

– Multiply $\mathrm{col}_d(\mathbf{D}^+)$ by a^r and subtract the result from $\mathrm{col}_u(\mathbf{D}^+)$ in $\mathbf{D}^+(a) \rightarrow \mathbf{D}^{++}(a)$.

5. Generate $\mathbf{\Gamma}_c(\mathbf{D}^{++})$ and set $\mathbf{D}^\star(a) = (\mathbf{\Gamma}_c(\mathbf{D}^{++}))^{-1}\mathbf{D}^{++}(a)$ and **goto** step 3

6. $\mathbf{D}^\star_\mathbf{K}(a) := \mathbf{D}^\star(a)$ and **return** $\mathbf{D}^\star_\mathbf{K}(a)$

If a closed-loop denominator matrix $\mathbf{D}^\star_\mathbf{K}(a)$ is returned then a linear state feedback matrix $\mathbf{K}$ exists that solves the CSSP. □

It only remains to show that the feedback matrix $\mathbf{K}$ can be computed from the closed-loop denominator matrix $\mathbf{D}^\star_\mathbf{K}(a)$, uniquely. To this end, recall equation (5.24), that is

$$\mathbf{B}^c_\sigma \mathbf{D}_\mathbf{K}(a) = \mathbf{\Lambda}(a) - \mathbf{A}^c_{\sigma,\mathbf{K}}\mathbf{P}(a) = \mathbf{D}^\star_\mathbf{K}(a)$$

which leads to

$$\mathbf{A}^c_{\sigma,\mathbf{K}}\mathbf{P}(a) = \mathbf{D}^\star_\mathbf{K}(a) - \mathbf{\Lambda}(a)\,. \tag{5.30}$$

By comparison of coefficients the matrix $\mathbf{A}^c_{\sigma,\mathbf{K}}$ is obtained which with the right hand part of equation (5.24) results in

$$\mathbf{K}^c = (\mathbf{B}^c_\sigma)^{-1}(\mathbf{A}^c_{\sigma,\mathbf{K}} - \mathbf{A}^c_\sigma) \tag{5.31}$$

Finally, the respective coordinate transform yields

$$\mathbf{K} = \mathbf{K}^c\mathbf{Q}\,, \tag{5.32}$$

which, unless assured by renamed inputs, has to allow for the permutation matrix that could have been necessary for transforming the CCF into its ordered form according to Remark 5.1.

Remark 5.4
There is some flexibility in choosing the unimodular transforms on $\mathbf{D}^\star(a)$, for instance, the addition of some row to an other row may not affect any column degree. Due to this flexibility, besides the denominator matrix $\mathbf{D}^\star_\mathbf{K}(a)$ that is returned by the algorithm, generally, other polynomial matrices may meet the conditions C1–C3. □

5.2.5 Example

This section is to illustrate the latter notions by an example taken from [RS03, Sch02]. Note that appendant calculations were carried out by making use of standard calculations with the package `LinearAlgebra` in Maple®. Given an LMS over $\mathbb{F}_2$ of order $n = 5$ with $m = 2$ inputs,

$$\mathbf{x}(k+1) = \mathbf{A}\mathbf{x}(k) + \mathbf{B}\mathbf{u}(k), \quad \mathbf{A} = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 \end{pmatrix}, \mathbf{B} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 1 \\ 0 & 1 \\ 0 & 1 \end{pmatrix}.$$

The corresponding reduced controllability matrix according to equation (5.3) results in

$$\mathbf{L} = (\mathbf{b}_1, \mathbf{A}\mathbf{b}_1, \mathbf{b}_2, \mathbf{A}\mathbf{b}_2, \mathbf{A}^2\mathbf{b}_2) = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \end{pmatrix},$$

which shows that the $m = 2$ controllability indices $c_1 = 2$, $c_2 = 3$ are not arranged decreasingly. In light of Remark 5.1 this entails the need of renaming the inputs, hence

$$\hat{u}_1(k) = u_2(k),\ \hat{u}_2(k) = u_1(k), \quad \Longrightarrow \quad \hat{\mathbf{b}}_1 = \mathbf{b}_2,\ \hat{\mathbf{b}}_2 = \mathbf{b}_1\,.$$

In what follows, let all variables that are affected by this renaming be marked by a hat. Now the corresponding reduced controllability matrix becomes

$$\hat{\mathbf{L}} = (\hat{\mathbf{b}}_1, \mathbf{A}\hat{\mathbf{b}}_1, \mathbf{A}^2\hat{\mathbf{b}}_1, \hat{\mathbf{b}}_2, \mathbf{A}\hat{\mathbf{b}}_2) = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

which has the required ordering property since $\hat{c}_1 = 3, \hat{c}_2 = 2$. Its inverse matrix reads

$$\hat{\mathbf{L}}^{-1} = \begin{pmatrix} 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 \end{pmatrix}$$

and by Theorem 5.3 with

$$\hat{\sigma}_1 = \hat{c}_1 = 3,\ \hat{\sigma}_2 = \hat{c}_1 + \hat{c}_2 = 5$$

and

$$\hat{\mathbf{q}}_1^{\mathrm{T}} = \mathrm{row}_{\hat{\sigma}_1}(\hat{\mathbf{L}}^{-1}) = (0,0,1,0,1),\ \hat{\mathbf{q}}_2^{\mathrm{T}} = \mathrm{row}_{\hat{\sigma}_2}(\hat{\mathbf{L}}^{-1}) = (0,1,0,1,0)$$

the transformation matrix

$$\hat{\mathbf{Q}} = \begin{pmatrix} \hat{\mathbf{q}}_1^{\mathrm{T}} \\ \hat{\mathbf{q}}_1^{\mathrm{T}}\mathbf{A} \\ \hat{\mathbf{q}}_1^{\mathrm{T}}\mathbf{A}^2 \\ \hat{\mathbf{q}}_2^{\mathrm{T}} \\ \hat{\mathbf{q}}_2^{\mathrm{T}}\mathbf{A} \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 \end{pmatrix}$$

for the state transform $\mathbf{x}^{\mathrm{c}} = \hat{\mathbf{Q}}\mathbf{x}$ is obtained. Consequently, the LMS can be represented in the CCF

$$\mathbf{x}^{\mathrm{c}}(k+1) = \mathbf{A}^{\mathrm{c}}\mathbf{x}^{\mathrm{c}}(k) + \mathbf{B}^{\mathrm{c}}\hat{\mathbf{u}}(k), \quad \mathbf{A}^{\mathrm{c}} = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \end{pmatrix}, \mathbf{B}^{\mathrm{c}} \begin{pmatrix} 0 & 0 \\ 1 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 1 \end{pmatrix}$$

from which the matrices

$$\mathbf{A}^{\mathrm{c}}_{\sigma} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \end{pmatrix}, \quad \mathbf{B}^{\mathrm{c}}_{\sigma} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

can be extracted for use within the image domain state feedback design.

As a control objective, assume that this LMS shall have 4 cycles of length 1, 2 cycles of length 2, 4 cycles of length 3 and 2 cycles of length 6 in the closed-loop. This is a CSSP with desired invariant polynomials $c_{1,\mathbf{K}}(a) = (a^2+a+1)(a+1)^2$ and $c_{2,\mathbf{K}}(a) = a+1$, see Example 4.2.1.3 in Chapter 4.

An appropriate state feedback matrix $\mathbf{K}$ can be determined by using the algorithm proposed in Theorem 5.2.4, accordingly

$$\xrightarrow{\text{i}} \quad \begin{aligned} \sum_{i=1}^{1} \deg(c_{i,\mathbf{K}}(a)) = 4 \geq \sum_{i=1}^{1} c_i = 3 \quad \surd \\ \sum_{i=1}^{2} \deg(c_{i,\mathbf{K}}(a)) = 5 \geq \sum_{i=1}^{2} c_i = 5 \quad \surd \end{aligned}$$

$$\xrightarrow{\text{ii}} \quad \mathbf{D}^{\star}(a) = \begin{pmatrix} (a^2+a+1)(a+1)^2 & 0 \\ 0 & a+1 \end{pmatrix} = \begin{pmatrix} a^4+a^3+a+1 & 0 \\ 0 & a+1 \end{pmatrix}$$

$$\xrightarrow{\text{iii,iv}} \quad \mathbf{D}^{+}(a) = \begin{pmatrix} a^4+a^3+a+1 & a^2+a \\ 0 & a+1 \end{pmatrix} \quad \Longrightarrow \quad \mathbf{D}^{++}(a) = \begin{pmatrix} a+1 & a^2+a \\ a^3+a^2 & a+1 \end{pmatrix}$$

$$\xrightarrow{\text{v}} \quad \mathbf{\Gamma}_{\mathrm{c}}(\mathbf{D}^{++}) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \Longrightarrow \quad \mathbf{D}^{\star}(a) = (\mathbf{\Gamma}_{\mathrm{c}}(\mathbf{D}^{++}))^{-1}\mathbf{D}^{++}(a) = \begin{pmatrix} a^3+a^2 & a+1 \\ a+1 & a^2+a \end{pmatrix}$$

$$\xrightarrow{\text{iii,vi}} \quad \mathbf{D}^{\star}_{\mathbf{K}}(a) = \begin{pmatrix} a^3+a^2 & a+1 \\ a+1 & a^2+a \end{pmatrix}$$

With $\mathbf{D}^{\star}_{\mathbf{K}}(a)$ the feedback matrix $\mathbf{K}$ can be computed. First, employing equation (5.30) yields

$$\mathbf{A}^{\mathrm{c}}_{\sigma,\mathbf{K}} \begin{pmatrix} 1 & 0 \\ a & 0 \\ a^2 & 0 \\ 0 & 1 \\ 0 & a \end{pmatrix} = \underbrace{\begin{pmatrix} a^3 & 0 \\ 0 & a^2 \end{pmatrix}}_{\mathbf{\Lambda}(a)} + \underbrace{\begin{pmatrix} a^3+a^2 & a+1 \\ a+1 & a^2+a \end{pmatrix}}_{\mathbf{D}^{\star}_{\mathbf{K}}(a)} = \begin{pmatrix} a^2 & a+1 \\ a+1 & a \end{pmatrix}$$

and by comparison of coefficients results

$$\mathbf{A}^{\mathrm{c}}_{\sigma,\mathbf{K}} = \begin{pmatrix} 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

which, secondly, as per (5.31) implies

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

Thus, the feedback matrix $\hat{\mathbf{K}}$ with respect to the renamed inputs follows from (5.32), that is

$$\hat{\mathbf{K}} = \mathbf{K}^{\mathrm{c}}\hat{\mathbf{Q}} = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 \end{pmatrix}$$

which by swapping rows results in the desired state feedback matrix

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

5.2.6 Non-controllable Parts

Controllable LMS of n-th order are characterized by the existence of a set of n linearly independent column vectors in the controllability matrix $\mathbf{L}$, see Definition 5.3. If the LMS contains non-controllable parts then it consists of an uncontrollable subsystem of order $\bar{n} \geq 1$ and of a controllable subsystem of corresponding order $n-\bar{n}$, and the controllability matrix only comprises $n-\bar{n}$ linearly independent vectors, which span the controllable vector space. Nevertheless it is possible to adapt the synthesis method of the last section.

To this end, consider the linearly independent column vectors in the non-square reduced controllability matrix $\mathbf{L} \in \mathbb{F}_q^{n\times(n-\bar{n})}$ in equation (5.3), i. e.

$$\mathbf{L} = \left(\mathbf{b}_1, \ldots, \mathbf{A}^{c_1-1}\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{A}^{c_2-1}\mathbf{b}_2, \ldots, \mathbf{b}_m, \ldots \mathbf{A}^{c_m-1}\mathbf{b}_m\right), \quad \sum_{i=1}^{m} c_i = n-\bar{n} < n, \tag{5.33}$$

which can be completed by a set of $\bar{n}$ linearly independent column vectors that span the orthogonal complement space of the controllable subspace with respect to the entire space $\mathbb{F}_q^n$, see[Wol74]. Let these vectors be the column vectors of the matrix $\mathbf{L}_{\bar{n}} \in \mathbb{F}_q^{n\times\bar{n}}$. Therefore, with

$$\mathbf{L}_{\bar{n}}^{\mathrm{T}}\mathbf{L} = \mathbf{0} \tag{5.34}$$

the adapted reduced controllability matrix

$$\bar{\mathbf{L}} = (\mathbf{L}, \mathbf{L}_{\bar{n}}), \ \bar{\mathbf{L}} \in \mathbb{F}_q^{n\times n} \tag{5.35}$$

becomes an invertible matrix.

This extension by $\mathbf{L}_{\bar{n}}$ acts as if the number of inputs were extended by $\bar{n}$ and the input matrix $\mathbf{B}$ were augmented to the right by the $\bar{n}$ linearly independent columns of $\mathbf{L}_{\bar{n}}$. Then by linear independence, each of these vectors can be interpreted as corresponding to a controllability index equal to one, which implies controllability of this extended system, and accordingly, the extended system can be transformed into CCF as per Definition 5.5. For this reason, proceeding in the same manner as for constructing the transformation matrix $\mathbf{Q}$ in Theorem 5.3, that is, by calculating the inverse matrix $\bar{\mathbf{L}}^{-1}$ and again using $\sigma_i = \sum_{j=1}^{i} c_j$, $i = 1, \ldots, m$ by defining

$$\bar{\mathbf{q}}_i^{\mathrm{T}} := \mathrm{row}_{\sigma_i}(\bar{\mathbf{L}}^{-1}), \tag{5.36}$$

the matrix

$$\mathbf{Q} = \begin{pmatrix} \bar{\mathbf{q}}_1^{\mathrm{T}} \\ \bar{\mathbf{q}}_1^{\mathrm{T}}\mathbf{A} \\ \vdots \\ \bar{\mathbf{q}}_1^{\mathrm{T}}\mathbf{A}^{c_1-1} \\ \bar{\mathbf{q}}_2^{\mathrm{T}} \\ \bar{\mathbf{q}}_2^{\mathrm{T}}\mathbf{A} \\ \vdots \\ \bar{\mathbf{q}}_2^{\mathrm{T}}\mathbf{A}^{c_2-1} \\ \vdots \\ \bar{\mathbf{q}}_m^{\mathrm{T}}\mathbf{A}^{c_m-1} \end{pmatrix} \tag{5.37}$$

is obtained, which here with $\mathbf{Q} \in \mathbb{F}_q^{(n-\bar{n})\times n}$ is non-square. In view of the interpretation of controllability index one from above, the missing $\bar{n}$ rows in order to quadratically supplement $\mathbf{Q}$ are simply the respective last rows of $\bar{\mathbf{L}}^{-1}$. These can be collected in

$$\mathbf{Q}_{\bar{n}} = \begin{pmatrix} \mathrm{row}_{n-\bar{n}+1}(\bar{\mathbf{L}}^{-1}) \\ \mathrm{row}_{n-\bar{n}+2}(\bar{\mathbf{L}}^{-1}) \\ \vdots \\ \mathrm{row}_{n}(\bar{\mathbf{L}}^{-1}) \end{pmatrix} \tag{5.38}$$

with $\mathbf{Q}_{\bar{n}} \in \mathbb{F}_q^{\bar{n}\times n}$. Consequently, an adapted version of the transformation matrix[13] reads

$$\bar{\mathbf{Q}} = \begin{pmatrix} \mathbf{Q} \\ \mathbf{Q}_{\bar{n}} \end{pmatrix}. \tag{5.39}$$

whose partitioning induces a partitioning of the state $\bar{\mathbf{x}}(k)$, the dynamics matrix $\mathbf{A}$, and the input matrix $\mathbf{B}$, i. e.

$$\bar{\mathbf{x}}(k) = \begin{pmatrix} \bar{\mathbf{x}}^{\mathrm{c}}(k) \\ \bar{\mathbf{x}}^{\bar{\mathrm{c}}}(k) \end{pmatrix} = \begin{pmatrix} \mathbf{Q} \\ \mathbf{Q}_{\bar{n}} \end{pmatrix} \mathbf{x}(k), \tag{5.40}$$

$$\bar{\mathbf{A}} = \begin{pmatrix} \bar{\mathbf{A}}^{\mathrm{c}} & \bar{\mathbf{A}}^{\mathrm{c}\,\bar{\mathrm{c}}} \\ \bar{\mathbf{A}}^{\bar{\mathrm{c}}\mathrm{c}} & \bar{\mathbf{A}}^{\bar{\mathrm{c}}} \end{pmatrix} = \begin{pmatrix} \mathbf{Q} \\ \mathbf{Q}_{\bar{n}} \end{pmatrix} \mathbf{A} \begin{pmatrix} \mathbf{Q} \\ \mathbf{Q}_{\bar{n}} \end{pmatrix}^{-1}, \tag{5.41}$$

$$\bar{\mathbf{B}} = \begin{pmatrix} \bar{\mathbf{B}}^{\mathrm{c}} \\ \bar{\mathbf{B}}^{\bar{\mathrm{c}}} \end{pmatrix} = \begin{pmatrix} \mathbf{Q} \\ \mathbf{Q}_{\bar{n}} \end{pmatrix} \mathbf{B} \tag{5.42}$$

such that the state equation is in a CCF-like form

$$\bar{\mathbf{x}}(k+1) = \bar{\mathbf{A}}\bar{\mathbf{x}}(k) + \bar{\mathbf{B}}\mathbf{u}(k). \tag{5.43}$$

"CCF-like" is to stress that the special choice of $\mathbf{L}_{\bar{n}}$ as an orthogonal complement — see equation (5.34) — implies even more structure than the representation in CCF. First, since the vectors $\mathbf{A}^i\mathbf{b}_j$, $i \geq c_j$ depend linearly on those vectors with $i < c_j$ note that

$$\mathbf{Q}_{\bar{n}}\mathbf{A}^i\mathbf{b}_j = \mathbf{0}, \quad i = 0,1,2,\ldots,\ j = 1,\ldots,m \tag{5.44}$$

by means of which an obvious consequence in (5.42) is that

$$\bar{\mathbf{B}}^{\bar{\mathrm{c}}} = \mathbf{0}. \tag{5.45}$$

Moreover, the first $n-\bar{n}$ columns in $\bar{\mathbf{Q}}^{-1}$ are orthogonal to the $\bar{n}$ rows in $\mathbf{Q}_{\bar{n}}$, by definition. But as the orthogonal complement space with respect to the row space of $\mathbf{Q}_{\bar{n}}$ is spanned by the $n-\bar{n}$ column vectors of $\mathbf{L}$ an other immediate implication of (5.44) in (5.41) is

$$\bar{\mathbf{A}}^{\bar{\mathrm{c}}\mathrm{c}} = \mathbf{0}. \tag{5.46}$$

Now it is clear that the lower system part with dynamics matrix $\bar{\mathbf{A}}^{\bar{\mathrm{c}}}$ cannot be influenced, neither by some input nor by the states $\bar{\mathbf{x}}^{\mathrm{c}}(k)$ from the upper system, hence, represents an autonomous uncontrollable subsystem. Even though by virtue of $\bar{\mathbf{A}}^{\mathrm{c}\,\bar{\mathrm{c}}}$ the uncontrollable subsystem can take influence on the upper system, however, the upper system represents a controllable subsystem. This is due to the fact that by choosing a suitable input — feedback of the uncontrollable states $\bar{\mathbf{x}}^{\bar{\mathrm{c}}}(k)$ — any element of the non-zero rows in $\bar{\mathbf{A}}^{\mathrm{c}\,\bar{\mathrm{c}}}$ can be specified arbitrarily, for example turned

[13] which is invertible by construction

into zero, see Section 5.2.6.1. For this reason, a feedback of the remaining controllable states $\overline{\mathbf{x}}^{\mathrm{c}}(k)$ allows of designing a customary controller for the controllable subsystem embodied by the dynamics matrix $\overline{\mathbf{A}}^{\mathrm{c}}$.

Summarizing the latter, the following theorem has been shown.

Theorem 5.11 (Adapted CCF for Uncontrollable Systems)
Let an uncontrollable LMS of order n with m inputs have $i = 1, \ldots, m$ controllability indices c_i with $\sigma_j := \sum_{i=1}^{j} c_i$ and $\overline{n} := n - \sum_{i=1}^{m} c_i$. Then the transformations in (5.40)-(5.42) transform the state equation of the LMS into

$$\overline{\mathbf{x}}(k+1) = \begin{pmatrix} \overline{\mathbf{A}}^{\mathrm{c}} & \overline{\mathbf{A}}^{\mathrm{c}\overline{\mathrm{c}}} \\ \mathbf{0} & \overline{\mathbf{A}}^{\overline{\mathrm{c}}} \end{pmatrix} \overline{\mathbf{x}}(k) + \begin{pmatrix} \overline{\mathbf{B}}^{\mathrm{c}} \\ \mathbf{0} \end{pmatrix} \mathbf{u}(k)\,. \tag{5.47}$$

- The matrices $\overline{\mathbf{A}}^{\mathrm{c}} \in \mathbb{F}_q^{(n-\overline{n})\times(n-\overline{n})}$ and $\overline{\mathbf{B}}^{\mathrm{c}} \in \mathbb{F}_q^{(n-\overline{n})\times m}$ represent an $(n-\overline{n})$-th order controllable subsystem in CCF, in complete accordance with Definition 5.5.
- The matrix $\overline{\mathbf{A}}^{\overline{\mathrm{c}}} \in \mathbb{F}_q^{\overline{n}\times\overline{n}}$ represents an $\overline{n}$-th order (autonomous) uncontrollable subsystem.
- The matrix $\overline{\mathbf{A}}^{\mathrm{c}\overline{\mathrm{c}}} \in \mathbb{F}_q^{(n-\overline{n})\times\overline{n}}$ represents a coupling of controllable and uncontrollable subsystem. Moreover, its σ_j-th rows, $j = 1, \ldots, m$, are the only non-zero rows in $\overline{\mathbf{A}}^{\mathrm{c}\overline{\mathrm{c}}}$. □

5.2.6.1 Decoupling the Uncontrollable from the Controllable Subsystem

The synthesis goal of specifying a set of desired elementary divisor polynomials (CSSP) in the overall closed-loop dynamics matrix of an uncontrollable LMS can be combined with a decoupling that breaks the influence of the uncontrollable subsystem on the controllable subsystem. Referring to the solution of the state equation (5.1) it turns out that this influence is incurred by non-zero initial states with respect to the uncontrollable subsystem only, and not by the input-sided portion. An additional benefit of decoupling is that the block-diagonal structure of the decoupled dynamics matrix allows to simplify the synthesis.

Theorem 5.11 indicates an easy way of how to decouple the uncontrollable subsystem from the controllable subsystem by an appropriate feedback. Obviously, decoupling requires that

$$\overline{\mathbf{A}}^{\mathrm{c}\overline{\mathrm{c}}}\overline{\mathbf{x}}^{\overline{\mathrm{c}}}(k) + \overline{\mathbf{B}}^{\mathrm{c}}\mathbf{u}(k) = \mathbf{0} \tag{5.48}$$

which can be achieved by a state feedback in the simple form $\mathbf{u}(k) = \mathbf{K}\mathbf{x}(k)$. In transformed coordinates the feedback matrix becomes

$$\overline{\mathbf{K}} = \mathbf{K}\overline{\mathbf{Q}}^{-1} \tag{5.49}$$

which in a partitioned form

$$\bar{\mathbf{K}} = (\bar{\mathbf{K}}^{\mathrm{c}}, \bar{\mathbf{K}}^{\mathrm{c}\bar{\mathrm{c}}}) \tag{5.50}$$

means that

$$\mathbf{u}(k) = \bar{\mathbf{K}}\,\bar{\mathbf{x}}(k) = \bar{\mathbf{K}}^{\mathrm{c}}\,\bar{\mathbf{x}}^{\mathrm{c}}(k) + \bar{\mathbf{K}}^{\mathrm{c}\bar{\mathrm{c}}}\bar{\mathbf{x}}^{\bar{\mathrm{c}}}(k)\,. \tag{5.51}$$

Thus, recalling equation (5.48) the influence of the coupling matrix $\bar{\mathbf{A}}^{\mathrm{c}\bar{\mathrm{c}}}$ vanishes if

$$\bar{\mathbf{B}}^{\mathrm{c}}\,\bar{\mathbf{K}}^{\mathrm{c}\bar{\mathrm{c}}} = -\bar{\mathbf{A}}^{\mathrm{c}\bar{\mathrm{c}}} \tag{5.52}$$

or with the denotation from (5.5) with (5.31), equivalently, if

$$\bar{\mathbf{K}}^{\mathrm{c}\bar{\mathrm{c}}} = -(\bar{\mathbf{B}}^{\mathrm{c}}_{\sigma})^{-1}\bar{\mathbf{A}}^{\mathrm{c}\bar{\mathrm{c}}}_{\sigma} \tag{5.53}$$

in which $\bar{\mathbf{B}}^{\mathrm{c}}_{\sigma}$ and $\bar{\mathbf{A}}^{\mathrm{c}\bar{\mathrm{c}}}_{\sigma}$ comprise the alterable entries in the matrices $\bar{\mathbf{B}}^{\mathrm{c}}$ and $\bar{\mathbf{A}}^{\mathrm{c}\bar{\mathrm{c}}}$, respectively. Therefore, the following theorem has been established.

Theorem 5.12 (Decoupling by State Feedback)
Let an LMS of order n with m inputs be uncontrollable. Let the uncontrollable subsystem be of order $\bar{n} < n$. Then the uncontrollable subsystem can always be decoupled from the controllable subsystem by linear state feedback with respect to the uncontrollable subsystem states. □

The Influence of Decoupling on the Closed-Loop Invariants

In light of the benefits from decoupling it is important to discuss its influence on the invariant polynomials of the dynamics matrix. On account of this, the following issues are addressed in the sequel:

- development of a sufficient criterion of when the dynamics matrix of a decoupled uncontrollable LMS shows the same invariant polynomials as the respective coupled LMS,
- present a particular case in which the invariant polynomials remain unaltered by decoupling whatever the coupling matrix in the dynamics matrix is,
- show that the characteristic polynomial of the dynamics matrix is invariant under decoupling,
- determine the elementary divisor polynomials of a decoupled dynamics out of the elementary divisor polynomials of its parts.

First, recall the following theorem, taken from literature for simplicity [GLR82, p. 342 ff.].

Theorem 5.13 (Similarity Criterion)
Let $\mathbf{M}_{11} \in \mathbb{F}^{n_1 \times n_1}$, $\mathbf{M}_{22} \in \mathbb{F}^{n_2 \times n_2}$, and $\mathbf{M}_{12} \in \mathbb{F}^{n_1 \times n_2}$. The matrices

$$\begin{pmatrix} \mathbf{M}_{11} & \mathbf{M}_{12} \\ \mathbf{0} & \mathbf{M}_{22} \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} \mathbf{M}_{11} & \mathbf{0} \\ \mathbf{0} & \mathbf{M}_{22} \end{pmatrix}$$

are similar iff the linear matrix equation

$$\mathbf{M}_{11}\mathbf{X} - \mathbf{X}\mathbf{M}_{22} = \mathbf{M}_{12} \tag{5.54}$$

has a solution. □

A solution which is valid in the majority of the cases is due to [Gan58, p. 208 ff.] and [New74].[14]

Theorem 5.14
Using the notation of Theorem 5.13 the linear matrix equation (5.54) has a solution for arbitrary coupling matrices $\mathbf{M}_{12} \in \mathbb{F}^{n_1 \times n_2}$ if

$$\gcd(\mathrm{cp}_{\mathbf{M}_{11}}(\lambda), \mathrm{cp}_{\mathbf{M}_{22}}(\lambda)) = 1\,.$$

Moreover, this solution is unique. □

The far-reaching interpretation for the purpose of this work is

Corollary 5.2 (Invariant Polynomials under Decoupling)
Let an uncontrollable LMS of order *n* with *m* inputs be given in the notation of Theorem 5.11. Then decoupling the uncontrollable subsystem from the controllable subsystem by use of a state feedback (5.53) does not change the invariant polynomials of the dynamics matrix iff the linear matrix equation

$$\bar{\mathbf{A}}^{\mathrm{c}}\mathbf{X} - \mathbf{X}\bar{\mathbf{A}}^{\bar{\mathrm{c}}} = \bar{\mathbf{A}}^{\mathrm{c}\bar{\mathrm{c}}} \tag{5.55}$$

has a solution. A unique such solution exists if

$$\gcd\left(\mathrm{cp}_{\bar{\mathbf{A}}^{\mathrm{c}}}(\lambda), \mathrm{cp}_{\bar{\mathbf{A}}^{\bar{\mathrm{c}}}}(\lambda)\right) = 1\,.$$

In this case the invariant polynomials remain unchanged under decoupling whatever $\bar{\mathbf{A}}^{\mathrm{c}\bar{\mathrm{c}}}$. □

[14] From linearity of equation (5.54) it is clear that the general statement can be derived as well; the general solution is attainable pursuing the lines in Appendix D. Since in addition to that, more notational effort is incurred by the associated introduction of the *Kronecker*-product of matrices for transforming the equation into a standard linear equation, the generalization becomes quite involved and distracts too much from the purposes here. Hence, keeping track of this way shall be left to the reader.

Thus, if the conditions stated in Corollary 5.2 are met then decoupling cannot change the invariant polynomials of the dynamics matrix; under these assumptions this can only be done by an adequate feedback with respect to the controllable part. Conversely, if the conditions stated in Corollary 5.2 are not met then the influence of decoupling on the invariant polynomials is still subject to a limit, but a less restrictive one.

Theorem 5.15 (Invariance of Characteristic Polynomials under Decoupling)
Let an uncontrollable LMS of order n with m inputs be given in the notation of Theorem 5.11. Then Decoupling the uncontrollable subsystem from the controllable subsystem by use of a state feedback (5.53) does not change the characteristic polynomial of the dynamics matrix. □

Proof Using unimodular matrices $\mathbf{U}(\lambda) = \operatorname{diag}(\mathbf{U}^{\mathrm{c}}(\lambda), \mathbf{U}^{\bar{\mathrm{c}}}(\lambda))$ and $\mathbf{V}(\lambda) = \operatorname{diag}(\mathbf{V}^{\mathrm{c}}(\lambda), \mathbf{V}^{\bar{\mathrm{c}}}(\lambda))$ the characteristic matrix $\lambda\mathbf{I} - \bar{\mathbf{A}}$ can be transformed into

$$\mathbf{U}(\lambda)(\lambda\mathbf{I} - \bar{\mathbf{A}})\mathbf{V}(\lambda) = \mathbf{U}(\lambda) \begin{pmatrix} \lambda\mathbf{I} - \bar{\mathbf{A}}^{\mathrm{c}} & \bar{\mathbf{A}}^{c\bar{c}} \\ \mathbf{0} & \lambda\mathbf{I} - \bar{\mathbf{A}}^{\bar{\mathrm{c}}} \end{pmatrix} \mathbf{V}(\lambda) = \begin{pmatrix} \mathbf{S}^{\mathrm{c}}(\lambda) & \mathbf{U}^{\mathrm{c}}(\lambda)\bar{\mathbf{A}}^{c\bar{c}}\mathbf{V}^{\bar{\mathrm{c}}}(\lambda) \\ \mathbf{0} & \mathbf{S}^{\bar{\mathrm{c}}}(\lambda) \end{pmatrix}, \quad (5.56)$$

which clearly has the same invariant polynomials and elementary divisor polynomials, respectively, as $\bar{\mathbf{A}}$. Hence,

$$\mathrm{cp}_{\bar{\mathbf{A}}}(\lambda) = \det\big(\mathbf{U}(\lambda)(\lambda\mathbf{I} - \bar{\mathbf{A}})\mathbf{V}(\lambda)\big) = \det\big(\mathbf{S}^{\mathrm{c}}(\lambda)\big)\det\big(\mathbf{S}^{\bar{\mathrm{c}}}(\lambda)\big) = \mathrm{cp}_{\bar{\mathbf{A}}^{\mathrm{c}}}(\lambda)\,\mathrm{cp}_{\bar{\mathbf{A}}^{\bar{\mathrm{c}}}}(\lambda)$$

which does not show any dependency on $\bar{\mathbf{A}}^{c\bar{c}}$. As a result, decoupling has no influence on the characteristic polynomial of the dynamics matrix. □

Setting $\bar{\mathbf{A}}^{c\bar{c}}$ equal to zero in equation (5.56), the same argument can be used for showing an important result [LT85], which applied to this work is

Theorem 5.16 (Elementary Divisor Polynomials of a Decoupled Dynamics Matrix)
Let an uncontrollable LMS of order n with m inputs be given in the notation of Theorem 5.11 and let the uncontrollable subsystem be decoupled from the controllable subsystem by use of a state feedback (5.53). Then the set of elementary divisor polynomials regarding the matrix $\operatorname{diag}(\bar{\mathbf{A}}^{\mathrm{c}}, \bar{\mathbf{A}}^{\bar{\mathrm{c}}})$ is the union of the sets of elementary divisor polynomials with respect to $\bar{\mathbf{A}}^{\mathrm{c}}, \bar{\mathbf{A}}^{\bar{\mathrm{c}}}$. □

As the respective elementary divisor polynomials divide each other this statement is sufficient for constructing the Smith normal form of $\operatorname{diag}(\bar{\mathbf{A}}^{\mathrm{c}}, \bar{\mathbf{A}}^{\bar{\mathrm{c}}})$ out of the Smith normal forms regarding $\bar{\mathbf{A}}^{\mathrm{c}}$ and $\bar{\mathbf{A}}^{\bar{\mathrm{c}}}$ — the formal description is rather cumbersome and omitted for clearness. A simpler formal description can be achieved in cases for which $\mathrm{cp}_{\bar{\mathbf{A}}^{\mathrm{c}}}(\lambda)$ and $\mathrm{cp}_{\bar{\mathbf{A}}^{\bar{\mathrm{c}}}}(\lambda)$ have no common factor [New72, New74].

Theorem 5.17 (Smith Normal Form of a Compound Matrix)
Let an uncontrollable LMS of order n with m inputs be given in the notation of Theorem 5.11 with arbitrary coupling matrix $\bar{\mathbf{A}}^{\mathrm{c}\,\bar{\mathrm{c}}} \in \mathbb{F}^{(n-\bar{n})\times\bar{n}}$. Without loss of generality, assume $\bar{n} \leq n - \bar{n}$. Moreover, let $\gcd\big(\mathrm{cp}_{\bar{\mathbf{A}}^{\mathrm{c}}}(\lambda), \mathrm{cp}_{\bar{\mathbf{A}}^{\bar{\mathrm{c}}}}(\lambda)\big) = 1$. Denote the Smith normal form with respect to $\bar{\mathbf{A}}^{\mathrm{c}}$ and $\bar{\mathbf{A}}^{\bar{\mathrm{c}}}$ by

$$\mathbf{S}^{\mathrm{c}}(\lambda) = \operatorname{diag}(c_1(\lambda), c_2(\lambda), \ldots, c_{n-\bar{n}}(\lambda)), \quad \mathbf{S}^{\bar{\mathrm{c}}}(\lambda) = \operatorname{diag}(\bar{c}_1(\lambda), \bar{c}_2(\lambda), \ldots, \bar{c}_{\bar{n}}(\lambda)),$$

respectively. Then the Smith normal form $\mathbf{S}(\lambda)$ with respect to

$$\bar{\mathbf{A}}(\lambda) = \begin{pmatrix} \bar{\mathbf{A}}^{\mathrm{c}} & \bar{\mathbf{A}}^{\mathrm{c}\bar{\mathrm{c}}} \\ \mathbf{0} & \bar{\mathbf{A}}^{\bar{\mathrm{c}}} \end{pmatrix}$$

is

$$\mathbf{S}(\lambda) = \mathrm{diag}(c_1\bar{c}_1, c_2\bar{c}_2, \ldots, c_{\bar{n}}\bar{c}_{\bar{n}}, c_{\bar{n}+1}, c_{\bar{n}+2}, \ldots, c_{n-\bar{n}}, 1, 1, \ldots, 1)\,. \qquad \square$$

In the preceding lines, the focus was on how to decouple the uncontrollable subsystem from the controllable subsystem of an LMS without changing the elementary divisor polynomials of the LMS. The subsequent remark comments on the remaining case.

Remark 5.5 (Conservation of Elementary Divisor Polynomials of the Uncontrollable Part) Even though decoupling does not change the characteristic polynomial of the dynamics matrix, however, decoupling can change the elementary divisor polynomials of the controllable subsystem if the condition in Corollary 5.2 is not met. This change can only affect the distribution of the factors in the characteristic polynomial, for instance by joining elementary divisor polynomials into a new one of higher degree. But note that in any case the elementary divisor polynomials of $\bar{\mathbf{A}}^{\bar{\mathrm{c}}}$ are preserved in the overall system, which can be concluded from the respective Smith normal form $\mathbf{S}^{\bar{\mathrm{c}}}$ in equation (5.56) and the fact that the uncontrollable system is an autonomous LMS. $\square$

Consequently, if striving to solve the CSSP for a set of desired elementary divisor polynomials in the overall closed-loop dynamics matrix of an uncontrollable LMS then this set has to include the set of elementary divisor polynomials with respect to the autonomous dynamics $\bar{\mathbf{A}}^{\bar{\mathrm{c}}}$ of the uncontrollable subsystem. This condition has to be fulfilled in addition to the condition imposed by Rosenbrock's control structure theorem.

5.2.6.2 Solving the Cycle Sum Synthesis Problem (CSSP) for Uncontrollable LMS

In what follows, the CSSP is solved assuming the decoupling of the uncontrollable from the controllable subsystem, for simplicity. After decoupling the remaining unspecified parameters reside in the feedback matrix $\bar{\mathbf{K}}^{\mathrm{c}}$. This matrix can be determined by the algorithm presented in Theorem 5.2.4 since the corresponding subsystem of order $n-\bar{n}$ is controllable. For specifying the set of closed-loop elementary divisor polynomials it is first necessary to enclose the set of elementary divisor polynomials regarding the uncontrollable dynamics $\bar{\mathbf{A}}^{\bar{\mathrm{c}}}$. Then, if in accordance with Rosenbrock's control structure theorem, the algorithm returns a denominator matrix, here $\mathbf{D}^{\star}_{\bar{\mathbf{K}}^{\mathrm{c}}}(a)$, which by a comparison of coefficients according to equation (5.30) yields a matrix $\mathbf{A}^{\mathrm{c}}_{\sigma,\bar{\mathbf{K}}^{\mathrm{c}}}$ that can finally be used for determining the feedback matrix $\bar{\mathbf{K}}^{\mathrm{c}}$, see equation (5.31). The resulting feedback matrix is

$$\bar{\mathbf{K}}^{\mathrm{c}} = (\mathbf{B}^{\mathrm{c}}_{\sigma})^{-1}(\bar{\mathbf{A}}^{\mathrm{c}}_{\sigma,\bar{\mathbf{K}}^{\mathrm{c}}} - \bar{\mathbf{A}}^{\mathrm{c}}_{\sigma})\,. \tag{5.57}$$

With $\overline{\mathbf{K}}^{\mathrm{c}}$ and $\overline{\mathbf{K}}^{\mathrm{c}\,\overline{\mathrm{c}}}$ all entries in the overall feedback matrix $\overline{\mathbf{K}}$ are fixed. Summing up, a possible procedure that solves the CSSP for an LMS with uncontrollable subsystem and decoupling is the following:

1. Transform the state equation into an adapted CCF as in equations (5.41) and (5.42).
2. Calculate the elementary divisor polynomials of the uncontrollable dynamics matrix $\overline{\mathbf{A}}^{\overline{\mathrm{c}}}$
3. Check whether the desired set of closed-loop elementary divisor polynomials includes the set of elementary divisor polynomials of $\overline{\mathbf{A}}^{\overline{\mathrm{c}}}$.
4. Check whether the desired closed-loop invariant polynomials with respect to the controllable part meet Rosenbrock's control structure theorem, Theorem 5.4.
5. If both checks are positive then
   - use the synthesis algorithm in Theorem 5.2.4 in order to determine a matrix $\overline{\mathbf{K}}^{\mathrm{c}}$ for feeding back the controllable states (5.31) and
   - with (5.53) calculate the decoupling state feedback matrix $\overline{\mathbf{K}}^{\mathrm{c}\,\overline{\mathrm{c}}}$ which feeds back the uncontrollable states.
   - A feedback matrix that solves the CSSP is $\mathbf{K} = \overline{\mathbf{K}}\,\overline{\mathbf{Q}}$ with $\overline{\mathbf{K}} = (\overline{\mathbf{K}}^{\mathrm{c}}, \overline{\mathbf{K}}^{\mathrm{c}\,\overline{\mathrm{c}}})$.

Remark 5.6
As already indicated, there are cases in which the set of desired closed-loop invariant polynomials cannot be realized under decoupling. Then a particular change of the coupling matrix might help to solve the problem. Notwithstanding, a coupling conserves that the state evolution depends on the initial state of the uncontrollable subsystem. Moreover, a coupling can just be used for a reassembly of the elementary divisor polynomials concerning the controllable part. For these reasons, this is not commented on in a deeper fashion. □

5.2.7 Example

Consider an LMS over $\mathbb{F}_2$ of order $n = 5$ with $m = 1$ input and

$$\mathbf{A} = \begin{pmatrix} 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 \end{pmatrix}, \quad \mathbf{B} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}.$$

The corresponding reduced controllability matrix according to equation (5.3) results in

$$\mathbf{L} = (\mathbf{B}, \mathbf{A}\mathbf{B}, \mathbf{A}^2\mathbf{B}) = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix}$$

which reveals that the sole controllability index is $c_1 = \sigma_1 = 3$ and implies that the LMS has an uncontrollable subsystem of order $\bar{n} = 2$. In view of equation (5.35) a simple choice of linearly independent column vectors yields

$$\mathbf{L}_{\bar{n}} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{pmatrix},$$

thus, the adapted reduced controllability matrix and its inverse reads

$$\bar{\mathbf{L}} = (\mathbf{L}, \mathbf{L}_{\bar{n}}) = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \end{pmatrix}, \quad \bar{\mathbf{L}}^{-1} = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 \end{pmatrix}.$$

Theorem 5.3 and equation (5.39) allows to calculate the transformation matrix, i. e. from

$$\mathbf{q}_1^{\mathrm{T}} = \mathrm{row}_{\sigma_1}(\hat{\mathbf{L}}^{-1}) = (0,0,1,0,0), \quad \mathbf{Q}_{\bar{n}} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 \end{pmatrix}$$

follows the transformation matrix

$$\bar{\mathbf{Q}} = \begin{pmatrix} \mathbf{q}_1^{\mathrm{T}} \\ \mathbf{q}_1^{\mathrm{T}}\mathbf{A} \\ \mathbf{q}_1^{\mathrm{T}}\mathbf{A}^2 \\ \mathbf{Q}_{\bar{n}} \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 \end{pmatrix}$$

which via (5.41) and (5.42) transforms the LMS in adapted CCF with

$$\bar{\mathbf{A}} = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix}, \quad \bar{\mathbf{B}} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}.$$

By inspection, the matrices

$$\bar{\mathbf{A}}^{\mathrm{c}} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}, \; \bar{\mathbf{A}}^{\mathrm{c}\bar{\mathrm{c}}} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \\ 1 & 0 \end{pmatrix}, \; \bar{\mathbf{A}}^{\bar{\mathrm{c}}} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \; \bar{\mathbf{B}}^{\mathrm{c}} = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$$

are obtained in the same way as the matrices

$$\bar{\mathbf{A}}^{\mathrm{c}}_{\sigma} = (0,1,1), \quad \bar{\mathbf{A}}^{\mathrm{c}\bar{\mathrm{c}}}_{\sigma} = (1,0), \quad \bar{\mathbf{B}}^{\mathrm{c}}_{\sigma} = 1\,.$$

Since the matrices $\bar{\mathbf{A}}^{\mathrm{c}}$ and $\bar{\mathbf{A}}^{\bar{\mathrm{c}}}$ are companion matrices, each of them has only one non-unity invariant polynomial, $c_{\bar{\mathbf{A}}^{\mathrm{c}}}(a)$ and $c_{\bar{\mathbf{A}}^{\bar{\mathrm{c}}}}(a)$, the coefficients of which are are just the elements of the matrices $\bar{\mathbf{A}}^{\mathrm{c}}_{\sigma}$ and $\bar{\mathbf{A}}^{\bar{\mathrm{c}}}_{\sigma}$, respectively. Hence,

$$c_{\bar{\mathbf{A}}^{\mathrm{c}}}(a) = a^3 + a^2 + a = a\,(a^2 + a + 1), \quad c_{\bar{\mathbf{A}}^{\bar{\mathrm{c}}}}(a) = a^2 + a + 1\,,$$

which in view of Theorem 5.16 reveals the Smith normal form of the dynamics $\bar{\mathbf{A}}$ after decoupling.[15] Note that $c_{\bar{\mathbf{A}}^{\bar{\mathrm{c}}}}(a)$ is an invariant polynomial with regard to the uncontrollable subsystem. Therefore, it has to be enclosed in the set of desired closed-loop elementary divisor polynomials.

Let the desired (single) closed-loop invariant polynomial with respect to the controllable subsystem be $c_{\bar{\mathbf{A}}^{\mathrm{c}},\mathbf{K}}(a) = (a+1)(a^2+a+1)$. This choice satisfies Rosenbrock's control structure theorem, Theorem 5.4, since $\deg(c_{\bar{\mathbf{A}}^{\mathrm{c}},\mathbf{K}}(a)) = c_1 = 3$ and additionally $c_{\bar{\mathbf{A}}^{\bar{\mathrm{c}}}}(a) | c_{\bar{\mathbf{A}}^{\mathrm{c}},\mathbf{K}}(a)$. Consequently, the CSSP with desired closed-loop elementary divisor polynomials

$$p_1(\lambda) = a+1, \quad p_2(\lambda) = a^2+a+1, \quad p_3(\lambda) = a^2+a+1$$

is solvable.

Obviously, the algorithm in Theorem 5.2.4 returns the denominator matrix

$$\mathbf{D}^{\star}_{\bar{\mathbf{K}}^{\mathrm{c}}}(a) = (a+1)(a^2+a+1)$$

which according to equation (5.30) yields

$$\mathbf{A}^{\mathrm{c}}_{\sigma,\bar{\mathbf{K}}^{\mathrm{c}}} \begin{pmatrix} 1 \\ a \\ a^2 \end{pmatrix} = a^3 + (a+1)(a^2+a+1) = 1\,.$$

By comparing coefficients this means that

$$\mathbf{A}^{\mathrm{c}}_{\sigma,\bar{\mathbf{K}}^{\mathrm{c}}} = (1,0,0)\,.$$

[15] This Smith normal form is different from the Smith normal form $\mathbf{S}(\lambda) = \mathrm{diag}(a\,(a^2+a+1)^2, 1, \ldots, 1)$ of the coupled dynamics matrix $\bar{\mathbf{A}}$ which is in full accordance with Corollary 5.2 because equation (5.55) has no solution.

With respect to the controllable part, using equation (5.31) results in the feedback matrix

$$\bar{\mathbf{K}}^{\mathrm{c}} = (\bar{\mathbf{B}}^{\mathrm{c}}_{\sigma})^{-1}(\mathbf{A}^{\mathrm{c}}_{\sigma,\bar{\mathbf{K}}^{\mathrm{c}}} + \mathbf{A}^{\mathrm{c}}_{\sigma}) = (1,1,1)\,.$$

Simple inspection, or reference to equation (5.53), yields the decoupling state feedback matrix

$$\bar{\mathbf{K}}^{\mathrm{c}\,\bar{\mathrm{c}}} = (1,0)\,.$$

With these results, the overall feedback matrix finally reads

$$\mathbf{K} = (\bar{\mathbf{K}}^{\mathrm{c}}, \bar{\mathbf{K}}^{\mathrm{c}\,\bar{\mathrm{c}}})\,\bar{\mathbf{Q}} = (1,0,0,1,1)\,.$$

Conclusion

In this chapter, a method for solving the cycle sum synthesis problem (CSSP) is presented for the first time. This problem is solved by an algorithm that fits a given multiple-input LMS, for instance representing a linear automaton model, with a specific cycle and/or tree structure in its state graph. In view of the analysis part, Chapter 4, this clearly means to alter the set of invariant polynomials of the dynamics matrix into a set of desired ones by determining an adequate input sequence. As this problem is strongly related to controllability, first, the notion of controllability is recalled from linear continuous system theory and reinterpreted into the finite field case. It turns out that this concept applies as it stands due to the field property.

Rosenbrock's control structure theorem is known to be the appropriate means for answering the question of when a linear state feedback exists that sets desired closed-loop invariant polynomials by linear state feedback. Fortunately, this theorem is valid for systems over finite fields as well, and as a consequence, an answer to the question whether a CSSP can be solved by linear state feedback can always be given.

For synthesizing a linear state feedback, however, original domain methods for multiple-input system synthesis as for example the parametric approach show to be insufficient for solving the CSSP — occurring problems are discussed extensively. In this context, the crucial problem is that an extension field is required for expressing eigenvalues and respective chains of generalized eigenvectors. For finite fields the concept of an extension field is more involved because generally polynomials do not factor in a common extension field. Thus, employing the parametric approach becomes very cumbersome — see Appendix C for the symbolic calculation effort. These problems naturally lead to synthesis methods in an image domain where polynomial factorizations in extension fields can be avoided.

The method employed here is the polynomial matrix method. It allows a complete specification of the invariant polynomials in the closed-loop dynamics, hence, solving the CSSP. Its main ingredients are polynomial matrix fractions of transfer matrices in an image domain. For LMS in

a particular state space representation, in the so-called controller companion form (CCF), a right-prime right polynomial matrix fraction in the image domain is obtained as an analytic expression without refactorization of the transfer matrix. Two other properties associated to representations in CCF proof to be of major value: feedback leaves the CCF-structure invariant, a property that is preserved in the image domain as well. Additionally, for systems over finite fields the similarity transform into CCF over finite fields is not subject to numerical problems by ill-conditioned matrices, consequently, the inversion of the (reduced) controllability matrix is unproblematic. By virtue of this factorization it can easily be seen that the closed-loop denominator (polynomial) matrix of the right-prime right polynomial matrix fraction for the LMS in CCF-representation can be specified to exact the extent which is imposed by Rosenbrock's control structure theorem — it is just this denominator matrix that has to comprise the desired closed-loop nonunity invariant polynomials. Therefore, by referring to such a closed-loop denominator matrix, if in accordance with the control structure theorem, a feedback matrix is determined without involving the solution of a diophantine equation. The main result is a synthesis algorithm which for a controllable LMS receives a set of desired closed-loop invariant polynomials as an input and returns a suitable denominator matrix — as long as the CSSP is solvable.

The second part of the chapter extends the results to LMS with an uncontrollable subsystem. To this end, the state equation of the LMS is transformed into an adapted CCF which reveals the autonomous uncontrollable subsystem. In light of the afore-presented synthesis algorithm which is based on controllability of the LMS, a separation into controllable and uncontrollable subsystems is ensured by a decoupling. This further breaks the influence of the initial state with respect to the uncontrollable subsystem on the evolution of state regarding the controllable subsystem. It is shown that such a decoupling exists for arbitrary LMS with uncontrollable part. As decoupling can alter the invariant polynomials of the dynamics matrix a novel criterion is developed which draws an exact line between when a decoupling takes an influence and when it entails no influence on the invariant polynomials. This criterion extends the well-known fact that such a decoupling cannot change the characteristic polynomial of the closed-loop dynamics. As a result, for uncontrollable LMS under decoupling, again, the afore-developed synthesis algorithm can be used for specifying the invariant polynomials, this time with respect to the controllable subsystem.

Chapter 6

Conclusions and Future Work

In this dissertation, a discrete state space model over a finite field is presented. For linear systems of this kind, methods are developed that allow a structural analysis and feedback controller synthesis. The general philosophy throughout this work is not to invoke deeper knowledge about finite ring theory but instead to ground the development and the proofs on a fundamental level of matrix theory. This way, a less involved but still consistent theory of linear systems over a finite field is given.

6.1 Summary

The mathematical preliminaries in Chapter 2 recall the algebraic fundamentals which are indispensable for a theoretical treatment of discrete dynamic systems over finite fields. In particular, the basic concepts of finite groups and finite fields are emphasized since these concepts imply some peculiarities for polynomials over finite fields, e. g. their periodicity and reducibility properties. In view of the subsequent analysis and synthesis methods, a review of an elementary level of linear algebra is given so as to motivate structural invariants of linear systems like invariant polynomials and elementary divisor polynomials. The closing part of the chapter briefly establishes a $\mathcal{Z}$-domain-like image domain for functions over finite fields, which due to its similarity to the $\mathcal{Z}$-domain formulae provides the benefit of using a variety of image domain methods for continuous systems.

For an illustration of the underlying idea of discrete dynamic systems over finite fields, first, a simple conveyor belt example is discussed at the beginning of Chapter 3. This example underlines the need for formal methods for deriving a model that describes the input-dependent evolution of state for such systems. For this purpose, a coding scheme that permits to determine a purely algebraic transition relation, similar to a state space model in the continuous world, is introduced.

Its construction is confined to the case of the finite field with characteristic 2 which is shown to be isomorphic to a boolean ring with the consequence that basics from boolean algebra can be employed for the model construction. Two ways for deriving this model have been pointed out: the first method invokes the calculation of the disjunctive normal form, elimination of the negations and using the law of DeMorgan. The second method is based on Reed-Muller generator matrices which prove to be tailored for the problem as less computation effort is required for deriving the coefficients of the transition function in view. In a general prospect, both methods yield a scalar implicit multilinear transition relation over the finite field with characteristic 2. If the systems under consideration are deterministic then this transition relation becomes a transition function. For depicting the ease of use of the Reed-Muller generator matrix method, it is applied to the conveyor belt example.

In Chapter 4 autonomous linear systems over finite fields are considered. The main result is that for the class of finite state automata which can be represented as autonomous linear modular systems, for the first time, a necessary and sufficient criterion is deduced that allows to determine all automaton cycles in length and number, the so-called cycle sum. For using this criterion, the periods of the periodic elementary divisor polynomials regarding the system dynamics matrix have to be determined. These periods are in strong relation with a complete decomposition of the state space into periodic subspaces, hence, are in strong relation with a respective criterion for the automaton cycles. It is worth mentioning that this criterion does not resort to a state space enumeration procedure, what, apart from more elegance, promises less calculation effort as long as the required periods can be found in tabulars (true for polynomial degrees of about 100). In contrast, the portion of non-periodic elementary divisor polynomials does not contribute to the cyclic behavior, but instead it entirely constitutes the state transition behavior which takes the form of a tree in a state graph. The results are superposed in a general statement on autonomous linear modular systems. The final part of this chapter gives answers to the afore-posed questions for systems that are extended by an affine constant term.

The final contribution of this dissertation, in Chapter 5, is to present the first method for solving the cycle sum synthesis problem for non-autonomous linear modular systems. In light of the results from Chapter 4 this task is associated with specifying the elementary divisor polynomials of the system dynamics. Assuming controllability it is shown that the cycle sum synthesis problem can be solved for non-autonomous systems by closing the loop; naturally referring to the notion of state feedback. As standard strategies for the computation of feedback for multiple-input systems like the parametric approach turn out to be inadequate for solving the problem, methods which encompass the synthesis of invariant polynomials have to be used. In this regard, image domain methods are found to be suitable. The proposed solution of the cycle sum synthesis problem is twofold. In a first step, Rosenbrock's control structure theorem is recalled in order to answer the question whether a state feedback exists that fits the closed-loop dynamics matrix with a desired set of elementary divisor polynomials. If this answer is positive, in a second step, such a feedback matrix

is determined by modifying the denominator matrix of a right-prime right polynomial matrix fraction of the transfer matrix with respect to the system in controllability companion form. The result is an algorithm that computes the denominator matrix of the right-prime right polynomial matrix fraction corresponding to the desired closed-loop transfer matrix, which after simple calculations yields a desired state feedback matrix. An advantage of this controllability companion form based approach is that the solution of a Diophantine equation for obtaining the state feedback matrix is not necessary. The second part of this chapter enhances the setting on systems with uncontrollable subsystem. To this end, an adapted form of the controllability companion form is introduced which reveals the controllable and uncontrollable subsystem. In order to break the influence of the initial state with regard to the uncontrollable subsystem, both subsystems are decoupled, which is shown to be feasible for arbitrary linear modular systems with uncontrollable part. A further result provides a criterion of when a decoupling has an influence on the elementary divisor polynomials of the system dynamics, which extends the well-known fact that such a decoupling cannot change the characteristic polynomial of the closed-loop dynamics. Finally, a procedure is proposed which allows to apply the afore-presented algorithm for the controllable subsystem, leaving the characteristic polynomial of the uncontrollable subsystem unchanged.

6.2 Future Work

Many practically relevant systems are non-linear in nature, which for systems over finite fields means polynomially non-linear. For facing this problem, the development of appropriate linearization techniques may be a first conceivable step of future work. In a next step, further research may keep track of the non-linear case, for which then real non-linear methods for analysis and control have to be established. Potentially fruitful work could be based on using ideal theoretic methods like Gröbner-bases [CLO98] for effective transformations of non-linear system models [NMGJ01], as proposed in the advanced approaches worked out in Rennes [Mar97, ML97, ML99, PML99] and Linköping [Ger95, Gun97]. In this regard, some attention could be directed to the structural analysis of the non-linear transition equations.

Appendix A

Permutations of a Block Matrix

Let a matrix $\mathbf{A} \in \mathbb{F}^{n\times n}$ be partitioned in blocks as per

$$\mathbf{A} = \begin{pmatrix} \mathbf{A}_{11} & \mathbf{A}_{12} & \cdots & \mathbf{A}_{1p} \\ \mathbf{A}_{21} & \mathbf{A}_{22} & \cdots & \mathbf{A}_{2p} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{A}_{p1} & \mathbf{A}_{p2} & \cdots & \mathbf{A}_{pp} \end{pmatrix}, \quad \mathbf{A}_{ij} \in \mathbb{F}^{d_i \times d_j}, \quad i,j = 1,\ldots,p \tag{A.1}$$

with $n = \sum_{i=1}^{p} d_i$. An other composition out of the same submatrices $\mathbf{A}_{ij}$ from $\mathbf{A}$ that shows the same structure is the block matrix

$$\bar{\mathbf{A}} = \begin{pmatrix} \mathbf{A}_{k_1k_1} & \mathbf{A}_{k_1k_2} & \cdots & \mathbf{A}_{k_1k_p} \\ \mathbf{A}_{k_2k_1} & \mathbf{A}_{k_2k_2} & \cdots & \mathbf{A}_{k_2k_p} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{A}_{k_pk_1} & \mathbf{A}_{k_pk_2} & \cdots & \mathbf{A}_{k_pk_p} \end{pmatrix}, \quad \mathbf{A}_{k_ik_j} \in \mathbb{F}^{d_{k_i}\times d_{k_j}}, \quad k_i,k_j = 1,\ldots,p, \tag{A.2}$$

which results from a permutation of the submatrices in $\mathbf{A}$ with respect to the permutation of dimension numbers from $(d_1,\ldots,d_p)$ into $(d_{k_1},\ldots,d_{k_p})$.

The following theorem is a straight-forward extension of the notion of an elementary matrix with scalar entries to an elementary matrix with matrix entries, a collection of which provides the necessary row and column permutations for transforming $\mathbf{A}$ into $\bar{\mathbf{A}}$.

Theorem A.1 (Permutation Matrix of a Block Matrix)
Let $\mathbf{A} \in \mathbb{F}^{n\times n}$ be a block matrix as denoted in equation (A.1) with the respective ordered set of dimension numbers $(d_1,\ldots,d_p)$. Let $\bar{\mathbf{A}} \in \mathbb{F}^{n\times n}$ be a block matrix that is a an other composition of the submatrices with respect to $\mathbf{A}$ as per equation (A.2) with the ordered set of dimension numbers

$(d_{k_1},\ldots,d_{k_p})$. Then the matrix

$$\mathbf{\Pi} = \begin{pmatrix} \mathbf{\Pi}_{11} & \mathbf{\Pi}_{12} & \cdots & \mathbf{\Pi}_{1p} \\ \mathbf{\Pi}_{21} & \mathbf{\Pi}_{22} & \cdots & \mathbf{\Pi}_{2p} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{\Pi}_{p1} & \mathbf{\Pi}_{p2} & \cdots & \mathbf{\Pi}_{pp} \end{pmatrix}, \quad \mathbf{\Pi}_{ij} = \begin{cases} \mathbf{I}_{d_{k_i}}, & j = k_i \\ \mathbf{0}_{d_{k_i} d_j}, & j \neq k_i \end{cases} \tag{A.3}$$

is orthogonal and transforms the block matrix $\mathbf{A}$ into the block matrix $\bar{\mathbf{A}}$ according to

$$\bar{\mathbf{A}} = \mathbf{\Pi}\mathbf{A}\mathbf{\Pi}^{\mathrm{T}}. \tag{A.4}$$

□

Example A.1
The block matrix

$$\mathbf{A} = \begin{pmatrix} \mathbf{A}_{11} & \mathbf{A}_{12} & \mathbf{A}_{13} \\ \mathbf{A}_{21} & \mathbf{A}_{22} & \mathbf{A}_{23} \\ \mathbf{A}_{31} & \mathbf{A}_{32} & \mathbf{A}_{33} \end{pmatrix}, \quad \mathbf{A}_{ij} \in \mathbb{F}^{d_i \times d_j}, \quad i,j = 1,\ldots,3$$

with the ordered set of dimension numbers (d_1,d_2,d_3) is to be transformed into

$$\bar{\mathbf{A}} = \begin{pmatrix} \mathbf{A}_{33} & \mathbf{A}_{31} & \mathbf{A}_{32} \\ \mathbf{A}_{13} & \mathbf{A}_{11} & \mathbf{A}_{12} \\ \mathbf{A}_{23} & \mathbf{A}_{21} & \mathbf{A}_{22} \end{pmatrix}.$$

The ordered set of dimension numbers associated to $\bar{\mathbf{A}}$ is (d_3,d_1,d_2), hence, $k_1 = 3$, $k_2 = 1$, $k_3 = 2$ and the permutation matrix becomes

$$\mathbf{\Pi} = \begin{pmatrix} \mathbf{0}_{d_3 d_1} & \mathbf{0}_{d_3 d_2} & \mathbf{I}_{d_3} \\ \mathbf{I}_{d_1} & \mathbf{0}_{d_1 d_2} & \mathbf{0}_{d_1 d_3} \\ \mathbf{0}_{d_2 d_1} & \mathbf{I}_{d_2} & \mathbf{0}_{d_2 d_3} \end{pmatrix}$$

with the respective square identity matrices and generally non-square zero matrices. □

Appendix B

The Transformation Matrix on Rational Canonical Form

For any matrix $\mathbf{A}$ over a finite field $\mathbb{F}_q$ the command `frobenius` in the *Share-Library* of the computer algebra package Maple® admits to calculate the so-called frobenius normal form $\mathbf{A}_{\mathrm{F}}$, which is a rational canonical form with respect to the invariant polynomials in non-factored form; the corresponding procedure returns the transformation matrix $\mathbf{T}_{\mathrm{F}}$ as well. This procedure can be used to determine the transformation matrix $\mathbf{T}$ which transforms $\mathbf{A}$ into the rational canonical form $\mathbf{A}_{\mathrm{rat}}$. To this end, it is taken advantage from the following relations.

By definition

$$\mathbf{A}_{\mathrm{rat}} = \mathbf{T}\mathbf{A}\mathbf{T}^{-1} \tag{B.1}$$

and

$$\mathbf{A}_{\mathrm{F}} = \mathbf{T}_{\mathrm{F}}\mathbf{A}\mathbf{T}_{\mathrm{F}}^{-1}. \tag{B.2}$$

Since $\mathbf{A}_{\mathrm{rat}}$ and $\mathbf{A}_{\mathrm{F}}$ are similar matrices it is clear that

$$\mathbf{A}_{\mathrm{F}} = \mathbf{Q}\mathbf{A}_{\mathrm{rat}}\mathbf{Q}^{-1} \tag{B.3}$$

being equivalent to

$$\mathbf{A}_{\mathrm{rat}} = \mathbf{Q}^{-1}\mathbf{A}_{\mathrm{F}}\mathbf{Q} \tag{B.4}$$

which employing equation (B.2) can be transformed into

$$\mathbf{A}_{\mathrm{rat}} = \mathbf{Q}^{-1}\mathbf{T}_{\mathrm{F}}\mathbf{A}(\mathbf{Q}^{-1}\mathbf{T}_{\mathrm{F}})^{-1}. \tag{B.5}$$

A comparison with equation (B.1) yields the required

$$\mathbf{T} = \mathbf{Q}^{-1}\mathbf{T}_{\mathrm{F}}, \tag{B.6}$$

because the matrices $\mathbf{Q}$ and $\mathbf{T}_{\mathrm{F}}$ are at one's disposal after transforming $\mathbf{A}$ and $\mathbf{A}_{\mathrm{rat}}$ both into $\mathbf{A}_{\mathrm{F}}$ via equations (B.2) and (B.3), using the Maple® command `frobenius`.

Appendix C

The Jordan Normal Form over an Extension Field of $\mathbb{F}_q$

For completeness, the Jordan normal form of a matrix over a finite field $\mathbb{F}_q$ shall be derived in an exemplary, tutorial manner.[1] For simplicity, let a matrix in $\mathbb{F}_2^{8\times 8}$ be given as

$$\mathbf{A} := \begin{pmatrix} 0&0&0&0&0&1&0&0\\ 1&0&0&0&0&0&0&0\\ 0&1&0&0&0&1&0&0\\ 0&0&1&0&0&0&0&0\\ 0&0&0&1&0&0&0&0\\ 0&0&0&0&1&0&0&0\\ 0&0&0&0&0&0&0&1\\ 0&0&0&0&0&0&1&1 \end{pmatrix},$$

in rational canonical form. The respective Smith normal form $\mathbf{S}(\lambda) = \mathbf{U}(\lambda)\,(\lambda\mathbf{I} - \mathbf{A})\mathbf{V}(\lambda)$ reads

$$\begin{aligned} \mathbf{S}(\lambda) &= \operatorname{diag}\big(c(\lambda), 1, 1, 1, 1, 1, 1, 1\big),\\ c(\lambda) = \lambda^8+\lambda^7+\lambda^6+\lambda^4+\lambda^3+\lambda+1 &= \underbrace{(\lambda^3+\lambda+1)^2}_{=:\,p_1(\lambda)}\,\underbrace{(\lambda^2+\lambda+1)}_{=:\,p_2(\lambda)}, \end{aligned}$$

where $p_1(\lambda)$ and $p_2(\lambda)$ are the elementary divisor polynomials in $\mathbb{F}_2[\lambda]$. The corresponding transformation matrices are

$$\mathbf{U}(\lambda) = \begin{pmatrix} \lambda^3+\lambda^2+\lambda & \lambda^4+\lambda^3+\lambda^2 & \lambda^5+\lambda^4+\lambda^3 & \lambda^6+\lambda^5+\lambda^4 & \lambda^7+\lambda^6+\lambda^5 & \lambda^4+\lambda^3+\lambda+1 & \lambda^8+\lambda^4+\lambda^2 & \lambda^6+\lambda^2+1\\ \lambda^2 & \lambda^3 & \lambda^4 & \lambda^5 & \lambda^6 & \lambda^3+\lambda & \lambda^7+\lambda^6+\lambda^4+\lambda^2+1 & \lambda^5+\lambda^4+\lambda^2+1\\ 0&0&0&0&0&0&1&0\\ 1&\lambda&\lambda^2+1&\lambda^3+\lambda&\lambda^4+\lambda^2&\lambda&0&0\\ 0&0&0&0&1&0&0&0\\ 0&0&0&1&0&0&0&0\\ 0&1&0&0&0&0&0&0\\ 0&0&1&0&0&0&0&0 \end{pmatrix}$$

[1] It is assumed that the reader is familiar with the derivation of the (complex) Jordan normal form for matrices with coefficients over the field of real numbers $\mathbb{R}$. For the details from finite field algebra refer to [LN94].

and

$$\mathbf{V}(\lambda) = \begin{pmatrix} \lambda^{13}+\lambda^{11}+\lambda^6+\lambda^4+\lambda^3+\lambda^2 & \lambda^6+\lambda^4+\lambda^2 & \lambda^6+\lambda^4+\lambda^2 & \lambda & 0 & 0 & 1 & 0 \\ \lambda^{12}+\lambda^{10}+\lambda^5+\lambda^3+\lambda^2+\lambda & \lambda^5+\lambda^3+\lambda & \lambda^5+\lambda^3+\lambda & 1 & 0 & 0 & 0 & 0 \\ \lambda^9+\lambda^5+\lambda^3+\lambda^2 & \lambda^2 & \lambda^2 & 0 & \lambda & 1 & 0 & 0 \\ \lambda^8+\lambda^4+\lambda^2+\lambda & \lambda & \lambda & 0 & 1 & 0 & 0 & 0 \\ \lambda^7+\lambda^3+\lambda+1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ \lambda^{12}+\lambda^6+\lambda^5+\lambda^4+\lambda^2+\lambda & \lambda^5+\lambda & \lambda^5+\lambda & 1 & \lambda^2 & \lambda & 0 & 1 \\ \lambda^7+\lambda^3+\lambda & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ \lambda^8+\lambda^4+\lambda^2 & \lambda & 1 & 0 & 0 & 0 & 0 & 0 \end{pmatrix},$$

all operations to be taken modulo 2.

The Jordan-form of a matrix is based on a linear factor representation of the elementary divisor polynomials over some splitting field, i. e. an extension field in which such a factorization is possible. For a finite field $\mathbb{F}_q$ the respective extension fields are defined upon the same operations as $\mathbb{F}_q$ and have the same characteristic q. In contrast to $\mathbb{F}_q$, the extension fields contain q^n elements — that is why those fields are denoted by $\mathbb{F}_{q^n}$. Any field element of $\mathbb{F}_{q^n}$ can be represented as a polynomial in $\mathbb{F}_q[\gamma]$ with a field-specific element γ that is a symbolic zero[2] of an n-th degree irreducible polynomial $p_{\text{irr}} \in \mathbb{F}_q[\lambda]$ and calculations can be carried out in the associated residue class ring $\mathbb{F}_q[\lambda]/p_{\text{irr}}(\lambda)$. Consequently, any polynomial $f \in \mathbb{F}_q[\lambda]$ is reduced with $p_{\text{irr}}(\lambda)$ by taking the remainder polynomial $r(\lambda)$ from

$$f(\lambda) = p_{\text{irr}}(\lambda)\, q(\lambda) + r(\lambda)\,,$$

obtained after possibly successive polynomial divisions until the degree of $r(\lambda)$ is less than the degree of $p_{\text{irr}}(\lambda)$. An irreducible polynomial of degree n over a finite field $\mathbb{F}_q$ splits into linear factors in any extension field $\mathbb{F}_{q^m}$ for which $n|m$. Hence, $\mathbb{F}_{q^n}$ is the least such splitting extension field because it contains the fewest field elements.

Therefore in the example problem, the irreducible basis polynomials with respect to the elementary divisor polynomials $p_1(\lambda)$ and $p_2(\lambda)$,

$$p_{\text{irr},1}(\lambda) = \lambda^3+\lambda+1, \quad p_{\text{irr},2}(\lambda) = \lambda^2+\lambda+1\,,$$

can be factored according to[3]

$$p_{\text{irr},1}(\lambda) = (\lambda+\lambda_{1,1})(\lambda+\lambda_{1,2})(\lambda+\lambda_{1,3}), \quad p_{\text{irr},2}(\lambda) = (\lambda+\lambda_{2,1})(\lambda+\lambda_{2,2})\,,$$

where $\lambda_{1,1}, \lambda_{1,2}, \lambda_{1,3} \in \mathbb{F}_{2^3}$ and $\lambda_{2,1}, \lambda_{2,2} \in \mathbb{F}_{2^2}$ are the zeroes in the extension fields $\mathbb{F}_{2^3}$ and $\mathbb{F}_{2^2}$.

[2] A customary analog is the symbolic zero "i" of the polynomial λ^2+1 over the field of real numbers $\mathbb{R}$. This symbolic zero is sufficient for describing any complex number in a polynomial of degree one.

[3] In the finite field $\mathbb{F}_2$ addition and subtraction coincide.

Now assume that α is a zero (in a splitting extension field of $\mathbb{F}_q$) of an n-th degree polynomial that is irreducible over $\mathbb{F}_q$. Then from [LN94] recall that all n zeroes of this polynomial can be written as

$$\alpha,\ \alpha^q,\ \alpha^{q^2},\ \ldots\ ,\ \alpha^{q^{n-1}}.$$

In the example, if $\alpha \in \mathbb{F}_{2^2}$ is a zero of $p_{\mathrm{irr},2}(\lambda) = \lambda^2+\lambda+1$ then substituting this zero in the identity $\lambda^2 = (\lambda^2+\lambda+1)+\lambda+1$ yields $\alpha^2 = \alpha+1$, accordingly,

$$p_{\mathrm{irr},2}(\lambda) = \lambda^2+\lambda+1 = (\lambda+\alpha)(\lambda+\alpha^2) = (\lambda+\alpha)(\lambda+\alpha+1)\,.$$

In general, the elements of $\mathbb{F}_{q^n}$ can be interpreted as the zeroes of the polynomial

$$\lambda^{q^n}-\lambda = \lambda(\lambda-1)\cdots(\lambda-(q-1))\,\rho(\lambda)\,,$$

in which $\rho(\lambda)$ is a polynomial that contains exactly those polynomials irreducible over $\mathbb{F}_q$ the degree of which is a proper divisor of n.[4] It is clear that the elements of $\mathbb{F}_q$ are always included in its extension fields. Additionally, in the particular case $\mathbb{F}_2$ it follows that

$$\lambda^{2^n}+\lambda = \lambda(\lambda+1)\sum_{i=0}^{2^n-2}\lambda^i\,.$$

Resorting to the example, the elements of $\mathbb{F}_{2^3}$ are the zeroes of

$$\lambda^{2^3}+\lambda = \lambda^8+\lambda = \lambda(\lambda+1)\sum_{i=0}^{6}\lambda^i = \lambda(\lambda+1)(\lambda^3+\lambda^2+1)(\lambda^3+\lambda+1)\,,$$

a polynomial that comprises all third degree irreducible polynomials over $\mathbb{F}_2$, and analogously, the elements of $\mathbb{F}_{2^2}$ are the zeroes of

$$\lambda^{2^2}+\lambda = \lambda^4+\lambda = \lambda(\lambda+1)(\lambda^2+\lambda+1)\,.$$

For an n-th degree polynomial $p \in \mathbb{F}_q[\lambda]$ that consists of $i = 1,\ldots,N$ irreducible factor polynomials $p_{\mathrm{irr},i}$ of degree δ_i to the power of e_i, i. e.

$$p(\lambda) = p_{\mathrm{irr},1}^{e_1}(\lambda)\cdots p_{\mathrm{irr},N}^{e_N}(\lambda)\,,$$

[4] In the ring $\mathbb{F}_q[\lambda]$ the number $N_q(n)$ of monic irreducible polynomials of degree n is given by

$$N_q(n) = \frac{1}{n}\sum_{d|n}\mu\left(\frac{n}{d}\right)q^d$$

in which the summation is carried out over all divisors d of n.

The function $\mu(d)$ is the Möbius-function

$$\mu(d) = \begin{cases} 1 & \text{if } d = 1 \\ (-1)^k & \text{if } d \text{ is the product of } k \text{ distinct primes} \\ 0 & \text{if } d \text{ is divisible by the square of a prime} \end{cases}$$

the least extension field which contains all N fields $\mathbb{F}_{q^{\delta_i}}$ is the field $\mathbb{F}_{q^\delta}$ with $\delta = \operatorname{lcm}(\delta_i, \ldots, \delta_N)$. Consequently, if the degree $n = \sum_{i=1}^{N} \delta_i e_i$ of polynomial p is divisible by the square of some prime number then $\delta < n$.

Returning to the example, an extension field for factoring the invariant polynomial $c(\lambda)$ into linear factors has to contain both finite fields, $\mathbb{F}_{2^3}$ and $\mathbb{F}_{2^2}$. In consequence, $\delta = 6$ and $\mathbb{F}_{2^6}$ is the least appropriate field.

Furthermore, an irreducible polynomial of degree 6 is needed for describing the elements of $\mathbb{F}_{2^6}$, e. g. $\lambda^6 + \lambda^3 + 1$. Let γ denote a zero of this polynomial in $\mathbb{F}_{2^6}$. With the arguments from above, using γ any field element of $\mathbb{F}_{2^6}$ can be represented as a polynomial in the ring $\mathbb{F}_2[\gamma]$ of maximal degree 5. It turns out that $c(\lambda)$ splits into linear factors according to

$$c(\lambda) = \underbrace{(\lambda+\gamma^3)(\lambda+\gamma^3+1)}_{=\lambda^2+\lambda+1} \underbrace{(\lambda+\gamma^4+\gamma^2+\gamma)^2(\lambda+\gamma^5+\gamma^4)^2(\lambda+\gamma^5+\gamma^2+\gamma)^2}_{=(\lambda^3+\lambda+1)^2}$$

with the respective zeroes

$$\lambda_1 = \gamma^3, \quad \lambda_2 = \gamma^3+1, \quad \lambda_3 = \gamma^4+\gamma^2+\gamma, \quad \lambda_4 = \gamma^5+\gamma^4, \quad \lambda_5 = \gamma^5+\gamma^2+\gamma.$$

Note that given the zeroes λ_1 and λ_3 the other zeroes are implied by

$$\begin{aligned}
(\gamma^3)^2 &= (\gamma^6+\gamma^3+1)+\gamma^3+1 = \gamma^3+1 \\
(\gamma^4+\gamma^2+\gamma)^2 &= (\gamma^6+\gamma^3+1)\gamma^2+\gamma^5+\gamma^4 = \gamma^5+\gamma^4 \\
(\gamma^5+\gamma^4)^4 &= (\gamma^6+\gamma^3+1)(\gamma^4+\gamma^2+\gamma)+\gamma^5+\gamma^2+\gamma = \gamma^5+\gamma^2+\gamma
\end{aligned}$$

which is in accordance with above since

$$\lambda_2 = \lambda_1^2, \quad \lambda_4 = \lambda_3^2, \quad \lambda_5 = \lambda_3^4.$$

Note that $\lambda_1, \ldots, \lambda_5$ are the eigenvalues of $\mathbf{A}$ rendering the respective characteristic matrix $\lambda_i \mathbf{I} - \mathbf{A}$ singular. Matrix $\mathbf{A}$ has 5 elementary divisor polynomials over the splitting field $\mathbb{F}_{2^6}$, thus, there are 5 Jordan-chains in the Jordan matrix: 3 of length 2 and 2 of length 1. As a result, the Jordan-form reads

$$\mathbf{J} = \begin{pmatrix}
\lambda_1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & \lambda_2 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & \lambda_3 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & \lambda_3 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & \lambda_4 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & \lambda_4 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & \lambda_5 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & \lambda_5
\end{pmatrix} = \begin{pmatrix}
\gamma^3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & \gamma^3+1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & \gamma^4+\gamma^2+\gamma & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & \gamma^4+\gamma^2+\gamma & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & \gamma^5+\gamma^4 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & \gamma^5+\gamma^4 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & \gamma^5+\gamma^2+\gamma & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & \gamma^5+\gamma^2+\gamma
\end{pmatrix}.$$

The associated transformation matrix $\mathbf{T}$ which transforms the matrix $\mathbf{A}$ into its similar Jordan-matrix $\mathbf{J}$ as per $\mathbf{A} = \mathbf{T}\mathbf{J}\mathbf{T}^{-1}$ is given by the respective Jordan-chains of generalized eigenvectors $\mathbf{v}_i^j$ for the i-th elementary divisor polynomials. These comply with the recursion

$$(\lambda_i \mathbf{I} - \mathbf{A})\,\mathbf{v}_i^{j+1} = \mathbf{v}_i^j, \quad (\lambda_i \mathbf{I} - \mathbf{A})\,\mathbf{v}_i^0 = \mathbf{0},$$

for any eigenvalue λ_i of $\mathbf{A}$. Here, the Jordan-chains for the $i = 1,\ldots,5$ eigenvalues λ_i result in

$$\mathbf{v}_1^0, \qquad \mathbf{v}_2^0, \qquad \mathbf{v}_3^0 \to \mathbf{v}_3^1, \qquad \mathbf{v}_4^0 \to \mathbf{v}_4^1, \qquad \mathbf{v}_5^0 \to \mathbf{v}_5^1$$

with

$$\mathbf{v}_1^0 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ \gamma^3 \end{pmatrix}, \quad \mathbf{v}_2^0 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ \gamma^3+1 \end{pmatrix}, \quad \mathbf{v}_3^0 = \begin{pmatrix} \gamma^5+\gamma^2+\gamma \\ \gamma^4+\gamma^2+\gamma+1 \\ \gamma^4+\gamma^2+\gamma \\ 1 \\ \gamma^5+\gamma^4+1 \\ \gamma^5+\gamma^2+\gamma+1 \\ 0 \\ 0 \end{pmatrix}, \quad \mathbf{v}_3^1 = \begin{pmatrix} \gamma^4+\gamma^2+\gamma+1 \\ 0 \\ 1 \\ 0 \\ \gamma^5+\gamma^2+\gamma+1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

$$\mathbf{v}_4^0 = \begin{pmatrix} 1 \\ \gamma^5+\gamma^2+\gamma+1 \\ \gamma^4+\gamma^2+\gamma \\ \gamma^5+\gamma^4+1 \\ \gamma^5+\gamma^2+\gamma \\ \gamma^5+\gamma^4 \\ 0 \\ 0 \end{pmatrix}, \quad \mathbf{v}_4^1 = \begin{pmatrix} 0 \\ \gamma^4+\gamma^2+\gamma+1 \\ 0 \\ \gamma^5+\gamma^2+\gamma \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \quad \mathbf{v}_5^0 = \begin{pmatrix} \gamma^5+\gamma^2+\gamma \\ 1 \\ \gamma^5+\gamma^4+1 \\ \gamma^5+\gamma^4 \\ \gamma^5+\gamma^2+\gamma+1 \\ \gamma^4+\gamma^2+\gamma \\ 0 \\ 0 \end{pmatrix}, \quad \mathbf{v}_5^1 = \begin{pmatrix} 0 \\ \gamma^4+\gamma^2+\gamma+1 \\ 0 \\ \gamma^5+\gamma^2+\gamma+1 \\ 0 \\ \gamma^5+\gamma^2+\gamma \\ 0 \\ 0 \end{pmatrix}$$

showing the geometric multiplicity of one with respect to each eigenvalue. Hence, the respective transformation matrix reads

$$\mathbf{T} = \left(\mathbf{v}_1^0, \mathbf{v}_2^0, \mathbf{v}_3^0, \mathbf{v}_3^1, \mathbf{v}_4^0, \mathbf{v}_4^1, \mathbf{v}_5^0, \mathbf{v}_5^1\right).$$

Given for convenience, the respective inverse matrix is

$$\mathbf{T}^{-1} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & \gamma^3+1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & \gamma^3 & 1 \\ 0 & \gamma^5+\gamma^2+\gamma & 0 & \gamma^5+\gamma^4+1 & 0 & \gamma^4+\gamma^2+\gamma & 0 & 0 \\ \gamma^5+\gamma^2+\gamma & \gamma^5+\gamma^2+\gamma+1 & \gamma^5+\gamma^4+1 & 1 & \gamma^4+\gamma^2+\gamma & \gamma^5+\gamma^4 & 0 & 0 \\ 1 & 0 & \gamma^5+\gamma^2+\gamma & 0 & \gamma^4+\gamma^2+\gamma & 0 & 0 & 0 \\ \gamma^5+\gamma^4 & \gamma^5+\gamma^2+\gamma & \gamma^5+\gamma^4+1 & \gamma^4+\gamma^2+\gamma & \gamma^4+\gamma^2+\gamma+1 & \gamma^5+\gamma^2+\gamma+1 & 0 & 0 \\ \gamma^4+\gamma^2+\gamma+1 & 0 & \gamma^5+\gamma^2+\gamma & 0 & \gamma^5+\gamma^2+\gamma+1 & 0 & 0 & 0 \\ 1 & \gamma^5+\gamma^2+\gamma & \gamma^4+\gamma^2+\gamma & \gamma^5+\gamma^2+\gamma+1 & \gamma^5+\gamma^4 & \gamma^5+\gamma^4+1 & 0 & 0 \end{pmatrix}.$$

Remark C.1
The above-employed irreducible polynomial $\lambda^6+\lambda^3+1$ has the period $9 \neq 2^6-1$, hence, it is not a primitive polynomial. If choosing the irreducible polynomial $\lambda^6+\lambda+1$ instead, then $c(\lambda)$ is factorable as

$$c(\lambda) = (\lambda^2+\lambda+1)\,(\lambda^3+\lambda+1)^2 = (\lambda+\varepsilon^5+\varepsilon^4+\varepsilon^3+\varepsilon+1)(\lambda+\varepsilon^5+\varepsilon^4+\varepsilon^3+\varepsilon)$$
$$(\lambda+\varepsilon^3+\varepsilon^2+\varepsilon)^2(\lambda+\varepsilon^4+\varepsilon^2+\varepsilon+1)^2(\lambda+\varepsilon^4+\varepsilon^3+1)^2$$

in which $\varepsilon \in \mathbb{F}_{2^6}$ is a zero of $\lambda^6+\lambda+1$. Converse to the polynomial $\lambda^6+\lambda^3+1$, the polynomial $\lambda^6+\lambda+1$ is an irreducible polynomial of maximal period, hence $2^6-1=63$ is the period.

An important theorem in Galois-theory states that any non-zero element in an extension field $\mathbb{F}_{q^n}$ can be represented as some power of a zero of an n-th degree irreducible polynomial over $\mathbb{F}_q$ iff this polynomial is primitive. Simple calculations show that

$$\begin{aligned}
\varepsilon^{21} &= \varepsilon^5+\varepsilon^4+\varepsilon^3+\varepsilon+1\\
\varepsilon^{42} &= (\varepsilon^{21})^2 = \varepsilon^5+\varepsilon^4+\varepsilon^3+\varepsilon\\
\varepsilon^{27} &= \varepsilon^3+\varepsilon^2+\varepsilon\\
\varepsilon^{54} &= (\varepsilon^{27})^2 = \varepsilon^4+\varepsilon^2+\varepsilon+1\\
\varepsilon^{45} &= (\varepsilon^{54})^2 = \varepsilon^4+\varepsilon^3+1\,,
\end{aligned}$$

which implies that $c(\lambda)$ can be represented as

$$c(\lambda) = (\lambda+\varepsilon^{21})(\lambda+\varepsilon^{42})(\lambda+\varepsilon^{27})^2(\lambda+\varepsilon^{54})^2(\lambda+\varepsilon^{45})^2\,.$$

Employing primitive polynomials renders polynomial calculations much easier as such expressed elements of $\mathbb{F}_{q^n}$ are periodic with period q^n-1. For instance

$$\varepsilon^{108} = \varepsilon^{45}\varepsilon^{63} = \varepsilon^{45}$$

since with $\lambda^6+\lambda+1\,|\,\lambda^\tau-1$ with period $\tau=63$ follows $\varepsilon^{63}=1$.

Conversely, no zero γ of the non-primitive irreducible polynomial $\lambda^6+\lambda^3+1$ over $\mathbb{F}_2$ can be used for representing the field elements in $\mathbb{F}_{2^6}$ as powers of γ. Nevertheless, there is a reason for taking a zero of some non-primitive n-th degree irreducible polynomial for defining the elements of $\mathbb{F}_{q^n}$ in a more complicated polynomial representation: primitive polynomials of arbitrary degree n cannot be calculated in an efficient straight-forward manner. If enumerations in tabulars are not sufficient any more there is fairly no way out from taking zeroes of just irreducible polynomials the determination of which is complicated enough for arbitrary degrees n. □

Remark C.2
The task of polynomial synthesis by starting with some desired zeroes in an extension field $\mathbb{F}_{q^\delta}$ turns out to be tricky. The problem is that any desired zero γ in the extension field $\mathbb{F}_{q^\delta}$ has to

be accompanied by a specification of corresponding conjugates γ^q, γ^{q^2}, ... and so on, in order to obtain a polynomial in $\mathbb{F}_q[\lambda]$ whose coefficients are elements from $\mathbb{F}_q$ only. Moreover, the number of necessary conjugates depends on the degree of the polynomial of which it is root of. Similarly, if specifying an eigenvector in $\mathbb{F}_{q^n}^n$ then its conjugate eigenvectors have to be specified as well.

An unpleasant consequence is that a controller synthesis by means of eigenvalue placement and parameter vector specification in some extension field, as proposed in the parametric approach [Rop86, DH01], becomes very cumbersome as many distinct cases entail unwieldy parameterization formulae. This is the main reason why the presented work is not based on the notion of an extension field. □

Appendix D

General Solution of Linear Systems using Singular Inverses

The solvability condition and the general solution of the linear system of equations

$$\mathbf{A}\mathbf{x} = \mathbf{b} \tag{D.1}$$

shall be determined, where $\mathbf{A} \in \mathbb{F}^{m\times n}$ is a possibly singular and non-square matrix and $\mathbf{x} \in \mathbb{F}^n$, $\mathbf{b} \in \mathbb{F}^m$ are column vectors. Refering to [LT85, CW94] the basic relation for an inverse matrix is the following.

Definition D.1 (Generalized Inverse)
Let $\mathbf{A} \in \mathbb{F}^{m\times n}$ and $\mathbf{G} \in \mathbb{F}^{n\times m}$ with

$$\mathbf{A}\mathbf{G}\mathbf{A} = \mathbf{A}. \tag{D.2}$$

Such a matrix $\mathbf{G}$ is called generalized inverse (g-inverse, singular inverse). □

This definition generalizes many concepts of inverse matrices, for example it is in accordance with the customary definition of an inverse $\mathbf{G} = \mathbf{A}^{-1}$ if the matrix $\mathbf{A}$ is square and invertible, or in accordance with the left (right) inverse matrix $\mathbf{G} = (\mathbf{A}^{\mathrm{T}}\mathbf{A})^{-1}\mathbf{A}^{\mathrm{T}}$ ($\mathbf{G} = \mathbf{A}^{\mathrm{T}}(\mathbf{A}\mathbf{A}^{\mathrm{T}})^{-1}$) with respect to a non-square matrix $\mathbf{A}$ whose column (row) rank is its column (row) dimension.

Without loss of generality, any matrix $\mathbf{A} \in \mathbb{F}^{m\times n}$ of rank r can be written as[1]

$$\mathbf{A} = \begin{pmatrix} \mathbf{A}_{r\times r} & \mathbf{A}_{r\times(n-r)} \\ \mathbf{A}_{(m-r)\times r} & \mathbf{A}_{(m-r)\times(n-r)} \end{pmatrix}$$

and a construction scheme [CW94] for a corresponding generalized inverse matrix $\mathbf{G} \in \mathbb{F}^{n\times m}$ is

$$\mathbf{G} = \begin{pmatrix} \mathbf{A}_{r\times r}^{-1} - \mathbf{A}_{r\times r}^{-1}\big(\mathbf{A}_{r\times(n-r)}\mathbf{G}_{21}\mathbf{A}_{r\times r} - \mathbf{A}_{r\times r}\mathbf{G}_{12}\mathbf{A}_{(m-r)\times r} - \mathbf{A}_{r\times(n-r)}\mathbf{G}_{22}\mathbf{A}_{(m-r)\times r}\big)\mathbf{A}_{r\times r}^{-1} & \mathbf{G}_{12} \\ \mathbf{G}_{21} & \mathbf{G}_{22} \end{pmatrix}$$

[1] Some elementary row and column operations may be necessary.

in which the matrices $\mathbf{G}_{12}$, $\mathbf{G}_{21}$ and $\mathbf{G}_{22}$ can be chosen arbitrarily, thus, *g*-inverses are not unique in general. A simple form of a *g*-inverse is

$$\mathbf{G} = \begin{pmatrix} \mathbf{A}_{r\times r}^{-1} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{pmatrix}, \quad \mathbf{G} \in \mathbb{F}^{n\times m}. \tag{D.3}$$

Employing a generalized inverse $\mathbf{G}$, equation (D.1) is solvable if a vector $\mathbf{x}$ exists such that

$$\mathbf{b} = \mathbf{A}\mathbf{x} = \mathbf{A}\mathbf{G}\mathbf{A}\mathbf{x} = \mathbf{A}\mathbf{G}\mathbf{b} \quad \Longleftrightarrow \quad (\mathbf{I} - \mathbf{A}\mathbf{G})\,\mathbf{b} = \mathbf{0}.$$

Conversely, if $(\mathbf{I} - \mathbf{A}\mathbf{G})\,\mathbf{b} = \mathbf{0}$ then $\mathbf{b} = \mathbf{A}\mathbf{G}\mathbf{b}$ and a (particular) solution $\mathbf{x}_\mathrm{p} = \mathbf{G}\mathbf{b}$ exists.

Theorem D.1 (Solvability Condition)
Let $\mathbf{A} \in \mathbb{F}^{m\times n}$ and $\mathbf{b} \in \mathbb{F}^m$. Then the linear system of equations $\mathbf{A}\mathbf{x} = \mathbf{b}$ is solvable iff

$$(\mathbf{I} - \mathbf{A}\mathbf{G})\,\mathbf{b} = \mathbf{0} \tag{D.4}$$

for some generalized inverse matrix $\mathbf{G} \in \mathbb{F}^{n\times m}$ with respect to $\mathbf{A}$. □

Given solvability the general solution of $\mathbf{A}\mathbf{x} = \mathbf{b}$ has the form

$$\mathbf{x} = \mathbf{x}_\mathrm{h} + \mathbf{x}_\mathrm{p} \tag{D.5}$$

in which $\mathbf{x}_\mathrm{h}$ is the solution of the homogeneous equation $\mathbf{A}\mathbf{x}_\mathrm{h} = \mathbf{0}$ and $\mathbf{x}_\mathrm{p}$ is a particular solution of $\mathbf{A}\mathbf{x}_\mathrm{p} = \mathbf{b}$. As has already been shown above such a particular solution is

$$\mathbf{x}_\mathrm{p} = \mathbf{G}\mathbf{b}. \tag{D.6}$$

For the purpose of deriving the homogeneous solution $\mathbf{x}_\mathrm{h}$ multiply $\mathbf{A}$ by an arbitrary vector $\mathbf{z} \in \mathbb{F}^n$ and use the general inverse relation in Definition D.1 to obtain

$$\mathbf{A}\mathbf{z} = \mathbf{A}\mathbf{G}\mathbf{A}\mathbf{z} \quad \Longleftrightarrow \quad \mathbf{A}(\mathbf{I} - \mathbf{G}\mathbf{A})\,\mathbf{z} = \mathbf{0}.$$

Hence, the homogeneous solution is

$$\mathbf{x}_\mathrm{h} = (\mathbf{I} - \mathbf{G}\mathbf{A})\,\mathbf{z} \tag{D.7}$$

for $\mathbf{z} \in \mathbb{F}^n$ arbitrary.

Theorem D.2 (General Solution of a Linear System of Equations)
Let $\mathbf{A} \in \mathbb{F}^{m\times n}$, $\mathbf{b} \in \mathbb{F}^m$. Let $\mathbf{G} \in \mathbb{F}^{n\times m}$ be a respective general inverse matrix that satisfies the solvability condition in Theorem D.1. Then the general solution of the linear system $\mathbf{A}\mathbf{x} = \mathbf{b}$ is

$$\mathbf{x} = (\mathbf{I} - \mathbf{G}\mathbf{A})\,\mathbf{z} + \mathbf{G}\mathbf{b} \tag{D.8}$$

for arbitrary $\mathbf{z} \in \mathbb{F}^n$. □

Example D.1
If $\mathbf{C} \in \mathbb{F}^{n\times n}$ is a nilpotent, hence singular, companion matrix an example of a generalized inverse matrix $\mathbf{G}$ simply follows from

$$\mathbf{C}\mathbf{C}^{\mathrm{T}}\mathbf{C} = \mathbf{C}\,,$$

that is $\mathbf{G} = \mathbf{C}^{\mathrm{T}}$. Note that

$$(\mathbf{C}^{\mathrm{T}})^{\kappa}\mathbf{C}^{\kappa} = \mathrm{diag}(\mathbf{I}_{n-\kappa}, \mathbf{0}_{\kappa}), \quad \kappa \in \mathbb{N}\,,$$

which implies that for $\kappa \geq 2$

$$(\mathbf{C}^{\mathrm{T}})^{\kappa}\mathbf{C}^{\kappa} \neq (\mathbf{C}^{\mathrm{T}}\mathbf{C})^{\kappa}\,. \qquad \square$$

Appendix E

Rank Deficiency of a Matrix-Valued Polynomial Function

When investigating the dimension of a linear subspace, for example when generalized eigenspaces are concerned, a criterion for the rank deficiency of a matrix $f(\mathbf{A})$ as a value of a polynomial function f is advantageous. Particularly, in cases when the elementary divisor polynomials of the matrix $\mathbf{A}$ and the multiplicities of the zeroes regarding the polynomial $f(\lambda)$ are known, a simple formula for the rank of $f(\mathbf{A})$ can be derived [Gan58].

First, observe that for any matrix $\mathbf{A} \in \mathbb{F}^{n\times n}$ a Jordan-form $\mathbf{J} \in \mathbb{F}_{\mathrm{s}}^{n\times n}$ with $\mathbf{A} = \mathbf{T}\mathbf{J}\mathbf{T}^{-1}$ exists.[1] A polynomial function $f : \mathbb{F}^{n\times n} \to \mathbb{F}^{n\times n}$ applied on $\mathbf{A}$ yields

$$f(\mathbf{A}) = \mathbf{T}\, f(\mathbf{J})\, \mathbf{T}^{-1}\,. \tag{E.1}$$

Given the $i = 1,\ldots,N_{\mathrm{s}}$ elementary divisor polynomials $p_i \in \mathbb{F}_{\mathrm{s}}[\lambda]$ of $\mathbf{A}$

$$p_1(\lambda) = (\lambda-\lambda_1)^{e_1},\ p_2(\lambda) = (\lambda-\lambda_2)^{e_2},\ \ldots\ ,\ p_{N_{\mathrm{s}}}(\lambda) = (\lambda-\lambda_{N_{\mathrm{s}}})^{e_{N_{\mathrm{s}}}}$$

made up of the (not necessarily distinct) eigenvalues $\lambda_i \in \mathbb{F}_{\mathrm{s}}$ with respect to $\mathbf{A}$, the Jordan-form reads

$$\mathbf{J} = \mathrm{diag}(\mathbf{J}_1,\ldots,\mathbf{J}_{N_{\mathrm{s}}})\,, \tag{E.2}$$

in which each matrix $\mathbf{J}_i$ corresponds to an elementary divisor polynomial. These matrices show the form

$$\mathbf{J}_i = \lambda_i\, \mathbf{I}_{e_i} + \mathbf{N}_{e_i} \tag{E.3}$$

[1] The field $\mathbb{F}_{\mathrm{s}}$ is a splitting field of $\mathbb{F}$. In other words $\mathbb{F}$ is an extension field of $\mathbb{F}$ in which any polynomial in $\mathbb{F}[\lambda]$ can be factored in linear factors with coefficients in $\mathbb{F}_{\mathrm{s}}$. Example: the field of complex numbers $\mathbb{C}$ is a splitting field with respect to the field of real numbers $\mathbb{R}$.

where $\mathbf{N}_{e_i}$ is a $e_i \times e_i$ nilpotent matrix

$$\mathbf{N}_{e_i} = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & 0 \\ 0 & 0 & 0 & \cdots & 1 \\ 0 & 0 & 0 & \cdots & 0 \end{pmatrix} \tag{E.4}$$

and $\mathbf{I}_{e_i}$ is the respective identity.

As $\mathbf{J}$ consists of diagonal blocks only, it follows

$$f(\mathbf{J}) = \operatorname{diag}(f(\mathbf{J}_1), \ldots, f(\mathbf{J}_{N_\mathrm{s}})) \tag{E.5}$$

and the rank deficiency of $f(\mathbf{J})$ can be obtained by summing up the rank deficiencies of the matrices $f(\mathbf{J}_1), \ldots, f(\mathbf{J}_{N_\mathrm{s}})$.

To this end, let the polynomial $f(\lambda)$ be represented by its Lagrange-Sylvester interpolation polynomial regarding λ_i, accordingly[2]

$$f(\lambda) = f(\lambda_i) + \frac{f'(\lambda_i)}{1!}(\lambda - \lambda_i) + \frac{f^{(2)}(\lambda_i)}{2!}(\lambda - \lambda_i)^2 + \ldots \tag{E.6}$$

by means of which for $i = 1, \ldots, N_\mathrm{s}$

$$\begin{aligned} f(\mathbf{J}_i) &= f(\lambda_i)\mathbf{I}_{e_i} + \frac{f'(\lambda_i)}{1!}(\mathbf{J}_i - \lambda_i \mathbf{I}_{e_i}) + \frac{f^{(2)}(\lambda_i)}{2!}(\mathbf{J}_i - \lambda_i \mathbf{I}_{e_i})^2 + \ldots \\ &= f(\lambda_i)\mathbf{I}_{e_i} + \frac{f'(\lambda_i)}{1!}\mathbf{N}_{e_i} + \frac{f^{(2)}(\lambda_i)}{2!}\mathbf{N}_{e_i}^2 + \cdots + \frac{f^{(e_i-1)}(\lambda_i)}{(e_i-1)!}\mathbf{N}_{e_i}^{e_i-1} \end{aligned}$$

since with $\mathbf{N}_{e_i} = \mathbf{J}_i - \lambda_i \mathbf{I}_{e_i}$ from (E.3) it turns out that the series truncates due to the nilpotency of $\mathbf{N}_{e_i}$. Hence, the result is

$$f(\mathbf{J}_i) = \begin{pmatrix} f(\lambda_i) & \frac{f'(\lambda_i)}{1!} & \cdots & \frac{f^{(e_i-1)}(\lambda_i)}{(e_i-1)!} \\ 0 & f(\lambda_i) & \ddots & \vdots \\ \vdots & \vdots & \ddots & \frac{f'(\lambda_i)}{1!} \\ 0 & 0 & \cdots & f(\lambda_i) \end{pmatrix} \tag{E.7}$$

On the one hand, if λ_i is no zero of the polynomial $f(\lambda)$ then $f(\mathbf{J}_i)$ is of full rank. On the other hand, if k_i is the multiplicity of a zero λ_i with regard to $f(\lambda)$ then for reason of

$$f(\lambda_i) = f'(\lambda_i) = \ldots = f^{(k_i-1)}(\lambda_i) = 0,\ f^{(k_i)}(\lambda_i) \neq 0, \quad i = 1, \ldots, N_\mathrm{s} \tag{E.8}$$

the rank deficiency of $f(\mathbf{J}_i)$ is k_i, unless the dimension of the matrix $\mathbf{N}_{e_i}$ is less than k_i. The result is fixed in the following theorem.

[2]Derivatives used are only formal derivatives and do not imply continuity.

Theorem E.1 (Rank Deficiency of a Matrix-Valued Polynomial Function)
Let $\mathbf{A} \in \mathbb{F}^{n\times n}$ be a matrix and let the $i = 1,\ldots,N_\mathrm{s}$ elementary divisor polynomials $p_i(\lambda)$ over the splitting field $\mathbb{F}_\mathrm{s}$ be given as

$$p_1(\lambda) = (\lambda-\lambda_1)^{e_1},\ p_2(\lambda) = (\lambda-\lambda_2)^{e_2},\ \ldots\ ,\ p_{N_\mathrm{s}}(\lambda) = (\lambda-\lambda_{N_\mathrm{s}})^{e_{N_\mathrm{s}}}\,.$$

Furthermore, let $f \in \mathbb{F}[\lambda]$ be a polynomial. Then the rank deficiency Δ of the matrix $f(\mathbf{A})$ is

$$\Delta = \sum_{i=1}^{N_\mathrm{s}} \min(k_i, e_i)$$

where k_i is the multiplicity of the eigenvalue λ_i as a zero of f. □

Example E.1
Consider a companion matrix $\mathbf{C} \in \mathbb{F}_q^{d\times d}$ whose d-th degree defining polynomial

$$p_\mathbf{C}(\lambda) = \big(p_{\mathrm{irr},\mathbf{C}}(\lambda)\big)^e$$

is the e-th power of an irreducible polynomial $p_{\mathrm{irr},\mathbf{C}}(\lambda)$ of degree δ. Hence, $p_\mathbf{C}(\lambda)$ is the only elementary divisor polynomial over $\mathbb{F}_q$.

The dimensions of the nullspaces concerning the matrices

$$f_j(\mathbf{C}) = \big(p_{\mathrm{irr},\mathbf{C}}(\mathbf{C})\big)^j, \quad j = 1,\ldots,e$$

are to be determined by means of Theorem E.1.

From Appendix C recall that an irreducible polynomial of degree δ over $\mathbb{F}_q$ has exactly δ distinct zeroes in the extension field $\mathbb{F}_{q^\delta}$, which represents a corresponding splitting field. Thus,

$$(\lambda-\lambda_1)^e,\ (\lambda-\lambda_2)^e,\ \ldots\ ,\ (\lambda-\lambda_\delta)^e\,.$$

are the δ elementary divisor polynomials of $\mathbf{C}$ over the splitting field $\mathbb{F}_{q^\delta}$.

As the dimension of the nullspaces of $f_j(\mathbf{C})$ equals the rank deficiency Δ_j of $f_j(\mathbf{C})$, consequently, Theorem E.1 can be applied. This results in the nullspace dimensions

$$\Delta_j = \sum_{i=1}^{\delta} \min(j,e) = \sum_{i=1}^{\delta} j = j\,\delta, \quad j = 1,\ldots,e$$

with respect to the matrices $f_j(\mathbf{C})$. □

Example E.2
Given a controllable LMS with dynamics matrix $\mathbf{A} \in \mathbb{F}_q^{n\times n}$ and input matrix $\mathbf{B} \in \mathbb{F}_q^{n\times m}$, respectively. Let $\mathbf{K} \in \mathbb{F}_q^{m\times n}$ denote a feedback matrix associated to a static state feedback of the form

$\mathbf{u}(k) = \mathbf{K}\mathbf{x}(k)$. As the closed-loop system is autonomous it is easy to see that the solution of the closed-loop state equation reads

$$\mathbf{x}(k) = (\mathbf{A}+\mathbf{B}\mathbf{K})^k \mathbf{x}(0) = (\mathbf{A}_\mathbf{K})^k \mathbf{x}(0)$$

with the closed-loop dynamics matrix $\mathbf{A}_\mathbf{K}$. Assume that the feedback matrix $\mathbf{K}$ is to be determined such that a maximal set of initial states $\mathbf{x}(0)$ can be steered to some desired state $\mathbf{x}_\mathrm{d}$ in a minimal number of steps k. Then by transforming the state as per $\tilde{\mathbf{x}} = \mathbf{x} - \mathbf{x}_\mathrm{d}$, solving the problem amounts to determine a feedback matrix $\mathbf{K}$ complying with

$$\mathbf{0} = (\mathbf{A}_\mathbf{K})^k \tilde{\mathbf{x}}(0)$$

which renders $(\mathbf{A}_\mathbf{K})^k = \mathbf{0}$ with a full rank deficiency $\Delta = n$ in a minimal number of steps k. This means that $\mathbf{A}_\mathbf{K}$ must be nilpotent, thus, its characteristic polynomial has to be

$$\mathrm{cp}_{\mathbf{A}_\mathbf{K}}(\lambda) = \lambda^n .$$

This control objective reminds of standard deadbeat-control [Kuč91] where all eigenvalues of the closed-loop dynamics matrix are equal to zero and the closed-loop dynamics matrix $\mathbf{A}_\mathbf{K}$ in CCF shows simple companion form. However, Theorem E.1 gives a hint for more refinement. The reason is that in the MIMO-case there is some liberty in choosing the elementary divisor polynomials, which are exactly the factors of the characteristic polynomial and coincide with the invariant polynomials, in this case. In view of this fact and Theorem E.1 denote $f(\mathbf{A}_\mathbf{K}) = (\mathbf{A}_\mathbf{K})^k$ and set the N elementary divisor polynomials

$$p_i(\lambda) = \lambda^{e_i},\ i = 1,\ldots,N, \qquad \sum_{i=1}^{N} e_i = n .$$

Then by Theorem E.1 the rank deficiency of $(\mathbf{A}_\mathbf{K})^k$ is

$$\Delta = \sum_{i=1}^{N} \min(k, e_i) .$$

Increasing the rank deficiency Δ by increasing the number N of elementary divisor polynomials is not possible above m. This originates from the fact that by Theorem 5.3, m is the maximum number of achievable nilpotent diagonal blocks in the closed-loop dynamics matrix represented in CCF, see Definition 5.5. Thus, $N = m$.

Again in light of Definition 5.5, the step number k that is necessary for obtaining $(\mathbf{A}_\mathbf{K})^k = \mathbf{0}$ can be bounded from above by the dimension of the largest nilpotent diagonal block matrix. This results in

$$\Delta = \sum_{i=1}^{m} \min(k, e_i) = \sum_{i=1}^{m} k = km$$

and, consequently, the $i = 1, \ldots, m$ elementary divisor exponents e_i have to be chosen equal to the ordered controllability indices c_i of the LMS, hence

$$p_i(\lambda) = \lambda^{c_i}, \quad i = 1, \ldots, m \qquad c_1 \geq \ldots \geq c_m \,.$$

Since these elementary divisor polynomials $p_i(\lambda)$ coincide with the invariant polynomials, it is obvious that the inequalities in Rosenbrock's control structure theorem, Theorem 5.4, are satisfied. Following the lines in Chapter 5.2.4, the polynomial matrix

$$\mathbf{D}^{\star}_{\mathbf{K}}(a) = \mathrm{diag}(a^{c_1}, \ldots, a^{c_m})$$

can be used for determining a feedback matrix $\mathbf{K}$ that guarantees to drive any state $\mathbf{x}(0)$ into some desired state $\mathbf{x}_{\mathrm{d}}$ in maximal $k = c_1$ steps, which as compared to standard deadbeat-control takes always less than n steps. □

Appendix F

Solving the Linear State Equation in the Image Domain

The image domain representation of the state equation (4.1) of an LMS directly leads to the $\mathcal{A}$-transform of the system state

$$\mathbf{X}(a) = (a\mathbf{I} - \mathbf{A})^{-1}\big(\mathbf{B}\mathbf{U}(a) + a\mathbf{x}(0)\big)\,,$$

recalling (5.12) for convenience. Employing the inverse $\mathcal{A}$-transform, Theorem 2.11, allows to determine the well-known solution of the state equation. With the geometric series formula applied on the expression

$$(a\mathbf{I} - \mathbf{A})^{-1} = \frac{1}{a}\Big(\mathbf{I} - \frac{\mathbf{A}}{a}\Big)^{-1} = \frac{1}{a}\sum_{i=0}^{\infty}\Big(\frac{\mathbf{A}}{a}\Big)^{i}$$

the original domain function results in

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

which equals the expression for the solution of the state equation, given in (5.1).

Appendix G

List of Publications

[1] J. Reger, “Deadlock Analysis for Deterministic Finite State Automata using Affine Linear Models”, in: *Proc. of 2001 European Control Conference*, (Porto, Portugal), 2001.

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

[3] J. Reger and K. Schmidt, “Modeling and Analyzing Finite State Automata in the Finite Field GF(2)”, in: *Proc. of 4th MATHMOD*, (Vienna, Austria), Argesim, 2003.

[4] K. Schmidt and J. Reger, “Synthesis of State Feedback for Linear Automata in the Finite Field GF(2)”, in: *Proc. of 4th MATHMOD*, (Vienna, Austria), Argesim, 2003.

[5] J. Reger, “Analysis of Multilinear Systems using Gröbner-bases over the Finite Field GF(2)”, in: *Proc. of 4th MATHMOD*, (Vienna, Austria), Argesim, 2003. best conference poster award

[6] J. Reger and K. Schmidt, “Aspects on Analysis and Synthesis of Linear Discrete Systems over the Finite Field $\mathbb{F}_q$”, in: *Proc. of 2003 European Control Conference*, (Cambridge, United Kingdom), 2003.

[7] J. Reger and K. Schmidt, “Modeling and Analyzing Finite State Automata in the Finite Field GF(2)”, *Mathematics and Computers in Simulation (MATCOM)*, 66(1–2):193–206, 2004.

[8] J. Reger and K. Schmidt, “A Finite Field Framework for Modelling, Analysis and Control of Finite State Automata”, *Mathematical and Computer Modelling of Dynamical Systems (MCMDS)*, 2004. accepted for publication.

[9] K. Schmidt, J. Reger, and T. Moor, “Hierarchical Control for Structural Decentralized DES”, in: *Proc. of 7th Workshop on Discrete Event Systems (WODES)*, (Reims, France), 2004. accepted for publication.

References

[Ant98] P. ANTSAKLIS. *Linear Systems*. McGraw-Hill, New York, 1998.

[Ber70] E. BERLEKAMP. Factoring polynomials over large finite fields. *Mathematics of Computation*, 24(111):713–735, 1970.

[BJT97] J. BUCHMANN, M. JACOBSEN, AND E. TESKE. On some computational problems in finite abelian groups. *Mathematics of Computation*, 66(220):1663–1687, 1997.

[BLL91] A. BENVENISTE, P. LE GUERNIC, AND M. LE BORGNE. Dynamical systems over galois fields and DEDS control problems. In *Proc. of 30th Conf. Decision and Control*, pages 1505–1509. IEEE Publications, 1991. Brighton, UK.

[BM77] G. BIRKHOFF AND S. MACLANE. *A Survey of Modern Algebra*. MacMillan, New York, 1977.

[Boo62] T. L. BOOTH. An Analytical Representation of Signals in Sequential Networks. In *Proc. of Symposium on The Mathematical Theory of Automata*, New York, 1962. Polytechnic Press and J. Wiley and Sons.

[Boo67] T. L. BOOTH. *Sequential Machines and Automata Theory*. Wiley, New York, 1967.

[BP81] D. BOCHMANN AND C. POSTHOFF. *Binäre Dynamische Systeme*. R. Oldenbourg, München, 1981.

[CLO98] D. COX, J. LITTLE, AND D. O'SHEA. *Using Algebraic Geometry*. Springer, New York, 1998.

[CLR90] T. H. CORMEN, C. E. LEISERSON, AND R. L. RIVEST. *Introduction to Algorithms*. MIT Press, Cambridge, MA, 1990.

[CW94] W. CASPARY AND K. WICHMANN. *Lineare Modelle*. Oldenbourg, München, 1994.

[DH78] L. L. DORNHOFF AND F. E. HOHN. *Applied Modern Algebra*. Macmillan, New York, 1978.

[DH01] J. DEUTSCHER AND P. HIPPE. Parametric compensator design in the frequency domain. *Int. J. Control*, (74):1467–1480, 2001.

[Els59] B. ELSPAS. The theory of autonomous linear sequential networks. *IEEE Trans. Circuit Theory*, 6:45–60, 1959.

[Fra94] D. FRANKE. *Sequentielle Systeme — Binäre und Fuzzy Automatisierung mit arithmetischen Polynomen*. Vieweg, Braunschweig, 1994.

[Fra96] D. FRANKE. Arithmetische Logik — Ein Brückenschlag zwischen diskreten Steuerungen und klassischen Regelungen. *Automatisierungstechnik*, 44:553–563, 1996.

[Fri59] B. FRIEDLAND. Linear modular sequential circuits. *IEEE Trans. Circuit Theory*, 6:71–68, 1959.

[Gan58] F. R. GANTMACHER. *Matrizenrechnung*, volume 1. VEB, Berlin, 1958.

[Gat87] J. VON ZUR GATHEN. Factoring polynomials and primitive elements for special primes. *Theoretical Computer Science*, 52:77–89, 1987.

[Ger95] R. GERMUNDSSON. *Symbolic Systems — Theory, Computation and Applications*. PhD thesis, Linköping, 1995.

[Gil64] A. GILL. Analysis of Linear Sequential Circuits by Confluence Sets. *IEEE Trans. Computers*, 30:226–231, 1964.

[Gil66a] A. GILL. Graphs of Affine Transformations, with Applications to Sequential Circuits. In *Proc. of the 7th IEEE International Symposium on Switching and Automata Theory*, pages 127–135. IEEE Publications, 1966. Berkeley, California, USA.

[Gil66b] A. GILL. *Linear Sequential Circuits: Analysis, Synthesis, and Applications*. McGraw-Hill, New York, 1966.

[Gil69] A. GILL. Linear Modular Systems. In L. A. ZADEH AND E. POLAK, editors, *System Theory*. McGraw-Hill, New York, 1969.

[GLR82] I. GOHBERG, P. LANCASTER, AND L. RODMAN. *Matrix Polynomials*. Academic Press, New York, 1982.

[Gös91] M. GÖSSEL. *Automatentheorie für Ingenieure*. Akademie Verlag, Berlin, 1991.

[Gun97] J. GUNNARSSON. *Symbolic Methods and Tools for Discrete Event Dynamic Systems*. PhD thesis, Linköping, 1997.

[HHL+00] D. HANKERSON, D. G. HOFFMANN, D. A. LEONARD, C. C. LINDNER, K. T. PHELPS, C. A. RODGER, AND J. R. WALL. *Coding Theory and Cryptography — The Essentials*. Marcel Dekker Inc., New York, 2nd edition, 2000.

[Huf56] D. A. HUFFMANN. *Information Theory*, chapter The Synthesis of Linear Sequential Coding Networks. Academic Press, New York, 1956. Paper read at a Symposium on Information Theory held at the Royal Institution, London, September 1955.

[Huf59] D. A. HUFFMANN. A linear circuit viewpoint on error-correcting codes. *IEEE Trans. Circuit Theory*, 6:45–60, 1959.

[Ili89] C. S. ILIOPOULUS. Worst-case complexity bounds on algorithms for computing the canonical structure of finite abelian groups and the Hermite and Smith normal forms of an integer matrix. *SIAM J. Comput.*, 18(4):658–669, 1989.

[Kai80] T. KAILATH. *Linear Systems*. Prentice Hall, Englewood Cliffs, 1980.

[Kau65] W. H. KAUTZ, editor. *Linear Sequential Switching Circuits - Selected Technical Papers*. Holden-Day, San Francisco, 1965.

[Kuč91] V. KUČERA. *Analysis and design of discrete linear control systems*. Prentice Hall, New York, 1991.

[Lan84] S. LANG, editor. *Algebra*. Addison-Wesley, Yale University, New Haven, Connecticut, 1984.

[LBL89] M. LE BORGNE, A. BENVENISTE, AND P. LE GUERNIC. Polynomial ideal theoretic methods in discrete event, and hybrid dynamical systems. In *Proc. 1989 IEEE Work. CACSD*, December 1989. Tampa, USA.

[LBL91] M. LE BORGNE, A. BENVENISTE, AND P. LE GUERNIC. Polynomial Dynamical Systems over Finite Fields. In G. JACOB AND F. LAMNABHI-LAGARRIGUE, editors, *Lecture Notes in Computer Science*, volume 165, pages 212–222. Springer, Berlin, 1991.

[LN94] R. LIDL AND H. NIEDERREITER. *Introduction to finite fields and their applications*. Cambridge Univ. Press, New York, 1994.

[LT85] P. LANCASTER AND M. TISMENETSKY. *The Theory of Matrices*. Academic Press, San Diego, 2nd edition, 1985.

[Mar97] H. MARCHAND. *Méthodes de synthèse d'automatismes d'écrits par des systèmes à événements discrets finis*. PhD thesis, Université de Rennes, October 1997.

[McE87] R. J. MCELIECE. *Finite fields for computer scientists and engineers*. Kluwer Academic Publishers, Dordrecht, 1987.

[Mei96] A. MEIJER. Groups, Factoring and Cryptography. *Mathematics Magazine*, 69(2):103–109, 1996.

[ML97] H. MARCHAND AND M. LE BORGNE. Partial Order Control and Optimal Control of Discrete Event Systems modeled as Polynomial Dynamical Systems over Galois fields. Rapport de recherche IRISA 1125, IRISA, October 1997.

[ML99] H. MARCHAND AND M. LE BORGNE. The Supervisory Control Problem of Discrete Event Systems using Polynomial Methods. Rapport de recherche IRISA 1271, IRISA, October 1999.

[Mul54] D. E. MULLER. Application of boolean algebra to switching circuit design and to error detection. *IEEE Transactions on Computers*, (3):6–12, 1954.

[New72] M. NEWMAN. *Integral Matrices*. Academic Press, New York, 1972.

[New74] M. NEWMAN. The Smith Normal Form of a Partitioned Matrix. *Journal of Research of the National Bureau of Standards - B, Mathematical Sciences*, 778(1), 1974.

[NMGJ01] D. NEŠIĆ, I. M. Y. MAREELS, T. GLAD, AND M. JIRSTRAND. Software for Control System Analysis and Design, Symbol Manipulation. In J. WEBSTER, editor, *Wiley Encyclopedia of Electrical and Electronics Engineering Online*. Wiley, 2001. http://www.interscience.wiley.com:83/eeee/.

[PML99] S. PINCHINAT, H. MARCHAND, AND M. LE BORGNE. Symbolic Abstractions of Automata and their application to the Supervisory Control Problem. Rapport de recherche IRISA 1279, IRISA, November 1999.

[PW72] W. W. PETERSON AND E. J. WELDON. *Error-Correcting Codes*. MIT Press, Cambridge, MA, 2nd edition, 1972.

[Ree54] I. S. REED. A class of multiple-error-correcting codes and the decoding scheme. *IEEE Transactions on Information Theory*, (4):38–49, 1954.

[Ric65] J. RICHALET. Operational Calculus for Finite Rings. *IEEE Trans. Circuit Theory*, 12:558–570, 1965.

[Rop86] G. ROPPENECKER. On Parametric State Feedback Design. *Int. J. Control*, (43):793–804, 1986.

[Ros70] H. H. ROSENBROCK. *State-space and Multivariable Theory*. Thomas Nelson Ltd., London, 1970.

[RS03] J. REGER AND K. SCHMIDT. Aspects on Analysis and Synthesis of Linear Discrete Systems over the Finite Field $\mathbb{F}_q$. In *Proc. of 2003 European Control Conference*, Cambridge, United Kingdom, 2003.

[Sch02] K. SCHMIDT. Entwurf von Zustandsrückführungen für lineare diskrete Systeme über GF(2) mit Hilfe der Polynommatrixmethode. Master's thesis, Lehrstuhl für Regelungstechnik, Friedrich-Alexander-Universität Erlangen-Nürnberg, March 2002.

[Sel66] E. S. SELMER. Linear recurrence relations over finite fields. Technical report, Department of Mathematics, University of Bergen, 1966.

[Sho90] V. SHOUP. On the deterministic complexity of factoring polynomials over finite fields. *Information Processing Letters*, 33(5):261–267, 1990.

[Son99] J. SONNENBERG. A New Method for Describing and Analyzing Finite Determined Automata by Walsh Functions. In *Proc. of 1999 European Control Conference*, Karlsruhe, Germany, 1999.

[Son00] J. SONNENBERG. *Verfahren zur linearen Modellierung dynamischer ereignisdiskreter Systeme mittels Walsh-Funktionen*. VDI-Verlag, Düsseldorf, 2000.

[Sto00] A. STORJOHANN. *Algorithms for Matrix Canonical Forms*. PhD thesis, Department of Computer Science, Swiss Federal Institute of Technology – ETH, Zürich, 2000.

[Tha88] A. THAYSE. Boolean calculus and differences. In *Lecture Notes in Computer Science*, volume 101. Springer, Berlin, 1988.

[Wen00] W.-M. WENDLER. Elements of Linear Binary System Theory. In *Proc. of 4th International Workshop on Boolean Problems*, pages 37–46, Freiberg (Germany), 2000.

[Wol74] W. A. WOLOVICH. *Linear Multivariable Systems*. Springer, New York, 1974.

[Wun75] G. WUNSCH. *Systemtheorie*. Akademische Verlagsgesellschaft Geest & Portig K.-G., Leipzig, 1975.

[Zhe27] I. I. ZHEGALKIN. Über eine Technik zur Berechnung von Sätzen in der symbolischen Logik. *Mat. sbornik*, (34):9–28, 1927. transl. from russian: Prof. Dr. D. Bochmann.

Lebenslauf

Zur Person:

Johann Reger
geboren am 18. 06. 1971 in Erbendorf in der Oberpfalz
verheiratet, ein Kind

Schulbildung:

1977–1981	Grundschule in Waldeck
1981–1990	Gymnasium in Eschenbach i. d. Opf.
Juni 1990	Abschluss mit Abitur

Wehrdienst:

1990–1992	2jähriger Wehrdienst als Soldat auf Zeit in der Stabskompanie der Panzergrenadierbrigade 10 in Weiden i. d. Opf.

Studium:

1992–1998	Studium der Fertigungstechnik an der Friedrich-Alexander-Universität Erlangen-Nürnberg und an der University of Liverpool
1993–1995	Tutor am Lehrstuhl für Technische Mechanik
1995–1999	Tutor am Lehrstuhl für Angewandte Mathematik II
1997	Praktikum bei der Siemens AG, Medical Solutions in Erlangen, Forchheim und Nürnberg
1994	Preis der FAG Kugelfischer-Stiftung für erzielte Examensergebnisse
seit 1995	Stipendiat der Studienstiftung des deutschen Volkes und Mitglied des internationalen Studentenprogramms SSP der Siemens AG
Dez. 1998	Studienabschluss Dipl.-Ing.

Hochschultätigkeit:

1999–2001	Promotionsstipendiat der Studienstiftung des deutschen Volkes
seit 2002	Wissenschaftlicher Assistent am Lehrstuhl für Regelungstechnik der Universität Erlangen-Nürnberg