Behaviors over Finite Fields

R.J. van de Kreeke

Supervisor:
Dr. J.W. Polderman

August 30, 2007

University of Twente
Department of Applied Mathematics
Systems & Control Group

Contents

Summary: Behaviors over Finite Fields

Discrete time behaviors given by $\mathfrak{B} = \{w\colon Z_+ \to \mathbb{F} \,|\, R(\sigma)w = 0\}$, where $\mathbb{F}$ is a finite field, σ a shift operator, and $R(\xi)$ a polynomial with coefficients in $\mathbb{F}$, can be determined explicitly if $R(\xi)$ splits over $\mathbb{F}$, i.e. can be factored into linear factors. We discuss the case that $R(\xi)$ does not split over $\mathbb{F}$. There holds that for every polynomial there exists a field extension $\mathbb{E}$ of $\mathbb{F}$ such that it splits over $\mathbb{E}$. We give an explicit expression for solutions of $R(\sigma)w = 0$ in case all roots in $\mathbb{E}$ are mutually distinct. The solution is extended to the multivariable case for autonomous systems. Again it is assumed that the characteristic values are mutually distinct. Single input, single output systems are discussed in the last chapter.

Notation

$\mathbb{Z}$	set of integers
$\mathbb{Z}_+$	set of nonnegative integers
$\mathbb{N}$	set of positive integers
$\mathbb{C}$	set of complex numbers
$\mathbb{Q}$	set of rational numbers
$\mathbb{R}$	set of real numbers
R^*	the set of nonzero elements of R
$\mathbb{F}[\xi]$	set of polynomials with coefficients in $\mathbb{F}$, in the indeterminate ξ
$\mathrm{char}(\mathbb{F})$	the characteristic of $\mathbb{F}$
$\lvert\mathbb{F}\rvert$	the order of $\mathbb{F}$
$\mathbb{E}/\mathbb{F}$	a field extension of $\mathbb{F}$
$[\mathbb{E} : \mathbb{F}]$	degree of $\mathbb{E}$ over $\mathbb{F}$
$\mathbb{F}_q$ or $\mathrm{GF}(q)$	finite field of order q
$\mathbb{F}^{m\times n}$	set of $m \times n$ matrices, with elements in $\mathbb{F}$
$\mathbb{F}^{m\times n}[\xi]$	set of $m \times n$ polynomial matrices, with coefficients in $\mathbb{F}$
$\mathbb{F}(a_1, a_2, \ldots, a_n)$	smallest field that contains $\mathbb{F}$ and $a_1, \ldots, a_n$
$\mathbb{W}^{\mathbb{T}}$	set of all maps from $\mathbb{T}$ to $\mathbb{W}$
$\mathfrak{L}^q$	the set of behaviors in q variables
	that admit a kernel representation $R(\sigma)w = 0$

Chapter 1

Introduction

In the behavioral approach to systems theory, a dynamical system is determined by a set of possible time trajectories. This set is called the behavior of a system. No a priori distinction is made between input and output variables. Notions like controllability, time invariance and linearity are viewed (and defined) as properties of the system and not as a consequence of its representation. A time-invariant and linear behavior can be represented in various ways, such as kernel representations, image representations and state space representations.
In a more mathematical setting: a *dynamical system* Σ is a triple $\Sigma = (\mathbb{T}, \mathbb{W}, \mathfrak{B})$ where $\mathbb{T}$ is the time set, $\mathbb{W}$ is the signal space and $\mathfrak{B} \subset \mathbb{W}^{\mathbb{T}}$ the behavior.

In this part, we will discuss discrete time linear time-invariant complete behaviors over finite fields. By this we mean sets of time trajectories w that take their values in $\mathbb{F}^q$, where $\mathbb{F}$ is a finite field and q is the number of variables. The time set $\mathbb{T}$ is the set of nonnegative integers $\mathbb{Z}_+$.

A field is an algebraic structure in which the operations of addition, subtraction, multiplication and division (except division by zero) may be performed, and the same rules hold which are familiar from the arithmetic of ordinary numbers. A finite field or Galois field (so named in honor of Évariste Galois) is a field that contains only finitely many elements. Finite fields are important in number theory, algebraic geometry, Galois theory, cryptography, and coding theory.
Chapter 2 contains a brief survey of the algebra that is needed to understand the concept of *finite fields* and also a number of important properties of finite fields.

Linear, time invariant and complete behaviors over finite fields admit a kernel representation, i.e. $\mathfrak{B} = \{w\colon Z_+ \to \mathbb{F}^q \,|\, R(\sigma)w(k) = 0\}$ where σ denotes the backward shift $(\sigma w)(k) = w(k+1)$. $R(\xi)$ is a $g \times q$ polynomial matrix, whose coefficients are elements of finite field $\mathbb{F}$. In Chapter 3 a number of definitions is given that reflect the behavioral approach to systems theory.

In Chapter 4 we will give explicit expressions for the behavior of autonomous systems. For autonomous systems there holds that the future of every trajectory is completely determined by its past. Their behavior can be represented by $R(\sigma)w = 0$ where $R(\xi)$ is a square polynomial matrix in $\mathbb{F}^{q\times q}[\xi]$ of which the determinant is a nonzero polynomial.
In their paper *R-S list decoding from a system theoretic perspective* [4], M. Kuijper and J.W. Polderman give an explicit description of such behaviors, in case all roots of $\det R(\xi)$ are elements of finite field $\mathbb{F}$. The problem is that $\det R(\xi)$ may contain irreducible polynomials as factors, i.e., polynomials that do not have roots in $\mathbb{F}$. For finite fields holds that there exist extension fields, finite fields of which $\mathbb{F}$ is a subfield, over which $\det R(\xi)$ splits into linear factors. The behaviors over these extension fields can be determined explicitly. In Chapter 4 we will restrict the expressions for the time trajectories such that they belong

to finite field $\mathbb{F}$. We will do this for the special case that $\det R(\xi)$ has mutually distinct roots (in the extension field).

Chapter 2

Preliminaries: Finite fields

In this Chapter we will give a brief survey of the algebra that is needed to understand the concept of *finite fields* and also a number of important properties of finite fields. Most of the definitions, theorems and proofs can be found in [5]; some in [1] or [2].

2.1 Definitions

2.1.1 Groups, Rings, Fields and Ideals

Definition 2.1.1 (Group) A *group* is a set G together with a binary operator $\cdot$ on G such that the following three properties hold.
1) $\cdot$ is *associative*, i.e $\forall x, y, z \in G \ : \ x \cdot (y \cdot z) = (x \cdot y) \cdot z$.
2) there exists an *identity element* 1 s.t. for all $x \in G$, $x \cdot 1 = 1 \cdot x = x$
3) For each $x \in G$, there exists an *inverse element* $x^{-1} \in G$ such that $x \cdot x^{-1} = 1$
The group is called *Abelian* or commutative if also holds
4) $\forall x, y \in G$, $x \cdot y = y \cdot x$.

In the additive notation $x \cdot y$, 1 and x^{-1} become $x + y$, 0 and $-x$ respectively.

Definition 2.1.2 (Finite group, Order) A group G is called *finite* if it contains finitely many elements. The number of elements in a finite group is called its *order*. We will use $|G|$ to denote the order of a group.

Definition 2.1.3 (Cyclic group) A multiplicative group G is called *cyclic* if there exists an element $x \in G$ such that for any $y \in G$ there is some integer n with $y = x^n$. Such an element x is called a generator of G. We write $G = \langle x \rangle$.

Definition 2.1.4 (Ring) $[R, +, \cdot]$ is called a *ring* with $+, \cdot$ binary operations, if
1) R is an Abelian group with respect to $+$
2) $\cdot$ is associative
3) the *distributive laws* hold: for all $x, y, z \in R$ we have $x \cdot (y + z) = x \cdot y + x \cdot z$ and $(y + z) \cdot x = y \cdot x + z \cdot x$
A ring is called *commutative* if $\cdot$ is commutative.

Definition 2.1.5 (Integral domain) A commutative ring $[R, +, \cdot]$ is called an *integral domain* R has no zero divisors, that is $\forall x, y \in R \ : \ x \cdot y = 0 \Rightarrow x = 0$ or $y = 0$), and R is not the trivial zero ring $\{0\}$.

Definition 2.1.6 (Field) An commutative ring $[R, +, \cdot]$ is called a *field* if every nonzero element has a multiplicative inverse in R, that is $\forall x \in R^*, \exists y \in R \ : \ x \cdot y = y \cdot x = 1$

So $[R, +, \cdot]$ is a *field* if

i. $[R, +]$ is an Abelian group

ii. $[R^*, \cdot]$ is a commutative group

iii. both distributive laws hold in $[R, +, \cdot]$

Definition 2.1.7 (Finite field, Galois field) A field $\mathbb{F}$ is called *finite* if the number of elements $|F|$ is finite. Such a field is also called *Galois field*. A finite field with q elements is denoted as $\mathbb{F}_q$ or as $\mathrm{GF}(q)$.

From now on we will denote a ring or a field simply as R or $\mathbb{F}$ and not as $[R, +, \cdot]$.

Definition 2.1.8 (Characteristic) If there exists a positive integer n such that $nr = 0$ for every element r of ring R then the least such positive integer n is called the *characteristic* of R, denoted by $\mathrm{char}(R)$. If no such positive integer n exists, R is said to have characteristic 0.

Definition 2.1.9 (Subring) A subset S of a ring R is a *subring* of R if S is itself a ring with the operations of R. A *subgroup* and a *subfield* are defined similarly.

Definition 2.1.10 (Ideal) A subset J of a ring R is called an *ideal* provided J is a subring of R and for all $x \in J$ and $r \in R$ we have $xr \in J$ and $rx \in J$.

Definition 2.1.11 (Principle ideal) Let R be a commutative ring. An ideal J of R is said to be *principle* if there is an $a \in R$ such that $J = (a)$, where $(a) = \{ra + na \,|\, r \in R,\ n \in \mathbb{Z}\}$, or, if R contains an identity, then $(a) = \{ra \,|\, r \in R\}$. The principle ideal J is *generated* by a.

Definition 2.1.12 (Principle ideal domain) The commutative ring R is called a principle ideal domain if R is an integral domain and if every ideal J of R is principle.

Definition 2.1.13 (Residue class, Factor ring) An ideal of J of a ring R defines a partition of R into disjoint cosets, called *residue classes* modulo J. The residue class of the element x of R modulo J is denoted by $[x] = x+J$. Elements $x, y \in R$ are *congruent* modulo J, written $x \equiv y \mod J$ if they are in the same residue class modulo J, i.e. $x - y \in J$. The set of residue classes forms a ring w.r.t. operations $(x + J) + (y + J) = (x + y) + J$ and $(x + J)(y + J) = xy + J$. The residue class ring (or *factor* ring) is denoted by R/J

Example 2.1.14 Examples of (infinite) fields are the set of integers $\mathbb{Z}$, the set of rational numbers $\mathbb{Q}$, and the set of real numbers $\mathbb{R}$.
Let $\mathbb{Z}_p$ denote the set of integers modulo p, $p \in \mathbb{N}$. So $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$. Then $\mathbb{Z}_p$ is a finite field if and only if p is prime.
$\mathbb{Z}/(p)$, p prime, is isomorphic to $\mathbb{Z}_p$ with the isomorphism defined by $\phi(a+(p)) = a \mod p$.

2.1.2 Morphisms

Definition 2.1.15 (Homomorphism) A mapping ϕ from a ring R to a ring S is called a *ring homomorphism* if it preserves the two ring operations $\phi(a + b) = \phi(a) + \phi(b)$ and $\phi(ab) = \phi(a)\phi(b)$.

Definition 2.1.16 An injective homomorphism is called a *monomorphism*. An *epimorphism* is surjective. An *isomorphism* is bijective.

A homomorphism from S to itself is called an *endomorphism*. An isomorphism from S onto itself is called an *automorphism*.

2.1.3 Polynomials

Definition 2.1.17 (Polynomial) Let R be an arbitrary ring. A *polynomial over* R is an expression of the form $\sum_{i=0}^{n} a_i x^i$, $n \in \mathbb{Z}_+$, The *coefficients* $a_i, i = 1, \ldots, n$ are elements of R.

Definition 2.1.18 (Polynomial ring) The ring formed by the polynomials over R is called the *polynomial ring* and is denoted by $R[x]$.

Definition 2.1.19 (Irreducible) Let $\mathbb{F}$ be an arbitrary field. A polynomial $p(x) \in \mathbb{F}[x]$ is called *irreducible over* $\mathbb{F}$ (or irreducible *in* $\mathbb{F}[x]$) if $p(x)$ has a positive degree and $p(x) = a(x)b(x)$ with $a(x), b(x) \in \mathbb{F}[x]$ implies that $a(x)$ or $b(x)$ is a constant polynomial.

Definition 2.1.20 (Derivative) The *derivative* of a polynomial $p(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{F}[x]$ is defined by $p'(x) = \sum_{i=1}^{n} i a_i x^{i-1} \in \mathbb{F}[x]$.

Definition 2.1.21 (Split) Let $\mathbb{F}$ be a field. A polynomial $p(x) \in \mathbb{F}[x]$ of positive degree n is said to *split* in $\mathbb{F}$ if it can be written as a product of linear factors in $\mathbb{F}[x]$, i.e. if $\exists a, \alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{F}$ such that $p(x) = a(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$.

2.1.4 Field extensions

Definition 2.1.22 (Extension field) A field $\mathbb{E}$ is called an *extension field* of $\mathbb{F}$ if $\mathbb{F}$ is a subfield of $\mathbb{E}$. The *field extension* is denoted as $\mathbb{E}/\mathbb{F}$ (read as $\mathbb{E}$ *over* $\mathbb{F}$). If $\mathbb{F} \neq \mathbb{E}$ then $\mathbb{F}$ is called a *proper* subfield.

Definition 2.1.23 (Prime field) A field containing no proper subfields is called a *prime* field.

Definition 2.1.24 (Prime subfield) The intersection of all subfields of $\mathbb{F}$ is a prime field. It is called the *prime subfield*.

Definition 2.1.25 (Finite extension, Degree) Let $\mathbb{E}$ be an extension field of $\mathbb{F}$. If $\mathbb{E}$, considered as a vector space over $\mathbb{F}$, is finite-dimensional then $\mathbb{E}/\mathbb{F}$ is called a finite extension. The dimension of $\mathbb{E}$ over $\mathbb{F}$ is called the *degree* and is denoted as $[\mathbb{E} : \mathbb{F}]$.

Definition 2.1.26 (Adjunction, simple field) Let $\mathbb{E}$ be an extension field of $\mathbb{F}$, and let $a_1, a_2, \ldots, a_n$ be elements of $\mathbb{E}$. The smallest subfield of $\mathbb{E}$ that contains $\mathbb{F}$ and the set $\{a_1, a_2, \ldots, a_n\}$ is denoted by $\mathbb{F}(a_1, a_2, \ldots, a_n)$. The elements $a_1, \ldots, a_n$ are *adjoined* to $\mathbb{F}$. If a single element a is adjoined, the field $\mathbb{F}(a)$ is called *simple*.

Definition 2.1.27 (Splitting field) An extension field $\mathbb{E}$ of field $\mathbb{F}$ is called a *splitting field* for $p(x) \in \mathbb{F}[x]$ if $p(x)$ splits in $\mathbb{E}$ but in no proper subfield of $\mathbb{E}$, i.e. $p(x) = a \prod_{i=1}^{n} (x - \alpha_i)$, $a, \alpha_1, \ldots, \alpha_n \in \mathbb{E}$ and $\mathbb{E} = \mathbb{F}(\alpha_1, \ldots, \alpha_n)$.

Definition 2.1.28 (Algebraic, Transcendental) Let $\mathbb{E}$ be an extension field of $\mathbb{F}$. An element $u \in \mathbb{E}$ is called *algebraic* over $\mathbb{F}$ if u is a root of some polynomial $p(x) \in \mathbb{F}[x]^*$. If such a nonzero polynomial does not exist, u is called *transcendental*. $\mathbb{E}$ is called an *algebraic extension* of $\mathbb{F}$ if all $u \in \mathbb{F}$ are algebraic over $\mathbb{E}$.

Definition 2.1.29 (Minimal polynomial) If $u \in \mathbb{E}$ is algebraic over $\mathbb{F}$, then the uniquely determined monic polynomial $p(x) \in \mathbb{F}[x]$ generating the ideal $J = \{p(x) \in \mathbb{F}[x] \,|\, p(u) = 0\}$ of $\mathbb{F}[x]$ is called the *minimal polynomial*. The minimal polynomial is *irreducible* in $\mathbb{F}[x]$. $p(x)$ is the monic polynomial in $\mathbb{F}[x]$ of least degree having u as a root.

Definition 2.1.30 (Conjugates) Let $\mathbb{F}_{q^m}$ be an extension of $\mathbb{F}_q$ and let $\alpha \in \mathbb{F}_q^m$. Then the elements $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{m-1}}$ are called the *conjugates* of α with respect to $\mathbb{F}_q$.

The conjugates of $\alpha \in \mathbb{F}_{q^m}$ w.r.t. $\mathbb{F}_q$ are distinct if and only if the minimal polynomial of α over $\mathbb{F}_q$ has degree m.

2.2 Properties of finite fields

Theorem 2.2.1 *A finite field has prime characteristic.*

Theorem 2.2.2 *The prime subfield of a finite field $\mathbb{F}$ is isomorphic to $\mathbb{F}_p$, where $p = \mathrm{char}(\mathbb{F})$.*

Theorem 2.2.3 ([5] Lemma 2.1) *Let $\mathbb{E}$ be a finite field containing a subfield $\mathbb{F}$ with q elements. Then $\mathbb{E}$ has q^m elements, where $m = [\mathbb{E} : \mathbb{F}]$.*

Theorem 2.2.4 ([5] Theorem 2.2) *Let $\mathbb{F}$ be a finite field. Then $\mathbb{F}$ has p^n elements, where p is the characteristic of $\mathbb{F}$ and n is the degree of $\mathbb{F}$ over its prime subfield.*

Theorem 2.2.5 ([5] Lemma 2.3) *If $\mathbb{F}$ is a finite field with q elements, then every $a \in \mathbb{F}$ satisfies $a^q = a$.*

Theorem 2.2.6 ([5] Theorem 2.5 Existence and Uniqueness of Finite Fields) *For every prime p and every positive integer n there exists a finite field with p^n elements. Any finite field with $q = p^n$ elements is isomorphic to the splitting field of $x^q - x$ over $\mathbb{F}_p$.*

Theorem 2.2.7 ([5] Theorem 2.6 Subfield criterion) *Let $\mathbb{F}_q$ be the finite field with $q = p^n$ elements. Then every subfield of $\mathbb{F}_q$ has order p^m, where m is a positive divisor of n. Conversely if m is a positive divisor of n, then there is exactly one subfield of $\mathbb{F}_q$ with p^m elements.*

Theorem 2.2.8 ([5] Theorem 2.8) *For every finite field $\mathbb{F}_q$ the multiplicative group $\mathbb{F}_q^*$ of nonzero elements of $\mathbb{F}_q$ is cyclic.*

Definition 2.2.9 (Primitive element) A generator of the cyclic group $\mathbb{F}_q^*$ is called a *primitive element* of $\mathbb{F}_q$.

Theorem 2.2.10 ([5] Theorem 1.61) *Let $f(\xi) \in \mathbb{F}[\xi]$. The residue class ring $\mathbb{F}[\xi]/f(\xi)$ is a field if and only $f(\xi)$ is irreducible over $\mathbb{F}$.*

Theorem 2.2.11 *If $\mathbb{E}$ is a finite extension of $\mathbb{F}$ and $\mathbb{D}$ is a finite extension of $\mathbb{E}$ then $\mathbb{D}$ is a finite extension of $\mathbb{F}$ with $[\mathbb{D} : \mathbb{F}] = [\mathbb{D} : \mathbb{E}][\mathbb{E} : \mathbb{F}]$.*

Theorem 2.2.12 ([5] Theorem 1.69) *The polynomial $f(\xi) \in \mathbb{F}[\xi]$ of degree 2 or 3 is irreducible in $\mathbb{F}[\xi]$ if and only if $f(\xi)$ has no root in $\mathbb{F}$.*

Theorem 2.2.13 ([5] Theorem 1.82) *If $a \in \mathbb{E}$ is algebraic over $\mathbb{F}$ then its minimal polynomial $g(\xi)$ over $\mathbb{F}$ has the following properties*
(i) *$g(\xi)$ is irreducible in $\mathbb{F}[\xi]$*
(ii) *For $f(\xi) \in \mathbb{F}[\xi]$, we have $f(a) = 0$ if and only $g(\xi)$ divides $f(\xi)$*
(iii) *$g(\xi)$ is the monic polynomial in $\mathbb{F}[\xi]$ of least degree having a as a root*

Theorem 2.2.14 ([5] Theorem 1.86) *Let $a \in \mathbb{E}$ be algebraic of degree n over $\mathbb{F}$ and let $f(\xi)$ be the minimal polynomial of a over $\mathbb{F}$. Then*
(i) *$\mathbb{F}(a)$ is isomorphic to $\mathbb{F}[\xi]/(f(\xi))$*
(ii) *$[\mathbb{F}(a) : \mathbb{F}] = n$ and $\{1, a, \ldots, a^{n-1}\}$ is a basis of $\mathbb{F}(a)$ over $\mathbb{F}$*
(iii) *Every $\alpha \in \mathbb{F}(\alpha)$ is algebraic over $\mathbb{F}$ and its degree over $\mathbb{F}$ is a divisor of n.*

Theorem 2.2.15 ([5] Theorem 1.91, Existence and Uniqueness of Splitting Field) *If $\mathbb{F}$ is a field and $f(\xi)$ any polynomial of positive degree in $\mathbb{F}[\xi]$, then there exists a splitting field of $f(x)$ over $\mathbb{F}$. Any two splitting fields of $f(x)$ over $\mathbb{F}$ are isomorphic under an isomorphism which keeps the elements of $\mathbb{F}$ fixed and maps roots of f into each other.*

Because isomorphic fields may be identified, one may speak of *the* splitting field. It is obtained from $\mathbb{F}$ by adjoining finitely many algebraic elements over $\mathbb{F}$, it follows that the splitting field of $f(x)$ over $\mathbb{F}$ is a finite extension of $\mathbb{F}$.

Theorem 2.2.16 ([5] Theorem 2.14) *If $f(\xi)$ is an irreducible polynomial in $\mathbb{F}_q[\xi]$ of degree m then $f(x)$ has a root α in $\mathbb{F}_{q^m}$. Furthermore, all roots of $f(x)$ are simple and are given by the distinct elements $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{m-1}}$ of $\mathbb{F}_{q^m}$.*

Corollary 2.2.17 ([5] Corollary 2.15) *Let $f(\xi)$ be an irreducible polynomial in $\mathbb{F}_q[\xi]$ of degree m. Then the splitting field of $f(x)$ over $\mathbb{F}_q$ is given by $\mathbb{F}_{q^m}$.*

Corollary 2.2.18 ([5] Corollary 2.16) *Any two irreducible polynomials in $\mathbb{F}_q[\xi]$ of the same degree have isomorphic splitting fields.*

Theorem 2.2.19 *Let $f(\xi) \in \mathbb{F}_q[\xi]$. The degree of the splitting field of $f(\xi)$ over $\mathbb{F}_q$ is the least common multiple of the degrees of its irreducible factors. Let m be this l.c.m. then $f(\xi)$ splits over $\mathbb{F}_{q^m}$.*

Chapter 3

Preliminaries: The behavioral approach

In this chapter we will discuss the behavior of discrete time, linear, time-invariant, complete autonomous systems over finite fields. In the following section we will explain briefly what we mean by that. The definitions are mainly taken from [6].

3.1 Definitions and properties

A dynamical system is determined by a set of possible time trajectories. This set is called the behavior of a system.

Definition 3.1.1 A *dynamical system* Σ is a triple $\Sigma = (\mathbb{T}, \mathbb{W}, \mathfrak{B})$ where $\mathbb{T}$ is the time set, $\mathbb{W}$ is the signal space and $\mathfrak{B}$ the behavior. The behavior is the set of signals $w\colon \mathbb{T} \to \mathbb{W}$ that are possible.

Definition 3.1.2 A dynamical system $\Sigma = (\mathbb{T}, \mathbb{W}, \mathfrak{B})$ is *linear* if $\mathbb{W}$ is a vector space over a field $\mathbb{F}$, and $\mathfrak{B}$ is a linear subspace of $\mathbb{W}^{\mathbb{T}}$, where $\mathbb{W}^{\mathbb{T}}$ denotes the collection of all maps from $\mathbb{T}$ to $\mathbb{W}$.

Linear systems obey the superposition principle, i.e. if $w_1, w_2 \in \mathfrak{B}$ then $\alpha w_1 + \beta w_2 \in \mathfrak{B}$ for all $\alpha, \beta \in \mathbb{F}$.

A discrete time system is time invariant if all trajectories in the behavior are also elements of the behavior when they are (backwardly) shifted.

Definition 3.1.3 A *discrete time system* with time axis $\mathbb{T} = \mathbb{Z}$ is *time-invariant* if $\sigma\mathfrak{B} = \mathfrak{B}$ where σ denotes the backward time shift $\sigma w(k) = w(k+1)$. If $\mathbb{T} = \mathbb{Z}_+$ then the system is time invariant if $\sigma\mathfrak{B} \subset \mathfrak{B}$.

Definition 3.1.4 A time invariant system $\Sigma = (\mathbb{T}, \mathbb{W}, \mathfrak{B})$ is *complete* if $w \in \mathfrak{B} \iff w|_{\mathbb{T}\cap[t_1,t_2]} \in \mathfrak{B}|_{\mathbb{T}\cap[t_1,t_2]}$ for all $t_1, t_2 \in \mathbb{T}, t_1 \leq t_2$.

Completeness means that the behavior at infinity is of no consequence for deciding wether the function $w\colon \mathbb{T} \to \mathbb{W}$ belongs to the behavior.

Discrete time, linear, time-invariant, complete systems admit a kernel representation. The class of behaviors in q variables that admit a representation of the form $R(\sigma)w = 0$ is denoted by $\mathfrak{L}^q$.

A system is autonomous if trajectories are uniquely defined by their restriction to a finite time-window.

Definition 3.1.5 A system $\Sigma = (\mathbb{Z}_+, \mathbb{W}, \mathfrak{B})$ is autonomous if there exists a (finite) interval $\mathcal{T} \subset \mathbb{Z}_+$ such that the mapping $\pi\colon \mathfrak{B} \to \mathfrak{B}|_{\mathcal{T}}$ defined by the restriction $\pi w := w|_{\mathcal{T}}$ is injective.

An autonomous behavior $\mathfrak{B} \in \mathfrak{L}^q$ can be represented by $R(\sigma)w = 0$ with $R(\xi) \in \mathbb{F}^{q\times q}[\xi]$ and $\det R(\xi)$ a nonzero polynomial.

Definition 3.1.6 A polynomial matrix $U(\xi) \in \mathbb{F}^{g\times g}[\xi]$, with $\mathbb{F}$ a field is called *unimodular* if there exists a polynomial matrix $V(\xi) \in \mathbb{F}^{g\times g}[\xi]$ such that $V(\xi)U(\xi) = I$, with $I \in \mathbb{F}^{g\times g}$ the identity matrix. Equivalently, if $\det U(\xi)$ is equal to a nonzero constant.

Theorem 3.1.7 (Representation theorem) *Two polynomial matrices of the same dimensions define the same behavior if and only if they are related through a left unimodular transformation. Let $\mathfrak{B}_1, \mathfrak{B}_2 \in \mathfrak{L}^q$ be given by $R_1(\sigma)w = 0$ and $R_2(\sigma)w = 0$ respectively, with $R_1(\xi), R_2(\xi) \in \mathbb{F}^{g\times q}[\xi]$, $\mathbb{F}$ a field. Then*

$$\mathfrak{B}_1 = \mathfrak{B}_2 \iff R_1(\xi) = U(\xi)R_2(\xi) \quad \textit{with } U(\xi) \in \mathbb{F}^{g\times g}[\xi] \textit{ unimodular.}$$

Chapter 4

Autonomous behaviors over finite fields

4.1 Problem Description

An autonomous behavior $\mathfrak{B} \in \mathfrak{L}^q$ is given by $\mathfrak{B} = \{w\colon \mathbb{Z}_+ \to \mathbb{F}^q \mid R(\sigma)w = 0\}$ with $R(\xi) \in \mathbb{F}^{q\times q}[\xi]$ and $\det R(\xi) \in \mathbb{F}[\xi]$ is a nonzero polynomial. The monic polynomial $\chi(\xi)$ that is obtained when $\det R(\xi)$ is divided by its leading coefficient is called the *characteristic polynomial*.

Note that, without loss of generality $R(\xi)$ can be chosen such that $\det R(\xi)$ is monic. (Follows from the Representation Theorem 3.1.7.)

4.1.1 Autonomous behaviors over $\mathbb{R}$, the scalar case

Now let us assume that $\mathbb{F}$ is the set of real numbers $\mathbb{R}$ and that $q = 1$, so w is scalar. The general solution of the difference equation $R(\sigma)w = 0$ is well-known and given by.

$$w(k) = \sum_{i=1}^{N} \sum_{j=0}^{m_i-1} a_{ij} k^j \lambda_i^k\,, \quad k \in \mathbb{Z}_+$$

where $\lambda_i, i = 1, \ldots, N$ are the distinct complex (!) roots of $R(\xi)$ and m_i the corresponding multiplicity. The coefficients a_{ij} are elements of $\mathbb{C}$. There holds that for every root λ_i with a nonzero imaginary part, its complex conjugate $\overline{\lambda_i}$ is also a root of $R(\xi)$ with the same multiplicity. Let us assume that this root has index h_i, that is $\overline{\lambda_i} = \lambda_{h_i}$. To ensure that the values $w(k)$ are elements of $\mathbb{R}$ there must hold that the coefficients $a_{h_i j}$ are the complex conjugates of the coefficients a_{ij}: $w(k) \in \mathbb{R}, k \in \mathbb{Z}_+ \iff a_{ij} = \overline{a_{h_i j}}$ for all i for which λ_i has a nonzero imaginary part.

We see that to derive a general solution of $R(\sigma)w = 0$ with $w\colon \mathbb{Z}_+ \to \mathbb{R}$ we need the extension field $\mathbb{C} = \mathbb{R}(i)$ of $\mathbb{R}$ with $i^2 + 1 = 0$ if $\det R(\xi)$ does not split in $\mathbb{R}$.

4.1.2 When the characteristic polynomial splits over finite field $\mathbb{F}$

In [4] M. Kuijper and J.W. Polderman present a theorem, that describes the behavior over a finite field $\mathbb{F}$ if $\det R(\xi)$ splits over $\mathbb{F}$. We will give this theorem here.

In the theorem the *Hasse derivative* is used. The jth Hasse derivative of a polynomial $P(\xi) = \sum_{i=0}^{n} p_i \xi^i$ is defined by $D_H^j P(\xi) := \sum_{i=j}^{n} \binom{i}{j} p_i \xi^{i-j}$.

Theorem 4.1.1 ([4], Theorem 2.13) *Let $R(\xi) \in \mathbb{F}^{q\times q}[\xi]$, let $\det R(\xi)$ be a polynomial of degree n, and let $\mathfrak{B} = \{w\colon \mathbb{Z}_+ \to \mathbb{F}^q \mid R(\sigma)w = 0\}$. Then $\mathfrak{B}$ is an n-dimensional subspace of $(\mathbb{F}^q)^{\mathbb{Z}_+}$. If*

$$\det R(\xi) = c\prod_{i=1}^{N}(\xi - \lambda_i)^{m_i}$$

with $c \neq 0$ and $\lambda_i \in \mathbb{F}$, then all trajectories in $\mathfrak{B}$ are of the form

$$\mathbf{w} = \sum_{i=1}^{N}\sum_{j=0}^{m_i-1} b_{ij} D_{\mathrm{H}}^{j}(\lambda_i^k)$$

with $b_{ij} \in \mathbb{F}^q$ satisfying the linear restrictions

$$\sum_{j=l}^{m_i-1}\left[D_{\mathrm{H}}^{j-l}R(\lambda_i)\right] b_{ij} = 0\,, \quad l = 0,\dots,m_i-1,\ i = 1,\dots,N.$$

The following theorem is a scalar version of Theorem 4.1.1. The Hasse derivatives have been evaluated.

Theorem 4.1.2 *Let $\mathbb{F}$ be a finite field and $R(\xi) \in \mathbb{F}[\xi]$ a monic polynomial of degree n. The behavior $\mathfrak{B}$, given by $\mathfrak{B} = \{w\colon \mathbb{Z}_+ \to \mathbb{F} \mid R(\sigma)w = 0\}$, is an n-dimensional subspace of $\mathbb{F}^{\mathbb{Z}_+}$. If the roots of $R(\xi)$ belong to $\mathbb{F}$, say $R(\xi) = \prod_{i=1}^{N}(\xi - \lambda_i)^{m_i}$, then*

$$\mathfrak{B} = \operatorname{span}\{w_i^j \mid i = 1,\dots,N; j = 0,\dots,m_i - 1\} \tag{4.1.1}$$

where the trajectories $w_i^j\colon \mathbb{Z}_+ \to \mathbb{F}$ are defined by

$$w_i^j(k) := \begin{cases} \binom{k}{j}\lambda_i^{k-j} & \text{for } k \geq j\,, \\ 0 & \text{for } k < j\,. \end{cases} \tag{4.1.2}$$

That is, $w \in \mathfrak{B}$ if and only if there exist coefficients $b_{ij} \in \mathbb{F}$ such that

$$w(k) = \sum_{i=1}^{N}\sum_{j=0}^{m_i-1}\binom{k}{j} b_{ij}\lambda_i^{k-j} \tag{4.1.3}$$

4.1.3 Problem formulation

As we have seen in subsection 4.1.1, the behavior $\tilde{\mathfrak{B}} = \{w\colon \mathbb{Z}_+ \to \mathbb{C} \mid R(\sigma)w = 0\}$ with $R(\xi) \in \mathbb{R}[\xi]$, where $\mathbb{C} = \mathbb{R}(i)$ is an extension field of $\mathbb{R}$, can be explicitly described. By putting restrictions on the coefficients (such that they are complex conjugates), the behavior $\mathfrak{B} = \{w\colon \mathbb{Z}_+ \to \mathbb{R} \mid R(\sigma)w = 0\}$ is obtained.

The question is now whether we can do something similar for Theorem 4.1.2. Can we define a field extension $\mathbb{E}$ for finite field $\mathbb{F}$ such that $R(\xi)$ splits over $\mathbb{E}$, derive the general solution from Theorem 4.1.2 for $\mathbb{W} = \mathbb{E}$ and then restrict the coefficients such that the values of all solutions $w(k)$ are elements of $\mathbb{F}$. This problem is discussed in Section 4.2.

The next question is if we can do this in the multivariable case. This is answered in Section 4.3.

It is important to note that every polynomial $R(\xi) \in \mathbb{R}[\xi]$ splits over $\mathbb{C}$. $\mathbb{C}$ is the algebraic closure of $\mathbb{R}$. This is, in general, not true for finite fields, i.e. there does not exist a *finite* field extension $\mathbb{E}$ for a finite field $\mathbb{F}$ such that every polynomial $R(\xi) \in \mathbb{F}[\xi]$ splits over $\mathbb{E}$. That is why we will define a field extension $\mathbb{E}/\mathbb{F}$ for a given specific polynomial $R(\xi) \in \mathbb{F}(\xi)$, such that $R(\xi)$ splits over $\mathbb{E}$.

4.2 Behaviors over extension fields, the scalar case

In this section we discuss behaviors that are linear subsets of $\mathbb{F}_+^{\mathbb{Z}}$, given by $\mathfrak{B} = \{w \colon \mathbb{Z}_+ \to \mathbb{F} \mid P(\sigma)w = 0\}$. Where $\mathbb{F}$ is a finite field and $P(\xi) \in \mathbb{F}[\xi]$ is a nonzero polynomial of degree n.

4.2.1 Construction of a splitting field

According to Theorem 2.2.15 there exists for every polynomial $P(\xi) \in \mathbb{F}[\xi]$ a finite field extension $\mathbb{E}/\mathbb{F}$ such that $P(\xi)$ splits over $\mathbb{E}$. In order to determine a splitting field $\mathbb{E}$ for $P(\xi)$, the polynomial can be factorized into linear factors and irreducible polynomials of higher degree. Factorization of polynomials over fields is discussed extensively in Chapter 4 of [5], we will not go into this.
A very useful property is Corollary 2.2.18: any two irreducible polynomials in $\mathbb{F}_q[\xi]$ of the same degree have isomorphic splitting fields. So if α is defined as a root of one of the irreducible factors $f(\xi)$ of degree m then, according to Theorem 2.2.16 and Corollary 2.2.17 all irreducible factors of degree m split over field extension $\mathbb{F}(\alpha) \cong \mathbb{F}[\xi]/(f(\xi)) \cong F_{q^m}$.
Let $\mathbb{F}_q$ be the finite field with $q = p^n$ elements. From Theorem 2.2.7 it follows that every subfield of $\mathbb{F}_q$ has order p^m, where m is a positive divisor of n. Conversely if m is a positive divisor of n, then there is exactly one subfield of $\mathbb{F}_q$ with p^m elements.
From this it follows that given an extension field $\mathbb{F}(\alpha) = \mathbb{F}_{p^{nk}}$, where α is the root of a k-th degree irreducible polynomial, then all irreducible polynomials of degree l split over $\mathbb{F}_{p^{nl}}$ which is a subfield of $\mathbb{F}_{p^{nk}} = \mathbb{F}(\alpha)$ if l divides k. So l-th degree irreducible polynomials split over $\mathbb{F}(\alpha)$.
According to Theorem 2.2.19 is the degree of the splitting field of $f(\xi)$ over $\mathbb{F}_q$ equal to the least common multiple of the degrees of its irreducible factors.
A splitting field of $f(\xi)$ can be constructed by consecutively adjoining roots of irreducible factors to $\mathbb{F}$. Starting with a factor $f_1(\xi)$ of highest degree, adjoin its root λ_1 to $\mathbb{F}$. Factorize $f(\xi)/f_1(\xi)$ over $\mathbb{F}(\lambda_1)$, adjoin root λ_2 of a irreducible nonlinear factor of highest degree $f_2(\xi) \in \mathbb{F}(\lambda_1)[\xi]$. Etcetera.

Example 4.2.1 (Adjoining roots) Let $\mathbb{F} = \mathbb{Z}_7$. Consider the polynomial

$$(x^2 + 3x + 1)(x^3 + x + 1)(x^4 + x + 1)$$

This polynomial is already factored into irreducible polynomials over $\mathbb{Z}_7$. Now let λ be a root of $(x^4 + x + 1)$. Then the dimension of $\mathbb{F}(\lambda)$ over $\mathbb{F}$ is $[\mathbb{F}(\lambda) : \mathbb{F}] = 4$. A basis for

$\mathbb{F}(\lambda)$ over $\mathbb{F}$ is $\{1, \lambda, \lambda^2, \lambda^3\}$. The 4-th degree factor splits over $\mathbb{F}(\lambda)$. And its roots are $\lambda, \lambda^7 = 6\lambda^3 + \lambda + 1, \lambda^{49} = \lambda^3 + 6\lambda^2 + 6$ and $\lambda^{343} = \lambda^2 + 4\lambda$.
The second degree polynomial also splits over $\mathbb{F}(\lambda)$ because 2 divides 4. Its roots are $6\lambda^3 + \lambda^2 + 5\lambda + 3$ and $\lambda^3 + 6\lambda^2 + 2\lambda + 1$.
The third degree polynomial does not split over $F(\lambda)$. Adjoining μ, defined as the root of $(x^3 + x + 1)$ yields $\mathbb{F}(\lambda, \mu)$. The dimension over $\mathbb{F}$ is $[\mathbb{F}(\lambda, \mu) : \mathbb{F}] = [\mathbb{F}(\lambda, \mu) : \mathbb{F}(\lambda)][\mathbb{F}(\lambda) : \mathbb{F}] = 3 \cdot 4 = 12 = \text{lcm}(2, 3, 4)$. A basis of $\mathbb{F}(\lambda, \mu)$ over $\mathbb{F}$ is $\{\lambda^i \mu^j \mid i = 0, \ldots 3, j = 0, \ldots, 2\}$. The roots of polynomial $(x^3 + x + 1)$ are $\mu, \mu^7 = 2\mu^2 + 6$ and $\mu^{49} = 5\mu^2 + 6\mu + 1$.
We have done the calculations using MAPLE commands `Nextprime`, `RootOf`, `Roots` and `Factor`.

4.2.2 Constraints on coefficients

A finite extension $\mathbb{E} = \mathbb{F}_{r^m}$ of $\mathbb{F} = \mathbb{F}_r$ can be considered as a vector space over $\mathbb{F}$. Then $\mathbb{E}$ has dimension m over $\mathbb{F}$ and if $\{\alpha_1, \ldots, \alpha_m\}$ is a basis of $\mathbb{E}$ over $\mathbb{F}$, each element $\alpha \in \mathbb{E}$ can be uniquely represented in the form

$$\alpha = c_1\alpha_1 + \cdots + c_m\alpha_m \quad \text{with } c_j \in \mathbb{F} \text{ for } 1 \leq j \leq m$$

A basis can be chosen such that $\alpha_m = 1 \in \mathbb{F}$. Now let us consider the solution in (4.1.3), where the signal space is $\mathbb{E}$. The coefficients b_{ij} are elements of $\mathbb{E}$, and so are the values $w(k), k \in \mathbb{Z}_+$.

$$w(k) = \sum_{i=1}^{N} \sum_{j=0}^{m_i - 1} \binom{k}{j} b_{ij} \lambda_i^{k-j}$$

The question is how the coefficients $b_{ij} := c_{ij1}\alpha_1 + \cdots + c_{ij(m-1)}\alpha_{m-1} + c_{ijm}$ should be chosen to ensure that $w(k) \in \mathbb{F}$. One way to solve this is to evaluate $w(k) = \tilde{c}_1(k)\alpha_1 + \cdots + \tilde{c}_{m-1}(k)\alpha_{m-1} + \tilde{c}_m(k)$ for a number of time instants k, where $w(k)$ is written as a linear combination of $\{\alpha_1, \ldots, \alpha_{m-1}, 1\}$. The coefficients $\tilde{c}_h(k)$ are linear combinations of $c_{ij1}, \ldots c_{ijm}, i = 1 \ldots N, j = 0, \ldots m_i - 1$. There holds that $w(k) \in \mathbb{F}$ if and only if $\tilde{c}_1(k) = \cdots = \tilde{c}_{m-1}(k) = 0$. This yields a number of linear equations, and for a sufficiently large number of time-instants k the coefficients b_{ij} can be determined. This is quite cumbersome. In the next subsection we will express the coefficients as linear combinations of powers of the characteristic values, assuming that they are mutually distinct (so $m_i = 0$). That way it is possible to ensure that $w(k) \in \mathbb{F}$.

4.2.3 The case that the characteristic values are mutually distinct

Theorem 4.2.2 *Let $\mathbb{F}$ be a finite field. Let $P(\xi) \in \mathbb{F}[\xi]$ be a monic polynomial of degree n, and let $\mathfrak{B} = \{w \colon \mathbb{Z}_+ \to \mathbb{F} \mid P(\sigma)w = 0\}$. Then $\mathfrak{B}$ is an n-dimensional subspace of $\mathbb{F}^{\mathbb{Z}_+}$. Let $\mathbb{E}/\mathbb{F}$ be a finite field extension such that $P(\xi)$ splits over $\mathbb{E}$, i.e. $P(\xi) = \prod_{i=1}^{n}(\xi - \lambda_i)$, $\lambda_i \in \mathbb{E}$. If the roots $\lambda_i \in \mathbb{E}$, $i = 1 \ldots n$ are mutually distinct then there holds $w \in \mathfrak{B}$ if and only if w of the form*

$$w(k) = \sum_{i=1}^{n} (a_0 + a_1\lambda_i + \cdots + a_{n-1}\lambda_i^{n-1})(\lambda_i)^k \tag{4.2.1}$$

with $a_m \in \mathbb{F}$, $m = 0, \ldots, n-1$.

Remark 4.2.3 Note that if $\mathbb{F}$ equals infinite field $\mathbb{R}$ and field extension $\mathbb{E} = \mathbb{R}(i) = \mathbb{C}$ then trajectories given by (4.2.1) are solutions that belong to $\mathbb{R}^{\mathbb{Z}_+}$.
Let $\lambda_1 = (a + bi)$ and $\lambda_2 = \overline{\lambda_1} = (a - bi)$ with $b \neq 0$ be two complex conjugate roots of $P(\xi)$. Then $(a_0+a_1\lambda_1+\cdots+a_{n-1}\lambda_1^{n-1})(\lambda_1)^k = (a_0(\lambda_1)^k+a_1(\lambda_1)^{k+1}+\cdots+a_{n-1}\lambda_1^{k+n-1}) = (a_0(\overline{\lambda_2})^k + a_1\overline{(\lambda_2)^{k+1}}+\cdots+a_{n-1}\overline{\lambda_2^{k+n-1}})$. So we see that all imaginary parts are cancelled out.

Lemma 4.2.4 *Let $P(\xi) = \xi^n + p_{n-1}\xi^{n-1} + \cdots + p_0 \in \mathbb{F}[\xi]$, with $\mathbb{F}$ a field. Let $\mathbb{E}/\mathbb{F}$ be a finite field extension such that $P(\xi)$ splits over $\mathbb{E}$, i.e. $P(\xi) = \prod_{i=1}^n(\xi - \lambda_i)$, $\lambda_i \in \mathbb{E}$, $i = 1 \ldots n$. For the power sums, defined by*

$$s_k := \sum_{i=1}^{n} \lambda_i^k, \quad k \in \mathbb{Z}_+ \tag{4.2.2}$$

holds that $s_k \in \mathbb{F}$ for $k \in \mathbb{Z}_+$.

Proof follows from *Newton's identities* that relate the power sums with the coefficients of polynomial $P(\xi)$. The identities are given by

$$s_0 = n \cdot 1 \tag{4.2.3}$$

$$s_1 = -p_{n-1} \tag{4.2.4}$$

$$s_k = -kp_{n-k} - \sum_{i=1}^{k-1} p_{n-k+i}\, s_i \qquad (2 \leq k \leq n) \tag{4.2.5}$$

$$s_k = -(p_{n-1}s_{k-1} + \cdots + p_0 s_{k-n}) \qquad (k > n) \tag{4.2.6}$$

Obviously $s_0, s_1 \in \mathbb{F}$. It is easy to see that indeed $p_{n-1} = -(\lambda_1 + \cdots + \lambda_n)$. It follows by induction from (4.2.5) that $s_k \in \mathbb{F}$ for $k = 2 \ldots n$, and from (4.2.6) that $s_k \in \mathbb{F}$ for $k > n$.

A very nice proof of Newton's identities is presented in [3]. It provides us with an *alternative proof*. Let $C \in \mathbb{F}^{n\times n}$ be the companion matrix of $P(\xi)$.

$$C = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & & 0 \\ \vdots & & & & \vdots \\ 0 & 0 & 0 & & 1 \\ -p_0 & -p_1 & -p_2 & \cdots & -p_{n-1} \end{bmatrix} \tag{4.2.7}$$

The characteristic polynomial of C is $P(\xi)$. The roots of $P(\xi)$ are the eigenvalues of C, and more generally, the k-th powers of the roots of $P(\xi)$ are the eigenvalues of C^k.
There also holds that the power sum s_k is the trace of C^k. Since $C \in \mathbb{F}^{n\times n}$, it follows that $C^k \in \mathbb{F}^{n\times n}$ for $k \in \mathbb{Z}_+$. Therefore

$$s_k = \text{trace}(C^k) \in \mathbb{F}\,, \quad \forall k \in \mathbb{Z}_+ \tag{4.2.8}$$

□

Proof of Theorem 4.2.2 First we prove the *if* part. We have to show that if w is given by (4.2.1) then $w(k) \in \mathbb{F}$ for all $k \in \mathbb{Z}_+$. Let w_m, $m = 0, \ldots, n-1$ be defined by

$$w_m(k) = \sum_{i=1}^{n} \lambda_i^{k+m} \tag{4.2.9}$$

then (4.2.1) can be written as

$$w(k) = \sum_{m=0}^{n-1} a_m w_m(k), \quad \text{with } a_m \in \mathbb{F},\ m = 0, \ldots, n-1. \tag{4.2.10}$$

In Lemma 4.2.4 it is shown that $\sum_{i=1}^{n} \lambda_i^k \in \mathbb{F}$ for all $k \in \mathbb{Z}_+$. This means that $\forall k \in \mathbb{Z}_+$ $w_m(k) \in \mathbb{F}$, with $m = 0, \ldots, n-1$. From (4.2.10) it follows that for all $k \in \mathbb{Z}_+$ holds that $w(k) \in \mathbb{F}$.
Now we have to show that w satisfies $P(\sigma)w = 0$. There holds

$$\begin{aligned} P(\sigma)w_m(k) &= P(\sigma) \sum_{i=1}^{n} \lambda_i^{k+m} = \sum_{i=1}^{n} P(\sigma)\lambda_i^{k+m} \\ &= \sum_{i=1}^{n} P(\lambda_i)\lambda_i^{k+m} = 0 \end{aligned}$$

The last equality holds because the λ_is are roots of $P(\xi)$. Hence

$$P(\sigma)w(k) = P(\sigma) \sum_{m=0}^{n-1} a_m w_m(k) = \sum_{m=0}^{n-1} a_m P(\sigma) w_m(k) = 0$$

Now we shall prove the *only if* part. First we show that the dimension of behavior $\mathfrak{B}$ equals $\deg(P(\xi)) = n$. A solution of (4.2.2) is completely determined by its initial values $w(0), \ldots, w(n-1)$. Let $\bar{w}_m$ denote the solution of (4.2.2) with

$$\bar{w}_m(k) = \begin{cases} 1 & \text{if } k = m \\ 0 & \text{if } k \neq m \end{cases} \quad m = 0, \ldots, n-1 \tag{4.2.11}$$

then $\mathfrak{B}$ is spanned by $\bar{w}_0, \ldots, \bar{w}_m$. The solutions $\bar{w}_m$, $m = 0, \ldots, n-1$ are obviously linearly independent. And *every* solution $w \in \mathfrak{B}$ is a linear combination of the solutions $\bar{w}_m$, $m = 0, \ldots, n-1$, given by

$$w = \sum_{m=0}^{n-1} \gamma_m \bar{w}_m\,, \qquad \text{with } \gamma_m = w(m)\,, \quad m = 0, \ldots, n-1 \tag{4.2.12}$$

We will now show that the n solutions w_m, $m = 0, \ldots n-1$ are linearly independent. Let $\alpha_m \in \mathbb{F}$, $m = 0, \ldots, n-1$ be such that $\sum_{m=0}^{n-1} \alpha_m w_m = 0$. That is

$$\alpha_0 \sum_{i=1}^{n} \lambda_i^k + \alpha_1 \sum_{i=1}^{n} \lambda_i^{k+1} + \cdots + \alpha_{n-1} \sum_{i=1}^{n} \lambda_i^{k+n-1} = 0\,, \qquad \text{for all } k \in \mathbb{Z}_+ \tag{4.2.13}$$

Alternatively we may write

$$\begin{bmatrix} \alpha_0 & \alpha_1 & \cdots & \alpha_{n-1} \end{bmatrix} \underbrace{\begin{bmatrix} 1 & 1 & \cdots & 1 \\ \lambda_1 & \lambda_2 & \cdots & \lambda_n \\ \vdots & & & \vdots \\ \lambda_1^{n-1} & \lambda_2^n & \cdots & \lambda_n^{n-1} \end{bmatrix}}_{V} \begin{bmatrix} \lambda_1^k \\ \lambda_2^k \\ \vdots \\ \lambda_n^k \end{bmatrix} = 0 \tag{4.2.14}$$

evaluating for $k = 0, \ldots, n-1$ yields

$$\begin{bmatrix} \alpha_0 & \alpha_1 & \cdots & \alpha_{n-1} \end{bmatrix} \begin{bmatrix} 1 & 1 & \cdots & 1 \\ \lambda_1 & \lambda_2 & \cdots & \lambda_n \\ \vdots & & & \vdots \\ \lambda_1^{n-1} & \lambda_2^n & \cdots & \lambda_n^{n-1} \end{bmatrix} \begin{bmatrix} 1 & \lambda_1 & \cdots & \lambda_1^{n-1} \\ 1 & \lambda_2 & \cdots & \lambda_2^{n-1} \\ \vdots & & & \vdots \\ 1 & \lambda_n & \cdots & \lambda_n^{n-1} \end{bmatrix} = \begin{bmatrix} 0 & \cdots & 0 \end{bmatrix} \quad (4.2.15)$$

or

$$\begin{bmatrix} \alpha_0 & \alpha_1 & \cdots & \alpha_n \end{bmatrix} V V^T = 0 \quad (4.2.16)$$

Matrix $V \in \mathbb{E}^{n \times n}$ is a Vandermonde matrix. Its determinant is given by $\det V = \prod_{1 \le i < j \le n} (\lambda_j - \lambda_i)$. Because the finite field $\mathbb{E}$ has no zero divisors, and $\lambda_1, \ldots, \lambda_n$ are mutually distinct, the Vandermonde matrix V is nonsingular. (In the proof of Lemma 4.3.6 in the next section, we give an alternative proof that V is nonsingular by showing that V has full row rank.) It follows that $\alpha_0, \ldots, \alpha_{n-1}$ must all be zero. This means that the solutions $w_0, \ldots w_{n-1}$ are linearly independent over $\mathbb{F}$. The dimension of $\mathfrak{B}$ is n, hence $\mathfrak{B}$ is spanned by $w_0, \ldots w_{n-1}$. So all solutions are of the form (4.2.1). □

Example 4.2.5 Let $\mathbb{F} = \mathbb{Z}_7$ and $P(\xi) = (\xi^2+\xi+3)(\xi^3+\xi+1)$. The second and third degree factors are irreducible because none of the elements of Z_7 is a root of either. Adjoining μ as root of $\xi^3 + \xi + 1$ and λ as root of $\xi^2 + \xi + 3$ yields $\mathbb{F}(\lambda, \mu)$. The roots of $\xi^3 + \xi + 1$ are $\lambda_1 = \mu$, $\lambda_2 = 2\mu^2 + 6$ and $\lambda_3 = 5\mu^2 + 6\mu + 1$. The roots of $\xi^2 + \xi + 3$ are $\lambda_4 = \lambda$ and $\lambda_5 = 6\lambda + 1$. The general solution is.

$$w(k) = \sum_{i=1}^{5} (a_0 + a_1\lambda_i + \cdots + a_4\lambda_i^4)(\lambda_i)^k, \quad a_0, \ldots, a_4 \in \mathbb{Z}_7$$

Example 4.2.6 Let the system $\Sigma(\mathbb{Z}_+, \mathbb{Z}_7, \mathfrak{B})$ be given by

$$R(\sigma)w = 0 \quad \text{with } R(\xi) = \xi^4 + 5\xi^2 + 4.$$

We can write $R(\xi)$ as a product of two 2nd-degree polynomials

$$R(\xi) = (\xi^2 + 1)(\xi^2 + 4)$$

These two *2nd-degree* polynomials are irreducible over $\mathbb{Z}_7$ because they don't have roots in $\mathbb{Z}_7$. Define λ as a root of $\xi^2 + 1$ then in $\mathbb{Z}_7(\lambda)$ the roots of $\xi^2 + 1$ are λ and $-\lambda \sim 6\lambda$.

$$(\xi - \lambda)(\xi + \lambda) = (\xi^2 - \lambda^2) = (\xi^2 + 1)$$

The second polynomial also splits over $\mathbb{Z}_7(\lambda)$. It has roots 2λ and 5λ

$$(\xi - 2\lambda)(\xi - 5\lambda) = \xi^2 + 3\lambda^2 = \xi^2 + 4$$

We see that $\mathbb{Z}_7(\lambda) \cong \mathbb{Z}_7[\xi]/(\xi^2 + 1)$ is a splitting field for $R(\xi)$.

The solution is given by

$$\begin{aligned} w(k) = & a_0 \left(\lambda^k + (6\lambda)^k + (2\lambda)^k + (5\lambda)^k\right) + \\ & a_1 \left(\lambda^{k+1} + (6\lambda)^{k+1} + (2\lambda)^{k+1} + (5\lambda)^{k+1}\right) + \\ & a_2 \left(\lambda^{k+2} + (6\lambda)^{k+2} + (2\lambda)^{k+2} + (5\lambda)^{k+2}\right) + \\ & a_3 \left(\lambda^{k+3} + (6\lambda)^{k+3} + (2\lambda)^{k+3} + (5\lambda)^{k+3}\right) \end{aligned}$$

Evaluating $w(k)$ for $k = 0, \ldots, 3$ yields

k	$w(k)$
0	$4a_0 + 4a_2$
1	$4a_1 + 6a_3$
2	$4a_0 + 6a_2$
3	$6a_1 + 3a_3$

The *scalar* system is given by $R(\sigma)w = 0$ with $R(\xi)$ a 4-th degree polynomial. A solution w is therefore completely determined by the initial conditions

$$w(k) = w_k \quad \text{for k=0,1,2,3}$$

We can express $a_0, \ldots, a_3$ in the initial values $w_0, \ldots, w_3$. There holds

$$\begin{bmatrix} w_0 \\ w_1 \\ w_2 \\ w_3 \end{bmatrix} = \underbrace{\begin{bmatrix} 4 & 0 & 4 & 0 \\ 0 & 4 & 0 & 6 \\ 4 & 0 & 6 & 0 \\ 0 & 6 & 0 & 3 \end{bmatrix}}_{M} \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix} \quad \Rightarrow \quad \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix} = \underbrace{\begin{bmatrix} 6 & 0 & 3 & 0 \\ 0 & 6 & 0 & 2 \\ 3 & 0 & 4 & 0 \\ 0 & 2 & 0 & 1 \end{bmatrix}}_{M^{-1}} \begin{bmatrix} w_0 \\ w_1 \\ w_2 \\ w_3 \end{bmatrix}$$

The solution should satisfy $(\sigma^4 + 5\sigma^2 + 4)w = 0$, that is

$$w(k+4) = 2w(k+2) + 3w(k) \tag{4.2.17}$$

Evaluating $w(k)$ for $k = 0, \ldots, 23$ yields

k	$w(k)$	k	$w(k)$	k	$w(k)$	k	$w(k)$
0	w_0	6	$6w_0$	12	w_0	18	$6w_0$
1	w_1	7	$6w_1$	13	w_1	19	$6w_1$
2	w_2	8	$6w_2$	14	w_2	20	$6w_2$
3	w_3	9	$6w_3$	15	w_3	21	$6w_3$
4	$3w_0 + 2w_2$	10	$4w_0 + 5w_2$	16	$3w_0 + 2w_2$	22	$4w_0 + 5w_2$
5	$3w_1 + 2w_3$	11	$4w_1 + 5w_2$	17	$3w_1 + 2w_3$	23	$4w_1 + 5w_2$

It is obvious that (4.2.17) is satisfied for $k = 0$ and $k = 1$. Also

$$\begin{aligned} w(6) &= 2w(4) + 3w(2) = (6w_0 + 4w_2) + 3w_2 = 6w_0 \\ w(7) &= 2w(5) + 3w(3) = (6w_1 + 4w_3) + 3w_3 = 6w_1 \\ w(8) &= 2w(6) + 3w(4) = (5w_0) + (2w_0 + 6w_2) = 6w_2 \end{aligned}$$

4.3 Multivariable autonomous systems

We consider the multivariable autonomous system $\Sigma = (\mathbb{Z}_+, \mathbb{F}^q, \mathfrak{B})$ with $\mathbb{F}$ a finite field. The behavior $\mathfrak{B}$ is given by

$$R(\sigma)w = 0 \tag{4.3.1}$$

with $R(\xi) \in \mathbb{F}^{q\times q}[\xi]$ and $\det R(\xi) \neq 0$. Let $\chi(\xi)$ be the corresponding characteristic polynomial and n the degree of $\chi(\xi)$. Let $\mathbb{E}$ be an extension field of $\mathbb{F}$ such that $\chi(\xi)$ splits over $\mathbb{E}$.

$$\chi(\xi) = \prod_{i=1}^{n}(\xi - \lambda_i) \quad \text{with } \lambda_i \in \mathbb{E}$$

As before, we only consider the case that $\lambda_1, \ldots, \lambda_n$ are mutually distinct.

Since each characteristic value λ_i is a simple root of $\chi(\xi)$ in $\mathbb{E}$, the kernel of $R(\lambda_i) \in \mathbb{E}^{q\times q}$ is one-dimensional.

Theorem 4.3.1 *There exists a nonzero polynomial vector $v(\xi) \in \mathbb{F}^q[\xi]$ such that*

$$\ker_{\mathbb{E}} R(\lambda_i) = \{v(\lambda_i)\}$$

where $\lambda_i, i = 1, \ldots, n$ are the distinct roots of $\det R(\xi)$.

Proof First we will show that there exists a polynomial vector $v(\xi)$ such that $v(\lambda_i) \neq 0$ and $R(\lambda_i)v(\lambda_i) = 0$ for $i = 1, \ldots, n$. Polynomial matrix $R(\xi)$ can be brought into Smith form.[1] That is, there exist unimodular matrices $U(\xi), V(\xi) \in \mathbb{F}^{q\times q}[\xi]$ such that

$$U(\xi)R(\xi)V(\xi) = D(\xi)$$

with $D(\xi)$ a diagonal matrix $D(\xi) = \operatorname{diag}(d_1(\xi), d_2(\xi), \ldots, d_q(\xi))$, where $d_i(\xi), i = 1, \ldots, q$ are monic polynomials in $\mathbb{F}[\xi]$ and $d_i(\xi)$ divides $d_{i+1}(\xi)$. Because $\det R(\xi) \neq 0$, there holds $d_i(\xi) \neq 0$ for $i = 1, \ldots, q$. The roots of $\det R(\xi)$ in extension field $\mathbb{E}$ are simple. This implies that $D(\xi)$ is given by

$$D(\xi) = \operatorname{diag}(1, \ldots, 1, \chi(\xi))$$

Define $v(\xi)$ as the last column of $V(\xi)$, that is

$$v(\xi) = V(\xi)u \quad \text{with } u = \begin{bmatrix}0 & 0 & \cdots & 0 & 1\end{bmatrix}^T$$

then

$$\begin{aligned} R(\xi)v(\xi) &= U^{-1}(\xi)D(\xi)V^{-1}(\xi)V(\xi)u = U^{-1}(\xi)D(\xi)u \\ &= U^{-1}(\xi)\begin{bmatrix}0 & 0 & \cdots & 0 & \chi(\xi)\end{bmatrix}^T \end{aligned}$$

For every λ_i, $i = 1, \ldots, n$ holds $R(\lambda_i)v(\lambda_i) = 0$ and $v(\lambda_i) = V(\lambda_i)u \neq 0$ because $V(\xi)$ is unimodular. The determinant of $V(\lambda_i)$ is nonzero, so the last column of $V(\lambda_i)$ has nonzero elements.

[1] cf. [6] Appendix B.1.

Now we will show that $\ker_{\mathbb{E}} R(\lambda_i) = \{v(\lambda_i)\}$. Let $R(\lambda_i)\tilde{v} = 0$ then $U^{-1}(\lambda_i)D(\lambda_i)V^{-1}(\lambda_i)\tilde{v} = 0$. So $D(\lambda_i)V^{-1}(\lambda_i)\tilde{v} = 0$. This means that $V^{-1}(\lambda_i)\tilde{v} = \begin{bmatrix}0,\ldots,0,c\end{bmatrix}^T$ and thus $\tilde{v} = cv(\lambda_i)$ for $c \in \mathbb{E}$. □

The multivariable version of Theorem 4.2.2 is

Theorem 4.3.2 *Let $v(\xi) \in \mathbb{F}^q[\xi]$ be a polynomial vector such that $\ker_{\mathbb{E}} R(\lambda_i) = \{v(\lambda_i)\}$. Then $w \in \mathfrak{B}$ if and only if w of the form*

$$w(k) = \sum_{i=1}^{n}(a_0 + a_1\lambda_i + \cdots + a_{n-1}\lambda_i^{n-1})v(\lambda_i)(\lambda_i)^k \tag{4.3.2}$$

with $a_i \in \mathbb{F}$, $i = 0,\ldots,n-1$.

Lemma 4.3.3 *Let w be given by (4.3.2). If $a_j \in \mathbb{F}$, $j = 1,\ldots,n$ then $w(k) \in \mathbb{F}^q$ for all $k \in \mathbb{Z}_+$*

Proof Let r be the maximum row degree of polynomial vector $v(\xi)$. Then $v(\xi)$ can be written as

$$v(\xi) = \sum_{j=0}^{r} v_j\xi^j, \quad \text{with } v_j \in \mathbb{F}^q, j = 0,\ldots,r$$

Rewriting (4.3.2) yields

$$\begin{aligned} w(k) &= \sum_{i=1}^{n}\left(\sum_{m=0}^{n-1} a_m\lambda_i^m\right)\left(\sum_{j=0}^{r} v_j\lambda_i^j\right)(\lambda_i)^k \\ &= \sum_{i=1}^{n}\sum_{j=0}^{r}\sum_{m=0}^{n-1} a_m v_j \lambda_i^{m+j+k} \\ &= \sum_{j=0}^{r}\sum_{m=0}^{n-1} a_m v_j \left(\sum_{i=1}^{n}\lambda_i^{m+j+k}\right) \end{aligned}$$

Because for $m = 0,\ldots,n-1$, $j = 0,\ldots,n-1$, and for all $k \in \mathbb{Z}_+$ holds $a_m \in \mathbb{F}, v_j \in \mathbb{F}^q$ and, by Lemma 4.2.4, $\sum_{i=1}^{n}\lambda_i^{m+j+k} \in \mathbb{F}$. It follows that $w(k) \in \mathbb{F}^q$ for all $k \in \mathbb{Z}_+$ □

Lemma 4.3.4 *4.3.2 Let w be given by (4.3.2) then there holds $R(\sigma)w = 0$.*

Proof For all $k \in \mathbb{Z}_+$

$$\begin{aligned} R(\sigma)w(k) &= R(\sigma)\sum_{i=1}^{n}(a_0 + a_1\lambda_i + \cdots + a_{n-1}\lambda_i^{n-1})v(\lambda_i)(\lambda_i)^k \\ &= \sum_{i=1}^{n}(a_0 + a_1\lambda_i + \cdots + a_{n-1}\lambda_i^{n-1})R(\sigma)\left(v(\lambda_i)(\lambda_i)^k\right) \\ &= \sum_{i=1}^{n}(a_0 + a_1\lambda_i + \cdots + a_{n-1}\lambda_i^{n-1})R(\lambda_i)v(\lambda_i)(\lambda_i)^k \\ &= 0 \end{aligned}$$

□

Lemma 4.3.5 *Behavior $\mathfrak{B}$ has dimension n.*

Proof Let $U(\xi)D(\xi)V(\xi)$ be a Smith form decomposition of $R(\xi)$. So $D(\xi) = \operatorname{diag}(1,\ldots,1,\chi(\xi))$ and $U(\xi)$ and $V(\xi)$ are unimodular matrices. Let $\tilde{\mathfrak{B}}$ be the behavior defined by

$$\tilde{\mathfrak{B}} = \{\tilde{w}\colon Z_+ \to \mathbb{F}^q \mid D(\sigma)\tilde{w} = 0\}\,.$$

It is obvious that $\tilde{w} \in \mathfrak{B}$ if and only if $\tilde{w} = (0,\ldots,0,\tilde{w}_n)$ where $\tilde{w}_n$ is a solution of the scalar differential equation

$$\chi(\sigma)\tilde{w}_n = 0\,. \tag{4.3.3}$$

It follows from Theorem 4.2.2 that $\tilde{\mathfrak{B}}$ has dimension n. Now let $\tilde{w} \in \tilde{\mathfrak{B}}$ then $w = V^{-1}(\sigma)\tilde{w} \in \mathfrak{B}$ because $R(\sigma)w = U(\sigma)D(\sigma)V(\sigma)V^{-1}(\sigma)\tilde{w} = U(\sigma)D(\sigma)\tilde{w} = 0$ Also if $w \in \mathfrak{B}$ then $\tilde{w} = V(\sigma)w \in \tilde{\mathfrak{B}}$ because $D(\sigma)\tilde{w} = U^{-1}(\sigma)R(\sigma)V^{-1}(\sigma)V(\sigma)w = U^{-1}(\sigma)R(\sigma)w = 0$ So $V(\sigma)$ defines an isomorphism between $\mathfrak{B}$ and $\tilde{\mathfrak{B}}$. Therefore $\mathfrak{B}$ has the same dimension as $\tilde{\mathfrak{B}}$, that is n. □

We can rewrite equation 4.3.2 as a linear combination

$$w(k) = \sum_{m=0}^{n-1} a_m w_m(k) \quad \text{with } a_0,\ldots,a_{n-1} \in \mathbb{F} \quad \text{and} \tag{4.3.4}$$

$$w_m(k) := \sum_{i=1}^{n} v(\lambda_i)\lambda_i^{k+m} \quad m = 0,\ldots,n-1\,, k \in \mathbb{Z}_+\,. \tag{4.3.5}$$

It follows from Lemmas 4.3.3 and 4.3.4 that $w_0,\ldots,w_{n-1}$ are elements of $\mathfrak{B}$.

Lemma 4.3.6 *The solutions $w_0,\ldots,w_{n-1}$ as defined in* (4.3.5) *are independent.*

Proof Let $w(k) = 0$ for $k \in Z_+$ with w as given in (4.3.4). Then for all $k \in \mathbb{Z}_+$

$$M(k)\begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix} \tag{4.3.6}$$

with $M(k)$ the $q \times n$ matrix given by

$$M(k) = \begin{bmatrix} w_0(k) & w_1(k) & \cdots & w_{n-1}(k) \end{bmatrix} \tag{4.3.7}$$

$$= \begin{bmatrix} \sum_{i=1}^{n} v(\lambda_i)\lambda_i^{k} & \sum_{i=1}^{n} v(\lambda_i)\lambda_i^{k+1} & \cdots & \sum_{i=1}^{n} v(\lambda_i)\lambda_i^{k+n-1} \end{bmatrix} \tag{4.3.8}$$

$$= \begin{bmatrix} \lambda_1^k v(\lambda_1) & \lambda_2^k v(\lambda_2) & \cdots & \lambda_n^k v(\lambda_n) \end{bmatrix} \begin{bmatrix} 1 & \lambda_1 & \cdots & \lambda_1^{n-1} \\ 1 & \lambda_2 & \cdots & \lambda_2^{n-1} \\ \vdots & \vdots & & \vdots \\ 1 & \lambda_n & \cdots & \lambda_n^{n-1} \end{bmatrix} \tag{4.3.9}$$

Evaluating (4.3.6) for $k = 0, \ldots, n-1$ yields the following equation, where the first matrix is formed by stacking the first matrix in (4.3.9) for $k = 0, \ldots, n-1$.

$$\begin{bmatrix} v(\lambda_1) & v(\lambda_2) & \cdots & v(\lambda_n) \\ \lambda_1 v(\lambda_1) & \lambda_2 v(\lambda_2) & \cdots & \lambda_n v(\lambda_n) \\ & & & \\ \lambda_1^{n-1} v(\lambda_1) & \lambda_2^{n-1} v(\lambda_2) & \cdots & \lambda_n^{n-1} v(\lambda_n) \end{bmatrix} \begin{bmatrix} 1 & \lambda_1 & \cdots & \lambda_1^{n-1} \\ 1 & \lambda_2 & \cdots & \lambda_2^{n-1} \\ \vdots & \vdots & & \vdots \\ 1 & \lambda_n & \cdots & \lambda_n^{n-1} \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix} \tag{4.3.10}$$

We can write the first matrix in (4.3.10) as a product of a big $nq \times nq$ VanderMonde-like matrix and a $nq \times n$ matrix

$$\underbrace{\begin{bmatrix} I_q & I_q & \cdots & I_q \\ \lambda_1 I_q & \lambda_2 I_q & \cdots & \lambda_n I_q \\ \vdots & \vdots & & \vdots \\ \lambda_1^{n-1} I_q & \lambda_2^{n-1} I_q & \cdots & \lambda_n^{n-1} I_q \end{bmatrix}}_{W} \begin{bmatrix} v(\lambda_1) & 0 & \cdots & 0 \\ 0 & v(\lambda_2) & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & v(\lambda_n) \end{bmatrix} \tag{4.3.11}$$

The rank of W is nq. Close inspectation of the rows of W shows that they are linearly independent. We will prove this. Let $\begin{bmatrix} c_1 & c_2 & \cdots & c_{qn} \end{bmatrix} W = 0$ then for $j = 1, \ldots, q$

$$\sum_{k=0}^{n-1} c_{j+kq} \lambda^k = 0 \quad \text{for } \lambda = \lambda_1, \lambda_2, \ldots, \lambda_n \tag{4.3.12}$$

The $n-1$ degree polynomial given in (4.3.12) has n distinct roots! From the fundamental theorem of algebra it follows that the coefficients $c_{j+kq}, k = 0, \ldots, n-1$ are all zero, with $j = 1, \ldots, q$. So all coefficients $c_1, \ldots, c_{nq}$ are equal to zero. Square matrix W has full row rank and is therefore invertible. If we premultiply both sides of (4.3.10) with W^{-1} we get

$$\begin{bmatrix} v(\lambda_1) & 0 & \cdots & 0 \\ 0 & v(\lambda_2) & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & v(\lambda_n) \end{bmatrix} \begin{bmatrix} 1 & \lambda_1 & \cdots & \lambda_1^{n-1} \\ 1 & \lambda_2 & \cdots & \lambda_2^{n-1} \\ \vdots & \vdots & & \vdots \\ 1 & \lambda_n & \cdots & \lambda_n^{n-1} \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix} \tag{4.3.13}$$

Since all vectors $v(\lambda_1), \ldots, v(\lambda_n)$ are nonzero, the first matrix has full column rank. The transposed Vandermonde matrix in this equation is nonsingular, as we have seen in Section 4.2. The product of these matrices is of full column rank. Therefore $a_0, \ldots, a_{n-1}$ must be equal to zero. The solutions $w_0, w_1, \ldots, w_{n-1}$ are independent. □

Proof of Theorem 4.3.2 The *if* part follows from Lemmas 4.3.3 and 4.3.4.
The *only if* part goes as follows. We see in Lemma 4.3.5 that $\dim \mathfrak{B} = n$. Equation 4.3.5 and Lemma 4.3.6 show that $w_0, \ldots, w_{n-1}$ are n independent solutions in $\mathfrak{B}$. It follows that $\mathfrak{B}$ is spanned by those solutions. So any solution $w \in \mathfrak{B}$ can be written as in (4.3.4), that is as in (4.3.2). □

Remark 4.3.7 There are many polynomial vectors $v(\xi)$ that satisfy $\ker_{\mathbb{E}} R(\lambda_i) = \{v(\lambda_i)\}, i = 1, \ldots, n$. It doesn't have to be the polynomial vector $v(\xi)$ we have derived in the proof of Theorem 4.3.1.

4.3.1 Relation with the scalar case

How does Theorem 4.3.2 relate to Theorem 4.2.2? Let $P(\xi)$ be a scalar polynomial of degree n and $\lambda_1, \ldots, \lambda_n$ the distinct roots of $P(\xi)$. Obviously, since $P(\lambda_i) = 0, i = 1, \ldots, n$, the polynomial $v(\xi) = 1$ satisfies $\ker_{\mathbb{E}} P(\lambda_i) = \{v(\lambda_i)\} = \{1\}$ for all $i = 1, \ldots, n$. Substitution of $v(\xi) = 1$ in (4.3.2) yields (4.2.1).
Note that we may also take for example $v(\xi) = \xi$ if all roots are nonzero. Then (4.3.2) becomes

$$w(k) = \sum_{i=1}^{n} (a_0\lambda_i + a_1\lambda_i^2 + \cdots + a_{n-1}\lambda_i^n)(\lambda_i)^k$$

Because $P(\lambda_i) = 0$ for all roots of $P(\xi) = \xi^n + p_{n-1}\xi^{n-1} + \cdots + p_0$ there holds $\lambda_i^n = -p_{n-1}\lambda_i^{n-1} - \cdots - p_0$, $i = 1, \ldots, n$. So again the solution can be written in the form (4.2.1).

4.3.2 Irreducible characteristic polynomials

Consider the multivariable system $\Sigma = (\mathbb{Z}_+, \mathbb{F}^q, \mathfrak{B})$ with $\mathbb{F}$ a finite field. Let the behavior be given by

$$R(\sigma)w = 0, \quad \text{with } R(\xi) \in \mathbb{F}^{q\times q}[\xi]$$

If the characteristic polynomial $\chi(\xi)$ is *irreducible* over $\mathbb{F}$, we can define a splitting field $\mathbb{F}(\lambda) \cong \mathbb{F}[\xi]/(\chi(\xi))$ of $\mathbb{F}$ with λ defined as a root of $\chi(\xi)$. The polynomial $\chi(\xi)$ splits over $\mathbb{F}(\lambda)$, and according to Theorem 2.2.16 the characteristic values λ_i, $i = 1, \ldots n$ are mutually distinct and given by

$$\lambda_i = \lambda^{(r^{i-1})}, \ i = 1, \ldots, n \quad \text{with } r = |\mathbb{F}| = p^m, p \text{ prime.}$$

The minimum polynomial of λ over $\mathbb{F}$ is $\chi(\lambda)$.

Theorem 4.3.8 *Let $v_\lambda \in \mathbb{F}(\lambda)^q$ be such that $\ker_{\mathbb{F}(\lambda)} R(\lambda) = \{v_\lambda\}$. Vector v_λ can be written as $\sum_{i=0}^{n-1} v_i\lambda^i$ with $v_i \in \mathbb{F}^q$ because $\{1, \lambda, \lambda^2, \ldots, \lambda^{n-1}\}$ is a basis of $\mathbb{F}(\lambda)$ over $\mathbb{F}$.*
Now define $v(\xi) := \sum_{i=0}^{n-1} v_i\xi^i \in \mathbb{F}^q[\xi]$. Then there holds

$$R(\lambda_i)v(\lambda_i) = 0, \quad i = 1, \ldots, n$$

Proof Define $w(\xi) = R(\xi)v(\xi)$ then $w(\lambda) = 0$, so λ is a root of each element of $w(\xi)$. Since $\chi(\xi)$ is the minimum polynomial of λ over $\mathbb{F}$, $\chi(\xi)$ divides all elements of $w(\xi)$ (Theorem 2.2.13). Each $\lambda_i, i = 1, \ldots, n$ is by definition a root of $\chi(\xi)$, hence $w(\lambda_i) = 0$.

Since the elements of $v(\xi)$ are polynomials of degree $< n$, it follows that $v(\lambda_i) \neq 0$ for $i = 1, \ldots, n$ because the λ_is are roots of the n-th degree *minimal* polynomial $\chi(\xi)$. □

We see that for an irreducible characteristic polynomial it is very easy to obtain a polynomial vector $v(\xi)$ that can be applied in Theorem 4.3.2.

Example 4.3.9 (Two variable system with irreducible characteristic polynomial) Consider the system $\Sigma(\mathbb{Z}_+, \mathbb{Z}_p^q, \mathfrak{B})$, with $p = 5, q = 2$ and the behavior given by

$$R(\sigma)w = 0, \quad \text{with } R(\xi) = \begin{bmatrix} 1 & 3\xi^2 + 1 \\ 3\xi & 4\xi + 1 \end{bmatrix}$$

The determinant is

$$\det R(\xi) = (4\xi + 1) - (3\xi^2 + 1)(3\xi) = \xi^3 + \xi + 1$$

This polynomial is monic, the characteristic polynomial is therefore $\chi(\xi) = \xi^3 + \xi + 1$. The *3rd degree* polynomial $\chi(\xi)$ has no roots in $\mathbb{Z}_5$ and is thus irreducible over $\mathbb{Z}_5$ (Theorem 2.2.12).

In field extension $\mathbb{Z}_5(\lambda)$, with λ defined as a root of $\chi(\xi)$, the roots of $\chi(\xi)$ are given by

$$\begin{aligned}
&\lambda_1 = \lambda, \\
&\lambda_2 = \lambda^5 = \lambda^2(\lambda^3) = \lambda^2(4\lambda + 4) = 4\lambda^3 + 4\lambda^2 = 4\lambda^2 + \lambda + 1 \\
&\lambda_3 = \lambda^{25} = \cdots = \lambda^2 + 3\lambda + 4
\end{aligned}$$

We see that the roots are mutually distinct.
The kernel of $R(\lambda)$ is $\{v(\lambda)\}$ with $v(\lambda) = \begin{bmatrix} 4\lambda + 1 & -3\lambda \end{bmatrix}^T \sim \begin{bmatrix} 4\lambda + 1 & 2\lambda \end{bmatrix}^T$. To verify this we calculate $R(\lambda)v(\lambda)$.

$$\begin{bmatrix} 1 & 3\lambda^2 + 1 \\ 3\lambda & 4\lambda + 1 \end{bmatrix} \begin{bmatrix} 4\lambda + 1 \\ 2\lambda \end{bmatrix} = \begin{bmatrix} 6\lambda^3 + 6\lambda + 1 \\ 20\lambda^2 + 5\lambda \end{bmatrix} = \begin{bmatrix} \lambda^3 + \lambda + 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$$

Substituting λ_1, λ_2 and λ_3 yields

$$v(\lambda_1) = \begin{bmatrix} 4\lambda + 1 \\ 2\lambda \end{bmatrix}, \quad v(\lambda_2) = \begin{bmatrix} \lambda^2 + 4\lambda \\ 3\lambda^2 + 2\lambda + 2 \end{bmatrix}, \quad v(\lambda_3) = \begin{bmatrix} 4\lambda^2 + 2\lambda + 2 \\ 2\lambda^2 + \lambda + 3 \end{bmatrix}$$

The general solution of $R(\sigma)w = 0$ is given by

$$w(k) = \sum_{i=1}^{3} (a_0 + a_1\lambda_i + a_2\lambda_i^2) v(\lambda_i)(\lambda_i)^k \quad \text{with } a_0, a_1, a_2 \in \mathbb{Z}_5.$$

Evaluating $w(k)$ for $k = 0, \ldots, 5$ yields

k	0	1	2
$w(k)$	$\begin{bmatrix} 3a_0 + 2a_1 + a_2 \\ a_1 + 4a_2 \end{bmatrix}$	$\begin{bmatrix} 2a_0 + a_1 \\ a_0 + 4a_1 + 4a_2 \end{bmatrix}$	$\begin{bmatrix} a_0 + 2a_2 \\ 4a_0 + 4a_1 \end{bmatrix}$
k	3	4	5
$w(k)$	$\begin{bmatrix} 2a_1 + 4a_2 \\ 4a_0 + 2a_2 \end{bmatrix}$	$\begin{bmatrix} 2a_0 + 4a_1 + 3a_2 \\ 2a_1 + a_2 \end{bmatrix}$	$\begin{bmatrix} 4a_0 + 3a_1 + 4a_2 \\ 2a_0 + a_1 + 3a_2 \end{bmatrix}$

We see that $w(0), \ldots, w(5) \in \mathbb{Z}_5^2$. We now check if this solution satisfies $R(\sigma)w = 0$. There should hold

$$\begin{aligned}
w_1(k) + 3w_2(k+2) + w_2(k) &= 0 \\
3w_1(k+1) + 4w_2(k+1) + w_2(k) &= 0
\end{aligned}$$

Substituting $k = 0$ yields

$$\begin{aligned}
&(3a_0 + 2a_1 + a_2) + 3(4a_0 + 4a_1) + (a_1 + 4a_2) = 0 \\
&3(2a_0 + a_1) + 4(a_0 + 4a_1 + 4a_2) + (a_1 + 4a_2) = 0
\end{aligned}$$

Substituting $k = 1$ yields

$$(2a_0 + a_1) + 3(4a_0 + 2a_2) + (a_0 + 4a_1 + 4a_2) = 0$$
$$3(a_0 + 2a_2) + 4(4a_0 + 4a_1) + (a_0 + 4a_1 + 4a_2) = 0$$

We could have derived another polynomial $v(\xi)$ by bringing $R(\xi)$ into Smith form, using Theorem 4.3.1. There holds that

$$\underbrace{\begin{bmatrix} 1 & 0 \\ 2\xi & 1 \end{bmatrix}}_{U(\xi)} \underbrace{\begin{bmatrix} 1 & 3\xi^2+1 \\ 3\xi & 4\xi+1 \end{bmatrix}}_{R(\xi)} \underbrace{\begin{bmatrix} 1 & 2\xi^2+4 \\ 0 & 1 \end{bmatrix}}_{V(\xi)} = \underbrace{\begin{bmatrix} 1 & 0 \\ 0 & \xi^3+\xi+1 \end{bmatrix}}_{D(\xi)}$$

Take $v(\xi) = V_{*2}(\xi) = \begin{bmatrix} 2\xi^2+4 \\ 1 \end{bmatrix}$. Note that $2\lambda v(\lambda) = \cdots = \begin{bmatrix} 4\lambda+1 \\ 2\lambda \end{bmatrix}$. □

Remark 4.3.10 If we define

$$A_i := (a_0 + a_1\lambda_i + a_2\lambda_i^2)v(\lambda_i) \quad \text{for } i = 1, \ldots, 3$$

then $w(k) = A_1\lambda_1^k + A_2\lambda_2^k + A_3\lambda_3^k$. There holds that the vectors $A_1, A_2, A_3 \in Z_5(\lambda)$ are *conjugated*. By this we mean that

$$(\xi - A_{11})(\xi - A_{12})(\xi - A_{13}) \in \mathbb{Z}_5[\xi], \quad i = 1, 2.$$

where A_{ij} denotes element i of vector A_j. We have checked this using `Maple`.

Chapter 5

Single input single output systems

The previous chapter dealt with autonomous behaviors over a finite field. In this chapter we will give a solution of the single input single output system given by

$$p(\sigma)y(k) = q(\sigma)u(k)\,, \quad k \in \mathbb{Z}_+ \tag{1}$$

where $p(\xi) = p_n\xi^n + \cdots + p_1\xi + p_0 \in \mathbb{F}[\xi]$ is a polynomial of degree $n \geq 1$, $q(\xi) = q_d\xi^n + \cdots + q_1\xi + q_0 \in \mathbb{F}[\xi]$ a polynomial of degree $d \leq n$, $\mathbb{F}$ a finite field. All input values $u(k), k \in \mathbb{Z}_+$ belong to $\mathbb{F}$. The output values $y(k)$ should also belong to $\mathbb{F}$.
Let $\mathbb{E}$ be an extension field of $\mathbb{F}$ such that $p(\xi)$ splits over $\mathbb{E}$. As in the previous chapter, we will assume that the roots of $p(\xi)$ are mutually distinct.
Every solution (u, y) of (1) can be written as $(0, y_\mathrm{h}) + (u, y_\mathrm{p})$, where y_h is a solution of the homogeneous difference equation

$$p(\sigma)y = 0 \tag{2}$$

and (u, y_p) is a particular solution of (1). In Theorem 4.2.2 it was shown that any solution $y_\mathrm{h} \in \mathbb{F}^{\mathbb{Z}_+}$ of (2) can be written as

$$y_\mathrm{h}(k) = \sum_{i=1}^{n}(a_0 + a_1\lambda_i + \cdots + a_{n-1}\lambda_i^{n-1})(\lambda_i)^k \tag{3}$$

with $a_m \in \mathbb{F}$, $m = 0, \ldots, n-1$.

5.1 A particular solution for a siso system

We can derive a particular solution in case $\mathbb{F} = \mathbb{R}$. Let $G(s) = q(s)/p(s)$ be the transfer function of (1). Then y satisfies (1) if it is given by the convolution sum

$$y(k) = \sum_{j=0}^{k} g(j)u(k-j) \tag{5.1.1}$$

where $g(j)$ is the inverse z-transform of $G(z)$. We can obtain $g(j)$ from the partial fraction expansion of $G(z)$. Let $\lambda_1, \ldots, \lambda_n$ be the mutually distinct roots of $p(\xi)$. (Note that with $\mathbb{F} = \mathbb{R}$, the roots belong to $\mathbb{E} = \mathbb{C}$). Then

$$G(z) = \frac{q(z)}{p(z)} = a_0 + \frac{a_1}{z-\lambda_1} + \frac{a_2}{z-\lambda_2} + \cdots + \frac{a_n}{z-\lambda_n}$$

With

$$a_0 = \begin{cases} 0 & \text{if } d < n \\ q_d/p_n & \text{if } d = n \end{cases}$$

where q_d, p_n are the leading coefficients of $q(\xi)$ and $p(\xi)$ respectively, and

$$a_i = \frac{q(\lambda_i)}{\tilde{p}_i(\lambda_i)} \quad \text{with } \tilde{p}_i := p(\xi)/(\xi - \lambda_i) \in \mathbb{E}[\xi]\,.$$

The inverse z-transform of a_0 is $a_0\delta(j)$. The inverse z-transform of $a_i/(z-\lambda_i)$ is $a_i\lambda_i^{j-1}$ for $j \geq 1$ and 0 for $j = 0$. From (5.1.1) it follows that a particular solution is given by

$$y_{\mathrm{p}}(k) = a_0 u(k) + \sum_{j=1}^{k}\sum_{i=1}^{n} a_i \lambda_i^{j-1} u(k-j) \tag{5.1.2}$$

It is a well-known solution of (1), also in case $\mathbb{F}$ is a finite field and $\mathbb{E}/\mathbb{F}$ the finite field extension over which $p(\xi)$ splits. It is actually a solution for $\mathbb{T} = \mathbb{Z}$ where $u(k) = y(k) = 0 \in \mathbb{F}$ for $k < 0$. There holds

$$p_n y(k+n) = -p_{n-1}y(k+n-1) - \cdots - p_0 y(k) + q_d u(k+d) + \cdots + q_0 u(k) \quad d \leq n$$

Since $u(k) \in \mathbb{F}$ for $k \geq 0$, it follows iteratively that $y(k) \in \mathbb{F}$ for $k \geq 0$. So every solution $y(k) = y_{\mathrm{h}}(k) + y_{\mathrm{p}}(k) \in \mathbb{F}$.
The Appendix contains the MAPLE code of an example, where $p(\xi) = \xi^3+\xi+1$, $q(\xi) = \xi+2$ and $\mathbb{F} = \mathbb{Z}_5$.

Chapter 6

Conclusion and further research

In this part we have discussed discrete time behaviors over finite fields. Explicit expressions have been obtained for scalar and multivariable autonomous systems given by $\mathfrak{B} = \{w\colon \mathbb{Z}_+ \to \mathbb{F}^q \mid R(\sigma)w = 0\}, R(\xi) \in \mathbb{F}^{q\times q}[\xi]$, $\mathbb{F}$ a finite field, for the case that roots of the characteristic polynomials are not necessarily elements of finite field $\mathbb{F}$. This was done by constructing an extension field of $\mathbb{F}$ in which the characteristic polynomial splits. Assuming that the characteristic values are mutually distinct, we were able to restrict the solutions $w\colon \mathbb{Z}_+ \to \mathbb{E}^q$ such that $w(k) \in \mathbb{F}^q$ for $k \in \mathbb{Z}_+$. Finally we derived a particular solution for the single input, single output case.

Suggestions for further research are

- The case that characteristic values have a multiplicity greater than one.
  This is more complicated because we have used Newton's identities, that relate power sums of the roots of a polynomial ($\sum_{i=1}^{n} \lambda_i^k$) to its coefficients, to prove that solutions were confined to $\mathbb{F}$. If the characteristic values are not simple, the solutions will not be linear combinations of power sums.
- multivariable input/output systems.

Appendix

Example Chapter 5

```
> restart;
F=Z_5
> p:=5;
                                  p := 5
> P:=xi^3+xi+1;
                                   3
                           P := xi  + xi + 1
> Q:=xi+2;
                              Q := xi + 2
P is irreducible over F
> Irreduc(P) mod p;
                                   true
Define lambda as a root of P
> alias(lambda=RootOf(P));
                                  lambda
Compute all roots
> r:=Roots(P,lambda) mod p:
> Lambda:=r[1..3,1];

                            2                          2
  Lambda := [lambda, lambda  + 3 lambda + 4, 4 lambda  + lambda + 1]

Define the transfer function
> G:=unapply(Q/P,xi);

                                     xi + 2
                        G := xi -> ------------
                                      3
                                   xi  + xi + 1

Compute one coefficient of the pfe, using limits
>
> simplify(limit(G(xi)*(xi-Lambda[1]),xi=Lambda[1])) mod p;

                                        2
                              2 + 3 lambda

Compute all coefficients a[i] of the pfe by dividing the denominator of G(xi) by
(xi-lambda[i]), then substitute xi=lambda[i])
> for i to 3 do
> numer(G(xi))/((Factor(denom(G(xi)),lambda) mod p)/(xi-Lambda[i] mod p)):
> a[i]:=simplify(subs(xi=Lambda[i],%)) mod p;
> od:
> a[1];a[2];a[3];
                                        2
                              2 + 3 lambda
                                   2
                          3 lambda  + 2 + lambda
```

```
                              2
                     4 lambda  + 1 + 4 lambda
```

```
Compute a particular solution
> som1:=a[1]*Lambda[1]^(j-1)+a[2]*Lambda[2]^(j-1)+a[3]*Lambda[3]^(j-1):
> yp:=sum(som1*u(k-j),j=1..k) mod p;
>
```

$$yp := \left(\sum_{j=1}^{k} \left((2 + 3\,\lambda)\,\lambda^{2}\right)^{(j-1)}\right) u(k-j)$$

$$\left(\sum_{j=1}^{k} \left(3\,\lambda^{2} + 2 + \lambda\right)\left(\lambda^{2} + 3\,\lambda + 4\right)^{(j-1)} + \left(4\,\lambda^{2} + 1 + 4\,\lambda\right)\left(4\,\lambda^{2} + \lambda + 1\right)^{(j-1)}\right) u(k-j)$$

```
> ypart:=t->simplify(eval(yp,k=t)) mod p;

                ypart := t -> simplify(yp|     ) mod p
                                        |k = t

Check whether the solution y(h) belongs to F
> for h from 0 to 8 do ypart(h) od;

                                    0
                                    0
                                   u(0)
                                u(1) + 2 u(0)
                             4 u(0) + u(2) + 2 u(1)
                          4 u(1) + u(3) + 2 u(2) + 2 u(0)
                       4 u(0) + 4 u(2) + u(4) + 2 u(3) + 2 u(1)
                    4 u(1) + 4 u(3) + u(5) + 2 u(4) + 4 u(0) + 2 u(2)
                 4 u(2) + 4 u(4) + u(6) + 2 u(5) + 4 u(0) + 2 u(3) + 4 u(1)

Check whether y(h) is s solution of the differential equation
> for h from 0 to 5 do (ypart(h+3)+ypart(h+1)+ypart(h)) mod p od;

                                u(1) + 2 u(0)
                                u(2) + 2 u(1)
                                u(3) + 2 u(2)
                                u(4) + 2 u(3)
                                u(5) + 2 u(4)
                                u(6) + 2 u(5)
```

Bibliography

[1] Joseph A. Gallian. *Contemporary Abstract Algebra*. Houghton Mifflin Company, Boston, sixth edition, 2006.

[2] A.A. Jagers. Algebraïsche structuren I and algebraïsche structuren II. Readers, Universiteit Twente, Enschede, the Netherlands, 1989.

[3] Dan Kalman. A matrix proof of Newtonś identities. *Mathematics Magazine*, 73:333–315, 2000. A preprint can be found on the web.

[4] M. Kuijper and J.W. Polderman. R-S list decoding from a system theoretic perspective. *IEEE Transactions on Information Theory*, 50:259–271, 2004.

[5] Rudolf Lidl and Harald Niederreiter. *Finite fields*, volume 20 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, second edition, 1997. With a foreword by P. M. Cohn.

[6] Jan Willem Polderman and Jan C. Willems. *Introduction to Mathematical System Theory: A Behavioral Approach*, volume 26 of *Texts in Applied Mathematics*. Springer, New York NY, USA, 1997.