Minimal Bases of Rational Vector Spaces and their Importance in Algebraic Systems Theory

Joachim Rosenthal*

Department of Mathematics
University of Notre Dame
Notre Dame, Indiana 46556-5683, USA

e-mail: Rosenthal.1@nd.edu

June 8, 2000

Abstract

Let $\mathcal{F}$ denote the field of rational functions over some base field. Every subspace V of $\mathcal{F}^n$ has a polynomial basis. A polynomial basis having minimal possible degrees is called a minimal basis of V. It was shown by G.D. Forney [4] that minimal bases always exist and that these bases are of great importance in multivariable systems theory and convolutional coding theory.

Keywords: Vector spaces over the rationals, multivariable systems, vector bundles over the projective line.

1 Introduction

In 1975 Dave Forney wrote a paper [4] entitled *Minimal Bases of Rational Vector Spaces, with Applications to Multivariable Linear Systems.* This paper had an immense impact in the mathematical systems theory literature. According to the full citation database of the Institute for Scientific Information on DIALOG, [4] has been cited 227 times in the period 1976–1999 and it has been the most cited paper by Forney. In this way the paper is a citation classic (compare with Table 1 in the Appendix).

In this article we will survey the results of [4]. Paper [4] contains several interesting contributions. The main theorem (see Theorem 2.2) on minimal polynomial bases of vector

*Supported in part by NSF grant DMS-96-10389. This research has been carried out while the author was a guest professor at EPFL in Switzerland. The author would like to thank EPFL for its support and hospitality.

spaces over the rationals is a purely mathematical result. Its essence has been first derived by Forney in the context of coding theory [3]. The result connects to some classical work in algebra and algebraic geometry and in Section 2 we will review this result. In Section 3 we will relate Theorem 2.2 to a theorem of Grothendieck [8] and a famous classical paper by Dedekind and Weber [2].

A major contribution of paper [4] was a very clear explanation on how to translate properties of a system from a polynomial matrix formulation into a state space formulation. In this way Forney was able to connect the controllability and the observability indices of a linear system to some minimal indices of a rational vector space. In Section 4 we will review these results.

One contribution of [4] was a concrete realization algorithm. In Section 5 we will explain how realization theory can be generalized to accommodate general behavioral systems [21] which have no predetermined input-output structure. The classical realization theory of a transfer function then becomes a special instance of this general realization theory.

The author would like to thank Thurston Miller from the University of Notre Dame to do the citation search for [4].

2 Minimal polynomial bases of rational vector spaces

Let $\mathbb{F}$ be an arbitrary field and consider the field $\mathcal{F} := \mathbb{F}(x)$ of rational functions in the in-determinant x. Let $\mathbb{F}[x]$ be the polynomial ring over $\mathbb{F}$.

Definition 2.1 One says $v = (v_1, \dots, v_n) \in \mathcal{F}^n$ is a polynomial vector if $v \in \mathbb{F}^n[x]$. If v is a polynomial vector then one defines its degree as $\deg v := \max\{\deg v_i \mid i = 1, \dots, n\}$.

Let $V \subset \mathcal{F}^n$ be a k-dimensional subspace. A basis $B := \{v^1, \dots, v^k\}$ is called a *polynomial basis* if $B \subset \mathbb{F}^n[x]$. One says that B forms a *minimal polynomial basis* if the total degree (order) $\sum_{j=1}^k \deg v^j$ is minimal. It is clear that a polynomial basis exists. The following is the main theorem in [4] and it characterizes a minimal polynomial basis:

Theorem 2.2 ([4]) *Let $V \subset \mathcal{F}^n$ be a k-dimensional subspace and assume the rows of a $k \times n$ matrix G represent a polynomial basis. Assume the jth row degree is ν_j and the total degree (order) is $\nu = \sum_{j=1}^k \nu_j$. Then the following are equivalent.*

1. *The rows of G form a minimal polynomial basis.*
2. *G is nonsingular modulo $p(x)$ for all irreducible polynomials $p(x) \in \mathbb{F}[x]$ and the high order coefficient matrix $[G]_h$ of G has full rank.*
3. *The greatest common divisor of the $k \times k$ full size minors is 1 and their greatest degree is ν.*

4. *If* $y = xG$ *is polynomial then* x *is polynomial and* $\deg y = \max_{1\le j\le k}\{\deg x_j + \nu_j\}$.

5. *For* $d \ge 0$ *let* $V_d \subset V$ *be the subset of all polynomial vectors of degree at most* d. *Then* V_d *is a finite* $\mathbb{F}$ *vector space and the indices* $\nu_1, \dots, \nu_k$ *have the property that* $\dim_{\mathbb{F}} V_d = \sum_{\nu_j<d}(d - \nu_j)$.

In coding theory [3, 10] a linear subspace $\mathcal{C} \subset \mathcal{F}^n$ defines a convolutional code. If the rows of a $k \times n$ matrix G represent a $\mathcal{F}$-basis for the code $\mathcal{C}$ then one says that G is an encoder. G defines the encoding map:

$$\varphi: \ \mathcal{F}^k \longrightarrow \mathcal{F}^n, \ m(x) \longmapsto c(x) = m(x)G(x). \tag{2.1}$$

Minimal polynomial encoder ares of great significance since they describe feed-forward encoders having a minimal number of delay elements. We will explain the significance of minimal polynomial bases in systems theory in Section 4.

It follows from the last conditions of Theorem 2.2 that the indices $\nu_1, \dots, \nu_k$ are invariants of the subspace $V \subset \mathcal{F}^n$. These indices are of crucial importance both in convolutional coding theory [3, 10] and in systems theory and we follow McEliece [16] and call them the *Forney indices* of V. Without loss of generality one can assume that they are ordered $\nu_1 \ge \dots \ge \nu_k$.

In [4, Remark 1] Forney questioned if Theorem 2.2 has not already been derived earlier since the Theorem spells out merely important properties of a subspace $V \subset \mathcal{F}^n$. Today it is clear that Theorem 2.2 was new at the time but that it is closely connected to some interesting results in mathematics. It has been recognized (compare with [5]), that minimal polynomial bases appeared already in 1908 by Plemelj [17] who did give a solution to Riemann's problem on functions with a given monodromic group. In the next section we show a connection to Grothendieck's Theorem [8] and to a classical paper by Dedekind and Weber [2].

3 Grothendieck's Theorem and the work of Dedekind and Weber

In [8] Grothendieck provided a complete classification of vector bundles over the Riemann sphere. For this let $\mathbb{C}$ denote the complex numbers and let

$$\mathbb{P}^1_{\mathbb{C}} := \{\ell \subset \mathbb{C}^2 \mid \dim \ell = 1\} \hat{=} \{(x, 1) \mid x \in \mathbb{C}\} \cup \{(1, 0)\}$$

denote the projective line over $\mathbb{C}$, i.e. the Riemann sphere. Then one has:

Theorem 3.1 ([8]) *If* ξ *is a holomorphic vector bundle over* $\mathbb{P}^1_{\mathbb{C}}$ *then* ξ *decomposes as a sum of line bundles:*

$$\xi = O(\nu_1) \oplus \dots \oplus O(\nu_k),$$

where $\nu_1, \dots, \nu_k$ *are the multiplicities of the line bundles. The nonnegative integers* $\nu_1, \dots, \nu_k$ *depend up to order only on* ξ.

The indices $\nu_1, \dots, \nu_k$ are sometimes referred to as the Grothendieck indices of ξ. The integer $\nu = \sum_{j=1}^{k} \nu_j$ is called the degree of ξ. The relation to the Forney indices is now as follows:

Consider the Grassmann manifold

$$\mathrm{Grass}(k, \mathbb{C}^n) := \{W \subset \mathbb{C}^n \mid \dim W = k\}$$

parameterizing all k-dimensional linear subspaces of $\mathbb{C}^n$. $\mathrm{Grass}(k, \mathbb{C}^n)$ is a smooth, compact manifold of complex dimension $k(n-k)$. Consider a k-dimensional linear subspace $V \subset \mathcal{F}^n$ and assume that G is a $k \times n$ matrix over $\mathcal{F}$ such that $\mathrm{rowspace}_{\mathcal{F}} G = V$. Consider the map:

$$h: \ \mathbb{P}^1_{\mathbb{C}} \longrightarrow \mathrm{Grass}(k, \mathbb{C}^n), \ \ z \mapsto \mathrm{rowspace}_{\mathbb{C}} G(z). \tag{3.1}$$

A priori h is not defined if $\mathrm{rank}\, G(z_0) < k$ or if an entry of G has a pole at a number z_0. The map is also not defined at $z = \infty$. Each singularity is however isolated and it is a well known result of complex analysis that each singularity is removable since $\mathrm{Grass}(k, \mathbb{C}^n)$ is compact. The map h extends therefore to a holomorphic map defined on all of $\mathbb{P}^1_{\mathbb{C}}$. In this way every subspace $V \subset \mathcal{F}^n$ describes a holomorphic map h and vice versa every holomorphic map h from $\mathbb{P}^1_{\mathbb{C}}$ to $\mathrm{Grass}(k, \mathbb{C}^n)$ defines a linear subspace $V \subset \mathcal{F}^n$.

The Grassmann manifold is equipped with a natural vector bundle called the universal bundle U. Let U^* be its dual. The following theorem is due to Martin and Hermann [15]:

Theorem 3.2 *Let ξ be the pull back of the bundle U^* under the holomorphic map h. Then the Grothendieck indices $\nu_1, \dots, \nu_k$ of ξ are up to order equal to the Forney indices of $V \subset \mathcal{F}^n$. Moreover the degree $\nu = \sum_{j=1}^{k} \nu_j$ of ξ is equal to the topological degree of the map h.*

The computation of a minimal polynomial basis works over an arbitrary base field $\mathbb{F}$. It is also known that Grothendieck's theorem and Theorem 3.2 are valid over an arbitrary base field. A simple proof of Grothendieck's theorem over a general field can be found in [9, 13].

In the situation of a general field, a morphism $h: \ \mathbb{P}^1_{\mathbb{F}} \longrightarrow \mathrm{Grass}(k, \mathbb{F}^n)$ is given through a map

$$(s,t) \longmapsto \mathrm{rowspace}_{\mathbb{F}} P(s,t),$$

where

$$P(s,t) = \begin{pmatrix} f_{11}(s,t) & f_{12}(s,t) & \dots & f_{1,m+p}(s,t) \\ f_{21}(s,t) & f_{22}(s,t) & \dots & f_{2,m+p}(s,t) \\ \vdots & \vdots & & \vdots \\ f_{p1}(s,t) & f_{p2}(s,t) & \dots & f_{p,m+p}(s,t) \end{pmatrix} \tag{3.2}$$

is a $k \times n$ matrix whose entries $f_{ij}(s,t) \in \mathbb{F}[s,t]$ are homogeneous polynomials of degree ν_i, $i = 1, \dots, k$.

For any base field $\mathbb{F}$ the Grassmannian $\mathrm{Grass}(k, \mathbb{F}^n)$ is a smooth projective variety of dimension $k(n-k)$. Moreover the set of all morphisms of the form $h: \ \mathbb{P}^1_{\mathbb{F}} \longrightarrow \mathrm{Grass}(k, \mathbb{F}^n)$

having total degree $\nu = \sum_{j=1}^{k} \nu_j$ forms itself a smooth projective variety of dimension $\nu n + k(n-k)$. In the algebraic geometry literature this variety is sometimes referred to as a *Quot scheme* and we refer to [18] for details.

Grothendieck did derive Theorem 3.1 using general results from the theory of holomorphic vector bundles like Serre duality and splitting theorems for subbundles. He was not aware that his result is also a straight forward consequence of some results by Dedekind and Weber [2]. The way on how one can derive Grothendieck's theorem from [2] was shown by Geyer [7]. In the last part of this section we outline this connection.

Dedekind and Weber consider a field extension $\Omega \supset \mathbb{F}$ having transcendental degree 1. Let $x \in \Omega$ be an element which is not algebraic over $\mathbb{F}$ and consider the ring $R := \mathbb{F}[x]$ and its quotient field $\mathcal{F} = F(x)$. $\Omega \supset \mathcal{F}$ is then a finite field extension of degree $k := [\Omega : \mathcal{F}]$. Let R_∞ be the ring of proper rational functions of the form $r(x) = \frac{p(x)}{q(x)}$, $\deg q(x) \geq \deg p(x)$. We define a vector bundle as a pair (M, M_∞), where M is a R-submodule of Ω and M_∞ is a R_∞-submodule of Ω.

In [2, §22] Dedekind and Weber define a norm for each $x \in M$. They show how to iteratively construct a "Normalbasis" $\lambda_1, \dots, \lambda_k$ of M having minimal norm $r_1, \dots, r_k$. Moreover the elements $\lambda_1, \dots, \lambda_k$ have the properties that

$$\frac{\lambda_1}{z^{r_1}}, \dots, \frac{\lambda_k}{z^{r_k}}$$

form a normal basis of M_∞. Geyer [7] explains, how Grothendieck's Theorem 3.1 is an immediate consequence once the existence of a normal basis of M has been shown. One finds similar arguments by Lomadze [13] who also shows how Theorem 2.2 relates to Grothendieck's theorem.

It is interesting to remark that Dedekind and Weber used in their paper already elements from valuation theory and maybe this paper started the development of valuation theory. The importance of valuation theory was stressed by Forney in [4] where he remarked that Theorem 2.2 might generalize to a broader context. For a historic account on the paper by Dedekind and Weber we refer to Geyer [7] and Strobl [20].

4 Applications to systems theory

The theory of minimal polynomial bases is key for understanding the relation between a state space description of a linear system and the corresponding transfer function (respectively matrix polynomial) description. In the sequel we just summarize some of these results. The reader who is not familiar with these results is advised to read Forney's article [4] or to have a look at the standard textbook [11].

Let $G(s)$ be a $p \times m$ proper transfer function. It is well known that the input-output map $\hat{y}(s) = G(s)\hat{u}(s)$ has a minimal state space realization of the form:

$$\dot{x} = Ax + Bu, \quad y = Cx + Du. \tag{4.1}$$

The size of the matrix A is called the McMillan degree of the transfer function $G(s) = C(sI - A)^{-1}B + D$ (respectively system (4.1)) and the left Kronecker indices of the pencil $\begin{bmatrix} sI - A \\ C \end{bmatrix}$ are called the observability indices of the transfer function $G(s)$ (respectively system (4.1)). See [11, page 413] for details. Similarly one defines the controllability indices of $G(s)$ as the right Kronecker indices of the pencil $[sI - A \mid B]$.

Consider the $\mathcal{F}$-vector space

$$V := \text{rowspace}_{\mathcal{F}} [I_p \mid G(s)] \subset \mathcal{F}^{m+p}.$$

Assume the rows of $[D(s) \mid N(s)]$ form a minimal polynomial basis of V having ordered Forney indices $\nu_1 \geq \cdots \geq \nu_p$ and total degree $\nu = \sum_{j=1}^{p} \nu_j$. Then one has:

Theorem 4.1 ([4]) *1. $D^{-1}(s)N(s) = G(s)$ forms a left coprime factorization.*

2. $\det D(s)$ is equal to the characteristic polynomial of the transfer function $G(s)$, in particular $\nu = \deg \det D(s)$ is equal to the McMillan degree of $G(s)$.

3. The indices ν_j are equal to the observability indices of $G(s)$.

The last Theorem did relate the observability indices of $G(s)$ to the Forney indices of some subspace $V \subset \mathcal{F}^{m+p}$. Combining this result with Theorem 3.2 we obtain a corollary due to Martin and Hermann [15]:

Corollary 4.2 *Let ξ be the pull back of the bundle U^* under the Hermann-Martin map*

$$h: \ \mathbb{P}^1_{\mathbb{C}} \longrightarrow \text{Grass}(p, \mathbb{C}^{m+p}), \ z \mapsto \text{rowspace}_{\mathbb{C}} G(z). \tag{4.2}$$

Then the Grothendieck indices of ξ are up to order equal to the observability indices of $G(s)$.

A minimal basis for the m-dimensional vector space

$$\tilde{V} := \text{rowspace}_{\mathcal{F}} \left[I_m \mid G(s)^t \right] \subset \mathcal{F}^{m+p}$$

results into the controllability indices of $G(s)$. In analogy to Theorem 4.1 one has:

Theorem 4.3 *Assume $Q(s)$ is a $m \times m$ polynomial matrix and the rows of $[Q(s) \mid R(s)]$ form a minimal polynomial basis of $\tilde{V}$ having ordered Forney indices $\kappa_1 \geq \cdots \geq \kappa_m$ and total degree $\kappa = \sum_{i=1}^{m} \kappa_i$. Then*

1. $R^t(s)(Q^t)^{-1}(s) = G(s)$ forms a right coprime factorization.

2. $\det Q(s)$ is equal to the characteristic polynomial of the transfer function $G(s)$, in particular $\kappa = \deg \det Q(s)$ is equal to the McMillan degree of $G(s)$.

3. The indices κ_i are equal to the controllability indices of $G(s)$.

5 Behaviors and generalized first order representations

The last section did show how one can transform results formulated in a state space formulation into results formulated in a polynomial formulation. [4] provided also an algorithm on how to compute a minimal state space realization from a polynomial description $[D(s) \mid N(s)]$ of the system. At the time of writing of [4] there were several algorithms known for computing a state space realization of the form (4.1) from a transfer function respectively polynomial description and we refer to [1, 6, 22].

In this section we will take a slightly more modern (and general) point of view and we will show how it is possible to rewrite linear time invariant behaviors given through a polynomial formulation into a generalized first order form. We follow in the sequel mainly [19].

Let $P(s)$ be a $p \times (m+p)$ polynomial matrix with entries in the polynomial ring $\mathbb{R}[s]$. The smooth behavior associated with $P(s)$ is defined by

$$\mathcal{B}(P) \;=\; \{w \in C^\infty(\mathbb{R};\mathbb{R}^{m+p}) \mid P(\tfrac{d}{dt})w = 0\}. \tag{5.1}$$

The following lemma is well known:

Lemma 5.1 *Assume $P(s)$ and $\tilde{P}(s)$ are both full rank polynomial matrices of the same size. Then $\mathcal{B}(P) = \mathcal{B}(\tilde{P})$ if and only if there is a unimodular matrix $U(s)$ such that $\tilde{P}(s) = U(s)P(s)$.*

Based on this lemma we can identify a smooth behavior with the row-module of a polynomial matrix. There are classical canonical forms describing the row-module of a polynomial matrix such as Hermite's normal form and we refer to [11, 14]. In the sequel we will simply assume that the polynomial matrix $P(s)$ has been row reduced using unimodular operations only and that the row degrees of $P(s)$ are ordered in non-increasing manner: $\nu_1 \geq \cdots \geq \nu_p$.

The indices $\nu_1, \ldots, \nu_p$ are in general different from the Forney indices of the rational row-space of $P(s)$ and they are often referred to as the Kronecker indices of the row-module of $P(s)$. Clearly equivalent polynomial matrices $P(s)$ and $\tilde{P}(s)$ have the same rational row-space. The converse is however in general not true. One has however the following:

Lemma 5.2 *Assume the rows of $P(s)$ and $\tilde{P}(s)$ form both a minimal polynomial basis of the same rational subspace $V \subset \mathcal{F}^n$. Then there is a unimodular matrix $U(s)$ such that $\tilde{P}(s) = U(s)P(s)$.*

This lemma allows one in particular to derive canonical forms (such as the Hermite normal form) for minimal polynomial bases, a subject which is also treated in [4].

Consider now a triple of real matrices (F, G, H), where F and G have size $n \times (n+m)$ and H has size $(m+p) \times (n+m)$. This triple defines a smooth behavior through:

$$\mathcal{B}(F,G,H) = \{w \in C^\infty(\mathbb{R};\mathbb{R}^{m+p}) \mid \exists z \in C^\infty(\mathbb{R};\mathbb{R}^{n+m}) : G\dot{z} = Fz,\ w = Hz\}.$$

One says that (F, G, H) forms a generalized first order representation (or simply a realization) of $\mathcal{B}(P)$ if $\mathcal{B}(F, G, H) = \mathcal{B}(P)$. If (F, G, H) is a realization of $P(s)$ and S and T are nonsingular matrices of appropriate size then $(SFT^{-1}, SGT^{-1}, HT^{-1})$ forms a realization of $\mathcal{B}(P)$ as well.

The following theorem can be found in [12, Theorem 4.3] and it provides the conditions of minimality for a realization (F, G, H) of a behavior $\mathcal{B}(F, G, H) = \mathcal{B}(P)$.

Theorem 5.3 *(F, G, H) forms a minimal realization of the behavior $\mathcal{B}(P)$ if and only if:*

(i) *G has full row rank.*

(ii) $\begin{bmatrix} G \\ H \end{bmatrix}$ *has full column rank.*

(iii) $\begin{bmatrix} sG - F \\ H \end{bmatrix}$ *has full column rank for all $s \in \mathbb{C}$.*

The question now arises how to compute efficiently a minimal realization. The following lemma gives a way to compute a realization, not necessarily a minimal one.

Lemma 5.4 ([19]) *Let a polynomial matrix $P(s) \in \mathbb{R}^{p\times(m+p)}[s]$ and a triple of constant matrices (F, G, H) (F and G in $\mathbb{R}^{n\times(n+m)}$, H in $\mathbb{R}^{(m+p)\times(n+m)}$) be given. If there exists a polynomial matrix $X(s) \in \mathbb{R}^{p\times n}[s]$ such that the rows $[X(s) \mid P(s)]$ form a minimal polynomial basis and the equality*

$$\ker_{\mathbb{R}(s)} [X(s) \mid P(s)] \;=\; \operatorname{im}_{\mathbb{R}(s)} \begin{bmatrix} sG - F \\ H \end{bmatrix} \tag{5.2}$$

holds, then $\mathcal{B}(P) = \mathcal{B}(F, G, H)$, so (F, G, H) is a realization of $P(s)$.

In order to compute a minimal realization it is best to choose a particular polynomial matrix $X(s)$ such that (F, G, H) satisfying property (5.2) is most easily computed. For this assume that $P(s)$ is row reduced with Kronecker indices $\nu_1 \geq \cdots \geq \nu_p$. Define:

$$X_\nu(s) = \begin{bmatrix} 1 & s & \cdots & s^{\nu_1-1} & 0 & \cdots & \cdots & & \cdots & \cdots & 0 \\ 0 & \cdots & \cdots & 0 & 1 & \cdots & s^{\nu_2-1} & 0 & \cdots & \cdots & 0 \\ \vdots & & & & & \ddots & \ddots & & & & \vdots \\ 0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 0 & 1 & \cdots & s^{\nu_p-1} \end{bmatrix}. \tag{5.3}$$

With this particular choice one has:

Theorem 5.5 ([19]) *Let $P(s)$, $X_\nu(s)$ be as above. Then:*

1. *A minimal polynomial basis of $\ker_{\mathbb{R}(s)} [X_\nu(s) \mid P(s)]$ is of the form $\operatorname{im}_{\mathbb{R}(s)} \left[\begin{smallmatrix} sG-F \\ H \end{smallmatrix}\right]$ and $\mathcal{B}(F, G, H)$ forms a minimal realization of $\mathcal{B}(P)$.*

2. *If the Kronecker indices of $P(s)$ have the property that $\nu_1 \geq \cdots \geq \nu_p \geq 1$ then $\ker_{\mathbb{R}(s)} [X_\nu(s) \mid P(s)]$ can be computed simply 'by inspection' this means by simply rearranging the entries of the polynomial matrix $P(s)$.*

We can now specialize Theorem 5.5 to the situation treated by Forney [4]. For this assume that $P(s)$ is partitioned into $P(s) = [D(s) \mid N(s)]$. Correspondingly partition the vector w into y and u. We are now seeking a first order realization of the form

$$\begin{bmatrix} sG - F \\ H \end{bmatrix} = \begin{bmatrix} sI - A & B \\ C & D \\ 0 & I \end{bmatrix}$$

which then describes a classical behavior of the form $\dot{x} = Ax + Bu$, $y = Cx + Du$.

Assume the rows of $[D(s) \mid N(s)]$ form a minimal basis of $\mathrm{rowspace}_{\mathbb{R}(s)} [I_p \mid G(s)]$. For simplicity assume that $D^{-1}(s)N(s) = G(s)$ is strictly proper. Assume that the Forney indices satisfy $\nu_1 \geq \cdots \geq \nu_p \geq 1$ and assume that the high order coefficient matrix of $[D(s) \mid N(s)]$ is of the form $[I_p \mid 0]$. For $i, j = 1, \ldots, p$ let

$$d_{i,j}(s) = \sum_{k=0}^{\nu_i} d_{i,j}^k \, s^k$$

denote the polynomial entries of $D(s)$. Similarly let

$$n_i(s) = \sum_{k=0}^{\nu_i} n_i^k \, s^k$$

denote the i-th row of $N(s)$. Define for $i = 1, \ldots, p$ matrices of sizes $\nu_i \times \nu_i$, $\nu_i \times m$ and $1 \times \nu_i$ respectively:

$$\begin{aligned} A_{i,i} &:= \begin{bmatrix} 0 & \cdots & \cdots & \cdots & -d_{i,i}^0 \\ 1 & 0 & & & -d_{i,i}^1 \\ 0 & 1 & \ddots & & \vdots \\ \vdots & & \ddots & 0 & \vdots \\ 0 & \cdots & 0 & 1 & -d_{i,i}^{\nu_i - 1} \end{bmatrix}, B_i := \begin{bmatrix} n_i^0 \\ n_i^1 \\ \vdots \\ n_i^{\nu_i - 1} \end{bmatrix}, \\ C_i &:= [0, \ldots, -1]. \end{aligned}$$

Finally for $i, j = 1, \ldots, p$, $i \neq j$ define matrices of size $\nu_i \times \nu_j$:

$$A_{i,j} := \begin{bmatrix} 0 & \cdots & 0 & -d_{i,j}^0 \\ \vdots & & \vdots & -d_{i,j}^1 \\ \vdots & & \vdots & \vdots \\ 0 & \cdots & 0 & -d_{i,j}^{\nu_i - 1} \end{bmatrix}.$$

Note that the matrices $A_{i,i}$, $A_{i,j}$, B_i and C_i were simply computed 'by inspection' from the data $[D(s) \mid N(s)]$.

Theorem 5.6 ([4, 19, 22]) *In the situation discussed above*

$$\begin{aligned} \dot{x}(t) &= \begin{bmatrix} A_{1,1} & \cdots & A_{1,p} \\ \vdots & \ddots & \vdots \\ A_{p,1} & \cdots & A_{p,p} \end{bmatrix} x(t) + \begin{bmatrix} B_1 \\ \vdots \\ B_p \end{bmatrix} u(t), \\ y(t) &= \begin{bmatrix} C_1 & & 0 \\ & \ddots & \\ 0 & & C_p \end{bmatrix} x(t) \end{aligned} \tag{5.4}$$

represents a (classical) minimal state space realization of the system

$$D(\tfrac{d}{dt})y(t) + N(\tfrac{d}{dt})u(t) = 0. \tag{5.5}$$

In particular one has $C(sI - A)^{-1}B = G(s)$.

6 Conclusion

In this paper we provided a survey about one of the most influential papers in systems theory. We showed how the result on minimal polynomial bases relates to some very classical results in mathematics. We also did show how the results on the relation between state space description of a system and polynomial description of a system can be treated in the broader context of behavioral theory.

Appendix

Table 1: Citations of [4] in the period 1976–1999:

Year	Cite's	Year	Cite's	Year	Cite's	Year	Cite's
1976	4	1982	3	1988	7	1994	14
1977	6	1983	11	1989	10	1995	7
1978	15	1984	12	1990	8	1996	8
1979	18	1985	7	1991	10	1997	10
1980	14	1986	10	1992	7	1998	7
1981	19	1987	6	1993	5	1999	9

References

[1] R. W. Brockett. *Finite Dimensional Linear Systems*. J. Wiley & Sons, 1970.

[2] R. Dedekind and H. Weber. Theorie der algebraischen Functionen einer Veränderlichen. *Journal für die reine und angewandte Mathematik*, 92:181–291, 1882.

[3] G. D. Forney. Convolutional codes I: Algebraic structure. *IEEE Trans. Inform. Theory*, IT-16(5):720–738, 1970.

[4] G. D. Forney. Minimal bases of rational vector spaces, with applications to multivariable linear systems. *SIAM J. Control*, 13(3):493–520, 1975.

[5] G. D. Forney. Algebraic structure of convolutional codes, and algebraic system theory. In A.C. Antoulas, editor, *Mathematical System Theory: The Influence of R.E. Kalman*, pages 527–557. Springer, Berlin, 1991.

[6] P. A. Fuhrmann. Algebraic system theory: an analyst's point of view. *J. Franklin Inst.*, 301:521–540, 1976.

[7] W.-D. Geyer. Die Theorie der algebraischen Funktionen einer Veränderlichen nach Dedekind und Weber. In W. Scharlau, editor, *Richard Dedekind, 1831–1981*, pages 109–133. Friedr. Vieweg & Sohn, Braunschweig, 1981. Eine Würdigung zu seinem 150. Geburtstag. [An appreciation on the occasion of his 150th birthday].

[8] A. Grothendieck. Sur la classification des fibres holomorphes sur la sphere de Riemann. *Amer J. Math.*, 79:121–138, 1957.

[9] M. Hazewinkel and C. Martin. A short elementary proof of Grothendieck's theorem on algebraic vectorbundles over the projective line. *J. Pure Appl. Algebra*, 25:207–211, 1982.

[10] R. Johannesson and K. Sh. Zigangirov. *Fundamentals of Convolutional Coding*. IEEE Press, New York, 1999.

[11] T. Kailath. *Linear Systems*. Prentice-Hall, Englewood Cliffs, N.J., 1980.

[12] M. Kuijper. *First-Order Representations of Linear Systems*. Birkhäuser, Boston, 1994.

[13] V. Lomadze. Applications of vector bundles to factorization of rational matrices. *Linear Algebra Appl.*, 288(1-3):249–258, 1999.

[14] C.C. MacDuffee. *The Theory of Matrices*. Chelsea, New York, 1956. Reprint of original, 1933.

[15] C. F. Martin and R. Hermann. Applications of algebraic geometry to system theory: The McMillan degree and Kronecker indices as topological and holomorphic invariants. *SIAM J. Control Optim.*, 16:743–755, 1978.

[16] R. J. McEliece. The algebraic theory of convolutional codes. In V. Pless and W.C. Huffman, editors, *Handbook of Coding Theory*, volume 1, pages 1065–1138. Elsevier Science Publishers, Amsterdam, The Netherlands, 1998.

[17] Plemelj. Riemannsche Funktionenscharen mit gegebener Monodromiegruppe. *Monath. Math.*, 19:211–246, 1908.

[18] M. S. Ravi and J. Rosenthal. A smooth compactification of the space of transfer functions with fixed McMillan degree. *Acta Appl. Math*, 34:329–352, 1994.

[19] J. Rosenthal and J. M. Schumacher. Realization by inspection. *IEEE Trans. Automat. Contr.*, AC-42(9):1257–1263, 1997.

[20] W. Strobl. Über die Beziehungen zwischen der Dedekindschen Zahlentheorie und der Theorie der algebraischen Funktionen von Dedekind und Weber. *Abh. Braunschweig. Wiss. Ges.*, 33:225–246, 1982.

[21] J. C. Willems. Paradigms and puzzles in the theory of dynamical systems. *IEEE Trans. Automat. Control*, AC-36(3):259–294, 1991.

[22] W. A. Wolovich. *Linear Multivariable Systems*, volume 11 of *Appl. Math. Sc.* Springer Verlag, New York, 1974.