A Computational Theory of Laurent Polynomial Rings and Multidimensional FIR Systems

by

HYUNG-JU PARK

B.S. in Physics (Seoul National University) 1986
Candidate in Philosophy (University of California at Berkeley) 1989

A dissertation submitted in partial satisfaction of the
requirements for the degree of
Doctor of Philosophy

in

Mathematics

in the

GRADUATE DIVISION
of the
UNIVERSITY of CALIFORNIA at BERKELEY

Committee in charge:

Professor Tsit-Yuen Lam, Co-Chair
Professor Martin Vetterli, Co-chair
Professor Beresford Parlett
Professor John Canny

1995

A Computational Theory of Laurent Polynomial Rings and Multidimensional FIR Systems

Abstract

A Computational Theory of Laurent Polynomial Rings and Multidimensional FIR Systems

by

HYUNG-JU PARK
Doctor of Philosophy in Mathematics

University of California at Berkeley

A Laurent polynomial ring is a natural ground ring for the study of FIR (Finite Impulse Response) systems in signal processing since an FIR filter bank can be seen as a matrix over this ring, and the notion of perfect reconstruction is represented by the unimodularity of the corresponding multivariate Laurent polynomial matrices. Contrary to the conventional **affine** approach to the theory of multidimensional FIR filter banks as a linear algebra over polynomial rings, the **toric** approach based on Laurent polynomial rings offers a more adequate framework. In connection with these applications, we look at the computational aspects of the theory of modules over Laurent polynomial rings, and develop a few of their applications to signal processing:

- A new, computationally effective algorithm for the Quillen-Suslin Theorem is found, and implemented using the computer algebra package SINGULAR.
- An algorithmic proof of Suslin's Stability Theorem is found, which gives an analogue of Gaussian Elimination over a polynomial ring.
- An algorithmic process of converting results over polynomial rings to their counterparts over Laurent polynomial rings is developed. With the help of this process, we extend the above two algorithms, the Quillen-Suslin Theorem and Suslin's Stability Theorem, to the case of Laurent polynomial rings.
- A notion of inner product spaces over Laurent polynomial rings is introduced, and a theoretical framework for this notion is developed.

- A few outstanding problems in multidimensional perfect reconstructing filter banks are shown to be solvable with the aid of the above algorithms. Explicit examples are included that are worked out by SINGULAR.

To God,

for his everlasting grace and glory.

To my parents, my bothers and my sister,

for the support and trust they never stopped giving me.

To my wife, Sueyoung,

for her love and caring.

Contents

Acknowledgements

As I look back over my past years at Berkeley, it occurs to me how fortunate I was to have the two wonderful people, Professor Tsit-Yuen Lam and Professor Martin Vetterli, as my research advisors. If there is anything I have achieved here, it was only made possible by their patience and encouragement. Their support and loving care will be remembered for long time to come.

I also want to thank Dr. Ton Kalker and Professor Bernd Sturmfels for being friends, mentors and role models for me and showing me many exciting mathematical problems and having much discussion with me in the course of this work.

Dr. Cynthia Woodburn who once surprised me by proving independently one of the major results of this thesis became a valuable friend, proofread this thesis very carefully, and shared the joy of doing mathematics with me.

Professor John Canny and Professor Beresford Parlett also read an earlier version of this thesis, and provided me with many valuable comments. Especially, the syzygy-based algorithm for the Quillen-Suslin Theorem in Chapter 3 was much improved by a suggestion from Professor Canny.

And it is a pleasure to thank my friends at Berkeley Wavelet Group with whom I spent an important and exciting part of my life.

Finally, if you have comments on this dissertation or want to contact me for any reason, you are welcome to do so by sending me an e-mail at apark@eecs.berkeley.edu.

Part I

Modules over Laurent Polynomial Rings

Chapter 1

Introduction to Part I: History and Problems

The theory of ideals and (finitely generated and projective) modules over polynomial rings and Laurent polynomial rings[1] has been studied in various contexts. Geometrically, such ideals and modules correspond to affine and toric varieties, and vector bundles over them, respectively. And algebro-geometric results concerning algebraic vector bundles over an algebraic torus directly affect the FIR filter bank theory since finitely generated projective modules over a Laurent polynomial ring are represented by such vector bundles.

Computational aspects of this theory, however, have a relatively short history, and Gröbner bases theory provides the foundation for them, with the Buchberger algorithm acting as the universal engine that drives many computations. In Chapter 2, we will review this Gröbner bases theory in a brief and self-contained manner.

In 1955, Jean Pierre Serre made a conjecture regarding the triviality of algebraic vector bundles over an affine space. This problem became a daunting task for many mathematicians, and was fully solved only in 1976, 20 years after the question was raised. Serre's conjecture, which is now known as the Quillen-Suslin theorem after the two mathematicians who independently solved this long standing problem, states that any finitely generated projective module over a polynomial rings is free. And in 1978, R.G. Swan [Swa78] extended this result to the case of Laurent polynomial rings.

[1] Unless otherwise specified, we will generally assume throughout this thesis that the coefficient rings of these polynomial rings and Laurent polynomial rings are fields even though many results can be readily extended to more general kinds of coefficient rings.

While the original proofs by Quillen [Qui76] and Suslin [Sus76] are nonconstructive, new constructive proofs were found lately [LS92], [Fit93], [FG90], which give us algorithmic ways of finding a free basis of any given (f.g. and projective) module over a polynomial ring. In Chapter 3, we give a new, and readily implementable algorithm for the same purpose, that is based on a syzygy computation. This algorithm is very easily implementable since syzygy computation is already a standard part of many computer algebra packages, e.g. *Macaulay*[2] and SINGULAR[3]. We present a few examples which are worked out in detail by the computer algebra package SINGULAR.

Immediately after proving the Serre Conjecture, A.A. Suslin went on to prove the following K_1-analogue of Serre's conjecture [Sus77, Thm. 6.3].

> **Suslin's Stability Theorem.** Let R be a commutative Noetherian ring and $n \geq \max(3, \dim(R)+2)$. Then, any $n \times n$ matrix $\mathbf{A} = (f_{ij})$ of determinant 1, with f_{ij} elements of the polynomial ring $R[x_1, \ldots, x_m]$, can be written as a product of elementary matrices over $R[x_1, \ldots, x_m]$.

In Chapter 4, we develop an algorithmic proof of the above assertion over a field $R = k$, which gives an analogue of the Gaussian elimination algorithm over a multivariate polynomial ring $k[x_1, \ldots, x_m]$. Our method is inspired by the Logar-Sturmfels algorithm, [LS92], for the Quillen-Suslin Theorem.

For a given $\mathbf{A} \in \mathrm{SL}_n(k[x_1, \ldots, x_m])$ with $n \geq 3$, the algorithm of this chapter produces elementary matrices $\mathbf{E}_1, \ldots, \mathbf{E}_t \in \mathrm{E}_n(k[x_1, \ldots, x_m])$ such that $\mathbf{A} = \mathbf{E}_1 \cdots \mathbf{E}_t$, and implementation of this algorithm involves use of Gröbner bases.

Suslin's stability theorem established in Chapter 4 fails for $n = 2$, and a counter-example was constructed by P.M. Cohn in [Coh66]. In Chapter 5, we will develop an algorithm determining precisely when a given matrix in $\mathrm{SL}_2(k[x_1, \ldots, x_m])$ allows such a factorization into elementary matrices, and if it does, expressing it as a product of elementary matrices.

In Chapter 6, we extend our algorithm for the Quillen-Suslin Theorem to the case of Laurent polynomial rings. For a commutative ring R, we call $\mathbf{v} = (v_1, \ldots, v_n) \in R^n$ **unimodular** if its components generate R, i.e. if there exist $g_1, \ldots, g_n \in R$ such that

[2] *Macaulay* is a computer algebra system for algebraic geometry and commutative algebra, developed by M. Stillman and D. Bayer. It is available freely by anonymous ftp from ftp.math.harvard.edu. For more information, see [BS].

[3] SINGULAR is a computer algebra system for singularity theory and algebraic geometry, developed in the University of Kaiserslautern, Germany. It is still being alpha-tested, and is freely available by anonymous ftp from helios.mathematik.uni-kl.de. For more information, see [GPS95].

$v_1 g_1 + \cdots + v_n g_n = 1$. And in this chapter, we develop a systematic process of converting Laurent polynomial vectors to polynomial vectors while preserving unimodularity. The same process will be used in Chapter 11 to extend our algorithm for the Suslin's Stability Theorem to the case of Laurent polynomial rings. A similar idea of changing variables was used by A. Suslin in [Sus77].

In Chapter 7, we develop the notion of inner product spaces over Laurent polynomial rings, and study the unitary group with respect to the canonical group ring involution over Laurent polynomial rings.

Notations

- A field is typically denoted by k while $\mathbb{R}, \mathbb{C}$ denote the field of real numbers and the field of complex numbers.
- A ring always means a commutative ring with identity unless otherwise specified, and is denoted by roman characters: e.g. A, R, etc.
- Modules over a ring are denoted by $\mathcal{M}, \mathcal{N}$, etc.
- Elements of a module are denoted by bold-face characters: e.g. $\mathbf{f}, \mathbf{v}$, etc.
- Matrices over a ring are denoted by bold-face characters: e.g. $\mathbf{A}, \mathbf{B}, \mathbf{E}$, etc.

Chapter 2

Gröbner Bases (Standard Bases)

> "$\cdots$ In view of the ubiquity of scientific problems modeled by polynomial equations, this subject is of interest not only to mathematicians, but also to an increasing number of scientists and engineers. In this context, Gröbner bases theory provides the foundation for many algorithms in algebraic geometry and commutative algebra, with the Buchberger algorithm acting as the engine that drives many computations. $\cdots$" (B. Sturmfels, [Stu94]).

2.1 Brief History

The Hilbert Basis Theorem states that any ideal of a polynomial ring is finitely generated. However, Hilbert's original proof is nonconstructive and does not offer an effective way of finding a finite set of generators for a given ideal of a polynomial ring. Determining if a given polynomial belongs to a particular ideal is not an easy problem, either. Even when we have an explicit (and finite) set of generators for the ideal and a polynomial known to be a member of the ideal, writing this polynomial as a linear combination with polynomial coefficients of the given generators could already be a daunting task.

In his celebrated 1964 paper [Hir64], H. Hironaka[1] answered this *ideal membership question* by introducing special kinds of ideal generators called *standard bases*. Slightly later, B. Buchberger independently and effectively addressed the same problem in his Ph.D thesis [Buc65], but used the name *Gröbner bases* in honor of his thesis advisor W. Gröbner. It was mainly Buchberger's continued works that inspired far more research on the theoretical and computational aspects of Gröbner bases and their applications to various mathematical

[1]According to D. Eisenbud [Eis95], earlier mathematicians like P. Gordan, F. Macaulay, and W. Gröbner already had found the notion of Gröbner Bases, and used them for their respective problems.

and scientific problems.

Nowadays, Gröbner bases have become a very important tool in computational algebra and computational algebraic geometry, and are implemented in many commercial and noncommercial computer algebra packages.

The explicit Gröbner basis computations for the examples in the remaining chapters of this thesis were carried out by using two noncommercial computer algebra packages: *Macaulay* (see [BS]) and SINGULAR (see [GPS95]).

[CLO92], [Mis93], [BW93], [Eis95] are excellent references for more information on Gröbner bases and their applications.

B. Sturmfels' unpublished lecture notes [Stu94] from New Mexico State University Holiday Symposium 94 offers a state-of-the-art exposition on relatively new polytope theoretic aspects of Gröbner bases and their application to integer programming.

2.2 Monomial Order

From now on, we will use the following shorthand notations.

- $\boldsymbol{x} := (x_1, \ldots, x_m)$,
- For $\mathbf{d} = (d_1, \ldots, d_m) \in \mathbb{Z}^m_{\geq 0}$, $\boldsymbol{x}^{\mathbf{d}} := x_1^{d_1} \cdots x_m^{d_m}$.

Definition 2.2.1 *Let $\mathcal{M}$ be a finitely generated free module over $k[\boldsymbol{x}] = k[x_1, \ldots, x_m]$ with basis $\mathbf{e}_i$, $1 \leq i \leq n$.*

1. *A* **monomial** *in $\mathcal{M}$ is an element of the form*

$$\mathbf{m} = \boldsymbol{x}^{\mathbf{d}}\mathbf{e}_i, \quad 0 \leq d_i \in \mathbb{Z},$$

   and $\mathrm{Mono}(\mathcal{M})$ *is the set of all the monomials in $\mathcal{M}$.*

2. *A* **term**[2] *in $\mathcal{M}$ is a monomial multiplied by a scalar.*

3. *A* **monomial order** *is a linear order $\prec$ on* $\mathrm{Mono}(\mathcal{M})$ *such that, if $\mathbf{t}_1, \mathbf{t}_2 \in \mathrm{Mono}(\mathcal{M})$ and $1 \neq \mathbf{s} \in \mathrm{Mono}(k[\boldsymbol{x}])$, then $\mathbf{t}_1 \prec \mathbf{t}_2$ implies $\mathbf{t}_1 \prec \mathbf{t}_1 \cdot \mathbf{s} \prec \mathbf{t}_2 \cdot \mathbf{s}$.*

[2] The definitions of **term** and **monomial** vary in the literature, e.g. our term (resp. monomial) is monomial (resp. term) in [Mis93].

4. *Let* $\mathbf{c} = (c_1, \ldots, c_m), \mathbf{d} = (d_1, \ldots, d_m) \in \mathbb{Z}^m_{\geq 0}$*. Then for two monomials* $\mathbf{l} = \boldsymbol{x}^{\mathbf{c}}\mathbf{e}_i$ *and* $\mathbf{m} = \boldsymbol{x}^{\mathbf{d}}\mathbf{e}_i$*, we say* $\mathbf{l}$ **divides** $\mathbf{m}$ *if* $i = j$ *and* $0 \leq c_s \leq d_s\ \forall s$*. In this case, we define*

$$\mathbf{m}/\mathbf{l} := \boldsymbol{x}^{\mathbf{d}-\mathbf{c}}\mathbf{e}_i.$$

Now, fix a monomial order $\prec$ on $\mathrm{Mono}(\mathcal{M})$. Any nonzero term $\mathbf{t} \in \mathcal{M}$ can be uniquely written in the form $\mathbf{t} = a\mathbf{m}$ for some nonzero $a \in k$ and $\mathbf{m} \in \mathrm{Mono}(\mathcal{M})$, and for two nonzero terms $\mathbf{t}_1 = a_1\mathbf{m}_1$ and $\mathbf{t}_2 = a_2\mathbf{m}_2$, we loosely say $0 \prec \mathbf{t}_1 \prec \mathbf{t}_2$ if $\mathbf{m}_1 \prec \mathbf{m}_2$. This is obviously an abuse of notation because it implies, for example, $2x^2y \preceq 3x^2y$ and $3x^2y \preceq 2x^2y$ at the same time. Note also that any $\mathbf{f} \in \mathcal{M}$ can be uniquely written as

$$\mathbf{f} = \mathbf{t}_1 + \mathbf{t}_2 + \cdots + \mathbf{t}_l$$

where $\mathbf{t}_1, \ldots, \mathbf{t}_l$ are nonzero terms in $\mathcal{M}$ such that $\mathbf{t}_1 \prec \mathbf{t}_2 \prec \cdots \prec \mathbf{t}_l$. The term $\mathbf{t}_l = a_l\mathbf{m}_l$ is called the *leading term* or *initial term* of $\mathbf{f}$ and is denoted as $\mathrm{lt}(\mathbf{f})$ or $\mathrm{in}(\mathbf{f})$. We call a_l and $\mathbf{m}_l$ the *leading coefficient* and the *leading monomial* of $\mathbf{f}$, respectively, and denote them by $\mathrm{lc}(\mathbf{f})$ and $\mathrm{lm}(\mathbf{f})$. For $\mathbf{f}, \mathbf{g} \in \mathcal{M}$, we say $\mathbf{f} \prec \mathbf{g}$ if $\mathrm{lm}(\mathbf{f}) \prec \mathrm{lm}(\mathbf{g})$. It should be noted that, if we change the monomial order on $\mathrm{Mono}(\mathcal{M})$, then we may have a different $\mathrm{lt}(\mathbf{f})$ for the same $\mathbf{f} \in \mathcal{M}$.

Throughout this thesis, we will use the word *leading* interchangeably with the word *initial*. Also, by a $k[\boldsymbol{x}]$-module, we will always mean a finitely generated $k[\boldsymbol{x}]$-module, and thus, is actually a submodule of a finitely generated free module over $k[\boldsymbol{x}]$. Since monomials in a finitely generated free $k[\boldsymbol{x}]$-module were defined in the above, we can now talk of monomials in an arbitrary finitely generated $k[\boldsymbol{x}]$-module by regarding them as elements in a fixed ambient free module. In the following subsections, we will describe some of the most commonly used monomial orders in practice: lexicographic, degree lexicographic, and reverse degree lexicographic order.

2.2.1 Univariate Case

There is a natural (and in fact unique) monomial order on $\mathrm{Mono}(k[x])$, that is,

$$1 \prec x \prec x^2 \prec x^3 \prec \cdots.$$

If $\mathcal{N}$ is a submodule of a free module $(k[x])^n$ with $\mathbf{e}_1, \ldots, \mathbf{e}_n$ being the free basis, then for two monomials $x^\alpha\mathbf{e}_i, x^\beta\mathbf{e}_j \in \mathcal{N}$,

$$x^\alpha\mathbf{e}_i \prec x^\beta\mathbf{e}_j \Longleftrightarrow i > j \text{ or } \alpha < \beta.$$

2.2.2 Lexicographic Order

When the ambient free module is $k[\boldsymbol{x}]$, for $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_m)$ and $\boldsymbol{\beta} = (\beta_1, \ldots, \beta_m)$,

$$\boldsymbol{x}^{\boldsymbol{\alpha}} \prec_{\text{lex}} \boldsymbol{x}^{\boldsymbol{\beta}} \iff \exists\, 1 \leq i \leq m : \alpha_1 = \beta_1, \ldots, \alpha_{i-1} = \beta_{i-1}, \alpha_i < \beta_i.$$

When the ambient free module is $(k[\boldsymbol{x}])^n$ with $\mathbf{e}_1, \ldots, \mathbf{e}_n$ being the free basis, for $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$ same as in the above,

$$\boldsymbol{x}^{\boldsymbol{\alpha}}\mathbf{e}_i \prec_{\text{lex}} \boldsymbol{x}^{\boldsymbol{\beta}}\mathbf{e}_j \iff i > j \text{ or } \boldsymbol{x}^{\boldsymbol{\alpha}} \prec_{\text{lex}} \boldsymbol{x}^{\boldsymbol{\beta}}.$$

Example 2.2.2 Let $\mathcal{M} = (k[x, y, z])^2$ with $k[x, y, z]$-basis $\mathbf{e}_1, \mathbf{e}_2$. Then, with respect to the lexicographic order, $x^2y^3z\mathbf{e}_1 \succ_{\text{lex}} x^2yz^2\mathbf{e}_1 \succ_{\text{lex}} y^3z^4\mathbf{e}_1 \succ_{\text{lex}} \mathbf{e}_1 \succ_{\text{lex}} x^5\mathbf{e}_2 \succ_{\text{lex}} xyz^2\mathbf{e}_2 \succ_{\text{lex}} z^5\mathbf{e}_2 \succ_{\text{lex}} \mathbf{e}_2$. Also, note that

$$\begin{aligned} \text{lt}(2x^2y^3z\mathbf{e}_1 + 3y^3z^4\mathbf{e}_1) &= 2x^2y^3z\mathbf{e}_1 \\ \text{lt}(-\mathbf{e}_1 + y\mathbf{e}_2 + xz\mathbf{e}_2) &= -\mathbf{e}_1. \end{aligned}$$

□

Proposition 2.2.3 *(Characteristic property of lex order) If $f \in k[x_1, \ldots, x_m]$ satisfies $\text{lt}_{lex}(f) \in k[x_s, x_{s+1}, \ldots, x_m]$ for some s, then $f \in k[x_s, x_{s+1}, \ldots, x_m]$.*

Proof: An easy exercise. □

2.2.3 Degree Lexicographic Order

When the ambient free module is $k[\boldsymbol{x}]$, for $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_m)$ and $\boldsymbol{\beta} = (\beta_1, \ldots, \beta_m)$,

$$\begin{aligned} \boldsymbol{x}^{\boldsymbol{\alpha}} \prec_{\text{dlex}} \boldsymbol{x}^{\boldsymbol{\beta}} \iff & \deg(\boldsymbol{x}^{\boldsymbol{\alpha}}) < \deg(\boldsymbol{x}^{\boldsymbol{\beta}}), \text{ where } \deg(\boldsymbol{x}^{\boldsymbol{\alpha}}) = \alpha_1 + \cdots + \alpha_m, \text{ or} \\ & \deg(\boldsymbol{x}^{\boldsymbol{\alpha}}) = \deg(\boldsymbol{x}^{\boldsymbol{\beta}}) \text{ and } \exists\, 1 \leq i \leq m : \\ & \alpha_1 = \beta_1, \ldots, \alpha_{i-1} = \beta_{i-1}, \alpha_i < \beta_i. \end{aligned}$$

When the ambient free module is $(k[\boldsymbol{x}])^n$, we extend above ideal-case order to this module case in the same way as in the previous subsections.

Proposition 2.2.4 *If $f \in k[x_1, \ldots, x_m]$ is homogeneous with $\text{lt}_{dlex}(f) \in k[x_s, x_{s+1}, \ldots, x_m]$ for some s, then $f \in k[x_s, x_{s+1}, \ldots, x_m]$.*

Proof: An easy exercise. □

2.2.4 Reverse Degree Lexicographic Order

When the ambient free module is $k[\boldsymbol{x}]$, for $\boldsymbol{\alpha} = (\alpha_1, \dots, \alpha_m)$ and $\boldsymbol{\beta} = (\beta_1, \dots, \beta_m)$,

$$\begin{aligned} \boldsymbol{x}^{\boldsymbol{\alpha}} \prec_{\text{rdlex}} \boldsymbol{x}^{\boldsymbol{\beta}} \iff & \deg(\boldsymbol{x}^{\boldsymbol{\alpha}}) < \deg(\boldsymbol{x}^{\boldsymbol{\beta}}), \text{ where } \deg(\boldsymbol{x}^{\boldsymbol{\alpha}}) = \alpha_1 + \cdots + \alpha_m, \text{ or} \\ & \deg(\boldsymbol{x}^{\boldsymbol{\alpha}}) = \deg(\boldsymbol{x}^{\boldsymbol{\beta}}) \text{ and } \exists\ 1 \le i \le m : \\ & \alpha_n = \beta_n, \dots, \alpha_{i+1} = \beta_{i+1}, \alpha_i > \beta_i. \end{aligned}$$

Again, we can extend this ideal-case order to the general module case in the same way as in the previous subsections.

This reverse degree lexicographic order (or simply reverse lexicographic order) is the monomial order that we will use for most of our computations throughout this thesis. As Bayer and Stillman showed in [BS87a] and [BS87b], the use of this monomial order sometimes improves the efficiency of the computation enormously.

Example 2.2.5 Consider the two monomials $x_1x_3, x_2^2 \in k[x_1, x_2, x_3]$. Then, $x_1x_3 \succ_{\text{dlex}} x_2^2$ while $x_1x_3 \prec_{\text{rdlex}} x_2^2$. □

Proposition 2.2.6 *If $f \in k[x_1, \dots, x_m]$ is homogeneous with $\mathrm{lt}_{drlex}(f) \in \langle x_s, x_{s+1}, \dots, x_m\rangle$ for some s, then $f \in \langle x_s, x_{s+1}, \dots, x_m\rangle$.*

Proof: An easy exercise. □

2.3 Gröbner Bases and Division Algorithm

Definition 2.3.1
1. *A $k[\boldsymbol{x}]$-module is called a* **monomial module** *if it is generated by a finite number of monomials.*

2. *For a subset S of a free $k[\boldsymbol{x}]$-module $\mathcal{M}$ with a fixed monomial order, we denote by $\mathrm{in}(S)$ (or $\mathrm{lt}(S)$) the set of the initial terms (or leading terms) of elements of S, i.e.*

$$\mathrm{in}(S) := \{\mathrm{lt}(f) \mid f \in S\}.$$

3. *The* **initial module** *associated to a subset S of a free $k[\boldsymbol{x}]$-module $\mathcal{M}$ with a fixed monomial order is the module generated by the elements of $\mathrm{in}(S)$, i.e.*

$$\langle \mathrm{in}(S)\rangle = \langle\{\mathrm{lt}(f) \mid f \in S\}\rangle.$$

Remark 2.3.2 By Dickson's Lemma, any $k[\boldsymbol{x}]$-module generated by monomials is actually generated by a finite number of monomials, and henceforth a monomial module. Therefore the finiteness condition in the above definition of a monomial module is not necessary, and the initial module $\langle \mathrm{lt}(S)\rangle$ associated to any subset S of a free $k[\boldsymbol{x}]$-module is a monomial module. For a proof of Dickson's Lemma, see [CLO92] or [Mis93].

Let $\{\mathbf{f}_1, \ldots, \mathbf{f}_l\}$ be a set of generators for $\mathcal{N}$. Then, since each $\mathrm{lt}(\mathbf{f}_i) \in \mathrm{lt}(\mathcal{N})$, the monomial module $\langle \mathrm{lt}(\mathbf{f}_1), \ldots, \mathrm{lt}(\mathbf{f}_l)\rangle$ is clearly contained in the monomial module $\langle \mathrm{lt}(\mathcal{N})\rangle$. Now one can ask when these two monomial modules coincide.

First note that $\mathcal{N}$ is the set of all the linear combinations (with coefficients from $k[\boldsymbol{x}]$) of $\mathbf{f}_i$'s. Therefore, if one can form a linear combination (with coefficients from $k[\boldsymbol{x}]$) of $\mathbf{f}_i$'s so that the resulting combination has the leading term not divisible by any of $\mathrm{lt}(\mathbf{f}_j)$, $1 \leq j \leq l$, then $\langle \mathrm{lt}(\mathbf{f}_1), \ldots, \mathrm{lt}(\mathbf{f}_l)\rangle$ is a proper submodule of $\langle \mathrm{lt}(\mathcal{N})\rangle$.

Example 2.3.3 Fix the degree lexicographic order on $k[x, y]$, and let $\mathcal{I} = \langle f, g\rangle$, with $f = 1 - xy$ and $g = x^2$. Then the relation

$$(1 + xy)f + y^2 g \quad = \quad 1$$

implies that we can form a linear combination of f and g so that the resulting combination is strictly smaller than f and g (w.r.t. the monomial order), i.e. the resulting combination has the leading term 1 which is not divisible by either of $\mathrm{lt}(f)$ or $\mathrm{lt}(g)$, and thus not in $\langle \mathrm{lt}(f), \mathrm{lt}(g)\rangle$. Therefore, $\langle \mathrm{lt}(f), \mathrm{lt}(g)\rangle$ is a proper submodule of $\langle \mathrm{lt}(\mathcal{I})\rangle$.

Actually, $\mathcal{I} = k[x, y]$, and therefore $\langle \mathrm{lt}(\mathcal{I})\rangle = k[x, y]$ while

$$\langle \mathrm{lt}(f), \mathrm{lt}(g)\rangle = \langle -xy, x^2\rangle \quad \subset \quad \langle x\rangle.$$

□

Definition 2.3.4 *Let $\mathcal{N}$ be a submodule of a a free $k[\boldsymbol{x}]$-module $\mathcal{M}$. Then w.r.t. a fixed monomial order on $\mathcal{M}$,*

1. *$G = \{\mathbf{f}_1, \ldots, \mathbf{f}_l\} \subset \mathcal{N} \subset \mathcal{M}$ is called a* **Gröbner basis** *of $\mathcal{N}$ if*

$$\langle \mathrm{lt}(\mathbf{f}_1), \ldots, \mathrm{lt}(\mathbf{f}_l)\rangle \quad = \quad \langle \mathrm{lt}(\mathcal{N})\rangle$$

   i.e. if the submodule generated by $\mathrm{lt}(\mathbf{f}_1), \ldots, \mathrm{lt}(\mathbf{f}_l)$ coincides with the initial module $\langle \mathrm{lt}(\mathcal{N})\rangle$ associated to $\mathcal{N}$.

2. $G = \{\mathbf{f}_1, \ldots, \mathbf{f}_l\} \subset \mathcal{N}$ *is called a* **minimal** *Gröbner basis of* $\mathcal{N}$ *if* G *is a Gröbner basis with* $\mathrm{lc}(\mathbf{f}_i) = 1\ \forall i$*, and no monomial in this set is redundant.*

3. $G = \{\mathbf{f}_1, \ldots, \mathbf{f}_l\} \subset \mathcal{N}$ *is called a* **reduced** *Gröbner basis of* $\mathcal{N}$ *if* G *is a Gröbner basis with* $\mathrm{lc}(\mathbf{f}_i) = 1\ \forall i$*, and for any two* $\mathbf{f}_i, \mathbf{f}_j \in G$*, no term of* $\mathbf{f}_j$ *is divisible by* $\mathrm{lt}(\mathbf{f}_i)$*.*

Remark 2.3.5 It actually turns out that $\mathcal{N}$ always has a unique reduced Gröbner basis.

Example 2.3.6 The computation done in the previous example shows that $\{1 - xy, x^2\}$ is a not a Gröbner basis. $\square$

Before proceeding to the multivariate division algorithm, let us take a look at the univariate polynomial case: For any given polynomials $f, g \in k[x]$ with $g \neq 0$, the Euclidean Division Algorithm constructs an expression of the form

$$f \quad = \quad qg + r$$

with $\deg(qg) = \deg(f)$ and $\deg(r) < \deg(g)$. With respect to the usual univariate monomial order, we can restate these conditions on q and r by saying that $\mathrm{lt}(f) = \mathrm{lt}(qg)$ and none of the monomials of r is in the monomial ideal $\langle \mathrm{lt}(g) \rangle$.

Now, we define a natural multivariate analogue of Euclidean Division.

Definition 2.3.7 *Let* $\mathcal{M}$ *be a free* $k[\boldsymbol{x}]$*-module with a fixed monomial order* $\prec$*, and* $F = \{\mathbf{f}_1, \ldots, \mathbf{f}_l\}$ *be an ordered subset of* $\mathcal{M}$*. Then for a nonzero* $\mathbf{f} \in \mathcal{M}$*, a* **standard expression** *of* $\mathbf{f}$ *in terms of* F *(or* $\mathbf{f}_i$*'s) is an expression*

$$\mathbf{f} \quad = \quad \sum_{i=1}^{l} h_i \mathbf{f}_i + \mathbf{r}, \qquad h_i \in k[\boldsymbol{x}], \mathbf{r} \in \mathcal{M}$$

such that $\mathrm{lt}(f) \succeq \mathrm{lt}(h_i f_i)\ \forall i$*, and* $\mathbf{r} \in k[\boldsymbol{x}]$ *is a* k*-linear combination of monomials not in* $\langle \mathrm{lt}(\mathbf{f}_1), \ldots, \mathrm{lt}(\mathbf{f}_l) \rangle$*.*

Example 2.3.8 Let $f_1 = 1 - xy,\ f_2 = x^2 \in k[x, y]$. Then, w.r.t. the lex order with $x \succ y$,

$$x^3 y - 1 \quad = \quad -x^2 f_1 + f_2 - 1$$

is a standard expression while

$$1 \quad = \quad (1 + xy) f_1 + y^2 f_2$$

is **not**. Actually, the unique standard expression of 1 in terms of f_1, f_2 is $1 = 0 \cdot f_1 + 0 \cdot f_2 + 1$, and thus 1 is not divisible by $\{f_1, f_2\}$. $\square$

Theorem 2.3.9 *Let $\mathcal{M}$ be a free $k[\boldsymbol{x}]$-module with a fixed monomial order $\prec$, and $F = \{\mathbf{f}_1, \ldots, \mathbf{f}_l\}$ be an ordered subset of $\mathcal{M}$. Then there is an algorithm that yields a unique standard expression in terms of $\mathbf{f}_i$'s for any given nonzero $\mathbf{f} \in \mathcal{M}$.*

Proof: We have to construct the following Division Algorithm.

Algorithm 2.1: **Division Algorithm**

Input:	$\mathbf{f}_1, \ldots, \mathbf{f}_l, \mathbf{f} \in \mathcal{M}$ with $\mathbf{f} \neq \mathbf{0}$
Output:	$h_1, \ldots, h_l \in k[\boldsymbol{x}]$, $\mathbf{r} \in \mathcal{M}$
Specification	$\mathbf{f} = \sum_{i=1}^{l} h_i \mathbf{f}_i + \mathbf{r}$ is a standard expression

Initialize $i = 0$ and let $\mathbf{r}_0 := \mathbf{f}$.

WHILE $\mathbf{r}_i := \mathbf{f} - \sum_{p=1}^{i} m_p \mathbf{f}_{s_p} \neq \mathbf{0}$ **DO**

IF no $\mathrm{lt}(\mathbf{f}_j)$ divides a monomial of $\mathbf{f}_i$

THEN for each $j = 1, \ldots, l$, set

$$\begin{aligned} \mathbf{f} &:= \mathbf{f}_i \\ h_j &:= \sum_{\{p \mid s_p = j\}} m_p \end{aligned}$$

ELSE let $\mathbf{f}$ be the maximal term of $\mathbf{f}_i$ that is divisible by some $\mathrm{lt}(\mathbf{f}_j)$, and let

$$\begin{aligned} s_{i+1} &:= j \\ \mathbf{f}_{i+1} &:= \mathbf{f}/\mathrm{lt}(\mathbf{f}_j) \\ i &:= i + 1 \end{aligned}$$

The termination of this algorithm is guaranteed since the maximal term of $\mathbf{r}_i$ divisible by some $\mathrm{lt}(\mathbf{f}_j)$ decreases at each step. □

Definition 2.3.10 1. *The unique polynomial vector $\mathbf{r} \in \mathcal{M}$ in the above Division Algorithm is called the* **remainder** *or* **normal form** *of $\mathbf{f}$ on division by F, and denoted by $N(\mathbf{f}, F)$.*

2. *If the Division Algorithm applied to $\mathbf{f}$ yields zero as its remainder, then we say $\mathbf{f}$ is* **divisible** *by F, or $\mathbf{f}$* **reduces to zero** *on division by F.*

Remark 2.3.11 The Division Algorithm depends on the ordering of the elements of $F = \{\mathbf{f}_1, \ldots, \mathbf{f}_l\}$, i.e. changing the order of $\mathbf{f}_i$'s will produce different standard expressions for the same $\mathbf{f}$.

Example 2.3.12 Let $f = 2x^2y - 3xy^2 + y^2$, $f_1 = xy - 1$, $f_2 = y^2 - 1 \in k[x, y]$, and use the lex order with $x \succ y$ as the fixed monomial order on $k[x, y]$. Apply the Division Algorithm to find a standard expression of f in terms of f_1 and f_2:

We note first that $\mathrm{lt}(f_1) = xy$ and $\mathrm{lt}(f_2) = y^2$.

- $i = 0$: Since $\mathrm{lt}(f_1) = xy$ divides $\mathrm{lt}(r_0) = 2x^2y$,

$$\begin{aligned} r_0 &= f = 2x^2y - 3xy^2 + y^2 \\ m &= 2x^2y \\ j &= 1 \\ s_1 &= 1 \\ m_1 &= m/\mathrm{lt}(f_j) = 2x^2y/(xy) = 2x. \end{aligned}$$

- $i = 1$:

$$\begin{aligned} r_1 &= f - m_1 f_{s_1} = (2x^2y - 3xy^2 + y^2) - 2x(xy - 1) = -3xy^2 + 2x + y^2 \\ m &= -3xy^2 \\ j &= 1 \\ s_2 &= 1 \\ m_2 &= m/\mathrm{lt}(f_j) = -3xy^2/(xy) = -3y. \end{aligned}$$

- $i = 2$:

$$\begin{aligned} r_2 &= f - m_1 f_{s_1} - m_2 f_{s_2} = r_1 - m_2 f_1 = (-3xy^2 + 2x + y^2) + 3y(xy - 1) \\ &= 2x + y^2 - 3y \\ m &= y^2 \\ j &= 2 \\ s_3 &= 2 \\ m_3 &= m/\mathrm{lt}(f_j) = y^2/y^2 = 1. \end{aligned}$$

- $i = 3$:

$$\begin{aligned} r_3 &= f - m_1 f_{s_1} - m_2 f_{s_2} - m_3 f_{s_3} = r_2 - m_3 f_2 = (2x + y^2 - 3y) - (y^2 - 1) \\ &= 2x - 3y + 1. \end{aligned}$$

Now, note that neither of $\mathrm{lt}(f_1)$ nor $\mathrm{lt}(f_2)$ divides a monomial of r_3. Therefore the process terminates here, and

$$\begin{aligned} r &= r_3 = 2x - 3y + 1 \\ h_1 &= \sum_{\{p|s_p=1\}} m_p = m_1 + m_2 = 2x - 3y \\ h_2 &= \sum_{\{p|s_p=2\}} m_p = m_3 = 1. \end{aligned}$$

Finally, we get the following standard expression of f in terms of f_1 and f_2:

$$\begin{aligned} f &= h_1 f_1 + h_2 f_2 + r \\ &= (2x - 3y) f_1 + f_2 + 2x - 3y + 1. \end{aligned}$$

□

The following corollary, together with the above Division Algorithm, shows why a Gröbner basis is so special among many sets of ideal generators.

Corollary 2.3.13 (Submodule Membership Algorithm) *Suppose $\mathcal{N}$ is a submodule of a free $k[\boldsymbol{x}]$-module $\mathcal{M}$ with a fixed monomial order $\prec$ and $G = \{\mathbf{f}_1, \ldots, \mathbf{f}_l\} \subset \mathcal{N}$ is a* **Gröbner basis** *of $\mathcal{N}$. Then, there is an algorithm for writing any $\mathbf{f} \in \mathcal{M}$ in the form*

$$\mathbf{f} = h_1 \mathbf{f}_1 + \cdots + h_l \mathbf{f}_l + \mathbf{r}, \quad h_i \in k[\boldsymbol{x}],\ \mathbf{r} \in \mathcal{M}$$

such that $\mathbf{f} \in \mathcal{N}$ if and only if $\mathbf{r} = \mathbf{0}$.

Proof: One direction ($\Longleftarrow$) is obvious.

If $\mathbf{f} \in \mathcal{N}$ and $\mathbf{r} \neq \mathbf{0}$, apply the Division Algorithm to get a standard expression of $\mathbf{f}$ in terms of $\mathbf{f}_i$'s: $\mathbf{f} = h_1 \mathbf{f}_1 + \cdots + h_l \mathbf{f}_l + \mathbf{r}$. Note that the Division Algorithm necessarily requires $\mathrm{lt}(\mathbf{r}) \notin \langle \mathrm{lt}(\mathbf{f}_1), \ldots, \mathrm{lt}(\mathbf{f}_l) \rangle$.

Now, noting $\mathbf{r} = \mathbf{f} - \sum_{i=1}^{l} h_i \mathbf{f}_i \in \mathcal{N}$ and $\langle \mathrm{lt}(\mathcal{N}) \rangle = \langle \mathrm{lt}(\mathbf{f}_1), \ldots, \mathrm{lt}(\mathbf{f}_l) \rangle$, we get

$$\mathrm{lt}(\mathbf{r}) \in \langle \mathrm{lt}(\mathcal{N}) \rangle = \langle \mathrm{lt}(\mathbf{f}_1), \ldots, \mathrm{lt}(\mathbf{f}_l) \rangle,$$

which is a contradiction. □

Theorem 2.3.14 (Buchberger Algorithm) *Any submodule of a free $k[\boldsymbol{x}]$-module has a Gröbner basis w.r.t. an arbitrary fixed monomial order.*

We will prove this theorem in the next section by giving an algorithm that constructs a Gröbner basis for any given submodule of a free $k[\boldsymbol{x}]$-module.

Definition 2.3.15 *Let $\mathcal{N}$ be a submodule of a free $k[\boldsymbol{x}]$-module $\mathcal{M}$. Then the monomials of $\mathcal{M}$ which do not lie in the initial module $\langle \mathrm{lt}(I)\rangle := \langle\{\mathrm{lt}(\mathbf{f}) \mid \mathbf{f} \in S\}\rangle$ associated to $\mathcal{N}$ are called the* **standard monomials** *w.r.t. $\mathcal{N}$.*

Corollary 2.3.16 *(Macaulay) Let $\mathcal{N}$ be a submodule of a free $k[\boldsymbol{x}]$-module $\mathcal{M}$. Then the (images of the) standard monomials w.r.t $\mathcal{N}$ form a k-vector space basis for $\mathcal{M}/\mathcal{N}$.*

Proof: In order to show that the standard monomials *span* $\mathcal{M}/\mathcal{N}$ as a k-vector space, let $\{\mathbf{g}_1, \ldots, \mathbf{g}_l\}$ be a Gröbner basis for $\mathcal{N}$ whose existence is guaranteed by the Theorem 2.3.14. Now choose an arbitrary $\bar{\mathbf{g}} \in \mathcal{M}/\mathcal{N}$, and use the above Division Algorithm to write $\mathbf{g} \in \mathcal{M}$ in the form $\mathbf{g} = h_1\mathbf{g}_1 + \cdots + h_l\mathbf{g}_l + \mathbf{r}$. Then $\mathbf{g} \equiv \mathbf{r} \pmod{I}$, where $\mathbf{r} \in \mathcal{M}$ is a k-linear combinations of monomials not in $\langle \mathrm{lt}(\mathbf{g}_1), \ldots, \mathrm{lt}(\mathbf{g}_l)\rangle = \langle \mathrm{lt}(\mathcal{N})\rangle$. Therefore, $\bar{\mathbf{g}} \in \mathcal{M}/\mathcal{N}$ is a k-linear combination of standard monomials w.r.t $\mathcal{N}$.

To show the linear independence, assume we have nonzero standard monomials, $\mathbf{m}_i$'s, $1 \leq i \leq l$, w.r.t. $\mathcal{N}$ such that

$$\mathbf{f} = \sum c_i \mathbf{m}_i \quad \in \quad \mathcal{N},$$

for some nonzero c_i's in k. Then $\mathrm{lt}(\mathbf{f}) \in \langle \mathrm{lt}(\mathcal{N})\rangle$. But this is a contradiction since $\mathrm{lt}(\mathbf{f})$ is one of $c_i\mathbf{m}_i$'s and $\mathbf{m}_i$ is a standard monomial, i.e. not in $\langle \mathrm{lt}(\mathcal{N})\rangle$. $\square$

2.4 Buchberger Algorithm

By the Hilbert Basis Theorem, any submodule $\mathcal{N}$ of a f.g. free module $\mathcal{M}$ over $k[\boldsymbol{x}]$ is generated by finitely many elements, say, $\mathbf{f}_1, \ldots, \mathbf{f}_l \in \mathcal{N}$. Now, we intend to construct a Gröbner basis for $\mathcal{N}$ out of these generators.

Definition 2.4.1 *Let $\mathcal{N}$ be a submodule of a free $k[\boldsymbol{x}]$-module $\mathcal{M}$ and $\mathbf{f}_1, \mathbf{f}_2$ be elements of $\mathcal{N}$ such that $\mathrm{lt}(\mathbf{f}_1)$ and $\mathrm{lt}(\mathbf{f}_2)$ involve the same basis element $\mathbf{e}_j$ of $\mathcal{M}$. Then the S-***pair** *of $\mathbf{f}_1$ and $\mathbf{f}_2$ is defined by*

$$S(\mathbf{f}_1, \mathbf{f}_2) \quad := \quad h_1\mathbf{f}_1 - h_2\mathbf{f}_2,$$

where $h_1, h_2 \in k[\boldsymbol{x}]$ *are the smallest degrees terms making the cancellation*

$$\mathrm{lt}(h_1\mathbf{f}_1) = \mathrm{lt}(h_2\mathbf{f}_2).$$

(One finds that $h_i\mathbf{e}_j = \mathrm{lt}(\mathbf{f}_i)/\gcd(\mathrm{lt}(\mathbf{f}_1), \mathrm{lt}(\mathbf{f}_2))$*.) If* $\mathrm{lt}(\mathbf{f}_1)$ *and* $\mathrm{lt}(\mathbf{f}_2)$ *involve distinct basis elements of* $\mathcal{M}$*, we set* $S(\mathbf{f}_1, \mathbf{f}_2) := 0$*.*

The following theorem offers an important algorithmic criterion in terms of S-pairs to test if a given set of generators for $\mathcal{N}$ is in fact a Gröbner basis.

Theorem 2.4.2 (Buchberger's Criterion) *The set* $G = \{\mathbf{f}_1, \ldots, \mathbf{f}_l\}$ *is a Gröbner basis iff for all pairs* $i \neq j$*, the remainder on division of the* S*-pair* $S(\mathbf{f}_i, \mathbf{f}_j)$ *by* G *is zero.*

Proof: See the Theorem 15.8 of [Eis95]. □

Now above theorem allows us to construct a Gröbner basis for $\mathcal{N}$ in a finite number steps by the following algorithm. Again we let $\mathcal{N}$ be a submodule of a free $k[\boldsymbol{x}]$-module $\mathcal{M}$.

Algorithm 2.2: **Buchberger Algorithm**

Input:	$G = \{\mathbf{f}_1, \ldots, \mathbf{f}_l\}$, a set of generators for $\mathcal{N}$
Output:	$\{\mathbf{g}_1, \ldots, \mathbf{g}_p\}$, a Gröbner basis for $\mathcal{N}$

- **Step 1:** If all the $S(\mathbf{f}_i, \mathbf{f}_j)$'s, $i \neq j$, have zero remainders on division by G, then G is a Gröbner basis by the Theorem 2.4.2. Give G as the output.

- **Step 2:** If some $S(\mathbf{f}_i, \mathbf{f}_j)$ has a nonzero remainder $\mathbf{S}_{ij} := N(S(\mathbf{f}_i, \mathbf{f}_j), G)$, then replace G by the enlarged set $\{\mathbf{f}_1, \ldots, \mathbf{f}_l, \mathbf{S}_{ij}\}$, and go back to **Step 1:**.

Since the submodule generated by the leading terms of $\mathbf{f}_1, \ldots, \mathbf{f}_l, \mathbf{S}_{ij}$ is strictly larger than $\langle \mathrm{lt}(\mathbf{f}_1), \ldots, \mathrm{lt}(\mathbf{f}_l) \rangle$, this process must terminate after finitely many steps.

The Buchberger Algorithm outlined in the above does not necessarily yield a minimal Gröbner basis, and the following lemma lets us eliminate some redundant generators.

Lemma 2.4.3 *Let* G *be a Gröbner basis for a submodule* $\mathcal{N}$ *of a free* $k[\boldsymbol{x}]$*-module. If there is* $\mathbf{f} \in G$ *such that* $\mathrm{lt}(\mathbf{f}) \in \langle \mathrm{lt}(G - \{\mathbf{f}\}) \rangle$*, then* $G - \{\mathbf{f}\}$ *is also a Gröbner basis for* $\mathcal{N}$*.*

Proof: By definition, $\langle \mathrm{lt}(G)\rangle = \langle \mathrm{lt}(I)\rangle$. If $\mathrm{lt}(\mathbf{f}) \in \langle \mathrm{lt}(G-\{\mathbf{f}\})\rangle$, then $\langle \mathrm{lt}(G-\{\mathbf{f}\})\rangle = \langle \mathrm{lt}(G)\rangle$. Now by definition, it follows that $G - \{\mathbf{f}\}$ is a Gröbner basis. $\square$

Example 2.4.4 Find a minimal Gröbner basis for $G = \{1 - xy, x^2\} \in k[x, y]$ using the Buchberger Algorithm, and express each element of the Gröbner basis as a linear combination (with coefficients from $k[x, y]$) of $1 - xy, x^2$:

- **Step 1:** The remainder of $S(1 - xy, x^2) = x \cdot (1 - xy) + y \cdot x^2 = x$ on division by $\{1 - xy, x^2\}$ is simply itself, x, which is nonzero. Hence, we have to enlarge G to $\{1 - xy, x^2, x\}$. But x^2 is redundant since it is divisible by x. Therefore, let $G_1 = \{1 - xy, x\}$.
- **Step 2:** The remainder of $S(1 - xy, x) = 1 \cdot (1 - xy) + y \cdot x = 1$ on division by $\{1 - xy, x\}$ is 1, which is nonzero. Hence, we have to enlarge G_1 to $\{1 - xy, x, 1\}$. Now, note that $1 - xy, x$ are redundant since each of them is divisible by 1. Therefore, $\{1\}$ is a Gröbner basis for $G = \{1 - xy, x^2\} \in k[x, y]$.

Since $\langle 1 - xy, x^2\rangle = \langle 1\rangle$, we should be able to express 1 as a linear combination of $1 - xy, x^2$. For this purpose, we retrace the above process of getting to $\{1\}$:

$$\begin{aligned} 1 &= S(1 - xy, x) = (1 - xy) + y \cdot x \\ &= (1 - xy) + yS(1 - xy, x^2) \\ &= (1 - xy) + y(x(1 - xy) + y \cdot x^2) \\ &= (1 + xy)(1 - xy) + y^2x^2. \end{aligned}$$

$\square$

Example 2.4.5 (**Ideal Membership**) Let $f = 2x^2y - 3xy^2 + y^2$, $f_1 = xy - 1$, $f_2 = y^2 - 1 \in k[x, y]$. Determine if f belongs to the ideal $\langle f_1, f_2\rangle \subset k[x, y]$.

We will use the lex order with $x \succ y$ as our fixed monomial order on $k[x, y]$. In order to apply the Corollary 2.3.13, we first have to find a Gröbner basis for $G = \{f_1, f_2\}$:

- **Step 1:** The remainder of $S(f_1, f_2) = y(xy - 1) - x(y^2 - 1) = x - y$ on division by $\{xy - 1, y^2 - 1\}$ is simply itself, $x - y$, which is nonzero. Hence, we have to enlarge G to $\{xy - 1, y^2 - 1, x - y\}$. But according to the Lemma 2.4.3, $xy - 1$ is redundant since its leading term xy is divisible by the leading term of $x - y$. Therefore, let $G_1 = \{y^2 - 1, x - y\}$.

- **Step 2:** $S(y^2 - 1, x - y) = x \cdot (y^2 - 1) - y^2 \cdot (x - y) = -x + y^3$ is divisible by $\{xy - 1, y^2 - 1\}$ since the Division Algorithm yields

$$-x + y^3 \;=\; y \cdot (y^2 - 1) - 1 \cdot (x - y).$$

Hence, $G_1 = \{y^2 - 1, x - y\}$ is a minimal Gröbner basis for $G = \{f_1, f_2\}$ (one checks easily that this is actually the unique reduced Gröbner basis for $G = \{f_1, f_2\}$).

Now apply the Division Algorithm to find a standard expression of f in terms of G_1. One finds that the remainder is $y + 1$, which is nonzero. Therefore, we conclude from the Corollary 2.3.13 that

$$f \notin \langle f_1, f_2 \rangle.$$

□

2.5 Syzygy Computation

Let $\mathcal{M}$ be a free $k[\boldsymbol{x}]$-module of rank q with free basis $\{\mathbf{e}_1, \ldots, \mathbf{e}_q\}$. We will occasionally identify an element of $\mathcal{M}$ with a q dimensional column vector with entries from $k[\boldsymbol{x}]$ by writing it as a unique linear combination (with coefficients from $k[\boldsymbol{x}]$) of the given basis elements.

Now let $\mathbf{v}_1, \ldots, \mathbf{v}_p$ be elements of $\mathcal{M} = (k[\boldsymbol{x}])^q$.

Definition 2.5.1 *A* **syzygy** *of the ordered set* $F = \{\mathbf{v}_1, \ldots, \mathbf{v}_p\}$ *is a polynomial vector* $\mathbf{h} = (h_1, \ldots, h_p) \in (k[\boldsymbol{x}])^p$ *such that*

$$h_1\mathbf{v}_1 + \cdots + h_p\mathbf{v}_p = 0 \in (k[\boldsymbol{x}])^q.$$

Consider the homomorphism α of free $k[\boldsymbol{x}]$-modules defined as follows:

$$\begin{aligned} \alpha :\ (k[\boldsymbol{x}^{\pm 1}])^p &\longrightarrow (k[\boldsymbol{x}^{\pm 1}])^q \\ (h_1, \ldots, h_p) &\mapsto h_1\mathbf{v}_1 + \cdots + h_p\mathbf{v}_p. \end{aligned}$$

Then a syzygy of $F = \{\mathbf{v}_1, \ldots, \mathbf{v}_p\}$ is simply an element of $\mathrm{Ker}(\alpha)$, and we see that the set of all the syzygies of F coincides with $\mathrm{Ker}(\alpha)$, thus makes a $k[\boldsymbol{x}]$-module itself.

Now the Hilbert Basis Theorem tells us that $\mathrm{Ker}(\alpha)$, the module of syzygies of F, has a finite number of generators, but it does not give us an effective way of finding them.

Actually, when $\mathbf{v}_1, \ldots, \mathbf{v}_p \in (k[\boldsymbol{x}])^q$ satisfy an additional condition called *unimodularity condition*, then $\mathrm{Ker}(\alpha)$ turns out to be **free**, and thus an arbitrary syzygy can be written as a **unique** linear combination (with coefficients from $k[\boldsymbol{x}]$) of the elements of a free basis of $\mathrm{Ker}(\alpha)$. This result is a consequence of the Quillen-Suslin Theorem, and will be studied in more detail in the next chapter.

Since the Buchberger Algorithm of the previous section gives us a way of expressing each remainder $\mathbf{S}_{ij} := N(S(\mathbf{f}_i, \mathbf{f}_j), G)$ as a linear combination of $\mathbf{f}_i$'s, if the remainder $\mathbf{S}_{ij} = 0$, then we get a linear combination among the $\mathbf{f}_i$'s being equal to zero, i.e. a syzygy. Now a theorem of Schreyer states that these syzygies generate the entire module of syzygies. For a more detailed exposition, see the section 15.5 in [Eis95].

Chapter 3

A Syzygy-based Algorithm for the Quillen-Suslin Theorem

3.1 A Conjecture of Serre

In FAC ([Ser55], 1955), J.-P. Serre pointed out that no example was known of a nontrivial algebraic vector bundle over an affine space, and this observation became a fact when D. Quillen and A. Suslin proved it as a theorem in 1976.

Definition 3.1.1 *Let R be a commutative ring with identity. Then a module $\mathcal{M}$ over R is called* **projective** *if it is a direct summand of a free module over R.*

Since locally trivial algebraic vector bundles are interpreted as locally free coherent sheaves, we can reformulate the Serre's Conjecture as

> **[1]** *Any finitely generated projective module over a polynomial ring (with coefficients from a field) is free.*

Definition 3.1.2 *Let R be a commutative ring.*

1. *Let $\mathbf{v} = (v_1, \ldots, v_n)^t \in R^n$ for some $n \in \mathbb{N}$. Then $\mathbf{v}$ is called a* **unimodular column vector** *if its components generate R, i.e. if there exist $g_1, \ldots, g_n \in R$ such that $v_1 g_1 + \cdots + v_n g_n = 1$.*

2. *A matrix $\mathbf{A} \in \mathrm{M}_{pq}(R)$ is called a* **unimodular matrix** *if its maximal minors generate the unit ideal in R.*

Remark 3.1.3 When $R = k[x_1, \ldots, x_m]$ is a polynomial ring and $\mathbf{v} \in R^n$ is a unimodular vector, we can explicitly find these g_i's either by using the effective Nullstellensatz (see [FG90]) or by retracing the steps in computing a Gröbner basis $G = \{1\}$ for $\langle v_1, \ldots, v_n \rangle$.

The following lemma gives an important property of a unimodular vector.

Lemma 3.1.4 *Let R be a commutative ring and $\mathbf{v} \in R^n$. Then, $R\mathbf{v} \subset R^n$ splits as a direct summand if and only if $\mathbf{v} \in R^n$ is unimodular.*

Proof: Suppose $R\mathbf{v}$ is a direct summand of R^n and $\mathbf{v} = \sum_{i=1}^n v_i \mathbf{e}_i$. Write $R\mathbf{v} \oplus \mathcal{N} = R^n$ for some submodule $\mathcal{N}$ of R^n. Then any element of R^n can be written uniquely in the form, $a\mathbf{v} + \mathbf{w}$, for some $a \in R$ and $\mathbf{w} \in \mathcal{N}$. Define an R-module homomorphism $f : R^n \to R$ by $f(a\mathbf{v} + \mathbf{w}) = a$. Then since $f(\mathbf{v}) = 1 = \sum_{i=1}^n v_i f(\mathbf{e}_i)$, $\mathbf{v}$ is unimodular. Conversely, if $\mathbf{v} = \sum_{i=1}^n v_i \mathbf{e}_i \in R^n$ is unimodular, then there exists $g_1, \ldots, g_n \in R$ such that $\sum_{i=1}^n v_i g_i = 1 \in R$. Defining an R-module homomorphism $\alpha : R^n \to R$ by $\alpha(\mathbf{e}_i) = g_i$, we get the following short exact sequence:

$$0 \longrightarrow \mathrm{Ker}(\alpha) \longrightarrow R^n \xrightarrow{\alpha} R \longrightarrow 0.$$

Defining an R-module homomorphism $\beta : R \to R^n$ by $\beta(a) = a\mathbf{v}$, we see that the above short exact sequence splits. Hence, $R\mathbf{v}$ is a direct summand of R^n. $\square$

Actually, this lemma is a special case of the following well known result whose proof is essentially same as in the above proof.

Lemma 3.1.5 *Let R be a commutative ring, and $\mathbf{M} \in \mathrm{M}_{pq}(R)$ for $p \geq q$. Then $\mathbf{M}$ is unimodular if and only if its q column vectors form a free basis of a rank q submodule of R^p that splits as a direct summand.*

Now consider the following statement over polynomial rings.

> **[2] (Unimodular Completion)** Let $\mathbf{A}$ be a $p \times q$ unimodular matrix, $p \geq q$, with polynomial entries, i.e. a matrix over $k[\boldsymbol{x}] := k[x_1, \ldots, x_m]$. Then $\mathbf{A}$ can be completed to a square $p \times p$ unimodular matrix $\bar{\mathbf{A}} \in \mathrm{GL}_p(k[\boldsymbol{x}])$ by adding $p - q$ columns to the matrix $\mathbf{A}$.

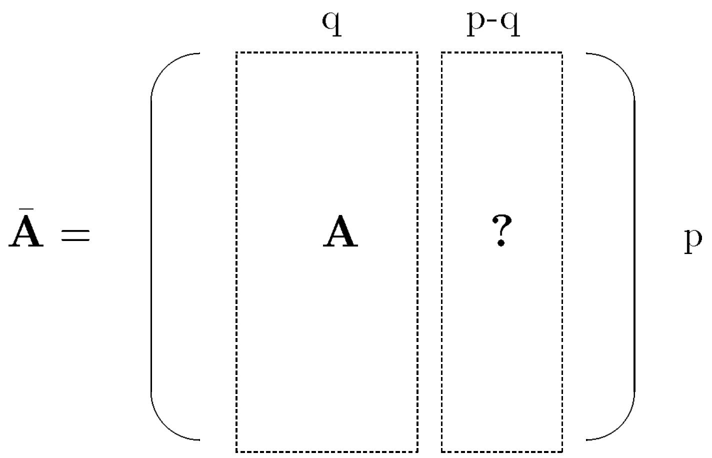

Figure 3.1: Unimodular completion of $\mathbf{A}$ to $\bar{\mathbf{A}}$

We claim that Serre's Conjecture **[1]** is equivalent to the above elementary linear algebraic statement **[2]**, which is actually the form Quillen and Suslin used to prove Serre's Conjecture.

Theorem 3.1.6 *The statement* **[1]** *is equivalent to the statement* **[2]**

Proof: [1] $\Longrightarrow$ [2]: Consider the submodule $\mathcal{N}$ of the free $k[\boldsymbol{x}]$-module $(k[\boldsymbol{x}])^p$, generated by the q columns of $\mathbf{A}$. Then the unimodularity of $\mathbf{A}$ implies that $\mathcal{N}$ separates as a direct summand of $(k[\boldsymbol{x}])^q$, i.e.

$$\mathcal{N} \oplus \mathcal{T} \quad = \quad (k[\boldsymbol{x}])^p$$

for some submodule $\mathcal{T}$ of $(k[\boldsymbol{x}])^p$. Since $\mathcal{T}$ is a direct summand of $(k[\boldsymbol{x}])^p$, it is a projective $k[\boldsymbol{x}]$-module. We can, therefore, apply the statement **[1]** to conclude that $\mathcal{T}$ is free. Let $\mathbf{v}_1, \ldots, \mathbf{v}_{p-q} \in (k[\boldsymbol{x}])^p$ be a free basis for $\mathcal{T}$, i.e.

$$\mathcal{T} \quad = \quad \oplus_{i=1}^{p-q} k[\boldsymbol{x}]\mathbf{v}_i.$$

Now regarding $\mathbf{v}_i$'s as p dimensional column vectors, add them to the matrix $\mathbf{A}$ to make a $p \times p$ matrix. The resulting square matrix is unimodular since its column vectors form a basis for $(k[\boldsymbol{x}])^p$.

[2] $\Longrightarrow$ [1]: First, we need to establish the fact that every projective module $\mathcal{N}$ over a polynomial ring $k[\boldsymbol{x}]$ is stably free, i.e. $\mathcal{N} \oplus (k[\boldsymbol{x}])^q \cong (k[\boldsymbol{x}])^p$ for some $p, q \in \mathbb{Z}_{\geq 0}$.

To see this, consider a free resolution of the projective module

$$0 \to \mathcal{F}_m \to \mathcal{F}_{n-1} \to \cdots \to \mathcal{F}_0 \to \mathcal{F}_{-1} = \mathcal{N} \to 0.$$

Note here that we are using the Hilbert Syzygy Theorem to obtain a free resolution of $\mathcal{N}$ whose length is bounded by m, the number of variables. Then, denoting the kernel of the module homomorphism $F_i \to F_{i-1}$ by $\mathcal{N}_i$, we have

$$\mathcal{F}_0 \cong \mathcal{N} \oplus \mathcal{N}_0, \mathcal{F}_1 \cong \mathcal{N}_0 \oplus \mathcal{N}_1, \mathcal{F}_2 \cong \mathcal{N}_1 \oplus \mathcal{N}_2, \cdots, \mathcal{F}_n \cong \mathcal{N}_{n-1}.$$

Therefore we get

$$\begin{aligned} \mathcal{N} \oplus \mathcal{F}_1 \oplus \mathcal{F}_3 \oplus \cdots &\cong \mathcal{N} \oplus (\mathcal{N}_0 \oplus \mathcal{N}_1) \oplus (\mathcal{N}_2 \oplus \mathcal{N}_3) \oplus \cdots \\ &\cong (\mathcal{N} \oplus \mathcal{N}_0) \oplus (\mathcal{N}_1 \oplus \mathcal{N}_2) \oplus \cdots \\ &\cong \mathcal{F}_0 \oplus \mathcal{F}_2 \oplus \cdots, \end{aligned}$$

which implies that $\mathcal{N}$ is stably free.

Now that we have $\mathcal{N} \oplus (k[\boldsymbol{x}])^q \cong (k[\boldsymbol{x}])^p$, we can make a $p \times q$ unimodular polynomial matrix whose column vectors form a free basis for $(k[\boldsymbol{x}])^q \subset (k[\boldsymbol{x}])^p$. Then apply the statement [**2**] to complete this $p \times q$ matrix to a square $p \times p$ unimodular matrix. Then the last $p - q$ columns of this square matrix form a free basis for $\mathcal{N}$. $\square$

Remark 3.1.7 The second part of the proof is based on the Hilbert Syzygy Theorem in assuming the existence of a finite free resolution of a projective module over a polynomial ring. An algorithmic construction of such a free resolution can be found in [LS92].

In the following section, we will attempt to develop an effective algorithm for Unimodular Completion. By using this algorithm, one not only knows the freeness of a given f.g. projective $k[\boldsymbol{x}]$-module but also can find a free basis for that module.

While there are recent algorithmic proofs of Unimodular Completion, ([LS92] and [Fit93]), our algorithm based on a syzygy computation using Gröbner basis seems to offer a very effective algorithm which can be easily implemented since syzygy computation is already a standard part of many computer algebra packages, e.g. *Macaulay* and SINGULAR.

3.2 A Syzygy-based Algorithm for Unimodular Completion

In the following, we will present an effective algorithm for Unimodular Completion based on a syzygy computation using Gröbner bases.

Algorithm 3.1: **UnimodCompletion**

Input:	$\mathbf{A} = (f_{ij}) \in \mathrm{M}_{pq}(k[\boldsymbol{x}])$, $p \geq q$, a unimodular polynomial matrix
Output:	$\bar{\mathbf{A}} \in \mathrm{GL}_p(k[\boldsymbol{x}])$, a square unimodular matrix
Specification:	the $p \times q$ matrix made of first q columns of $\bar{\mathbf{A}}$ is $\mathbf{A}$

This will by no means replace the proof of Unimodular Completion given in Chapter 4 as the Corollary 4.3.6, since we need to assume the validity of the statement of the Quillen-Suslin Theorem to deduce the right size of a minimal syzygy basis.

Also, the first step in the algorithm is about finding a particular left inverse of $\mathbf{A} \in \mathrm{M}_{pq}(k[\boldsymbol{x}])$, and our method for this step is due to A. Logar and B. Sturmfels [LS92].

- **Step 1:** Find a $q \times p$ matrix $\mathbf{B} \in \mathrm{M}_{qp}(k[\boldsymbol{x}])$ such that $\mathbf{BA} = \mathbf{I}_q$ in the following way:

  The column vectors of the unimodular matrix $\mathbf{A}^t = (f_{ji}) \in \mathrm{M}_{qp}(k[\boldsymbol{x}])$ span the free $k[\boldsymbol{x}]$-module $(k[\boldsymbol{x}])^q$. Therefore, we can use Gröbner bases to express the standard basis vectors $\mathbf{e}_1, \ldots \mathbf{e}_q \in (k[\boldsymbol{x}])^q$ as linear combinations (with polynomial coefficients) of the column vectors of $\mathbf{A}^t$.

  More explicitly, denoting the i-th column vector of $\mathbf{A}^t$ by $\mathbf{w}_i$, $1 \leq i \leq p$, we have $\mathbf{w}_i := \begin{pmatrix} f_{i1} \\ \vdots \\ f_{iq} \end{pmatrix}$. Now, use Gröbner basis to find g_{ij}'s such that

$$
\begin{aligned}
\mathbf{e}_1 &:= \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} = g_{11}\mathbf{w}_1 + \cdots + g_{1p}\mathbf{w}_p = g_{11} \begin{pmatrix} f_{11} \\ \vdots \\ f_{1q} \end{pmatrix} + \cdots + g_{1p} \begin{pmatrix} f_{p1} \\ \vdots \\ f_{pq} \end{pmatrix} \\
&\vdots \\
\mathbf{e}_q &:= \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix} = g_{q1}\mathbf{w}_1 + \cdots + g_{qp}\mathbf{w}_p = g_{q1} \begin{pmatrix} f_{11} \\ \vdots \\ f_{1q} \end{pmatrix} + \cdots + g_{qp} \begin{pmatrix} f_{p1} \\ \vdots \\ f_{pq} \end{pmatrix}.
\end{aligned}
$$

  Denoting the $q \times p$ matrix (g_{ij}) by $\mathbf{B}$, we can rewrite the above set of equations as

$$
\begin{aligned}
\mathbf{I}_q &= \begin{pmatrix} g_{11} & \cdots & g_{1p} \\ \vdots & & \vdots \\ g_{q1} & \cdots & g_{qp} \end{pmatrix} \begin{pmatrix} f_{11} & \cdots & f_{1q} \\ \vdots & & \vdots \\ f_{p1} & \cdots & f_{pq} \end{pmatrix} \\
&= \mathbf{BA}.
\end{aligned}
$$

- **Step 2:** Again, let $\mathbf{w}_1, \ldots, \mathbf{w}_p \in (k[\boldsymbol{x}])^q$ be the column vectors of $\mathbf{A}^t$. Now, find a syzygy basis $\mathbf{s}_1, \ldots, \mathbf{s}_{p-q} \in (k[\boldsymbol{x}])^p$ for the set $\{\mathbf{w}_1, \ldots, \mathbf{w}_p\}$ in the following way:

  Consider the $k[\boldsymbol{x}]$-module homomorphism $\alpha : (k[\boldsymbol{x}])^p \to (k[\boldsymbol{x}])^q$ defined by $\mathbf{A}^t$, i.e. for any p-dimensional column vector $\mathbf{v} \in (k[\boldsymbol{x}])^p$,

$$\alpha(\mathbf{v}) \quad := \quad \mathbf{A}^t\mathbf{v}.$$

  First, note that α is surjective due to the unimodularity of $\mathbf{A}$. More explicitly, let $\mathbf{B}$ be the left inverse of $\mathbf{A}$ found in the **Step 1**. Then, for any $\mathbf{w} \in (k[\boldsymbol{x}])^q$, $\mathbf{B}^t\mathbf{w} \in (k[\boldsymbol{x}])^p$ and

$$\begin{aligned} \alpha(\mathbf{B}^t\mathbf{w}) &= \mathbf{A}^t(\mathbf{B}^t\mathbf{w}) \\ &= (\mathbf{BA})^t\mathbf{w} \\ &= \mathbf{I}_q\mathbf{w} = \mathbf{w}. \end{aligned}$$

  Thus we get the following short exact sequence:

$$0 \longrightarrow \mathrm{Ker}(\alpha) \longrightarrow (k[\boldsymbol{x}])^p \xrightarrow{\alpha} (k[\boldsymbol{x}])^q \longrightarrow 0. \tag{3.1}$$

  Defining a $k[\boldsymbol{x}]$-module homomorphism $\beta : (k[\boldsymbol{x}])^q \to (k[\boldsymbol{x}])^p$ by $\beta(\mathbf{w}) = \mathbf{B}^t\mathbf{w}$, we see that the above short exact sequence splits. Hence, $\mathrm{Ker}(\alpha)$ is a direct summand of $(k[\boldsymbol{x}])^p$, i.e. a projective module over $k[\boldsymbol{x}]$, and therefore free of rank $p - q$ by the Quillen-Suslin Theorem. Now find the reduced Gröbner basis $\mathbf{s}_1, \ldots, \mathbf{s}_{p-q} \in (k[\boldsymbol{x}])^p$ of $\mathrm{Ker}(\alpha)$.

  Note that $\alpha : (k[\boldsymbol{x}])^p \to (k[\boldsymbol{x}])^q$ satisfies the following property:

$$\alpha\left(\begin{pmatrix} h_1 \\ \vdots \\ h_p \end{pmatrix}\right) \quad = \quad h_1\mathbf{w}_1 + \cdots + h_p\mathbf{w}_p,$$

  where $\mathbf{w}_1, \ldots, \mathbf{w}_p \in (k[\boldsymbol{x}])^q$ are the column vectors of $\mathbf{A}^t$.

  Therefore, $\mathrm{Ker}(\alpha)$ is precisely the (first) module of syzygies of the vectors $\mathbf{w}_1, \ldots, \mathbf{w}_p \in (k[\boldsymbol{x}])^q$.

- **Step 3:** Let

$$\begin{aligned} \mathbf{s}_i &= (s_{i1}, \ldots, s_{ip})^t, \quad 1 \le i \le p - q \\ \mathbf{S} &= (s_{ij}) \in \mathrm{M}_{(p-q)q}(k[\boldsymbol{x}]) \end{aligned}$$

and define a square polynomial matrix $\mathbf{C} \in \mathrm{M}_p(k[\boldsymbol{x}])$ by

$$\begin{aligned}
\mathbf{C} &= \begin{pmatrix} \mathbf{B} \\ \mathbf{S} \end{pmatrix} \\
&= \begin{pmatrix} g_{11} & \cdots & g_{1p} \\ \vdots & & \vdots \\ g_{q1} & \cdots & g_{qp} \\ s_{11} & \cdots & s_{1p} \\ \vdots & & \vdots \\ s_{(p-q)1} & \cdots & s_{(p-q)p} \end{pmatrix}.
\end{aligned}$$

Now, let $\bar{\mathbf{A}} := \mathbf{C}^{-1}$, and terminate the process.

To verify the validity of this algorithm, it remains to show, (1) that the polynomial matrix $\mathbf{C} \in \mathrm{M}_p(k[\boldsymbol{x}])$ is unimodular, and (2) that $\bar{\mathbf{A}}$ ia really a unimodular completion of $\mathbf{A}$, i.e. the first q columns of $\bar{\mathbf{A}} := \mathbf{C}^{-1}$ make $\mathbf{A}$.

To show (1), just note that the row vectors of $\mathbf{C}$ span the free module $(k[\boldsymbol{x}])^p = \mathrm{Im}(\beta) \oplus \mathrm{Ker}(\alpha) \simeq (k[\boldsymbol{x}])^q \oplus (k[\boldsymbol{x}])^{p-q}$ since the first q rows span $\mathrm{Im}(\beta)$ and the rest of the rows span $\mathrm{Ker}(\alpha)$.

To show (2), note that

$$\begin{aligned}
\mathbf{CA} &= \begin{pmatrix} \mathbf{B} \\ \mathbf{S} \end{pmatrix} \mathbf{A} \\
&= \begin{pmatrix} \mathbf{I}_q \\ \mathbf{0} \end{pmatrix} \in \mathrm{M}_{pq}(k[\boldsymbol{x}])
\end{aligned}$$

implies

$$\mathbf{A} = \mathbf{C}^{-1} \begin{pmatrix} \mathbf{I}_q \\ \mathbf{0} \end{pmatrix}.$$

Therefore, for each $1 \leq i \leq q$,

$$\begin{aligned}
i\text{-th column of } \mathbf{A} &= \mathbf{A}\mathbf{e}_i \\
&= \mathbf{C}^{-1} \begin{pmatrix} \mathbf{I}_q \\ \mathbf{0} \end{pmatrix} \mathbf{e}_i \\
&= i\text{-th column of } \mathbf{C}^{-1},
\end{aligned}$$

i.e. the first q columns of $\bar{\mathbf{A}} := \mathbf{C}^{-1}$ are same as the q columns of $\mathbf{A}$ as desired.

3.3 Examples

Example 3.3.1 Define four polynomials in $k[x,y,z]$ by

$$\begin{aligned} f_1 &= 1-xy-2z-4xz-x^2z-2xyz+2x^2y^2z-2xz^2-2x^2z^2+2x^2yz^2 \\ f_2 &= 2+4x+x^2+2xy-2x^2y^2+2xz+2x^2z-2x^2yz \\ f_3 &= 1+2x+xy-x^2y^2+xz+x^2z-x^2yz \\ f_4 &= 2+x+y-xy^2+z-xyz. \end{aligned}$$

Verify that the polynomial vector $\mathbf{v} := (f_1, f_2, f_3, f_4)^t \in (k[x,y,z])^4$ is unimodular and find a unimodular completion of $\mathbf{v}$. Defining a projective module $\mathcal{M} \subset (k[x,y,z])^4$ by $\langle \mathbf{v} \rangle \oplus \mathcal{M} = (k[x,y,z])^4$, find a free basis of $\mathcal{M}$ whose existence is guaranteed by the Quillen-Suslin Theorem.

- **Step 1:** The following SINGULAR script computes a Gröbner basis `G` of the ideal $\langle f_1, f_2, f_3, f_4 \rangle$ w.r.t. the reverse degree lexicographic order, and the transformation matrix `T` such that `G` $= (f_1, f_2, f_3, f_4)$`T`, and a syzygy basis `G` of $\{f_1, f_2, f_3, f_4\}$.

```
ring r=0,(x,y,z),(c,dp);
poly f(1)=1-x*y-2*z-4*x*z-x2*z-2*x*y*z+2*x2*y2*z-2*x*z2-2*x2*z2
+2*x2*y*z2;
poly f(2)=2+4*x+x2+2*x*y-2*x2*y2+2*x*z+2*x2*z-2*x2*y*z;
poly f(3)=1+2*x+x*y-x2*y2+x*z+x2*z-x2*y*z;
poly f(4)=2+x+y-x*y2+z-x*y*z;
ideal I=f(1),f(2),f(3),f(4);
ideal G=std(I); matrix T=lift(I,G); module S=syz(I);
```

Now SINGULAR responds with

```
> G;
G[1]=1

> T;
T[1,1]=0
```

```
T[2,1]=-1z+1
T[3,1]=2z-1
T[4,1]=-1x
```

The relation $\mathtt{G} = (f_1, f_2, f_3, f_4)\mathtt{T} = 1$ implies $\mathtt{T}^t\mathbf{v} = 1$, and thus $\mathbf{v}$ is unimodular, and

$$\mathbf{B} = \mathtt{T}^t = (0, -z+1, 2z-1, -x)$$

is a particular left inverse.

- **Step 2:** In order to find a unimodular completion of the column vector $\mathbf{v}$, we need to find a syzygy basis of $\{f_1, f_2, f_3, f_4\}$.

```
> S;
S[1]=[0,x2z-1x2+1,-2x2z+x2-2,x3]
S[2]=[1,-1xyz+xy+2z-1,2xyz-1xy-2z+1,-1x2y+x]
S[3]=[-1y-1z,xz-1yz-1z2-1x+2z-2,-2xz+x-4z+2,x2+2x+1]
```

Therefore,

$$\begin{aligned}\mathbf{C} &= \begin{pmatrix}\mathbf{B}\\ \mathbf{S}\end{pmatrix}\\ &= \begin{pmatrix} 0 & -z+1 & 2z-1 & -x \\ 0 & x^2z-x^2+1 & -2x^2z+x^2-2 & x^3 \\ 1 & -xyz+xy+2z-1 & 2xyz-xy-2z+1 & -x^2y+x \\ -y-z & xz-yz-z2-x+2z-2 & -2xz+x-4z+2 & x^2+2x+1 \end{pmatrix}.\end{aligned}$$

- **Step 3:** One checks easily that $\det(\mathbf{C}) = -1$, i.e. $\mathbf{C}$ is unimodular, and the resulting unimodular completion of $\mathbf{v}$ is

$$\begin{aligned}\bar{\mathbf{A}} &= \mathbf{C}^{-1}\\ &= \begin{pmatrix} f_1 & z-2z^2 & 1-2xyz-2xz^2 & -2xz \\ f_2 & -1+2z & 2xy+2xz & 2x \\ f_3 & -1+z & xy+xz & x \\ f_4 & 0 & y+z & 1 \end{pmatrix}.\end{aligned}$$

The three column vectors of $\bar{\mathbf{A}}$ other than the first make a free basis of the rank 3 free module $\mathcal{M} \subset (k[x,y,z])^4$ which is the complement of the rank 1 submodule $\langle\mathbf{v}\rangle := k[x,y,z]\mathbf{v} \subset (k[x,y,z])^4$, i.e. $\langle\mathbf{v}\rangle \oplus \mathcal{M} = (k[x,y,z])^4$.

□

Example 3.3.2 Consider the two polynomial vectors $\mathbf{v}_1, \mathbf{v}_2 \in (k[x,y,z])^3$ given by

$$\begin{aligned} \mathbf{v}_1 &:= \begin{pmatrix} xy - y + 1 \\ yz + w \\ -y \end{pmatrix} \\ \mathbf{v}_2 &:= \begin{pmatrix} 1 - x \\ -z \\ 1 \end{pmatrix}. \end{aligned}$$

Verify that the $k[x,y,z]$-module $\mathcal{M} \subset (k[x,y,z])^3$ generated by $\mathbf{v}_1$ and $\mathbf{v}_1$ splits as a rank 2 direct summand of the free module $(k[x,y,z])^3$. Also, find the $k[x,y,z]$-module $\mathcal{N} \subset (k[x,y,z])^3$ such that $\mathcal{M} \oplus \mathcal{N} = (k[x,y,z])^3$.

We have to show the unimodularity of the matrix $\mathbf{A} := \begin{pmatrix} xy - y + 1 & 1 - x \\ yz + w & -z \\ -y & 1 \end{pmatrix}$, and find a unimodular completion $\bar{\mathbf{A}}$ of $\mathbf{A}$. Then the last column vector of $\bar{\mathbf{A}}$ generates $\mathcal{N}$.

Our SINGULAR script for this purpose goes as follows.

```
ring r=0,(x,y,z,w),(c,dp);option(redSB);
vector v(1)=[xy-y+1,1-x];vector v(2)=[yz+w,-z];vector v(3)=[-y,1];
module M=v(1),v(2),v(3);
module G=std(M); matrix T=lift(M,G); module S=syz(M);
```

And the results are

```
> G;
G[1]=[0,1]
G[2]=[1]

> T;
T[1,1]=y
T[1,2]=1
T[2,1]=0
T[2,2]=0
T[3,1]=xy-1y+1
T[3,2]=x-1
```

```
> S;
S[1]=[w,-1,xw-1z-1w]
```

Since $\{(1,0),(0,1)\}$ is a Gröbner basis of the row vectors of $\mathbf{A}$, $\mathbf{A}$ is unimodular, and the relation $\mathtt{G} = \mathtt{MT}$ translates to

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \mathbf{A}^t\mathtt{T}.$$

By taking transpose of both sides, we get $\mathtt{T}^t\mathbf{A} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, i.e.

$$\begin{pmatrix} 1 & 0 & x-1 \\ y & 0 & xy-y+1 \end{pmatrix} \mathbf{A} = \mathbf{I}_2.$$

Hence, $\mathbf{B} := \begin{pmatrix} 1 & 0 & x-1 \\ y & 0 & xy-y+1 \end{pmatrix}$ is a left inverse of $\mathbf{A}$, and

$$\begin{aligned} \mathbf{C} &= \begin{pmatrix} \mathbf{B} \\ \mathbf{S} \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 & x-1 \\ y & 0 & xy-y+1 \\ w & -1 & xw-z-w \end{pmatrix}. \end{aligned}$$

The resulting unimodular completion of $\mathbf{A}$ is

$$\begin{aligned} \bar{\mathbf{A}} &= \mathbf{C}^{-1} \\ &= \begin{pmatrix} 1-y+xy & 1-x & 0 \\ w+yz & -z & -1 \\ -y & 1 & 0 \end{pmatrix}. \end{aligned}$$

□

Chapter 4

An Algorithmic Proof of Suslin's Stability Theorem

Over a field k, Gaussian elimination tells us that we can repeatedly apply elementary row and column operations to reduce any matrix in $\mathrm{SL}_n(k)$ to the identity matrix $\mathbf{I}_n$, where the standard linear group $\mathrm{SL}_n(k)$ denotes the group of all the $n \times n$ matrices of determinant 1 whose entries are elements of k.

Less obvious but still true is that, due to the Euclidean Division Algorithm for $k[x]$, this elementary reduction is also possible for the matrices with entries from the univariate polynomial ring $k[x]$.

Even more strikingly, while the Euclidean Division Algorithm is not valid any more for the multivariate polynomial ring $k[\boldsymbol{x}] := k[x_1, \ldots, x_m]$, Suslin's Stability Theorem states that the same is true for $\mathrm{SL}_n(k[\boldsymbol{x}])$ with $n \geq 3$ and $m \geq 1$.

Definition 4.0.3 *A square matrix* $\mathbf{A}$ *over a ring* R *is called* **realizable**, *if* $\mathbf{A}$ *can be written as a product of elementary matrices over* R.

Recall that for any ring R, an $n \times n$ elementary matrix $\mathbf{E}_{ij}(a)$ over R is a matrix of the form $\mathbf{I}_n + a \cdot \mathbf{E}_{ij}$ where $i \neq j, a \in R$ and $\mathbf{E}_{ij}$ is the $n \times n$ matrix whose (i, j) entry is 1 and all other entries are zero. Now letting $\mathrm{E}_n(R)$ be the subgroup of $\mathrm{SL}_n(R)$ generated

After it was discovered that Cynthia Woodburn [Woo94] obtained the result of this chapter independently of the author at the same time, she and the author started collaborating and wrote a joint paper [PW94] based on the collaboration. The result of this section will be extended, in Chapter 11, to the case of Laurent polynomial rings.

by the elementary matrices, for a commutative coefficient ring R, Suslin's stability theorem can be expressed as

$$\mathrm{SL}_n(R[x_1,\ldots,x_m]) = \mathrm{E}_n(R[x_1,\ldots,x_m]) \quad \text{for all } n \geq \max(3, \dim(R)+2).$$

When the coefficient ring is a field $R = k$, this is equivalent to saying that any $n \times n$ ($n \geq 3$) unimodular matrix is realizable. Therefore, the algorithm to be developed in this chapter could be called a realization algorithm.

This chapter is organized as follows.

- In Section 4.1, an algorithmic proof of the normality of $\mathrm{E}_n(k[\boldsymbol{x}])$ as a subgroup of $\mathrm{SL}_n(k[\boldsymbol{x}])$ for $n \geq 3$ is given. Nonconstructive proofs of the results in this section can be found elsewhere, e.g. [Sus77] or [Vas81].

- In Section 4.2, we give an algorithm for the *Quillen Induction Process*, a standard way of reducing a given problem over a ring to an easier problem over a local ring. Using this *Quillen Induction Algorithm*, we reduce our realization problem over the polynomial ring $R[x_m]$ to one over $R_{\mathfrak{M}}[x_m]$'s, where $R = k[x_1,\ldots,x_{m-1}]$ and $\mathfrak{M}$ ranges over a finite set of maximal ideals of R.

- In Section 4.3, an algorithmic proof of the *Elementary Column Property*, a stronger version of the *Unimodular Column Property*, is given, and we note that this algorithm gives another constructive proof of the Quillen-Suslin theorem. Using the *Elementary Column Property*, we show that a realization algorithm for $\mathrm{SL}_n(k[\boldsymbol{x}])$ is obtained from a realization algorithm for matrices of the special form

$$\begin{pmatrix} p & q & 0 \\ r & s & 0 \\ 0 & 0 & 1 \end{pmatrix} \in \mathrm{SL}_3(k[\boldsymbol{x}]),$$

where p is monic in the last variable x_m (note $\boldsymbol{x} := (x_1,\ldots,x_m)$).

- In Section 4.4, in view of the results in the preceding two sections, we note that a realization algorithm over $k[\boldsymbol{x}] = k[x_1,\ldots,x_m]$ can be obtained from a realization algorithm for the matrices of the special form $\begin{pmatrix} p & q & 0 \\ r & s & 0 \\ 0 & 0 & 1 \end{pmatrix}$ over $R[X]$, where R is now a local ring and p is monic in X. A realization algorithm for this case found by M.P. Murthy in [GM80] is reproduced in this section.

4.1 E_n is normal in SL_n, for $n \geq 3$

Lemma 4.1.1 *The Cohn matrix* $\mathbf{A} = \begin{pmatrix} 1+xy & x^2 \\ -y^2 & 1-xy \end{pmatrix}$ *is not realizable, but* $\begin{pmatrix} \mathbf{A} & 0 \\ 0 & 1 \end{pmatrix}$ $\in \mathrm{SL}_3(k[x,y])$ *is.*

Proof: The nonrealizability of $\mathbf{A}$ was first proved by P. M. Cohn in [Coh66], and a complete algorithmic criterion for the realizability of matrices in $\mathrm{SL}_2(k[x_1,\ldots,x_m])$ will be developed in Chapter 5.

Now noting that

$$\begin{pmatrix} \mathbf{A} & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1+xy & x^2 & 0 \\ -y^2 & 1-xy & 0 \\ 0 & 0 & 1 \end{pmatrix} = \mathbf{I}_3 + \begin{pmatrix} x \\ -y \\ 0 \end{pmatrix} \cdot (y,x,0),$$

we see that the realizability of this matrix is a special case of Lemma 4.1.3 below. □

Definition 4.1.2 *Let $n \geq 2$. A* **Cohn-type matrix** *is a matrix of the form*

$$\mathbf{I}_n + a\mathbf{v}(v_j\mathbf{e}_i - v_i\mathbf{e}_j)^t, \quad i < j \in \{1,\ldots,n\},$$

where $\mathbf{v} = (v_1,\ldots,v_n)^t \in (k[\boldsymbol{x}])^n$, $a \in k[\boldsymbol{x}]$, and $\mathbf{e}_i = (0,\ldots,0,1,0,\ldots,0)^t$ with 1 occurring only at the i-th position.

Lemma 4.1.3 *(Mennicke) Any Cohn-type matrix for $n \geq 3$ is realizable.*

Proof: First, consider the case $i = 1, j = 2$. In this case,

$$\begin{aligned}
\mathbf{B} &= \mathbf{I}_n + a \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} (v_2, -v_1, 0, \ldots, 0) \\
&= \begin{pmatrix} 1+av_1v_2 & -av_1^2 & 0 & \cdots & 0 \\ av_2^2 & 1-av_1v_2 & 0 & \cdots & 0 \\ av_3v_2 & -av_3v_1 & & & \\ \vdots & \vdots & & I_{n-2} & \\ av_nv_2 & -av_nv_1 & & & \end{pmatrix} \\
&= \begin{pmatrix} 1+av_1v_2 & -av_1^2 & 0 & \cdots & 0 \\ av_2^2 & 1-av_1v_2 & 0 & \cdots & 0 \\ 0 & 0 & & & \\ \vdots & \vdots & & I_{n-2} & \\ 0 & 0 & & & \end{pmatrix} \prod_{l=3}^{n} \mathbf{E}_{l1}(av_lv_2)\mathbf{E}_{l2}(-av_lv_1).
\end{aligned}$$

So, it is enough to show that

$$\mathbf{A} = \begin{pmatrix} 1+av_1v_2 & -av_1^2 & 0 \\ av_2^2 & 1-av_1v_2 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

is realizable for any $a, v_1, v_2 \in k[\boldsymbol{x}]$. Let "$\to$" indicate that we are applying elementary operations, and consider the following:

$$\begin{aligned} \mathbf{A} &= \begin{pmatrix} 1+av_1v_2 & -av_1^2 & 0 \\ av_2^2 & 1-av_1v_2 & 0 \\ 0 & 0 & 1 \end{pmatrix} \to \begin{pmatrix} 1+av_1v_2 & -av_1^2 & v_1 \\ av_2^2 & 1-av_1v_2 & v_2 \\ 0 & 0 & 1 \end{pmatrix} \\ &\to \begin{pmatrix} 1 & -av_1^2 & v_1 \\ 0 & 1-av_1v_2 & v_2 \\ -av_2 & 0 & 1 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & v_1 \\ 0 & 1 & v_2 \\ -av_2 & av_1 & 1 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & v_1 \\ 0 & 1 & v_2 \\ 0 & av_1 & 1+av_1v_2 \end{pmatrix} \\ &\to \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & v_2 \\ 0 & av_1 & 1+av_1v_2 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & v_2 \\ 0 & 0 & 1 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}. \end{aligned} \tag{4.1}$$

Keeping track of all the elementary operations involved in 4.1, we get

$$\mathbf{A} = \mathbf{E}_{13}(-v_1)\mathbf{E}_{23}(-v_2)\mathbf{E}_{31}(-av_2)\mathbf{E}_{32}(av_1)\mathbf{E}_{13}(v_1)\mathbf{E}_{23}(v_2)\mathbf{E}_{31}(av_2)\mathbf{E}_{32}(-av_1).$$

In general (i.e., for arbitrary $i < j$),

$$\mathbf{B} = \mathbf{I}_n + a \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} (0, \ldots, 0, v_j, 0, \ldots, 0, -v_i, 0, \ldots, 0)$$

with v_j occurring at the i-th position and $-v_i$ occurring at the j-th position. Therefore, we have

$$\mathbf{B} = \begin{pmatrix} 1 & \cdots & av_1v_j & \cdots & -av_1v_i & \cdots & 0 \\ & \ddots & \vdots & & \vdots & & 0 \\ & & 1+av_iv_j & & -av_i^2 & & \\ & & \vdots & & \vdots & & \\ & & av_j^2 & & 1-av_iv_j & & \\ & & \vdots & & \vdots & & \\ & & v_nv_j & & -v_nv_i & & 1 \end{pmatrix}$$

$$
\begin{aligned}
&= \begin{pmatrix}
1 & \cdots & 0 & \cdots & 0 & \cdots & 0 \\
 & \ddots & \vdots & & \vdots & & 0 \\
 & & 1 + av_iv_j & & -av_i^2 & & \\
 & & \vdots & & \vdots & & \\
 & & av_j^2 & & 1 - av_iv_j & & \\
 & & \vdots & & \vdots & & \\
 & & 0 & & 0 & & 1
\end{pmatrix} \cdot \prod_{\substack{1 \le l \le n \\ l \ne i,j}} \mathbf{E}_{li}(av_lv_j)\mathbf{E}_{lj}(-av_lv_i) \\
&= \mathbf{E}_{it}(-v_i)\mathbf{E}_{jt}(-v_j)\mathbf{E}_{ti}(-av_j)\mathbf{E}_{tj}(av_i)\mathbf{E}_{it}(v_i)\mathbf{E}_{jt}(v_j)\mathbf{E}_{ti}(av_j)\mathbf{E}_{tj}(-av_i) \\
&\quad \cdot \prod_{\substack{1 \le l \le n \\ l \ne i,j}} \mathbf{E}_{li}(av_lv_j)\mathbf{E}_{lj}(-av_lv_i),
\end{aligned}
$$

where $t \in \{1, \ldots, n\}$ can be chosen to be any number other than i or j. □

Since a Cohn-type matrix is realizable, any product of Cohn-type matrices is also realizable. This observation motivates the following generalization of the above lemma.

Lemma 4.1.4 *(Suslin) Suppose that $\mathbf{A} \in \mathrm{SL}_n(k[\boldsymbol{x}])$ with $n \ge 3$ can be written in the form $\mathbf{A} = \mathbf{I} + \mathbf{v}\mathbf{w}^t$ for unimodular column vectors $\mathbf{v}, \mathbf{w} \in (k[\boldsymbol{x}])^n$ such that $\mathbf{w}^t\mathbf{v} = 0 \in k[\boldsymbol{x}]$. Then A is realizable.*

Proof: Since $\mathbf{v} = (v_1, \ldots, v_n)^t$ is unimodular, we can use the effective Nullstellensatz or Gröbner bases to find $g_1, \ldots, g_n \in k[\boldsymbol{x}]$ such that $v_1g_1 + \cdots + v_ng_n = 1$.

This, combined with $\mathbf{w}^t\mathbf{v} = w_1v_1 + \cdots + w_nv_n = 0$, yields a new expression for $\mathbf{w}$:

$$
\mathbf{w} = \sum_{i<j} a_{ij}(v_j\mathbf{e}_i - v_i\mathbf{e}_j)
$$

where $a_{ij} = w_ig_j - w_jg_i$. Now,

$$
\begin{aligned}
\mathbf{A} &= \mathbf{I}_n + \mathbf{v}\left(\sum_{i<j} a_{ij}(v_j\mathbf{e}_i - v_i\mathbf{e}_j)\right)^t \\
&= \mathbf{I}_n + \sum_{i<j} \mathbf{v}a_{ij}(v_j\mathbf{e}_i - v_i\mathbf{e}_j)^t \\
&= \prod_{i<j} \left(I + \mathbf{v}a_{ij}(v_j\mathbf{e}_i - v_i\mathbf{e}_j)^t\right).
\end{aligned}
$$

Each factor on the right hand side of this equation is a Cohn-type matrix and thus realizable, so A is also realizable. □

Corollary 4.1.5 $\mathbf{B}\mathbf{E}_{ij}(a)\mathbf{B}^{-1}$ *is realizable for any* $\mathbf{B} \in \mathrm{GL}_n(k[\boldsymbol{x}])$ *with* $n \geq 3$ *and* $a \in k[\boldsymbol{x}]$.

Proof: Note that $i \neq j$, and

$$\mathbf{B}\mathbf{E}_{ij}(a)\mathbf{B}^{-1} = \mathbf{I}_n + (i\text{-th column vector of } \mathbf{B})a(j\text{-th row vector of } \mathbf{B}^{-1}).$$

Let $\mathbf{v}$ be the i-th column vector of $\mathbf{B}$ and $\mathbf{w}^t$ be a times the j-th row vector of $\mathbf{B}^{-1}$. Then (i-th row vector of $\mathbf{B}^{-1}$)$\cdot \mathbf{v} = 1$ implies $\mathbf{v}$ is unimodular, and $\mathbf{w}^t\mathbf{v}$ is clearly zero since $i \neq j$. Therefore, $\mathbf{B}\mathbf{E}_{ij}(a)\mathbf{B}^{-1} = \mathbf{I}_n + \mathbf{v}\mathbf{w}^t$ satisfies the condition of the above lemma, and is thus realizable. $\square$

Corollary 4.1.6 $\mathrm{E}_n(k[\boldsymbol{x}])$ *is a normal subgroup of* $\mathrm{GL}_n(k[\boldsymbol{x}])$, *for* $n \geq 3$.

Proof: Let $\mathbf{A} \in \mathrm{GL}_n(k[\boldsymbol{x}])$ and $\mathbf{E} \in \mathrm{E}_n(k[\boldsymbol{x}])$. Then the above corollary gives us an algorithm for finding elementary matrices $\mathbf{E}_1, \ldots, \mathbf{E}_t$ such that $\mathbf{A}^{-1}\mathbf{E}\mathbf{A} = \mathbf{E}_1 \cdots \mathbf{E}_t$. $\square$

4.2 Gluing of Local Realizability

Let $R = k[x_1, \ldots, x_{m-1}]$, $X = x_m$ and $\mathfrak{M} \in \mathrm{Max}(R)$ ={maximal ideals of R}. For $\mathbf{A} \in \mathrm{SL}_n(R[X])$, we let $\mathbf{A}_{\mathfrak{M}} \in \mathrm{SL}_n(R_{\mathfrak{M}}[X])$ be its image under the canonical mapping $\mathrm{SL}_n(R[X]) \to \mathrm{SL}_n(R_{\mathfrak{M}}[X])$. We will occasionally write $\mathbf{A} = \mathbf{A}(X)$ to emphasize that we are viewing the entries of the matrix $\mathbf{A}$ as polynomials in one variable. Now consider the following analogue of Quillen's patching theorem for elementary matrices:

> Suppose $n \geq 3$ and $\mathbf{A} \in \mathrm{SL}_n(R[X])$. Then $\mathbf{A}$ is realizable over $R[X]$ if and only if $\mathbf{A}_{\mathfrak{M}} \in \mathrm{SL}_n(R_{\mathfrak{M}}[X])$ is realizable over $R_{\mathfrak{M}}[X]$ for every $\mathfrak{M} \in \mathrm{Max}(R)$.

While a non-constructive proof of this assertion is given in [Sus77] and a more general functorial treatment of this Quillen Induction Process can be found in [Knu91], we will give a constructive proof for it here, thus providing a patching algorithm with input certain local factorizations of a given matrix A and output a global factorization of A into elementary matrices. Since the necessity of the condition is clear, we have to prove the following theorem.

Theorem 4.2.1 *(Quillen Induction Algorithm) Let* $\mathbf{A} \in \mathrm{SL}_n(R[X])$. *If* $\mathbf{A}_{\mathfrak{M}} \in \mathrm{E}_n(R_{\mathfrak{M}}[X])$ *for every* $\mathfrak{M} \in \mathrm{Max}(R)$, *then* $\mathbf{A} \in \mathrm{E}_n(R[X])$.

Proof: Let $\mathbf{a}_1 = (0, \ldots, 0) \in k^{m-1}$, and let $\mathfrak{M}_1 = \{g \in k[x_1, \ldots, x_{m-1}] \mid g(\mathbf{a}_1) = 0\}$ be the corresponding maximal ideal. Then by assumption, $\mathbf{A}_{\mathfrak{M}_1}$ is realizable over $R_{\mathfrak{M}_1}[X]$. Hence, we can write

$$\mathbf{A}_{\mathfrak{M}_1} = \prod_j \mathbf{E}_{s_j t_j}\left(\frac{c_j}{d_j}\right) \tag{4.2}$$

where $c_j, d_j \in R, d_j \notin \mathfrak{M}_1$. Letting $r_1 = \prod_j d_j \notin \mathfrak{M}_1$, we can rewrite 4.2 as

$$\mathbf{A}_{\mathfrak{M}_1} = \prod_j \mathbf{E}_{s_j t_j}\left(\frac{c_j \prod_{k \neq j} d_k}{r_1}\right) \in \mathrm{E}_n(R_{r_1}) \subset \mathrm{E}_n(R_{\mathfrak{M}_1}).$$

Denote an algebraic closure of k by $\bar{k}$. Inductively, let $\mathbf{a}_j \in \bar{k}^{m-1}$ be a common zero of $r_1, \ldots, r_{j-1}$ and $\mathfrak{M}_j = \{g \in k[x_1, \ldots, x_{m-1}] \mid g(\mathbf{a}_j) = 0\}$ be the corresponding maximal ideal of R for each $j \geq 2$. (See Chapter 3 of [CLO92] for details and references for using Gröbner bases to find a common zero of a finite set of polynomials.) Define $r_j \notin \mathfrak{M}_j$ in the same way as r_1 above, so that

$$\mathbf{A}_{\mathfrak{M}_j} \in \mathrm{E}_n(R_{r_j}[X]).$$

Since $\mathbf{a}_j$ is a common zero of $r_1, \ldots, r_{j-1}$ in this construction, we immediately see that $r_1, \ldots, r_{j-1} \in \mathfrak{M}_j = \{g \in R \mid g(\mathbf{a}_j) = 0\}$. But noting $r_j \notin \mathfrak{M}_j$, we conclude that $r_j \notin r_1R + \cdots + r_{j-1}R$. Now, since R is Noetherian, we will get to some l after a finite number of steps such that $r_1R + \cdots + r_lR = R$. (We can use Gröbner bases to determine when 1_R is in the ideal $r_1R + \cdots + r_lR$, e.g. see [CLO92, p. 94].)

Let d be a natural number. Then since $r_1^dR + \cdots + r_l^dR = R$, we can find $g_1, \ldots, g_l \in R$ such that $r_1^dg_1 + \cdots + r_l^dg_l = 1$. Now, we express $\mathbf{A}(X) \in \mathrm{SL}_n(R[X])$ in the following way:

$$\begin{aligned}
\mathbf{A}(X) &= \mathbf{A}(X - Xr_1^dg_1) \cdot [\mathbf{A}^{-1}(X - Xr_1^dg_1)A(X)] \\
&= \mathbf{A}(X - Xr_1^dg_1 - Xr_2^dg_2) \cdot [\mathbf{A}^{-1}(X - Xr_1^dg_1 - Xr_2^dg_2)\mathbf{A}(X - Xr_1^dg_1)] \\
&\quad \cdot [\mathbf{A}^{-1}(X - Xr_1^dg_1)\mathbf{A}(X)] \\
&= \cdots \\
&= \mathbf{A}(X - \sum_{i=1}^{l} Xr_i^dg_i) \cdot [\mathbf{A}^{-1}(X - \sum_{i=1}^{l} Xr_i^dg_i)\mathbf{A}(X - \sum_{i=1}^{l-1} Xr_i^dg_i)] \cdots \\
&\quad \cdots [\mathbf{A}^{-1}(X - Xr_1^dg_1)\mathbf{A}(X)].
\end{aligned}$$

Note here that the first matrix $\mathbf{A}(X-\sum_{i=1}^{l} X r_i^d g_i) = \mathbf{A}(0)$ on the right hand side is in $\mathrm{E}_n(R)$ by the induction hypothesis. We will now show that for a sufficiently large d, each bracketed expression in the above equation is actually in $\mathrm{E}_n(R[X])$, so that A itself is in $\mathrm{E}_n(R[X])$. To this end, we let $\mathbf{A}_{\mathfrak{M}_i} = \mathbf{A}_i$ and identify $\mathbf{A} \in \mathrm{SL}_n(R[X])$ with $\mathbf{A}_i \in \mathrm{SL}_n(R_{\mathfrak{M}_i}[X])$. Then each bracketed expression is of the form

$$\mathbf{A}_i^{-1}(cX)\mathbf{A}_i((c+r_i^d g)X).$$

Claim: For any $c, g \in R$, we can find a sufficiently large d such that $\mathbf{A}_i^{-1}(cX)\mathbf{A}_i((c+r_i^d g)X) \in \mathrm{E}_n(R[X])$ for $i = 1, \ldots, l$.

Let

$$\mathbf{D}_i(X,Y,Z) = \mathbf{A}_i^{-1}(Y \cdot X)\mathbf{A}_i((Y+Z)\cdot X) \in \mathrm{E}_n(R_{r_i}[X,Y,Z])$$

and write $\mathbf{D}_i$ in the form

$$\mathbf{D}_i = \prod_{j=1}^{h} \mathbf{E}_{s_j t_j}(b_j + Z f_j)$$

where $b_j \in R_{r_i}[X,Y]$ and $f_j \in R_{r_i}[X,Y,Z]$. From now on, the elementary matrix $\mathbf{E}_{s_j t_j}(a)$ will be simply denoted as $\mathbf{E}^j(a)$ for notational convenience. For $p = 1, \ldots, h$, define $\mathbf{C}_p$ by

$$\mathbf{C}_p = \prod_{j=1}^{p} \mathbf{E}^j(b_j) \in \mathrm{E}_n(R_{r_i}[X,Y]).$$

Then the $\mathbf{C}_p$'s satisfy the following recursive relations:

$$\begin{aligned}
\mathbf{E}^1(b_1) &= \mathbf{C}_1, \\
\mathbf{E}^p(b_p) &= \mathbf{C}_{p-1}^{-1}\mathbf{C}_p \quad (2 \le p \le h), \\
\mathbf{C}_h &= \mathbf{I}.
\end{aligned}$$

Hence, using the fact that $\mathbf{E}_{ij}(a+b) = \mathbf{E}_{ij}(a)\mathbf{E}_{ij}(b)$, we have

$$\begin{aligned}
\mathbf{D}_i &= \prod_{j=1}^{h} \mathbf{E}^j(b_j + Z f_j) \\
&= \prod_{j=1}^{h} \mathbf{E}^j(b_j)\mathbf{E}^j(Z f_j) \\
&= [\mathbf{E}^1(b_1)\mathbf{E}^1(Z f_1)][\mathbf{E}^2(b_2)\mathbf{E}^2(Z f_2)] \cdots [\mathbf{E}^h(b_h)\mathbf{E}^h(Z f_h)] \\
&= [\mathbf{C}_1\mathbf{E}^1(Z f_1)][\mathbf{C}_1^{-1}\mathbf{C}_2\mathbf{E}^2(Z f_2)] \cdots [\mathbf{C}_{h-1}^{-1}\mathbf{C}_h\mathbf{E}^h(Z f_h)] \\
&= \prod_{j=1}^{h} \mathbf{C}_j\mathbf{E}^j(Z f_j)\mathbf{C}_j^{-1}.
\end{aligned}$$

Now in the same way as in the proof of Lemma 4.1.4 and Corollary 4.1.5, we can write $\mathbf{C}_j\mathbf{E}^j(Zf_j)\mathbf{C}_j^{-1}$ as a product of Cohn-type matrices, i.e. for any given $j \in \{1, \ldots, h\}$, let $\mathbf{v} = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}$ be the s_j-th column vector of $\mathbf{C}_j$. Then

$$\mathbf{C}_j\mathbf{E}_{s_jt_j}(Zf_j)\mathbf{C}_j^{-1} = \prod_{1\le\gamma<\delta\le n} [\mathbf{I} + \mathbf{v}\cdot Zf_j \cdot a_{\gamma\delta}(v_\gamma\mathbf{e}_\delta - v_\delta\mathbf{e}_\gamma)]$$

for some $a_{\gamma\delta} \in R_{r_i}[X,Y]$. Also, we can find a natural number d such that

$$v_\gamma = \frac{v'_\gamma}{r_i^d}, \quad a_{\gamma\delta} = \frac{a'_{\gamma\delta}}{r_i^d}, \quad f_j = \frac{f'_j}{r_i^d}$$

for some $v'_\gamma, a'_{\gamma\delta} \in R[X,Y]$, $f'_j \in R[X,Y,Z]$. Now, replacing Z by $r_i^{4d}g$, we see that all the Cohn-type matrices in the above expression for $\mathbf{C}_j\mathbf{E}^j(Zf_j)\mathbf{C}_j^{-1}$ have denominator-free entries. Therefore,

$$\mathbf{C}_j\mathbf{E}^j(r_i^{4d}gf_j)\mathbf{C}_j^{-1} \in \mathrm{E}_n(R[X,Y]).$$

Since this is true for each j, we conclude that for a sufficiently large d,

$$\mathbf{D}_i(X,Y,r_i^dg) = \prod_{j=1}^{h} \mathbf{C}_j\mathbf{E}^j(r_i^dgf_j)\mathbf{C}_j^{-1} \in \mathrm{E}_n(R[X,Y]).$$

Now, setting $Y = c$ proves the claim, and completes the proof of the theorem. $\square$

4.3 Reduction to SL_3

Let $\mathbf{A} \in \mathrm{SL}_n(k[\boldsymbol{x}])$ with $n \ge 3$, and let $\mathbf{v}$ be its last column vector. Then $\mathbf{v}$ is unimodular. (Recall that the cofactor expansion along the last column gives a required relation.) Now, if we can reduce $\mathbf{v}$ to $\mathbf{e}_n = (0,0,\ldots,0,1)^t$ by applying elementary operations, i.e. if we can find $\mathbf{B} \in \mathrm{E}_n(k[\boldsymbol{x}])$ such that $\mathbf{B}\mathbf{v} = \mathbf{e}_n$, then

$$\mathbf{BA} = \begin{pmatrix} & & & 0 \\ & \tilde{\mathbf{A}} & & \vdots \\ & & & 0 \\ p_1 & \ldots & p_{n-1} & 1 \end{pmatrix}$$

for some $\tilde{\mathbf{A}} \in \mathrm{SL}_{n-1}(k[\boldsymbol{x}])$ and $p_i \in k[\boldsymbol{x}]$ for $i = 1, \ldots, n-1$. Hence,

$$\mathbf{BAE}_{n1}(-p_1) \cdots \mathbf{E}_{n(n-1)}(-p_{n-1}) \quad = \quad \begin{pmatrix} \tilde{\mathbf{A}} & 0 \\ 0 & 1 \end{pmatrix}.$$

Therefore, our problem of expressing $\mathbf{A} \in \mathrm{SL}_n(k[\boldsymbol{x}])$ as a product of elementary matrices is now reduced to the same problem for $\tilde{\mathbf{A}} \in \mathrm{SL}_{n-1}(k[\boldsymbol{x}])$. By repeating this process, we get to the problem of expressing $\mathbf{A} = \begin{pmatrix} p & q & 0 \\ r & s & 0 \\ 0 & 0 & 1 \end{pmatrix} \in \mathrm{SL}_3(k[\boldsymbol{x}])$ as a product of elementary matrices, which is the subject of the next section.

In this section, we will develop an algorithm for finding elementary operations that reduce a given unimodular column vector $\mathbf{v} \in (k[\boldsymbol{x}])^n$ to $\mathbf{e}_n$. Also, as a corollary to this Elementary Column Property, we give an algorithmic proof of the Unimodular Column Property which states that for any given unimodular column vector $\mathbf{v} \in (k[\boldsymbol{x}])^n$, there exists a unimodular matrix $\mathbf{B}$, i.e. a matrix with constant nonzero determinant, over $k[\boldsymbol{x}]$ such that $\mathbf{Bv} = \mathbf{e}_n$. Therefore, our algorithm gives another constructive proof of the Quillen-Suslin theorem.

Definition 4.3.1 *For a ring R, $\mathrm{Um}_n(R) = \{$n-dimensional unimodular column vectors over $R\}$.*

As in Section 4.2, let $R = k[x_1, \ldots, x_{m-1}]$ and $X = x_m$. Then $k[x_1, \ldots, x_m] = R[X]$. By identifying $\mathbf{A} \in \mathrm{SL}_2(R[X])$ with $\begin{pmatrix} \mathbf{A} & 0 \\ 0 & I_{n-2} \end{pmatrix} \in \mathrm{SL}_n(R[X])$, we can regard $\mathrm{SL}_2(R[X])$ as a subgroup of $\mathrm{SL}_n(R[X])$. As before, we use the notation $\mathbf{A} = \mathbf{A}(X)$ and $\mathbf{v} = \mathbf{v}(X)$ to emphasize that we are viewing the entries of a matrix $\mathbf{A}$ or a vector $\mathbf{v}$ as polynomials in one variable. Now consider the following lemma and theorem, which will be used to prove the Elementary Column Property.

Lemma 4.3.2 *Let $f_1, f_2, b, d \in R[X]$ and let $r \in R$ be the resultant of f_1 and f_2. Then there exists $\mathbf{B} \in \mathrm{SL}_2(R[X])$ such that*

$$\mathbf{B}\begin{pmatrix} f_1(b) \\ f_2(b) \end{pmatrix} \quad = \quad \begin{pmatrix} f_1(b+rd) \\ f_2(b+rd) \end{pmatrix}.$$

Proof: By a property of the resultant of two polynomials, we can find $g_1, g_2 \in R[X]$ such that $f_1g_1 + f_2g_2 = r$. (See [CLO92, Prop. 3.5.9] or [GM80, p. 28] for details.) Let

$s_1, s_2, t_1, t_2 \in R[X, Y, Z]$ be the polynomials defined by

$$\begin{aligned}
f_1(X+YZ) &= f_1(X) + Ys_1(X,Y,Z), \\
f_2(X+YZ) &= f_2(X) + Ys_2(X,Y,Z), \\
g_1(X+YZ) &= g_1(X) + Yt_1(X,Y,Z), \\
g_2(X+YZ) &= g_2(X) + Yt_2(X,Y,Z).
\end{aligned}$$

Now, define

$$\begin{aligned}
B_{11} &= 1 + s_1(b,r,d)\cdot g_1(b) + t_2(b,r,d)\cdot f_2(b), \\
B_{12} &= s_1(b,r,d)\cdot g_2(b) - t_2(b,r,d)\cdot f_1(b), \\
B_{21} &= s_2(b,r,d)\cdot g_1(b) - t_1(b,r,d)\cdot f_2(b), \\
B_{22} &= 1 + s_2(b,r,d)\cdot g_2(b) + t_1(b,r,d)\cdot f_1(b).
\end{aligned}$$

Then one checks easily that $\mathbf{B} := \begin{pmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{pmatrix}$ satisfies the desired property and that $\mathbf{B} \in \mathrm{SL}_2(R[X])$. □

Theorem 4.3.3 *Suppose* $\mathbf{v}(X) = \begin{pmatrix} v_1(X) \\ \vdots \\ v_n(X) \end{pmatrix} \in \mathrm{Um}_n(R[X])$, *and* $v_1(X)$ *is monic in* X. *Then there exists* $\mathbf{B}_1 \in \mathrm{SL}_2(R[X])$ *and* $\mathbf{B}_2 \in E_n(R[X])$ *such that* $\mathbf{B}_1\mathbf{B}_2 \cdot \mathbf{v}(X) = \mathbf{v}(0)$.

Proof: Let $\mathbf{a}_1 = (0, \ldots, 0) \in k^{m-1}$, and $\mathfrak{M}_1 = \{g \in k[x_1, \ldots, x_{m-1}] \mid g(\mathbf{a}_1) = 0\}$ be the corresponding maximal ideal. We identify residue field $R/\mathfrak{M}_1$ with k. By hypothesis $\mathbf{v} \in (R[X])^n$ is a unimodular column vector, so its image $\bar{\mathbf{v}}$ in $(k[X])^n = ((R/\mathfrak{M}_1)[X])^n$ is also unimodular. Since $k[X]$ is a principal ideal ring, the ideal $\langle \bar{v}_2, \ldots, \bar{v}_n \rangle$ is generated by a single element, $G_1 = \gcd(\bar{v}_2, \ldots, \bar{v}_n)$. Then $\bar{v}_1$ and G_1 generate the unit ideal in $k[X]$ since $\bar{v}_1, \bar{v}_2, \ldots, \bar{v}_n$ generate the unit ideal. Using the Euclidean division algorithm for $k[X]$, we can find $\mathbf{E}_1 \in \mathrm{E}_{n-1}(k[X])$ such that

$$\mathbf{E}_1 \begin{pmatrix} \bar{v}_2 \\ \vdots \\ \bar{v}_n \end{pmatrix} = \begin{pmatrix} G_1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Since we may regard $\mathbf{E}_1$ as an element of $\mathrm{E}_n(R[X])$ and G_1 as an element of $R[X]$. Then,

$$\begin{pmatrix} 1 & 0 \\ 0 & \mathbf{E}_1 \end{pmatrix} \mathbf{v} = \begin{pmatrix} v_1 \\ G_1 + q_{12} \\ q_{13} \\ \vdots \\ q_{1n} \end{pmatrix}$$

for some $q_{12}, \ldots, q_{1n} \in \mathfrak{M}_1[X]$. Now, define $r_1 \in R$ by $r_1 = \mathrm{Res}_{\mathrm{X}}(v_1, G_1 + q_{12})$, the resultant of v_1 and $G_1 + q_{12}$ with respect to X, and find $f_1, h_1 \in R[X]$ such that

$$f_1 \cdot v_1 + h_1 \cdot (G_1 + q_{12}) = r_1.$$

Since v_1 is monic, and $\bar{v}_1$ and $G_1 \in k_1[X]$ generate the unit ideal, we have

$$\begin{aligned} \bar{r}_1 &= \overline{\mathrm{Res}_{\mathrm{X}}(v_1, G_1 + q_{12})} \\ &= \mathrm{Res}_{\mathrm{X}}(\bar{v}_1, G_1) \\ &\neq 0. \end{aligned}$$

Therefore, $r_1 \notin \mathfrak{M}_1$. Denote an algebraic closure of k by $\bar{k}$. Inductively, let $\mathbf{a}_j \in \bar{k}^{m-1}$ be a common zero of $r_1, \ldots, r_{j-1}$ and $\mathfrak{M}_j$ be the corresponding maximal ideal of R for each $j \geq 2$. Define $r_j \notin \mathfrak{M}_j$ in the same way as above. Define also $\mathbf{E}_j \in \mathrm{E}_{n-1}(k_j[X]), G_j \in k_j[X]$, $f_j, h_j \in R[X]$, and $q_{j2}, \ldots, q_{jn} \in \mathfrak{M}_j[X]$ in an analogous way. As we saw in the proof of Theorem 3.1, there is a finite l such that $r_1 R + \cdots + r_l R = R$. Find g_i's in R such that $r_1 g_1 + \cdots + r_l g_l = 1$. Now, define $b_0, b_1, \ldots, b_l \in R[X]$ by

$$\begin{aligned} b_0 &= 0 \\ b_1 &= r_1 g_1 X \\ b_2 &= r_1 g_1 X + r_2 g_2 X \\ &\vdots \\ b_l &= r_1 g_1 X + r_2 g_2 X + \cdots + r_l g_l X = X. \end{aligned}$$

Then these b_i's satisfy the recursive relations:

$$\begin{aligned} b_0 &= 0 \\ b_i &= b_{i-1} + r_i g_i X \quad \text{for } i = 1, \ldots, l. \end{aligned}$$

Claim: For each $i \in \{1, \ldots, l\}$, there exist $\mathbf{B}_i \in \mathrm{SL}_2(R[X])$ and $\mathbf{B}'_i \in \mathrm{E}_n(R[X])$ such that $\mathbf{v}(b_i) = \mathbf{B}_i\mathbf{B}'_i\mathbf{v}(b_{i-1})$.

Using this and the fact that $\mathrm{E}_n(R[X]) \cdot \mathrm{SL}_2(R[X]) \subseteq \mathrm{SL}_2(R[X]) \cdot \mathrm{E}_n(R[X])$ (Corollary 4.1.5), we get inductively

$$\begin{aligned}
\mathbf{v}(X) &= \mathbf{v}(b_l) \\
&= \mathbf{B}_l\mathbf{B}'_l\mathbf{v}(b_{l-1}) \\
&\vdots \\
&= \mathbf{B}\mathbf{B}'\mathbf{v}(b_0) \\
&= \mathbf{B}\mathbf{B}'\mathbf{v}(0)
\end{aligned}$$

for some $\mathbf{B} \in \mathrm{SL}_2(R[X])$ and $\mathbf{B}' \in \mathrm{E}_n(R[X])$. Therefore, it is enough to prove the above claim.

Proof of claim: Let $\tilde{G}_i = G_i + q_{i2}$. Then

$$\begin{pmatrix} 1 & 0 \\ 0 & \mathbf{E}_i(X) \end{pmatrix} \mathbf{v}(X) = \begin{pmatrix} v_1(X) \\ \tilde{G}_i(X) \\ q_{i3}(X) \\ \vdots \\ q_{in}(X) \end{pmatrix}.$$

For $3 \leq j \leq n$, we have

$$q_{ij}(b_i) - q_{ij}(b_{i-1}) \in (b_i - b_{i-1}) \cdot R[X] = r_i g_i X \cdot R[X].$$

Since $r_i \in R$ doesn't depend on X, we have

$$\begin{aligned}
r_i &= f_i(X)v_1(X) + h_i(X)\tilde{G}_i(X) \\
&= f_i(b_{i-1})v_1(b_{i-1}) + h_i(b_{i-1})\tilde{G}_i(b_{i-1}) \\
&= \text{a linear combination of } v_1(b_{i-1}) \text{ and } \tilde{G}_i(b_{i-1}) \text{ over } R[X].
\end{aligned}$$

Therefore, we see that for $3 \leq j \leq n$,

$$q_{ij}(b_i) = q_{ij}(b_{i-1}) + \text{a linear combination of } v_1(b_{i-1}) \text{ and } \tilde{G}_i(b_{i-1}) \text{ over } R[X].$$

Hence we can find $\mathbf{C} \in \mathrm{E}_n(R[X])$ such that

$$\mathbf{C}\begin{pmatrix} 1 & 0 \\ 0 & \mathbf{E}_i(b_{i-1}) \end{pmatrix}\mathbf{v}(b_{i-1}) = \mathbf{C}\begin{pmatrix} v_1(b_{i-1}) \\ \tilde{G}_i(b_{i-1}) \\ q_{i3}(b_{i-1}) \\ \vdots \\ q_{in}(b_{i-1}) \end{pmatrix} = \begin{pmatrix} v_1(b_{i-1}) \\ \tilde{G}_i(b_{i-1}) \\ q_{i3}(b_i) \\ \vdots \\ q_{in}(b_i) \end{pmatrix}.$$

Now, by Lemma 4.3.2, we can find $\tilde{B} \in \mathrm{SL}_2(R[X])$ such that

$$\tilde{\mathbf{B}}\begin{pmatrix} v_1(b_{i-1}) \\ \tilde{G}_i(b_{i-1}) \end{pmatrix} = \begin{pmatrix} v_1(b_i) \\ \tilde{G}_i(b_i) \end{pmatrix}.$$

Finally, define $\mathbf{B} \in \mathrm{SL}_n(R[X])$ as follows:

$$\mathbf{B} = \begin{pmatrix} 1 & 0 \\ 0 & \mathbf{E}_i(b_i)^{-1} \end{pmatrix}\begin{pmatrix} \tilde{\mathbf{B}} & 0 \\ 0 & \mathbf{I}_{n-2} \end{pmatrix} \cdot \mathbf{C} \cdot \begin{pmatrix} 1 & 0 \\ 0 & \mathbf{E}_i(b_i) \end{pmatrix}.$$

Then this $\mathbf{B}$ satisfies

$$\mathbf{B}\mathbf{v}(b_{i-1}) = \mathbf{v}(b_i),$$

and, by using the normality of $\mathrm{E}_n(R[X])$ again, we see that

$$\mathbf{B} \in \mathrm{SL}_2(R[X])\mathrm{E}_n(R[X]),$$

which proves the claim and completes the proof of the theorem. □

Remark 4.3.4 Note that the groups $\mathrm{GL}_n(k[\boldsymbol{x}])$ and $\mathrm{E}_n(k[\boldsymbol{x}])$ act on the set $\mathrm{Um}_n(k[\boldsymbol{x}])$ by matrix multiplication. If the group action of $\mathrm{E}_n(k[\boldsymbol{x}])$ on $\mathrm{Um}_n(k[\boldsymbol{x}])$ is transitive, then we get a desired algorithm in the following way: For any n-dimensional unimodular column vectors $\mathbf{v}, \mathbf{v}'$ over $k[\boldsymbol{x}]$, we can find $\mathbf{B} \in \mathrm{E}_n(k[\boldsymbol{x}])$ such that $\mathbf{B}\mathbf{v} = \mathbf{v}'$. Now, let $\mathbf{v}' = \mathbf{e}_n$.

Theorem 4.3.5 (Elementary Column Property) *The group* $\mathrm{E}_n(k[\boldsymbol{x}])$ *acts transitively on the set* $\mathrm{Um}_n(k[\boldsymbol{x}])$, *for* $n \geq 3$.

Corollary 4.3.6 (Unimodular Column Property) *The group* $\mathrm{GL}_n(k[\boldsymbol{x}])$ *acts transitively on the set* $\mathrm{Um}_n(k[\boldsymbol{x}])$, *for* $n \geq 2$.

Proof: For $n \geq 3$, the Elementary Column Property clearly implies the Unimodular Column Property since a product of elementary matrices is always unimodular, i.e. has a constant nonzero determinant.

If $n = 2$, for any $\mathbf{v} = (v_1, v_2)^t \in \mathrm{Um}_2(k[\boldsymbol{x}])$, by using Buchberger's algorithm for computing a Gröbner basis, we can find $g_1, g_2 \in k[\boldsymbol{x}]$ such that $v_1 g_1 + v_2 g_2 = 1$. Then the unimodular matrix $U_{\mathbf{v}} = \begin{pmatrix} v_2 & -v_1 \\ g_1 & g_2 \end{pmatrix}$ satisfies $U_{\mathbf{v}} \cdot \mathbf{v} = \mathbf{e}_2$. Therefore we see that, for any $\mathbf{v}, \mathbf{w} \in \mathrm{Um}_2(k[\boldsymbol{x}])$, $U_{\mathbf{w}}^{-1} U_{\mathbf{v}} \cdot \mathbf{v} = \mathbf{w}$ where $U_{\mathbf{w}}^{-1} U_{\mathbf{v}} \in \mathrm{GL}_2(k[\boldsymbol{x}])$. □

Proof of Theorem 4.3.5: Since the Euclidean division algorithm for $k[x_1]$ proves the theorem for $m = 1$, we may assume by induction the statement of the theorem for $R = k[x_1, \ldots, x_{m-1}]$. Let $X = x_m$ and $\mathbf{v} = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \in \mathrm{Um}_n(R[X])$. We may also assume that v_1 is monic by applying a change of variables (as in the proof of the Noether Normalization Lemma). Now by Theorem 4.3.3, we can find $\mathbf{B}_1 \in \mathrm{SL}_2(R[X])$ and $\mathbf{B}_2 \in \mathrm{E}_n(R[X])$ such that

$$\mathbf{B}_1 \mathbf{B}_2 \cdot \mathbf{v}(X) \quad = \quad \mathbf{v}(0) \in R.$$

Then by the inductive hypothesis, we can find $\mathbf{B}' \in \mathrm{E}_n(R)$ such that

$$\mathbf{B}' \cdot \mathbf{v}(0) \quad = \quad \mathbf{e}_n.$$

Therefore, we get

$$\mathbf{v} \quad = \quad \mathbf{B}_2^{-1} \mathbf{B}_1^{-1} \mathbf{B}'^{-1} \mathbf{e}_n.$$

By the normality of $\mathrm{E}_n(R[X])$ in $\mathrm{SL}_n(R[X])$ (Corollary 4.1.5), we can write $\mathbf{B}_1^{-1} \mathbf{B}'^{-1} = \mathbf{B}'' \mathbf{B}_1^{-1}$ for some $\mathbf{B}'' \in \mathrm{E}_n(R[X])$. Since

$$\mathbf{B}_1^{-1} = \begin{pmatrix} p & q & 0 & \ldots & 0 \\ r & s & 0 & \ldots & 0 \\ 0 & 0 & & & \\ \vdots & \vdots & & \mathbf{I}_{n-2} & \\ 0 & 0 & & & \end{pmatrix}$$

for some $p, q, r, s \in R[X]$, we have

$$\begin{aligned} \mathbf{v} &= \mathbf{B}_2^{-1} \mathbf{B}_1^{-1} \mathbf{B}'^{-1} \mathbf{e}_n \\ &= (\mathbf{B}_2^{-1} \mathbf{B}'') \mathbf{B}_1^{-1} \mathbf{e}_n \end{aligned}$$

$$= \quad (\mathbf{B}_2^{-1}\mathbf{B}'') \begin{pmatrix} p & q & 0 & \dots & 0 \\ r & s & 0 & \dots & 0 \\ 0 & 0 & & & \\ \vdots & \vdots & & \mathbf{I}_{n-2} & \\ 0 & 0 & & & \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}$$

$$= \quad (\mathbf{B}_2^{-1}\mathbf{B}'')\mathbf{e}_n$$

where $\mathbf{B}_2^{-1}\mathbf{B}'' \in \mathrm{E}_n(R[X])$. Since we have this relationship for any $\mathbf{v} \in \mathrm{Um}_n(R[X])$, we get the desired transitivity. □

4.4 Realization Algorithm for $\mathrm{SL}_3(R[X])$

Now, we give a realization algorithm for the matrices of the form:

$$\begin{pmatrix} p & q & 0 \\ r & s & 0 \\ 0 & 0 & 1 \end{pmatrix} \in \mathrm{SL}_3(k[\boldsymbol{x}]).$$

Again, by applying a change of variables, we may assume that $p \in k[\boldsymbol{x}] = k[x_1, \dots, x_m]$ is a monic polynomial in the last variable x_m. In view of the Quillen Induction Algorithm developed in Section 4.2, we see that it is enough to develop a realization algorithm for matrices of the form $\begin{pmatrix} p & q & 0 \\ r & s & 0 \\ 0 & 0 & 1 \end{pmatrix} \in \mathrm{SL}_3(R[X])$, in the case where R is a commutative local ring and $p \in R[X]$ is a monic polynomial. A realization algorithm for this case was obtained by M.P. Murthy [GM80, Lemma 3.6]. We present below a slightly modified version.

Lemma 4.4.1 *Let L be a commutative ring, and $a, a', b \in L$. Then, the following are true.*

1. *(a, b) and (a', b) are unimodular over L if and only if (aa', b) is unimodular over L.*

2. *For any $c, d \in L$ such that $aa'd - bc = 1$, there exist $c_1, c_2, d_1, d_2 \in L$ such that $ad_1 - bc_1 = 1$, $a'd_2 - bc_2 = 1$, and*

$$\begin{pmatrix} aa' & b & 0 \\ c & d & 0 \\ 0 & 0 & 1 \end{pmatrix} \equiv \begin{pmatrix} a & b & 0 \\ c_1 & d_1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} a' & b & 0 \\ c_2 & d_2 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad (\mathrm{mod}\ \mathrm{E}_3(L)).$$

Proof: (1) If (aa', b) is unimodular over L, then (a, b) and (a', b) are clearly unimodular.

Suppose, now, that (a, b) and (a', b) are unimodular over L. Then, we can find $h_1, h_2, h'_1, h'_2 \in L$ such that $h_1 a + h_2 b = 1,\ h'_1 a' + h'_2 b = 1$. Now, by letting $g_1 = h_1 h'_1,\ g_2 = h'_2 + a' h_2 h'_1$, we get $g_1 aa' + g_2 b = 1$.

(2) If $c, d \in L$ satisfy $aa'd - bc = 1$, then (aa', b) is unimodular, which in turn implies that (a, b) and (a', b) are unimodular. Therefore, we can find $c_1, d_1, d_1, d_2 \in L$ such that $ad_1 - bc_1 = 1$ and $a'd_2 - bc_2 = 1$. For example, we can let

$$c_1 = c_2 = c, \quad d_1 = a'd, \quad d_2 = ad.$$

Now, consider

$$\begin{aligned}
\begin{pmatrix} aa' & b & 0 \\ c & d & 0 \\ 0 & 0 & 1 \end{pmatrix} &= \mathbf{E}_{21}(cd_1d_2 - d(c_2 + a'c_1d_2)) \begin{pmatrix} aa' & b & 0 \\ c_2 + a'c_1d_2 & d_1d_2 & 0 \\ 0 & 0 & 1 \end{pmatrix} \\
&= \mathbf{E}_{21}(cd_1d_2 - d(c_2 + a'c_1d_2))\mathbf{E}_{23}(d_2 - 1)\mathbf{E}_{32}(1)\mathbf{E}_{23}(-1) \\
&\quad \cdot \begin{pmatrix} a & b & 0 \\ c_1 & d_1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \mathbf{E}_{23}(1)\mathbf{E}_{32}(-1)\mathbf{E}_{23}(1) \begin{pmatrix} a' & b & 0 \\ c_2 & d_2 & 0 \\ 0 & 0 & 1 \end{pmatrix} \\
&\quad \cdot \mathbf{E}_{23}(-1)\mathbf{E}_{32}(1)\mathbf{E}_{23}(a - 1)\mathbf{E}_{31}(-a'c_1)\mathbf{E}_{32}(-d_1).
\end{aligned}$$

This explicit expression shows that

$$\begin{pmatrix} aa' & b & 0 \\ c & d & 0 \\ 0 & 0 & 1 \end{pmatrix} \equiv \begin{pmatrix} a & b & 0 \\ c_1 & d_1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} a' & b & 0 \\ c_2 & d_2 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad (\text{mod } \mathrm{E}_3(L)).$$

□

Theorem 4.4.2 *Suppose* $(R, \mathfrak{M})$ *is a commutative local ring, and* $\mathbf{A} = \begin{pmatrix} p & q & 0 \\ r & s & 0 \\ 0 & 0 & 1 \end{pmatrix} \in \mathrm{SL}_3(R[X])$ *where* p *is monic. Then* $\mathbf{A}$ *is realizable over* $R[X]$.

Proof: We induct on $\deg(p)$. If $\deg(p) = 0$, then $p = 1$, and A is clearly realizable. More explicitly, we have

$$\mathbf{A} = \mathbf{E}_{21}(r - 1)\mathbf{E}_{21}(1)\mathbf{E}_{12}(1 - p + q).$$

Now, suppose $\deg(p) = d > 0$ and $\deg(q) = l$. Since $p \in R[X]$ is monic, we can find $f, g \in R[X]$ such that

$$q = fp + g, \quad \deg(g) < d.$$

Then,

$$\mathbf{AE}_{12}(-f) = \begin{pmatrix} p & q - fp & 0 \\ r & s - fr & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} p & g & 0 \\ r & s - fr & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Hence we may assume $\deg(q) < d$. Now, we note that either $p(0)$ or $q(0)$ is a unit in R, otherwise, we would have $p(0)s(0) - q(0)r(0) \in \mathfrak{M}$, which contradicts the fact that $ps - qr = p(0)s(0) - q(0)r(0) = 1$. Consider these two cases separately.

- **Case 1:** Suppose that $q(0)$ is a unit.
  We have
  $$\mathbf{AE}_{21}(-q(0)^{-1}p(0)) = \begin{pmatrix} p - q(0)^{-1}p(0)q & q & 0 \\ r - q(0)^{-1}p(0)s & s & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$
  So, we may assume $p(0) = 0$. Now, write $p = Xp'$. Then, by Lemma 4.4.1, we can find $c_1, d_1, c_2, d_2 \in R[X]$ such that $Xd_1 - qc_1 = 1$, $p'd_2 - qc_2 = 1$ and
  $$\begin{pmatrix} p & q & 0 \\ r & s & 0 \\ 0 & 0 & 1 \end{pmatrix} \equiv \begin{pmatrix} X & q & 0 \\ c_1 & d_1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} p' & q & 0 \\ c_2 & d_2 & 0 \\ 0 & 0 & 1 \end{pmatrix} \pmod{\mathrm{E}_3(R[X])}.$$
  Since p' is monic and $\deg(p') < d$, the second matrix on the right hand side is realizable by the induction hypothesis. As for the first matrix, we may assume that q is a unit of R since we can assume $\deg(q) < \deg(X) = 1$ and $q(0)$ is a unit. Then invertibility of q leads easily to an explicit factorization of $\begin{pmatrix} X & q & 0 \\ c_1 & d_1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ into elementary matrices.

- **Case 2:** Suppose that $q(0)$ is not a unit.
  First we claim that there exist $p', q' \in R[X]$ such that $\deg(p') < l, \deg(q') < d$ and $p'p - q'q = 1$. To prove this claim, we let $s \in R$ be the resultant of p and q. Then there exist $f, g \in R[X]$ with $\deg(f) < l, \deg(g) < d$ such that $fp + gq = s$. Since

p is monic and $p, q \in R[X]$ generate the unit ideal, we see that $s \notin \mathfrak{M}$, hence s is a unit in R. Now, setting $p' = f/s$, $q' = -g/s$ proves the claim. Also note that $p'(0)p(0) - q'(0)q(0) = 1$ and $q(0) \in \mathfrak{M}$ implies $p'(0) \notin \mathfrak{M}$. This means that $q(0) + p'(0)$ is a unit. Now, we have that

$$\begin{aligned} \begin{pmatrix} p & q & 0 \\ r & s & 0 \\ 0 & 0 & 1 \end{pmatrix} &= \mathbf{E}_{21}(rp' - sq') \begin{pmatrix} p & q & 0 \\ q' & p' & 0 \\ 0 & 0 & 1 \end{pmatrix} \\ &= \mathbf{E}_{21}(rp' - sq')\mathbf{E}_{12}(-1) \begin{pmatrix} p + q' & q + p' & 0 \\ q' & p' & 0 \\ 0 & 0 & 1 \end{pmatrix}. \end{aligned}$$

Note that the last matrix on the right hand side is realizable by Case 1, since $q(0) + p'(0)$ is a unit and $\deg(p + q') = d$. Thus, $\begin{pmatrix} p & q & 0 \\ r & s & 0 \\ 0 & 0 & 1 \end{pmatrix}$ is also realizable.

□

4.5 Eliminating Redundancies in the Realization Algorithm

When applied to a specific polynomial matrix, the realization algorithm obtained in this chapter will produce a factorization into elementary polynomial matrices, but this factorization may not have minimal length. The Steinberg relations [Mil71, p. 39] from algebraic K-theory provide a method for improving a given factorization by eliminating some of the unnecessary factors. The Steinberg relations which elementary matrices satisfy are

1. $\mathbf{E}_{ij}(0) = I$;
2. $\mathbf{E}_{ij}(a)\mathbf{E}_{ij}(b) = \mathbf{E}_{ij}(a + b)$;
3. For $i \neq l$, $[\mathbf{E}_{ij}(a), \mathbf{E}_{jl}(b)] = \mathbf{E}_{ij}(a)\mathbf{E}_{jl}(b)\mathbf{E}_{ij}(-a)\mathbf{E}_{jl}(-b) = \mathbf{E}_{il}(ab)$;
4. For $j \neq l$, $[\mathbf{E}_{ij}(a), \mathbf{E}_{li}(b)] = \mathbf{E}_{ij}(a)\mathbf{E}_{li}(b)\mathbf{E}_{ij}(-a)\mathbf{E}_{li}(-b) = \mathbf{E}_{lj}(-ab)$;
5. For $i \neq p$, $j \neq l$, $[\mathbf{E}_{ij}(a), \mathbf{E}_{lp}(b)] = \mathbf{E}_{ij}(a)\mathbf{E}_{lp}(b)\mathbf{E}_{ij}(-a)\mathbf{E}_{lp}(-b) = I$.

The realization algorithm developed in this chapter can be implemented together with a redundancy elimination algorithm based on the above set of relations using existing computer algebra systems.

Chapter 5

A Realization Algorithm for $\mathrm{SL}_2(k[x_1, \ldots, x_m])$

5.1 Introduction

Suslin's stability theorem established in the previous chapter fails for $n = 2$, and a counter-example was constructed by P.M. Cohn in [Coh66], i.e. the *Cohn matrix*, $\begin{pmatrix} 1+xy & x^2 \\ -y^2 & 1-xy \end{pmatrix} \in \mathrm{SL}_2(\mathbb{C}[x, y])$, was shown to be nonrealizable. On this matter, L. Tolhuizen, H. Holmann and A. Kalker have developed an algorithm in [THK95] that determines precisely when a given matrix in $\mathrm{SL}_2(k[\boldsymbol{x}]) := \mathrm{SL}_2(k[x_1, \ldots, x_m])$ is realizable, and if it is, expresses it as a product of elementary matrices.

In this chapter, we will develop another algorithm for the same task based on degree lexicographic order on the polynomial ring $k[\boldsymbol{x}]$. Actually, usual lexicographic order doesn't work for our purpose since it does not necessarily guarantee the termination of our algorithm in a finite number of steps.

5.2 Main Theorem

For an $p \times q$ matrix $\mathbf{A} = (a_{ij}) \in \mathrm{M}_{pq}(k[\boldsymbol{x}])$, we can define its rank, viewing it as a matrix over $k(\boldsymbol{x})$, the field of quotients of $k[\boldsymbol{x}]$. Also, for a fixed monomial order on $\mathrm{Mono}(k[\boldsymbol{x}])$, we define the matrix of its leading terms as $\mathrm{lt}(\mathbf{A}) := (\mathrm{lt}(a_{ij}))$.

Now, the following theorem gives a characterizing property for the realizable 2×2

matrices.

Theorem 5.2.1 *Suppose that* $\mathbf{A} = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \in \mathrm{SL}_2(k[\boldsymbol{x}])$ *is realizable, and fix a monomial order on* $\mathrm{Mono}(k[\boldsymbol{x}])$*. Then, either the matrix of its leading terms,* $\mathrm{lt}(\mathbf{A})$*, is of rank* 2*, or one of its row vectors is a monomial multiple of the other row.*

Remark 5.2.2 In the case of the Cohn matrix $\mathbf{A} = \begin{pmatrix} 1+xy & x^2 \\ -y^2 & 1-xy \end{pmatrix}$, note that $\mathrm{lt}(\mathbf{A}) = \begin{pmatrix} xy & x^2 \\ -y^2 & -xy \end{pmatrix}$ is of rank 1, but neither of the two row vectors $(xy, x^2) = x \cdot (y, x)$ and $(-y^2, -xy) = -y \cdot (y, x)$ is a monomial multiple of the other.

Proof: Since $\mathbf{A}$ is realizable, we can write $\mathbf{A}$ as a product of elementary matrices. Let $\mathbf{A} = \mathbf{E}_1 \cdots \mathbf{E}_l$ be such a representation without a trivial factor , i.e. for each $i = 1, \ldots, l$, $\mathbf{E}_i$ is either $\mathbf{E}_{12}(f)$ or $\mathbf{E}_{21}(f)$ for some $f \neq 0 \in k[\boldsymbol{x}]$. Now, we will do an induction on l.

If $l = 1$, the statement of the theorem is trivial since we have either $\mathbf{A} = \begin{pmatrix} 1 & q \\ 0 & 1 \end{pmatrix}$ or $\mathbf{A} = \begin{pmatrix} 1 & 0 \\ r & 1 \end{pmatrix}$ for some $q, r \in k[\boldsymbol{x}]$, and in both cases, $\mathrm{lt}(\mathbf{A})$ is of rank 2.

Now let

$$\begin{aligned} \mathbf{A}' &= \mathbf{E}_1 \cdots \mathbf{E}_{k-1} \\ &= \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(k[\boldsymbol{x}]). \end{aligned}$$

Suppose that the rank of $\mathrm{lt}(\mathbf{A}')$ is 1. Then by the induction hypothesis, we may assume without loss of generality that

$$(\mathrm{lt}(a), \mathrm{lt}(b)) = h \cdot (\mathrm{lt}(c), \mathrm{lt}(d))$$

for some nonzero monomial $h \in k[\boldsymbol{x}]$.

Now, we have two cases:

$$\mathbf{A} = \begin{pmatrix} p & q \\ r & s \end{pmatrix} = \mathbf{A}'\mathbf{E}_{12}(f) = \begin{pmatrix} a & b+fa \\ c & d+fc \end{pmatrix}$$

or

$$\mathbf{A} = \begin{pmatrix} p & q \\ r & s \end{pmatrix} = \mathbf{A}'\mathbf{E}_{21}(f) = \begin{pmatrix} a+fb & b \\ c+fd & d \end{pmatrix}.$$

In the first case, $\det(\mathbf{A}) = 1$ implies

$$\begin{aligned} \mathrm{lt}(c) \cdot \mathrm{lt}(b + fa) &= \mathrm{lt}(a) \cdot \mathrm{lt}(d + fc) \\ &= h \cdot \mathrm{lt}(c) \cdot \mathrm{lt}(d + fc). \end{aligned}$$

Therefore, $\mathrm{lt}(b + fa) = h \cdot \mathrm{lt}(d + fc)$.

Now,

$$(\mathrm{lt}(r), \mathrm{lt}(s)) = (\mathrm{lt}(c), \mathrm{lt}(d + fc))$$

and

$$\begin{aligned} (\mathrm{lt}(p), \mathrm{lt}(q)) &= (\mathrm{lt}(a), \mathrm{lt}(b + fa)) \\ &= (h \cdot \mathrm{lt}(c), h \cdot \mathrm{lt}(d + fc)) \\ &= h \cdot (\mathrm{lt}(c), \mathrm{lt}(d + fc)) \\ &= h \cdot (\mathrm{lt}(r), \mathrm{lt}(s)) \end{aligned}$$

as desired.

The same method gives the same conclusion in the second case.

Now, to complete the proof, we have to consider the case when

$$\mathrm{lt}(\mathbf{A}') = \begin{pmatrix} \mathrm{lt}(a) & \mathrm{lt}(b) \\ \mathrm{lt}(c) & \mathrm{lt}(d) \end{pmatrix},$$

is of rank 2.

In this case, note that both ad and bc are constants, otherwise, $\det \mathbf{A}(') = 1$ implies $\det(\mathrm{lt}(\mathbf{A}')) = 0$ contradicting $\mathrm{rank}(\mathrm{lt}(\mathbf{A}')) = 2$. So, let us assume a is a constant. If one of b or d is also a constant, then $\mathbf{A}'\mathbf{E}_{12}(f) = \begin{pmatrix} a & b + fa \\ c & d + fc \end{pmatrix}$ and $\mathbf{A}'\mathbf{E}_{21}(f) = \begin{pmatrix} a + fb & b \\ c + fd & d \end{pmatrix}$ always have at least one constant entry, so we are done. Hence we assume that both of b and d are nonconstants.

In this case, note that $a \neq 0$ and $c \neq 0$, otherwise $\det(\mathbf{A}') = ad - bc = 1$ can not be satisfied.

Claim: $\mathrm{lt}(b) \mid \mathrm{lt}(d)$

$\det(\mathbf{A}) = 1$ implies $a \cdot \mathrm{lt}(d) = \mathrm{lt}(b)\mathrm{lt}(c)$, and $a \neq 0$. So, $\mathrm{lt}(d) = (a^{-1}\mathrm{lt}(c)) \cdot \mathrm{lt}(b)$. There are two cases to consider, again.

$$\mathbf{A} = \begin{pmatrix} p & q \\ r & s \end{pmatrix} = \mathbf{A}'\mathbf{E}_{12}(f) = \begin{pmatrix} a & b + fa \\ c & d + fc \end{pmatrix}$$

or

$$\mathbf{A} \;=\; \begin{pmatrix} p & q \\ r & s \end{pmatrix} = \mathbf{A}'\mathbf{E}_{21}(f) = \begin{pmatrix} a+fb & b \\ c+fd & d \end{pmatrix}.$$

In the first case, $p = a$ is a constant entry of $\mathbf{A}$, so we are done.

In the second case, note that $\mathrm{lt}(a) \le \mathrm{lt}(c) < \mathrm{lt}(d)$ since $a \cdot \mathrm{lt}(d) = \mathrm{lt}(b)\mathrm{lt}(c)$ and b is not a constant. Hence, we have $\mathrm{lt}(c + fd) = \mathrm{lt}(fd)$. Recall we are assuming $f \neq 0$. Therefore,

$$(\mathrm{lt}(r), \mathrm{lt}(s)) = (\mathrm{lt}(f) \cdot \mathrm{lt}(d), \mathrm{lt}(d)) = \mathrm{lt}(d) \cdot (\mathrm{lt}(f), 1)$$

and

$$(\mathrm{lt}(p), \mathrm{lt}(q)) = (\mathrm{lt}(f) \cdot \mathrm{lt}(b), \mathrm{lt}(b)) = \mathrm{lt}(b) \cdot (\mathrm{lt}(f), 1) = h \cdot (\mathrm{lt}(r), \mathrm{lt}(s))$$

as desired. $\square$

5.3 Realization Algorithm for $\mathrm{SL}_2(k[x_1, \ldots, x_m])$

Now, let us see how to obtain a realization algorithm for $\mathrm{E}_2(k[\boldsymbol{x}])$ from the Theorem 5.2.1 of the previous section.

If one of the entries of $\mathbf{A} := \begin{pmatrix} p & q \\ r & s \end{pmatrix} \in \mathrm{SL}_2(k[\boldsymbol{x}])$, say p, is a constant, then $\mathbf{A}$ is always realizable in the following way.

- If $p = 0$, then $\det(\mathbf{A}) = -rq = 1$ necessarily implies r, q are invertible. Using the invertibility of r, we easily get

$$\mathbf{A} \;=\; \begin{pmatrix} 0 & q \\ r & s \end{pmatrix} = \mathbf{E}_{12}(-r^{-1})\mathbf{E}_{21}(r)\mathbf{E}_{12}(q + r^{-1}s).$$

- If $p \neq 0$, then using the invertibility of p, we get

$$\mathbf{A} \;=\; \mathbf{E}_{21}(p^{-1}(r-1))\mathbf{E}_{12}(p-1)\mathbf{E}_{21}(1)\mathbf{E}_{12}(p^{-1}(1-p+q)).$$

Definition 5.3.1 *For* $\mathbf{B} = (b_{ij}) \in \mathrm{SL}_n(k[\boldsymbol{x}])$, *we define* $\deg(\mathbf{B}) \in (\mathbb{Z}_{\ge 0})^m$ *by*

$$\deg(\mathbf{B}) = \max_{1 \le i,j \le n} \{\deg(b_{ij})\} \in (\mathbb{Z}_{\ge 0})^m.$$

Remark 5.3.2 If $\deg(\mathbf{B}) = (0, \ldots, 0) \in (\mathbb{Z}_{\ge 0})^m$, then clearly all the entries of $\mathbf{B}$ are constants.

Now, out of a given $\mathbf{A} \in \mathrm{SL}_2(k[\boldsymbol{x}])$, we try to make a matrix with a constant entry by applying elementary operations. If $\mathbf{A} = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \in \mathrm{SL}_2(k[\boldsymbol{x}])$ doesn't have any constant entries, then compare the two vectors $(\mathrm{lt}(p), \mathrm{lt}(q))$ and $(\mathrm{lt}(r), \mathrm{lt}(s))$.

- **Step 1:** If neither of them is a monomial multiple of the other, then by the Theorem 5.2.1, $\mathbf{A}$ is not realizable. Otherwise, go to step 2.

- **Step 2:** Assume without loss of generality that

$$(\mathrm{lt}(p), \mathrm{lt}(q)) \quad = \quad h \cdot (\mathrm{lt}(r), \mathrm{lt}(s))$$

  for some monomial $h \in k[\boldsymbol{x}]$. There are two cases to consider. If h is a constant, replace $\mathbf{A}$ by $\mathbf{E}_{12}(-h)\mathbf{A}$ and go to step 1. Otherwise, go to step 3.

- **Step 3:** Note that the matrix $\mathbf{E}_{12}(-h)\mathbf{A} = \begin{pmatrix} p - hr & q - hs \\ r & s \end{pmatrix}$ has a strictly smaller degree than $\mathbf{A}$. Now replace $\mathbf{A}$ by $\mathbf{E}_{12}(-h)\mathbf{A}$, and see if it has a constant entry. If it does, then terminate the process. Otherwise go to step 1 with the new $\mathbf{A}$.

If any intermediate matrix in the above process is not realizable by step 1, then $\mathbf{A}$ itself is not realizable. Otherwise, since the above procedure strictly reduces the degree of $\mathbf{A}$ each time and there are only finitely many elements of $(\mathbb{Z}_{\geq 0})^m$ between $\mathbf{0} \in (\mathbb{Z}_{\geq 0})^m$ and $\deg(\mathbf{A}) \in (\mathbb{Z}_{\geq 0})^m$, we get a matrix in $\mathrm{SL}_2(k[\boldsymbol{x}])$ with a constant entry after a finite number of steps. By keeping track of all the intermediate matrices, we find elementary matrices $\mathbf{E}_1, \ldots, \mathbf{E}_l$ over $k[\boldsymbol{x}]$ such that $\mathbf{A} = \mathbf{E}_1 \cdots \mathbf{E}_l$.

Remark 5.3.3 With respect to lexicographic order, there are infinitely many elements of $(\mathbb{Z}_{\geq 0})^m$ between $\mathbf{0} \in (\mathbb{Z}_{\geq 0})^m$ and $\deg(\mathbf{A}) \in (\mathbb{Z}_{\geq 0})^m$ for a nonconstant matrix $\mathbf{A} \in \mathrm{SL}_2(k[\boldsymbol{x}])$. Therefore, even though the above procedure strictly reduces the degree of $\mathbf{A}$ each time, we may not get to a matrix with constant entry in a finite number of steps.

Chapter 6

Extensions to Laurent Polynomial Rings

6.1 Polynomial Rings and Laurent Polynomial Rings

So far, we have studied unimodular matrices exclusively over polynomial rings. We now want to study unimodular matrices over Laurent polynomial rings, and see the possibility of extending the results of the preceding chapters to the case of Laurent polynomial rings. Therefore, in this chapter, we develop an algorithm that transforms a Laurent polynomial column vector to a polynomial column vector while preserving unimodularity.

Let $n \geq 2$ be a nonzero integer.

Algorithm 6.1: **LaurentToPoly**

Input:	$\mathbf{v}(\boldsymbol{x}) \in (k[\boldsymbol{x}^{\pm 1}])^n$, a **Laurent** polynomial column vector
Output:	$\boldsymbol{x} \to \boldsymbol{y}$, a change of variables $\mathbf{T}(\boldsymbol{x}) \in \mathrm{GL}_n(k[\boldsymbol{x}^{\pm 1}])$, a square unimodular Laurent polynomial matrix
Specification:	(1) $\hat{\mathbf{v}}(\boldsymbol{y}) := \mathbf{T}(\boldsymbol{x})\mathbf{v}(\boldsymbol{x}) \in (k[\boldsymbol{y}])^n$ is a **polynomial** column vector in the new variable $\boldsymbol{y}$ (2) $\mathbf{v}(\boldsymbol{x})$ is unimodular over $k[\boldsymbol{x}^{\pm 1}]$ if and only if $\hat{\mathbf{v}}(\boldsymbol{y})$ is unimodular over $k[\boldsymbol{y}]$

This process is very powerful essentially because the unimodularity of the Laurent polynomial vector $\mathbf{v}(\boldsymbol{x}) \in (k[\boldsymbol{x}^{\pm 1}])^n$ is converted to the unimodularity of the polynomial vector $\hat{\mathbf{v}}(\boldsymbol{y}) \in (k[\boldsymbol{x}])^n$.

Algorithm 6.2: **ReduceToSingle**

Input:	An Algorithm for the **Unimodular Column Property**, i.e. an algorithm that completes any unimodular column vector $\mathbf{v} = (f_1, \ldots, f_p)^t \in (k[\boldsymbol{x}^{\pm 1}])^p$ to a $p \times p$ unimodular matrix over $k[\boldsymbol{x}^{\pm 1}]$
Output:	A general Unimodular Completion Algorithm

Now we can use this process to give an algorithmic proof of the following important result.

Corollary 6.1.1 (Laurent polynomial analogue of Quillen-Suslin Theorem) *Let* $\mathbf{B}$ *be a* $p \times q$ *unimodular matrix,* $p \geq q$*, with Laurent polynomial entries. Then* $\mathbf{B}$ *can be completed to a square* $p \times p$ *unimodular matrix* $\bar{\mathbf{B}}$ *by adding* $p - q$ *columns to the matrix* $\mathbf{B}$.

Proof:

Single Column Case: For a given unimodular Laurent polynomial vector $\mathbf{v} \in (k[\boldsymbol{x}^{\pm 1}])^n$, one can use the algorithm **UnimodCompletion** to complete the unimodular **polynomial** vector $\hat{\mathbf{v}}(\boldsymbol{y}) \in (k[\boldsymbol{y}])^n$ to a square unimodular polynomial matrix $\hat{\mathbf{A}} \in \mathrm{M}_n(k[\boldsymbol{y}])$. Then, $\mathbf{T}^{-1}\hat{\mathbf{A}} \in k[\boldsymbol{x}^{\pm 1}]$ expressed in terms of the original variables $\boldsymbol{x} := (x_1, \ldots, x_m)$ is a unimodular completion of $\mathbf{v} \in (k[\boldsymbol{x}^{\pm 1}])^n$.

General Case: We reduce this to a single column case.

For a given $p \times q$ $(p \geq q)$ unimodular matrix $\mathbf{A}$, consider its first column vector $\mathbf{v} := \mathbf{A}\begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$. By using the input algorithm, we can complete $\mathbf{v}$ to a $p \times p$ unimodular matrix $\mathbf{B}$ and from $\mathbf{B}\begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \mathbf{v}$, we have

$$\mathbf{B}^{-1}\mathbf{v} = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

This implies

$$\mathbf{B}^{-1}\mathbf{A} \;=\; \begin{pmatrix} 1 & h_2 & \cdots & h_q \\ 0 & & & \\ \vdots & & \mathbf{C} & \\ 0 & & & \end{pmatrix}.$$

for some $h_2, \ldots, h_q \in k[\boldsymbol{x}^{\pm 1}]$, and a $(p-1)\times(q-1)$ matrix $\mathbf{C}$.

Now, $\mathbf{C}$, the cofactor of $(\mathbf{B}^{-1}\mathbf{A})_{11} = 1$, is also unimodular, and by induction, we can complete $\mathbf{C}$ to a $(p-1)\times(p-1)$ unimodular matrix $\bar{\mathbf{C}}$. Then the $p \times p$ matrix

$$\bar{\mathbf{A}} \;=\; \mathbf{B}\begin{pmatrix} 1 & h_2 & \cdots & h_q & 0 & \cdots 0 \\ 0 & & & & & \\ \vdots & & & \bar{\mathbf{C}} & & \\ 0 & & & & & \end{pmatrix}$$

is a unimodular completion of $\mathbf{A}$. $\square$

We start with generalizing the Noether Normalization Lemma to the case of Laurent polynomial rings.

6.2 Laurent analogue of Noether Normalization

The Noether Normalization Lemma states that, for any given polynomial $f \in k[\boldsymbol{x}]$, by defining new variables $y_1, \ldots, y_m$ by $x_1 = y_1, x_2 = y_2 + y_1^l, \ldots, x_m = y_m + y_1^{l^{m-1}}$ for a sufficiently large $l \in \mathbb{N}$ and regarding f as a polynomial in the new variables $y_1, \ldots, y_m$, we can make f a monic polynomial in the first variable y_1.

Now, we extend this to the Laurent polynomial ring $k[\boldsymbol{x}^{\pm 1}] = k[x_1^{\pm 1}, \ldots, x_m^{\pm 1}]$.

Algorithm 6.3: **LaurentNoether**

Input:	$f \in k[\boldsymbol{x}^{\pm 1}]$
Output:	$\boldsymbol{x} \to \boldsymbol{y}$, a change of variables
Specification:	the leading and the lowest coefficients of $f \in k[\boldsymbol{y}^{\pm 1}]$ with respect to the first variable y_1 are units in the ring $k[y_2^{\pm 1}, \ldots, y_m^{\pm 1}]$

Theorem 6.2.1 (Laurent polynomial analogue of Noether Normalization) *Let $f \in k[\boldsymbol{x}^{\pm 1}]$ be a Laurent polynomial, and define new variables $y_1, \ldots, y_m$ by $x_1 = y_1, x_2 =$*

$y_2y_1^l, \ldots, x_m = y_my_1^{l^{m-1}}$. Then, for a sufficiently large $l \in \mathbb{N}$, the leading and the lowest coefficients of $f \in k[\boldsymbol{x}^{\pm 1}]$ with respect to the first variable y_1 are units in the ring $k[y_2^{\pm 1}, \ldots, y_m^{\pm 1}]$.

Proof: Since f is a finite sum of monomials, we can write

$$f = \sum_{(i_1,\ldots,i_m)\in I} a_{i_1,\ldots,i_m} x_1^{i_1} \cdots x_m^{i_m}$$

where I is a finite index set.

Defining new variables $y_1, \ldots, y_m$ by $x_1 = y_1, x_2 = y_2y_1^l, \ldots, x_m = y_my_1^{l^{m-1}}$, and letting $\mathbf{i} = (i_1, \ldots, i_m)$ and $\mathbf{l} = (1, l, l^2, \ldots, l^{m-1})$, we have

$$\begin{aligned} f &= \sum_{\mathbf{i}\in I} a_{\mathbf{i}} x_1^{i_1} \cdots x_m^{i_m} \\ &= \sum_{\mathbf{i}\in I} a_{\mathbf{i}} y_1^{i_1} (y_2^{i_2} y_1^{i_2 l}) \cdots (y_m^{i_m} y_1^{i_m l^{m-1}}) \\ &= \sum_{\mathbf{i}\in I} a_{\mathbf{i}} y_1^{i_1+i_2 l+\cdots i_m l^{m-1}} y_2^{i_2} \cdots y_m^{i_m} \\ &= \sum_{\mathbf{i}\in I} a_{\mathbf{i}} y_1^{\mathbf{i}\cdot\mathbf{l}} y_2^{i_2} \cdots y_m^{i_m}. \end{aligned}$$

Now, as in the proof of the usual Noether Normalization Lemma, by choosing a sufficiently large l, we can make the integers $\mathbf{i}\cdot\mathbf{l}$ for $\mathbf{i} \in I$ all distinct. Let

$$\begin{aligned} p &= \min\{\mathbf{i}\cdot\mathbf{l} \mid i \in I\} \\ q &= \max\{\mathbf{i}\cdot\mathbf{l} \mid i \in I\}. \end{aligned}$$

Then we can write

$$f = b_p y_1^p + b_{p+1} y_1^{p+1} + \cdots + b_q y_1^q$$

where all the b_i's are units of $k[y_2^{\pm 1}, \ldots, y_m^{\pm 1}]$, i.e. monomials. □

6.3 Description of the Algorithm

Let $n \geq 2$, $S = k[x_2^{\pm 1}, \ldots, x_m^{\pm 1}]$, and $\mathbf{v} = (v_1, \ldots, v_n)^t \in (k[\boldsymbol{x}^{\pm 1})^n = (S[x_1])^n$. By using the algorithm **LaurentNoether**, we may assume that the leading and the lowest coefficients of v_1 w.r.t. x_1 are invertible elements of S. Write

$$v_1 = a_p x_1^p + a_{p+1} x_1^{p+1} + \cdots + a_q x_1^q$$

where a_p and a_q are units of S.

- **Step 1:** Using the invertibility of $a_p \in S$, define $\mathbf{D} \in \mathrm{M}_n(S[x_1^{\pm 1}])$ and $\mathbf{v}' \in (S[x_1^{\pm 1}])^n$ by

$$\begin{aligned}
\mathbf{D} &:= \begin{pmatrix} a_p^{-1}x_1^{-p} & 0 & \\ 0 & a_p x_1^p & \\ & & I_{n-2} \end{pmatrix} \\
\mathbf{v}' &= (v_1', \ldots, v_n')^t := \mathbf{D}\mathbf{v}.
\end{aligned}$$

Note here that the matrix

$$\mathbf{D} = \mathbf{E}_{21}(a_p x_1^p)\mathbf{E}_{12}(1 - a_p^{-1}x_1^{-p})\mathbf{E}_{21}(1)\mathbf{E}_{12}(1 - a_p x_1^p)$$

is realizable over $S[x_1^{\pm 1}]$, and

$$v_1' = a_p^{-1}x_1^{-p}v_1 = 1 + a_{p+1}/a_p x_1 + \cdots + a_q/a_p x_1^{q-p}$$

is a **polynomial** in $S[x_1]$.

- **Step 2:** Since the constant term of $v_1' \in S[x_1]$ is 1, by adding suitable multiples of v_1' to v_i''s, $i = 2, \ldots, n$, we can make $v_2', \ldots, v_n'$ polynomials in $S[x_1]$ whose constant terms are zero, i.e. find $\mathbf{E} \in E_n(k[\boldsymbol{x}^{\pm 1}])$ such that

$$\mathbf{E}\mathbf{v}' = \hat{\mathbf{v}} = \begin{pmatrix} \hat{v}_1 \\ \vdots \\ \hat{v}_n \end{pmatrix} \in (S[x_1])^n,$$

where $\hat{v}_1 \equiv 1 \bmod x_1$ and $\hat{v}_i \equiv 0 \bmod x_1$ for all $i = 2, \ldots, n$.

- **Step 3:** Choose a sufficiently large number $l \in \mathbb{N}$ so that, with the following change of variables,

$$\begin{aligned}
x_1 &= y_1 \cdot (y_2 \cdots y_m)^l \\
x_2 &= y_2 \\
&\vdots \\
x_m &= y_m,
\end{aligned}$$

all the $\hat{v}_i$'s become polynomials in $k[\boldsymbol{y}]$. Then $\hat{v}_1 \equiv 1 \bmod y_1 \cdots y_m$.

Now give the transformation matrix $\mathbf{T} := \mathbf{ED}$ as the output.

Lemma 6.3.1 *With the notations as in the above,* $\mathbf{v}(\boldsymbol{x})$ *is unimodular over* $k[\boldsymbol{x}^{\pm 1}]$ *if and only if* $\hat{\mathbf{v}}(\boldsymbol{y})$ *is unimodular over* $k[\boldsymbol{y}]$.

Proof: ($\Longleftarrow$) The unimodularity of $\hat{\mathbf{v}}(\boldsymbol{y})$ over $k[\boldsymbol{y}]$ trivially implies the unimodularity of $\hat{\mathbf{v}}(\boldsymbol{x})$ over $k[\boldsymbol{x}^{\pm 1}]$. This, together with the unimodularity of $\mathbf{T} \in \mathrm{M}_n(k[\boldsymbol{x}^{\pm 1}])$ immediately implies the unimodularity of $\mathbf{v}(\boldsymbol{x}) = \mathbf{T}^{-1}\hat{\mathbf{v}}(\boldsymbol{x})$ over $k[\boldsymbol{x}^{\pm 1}]$.

($\Longrightarrow$) Since $\hat{\mathbf{v}}$ is a unimodular column vector over $k[\boldsymbol{y}^{\pm 1}]$, we can use Gröbner bases to find $h_1, \ldots, h_n \in k[\boldsymbol{y}]$ and $k \in \mathbb{N}$ such that

$$h_1\hat{v}_1 + \cdots + h_n\hat{v}_n \quad = \quad (y_1 \cdots y_m)^k.$$

Since $\hat{v}_1 \equiv 1 \bmod y_1 \cdots y_m$, we can find $g \in k[\boldsymbol{y}]$ such that

$$\hat{v}_1 \quad = \quad 1 + g \cdot (y_1 \cdots y_m).$$

Now, define recursively a sequence of polynomials $\{f_i \in k[\boldsymbol{y}] \mid i \in \mathbb{N}\}$ in the following way:

$$\begin{aligned} f_1 &= 1 - g \cdot (y_1 \cdots y_m) \\ f_{i+1} &= (1 - g^{2^i} \cdot (y_1 \cdots y_m)^{2^i}) \cdot f_i. \end{aligned}$$

Then the f_i's defined in this way satisfy the following property:

$$\begin{aligned} f_1\hat{v}_1 &= (1 - g \cdot (y_1 \cdots y_m)) \cdot (1 + g \cdot (y_1 \cdots y_m)) = 1 - g^2 \cdot (y_1 \cdots y_m)^2 \\ f_2\hat{v}_1 &= (1 - g^2 \cdot (y_1 \cdots y_m)^2) \cdot f_1\hat{v}_1 = 1 - g^4 \cdot (y_1 \cdots y_m)^4 \\ &\vdots \\ f_i\hat{v}_1 &= 1 - g^{2^i}(y_1 \cdots y_m)^{2^i}. \end{aligned}$$

Let $r \in \mathbb{N}$ be the smallest number such that $2^r \geq k$, and define $h \in k[\boldsymbol{y}]$ by $h = g^{2^r}(y_1 \cdots y_m)^{2^r - k}$. Then,

$$\begin{aligned} 1 &= f_r\hat{v}_1 + g^{2^r}(y_1 \cdots y_m)^{2^r} \\ &= f_r\hat{v}_1 + g^{2^r}(y_1 \cdots y_m)^{2^r - k} \cdot (h_1\hat{v}_1 + \cdots + h_n\hat{v}_n) \\ &= f_r\hat{v}_1 + h(h_1\hat{v}_1 + \cdots + h_n\hat{v}_n) \\ &= (f_r + hh_1)\hat{v}_1 + hh_2\hat{v}_2 + \cdots + hh_n\hat{v}_n. \end{aligned}$$

This gives a required unimodular relation. $\square$

Chapter 7

Parahermitian Modules and Paraunitary Groups

7.1 Introduction

Let R be a commutative ring with an involution σ, and

$$G = \{x_1^{n_1} x_2^{n_2} \cdots x_m^{n_m} \mid n_1, n_2, \ldots n_m \in \mathbb{Z}\}$$

be the free abelian group with m generators $x_1, x_2, \ldots x_m$. Then the Laurent polynomial ring over R,

$$R[\boldsymbol{x}^{\pm 1}] := R[x_1^{\pm 1}, \ldots, x_m^{\pm 1}] = R[x_1, x_1^{-1}, \ldots, x_m, x_m^{-1}],$$

as viewed as a group ring $R[G]$, has a natural involution σ_p that is compatible with σ, i.e. for $f = \sum a_{i_1 \cdots i_m} x^{i_1} \cdots x^{i_m}$ with $a_{i_1 \cdots i_m} \in R$, $\sigma_p(f) = \sum \sigma(a_{i_1 \cdots i_m}) x^{-i_1} \cdots x^{-i_m}$. One can consider other (actually 2 more) involutions on $R[\boldsymbol{x}^{\pm 1}]$ that extends σ, for one thing, σ_h defined by $\sigma_h(f) = \sum \sigma(a_{i_1 \cdots i_m}) x^{i_1} \cdots x^{i_m}$. Over the polynomial ring $R[\boldsymbol{x}]$, this *polynomial involution* $\sigma_h \mid_{R[\boldsymbol{x}]}$ has been studied in hermitian K-theory for various reasons.

To distinguish the hermitian structure associated with the involution σ_p from the one associated with σ_h, we use the term *parahermitian* in the first case, following its usage in electrical engineering. The unitary group associated with the involution σ_p is called the *paraunitary group*. The coefficient ring R for us will mainly be $\mathbb{R}$ or $\mathbb{C}$. Among the signal processing researchers, it is well recognized that an element of this paraunitary group represents a lossless or energy-preserving system. When $m = 0$, paraunitary matrices are just ordinary unitary matrices and, over $\mathbb{R}$, they are simply a product of rotations (up to sign). When $m = 1$ (1-D case), a classification theorem on the paraunitary group was obtained by P. P. Vaidyanathan [Vai93], which, over $\mathbb{R}$, asserts that *rotations* (constant unitary matrices) and *delays* (diagonal matrices with monomial entries) generate the paraunitary group $\mathrm{U}_n(\mathbb{R}[x^{\pm 1}])$. As for its multivariable analogue, while there was a conjecture asserting the existence of a similar factorization in the multivariable case (e.g. [HP94]), S. Venkataraman and B. Levy ([VL94]) successfully used the theory of 2-D state space to construct a numerical example of a paraunitary matrix in $\mathrm{M}_2(\mathbb{C}[X, Y])$ that is not factorizable into any smaller paraunitary polynomial matrices.

In the following section 2, the general aspect of the hermitian modules over the Laurent polynomial ring $R[\boldsymbol{x}^{\pm 1}]$ arising from the involution σ_p is studied. In the remaining sections, we study the structure of the paraunitary group $\mathrm{U}_n(\mathbb{C}[\boldsymbol{x}^{\pm 1}])$, $n \geq 2$, in particular, its subgroup of the completely separable paraunitary matrices, i.e. those that can be written as a product of constant unitary matrices and delays. We do this by giving a convex geometric look at the system of polynomials involved. As an application of these techniques, we will construct a closed form 2×2 paraunitary matrix that is not factorizable into rotations and delays.

7.2 Orthogonal Summands of Parahermitian Modules

Definition 7.2.1 *Suppose $\mathcal{M}$ is a finitely generated projective module over a Laurent polynomial ring $R[\boldsymbol{x}^{\pm 1}]$, and $\langle , \rangle$ is a hermitian sesquilinear form on $\mathcal{M}$ w.r.t the involution σ_p. We call a pair $(\mathcal{M}, \langle , \rangle)$ a* **parahermitian space** *over $R[\boldsymbol{x}^{\pm 1}]$ if $\langle , \rangle$ is nonsingular, i.e. if its adjoint $h : \mathcal{M} \to \mathcal{M}^*$ defined by $h(\mathbf{v}) = \langle \mathbf{v}, \cdot \rangle$ for $\mathbf{v} \in \mathcal{M}$ is an isomorphism.*

On $R = \mathbb{C}$, we take σ to be the usual complex conjugation, i.e. $\sigma(a) = \bar{a}$ for any $a \in \mathbb{C}$. For any $f \in \mathbb{C}[\boldsymbol{x}^{\pm 1}]$, we simply denote $\sigma_p(f)$ by $\tilde{f}$.

Definition 7.2.2 *For a matrix $\mathbf{H} = (h_{i,j}) \in \mathrm{M}_{kl}(\mathbb{C}[\boldsymbol{x}^{\pm 1}])$, its* **parahermitian conjugate** *$\tilde{\mathbf{H}} = (h'_{i,j}) \in \mathrm{M}_{lk}(\mathbb{C}[\boldsymbol{x}^{\pm 1}])$ is defined by $h'_{i,j} = \widetilde{h_{j,i}}$. We call a square matrix $\mathbf{H} \in \mathrm{M}_n(\mathbb{C}[\boldsymbol{x}^{\pm 1}])$* **parahermitian** *if it satisfies $\tilde{\mathbf{H}} = \mathbf{H}$.*

Example 7.2.3 Let $\mathbf{H}_1 = \begin{pmatrix} 1-x & 2+1/y \\ y/x & 1+i \end{pmatrix} \in \mathrm{M}_2(\mathbb{C}[x^{\pm 1}, y^{\pm 1}])$. Then one gets $\tilde{\mathbf{H}}_1 =$

$\begin{pmatrix} 1-1/x & x/y \\ 2+y & 1-i \end{pmatrix}$. For $\mathbf{H}_2 = \begin{pmatrix} x+1/x & y+1/x \\ 1/y+x & xy-1+1/xy \end{pmatrix}$, one checks easily that $\tilde{\mathbf{H}}_2 = \mathbf{H}_2$. Therefore, $\mathbf{H}_2$ is parahermitian while $\mathbf{H}_1$ is not. □

Definition 7.2.4 *A square matrix* $\mathbf{H} \in \mathrm{M}_n(\mathbb{C}[\boldsymbol{x}^{\pm 1}])$ *is called* **paraunitary** *if it satisfies* $\tilde{\mathbf{H}} \cdot \mathbf{H} = \mathbf{H} \cdot \tilde{\mathbf{H}} = I$. *The* **paraunitary group**, $\mathrm{U}_n(\mathbb{C}[\boldsymbol{x}^{\pm 1}])$, *is the group of all the* $n \times n$ *paraunitary matrices in* $\mathrm{M}_n(\mathbb{C}[\boldsymbol{x}^{\pm 1}])$.

Remark 7.2.5 Let $\mathbf{H}(x_1, \ldots, x_m) \in \mathrm{M}_n(\mathbb{C}[\boldsymbol{x}^{\pm 1}])$ be paraunitary, and $(a_1, \ldots, a_m)$ be a point on the topological torus $S^1 \times \cdots \times S^1$. Then $\mathbf{H}(a_1, \ldots, a_m) \in \mathrm{M}_n(\mathbb{C})$ is just unitary as a matrix over $\mathbb{C}$ (because $\bar{a_i} = a_i^{-1}$ for any $a_i \in S^1$). This shows that a paraunitary matrix is a natural Laurent polynomial analogue of a unitary matrix.

Remark 7.2.6 For the free $\mathbb{C}[\boldsymbol{x}^{\pm 1}]$-module $(\mathbb{C}[\boldsymbol{x}^{\pm 1}])^n$, define a sesquilinear form $\langle , \rangle$ on $(\mathbb{C}[\boldsymbol{x}^{\pm 1}])^n$ by $\langle \mathbf{v}, \mathbf{w} \rangle = \sum_{i=1}^n \tilde{v}_i w_i$ where $\mathbf{v} = \sum_{i=1}^n v_i \mathbf{e}_i, \mathbf{w} = \sum_{i=1}^n w_i \mathbf{e}_i \in (\mathbb{C}[\boldsymbol{x}^{\pm 1}])^n$ with $\{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$ being the standard basis of $(\mathbb{C}[\boldsymbol{x}^{\pm 1}])^n$. Then, $((\mathbb{C}[\boldsymbol{x}^{\pm 1}])^n, \langle , \rangle)$ becomes a parahermitian space, and a paraunitary matrix $\mathbf{H} \in \mathrm{U}_n(\mathbb{C}[\boldsymbol{x}^{\pm 1}])$ defines an isometry from $((\mathbb{C}[\boldsymbol{x}^{\pm 1}])^n, \langle , \rangle)$ onto itself.

One deduces easily that an $n \times n$ matrix $\mathbf{H}$ over $\mathbb{C}[\boldsymbol{x}^{\pm 1}]$ is paraunitary if and only if its column vectors (or row vectors), $\mathbf{v}_1, \ldots, \mathbf{v}_n$, satisfy the usual orthonormality condition: $\langle \mathbf{v}_i, \mathbf{v}_j \rangle = \delta_{ij}$.

Example 7.2.7 Consider $\mathbf{H} = \frac{1}{\sqrt{2}} \begin{pmatrix} x^2 & x \\ xy^2 & -y^2 \end{pmatrix} \in \mathrm{M}_2(\mathbb{C}[x^{\pm 1}, y^{\pm 1}])$. Then, one verifies easily that $\tilde{\mathbf{H}} \cdot \mathbf{H} = \mathbf{H} \cdot \tilde{\mathbf{H}} = I$. So, $\mathbf{H}$ is paraunitary. Let $\mathbf{v} = \frac{1}{\sqrt{2}}(x^2, xy^2)^t$ and $\mathbf{w} = \frac{1}{\sqrt{2}}(x, -y^2)^t$ be the column vectors of $\mathbf{H}$. Then,

- $\langle \mathbf{v}, \mathbf{v} \rangle = \frac{1}{2}(\frac{1}{x^2}, \frac{1}{xy^2}) \begin{pmatrix} x^2 \\ xy^2 \end{pmatrix} = 1$
- $\langle \mathbf{w}, \mathbf{w} \rangle = \frac{1}{2}(\frac{1}{x}, \frac{-1}{y^2}) \begin{pmatrix} x \\ -y^2 \end{pmatrix} = 1$
- $\langle \mathbf{v}, \mathbf{w} \rangle = \frac{1}{2}(\frac{1}{x^2}, \frac{1}{xy^2}) \begin{pmatrix} x \\ -y^2 \end{pmatrix} = 0$

This shows that $\mathbf{v}$ and $\mathbf{w}$ are unit norm vectors in $\mathbb{C}[x^{\pm 1}, y^{\pm 1}]^2$ that are orthogonal to each other. □

Remark 7.2.8 Let $\mathcal{M}$ be a submodule of $(\mathbb{C}[\boldsymbol{x}^{\pm 1}])^n$ that splits as a direct summand. Then $\mathcal{M}$ is projective. Now by the theorem of R. G. Swan [Swa78] that generalizes the *Quillen-Suslin theorem* over polynomial rings to the same statement over Laurent polynomial rings, $\mathcal{M}$ is free.

Let $\{\mathbf{v}_1, \ldots, \mathbf{v}_k\}$ be a free basis of $\mathcal{M}$, $k \leq n$. Then the adjoint of $\langle , \rangle \mid_{\mathcal{M}}$ is described by the $k \times k$ matrix $(\langle \mathbf{v}_i, \mathbf{v}_j \rangle)$. Therefore, $(\mathcal{M}, \langle , \rangle \mid_{\mathcal{M}})$ is nonsingular if and only if $\det(\langle \mathbf{v}_i, \mathbf{v}_j >)$ is a unit of $\mathbb{C}[\boldsymbol{x}^{\pm 1}]$. In this case, $(\mathcal{M}, \langle , \rangle \mid_{\mathcal{M}})$ itself forms a parahermitian space.

Conversely, if $(\mathcal{M}, \langle , \rangle \mid_{\mathcal{M}}) \subset ((\mathbb{C}[\boldsymbol{x}^{\pm 1}])^n, \langle , \rangle)$ is a parahermitian subspace, then the following proposition states that $\mathcal{M} \subset (\mathbb{C}[\boldsymbol{x}^{\pm 1}])^n$ is a projective submodule that splits as an orthogonal summand.

Proposition 7.2.9 *1. Let $(\mathcal{U}, \langle , \rangle)$ be a parahermitian module over $\mathbb{C}[\boldsymbol{x}^{\pm 1}]$ and $\mathcal{M}$ be a submodule of $\mathcal{U}$ which is finitely generated and projective.*

If $(\mathcal{M}, \langle , \rangle \mid_{\mathcal{M}})$ is nonsingular, then

$$(\mathcal{U}, \langle , \rangle) \quad = \quad (\mathcal{M}, \langle , \rangle \mid_{\mathcal{M}}) \perp (\mathcal{M}^{\perp}, \langle , \rangle \mid_{\mathcal{M}^{\perp}}).$$

2. If there exist parahermitian modules $(\mathcal{U}_i, \langle , \rangle_i)$, $i = 1, 2$, such that

$$(\mathcal{U}, \langle , \rangle) \simeq (\mathcal{U}_1, \langle , \rangle_1) \perp (\mathcal{U}_2, \langle , \rangle_2),$$

then $\langle , \rangle_i$, $i = 1, 2$ are nonsingular if and only if $\langle , \rangle$ is nonsingular.

Proof: See Lemma 3.6.2 in [Knu91]. □

From now on, we will identify $\mathbf{v} = \sum_{i=1}^{n} v_i \mathbf{e}_i \in (\mathbb{C}[\boldsymbol{x}^{\pm 1}])^n$ with the column vector $(v_1, \ldots, v_n)^t$. Also, we will denote the Laurent polynomial ring $\mathbb{C}[\boldsymbol{x}^{\pm 1}]$ by A.

Corollary 7.2.10 *Let $(\mathcal{M}, \langle , \rangle \mid_{\mathcal{M}}) \subset (A^n, \langle , \rangle)$ be a parahermitian subspace, and $\mathbf{v} \in \mathcal{M}$. Consider the submodule $A\mathbf{v} \subset \mathcal{M}$ of rank 1.*

1. $A\mathbf{v} \subset \mathcal{M}$ splits as a direct summand if and only if $\mathbf{v} \in A^n$ is unimodular.

2. $(A\mathbf{v}, \langle , \rangle \mid_{A\mathbf{v}}) \subset (\mathcal{M}, \langle , \rangle)$ splits as an orthogonal summand if and only if $\langle \mathbf{v}, \mathbf{v} \rangle \in \mathbb{R}_{>0}$.

Proof: (1) This is the Lemma 3.1.4.

(2) If $\langle \mathbf{v}, \mathbf{v} >\rangle \in \mathbb{R}_{>0}$, then $\mathbf{v}$ is clearly unimodular, and thus by the first part of this **Corollary**, $A\mathbf{v}$ is a direct summand of $\mathcal{M}$. Hence, in view of *Proposition 7.2.9*, we only need to check if $\langle , \rangle \mid_{A\mathbf{v}}$ is nonsingular. As we observed in the **Remark** 7.2.8, $\langle , \rangle \mid_{A\mathbf{v}}$ is nonsingular since $\det(\langle \mathbf{v}, \mathbf{v}\rangle) = \langle \mathbf{v}, \mathbf{v}\rangle \in A^*$.

Conversely, if $(A\mathbf{v}, \langle , \rangle \mid_{A\mathbf{v}}) \subset (\mathcal{M}, \langle , \rangle)$ splits as an orthogonal summand, then $\langle , \rangle \mid_{A\mathbf{v}}$ is nonsingular, which occurs precisely when $\det(\langle \mathbf{v}, \mathbf{v}\rangle) = \langle \mathbf{v}, \mathbf{v}\rangle \in A^*$. Now, the following *Lemma* gives the result. □

Lemma 7.2.11 *Let* $A = \mathbb{C}[\boldsymbol{x}^{\pm 1}]\}$, *and* $\mathbf{v} \in A^n$. *Then,*

$$\langle \mathbf{v}, \mathbf{v}\rangle \in A^* \iff \langle \mathbf{v}, \mathbf{v}\rangle \in \mathbb{R}_{>0}.$$

Proof: One direction ($\Longleftarrow$) is obvious.

If $\langle \mathbf{v}, \mathbf{v}\rangle \in A^*$, then $\langle \mathbf{v}, \mathbf{v}\rangle$ is a nonzero monomial in $A = \mathbb{C}[\boldsymbol{x}^{\pm 1}]$ satisfying $\overline{\langle \mathbf{v}, \mathbf{v}\rangle} = \langle \mathbf{v}, \mathbf{v}\rangle$. Involution invariant nonzero monomials in A are just nonzero real numbers. To show that $\langle \mathbf{v}, \mathbf{v}\rangle$ is a positive real number, write $\mathbf{v} = \sum \mathbf{v}_{i_1 \cdots i_m} x^{i_1} \cdots x^{i_m}$ with $\mathbf{v}_{i_1 \cdots i_m} \in \mathbb{R}^n$. Then, by an explicit computation, we see that the constant term of $\langle \mathbf{v}, \mathbf{v}\rangle$ is equal to $\sum \| \mathbf{v}_{i_1 \cdots i_m} \|^2$ which must be same as the nonzero real number $\langle \mathbf{v}, \mathbf{v}\rangle$. □

Example 7.2.12 Let $A = \mathbb{C}[x^{\pm 1}, y^{\pm 1}]$, $\mathcal{M} = A^2$, $\mathbf{v}_1 = (1 - xy, x^2)^t \in \mathcal{M}$, and $\mathbf{v}_2 = (1 - xy, 1 + xy)^t \in \mathcal{M}$. Then both of $\mathbf{v}_1$ and $\mathbf{v}_2$ are unimodular since $(1+xy)\cdot(1-xy) + y^2 \cdot x^2 = 1$ and $\frac{1}{2} \cdot (1 - xy) + \frac{1}{2} \cdot (1 + xy) = 1$. Therefore, both of $A\mathbf{v}_1$ and $A\mathbf{v}_2$ are direct summands of $\mathcal{M}$. However, since

$$\begin{aligned}
\langle \mathbf{v}_1, \mathbf{v}_1\rangle &= (1 - \frac{1}{xy})(1 - xy) + \frac{1}{x^2}x^2 \notin A^*, \\
\langle \mathbf{v}_2, \mathbf{v}_2\rangle &= (1 - \frac{1}{xy})(1 - xy) + (1 + \frac{1}{xy})(1 + xy) = 4 \in A^*,
\end{aligned}$$

we see that $A\mathbf{v}_1$ is not an orthogonal summand of $\mathcal{M}$ while $A\mathbf{v}_2$ is. Actually, we claim that $\mathbf{w}_1 = (-y^2, 1 + xy)^t$ and $\mathbf{w}_2 = (1 + xy, 1 - xy)^t$ satisfy

$$\begin{aligned}
A\mathbf{v}_1 \oplus A\mathbf{w}_1 &= \mathcal{M} \\
A\mathbf{v}_2 \perp A\mathbf{w}_2 &= \mathcal{M}.
\end{aligned}$$

First, in order to show $A\mathbf{v}_1 \oplus A\mathbf{w}_1 = \mathcal{M}$, it is enough to show that any $(f, g)^t \in \mathcal{M}$ can be uniquely written in the form, $f'\mathbf{v}_1 + g'\mathbf{w}_1$, for some $f', g' \in A$. This translates into the following linear system:

$$\begin{pmatrix} 1-xy & -y^2 \\ x^2 & 1+xy \end{pmatrix} \begin{pmatrix} f' \\ g' \end{pmatrix} = \begin{pmatrix} f \\ g \end{pmatrix}.$$

This system has unique solution since $\det \begin{pmatrix} 1-xy & -y^2 \\ x^2 & 1+xy \end{pmatrix} = 1$, i.e.

$$\begin{pmatrix} 1-xy & -y^2 \\ x^2 & 1+xy \end{pmatrix} \in GL_2(A).$$

To show $A\mathbf{v}_2 \perp A\mathbf{w}_2 = \mathcal{M}$, first verify in the same manner that $A\mathbf{v}_2 \oplus A\mathbf{w}_2 = \mathcal{M}$, and then note that

$$\begin{aligned} \langle \mathbf{v}_2, \mathbf{v}_2 \rangle &= 4 \in A^*, \\ \langle \mathbf{w}_2, \mathbf{w}_2 \rangle &= 4 \in A^*, \\ \langle \mathbf{v}_2, \mathbf{w}_2 \rangle &= (1 - 1/xy)(1+xy) + (1+1/xy)(1-xy) = 0. \end{aligned}$$

7.3 Paraunitary Completion

Suppose that $\mathbf{H}$ $(n > k)$ is an $n \times k$ paraunitary matrix over $A := \mathbb{C}[\boldsymbol{x}^{\pm 1}]$, i.e. a rectangular matrix with entries in A whose column vectors are orthonormal to each other. Now the question is,

Can we complete this matrix to a square $n \times n$ paraunitary matrix by adding more columns to it?

Let $\mathbf{v}_1, \ldots, \mathbf{v}_k \in A^n$ be the column vectors of $\mathbf{H}$, and $\mathcal{V} \subset A^n$ be the submodule of A^n generated by these vectors. Then since $\mathcal{V}$ is an orthogonal summand of A^n, we have $\mathcal{V} \perp \mathcal{V}^\perp = A^n$. Now the above question can be rephrased as,

Can we find an orthonormal basis of $\mathcal{V}^\perp$?

If the answer to this question is positive, then the members of this orthonormal basis will be the extra column vectors we can add to $\mathbf{H}$ to make a square paraunitary matrix.

Let $\mathrm{V}_n(A)$ be the set of the n-dimensional vectors over A of unit norm, and $\mathrm{W}_n(A)$ be the subset of $\mathrm{V}_n(A)$ consisting of the vectors of norm equal to 1. Note that, according to the Corollary 7.2.10 and Lemma 7.2.11,

$$\begin{aligned}
\mathrm{V}_n(A) &= \{\mathbf{v} \in A^n \mid <\mathbf{v},\mathbf{v}> \in A^*\} \\
&= \{\mathbf{v} \in A^n \mid <\mathbf{v},\mathbf{v}> \in \mathbb{R}_{>0}\} \\
&= \{\mathbf{v} \in A^n \mid A\mathbf{v} \text{ separates as a 1-dimensional orthogonal} \\
&\qquad \text{summand of } A^n\}. \qquad (7.1)
\end{aligned}$$

The paraunitary group $\mathrm{U}_n(A)$ acts on the set $\mathrm{W}_n(A)$ by matrix multiplication, and the above problem of paraunitray completion can also be expressed in terms of the transitivity of this group action. For $\mathbf{v}, \mathbf{w} \in \mathrm{W}_n(A)$, we will denote $\mathbf{v} \overset{\mathrm{U}_n}{\sim} \mathbf{w}$ if there exists $\mathbf{U} \in \mathrm{U}_n(A)$ such that $\mathbf{v} = \mathbf{U}\mathbf{w}$.

Proposition 7.3.1 *The paraunitary completion problem has a positive answer if and only if the above group action of* $\mathrm{U}_n(A)$ *on* $\mathrm{W}_n(A)$ *is transitive.*

Proof: An easy exercise. □

Lemma 7.3.2 *Any paraunitary matrix* $\mathbf{H} \in \mathrm{U}_2(A)$ *can be written uniquely in the form*

$$\mathbf{H} = \begin{pmatrix} f & -\alpha\tilde{g} \\ g & \alpha\tilde{f} \end{pmatrix} \qquad (7.2)$$

for a vector $\begin{pmatrix} f \\ g \end{pmatrix} \in A^2$ *of norm* 1*, and a monomial* $\alpha \in A$*.*

Proof: Let the first column of $\mathbf{H}$ be $\mathbf{v} = \begin{pmatrix} f \\ g \end{pmatrix}$, which is clearly of unit norm. Then by Corollary 7.2.10, $A\mathbf{v}$ splits as an orthogonal summand of A^2. And its orthogonal complement $(A\mathbf{v})^\perp$ is a free submodule of A^2 of rank 1 whose generator can be any of its elements of unit norm. We easily see that $\mathbf{w} = \begin{pmatrix} -\tilde{g} \\ \tilde{f} \end{pmatrix}$ is one such element of $(A\mathbf{v})^\perp$. Since the second column vector of $\mathbf{H}$ is in $(A\mathbf{v})^\perp$, it can be written as $\alpha\mathbf{v}$ for some $\alpha \in A$, and since it is also of unit norm, α should be a unit of $A = \mathbb{C}[\boldsymbol{x}^{\pm 1}]$ which must be a monomial. □

Proposition 7.3.3 $\mathrm{U}_2(A)$ *acts transitively on* $\mathrm{W}_2(A)$*.*

Proof: It's enough to show that $\mathbf{v} \overset{\mathrm{U}_n}{\sim} (1,0)^t$ for any $\mathbf{v} = (v_1, v_2)^t \in \mathrm{W}_n(A)$. For this purpose, define $\mathbf{U} \in \mathrm{M}_2(A)$ by

$$\mathbf{U} = \begin{pmatrix} \tilde{v_1} & \tilde{v_2} \\ -v_2 & v_1 \end{pmatrix}.$$

Using $\langle \mathbf{v}, \mathbf{v} \rangle = \tilde{v}_1 v_1 + \tilde{v}_2 v_2 = 1$, one easily checks that $\mathbf{U}$ is paraunitary i.e. $\tilde{\mathbf{U}}\mathbf{U} = I$ and satisfy $\mathbf{U}\mathbf{v} = (1, 0)^t$. □

Remark 7.3.4 It is still an open problem to determine if the group action of $\mathrm{U}_n(A)$ on $\mathrm{W}_n(A)$ is transitive for $n \geq 3$. The transitivity can be deduced if the *parahermitian analogue of Serre's conjecture* is true, that is, if any parahermitian space is isometric to a free module with trivial inner product. This problem will be more carefully analyzed elsewhere. However, when $m = 1$, more can be said without this conjecture. Actually, it will be shown in the next section that the separable subgroup $\mathrm{S}_n(\mathbb{C}[x^{\pm 1}])$ of $\mathrm{U}_n(\mathbb{C}[x^{\pm 1}])$ generated by constant unitary matrices (elements of $\mathrm{U}_n(\mathbb{C})$) and delays (diagonal matrices with monomial entries) already acts transitively on $\mathrm{W}_n(\mathbb{C}[x^{\pm 1}])$. This means that any rectangular paraunitary matrix over $\mathbb{C}[x^{\pm 1}]$ can be completed to a square paraunitary matrix.

We will need the following lemma later.

Lemma 7.3.5 *The determinant of a paraunitary matrix* $\mathbf{H} \in \mathrm{U}_n(A)$ *is a monomial of the form* $\alpha \boldsymbol{x}^{\mathbf{n}}$ *for some* $\mathbf{n} = (n_1, \ldots, n_m) \in \mathbb{Z}^m$ *and* $\alpha \in \mathbb{C}$ *with* $\|\alpha\| = 1$.

Proof: From $\mathbf{H} \cdot \tilde{\mathbf{H}} = I$, we see that $\det(\mathbf{H}) \cdot \det(\tilde{\mathbf{H}}) = 1$, i.e. $\det(\mathbf{H})$ is an invertible element of $\mathbb{C}[\boldsymbol{x}^{\pm 1}]$, which must be a monomial. Let $\det(\mathbf{H}) = \alpha \boldsymbol{x}^{\mathbf{n}}$. Then $\det(\tilde{\mathbf{H}}) = \bar{\alpha} \boldsymbol{x}^{-\mathbf{n}}$. Now, $\det(\mathbf{H}) \cdot \det(\tilde{\mathbf{H}}) = 1$ gives $\alpha \bar{\alpha} = 1$. □

7.4 Paraunitary Groups over $\mathbb{C}[x^{\pm 1}]$

If $\mathbf{v} \in \mathrm{W}_n(\mathbb{C}[x^{\pm 1}])$ is a monomial vector, i.e. $\mathbf{v} = \mathbf{v}_0 x^k$ for $\mathbf{v}_0 \in \mathbb{C}^n$ and $k \in \mathbb{Z}$, then it is easy to see that $\mathbf{v} \overset{\mathrm{S}_n}{\approx} (1, 0, \ldots, 0)^t$. That is, since $\mathbf{v} \in \mathrm{W}_n(A)$, we have

$$\langle \mathbf{v}, \mathbf{v} \rangle = 1 = < x^k \mathbf{v}_0, x^k \mathbf{v}_0 > = \langle \mathbf{v}_0, \mathbf{v}_0 > = \| \mathbf{v}_0 \|^2 .$$

Now find an orthonormal basis $\{\mathbf{w}_1, \ldots, \mathbf{w}_{n-1}\}$ of $(\mathbb{C}\mathbf{v}_0)^\perp \subset \mathbb{C}^n$ (the standard Gram-Schmidt process will do this). Then the matrix

$$\mathbf{U} = (\mathbf{v}_0, \mathbf{w}_1, \ldots, \mathbf{w}_{n-1}) \in \mathrm{M}_n(\mathbb{C})$$

is clearly unitary. Denoting the delay, $\mathrm{diag}(x, 1, \ldots, 1) \in \mathrm{M}_n(\mathbb{C}[x^{\pm 1}])$, by $\mathbf{D}$, we have

$$\mathbf{D}^{-k} \tilde{\mathbf{U}} \mathbf{v} = (1, 0, \ldots, 0)^t.$$

Since $\mathbf{D}^{-k} \tilde{\mathbf{U}} \in \mathrm{S}_n(\mathbb{C}[x^{\pm 1}])$, this implies $\mathbf{v} \overset{\mathrm{S}_n}{\approx} (1, 0, \ldots, 0)^t$.

Lemma 7.4.1 *If* $\mathbf{v} \in \mathrm{W}_n(\mathbb{C}[x^{\pm 1}])$ *is a binomial vector, i.e.* $\mathbf{v} = \mathbf{v}_0 x^k + \mathbf{v}_1 x^l$ *for* $\mathbf{v}_0, \mathbf{v}_1 \in \mathbb{C}^n$ *and* $k < l \in \mathbb{Z}$*, then* $\mathbf{v} \overset{\mathrm{S}_n}{\sim} (1, 0, \ldots, 0)^t$.

Proof: Since the monomial case is considered above, assume that $\mathbf{v}_0 \neq \mathbf{0}$ and $\mathbf{v}_1 \neq \mathbf{0}$.

$$\begin{aligned} 1 &= \langle \mathbf{v}, \mathbf{v} \rangle \\ &= \langle \mathbf{v}_0 x^k + \mathbf{v}_1 x^l, \mathbf{v}_0 x^k + \mathbf{v}_1 x^l > \\ &= \| \mathbf{v}_0 \|^2 + \| \mathbf{v}_1 \|^2 + \langle \mathbf{v}_0, \mathbf{v}_1 > \ x^{l-k} + \ \langle \mathbf{v}_1, \mathbf{v}_0 > \ x^{k-l}. \end{aligned}$$

Therefore, we have $\| \mathbf{v}_0 \|^2 + \| \mathbf{v}_1 \|^2 = 1$ and $\langle \mathbf{v}_0, \mathbf{v}_1 > = \ \langle \mathbf{v}_1, \mathbf{v}_0 > = 0$. Now find an orthonormal basis $\{\mathbf{w}_1, \ldots, \mathbf{w}_{n-1}\}$ of $(\mathbb{C}\mathbf{v}_0)^\perp \subset \mathbb{C}^n$, and define $\mathbf{U}_1 \in \mathrm{M}_n(\mathbb{C})$ by $\mathbf{U}_1 = (\frac{\mathbf{v}_0}{\|\mathbf{v}_0\|}, \mathbf{w}_1, \ldots, \mathbf{w}_{n-1})$ which is clearly unitary. Denote the delay $\mathrm{diag}(x^{-k}, x^{-l}, \ldots, x^{-l}) \in \mathrm{M}_n(A)$ by $\mathbf{D}$, and let $\mathbf{v}' = \mathbf{D}\tilde{\mathbf{U}}_1\mathbf{v}$. Since

$$\begin{aligned} \tilde{\mathbf{U}}_1 \mathbf{v} &= \begin{pmatrix} \frac{\tilde{\mathbf{v}}_0}{\|\mathbf{v}_0\|} \\ \tilde{\mathbf{w}}_1 \\ \vdots \\ \tilde{\mathbf{w}}_{n-1} \end{pmatrix} (\mathbf{v}_0 x^k + \mathbf{v}_1 x^l) \\ &= \begin{pmatrix} \| \mathbf{v}_0 \| \ x^k \\ \langle \mathbf{w}_1, \mathbf{v}_1 > \ x^l \\ \vdots \\ \langle \mathbf{w}_{n-1}, \mathbf{v}_1 > \ x^l \end{pmatrix}, \end{aligned}$$

we see that $\mathbf{v}' = \mathbf{D}\tilde{\mathbf{U}}_1\mathbf{v} = (\| \mathbf{v}_0 \|, \langle \mathbf{w}_1, \mathbf{v}_1 >, \ldots, \langle \mathbf{w}_{n-1}, \mathbf{v}_1 >)^t$, and $\| \mathbf{v}' \| = 1$.

Now find an orthonormal basis $\{\mathbf{w}'_1, \ldots, \mathbf{w}'_{n-1}\}$ of $(\mathbb{C}\mathbf{v}')^\perp \subset \mathbb{C}^n$, and define $\mathbf{U}_2 \in \mathrm{M}_n(\mathbb{C})$ by $\mathbf{U}_2 = (\mathbf{v}', \mathbf{w}'_1, \ldots, \mathbf{w}'_{n-1})$. Then $\tilde{\mathbf{U}}_2\mathbf{v}' = (1, 0, \ldots, 0)^t = \tilde{\mathbf{U}}_2\mathbf{D}\tilde{\mathbf{U}}_1\mathbf{v}$. □

Lemma 7.4.2 *If* $\mathbf{v} \in \mathrm{W}_n(\mathbb{C}[x^{\pm 1}]) \cap \mathrm{M}_n(\mathbb{C}[x])$*, i.e. a polynomial vector of unit norm, then there exists* $\mathbf{S} \in \mathrm{S}_n(\mathbb{C}[x^{\pm 1}]) \cap \mathrm{M}_n(\mathbb{C}[x])$*, a product of constant unitary matrices and negative delays, such that* $\mathbf{S}\mathbf{v} = (1, 0, \ldots, 0)^t$.

Proof: Multiplying by a negative delay if necessary, we may assume without loss of generality that

$$\mathbf{v} \ = \ \mathbf{v}_0 + \mathbf{v}_1 x + \cdots + \mathbf{v}_l x^l, \quad \mathbf{v}_i \in \mathbb{C}^n, \ \mathbf{v}_0 \neq \mathbf{0}, \ \mathbf{v}_l \neq \mathbf{0}.$$

Now the condition $\langle \mathbf{v}, \mathbf{v} \rangle \ \in \mathbb{C}^*$ implies $\langle \mathbf{v}_0, \mathbf{v}_l > = 0$, which means $\mathbf{v}_0 + \mathbf{v}_l x^l$ is a unit norm vector. By the proof of Lemma 7.4.1 above, we can find $\mathbf{U}_1, \mathbf{U}_2 \in \mathrm{U}_n(\mathbb{C})$, and

$c \in \mathbb{R}$ such that

$$\mathbf{v}_0 + \mathbf{v}_l x^l = \mathbf{U}_1 \mathrm{diag}(1, x^l, \cdots, x^l) \mathbf{U}_2 \begin{pmatrix} c \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

From this representation, letting $\tilde{\mathbf{v}}_i = \mathbf{U}_1 \mathbf{v}_i$, we deduce that

$$\begin{aligned} \mathbf{v}_0 + \mathbf{v}_l x^l &= \mathbf{U}_1 \mathrm{diag}(1, x^l, \cdots, x^l) \tilde{\mathbf{U}}_1 (\mathbf{v}_0 + \mathbf{v}_{l-1} x^{l-1}) \\ &= \mathbf{U}_1 \mathrm{diag}(1, x^l, \cdots, x^l)(\tilde{\mathbf{v}}_0 + \tilde{\mathbf{v}}_{l-1} x^{l-1}). \end{aligned}$$

Also, note that

$$\begin{aligned} & \mathbf{v}_1 x + \cdots + \mathbf{v}_{l-1} x^{l-1} \\ = \; & \mathbf{U}_1 \mathrm{diag}(x, x, \cdots, x)(\tilde{\mathbf{v}}_1 + \cdots + \tilde{\mathbf{v}}_{l-1} x^{l-2}) \\ = \; & \mathbf{U}_1 \mathrm{diag}(1, x, \cdots, x) \mathrm{diag}(x, 1, \cdots, 1)(\tilde{\mathbf{v}}_1 + \cdots + \tilde{\mathbf{v}}_{l-1} x^{l-2}). \end{aligned}$$

Therefore, we get

$$\begin{aligned} \mathbf{v} &= (\mathbf{v}_0 + \mathbf{v}_l x^l) + (\mathbf{v}_1 x + \cdots + \mathbf{v}_{l-1} x^{l-1}) \\ &= \mathbf{U}_1 \mathrm{diag}(1, x^l, \cdots, x^l)(\tilde{\mathbf{v}}_0 + \tilde{\mathbf{v}}_{l-1} x^{l-1}) + \\ &\quad\; \mathbf{U}_1 \mathrm{diag}(1, x, \cdots, x) \mathrm{diag}(x, 1, \cdots, 1)(\tilde{\mathbf{v}}_1 + \cdots + \tilde{\mathbf{v}}_{l-1} x^{l-2}) \\ &= \mathbf{U}_1 \mathrm{diag}(1, x^l, \cdots, x^l)\{\tilde{\mathbf{v}}_0 + \tilde{\mathbf{v}}_{l-1} x^{l-1} + \\ &\quad\; \mathrm{diag}(x, 1, \cdots, 1)(\tilde{\mathbf{v}}_1 + \cdots + \tilde{\mathbf{v}}_{l-1} x^{l-2})\}. \end{aligned}$$

Since the degree of the vector polynomial $\tilde{\mathbf{v}}_0 + \tilde{\mathbf{v}}_{l-1} x^{l-1} + \mathrm{diag}(x, 1, \cdots, 1)(\tilde{\mathbf{v}}_1 + \cdots + \tilde{\mathbf{v}}_{l-1} x^{l-2}$ is $l-1$, by induction on the degree, the lemma is proved. $\square$

Now we can use the above lemmas to show the transitivity of $\mathrm{S}_n(\mathbb{C}[x^{\pm 1}])$ on $\mathrm{W}_n(\mathbb{C}[x^{\pm 1}])$.

Proposition 7.4.3 *If $m = 1$, $\mathrm{S}_n(\mathbb{C}[x^{\pm 1}])$ acts transitively on $\mathrm{W}_n(\mathbb{C}[x^{\pm 1}])$.*

Corollary 7.4.4 *If $m = 1$, $\mathrm{U}_n(\mathbb{C}[x^{\pm 1}])$ acts transitively on $\mathrm{W}_n(\mathbb{C}[x^{\pm 1}])$.*

Proof of Proposition: Let $\mathbf{v} \in \mathrm{W}_n(\mathbb{C}[x^{\pm 1}])$. Multiplying by a delay if necessary, we may assume that $\mathbf{v}$ is a polynomial vector, i.e. has no negative exponents involved. Write

$$\mathbf{v} \;=\; \mathbf{v}_0 + \mathbf{v}_1 x + \cdots + \mathbf{v}_l x^l, \quad \mathbf{v}_i \in \mathbb{C}^n, \; \mathbf{v}_0 \neq \mathbf{0} \; \mathbf{v}_k \neq \mathbf{0}.$$

Now the proposition follows from the Lemma 7.4.2. $\square$

Theorem 7.4.5 *(P. P. Vaidyanathan)* $\mathrm{S}_n(\mathbb{C}[x^{\pm 1}]) = \mathrm{U}_n(\mathbb{C}[x^{\pm 1}])$ *for any* $n \geq 2$, *i.e. any paraunitary matrix* $\mathbf{H} \in \mathrm{U}_n(\mathbb{C}[x^{\pm 1}])$ *can be written as a product of constant unitary matrices and delays. If* $\mathbf{H} \in \mathrm{U}_n(\mathbb{C}[x^{\pm 1}]) \cap \mathrm{M}_n(\mathbb{C}[x])$ *is a polynomial matrix, then it can be written as a product of constant unitary matrices and positive delays.*

Proof: Let $\mathbf{v}_1 = \mathbf{H}(1, 0, \ldots, 0)^t \in \mathrm{W}_n(\mathbb{C}[x^{\pm 1}])$ be the first column vector of $\mathbf{H}$. Then by Proposition 7.4.3, there exists $\mathbf{S}_1 \in \mathrm{S}_n(\mathbb{C}[x^{\pm 1}])$ such that

$$\mathbf{S}_1 \mathbf{v}_1 \;=\; (1, 0, \ldots, 0)^t.$$

Since the matrix $\mathbf{S}_1\mathbf{H}$ is again paraunitary, it must be of the following form:

$$\mathbf{S}_1\mathbf{H} \;=\; \begin{pmatrix} 1 & 0 \\ 0 & \mathbf{H}_1 \end{pmatrix}$$

where $\mathbf{H}_1 \in H_{n-1}(\mathbb{C}[x^{\pm 1}])$.

Now apply the same procedure to the first column vector of $\mathbf{H}_1$. Repeating this procedure, we find $\mathbf{S}_1, \ldots, \mathbf{S}_n \in \mathrm{S}_n(\mathbb{C}[x^{\pm 1}])$ such that

$$\mathbf{S}_1 \cdots \mathbf{S}_n \mathbf{U} \;=\; I.$$

This implies that $\mathbf{H} = \tilde{\mathbf{S}}_n \cdots \tilde{\mathbf{S}}_1 \in \mathrm{S}_n(\mathbb{C}[x^{\pm 1}])$, i.e. $\mathbf{H}$ is a product of constant unitary matrices and delays. When $\mathbf{H}$ is a polynomial matrix, the statement follows from the Lemma 7.4.2 since all the $\mathbf{S}_i$'s involved can be chosen to be products of constant unitary matrices and *positive* delays. $\square$

Example 7.4.6 Consider $\mathbf{H} = \frac{1}{4}\begin{pmatrix} \frac{\sqrt{2}}{x} - \sqrt{6} & \sqrt{6} + \sqrt{2}x \\ -\frac{\sqrt{2}}{x^2} - \frac{\sqrt{6}}{x} & -\frac{\sqrt{6}}{x} + \sqrt{2} \end{pmatrix} \in \mathrm{U}_2(\mathbb{C}[x^{\pm 1}])$. One checks easily that $\mathbf{H}$ is paraunitary. Applying the above algorithm, we get the factorization, $\mathbf{H} = \mathbf{D}_0 \cdot (\mathbf{R}_1 \cdot \mathbf{D}_1) \cdot (\mathbf{R}_2 \cdot \mathbf{D}_2)$ where $\mathbf{D}_0 = \begin{pmatrix} \frac{1}{x} & 0 \\ 0 & \frac{1}{x^2} \end{pmatrix}$, $\mathbf{D}_1 = \mathbf{D}_2 = \begin{pmatrix} 1 & 0 \\ 0 & x \end{pmatrix}$ are delays, and $\mathbf{R}_1 = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}$, $\mathbf{R}_2 = \frac{1}{2}\begin{pmatrix} 1 & \sqrt{3} \\ -\sqrt{3} & 1 \end{pmatrix}$ are rotations. $\square$

Definition 7.4.7 *1. The* **standard delay** *in* $\mathrm{U}_n(\mathbb{C}[x^{\pm 1}])$ *is the diagonal matrix* $\mathbf{D}$ *defined by* $\mathbf{D} = \mathrm{diag}(1, \ldots, 1, x)$.

2. The i**-th standard delay** *in* $\mathrm{U}_n(\mathbb{C}[x_1^{\pm 1}, \ldots, x_m^{\pm 1}])$ *is the diagonal matrix* $\mathbf{D}_i$ *defined by* $\mathbf{D}_i = \mathrm{diag}(1, \ldots, 1, x_i)$.

A slight variation of the above theorem over the polynomial ring $\mathbb{C}[x]$ (rather than over $\mathbb{C}[x^{\pm 1}]$) which is often used in many applications in 1-D filter banks and wavelets is the following.

Theorem 7.4.8 *(P. P. Vaidyanathan) Let* $\mathbf{H}(x) \in \mathrm{U}_n(\mathbb{C}[x^{\pm 1}]) \cap \mathrm{M}_n(\mathbb{C}[x])$ *be paraunitary with* $\det(\mathbf{H}) = x^d$. *Then it can be written in the form,* $\mathbf{H} = \mathbf{V}_d(x)\mathbf{V}_{d-1}(x)\cdots\mathbf{V}_1(x)\mathbf{H}_0$, *where* $\mathbf{H}_0$ *is a constant unitary matrix, and for each* $1 \leq i \leq d$, ${}_i(x) = I - \mathbf{v}_i\tilde{\mathbf{v}}_i + x\mathbf{v}_i\tilde{\mathbf{v}}_i$ *for certain constant unit norm vector* $\mathbf{v}_i$.

Proof: Consider the rotation matrix $\mathbf{R} = \begin{pmatrix} I_{n-2} & & \\ & 0 & 1 \\ & -1 & 0 \end{pmatrix} \in \mathrm{U}_n(\mathbb{C})$. Then,

$$\mathbf{R}^t \mathrm{diag}(1, \ldots, 1, x, 1)\mathbf{R} = \mathrm{diag}(1, \ldots, 1, x).$$

Therefore, the unitary polynomial matrix $\mathbf{H} \in \mathrm{U}_n(\mathbb{C}[x])$, which is a product of constant unitary matrices and delays, can be rewritten as a product of constant unitary matrices and standard delays, i.e.

$$\mathbf{H} = \mathbf{U}_0\mathbf{D}\mathbf{U}_1 \cdots \mathbf{U}_{d-1}\mathbf{D}\mathbf{U}_d$$

where $\mathbf{D}$ is the standard delay $\mathrm{diag}(1, \ldots, 1, x)$.

Note here that $\det(\mathbf{H}) = x^d$ was used to deduce the right number of factors. Now rewriting $\mathbf{H}$ as

$$\mathbf{H} = (\mathbf{U}_0\mathbf{D}\tilde{\mathbf{U}}_0)(\mathbf{U}_0\mathbf{U}_1\mathbf{D}\tilde{\mathbf{U}}_1\tilde{\mathbf{U}}_0)\cdots$$

we see that it is enough to show the theorem for $\mathbf{H} = \tilde{\mathbf{U}}\mathrm{diag}(1, \ldots, 1, x)\mathbf{U}$, where $\mathbf{U} = (u_{ij}) \in \mathrm{U}_n(\mathbb{C})$.

Noting that

$$\begin{aligned} \mathbf{H} &= \tilde{\mathbf{U}}\mathrm{diag}(1, \ldots, 1, x)\mathbf{U} \\ &= \tilde{\mathbf{U}}(I + \mathrm{diag}(0, \ldots, 0, x-1))\mathbf{U} \\ &= I + \tilde{\mathbf{U}}\mathrm{diag}(0, \ldots, 0, x-1)\mathbf{U}, \end{aligned}$$

and

$$\tilde{\mathbf{U}}\mathrm{diag}(0,\ldots,0,x-1)\mathbf{U} = \begin{pmatrix} (x-1)\bar{u}_{n1}u_{n1} & \cdots & (x-1)\bar{u}_{n1}u_{nn} \\ \vdots & & \vdots \\ (x-1)\bar{u}_{nn}u_{n1} & \cdots & (x-1)\bar{u}_{nn}u_{nn} \end{pmatrix}$$

$$= (x-1)\begin{pmatrix} u_{n1} \\ u_{n2} \\ \vdots \\ u_{nn} \end{pmatrix}(\bar{u}_{n1}, \bar{u}_{n2}, \ldots, \bar{u}_{nn}),$$

we prove the theorem. □

Remark 7.4.9 If $\mathbf{H} \in \mathrm{M}_N(\mathbb{C}[x])$ is paraunitary with $\det(\mathbf{H}) = x^n$, then according to the above theorem, we can write it as a product of $\mathbf{V}_i(x)$'s, $1 \leq i \leq n$. Now, it is easy to see that the highest degree term appearing in the expansion of this product could be at most x^n. Note that this means, any paraunitary matrix $\mathbf{H} \in \mathrm{M}_N(\mathbb{C}[x])$ with $\det(\mathbf{H}) = \pm 1x^n$ can be written uniquely as

$$\mathbf{H} = h_0 + h_1 x + \cdots + h_k x^k, \quad k \leq n,$$

i.e. the order k of a paraunitary matrix $\mathbf{H} \in \mathrm{M}_N(\mathbb{C}[x])$ is bounded by the degree n of its determinant.

7.5 The Structure of $\mathrm{U}_2(\mathbb{C}[x_1^{\pm 1}, \cdots, x_m^{\pm 1}])$

Again, multiplying by a delay if necessary, we assume that all the paraunitary matrices being considered are polynomial matrices. First, we need a few lemmas.

Proposition 7.5.1 *Let $\mathbf{H}(\boldsymbol{x}) \in \mathrm{M}_2(\mathbb{C}[\boldsymbol{x}])$ be a paraunitary* **polynomial** *matrix of determinant $e^{i\theta}\boldsymbol{x}^{\mathbf{n}}$. Then it can be written uniquely in the following form:*

$$\mathbf{H}(\boldsymbol{x}) = \sum_{i_1=0}^{k_1}\sum_{i_2=0}^{k_2}\cdots\sum_{i_m=0}^{k_m} h_{i_1\cdots i_m} x_1^{i_1} x_2^{i_2}\cdots x_m^{i_m}$$

where $0 \leq k_j \leq n_j$ for each $j = 1, \ldots, m$, and $h_{i_1\cdots i_m} \in \mathrm{M}_2(\mathbb{C})$ for all $(i_1, \cdots, i_m) \in \{0, \ldots, k_1\} \times \cdots \times \{0, \ldots, k_m\}$.

Proof: Since we can always write uniquely

$$\mathbf{H}(\boldsymbol{x}) = \sum_{(i_1,\dots,i_m)\in I} h_{i_1\cdots i_m} x_1^{i_1} x_2^{i_2} \cdots x_m^{i_m}$$

for a finite index set I, we have only to show that $h_{i_1\cdots i_m} = 0$ if $i_k > n_k$ for any $k = 1, \dots, m$. Suppose $\delta = \max\{i_1 \mid h_{i_1\cdots i_m} \neq 0 \text{ for some } (i_2 \cdots i_m)\} > n_1$. Then we can write

$$\mathbf{H}(x_1, \dots, x_m) = h_0(x_2, \dots, x_m) + h_1(x_2, \dots, x_m)x_1 + \cdots + h_\delta(x_2, \dots, x_m)x_1^\delta$$

for some polynomial matrices $h_i(x_2, \dots, x_m) \in \mathrm{M}_2(\mathbb{C}[x_2, \dots, x_m])$ with $h_\delta(x_2, \dots, x_m)$ being not identically zero. Now, let $(a_2, a_3, \dots, a_m)$ be any fixed point on the torus $S^1 \times \cdots \times S^1$. Then $\mathbf{H}(x_1, a_2, a_3, \dots, a_m)$ is a paraunitary matrix in $\mathrm{M}_2(\mathbb{C}[x_1])$ whose determinant has degree n_1. Therefore, by Remark 7.4.9, the highest degree term in the expansion of $\mathbf{H}(x_1, a_2, a_3, \dots, a_m)$ with respect to x_1 can be at most $x_1^{n_1}$. This means $h_\delta(a_2, a_3, \dots, a_m) = 0$ since $\delta > n_1$. Now that this is true for any $(a_2, a_3, \dots, a_m)$ on the torus $S^1 \times \cdots \times S^1$, the polynomial matrix $h_\delta(x_2, \dots, x_m)$ must be a zero matrix, which contradicts the definition of δ. Therefore, $h_{i_1\cdots i_m} = 0$ for any $i_1 > n_1$. And the same method gives $h_{i_1\cdots i_m} = 0$ for any $i_k > n_k$, $k = 1, \dots, m$. □

Definition 7.5.2 *For any polynomial matrix $G \in \mathrm{M}_{lm}(\mathbb{C}[\boldsymbol{x}])$ with the minimal representation $G = \sum_{i_1=0}^{k_1} \sum_{i_2=0}^{k_2} \cdots \sum_{i_m=0}^{k_m} h_{i_1\cdots i_m} x_1^{i_1} x_2^{i_2} \cdots x_m^{i_m}$, we say G is* **of type** $(k_1, \dots, k_m) \in \mathbb{Z}^m$ *and we call $k = k_1 + \cdots + k_m$ the* **total order** *of G.*

Using this new terminology, the above Proposition 7.5.1 can be rephrased as "*the type of a paraunitary polynomial matrix is bounded by the exponents of its determinant*". An immediate but very useful corollary of this lemma is,

Corollary 7.5.3 *Let $\mathbf{H} \in \mathrm{M}_2(\mathbb{C}[x_1, \dots, x_m])$ be a paraunitary polynomial matrix. If the determinant of $\mathbf{H}$ doesn't involve a variable x_k, then*

$$\mathbf{H} \in \mathrm{M}_2(\mathbb{C}[x_1, \dots, \widehat{x_k}, \dots, x_m]),$$

i.e. $\mathbf{H}$ is a polynomial matrix not involving the variable x_k at all.

Remark 7.5.4 Any paraunitary polynomial matrix $\mathbf{H} \in \mathrm{M}_2(\mathbb{C}[\boldsymbol{x}])$ whose determinant involves only one variable must have all of its components involving only one variable by Corollary 7.5.3 above, and is trivially factorizable by Theorem 7.4.5.

Lemma 7.5.5 *Suppose* $\mathbf{H} \in \mathrm{M}_2(\mathbb{C}[\boldsymbol{x}])$ *with* $\det(\mathbf{H}) = \boldsymbol{x}^{\mathbf{n}} = x_1^{n_1} \cdots x_m^{n_m}$ *is factorizable into (constant) unitary matrices and delays, and* $n = n_1 + \cdots + n_m$ *is the total degree of* $\det(\mathbf{H})$*. Then* $\mathbf{H}$ *has a canonical factorization into* $n+1$ *unitary matrices and* n *standard delays, i.e.*

$$\mathbf{H} \;\; = \;\; \mathbf{U}_n \mathbf{D}_n \mathbf{U}_{n-1} \mathbf{D}_{n-1} \cdots \mathbf{U}_1 \mathbf{D}_1 \mathbf{U}_0 \tag{7.3}$$

for some unitary matrices $\mathbf{U}_0, \ldots, \mathbf{U}_n \in \mathrm{U}_2(\mathbb{C})$ *and standard delays* $\mathbf{D}_1, \ldots, \mathbf{D}_n$*'s with the number of i-th standard delays appearing in this expression being precisely* n_i *for each* $1 \le i \le n$*.*

Proof: Let $\mathbf{R}(\theta) = \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}$ be the rotation matrix. Since a delay is a product of $\begin{pmatrix} 1 & 0 \\ 0 & x_i \end{pmatrix}$'s and $\begin{pmatrix} x_j & 0 \\ 0 & 1 \end{pmatrix}$'s, by noting $\begin{pmatrix} x_j & 0 \\ 0 & 1 \end{pmatrix} = \mathbf{R}(-\pi/2) \begin{pmatrix} 1 & 0 \\ 0 & x_j \end{pmatrix} \mathbf{R}(\pi/2)$, we see that any delay can be expressed as a product of unitary matrices and standard delays. Therefore, $\mathbf{H}$ itself can be written as a product of unitary matrices and standard delays, i.e. $\mathbf{H} = \mathbf{U}_l \mathbf{D}_l \mathbf{U}_{l-1} \mathbf{D}_{l-1} \cdots \mathbf{U}_1 \mathbf{D}_1 \mathbf{U}_0$, for some unitary matrices $\mathbf{U}_i$'s and standard delays $\mathbf{D}_i$'s. To see that $l = n$, take the determinant of both sides:

$$\det(\mathbf{H}) = x_1^{n_1} \cdots x_m^{n_m} = \prod_{k=1}^{l} \det(\mathbf{D}_k).$$

From this expression, we see that the number of i-th standard delays appearing in this product must be n_i, and the l must be equal to the total degree of $\det(\mathbf{H}) = n$. □

Let $\mathbf{H} \in \mathrm{M}_2(\mathbb{C}[\boldsymbol{x}])$ be a paraunitary polynomial matrix, and let $\mathbf{v}$ be its first column vector. Then the separability of $\mathbf{H}$ clearly implies the separability of $\mathbf{v}$: if $\mathbf{H} = \mathbf{H}_1 \mathbf{H}_2$ for two paraunitary polynomial matrices $\mathbf{H}_1, \mathbf{H}_2 \in \mathrm{M}_2(\mathbb{C}[\boldsymbol{x}])$, then $\mathbf{v} = \mathbf{H}_1 \mathbf{v}_2$ where $\mathbf{v}_2$ is the first column vector of $\mathbf{H}_2$.

Now, the following lemma asserts that the converse is also true, thereby relating the separability of a paraunitary matrix with that of a unit norm vector. Since, from a computational point of view, the unit norm vectors are easier to deal with than the paraunitary matrices, we will actually consider the separability of the polynomial vectors of unit norm rather than that of the paraunitary matrices.

Lemma 7.5.6 *Let* $\mathbf{H} \in \mathrm{U}_2(\mathbb{C}[\boldsymbol{x}])$ *be paraunitary with* $\det(\mathbf{H}) = \boldsymbol{x}^{\mathbf{n}}$*, and* $\mathbf{v}$ *be its first column vector of type* $\mathbf{k} := (k_1, \ldots, k_m)$*. Suppose* $\mathbf{v}$ *is perfectly separable, i.e.*

$$\mathbf{v} \;\; = \;\; \mathbf{U}_d \mathbf{D}_d \mathbf{U}_{d-1} \mathbf{D}_{d-1} \cdots \mathbf{U}_1 \mathbf{D}_1 \mathbf{v}_0 \tag{7.4}$$

for some unitary matrices $\mathbf{U}_1, \ldots, \mathbf{U}_d \in \mathrm{U}_2(\mathbb{C})$, *a constant unit norm vector* $\mathbf{v}_0 \in \mathbb{C}^2$, *and standard delays* $\mathbf{D}_1, \ldots, \mathbf{D}_d$ *with the number of the i'th standard delays appearing in this expression being precisely* k_i. *Then* $\mathbf{H}$ *is also perfectly separable.*

Proof: Write $\mathbf{v}_0 = \begin{pmatrix} a \\ b \end{pmatrix}$ for $a, b \in \mathbb{C}$ with $a^2 + b^2 = 1$. Then one checks easily that

$$\begin{aligned} \mathbf{H} &= \mathbf{U}_d\mathbf{D}_d\mathbf{U}_{d-1}\mathbf{D}_{d-1}\cdots\mathbf{U}_1\mathbf{D}_1 \begin{pmatrix} a & -\boldsymbol{x}^{\mathbf{n}-\mathbf{k}}\bar{b} \\ b & \boldsymbol{x}^{\mathbf{n}-\mathbf{k}}\bar{a} \end{pmatrix} \\ &= \mathbf{U}_d\mathbf{D}_d\mathbf{U}_{d-1}\mathbf{D}_{d-1}\cdots\mathbf{U}_1\mathbf{D}_1 \begin{pmatrix} a & -\bar{b} \\ b & \bar{a} \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & \boldsymbol{x}^{\mathbf{n}-\mathbf{k}} \end{pmatrix}. \end{aligned}$$

□

7.6 Computational Aspects

Consider a vector $\mathbf{v} = \begin{pmatrix} f \\ g \end{pmatrix} \in (\mathbb{R}[x,y])^2$ of unit norm. Then its component polynomials $f, g \in \mathbb{R}[\boldsymbol{x}]$ are constrained by the unit norm condition $\tilde{\mathbf{v}}\mathbf{v} = 1$, and this constraint can be described by a system of quadratic polynomials in the coefficients of f, g. Now we would like to see when these algebraic relations describing the unit norm condition on $\mathbf{v}$ guarantee the decomposition of $\mathbf{v}$ into the form 7.4.

Let $\mathbf{v} = \begin{pmatrix} f \\ g \end{pmatrix} \in (\mathbb{R}[x,y])^2$ be of unit norm of type (k_1, k_2) with total order 2, and let $\alpha = x^{k_1}y^{k_2} \in \mathbb{R}[x,y]$. Then $\alpha\tilde{\mathbf{v}}$ becomes a polynomial vector. Define a paraunitary matrix $\mathbf{H} \in \mathrm{M}_2(\mathbb{R}[x,y])$ by

$$\mathbf{H} = \begin{pmatrix} f & -\alpha\tilde{g} \\ g & \alpha\tilde{f} \end{pmatrix},$$

in which we get the following three cases to consider; $\det(\mathbf{H}) = x^2, xy, y^2$.

In terms of $\mathbf{v}$, we see that $\mathbf{v}$ is of type $(2,0)$, $(1,1)$ and $(0,2)$, in respective cases.

The two cases when $\mathbf{v}$ is of type $(2,0)$ and of type $(0,2)$ are trivial by Corollary 7.5.3.

Suppose, therefore, $\mathbf{v}$ is of type $(1,1)$, i.e. $\det(\mathbf{H}) = xy$. In this case, by Proposition 7.5.1, we can write

$$\mathbf{H} = h_{00} + h_{10}x + h_{0,1}y + h_{11}xy$$

for some $h_{00}, h_{10}, h_{0,1}, h_{11} \in \mathrm{M}_2[\mathbb{R}]$. The corresponding expression for $\mathbf{v}$ is,

$$\mathbf{v} \;=\; \mathbf{v}_{00} + \mathbf{v}_{10}x + \mathbf{v}_{0,1}y + \mathbf{v}_{11}xy$$

for some $\mathbf{v}_{00}, \mathbf{v}_{10}, \mathbf{v}_{0,1}, \mathbf{v}_{11} \in \mathbb{R}^2$. Define the real numbers a_{ij}, b_{ij}, $0 \le i, j \le 1$, by $\mathbf{v}_{ij} = \begin{pmatrix} a_{ij} \\ b_{ij} \end{pmatrix}$ and consider

$$\begin{aligned} 1 &= \tilde{\mathbf{v}}\mathbf{v} \\ &= (\mathbf{v}_{00}^t + \mathbf{v}_{10}^t x^{-1} + \mathbf{v}_{0,1}^t y^{-1} + \mathbf{v}_{11}^t x^{-1}y^{-1})(\mathbf{v}_{00} + \mathbf{v}_{10}x + \mathbf{v}_{0,1}y + \mathbf{v}_{11}xy). \end{aligned}$$

Equating the respective coefficients of x and y, we get the following set of relations:

$$\begin{aligned} 0 &= \mathbf{v}_{11}^t\mathbf{v}_{00} = a_{01}\,a_{10} + b_{01}\,b_{10} \\ 0 &= \mathbf{v}_{10}^t\mathbf{v}_{01} = a_{00}\,a_{11} + b_{00}\,b_{11} \\ 0 &= \mathbf{v}_{10}^t\mathbf{v}_{00} + \mathbf{v}_{11}^t\mathbf{v}_{01} = a_{00}\,a_{10} + a_{01}\,a_{11} + b_{00}\,b_{10} + b_{01}\,b_{11} \\ 0 &= \mathbf{v}_{01}^t\mathbf{v}_{00} + \mathbf{v}_{11}^t\mathbf{v}_{10} = a_{00}\,a_{01} + a_{10}\,a_{11} + b_{00}\,b_{01} + b_{10}\,b_{11} \\ 1 &= \mathbf{v}_{00}^t\mathbf{v}_{0,0} + \mathbf{v}_{01}^t\mathbf{v}_{0,1} + \mathbf{v}_{10}^t\mathbf{v}_{1,0} + \mathbf{v}_{11}^t\mathbf{v}_{11} \\ &= {a_{00}}^2 + {a_{01}}^2 + {a_{10}}^2 + {a_{11}}^2 + {b_{00}}^2 + {b_{01}}^2 + {b_{10}}^2 + {b_{11}}^2. \end{aligned} \tag{7.5}$$

Note here that the above set of relations gives defining equations for a unit norm vector of type bounded by $(1,1)$, that is, if we choose any real numbers a_{ij}'s and b_{ij}'s satisfying above set of relations, and define a polynomial vector $\mathbf{v}$ by $\mathbf{v} = \sum_{i=0}^{1}\sum_{j=0}^{1} \begin{pmatrix} a_{ij} \\ bij \end{pmatrix} x^i y^j$, then $\mathbf{v}$ will be a unit norm vector of type $\le (1,1)$.

Therefore, we can view above set of relations as quadratic polynomials $f_i, 1 \le i \le 5$ in the polynomial ring $\mathbb{R}[a_{00}, a_{10}, a_{01}, a_{11}, b_{00}, b_{10}, b_{01}, b_{11}]$ defining a variety which we may call the **Paraunitary Variety of type** $(1,1)$. The real valued points on this subvariety of affine 8-space are in one-to-one correspondence with the unit norm polynomial vectors of type $\le (1,1)$, and thus paraunitary matrices of determinant $x^{n_1}y^{n_2}$ with $(n_1, n_2) \le (1,1)$. Therefore, this variety precisely parametrizes all the paraunitary matrices whose determinant is a factor of xy.

To see what type of algebraic relations on the a_i's and b_i's assure the factorizability of $\mathbf{v}$ as in 7.4, assume

$$\mathbf{v} \;=\; \mathbf{R}(\theta)\mathbf{D}(x)\mathbf{v}' \tag{7.6}$$

for a certain rotation matrix $\mathbf{R}(\theta)$, the first standard delay $\mathbf{D}(x) = \begin{pmatrix} 1 & 0 \\ 0 & x \end{pmatrix}$, and a polynomial vector $\mathbf{v}' \in (\mathbb{R}[x,y])^2$. Letting $\mathbf{v}_0(y) = \mathbf{v}_{00} + \mathbf{v}_{01}y$ and $\mathbf{v}_1(y) = \mathbf{v}_{10} + \mathbf{v}_{11}y$, we now get

$$\begin{aligned} \mathbf{R}(\theta)^t\mathbf{v} &= \mathbf{R}(\theta)^t(\mathbf{v}_0(y) + \mathbf{v}_1(y)x) \\ &= \mathbf{R}(\theta)^t\mathbf{v}_0(y) + \mathbf{R}(\theta)^t\mathbf{v}_1(y)x \\ &= \mathbf{D}(x)\mathbf{v}' \\ &= \begin{pmatrix} 1 & 0 \\ 0 & x \end{pmatrix}\mathbf{v}' \end{aligned}$$

Since the second component of the vector $\mathbf{R}(\theta)^t\mathbf{v}$ is divisible by x, its constant term, that is, the second component of the vector $\mathbf{R}(\theta)^t\mathbf{v}_0(y)$, should be zero. So, we get $(-\sin(\theta), \cos(\theta))\mathbf{v}_0(y) = 0$, i.e.

$$(-\sin(\theta), \cos(\theta))\mathbf{v}_{00} = (-\sin(\theta), \cos(\theta))\mathbf{v}_{01} = 0$$

Conversely, if there exists a nonzero constant vector (a,b) such that $(a,b)\mathbf{v}_0(y) = 0$, then $\mathbf{v}$ splits as in 7.6, with $\mathbf{R}(\theta) = \frac{1}{\sqrt{a^2+b^2}}\begin{pmatrix} b & a \\ -a & b \end{pmatrix}$. We can do the same to see when $\mathbf{v}$ splits with the factor $\mathbf{R}(\theta)\mathbf{D}(y)$. What we get is the following:

$$\begin{aligned} & \text{The vector } \mathbf{v} \text{ splits as in } 7.4 \\ \iff & \text{"}(a,b)\mathbf{v}_{00} = (a,b)\mathbf{v}_{01} = 0\text{" or "}(a,b)\mathbf{v}_{00} = (a,b)\mathbf{v}_{10} = 0\text{" has a} \\ & \text{nontrivial solution } (a,b). \\ \iff & \begin{pmatrix} a_{00} & b_{00} \\ a_{01} & b_{01} \end{pmatrix}\begin{pmatrix} a \\ b \end{pmatrix} = \mathbf{0} \text{ or } \begin{pmatrix} a_{00} & b_{00} \\ a_{10} & b_{10} \end{pmatrix}\begin{pmatrix} a \\ b \end{pmatrix} = \mathbf{0} \text{ has a nontrivial solution} \\ & \begin{pmatrix} a \\ b \end{pmatrix}. \\ \iff & a_{00}b_{01} - b_{00}a_{01} = 0 \text{ or } a_{00}b_{10} - b_{00}a_{10} = 0. \\ \iff & f := (a_{00}b_{01} - b_{00}a_{01})(a_{00}b_{10} - b_{00}a_{10}) = 0. \end{aligned} \tag{7.7}$$

Let $I(1,1) \subset \mathbb{R}[a_{00}, a_{10}, a_{01}, a_{11}, b_{00}, b_{10}, b_{01}, b_{11}]$ be the ideal generated by the 5 quadratic polynomials $f_i, 1 \le i \le 5$. Since any point in the variety $V(I(1,1))$ defines a unit norm vector of type $\le (1,1)$ and an arbitrary point in $V(f)$ defines a vector decomposable into the form in 7.4, showing $V(I(1,1)) \subset V(f)$ is equivalent to showing that any unit norm vector of type $\le (1,1)$ is factorizable as in 7.4. Therefore, our question has boiled down to:

$V(I(1,1)) \subset V(f)$?

The following lemma gives a sufficient condition for the above question to have a positive answer.

Lemma 7.6.1 *Let k be an arbitrary field. Then,*

$$g \in \sqrt{I} \implies V(I) \subset V(g) \tag{7.8}$$

Now the following radical ideal membership algorithm can be used for our computational test of $f \in \sqrt{I(1,1)}$.

Lemma 7.6.2 *(Radical Ideal Membership) $f \in \sqrt{I}$ iff the ideal $(f_1, f_2, f_3, f_4, f_5, 1 - t \cdot f)$ of the ring $\mathbb{R}[a_{00}, a_{10}, a_{01}, a_{11}, b_{00}, b_{10}, b_{01}, b_{11}, t]$ is the unit ideal, i.e. 1 belongs to the ideal $(f_1, f_2, f_3, f_4, f_5, 1 - t \cdot f)$.*

Remark 7.6.3 Note here that we have introduced a new variable t.

Noting that the ideal $(f_1, f_2, f_3, f_4, f_5, 1 - t \cdot f)$ is a unit ideal iff its Gröbner bases is $\{1\}$, we can use any existing computer algebra packages to compute the Gröbner bases of the six polynomials $f_1, f_2, f_3, f_4, f_5, 1 - t \cdot f$ in 9 variables. We used *Macaulay* and SINGULAR for this computation, which gave us the positive answer for the above case ($d = 2$), that is, it showed that the Gröbner bases of $f_1, f_2, f_3, f_4, f_5, 1 - t \cdot f$ is just 1.

For higher d's, the corresponding radical ideal membership can be checked in the same fashion even though the involved Gröbner bases computation takes much more time.

For $d = 3$, there are 4 types of Paraunitary Variety; of type $(3,0), (2,1), (1,2)$, and $(0,3)$. The $(3,0), (0,3)$ cases are trivial by Corollary 7.5.3, and by symmetry, we have only to consider type $(2,1)$ case. The Paraunitary Variety of type $(2,1)$ is defined by 8 quadratic polynomials in the affine 12-space, and there are 3 polynomials of degree 4 whose radical ideal membership is to be checked. Hours of Gröbner bases computation in this case confirmed that the answer is still positive.

For the $d = 4$ case, there are two nontrivial cases to consider; of type $(3,1)$ and of type $(2,2)$. The Paraunitary Variety of type $(3,1)$ is defined by 11 quadratic polynomials in the affine 16-space, and there are 6 polynomials of degree 4 whose radical ideal membership is to be checked. For the type $(2,2)$ case, which is defined by 13 quadratic polynomials in the affine 18-space, there are 9 polynomials of degree 4 whose radical ideal membership is to be checked. The computation showed that the the Paraunitary Varieties of type $(3, 1)$ and $(1, 3)$ are completely separable while the Paraunitary Variety of type $(2, 2)$ is not. So the first counter-example may occur at type $(2, 2)$.

7.7 Convex Geometric Approach

The computation done in the preceding section shows the peculiar behavior of the Paraunitary Varieties of type $(n, 1)$ or $(1, n)$, and that the first nonseparable example may be found in $(2, 2)$ case. With the convex geometric approach to be taken in this section, we will actually construct the following nonseparable unit norm vector $\mathbf{V}$ of type $(2, 2)$.

$$\mathbf{V} = \frac{1}{26}\sqrt{\frac{105}{13}} \begin{pmatrix} -\sqrt{\frac{5}{7}}x - \frac{x^2}{2} - \frac{y}{3} - \frac{22xy}{\sqrt{35}} + \frac{11x^2y}{3} - \frac{y^2}{2} - \frac{17xy^2}{\sqrt{35}} - 4x^2y^2 \\ 2 + \frac{12x}{\sqrt{35}} + \frac{x^2}{2} + \frac{8y}{3} - \frac{61xy}{3\sqrt{35}} - \frac{2x^2y}{3} - \frac{y^2}{2} - 2\sqrt{\frac{5}{7}}xy^2 \end{pmatrix}$$

First, to understand the convex geometry behind our parahermitian structure, consider a vector

$$\begin{aligned} \mathbf{v} &= \begin{pmatrix} f \\ g \end{pmatrix} \\ &= \mathbf{v}_{00} + \mathbf{v}_{10}x + \mathbf{v}_{01}y, \quad \mathbf{v}_{ij} \in \mathbb{C}^2 - \{\mathbf{0}\}. \end{aligned}$$

Then the convex hull of its exponent vectors is spanned by $\{(0, 0), (1, 0), (0, 1)\}$.

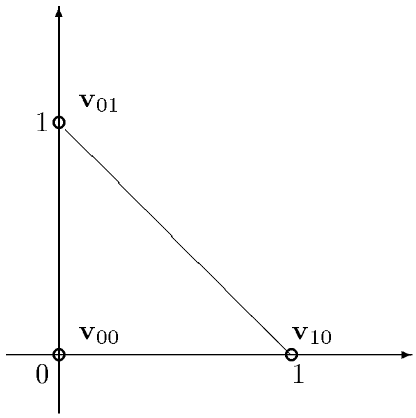

Figure 7.1: The convex hull of the exponent vectors of $\mathbf{v}$

Now we claim that $\mathbf{v} \in \mathbb{C}[x, y]$ is not of unit norm. To see this, note that $\langle \mathbf{v}, \mathbf{v} \rangle \in \mathbb{C}^*$ implies

$$\langle \mathbf{v}, \mathbf{v} \rangle = \langle \mathbf{v}_{00} + \mathbf{v}_{10}x + \mathbf{v}_{01}y, \mathbf{v}_{00} + \mathbf{v}_{10}x + \mathbf{v}_{01}y \rangle$$

$$\begin{aligned}
&= (\tilde{\mathbf{v}}_{00}\mathbf{v}_{00} + \tilde{\mathbf{v}}_{10}\mathbf{v}_{10} + \tilde{\mathbf{v}}_{01}\mathbf{v}_{01}) + (\tilde{\mathbf{v}}_{00}\mathbf{v}_{10}x + \tilde{\mathbf{v}}_{10}\mathbf{v}_{00}\frac{1}{x}) + \\
&\quad (\tilde{\mathbf{v}}_{00}\mathbf{v}_{01}y + \tilde{\mathbf{v}}_{01}\mathbf{v}_{00}\frac{1}{y}) + (\tilde{\mathbf{v}}_{01}\mathbf{v}_{10}\frac{x}{y} + \tilde{\mathbf{v}}_{10}\mathbf{v}_{01}\frac{y}{x}) \\
&\in \mathbb{C}^*.
\end{aligned}$$

From the fact that the last expression has to be a constant, we deduce that

$$\begin{aligned}
\mathbf{v}_{00} &\perp \mathbf{v}_{10} \\
\mathbf{v}_{00} &\perp \mathbf{v}_{01} \\
\mathbf{v}_{10} &\perp \mathbf{v}_{01}.
\end{aligned}$$

Quite clearly, no three vectors $\mathbf{v}_{00}, \mathbf{v}_{10}, \mathbf{v}_{01} \in \mathbb{C} - \{0\}$ can satisfy this mutual orthogonality.

Theorem 7.7.1 *The 2×2 paraunitary matrices of type $(n, 1)$ or $(1, n)$ are completely separable.*

Remark 7.7.2 This theorem was first observed and proved in [LV90]. We present here a new proof based on our convex geometric method.

Proof: Suppose that

$$\mathbf{v} = \sum_{i=0}^{1}\sum_{j=0}^{k} \mathbf{v}_{ij} x^i y^j.$$

Write $\mathbf{v} = \mathbf{v}_{i=0}(y) + \mathbf{v}_{i=1}(y)x$. Then it is easy to verify that the two face components, $\mathbf{v}_{i=0}(y)$, $\mathbf{v}_{i=1}(y) \in \mathbb{C}[y]$, of $\mathbf{v}$ are of unit norm and orthogonal to each other since $\mathbf{v}$ is of unit norm. And from the orthogonality of these two vectors;

$$\begin{aligned}
\langle \mathbf{v}_{i=0}(y), \mathbf{v}_{i=1}(y) > &= \widetilde{f_{i=0}(y)} f_{i=1}(y) + \widetilde{g_{i=0}(y)} g_{i=1}(y) \\
&= \overline{f_{i=0}(1/\bar{y})} f_{i=1}(y) + \overline{g_{i=0}(1/\bar{y})} g_{i=1}(y) \\
&= 0,
\end{aligned}$$

one deduces that, if $u \in \mathbb{C}$ is a zero of $f_{i=0}$ but not a zero of $g_{i=0}$, then $1/\bar{u}$ is a zero of $g_{i=1}$. There are the following two cases to consider:

1. when $f_{j=0}$ and $g_{j=0}$ have no common root

2. when $f_{j=0}$ and $g_{j=0}$ have a common root.

Case 1: When $f_{j=0}$ and $g_{j=0}$ have no common root.

In this case, we can write

$$\begin{aligned} f_{j=0}(y) &= a_{j=0}(y-\alpha) \\ g_{j=0}(y) &= b_{j=0}(y-\beta), \quad \alpha \neq \beta. \end{aligned}$$

Using the orthogonality of $\mathbf{v}_{j=0}$ and $\mathbf{v}_{j=k}$, we see that

$$\begin{aligned} f_{j=k}(y) &= a_{j=k}(y-1/\bar{\beta}) \\ g_{j=k}(y) &= b_{j=k}(y-1/\bar{\alpha}). \end{aligned}$$

where $a_{j=0}\bar{a}_{j=k}\alpha + b_{j=0}\bar{b}_{j=k}\beta = 0$. Now the convex hull generated by the exponent vectors of $\mathbf{v}$ has the structure shown in the Figure 7.2.

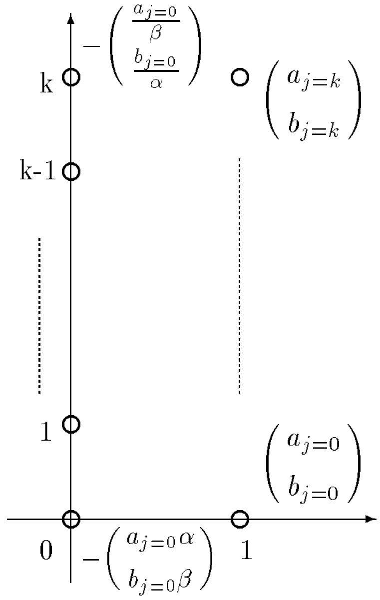

Figure 7.2: The convex hull of the exponent vectors of $\mathbf{v}$

Letting c_i's and d_i's, $1 \leq i \leq l$, be the common roots of $\{f_{i=0}(y), g_{i=0}(y)\}$ and $\{f_{i=1}(y), g_{i=1}(y)\}$, respectively, one gets the following representation.

$$\begin{aligned} f_{i=0}(y) &= -\frac{a_{j=k}}{\beta}(y-c_1)\cdots(y-c_l)\cdot(y-u_1)\cdots(y-u_{k-l}) \\ g_{i=0}(y) &= -\frac{b_{j=k}}{\alpha}(y-c_1)\cdots(y-c_l)\cdot(y-v_1)\cdots(y-v_{k-l}) \end{aligned}$$

$$
\begin{aligned}
f_{i=1}(y) &= a_{j=k}(y-d_1)\cdots(y-d_l)\cdot(y-\frac{1}{\bar{v}_1})\cdots(y-\frac{1}{\bar{v}_{k-l}}) \\
g_{i=1}(y) &= b_{j=k}(y-d_1)\cdots(y-d_l)\cdot(y-\frac{1}{\bar{u}_1})\cdots(y-\frac{1}{\bar{u}_{k-l}}).
\end{aligned}
$$

Now note in Figure 7.2 that

1. at $(0,0)$, constant coefficient of $\mathbf{v}_{j=0}$ = constant coefficient of $\mathbf{v}_{i=0}$,
2. at $(1,0)$, leading coefficient of $\mathbf{v}_{j=0}$ = constant coefficient of $\mathbf{v}_{i=1}$,
3. at $(0,k)$, constant coefficient of $\mathbf{v}_{j=k}$ = leading coefficient of $\mathbf{v}_{i=0}$,
4. at $(1,k)$, leading coefficient of $\mathbf{v}_{j=k}$ = leading coefficient of $\mathbf{v}_{i=1}$.

Comparing the coefficients of the polynomials involved, we get the following relations.

$$
\begin{aligned}
-\frac{a_{j=k}}{\beta}(-1)^k c_1\cdots c_l\cdot u_1\cdots u_{k-l} &= -a_{j=0}\alpha \\
-\frac{b_{j=k}}{\alpha}(-1)^k c_1\cdots c_l\cdot v_1\cdots v_{k-l} &= -b_{j=0}\beta \\
a_{j=k}(-1)^k d_1\cdots d_l\cdot\frac{1}{\bar{v}_1}\cdots\frac{1}{\bar{v}_{k-l}} &= a_{j=0} \\
b_{j=k}(-1)^k d_1\cdots d_l\cdot\frac{1}{\bar{u}_1}\cdots\frac{1}{\bar{u}_{k-l}} &= a_{j=0}.
\end{aligned}
$$

Therefore, we have

$$
\frac{a_{j=k}}{b_{j=k}}\frac{u_1\cdots u_{k-l}}{v_1\cdots v_{k-l}} = \frac{a_{j=0}}{b_{j=0}}.
$$

Let

$$
\begin{aligned}
A &= \frac{b_{j=k}}{\alpha}\prod_{i=1}^{l}(y-c_i) \\
B &= (-1)^{k-l}\frac{a_{j=k}}{\prod_{i=1}^{k-l}\bar{v}_i}\prod_{i=1}^{l}(y-d_i) \\
F &= \frac{\bar{b}_{j=0}}{\bar{a}_{j=0}}\prod_{i=1}^{k-l}(y-u_i) \\
G &= \prod_{i=1}^{k-l}(y-v_i).
\end{aligned}
$$

Then using the above relations, one obtains

$$
\mathbf{v} = \begin{pmatrix} f \\ g \end{pmatrix}
$$

$$= \begin{pmatrix} AF + x \cdot B\tilde{G}y^{k-l} \\ -AG + x \cdot B\tilde{F}y^{k-l} \end{pmatrix}$$

Now $\langle \mathbf{v}, \mathbf{v} \rangle = 1$ translates into

$$\begin{aligned} & A\tilde{A}F\tilde{F} + B\tilde{B}G\tilde{G} + A\tilde{A}G\tilde{G} + B\tilde{B}F\tilde{F} \\ = \ & (A\tilde{A} + B\tilde{B}) \cdot (F\tilde{F} + G\tilde{G}) \\ = \ & 1 \end{aligned}$$

From the last expression, we conclude that both of $A\tilde{A} + B\tilde{B}$ and $F\tilde{F} + G\tilde{G}$ are nonzero constants since they are involution invariant monomials. By dividing by their norms if necessary, we may assume that $A\tilde{A} + B\tilde{B} = F\tilde{F} + G\tilde{G} = 1$. In this case, we have

$$\begin{aligned} \mathbf{v} &= \begin{pmatrix} f \\ g \end{pmatrix} \\ &= \begin{pmatrix} AF + x \cdot B\tilde{G}y^{k-l} \\ -AG + x \cdot B\tilde{F}y^{k-l} \end{pmatrix} \\ &= \begin{pmatrix} F & \tilde{G} \\ -G & \tilde{F} \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & x \end{pmatrix} \begin{pmatrix} A \\ B \end{pmatrix}. \end{aligned}$$

This shows the separability.

Case 2: When $f_{j=0}$ and $g_{j=0}$ have a common root.

In this case, we can write

$$\begin{aligned} f_{j=0}(y) &= a_{j=0}(y - \gamma) \\ g_{j=0}(y) &= b_{j=0}(y - \gamma) \\ f_{j=k}(y) &= a_{j=k}(y - \delta) \\ g_{j=k}(y) &= b_{j=k}(y - \delta) \end{aligned}$$

where $a_{j=0}\bar{a}_{j=k} + b_{j=0}\bar{b}_{j=k} = 0$. Now the convex hull generated by the exponent vectors of $\mathbf{v}$ has the structure shown in the Figure 7.3. Now we can proceed in the same fashion as in the previous case. □

Now we will construct a nonseparable paraunitary matrix of type $(2, 2)$. And in doing this, we will actually construct a continuously parametrized family of nonseparable

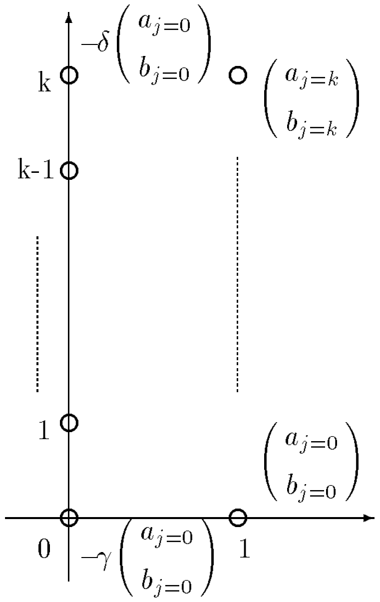

Figure 7.3: The convex hull of the exponent vectors of $\mathbf{v}$

paraunitary matrices of type $(2, 2)$. Let

$$\begin{aligned} \mathbf{v} &= \sum_{i=0}^{2}\sum_{j=0}^{2} \mathbf{v}_{ij} x^i y^j \\ &= \sum_{i=0}^{2}\sum_{j=0}^{2} \begin{pmatrix} a_{ij} \\ b_{ij} \end{pmatrix} x^i y^j \end{aligned}$$

be a nonseparable vector of unit norm. As we observed in the Equation 7.7 of the previous section, the separability (or nonseparability) of a vector of type $(2, 2)$ is characterized by the following.

$$\begin{aligned} &\mathbf{w} = \sum_{i=0}^{2}\sum_{j=0}^{2} \mathbf{w}_{ij} x^i y^j \text{ is separable} \\ \Longleftrightarrow\ &\mathbf{w}_{00}, \mathbf{w}_{10}, \mathbf{w}_{20} \text{ are all parallel or } \mathbf{w}_{00}, \mathbf{w}_{01}, \mathbf{w}_{02} \text{ are all parallel.} \end{aligned}$$

Assuming $\mathbf{v}_{00} \neq 0$, define parameters $r \in \mathbb{R}_{\geq 0}$ and $\theta \in [0, 2\pi)$ by $a_{00} = r\cos(\theta), b_{00} = r\sin(\theta)$. Now introduce two new parameters s and t by

$$\begin{aligned} s &= \langle \mathbf{v}_{00}, \mathbf{v}_{20} \rangle = a_{00}a_{20} + b_{00}b_{20} \\ t &= [0, 0, 2]_x = \det[\mathbf{v}_{00}, \mathbf{v}_{20}] = a_{00}b_{20} - a_{20}b_{00} \end{aligned}$$

where the bracket notation is defined by $[i, j, k]_y = \det[\mathbf{v}_{ji}, \mathbf{v}_{ki}]$ and $[i, j, k]_x = \det[\mathbf{v}_{ij}, \mathbf{v}_{ik}]$.

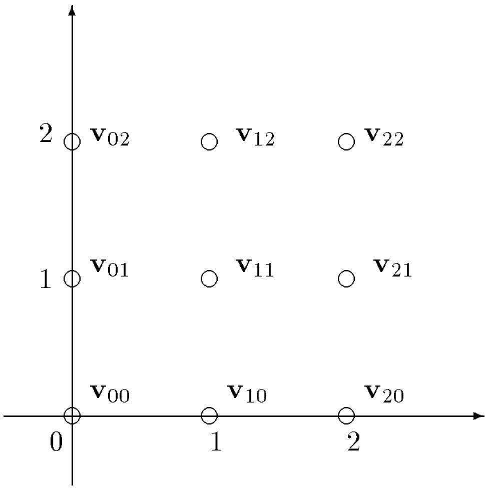

Figure 7.4: The exponent vectors of $\mathbf{v}$ of type $(2,2)$

The above relation can be rewritten in matrix form,

$$\begin{aligned}\begin{pmatrix} s \\ t \end{pmatrix} &= \begin{pmatrix} a_{00} & b_{00} \\ -b_{00} & a_{00} \end{pmatrix} \begin{pmatrix} a_{20} \\ b_{20} \end{pmatrix} \\ &= r \begin{pmatrix} \cos(\theta) & \sin(\theta) \\ -\sin(\theta) & \cos(\theta) \end{pmatrix} \begin{pmatrix} a_{20} \\ b_{20} \end{pmatrix}.\end{aligned}$$

Inverting this relation, we can express a_{20}, b_{20} in terms of r, θ, s, t.

$$\begin{pmatrix} a_{20} \\ b_{20} \end{pmatrix} = 1/r^2 \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix} \begin{pmatrix} s \\ t \end{pmatrix}.$$

Now $\mathbf{v}_{00} \perp \mathbf{v}_{22}$ and $\mathbf{v}_{20} \perp \mathbf{v}_{02}$ imply that

$$\begin{aligned}\mathbf{v}_{02} &= u \begin{pmatrix} -d \\ c \end{pmatrix} \\ \mathbf{v}_{22} &= v \begin{pmatrix} -b \\ a \end{pmatrix}\end{aligned}$$

for some $u, v \in \mathbb{C}$. Now we will further assume that, on each of the 4 faces of the convex hull in the Figure 4, the corresponding face components of f and g have a common root.

In this case, on the face $j = 0$, the fact that $f_{j=0} = a_{00} + a_{10}x + a_{20}x^2$ and $g_{j=0} = b_{00} + b_{10}x + b_{20}x^2$ have a common root is equivalent to the vanishing of the Bezóut resultant of $f_{j=0}$ and $g_{j=0}$, which is $[0,0,2]_y^2 - [0,0,1]_y \cdot [0,1,2]_y$. Therefore we can introduce two new parameters w and z by letting

$$\begin{aligned} w &= [0,0,1]_y/[0,0,2]_y = [0,0,2]_y/[0,1,2]_y \\ z &= [0,0,1]_x/[0,0,2]_x = [0,0,2]_x/[0,1,2]_x. \end{aligned}$$

Now we claim that these 8 parameters $(r, \theta, s, t, u, v, w, z)$, subject to 2 polynomial relations among them, determine all the possible nonseparable unit norm vectors of type $(2,2)$ satisfying the above boundary conditions. This means that the set of the nonseparable paraunitary vectors of type $(2,2)$ with the additional boundary conditions is a variety of dimension 6. For this purpose, we only need to express $\mathbf{v}_{10}, \mathbf{v}_{01}, \mathbf{v}_{12}, \mathbf{v}_{21}, \mathbf{v}_{11}$ in terms of these parameters, and describe all the relations among these parameters. Actually, from the vanishing of the 4 face-resultants, it is not hard to derive the following relations.

$$\begin{aligned} \mathbf{v}_{10} &= \begin{pmatrix} s & a \\ t & b \end{pmatrix} \begin{pmatrix} w \\ 1/w \end{pmatrix} \\ \mathbf{v}_{01} &= \begin{pmatrix} -t & a \\ s & b \end{pmatrix} \begin{pmatrix} uz \\ 1/z \end{pmatrix} \\ \mathbf{v}_{12} &= \begin{pmatrix} t & -b \\ -s & a \end{pmatrix} \begin{pmatrix} -vw \\ u/w \end{pmatrix} \\ \mathbf{v}_{21} &= \begin{pmatrix} -s & b \\ -t & -a \end{pmatrix} \begin{pmatrix} uvz \\ 1/uz \end{pmatrix}. \end{aligned}$$

Therefore, we only have to express the interior coefficient $\mathbf{v}_{11}$ in terms of these parameters. Consider the A_{ij}'s defined by the expansion $\langle \mathbf{v}, \mathbf{v} \rangle = \sum_{i=-2}^{2} \sum_{j=-2}^{2} A_{ij} x^i y^j$. Then since $\langle \mathbf{v}, \mathbf{v} \rangle = 1$, we have to have $A_{ij} = 0$ for any $i \neq 0$ or $j \neq 0$. In particular,

$$\begin{aligned} A_{01} &= \langle \mathbf{v}_{00}, \mathbf{v}_{01} \rangle + \langle \mathbf{v}_{01}, \mathbf{v}_{02} \rangle + \langle \mathbf{v}_{10}, \mathbf{v}_{11} \rangle + \langle \mathbf{v}_{11}, \mathbf{v}_{12} \rangle + \\ &\quad \langle \mathbf{v}_{20}, \mathbf{v}_{21} \rangle + \langle \mathbf{v}_{21}, \mathbf{v}_{22} \rangle = 0 \\ A_{10} &= \langle \mathbf{v}_{00}, \mathbf{v}_{10} \rangle + \langle \mathbf{v}_{10}, \mathbf{v}_{20} \rangle + \langle \mathbf{v}_{01}, \mathbf{v}_{11} \rangle + \langle \mathbf{v}_{11}, \mathbf{v}_{21} \rangle + \\ &\quad \langle \mathbf{v}_{02}, \mathbf{v}_{12} \rangle + \langle \mathbf{v}_{12}, \mathbf{v}_{22} \rangle = 0 \\ A_{11} &= \langle \mathbf{v}_{10}, \mathbf{v}_{21} \rangle + \langle \mathbf{v}_{00}, \mathbf{v}_{11} \rangle + \langle \mathbf{v}_{11}, \mathbf{v}_{22} \rangle + \langle \mathbf{v}_{01}, \mathbf{v}_{12} \rangle = 0 \\ A_{-11} &= \langle \mathbf{v}_{10}, \mathbf{v}_{01} \rangle + \langle \mathbf{v}_{20}, \mathbf{v}_{11} \rangle + \langle \mathbf{v}_{11}, \mathbf{v}_{02} \rangle + \langle \mathbf{v}_{21}, \mathbf{v}_{12} \rangle = 0. \end{aligned}$$

From $A_{11} = A_{-11} = 0$, we get an expression of $\mathbf{v}_{11}$ in terms of our parameters, and $A_{01} = A_{10} = 0$ gives the relations among the parameters. One verifies easily that $\{r =$

$2, \theta = \pi/2, s = 1, t = 1, u = 1, v = 2, w = \sqrt{20/7}, z = 2/3\}$ is a legitimate set of values for the parameters, i.e. satisfies the two constraint equation $A_{01} = A_{10} = 0$. And specializing at these values gives the nonseparable example introduced at the beginning of this section.

Part II

Applications to Signal Processing

Chapter 8

Introduction to Part II

While there has been much recent research done on multidimensional (MD) multirate systems, some basic questions have been left untouched. In the following, we will describe some of the basic problems arising from the multidimensional multirate systems, and all the systems, henceforth, will be assumed to be FIR (Finite Impulse Response).

In many applications, the design and analysis of invertible MD multirate schemes boil down to the following mathematical question:

> *Given a matrix of polyphase components, can we effectively decide whether or not that matrix has a left inverse, and give a complete parametrization of all the left inverses of that matrix?*

In order to show how the various problems are reduced to the above simple form, the following three problems will be used as demonstrating examples. The same three problems were used in [KPV95] to show the relevancy of Gröbner bases in the theory of multidimensional FIR systems.

1. *Given an MD FIR low-pass filter $G(\boldsymbol{z})$, decide effectively whether or not $G(\boldsymbol{z})$ can occur as an analysis filter in a critically downsampled, 2-channel, perfect reconstructing (PR) FIR filter bank. When this decision process yields a positive answer, find* **all** *such filter banks.*

2. *Given a sample rate conversion scheme consisting of upsampling by p, filtering with an MD FIR filter $U(\boldsymbol{z})$ and downsampling by q, decide effectively whether or not this scheme is FIR invertible.*

3. *Given an oversampled MD FIR analysis filter bank, decide effectively whether or not there is an FIR synthesis filter bank such that the overall system is PR. When this decision process yields a positive answer, provide a complete parametrization of all such FIR synthesis filter banks.*

In the following chapters, we will show how these problems are reduced to the above simple form, and how our previous results on unimodular polynomial matrices are relevant to these problems in MD systems. The reason unimodularity comes in can be seen easily from the following statement whose proof will be given in Chapter 10:

> *A (not necessarily square) Laurent polynomial matrix has a left inverse if and only if it is unimodular.*

Therefore, mathematically, we are dealing with the problem of determining if a given **Laurent polynomial** matrix is unimodular, and in case it is, if we can explicitly find all the (not unique in non-square cases) left inverses for it. This allows us to see the study of perfect reconstructing FIR filter banks as the study of unimodular matrices over Laurent polynomial rings [KPV95].

Exploiting the results developed mainly for polynomial rings, we immediately see that the answers to these questions are positive over polynomial rings, i.e. when the matrices involved are unimodular **polynomial** matrices rather than Laurent polynomial matrices. In system theoretic terminology, causal invertibility of causal filters are therefore covered by these methods. Geometrically, this demonstrates the relative simplicity associated with affine systems compared to toric systems.

The situation, however, is more complicated partly because an FIR-invertible causal filter may not be causal-invertible.

For an example, consider the polynomial vector $\begin{pmatrix} z \\ z^2 \end{pmatrix} \in (k[z])^2$. While the relation $\frac{1}{2z} \cdot z + \frac{1}{2z^2} \cdot z^2 = 1$ clearly shows the FIR-invertibility of this vector, it is not causal-invertible since there are no polynomials $f(z), g(z) \in k[z]$ satisfying

$$f(z) \cdot z + g(z) \cdot z^2 \quad = \quad 1$$

as we can see easily by evaluating both sides at $z = 0$.

Now, in order to extend our affine results (i.e. causal cases) to general FIR systems, we need an effective process of converting a given Laurent polynomial matrix to a polynomial matrix while preserving unimodularity. A systematic process to that effect was developed in Chapter 6, and will be used through the remaining chapters.

In Chapter 9, the above three problems are thoroughly examined in the transparent one-dimensional (1-D) causal setup.

In Chapter 10, we will get to the same problems in MD multirate signal processing, for which our main tools are the Syzygy-based algorithm for the Quillen-Suslin Theorem developed in Chapter 3.

There are far more classes of MD problems for which Gröbner bases are an essential tool. For example, in obtaining the Realization Algorithm in Chapter 4, we relied on the Gröbner bases method to determine the termination of the subprocesses. And in Chapter 11, we will give a complete parametrization (in terms of ladder structures) of MD bi-orthogonal filter banks with 3 or more channels by using this Realization Algorithm.

Chapter 9

One-dimensional Multirate Systems

9.1 Reduction to Causal Systems

Many problems in signal processing give rise to Laurent polynomial matrices, and perfect reconstructing filter banks are represented by the unimodularity of these matrices. A preparatory process to be carried out first in this case is to apply the algorithm **LaurentToPoly** that will allow us to apply the techniques known for polynomial matrices to this situation. Let us recall the algorithm **LaurentToPoly**.

Input:	$\mathbf{v}(\boldsymbol{x}) \in (k[\boldsymbol{x}^{\pm 1}])^n$, a **Laurent** polynomial column vector
Output:	$\boldsymbol{x} \to \boldsymbol{y}$, a change of variables $\mathbf{T}(\boldsymbol{x}) \in \mathrm{GL}_n(k[\boldsymbol{x}^{\pm 1}])$, a square unimodular Laurent polynomial matrix
Specification:	(1) $\hat{\mathbf{v}}(\boldsymbol{y}) := \mathbf{T}(\boldsymbol{x})\mathbf{v}(\boldsymbol{x}) \in (k[\boldsymbol{y}])^n$ is a **polynomial** column vector in the new variable $\boldsymbol{y}$ (2) $\mathbf{v}(\boldsymbol{x})$ is unimodular over $k[\boldsymbol{x}^{\pm 1}]$ if and only if $\hat{\mathbf{v}}(\boldsymbol{y})$ is unimodular over $k[\boldsymbol{y}]$

A graphical demonstration of this process is shown in the Figure 9.1.

Now finding an FIR inverse $\mathbf{S}$ to the given FIR filter $\mathbf{A}$ is equivalent to finding a causal inverse $\hat{\mathbf{S}}$ to the causal filter $\hat{\mathbf{A}}$.

Example 9.1.1 Consider the unimodular Laurent polynomial vector $\mathbf{v} = (z, z^2)^t \in k[z^{\pm 1}]$. Convert $\mathbf{v}$ to a unimodular polynomial vector.

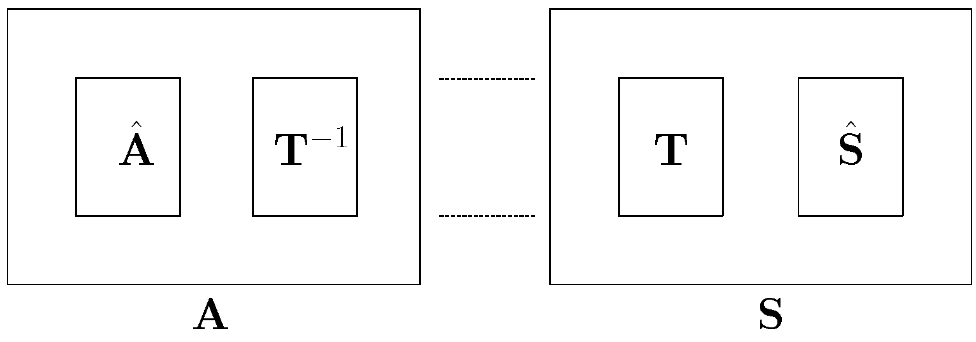

Figure 9.1: Conversion of an FIR system $\mathbf{A}$ to a causal system $\hat{\mathbf{A}}$

In this case, the transformation matrix is

$$\mathbf{T} = \begin{pmatrix} 1/z & 0 \\ 0 & z \end{pmatrix}.$$

And the converted unimodular polynomial vector is

$$\hat{\mathbf{v}} = (1, z^3)^t.$$

□

9.2 Applications of Euclidean Division Algorithm

In this section, we will derive a mathematical formulation for the three problems described in the Introduction and show how unimodularity is involved, and how to solve them in the 1-D case.

Problem 1: *Given a 1-D FIR low-pass filter $G(z)$, decide effectively whether or not $G(z)$ can occur as an analysis filter in a critically downsampled, 2-channel, perfect reconstructing (PR) FIR filter bank. When this decision process yields a positive answer, find* **all** *such filter banks.*

To answer this question, we decompose $G(z)$ into its polyphase components:

$$G(z) = G_0(z^2) + zG_1(z^2).$$

As noted in [VH92], the filter $G(z)$ occurs as the low-pass filter in a 2-channel PR filter bank if and only if there exist Laurent polynomials $\alpha(z)$ and $\beta(z)$ such that

$$\alpha(z)G_0(z) + \beta(z)G_1(z) = 1. \tag{9.1}$$

First, by conducting the preparatory step outlined above, we assume $G_0(z), G_1(z)$ and $\alpha(z), \beta(z)$ are polynomials. Then the condition and the construction of the polynomials $\alpha(z)$ and $\beta(z)$ can be simultaneously solved by the Euclidean Division Algorithm: apply a succession of elementary row operations to the polynomial vector $\begin{pmatrix} G_0(z) \\ G_1(z) \end{pmatrix}$ to reduce it to $\begin{pmatrix} G(z) \\ 0 \end{pmatrix}$ where $G(z) := \gcd(G_0(z), G_1(z))$, i.e. find a $\mathbf{E} \in E_2(k[z])$ such that

$$\mathbf{E} \begin{pmatrix} G_0(z) \\ G_1(z) \end{pmatrix} = \begin{pmatrix} G(z) \\ 0 \end{pmatrix}.$$

If the greatest common divisor of $G_0(z)$ and $G_1(z)$ is not 1 (up to multiplication by constants), then $G(z)$ can not act as the low-pass filter in a 2-channel filter bank. If the greatest common divisor is indeed 1, then the first row

$$(\alpha_0(z), \beta_0(z)) := (1, 0)\mathbf{E}$$

of the unimodular polynomial matrix $\mathbf{E} \in E_2(k[z])$ can be a choice for $(\alpha(z), \beta(z))$, thereby yielding a filter bank with $G(z)$ as its low-pass filter. To find all the filter banks having $G(z)$ as its low-pass filter, let $u(\alpha, \beta) := -\beta_0\alpha + \alpha_0\beta$. Then,

$$\begin{pmatrix} G_0(z) & G_1(z) \\ -\beta_0 & \alpha_0 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} 1 \\ u \end{pmatrix}.$$

Therefore,

$$\begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \alpha_0 & -G_1(z) \\ \beta_0 & G_0(z) \end{pmatrix} \begin{pmatrix} 1 \\ u \end{pmatrix}.$$

Now, regarding u as a free parameter ranging over the Laurent polynomials in $k[z^{\pm 1}]$, we get all the possible FIR filter banks with $G(z)$ as its low-pass filter.

In the following examples, to illustrate the method of consecutive elementary operations, we will first consider a simple FIR filter which is actually not a lowpass filter, but is easy to handle. A real-world lowpass filter for which the construction of the corresponding synthesis filters involves more computational steps will be treated in the second example.

Example 9.2.1 Consider a simple FIR filter $G(z)$ given by

$$G(z) = \frac{1}{z^2} + 1 + 2z - 2z^2 + 5z^3 - 6z^5$$

This $G(z)$ is decomposed into polyphase components as

$$G(z) = G_0(z^2) + zG_1(z^2),$$

where $G_0(z)$ and $G_1(z)$ are found as

$$\begin{aligned} G_0(z) &= \frac{1}{z} + 1 - 2z \\ G_1(z) &= 2 + 5z - 6z^2. \end{aligned}$$

Now we apply the preparatory algorithm **LaurentToPoly** to $\mathbf{A}(z) := (G_0(z), G_1(z))^t$:

- **Preparatory Step 1:**

$$\begin{pmatrix} z & 0 \\ 0 & \frac{1}{z} \end{pmatrix} \begin{pmatrix} G_0(z) \\ G_1(z) \end{pmatrix} = \begin{pmatrix} 1 + z - 2z^2 \\ \frac{2}{z} + 5 - 6z \end{pmatrix}.$$

- **Preparatory Step 2:**

$$\mathbf{E}_{21}(-\frac{2}{z}) \begin{pmatrix} 1 + z - 2z^2 \\ \frac{2}{z} + 5 - 6z \end{pmatrix} = \begin{pmatrix} 1 + z - 2z^2 \\ 3 - 2z \end{pmatrix}.$$

- **Preparatory Step 3:**

$$\mathbf{E}_{21}(-3) \begin{pmatrix} 1 + z - 2z^2 \\ 3 - 2z \end{pmatrix} = \begin{pmatrix} 1 + z - 2z^2 \\ -5z + 6z^2 \end{pmatrix} := \begin{pmatrix} \hat{G}_0(z) \\ \hat{G}_1(z) \end{pmatrix}.$$

  Therefore, we have

$$\hat{\mathbf{A}}(z) = \mathbf{T}(z)\mathbf{A}(z)$$

  where the converted causal filter $\hat{\mathbf{A}}(z) = (\hat{G}_0(z), \hat{G}_1(z))^t$ and the transformation matrix $\mathbf{T}(z)$ are given by

$$\begin{aligned} \hat{\mathbf{A}}(z) &= \begin{pmatrix} 1 + z - 2z^2 \\ -5z + 6z^2 \end{pmatrix} \\ \mathbf{T}(z) &:= \mathbf{E}_{21}(-3)\mathbf{E}_{21}(-\frac{2}{z}) \begin{pmatrix} z & 0 \\ 0 & \frac{1}{z} \end{pmatrix} \\ &= \begin{pmatrix} z & 0 \\ -2 - 3z & \frac{1}{z} \end{pmatrix}. \end{aligned}$$

Now we apply the Euclidean Division Algorithm to $\hat{\mathbf{A}}(z) = (\hat{G}_0(z), \hat{G}_1(z))^t$.

- **Step 1:** Since Euclidean Division yields $\hat{G}_0(z) = -\frac{1}{3}\hat{G}_1(z) + 1 - \frac{2}{3}z$, we have

$$\mathbf{E}_{12}(\frac{1}{3})\begin{pmatrix}\hat{G}_0(z)\\ \hat{G}_1(z)\end{pmatrix} = \begin{pmatrix}1-\frac{2}{3}z\\ -5z+6z^2\end{pmatrix}.$$

- **Step 2:** Since Euclidean Division yields $-5z + 6z^2 = (-6-9z)(1-\frac{2}{3}z) + 6$,

$$\mathbf{E}_{21}(6+9z)\begin{pmatrix}1-\frac{2}{3}z\\ -5z+6z^2\end{pmatrix} = \begin{pmatrix}1-\frac{2}{3}z\\ 6\end{pmatrix}.$$

- **Step 3:**

$$\mathbf{E}_{12}(\frac{-3+2z}{18})\begin{pmatrix}1-\frac{2}{3}z\\ 6\end{pmatrix} = \begin{pmatrix}0\\ 6\end{pmatrix}$$

Combining these together, we have

$$\begin{aligned}
&\mathbf{E}_{12}(\frac{-3+2z}{18})\mathbf{E}_{21}(6+9z)\mathbf{E}_{12}(\frac{1}{3})\begin{pmatrix}\hat{G}_0(z)\\ \hat{G}_1(z)\end{pmatrix}\\
= &\begin{pmatrix}-\frac{5z}{6}+z^2 & \frac{-1-z+2z^2}{6}\\ 6+9z & 3+3z\end{pmatrix}\begin{pmatrix}\hat{G}_0(z)\\ \hat{G}_1(z)\end{pmatrix}\\
= &\begin{pmatrix}0\\ 6\end{pmatrix},
\end{aligned}$$

which implies

$$(6+9z)\cdot\hat{G}_0(z) + (3+3z)\cdot\hat{G}_1(z) = 6,$$

i.e.

$$(1+\frac{3}{2}z)\cdot\hat{G}_0(z) + \frac{1+z}{2}\cdot\hat{G}_1(z) = 1.$$

Therefore, $\hat{\mathbf{S}} := (1+\frac{3}{2}z, \frac{1+z}{2})$ is a left inverse to $\hat{\mathbf{A}}$, and changing back to the original system, we get the corresponding left inverse $\mathbf{S}$ to $\mathbf{A}$:

$$\begin{aligned}
\mathbf{S} &= \hat{\mathbf{S}}\mathbf{B}\\
&= (1+\frac{3}{2}z, \frac{1+z}{2})\begin{pmatrix}z & 0\\ -2-3z & \frac{1}{z}\end{pmatrix}\\
&= \begin{pmatrix}-1-\frac{3}{2}z\\ \frac{1}{2}+\frac{1}{2z}\end{pmatrix}
\end{aligned}$$

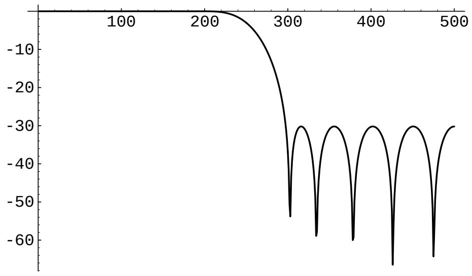

Figure 9.2: Frequency Response of the Lowpass Filter $H(z)$

This gives a synthesis filter

$$\begin{aligned} S(z) &:= -1 - \frac{3}{2}z^2 + z(1 + 1/z^2)/2 \\ &= \frac{1}{2z} - 1 + \frac{z}{2} - \frac{3}{2}z^2. \end{aligned}$$

Now, the one-parameter family of Laurent polynomials

$$\begin{aligned} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} &= \begin{pmatrix} -1 - \frac{3}{2}z & -G_1(z) \\ \frac{1}{2} + \frac{1}{2z} & G_0(z) \end{pmatrix} \begin{pmatrix} 1 \\ u \end{pmatrix} \\ &= \begin{pmatrix} -1 - \frac{3}{2}z - u(2 + 5z - 6z^2) \\ \frac{1}{2} + \frac{1}{2z} + u(\frac{1}{z} + 1 - 2z) \end{pmatrix}, \quad u \in k[z^{\pm 1}] \end{aligned}$$

cover all the possible Laurent polynomial solutions to $\alpha(z)G_0(z) + \beta(z)G_1(z) = 1$. □

Example 9.2.2 Consider a causal lowpass filter $H(z)$ given by

$$\begin{aligned} H(z) &= 0.1605 + 0.4156z + 0.4592z^2 + 0.1487z^3 - 0.1643z^4 - 0.1245z^5 + 0.0825z^6 + \\ &\quad 0.0887z^7 - 0.0508z^8 - 0.0608z^9 + 0.0351z^{10} + 0.0399z^{11} - 0.0256z^{12} - \\ &\quad 0.0244z^{13} + 0.0186z^{14} + 0.0135z^{15} - 0.0131z^{16} - 0.0074z^{17} + 0.0129z^{18} - \\ &\quad 0.0050z^{19} \end{aligned}$$

whose lowpass characteristic is shown in the Figure 9.2.

This is decomposed into polyphase components as

$$H(z) = H_0(z^2) + zH_1(z^2),$$

where $H_0(z)$ and $H_1(z)$ are

$$H_0(z) = 0.1605 + 0.4592z - 0.1643z^2 + 0.0825z^3 - 0.0508z^4 + 0.0351z^5 - 0.0256z^6 +$$

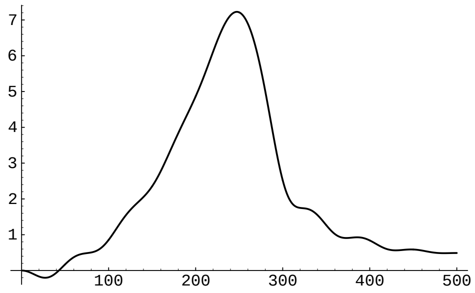

Figure 9.3: Frequency Response of the Synthesis Filter $F(z)$

$$
\begin{aligned}
& 0.0186z^7 - 0.0131z^8 + 0.0129z^9, \\
H_1(z) &= 0.4156 + 0.1487z - 0.1245z^2 + 0.0887z^3 - 0.0608z^4 + 0.0399z^5 - 0.0244z^6 + \\
& 0.0135z^7 - 0.0074z^8 - 0.0050z^9.
\end{aligned}
$$

Euclidean Division yields

$$H_0(z) = -2.5893H_1(z) + r(z)$$

with the remainder

$$
\begin{aligned}
r(z) &= 1.2367 + 0.8442\,z - 0.4867\,z^2 + 0.3123\,z^3 - 0.208349\,z^4 + 0.138472\,z^5 \\
& -0.0888109\,z^6 + 0.0536797\,z^7 - 0.0323696\,z^8.
\end{aligned}
$$

Carrying out the corresponding elementary operation gives

$$\mathbf{E}_{12}(2.5893)\begin{pmatrix} H_0(z) \\ H_1(z) \end{pmatrix} = \begin{pmatrix} r(z) \\ H_1(z) \end{pmatrix}.$$

Repeating the same procedure to the polynomial vector $\begin{pmatrix} r(z) \\ H_1(z) \end{pmatrix}$, we eventually get $\mathbf{A} \in E_2(\mathbb{C}[z])$, a product of 10 elementary matrices, such that

$$\mathbf{A}\begin{pmatrix} H_0(z) \\ H_1(z) \end{pmatrix} = \begin{pmatrix} 0.7661 \\ 0 \end{pmatrix}.$$

Let $\mathbf{B} := \frac{1}{0.7661}\mathbf{A}$. Then

$$\mathbf{B}\begin{pmatrix} H_0(z) \\ H_1(z) \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

An explicit computation shows

$$\begin{aligned}
B_{11}(z) &= -0.4138 + 0.5743\,z - 0.3989\,z^2 + 0.2652\,z^3 - 0.1667\,z^4 + 0.0960\,z^5 - \\
&\quad 0.0478\,z^6 + 0.0164\,z^7 + 0.0154\,z^8 \\
B_{12}(z) &= 2.5658 - 0.6827\,z + 0.3689\,z^2 - 0.2369\,z^3 + 0.1658\,z^4 - 0.1189\,z^5 + \\
&\quad 0.0839\,z^6 - 0.0572\,z^7 + 0.0398\,z^8 \\
B_{21}(z) &= -0.7081 - 0.2533\,z + 0.2121\,z^2 - 0.1512\,z^3 + 0.1036\,z^4 - 0.0679\,z^5 + \\
&\quad 0.0416\,z^6 - 0.0231\,z^7 + 0.0127\,z^8 + 0.0085\,z^9 \\
B_{22}(z) &= 0.2735 + 0.7824\,z - 0.2799\,z^2 + 0.1406\,z^3 - 0.0865\,z^4 + 0.0599\,z^5 - \\
&\quad 0.0436\,z^6 + 0.0317\,z^7 - 0.0223\,z^8 + 0.0220\,z^9.
\end{aligned}$$

Hence, we have

$$B_{11}H_0(z) + B_{12}H_1(z) = 1.$$

Now, the filter

$$\begin{aligned}
F(z) &= B_{11}(z^2) + zB_{12}(z^2) \\
&= -0.4138 + 2.5658\,z + 0.5743\,z^2 - 0.6827\,z^3 - 0.3989\,z^4 + 0.3689\,z^5 + \\
&\quad 0.2652\,z^6 - 0.2369\,z^7 - 0.1667\,z^8 + 0.1657\,z^9 + 0.0960\,z^{10} - 0.1189\,z^{11} - \\
&\quad 0.0478\,z^{12} + 0.0839\,z^{13} + 0.0164\,z^{14} - 0.0572\,z^{15} + 0.0154\,z^{16} + 0.0398\,z^{17}
\end{aligned}$$

is a desired synthesis filter, whose frequency response is shown in the Figure 9.3. Actually, what we get is a 1-parameter family of synthesis filters, and making a good choice of $u \in k[z^{\pm 1}]$ will give us a synthesis filter with a more desirable frequency response. $\square$

Problem 2: *Given a sample rate conversion scheme consisting of upsampling by p, filtering with a 1-D FIR filter $U(z)$ and downsampling by q, decide effectively whether or not this scheme is FIR invertible.*

To answer this question, we may assume that the numbers p and q are coprime, $p > q$. Let $U(z) = \sum_{i=0}^{pq-1} z^i U_i(z^{pq})$ be its polyphase decomposition with respect to pq. Let the expression $U_{kl}(z)$, $0 \le k < p$, $0 \le l < q$, be the polyphase component $U_i(z)$ such that $i \equiv k \pmod{p}$ and $i \equiv l \pmod{q}$. Invertibility of the sample rate conversion scheme can then be formulated as the existence of a Laurent polynomial matrix $\mathbf{D} = (D_{m,k}(z))$ which is a left inverse of $\mathbf{U} = (U_{kl}(z))$.

Since a Laurent polynomial matrix has a left inverse if and only if it is unimodular (Theorem 10.1.3), there exist $l := \binom{p}{q}$ polynomials $D_i(z)$ such that

$$\sum_{i=1}^{l} D_i(z) M_i(z) \quad = \quad 1,$$

where $M_i(z)$ ranges over the maximal minors of $\mathbf{U}$.

So, the second question is about determining the unimodularity of the Laurent polynomial matrix $\mathbf{U}$, or equivalently, the unimodularity of the Laurent polynomial vector $(M_1, \ldots, M_l) \in (\mathbb{C}[z^{\pm 1}])^l$.

This unimodularity determination problem can be readily solved once we notice that, due to the the Laurent polynomial analogue of Hilbert Nullstellensatz over $\mathbb{C}$, $\sum_i D_i(z) M_i(z) = 1$ is possible if and only if the Laurent polynomials $M_i(z)$'s, $1 \leq i \leq \binom{p}{q}$, have no nonzero common roots, i.e. no roots in $\mathbb{C}^*$. Since each univariate Laurent polynomial $M_i(z)$ has only finitely many zeros which can be explicitly found using any existing computer algebra packages, we can tell if $M_i(z)$'s have a nonzero common root or not, and thereby determining if $\mathbf{U}$ is unimodular.

Example 9.2.3 Consider a sample rate conversion scheme consisting of upsampling by $p = 3$, filtering with an FIR filter $U(z)$ and downsampling by $q = 2$, where $U(z)$ is given by

$$\begin{aligned} U(z) \quad = \quad & \frac{3}{z^6} + \frac{6}{z^5} + \frac{6}{z^3} + \frac{3}{z^2} - 2 + 29z + 25z^3 + 2z^5 - 2z^6 - 4z^7 + 2z^8 - 23z^9 - 2z^{10} + \\ & 4z^{11} + 2z^{12} - 20z^{13} - 16z^{15} + 20z^{17} + 20z^{21}. \end{aligned}$$

Then we get the polyphase decomposition $U(z) = \sum_{i=0}^{5} z^i U_i(z^6)$ of $U(z)$ where $U_i(z)$'s are found as

$$\begin{aligned} U_0(z) &= \frac{3}{z} - 2 - 2z + 2z^2 \\ U_1(z) &= \frac{6}{z} + 29 - 4z - 20z^2 \\ U_2(z) &= 2z \\ U_3(z) &= \frac{6}{z} + 25 - 23z - 16z^2 + 20z^3 \\ U_4(z) &= \frac{3}{z} - 2z \\ U_5(z) &= 2 + 4z + 20z^2. \end{aligned}$$

Now, note that $U_{10}(z) = U_4(z)$ since $i = 4$ is the only integer in $[0, 5]$ such that

$$\begin{aligned} i &\equiv 1 \pmod 3 \\ i &\equiv 0 \pmod 2. \end{aligned}$$

Continuing in this way, we get

$$\mathbf{U} = \begin{pmatrix} U_0(z) & U_3(z) \\ U_4(z) & U_1(z) \\ U_2(z) & U_5(z) \end{pmatrix}$$

The three maximal minors of $\mathbf{U}$ are

$$\begin{aligned} M_1(z) &= \begin{vmatrix} U_0(z) & U_3(z) \\ U_4(z) & U_1(z) \end{vmatrix} = -1 \\ M_2(z) &= \begin{vmatrix} U_0(z) & U_3(z) \\ U_2(z) & U_5(z) \end{vmatrix} = \frac{6}{z} - 4 - 2z + 2z^2 \\ M_3(z) &= \begin{vmatrix} U_4(z) & U_1(z) \\ U_2(z) & U_5(z) \end{vmatrix} = \frac{6}{z} - 2z \end{aligned}$$

which obviously don't have any common roots.

Consequently the given scheme is FIR invertible. □

Problem 3: *Given an oversampled 1-D FIR analysis filter bank, decide effectively whether or not there is an FIR synthesis filter bank such that the overall system is PR. When this decision process yields a positive answer, provide a complete parametrization of all such FIR synthesis filter banks.*

An oversampled filter bank corresponds to a non-square polyphase matrix, and the problem is asking whether or not we can find a left inverse for this non-square polyphase matrix. Let the polyphase matrix be $\mathbf{A}$, a $p \times q$ Laurent polynomial matrix, $p \geq q$. Since this polyphase matrix has a left inverse if and only if it is unimodular, we can first determine its unimodularity by the method outlined for the second problem. If this test shows the unimodularity of $\mathbf{A}$, we first apply the algorithm **LaurentToPoly** to $\mathbf{A}$ converting $\mathbf{A}$ to a unimodular polynomial matrix $\hat{\mathbf{A}}$. Then, by using the Euclidean Division Algorithm, we apply a succession of elementary operations to $\hat{\mathbf{A}}$ to reduce it to the following $p \times q$ matrix

$$\begin{pmatrix} \mathbf{I}_q \\ \mathbf{0} \\ \vdots \\ \mathbf{0} \end{pmatrix} \in \mathrm{M}_{pq}(k),$$

where $\mathbf{I}_q$ is the $q \times q$ identity matrix, and $\mathbf{0}$ is the q-dimensional zero row vector.

This means that we can find $\mathbf{E} \in \mathrm{E}_p(k[z])$, a product of elementary matrices, such that

$$\mathbf{EA} = \begin{pmatrix} \mathbf{I}_q \\ \mathbf{0} \\ \vdots \\ \mathbf{0} \end{pmatrix}.$$

Now take the first q rows of $\mathbf{E}$ to make a $q \times p$ matrix $\mathbf{F}$, i.e.

$$\mathbf{F} := (\mathbf{I}_q, \mathbf{0}, \ldots, \mathbf{0})\mathbf{E}.$$

Then $\mathbf{F}$ is a desired left inverse of $\mathbf{A}$. Note here that $\mathbf{A} = \mathbf{E}^{-1} \begin{pmatrix} \mathbf{I}_q \\ \mathbf{0} \\ \vdots \\ \mathbf{0} \end{pmatrix}$ implies $\mathbf{E}^{-1} \in \mathrm{GL}_p(k[z])$ is a unimodular completion of $\mathbf{A}$.

To get a complete parametrization of all the possible left inverses of $\mathbf{A}$, let $\mathbf{B} \in \mathrm{M}_{qp}(k[z])$ an arbitrary left inverse of $\mathbf{A}$. Then

$$\mathbf{BA} = \mathbf{I}_q.$$

Now, since $\mathbf{E}^{-1}$ is a unimodular completion of $\mathbf{A}$,

$$\mathbf{BE}^{-1} = (\mathbf{I}_q, \mathbf{u}_1, \ldots, \mathbf{u}_{p-q})$$

for some $\mathbf{u}_1, \ldots, \mathbf{u}_{p-q} \in (k[z^{\pm 1}])^q$. Now, regarding $\mathbf{u}_1, \ldots, \mathbf{u}_{p-q}$ as free parameters ranging over q-dimensional Laurent polynomial vectors, we get a complete parametrization of the left inverses to $\mathbf{A}$ in terms of $(p-q)q$ parameters ranging over the Laurent polynomials in $k[z^{\pm 1}]$:

$$\mathbf{B} = (\mathbf{I}_q, \mathbf{u}_1, \ldots, \mathbf{u}_{p-q})\mathbf{E}.$$

Remark 9.2.4 If $p = q$, i.e. if the polyphase matrix $\mathbf{A}$ is a square unimodular matrix, then the number of free parameters is $(p-q)q = 0$. This coincides with the fact that a square unimodular matrix has a unique inverse.

Example 9.2.5 Consider an oversampled 1-D FIR analysis filter bank whose polyphase matrix is the matrix $\mathbf{U}$ of the previous example. We already saw in that example that

$$\mathbf{U} \;\; = \;\; \begin{pmatrix} \frac{3}{z} - 2 - 2z + 2z^2 & \frac{6}{z} + 25 - 23z - 16z^2 + 20z^3 \\ \frac{3}{z} - 2z & \frac{6}{z} + 29 - 4z - 20z^2 \\ 2z & 2 + 4z + 20z^2 \end{pmatrix}$$

is unimodular, so there is an FIR synthesis filter bank such that the overall system is PR. Now we want to find all such FIR synthesis filter banks.

Closely following the algorithm outlined in the above, we get

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

where the 3×3 matrix $\mathbf{E}$ is found as

$$\begin{pmatrix} \frac{z}{18}(-18-125z-188z^2+252z^3-215z^4+178z^5+6z^6) & \frac{z}{3}(-2-27z+30z^2+z^3) & \frac{(-12-89z+51z^2-60z^3-2z^4)}{6} \\ \frac{z}{6}(3+19z-32z^2+23z^3-9z^4-8z^5+6z^6) & z(4-3z-z^2+z^3) & 9/2-4z+3z^2/2+z^3-z^4 \\ z(-4z+23z^2/3-5z^3+z^4+8z^5/3-2z^6) & 2z(-3+2z+z^2-z^3) & -6+6z-z^2-2z^3+2z^4 \end{pmatrix}.$$

Now a general left inverse of $\mathbf{U}$ is in the form

$$\begin{pmatrix} 1 & 0 & u \\ 0 & 1 & v \end{pmatrix} \mathbf{E},$$

where u, v are arbitrary Laurent polynomials in $k[z^{\pm 1}]$. $\square$

Chapter 10

Multidimensional Multirate Systems

10.1 Unimodularity and Left Inverses

For $p \geq q$, let $\mathbf{A} \in \mathrm{M}_{pq}(k[\boldsymbol{x}^{\pm 1}])$, and $\mathbf{B} \in \mathrm{M}_{qp}(k[\boldsymbol{x}^{\pm 1}])$. Denote the i-th column vectors of the $q \times p$ matrices $\mathbf{B}$ and $\mathbf{A}^t$ by $\mathbf{v}_i$ and $\mathbf{w}_i$, respectively. For a sequence of integers $\mathbf{i} = (i_1, \ldots, i_q)$ with $1 \leq i_1 < \cdots < i_q \leq p$, take the q column vectors $\mathbf{v}_{i_1}, \ldots, \mathbf{v}_{i_q}$ from $\mathbf{B}$, and q row vectors $\mathbf{w}_{i_1}^t, \ldots, \mathbf{w}_{i_q}^t$ from $\mathbf{A}$ to define $q \times q$ square matrices $\mathbf{B}_{\mathbf{i}}$ and $\mathbf{A}^{\mathbf{i}}$.

Then $\mathbf{BA} \in \mathrm{M}_q(k[\boldsymbol{x}^{\pm 1}])$ is a square matrix and its determinant can be computed from the maximal minors of $\mathbf{A}$ and $\mathbf{B}$ by the following formula:

Lemma 10.1.1 (Binet-Cauchy Formula) *With notations in the above,*

$$\det(\mathbf{BA}) = \sum_{\mathbf{i} \in I} \det(\mathbf{B}_{\mathbf{i}}) \det(\mathbf{A}^{\mathbf{i}}),$$

where $I := \{(i_1, \ldots, i_q) \mid 1 \leq i_1 < \cdots < i_q \leq p\}$.

Proof: See [Gan77]. $\square$

Example 10.1.2 Let $\mathbf{A} = \begin{pmatrix} 1 & 3 \\ 2 & 1 \\ 4 & -1 \end{pmatrix}$, and $\mathbf{B} = \begin{pmatrix} 2 & 1 & 1 \\ -1 & 2 & 1 \end{pmatrix}$. Then,

$$\begin{aligned} \det(\mathbf{BA}) &= \begin{vmatrix} 8 & 6 \\ 7 & -2 \end{vmatrix} \\ &= -58. \end{aligned}$$

Since the index set is $I = \{(1,2),(1,3),(2,3)\}$, the right hand side of the Binet-Cauchy Formula reads as

$$\begin{aligned}
& \sum_{\mathbf{i}\in I} \det(\mathbf{B_i}) \det(\mathbf{A^i}) \\
= \; & \det(\mathbf{B}_{(1,2)}) \det(\mathbf{A}^{(1,2)}) + \det(\mathbf{B}_{(1,3)}) \det(\mathbf{A}^{(1,3)}) + \det(\mathbf{B}_{(2,3)}) \det(\mathbf{A}^{(2,3)}) \\
= \; & \begin{vmatrix} 2 & 1 \\ -1 & 2 \end{vmatrix} \cdot \begin{vmatrix} 1 & 3 \\ 2 & 1 \end{vmatrix} + \begin{vmatrix} 2 & 1 \\ -1 & 1 \end{vmatrix} \cdot \begin{vmatrix} 1 & 3 \\ 4 & -1 \end{vmatrix} + \begin{vmatrix} 1 & 1 \\ 2 & 1 \end{vmatrix} \cdot \begin{vmatrix} 2 & 1 \\ 4 & -1 \end{vmatrix} \\
= \; & 5 \cdot (-5) + 3 \cdot (-13) + (-1) \cdot (-6) \\
= \; & -58.
\end{aligned}$$

This coincides with the prediction of the Binet-Cauchy Formula. □

The following theorem has many important consequences as mentioned in Chapter 8, and has been already used in the previous chapter.

Theorem 10.1.3 *A $p \times q$ Laurent polynomial matrix $\mathbf{A}$ ($p \geq q$) has a left inverse if and only if it is unimodular.*

Proof: ($\Longrightarrow$:) Suppose $\mathbf{B} \in \mathrm{M}_{qp}(k[\boldsymbol{x}^{\pm 1}])$ is a left inverse of $\mathbf{A}$. Then the Binet-Cauchy Formula applied to $\mathbf{BA} = \mathbf{I}_q$ implies

$$\sum_{\mathbf{i}\in I} \det(\mathbf{B_i}) \det(\mathbf{A}^t_{\mathbf{i}}) = 1.$$

Hence, the maximal minors of $\mathbf{A}$, $\{\det(\mathbf{A}^t_{\mathbf{i}}) \mid \mathbf{i} \in I\}$, generate the unit ideal in $k[\boldsymbol{x}^{\pm 1}]$, i.e. $\mathbf{A}$ is unimodular.

($\Longleftarrow$:) By using the Unimodular Completion Algorithm for Laurent polynomial rings developed in Corollary 6.1.1, we can complete the unimodular matrix $\mathbf{A} \in \mathrm{M}_{pq}(k[\boldsymbol{x}^{\pm 1}])$ to a square unimodular matrix $\bar{\mathbf{A}} \in \mathrm{GL}_p(k[\boldsymbol{x}^{\pm 1}])$. Now, from $\bar{\mathbf{A}}^{-1}\bar{\mathbf{A}} = \mathbf{I}_p$, one sees easily that the $q \times p$ matrix $\mathbf{B}$ made from the first q rows of $\bar{\mathbf{A}}^{-1}$ is a left inverse of the $p \times q$ matrix made from the first q columns of $\bar{\mathbf{A}}$, i.e. $\mathbf{BA} = \mathbf{I}_q$. □

10.2 Two Methods of Causal Reduction

If we consider the three problems in their MD versions, the conditions which need to be satisfied resemble their 1-D counter parts Eq. (9.1) and Eq. (9.2). The only difference is that we have to replace the variable z by $\boldsymbol{z} := (z_1, \cdots, z_n)$. However, the Euclidean Division Algorithm is no longer valid, and thus the coefficients $\alpha(z)$, $\beta(z)$ and $D_i(z)$ and their existence have to be found in another way.

Naturally, the Gröbner bases techniques offer a solution in this MD set-up, and we should be able to apply Gröbner bases computations to solve our three problems.

However, since our questions involve **Laurent** polynomials, we have to perform a preparatory process to convert the problems to causal problems.

While we already have presented a systematic method to this effect in Chapter 6, there is an alternative method for this causal reduction outlined in [KPV95]: for every variable z_i we introduce two new variables x_i and y_i. Substituting x_i^m for every positive power z_i^m and y_i^k for every negative power z_i^{-k}, we transform the original set of Laurent polynomials into a set of regular polynomials. We then enlarge this set by adding the polynomials $x_iy_i - 1$. One verifies that the constant 1 is a linear combination of the original set of Laurent polynomials if and only if the same is true for the constructed set of regular polynomials. Moreover, given a linear combination of polynomials , we find a linear combination of Laurent polynomials by back substitution: x_i and y_i are replaced by z_i and z_i^{-1} respectively.

There are, however, some drawbacks with this method. First, it significantly increases the complexity of the problem by introducing extra variables and by enlarging the size of the given polynomial vector. Also, a complete parametrization of solutions needs separate computation.

Therefore, we will mainly use the algorithm **LaurentToPoly** for the purpose of our causal reduction.

In the following, we give an example in which we apply the algorithm **LaurentToPoly** to reduce the given multidimensional FIR systems to causal systems of the same dimension.

Example 10.2.1 Let $\mathbf{v} := \begin{pmatrix} v_1 \\ v_2 \end{pmatrix} = \begin{pmatrix} \frac{1}{y} + \frac{x}{y} + x \\ \frac{x}{y^2} + 1 + y + xy \end{pmatrix} \in (k[x^{\pm 1}, y^{\pm 1}])^2$.

- **Step 1:** Write v_1 in terms of x, i.e. express it as a polynomial in $S[x]$ where $S := k[y^{\pm 1}]$: $v_1 = \frac{1}{y} + (\frac{1}{y} + 1)x$. One sees that the leading coefficient $\frac{1}{y} + 1$ of v_1 is not a unit in S. So we apply the algorithm **LaurentNoether** to v_1.

  Define a new variable z by putting $y = zx^l$ where the integer l is to be determined. With respect to the new variables x and z, v_1 becomes $v_1 = \frac{1}{zx^l} + \frac{1}{zx^{l-1}} + x$. Let $l = 1$.

Then $v_1 = \frac{1}{zx} + \frac{1}{z} + x \in S'[x^{\pm 1}]$ where $S' := k[z^{\pm 1}]$ and the leading and the lowest coefficients of $v_1 \in S'[x^{\pm 1}]$ are units of S'.

- **Step 2:** We have

$$\mathbf{v} = \begin{pmatrix} \frac{1}{zx} + \frac{1}{z} + x \\ \frac{1}{z^2 x} + 1 + zx + zx^2 \end{pmatrix} \in (S'[x^{\pm 1}])^2.$$

Then

$$\begin{aligned} \mathbf{v}_1 &:= \begin{pmatrix} zx & 0 \\ 0 & \frac{1}{zx} \end{pmatrix} \mathbf{v} \\ &= \begin{pmatrix} 1 + x + x^2 z \\ \frac{1}{z^3 x^2} + \frac{1}{zx} + 1 + x \end{pmatrix}. \end{aligned}$$

Now we apply elementary operations to $\mathbf{v}_1$ to make its second component a polynomial in x whose constant term is zero.

1.

$$\begin{aligned} \mathbf{v}_2 &:= \mathbf{E}_{21}(-\frac{1}{z^3 x^2})\mathbf{v}_1 \\ &= \begin{pmatrix} 1 + x + x^2 z \\ -\frac{1}{z^3 x} + \frac{1}{zx} + 1 - z^{-2} + x \end{pmatrix}. \end{aligned}$$

2.

$$\begin{aligned} \mathbf{v}_3 &:= \mathbf{E}_{21}((\frac{1}{z^3} - \frac{1}{z})x)\mathbf{v}_2 \\ &= \begin{pmatrix} 1 + x + x^2 z \\ \frac{1}{z^3} - \frac{1}{z^2} - \frac{1}{z} + 1 + \frac{x}{z^2} \end{pmatrix}. \end{aligned}$$

3.

$$\begin{aligned} \hat{\mathbf{v}} &:= \mathbf{E}_{21}(-\frac{1}{z^3} + \frac{1}{z^2} + \frac{1}{z} - 1)\mathbf{v}_3 \\ &= \begin{pmatrix} 1 + x + x^2 z \\ \frac{x\left(-1+2z-xz+z^2+xz^2-z^3+xz^3-xz^4\right)}{z^3} \end{pmatrix}. \end{aligned}$$

The transformation matrix is

$$\mathbf{T} := \mathbf{E}_{21}(-\frac{1 - z - z^2 + z^3}{z^3})\mathbf{E}_{21}((\frac{1}{z^3} - \frac{1}{z})x)\mathbf{E}_{21}(-\frac{1}{z^3 x^2}) \begin{pmatrix} zx & 0 \\ 0 & \frac{1}{zx} \end{pmatrix},$$

and the converted vector is

$$\hat{\mathbf{v}} = \mathbf{T}\mathbf{v} = \begin{pmatrix} 1 + x + x^2 z \\ \frac{x\left(-1+2z-xz+z^2+xz^2-z^3+xz^3-xz^4\right)}{z^3} \end{pmatrix}.$$

- Now we make another change of variables. Define a new variable w by $x = w \cdot z^l$ where the integer l is to be determined.

  Then w.r.t. the new variables z, w, $\hat{\mathbf{v}}$ becomes

$$\hat{\mathbf{v}} = \begin{pmatrix} 1 + wz^l + w^2 z^{2l+1} \\ wz^{l-3}\left(-1 + 2z - wz^{l+1} + z^2 + wz^{l+2} - z^3 + wz^{l+3} - wz^{l+4}\right) \end{pmatrix}.$$

  Let $l = 3$ since it is the smallest integer that makes the components of $\hat{\mathbf{v}}$ polynomials in z and w. Then

$$\begin{aligned} \hat{\mathbf{v}} &:= \begin{pmatrix} \hat{v_1} \\ \hat{v_2} \end{pmatrix} \\ &= \begin{pmatrix} 1 + wz^3 + w^2 z^7 \\ w\ (-1 + 2z + z^2 - z^3 - wz^4 + wz^5 + wz^6 - wz^7) \end{pmatrix}. \end{aligned}$$

Now the unimodularity of $\mathbf{v}$ as a Laurent polynomial vector in $k[x^{\pm 1}, y^{\pm 1}]$ is equivalent to the unimodularity of $\hat{\mathbf{v}}$ as a polynomial vector in $k[z, w]$.

Now a computation with SINGULAR shows that the reduced Gröbner basis of $\{\hat{v_1}, \hat{v_2}\} \subset k[w, z]$ w.r.t. the reverse degree lexicographic order is

$$\{-z^2 + 81w + 17z - 11, -21wz - 4z^2 + 9w + 5z - 2, -567w^2 - 116wz - z^2 + 77w - 2z + 4\}.$$

Therefore $\hat{\mathbf{v}}$ is not unimodular over $k[w, z]$, and neither is $\mathbf{v}$ over $k[x^{\pm 1}, y^{\pm 1}]$. $\square$

10.3 Syzygies and Parametrization of Filter Banks

For any given multidimensional FIR filter which can be the analysis filter of an MD perfect reconstructing FIR filter bank, we can find a corresponding synthesis filter by using the the method of Gröbner basis as was demonstrated in the proof of Theorem 10.1.3. But this particular filter is by no means unique. And the nonuniqueness of solutions is measured by syzygy.

In this section, for an arbitrary Laurent polynomial matrix, we will attempt to give a **complete** and **canonical** parametrization for all of its left inverses if there is any.

In matrix terminology, we will find some free parameters in terms of which an arbitrary left inverse of the given unimodular Laurent polynomial matrix can be **uniquely** written. Because of the uniqueness here, the number of such free parameters is an invariant for the given matrix and represents the **degree of freedom** in obtaining its left inverses.

It will be shown that, for a $p \times q$ unimodular matrix, the degree of freedom associated to finding its left inverses is $q \times (p-q)$.

In [KPV95], a complete parametrization formula was achieved with which we can express any synthesis filter corresponding to the given analysis filter. While this parametrization is **complete** in the sense that it exhausts all the possible synthesis filters corresponding to the given analysis filter, it is not **canonical**, i.e. the expression of a synthesis filter in terms of the parameters is not unique. We will remedy this situation here with the aid of the Quillen-Suslin Theorem.

For a simple example, consider an invertible FIR filter whose polyphase matrix is $(f_1, \ldots, f_n)^t \in k[\boldsymbol{x}^{\pm 1}]$. In order to find its left inverses, we have to consider all the solutions to the following equation:

$$\sum_{i=1}^{n} \lambda_i(\boldsymbol{x}) f_i(\boldsymbol{x}) \quad = \quad 1. \tag{10.1}$$

If $\{\lambda_i(\boldsymbol{x}) \in k[\boldsymbol{x}^{\pm 1}] \mid i = 1, \ldots, n\}$ is a solution to this equation, then $\{\mu_i(\boldsymbol{x}) \in k[\boldsymbol{x}^{\pm 1}] \mid i = 1, \ldots, n\}$ is also a solution if and only if $(\mu_1(\boldsymbol{x}) - \lambda_1(\boldsymbol{x}), \ldots, \mu_n(\boldsymbol{x}) - \lambda_n(\boldsymbol{x}))$ belongs to the syzygy module $S := \{(h_1, \ldots, h_n) \in (k[\boldsymbol{x}^{\pm 1}])^n \mid \sum_{i=1}^{n} h_i f_i(\boldsymbol{x}) = 0\}$.

Therefore the problem of giving a complete parametrization for the solutions to Eq. 10.1 is equivalent to finding a finite basis for the syzygy module S.

In the 1-D case, an explicit process of finding such a basis using the Euclidean Division Algorithm was shown in detail in the previous chapter.

In the MD case, the syzygy module

$$S := \{(h_1, \ldots, h_n) \in (k[\boldsymbol{x}^{\pm 1}])^n \mid \sum_{i=1}^{n} h_i f_i(\boldsymbol{x}) = 0\}$$

ia a free module of rank $n-1$ by the Laurent polynomial analogue of the Quillen-Suslin Theorem, and its free basis $\{\mathbf{s}_1(\boldsymbol{x}), \ldots, \mathbf{s}_{n-1}(\boldsymbol{x})\}$ can be found by the algorithm developed in Chapter 6, i.e. convert the problem to the case of polynomial rings by using the algorithm **LaurentToPoly** and then compute its reduced Gröbner basis w.r.t. any fixed monomial order.

Then $\{\mu_i(\boldsymbol{x}) \mid i = 1, \ldots, n\}$ is a solution to the Eq. 10.1 if and only if there exist $\{u_1(\boldsymbol{x}), \ldots, u_{n-1}(\boldsymbol{x})\} \subset k[\boldsymbol{x}^{\pm 1}]$ such that

$$(\mu_1(\boldsymbol{x}), \ldots, \mu_n(\boldsymbol{x})) \quad = \quad (\lambda_1(\boldsymbol{x}), \ldots, \lambda_n(\boldsymbol{x})) + u_1(\boldsymbol{x})\mathbf{s}_1(\boldsymbol{x}) + \cdots + u_{n-1}(\boldsymbol{x})\mathbf{s}_{n-1}(\boldsymbol{x}).$$

So, there are $n-1$ free parameters involved in this case, too.

For the general case, consider an invertible FIR filter whose polyphase matrix is $\mathbf{A} = (f_{ij}) \in \mathrm{M}_{pq}(k[\boldsymbol{x}^{\pm 1}])$, $p \geq q$, which is unimodular due to the FIR invertibility of the filter it represents. In order to find its left inverses, we have to consider all the $q \times p$ Laurent polynomial matrices that are solutions to the following equation:

$$\mathbf{BA} \;=\; \mathbf{I}_q. \tag{10.2}$$

Denote the p row vectors of $\mathbf{A}$ by

$$\begin{aligned}
\mathbf{v}_1 &:= (f_{11}, \ldots, f_{1q}) \\
&\vdots \\
\mathbf{v}_p &:= (f_{p1}, \ldots, f_{pq}).
\end{aligned}$$

If $\mathbf{B}_{part} \in \mathrm{M}_{qp}(k[\boldsymbol{x}^{\pm 1}])$ is a particular solution to the above Equation 10.2, then $\mathbf{B} \in \mathrm{M}_{qp}(k[\boldsymbol{x}^{\pm 1}])$ is also a solution to it if and only if $(\mathbf{B} - \mathbf{B}_{part})\mathbf{A} = \mathbf{0} \in \mathrm{M}_q(k[\boldsymbol{x}^{\pm 1}])$.

For each $i = 1, \ldots, q$, let $\mathbf{w}_i := (w_{i1}, \ldots, w_{iq}) \in (k[\boldsymbol{x}])^p$ denote the i-th row vector of $\mathbf{B} - \mathbf{B}_{part}$. Then

$$\begin{aligned}
(\mathbf{B} - \mathbf{B}_{part})\mathbf{A} &= \begin{pmatrix} w_{11} & \cdots & w_{1p} \\ \vdots & & \vdots \\ w_{q1} & \cdots & w_{qp} \end{pmatrix} \begin{pmatrix} f_{11} & \cdots & f_{1q} \\ \vdots & & \vdots \\ f_{p1} & \cdots & f_{pq} \end{pmatrix} \\
&= \begin{pmatrix} w_{11}\mathbf{v}_1 + \cdots + w_{1p}\mathbf{v}_p \\ \vdots \\ w_{q1}\mathbf{v}_1 + \cdots + w_{qp}\mathbf{v}_p \end{pmatrix}.
\end{aligned}$$

Therefore, $\mathbf{B} \in \mathrm{M}_{qp}(k[\boldsymbol{x}^{\pm 1}])$ is a a solution to the Equation 10.2 if and only if each row of $\mathbf{B} - \mathbf{B}_{part}$ belongs to the kernel of the following $k[\boldsymbol{x}]$-module homomorphism:

$$\begin{aligned}
\alpha :\; (k[\boldsymbol{x}^{\pm 1}])^p &\longrightarrow (k[\boldsymbol{x}^{\pm 1}])^q \\
\mathbf{h} = (h_1, \ldots, h_p) &\mapsto h_1\mathbf{v}_1 + \cdots + h_p\mathbf{v}_p.
\end{aligned}$$

Due to the unimodularity of $\mathbf{A}$, α is onto and the kernel of this homomorphism α is a direct summand of $(k[\boldsymbol{x}^{\pm 1}])^p$ i.e. projective and therefore free of rank $p-q$ by the Laurent polynomial analogue of the Quillen-Suslin Theorem. And its free basis $\mathbf{s}_1(\boldsymbol{x}), \ldots, \mathbf{s}_{p-q}(\boldsymbol{x}) \in (k[\boldsymbol{x}^{\pm 1}])^p$ can be explicitly found using the algorithm of Chapter 6.

Since each row of $\mathbf{B}-\mathbf{B}_{part}$ is a **unique** linear combination (with Laurent polynomial coefficient) of $\mathbf{s_i}(\boldsymbol{x})$'s, we have

$$\begin{aligned}
\mathbf{w}_1 &= u_{11}(\boldsymbol{x})\mathbf{s}_1(\boldsymbol{x}) + \cdots + u_{1(p-q)}(\boldsymbol{x})\mathbf{s}_{p-q}(\boldsymbol{x}) \\
&\vdots \\
\mathbf{w}_q &= u_{q1}(\boldsymbol{x})\mathbf{s}_1(\boldsymbol{x}) + \cdots + u_{q(p-q)}(\boldsymbol{x})\mathbf{s}_{p-q}(\boldsymbol{x}),
\end{aligned}$$

for some Laurent polynomials u_{ij}, $1 \le i \le q$, $1 \le j \le p-q$. Therefore,

$$\mathbf{B}-\mathbf{B}_{part} = \begin{pmatrix} u_{11}(\boldsymbol{x}) & \dots & u_{1(p-q)}(\boldsymbol{x}) \\ \vdots & & \vdots \\ u_{q1}(\boldsymbol{x}) & \dots & u_{q(p-q)}(\boldsymbol{x}) \end{pmatrix} \begin{pmatrix} \mathbf{s}_1(\boldsymbol{x}) \\ \vdots \\ \mathbf{s}_{p-q}(\boldsymbol{x}) \end{pmatrix},$$

where each $\mathbf{s}_i(\boldsymbol{x})$ is regarded as a p-dimensional row vector. Therefore the general solution to Eq. 10.2 can be expressed in terms of $(p-q)q$ free parameters:

$$\mathbf{B} = \mathbf{B}_{part} + \begin{pmatrix} u_{11}(\boldsymbol{x}) & \dots & u_{1(p-q)}(\boldsymbol{x}) \\ \vdots & & \vdots \\ u_{q1}(\boldsymbol{x}) & \dots & u_{q(p-q)}(\boldsymbol{x}) \end{pmatrix} \begin{pmatrix} \mathbf{s}_1(\boldsymbol{x}) \\ \vdots \\ \mathbf{s}_{p-q}(\boldsymbol{x}) \end{pmatrix}.$$

Note that this is a **minimal** complete parametrization in the sense that any complete parametrization of the left inverses of $\mathbf{A}$ always involve at least $(p-q)q$ free parameters.

10.4 Unimodular Completion and Parametrization of Filter Banks

Since our Unimodular Completion Algorithm developed in Chapter 3 already contains a syzygy computation as its central ingredient, it's natural to ask if one could obtain the parametrization outlined in the previous section from the Unimodular Completion Algorithm. It turns out that this is indeed the case.

Suppose $\mathbf{A} \in \mathrm{M}_{pq}(k[\boldsymbol{x}^{\pm 1}])$ is unimodular and $\bar{\mathbf{A}} \in \mathrm{GL}_p(k[\boldsymbol{x}^{\pm 1}])$ is a unimodular completion of $\mathbf{A}$. If $\mathbf{S} \in \mathrm{M}_{qp}(k[\boldsymbol{x}^{\pm 1}])$ is an arbitrary left inverse of $\mathbf{A}$, then

$$\begin{aligned}
\mathbf{SA} = \mathbf{I}_q &\implies \mathbf{S}\bar{\mathbf{A}} = (\mathbf{I}_q, \mathbf{u}_1, \ldots, \mathbf{u}_{p-q}) \\
&\implies \mathbf{S} = (\mathbf{I}_q, \mathbf{u}_1, \ldots, \mathbf{u}_{p-q})\bar{\mathbf{A}}^{-1}
\end{aligned}$$

for some $\mathbf{u}_1, \ldots, \mathbf{u}_{p-q} \in (k[\boldsymbol{x}^{\pm 1}])^q$.

Now regarding $\mathbf{u}_1, \ldots, \mathbf{u}_{p-q}$ as free vector parameters ranging over $(k[\boldsymbol{x}^{\pm 1}])^q$, we get a complete parametrization involving $q \times (p-q)$ free parameters. More explicitly,

$$\begin{aligned}
\mathbf{S} &= (\mathbf{I}_q, \mathbf{u}_1, \ldots, \mathbf{u}_{p-q})\bar{\mathbf{A}}^{-1} && (10.3)\\
&= \begin{pmatrix} 1 & 0 & \cdots & 0 & u_{11} & \cdots & u_{1(p-q)} \\ 0 & 1 & \cdots & 0 & u_{21} & \cdots & u_{2(p-q)} \\ \vdots & \ddots & \vdots & \vdots & & \vdots & \\ 0 & 0 & \cdots & 1 & u_{q1} & \cdots & u_{q(p-q)} \end{pmatrix} \bar{\mathbf{A}}^{-1}. && (10.4)
\end{aligned}$$

Note that any complete parametrization involving $q \times (p-q)$ parameters gives a syzygy basis since the degree of freedom associated to finding the left inverses of a $p \times q$ unimodular matrix is precisely $q \times (p-q)$. Therefore the above parametrization obtained from the Unimodular Completion Algorithm is a **complete** and **canonical** parametrization.

Example 10.4.1 Define four polynomials in $\mathbb{C}[x^{\pm 1}, y^{\pm 1}, z^{\pm 1}]$ by

$$\begin{aligned}
f_1 &= 1 - x\,y - 2\,z - 4\,x\,z - x^2\,z - 2\,x\,y\,z + 2\,x^2\,y^2\,z - 2\,x\,z^2 - 2\,x^2\,z^2 + 2\,x^2\,y\,z^2 \\
f_2 &= 2 + 4\,x + x^2 + 2\,x\,y - 2\,x^2\,y^2 + 2\,x\,z + 2\,x^2\,z - 2\,x^2\,y\,z \\
f_3 &= 1 + 2\,x + x\,y - x^2\,y^2 + x\,z + x^2\,z - x^2\,y\,z \\
f_4 &= 2 + x + y - x\,y^2 + z - x\,y\,z.
\end{aligned}$$

Find a complete parametrization for all the left inverses of the 4×1 matrix $\mathbf{A} := \begin{pmatrix} f_1 \\ f_2 \\ f_3 \\ f_4 \end{pmatrix}$.

The unimodularity of the matrix $\mathbf{A}$ was shown in the Example 3.3.1, and an explicit unimodular completion $\bar{\mathbf{A}}$ of $\mathbf{A}$ was also constructed there:

$$\bar{\mathbf{A}} = \begin{pmatrix} f_1 & -y - xz + 2xy^2z - 2xz^2 + 2xyz^2 & 1 - 2xyz - 2xz^2 & z - 2z^2 \\ f_2 & x - 2xy^2 + 2xz - 2xyz & 2xy + 2xz & -1 + 2z \\ f_3 & -(xy^2) + xz - xyz & xy + xz & -1 + z \\ f_4 & 1 - y^2 - yz & y + z & 0 \end{pmatrix}.$$

Therefore, an arbitrary left inverse $\mathbf{S}$ of $\mathbf{A}$ is of the form

$$\mathbf{S} = (1, u_1, u_2, u_3)\bar{\mathbf{A}}^{-1}$$

$$
\begin{aligned}
&= (1, u_1, u_2, u_3) \begin{pmatrix} 0 & -z+1 & 2z-1 & -x \\ -y-z & xz-yz-z^2-x+2z-2 & -2xz+x-4z+2 & x^2+2x+1 \\ -y^2-yz+1 & -y^2z-yz^2+2yz-2y+2z-1 & -4yz+2y-2z+1 & 2xy+x+y \\ xy+xz & xyz+xz^2-2xz+2x+1 & 4xz-2x-2 & -2x^2-x \end{pmatrix} \\
&= (0, -z+1, 2z-1, -x) \\
&\quad +u_1(-y-z, xz-yz-z^2-x+2z-2, -2xz+x-4z+2, x^2+2x+1) \\
&\quad +u_2(-y^2-yz+1, -y^2z-yz^2+2yz-2y+2z-1, -4yz+2y-2z+1, 2xy+x+y) \\
&\quad +u_3(xy+xz, xyz+xz^2-2xz+2x+1, 4xz-2x-2, -2x^2-x).
\end{aligned}
$$

Note here how unimodular completion is closely related to syzygy basis. □

10.5 Gröbner Bases and Multidimensional Filter Banks

We now consider the first question: We can check whether or not a given MD low-pass $G(\boldsymbol{z})$ can act as an analysis filter in a 2-channel filter bank by decomposing $G(\boldsymbol{z})$ into polyphase components, and checking the unimodularity of the resulting polyphase matrix by combining the algorithm **LaurentToPoly** and a Gröbner basis computation. Moreover, if the answer is yes, we explicitly find a particular low-pass synthesis filter $H_{part}(\boldsymbol{z})$ by tracing the steps in the Gröbner basis computation. We also derive a complete parametrization of the synthesis filters by the syzygy basis computation outlined in the previous section.

Example 10.5.1 Consider the filter $G(z_1, z_2)$ with impulse response

$$
\frac{1}{4096}\begin{pmatrix} 0 & 0 & 0 & 8 & 0 & 0 & 0 \\ 0 & 0 & 24 & -96 & 24 & 0 & 0 \\ 0 & 24 & -192 & 456 & -192 & 24 & 0 \\ 8 & -96 & 456 & 3200 & 456 & -96 & 8 \\ 0 & 24 & -192 & 456 & -192 & 24 & 0 \\ 0 & 0 & 24 & -96 & 24 & 0 & 0 \\ 0 & 0 & 0 & 8 & 0 & 0 & 0 \end{pmatrix}.
$$

The filter $G(z_1, z_2)$ is designed to have a diamond-shaped low-pass frequency response. It is flat of order 2 at DC, and vanishing at the aliasing frequencies of the quincunx sampling lattice (see Fig. 10.1). These properties make it a likely candidate for the low-pass analysis filter of a 2-channel, PR filter bank (downsampling on the quincunx lattice). Applying the Gröbner bases computation, we indeed find that this is the case, and the filter

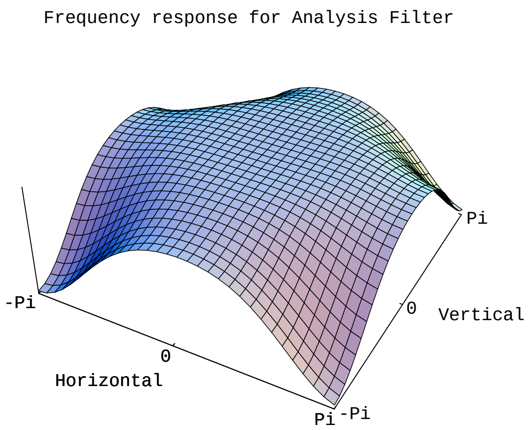

Figure 10.1: The frequency response of $G(z_1, z_2)$.

$H_{part}(z_1, z_2)$ with impulse response

$$\frac{1}{3585}\begin{pmatrix} 0 & 0 & 48 & 0 & 0 \\ 0 & 96 & 576 & 96 & 0 \\ 48 & 576 & 4288 & 576 & 48 \\ 0 & 96 & 576 & 96 & 0 \\ 0 & 0 & 48 & 0 & 0 \end{pmatrix}$$

is found as a particular solution for the synthesis filter. By choosing appropriate values for the parameters in the parametrization outlined in the previous section, we can modify $H_{part}(z_1, z_2)$ in order to meet or approximate extra conditions. □

We will now consider the second question and show how Gröbner bases can be used in 2D sample rate conversion schemes.

Example 10.5.2 Consider the 2D sample rate conversion scheme which consists of vertical upsampling by a factor 3, filtering with a filter $H(\boldsymbol{z}) = H(z_1, z_2)$ and horizontal downsampling with a factor 2. We assume that H is FIR, and we would like to know if this scheme has an FIR inverse. To be more precise, we are looking for an FIR filter $G(\boldsymbol{z})$, such that horizontal upsampling by a factor 2, filtering with $G(\boldsymbol{z})$ and vertical downsampling with a factor 3, cancels the effect of the first sample rate conversion scheme.

Let the filter $H(\boldsymbol{z})$ be given by $H(\boldsymbol{z}) = \sum h_{i,j} z_1^i z_2^j$. Following the method outlined in Section 9.2, but now for this 2D case, we construct the 3×2 polynomial matrix $H_{k,l}(\boldsymbol{z}) = \sum h_{3i+k,2j+l} z_1^i z_2^j$, where $0 \leq k \leq 2$ and $0 \leq l \leq 1$.

Assume momentarily that $H(\boldsymbol{z})$ is a separable filter $H^h(z_1)H^v(z_2)$. It is easily seen that in this case the filters $H_{k,l}(\boldsymbol{z})$ are products of 1D polyphase components, i.e. $H_{k,l}(\boldsymbol{z}) = H_k^h(z_1)H_l^v(z_2)$. Consequently, all the maximal minors of $H_{k,l}(\boldsymbol{z})$ have determinants equal to 0. Therefore the 2D analogue of Eq. 9.2 cannot be satisfied, and inversion is impossible.

Now we consider a non-separable case, where the filter $H(\boldsymbol{z})$ is given by the 4×6 (horizontal $\times$ vertical) impulse response

$$\begin{pmatrix} 2 & 3 & 2 & 1 & 3 & 2 \\ 3 & 5 & 3 & 1 & 3 & 2 \\ 1 & 1 & 1 & 1 & 1 & 1 \\ 2 & 2 & 2 & 1 & 1 & 1 \end{pmatrix}.$$

The polyphase component matrix $\mathbf{H}_p = (H_{kl})$ of $H(\boldsymbol{z})$ is defined by

$$H(\boldsymbol{z}) \quad = \quad \sum_{k=0}^{2} \sum_{l=0}^{1} z_1^k z_2^l H_{kl}(z_1^2, z_2^3),$$

which is found as

$$\mathbf{H}_p = \begin{pmatrix} 2 + z_1 + z_2 + z_1 z_2 & 3 + 2z_1 + z_2 + z_1 z_2 \\ 3 + z_1 + 3z_2 + z_1 z_2 & 5 + 2z_1 + 3z_2 + z_1 z_2 \\ 2 + z_1 + 2z_2 + z_1 z_2 & 3 + 2z_1 + 2z_2 + z_1 z_2 \end{pmatrix}.$$

Computing the determinants of the maximal minors we find $D_0(\boldsymbol{z}) = -1 - z_2$, $D_1(\boldsymbol{z}) = -z_2 - z_1 z_2$ and $D_2(\boldsymbol{z}) = 1 - z_2 - z_1 z_2$. These determinants are proper multivariable expressions and the Euclidean algorithm will therefore not work. In this case one easily verifies that $D_2 - D_1 = 1$, and therefore $\mathbf{H}_p$ is unimodular and there exist an inverse FIR filter $G(\boldsymbol{z})$. To find $G(\boldsymbol{z})$ we first need to find a left inverse $\mathbf{G}_p$ to $\mathbf{H}_p$.

We apply the Unimodular Completion Algorithm developed in Chapter 3 to $\mathbf{H}_p$ now, and the following is the SINGULAR script we used. For notational convenience, we let $x := z_1$, $y := z_2$.

```
ring r=0,(x,y),(c,dp); option(redSB);
vector v(1)=[2+x+y+xy,3+2*x+y+xy];
vector v(2)=[3+x+3*y+xy,5+2*x+3*y+xy];
vector v(3)=[2+x+2*y+xy,3+2*x+2*y+xy];
module M=v(1),v(2),v(3);
module G=std(M); matrix T=lift(M,G); module S=syz(M);
```

The output from SINGULAR is as follows:

```
> G;
G[1]=[0,1]
G[2]=[1]

> T;
T[1,1]=0
T[1,2]=1
T[2,1]=x+2
T[2,2]=-2x-3
T[3,1]=-1x-3
T[3,2]=2x+4

> S;
S[1]=[y+1,-1xy-1y,xy+y-1]
```

Since $\{(1,0),(0,1)\}$ is a Gröbner basis of the row vectors of $\mathbf{A}$, $\mathbf{A}$ is unimodular, and the relation $\mathtt{G} = \mathtt{MT}$ translates to

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \mathbf{A}^t\mathtt{T}.$$

By taking transpose of bothe sides, we get $\mathtt{T}^t\mathbf{A} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, i.e.

$$\begin{pmatrix} 1 & -2x-3 & 2x+4 \\ 0 & x+2 & -x-3 \end{pmatrix} \mathbf{A} = \mathbf{I}_2.$$

Hence, $\mathbf{B} := \begin{pmatrix} 1 & -2z_1-3 & 2z_1+4 \\ 0 & z_1+2 & -z_1-3 \end{pmatrix}$ is a left inverse of $\mathbf{A}$, and

$$\begin{aligned} \mathbf{C} &= \begin{pmatrix} \mathbf{B} \\ \mathbf{S} \end{pmatrix} \\ &= \begin{pmatrix} 1 & -2z_1-3 & 2z_1+4 \\ 0 & z_1+2 & -z_1-3 \\ z_2+1 & -z_1z_2-z_2 & z_1z_2+z_2-1 \end{pmatrix}. \end{aligned}$$

The resulting unimodular completion of $\mathbf{A}$ is

$$\bar{\mathbf{A}} = \mathbf{C}^{-1}.$$

Now the most general form of $\mathbf{G}_p$ is given by the Formula 10.3:

$$
\begin{aligned}
\mathbf{G}_p &= \begin{pmatrix} 1 & 0 & u_1 \\ 0 & 1 & u_2 \end{pmatrix} \bar{\mathbf{A}}^{-1} \\
&= \begin{pmatrix} 1 & 0 & u_1 \\ 0 & 1 & u_2 \end{pmatrix} \mathbf{C} \\
&= \begin{pmatrix} 1 & 0 & u_1 \\ 0 & 1 & u_2 \end{pmatrix} \begin{pmatrix} 1 & -2z_1 - 3 & 2z_1 + 4 \\ 0 & z_1 + 2 & -z_1 - 3 \\ z_2 + 1 & -z_1 z_2 - z_2 & z_1 z_2 + z_2 - 1 \end{pmatrix} \\
&= \begin{pmatrix} 1 & -2z_1 - 3 & 2z_1 + 4 \\ 0 & z_1 + 2 & -z_1 - 3 \end{pmatrix} \\
&\quad + \begin{pmatrix} u_1(z_2 + 1) & u_1(-z_1 z_2 - z_2) & u_1(z_1 z_2 + z_2 - 1) \\ u_2(z_2 + 1) & u_2(-z_1 z_2 - z_2) & u_2(z_1 z_2 + z_2 - 1) \end{pmatrix}
\end{aligned} \tag{10.5}
$$

where u_1, u_2 are arbitrary Laurent polynomials.

Finally, the matrix $\mathbf{G}_p = (G_{kl})$ is related to the inverse filter $G(\boldsymbol{z})$ as the set of *backward* polyphase components. To be precise, $G(\boldsymbol{z})$ is given by $G(\boldsymbol{z}) = \sum z_1^k z_2^l G_{kl}(z_1^2, z_2^3)$. Working out these formulas one finds the following impulse response for the filter $G(\boldsymbol{z})$:

$$
\begin{pmatrix} -2 & 2 & -1 & -1 & 1 & -1 \\ 3 & -3 & 2 & 1 & -1 & 1 \\ -1 & 1 & 0 & -1 & 1 & 0 \\ 2 & -2 & 0 & 1 & -1 & 0 \end{pmatrix}.
$$

Again, one can change the values for u_1 and u_2 in the Eq. 10.5 to adjust to some specific needs. $\square$

Chapter 11

Ladder Decomposition of Multidimensional Perfect Reconstructing Filter Banks

11.1 Introduction

In Chapter 4, we obtained a realization algorithm that lets us write a given square unimodular polynomial matrix as a product of elementary polynomial matrices. As suggested in [THK95], such an algorithm has application in signal processing since it gives a way of expressing a given multidimensional biorthogonal filter bank as a cascade of simpler filter banks called elementary ladder steps.

Mathematically, representing a perfect reconstructing FIR filter bank as a cascade of elementary ladder steps is equivalent to expressing a unimodular Laurent polynomial matrix as a product of elementary matrices over Laurent polynomial ring. Since we already obtained a **Realization Algorithm** over polynomial rings and the algorithm **Laurent-ToPoly** for transforming a noncausal system to a causal system, we can readily develop a realization algorithm for an arbitrary unimodular Laurent polynomial matrix.

11.2 Elementary Column Property over Laurent polynomial rings

In Chapter 6, for any given $\mathbf{v} = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \in \mathrm{Um}_n(\mathbb{C}[\boldsymbol{x}^{\pm 1}])$, we found $\mathbf{E} \in \mathrm{E}_n(\mathbb{C}[\boldsymbol{x}^{\pm 1}])$ such that

$$\mathbf{E}\mathbf{v} = \mathbf{w} = \begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix} \in (S[x_1])^n.$$

And with the change of variables:

$$x_1 = y_1 \cdot (y_2 \cdots y_m)^l,\ x_2 = y_2,\ \ldots,\ x_m = y_m,$$

we showed that $\mathbf{w}$ is unimodular over the polynomial ring $\mathbb{C}[\boldsymbol{y}]$. Now we can apply the Elementary Column Property of Chapter 4 to $\mathbf{w}$, if $n \geq 3$, to reduce it to $\mathbf{e}_n$ using elementary operations. Since we used only elementary operations to reduce $\mathbf{v}$ to $\mathbf{w}$, by changing variables back to $\boldsymbol{x}$, we have reduced $\mathbf{v}$ to $\mathbf{e}_n$ by applying elementary operations. This proves the following Laurent analogue of the Elementary Column Property.

Theorem 11.2.1 *(Elementary Column Property for Laurent polynomial rings) The group* $\mathrm{E}_n(\mathbb{C}[\boldsymbol{x}^{\pm 1}])$ *acts transitively on the set* $\mathrm{Um}_n(\mathbb{C}[\boldsymbol{x}^{\pm 1}])$ *when* $n \geq 3$.

11.3 Realization Algorithm over Laurent Polynomial Rings

Now, the desired realization algorithm for $\mathrm{SL}_n(\mathbb{C}[\boldsymbol{x}^{\pm 1}])$, $n \geq 3$, proceeds as follows:

- **Step 1:** Use the Elementary Column Property provided by Theorem 11.2.1 to reduce the problem of obtaining a general realization algorithm over the Laurent polynomial ring $\mathbb{C}[\boldsymbol{x}^{\pm 1}]$ to the problem of finding a realization algorithm for the matrices of the following special form:

$$\begin{pmatrix} p & q & 0 \\ r & s & 0 \\ 0 & 0 & 1 \end{pmatrix} \in \mathrm{SL}_3(\mathbb{C}[\boldsymbol{x}^{\pm 1}]).$$

That is, for a given unimodular matrix $\mathbf{A} \in \mathrm{SL}_n(\mathbb{C}[\boldsymbol{x}^{\pm 1}])$, find elementary matrices $\mathbf{E}_1, \ldots, \mathbf{E}_l$ such that

$$\mathbf{E}_l \cdots \mathbf{E}_1 \mathbf{A} \;=\; \begin{pmatrix} p & q & \mathbf{0} \\ r & s & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{I}_{n-2} \end{pmatrix}.$$

- **Step 2:** Since $\begin{pmatrix} p \\ r \end{pmatrix}$ is a unimodular column vector over $\mathbb{C}[\boldsymbol{x}^{\pm 1}]$, by following the procedure outlined in the previous section, we can assume that $\begin{pmatrix} p \\ r \end{pmatrix}$ is a unimodular column vector over the polynomial ring $\mathbb{C}[\boldsymbol{x}]$, $p \equiv 1 \pmod{x_1 \cdots x_m}$ and $r \equiv 0 \pmod{x_1 \cdots x_m}$.

- **Step 3:** Now, consider the unimodular row vector (p, q) over $S[x_1^{\pm 1}]$ with the coefficient ring S being $\mathbb{C}[x_2^{\pm 1}, \ldots, x_m^{\pm 1}]$. Since p is a polynomial in $S[x_1]$ and its constant term is 1, by adding a suitable multiple of p to q and by noting that this elementary column operation does not change r, we can assume that q is a polynomial in $S[x_1]$ and its constant term is zero. Then the condition, $\begin{vmatrix} p & q \\ r & s \end{vmatrix} = 1$, forces s to be also a polynomial in $S[x_1]$ whose constant term is 1. Now, using the new variables $y_1, \ldots, y_m$ defined by $x_1 = y_1 \cdot (y_2 \cdots y_m)^l$, $x_2 = y_2, \ldots, x_m = y_m$ for a sufficiently large $l \in \mathbb{N}$, we see that
$$\begin{pmatrix} p & q & 0 \\ r & s & 0 \\ 0 & 0 & 1 \end{pmatrix} \in \mathrm{SL}_3(\mathbb{C}[\boldsymbol{y}]).$$

- **Step 4:** Use the Realization Algorithm over polynomial rings developed in the chapter 4 to write $\begin{pmatrix} p & q & 0 \\ r & s & 0 \\ 0 & 0 & 1 \end{pmatrix} \in \mathrm{SL}_3(\mathbb{C}[\boldsymbol{y}])$ as a product of elementary matrices over $\mathbb{C}[\boldsymbol{y}]$ and then change the variables back to $x_1, \ldots, x_m$.

Bibliography

[ABS64] M. Atiyah, R. Bott, and A. Shapiro. Clifford modules. *Topology*, 3:3–38, 1964.

[Bak81] A. Bak. *K-theory of forms*. Number 98, Annals of Mathematical Studies. Princeton University Press, 1981.

[Bas73] H. Bass. *Unitary algebraic K-theory in Algebraic K-theory III. Hermitian K-theory and geometric applications*, pages 57–265. volume 343, Lecture Notes in Mathematics. Springer-Verlag, 1973.

[Bay82] D. Bayer. *The Division Algorithm and the Hilbert Scheme*. PhD thesis, Harvard University, 1982.

[BC94] S. Basu and H. M. Choi. Multidimensional causal, stable, perfect reconstruction filter banks. *Proceedings of the ICIP-94*, 1:805–809, Nov. 1994.

[BCC94] S. Basu, H. Choi, and C. Chiang. On non-separable multidimensional perfect reconstruction filter banks. *Preprint*, 1994.

[BS] D. Bayer and M. Stillman. *Macaulay: a computer algebra system for algebraic geometry.* available by anonymous ftp from ftp.math.harvard.edu.

[BS87a] D. Bayer and M. Stillman. A criterion for detecting m-regularity. *Invent. Math.*, 87:1–11, 1987.

[BS87b] D. Bayer and M. Stillman. A theorem on redefining division orders by the reverse lexicographic orders. *Duke J. of Math.*, 55:321–328, 1987.

[Buc65] B. Buchberger. *Ein Algorithmus zum Auffinden der Basis Elemente des Restklassenringes nach einem nulldimensionalen Polynomideal.* PhD thesis, University of Innsbruck, Austria, 1965.

[Buc85] B. Buchberger. Gröbner bases – an algorithmic method in polynomial ideal theory. In N. K. Bose, editor, *Multidimensional systems theory*, chapter 6, pages 184–232. Dordrecht: D. Reidel, 1985.

[BW93] T. Becker and V. Weispfenning. *Gröbner Bases*, volume 141, Graduate Texts in Mathematics. Springer-Verlag, 1993.

[CLO92] D. Cox, J. Little, and D. O'Shea. *Ideals, Varieties, and Algorithms.* Undergraduate Texts in Mathematics. Springer-Verlag, 1992.

[Coh66] P. M. Cohn. On the structure of the GL_2 of a ring. *Inst. Hautes Études Sci. Publ. Math.*, 30:365–413, 1966.

[CV93] T. Chen and P. Vaidyanathan. Recent Developments in Multidimensional Multirate Systems. *IEEE Transactions on Circuits and Systems for Video Technology*, 3:116–137, April 1993.

[Eis95] D. Eisenbud. *Introduction to Commutative Algebra with a View Towards Algebraic Geometry.* volume 150, Graduate Texts in Mathematics. Springer-Verlag, 1995.

[FG90] N. Fitchas and A. Galligo. Nullstellensatz effectif et Conjecture de Serre (Théorème de Quillen-Suslin) pour le Calcule Formel. *Math. Nachr*, 149:232–253, 1990.

[Fit93] N. Fitchas. Algorithmic aspects of Suslin's proof of Serre's conjecture. *Comput Complexity*, 3:31–55, 1993.

[Ful93] W. Fulton. *Introduction to toric varieties.* Number 131, Annals of Mathematics Studies. Princeton University Press, 1993.

[Gan77] F. R. Gantmacher. *The theory of matrices.* Chelsea Publishing Company, New York, 1977.

[GKZ94] I.M. Gelfand, M.M. Kapranov, and A.V. Zelevinsky. *Discriminants, Resultants and Multidimensional Determinants.* Mathematics: Theory & Applications. Birkhäuser, 1994.

[GM80] S. K. Gupta and M. P. Murthy. *Suslin's work on linear groups over polynomial rings and Serre problem.* Number 8, Indian Statistical Institute Lecture Notes Series. MacMillan, New Delhi, 1980.

[GPS95] G. Greuel, G. Pfister, and H. Schoenemann. *Singular User Manual.* University of Kaiserslautern, version 0.90 edition, 1995. available by anonymous ftp from helios.mathematik.uni-kl.de.

[Har77] R. Hartshorne. *Algebraic Geometry*, volume 52, Graduate Texts in Mathematics. Springer-Verlag, 1977.

[Hir64] H. Hironaka. Resolution of singularities of an algebraic variety over a field of characteristic 0. *Ann. of Math.*, 79:109–326, 1964.

[HO89] A. Hahn and O.T.O'Meara. *The classical groups and K-theory.* volume 291, Grundlehren der mathematischen Wissenschaften. Springer-Verlag, 1989.

[HP94] M. Holschneider and U. Pinkall. Quadrature Mirror Filters and Loop Groups. Preprint, 1994.

[Knu91] M. A. Knus. *Quadratic and Hermitian Forms over Rings.* volume 294, Grundlehren der mathematischen Wissenschaften. Springer-Verlag, 1991.

[KPV95] T. Kalker, H. Park, and M. Vetterli. Groebner Basis Techniques in Multidimensional Multirate Systems. *Proceedings of ICASSP 95 (International Conference on Accoustics, Speech, and Signal Processing)*, 1995.

[Lam78] T. Y. Lam. *Serre's Conjecture*, volume 635, Lecture Notes in Mathematics. Springer-Verlag, 1978.

[LS92] A. Logar and B. Sturmfels. Algorithms for the Quillen-Suslin theorem. *J. Algebra*, 145:231–239, 1992.

[LV90] V.C. Liu and P.P. Vaidyanathan. On factorization of a subclass of 2-D digital FIR lossless matrices for 2-D QMF bank applications. *IEEE Trans. Cir. Syst.*, 37:852–854, June 1990.

[Mil71] J. Milnor. *Introduction to Algebraic K-Theory.* Number 72, Annals of Mathematics Studies. Princeton University Press, 1971.

[Mis93] B. Mishra. *Algorithmic Algebra.* Texts and Monographs in Computer Science. Springer-Verlag, 1993.

[PS91] A. Pressley and G. Segal. *Loop Groups.* Oxford Mathematical Monographs. Oxford University Press, 1991.

[PS93] P. Pedersen and B. Sturmfels. Product formulas for resultants and Chow form. *Mathematische Zeitschrift*, 145:377–396, 1993.

[PW94] H. Park and C. Woodburn. An Algorithmic Proof of Suslin's Stability Theorem for Polynomial Rings. *To appear in Journal of Algebra*, 1995.

[Qui76] D. Quillen. Projective modules over polynomial rings. *Invent. Math*, 36:167–171, 1976.

[Roj94] M. Rojas. A convex geometric approach to counting the roots of a polynomial system. *Theoretical Computer Science*, November 1994.

[Ser55] J. P. Serre. Faisceaux algébriques cohérents. *Ann. Math.*, 61:191–274, 1955.

[Stu91] B. Sturmfels. Sparse elimination theory. In *Computational Algebraic Geometry and Commutative Algebra.* Cambridge University Press, June 1991.

[Stu93] B. Sturmfels. *Algorithms in Invariant Theory.* Springer-Verlag, 1993.

[Stu94] B. Sturmfels. Gröbner Bases and Convex Polytopes. Lecture notes presented at the Holiday Symposium at New Mexico State University, Las Cruces, December 1994.

[Sus76] A. A. Suslin. Projective modules over a polynomial ring are free. *Soviet Math. Dokl.*, 17:1160–1164, 1976.

[Sus77] A. A. Suslin. On the structure of the special linear group over polynomial rings. *Math. USSR Izv.*, 11:221–238, 1977.

[Swa78] R. G. Swan. Projective Modules over Laurent polynomial rings. *Trans. Am. Math. Soc.*, 237:111–120, 1978.

[THK95] L. Tolhuizen, H. Hollmann, and A. Kalker. On the realizability of Bi-orthogonal M-dimensional 2-band Filter Banks. *IEEE Transactions on Signal processing*, March 1995.

[Vai93] P. P. Vaidyanathan. *Multirate Systems and Filter Banks.* Prentice Hall Signal Processing Series. Prentice Hall, 1993.

[Vas81] L.N. Vaserstein. On the normal subgroups of GL_n over a ring. In E.M. Friedlander and M.R. Stein, editors, *Algebraic K-theory*, volume 854, Lecture Notes in Mathematics, pages 456–465. Springer-Verlag, 1981.

[VD89] P.P. Vaidyanathan and Z. Dognŏgnata. The Role of Lossless Systems in Modern Digital Signal Processing. A tutorial. *Special issue on Circuits and Systems. IEEE Transactions on Education*, 32(3):181–197, August 1989.

[VH92] M. Vetterli and C. Herley. Wavelets and Filter Banks: theory and design. *IEEE Transactions on Signal Processing*, 40:2207–2232, Sept 1992.

[VK95] M. Vetterli and J. Kovačević. *Wavelets and Subband Coding.* Prentice Hall Signal Processing Series. Prentice Hall, 1995.

[VL94] S. Venkataraman and B. Levy. State Space Representations of 2-D FIR Lossless Transfer Matrices. *IEEE Transactions on Circuits and Systems-II: Analog and Digital Signal Processing*, 41(2):117–132, Feb 1994.

[Wol88] S. Wolfram. *Mathematica: A System for doing Mathematics by Computer.* Addison-Wesley, Reading, MA, 1988.

[Woo94] C. Woodburn. *An Algorithm for Suslin's Stability Theorem.* PhD thesis, New Mexico State University, 1994.

[You61] D. Youla. On the factorization of rational matrices. *IRE Trans. on IT*, 7(7):172–189, 1961.

[YP84] D. C. Youla and P. F. Pickel. The Quillen-Suslin Theorem and the structure of n-dimensional elementary polynomial matrices. *IEEE Trans. Circuits and Systems*, CAS-31(6):513–518, June 1984.

[Zie95] G. Ziegler. *Lectures on Polytopes*, volume 152, Graduate Texts in Mathematics. Springer-Verlag, 1995.