An Algebraic View of Multidimensional Multiple-Input Multiple-Output Finite Impulse Response Equalizers

DISSERTATION

Presented in Partial Fulfillment of the Requirements for the Degree Doctor of Philosophy in the Graduate School of The Ohio State University

By

Ravikiran Rajagopal, B.E., M.S.

* * * * *

The Ohio State University

2003

Dissertation Committee:

Lee C. Potter, Adviser
Jose Cruz
Bostwick F. Wyman
Andras Nemethi

Approved by

Adviser
Department of Electrical Engineering
© Copyright by

Ravikiran Rajagopal

2003
ABSTRACT

The problem of computing equalizers for multidimensional multiple-input multiple-output (MIMO) finite impulse response (FIR) filters using MIMO FIR filters is considered. Prior results are reviewed establishing conditions for the equalizability of a given MIMO FIR filter and of a generic MIMO FIR filter. Algorithms for the computation of MIMO FIR equalizers are derived and their relative strengths and weaknesses are discussed. A parametrization of the set of all equalizers for a given MIMO FIR filter is derived. Known bounds on the orders of the equalizer are doubly exponential in the order of the given MIMO FIR filter; alternative generic bounds are derived which are linear in the order of the given MIMO FIR filter, and the behavior of the bound for large number of outputs is characterized. A fast algorithm (generalizing the Levinson algorithm to the multidimensional case) is proposed for multidimensional Wiener filtering and for computing equalizers for single-input multiple-output (SIMO) systems. A minimal set of test targets is established for polarimetric calibration of ultra-wide band synthetic aperture radar systems, and equalizer orders for multiple antenna systems are computed. A brief overview of the applicability of the results to blind equalization problems is provided.
ACKNOWLEDGMENTS

I would like to thank my advisor, Prof. Lee Potter, for his guidance, and for encouraging me to work on topics that interested me. I am grateful to the members of the Information Processing systems laboratory for the stimulating research atmosphere.

I learnt the mathematical method from Profs. Paul Nevai and Jeffery McNeal. Profs. Mityagin, Wyman, Rosenthal and Nemethi pointed me to various techniques in algebraic geometry, which provide the bulk of the proofs in this dissertation. My understanding of the theory of orthogonal polynomials on the unit circle benefited immensely from reading an unpublished textbook of Prof. Simon.

Without the influence of the dance people at Ohio State (Laura Stonerock, Svetlana Iskhakov, Kathryn Iammarino, Neil Coplin, Aleksander Daskalov and Lonelle Yoder) and of the KDE development team, this dissertation might have been finished much earlier but it would not have been as much fun.
VITA

April 26, 1976 .................................. Born - Coimbatore, India

1997 ............................................. B.E.
Electronics & Communication Engineering
University of Madras, India

1997-8 ........................................... Graduate Fellow,
Ohio State University

2000 ............................................. M.S.
Electrical Engineering
Ohio State University

2002 ............................................. M.S.
Mathematics
Ohio State University

1998-2002 ..................................... Graduate Research Associate,
Ohio State University

2003-present ................................... DAGSI Fellow,
Ohio State University

PUBLICATIONS

Research Publications


R. Rajagopal, “Exact FIR Inverses of FIR Filters” M.S. Thesis, 2000, Ohio State University


**FIELDS OF STUDY**

Major Field: Electrical Engineering

Studies in:

- Signal processing: Prof. Lee Potter
- Real analysis: Prof. Paul Nevai
- Complex analysis: Prof. Jeffery McNeal
- Algebra: Prof. Joseph Ferrar
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Abstract</td>
<td>ii</td>
</tr>
<tr>
<td>Acknowledgments</td>
<td>iii</td>
</tr>
<tr>
<td>Vita</td>
<td>iv</td>
</tr>
<tr>
<td>List of Figures</td>
<td>ix</td>
</tr>
<tr>
<td><strong>I Background</strong></td>
<td></td>
</tr>
<tr>
<td>1. Introduction</td>
<td>2</td>
</tr>
<tr>
<td>1.1 Background</td>
<td>2</td>
</tr>
<tr>
<td>1.2 Literature Survey</td>
<td>5</td>
</tr>
<tr>
<td>1.3 Organization and Contributions</td>
<td>8</td>
</tr>
<tr>
<td>2. Algebra</td>
<td>10</td>
</tr>
<tr>
<td>2.1 Definitions</td>
<td>10</td>
</tr>
<tr>
<td>2.2 Multi-indices</td>
<td>12</td>
</tr>
<tr>
<td>2.3 Ideals and Varieties</td>
<td>13</td>
</tr>
<tr>
<td>2.4 Algorithms</td>
<td>14</td>
</tr>
<tr>
<td>2.4.1 Univariate polynomials</td>
<td>14</td>
</tr>
<tr>
<td>2.4.2 Multivariate polynomials</td>
<td>14</td>
</tr>
<tr>
<td>2.4.3 Gröbner bases</td>
<td>15</td>
</tr>
<tr>
<td>2.5 The Nullstellensatz</td>
<td>16</td>
</tr>
<tr>
<td>3. MIMO Inverses</td>
<td>17</td>
</tr>
<tr>
<td>3.1 Problem Statement</td>
<td>17</td>
</tr>
</tbody>
</table>

vi
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1.1</td>
<td>Notation</td>
<td>17</td>
</tr>
<tr>
<td>3.1.2</td>
<td>System model</td>
<td>18</td>
</tr>
<tr>
<td>3.2</td>
<td>Existence of Polynomial Inverse</td>
<td>19</td>
</tr>
<tr>
<td>3.2.1</td>
<td>Inverse</td>
<td>19</td>
</tr>
<tr>
<td>3.2.2</td>
<td>Special cases</td>
<td>21</td>
</tr>
<tr>
<td>3.3</td>
<td>Random Systems</td>
<td>22</td>
</tr>
<tr>
<td>3.4</td>
<td>Filter Orders</td>
<td>25</td>
</tr>
<tr>
<td>II</td>
<td>Signal Processing</td>
<td>28</td>
</tr>
<tr>
<td>4</td>
<td>Equalizer Computation</td>
<td>29</td>
</tr>
<tr>
<td>4.1</td>
<td>Linear Algebra for Computation</td>
<td>29</td>
</tr>
<tr>
<td>4.2</td>
<td>Algebra for Computation</td>
<td>31</td>
</tr>
<tr>
<td>4.3</td>
<td>Example: Radar Calibration</td>
<td>34</td>
</tr>
<tr>
<td>4.4</td>
<td>Gröbner Bases of Modules</td>
<td>36</td>
</tr>
<tr>
<td>5</td>
<td>Class of Equalizers</td>
<td>38</td>
</tr>
<tr>
<td>5.1</td>
<td>Existence of Basis</td>
<td>38</td>
</tr>
<tr>
<td>5.2</td>
<td>Characterization of Inverses</td>
<td>40</td>
</tr>
<tr>
<td>6</td>
<td>Generic Orders</td>
<td>42</td>
</tr>
<tr>
<td>6.1</td>
<td>Motivation</td>
<td>42</td>
</tr>
<tr>
<td>6.2</td>
<td>Generic Orders of Equalizers</td>
<td>43</td>
</tr>
<tr>
<td>6.3</td>
<td>The Operator $T_{\delta,\alpha}^n(.)$</td>
<td>45</td>
</tr>
<tr>
<td>6.4</td>
<td>A Generic Effective Nullstellensatz</td>
<td>46</td>
</tr>
<tr>
<td>6.5</td>
<td>A Partial Converse of the Generic Effective Nullstellensatz</td>
<td>51</td>
</tr>
<tr>
<td>6.6</td>
<td>A Generic Effective Nullstellensatz for Matrices</td>
<td>56</td>
</tr>
<tr>
<td>7</td>
<td>Multivariate Szegő-Levinson algorithm</td>
<td>59</td>
</tr>
<tr>
<td>7.1</td>
<td>Preliminaries</td>
<td>60</td>
</tr>
<tr>
<td>7.2</td>
<td>Multivariate Szegő Recursion</td>
<td>63</td>
</tr>
<tr>
<td>7.3</td>
<td>Computation of Inverse</td>
<td>68</td>
</tr>
<tr>
<td>7.4</td>
<td>Equalizer Computation</td>
<td>70</td>
</tr>
<tr>
<td>III</td>
<td>Applications &amp; Examples</td>
<td>72</td>
</tr>
<tr>
<td>8</td>
<td>SAR calibration</td>
<td>73</td>
</tr>
</tbody>
</table>
8.1 SAR System Model .................................................. 73
8.2 Calibration Target Selection ................................. 75

9. Equalizer Orders ..................................................... 77
  9.1 Total Degree Versus Multidegree ......................... 77
  9.2 Tight Bounds ..................................................... 81
    9.2.1 One-dimensional signals ............................... 82
    9.2.2 \(n\)-dimensional signals ........................... 83
  9.3 Delays and Equalization .................................... 84
  9.4 Examples ....................................................... 85
    9.4.1 Generic versus absolute bounds .................... 85
    9.4.2 Filter versus equalizer orders ...................... 86

IV Appendices ......................................................... 87
A. Unsolved Problems ............................................. 88
   A.1 Signal Subspace Estimation Based on Rank .......... 88
   A.2 Multivariate Orthogonal Polynomials ................. 91
B. Notation .......................................................... 93
# LIST OF FIGURES

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1</td>
<td>MIMO FIR Equalization</td>
<td>4</td>
</tr>
<tr>
<td>8.1</td>
<td>SAR forward system model ($N = 3$ inputs, $M = 4$ outputs, images: $n = 2$)</td>
<td>76</td>
</tr>
<tr>
<td>9.1</td>
<td>Total degree versus multidegree</td>
<td>78</td>
</tr>
</tbody>
</table>
VOLUME I

Background
CHAPTER 1

INTRODUCTION

1.1 Background

Constrained inverse problems arise naturally in practice. In simple terms, a data collection procedure is analogous to viewing the actual scene through an observation window which tends to distort, modify and hide portions of the object under study. The objective is to resolve the true scene from the observed data and the a priori knowledge of the scene. Following a system theory formulation, a data collection experiment can be cast as a transformation of an input signal by a measurement scheme into the observed data. The input signal abstractly represents the event under investigation. The process of collecting data is usually modeled as an operator in an appropriate space.

In signal processing, numerous estimation and design problems can be formulated as inverse problems accompanied by the prior knowledge of the properties which any solution should satisfy. For instance:

- *Channel Equalization.* In wireless communications, signals sent from one station to another using multiple transmit or receive antennas pass through
quantitatively different channels which distort the signal. The estimation of channels is typically followed by the equalization of the channel distortion before demodulation of the message. The channel is constrained in space and hence the propagation time of the signal is finite. Therefore each transmitted signal is “spread” inside a time window of finite length \[55\].

• Polarimetric Radar. In polarimetric synthetic aperture radar imaging, signals are transmitted and received in two polarizations. The objective is to construct a reflectivity profile of the target for each transmitter-receiver pair. However, the nonideal nature of the antenna used, systematic errors such as cable delays, and errors in the imaging system redistribute energy among the transmitter-receiver pairs \([21, 64]\). However, the physics of the data collection and imaging imply that the energy in any pixel is smeared only over a finite neighborhood.

• Space Object Recognition. The objective is to estimate the three dimensional orientation of a satellite and its subcomponents by analyzing images obtained from ground-based surveillance systems \([3, 19]\). Multiple images of the same object are obtained over time and contain essentially the same information because the object is approximately stationary. The images are observed through a distorting medium (the atmosphere) whose characteristics are different for each observation. Again, the physics of the data collection implies that the energy in any pixel is smeared only over a finite neighborhood.

The preceding examples can be modeled as multiple-input multiple-output (MIMO) finite impulse response (FIR) filters in multiple dimensions (one for time, two for images, etc.). The topic of this dissertation is the construction of exact (zero-forcing)
MIMO FIR equalizers. Figure 1.1 provides a schematic representation of equalization with MIMO FIR filters. The objective is to recover the inputs exactly from the observed outputs and the knowledge of the forward (distortion) system. Several questions arise immediately:

1. Given the distorting MIMO FIR filter $H$, does there exist a MIMO FIR equalizer $G$?

2. If $G$ exists, is it unique?

3. If $G$ is not unique, can we characterize the class of all equalizers?

4. What is the minimum order (size) of an equalizer?

5. Are there fast algorithms for computing an equalizer?

6. Given only partial knowledge of $H$, what minimal set of test inputs to $H$ would provide us with sufficient information to design $G$?

For the single-input multiple-output (SIMO) case, the forward filter is invertible by a FIR filter if the channels do not share a common zero. This familiar concept generalizes, for multiple inputs, to the requirement that all minors of the matrix $H$
are coprime [6, 24, 45]. It can be shown in a straightforward manner [46] that the equalizer is not unique except in rare special cases. We answer questions (3)-(6) in this dissertation.

In the examples above, the distortion systems are not known \textit{a priori} and must be estimated. One of the ultimate goals of developing the theory of MIMO FIR equalizers is the estimation of multiple transmitted signals blindly from multiple received convolutional mixtures. We use the concept of \textit{genericity} to model events occurring almost surely and obtain results which answer the following additional questions:

7. What are the conditions required for generic invertibility of \( \mathcal{H} \)?

8. Given orders of \( \mathcal{H} \), what are the generic minimum orders of \( G \)?

We believe that the answers to questions (7)-(8) are part of the fundamental tools necessary to solve the blind deconvolution problem in the multivariate case.

### 1.2 Literature Survey

The inversion of a multivariate polynomial matrix is a classical problem problem in module theory [2]; the invertibility of a given multivariate polynomial matrix is known to be equivalent [11, chapter 3] to an associated projective module being free. The key result that characterizes such invertible matrices (also known as \textit{unimodular} matrices) is the celebrated Quillen-Suslin theorem; see [37] for a detailed discussion and a historical overview. Invertible univariate polynomial matrices have been extensively studied in the context of linear control systems [34]; however, much of the univariate theory (such as canonical representations) relies on the factorizability of univariate
polynomials and the fundamental theorem of algebra, neither of which hold in the multivariate case.

The connections between systems described by multivariate polynomial matrices and behavior theory were highlighted in [24]. Further relationships with symbolic dynamics, coding theory and automata theory were described in the review [53]. The relationships and the equivalences among the various theories are algebraic; analogous analytic results are hard to prove because (1) much of the theory applies to polynomial rings over arbitrary fields (see Chapter 2 for definitions) and (2) it is difficult to find analytic metrics (in the Hilbert space sense) which are tractable algebraically.

The necessary and sufficient conditions for the invertibility of a multivariate polynomial were found independently in [6, 24, 45]. For the case of single-input multiple-output (SIMO) systems, the matrix becomes a vector, and the solution reduces to the Nullstellensatz [10].

The concept of random systems was introduced in [29]; however, the underlying concept of genericity is well-known; see [11] for a historical overview. The conditions for the generic invertibility of a SIMO system can be derived using the theory of resultants [26]. We extend this result to the multiple-input case. The results of [29] were stated for generic univariate multichannel systems, and were extended to the case of restoration of images blurred by multiple FIR filters in [30, 31].

For the SIMO case, bounding the orders of the equalizer is the classical problem of finding the sharp effective Nullstellensatz which was solved in [35]. Bounding the orders of a generic system is a problem first considered in [29] for the case of univariate SIMO systems; the orders were found to be roughly inversely proportional to the number of outputs. Their results were implicitly used in [1, 58] in the context of
wireless channel equalization to estimate channel lengths. We extend the results to multivariate MIMO systems.

The advent of fast computers provided the impetus for the development of computational commutative algebra. Computing the inverse of a polynomial matrix can be shown to be equivalent (see Chapter 5) to computing the basis of certain free modules. Two families of algorithms are known: algorithms which use Gröbner basis techniques [40], and those which make use of commutative algebra [23]. Both families have huge computational complexity (doubly exponential in $\alpha_1 + \cdots + \alpha_n$, where $(\alpha_1, \ldots, \alpha_n)$ is the order of the forward filter); we present a Levinson-type algorithm in Chapter 7 which has much lower computational complexity (of order $\alpha_1^3 \cdot \cdots \cdot \alpha_{n-1}^3 \alpha_n^2$).

Algorithms for 2-D SIMO systems were considered in [30, 31]. Two classes of extensions to the Levinson algorithm can be found in the literature: block matrix extensions [4, 7, 36] and polynomial matrix extensions (see [15, 16] and the references therein). Both approaches can be viewed in the context of univariate Szegő polynomial theory - the block matrix approach emphasizes the forward predictor polynomials whereas the polynomial matrix approach emphasizes the reverse predictor polynomials. Neither approach makes (nor is designed to make) full use of the structure of nested Toeplitz matrices of nesting order greater than 1; the algorithm from [14] makes partial use of the structure when the nesting level is 2 using the so-called centrohermitian structure.

The equivalence of the Szegő polynomial recursion and the Levinson algorithm is well known [28]; see [57, chapter 1] for a historical overview. The concept of orthogonality of scalar polynomials on the unit circle was extended to the case of univariate
polynomial matrices in [13]. A limited extension to bivariate scalar orthogonal polynomials is provided in [33], which suffices for the development of a Levinson-type algorithm. The primary difference between the univariate algorithm and the bivariate algorithm (from the viewpoint of applying the algorithm) is the nonuniqueness of the monomial ordering; see Chapter 7 for more details.

Polarimetric calibration of synthetic aperture radar (SAR) systems provided the initial impetus for the consideration of many of this problems in this dissertation. The problem of estimating the minimal number of calibration targets is considered in [25, 56]. Under the assumptions (1) that energy does not leak between pixels in the same channel, i.e., $H$ is a constant matrix, (2) that the output is corrupted by additive white Gaussian noise whose variance is known, (3) and that clutter statistics can be estimated reliably, the algorithms in [25, 56] can estimate the equalizer nearly blindly - only one known trihedral is required to be part of the scene. Both schemes are sensitive to poor estimates of clutter statistics, and are not known to be extensible to the case of polynomial $H$.

### 1.3 Organization and Contributions

The point of view of this dissertation is primarily algebraic. We view MIMO FIR filters as polynomial matrices over a field, allowing us to treat MIMO FIR filters within a unified framework regardless of the dimension of the space in which convolution is performed. Our viewpoint also allows us to apply powerful techniques from algebraic geometry to characterize and quantify the class of all invertible MIMO FIR filters, and to obtain results that hold only generically.
This dissertation is divided into three parts. The first part presents the background and the basic mathematical tools. For ease of reference, we collect basic algebra definitions and results in Chapter 2. Chapter 3 presents prior work on the existence of and the orders of equalizers. Individual chapters in the second and third parts are mostly self-contained, and the interested reader can directly pass from Chapter 3 to any further chapter.

The second part presents the main theoretical results formulated in the language of polynomial modules. Chapter 4 discusses algorithms for the computation of equalizers for a given distortion system $\mathcal{H}$. Two computation techniques (based on matrix inversion and Gröbner bases) are provided along with a discussion of their strengths and weaknesses. Chapter 5 characterizes the class of all equalizers of a given distortion system $\mathcal{H}$. In Chapter 6, we derive nearly sharp generic bounds for the orders of the equalizer $\mathcal{G}$ given only knowledge of the orders of $\mathcal{H}$. Finally, in Chapter 7, we abandon the algebraic viewpoint temporarily to obtain an $n$-D Levinson-like algorithm (using a multivariate analog of Szegö polynomials) for fast computation of the equalizer.

The third part illustrates the utility of the results from the second by specializing them to concrete applications. The results of Chapter 5 are applied in Chapter 8 to obtain a minimal set of calibration targets for polarimetric ultra-wideband synthetic aperture radar. Signal processing consequences of the generic equalizer order results are discussed in Chapter 9. The third part can be read independently of the second (taking the relevant results without proof, of course).
CHAPTER 2

ALGEBRA

The statements and proofs of many results in this dissertation use concepts from algebra. In this chapter, we collect (for ease of reference) the definitions and the results from algebra used in subsequent chapters. The reader may skip this chapter on a first reading, and refer back to it later as needed.

2.1 Definitions

An excellent introduction to elementary algebraic geometry can be found in the book by Cox, Little and O'Shea [10]. The proofs of the propositions here can be found in [10, 12].

**Definition 1** A **field** consists of a set $F$ and two binary operations “.” and “+” defined on $F$ for which the following conditions are satisfied:

1. $(a + b) + c = a + (b + c)$ and $(a.b).c = a.(b.c)$ for all $a, b, c \in F$ (associative).

2. $a + b = b + a$ and $a.b = b.a$ for all $a, b, c \in F$ (commutative).

3. $a.(b + c) = a.b + a.c$ for all $a, b, c \in F$ (distributive).

4. There are $0, 1 \in F$ such that $a + 0 = a.1 = a$ for all $a \in F$ (identities).
5. Given \( a \in \mathbb{F} \), there is \( b \in \mathbb{F} \) such that \( a + b = 0 \) (additive inverses).

6. Given \( a \in \mathbb{F}, a \neq 0 \), there is \( c \in \mathbb{F} \) such that \( a.c = 1 \) (multiplicative inverses).

The fields most commonly used are \( \mathbb{Q}, \mathbb{R}, \) and \( \mathbb{C} \). If we do not require multiplicative inverses, then we get a commutative ring.

**Definition 2** A **commutative ring** consists of a set \( S \) and two binary operations 
"." and "+" defined on \( S \) for which the following conditions are satisfied:

1. \( (a + b) + c = a + (b + c) \) and \( (a.b).c = a.(b.c) \) for all \( a, b, c \in S \) (associative).

2. \( a + b = b + a \) and \( a.b = b.a \) for all \( a, b, c \in S \) (commutative).

3. \( a.(b + c) = a.b + a.c \) for all \( a, b, c \in S \) (distributive).

4. There are \( 0, 1 \in S \) such that \( a + 0 = a.1 = a \) for all \( a \in S \) (identities).

5. Given \( a \in S \), there is \( b \in S \) such that \( a + b = 0 \) (additive inverses).

**Definition 3** A commutative ring \( S \) is an **integral domain** if whenever \( a, b \in S \) and \( a.b = 0 \), then either \( a = 0 \) or \( b = 0 \).

**Definition 4** Let \( S \) be a commutative ring. A subset \( I \subset S \) is an **ideal** if it satisfies:

1. \( 0 \in I \).

2. If \( a, b \in I \), then \( a + b \in I \).

3. If \( a \in I \) and \( b \in S \), then \( b.a \in I \).

Let \( S_n \) be the set of permutations of the integers \( 1, \ldots, n \):

\[
S_n = \{ \sigma : \{1, \ldots, n\} \to \{1, \ldots, n\} : \sigma \text{ is bijective} \}
\] (2.1)
Definition 5 If $\sigma \in S_n$, let $P_\sigma$ be the matrix obtained by permuting the columns of the $n \times n$ identity according to $\sigma$. Then the sign of $\sigma$, denoted $\text{sgn}(\sigma)$, is defined by

$$\text{sgn}(\sigma) = \det(P_\sigma)$$

(2.2)

Proposition 6 If $A = (a_{ij})$ is an $n \times n$ matrix, then

$$\det(A) = \sum_{\sigma \in S_n} \text{sgn}(\sigma)a_{1\sigma(1)}a_{2\sigma(2)}...a_{n\sigma(n)}$$

(2.3)

Proposition 7 (Cramer’s Rule) Suppose we have a system of equations $AX = B$, where $A$ and $B$ have sizes $n \times n$ and $n \times 1$ respectively. If $A$ is invertible, then the unique solution is given by

$$x_i = \frac{\det(M_i)}{\det(A)}$$

(2.4)

where $M_i$ is the matrix obtained from $A$ by replacing its $i$th column with $B$.

2.2 Multi-indices

Let $\lambda = (\lambda_1, \ldots, \lambda_n)$ be an $n$-tuple of non-negative integers. Then if $z = (z_1, \ldots, z_n)$, the monomial $z^\lambda$ is defined as

$$z^\lambda = z_1^{\lambda_1}z_2^{\lambda_2}...z_n^{\lambda_n}$$

(2.5)

Also $|\lambda| = \lambda_1 + \ldots + \lambda_n$. Let

$$\mathbb{Z}_n^+ = \{\lambda = (\lambda_1, \ldots, \lambda_n) : \lambda_i \geq 0, \forall i\}$$

(2.6)

Definition 8 A polynomial $f$ in $z_1, \ldots, z_n$ with coefficients in a field $\mathbb{F}$ is a finite linear combination (with coefficients in $\mathbb{F}$) of monomials.

$$f = \sum_{\lambda} a_\lambda z^\lambda, \quad a_\lambda \in \mathbb{F}$$

(2.7)
where the sum is over a finite number of n-tuples $\lambda$. The set of all polynomials in $z_1, \ldots, z_n$ with coefficients in $F$ is denoted by $F[z_1, \ldots, z_n]$. $a_\lambda$ is called the coefficient of the monomial $z^\lambda$. The total degree of $f$, denoted $\text{totaldeg}(f)$, is the maximum $|\lambda|$ such that the coefficient $a_\lambda$ is nonzero. A rational function in $z_1, \ldots, z_n$ with coefficients in $F$ is a quotient $f/g$ of two polynomials $f, g \in F[z_1, \ldots, z_n]$, where $g$ is not the zero polynomial. The set of all rational functions in $z_1, \ldots, z_n$ with coefficients in $F$ is denoted by $F(z_1, \ldots, z_n)$.

### 2.3 Ideals and Varieties

**Definition 9** Let $F$ be a field, and let $f_1, \ldots, f_s$ be polynomials in $F[z_1, \ldots, z_n]$. Then the **affine variety** defined by $f_1, \ldots, f_s$ is

$$V(f_1, \ldots, f_s) = \{ (a_1, \ldots, a_n) \in \mathbb{F}^n : f_i(a_1, \ldots, a_n) = 0, \ 1 \leq i \leq s \}$$

(2.8)

**Definition 10** Let $f_1, \ldots, f_s$ be polynomials in $F[z_1, \ldots, z_n]$. Then the **ideal** generated by $f_1, \ldots, f_s$ is denoted as

$$\langle f_1, \ldots, f_s \rangle = \left\{ \sum_{i=1}^{s} h_i f_i : h_1, \ldots, h_s \in F[z_1, \ldots, z_n] \right\}$$

(2.9)

**Proposition 11** If $f_1, \ldots, f_s$ and $g_1, \ldots, g_t$ are bases of the same ideal in $F[z_1, \ldots, z_n]$, so that $\langle f_1, \ldots, f_s \rangle = \langle g_1, \ldots, g_t \rangle$, then $V(f_1, \ldots, f_s) = V(g_1, \ldots, g_t)$.

**Definition 12** If $V \subset k^n$ be an affine variety. Then the **ideal of $V$** is

$$\mathbb{I}(V) = \{ f \in F[z_1, \ldots, z_n] : f(a_1, \ldots, a_n) = 0 \quad \forall (a_1, \ldots, a_n) \in V \}$$

(2.10)
2.4 Algorithms

2.4.1 Univariate polynomials

For polynomials in one variable, there exist nice algorithms for division and for finding the greatest common divisor of two polynomials. The following is the Euclidean division algorithm.

**Proposition 13 (Euclidean division algorithm)** Let $\mathbb{F}$ be a field and let $g$ be a nonzero polynomial in $\mathbb{F}[z]$. Then every $f \in \mathbb{F}[z]$ can be written as

$$f = qg + r$$

(2.11)

where $q, r \in \mathbb{F}[z]$, and either $r = 0$ or $\deg(r) < \deg(g)$. Furthermore, $q$ and $r$ are unique, and there is an algorithm for finding $q$ and $r$.

2.4.2 Multivariate polynomials

For multivariate polynomials, there exists a division algorithm which, however, does not behave so nicely as the Euclidean division algorithm.

**Proposition 14** Let $\mathbb{F}$ be a field and let $g_1, \ldots, g_N$ be nonzero polynomials in $\mathbb{F}[z_1, \ldots, z_n]$. Then every $h \in \mathbb{F}[z]$ can be written as

$$h = q_1g_1 + \ldots + q_Ng_N + r$$

(2.12)

where $q_i, r \in \mathbb{F}[z]$, and either $r = 0$ or $r$ is divisible by the leading terms of none of the polynomials $g_i$.

The multivariate division algorithm guarantees the uniqueness of neither the quotients $q_i$ nor the remainder $r$. For example, let $g_1 = z_2^2 - 1$ and $g_2 = z_1z_2 - 1$ with
\( h = z_1^2 z_2 + z_1 z_2^2 + z_2^2 \). Then, \( h \) can be written

\[
\begin{align*}
    h &= (z_1 + 1)g_1 + (z_1)g_2 + (2z_1 + 1) \\
    &= (1)g_1 + (z_1 + z_2)g_2 + (z_1 + z_2 + 1)
\end{align*}
\]

Note that neither of the remainders, \( 2z_1 + 1 \) and \( z_1 + z_2 + 1 \), is divisible by \( g_1 \) or \( g_2 \), because the remainders have smaller total degrees.

The multivariate division algorithm produces remainders which are dependent only on

- the ordering of the divisors \( g_i \) and
- the ordering of the monomials in \( \mathbb{F}[z_1, \ldots, z_n] \).

The choice of monomial ordering is usually independent of the problems considered in this dissertation, and hence can be chosen \textit{a priori}. However, the nonuniqueness of remainders is a fundamental problem which can handled using Gröbner basis techniques. Section 2.4.3 provides a brief overview of Gröbner bases.

### 2.4.3 Gröbner bases

Gröbner bases generalize the concepts of greatest common divisor and division algorithm for univariate polynomials to multivariate polynomials. Details can be found in [10], and computational issues are addressed in [12]. The problem solved by Gröbner bases is the following:

Given \( g_1, \ldots, g_k \) and \( h \), all in \( \mathbb{F}[z_1, \ldots, z_n] \), can \( h \) be expressed as

\[
    h = \sum q_i g_i, \quad q_i \in \mathbb{F}[z_1, \ldots, z_n]
\]

and if so, find such a representation.
For the univariate case, $n = 1$, the solution requires only the computation of the greatest common divisor (gcd) of the $g_i$ and a check that the gcd divides $h$, where the division yields a unique quotient and a unique remainder. The multivariate division algorithm can be used to compute remainders on division of $h$ by $g_1, \ldots, g_k$. However, the remainder is not unique and depends on the ordering of $g_1, \ldots, g_k$. In particular, the remainder may be nonzero even if $h$ can be expressed as in equation (2.13).

A Gröbner basis $F$ of $\langle g_1, \ldots, g_k \rangle$ is a set of polynomials such that the multivariable division algorithm yields a unique remainder, regardless of the order. In particular, if $h$ allows a representation of the form of equation (2.13), then, on division by $F$, the remainder is guaranteed to be zero. Further, with respect to the chosen ordering of the monomials in $F[z_1, \ldots, z_n]$, the remainder is of minimal degree.

### 2.5 The Nullstellensatz

**Theorem 15 (Weak Nullstellensatz)** Let $F$ be an algebraically closed field, and let $I \subset F[z_1, \ldots, z_n]$ be an ideal satisfying $\mathbb{V}(I) = \emptyset$. Then $I = F[z_1, \ldots, z_n]$.

The preceding is known as the weak Nullstellensatz and can be found in [10, p. 169].
CHAPTER 3

MIMO INVERSES

The problem of computing MIMO FIR equalizers is formulated in this chapter, and the question of existence\(^1\) is resolved. We begin by establishing the notational conventions used throughout this dissertation. We derive the conditions necessary and sufficient for a MIMO FIR system to be FIR equalizable. We then define random systems and obtain the necessary and sufficient conditions for the generic equalizability of a random system.

3.1 Problem Statement

3.1.1 Notation

We use polynomials to represent \(n\)-dimensional \((n\text{-D})\) signals of finite extent. With each finite support signal, we associate a polynomial \((z\text{-transform})\) in the variables \(z_1,\ldots,z_n\):

\[
\sum_{k_i \in \mathbb{Z}^+, 1 \leq i \leq n} x(k_1, \ldots, k_n) z_1^{k_1} z_2^{k_2} \cdots z_n^{k_n} = \sum_{\mathbf{k} \in \mathbb{Z}_n^+} x(\mathbf{k}) z^\mathbf{k} \tag{3.1}
\]

We denote both the \(n\text{-D}\) signal and its associated polynomial by \(x\) and suppress the variables \(z_1,\ldots,z_n\). Likewise, we write the \(n\text{-D}\) convolution of sequences \(x_1\) and \(x_2\)

\(^1\)The main results of this chapter can be found in [51].
as the multiplication of the associated polynomials. Accordingly, a MIMO FIR filter is described as a polynomial matrix in \( n \) variables.

As an example, consider the real 2-D FIR filter mask given by the following array:

\[
\mathbf{x} = \begin{bmatrix} 2 & 3 & -6 \\ 0 & 5 & 1 \\ 1 & 9 & 0 \end{bmatrix}
\] (3.2)

Letting the \( z_1 \) axis travel from left to right, and the \( z_2 \) axis from bottom to top (or placing the matrix \( \mathbf{x} \) in the first quadrant), we obtain the following associated polynomial in \( \mathbb{R}[z_1, z_2] \):

\[
\mathbf{x} = 1 + 9z_1 + 5z_1z_2 + z_1^2z_2 + 2z_2^2 + 3z_1z_2^2 - 6z_1^2z_2^2
\] (3.3)

The coefficient of the monomial \( z^{(0,2)} = (z_1, z_2)^{(0,2)} = z_1^0z_2^2 \) is 2, and totaldeg(\( \mathbf{x} \)) = 4. This is just the familiar \( z \)-transform of the filter’s impulse response with \( z^{-1} \) replaced by \( z \) [20].

### 3.1.2 System model

We represent finite support \( n \)-D signals and channel responses as polynomials in \( \mathbb{F}[z_1, \ldots, z_n] \). Denote the \( N \) input signals as \( \mathbf{x}_i, \ i = 1, \ldots, N \). Let the \( M \) output signals \( \mathbf{y}_j \) be defined as

\[
\mathbf{y}_j = \sum_{i=1}^{N} \mathbf{h}_{ji} \mathbf{x}_i \quad j = 1, \ldots, M,
\] (3.4)

where \( \mathbf{h}_{ji} \) is the FIR response, or channel, from input \( i \) to output \( j \). We seek polynomials \( \mathbf{g}_{ij} \) such that

\[
\sum_{j=1}^{M} \mathbf{g}_{ij} \mathbf{y}_j = \sum_{j=1}^{M} \sum_{k=1}^{N} \mathbf{g}_{ij} \mathbf{h}_{jk} \mathbf{x}_k = \mathbf{x}_i, \quad i = 1, \ldots, N.
\] (3.5)

In matrix notation, equation (3.5) can be written as

\[
\mathbf{G}\mathbf{H} = \mathbf{I}_N,
\] (3.6)
where
\[
\mathcal{H} = \begin{pmatrix}
h_{11} & h_{12} & \cdots & h_{1N} \\
h_{21} & h_{22} & \cdots & h_{2N} \\
\vdots & \vdots & \ddots & \vdots \\
h_{M1} & h_{M2} & \cdots & h_{MN}
\end{pmatrix}, \quad
\mathcal{G} = \begin{pmatrix}
g_{11} & g_{12} & \cdots & g_{1M} \\
g_{21} & g_{22} & \cdots & g_{2M} \\
\vdots & \vdots & \ddots & \vdots \\
g_{N1} & g_{N2} & \cdots & g_{NM}
\end{pmatrix},
\] (3.7)

and \( I_N \) denotes the \( N \times N \) identity matrix. A matrix \( \mathcal{H} \) is said to be polynomial if each of its elements \( h_{ji} \in \mathbb{F}[z_1, \ldots, z_n] \). Thus, we seek a polynomial left inverse \( \mathcal{G} \) of the MIMO FIR filter \( \mathcal{H} \).

### 3.2 Existence of Polynomial Inverse

For the single input, multiple output case, the forward filter is invertible by a FIR filter if the channels do not share a common zero. This familiar concept generalizes, for multiple inputs, to the requirement that all minors of the matrix \( \mathcal{H} \) are coprime. The result has been independently proven in several contexts \([6, 24, 45]\); the constructive proof is reviewed here to provide a foundation for new results presented later.

#### 3.2.1 Inverse

**Theorem 16** A matrix \( \mathcal{H} \), whose elements are multivariate polynomials with coefficients in an algebraically closed field, has a polynomial left inverse \( \mathcal{G} \) iff

1. \( M \geq N \) and

2. the \( N \times N \) minors of \( \mathcal{H} \) are coprime.

**Proof:** Let \( \mathcal{H}_i \) denote the \( N \times N \) submatrices of \( \mathcal{H} \), which are totally \( C^M_N \) in number, where

\[
C^M_N = \frac{M!}{N!(M - N)!}
\] (3.8)
Let $D_i$ denote the determinant of $H_i$. If the $N \times N$ minors of $H$ are coprime, by the weak form of the Nullstellensatz [10, p. 169] for polynomials, there exist $a_i, \quad 1 \leq i \leq C_M^N$ such that

$$\sum_{i=1}^{C_M^N} a_i D_i = 1.$$  \hfill (3.9)

Because finite products and finite sums of polynomials are also polynomials, for those $H_i$ such that $D_i \neq 0$, by Cramer’s rule, there exist square matrices $G_i$ (adjoints of $H_i$) such that

$$G_i H_i = D_i I_N.$$  \hfill (3.10)

Thus, there exist $N \times M$ matrices $\tilde{G}_i$ (which are $G_i$ with additional zero rows corresponding to those columns in $H$ which are not in $H_i$) such that

$$\tilde{G}_i H = D_i I_N.$$  \hfill (3.11)

From equations 3.9 and 3.11 it follows that

$$\sum_{i=1}^{C_M^N} (a_i \tilde{G}_i) H = \sum_{i=1}^{C_M^N} a_i D_i I_N = I_N,$$

whence

$$G = \sum_{i=1}^{C_M^N} (a_i \tilde{G}_i).$$  \hfill (3.13)

Conversely, suppose that the $N \times N$ minors of $H$ share a common zero $w \in \mathbb{F}^n$, i.e., $D_i(w) = 0, 1 \leq i \leq C_M^N$. Then $\text{rank}(H(w)) < N$. Then, there does not exist $G(w)$ such that $G(w) H(w) = I_N$. Thus, a polynomial left inverse of $H$ does not exist. \hfill $\blacksquare$

When inputs and outputs are equal in number (i.e., $N = M$), there is $C_M^N = 1$ minor of size $N$, namely $H$ itself. Thus, for square $H$, FIR invertibility is equivalent to the determinant of $H$ being a nonzero constant.
The proof of the preceding theorem establishes more than just the existence of an inverse. The minors $D_k$ can be computed easily, and $G_i$ can be computed using Cramer's rule. Thus, the only part of the solution not explicitly computed in the proof are the $a_i$. Solving for the $a_i$ in equation (3.9) is equivalent to solving for the inverses of single input systems with transfer functions $D_i$. Hence, the MIMO problem of equation (3.5) reduces to the SIMO problem of equation (3.9).

### 3.2.2 Special cases

When $n = 1$, the signals under consideration are usually thought of as time signals, e.g., in communication applications. When $N = 1$, the problem of inversion of the resulting single input multiple output system has been studied extensively. Recent results based on properites of $T(H)^HT(H)$ yield blind SIMO deconvolution algorithms [39, 63]. An algorithm for efficient computation of SIMO inverses is given in [47]. If $N > 1$, inversion of $H$ can be obtained through, e.g., the Smith normal form. The inversion of such MIMO systems is considered in [42, 43, 59]. The fundamental principle on which all these univariate polynomial algorithms are based is the Euclidean division algorithm.

When $n > 1$, the Euclidean division algorithm fails. For $N = 1$ and $n = 2$, the problem of estimation of the input blindly is considered in [30], and inversion of known systems is considered in [31].

The problem of inversion of matrices whose elements are rational functions has been extensively studied in the context of control theory [34, 66]. Conditions for the invertibility of such matrices using rational matrices are collected in [34]. This chapter considers the related problem of inversion using only matrices with polynomial entries.
3.3 Random Systems

Theorem 16 characterizes the invertibility of an arbitrary MIMO FIR system. A natural question is “How restrictive is invertibility?” We show that if the outputs outnumber the inputs, a generic system is indeed invertible, and we use a probability measure on the FIR coefficients to define genericness. Further, this notion of genericness is applicable to structured convolution systems.

Consider FIR systems of bounded degree, and let $\phi$ denote the upper bound on the exponent of the variables $z_1, \ldots, z_n$ appearing in $H$. Thus, for an $N$-input $M$-output system, $J = MN(\phi + 1)^n$ coefficients uniquely specify $H$.

**Definition 17**  Let $H$ be as in equation (3.7). Let $\phi$ denote a fixed upper bound on the exponent of each of $z_1, \ldots, z_n$ appearing in each of the polynomials $h_{ij}$. Suppose that the coefficients of $h_{ij}$ are chosen from a continuous probability density (pdf) $\Psi$ on $\mathbb{C}^J$, where $J = MN(\phi + 1)^n$, the number of coefficients needed to determine $H$ uniquely. Then the system is said to be freely random.\(^2\)

However, structured systems may be specified by fewer than $MN(\phi + 1)^n$ coefficients yielding a probability distribution function that is discontinuous in $\mathbb{C}^J$. Consider a single-input single-output system such that the transfer function is given by

$$h_{11}(z_1, z_2) = a_{30}z_1^3 + a_{02}z_2^2 + 3z_1z_2 + (a_{02} + a_{30}),$$  \hspace{1cm} (3.14)

where the $a_{ij}$ are chosen randomly. Then, the highest degree appearing in the definition is 3, but the probability distribution is not continuous on the space $\mathbb{C}^{16}$, i.e.,

\(^2\)This definition depends on choosing a bound on the exponent of each variable. An analogous definition can be made for the case of a bound on the degree of the polynomials.
structure in the system is not modeled. Hence, we choose to model each of the coefficients in $\mathcal{H}$ as functions of set of $K$ numbers, $K \leq J$. For our purposes, the functions can be restricted to polynomials in the variables. Incorporating this idea of structure, we arrive at a second definition of random systems.

**Definition 18** Let $\mathcal{H}$ be as in equation (3.7). Let $\phi$ denote a fixed upper bound on the exponent of each of $z_1, \ldots, z_n$ appearing in each of the polynomials $h_{ij}$. Suppose that the coefficients of $h_{ij}$ are polynomial functions of $K$ random numbers chosen from a continuous probability density (pdf) $\Psi$ on $\mathbb{C}^K$. Then the FIR system is said to be random with $K$ degrees of freedom.

Armed with a continuous distribution $\Psi$ on the set of FIR systems, we formally define generic following Cox, et al. [11, Definition 5.6, p. 109].

**Definition 19** Let a FIR system $\mathcal{H}$ be random with $K$ degrees of freedom. A property is generic for $\mathcal{H}$ iff the set $B \subseteq \mathbb{C}^K$ where the property does not hold is an algebraic variety, i.e., $B$ is the solution set of a finite set of nontrivial polynomial equations.

Note that an algebraic variety is a closed set of (Lebesgue) measure zero. Since $\Psi$ is continuous w.r.t. the Lebesgue measure, a generic property holds almost surely; further, given any $\mathcal{H}$ satisfying a generic property, every point in some neighborhood of $\mathcal{H}$ also satisfies the property.

The following theorem provides that a random system invertible at one point is invertible generically.

**Theorem 20** Let a FIR system $\mathcal{H}$ be random system with $K$ degrees of freedom. Further, assume $\mathcal{H}$ is left invertible for some choice of coefficients. Then, $\mathcal{H}$ is left invertible almost surely if $C_N^M > n$.  

23
Proof: We shall use the notation of the proof of Theorem 16. Note that the coefficients of the minors $D_k$ are polynomials of the coefficients of $h_{ij}$. Consider the homogeneous polynomials:

$$E_k(z_1, \ldots, z_n) = z_0^\text{totaldeg}(D_k) D_k\left(\frac{z_1}{z_0}, \frac{z_2}{z_0}, \ldots, \frac{z_n}{z_0}\right)$$  \hspace{1cm} (3.15)

$E_k$ share a common zero in $\mathbb{C}^{n+1} - \{0\}$ if $D_k$ share a common zero in $\mathbb{C}^n$. The resolvent $R(\rho_1, \ldots, \rho_{n+1})$ of $n + 1$ homogeneous polynomials $\rho_1, \ldots, \rho_{n+1}$ in $n + 1$ variables is a polynomial in the coefficients of $\rho_1, \ldots, \rho_{n+1}$ which vanishes iff the polynomials $\rho_1, \ldots, \rho_{n+1}$ share a common zero in $\mathbb{C}^{n+1} - \{0\}$. Then $R(D_1, \ldots, D_{n+1})$ is a polynomial in the coefficients of $D_k$, and hence a polynomial in $K$ variables [26, p. 427, Prop. 1.1]. Hence, it vanishes only on an affine variety $B$ which is a closed and nowhere dense set of measure zero. The polynomial cannot vanish everywhere because it cannot vanish on the point where $\mathcal{H}$ is left invertible.

We conjecture that if $C_N^M \leq n$, then $\mathcal{H}$ is almost surely not invertible. In this case, if the determinants were independent, one could use [11, p. 119, Ex. 6] to prove the result. However, the determinants are not independent of each other, and one needs to show that they are still “sufficiently independent”.

Theorem 20 can be specialized to freely random systems as follows.

Corollary 21 Let $\mathcal{H}$ be an $M \times N$ polynomial matrix with coefficients drawn from a continuous density function. If $C_N^M > n$, $\mathcal{H}$ is invertible almost surely.

Proof: Note that the constant coefficients of $D_k$ are nonzero almost everywhere and hence there exists a point in $\mathbb{C}^K$ where $\mathcal{H}$ is left invertible. ■

24
The result in Theorem 20 may intuitively be viewed via intersections of zero sets in $\mathbb{C}^n$. Algebraic varieties corresponding to the zero sets of the $N \times N$ minors of $\mathcal{H}$ in $\mathbb{C}^n$ can be visualized as curved manifolds, or locally as hyperplanes. The intersection of two randomly chosen hyperplanes is another manifold with dimension strictly smaller than the dimensions of the intersecting manifolds. Thus, when we start with $n$ varieties of dimension $n - 1$, generically the intersection is a finite set of points in $\mathbb{C}^n$. Another generic variety would not intersect with these points. Hence $n + 1$ generic varieties have no common intersection, i.e., $n + 1$ generic polynomials are coprime.

3.4 Filter Orders

The proof of Theorem 16 answers the question of existence of a polynomial left inverse, and the constructive proof leads to algorithms for computing $\mathcal{G}$ given $\mathcal{H}$. In this section, we present bounds for the orders of the polynomials, $g_{ij}$, in the inverse filter. Bounds may be obtained by application of a result by Kollar [23, 35, sections 1.5, 1.7].

**Theorem 22** Given $x_1, \ldots, x_k$ and $y \in \mathbb{F}[z_1, \ldots, z_n]$, assume that $y$ vanishes on all the common zeros of $x_1, \ldots, x_k$. Let $d_i = \text{totaldeg}(x_i)$ and assume that atmost three of the $d_i$ are equal to 2. Then, one can find $w_1, \ldots, w_k \in \mathbb{F}[z_1, \ldots, z_n]$ and a natural number $s$ satisfying

$$\sum_{i=1}^{k} w_i x_i = y^s \quad (3.16)$$
such that $s \leq N'(n, d_1, \ldots, d_k)$ and $\text{totaldeg}(\mathbf{w, x}_i) \leq (1 + \text{totaldeg}(\mathbf{x}))N'(n, d_1, \ldots, d_k)$, where

$$N'(n, d_1, \ldots, d_k) = \begin{cases} d_1 \cdots d_k & \text{if } k \leq n \\ d_1 \cdots d_n & \text{if } k > n > 1 \\ d_1 + d_2 - 1 & \text{if } k > n = 1 \end{cases} \quad (3.17)$$

The technical restriction that atmost three of the $d_i$ are equal to 2 is required in the proof technique, but is not restrictive in practice because multidimensional distortion filters are typically larger than degree 2. Further, for time signals ($n = 1$), the restriction can be removed [47]. As an aside, absolute values of the coefficients of $\mathbf{w}_i$ can be bounded [35] given bounds on the absolute values of the coefficients of $\mathbf{x}_i, 1 \leq i \leq k$.

Theorem 22 may be used to bound the degree of the equalizing filter, $\mathcal{G}$. Suppose the conditions of Theorem 16 are satisfied and that each channel of the distortion filter is bounded in degree by $d$:

$$d = \max_{i,j} \text{totaldeg}(h_{ij}) \quad (3.18)$$

Then, the determinants $D_i$ are bounded in degree by $Nd$, and the degree of every element of the adjoint, $\mathcal{G}_i$, is bounded by $(N - 1)d$. In the sequel, we assume that $C^M_N > n$. The results for invertible systems with $C^M_N \leq n$ can be derived analogously. Application of Theorem 22 to equation (3.9) yields $\text{totaldeg}(a_i) \leq (Nd)^n$ whence we have the following corollary.

**Corollary 23**

$$\xi \triangleq \max_{i,j} \text{totaldeg}(g_{ij}) \leq (Nd)^n + (N - 1)d \quad (3.19)$$
Corollary 23 an answer to question 4 from Chapter 1. For example, with $N = 3$ desired input images, $n = 2$ dimensions, and $5 \times 5$ point response spread, we have $\xi = 235$, which is large, but not doubly exponential [41]. The bounds in [41] are tight for the case of arbitrary right hand sides, i.e., $s = 1$ in Theorem 22. The bound presented here is tighter because we consider the special case $h = 1$. With the doubly exponential bound, $\xi = 512$ for the example considered above.

The bound in equation (3.19) is independent of the number of outputs, $M$. It allows, for example, some outputs to be zero regardless of the input.
CHAPTER 4

EQUALIZER COMPUTATION

Given the existence of FIR equalizers from Theorem 16, we turn our attention to the problem of computing the equalizer for a given $H$. We propose two approaches, one based on matrix inversion via linear algebra, and another based on Gröbner bases for computing the equalizer: we then discuss the relative strengths and weaknesses of the two approaches. For the special case of single-input multiple-output systems, a fast algorithm for equalizer computation is given in Chapter 7.

4.1 Linear Algebra for Computation

Because the equalizer is a linear system with finite impulse response, the solution of the equalizer coefficients, $g_{ij}$, can be written as a large system of linear equations; this provides a direct, “brute force” solution for $G$. In section 4.2, we present an alternative algebraic solution technique and discuss its advantages.

The convolution of two sequences $x$ and $y$ can be written as

$$x \ast y = T(x) \text{vec}(y)$$ (4.1)

where $T(x)$ is a Toeplitz matrix if $x$ is a time signal, or a Toeplitz-block Toeplitz matrix if $x$ is an image signal [30], and vec$(y)$ denotes the vectorized version of $y$.

The main results of this chapter can be found in [50].
This process can be extended to signals of arbitrary dimension with nested Toeplitz matrices with nesting level equal to the dimension of the underlying signal space. Then, solving equation (3.6) is equivalent to solving the following system of linear equations:

\[
\begin{bmatrix}
T(h_{11}) & T(h_{21}) & \cdots & T(h_{M1}) \\
T(h_{12}) & T(h_{22}) & \cdots & T(h_{M2}) \\
\vdots & \vdots & \ddots & \vdots \\
T(h_{1N}) & T(h_{2N}) & \cdots & T(h_{MN})
\end{bmatrix}
\begin{bmatrix}
\text{vec}(g_{i1}) \\
\text{vec}(g_{i2}) \\
\vdots \\
\text{vec}(g_{iM})
\end{bmatrix}
= \begin{bmatrix}
0 \\
\text{vec}(\delta^{(n)}) \\
\vdots \\
0
\end{bmatrix}, \quad i = 1, \ldots, N \quad (4.2)
\]

where \(\delta^{(n)}\) is in the \(i\)th block row and denotes the appropriately zero-padded \(n\)-dimensional Kronecker delta function.

Alternatively, equation (3.9) in the proof of Theorem 16 converts the MIMO inversion problem to the SIMO problem of computing \(a_i\) from the determinants, \(D_i\). Therefore, the approach in equation (4.2) can be applied to solve for \(a_i\), from which \(G\) can be computed.

Equation (4.2) provides for solution of \(G\) from knowledge of \(H\). Suppose instead that only input and output pairs, \(\{x, y\}\), are known. Such would be the case with known calibration targets placed in a scene. The inverse (which equalizes for sources in the subspace spanned by the test targets) is then found by solving, for each \(i\), the equation

\[
\sum_j g_{ij} y_j = x_i \quad (4.3)
\]

Equations (4.2) and (4.3) require prior knowledge of the support, and hence order, of each \(g_{ij}\). This is a deficiency in the linear algebraic approach. For an overdetermined system in equation (4.3), a bound on \(\text{deg}(g_{ij})\) may be used. As an aside, we note that for \(n = 1\) and \(N = 1\), the block nested Toeplitz matrix (called the Sylvester
resultant matrix in this special case) is rank deficient when the order of the inverse filters is overestimated and/or when the forward filters are not coprime. This property is exploited in [63], where the order of the inverse filters are estimated by computing the rank of the Sylvester matrix for increasing orders of the filters until it becomes rank deficient.

A second deficiency with the linear algebraic approach is the size of the coupled system of equations to be solved. Even for reasonably sized filters, the left-hand side matrix is very large and may not fit in computer memory. While Szegő polynomials have been used to derive fast algorithms for square nested Toeplitz matrices with square blocks [33, 65], such algorithms have not been extended to rectangular matrices for an arbitrary number of inputs; see Chapter 7. A third drawback is the lack of an existence test; the rank of $T(H)$ is affected by both coprimeness and by any selection for the unknown support of the $g_{ij}$ filters, and the separate effects cannot be discerned.

### 4.2 Algebra for Computation

In this section, we propose an algebraic procedure, using Gröbner bases, for computing a FIR equalizer. The algebraic coprimeness condition for existence in Theorem 16 and the algebraic nature of the constructive proof both suggest algebraic techniques for computation of $G$. Indeed, the proposed procedure provides a memory efficient computational approach that, significantly, does not require prior knowledge of the inverse filter orders.

We propose the following algorithm for computation of $G$, given $H$ and $M \geq N$.

1. Compute the determinants and adjoints, $D_i$ and $\tilde{G}_i$, as in the proof of Theorem 16.
2. Compute a Gröbner basis $F$ for $\langle D_1, \ldots, D_Q \rangle$.

3. Check whether $1 \in F$. If not, $H$ is not left invertible.

4. Determine $a_i$ in equation (3.9); these polynomials computed while forming the basis $F$ in step 2.

5. Substitute $a_i$ from step 4 into equation (3.13) to obtain $G$.

This procedure is not as memory intensive as the linear algebra approach, because no more than three polynomials ever need be stored in memory at once. In addition, by permutation of the reduced Gröbner basis polynomials, an inverse can be computed with either minimal order or minimum number of nonzero coefficients. Note that nonrectangular support regions may be returned for $g_{ij}$, and no prior knowledge of the support is required. Construction of the Gröbner basis in step 2 is the most computationally intensive element of the algorithm. \(^4\)

This Gröbner basis technique can be used to compute the inverse given an input-output description rather than given $H$ directly, \textit{i.e.}, to solve equation (4.3).

As an additional benefit of the algebraic approach, the algorithm may be used to produce a physically meaningful FIR equalizer when no exact inverse exists. Suppose that step 3 of the algorithm above fails, \textit{i.e.}, $1 \notin F$. In this case, we can still recover filtered versions of the input signals, \textit{i.e.}, we can find $G$ such that

$$G H = \text{diag}(q_1, \ldots, q_M)I_N$$

(4.4)

where $q_i \in \mathbb{C}[z_1, \ldots, z_n]$. That is, we can recover $x_i$ filtered by $q_i$. The single-channel filters $q_i$ can come from the common zeros of $D_i$, or may be constructed from prior

\(^4\)The computations can be performed using freely available packages such as Macaulay2 from \url{http://www.math.uiuc.edu/Macaulay2}. The relevant commands are \texttt{gb}, \texttt{minors}, \texttt{generators}, \texttt{getChangeMatrix}. 

32
physical considerations, such as frequency notches in every channel (or the desire to null cross-polarized returns in synthetic aperture radar applications; see Chapter 8).

The following algorithm can be used to compute such a $\mathcal{G}$:

1. Compute $D_i, \tilde{G}_i$ as in the proof of Theorem 16.

2. Compute a Gröbner basis $F$ for $\langle D_1, \ldots, D_Q \rangle$.

3. Compute a reduced $\mathcal{G}$ Gröbner basis $\tilde{F}$ and its representation in terms of the $D_i$.

4. For each $i$ from 1 to $M$, do

(a) Check whether the remainder of $q_i$ on division by $F$ is 0. If not, the required $\mathcal{G}$ does not exist.

(b) The division in step 4(a) and the representation of $F$ gives quotients $a_k$ such that

$$\sum_{k=1}^{Q} a_k D_k = q_i$$

(4.5)

(c) Compute the $i$th row of $\mathcal{G}$ as

$$(i \text{th row of } \mathcal{G}) = \sum_{k=1}^{Q} a_k (i \text{th row of } \tilde{G}_k)$$

(4.6)

This procedure may be viewed as producing an algebraic “pseudo-inverse” that inverts $\mathcal{H}$ at those points in $\mathbb{C}^n$ where an inverse exists. Step 4(c) implies that the rows of $\mathcal{G}$ are independent of each other. Hence, it is possible to split the inversion problem into $N$ subproblems which can be solved separately, as we will see in Section 4.4.

Suppose that the desired $q_i$ are monomials $z^k$, which would correspond to “delays” or shifts. Thus, if the reduced Gröbner basis computed in step 3 divides the delays,
it is possible to recover shifted versions of the output. One can show that this is equivalent to requiring in Theorem 16 that all common zeros of the minors $D_i$ lie at the origin. A reformulation of Theorem 16 in terms of Laurent polynomials would provide a more succint description [24] of this characterization of delayed inverses, without providing any additional insight, and while requiring an increase in the complexity of the proof.

4.3 Example: Radar Calibration

Consider a polarimetric SAR system which transmits and receives both horizontally and vertically polarized waves. By reciprocity [64], this system can be modeled as a 3-input 4-output MIMO FIR system of the form in equation (3.7). For illustrative purposes, suppose $\mathcal{H}$ is given by

$$\mathcal{H} = \begin{bmatrix} 3x^2 + 2y^2 - 1 & x^2 + y + 4 & y^2 + 2 \\ x & x & xy + 1 \\ 1 & 1 & y \\ x^2 + y^2 - 3 & y + 3 & y^2 + x + 4 \end{bmatrix} \quad (4.7)$$

First, from the `gb(generators(minors(3,H)),ChangeMatrix=>true)` and `getChangeMatrix` commands of Macaulay2, we find that the Gröbner basis of the determinants $D_i$ is given by

$$F = \{ y + 7, \quad x^2 + y^2 - \frac{1}{2}y - \frac{5}{2} \} \quad (4.8)$$

$$y + 7 = 2D_4 - D_1 \quad (4.9)$$

$$x^2 + y^2 - \frac{1}{2}y - \frac{5}{2} = \frac{1}{2}D_1 \quad (4.10)$$

Note that the Gröbner basis has only two elements; hence, any polynomial which is expressible as a combination of $D_1, \ldots, D_4$ can be expressed as a combination of these two polynomials and conversely.
Second, since $1 \not\in F$, $\mathcal{H}$ is not invertible.

Third, we decide to compute $\mathcal{G}$ such that $\mathcal{G}\mathcal{H} = (y + 7)I_3$. The corresponding inverse is

$$\mathcal{G} = 2\tilde{\mathcal{G}}_4 - \tilde{\mathcal{G}}_1 = \begin{bmatrix}
1 & 2x + 6 - 2y + yx^2 & -3x^2 - 6x + 2xy + y + 2 - x^3y & -2 \\
-1 & -y^2 - 2x - 6 - yx^2 - 5y & xy^2 + 6x + x^3y + 5xy + 5 + 3x^2 & 2 \\
0 & y + 7 & -xy - 7x & 0
\end{bmatrix}$$

(4.11)

where the $\tilde{\mathcal{G}}_i$ are the adjoints of $\mathcal{H}_i$ with appropriate zero columns added:

$$\tilde{\mathcal{G}}_1 = \begin{bmatrix}
-1 & -yx^2 - 4y + 2 & x^3y + x^2 + y + 4xy + 4 - 2x & 0 \\
1 & 3yx^2 + 2y^3 - y - y^2 - 2 & -3x^3y - 3x^2 - 2y^3x - 2y^2 + xy + 1 + xy^2 + 2x & 0 \\
0 & -2x^2 - 2y^2 + 5 + y & 2x^3 + 2xy^2 - 5x - xy & 0
\end{bmatrix}$$

(4.12)

$$\tilde{\mathcal{G}}_4 = \begin{bmatrix}
0 & x + 4 - 3y & -x^2 - 4x + 3xy + y + 3 & -1 \\
0 & -y^2 - x - 4 + yx^2 + y^3 - 3y & xy^2 + 4x - x^3y - y^3x + 3xy - y^2 + 3 & 1 \\
0 & y + 6 - x^2 - y^2 & -xy - 6x + x^3 + xy^2 & 0
\end{bmatrix}$$

(4.13)

For a simpler case, consider the 2-by-3 forward system where a second image is summed with filtered versions of the first:

$$\mathcal{H} = \begin{bmatrix}
2x - y + 3 & 1 \\
x & 1 \\
x + 3 & 1 \\
x + y + 2 & 1
\end{bmatrix}$$

(4.14)

In this case, the Gröbner basis of the minors contains 1, and an exact equalizer exists. Following the procedure above, the inverse is found to be...
\[ \mathcal{G} = \frac{1}{3} \begin{bmatrix} 1 & -1 & 0 & 0 \\ -xy & 2x - y + 3 & 0 & 0 \end{bmatrix} - \frac{1}{3} \begin{bmatrix} 1 & 0 & -1 & 0 \\ -x - 3 & 0 & 2x - y + 3 & 0 \end{bmatrix} \]
\[ -\frac{x}{3} \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & -x - y - 2 & x + 3 \end{bmatrix} \]
\[ = \begin{bmatrix} 0 & -1 & -x + 1 & x \\ x - xy + 3 & 2x - y + 3 & x^2 + xy + y - 3 & -x^2 - 3x \end{bmatrix} \] (4.15)

Note that many of the inverse filters do not have rectangular support; the support regions found here could not have been predicted in advance. When the equalizer computed here is applied on a set of images, it yields computational savings over the linear algebra solution which typically yields filters with maximum support.

### 4.4 Gröbner Bases of Modules

The computation technique in section 4.2 uses Gröbner bases of polynomial ideals. It is useful when the system \( \mathcal{H} \) is actually invertible. When \( \mathcal{H} \) is not invertible, the procedure can still provide certain meaningful inverses. However, it can occur that the system is partially invertible. For example, let

\[ \mathcal{H} = \begin{bmatrix} 2x - y + 3 & xy + 1 \\ xy & xy + 1 \\ x + 3 & xy + 1 \\ x + y + 2 & xy + 1 \end{bmatrix} \] (4.16)

Then \( \mathcal{G} \) from equation (4.15) can act as an “inverse” which can restore the first input but not the second. If we are interested in restoring as many inputs as possible even if the system \( \mathcal{H} \) is not completely invertible, the algorithm from section 4.2 is inadequate. For completeness, we provide an algorithm for the computation of partial inverses.

Gröbner bases can be computed not only for polynomials but also for free modules over polynomial rings. Using such Gröbner bases, we can provide a general algorithm for computing partial inverses:
1. Compute a Gröbner basis $F$ for the columns of $\mathcal{H}$. Each element of $F$ can be expressed as a $\mathbb{F}[z]$-linear combination of the columns of $\mathcal{H}$.

2. A particular input $x_j$ is recoverable iff $e_j \in F$ where $e_j$ is the $j$-th element of the natural basis:

   $e_j = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$  \hspace{1cm} (4.17)

3. The coefficients in the expansion of $e_j$ in terms of the columns of $\mathcal{H}$ from step 1 form the $j$-th row of $\mathcal{G}$. (Recall that the coefficients have already been computed in step 1.)

While the procedure presented above is the most general one (as it can be used to transform $\mathcal{H}$ into any matrix if $\mathcal{H}$ is invertible), it provides the least physical insight. The elements of $F$ do not lead themselves readily to physical interpretation. Further, the procedure involves computation of Gröbner bases of modules which can be (and usually is) much more intensive than computation of Gröbner bases of polynomial ideals [12].
CHAPTER 5

CLASS OF EQUALIZERS

From Theorem 16 of Chapter 3, and from the algorithms in Chapter 4, we have an algorithm to check for the invertibility of a given system $\mathcal{H}$ and to compute one equalizer. However, it is possible that the equalizer is not be unique. In this chapter, we obtain a characterization of the class of all inverses for a given system $\mathcal{H}$, thereby answering question (3) posed in Chapter 1. The characterization will require the computation of one explicit inverse $\mathcal{G}$, which can obtained using the techniques from Chapter 4.

5.1 Existence of Basis

$\mathcal{H}$ represents the transfer function of some system, and one may seek left inverses $\mathcal{G}$ of $\mathcal{H}$ that satisfy some particular criterion, usually in terms of optimizing some metric. In such cases, it is desirable to have a characterization of the set of all left inverses so that one may optimize over it. In order to proceed, we need the following proposition which shows that the kernel of the homomorphism defined by $\mathcal{H}^t$ is a free module, where $(.)^t$ denotes the transpose. The rank of $\ker(\mathcal{H}^t)$ characterizes the freedom one has in choosing a left inverse.
To show that the $\ker(H^t)$ is a free module, we will use the celebrated Quillen-Suslin theorem [54, Theorem 4.63, p. 149]:

**Theorem 24** If $D$ is a principal ideal domain, then every finitely generated projective $D[z_1, \ldots, z_n]$-module is free.

**Proposition 25** $\ker(H^t)$ is free with rank $M - N$ iff $H$ is unimodular.

**Proof:** Suppose $H$ is unimodular. Then, by Theorem 16, $\exists G$ such that $H'G^t = I_N$. If $g \in R^N$, then

$$g = H^t(G^t g) \quad \text{(5.1)}$$

whence $H^t$ is surjective. Further, $R^M = \ker(H^t) \oplus \text{Im}(G^t)$ because:

1. If $g \in \ker(H^t) \cap \text{Im}(G^t)$, then $\exists h \in R^N$ such that $g = G^t h$, whence $0 = H'G^t h = h$. Thus

$$\ker(H^t) \cap \text{Im}(G^t) = \{0\} \quad \text{(5.2)}$$

2. If $g \in R^M$, then

$$g = G^t H^t g + (g - G^t H^t g) \quad \text{(5.3)}$$

where $G^t H^t g \in \text{Im}(G^t)$ and $g - G^t H^t g \in \ker(H^t)$ as $H'(g - G^t H^t g) = H'^t g - H^t g = 0$.

Thus $\ker(H^t)$ is a direct summand of the free module $R^M$, and is hence projective [54, Theorem 3.12, p. 62]. By the Quillen-Suslin theorem, $\ker(H^t)$ is free, and hence has a basis.
Conversely, suppose that \( \ker(H^t) \) is free with rank \( M - N \). Let \( R^M = \mathcal{I} \oplus \ker(H^t) \), where \( \text{rank}(\mathcal{I}) = N \). Then, every \( g \in R^N \) can be expressed uniquely as \( g = \tilde{g}_1 + \tilde{g}_2 \) with \( \tilde{g}_1 \in \mathcal{I} \) and \( \tilde{g}_2 \in \ker(H^t) \). Hence, \( \mathcal{I} \to R^N \) is injective, which implies that \( \text{Im}(\mathcal{H}^t) \) has rank \( N \) and hence must be the whole space \( R^N \). Thus, there exists an inverse for \( \mathcal{H}^t|_{\mathcal{I}} \), and hence \( \mathcal{H}^t \) is unimodular.

5.2 Characterization of Inverses

Let \( s_1, \ldots, s_{M-N} \) be a basis for \( \ker(H^t) \). Let

\[
\mathcal{S} = (s_1 \ldots s_{M-N})
\] (5.4)

Now, let

\[
\mathcal{G} = \begin{pmatrix} g_1^t \\ \vdots \\ g_N^t \end{pmatrix}
\] (5.5)

represent the rows of a left inverse of \( \mathcal{H} \), and \( \mathbf{v}_i \) represent \( \mathbb{F}[z] \)-linear combinations of \( s_1, \ldots, s_{M-N} \),

\[
\begin{pmatrix} g_1^t + v_1^t \\ \vdots \\ g_N^t + v_N^t \end{pmatrix} \mathcal{H} = I_N
\] (5.6)

since

\[
\mathbf{v}_i^t \mathcal{H} = 0_{M \times 1}
\] (5.7)

as \( \mathbf{v}_i \in \ker(H^t) \).

Now, any \( N \)-tuple of “vectors” from \( \ker(H^t) \) can be generated as \( \mathcal{S} \mathbf{B} \) where \( \mathbf{B} \) is an arbitrary \( (M - N) \times N \) matrix with elements from \( \mathbb{F}[z] \). Thus, we are led to the following characterization of all left inverses of \( \mathcal{H}^t \).
Corollary 26 Let $\mathcal{H}$ be as in equation (3.7), and let $\mathcal{S}$ be as in equation (5.4). Then, if $\mathcal{G}$ is one left inverse of $\mathcal{H}$, the set of all left inverses of $\mathcal{H}$ is as follows:

$$\{ \mathcal{G} + A\mathcal{S}^T : A \text{ is an arbitrary } N \times (M - N) \text{ matrix} \}$$

(5.8)

Thus in obtaining left inverses $\mathcal{G}$, we are free to choose the elements of $A$. In this sense, we can consider $N(M - N)$ as the degrees of freedom of the space of left inverses of $\mathcal{H}$. Now, one can optimize over this set to obtain a desired left inverse. The computation of kernel bases can be accomplished in practice (through Gröbner basis techniques) via computer algebra systems such as Macaulay, CoCoA, Maple and Singular.

We may then distinguish the following special cases:

1. If $N > M$, $\mathcal{H}$ cannot be unimodular and $\mathcal{G}$ does not exist.

2. If $N = M$ and $\mathcal{H}$ is unimodular, $\mathcal{G}$ is unique.

3. If $N < M$ and $\mathcal{H}$ is unimodular, $\mathcal{G}$ is not unique and has $N(M - N)$ degrees of freedom. The set of all inverses is given by Corollary 26.
CHAPTER 6

GENERIC ORDERS

Given a specific equalizable distortion system $\mathcal{H}$, the techniques of the preceding three chapters let us compute a basis for the set of all equalizers for $\mathcal{H}$. We now turn our attention to the problem of obtaining bounds on the minimum orders of $\mathcal{G}$, given only $\deg(\mathcal{H})$. Signal processing applications of the results in this chapter will presented in Chapter 9. Bounds on $\text{totaldeg}(\mathcal{G})$ given knowledge of $\text{totaldeg}(\mathcal{H})$ were presented in Section 3.4. However, the bounds presented there are pessimistic for a large class of distortion systems. In this chapter, we present\(^5\) much smaller (almost tight) bounds on the multidegrees of $\mathcal{H}$.

6.1 Motivation

Sharpening the effective Nullstellensatz has recently been a focus of effective algebra [5, 35, 41], successfully culminating in the following result [35]:

**Theorem 27** Suppose $\mathbb{F}$ is a field, and $h_i \in \mathbb{F}[z_1, \ldots, z_n], 1 \leq i \leq M$ with maximum total degree $\delta$ such that $\langle h_1, \ldots, h_M \rangle = \mathbb{F}[z_1, \ldots, z_n]$. Then, $\exists g_1, \ldots, g_M \in\)

\(^5\)The main results of this chapter can be found in [48].
$F[z_1, \ldots, z_n]$ with maximum total degree $\delta_{\min(n,M)}$ such that

$$\sum_{i=1}^{M} g_i h_i = 1. \quad (6.1)$$

An issue noted in [35] is the difficulty of finding examples of $h_1, \ldots, h_M$ such that the bound on the total degree of the corresponding $g_1, \ldots, g_M$ is achieved. In this chapter, we provide a reason for the paucity of such examples. In particular, we show that if $M \geq 2^n$, for a generic set of $h_1, \ldots, h_M$, the minimal maximum total degree of the corresponding $g_1, \ldots, g_M$ is much smaller.

The a priori knowledge of a bound on the degrees of $g_1, \ldots, g_M$ is crucial in their computation [50]. Once such a bound is known, the computation of $g_1, \ldots, g_M$ can be accomplished via simple linear algebra without recourse to Gröbner basis techniques (cf. [8, 40]). In fact, almost all the results used in our proof arise from linear algebra.

### 6.2 Generic Orders of Equalizers

For the sake of convenience, we will work with multi-degrees of polynomials rather than total degrees. Let $\mathbb{Z}_n^+$ denote the set of all $n$-tuples of nonnegative integers. Let $F$ be a field (of arbitrary characteristic), and let $P_{\delta}(F[z_1, \ldots, z_n])$ denote the set of all $n$-variate polynomials over $F$ of multidegree at most $\delta$, where

$$\delta = (\delta_1, \ldots, \delta_n) \in \mathbb{Z}_n^+. \quad (6.2)$$

Let $M_{M \times N}(S)$ denote the set of all $M \times N$ matrices with elements from a set $S$. For $X \in F[z_1, \ldots, z_n]$, let $V(X)$ denote the variety in $F^n$ defined by $X$.

**Theorem 28** Suppose $M, N \in \mathbb{N}$ and $\delta \in \mathbb{Z}_n^+$ are given. Let $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}_n^+$ be such that

$$N \prod_{i=1}^{n} \left[ \frac{\delta_i + \alpha_i + 1}{\alpha_i + 1} \right] \leq M,$$
then, there exists a nonempty Zariski open subset $V$ of $\mathcal{M}_{M \times N}(\mathcal{P}_\delta(\mathbb{F}[z_1, \ldots, z_n]))$ such that for every $\mathcal{H} \in V$ and for every $\mathcal{I} \in \mathcal{M}_{1 \times N}(\mathcal{P}_{\delta+\alpha}(\mathbb{F}[z_1, \ldots, z_n]))$, the equation

$$G \mathcal{H} = \mathcal{I}.$$ 

can be solved for $G \in \mathcal{M}_{1 \times M}(\mathcal{P}_\alpha(\mathbb{F}[z_1, \ldots, z_n]))$.

However, if $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}_n^+$ is such that

$$N \prod_{i=1}^n \left\lceil \frac{\delta_i + \alpha_i + 1}{\alpha_i + 1} \right\rceil \geq M \quad (6.3)$$

and

$$N \prod_{i=1}^n \left\lceil \frac{\delta_i + \alpha_i + 1}{\alpha_i + 1} \right\rceil > M,$$

then, there exists a nonempty Zariski open subset $W$ of $\mathcal{M}_{M \times N}(\mathcal{P}_\delta(\mathbb{F}[z_1, \ldots, z_n]))$ such that for every $\mathcal{H} \in W$ and for every $\beta \in \mathbb{Z}_n^+$, the equation

$$G \mathcal{H} = (0 \cdots z^{\beta} \cdots 0)$$

cannot be solved for $G \in \mathcal{M}_{1 \times M}(\mathcal{P}_\alpha(\mathbb{F}[z_1, \ldots, z_n]))$.

The second part of Theorem 28 is not a true converse of the first part because of the condition (6.3). However, inequality (6.3) arises from the proof technique, and we conjecture that it is superfluous.

One of the reasons for the difficulty in obtaining the sharp effective Nullstellensatz is that the maximum total degree of $g_1, \ldots, g_M$ in

$$\sum_{i=1}^M g_i \mathbf{h}_i = f \quad (6.4)$$

is bounded by different constants depending on whether $f = 1$. In the case of univariate polynomials, this distinction does not exist. Theorem 28 shows that even in the case of multivariate polynomials, for a generic set of $\mathbf{h}_1, \ldots, \mathbf{h}_M$, the distinction does not exist.
6.3 The Operator $T_{\delta,\alpha}^n(.)$

Before proceeding to the proof of Theorem 28, we define an operator that expresses polynomial multiplication as an $\mathbb{F}$-linear operator.

Let $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}_n^+$ and $\delta = (\delta_1, \ldots, \delta_n) \in \mathbb{Z}_n^+$. Recall that

$$\mathcal{P}_\delta(\mathbb{F}[z_1, \ldots, z_n]) \triangleq \{ w \in \mathbb{F}[z] : \text{multideg}(w) \leq \delta \}$$

(6.5)
denotes the space of polynomials whose multidegrees are bounded by $\delta$. Let

$$\delta^* = \prod_{i=1}^n (\delta_i + 1)$$

(6.6)
denote the number of monomials in $\mathcal{P}_\delta(\mathbb{F}[z_1, \ldots, z_n])$. Since every $w \in \mathcal{P}_\delta(\mathbb{F}[z_1, \ldots, z_n])$ is a unique $\mathbb{F}$-linear combination of $\delta^*$ monomials, there exists a natural isomorphism (with respect to the ‘+’ operator):

$$\text{vec} : \mathcal{P}_\delta(\mathbb{F}[z_1, \ldots, z_n]) \longrightarrow \mathbb{F}^{\delta^*}$$

(6.7)

which can be obtained by ordering the $\delta^*$ monomials via some monomial ordering [10]. We shall call $\text{vec}(.)$ the “vectorizing” operator; its dependence on $\delta$ and on the chosen monomial ordering will be clear from context. If $w_1 \in \mathcal{P}_\delta(\mathbb{F}[z_1, \ldots, z_n])$ and $w_2 \in \mathcal{P}_\alpha(\mathbb{F}[z_1, \ldots, z_n])$, then $w_1 w_2 \in \mathcal{P}_{\delta + \alpha}(\mathbb{F}[z_1, \ldots, z_n])$. This multiplication can be represented by a linear operator in the corresponding isomorphic vector spaces:

$$T_{\delta,\alpha}^n(w_1) \text{vec}(w_2) = \text{vec}(w_1 w_2)$$

(6.8)

$$\Rightarrow T_{\delta,\alpha}^n(w_1) : \mathbb{F}^{\alpha^*} \longrightarrow \mathbb{F}^{(\delta + \alpha)^*}, \quad \forall w_1 \in \mathcal{P}_\delta(\mathbb{F}[z_1, \ldots, z_n])$$

(6.9)

$$\Rightarrow T_{\delta,\alpha}^n : \mathcal{P}_\delta(\mathbb{F}[z_1, \ldots, z_n]) \longrightarrow \mathcal{M}_{(\delta + \alpha)^* \times \alpha^*}(\mathbb{F}).$$

(6.10)

Note that $(\delta + \alpha)^* = \delta^* + \alpha^*$ iff $n = 1$. 

45
We will abuse notation slightly by extending the definition of $T_{\delta,\alpha}^n(.)$. When $\mathcal{H} \in \mathcal{M}_{M \times N}(\mathcal{P}_\delta(\mathbb{F}[z_1, \ldots, z_n]))$ is multiplied on the left by a $M \times 1$ row of polynomials, whose degrees are bounded by $\alpha$, the resulting $N \times 1$ row vector has elements whose degrees are bounded by $\delta + \alpha$. As in the case of multiplication of polynomials, this multiplication can be represented as an $\mathbb{F}$-linear operator which we continue to denote by $T_{\delta,\alpha}^n$:

$$T_{\delta,\alpha}^n : \mathcal{M}_{M \times N}(\mathcal{P}_\delta(\mathbb{F}[z_1, \ldots, z_n])) \longrightarrow \mathcal{M}_{N(\delta + \alpha)^* \times M \alpha^*}(\mathbb{F})$$

(6.11)

$$T_{\delta,\alpha}^n(\mathcal{H}) \triangleq \begin{pmatrix}
T_{\delta,\alpha}^n(h_{11}) & T_{\delta,\alpha}^n(h_{21}) & \cdots & T_{\delta,\alpha}^n(h_{M1}) \\
T_{\delta,\alpha}^n(h_{12}) & T_{\delta,\alpha}^n(h_{22}) & \cdots & T_{\delta,\alpha}^n(h_{M2}) \\
\vdots & \vdots & \ddots & \vdots \\
T_{\delta,\alpha}^n(h_{1N}) & T_{\delta,\alpha}^n(h_{2N}) & \cdots & T_{\delta,\alpha}^n(h_{MN})
\end{pmatrix}$$

(6.12)

The dependence of $T_{\delta,\alpha}^n(.)$ on $M, N$ will be clear from context.

### 6.4 A Generic Effective Nullstellensatz

The proof of Theorem 28 is organized as a series of five propositions. In this section, the generic solvability of $\mathcal{G}\mathcal{H} = \mathcal{I}$ is established for $\mathcal{H}$ consisting of a single column (i.e., for $N = 1$). In section 6.5, the partial converse is proven for $N = 1$. The extensions for the case when $N > 1$ are then considered in section 6.6.

To begin, Proposition 29 provides a construction for $N = 1$ of one $\mathcal{H}$ such that $\mathcal{G}\mathcal{H} = \mathbf{w}$ admits a solution for all $\mathbf{w}$, given the hypothesized restrictions on the multidegrees from Theorem 28.

**Proposition 29** Suppose $M \in \mathbb{N}$, $\delta \in \mathbb{Z}_n^+$ and $\alpha \in \mathbb{Z}_n^+$ such that

$$\prod_{i=1}^n \left[ \frac{\delta_i + \alpha_i + 1}{\alpha_i + 1} \right] \leq M.$$ 

(6.13)
Then, \( \exists h_{k_1} \in P_\delta(\mathbb{F}[z_1, \ldots, z_n]), 1 \leq k \leq M \) such that \( \forall w \in P_{\delta+\alpha}(\mathbb{F}[z_1, \ldots, z_n]), \exists g_{1k} \in P_\alpha(\mathbb{F}[z_1, \ldots, z_n]), 1 \leq k \leq M \) satisfying

\[
\sum_{k=1}^{M} h_{k_1} g_{1k} = w. \tag{6.14}
\]

The constructive proof partitions the integer lattice \( \{ \beta \in \mathbb{Z}^+_n : \beta \leq \delta + \alpha \} \) into \( M \) cells, and then builds \( w \) as a sum of monomials.

**Proof:** For convenience, let \( 1 \in \mathbb{Z}^+_n \) denote \((1, 1, \ldots, 1)\), and let \( 0 = (0, 0, \ldots, 0) \in \mathbb{Z}^+_n \). Let

\[
\lambda_i \triangleq \left\lceil \frac{\delta_i + \alpha_i + 1}{\alpha_i + 1} \right\rceil, \quad 1 \leq i \leq n \tag{6.15}
\]

whence, by hypothesis,

\[
(\lambda - 1)^* = \lambda_1 \lambda_2 \ldots \lambda_n \leq M. \tag{6.16}
\]

Consider monomials indexed by \( r \in \mathbb{Z}^+_n, 0 \leq r \leq \lambda - 1 \):

\[
m_r = \prod_{i=1}^{n} z_i^{\min(\delta_i, r_i(\alpha_i+1))} \tag{6.17}
\]

From equations (6.15) and (6.16), there are atmost \( M \) distinct monomials specified by equation (6.17). Next, any \( w \in P_{\delta+\alpha}(\mathbb{F}[z_1, \ldots, z_n]) \) can be written as

\[
w = \sum_{\beta \leq \delta+\alpha} w_{\beta} z^{\beta}. \tag{6.18}
\]

Given any \( \beta \leq \delta + \alpha, \exists r_{\beta} \in \mathbb{Z}^+_n \) satisfying

\[
\beta_i = r_{\beta_i}(\alpha_i + 1) + (\beta_i \mod (\alpha_i + 1)), \quad 1 \leq i \leq n. \tag{6.19}
\]

Thus a partition of \( \{ \beta \in \mathbb{Z}^+_n : \beta \leq \delta + \alpha \} \) is formed by counting \( \beta_i \mod (\alpha_i + 1) \). Hence, for any monomial \( z^{\beta} \in P_{\delta+\alpha}(\mathbb{F}[z_1, \ldots, z_n]) \), there exists a unique \( q_\beta \in \mathbb{Z}^+_n \).
\( \mathcal{P}_\alpha(\mathbb{F}[z_1, \ldots, z_n]) \) such that

\[
z_\beta = q_\beta m_{r_\beta}. \tag{6.20}
\]

From equations (6.18) and (6.20) and the \( \mathbb{F} \)-linearity of addition in \( \mathcal{P}_\alpha(\mathbb{F}[z_1, \ldots, z_n]) \),

\[
\exists g_r \in \mathcal{P}_\alpha(\mathbb{F}[z_1, \ldots, z_n]) \text{ such that }
\sum_r m_r q_r = w. \tag{6.21}
\]

Finally, identifying \( h_{k1} = m_r \) for \( 1 \leq k \leq \lambda_1 \lambda_2 \ldots \lambda_n \), assigning \( h_{k1} = 0 \) for \( k > \lambda_1 \lambda_2 \ldots \lambda_n \), and similarly reindexing \( q_r \) to \( g_{1k} \), equation (6.21) is rewritten in the form

\[
\sum_{k=1}^M h_{k1} g_{1k} = w
\]

as desired. \( \blacksquare \)

**Remark 30** The main idea of the proof is to obtain all monomials by combinations of the form

\[
h_{k1} q_\beta = z_\beta, \tag{6.22}
\]

where multideg(\( q_\beta \)) \( \leq \alpha \). In other words, we needed to pack the lattice block of size \( \delta + \alpha + 1 \) in \( \mathbb{Z}_n^+ \) by \( M \) blocks of size \( \alpha + 1 \). This concept may be extended easily to other sets of monomials. Suppose multideg(\( h_{k1} \)) and multideg(\( g_{1k} \)) were constrained to be in some polytopes \( D, E \subset \mathbb{Z}_n^+ \) respectively. Let \( F \subset \mathbb{Z}_n^+ \) be the set of all monomial degrees achievable by products of monomials in \( D \) and \( E \). If \( F \) can be packed by \( M \) polytopes of type \( E \), then \( \exists h_{k1} \) such that Proposition 29 holds. This packing can be used in conjunction with Proposition 29 to establish a generic effective Nullstellensatz.
Proposition 31 Let $N = 1$. Suppose $M \in \mathbb{N}$ and $\delta \in \mathbb{Z}_n^+$ are given. Let $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}_n^+$ be such that

$$\prod_{i=1}^n \left[ \frac{\delta_i + \alpha_i + 1}{\alpha_i + 1} \right] \leq M. \quad (6.23)$$

Then, there exists a nonempty Zariski open subset $V$ of $\mathcal{M}_{M \times 1}(\mathcal{P}_\delta(\mathbb{F}[z_1, \ldots, z_n]))$ such that for every $\mathcal{H} \in V$ and for every $\mathbf{w} \in \mathcal{P}_{\delta+\alpha}(\mathbb{F}[z_1, \ldots, z_n])$, the equation

$$\mathcal{G}_\mathbf{w} \mathcal{H} = \mathbf{w}$$

can be solved for $\mathcal{G}_\mathbf{w} \in \mathcal{M}_{1 \times M}(\mathcal{P}_\alpha(\mathbb{F}[z_1, \ldots, z_n])).$

Proof: Given $\mathcal{H} \in \mathcal{M}_{M \times 1}(\mathcal{P}_\delta(\mathbb{F}[z_1, \ldots, z_n]))$ and $\mathcal{G} \in \mathcal{M}_{1 \times M}(\mathcal{P}_\alpha(\mathbb{F}[z_1, \ldots, z_n]))$, the matrix multiplication $\mathcal{G} \mathcal{H}$ can be represented as follows in the corresponding isomorphic vector spaces:

$$T_{\delta,\alpha}^n(\mathcal{H}) \text{vec}(\mathcal{G}) = \text{vec}(\mathcal{G} \mathcal{H}) \quad (6.24)$$

$$(T_{\delta,\alpha}^n(\mathbf{h}_{11}) \ T_{\delta,\alpha}^n(\mathbf{h}_{21}) \ \cdots \ T_{\delta,\alpha}^n(\mathbf{h}_{M1})) \begin{pmatrix} \text{vec}(\mathbf{g}_{11}) \\ \text{vec}(\mathbf{g}_{12}) \\ \vdots \\ \text{vec}(\mathbf{g}_{1M}) \end{pmatrix} = \text{vec} \left( \sum_{k=1}^M \mathbf{h}_{k1} \mathbf{g}_{1k} \right) \quad (6.25)$$

whence

$$T_{\delta,\alpha}^n(\mathcal{H}) : \mathbb{F}^{M\alpha^*} \longrightarrow \mathbb{F}^{(\delta+\alpha)^*} \quad (6.26)$$

Since equation (6.23) holds,

$$\prod_{i=1}^n \left( \frac{\delta_i + \alpha_i + 1}{\alpha_i + 1} \right) \leq M \quad (6.27)$$

$$\Rightarrow \prod_{i=1}^n (\delta_i + \alpha_i + 1) \leq M \prod_{i=1}^n (\alpha_i + 1). \quad (6.28)$$

49
Thus, the domain of $T_{\delta,\alpha}^n(\mathcal{H})$ has higher dimension than its range. By Proposition 29, there exists $\hat{\mathcal{H}} \in \mathcal{M}_{M \times 1}(\mathcal{P}_\delta(\mathbb{F}[z_1, \ldots, z_n]))$ such that

$$\forall \mathbf{w} \in \mathcal{P}_{\delta+\alpha}(\mathbb{F}[z_1, \ldots, z_n]), \exists \mathcal{G}_w \in \mathcal{M}_{1 \times M}(\mathcal{P}_\alpha(\mathbb{F}[z_1, \ldots, z_n]))$$

such that

$$\mathcal{G}_w \hat{\mathcal{H}} = \mathbf{w}$$

(6.29)

$$\Rightarrow \text{range}(T_{\delta,\alpha}^n(\hat{\mathcal{H}})) = \mathbb{F}^{N(\delta+\alpha)^*}$$

(6.30)

$$\Rightarrow \text{rank}(T_{\delta,\alpha}^n(\hat{\mathcal{H}})) = \prod_{i=1}^{n}(\delta_i + \alpha_i + 1)$$

(6.31)

Thus, the matrix $T_{\delta,\alpha}^n(.)$ has at least one submatrix $X$ of size $\prod_{i=1}^{n}(\delta_i + \alpha_i + 1) \times \prod_{i=1}^{n}(\delta_i + \alpha_i + 1)$ whose determinant is nonzero for at least $\hat{\mathcal{H}}$. Hence $\det(X)$ is a nonzero polynomial in the coefficients of the elements of $\mathcal{H}$. Let $V = \mathbb{F}^n - \mathcal{V}(\det(X))$.

It is possible for $T_{\delta,\alpha}^n(\mathcal{H})$ to be rank deficient only if the determinant polynomial vanishes, i.e., only if $\mathcal{H} \not\in V$, whence we reach the desired conclusion for a generic $\mathcal{H}$.

The proof of Proposition 31 has two main elements. First, the fixed sets of monomials allowable for $\mathcal{H}$, $\mathcal{G}$ and $\mathcal{GH}$ allowed the posing of the problem in terms of matrices over $\mathbb{F}$. Second, the existence of a full rank $T_{\delta,\alpha}^n(\mathcal{H})$ was deduced from Proposition 29.

**Remark 32** As explained in Remark 30, given the polytopes $D$ and $E$, we can establish an effective Nullstellensatz for $D$ and $E$. Thus, the techniques of the proofs of Propositions 29 and 31 can be used to establish a family of Nullstellensätze. In the context of image processing, the polytopes $D$ and $E$ represent the shapes of the 2-D lattice support regions of the distortion and equalization filters respectively.
Recasting equation (6.23) to display the dependence of \( \alpha \) on \( M \) for a fixed \( \delta \), we obtain the following corollary.

**Corollary 33** Let \( N = 1 \). Suppose \( M \geq 2^n \), and

\[
\alpha = \left( \frac{\delta_1}{\left\lfloor M^{\frac{1}{n}} \right\rfloor - 1}, \ldots, \frac{\delta_n}{\left\lfloor M^{\frac{1}{n}} \right\rfloor - 1} \right). \tag{6.32}
\]

Then, for a generic \( \mathcal{H} \in \mathcal{M}_{M \times 1}(\mathcal{P}_\delta(\mathbb{F}[z_1, \ldots, z_n])) \), if \( w \in \mathcal{P}_{\delta + \alpha}(\mathbb{F}[z_1, \ldots, z_n]) \), \( \exists \mathcal{G} \in \mathcal{M}_{1 \times M}(\mathcal{P}_\alpha(\mathbb{F}[z_1, \ldots, z_n])) \) such that

\[ \mathcal{G}\mathcal{H} = w. \]

Thus, the total number of monomials in the inverse \( \mathcal{G} \) is generically roughly inversely proportional to \( M \) as \( M \) becomes large.

### 6.5 A Partial Converse of the Generic Effective *Nullstellensatz*

Paralleling propositions 29 and 31, we begin with a construction.

**Proposition 34** Suppose \( N = 1 \) and \( \alpha \in \mathbb{Z}_n^+ \) such that

\[
\prod_{i=1}^{n} \left\lfloor \frac{\delta_i + \alpha_i + 1}{\alpha_i + 1} \right\rfloor \geq M \tag{6.33}
\]

and

\[
\prod_{i=1}^{n} \left\lceil \frac{\delta_i + \alpha_i + 1}{\alpha_i + 1} \right\rceil > M \tag{6.34}
\]

Then, given any monomial \( z^\delta \in \mathcal{P}_{\delta + \alpha}(\mathbb{F}[z_1, \ldots, z_n]) \), \( \exists h_{k1} \in \mathcal{P}_\delta(\mathbb{F}[z_1, \ldots, z_n]), 1 \leq k \leq M \) such that
1. \( z^\beta \) cannot be expressed in the form

\[
\sum_{k=1}^{M} h_{1k} g_{1k} = z^\beta
\]  

with \( g_{1k} \in \mathcal{P}_\alpha(\mathbb{F}[z_1, \ldots, z_n]), 1 \leq k \leq M, \) and

2. every \( w \in \mathbb{F}[z] \) expressible in the form

\[
\sum_{k=1}^{M} h_{1k} g_{1k} = w
\]  

with \( g_{1k} \in \mathcal{P}_\alpha(\mathbb{F}[z_1, \ldots, z_n]), 1 \leq k \leq M, \) is expressible uniquely, i.e., the \( g_{1k} \) corresponding to \( w \) are unique.

**Proof:** For \( 1 \leq i \leq n, \) let

\[
\mu_i \triangleq \left\lfloor \frac{\delta_i + \alpha_i + 1}{\alpha_i + 1} \right\rfloor
\]  

Then \( \mu_1 \mu_2 \cdots \mu_n \geq M. \) Without loss of generality, let

\[
\mu_1 \mu_2 \cdots \mu_n = M.
\]  

When \( M \) is strictly smaller, we can use any subset of \( \{h_{1k}\} \) of size \( M. \) From equations (6.33) and (6.34), \( \exists i_0 \) such that

\[
\frac{\delta_{i_0} + \alpha_{i_0} + 1}{\alpha_{i_0} + 1} > \left\lfloor \frac{\delta_{i_0} + \alpha_{i_0} + 1}{\alpha_{i_0} + 1} \right\rfloor
\]

\[
\Rightarrow \delta_{i_0} > (\mu_{i_0} - 1)(\alpha_{i_0} + 1)
\]  

Consider monomials indexed by \( r \in \mathbb{Z}_n^+, 0 \leq r \leq \mu - 1: \)

\[
m_r = \prod_{i=1}^{n} z_i^{r_i(\alpha_i+1)}
\]  

52
Similar to the proof of Proposition 29, these monomials partition the lattice \( \{ \beta \in \mathbb{Z}_n^+ : \beta \leq (\mu_1(\alpha_1 + 1), \mu_2(\alpha_2 + 1), \ldots, \mu_n(\alpha_1 + n)) \} \) into \( M \) blocks formed by counting \( \beta_i \mod (\alpha_i + 1) \).

\( \beta_{i_0} \) lies in one of the following intervals:

\[
\begin{align*}
[0, \alpha_{i_0} + 1), \\
[(\alpha_{i_0} + 1), 2(\alpha_{i_0} + 1)), \\
\vdots \\
[\mu_{i_0} - 1)(\alpha_{i_0} + 1), \mu_{i_0}(\alpha_{i_0} + 1)), \\
[\mu_{i_0}(\alpha_{i_0} + 1), \delta_{i_0} + \alpha_{i_0}]
\end{align*}
\]

We now distinguish the following two cases.

**Case 1:** \( \beta_{i_0} \) lies in \([\mu_{i_0}(\alpha_{i_0} + 1), \delta_{i_0} + \alpha_{i_0}]\).

Then, we identify \( m_r \) as \( h_{k1}, 1 \leq k \leq M \). Since \( \beta_{i_0} \geq \mu_{i_0}(\alpha_{i_0} + 1) \), no product of polynomials with \( z_{i_0} \)-degrees \( (\mu_{i_0} - 1)(\alpha_{i_0} + 1) \) and \( \alpha_{i_0} \) yields \( z_{\beta_{i_0}} \). Further, since no monomial \( z^\gamma \) can be produced by two different combinations

\[
z^\gamma = g_{1k0}h_{k01} = g_{1k1}h_{k11}, \tag{6.42}
\]

as the degrees of the monomials \( h_{k1} \) are placed \( \alpha + 1 \) apart and \( g_{1k} \in \mathcal{P}_\alpha(\mathbb{F}[z_1, \ldots, z_n]) \), we have

\[
\sum_{k=1}^{M} g_{1k}h_{k1} = 0 \Rightarrow g_{1k} = 0, \forall k \tag{6.43}
\]

as desired.

**Case 2:** Let \( \hat{r}_{i_0} \) be such that \( \beta_{i_0} \) lies in \([(\hat{r}_{i_0} - 1)(\alpha_{i_0} + 1), \hat{r}_{i_0}(\alpha_{i_0} + 1))\).
Then, we let
\[
\hat{m}_r = \begin{cases} 
m_r, & r_{i_0} < \hat{r}_{i_0}, \\
m_r(1 + z_{i_0}), & r_{i_0} = \hat{r}_{i_0}, \\
m_r z_{i_0}, & r_{i_0} > \hat{r}_{i_0}. 
\end{cases}
\] (6.44)

(Intuitively, we are moving the sequence of monomials 1 down in the direction of the \(i_0\)-th component in \(\mathbb{Z}_n^+\).) Now,
\[
\delta_{i_0} > (\mu_{i_0} - 1)(\alpha_{i_0} + 1) \quad (6.45)
\]
\[
\Rightarrow \delta_{i_0} \geq (\mu_{i_0} - 1)(\alpha_{i_0} + 1) + 1 \quad (6.46)
\]
\[
\Rightarrow \hat{m}_r \in \mathcal{P}_\delta(\mathbb{F}[z_1, \ldots, z_n]) \quad (6.47)
\]

Next, we reindex \(\hat{m}_r\) to obtain \(h_{k_1}, 1 \leq k \leq M\). Since each of the monomials in any \(h_{k_1}\) are placed at least \(\alpha\) units away from those in others, if \(g_{1k} \in \mathcal{P}_\alpha(\mathbb{F}[z_1, \ldots, z_n])\),
\[
1 \leq k \leq M,
\]
\[
\sum_{k=1}^{M} g_{1k} h_{k_1} = 0 \quad \Rightarrow \quad g_{1k} = 0, \forall k \quad (6.48)
\]
as desired. Further, \(z^\beta\) cannot be achieved as in equation (6.35) because all \(\hat{m}_r\) which can yield \(z^\beta\) have two monomial terms, both of which involve \(z_{i_0}\), and we have the desired result.

We can now state a partial converse to the generic effective Nullstellensatz. Note that the proof is almost identical to that of Proposition 31.

**Proposition 35** Let \(N = 1\). Suppose \(M \in \mathbb{N}\) and \(\delta \in \mathbb{Z}_n^+\) are given. Let \(\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}_n^+\) satisfy equations (6.33) and (6.34). Then, there exists a nonempty Zariski open subset \(V\) of \(\mathcal{M}_{M \times 1}(\mathcal{P}_\delta(\mathbb{F}[z_1, \ldots, z_n]))\) such that for every \(H\) in \(V\) and for every \(z^\beta \in \mathcal{P}_{\delta + \alpha}(\mathbb{F}[z_1, \ldots, z_n])\), the equation
\[
G \mathcal{H} = z^\beta
\]
cannot be solved for $\mathcal{G} \in \mathcal{M}_{1 \times M}(\mathcal{P}_n(\mathbb{F}[z_1, \ldots, z_n]))$.

**Proof:** Consider

$$T^n_{\delta, \alpha}(\mathcal{H}) \text{vec}(\mathcal{G}) = \text{vec}(\mathcal{G}\mathcal{H})$$  \hspace{1cm} (6.49)

whence, as in equation (6.25),

$$T^n_{\delta, \alpha}(\mathcal{H}) : \mathbb{F}^{M\alpha^*} \longrightarrow \mathbb{F}^{(\delta + \alpha)^*}$$  \hspace{1cm} (6.50)

Since equation (6.34) holds,

$$\prod_{i=1}^{n} \left( \frac{\delta_i + \alpha_i + 1}{\alpha_i + 1} \right) > M$$  \hspace{1cm} (6.51)

$$\Rightarrow \prod_{i=1}^{n} (\delta_i + \alpha_i + 1) > M \prod_{i=1}^{n} (\alpha_i + 1).$$  \hspace{1cm} (6.52)

Thus, the domain of $T^n_{\delta, \alpha}(\mathcal{H})$ has lower dimension than its range. By Proposition 34, \exists $\hat{\mathcal{H}}$ which has full rank and

$$\text{vec}(z^\beta) \notin \text{range}(T^n_{\delta, \alpha}(\hat{\mathcal{H}}))$$  \hspace{1cm} (6.53)

$$\Rightarrow \text{rank} \left( \text{vec}(z^\beta) \ T^n_{\delta, \alpha}(\hat{\mathcal{H}}) \right) = M \prod_{i=1}^{n} (\alpha_i + 1) + 1$$  \hspace{1cm} (6.54)

Thus, $\mathcal{A}$ has full rank and has atleast one submatrix $X$ of size $M \prod_{i=1}^{n} (\alpha_i + 1) \times M \prod_{i=1}^{n} (\alpha_i + 1)$ whose determinant is nonzero. Hence $\text{det}(X)$ is a *nonzero* polynomial in the coefficients of the elements of $\mathcal{H}$. Let $V = \mathbb{F}^{n} - \mathbb{V}$(det$(X)$). It is possible for $T^n_{\delta, \alpha}(\mathcal{H})$ to be rank deficient only if the determinant polynomial vanishes, *i.e.*, $\mathcal{H} \notin V$ since $\mathcal{A}$ is rank deficient when $\text{vec}(z^\beta) \notin \text{range}(T^n_{\delta, \alpha}(\mathcal{H}))$, whence we reach the desired conclusion for a generic $\mathcal{H}$. 

$\blacksquare$
6.6 A Generic Effective Nullstellensatz for Matrices

We now extend the results of the preceding two sections to the case when \( N > 1 \).

Proposition 36 Suppose \( M, N \in \mathbb{N} \) and \( \delta \in \mathbb{Z}_n^+ \) are given. Let \( \alpha \in \mathbb{Z}_n^+ \) be such that

\[
N \prod_{i=1}^n \left( \frac{\delta_i + \alpha_i + 1}{\alpha_i + 1} \right) \leq M. \tag{6.55}
\]

Then, there exists a nonempty Zariski open subset \( V \) of \( \mathcal{M}_{M \times N}(\mathcal{P}_\delta(\mathbb{F}[z_1, \ldots, z_n])) \) such that for every \( \mathcal{H} \in V \) and for every \( \mathcal{I} \in \mathcal{M}_{1 \times N}(\mathcal{P}_{\delta+\alpha}(\mathbb{F}[z_1, \ldots, z_n])) \), the equation

\[
\mathcal{G}\mathcal{H} = \mathcal{I}
\]

can be solved for \( \mathcal{G} \in \mathcal{M}_{1 \times M}(\mathcal{P}_{\alpha}(\mathbb{F}[z_1, \ldots, z_n])) \).

Proof: Let

\[
\lambda \triangleq \prod_{i=1}^n \left( \frac{\delta_i + \alpha_i + 1}{\alpha_i + 1} \right). \tag{6.56}
\]

Now,

\[
T_{\delta,\alpha}^n(\mathcal{H}) : \mathbb{F}^{M\lambda^*} \longrightarrow \mathbb{F}^{N(\delta+\alpha)^*} \tag{6.57}
\]

From equation (6.55),

\[
N \prod_{i=1}^n \left( \frac{\delta_i + \alpha_i + 1}{\alpha_i + 1} \right) \leq M \tag{6.58}
\]

\[
\Rightarrow M \prod_{i=1}^n (\alpha_i + 1) \geq N \prod_{i=1}^n (\delta_i + \alpha_i + 1), \tag{6.59}
\]

whence the range of \( T_{\delta,\alpha}^n(\mathcal{H}) \) has lower dimension than its domain. By the same argument used in the proof of Proposition 31, all we need for the desired result is an example \( \mathcal{H} \) such that

\[
\text{range}(T_{\delta,\alpha}^n(\mathcal{H})) = \mathbb{F}^{N(\delta+\alpha)^*}. \tag{6.60}
\]
By Proposition 29, \( \exists \hat{h}_{k_1} \in \mathcal{P}_\mathcal{B}(\mathbb{F}[z_1, \ldots, z_n]) \), \( 1 \leq k \leq \lambda \) such that 

\[
\forall w \in \mathcal{P}_{\mathcal{B}+\alpha}(\mathbb{F}[z_1, \ldots, z_n]), \ \exists g^w_{1k} \in \mathcal{P}_\alpha(\mathbb{F}[z_1, \ldots, z_n]), \ 1 \leq k \leq \lambda \text{ for which }
\sum_{k=1}^{M} g^w_{1k} h_{k1} = w.
\]

(6.61)

Consider the matrix

\[
\mathcal{H} = \begin{pmatrix}
h_{11} \\
\vdots \\
h_{\lambda1} \\
h_{11} \\
\vdots \\
h_{\lambda1} \\
\vdots \\
\vdots \\
0
\end{pmatrix}
\]

(6.62)

where the empty spaces correspond to 0 elements. Then, \( \exists G_{\mathcal{I}} \),

\[
G_{\mathcal{I}} = \begin{pmatrix}
g_{11,1} & \cdots & g_{1\lambda,1} \\
\vdots & \ddots & \vdots \\
g_{11,2} & \cdots & g_{1\lambda,2} \\
\vdots & \ddots & \vdots \\
g_{11,N} & \cdots & g_{1\lambda,N}
\end{pmatrix}
\]

(6.63)

such that

\[
(g_{11,i} \ \cdots \ g_{1\lambda,i}) \begin{pmatrix} h_{11} \\ \vdots \\ h_{\lambda1} \end{pmatrix} = i\text{-th element of } \mathcal{I}
\]

(6.64)

\[
\Rightarrow G_{\mathcal{I}} \mathcal{H} = \mathcal{I}
\]

(6.65)

Since \( \mathcal{I} \) is arbitrary, \( T^{\alpha}_{\mathcal{B},\mathcal{B}}(\mathcal{H}) \) has full rank yielding the desired result.

\[
\text{Proposition 37 Suppose } M, N \in \mathbb{N} \text{ and } \delta \in \mathbb{Z}_n^+ \text{ are given. Let } \alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}_n^+ \text{ be such that }
\]

\[
N \prod_{i=1}^{n} \left\lfloor \frac{\delta_i + \alpha_i + 1}{\alpha_i + 1} \right\rfloor \geq M
\]

(6.66)
and

\[ N \prod_{i=1}^{n} \left\lceil \frac{\delta_i + \alpha_i + 1}{\alpha_i + 1} \right\rceil > M. \] (6.67)

Then, there exists a nonempty Zariski open subset \( V \) of \( \mathcal{M}_{M \times N}(\mathcal{P}_\delta(F[z_1, \ldots, z_n])) \) such that for every \( \mathcal{H} \in V \) and for every \( \beta \in \mathbb{Z}_n^+ \), the equation

\[ \mathcal{G} \mathcal{H} = (0 \cdots z^\beta \cdots 0) \] (6.68)

cannot be solved for \( \mathcal{G} \in \mathcal{M}_{1 \times M}(\mathcal{P}_\alpha(F[z_1, \ldots, z_n])) \).

**Proof:**

Repeat the proof of Proposition 36 *mutatis mutandis.*

Propositions 36 and 37 give identical necessary and sufficient conditions for the generic invertibility of \( \mathcal{H} \) under the following conditions:

1. \( N \) divides \( M \), and

2. for each \( i \), \( \alpha_i + 1 \) divides \( \delta_i \).

Signal processing applications of the criteria for necessity and sufficiency are considered in Chapter 9.
CHAPTER 7

MULTIVARIATE SZEGRÖ-LEVINSON ALGORITHM

The algorithm from Chapter 4 can be used to compute the inverse of a known system $\mathcal{H}$ when the minimum number of taps in the equalizer is the maximum allowed. However, the algorithm has the disadvantage of being doubly exponential or higher (in the size of $\mathcal{H}$) in computational complexity [40]. An alternative algorithm from [8] has a reduced computational complexity but is still doubly exponential. In this chapter, we consider an alternative computational technique with drastically reduced complexity that is applicable only for single input multiple output systems.

The algebraic computational techniques in [8, 40] do not make use of a priori knowledge of the bounds on the orders of the equalizer. However, as we have seen in Chapter 6, generic bounds are available (in multidegree form) which can be used to compute the equalizer. Given bounds on the order of the equalizer, we generalize the Levinson algorithm to compute the inverse of the nested Toeplitz matrix in equation (4.2) when $N = 1$, partially answering question 5 from Chapter 1.
7.1 Preliminaries

Suppose $\delta = (\delta_1, \ldots, \delta_n) \in \mathbb{Z}_n^+$ is given. Then consider the following lexicographic ordering of the set

$$\Gamma = \{ \beta \in \mathbb{Z}_n^+ | \beta_k \leq \delta_k, \forall k \}$$

(7.1)

given by

$$\beta < \lambda \iff \exists l, \beta_l < \lambda_l, \beta_k = \lambda_k, \forall k > l$$

(7.2)

(In words, the leftmost index varies the fastest.) Let $\bar{\beta}$ denote the predecessor of $\beta$ in the monomial ordering given by equation (7.2).

Let $\iota(z)$ be a polynomial of degree $\delta$. When evaluated on the hypercircle in $\mathbb{C}^n$, $\iota$ can be written as follows:

$$\iota(z) = \sum_{\beta \leq \delta} \iota_\beta z^\beta$$

(7.3)

$$\iota(\theta_1, \ldots, \theta_n) = \sum_{\beta \leq \delta} \iota_\beta \exp(i(\theta_1 \beta_1 + \cdots + \theta_n \beta_n))$$

(7.4)

Interpreting $\iota$ as the multidimensional Fourier transform of the multidimensional filter $\iota_\beta$, one obtains the following squared magnitude response of $\iota_\beta$:

$$\mu = |\iota(\theta_1, \ldots, \theta_n)|^2$$

$$= \sum_{\beta \leq \delta} \left( c_\beta^* \exp(i(\theta_1 \beta_1 + \cdots + \theta_n \beta_n)) + c_\beta \exp(-i(\theta_1 \beta_1 + \cdots + \theta_n \beta_n)) \right)$$

(7.5)

Since $\mu \geq 0$ on the hypercircle, we can interpret it as a measure; in particular, since the support of $\mu$ is nontrivial, no nontrivial polynomial vanishes $\mu$ a.e., and hence $z^\beta$, $\beta \in \mathbb{Z}_n^+$ are linearly independent. For any nontrivial polynomial $g \in \mathbb{C}[z_1, \ldots, z_n]$,

$$\int |g|^2 d\mu > 0$$

(7.6)
since \(|g|^2|\ell|^2\) is positive a.e. on the hypercircle. We define the following inner product on \(\mathcal{P}_\delta(\mathbb{C}[z_1, \ldots, z_n])\):

\[
\langle z^\beta, z^\gamma \rangle_{\mathcal{C}_\delta} = \int \exp(i((\gamma_1 - \beta_1)\theta_1 + \cdots + (\gamma_n - \beta_n)\theta_n))d\mu = c_{\gamma - \beta} \quad (7.7)
\]

where the integral is taken over the \(n\)-fold hypercircle (the meaning of the subscript \(\mathcal{C}_\delta\) will become clear later). The inner product is linear in the second term and conjugate linear in the first term. The inner product has the following important property. If \(\lambda \in \mathbb{Z}_n^+\),

\[
\langle z^\lambda g_1(z), g_2(z) \rangle_{\mathcal{C}_\delta} = \langle g_1(z), z^{-\lambda} g_2(z) \rangle_{\mathcal{C}_\delta} \quad (7.8)
\]

since \((z^\lambda)^* = z^{-\lambda}\) on the hypercircle. In particular,

\[
\|z^\lambda g(z)\|_{\mathcal{C}_\delta}^2 = \|g(z)\|_{\mathcal{C}_\delta}^2 \quad (7.9)
\]

On the finite dimensional vector space \(\mathbb{C}^{\delta^*}\) (isomorphic to \(\mathcal{P}_\delta(\mathbb{C}[z_1, \ldots, z_n])\), see Chapter 6 for details), the inner product can be expressed as follows:

\[
\langle.,.\rangle_{\mathcal{C}_\delta} : \mathbb{C}^{\delta^*} \times \mathbb{C}^{\delta^*} \longrightarrow \mathbb{C} \quad (7.10)
\]

\[
\langle x, y \rangle_{\mathcal{C}_\delta} \triangleq x^HC_\delta y \quad (7.11)
\]

where \((.)^H\) denotes the conjugate transpose and \(C_\delta\) is the \(\delta^* \times \delta^*\) matrix defined by

\[
e^H_\beta C_\delta e_\gamma = [C_\delta]_{\beta,\gamma} = c_{\gamma - \beta} \quad (7.12)
\]

where \(e_\beta\) is the vectorized form of \(z^\beta\) in \(\mathbb{C}^{\delta^*}\), the elements of whose natural basis we will index by the elements of \(\Gamma\). By equation (7.6), \(C_\delta\) is positive definite. (Because

\[\text{As in Chapter 6, } \mathcal{P}_\delta(\mathbb{C}[z_1, \ldots, z_n]) \text{ denotes the set of all } n\text{-variate polynomials (with complex coefficients).}\]
the Fejer-Riesz theorem does not extend to the multivariate case, we cannot make a bijective identification of all measures on the hypercircle with all positive definite nested Toeplitz matrices.)

\( \mathcal{C}_\delta \) is a nested Toeplitz matrix with nesting level \( n \), where the “number of blocks” at level \( k \) is \( \delta_{n-k+1} \). For example, if \( n = 3 \) and \( \delta = (1, 1, 2) \), \( \mathcal{C}_\delta \) is a 12 \( \times \) 12 matrix, arranged in the form of a 3 \( \times \) 3 block-Toeplitz matrix, where each block is a 2 \( \times \) 2 block-Toeplitz matrix, whose blocks in turn are 2 \( \times \) 2 Toeplitz matrices:

\[
\mathcal{C}_\delta = \begin{pmatrix}
c_{000} & c_{100} & c_{010} & c_{110} & c_{001} & c_{101} & c_{011} & c_{111} & c_{002} & c_{102} & c_{012} & c_{112} \\
c_{100} & c_{000} & c_{010} & c_{110} & c_{001} & c_{101} & c_{011} & c_{111} & c_{002} & c_{102} & c_{012} & c_{112} \\
c_{010}^* & c_{100}^* & c_{000} & c_{110} & c_{001} & c_{101} & c_{011} & c_{111} & c_{002} & c_{102} & c_{012} & c_{112} \\
c_{110}^* & c_{010}^* & c_{000} & c_{110} & c_{001} & c_{101} & c_{011} & c_{111} & c_{002} & c_{102} & c_{012} & c_{112} \\
c_{001}^* & c_{101}^* & c_{010}^* & c_{110} & c_{000} & c_{100} & c_{010} & c_{110} & c_{001} & c_{101} & c_{011} & c_{111} \\
c_{101}^* & c_{011}^* & c_{010}^* & c_{110} & c_{000} & c_{100} & c_{010} & c_{110} & c_{001} & c_{101} & c_{011} & c_{111} \\
c_{011}^* & c_{101}^* & c_{011}^* & c_{110} & c_{000} & c_{100} & c_{010} & c_{110} & c_{001} & c_{101} & c_{011} & c_{111} \\
c_{111}^* & c_{011}^* & c_{011}^* & c_{110} & c_{000} & c_{100} & c_{010} & c_{110} & c_{001} & c_{101} & c_{011} & c_{111} \\
c_{002}^* & c_{102}^* & c_{012}^* & c_{112} & c_{000} & c_{100} & c_{010} & c_{110} & c_{001} & c_{101} & c_{011} & c_{111} \\
c_{102}^* & c_{012}^* & c_{012}^* & c_{112} & c_{000} & c_{100} & c_{010} & c_{110} & c_{001} & c_{101} & c_{011} & c_{111} \\
c_{012}^* & c_{102}^* & c_{012}^* & c_{112} & c_{000} & c_{100} & c_{010} & c_{110} & c_{001} & c_{101} & c_{011} & c_{111} \\
c_{112}^* & c_{012}^* & c_{012}^* & c_{112} & c_{000} & c_{100} & c_{010} & c_{110} & c_{001} & c_{101} & c_{011} & c_{111}
\end{pmatrix}
\] (7.13)

where \((.)^*\) denotes\(^7\) conjugation. Note that the first row contains all the values needed to populate the entire matrix.

Finally, we define the flipping operator \( R_u \). Let \( u \) be a positive integer. Suppose

\[
g(z) = \sum_{\beta \leq (\delta_1, \ldots, \delta_{n-1}, u)} g_\beta z^\beta. \quad (7.14)
\]

Then, \( R_u \) is defined as follows:

\[
R_u : \mathcal{P}(\delta_1, \ldots, \delta_{n-1}, u)(\mathbb{C}[z_1, \ldots, z_n]) \to \mathcal{P}(\delta_1, \ldots, \delta_{n-1}, u)(\mathbb{C}[z_1, \ldots, z_n]) \quad (7.15)
\]

\[
R_u g(z) = \sum_{\beta \leq (\delta_1, \ldots, \delta_{n-1}, u)} g_\beta^* z^{\beta}. \quad (7.16)
\]

\(^7\)When \( \delta \in \mathbb{Z}_n^+ \), \( \delta^* \) will continue to denote the number of monomials in \( \delta \) as in equation (6.6). The meaning of the operator should be clear from context.
Note that \( R_u^2 \) is the identity. The flipping operator \( R_u \), while not linear, does have the following important property.

**Lemma 38**

\[
\langle g, h \rangle_{C_\delta} = \langle R_u h, R_u g \rangle_{C_\delta}
\]

**Proof:**

\[
\langle g, h \rangle_{C_\delta} = \left\langle \sum_{\beta \leq (\delta_1, \ldots, \delta_{n-1}, u)} g_\beta z^\beta, \sum_{\lambda \leq (\delta_1, \ldots, \delta_{n-1}, u)} h_\lambda z^\lambda \right\rangle_{C_\delta}
\]

\[
= \sum_{\beta \leq (\delta_1, \ldots, \delta_{n-1}, u)} \sum_{\lambda \leq (\delta_1, \ldots, \delta_{n-1}, u)} g_\beta h_\lambda \langle z^\beta, z^\lambda \rangle_{C_\delta}
\]

\[
= \sum_{\beta \leq (\delta_1, \ldots, \delta_{n-1}, u)} \sum_{\lambda \leq (\delta_1, \ldots, \delta_{n-1}, u)} g_\beta h_\lambda c_{\lambda-\beta}
\]

Letting \( \hat{\beta} = (\delta_1, \ldots, \delta_{n-1}, u) - \beta \) and \( \hat{\lambda} = (\delta_1, \ldots, \delta_{n-1}, u) - \lambda \),

\[
\langle g, h \rangle_{C_\delta} = \sum_{\hat{\beta} \leq (\delta_1, \ldots, \delta_{n-1}, u)} \sum_{\hat{\lambda} \leq (\delta_1, \ldots, \delta_{n-1}, u)} (R_u g)^\hat{\beta} (R_u h)^\hat{\lambda} c_{\hat{\beta}-\hat{\lambda}}
\]

\[
= \langle R_u h, R_u g \rangle_{C_\delta}
\]

In particular,

\[
\langle g, h \rangle_{C_\delta} = 0 \Rightarrow \langle R_u h, R_u g \rangle_{C_\delta} = 0
\]

Further, if \( g \) has degree at most \( \beta \leq (\delta_1, \ldots, \delta_{n-1}, u) \), the lowest degree monomial appearing in \( R_u g \) is \( z^{(\delta_1, \ldots, \delta_{n-1}, u) - \beta} \).

### 7.2 Multivariate Szegő Recursion

We call the orthogonalization of the monomials

\[
\{z^\beta : \beta \in \Gamma\}
\]

63
with respect to the inner product $\langle \cdot, \cdot \rangle_{C_\delta}$ as the $n$-variate Szegő orthogonal polynomials corresponding to $C_\delta$ (or equivalently, to $\mu$). The objective of this section is to obtain recursion formulas for generating the Szegő polynomials. We will consider $C_\delta$ as fixed. We denote by $\Phi_\beta$ the monic polynomial obtained by orthogonalizing $z^\beta$ with respect to all the monomials preceding $z^\beta$ in the monomial ordering from equation (7.2).

The Levinson algorithm [38] can be used to compute the Szegő polynomials when $n = 1$. The Levinson algorithm (and the underlying Szegő recurrence relation) were generalized to the case $n = 2$ in [33]. Suppose the generalized Szegő-Levinson algorithm for dimension $n - 1$ is known. Then the $n$-dimensional generalized Szegő-Levinson algorithm can be formulated as in the sequel.

**Basic step:** The orthogonal polynomials for the "first layer" can be computed using the $n - 1$-dimensional algorithm, i.e.,

$$\Phi_\beta, \quad \beta \leq (\delta_1, \ldots, \delta_{n-1}, 0) \quad (7.22)$$

can be computed using the $n - 1$-dimensional algorithm since none of the monomials involved have a factor containing $z_n$.

**Induction step:** Now suppose (induction hypothesis) that the $u$-th layer has been completed, i.e., the polynomials

$$\Phi_\beta, \quad \beta \leq (\delta_1, \ldots, \delta_{n-1}, u) \quad (7.23)$$

have been computed. Then, since the $(\delta_1, \ldots, \delta_{n-1}, u)^*$ monomials

$$\{z^\beta : \beta \leq (\delta_1, \ldots, \delta_{n-1}, u)\}$$

form a basis for $\mathcal{P}_{(\delta_1, \ldots, \delta_{n-1}, u)}(\mathbb{C}[z_1, \ldots, z_n])$, so does the orthogonal set

$$\{\Phi_\beta : \beta \leq (\delta_1, \ldots, \delta_{n-1}, u)\}$$

64
since any orthogonal set is linearly independent, and since any linearly independent set whose cardinality is the same as the dimension of the underlying vector space is a basis. Hence, the orthogonal set

\[ \{ R_u \Phi_\beta : \beta \leq (\delta_1, \ldots, \delta_{n-1}, u) \} \]

is also a basis for \( P_{(\delta_1, \ldots, \delta_{n-1}, u)}(\mathbb{C}[z_1, \ldots, z_n]) \), where we have used equation (7.20) to obtain \( \langle R_u \Phi_\beta, R_u \Phi_\lambda \rangle_{C_\delta} = 0 \). By construction, \( z^\beta \) is a linear combination of \( \{ \Phi_\gamma \} \) for all \( \gamma \leq \beta \). Hence, \( \forall \beta < \lambda \),

\[ \langle \Phi_\beta, \Phi_\lambda \rangle_{C_\delta} = 0 \]

\[ \Rightarrow \langle z^\beta, \Phi_\lambda \rangle_{C_\delta} = 0 \] (7.24)

\[ \Rightarrow \langle R_u (z^\beta), R_u \Phi_\lambda \rangle_{C_\delta} = 0 \]

using equation (7.19). Thus,

\[ \langle z^{(\delta_1, \ldots, \delta_{n-1}, u) - \beta}, R_u \Phi_\lambda \rangle_{C_\delta} = 0, \quad \forall \beta < \lambda. \] (7.25)

Now suppose \( \lambda \) is in the next layer, i.e., \( \lambda = (\lambda_1, \ldots, \lambda_{n-1}, u + 1) \), and that \( \Phi_\beta \) have been computed for all \( \beta < \lambda \). Since \( \Phi_{(\lambda_1, \ldots, \lambda_{n-1}, u)} \) is monic with degree \( (\lambda_1, \ldots, \lambda_{n-1}, u) \), \( z_n \Phi_{(\lambda_1, \ldots, \lambda_{n-1}, u)} \) is monic with degree \( (\lambda_1, \ldots, \lambda_{n-1}, u + 1) \). Since \( \Phi_{(\lambda_1, \ldots, \lambda_{n-1}, u+1)} \) is also monic,

\[ \Phi_{(\lambda_1, \ldots, \lambda_{n-1}, u+1)} - z_n \Phi_{(\lambda_1, \ldots, \lambda_{n-1}, u)} \]

has degree at most \( \hat{\lambda} \). Thus, it can be expressed as follows:

\[ \Phi_{(\lambda_1, \ldots, \lambda_{n-1}, u+1)} - z_n \Phi_{(\lambda_1, \ldots, \lambda_{n-1}, u)} = \sum_{\beta \leq \hat{\lambda}} \tilde{s}_\beta \Phi_\beta \]

\[ = \sum_{\beta \leq (\delta_1, \ldots, \delta_{n-1}, u)} \tilde{s}_\beta \Phi_\beta + \sum_{(\delta_1, \ldots, \delta_{n-1}, u) \leq \beta < \lambda} \tilde{s}_\beta \Phi_\beta \]

\[ = \sum_{\beta \leq (\delta_1, \ldots, \delta_{n-1}, u)} -s_{\lambda, \beta} R_u \Phi_\beta + \sum_{(\delta_1, \ldots, \delta_{n-1}, u) \leq \beta < \lambda} -r_{\lambda, \beta} \Phi_\beta \] (7.26)
for some (as yet undetermined) complex constants $s_{\lambda, \beta}$ and $r_{\lambda, \beta}$, where we have used the fact that the flipped orthogonal polynomials form a basis for the set in the first term. Equation (7.26) can be rewritten as

$$z_n \Phi_{(\lambda_1, \ldots, \lambda_{n-1}, u)} = \Phi_{(\lambda_1, \ldots, \lambda_{n-1}, u+1)} + \sum_{\beta \leq (\delta_1, \ldots, \delta_{n-1}, u)} s_{\lambda, \beta} R_u \Phi_{\beta} + \sum_{(\delta_1, \ldots, \delta_{n-1}, u) < \beta < \lambda} r_{\lambda, \beta} \Phi_{\beta}$$

(7.27)

Since the Szegő polynomials in the $u + 1$st layer are orthogonal to all polynomials in the $u$th layer and lower, all the polynomials on the right hand side of equation (7.27) are orthogonal to each other. Hence, we may obtain the coefficients $s_{\lambda, \beta}$ and $r_{\lambda, \beta}$ as follows:

$$\langle \Phi_{\beta}, z_n \Phi_{(\lambda_1, \ldots, \lambda_{n-1}, u)} \rangle_{C_\delta} = r_{\lambda, \beta} \langle \Phi_{\beta}, \Phi_{\beta} \rangle_{C_\delta}, \quad (\delta_1, \ldots, \delta_{n-1}, u) < \beta < \lambda$$

(7.28)

$$\Rightarrow r_{\lambda, \beta} = \frac{\langle \Phi_{\beta}, z_n \Phi_{(\lambda_1, \ldots, \lambda_{n-1}, u)} \rangle_{C_\delta}}{\| \Phi_{\beta} \|_{C_\delta}^2}, \quad (\delta_1, \ldots, \delta_{n-1}, u) < \beta < \lambda$$

(7.29)

and

$$\langle R_u \Phi_{\beta}, z_n \Phi_{(\lambda_1, \ldots, \lambda_{n-1}, u)} \rangle_{C_\delta} = s_{\lambda, \beta} \langle R_u \Phi_{\beta}, R_u \Phi_{\beta} \rangle_{C_\delta}, \quad \beta \leq (\delta_1, \ldots, \delta_{n-1}, u)$$

(7.30)

$$\Rightarrow s_{\lambda, \beta} = \frac{\langle R_u \Phi_{\beta}, z_n \Phi_{(\lambda_1, \ldots, \lambda_{n-1}, u)} \rangle_{C_\delta}}{\| \Phi_{\beta} \|_{C_\delta}^2}, \quad \beta \leq (\delta_1, \ldots, \delta_{n-1}, u)$$

(7.31)

as the other terms vanish.

The inner product on the left hand side of equation (7.30) can be rewritten using equation (7.8) as

$$\langle z_n^{-1} R_u \Phi_{\beta}, \Phi_{(\lambda_1, \ldots, \lambda_{n-1}, u)} \rangle_{C_\delta}$$

Since the lowest degree monomial appearing in $R_u \Phi_{\beta}$ is $z^{(\delta_1, \ldots, \delta_{n-1}, u) - \beta}$, $(z_n^{-1}) R_u \Phi_{\beta}$ remains a polynomial if $\beta \leq (\delta_1, \ldots, \delta_{n-1}, u - 1)$, and has degree at most $(\delta_1, \ldots, \delta_{n-1}, u - \ldots$
1) since \( R_u \Phi_\beta \) has degree at most \((\delta_1, \ldots, \delta_{n-1}, u)\). In this case, since \( \Phi_{(\lambda_1, \ldots, \lambda_{n-1}, u)} \) is orthogonal to polynomials of lower degree,

\[
\langle z_n^{-1} R_u \Phi_\beta, \Phi_{(\lambda_1, \ldots, \lambda_{n-1}, u)} \rangle_{C_\delta} = 0, \quad \forall \beta \leq (\delta_1, \ldots, \delta_{n-1}, u - 1)
\]

(7.32)

Hence, the \( n \)-variate Szegő-Levinson recursion assumes the following form:

\[
\Phi_{(\lambda_1, \ldots, \lambda_{n-1}, u+1)} = z_n \Phi_{(\lambda_1, \ldots, \lambda_{n-1}, u)} - \sum_{(\delta_1, \ldots, \delta_{n-1}, u-1) < \beta \leq (\delta_1, \ldots, \delta_{n-1}, u)} s_{\lambda, \beta} R_u \Phi_\beta
\]

\[
- \sum_{(\delta_1, \ldots, \delta_{n-1}, u) < \beta < \lambda} r_{\lambda, \beta} \Phi_\beta
\]

(7.33)

Thus, the computation of the Szegő polynomials for layer \( u + 1 \) depends only on the the polynomials from layers \( u \) and \( u + 1 \).

Further computational savings may be obtained by noting the following:

1. The computation of \( \| \Phi_\beta \|_{C_\delta}^2 \) efficiently may be accomplished in one of two ways.

From equation (7.33), we obtain

\[
\| z_n \Phi_{(\lambda_1, \ldots, \lambda_{n-1}, u)} \|_{C_\delta}^2 = \| \Phi_{(\lambda_1, \ldots, \lambda_{n-1}, u+1)} \|_{C_\delta}^2 + \sum_{(\delta_1, \ldots, \delta_{n-1}, u-1) < \beta \leq (\delta_1, \ldots, \delta_{n-1}, u)} |s_{\lambda, \beta}|^2 \| R_u \Phi_\beta \|_{C_\delta}^2
\]

(7.34)

whence

\[
\| \Phi_{(\lambda_1, \ldots, \lambda_{n-1}, u)} \|_{C_\delta}^2 = \| \Phi_{(\lambda_1, \ldots, \lambda_{n-1}, u+1)} \|_{C_\delta}^2 + \sum_{(\delta_1, \ldots, \delta_{n-1}, u-1) < \beta \leq (\delta_1, \ldots, \delta_{n-1}, u)} |s_{\lambda, \beta}|^2 \| \Phi_\beta \|_{C_\delta}^2
\]

(7.35)
It is then simple to compute $\| \Phi(\lambda_1, \ldots, \lambda_{n-1}, u+1) \|_{C_δ}^2$:

$$\| \Phi(\lambda_1, \ldots, \lambda_{n-1}, u+1) \|_{C_δ}^2 = \| \Phi(\lambda_1, \ldots, \lambda_{n-1}, u) \|_{C_δ}^2$$

$$- \sum_{(\delta_1, \ldots, \delta_{n-1}, u-1)<\beta\leq(\delta_1, \ldots, \delta_{n-1}, u)} |\langle \Phi(\beta, z_n \Phi(\lambda_1, \ldots, \lambda_{n-1}, u) \rangle_{C_δ} |^2$$

$$- \sum_{(\delta_1, \ldots, \delta_{n-1}, u)<\beta<\lambda} |\langle R_u \Phi(\beta, z_n \Phi(\lambda_1, \ldots, \lambda_{n-1}, u) \rangle_{C_δ} |^2$$

(7.36)

since the inner products under the summations needed to be computed in equation (7.33). The other method for computing $\| \Phi_\beta \|_{C_δ}^2$ follows directly from its definition:

$$\| \Phi_\beta \|_{C_δ}^2 = \langle \Phi_\beta, \Phi_\beta \rangle_{C_δ}$$

$$= \langle z^{\beta}, \Phi_\beta \rangle_{C_δ}$$

$$= \sum_{\gamma\leq\beta} (\Phi_\beta)_{\gamma} \langle z^{\beta}, z^{\gamma} \rangle_{C_δ}$$

$$= \sum_{\gamma\leq\beta} (\Phi_\beta)_{\gamma} c_{\gamma-\beta}$$

(7.37)

2. Whenever an inner product is computed with $\Phi_\beta$, one sets to zero the coefficients of all monomials of degree lower than $\beta$. This simple rule more than halves the computation required on a naive implementation of (7.33). Similarly, whenever an inner product is computed with $R_u \Phi_\beta$, one sets to zero the coefficients of all monomials of degree between $(\delta_1, \ldots, \delta_{n-1}, u) - \beta$ and $(\delta_1, \ldots, \delta_{n-1}, u)$.

### 7.3 Computation of Inverse

From the monic Szegő orthogonal polynomials, we obtain the orthonormal polynomials:

$$\phi_\beta = \frac{\Phi_\beta}{\| \Phi_\beta \|_{C_δ}}, \quad \forall \beta \leq \delta$$

(7.38)
Given the orthonormal polynomials \( \phi_\beta \) for all \( \beta \leq \delta \), we may compute the inverse of \( C_\delta \) easily.

**Proposition 39**

\[
C_\delta^{-1} = SS^H \tag{7.39}
\]

where

\[
S = (\text{vec}(\phi_0) \; \cdots \; \text{vec}(\phi_\delta)) \tag{7.40}
\]

**Proof:**

\[
\langle \phi_\beta, \phi_\gamma \rangle_{C_\delta} = \text{vec}(\phi_\beta)^H C_\delta \text{vec}(\phi_\gamma) = \begin{cases} 
0 & \text{if } \beta \neq \gamma \\
1 & \text{if } \beta = \gamma 
\end{cases} \tag{7.41}
\]

whence

\[
S^H C_\delta S = I_{\delta^*}
\]

\[
\Rightarrow C_\delta^{-1} = SS^H
\]  

Note that \( S \) is an upper triangular matrix, and hence \( SS^H \) can be computed with \( O((\delta^*)^2) \) multiplications and additions. For simplicity, we have proved Proposition 39 without using the theory of reproducing kernels; see [32].

In order to avoid computing square roots, the algorithm from Proposition 39 should typically be implemented in the following manner:

\[
C_\delta^{-1} = S_1 S_2^H
\]

\[
S_1 = (\text{vec}(\Phi_0) \; \cdots \; \text{vec}(\Phi_\delta)) \tag{7.43}
\]

\[
S_2 = \begin{pmatrix}
\text{vec} \left( \frac{\Phi_0}{\|\Phi_0\|_C} \right) & \cdots & \text{vec} \left( \frac{\Phi_\delta}{\|\Phi_\delta\|_C} \right)
\end{pmatrix}
\]

To compute one orthogonal polynomial using equation (7.33), we require the following steps:
• \((\delta_1 + 1)(\delta_2 + 1) \cdots (\delta_{n-1} + 1))^2(u + 1)\) multiplications for each of the last two terms of the recursion

• \(((\delta_1 + 1)(\delta_2 + 1) \cdots (\delta_{n-1} + 1))^2(u + 1)\) multiplications for computing each \(s_{\lambda, \beta}\) and for each \(r_{\lambda, \beta}\)

• \(2(\delta_1 + 1)(\delta_2 + 1) \cdots (\delta_{n-1} + 1)\) multiplications for computing the norm

Thus, the computation of all the orthogonal polynomials requires \(O(((\delta_1 + 1)(\delta_2 + 1) \cdots (\delta_{n-1} + 1))^3(\delta_n + 1)^2)\) multiplications. Further, since \(S\) is triangular, the computation of \(SS^H\) requires \(O(((\delta_1 + 1)(\delta_2 + 1) \cdots (\delta_n + 1))^2)\) multiplications. Hence the computation of the inverse requires altogether \(O(((\delta_1 + 1)(\delta_2 + 1) \cdots (\delta_{n-1} + 1))^3(\delta_n + 1)^2)\) multiplications. Letting \(\delta_1, \ldots, \delta_{n-1}\) be fixed, we see that \(O(\delta_n^2)\) multiplications are required to compute the inverse, in contrast to the brute force technique which requires \(O(\delta_n^3)\) multiplications.

### 7.4 Equalizer Computation

Suppose that we are given \(\delta \in \mathbb{Z}_n^+\) and \(x, y \in \mathbb{C}[z]\), and are required to find \(g \in \mathcal{P}_\alpha(\mathbb{C}[z_1, \ldots, z_n])\) such that \(y \odot g\) is the best least squares approximation to \(x\), i.e., the Wiener filter of order \(\delta\). Thus, we minimize the norm

\[
\|y \odot g - c\| \quad (7.44)
\]

It is well known that the solution satisfies the orthogonality condition (also known as normal equations):

\[
K_{yy} \odot g = K_{xy} \quad (7.45)
\]
where \( K_{yy} \) is the autocorrelation of \( y \), and \( K_{xy} \) is the crosscorrelation between \( x \) and \( y \). Thus we solve

\[
T_{n,\alpha}(K_{yy}) \text{vec}(g) = \text{vec}(K_{xy})
\]  

(7.46)

where \( T_{n,\alpha}(K_{yy}) \) is a nested Toeplitz matrix of the form (7.12). We may then compute the inverse of \( T_{n,\alpha}(K_{yy}) \) using Proposition 39. Note that the autocorrelation and the crosscorrelation can be computed efficiently using the \( n \)-dimensional fast Fourier transform.

Suppose we would like to equalize a single-input multiple-output system. Then, we can form a single-input single-output system in \( n + 1 \) dimensions by stacking the given filters in the following manner:

\[
y(z_1, \ldots, z_{n+1}) = \sum_{i=1}^{M} z_{n+1}^{i-1} h_i(z_1, \ldots, z_{n+1})
\]  

(7.47)

\[
g(z_1, \ldots, z_{n+1}) = \sum_{i=1}^{M} z_{n+1}^{i-1} g_i(z_1, \ldots, z_{n+1})
\]  

(7.48)

We can now apply the procedure outlined above to compute \( g \).

The orthogonal polynomials developed in this chapter are closely related to the matrix orthogonal polynomials from [13, 15], where the additional structure of nested Toeplitz matrices (in contrast to block Toeplitz matrices) is ignored. We use the extra structure to provide efficient initialization, and to avoid the theory of matrix-valued measures altogether. We also do not consider reverse predictor polynomials. It may be possible to combine our approach with that of [13, 15] to obtain efficient algorithms for the multiple input problem.
VOLUME III

Applications & Examples
CHAPTER 8

SAR CALIBRATION

We begin the applications part of this dissertation by computing the minimum number of test targets required for the identification of ultra-wide band polarimetric synthetic aperture radars. In this chapter, we provide a rigorous mathematical basis for the long held belief among engineers that three targets are sufficient for the identification of the system under reciprocity assumptions. We also show that three targets are necessary. The technique used in chapter answers question (6) from Chapter 1.

8.1 SAR System Model

Polarimetric diversity in synthetic aperture radar (SAR) measurements yields improved detection and characterization of man-made targets in clutter [22, 44, 62]. Two linearly independent polarizations are used on transmit and receive to observe the $2 \times 2$ polarimetric scattering matrix describing reflectivity at each scene location. However, physically realizable radar systems exhibit channel cross-talk and gain imbalances which distort the polarimetric measurements; therefore, polarimetric calibration is required to equalize this distortion.

Established calibration techniques [64, 67] adopt a system model for distortion that is independent of frequency and radar aspect angle. Accordingly, equalization
of the “flat fading” model is achieved by a matrix multiply directly applied, pixel by pixel, to the four coregistered polarimetric images.

However, emerging wide-band radar systems transmit a fractional bandwidth\(^8\) exceeding 25% and tens of degrees of antenna beam width, thereby rendering the flat fading model inadequate. For example, 8 cm resolution SAR imagery is obtained by an X-band system with 10 GHz center frequency, 40% fractional bandwidth, and a 12 degree aperture. Similarly, foliage and ground penetrating SAR imagery with 60 cm resolution can be obtained at UHF-band wavelengths using 50% fractional bandwidth and a 35 degree aperture. For these wide-band systems, the magnitude response, phase response and polarization rotation of antennas varies significantly as a function of frequency and angle. Consequently, frequency and angle dependent, or “frequency selective,” equalization must be used for calibration.

For wide-band, wide-angle radar systems, the combination of data collection, polarimetric antenna response, and SAR image processing is well modelled as a linear shift-invariant (LSI) distortion acting on the desired images of scene reflectivity \([21, 52, 61]\). The physical sources of distortion include nonideal transmit pulse, antenna response, phase center displacement, cable delays and amplifier gains. As a result of SAR image processing, these nonideal effects essentially disperse energy only in a neighborhood of a pixel. Therefore, we model the multiple-input, multiple-output (MIMO) LSI operator as a finite impulse response (FIR) MIMO filter.

We seek a MIMO FIR filter to calibrate, or equalize, the multi-channel images. A FIR equalizer is desirable because of inherent stability, robustness against quantization effects, limited error propagation, and ease of implementation. While the

\(^8\)Fractional bandwidth is defined as system bandwidth divided by center frequency.
flat fading approach can be applied independently to thousands of samples in the frequency-Doppler plane [21, 56], a FIR parameterization of the equalization filter-bank provides a large and physically meaningful dimensionality reduction.

A system model for polarimetric wide-band SAR is given in [21, 52]. For range much larger than image diameter, the image is related to the desired scene reflectivity by a shift-invariant two-dimensional filtering operation

\[ y(u, r) = h(u, r) *_u *_r x(u, r) \]  

(8.1)

where \((u, r)\) denotes the cross-range and down-range scene location. The distortion, \(h\), incorporates system effects including antenna response, image processing, transmit pulse, phase center displacements, cable delays, and amplifier gains. For reciprocal scattering, the desired image \(x\) is vector-valued with \(N = 3\) values per pixel (see figure 8.1). The uncalibrated polarimetric image, \(y\), represents \(M = 4\) pixels per location. For example, in a horizontal-vertical polarization basis, images are formed from each combination of transmit and receive polarization to yield \(y_{HH}, y_{HV}, y_{VH},\) and \(y_{VV}\). Thus, 12 two-dimensional FIR filters comprise the MIMO equalizer \(h(u, r)\) in equation (8.1).

### 8.2 Calibration Target Selection

In this section, we will consider the problem of identifying \(H\) through calibration targets. Since \(M = 4\), \(N = 3\) and \(n = 2\), by Theorem 20, \(H\) is generically invertible. For the rest of this section, we will assume that the given \(H\) is invertible.

Since \(H\) is invertible, its image is a free module of rank 3 by Theorem 24. Further, since \(\mathbb{C}[z]\) is commutative, the free module \(\text{Im}(H)\) has invariant basis number. Thus,
to identify the system completely, we need to observe the action of $\mathcal{H}$ on three $\mathbb{C}[z]$-linearly independent elements of $\mathbb{C}[z]^3$. (This extends our intuition from linear algebra to commutative free modules.) Thus, we have the following proposition.

**Proposition 40** Three $\mathbb{C}[z_1, z_2]$-linearly independent targets are necessary and sufficient for identification of a reciprocal polarimetric synthetic aperture radar system.

To check whether a set of three targets is $\mathbb{C}[z_1, z_2]$-linearly independent, check that the $3 \times 3$ matrix formed by the response of the targets has a nonzero determinant.

One issue of practical importance not addressed by this formulation is the sensitivity of the distortion system estimates to noise. One must choose “sufficiently different” test targets for robust estimation.
CHAPTER 9

EQUALIZER ORDERS

Theorem 28 from Chapter 6 provides a nearly sharp bound on the multidegree of the equalizer $\mathcal{G}$ for a generic $\mathcal{H}$. In this chapter, we outline the motivation for the use of multidegrees rather than total degrees as the apposite metric for signal processing applications. We consider the conditions under which the generic bounds are tight and show that generic multivariate systems behave as well as univariate systems. We also provide examples illustrating the use of the generic bounds.

9.1 Total Degree Versus Multidegree

Given only that $\mathcal{H}$ is invertible and that $\deg(\mathcal{H}) = \delta$, the problem of estimating the minimum orders of an equalizer stated as follows. Given $\deg(\mathcal{H}) = \delta$, and $\alpha \in \mathbb{Z}_{+}^{n}$, does there exist $\mathcal{G}$ with $\deg(\mathcal{G}) \leq \alpha$? If so, is it the smallest such $\alpha$? The smallest $\alpha$ can be found from [8]:

$$|\alpha| = (N|\delta|)^{O(n)}$$  \hspace{1cm} (9.1)

In signal processing applications, the multidegree $\delta$ is typically known for the forward system (e.g., maximum delay spread, or maximum energy leakage area in SAR).

\textsuperscript{9}The main results of this chapter can be found in [49].
However, the existing algebraic formulations (e.g., [8]) take only the total degree $|\delta|$ rather than $\delta$ into account, and the equalizer orders in equation (9.1) leave open the choice of $\alpha$. Further, total degrees do not correspond to the number of equalizer taps. For the 2D example in figure 9.1, the total degree for the given rectangular filtermask contains other points on $\mathbb{Z}^2$ as well. Hence, existing bounds based on total degrees are ill-suited to signal processing considerations, and here we present bounds on the multi-degree, $\delta$. Figure 9.1 shows a case when the equalizer mask for a generic system $\mathcal{H}$ is smaller than the mask for $\mathcal{H}$ itself.

The size of the class of all generically equalizable systems can be characterized as follows using Theorem 28.
Theorem 41  Given the number of inputs $N$, the number of outputs $M$, and the dimension $n$ of a random system, invertibility is guaranteed generically iff

$$\left( \frac{M}{N} \right) \geq n + 1. \quad (9.2)$$

from Theorem 20. Further, if equation (9.2) does not hold, a generic system is not invertible.

Since invertibility of a random system is guaranteed only generically, one may ask whether restriction to a generic subset of equalizable systems would reduce guaranteed equalizer orders. In other words, since we throw out a negligible fraction of systems as nonequalizable, could we also throw out a negligible set of pathological systems which require large equalizers in order to obtain smaller equalizer orders for the remainder? From Theorem 28 (restated here for convenience), the answer is yes.

Theorem 42  Suppose the number of inputs $N \in \mathbb{N}$, the number of outputs $M \in \mathbb{N}$ and the order of the forward system $\delta \in \mathbb{Z}_n^+$ are given, and $M \geq 2^n N$. Let $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}_n^+$ be such that

$$N \prod_{i=1}^{n} \left\lceil \frac{\delta_i + \alpha_i + 1}{\alpha_i + 1} \right\rceil \leq M. \quad (9.3)$$

Then, for a generic $\mathcal{H}$, for every $N \times N$ matrix $\mathcal{I}$ with $\deg(\mathcal{I}) \leq \delta + \alpha$, the equation

$$\mathcal{G}\mathcal{H} = \mathcal{I}$$

can be solved with $\deg(\mathcal{G}) \leq \alpha$. Conversely, if $\alpha$ is such that

$$N \prod_{i=1}^{n} \left\lfloor \frac{\delta_i + \alpha_i + 1}{\alpha_i + 1} \right\rfloor \geq M \quad (9.4)$$

79
and

\[ N \prod_{i=1}^{n} \left\lceil \frac{\delta_i + \alpha_i + 1}{\alpha_i + 1} \right\rceil > M, \quad (9.5) \]

for a generic \( \mathcal{H} \), for any diagonal \( N \times N \) matrix \( \mathcal{I} \) whose main diagonal entries are monomials (delays), there does not exist a \( \mathcal{G} \) with \( \deg(\mathcal{G}) \leq \alpha \) such that \( \mathcal{G}\mathcal{H} = \mathcal{I} \).

Whereas generic invertibility of \( \mathcal{H} \) requires \( M\)-choose-\( N \) greater than \( n \), Theorem 42 establishes generic bounds on the order of the inverse filters provided \( M \geq 2^n N \). Thus, applicability of the inverse order bounds requires at least as many output channels as required for generic invertibility.

Specialized to the case of 1-dimensional signals, Theorem 42 can be restated.

**Corollary 43** Let \( \mathcal{H} \) be generic with \( \deg(\mathcal{H}) \leq \delta_1 \) and \( M \geq 2N \). Then, if

\[ \alpha_1 \geq \frac{\delta_1}{\left\lfloor \frac{M}{N} \right\rfloor} - 1, \quad (9.6) \]

an equalizer \( \mathcal{G} \) of order \( \alpha_1 \) exists. If

\[ \alpha_1 < \frac{\delta_1}{\left\lfloor \frac{M}{N} \right\rfloor} - 1, \text{ and } \alpha_1 \leq \frac{\delta_1}{\left\lceil \frac{M}{N} \right\rceil} - 1, \quad (9.7) \]

an equalizer \( \mathcal{G} \) of order \( \alpha_1 \) does not exist.

In the language of MIMO communications channels, Corollary 43 has the following interpretation. Let each of the \( MN \) channels have delay spread not exceeding \( \delta_1 \). Suppose further that the number of receive channels, after fractional sampling, is no fewer than twice the number of transmit channels. Then, a delay of

\[ \alpha_1 \geq \frac{\delta_1}{\left\lfloor \frac{M}{N} \right\rfloor} - 1, \quad (9.8) \]
is sufficient to almost surely guarantee the existence of an equalizer. Further, the same filter orders suffice for producing a delayed version of the desired input signal, for any delay up to \( \delta_1 + \alpha_1 \). Note that \( \alpha_1 + 1 \) denotes the number of taps in each of \( MN \) equalization filters. In particular, an equalizer delay of (significantly) less than the delay spread of the channel suffices.

Returning to the multidimensional signal case, \( n > 1 \), equation (9.3) is easily manipulated to yield a sufficient condition that more readily reveals the dependence of required inverse orders on the number of outputs.

**Corollary 44** Suppose \( \delta \) is as in Theorem 42. Then,

\[
\alpha_i + 1 = \frac{\delta_i}{\left( \frac{M}{N} \right)^{\frac{1}{n}}} - 1, \quad i = 1, \ldots, n
\]  

(9.9)

is sufficient for the generic existence of an equalizer.

Thus, the total number of required filter taps decreases linearly with the ratio, \( M/N \), of outputs to inputs.

### 9.2 Tight Bounds

The inequality in equation 9.3 of Theorem 42 becomes both necessary and sufficient provided there is no difference between the floor and ceiling values given in equations (9.4) and (9.5). In this case, equality in equation 9.3 yields a unique relation between \( \alpha \) and \( \delta \), and therefore is very useful in channel order estimation and blind equalization. Thus, when equation (9.3) is necessary and sufficient, Theorem 42 provides a multivariate MIMO extension to the iterative rank-based determination of \( \delta \) given, e.g., in [58, 60].
In this section, we consider two special cases for which Theorem 42 provides a tight converse: when \((\alpha_i + 1)\) divides \(\delta_i\) and, for one-dimensional signals, when \(N\) divides \(M\). As an aside, we conjecture that the condition in equation (9.4) is superfluous and hence equation (9.3) is actually both necessary and sufficient; however, the condition is used in our proof of Theorem 42 as a counting device.

### 9.2.1 One-dimensional signals

For one-dimensional signals, consider the special case in which the number of outputs \(M\) is an integer multiple of the number of inputs \(N\). In this case, the range of \(\alpha_1\) not covered by Theorem 42,

\[
\left[ \left\lfloor \frac{\delta_1}{M/N} \right\rfloor - 1, \left\lceil \frac{\delta_1}{M/N} \right\rceil - 2 \right]
\]

becomes empty, and we obtain a necessary and sufficient condition on the equalizer orders.

**Corollary 45** Let \(M = LN\), \(1 < L \in \mathbb{N}\) and \(n = 1\). Let \(\mathcal{H}\) be generic with \(\deg(\mathcal{H}) \leq \delta_1\). Then, given \(w\) with \(\deg(w) \leq \delta_1 + \alpha_1\),

\[
\alpha_1 = \left\lceil \frac{\delta_1}{L-1} \right\rceil - 1 \quad (9.10)
\]

is necessary and sufficient for the existence of a \(\mathcal{G}\) with \(\deg(\mathcal{G}) \leq \alpha_1\) such that

\[
\mathcal{G}\mathcal{H} = \text{diag} \left(0 \cdots w \cdots 0\right) \quad (9.11)
\]

Further, if \(\beta_1 < \alpha_1\), generically no matrix of the form \(\text{diag} \left(0 \cdots z_1^\gamma \cdots 0\right)\) can be obtained as \(\mathcal{G}\mathcal{H}\) when \(\deg(\mathcal{G}) \leq \beta_1\).

For a single-input, multiple-output system in one variable, Corollary 45 reduces to the bound presented in [29]. The bound from [29] was implicitly assumed (via properties of the Sylvester matrix) in [1, 58] to estimate the channel length.
Corollary 46 (Harikumar & Bresler, [29]) Let $N = 1$ and $n = 1$. Let $H$ be generic with $\deg(H) \leq \delta_1$. Then, given $w$ with $\deg(w) \leq \delta_1 + \alpha_1$,

$$\alpha_1 = \left\lceil \frac{\delta_1}{M-1} \right\rceil - 1$$ (9.12)

is necessary and sufficient for the existence of a $G$ with $\deg(G) \leq \alpha_1$ such that

$$GH = \text{diag}(0 \cdots w \cdots 0).$$ (9.13)

Further, if $\beta_1 < \alpha_1$, generically no matrix of the form $\text{diag}(0 \cdots z_1^\gamma \cdots 0)$ can be obtained as $GH$ when $\deg(G) \leq \beta_1$.

9.2.2 $n$-dimensional signals

Next, for signals of arbitrary dimension $n$, the special case of $(\alpha_i + 1)$ divides $\delta_i$, $i = 1, \ldots , n$, yields a necessary and sufficient condition on the equalizer orders.

Corollary 47 Suppose $M, N \in \mathbb{N}$ and $\delta \in \mathbb{Z}_n^+$ are given. Let $\alpha = (\alpha_1, \ldots , \alpha_n) \in \mathbb{Z}_n^+$ be such that $\alpha_i + 1$ divides $\delta_i$ for every $i \leq n$. If

$$N \prod_{i=1}^{n} \left( \frac{\delta_i + \alpha_i + 1}{\alpha_i + 1} \right) \leq M,$$ (9.14)

then for a generic $H$, for every $N \times N$ matrix $I$ with $\deg(I) \leq \delta + \alpha$, the equation

$$GH = I$$

can be solved with $\deg(G) \leq \alpha$. If not, for a generic $H$, for any diagonal $N \times N$ matrix $I$ whose main diagonal entries are monomials (delays), there does not exist a $G$ with $\deg(G) \leq \alpha$ such that $GH = I$.

Remark 48 Note that equation (9.14) can be rewritten as

$$N \frac{(\delta + \alpha)^*}{\alpha^*} \leq M$$ (9.15)

where we can see the dependence on the number of taps rather than on total degrees.
Remark 49 Note that the condition in equation (9.3) essentially depends only on the factors of the product \((\alpha_1 + 1) \cdots (\alpha_n + 1)\) which is the size of the equalizer. Since we can control the allocation of the factors during the design of the equalizer, we can impose further constraints on \(\alpha\) in order to check for equalizability. When \(\delta^*\) becomes large and has a large number of prime factors, it becomes divisible by large sets of possible values for \(\alpha\). As \(\delta^*\) becomes large, the density of primes becomes small, whence the theorem provides necessary and sufficient conditions with high probability for large systems.

When the bounds are tight, and equality is achieved in equation (9.14), we can trace the steps of the proof of Theorem 42 to show that \(T_{\delta,\alpha}^n(H)\) is a full rank square matrix, indicating that the minimal order equalizer for any particular delay is unique.

9.3 Delays and Equalization

In many applications, it is not necessary to equalize exactly. It is sufficient to recover a delayed, or shifted, version of the signal. For univariate systems, it is well known [35] that allowing for delays does not change the order of the equalizer if the system is equalizable; however, it may (and typically does) allow more robust computation. In the case of multivariate systems however, allowing for delays dramatically increases the order of the equalizers [41]:

\[
\text{totaldeg}(G) \leq cN \text{totaldeg}(H)^{2^{O(n)}}
\]

However, Theorem 42 assures us that the orders do not increase for a generic system matrix. Thus, for almost all systems, one may choose to obtain delayed recovery of signals without incurring a penalty in the orders of the equalizer.
Suppose that we wish to minimize processing delay (which is equal to the order of the inverse filters) without sacrificing computation. By Theorem 42, increasing the number of outputs does not increase the computational complexity; however, it does decrease the processing delay. Hence, for a sufficiently large number of outputs, the inputs required may be recovered by an instantaneous mixture of the outputs.

9.4 Examples

In this section, we present two examples to illustrate consequences of Theorem 42. First, we demonstrate the striking reduction in equalizer orders provided by adopting generic bounds, rather than existing bounds [8, 35, 50] that hold for all systems, including the pathological special cases. Second, we illustrate that the inverse filters may have a significantly smaller filter order than the forward system.

9.4.1 Generic versus absolute bounds

Consider a 2-input 12-output system which operates on images whose order is \( \delta = (6, 14) \). Then \( N = 2, M = 12, \) and \( n = 2 \). If \( \alpha = (5, 6) \), then

\[
2 \left\lceil \frac{6 + 5 + 1}{5 + 1} \right\rceil \left\lceil \frac{14 + 6 + 1}{6 + 1} \right\rceil \leq 12
\] (9.17)

whence equation (9.3) is satisfied and the inputs are recoverable for a generic system. If \( \alpha = (4, 6) \) or \( \alpha = (5, 5) \), the conditions in equations (9.4) and (9.5) are satisfied, whence the inputs are not recoverable even if we allow for delays. In this case, the equalizer filters have atmost \( \alpha^* = 42 \) taps. In contrast, the bound from [8] gives equalizers with 7261 taps.

However, \((5, 6)\) is not the only possible smallest filter size. For example, \( \alpha = (2, 13) \) satisfies equation (9.3), and both \( \alpha = (1, 13) \) and \( \alpha = (2, 12) \) satisfy equations (9.4)
and (9.5), whence smaller equalizer sizes are generically not allowable. The choice of \( \alpha \) is now application-dependent. If the deconvolution is implemented in hardware via FFTs, it may be advantageous to choose \( \alpha = (5, 6) \) as it can be implemented using only length 8 FFTs.

### 9.4.2 Filter versus equalizer orders

Consider a two-input six-output blind source separation problem with one-dimensional inputs and outputs. Suppose that the six outputs are corrupted by additive noise and that the maximum delay spread, \( \delta_1 \), is known \textit{a priori}. One seeks to blindly estimate a FIR equalizer according to a design criterion, such as minimum mean squared error subject to a complexity constraint. Typically, the equalizer must be zero-forcing in the noiseless case, \textit{e.g.}, for unbiased signal estimates.

Estimation procedures for the equalizer require the order of the equalizer. From Theorem 42, the minimum order of the equalizer is generically

\[
\alpha_1 \geq \frac{\delta_1}{\left\lceil \frac{M}{N} \right\rceil} - 1 = \frac{\delta_1}{\left\lfloor \frac{2}{N} \right\rfloor} - 1 = \frac{\delta_1}{2} - 1
\]

Further, the filter order \( \alpha_1 \) suffices for recovery of any delayed version of the inputs, with delay not exceeding \( \delta_1 + \alpha_1 \). Note that, in this case, the equalizer order is \textit{less than one-half} the order of the forward system. Further, from Corollary 45, we note that no smaller equalizer order will suffice, generically. However, an equalizer of larger order may provide advantage, for example, in mean squared error. Thus, Theorem 42 provides a starting point for the design trade-off between complexity (namely, filter length) and performance.
VOLUME IV

Appendices
APPENDIX A

UNSOLVED PROBLEMS

The ultimate goal of developing a unified theory of MIMO FIR equalizers is to estimate the equalizer and/or the inputs blindly. The tools developed in the second part of this monograph are insufficient to solve the blind estimation problem in its full generality. The assumption of a generic MIMO FIR distortion system must be augmented by other assumptions (in the general case) to make the problem of blind estimation well-posed. In this chapter, we present\(^\text{10}\) some unsolved problems, the solutions to which we believe would aid in tackling the blind estimation problem.

A.1 Signal Subspace Estimation Based on Rank

In traditional blind estimation approaches, the input is typically modeled statistically, and the system model usually involves the addition of Gaussian noise (white or colored) at the observation point. Given knowledge of the statistics of the input and the noise, one obtains an estimator minimizing an appropriately chosen cost function typically by forcing the equalized output to have some statistical profile. In contrast, we model our input signals as deterministic (but unknown) which pass through a generic MIMO FIR distortion system, and observe the outputs. Note that we do not

\(^{10}\)This chapter uses results and their proofs from all preceding chapters.
have an additive noise component in our model; this model is useful in high SNR situations, and in providing initial points for iterative solution techniques.

Consider the outputs of a generic single-input multiple-output (SIMO) system:

\[ y_j = h_j x, \quad 1 \leq j \leq M \]  

(A.1)

Suppose that \( M \geq 2^n \), and \( \deg(h_j) \leq \delta \). Then, by Theorem 28, for any \( \alpha \in \mathbb{Z}_n^+ \) satisfying inequality (6.23), we can find an equalizer (for any arbitrary delay), \( i.e., \) for any \( \beta \leq \alpha + \delta \), we can find \( g_{\beta,j} \) such that

\[ \sum_j g_{\beta,j} h_j = z^\delta \]  

(A.2)

\[ \sum_j g_{\beta,j} y_j = z^\delta x \]  

(A.3)

Since \( x \) is a factor of all \( y_j \), it must be a factor of all \( \mathbb{C}[z] \)-linear combinations of the form (A.3). Hence,

\[ \text{rank} \left( T_{n,\delta,\alpha}(h_1) \quad T_{n,\delta,\alpha}(h_2) \quad \cdots \quad T_{n,\delta,\alpha}(h_M) \right) = (\delta + \alpha)^* \]  

(A.4)

\[ \text{rank} \left( T_{n,\delta,\alpha}(y_1) \quad T_{n,\delta,\alpha}(y_2) \quad \cdots \quad T_{n,\delta,\alpha}(y_M) \right) = (\delta + \alpha)^* \]  

(A.5)

Suppose that the conjecture following Theorem 28 is true, \( i.e., \) inequality (6.3) is superfluous in the statement of Theorem 28. (Note that the conjecture is true for the cases considered in Section 9.2.) Then, for any \( \alpha \in \mathbb{Z}_n^+ \) not satisfying inequality (6.23), and for any \( \beta \leq \alpha + \delta \), we cannot find an equalizer satisfying equation (A.3). Thus, for such \( \alpha \),

\[ \text{rank} \left( T_{n,\delta,\alpha}(y_1) \quad T_{n,\delta,\alpha}(y_2) \quad \cdots \quad T_{n,\delta,\alpha}(y_M) \right) < (\delta + \alpha)^* \]  

(A.6)

Suppose the distortion system is not equalizable simply by instantaneous linear combinations of the outputs, \( i.e., \) \( \min \deg(G) > 0 \). Then, we have the following algorithm
for estimating deg(x). Define a sequence $\beta^{(k)} \in \mathbb{Z}_n^+$ such that $\beta^{(k)} < \beta^{(k+1)}$, and

$$\beta^{(0)} = 0$$  \hspace{1cm} (A.7)

$$\lim_{k \to \infty} \beta^{(k)}_i = \infty, \quad 1 \leq i \leq n$$  \hspace{1cm} (A.8)

so that the set

$$\{ \gamma : \gamma \leq \beta^{(k)} \}$$  \hspace{1cm} (A.9)

eventually covers the entire space $\mathbb{Z}_n^+$. We compute

$$\text{rank} \begin{pmatrix} T_n^{\alpha}(y_1) & T_n^{\alpha}(y_2) & \cdots & T_n^{\alpha}(y_M) \end{pmatrix}_{\alpha = \beta^{(k)}} = \infty$$  \hspace{1cm} (A.10)

Once we reach $\alpha = \beta^{(k)}$ satisfying equation (6.23) (checked using the rank criteria from equations (A.5) and (A.6)), we have an upper bound on the minimum $\alpha$ satisfying equation (6.23). To obtain $x$, we use projections of the range space of the matrix in equation (A.5) as follows. Let $\Pi_\beta$ be the projection operator

$$\text{range}(\Pi_\beta) = \text{span}\{ z^\gamma : \gamma \leq \beta \}$$  \hspace{1cm} (A.11)

We now “shrink” the possible size of $x$ to the minimum:

$$\xi = \arg \min_{\gamma \leq \beta^{(k)}} \text{range}(\Pi_\beta) \cap \text{range} \begin{pmatrix} T_n^{\alpha}(y_1) & T_n^{\alpha}(y_2) & \cdots & T_n^{\alpha}(y_M) \end{pmatrix}_{\alpha = \beta^{(k)} \neq \emptyset}$$  \hspace{1cm} (A.12)

The minimum exists because the range of the matrix contains only multiples of $x$. Thus,

$$\Pi_\xi \begin{pmatrix} T_n^{\alpha}(y_1) & T_n^{\alpha}(y_2) & \cdots & T_n^{\alpha}(y_M) \end{pmatrix}_{\alpha = \beta^{(k)}} = \text{span}(x)$$  \hspace{1cm} (A.13)

from which we obtain $x$ subject to a constant.
In the algorithm proposed above, we required the knowledge of $\delta$ in order to check for $\beta^{(k)}$ satisfying equation (6.23). In the case of communications channels ($n = 1$), we simply check whether

$$\text{rank} \left( T_{\delta,\alpha}^n(y_1) \ T_{\delta,\alpha}^n(y_2) \ \cdots \ T_{\delta,\alpha}^n(y_M) \right)_{\alpha = \beta}$$

$$- \text{rank} \left( T_{\delta,\alpha}^n(y_1) \ T_{\delta,\alpha}^n(y_2) \ \cdots \ T_{\delta,\alpha}^n(y_M) \right)_{\alpha = \beta + 1} > 1$$

(A.14)

Analogous techniques can be used in the multidimensional case. Thus, the entire algorithm works solely on rank and projection computations. This may seem like an unnecessarily expensive way to compute the greatest common divisor of the observed outputs, but has the feature that it may now be extended to output signals corrupted by noise. Assuming a high signal to noise ratio, we estimate ranks via singular decompositions, and ignore small singular values. Thus, blind estimation of $x$ is possible in the single input case, if the conjecture following Theorem 28 can be proven.

In the multiple-input case, the problem becomes much more involved. The primary difficulty is as follows. The algorithm stated above uses the fact that the largest common factor of the observed outputs is the input. In particular, the range space projections cannot contain a smaller vector. In the multiple-input case, the range space contains $\mathbb{C}[z]$-linear combinations of the inputs, which could be smaller than the inputs themselves, and hence the projection onto the smallest subspace does not work. Further assumptions on the input and/or noise model are necessary to make the blind MIMO estimation problem well-posed.

A.2 Multivariate Orthogonal Polynomials

The recursion relation for the Szegö orthogonal polynomials presented in Chapter 7 suffers from a major deficiency. Since the recursive scheme was developed by
induction on the last dimension, the polynomial structure in the other dimensions was not exploited, save for the initialization. It may be possible to develop relationships between the orthogonal polynomials developed for each dimension, which could be utilized to further reduce computation.

Key related issues in eliminating redundant computation are the development of multivariate split algorithms and of matrix-valued multivariate orthogonal polynomial theory. The algorithm from Chapter 7 works with complex-valued data. Split algorithms [17] would help reduce computation with real-valued data. Recurrence relations for matrix-valued multivariate polynomials should help develop fast computational techniques for multiple input systems as well.

The theory of Szegő univariate orthogonal polynomials has deep connections with several areas of modern mathematics: Caratheodory and m- functions [9], Schur algorithm & Wall polynomials [27], non-Euclidean geometry [18], etc. It is interesting to note that the theory of multivariate Szegő orthogonal polynomials has been neglected (primarily due to the lack of a Fejer-Riesz theorem in the multivariate case) in the math literature. Investigation of multivariate extensions of the connections of univariate orthogonal polynomials might prove fruitful.
APPENDIX B

NOTATION

\( (\delta)^* \) Number of taps in filter of size \( \delta \) \hspace{1cm} Equation (6.6)
\( \langle \cdot, \cdot \rangle_{c_\delta} \) Szegö inner product \hspace{1cm} Equation (7.12)
\( \emptyset \) Empty set
\( \alpha \) Multidegree of \( G \) \hspace{1cm} Section 6.3
\( \delta \) Multidegree of \( H \) \hspace{1cm} Section 6.3
\( \Phi_\beta \) Monic Szegö orthogonal polynomial \hspace{1cm} Section 7.2
\( \phi_\beta \) Szegö orthonormal polynomial \hspace{1cm} Equation (7.38)
\( C_\delta \) Positive definite nested Toeplitz matrix \hspace{1cm} Section 7.1
\( D_i \) \( N \times N \) minors of \( H \) \hspace{1cm} Theorem 16
\( e_j \) \( j \)th element of the natural basis \hspace{1cm} Equation (4.17)
\( G \) Equalizer (inverse system) \hspace{1cm} Equation (3.7)
\( g_{ij} \) Element of \( G \) (component of inverse filter) \hspace{1cm} Section 3.1.2
\( H \) Distortion filter (forward system) \hspace{1cm} Equation (3.7)
\( h_{ij} \) Element of \( H \) (component of forward filter) \hspace{1cm} Section 3.1.2
\( I_N \) \( N \times N \) identity matrix \hspace{1cm} Section 3.1.2
\( M \) Number of outputs \hspace{1cm} Section 3.1.2
\( N \) Number of inputs \hspace{1cm} Section 3.1.2
\( n \) Dimension of convolution space \hspace{1cm} Equation (3.1)
\( P_\delta(\mathbb{F}[z_1, \ldots, z_n]) \) Polynomials over \( \mathbb{F} \) of degree at most \( \delta \) \hspace{1cm} Equation (6.5)
\( R_u \) Flipping operator \hspace{1cm} Equation (7.15)
\( r_{\lambda,\beta} \) Szegö recursion coefficient \hspace{1cm} Equation (7.27)
\( s_{\lambda,\beta} \) Szegö recursion coefficient \hspace{1cm} Equation (7.27)
\( T_{\delta,\alpha}^n \) Matrix-vector multiplication operator \hspace{1cm} Section 6.3
\( x_i \) Inputs \hspace{1cm} Section 3.1.2
\( y_i \) Outputs \hspace{1cm} Section 3.1.2
\( z \) Point in \( n \)-space \hspace{1cm} Equation (2.5)
\( \mathbb{Z}_n^+ \) Space of non-negative integer \( n \)-tuples \hspace{1cm} Equation (2.6)
BIBLIOGRAPHY


