

APPROXIMATE GRÖBNER BASES
A BACKWARDS APPROACH

(Thesis format: Monograph)

By
Robin J. Scott

GRADUATE PROGRAM IN APPLIED MATHEMATICS

A THESIS SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF SCIENCE

FACULTY OF GRADUATE STUDIES
THE UNIVERSITY OF WESTERN ONTARIO
LONDON, ONTARIO, CANADA

© Robin J. Scott, 2006

THE UNIVERSITY OF WESTERN ONTARIO
FACULTY OF GRADUATE STUDIES

CERTIFICATE OF EXAMINATION

Supervisor

Dr. Greg Reid

Examiners

Dr. Mark Giesbrecht

Dr. David Jeffrey

Dr. Stephen Watt

The thesis by

Robin Jennifer Scott

entitled:

Approximate Gröbner Bases - a Backwards Approach

is accepted in partial fulfillment of the
requirements for the degree of
Master of Science

Date: _____

Chair of the Thesis Examination Board

Abstract

The main result of this thesis is to give a method for approximating the Gröbner basis of an approximate polynomial system.

The Gröbner basis of a polynomial system is arguably the most fundamental object of exact computation polynomial algebra, as it answers many of the important questions of commutative algebra, such as ideal membership and computation of the Hilbert polynomial. It is traditionally computed using variants of Buchberger's algorithm. Here, we take a backwards approach, and show that a Gröbner basis can be computed using the Hilbert polynomial and another important basis from the jet theory of partial differential equations: an involutive basis. This direction, motivated by approximate systems, will allow us to avoid the strict monomial orderings and ordered elimination (reduction) strategies, at the heart of Buchberger-type methods, which are usually numerically unstable.

For the the computation of exact bases for an ideal near to the one from which we began, we make avid use of structured (numerical) linear algebra. Additionally, we introduce approximate leading terms and an approximate reduced row echelon form. Neither of these require Gaussian elimination, unlike the exact case.

Keywords: *Approximate Coefficients, Gröbner Bases, Hilbert Polynomial, Partial Differential Equations, Involutive Systems, Nearby Systems, Numerical Linear Algebra, Polynomial Algebra, Reduced Row Echelon Form, Singular Value Decomposition, Structured Matrices.*

In 1875 Fanny Crosby, blinded as an infant by an incompetent doctor, wrote the since-cherished phrase:

“To God be the glory, great things He hath done.”

Acknowledgements

With absolute sincerity, I thank Greg Reid, my advisor and mentor. I am so very thankful for your kind patience, encouragement, and inspiration; through two summers of undergraduate research assistantship, and over these past two years of my M.Sc. It has been a such a privilege to work with you. You are a gifted teacher; I never expected to learn so much, or to truly enjoy what I have learned.

I respectfully thank Karin Gatermann, who so enthusiastically introduced me to Gröbner bases. Her interest in framing the theory of involutive systems in terms of commutative algebra, and the Hilbert function, influenced the way of development of this work. I hope that this will adequately represent her intentions, and insights.

To Lihong Zhi, I am much indebted. I thank you for sharing your understanding and experience, especially regarding convergence methods and nearby approximate polynomial systems. Much success is due to discussions at the MMRC, Beijing, to which you graciously invited our group.

The results of this thesis are part of a joint project in which my fellow student, Wenyuan Wu, has been deeply involved. Always ready and willing to provide ideas and assistance - you are a trooper! Thank you.

I thank the members of ORCCA, especially those of the SCL: David Jeffrey, Marc Moreno Maza, and Steven Watt, as well as the students. It is not an easy task to provide a working environment which is genuinely friendly, and ever supportive. To Rob Corless: you had faith in my abilities when I did not, and for that I am very grateful.

With love, I thank my family. To Kristen: you inspire me to work hard and to be strong. To my parents: I sincerely thank you for your encouragement and selfless support - even and especially for my non-scholastic endeavors. You have both taught me about dedication, the importance of taking pride in one's work, and, most of all, to persevere.

Contents

Certificate of Examination	ii
Abstract	iii
Epigraph	iv
Acknowledgements	v
Contents	vi
List of Figures	viii
1 Introduction	1
2 The Hilbert Function	6
2.1 Monomials, Polynomials, and Ideals	6
2.2 Ideals, Vector Spaces, and the Hilbert Function	10
2.3 The Hilbert Function of a Monomial Ideal	12
2.4 The Hilbert Function of a Polynomial Ideal	16
3 The Dimension of a Variety	18
3.1 Varieties of Polynomial Systems and Ideals	18
3.2 Dimension and the Hilbert Polynomial	19
4 Gröbner Bases	24
4.1 Gröbner Bases and the Hilbert Function	24
4.2 Buchberger's Algorithm and Gaussian Elimination	26
4.3 Computational Difficulties in the Approximate Case	29
5 The Approximate RREF	33
5.1 Nearby Systems and the Singular Value Decomposition	33
5.2 Approximate Pivot Columns	34
5.3 Convergence to the Exact Pivot Conditions	37
5.4 On Completing the Reduced Row Echelon Form	40

6	Involutive Systems	43
6.1	Polynomials, PDE, and Linear Algebra	43
6.2	Involutive Systems and the Hilbert Polynomial	48
6.3	Projectively Involutive Systems	53
6.4	Approximately Involutive Systems	57
7	Approximate Gröbner Bases	62
7.1	From Involutive Systems to Gröbner Bases	62
7.2	Approximate Gröbner Bases	67
8	Discussion	71
	Bibliography	74
	Vita	77

List of Figures

Chapter 2

p.7. Figure 2.1.3: The monomial $\mathbf{x}^\alpha = x_1^3 x_2^2$, on the line of monomials with total degree 5, on a monomial diagram.

p.13. Figure 2.3.4: Monomial diagram showing the partitioning of $\mathbb{F}[x, y]$ into I and $C(I)$ for the monomial ideal $I = \langle x^3 y^2, x y^4 \rangle$.

p.14. Figure 2.3.8: Monomial diagram showing the complement of the monomial ideal $I = \langle x^3 y^4, x^4 y^2 \rangle$.

Chapter 3

p.20. Figure 3.2.5: Monomial diagram showing the complement of the monomial ideal $I = \langle y^2 \rangle$.

p.21. Figure 3.2.9: Monomial diagrams showing the complements of the monomial ideals $\mathcal{M}_1 = \langle y^3, x^2 y^2 \rangle$ and $\mathcal{M}_2 = \langle x y^2, x^3 y \rangle$. They have the same Hilbert polynomial: $\mathcal{HP}_{\mathcal{M}}^{\text{aff}}(q) = 2q + 3$.

Chapter 6

p.58. Figure 6.4.6: Table of $\dim \pi^\ell \mathcal{D}^r R$ for $R = \{u_{x,x} - u_y, u_{x,y} - u_z\}$.

Chapter 7

p.66. Figure 7.1.8: Monomial diagram for $I = \langle x^3, y^2 \rangle$. $P = \{x^3, y^2\}$ is a Gröbner basis, but cannot be involutive until its third prolongation, $\mathcal{D}^3 P$. The black squares are Cartan characters in $\mathcal{SD}^3 P$, which has full rank.

Chapter 1

Introduction

Approximate computational commutative algebra requires methods which are radically different to the traditional ones developed for exact computation. In this thesis, we avoid ordering-dependent methods, such as Buchberger's algorithm for Gröbner bases, and Gaussian elimination for reduced row echelon forms. Instead, our approach relies on the Hilbert function, which is, by definition, an ordering-independent and linear object. As such, it allows for stable methods from numerical linear algebra, such as the Singular Value Decomposition, to be applied. Together, the Hilbert function and the SVD provide information about nearby, higher-dimensional systems, lost to approximate coefficients. Known methods for determining the Hilbert function rely on Gröbner bases. To avoid this, we use results for involutive systems for partial differential equations. Unfortunately, the computation of an involutive system, even for linear PDE with constant coefficients, requires methods not unlike Gaussian elimination. Moreover, for the approximate case, the systems which we face are highly structured. We propose a method for computing the RREF of a structured, approximate system, which does not rely on Gaussian elimination. Finally, we show that a Gröbner basis may be computed as a natural extension of an involutive system, through the Hilbert function, and as an application of our approximate RREF.

In numerical computation, it is well-known that methods which rely on strict variable orderings can be very unstable. For example, this may force division by small leading coefficients, in Gaussian elimination and Buchberger-type algorithms. It is better to work, if possible, without imposing any ordering at all. Obviously, as a Gröbner basis is, by definition, ordering-dependent, then to compute one it is necessary, at some point, to choose a variable ordering. However, other objects are ordering-independent. For example, the dimension of a variety remains the same regardless of the representation of the polynomial system which encodes that variety. In cases such as this, it may be best to compute such objects via others which are also not ordering-dependent. In the approximate case, this strategy may even be necessary.

Aside from the usual numerical difficulties, failure of methods, which succeed for exact input, can be attributed to small, structure-altering errors in the coefficients of an approximate system. Thus, a given an approximate polynomial system, viewed exactly, is likely to be generic. In this way, fuzzy data may mask interesting and important properties.

Furthermore, viewed approximately, a system and its solutions do not have a one to one relationship. There may be *many* systems surrounding a given one which could each be a valid candidate to represent the true system, in the absence of errors. Alternatively, a desirable, representative, nearby system may not exist at all. A central focus of this thesis concerns alternative methods for processing such approximate systems, rendering them in a form which exposes the greater structure of nearby systems.

The main tool in numerical linear algebra, for gaining information about higher-dimensional systems near to a given one is the *Singular Value Decomposition*. Given $A \in \mathbb{F}^{m \times n}$, with \mathbb{F} is either \mathbb{R} or \mathbb{C} , one can compute:

$$A = U\Sigma V^t, \quad (1.0.1)$$

where, $U \in \mathbb{F}^{m \times m}$ and $V \in \mathbb{F}^{n \times n}$ are orthogonal and, of utmost importance to us, is the diagonal matrix $\Sigma \in \mathbb{R}^{m \times n}$. The number of its nonzero *singular values*: $\sigma_1 \geq \sigma_2 \geq \dots \geq \sigma_r > \sigma_{r+1} = \dots = \sigma_{\min(m,n)} = 0$, is equal to the rank, r , of A . In the case of approximate systems, errors in the entries of A tend to destroy relationships between them. This increase in matrix rank is reflected in small singular values σ_{r+1}, \dots which would otherwise be equal to zero. The following theorem [10] is key to understanding the geometry of linear systems and their surroundings. In particular, it actually provides a distance to nearby singular systems, and a way to compute them.

Theorem 1. *Let $A = U\Sigma V^t \in \mathbb{F}^{m \times n}$ have rank r . A closest matrix to A , with rank $q < r$, can be constructed by forming: $\tilde{A} = U\tilde{\Sigma}V^t$, where $\tilde{\Sigma}$ is equal to Σ with σ_i , $q + 1 \leq i \leq r$, replaced by zero. Furthermore, $\|A - \tilde{A}\|_2 = \sigma_{q+1}$.*

A technique which is used frequently throughout this thesis is to consider polynomial equations as linear functions of their monomials. Hence, we arrive at a matrix problem to which the methods of numerical linear algebra, such as the Singular Value Decomposition, can be applied. As a simple example, consider the system $P(\alpha) = 0$,

$$\begin{aligned} p_1 &= \alpha_1 x^2 + \alpha_2 xy + \alpha_3 y^2 + \alpha_4 x + \alpha_5 y + \alpha_6 = 0, \\ p_2 &= \alpha_7 x^2 + \alpha_8 xy + \alpha_9 y^2 + \alpha_{10} x + \alpha_{11} y + \alpha_{12} = 0, \end{aligned} \quad (1.0.2)$$

which may also be realized as the matrix system $M(\alpha)X = 0$:

$$\begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 & \alpha_5 & \alpha_6 \\ \alpha_7 & \alpha_8 & \alpha_9 & \alpha_{10} & \alpha_{11} & \alpha_{12} \end{pmatrix} \begin{pmatrix} x^2 \\ xy \\ y^2 \\ x \\ y \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}. \quad (1.0.3)$$

In applications, the α 's are likely to be some approximate real or complex numbers. Further, note that completion methods, such as Gröbner bases, rely on multiplying polynomials by monomials. For example, the extended system: $\{xp_1 = 0, yp_2 = 0, p_1 = 0, p_2 = 0\}$ would

be equivalent to:

$$\begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & 0 & \alpha_4 & \alpha_5 & 0 & \alpha_6 & 0 & 0 \\ 0 & \alpha_7 & \alpha_8 & \alpha_9 & 0 & \alpha_{10} & \alpha_{11} & 0 & \alpha_{12} & 0 \\ 0 & 0 & 0 & 0 & \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 & \alpha_5 & \alpha_6 \\ 0 & 0 & 0 & 0 & \alpha_7 & \alpha_8 & \alpha_9 & \alpha_{10} & \alpha_{11} & \alpha_{12} \end{pmatrix} \begin{pmatrix} x^3 \\ x^2y \\ xy^2 \\ y^3 \\ x^2 \\ xy \\ y^2 \\ x \\ y \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}. \quad (1.0.4)$$

All such extended systems define structured classes. Each structured matrix $M(\alpha)$ embeds an extension of the polynomial system $P(\alpha)$, for some particular values of the parameters: $\tilde{\alpha}$.

The Singular Value Decomposition may be applied to $M(\tilde{\alpha})$ to detect nearby matrices with higher-dimensional solution spaces. The worry here, is that these nearby matrices will not lie in necessary structured class. This problem introduces the necessity for convergence methods, with which one can iterate to such nearby systems which do lie on a given structured class. This is a familiar problem to the signal processing community, with works dating back to Cadzow [4], and more recently [25, 20]. However, applications to the areas of approximate commutative algebra [2, 18, 29], and even the geometry of PDE [1], are less widely known.

Exact methods for the completion of PDE system to involutive form [5, 19, 34], also rely on extending that system, as described above. In the PDE case, however, multiplication by monomials is replaced with differentiation with respect to independent variables. Also of interest is the application of such methods to approximate polynomials, through the well-known bijection [13, 30, 31]:

$$\phi : x_i \leftrightarrow \frac{\partial}{\partial x_i}, \quad (1.0.5)$$

which induces a ring isomorphism between polynomials and linear PDEs, preserving the ideals in both cases. For example, the System (1.0.6) would map to $R(\alpha) = 0$:

$$\begin{aligned} r_1 &= \alpha_1 u_{x,x} + \alpha_2 u_{x,y} + \alpha_3 u_{y,y} + \alpha_4 u_x + \alpha_5 u_y + \alpha_6 u = 0 \\ r_2 &= \alpha_7 u_{x,x} + \alpha_8 u_{x,y} + \alpha_9 u_{y,y} + \alpha_{10} u_x + \alpha_{11} u_y + \alpha_{12} u = 0. \end{aligned} \quad (1.0.6)$$

Through the jet theory of PDE, derivatives are considered as independent variables. Thus, the differential system, above, and the system $\{\frac{\partial}{\partial x} r_1 = 0, \frac{\partial}{\partial y} r_2 = 0, r_1 = 0, r_2 = 0\}$ would have the defining structured matrices in Equations (1.0.3) and (1.0.4), respectively.

Additionally, these methods for PDE also require Gröbner type elimination methods, akin to Gaussian elimination for linear systems. Thus, in most cases, knowledge of certain leaders (quantities to be solved for), is required, and thus also a possibly unstable application of Gaussian elimination to compute an RREF. In this thesis, we propose a method to detect leaders without computing an RREF. We go further to construct an approximate RREF, which we compute with no direct appeal to Gaussian elimination. This method,

unlike Gaussian elimination for approximate systems, is also applicable to structured linear systems and, again, requires convergence to a nearby such system, satisfying certain specific dimension criteria.

It is well worth noting that, aside from the bijection ϕ , and jet theory, the Hilbert Function [17] also provides a natural way to view a polynomial ideal from a linear perspective, by breaking up the ideal into vector spaces, and considering their dimensions. Furthermore, as it is linear, its relationship to involutive systems [35] is not surprising. Thus, computing the Hilbert function, without relying on Gröbner bases is as easy as it is to compute an approximate involutive system, given a starting system $P(\tilde{\alpha})$. Recent [1] and ongoing work is to make completion methods for PDE applicable to approximate linear, homogeneous, PDE systems. Our approximate RREF has also proved to be useful here.

The linear algebraic approach which we take allows for the use of the the SVD to gain information about neighboring, higher-dimensional linear systems. A collection of such systems provides a set of fingerprints of an approximate polynomial system as, together, they may identify a higher-degree Hilbert function. In turn, it gives us a evidence that there may be nearby systems with higher-dimensional solution sets, as the degree of the Hilbert function of an ideal and the dimension of that ideal's variety are equivalent. Overall, we have a clearer picture of the surrounding systems, from the point of view of structure and dimension.

Lastly, we exploit the relationship between Gröbner bases and the Hilbert function [8]. Essentially, this is due to Macaulay's observation that the Hilbert functions of an ideal, I , and the ideal generated by its leading terms, $\langle LT(I) \rangle$, are identical [21]. Furthermore, it is interesting to note that Mansfield [22] was able to prove that a (differential) Gröbner basis can be easily extended to an involutive system. Here, we will show that a Gröbner basis may be extended from an involutive system, using the Hilbert function as a guide, and making an application of the approximate RREF. This is opposite to traditional approaches, which compute the Hilbert function from a Gröbner basis, and facilitates approximate computation.

Our backwards approach begins in Chapter 2, with preliminary information on ideals, an explanation of how they can be realized as vector spaces, and an introduction to the Hilbert function. In that same chapter, emphasis is placed upon those properties of the Hilbert polynomial which lay the foundation for most of our further development. In particular, the relationship between the Hilbert polynomial of an ideal and that of the ideal generated by its leading terms is described. In Chapter 3, we focus on a connection between the Hilbert polynomial and the dimension of a variety. This will be useful, later, in the detection of a nearby system whose Hilbert polynomial uncovers a higher level of structure in its solutions. Chapter 4 provides a small introduction to Gröbner bases. However, as our approach differs radically from Buchberger's algorithm, we do not present much of the material which would usually appear in a chapter titled "Gröbner bases." Our concern is mainly to introduce Gröbner bases, by definition, remark about their relation to the Hilbert polynomial, and illustrate our need for an alternative method of computation, in the approximate case. In Chapter 5, we introduce an approximate RREF, which is based on the singular value decomposition, and applicable to structured systems. It makes a second appearance in

Chapter 6, to address certain issues surrounding approximately involutive systems. Also in that chapter, the connection between involutive systems and the Hilbert polynomial is described. Further, the Hilbert polynomial is the link between involutive systems and Gröbner bases. This is the topic of Chapter 7, where, in contrast to other methods, we try to use only one single application of the approximate RREF to compute an approximate Gröbner basis. The current status of the entire approach is described in examples and comments within each chapter. Where we can, we outline the flaws of this method, and make final comments and suggestions about future directions, to conclude with Chapter 8.

Chapter 2

The Hilbert Function

The ideal generated by a system of polynomials p_1, p_2, \dots, p_m from a ring is the set of all combinations $\langle p_1, p_2, \dots, p_m \rangle = \{h_1 p_1 + h_2 p_2 + \dots + h_m p_m\}$, where h_1, h_2, \dots, h_m are arbitrary polynomials in the same ring. This ideal is an important object to study if one is interested in solving the system. Informally, the Hilbert polynomial measures the degree of freedom in the ideal, and is related to the dimension of the solution set of the polynomial system. In this chapter, we introduce monomials, polynomials, and ideals, and give a precise definition of the Hilbert function. Much emphasis is placed upon ideals generated by monomials as, computationally, they are more easily treated than are arbitrary polynomial ideals. Furthermore, these results can be applied to the general case. This will also be discussed.

2.1 Monomials, Polynomials, and Ideals

In order to understand the Hilbert Function, it is important to have, at least, a basic understanding of polynomial ideals. So, we will provide a brief description of them and their components: polynomials. Furthermore, as a special case of polynomial ideals, monomial ideals are also fundamental to our development. The natural objects to first introduce, then, are the basic common building blocks of both polynomials and monomial ideals: monomials.

Definition 2.1.1. [*Monomials, coordinate vectors, and total degree*]

A monomial is simply a product of n variables, each raised to the power of a non-negative integer. It can be written concisely as

$$\mathbf{x}^\alpha = x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}, \quad (2.1.1)$$

where the coordinate vector $\alpha = (\alpha_1, \alpha_2, \dots, \alpha_n) \in \mathbb{Z}_{\geq 0}^n$ contains the exponents of the variables x_1, x_2, \dots, x_n . In this way, a monomial is completely specified by its exponent vector. The total degree (tdeg) of a monomial, $|\alpha| = \sum_{i=1}^n \alpha_i$, is the sum of its exponent vector's coordinates.