DIFFERENTIAL GRÖBNER BASES

by

Elizabeth Mansfield

Ph.D Thesis

University of Sydney, 1991

This thesis is dedicated affectionately
to my father, Colin H. Mansfield.

Table of Contents

Introduction

System of differential equations are at the core of exact sciences, those disciplines readily quantified and modelled mathematically. Perhaps the most famous examples of systems of partial differential equations are Einstein's gravitational field equations and Maxwell's equations for the electromagnetic field. Many papers have considered special cases of these equations, with specified boundary conditions, symmetries or asymptotic behaviour. These papers rely on insight into the structure of the equations with the additional conditions. There has been to date no coherent method, with the notable exception of the use of symmetries, to analyse a general system of partial differential equations, not requiring extensive training in advanced methods of pure mathematics.

The algorithm presented in this thesis is a generally applicable, practical method that can be applied to all systems met in physics, engineering and applied mathematics. The theory from which the algorithm evolved, the concept of Gröbner bases for polynomial ideals, has proven its power, flexibility and utility. Some of the applications for Gröbner bases that have analogues in differential algebra are examined, and are found to be valid in context of differential ideals.

Consider a set of equations $F = \{f_1 = 0, \ldots, f_r = 0\}$, where the f_i are polynomial in the variables $\{x_1, \ldots, x_n\}$, the functions $\{u^1, \ldots, u^n\}$ and the derivative terms $\left\{D^\alpha u^i = \dfrac{\partial^{|\alpha|} u^i}{\partial x^\alpha}\right\}$. A typical example of such an equation would be $f = u_{xx}u_z^2 - 3yu_{yy}$,

where subscripts denote partial derivatives. A solution to the set of equations F will also be a solution to any equation obtained from the given set by taking derivatives, sums, and products with other differential polynomials. The set of all such equations is called the ideal generated by the set $\{f_1, \ldots, f_r\}$. There is no need to be confined to the original set of equations; one can operate with any set of equations that generates the same ideal. Such a set of generators is called a basis.

When seeking a solution to a system of differential equations, one looks for equations implied by the given set that are in some sense simplest. "Simplest" describes those equations with the least number of unknown functions involving derivatives with respect to the smallest number of variables. A Gröbner basis for an algebraic polynomial ideal has the property that it contains a least element with respect to some ordering on the set of polynomials. Gröbner bases solve this and many other questions; herein lies the motivation to modify Buchberger's algorithm for differential ideals.

Buchberger's original definition of a Gröbner basis of a polynomial ideal is a basis with the property that every element of the ideal reduced to zero with respect to that basis. Not every basis is a Gröbner basis.

In 1950, J. F. Ritt defined a characteristic set of a differential ideal as a "lowest", "strictly increasing" sequence of differential equations in the ideal. Note the definition presupposes an ordering on the set of equations. He proved that pseudo-reduction of every member of the differential ideal with respect to a characteristic set necessarily yields zero. The similarity of this property to Buchberger's definition of a Gröbner basis is striking. Buchberger's algorithm to generate a Gröbner basis for a polynomial ideal also depends upon an ordering on the set of polynomials.

The algorithm given in this thesis developed from a true differential adaptation of Buchberger's algorithm, during which a number of problems were met. The main

problem is that algebraically, differential ideals do not have the property used by Buchberger to prove termination of his algorithm. To guarantee termination of the differential algorithm, pseudo-reduction is substituted for reduction, but pseudo-reduction has several implications. The first is that some of the properties of Gröbner bases only hold up to a set of differential coefficients when translated to differential Gröbner bases. The second implication is that these differential coefficients must not lie in the ideal. This is because pseudo-reduction involves multiplying by such terms before reduction.

These provisos imply the output of the algorithm cannot be guaranteed to be a differential Gröbner basis for the ideal generated by the input equations. Nevertheless, for a large number of systems, including all linear systems, the output is indeed a differential Gröbner basis. For other systems, it is necessary to show the differential coefficients lie outside the ideal.

It is possible to use Buchberger's algorithm for differential systems in a strictly algebraic way. After prolonging the equations to some degree, one then regards all derivative terms of that degree or lower as separate indeterminates. While the method does not require attending to the differential coefficients discussed above, one does not know in advance the degree of prolongation needed to obtain a complete differential Gröbner basis and the calculation for even simple examples is too large for medium range computers, because the number of indeterminates grows quickly as the prolongation degree increases. A comparison of the algebraic and differential methods is given in Chapter 5, in which Example 8 shows a system that utilizes both methods to advantage.

The intersection of the algebraic and differential theories occurs for those systems of equations that are linear (as differential equations), in one unknown, with constant coefficients. These equations can be regarded as polynomials in the operators $\frac{\partial}{\partial x_i}$, over $\mathbb{R}$, with the unknown function acting merely as an argument; alternatively one

can use the Laplace operator to transform the equations into polynomials. Every differential ideal consisting of such equations corresponds to a polynomial ideal, and vice versa. In this case, a differential Gröbner basis for such an ideal transforms into a Gröbner basis for the corresponding polynomial ideal, and vice versa.

Apart from finding the least element in the ideal with respect to some ordering, there are a number of ways in which differential Gröbner bases can be used. One can systematically eliminate a subset of the unknowns or differentiations with respect to a subset of the variables, to see what the given equations imply in the lower dimensional setting. In many cases it is then possible to solve the system "form the bottom up", much as one solves a linear system by putting it into echelon form. In fact, the echelon form of a linear (algebraic) system is an example of a Gröbner basis for a system of polynomials of degree one. Differential Gröbner bases yield a basis for the equations in the differential ideal that depend only on the unknowns and variables of interest. Thus the algorithm can be used to attempt to generate Pommaret's "resolvents" and "cascade decomposition" of the differential ideal ([42, 17].) This theory is discussed fully in Chapter 4 under the title of ellimination ideals.

Another problem that can be solved by differential Gröbner bases, is the problem of finding the ideal of compatibility conditions, also called the resolvent system. One can go further, and find the compatibility conditions for the ideal of compatibility conditions, and so forth. The entire sequence of such compatibility ideals, or resolvent systems, is called the Janet resolution. This sequence can be compared to the algebraic syzygy resolution of a polynomial ideal. In fact, in the case of systems of equations that are linear, with one unknown and with constant coefficients, the resolution of the system is precisely the dual of the chain of syzygy modules of the corresponding algebraic system in the operators. Chapter 4 contains the method whereby the differential Gröbner basis calculation can be utilized to generate the resolution of the differential ideal.

The theoretical foundations, the characterisation theorem for differential Gröbner bases, and the algorithms are presented in Chapter 2. The algorithms in this thesis have termination and correctness proved for systems of equations that are polynomials in variables, the unknowns and their derivatives, over $\mathbb{R}$ or $\mathbb{C}$. Examples are discussed in Chapter 3.

Other ways to use the algorithm are discussed in Chapter 5. It is possible to view some systems containing transcendental functions of the unknowns as being differential polynomials, since their defining differential equations are polynomial. For example, the differential equation defining $u = \sin(x)$ is $u_{xx} + u = 0$. When arbitrary functions of the unknowns are involved, the algorithm terminates leading to equations that must be satisfied by the arbitrary functions if a solution is to exist. In solving equations, it is efficacious to seek factors and then set the factors to zero, since the factors will give rise to simpler equations. This is the first step to writing the ideal as an intersection of simpler ideals, whose generators are irreducible, and where at least one factor of an equation in the ideal is already in the ideal. Such ideals are called prime ideals. The difficulty in dealing with differential ideals is that a differential ideal generated by a single irreducible polynomial will not necessarily be prime. A first step towards finding the prime decomposition of a differential ideal is given here by describing a branching generalization of the differential Gröbner basis algorithm.

The final chapter, Chapter 6, is concerned with formal integrability and involutivity, and the relation of these concepts to differential Gröbner bases. We show that differential Gröbner bases satisfy the first condition of being formally integrable. The second condition requires an extra condition: transversality of the loci of the equations, in the relevant jet bundle.

We then find an equivalent formulation of involutivity that involves the symbol equations themselves rather than the kernel of the symbol. In this equivalent formulation,

the obstructions to involutivity are syzygies of the symbol equations provided the system is integrable. The differential Gröbner basis algorithm is thus used to calculate all integrability conditions, and can be adapted to calculate symbolic syzygies, just as Buchberger's algorithm can calculate algebraic syzygies. The highest multiplication needed in the algorithm at any stage of a "symbolic" Janet Resolution provides the answer to how much differentiation is needed in order to make the system involutive.

The algorithm to generate a differential Gröbner basis as presented in this thesis has been implemented as a package in MAPLE^{TM} for the Macintosh and for Apollo Workstations (UNIX). A "User's Manual", a short description of each procedure and a complete listing of the code appear in the Appendices. The longer examples described in Chapters 3, 4 and 5 were calculated with this package.

The idea that Buchberger's algorithm was adaptable to the differential case, and the realization that syzygy and resolution were similar concepts belong to the supervising professor Dr. E. D. Fackerell, who was stimulated by a comparison of algebraic calculations in the Bayer and Stillman programme Macaulay with the description of the linear Janet sequence in Stormark ([53]). The precise formulation, proofs and implementation of the algorithm, and the theorems concerning involutivity and integrability are the work of the author. A list of further research directions appears in the Appendix. Other unsolved problems can be found in Ritt's Appendix ([43].)

Acknowledgements

The writing of this thesis has been a challenging and creative experience.
My supervisor, Prof. Ted Fackerell, with his breadth of experience in helping doctoral students, his enthusiasm and vitality, his mathematical knowledge and proficiency and his patience, has the ability to build confidence in others – I thank him sincerely. I thank also Dr. Scott McCallum and Prof. Larry Lambe for expert discussion and mathematical companionship.

This volume is dedicated to my father, Dr. Colin Mansfield. Without his encouragements, assistance and sense of value, my student years would have proved too difficult. His faith in me never wavers and his joy in my efforts seems greater than my own.

A special "thank you" goes to my mother, Janet Mansfield OAM, who taught me (as far as I was able to learn) editorial skills and how to live with a minimum of fuss, and who gave me good things to think about other than maths. She also bought me a copy of MAPLE for my computer. This wonderful present was a factor in finishing this thesis.

Chapter 1

GRÖBNER BASES IN POLYNOMIAL RINGS

This chapter consists of a discussion of concepts, theorems and examples relevant to the study of Gröbner bases in algebraic polynomial rings, to serve as an introduction to the thesis. The chapter concludes with a discussion of applications and extensions that are of interest to people concerned with differential equations.

1.1 Polynomial Rings

Let $x_1, x_2, \ldots, x_n$ be a fixed set of indeterminates, and fix a field $\mathbb{F}$, of constants and coefficients, taken to be one of $\mathbb{Q}$, $\mathbb{R}$ or $\mathbb{C}$, for convenience. If $\alpha = (\alpha_1, \alpha_2, \ldots \alpha_n)$ is an n-tuple of non-negative integers (i.e. a multi-index) we write the monomial term $x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n}$ as x^α. In this notation, multiplication of monomials is given by the addition of the multi-indices, which are added like vectors, i.e. componentwise: $x^\alpha x^\beta = x^{\alpha+\beta}$, where $\alpha + \beta = (\alpha_1 + \beta_1, \ldots, \alpha_n + \beta_n)$. (Components of multi-indices are italicized so that the components of the multi-index α, namely $\alpha_1, \alpha_2, \ldots$

can be distinguished from two distinct multi-indices α_1, α_2.) The polynomial ring $\mathbb{F}[x_1, x_2, \ldots, x_n]$ is the set of all finite sums having the form $\Sigma c_\alpha x^\alpha$, where $c_\alpha \in \mathbb{F}$. Sums and products in $\mathbb{F}[x_1, x_2, \ldots, x_n]$ have the usual formulae:

$$\sum c_\alpha x^\alpha + \sum d_\alpha x^\alpha = \sum (c_\alpha + d_\alpha) x^\alpha,$$

$$(\sum c_\alpha x^\alpha).(\sum c_\beta x^\beta) = \sum_\delta (\sum_{\alpha+\beta=\delta} c_\alpha c_\beta x^\delta)$$

An ideal I of a ring R is a subset of R such that

1. $a_1 \in I$ and $a_2 \in I \Longrightarrow a_1 - a_2 \in I$
2. $a \in I$ and $r \in R \Longrightarrow r.a \in I$.

The subset $B = \{b_1, b_2, \ldots, b_m\}$ of I is a basis of I if every element of I can be written in the form $r_1 b_1 + r_2 b_2 + \cdots + r_m b_m$, where $r_i \in R$. We write $I = \langle b_1, b_2, \ldots, b_m \rangle_{\mathbb{F}}$, and say I is generated by B.

Example 1 (a polynomial ideal). *The subset I of $\mathbb{F}[x, y, z]$ consisting of all polynomials of the form*

$$p_1(x, y, z).x^2 + p_2(x, y, z).y$$

where p_1 and p_2 are arbitrary polynomials, is an ideal of $\mathbb{F}[x, y, z]$. The ideal I is generated by $\{x^2, y\}$, that is, $\{x^2, y\}$ is a basis for I, and we write $I = \langle x^2, y \rangle_{\mathbb{F}}$.

1.2 Orderings on Monomials

All the operations and calculations we shall perform on polynomials require knowledge of the "leading monomial", the coefficient of the leading monomial, and so forth. There are many ways of deciding which is the leading monomial, all of which require

a total ordering on the set of monomials. The ordering on the monomials must be compatible in the sense that

$$x^\alpha > x^\beta \Longrightarrow x^\delta.x^\alpha > x^\delta.x^\beta$$

where α, β, δ are multi-indices. The monomial $1 = x^0$ is the least monomial in any polynomial ring. We define the most important orderings in use today, and how to obtain more general orderings.[1]

LEXICOGRAPHIC ORDER

In the lexicographic order we have $x^\alpha > x^\beta$ if there exists an i such that $\alpha_1 = \beta_2$, $\alpha_2 = \beta_2, \ldots, \alpha_i > \beta_i$. This order has the property that any monomial involving $x_1, x_2, \ldots, x_{i-1}$ is greater than any monomial free of $x_1, x_2, \ldots, x_{i-1}$. In the lexicographic order, if the leading monomial of a polynomial is free of $x_1, x_2, \ldots, x_{i-1}$, then so is every monomial in that polynomial.

INVERSE LEXICOGRAPHIC ORDER

In the inverse-lexicographic order we have $x^\alpha > x^\beta$ if there exists an i such that $\alpha_n = \beta_n$, $\alpha_{n-1} = \beta_{n-1}, \ldots, \alpha_i > \beta_i$. This order has the property that any monomial involving $x_n, x_{n-1}, \ldots, x_{n-i}$ is greater than any monomial free of $x_n, x_{n-1}, \ldots, x_{n-i}$. In the inverse lexicographic order, if the leading monomial of a polynomial is free of $x_n, x_{n-1}, \ldots, x_{n-i}$. then so is every monomial in that polynomial.

Any ordering on the indeterminates generates a "lexicographic" ordering with respect to the ordering on the indeterminates.

TOTAL DEGREE ORDER

If $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ is a multi-index then $|\alpha| = \alpha_1 + \alpha_2 + \cdots + \alpha_n$ is called the degree of α. In the total degree ordering we say $x^\alpha > x^\beta$ if $|\alpha| > |\beta|$, or if $|\alpha| = |\beta|$ then there exists an i such that $\alpha_1 = \beta_1, \alpha_2 = \beta_2, \ldots, \alpha_i > \beta_i$.

[1] A discussion of the various terminologies dealing with term orderings in use in the Gröbner basis literature is given by Sit [49], "Some comments on Term-Ordering in Gröbner Basis Computations". He points to imprecisions in labelling term-orderings; the terminology given here follows Bayer.

REVERSE-LEXICOGRAPHIC ORDER

In the reverse lexicographic ordering we say $x^\alpha > x^\beta$ if $|\alpha| > |\beta|$ or if $|\alpha| = |\beta|$ then there exists an i such that $\alpha_n = \beta_n, \alpha_{n-1} = \beta_{n-1}, \ldots, \alpha_1 < \beta_i$. Within a given degree, any monomial not divisible by x_n is greater than any monomial divisible by x_n. If a polynomial p is homogeneous (that is, every monomial term has the same degree) and x_n divides its leading monomial, in the reverse lexicographic ordering, then x_n divides p.

Example 2 (leading monomials for different orderings). *Consider the polynomial $p = z^2 - xy^3z + y + x^3 + x^3y + y^5$. We have the following table of orderings and leading monomials:*

Ordering	*Leading monomial*
lexicographic	x^3y
total degree	xy^3z
inverse lex	z^2
reverse lex	y^5

WEIGHTED ORDERS

It is possible to attach a series of weights to the indeterminates in order to obtain more general orders. We do this in the following way. Take an $r \times n$ matrix of non-negative integers $(A_i^t)_{r\times n}$ (where n is the number of indeterminates), and a multi-index α, and form the vector $(A_1^t\alpha_t, \ldots, A_r^t\alpha_t)$. (Repeated indices are summed.) Then say $x^\alpha > x^\beta$ if there exists an i such that $A_1^t\alpha_t = A_1^t\beta_t$, $A_2^t\alpha_t = A_2^t\beta_t, \ldots, A_i^t\alpha_t > A_i^t\beta_t$.

With this notation, the lexicographic order corresponds to the $n \times n$ identity matrix. The inverse lexicographic order corresponds to the matrix (non-specified entries are

zero):

$$\begin{bmatrix} & & & 1 \\ & & 1 & \\ & . & & \\ . & & & \\ 1 & & & \end{bmatrix}$$

The total degree order corresponds to the $(n+1) \times n$ matrix (non-specified entries are zero):

$$\begin{bmatrix} 1 & \cdot & \cdot & 1 & 1 \\ & & & & 1 \\ & & & 1 & \\ & & . & & \\ & . & & & \\ 1 & & & & \end{bmatrix}$$

The reverse lexicographic order corresponds to the $n \times n$ matrix (all entries left of the off-diagonal are 1, entries to the right of the off-diagonal are zero):

$$\begin{bmatrix} & & & 1 \\ & \mathbf{1} & 1 & \\ & . & & \\ . & & & \\ 1 & & & \end{bmatrix}$$

To see this last matrix gives the reverse-lexicographic order, call the matrix for the reverse lexicographic order A and consider $A(\alpha), A(\beta)$ for some multi-indices α and β. Then the first components $A(\alpha)_1, A(\beta)_1$ are the degrees of α and β, as desired. If $A(\alpha)_1 = A(\beta)_1$ and $A(\alpha)_2 > A(\beta)_2$ so that $\alpha_1 + \alpha_2 + \cdots + \alpha_n = \beta_1 + \beta_2 + \cdots + \beta_n$ and $\alpha_1 + \alpha_2 + \cdots + \alpha_{n-1} > \beta_1 + \beta_2 + \cdots + \beta_{n-1}$, then adding α_n to both sides of the inequality and subtracting $|\beta|$ from both sides we obtain $\alpha_n < \beta_n$, and so forth. (Note that it is not possible for two distinct multi-indices α and β to satisfy $|\alpha| = |\beta|, \alpha_n = \beta_n, \ldots, \alpha_2 = \beta_2$ and $\alpha_1 \neq \beta_1$.)

Other references for admissible orderings are [44], [48] and [56].

1.3 Reduction

In Buchberger, Collins and Kutzler ([11]) one reads (where f, g and u are polynomials, and a is a field element):

> "The basic notion of Gröbner bases theory is *polynomial reduction.* Roughly f reduces to g modulo F iff g results from f by subtracting a suitable multiple $a.u.h$ of a polynomial $h \in F$ such that g is lower in an "admissible ordering" than f."

We give an example and then a precise definition.

Example 3 (reduction of a polynomial by another polynomial). *Consider two polynomials $p_1 = xy^2 - 2.zx + y^3$ and $p_2 = z - y^2 + y$. We reduce p_1 with respect to p_2. In the inverse lexicographic order (so that $z > y > x$) the leading monomial in p_2 is z. The reduction is given by the formula $p_1 + 2.x.p_2 = 2xy + y^3 - xy^2$. It is necessary for the leading monomial of p_2 to divide a term in p_1 for a reduction to be possible. Since z is eliminated, we cannot reduce p_1 further with respect to p_2 in the inverse lexicographic ordering.*

Suppose instead we are using the lexicographic ordering. Then the leading monomial in p_2 is y^2. The polynomial p_1 can be reduced at two terms, namely at xy^2 or y^3. The reductions at each term are given respectively by $p_1 + x.p_2$ and $p_1 + y.p_2$. Reducing at both these terms yields $xy + yz - zx + y^2$. Continuing, we reduce the y^2 term yielding $-zx + xy + yz + y + z$. There are no further reductions possible in the lexicographic ordering. Clearly different orderings determine different reductions.

The *coefficient* of a monomial term t in a polynomial p is the sum of the field coefficients of that monomial term, and we denote it by $\mathsf{coeff}(t, p)$. We have to make this definition because it is possible to write each polynomial in many different ways. For example, we can write $x^2 + y^2$ as $(3/7)x^2 + y^2 + z + (4/7)x^2 - z$.

A monomial term is said to occur in a polynomial if its coefficient is not zero.

The coefficient of the leading monomial term in a polynomial p is called the *highest coefficient* and is denoted $\mathsf{Hcoeff}(p)$. The leading monomial term is denoted $\mathsf{Hmon}(p)$. The H stands for highest. This is because L could stand for both leading and lowest! In addition H works in German (haupt) and French (haut).

Let two polynomials p_1 and p_2 be given. Let the leading monomial of $p_2, \mathsf{Hmon}(p_2)$ divide some monomial t in p_1, so that $x^\gamma.\mathsf{Hmon}(p_2) = t$. Then the *reduction* of p_1 by p_2 at the term t is given by

$$p_1 - (\mathsf{coeff}(t, p_1)/\mathsf{Hcoeff}(p_2)).x^\gamma.p_2$$

We say p_1 is reduced with respect to p_2 when no further reductions of p_1 by p_2 are possible. The reduced polynomial is denoted by

$$p_1 \ \mathsf{remainder}\ p_2.$$

By following the calculations in completely reducing a polynomial p with respect to a set of polynomials $F = \{f_1, f_2, \ldots, f_r\}$, we obtain an expression of the form

$$p = g_1 f_1 + g_2 f_2 + \cdots + g_r f_r + (p \ \mathsf{remainder}\ F).$$

We define p *quotient* f_i to be g_i. The remainder is denoted $\mathsf{normalForm}(p, F)$.

We say a polynomial p is in *normal form* if it is reduced with respect to a set F of generators of an ideal, i.e., if p is reduced with respect to each member of F.

A normal form is not unique. Consider the example in $\mathbb{F}[x, y]$ with $p = x^2y$ and $F = \{x^2 + y^2, xy\}$. Reducing p with respect to the second member of F yields zero,

while reducing p with respect to the first member of F yields $-y^3$.

Recall now the definition of an ideal $I \subset \mathbb{F}[x_1, x_2, \ldots, x_n]$, generated by a basis $B = \{f_1, f_2, \ldots, f_r\}$. Every element of the ideal can be written in the form $\Sigma p_i.f_i$ where p_i is an arbitrary polynomial in $\mathbb{F}[x_1, x_2, \ldots, x_n]$. This suggests that every element of I will reduce to zero with respect to the elements of B. However, this is false. Consider the ideal $I \subset \mathbb{F}[x, y]$ generated by $\{x^2+y^2, xy\}$; the leading monomials in the lexicographic or total degree orders are x^2 and xy respectively. Then $p = y(x^2+y^2)-x(xy) = y^3 \in I$ but no element of B reduces p. The problem is clearly that the leading terms have been cancelled by the choice of polynomial coefficients of the basis elements in p.

1.4 "S" polynomials

Let two polynomials f_1 and f_2 be given with leading terms $\mathsf{Hmon}(f_1), \mathsf{Hmon}(f_2)$ and leading coefficients $\mathsf{Hcoeff}(f_1), \mathsf{Hcoeff}(f_2)$, respectively. Let the monomial LCM be the least common multiple of $\mathsf{Hmon}(f_1)$ and $\mathsf{Hmon}(f_2)$. Then the "S" polynomial of f_1 and f_2 is given by

$$f_1 S f_2 = \mathsf{Hcoeff}(f_2)(\mathsf{LCM}/\mathsf{Hmon}(f_1)).f_1 - \mathsf{Hcoeff}(f_1).(\mathsf{LCM}/\mathsf{Hmon}(f_2)).f_2$$

The "S" polynomials of the basis elements B are precisely those ideal elements for which reduction with respect to B might fail to yield zero.

Buchberger's aim was to find a basis with respect to which every element of I reduces to zero. Such a basis is called a Gröbner basis.

1.5 Algorithm (Buchberger)

INPUT: A set of generators $B = \{f_1, f_2, \ldots, f_r\}$ for an ideal $I \subset \mathbb{F}[x_1, x_2, \ldots, x_n]$

OUTPUT: A Gröbner basis for I

Set $P = \{\{f_i, f_k\} \mid f_i, f_k \in B, i \neq k\}$

while $P \neq \emptyset$, do
$\{f_i, f_k\}$ a pair in P
$P := P \backslash \{\{f_i, f_k\}\}$
$h := f_i S f_k$
$h' := \mathsf{normalForm}(h, P)$
if $h' \neq 0$ then
$P := P \cup \{\{f, h'\} \mid f \in B\}$
$B := B \cup \{h'\}$

Theorem 1 (Buchberger)([2]).

(1) the algorithm terminates

(2) if $f_i S f_k$ $\mathsf{remainder}$ $B = 0$ for each pair $f_i, f_k \in B$, then B is a Gröbner basis.

Buchberger's proof that the algorithm terminates uses the fact that $\mathbb{F}[x_1, x_2, \ldots, x_n]$ is noetherian. That is, for every chain of ideals $I_1 \subseteq I_2 \subseteq \cdots \subseteq I_m \subseteq \cdots \subseteq \mathbb{F}[x_1, x_2, \ldots x_n]$ there exists an M such that $I_m = I_M$ for all $m \geq M$. This implies Dickson's Lemma, that for every infinite sequence of monomials $\{m_k\}$ there exists an index K such that all monomials appearing in the sequence after that index are multiples of monomials appearing before that index.

Buchberger's proof of correctness of the algorithm, Theorem 1 (2), involves a comparison of different one-step reductions of a polynomial and a careful use of the notion of "successor" in a reduction calculation.

A Gröbner basis allows ideal membership to be decided in an algorithmic way. The Gröbner basis generated by Buchberger's algorithm depends on the term ordering

used.

Since the basic algorithm above was first published, there have been improvements to its efficiency, mainly by reducing the number of pairs that have to be considered, and by the choice of term orderings. Packages to compute Gröbner bases are available in commercial symbolic algebra programmes, such as Maple, MACSYMA and so on.

Gröbner bases have applications to many problems. Some of the applications that are of interest in differential ideal theory are discussed below. Some references for applications are [10, 9] and [34]. Other survey papers co-authored by Buchberger are listed in the Bibliography. See also [57] and [3].

1.6 Simplest Element

A Gröbner basis for an ideal I for a given ordering must contain the least element of the ideal with respect to that ordering. For if it did not, no element of the Gröbner basis would reduce the least element, contradicting the definition of Gröbner basis.

1.7 Elimination

The aim of elimination is to find from the ideal generated by polynomials $\{f_1, f_2, \ldots, f_r\}$ in the variables $\{x_1, x_2, \ldots, x_n\}$ a subset of polynomials involving only $x_i, x_{i+1}, \ldots, x_n$. In other words we wish to find a basis for $\langle f_1, f_2, \ldots, f_r\rangle_{\mathbb{F}} \cap \mathbb{F}[x_i, x_2, \ldots, x_n]$.

In the lexicographic ordering, each monomial involving $x_1, x_2, \ldots, x_{i-1}$ is greater than any free of $x_1, x_2, \ldots, x_{i-1}$. Alternatively, if the leading monomial of a polynomial p is

free of $x_1, x_2, \ldots, x_{i-1}$, then so is p. The process of forming "S" polynomials in Buchberger's algorithm eliminates the highest terms, or those involving $x_1, x_2, \ldots, x_{i-1}$. The defining property of a Gröbner basis then implies the following theorem due to Trinks (1978):

Theorem 2 (TRINKS) ([54]). *If $B = \{f_1, f_2, \ldots, f_r\}$ is a Gröbner basis for I in the lexicographic order, then $\langle f_1, f_2, \ldots, f_r \rangle_{\mathbb{F}} \cap \mathbb{F}[x_i, x_{i+1}, \ldots, x_n]$ is a Gröbner basis for $I \cap \mathbb{F}[x_i, x_{i+1}, \ldots, x_n]$.*

The process of computing a Gröbner basis from B using the lexicographic order is to see a diagonalization of the basis.

Example 4 (elimination ideals). *We show the output of an algebraic Gröbner basis algorithm implemented by the author as part of the package DIFFGROB. Full details of this package are contained in the Appendices. We take a system of partial differential equations, and prolong them to degree (of differentiation) three. We then treat all derivative terms as separate indeterminates, and find a Gröbner basis for the algebraic ideal generated by the prolonged equations. The output of the algorithm will be used in Chapter 5, Example 8. The system has one unknown function u that depends on two variables $\{x, t\}$. There is also an arbitrary function of u, $f(u)$. The system is*

$$\begin{cases} (u_x)^2 - (u_t)^2 - 1 = 0 \\ u_{xx} - u_{tt} - f(u) = 0 \end{cases}$$

We call the left hand side of the first equation f_1 and the left hand side of the second, f_2. We input the equations

$$F = \left[f_1, f_2, \frac{\partial f_1}{\partial x}, \frac{\partial f_1}{\partial t}, \frac{\partial^2 f_1}{\partial x^2}, \frac{\partial^2 f_1}{\partial x \partial t}, \frac{\partial^2 f_1}{\partial t^2}, \frac{\partial f_2}{\partial x}, \frac{\partial f_2}{\partial t} \right]$$

and choose a lexicographic ordering on the indeterminates determined first by any derivative of u being greater than any derivative of $f(u)$, then by the number of derivatives with respect to the variable t, and then by the number of derivatives with respect

to x. The output is, in descending order,

$$\begin{cases} u_{xxt} - u_{ttt} + u_t f^2 \\ u_{xxx} - u_{xtt} + u_x f^2 \\ u_{xx} - u_{tt} - f(u) \\ u_x u_{xxt} - u_t u_{xxt} + f^2 - u_x^2 f^2 \\ u_{xxt} - u_x^2 u_{xxt} + u_t u_x u_{xxx} + u_t f^2 - u_x^2 u_t f^2 \\ u_{xt} + u_x u_t f \\ u_x^2 - u_t^2 - 1 \\ u_{xx} + u_x^2 - f \\ f_u + f^2 \end{cases}$$

We can now read off some elimination ideals: the sub-ideal depending only on the x-derivatives of u and on derivatives of f is $\langle u_{xx} + u_x^2 - f, f_u + f^2 \rangle$, while the sub-ideal depending only on the derivatives of f is $\langle f_u + f^2 \rangle$.

A feature of the output of the Gröbner basis calculation with the lexicographic order is that polynomial equations can be solved by successive substitution, in much the same way as one would solve a system of linear equations by converting to the echelon form of the matrix. In fact, the process of converting to the echelon form is an example of elimination ideals, where the polynomials have degree one. Other examples can be found in [10]. In contrast with the method of resultants, no spurious roots are found ([3]). Furthermore, the method guarantees that all roots are found.

The lexicographic ordering is claimed by several authors to be quite inefficient ([16], [5].) Bayer and Stillman find the elimination ideals using refinements of non-strict orders. Their preferred refining order is the reverse-lexicographic one. Faugère et. al. describe an efficient (polynomial complexity) algorithm for computing a Gröbner basis for a particular ordering given a Gröbner basis for a different ordering. (The complexity of the Buchberger algorithm for the lexicographic ordering is doubly exponential.) They give examples where the problem of finding a Gröbner basis for

the lexicographic ordering is intractable, but which can be done by first finding the Gröbner basis for the reverse-lexicographic ordering and then using their algorithm to convert it to a Gröbner basis in a lexicographic order.

1.8 Philosophy of Gröbner Bases

The philosophy of using different orderings to compute Gröbner bases is expressed well by Dave Bayer in his lecture notes "Computational Algebraic Geometry: Part One":

> "We can't scrounge through every element of an ideal looking for elements with some property (since I is infinite.)
>
> "It doesn't work to just scan the set of generators of I for elements with some property.
>
> "If we choose an order on the monomials whose structure reflects the property we seek, then it works just to scan a standard or Gröbner basis for I, for elements with the property."

1.9 Test for Inconsistency

The algorithm provides a test for the consistency of a set of polynomial equations. A set of polynomial equations is inconsistent if they imply 1=0.

A set F of polynomials is inconsistent if and only if every Gröbner basis for the ideal generated by F contains the unit element 1.

To see this, first note that if they imply 1=0, then 1 is in the ideal. But 1 is the least element relative to any ordering, so it must be in every Gröbner basis for the ideal. Conversely, if 1 is in the Gröbner basis, then the equations imply 1=0.

1.10 Ideal Quotients

Another example of this philosophy given by Dave Bayer is using the reverse-lexicographic order to compute ideal quotients. If I is an ideal and $f \in \mathbb{F}[x_1, x_2, \ldots, x_n]$, then $(I : f) = \{g \in \mathbb{F}[x_1, x_2, \ldots, x_n] \mid gf \in I\}$ is called the ideal quotient of I by f.

For a homogeneous polynomial p and with the reverse-lexicographic order, x_n divides the leading monomial if and only if x_n divides p.

Theorem 3 ([3]). *If $\{f_1, f_2, \ldots, f_r, x_n f_{r+1}, \ldots, x_n f_s\}$ is a Gröbner basis of homogeneous polynomials for I using the reverse-lexicographic ordering, and $f_1, f_2, \ldots, f_r$ are not divisible by x_n, then $\{f_{r+1}, \ldots, f_s\}$ is a Gröbner basis for $(I : x_n)$.*

The ideal quotient for an arbitrary $f \in I$ can be calculated by including the variable z (with the appropriate weighting) in the set of indeterminates and the relation $f - z$ in the set of generators, and then calculating $(I : z)$.

1.11 Syzygies

The r-tuple of polynomials $(h_1, h_2, \ldots, h_r)$ is a syzygy of the list of polynomials $f_1, f_2, \ldots, f_r$ if

$$h_1 f_1 + h_2 f_2 + \cdots + h_r f_r = 0.$$

The set of all syzygies of $f_1, f_2, \ldots, f_r$ form a submodule $S(I)$ of the ring M consisting of a direct sum of r copies of $\mathbb{F}[x_1, x_2, , x_n]$.

To find syzygies, recall that our criterion for determining whether a basis is a Gröbner basis is that all the "S" polynomials reduce to zero. Keeping track of the coefficients in the reductions yields syzygies.

Example 5 ([3]) (the syzygy module of a polynomial ideal). *Let* $I = \langle x^2 - wy, xy - wz, y^2 - xz\rangle_{\mathbb{R}}$. *Assume the reverse-lexicographic order, so that the leading monomials are* x^2, xy *and* y^2, *respectively. Set*

$$\begin{aligned} f_1 &= x^2 - wy, \\ f_2 &= xy - wz, \\ f_3 &= y^2 - xz, \\ \textit{and} \quad F &= \{f_1, f_2, f_3\}. \end{aligned}$$

$$\begin{aligned} f_1 S f_2 &= y f_1 - x f_2 \\ &= y(x^2 - wy) - x(xy - wz) \\ &= -wy^2 + wxz \\ &= -w(y^2 - xz) \\ &= -w f_3 \end{aligned}$$

so that $f_1 S f_2$ remainder $F = 0$.

$$\begin{aligned} f_1 S f_3 &= y^2 f_1 - x^2 f_3 \\ &= y^2(x^2 - wy) - x^2(y^2 - xz) \\ &= -wy^3 + x^3 z \end{aligned}$$

Now $wy^3 = wyy^2 = wy(f_3 + xz)$ *and* $x^2 z = zxx^2 = zx(f_1 + wy)$ *so that*

$$\begin{aligned} f_1 S f_3 &= -wy(f_3 + xz) + xz(f_1 + wy) \\ &= xz f_1 - wy f_3. \end{aligned}$$

Hence $f_1 S f_3$ remainder $F = 0$.

$$\begin{aligned} f_2 S f_3 &= y f_2 - x f_3 \\ &= y(xy - wz) - x(y^2 - xz) \\ &= -wzy + x^2 z \\ &= z(x^2 - wy) \\ &= z f_1 \end{aligned}$$

Hence $f_2 S f_3$ remainder $F = 0$.

So F is a Gröbner basis for I in the reverse-lexicographic order. Examining the calculations we obtain three syzygies,

$$\begin{gathered} y f_1 - x f_2 + w f_3 = 0 \\ (y^2 - xz) f_1 - (x^2 - wy) f_3 = 0 \\ -z f_1 + y f_2 - x f_3 = 0. \end{gathered}$$

The syzygies are written in vector notation as:

$(y, -x, w)$,
$(y^2 - xz, 0, -x^2 + wy)$,
$(-z, y, -x)$.

By this notation is meant that the dot product of each vector with the column matrix

$$\begin{pmatrix} f_1 \\ f_2 \\ f_3 \end{pmatrix}$$

is zero.
The second syzygy can be generated from the first and the third:
$(y^2 - xz, 0, -x^2 + wy) = y(y, -x, w) + x(-z, y, -x)$.

By Theorem 4 below, the two syzygies $(y, -x, w)$ and $(-z, y, -x)$ generate the module of syzygies for f_1, f_2, f_3.

To be more precise, we need some notation. The module M consisting of a direct sum of r copies of $\mathbb{F}[x_1, x_2, \ldots, x_n]$ has elements that can be written as $g_1e_1 + \cdots + g_re_r$ where $g_i \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ and the e_i act as place-holders for the components of M. In other words, $e_i = (0, \ldots, 0, 1, 0, \ldots, 0)$ where the 1 is in the ith place. In this notation, the syzygies of the above example would be written

$$ye_1 - xe_2 + we_3$$

$$-ze_1 + ye_2 - xe_3.$$

Recall $f_iSf_j = a_jx^\Gamma f_i - a_ix^\Delta f_j$ where

$$x^\Gamma = \frac{\mathsf{lcm}(\mathsf{Hmon}(f_i, f_j))}{\mathsf{Hmon}(f_j)}, \quad a_i = \mathsf{Hcoeff}(f_i)$$

and

$$x^\Delta = \frac{\mathsf{lcm}(\mathsf{Hmon}(f_i, f_j))}{\mathsf{Hmon}(f_i)}, \quad a_j = \mathsf{Hcoeff}(f_j)$$

Theorem 4 (Spear, Schreyer). *If $f_1, \ldots, f_r$ is a Gröbner basis for I, then for all pairs f_i, f_j, the expressions*

$$a_jx^\Gamma e_i - a_ix^\Delta e_j - \left(\sum_k f_iSf_j \ \mathsf{quotient}\ f_k\right) e_k$$

generate the module $S(I)$ of all syzygies of $f_1, \ldots, f_r$.

(The definition of p quotient F is on page 7.)

The expressions are a record of how the Spolynomials reduce to zero.

Consider the map $\phi : M \to \mathbb{F}[x_1, x_2, \ldots, x_n]$ defined by $\phi(e_i) = f_i$, and extended linearly. Then a syzygy $h_1e_1 + \cdots + h_re_r$ maps to $h_1f_1 + \cdots + h_rf_r = 0$. The syzygies are precisely the kernel of this map. The expression $a_jx^\Gamma e_i - a_ix^\Delta e_j$ maps to $a_jx^\Gamma f_i - a_ix^\Delta f_j$ which is f_iSf_j. The criterion for a Gröbner basis is that $(\sum_k f_iSf_j \ \mathsf{quotient}\ f_k)e_k$

is zero so that $f_i S f_j$ quotient $\{f_1, \ldots, f_r\}$ maps to $f_i S f_j$. Hence the expression $a_j x^{\Gamma} e_i - a_i x^{\Delta} e_j - f_i S f_j$ quotient $\{f_1, \ldots, f_r\}$ maps to zero, i.e. it is a syzygy.

APPLICATION OF SYZYGIES: INTERSECTION OF IDEALS

Let $I = \langle f_1, \ldots, f_r \rangle_R$ and $J = \langle g_1, \ldots, g_s \rangle_R$. If we find all the $(r+s)$-tuples

$$(h_1, \ldots, h_r, j_1, \ldots, j_s)$$

of elements of $\mathbb{F}[x_1, x_2, \ldots, x_n]$, with the property

$$h_1 f_1 + \ldots + h_r f_r + j_1 g_1 + \ldots + j_s g_s = 0,$$

then

$$h_1 f_1 + \ldots + h_r f_r \in I$$

$$= -j_1 g_1 - \ldots - j_s g_s \in J.$$

In this way, each syzygy of $f_1, \ldots, f_r, g_1, \ldots, g_s$ gives an element of $I \cap J$.

THE PROJECTIVE RESOLUTION OF SYZYGY MODULES

Recall the syzygy module of an ideal I is contained in a ring M that consists of r_1 copies of $\mathbb{F}[x_1, x_2, \ldots, x_n]$. The integer r_1 is the number of generators in the ideal I. Given a basis with r_2 elements for the module of syzygies $S(I)$ for an ideal I, it is possible to then form the module of syzygies $S(S(I))$ for the ideal $S(I)$. The ideal $S(S(I))$ is contained in a ring M_2 that consists of r_2 copies of M. Iterating this process forms the syzygy resolution of the ideal I. Denote the nth syzygy module by $S^{(n)}(I)$.
We write the resolution as

$$\ldots \longrightarrow M_n \xrightarrow{\phi_n} M_{n-1} \longrightarrow \ldots \longrightarrow M \xrightarrow{\phi} I \longrightarrow 0$$

The kernel of each map ϕ_i is the module $S^{(i)}(I)$, and the image of each map ϕ_i is $S^{(i-1)}(I)$. This sequence is called the injective resolution of syzygy modules. (A sequence $\ldots \longrightarrow A^{(n)} \longrightarrow A^{(n-1)} \longrightarrow \ldots \longrightarrow A^{(2)} \longrightarrow A \longrightarrow 0$ is called an projective resolution of A if the kernel of one map is the image of the previous map.) It was proved by Hilbert late last century that the syzygy resolution terminates. In fact, if the original ideal contains n indeterminates, then $S^{(n+1)}(I) = 0$.

1.12 Primary Decomposition

It is clear that in seeking a locus to a set of polynomials, one seeks the simplest equations implied by the given set, and then factors them. Indeed, one seeks all factors implied by the given equations. Irreducible components of the locus correspond in some way to irreducible components of the equations.

Example 6 (primary decomposition of a polynomial ideal (Bayer)). *Consider the zero set of*

$$\begin{cases} f_1 = xy + x - x^3 \\ f_2 = y^2 + y - x^2 y. \end{cases}$$

The S polynomial $f_1 S f_2$ is zero. Factoring f_1 and f_2 yields $x(y + 1 - x^2)$ and $y(y + 1 - x^2)$ respectively. There are four possibilities, namely

$$\begin{aligned} &\{x, y \mid x = 0, y = 0\}, \\ &\{x, y \mid x = 0, y + 1 - x^2 = 0\}, \\ &\{x, y \mid y + 1 - x^2 = 0, y = 0\} \quad \textit{and} \\ &\{x, y \mid y + 1 - x^2 = 0\}. \end{aligned}$$

These possibilities are contained in the sets $\{x = 0, y = 0\}$ and $\{x, y \mid y+1-x^2 = 0\}$. The ideal I generated by f_1 and f_2 can be written as the intersection of the ideals $q_1 = \langle x, y \rangle$ and $q_2 = \langle y + 1 - x^2 \rangle$. (Note that q_1 is not the whole of $\mathbb{F}[x, y]$ since the

latter includes polynomials with a constant term whereas q_1 does not.) The zero set of I is the union of the zero sets of q_1 and q_2.

The primary decomposition of an ideal is the algebraic foundation for decomposing an algebraic variety into its irreducible components. It is the generalization of the factorization of an integer as a product of prime-powers.

An ideal I of a ring R is said to be prime if $I \neq R$ and $a.b \in I$ implies either $a \in I$ or $b \in I$.

An ideal I of a ring R is said to be primary if $I \neq R$ and $a.b \in I$ implies either $a \in I$ or $b^n \in I$ for some $n > 0$.

The radical of an ideal I is denoted $\mathsf{rad}(I)$ or $\sqrt{I}$, and is defined by

$$\sqrt{I} = \{a \in R \mid a^n \in I \quad \text{some} \;\; n > 0\}.$$

The radical of a primary ideal is a prime ideal. For suppose $ab \in \mathsf{rad}(I)$, so that $a^n b^n \in I$ (note we are only concerned with commutative ideals). If $a \notin \mathsf{rad}(I)$ so that no power of a is in I, then since I is primary some power of b^n is in I. But then $b \in \mathsf{rad}(I)$.

LASKER-NOETHER THEOREM

Every polynomial ideal can be expressed as an intersection of finitely many primary ideals. We write

$$I = \cap_{i=1,\ldots,n} \; q_i$$

While the primary ideals q_i used in the intersection may not be unique, the radicals of the primary ideals form a set that is independent of the particular decomposition of I.

In their paper "Gröbner Bases and Primary Decomposition of Polynomial Ideals",

P. Gianni, B. Trager and G. Zacharias [20] present an algorithm to compute the primary decomposition of any ideal in a polynomial ring. Their algorithm relies on those properties of Gröbner bases already discussed here, namely, elimination ideals, ideal membership and ideal intersection.

A simpler algorithm, to decompose the algebraic variety into its irreducuble components, is given in [35]. [33] contains a discussion of the Buchberger algorithm where polynomials are factored after every iteration. This provides an approximation to the primary decomposition.

A discussion of primary decompositions, and further references are given in [10].

In his book "Differential Algebra", Ritt proves that every perfect differential ideal has a prime decomposition. (An ideal I of a ring R is said to be *perfect* or *radical* if $b^n \in I$ for some $n > 0$ implies $b \in I$.) Ritt gives an extensive discussion of prime differential ideals, which have many applications in the formal theory of PDE ([39, 41].) Pommaret ([39] p. 246) gives a criterion for a differential ideal to be prime. Note that a perfect primary ideal is prime. Ritt's discussion is for the most part non-constructive; it is clearly desirable to extend the work of Gianni et al to the differential case.

1.13 Implicitization of Parametrically described Varieties

The general implicitization problem is to remove all parametric variables in the description of an algebraic variety. More precisely, given polynomials $p_1, \ldots, p_m \in \mathbb{F}[x_1, \ldots, x_n]$, find $f_1, \ldots f_k \in \mathbb{F}[y_1, \ldots, y_n]$ such that for all $a_1, \ldots, a_m \in \mathbb{F}$,

$$f_1(a_1, \ldots, a_m) = \cdots = f_k(a_1, \ldots, a_m) = 0$$

if and only if for some $b_1, \ldots, b_n \in \mathbb{F}$,

$$\begin{aligned} a_1 &= p_1(b_1, \ldots, b_n), \\ &\ldots, \\ a_m &= p_m(b_1, \ldots, b_n). \end{aligned}$$

The b_i are the parametric variables, and the p_i are the parametric equations, while the a_i are the non-parametric variables and the f_i the non-parametric equations.

The polynomials f_i are computed by finding the Gröbner basis of the ideal generated by $\{y_1 - p_1, \ldots, y_m - p_m\}$ using the lexicographical ordering based on $y_1 < \ldots < y_m < x_1 < \ldots < x_n$, and taking the intersection with $\mathbb{F}[y_1, \ldots, y_n]$. ([9])

It will be seen in Chapter 4 that this is analogous to the algorithm used to calculate the resolution of a system of partial differential equations. It is the dual of the syzygy calculation.

The inversion problem, namely that of finding the co-ordinates of a particular point on a variety given parametrically, can be solved using the same algorithm as used for the implicitization problem.

1.14 Detection of Singularities

The method of Gröbner bases yields an immediate approach to detect all singular points of implicitly given planar curves. The singular points of a planar curve given by $f(x, y) = 0$ are exactly the points that are common zeros of f, f_x and f_y. One calculates the Gröbner basis of the ideal generated by $\{f, f_x, f_y\}$ with respect to a lexicographical ordering and then finds the set of zeros by the successive substitution method (see the Elimination Ideals section.) ([9])

1.15 Radicals

It is possible to use the Gröbner basis algorithm to ascertain whether an element x of a ring R is in the radical of an ideal I. Let I be generated by the set F, and let y be a new indeterminate. Then $x \in \mathsf{rad}(I)$ if the Gröbner basis generated by the set $F \cup \{1 - xy\}$ contains the unit element 1. ([9])

1.16 Generalization to polynomials of operators

Polynomials of operators are not to be confused with polynomials in which the indeterminates are operators each acting on its own argument.

The set of operators $\mathcal{D}$ is assumed to satisfy the following: for $D^1, D^2 \in \mathcal{D}$,

$$\begin{aligned}
&[D^1, D^2] = D^1 D^2 - D^2 D^1 \in \mathcal{D}, \\
&[D^1, D^1] = 0, \\
&[D^1, D^2] = -[D^2, D^1],
\end{aligned}$$

and the Jacobi Identity

$$[D^1, [D^2, D^3]] + [D^2, [D^3, D^1]] + [D^3, [D^1, D^2]] = 0,$$

in which case polynomial rings of operators are precisely enveloping algebras of Lie algebras.

Apel and Lassner in their paper "An Extension of Buchberger's Algorithm and Calculations in Enveloping Fields of Lie Algebras" present an extension to non-commutative finite-dimensional Lie algebras. Examples are algebras of angular momentum operators, Weyl algebras, symmetry algebras and so on. Equations in the Weyl algebra are linear systems with variable coefficients. These equations have the form

$\left(\sum_{\alpha,\beta\in\mathbb{N}^n} c_{\alpha,\beta}x^\beta D^\alpha\right)u = 0$, where $c_{\alpha,\beta}$ are elements of the relevant field. The operators can be regarded as elements of the algebra $\mathbb{F}\left[x_i, \frac{\partial}{\partial x_i} \mid i = 1,\ldots n\right]$ which is the enveloping algebra for the Lie algebra $\langle x_i, \frac{\partial}{\partial x_i} \mid i = 1,\ldots n\rangle_{\mathbb{F}}$. These systems have been studied by Galligo ([19]). An example of the differential Gröbner basis of such an ideal is given in Example 2 of Chapter 3.

Chapter 2

DIFFERENTIAL GRÖBNER BASES

The place of monomials in the polynomial ideal theory is given in differential ideal theory to derivative terms. A derivative term is the (partial) derivative of an unknown function u^i with respect to n variables $\{x_1, ..., x_n\}$. In differential algebra, there is an additional complication which is that derivative terms can themselves be multiplied or taken to powers. A product of two monomials or a power of a monomial is again a monomial, while a product of two derivative terms or a power of a derivative term is not again a derivative term.

This chapter contains a theorem that characterizes an analogue of Gröbner bases in differential ideals. Differential ideals are not noetherian (they have an infinite number of generators, algebraically speaking), and replacing the S polynomial and reduction calculations with their differential analogues yields infinite Gröbner bases ([37], [12]). To achieve a finite theory, we replace reduction with pseudo-reduction. This leads to several subtleties when formulating an algorithm to calculate a differential Gröbner

basis. Pseudo-reduction involves multiplying equations by certain differential coefficients before reducing them. These differential coefficients must not lie in the ideal generated by the given equations. The equations output by the algorithm satisfy all conditions sufficient for them to be a differential Gröbner basis, except the condition concerning these differential coefficients, which must be checked on a case-by-case basis. The details of the output, and the termination of the algorithm, are discussed and proved. Examples are studied in Chapter 3.

Notations

$\mathbb{N}$ is the set of natural numbers

$\mathbb{F}$ a field of characteristic zero, usually $\mathbb{R}$ or $\mathbb{C}$.

$\alpha, \beta, \gamma \in \mathbb{N}^n$ are multi-indices

If $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ then $|\alpha| = \alpha_1 + \alpha_2 + \cdots, \alpha_n$.

Note: components of a multi-index α are denoted by $\alpha_1, \alpha_2 \ldots$, to prevent confusion between the *components* of a multi-index α, and distinct multi-indices α^1, α^2.

A monomial is labelled by a multi-index α thus: $x^\alpha = x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n}$. A derivative term is labelled both by a multi-index α and an index i to specify which unknown function is being differentiated:

$$p^i_\alpha = D^\alpha u^i = \frac{\partial^{|\alpha|} u^i}{\partial x^\alpha} = \frac{\partial^{|\alpha|} u^i}{\partial x_1^{\alpha_1} \partial x_2^{\alpha_2} \ldots \partial x_n^{\alpha_n}}$$

$p^j_0 = u^j$

$\mu_j = (0, \ldots, 0, 1, 0, \ldots, 0) \in \mathbb{N}^n$ with the 1 in the j^{th} place. Where the notation μ is already in use, we use $1_j = (0, ..., 0, 1, 0, ..., 0)$ with the 1 in the j^{th} place.

For indices of small degree, derivatives are also denoted by the usual notation, e.g. $u_{xx} = p_{(2,0,\ldots,0)}$.

We will use the following abbreviations:

d.p	differential polynomial
DGB	differential Gröbner basis

2.1 Differential rings and ideals

A differential ring is a commutative ring R together with a finite set of derivations $\{D_i : R \to R \mid i = 1, ..., n\}$ which are linear, which commute with each other and which satisfy the product rule

$$D_i(r_1 r_2) = D_i(r_1)r_2 + r_1 D_i(r_2).$$

A differential ideal I of a differential ring is an ideal which also satisfies

$$r \in I \Longrightarrow D_i(r) \in I \text{ for all } i = 1, \ldots, n.$$

We define $R_{n,m}$ to be the ring of polynomials in the variables $\{x_i \mid i = 1, ..., n\}$, the C^∞ unknown functions of the variables $\{u^j | j = 1, ..., m\}$ and their derivatives $\{p^j_\alpha = D^\alpha u_j\}$ over the field $\mathbb{F}$, with $D_i = \dfrac{\partial}{\partial x_i}$:

$$R_{n,m} = \mathbb{F}[x_i, u^j, p^j_\alpha \mid i = 1, \ldots, n; j = 1, \ldots, m; \alpha \in \mathbb{N}^n]$$

The field $\mathbb{F}$ is usually $\mathbb{R}$ or $\mathbb{C}$, but can be any field of characteristic zero on which differentiation is defined. (Notations as above.) Elements of $R_{n,m}$ are called differential polynomials (d.p.'s).
As a differential ring, $R_{n,m}$ is finitely generated by $\{x_1, ..., x_n, u^1, ..., u^m\}$. We restrict ourselves to ideals whose elements contain derivative terms.

2.2 Orderings on the differential polynomials

The ordering on the differential polynomials (d.p.'s) depends upon an ordering on the variables $\{x_i \mid i = 1, ..., n\}$, and the functions $\{u^j \mid j = 1, ..., m\}$. A compatible ordering is desired, that is,

$$f_1 > f_2 \Longrightarrow D_i(f_1) > D_i(f_2) \quad \text{and} \quad f.f_1 > f.f_2$$

for all i and all d.p.'s f. We assume the ordering $u_m > u_{m-1} > ... > u_1$ and $x_1 > x_2 > ... > x_n$. The $\{p^i_\alpha\}$ are called derivative terms. We first define orderings on the set of derivative terms.

The **lexicographic** ordering on the derivative terms is given by

$$p^i_\alpha > p^j_\beta \quad \text{if} \quad i > j$$

else $i = j$ and the first non-zero difference

$$\alpha_1 - \beta_1, \alpha_2 - \beta_2, \ldots, \alpha_n - \beta_n$$

is positive.

The **total degree** ordering on the derivative terms is given by

$$p^i_\alpha > p^j_\beta \quad \text{if} \quad i > j$$

else $i = j$ and $|\alpha| > |\beta|$
else $i = j$, $|\alpha| = |\beta|$ and the first non-zero difference

$$\alpha_n - \beta_n, \alpha_{n-1} - \beta_{n-1}, \ldots, \alpha_1 - \beta_1$$

is positive.

The total-degree ordering given by other authors is determined first by total degree, then the unknown, and then inverse-lexicographic ordering ([53]).

The **reverse-lexicographic** ordering on the derivative terms is given by

$$p^i_\alpha > p^j_\beta \quad \text{if} \quad i > j$$

else $i = j$ and $|\alpha| > |\beta|$
else $i = j, |\alpha| = |\beta|$ and the first non-zero difference

$$\alpha_n - \beta_n, \alpha_{n-1} - \beta_{n-1}, \ldots, \alpha_1 - \beta_1$$

is negative.

It is clear that any ordering on the variables $\{x_i\}$ determines a lexicographic, total-degree or reverse-lexicographic ordering on $\{p^i_\alpha\}$. For these three orders, since $u^j = p^j_0$, we have $p^j_\alpha > u^j$ for all $\alpha \neq 0$.

While the lexicographic ordering is what we need to use for the elimination ideals results, nevertheless, in the formal theory of partial derivative equations it has been orderings graded by total degree that have been used to determine the symbol of the system, motivated by the proof of the Cauchy-Kovalevska Theorem on analytic equations. ([53], [38].) For a discussion of the symbol of a system of PDE's and its relationship to differential Gröbner bases, see Chapter 6.

As in Chapter 1, it is possible to attach "weights" to obtain more general ordering schemes ([53, Section 2.2], [54]). Our matrices are the transpose of Trinks'.)
For $h = 1, ..., s$, $k = 1, ..., m$ and $i = 1, ..., n$, define the weights $w_h(u^k)$, $w_h(x_i)$ and set

$$w_h(p^k_\alpha) = w_h(u^k) + \alpha_1 w_h(x_1) + \cdots + \alpha_n w_h(x_n).$$

Then $p^k_\alpha > p^j_\beta$ if the first non-zero difference

$$w_h(p^k_\alpha) - w_h(p^j_\beta), h = 1, ..., s$$

is positive. We can define a matrix A such that

$$w_h(p^k_\alpha) = \left(A \begin{pmatrix} \alpha^T \\ (\mu^k)^T \end{pmatrix} \right)_h .$$

(See Notations for definition of μ^k). For example, the total degree ordering above has

the matrix

x				u			
0	0	...	0	**1**	0	...	0
0	0	...	0	0	**1**	...	0
						.	
						.	
						.	
0	0	...	0	0	0	...	**1**
1	**1**	...	**1**	0	0	...	0
0	0	...	**1**	0	0	...	0
		.					
		.					
		.					
0	**1**	...	0	0	0	...	0
1	0	...	0	0	0	...	0

By contrast, the total degree ordering used by Stormark has the matrix

x				u			
1	**1**	...	**1**	0	0	...	0
0	0	...	0	**1**	**2**	...	**m**
0	0	...	**1**	0	0	...	0
		.					
		.					
		.					
0	**1**	...	0	0	0	...	0
1	0	...	0	0	0	...	0

Definitions

Let DT^p be a derivative term raised to a power p. The **coefficient** of DT^p in a d.p.,

f, is the sum of all coefficients DT^p in f (note the coefficient contains no powers of DT), and is denoted $\mathsf{coeff}(f, \mathsf{DT}^p)$. If DT^p has a non-zero coefficient in f, we say DT^p occurs in f.

The **highest derivative term** occurring in a d.p. f is denoted $\mathsf{HDT}(f)$.
The **highest power** of the $\mathsf{HDT}(f)$ occurring in f is denoted $\mathsf{Hp}(f)$.
The **highest coefficient**, denoted $\mathsf{Hcoeff}(f)$, is the d.p.,

$$\mathsf{coeff}(f, \mathsf{HDT}(f)^{\mathsf{Hp}(f)}).$$

The **head** of f is $\mathsf{Head}(f) = \mathsf{Hcoeff}(f).\mathsf{HDT}(f)^{\mathsf{Hp}(f)}$.

The **highest unknown** function occurring in f, the unknown function involved in the highest derivative term, is denoted $\mathsf{Hu}(f)$.

The **separant** of f is the highest coefficient of $D^\alpha f$, for any non-zero multi-index α, and is denoted $\mathsf{Sep}(f)$.

The **highest monomial**, $\mathsf{Hmon}(f)$, is defined recursively as follows: if f is a monomial, $\mathsf{Hmon}(f) = f$, else $\mathsf{Hmon}(f) = \mathsf{Hmon}(\mathsf{Head}(f))$.

Example 1. *In the differential polynomial*

$$f = (u_x^2 - 1)u_{xxy} + u_{zz}^3 - (v_{yy} - v_z)u_{xyy}$$

we have

	lex $u > v$, $z > y > x$	***total degree*** $u > v$, $x > y > z$	***reverse lex*** $u > v$, $x > y > z$	***lex*** $v > u$, $x > y > z$
$\mathsf{HDT}(f)$	u_{zz}	u_{xyy}	u_{xxy}	v_{yy}
$\mathsf{HP}(f)$	*3*	*1*	*1*	*1*
$\mathsf{Hcoeff}(f)$	*1*	$-(v_{yy} - v_z)$	$u_x^2 - 1$	$-u_{xyy}$
$\mathsf{Sep}(f)$	$3(u_{zz})^2$	$-(v_{yy} - v_z)$	$u_x^2 - 1$	$-u_{xyy}$
$\mathsf{Hmon}(f)$	u_{zz}^3	$-v_{yy}u_{xyy}$	$u_x^2 u_{xxy}$	$-v_{yy}u_{xyy}$
$\mathsf{Hu}(f)$	u	u	u	v

We now define the ordering on the differential polynomials, given an ordering on the derivative terms.

If $\mathsf{HDT}(f_1) > \mathsf{HDT}(f_2)$ we say $f_1 > f_2$. If two polynomials have equal HDT's but the HDT occurs to a higher power in f_1 than in f_2, then $f_1 > f_2$. If two polynomials have the same HDT's and the same Hp's then the ordering is determined by the ordering on the Hcoeff's. If $\mathsf{Head}(f_1)$ and $\mathsf{Head}(f_2)$ differ by a field coefficient, then the ordering is determined by that on $f_1 - \mathsf{Head}(f_1), f_2 - \mathsf{Head}(f_2)$.

If the summands of f_1 and f_2 differ only in their field coefficients, we say f_1 and f_2 are of equal rank.

2.3 Sequences of differential polynomials

Recall from Chapter 1 that a ring is said to be noetherian if it satisfies the "ascending chain condition", namely, that for any nested sequence of ideals $I_0 \subseteq I_1 \subseteq \ldots \subseteq I_n \subseteq \ldots$ there is an N such that $I_n = I_N$ for all $n \geq N$. This property was used by Buchberger to prove termination of his algorithm. A differential ideal, regarded as an algebraic ideal, is not noetherian, because there are infinitely many indeterminates. Ritt ([43]) proves that ascending chains of *perfect* or *radical* differential ideals terminate.

(An ideal I is said to be **perfect**, or **radical**, if $a^q \in I \Longrightarrow a \in I$. Generalisations to this theorem appear in [30, Ch III] and [39, pp235-257].) Therefore, we need to prove termination for general ideals "by hand", that is, by examining sequences of differential polynomials. The following two lemmas prove that any strictly decreasing sequence of d.p.'s terminates. The strictly decreasing sequences are bounded below by a least element in the ring, namely the zero polynomial.

Lemma 1. *Any strictly decreasing sequence of the form*

$$\{t_\nu = (p^{i_\nu}\alpha^\nu)^{k_\nu} \mid i_\nu \in \{1,\ldots,m\}, k_\nu \in \mathbb{N}, \alpha^\nu \in \mathbb{N}^n\}$$

terminates after a finite number of terms. Hence for any infinite decreasing sequence there must exist an N such that $n > N \Longrightarrow t_n = t_N$.

Proof. For $m > 1$, the sequence $\{t_\nu\}$ can only be infinite if it is infinite for one of the indices that label the unknowns. Thus we prove the result for $m = 1$ (i.e. $i_\nu = 1$ all ν.). Consider the associated sequence

$$S = \{s_\nu = x^{\alpha^\nu}\}_{\nu=1}^{\infty} \subset \mathbb{F}[x_1,\ldots,x_n].$$

The monomials have the ordering $x^\alpha > x^\beta$ if and only if $p_\alpha > p_\beta$ with respect to some compatible order. (See notations above). The sequence S is decreasing. For any decreasing sequence $\{s_i\}$ in $\mathbb{F}[x_1,...,x_n]$ there exists an integer M such that $i > M$ implies $s_i = s_M$. Considering our original sequence $\{(p_{\alpha^\nu})^{k_\nu}\}$, we now have $\alpha^i = \alpha^M$ for $i > M$, so the only way the sequence can be strictly decreasing is for $\{k_\nu \mid \nu > M\}$ to be a strictly decreasing sequence of positive integers, which must terminate. □

Lemma 2. *Let $\{f_n\}$ be a decreasing sequence of differential polynomials in $R_{n,m}$. Then there exists an N such that for $n > N$, f^n and f^N are of equal rank.*

Proof. We first show that a strictly decreasing sequence of monomials $\{m_k\}$ terminates. A monomial has the form $x^\alpha \mathsf{DT}_1^{p_1}.\mathsf{DT}_2^{p_2}\ldots\mathsf{DT}_n^{p_n}$. Firstly, by Lemma 1, the

sequence $\{\mathsf{HDT}(m_k)^{\mathsf{Hp}(m_k)}\}$ terminates. Let M_1 be the terminal value, occurring for $k > K_1$. Repeat the argument on the sequence of monomials $\{m_k/M_1 \mid k > K_1\}$, to produce a terminal value M_2 occurring for $k > K_2$. Iterating, we obtain a sequence $\{M_r\}$. This sequence is strictly decreasing and so is finite, finishing at $r = R$. Then the terminal value of the sequence $\{m_k\}$ is $M_1.M_2...M_R$, which is reached in a finite number of steps.

Let us now consider the given sequence $\{f^n\}$.

Let $f_1^n = f^n$. Considering the sequence $\{\mathsf{HDT}(f^n)^{\mathsf{Hp}(f^n)}\}$ we have by Lemma 1 that there exists an N_1 such that the sequence is stationary for $n > N_1$. Consider next the sequence

$$\{f_2^m = \mathsf{Hcoeff}(f^n) \mid m = n - N_1 + 1, n \geq N_1\}.$$

Applying the above argument to f_2^m we again find an N_2 for which $\mathsf{HDT}(f_2^n) = \mathsf{HDT}(f_2^{N_2})$, and $\mathsf{Hp}(f_2^n) = \mathsf{Hp}(f_2^{N_2})$ for $n > N_2$. We can iterate this procedure indefinitely creating an infinite sequence of sequences. Consider now the sequence $\{f_n^1\}_{n=1}^{\infty}$. Since by definition $\mathsf{Hcoeff}(f) < \mathsf{HDT}(f)^{\mathsf{Hp}(f)}$ for any f, this is a strictly decreasing sequence, which terminates by Lemma 1.

This shows that there is an index K_1 for which $k > K_1$ implies $\mathsf{Hmon}(f^k)$ and $\mathsf{Hmon}(f^{K_1})$ differ by a field coefficient. Let m_1 denote $\mathsf{Hmon}(f^{K_1})$ divided by its field coefficient.

We now iterate the whole argument on $\{f^n - \mathsf{Hmon}(f^n) \mid n > K_1\}$, to produce a strictly decreasing sequence of monomials $\{m_r\}$. This sequence terminates, implying the required result. □

2.4 Reduction

There are two methods of reduction. The first is a strictly algebraic reduction.

Definition 1 (reduction). If f and g are two d.p.s, we say that g reduces f at the monomial M, where M is a summand of f, if $\mathsf{Hmon}(g) \mid M$.

We write $f \rightarrow_g f'$ where $f' = f - \dfrac{M}{\mathsf{Hmon}(g)}\, g$.

This type of reduction is that used when calculating Gröbner bases of algebraic ideals.

The second type of reduction we denote differential reduction. The d.p. g (differentially) reduces f if for some derivative term DT occurring in f to the power p, we have

(1) $\quad D^\alpha \mathsf{HDT}(g) = \mathsf{DT} \qquad$ some multi-index α,

(2) $\quad \mathsf{Hp}(g) \leq p \qquad$ if $\alpha = 0$

and

(3) $\quad \mathsf{coeff}(f, DT^p) = h_1 \mathsf{Hcoeff}(D^\alpha g) + h_2 \qquad h_1, h_2$ d.p.'s and $h_1 \neq 0$.

Then we write $f \rightarrow_g f'$ where

$$f' = \begin{cases} f - h_1 \mathsf{DT}^{p-1} D^\alpha g & \alpha \neq 0 \\ f - h_1 \mathsf{DT}^{p-\mathsf{Hp}(g)} g & \alpha = 0 \end{cases}$$

The reduction depends on the choice of term ordering.

We speak of the reduction of a d.p. f with respect to a finite set F of d.p.'s as yielding a normal form of f with respect to F. A normal form is achieved when no further reduction of f with respect to any member of F is possible. A normal form is not unique; it depends upon the ordering used and the order in which the different terms

are reduced. We write

$$f \rightarrow_F \ \mathsf{normal}(f, F).$$

Example 2 (reduction).

Set $f = (u_x u_y - u_x)u_{yy} - 1$
and $g = u_x u_y - u.$

Assume the lexicographic order with $y > x$. *Then* $\mathsf{HDT}(g) = u_y$, *and the algebraic reduction of* f *with respect to* g *is* $f' = (u - u_x)u_{yy} - 1$. *We can reduce* f' *(differentially) with respect to* g *to obtain*

$$f'' = uu_{yy} - 1 + u_{xy}u_y - u_y.$$

2.5 Pseudo-Reduction

Pseudo-reduction of f by a set of d.p.'s G effects an elimination from f of all derivative terms that can be obtained by differentiation of the highest derivative terms of the elements of G.

Let a derivative term DT occur in f to some power p. Suppose there exists an α such that $D^\alpha \mathsf{HDT}(g) = \mathsf{DT}$. If $\alpha = 0$ assume further that $p \geq \mathsf{Hp}(g)$. A pseudo-reduction, f', of f by g is given by the formulae

$$f' = \begin{cases} \dfrac{(\mathsf{Hcoeff}(D^\alpha g).f - \mathsf{coeff}(f, \mathsf{DT}^p).\mathsf{DT}^{p-1}.D^\alpha g)}{Z} & \alpha \neq 0 \\ \\ \dfrac{(\mathsf{Hcoeff}(g).f - \mathsf{coeff}(f, \mathsf{DT}^p).\mathsf{HDT}(g)^{(p-\mathsf{Hp}(g))}.g)}{Z} & \alpha = 0 \end{cases}$$

where $Z = \mathsf{gcd}(\mathsf{Hcoeff}(D^\alpha g), \mathsf{coeff}(f, \mathsf{DT}^p))$.(The notation gcd stands for greatest common divisor.)

Denote pseudo-reduction with respect to G by $f \rightarrow_{G,p} f'$.

Thus if $\mathsf{Hcoeff}(D^\alpha g)$ divides $\mathsf{coeff}(f, \mathsf{DT}^p)$ pseudo-reduction equals differential reduction. **Note**: the coefficient of a term DT^p contains no powers of DT: a reduction or pseudo-reduction of a term DT^p is not a reduction or pseudo-reduction of DT^q where $q > p$.

The reduction used by Ritt ([43, Chapters I, IX].) is actually pseudo-reduction, except that Ritt does not divide out by Z. Although doing so makes the proofs that follow a little more cumbersome, it is clearly advantageous to not introduce spurious factors into the equations. When no further pseudo-reduction operations can be performed on f with respect to the members of a set G, we say f is in $\mathsf{normal}^{\mathsf{p}}$ form with respect to G; the normal form is denoted $\mathsf{normal}^{\mathsf{p}}(f, G)$.

Example 3 (pseudo-reduction).

Let $f = u_{xyy} + xu_y u_{xy}$,
$g = u.u_{xy} - u_y$.

Then in either lexicographic or total degree ordering $\mathsf{HDT}(g) = u_{xy}$.

We can pseudo-reduce f *at both the* u_{xy} *and the* u_{xyy} *terms. Doing so yields*

$$f' = u.f - \frac{\partial}{\partial y} g - xu_y.g = -u_y u_{xy} + u_{yy} + xu_y^2.$$

The difference between reduction and pseudo-reduction is that in pseudo-reduction we are allowed to multiply the polynomial we are reducing by non-constant terms. We can pseudo-reduce the result again at u_{xy}*, yielding*

$$\mathsf{normal}^{\mathsf{p}}(f, \{g\}) = -u_y^2 + u_{yy}u + xu_y^2.$$

All three types of reduction defined here are noetherian relations, i.e. a normal form is achieved in a finite number of steps. In Lemma 3, we prove that pseudo-reduction is noetherian.

Lemma 3. *The pseudo-reduction relation $\longrightarrow_{F,p}$ is noetherian. That is, a* $\mathsf{normal}^{\mathsf{p}}$ *form of a d.p. f with respect to a finite set F of d.p.'s is achieved after a finite number of steps.*

Proof. Let $H(F)$ be the set

$$H(F) = \{\mathsf{HDT}(g)^q, (D^\alpha \mathsf{HDT}(g))^p \mid g \in F, q \geq \mathsf{Hp}(g), p \in \mathbb{N}, \alpha \in \mathbb{N}^n\}.$$

Suppose the pseudo-reduction process yields an infinite sequence of d.p.'s $\{f_i\}$, where $f_0 = f$. Let $S_n = \{\mathsf{DT}^p \mid \mathsf{DT}^p \text{ occurs in } f_n\}$. The set $S_n \cap H(F)$ is the list of terms where pseudo-reduction is possible. Let dt_n be the highest element in $S_n \cap H(F)$. After each reduction step, an element in S_n is replaced in S_{n+1} by a list of derivative terms (with powers), all of which are lower than the element replaced. Therefore $i > j$ implies $dt_i \leq dt_j$. By Lemma 1 we have, for N large enough, that $dt_m = dt_N$ for $m \geq N$. Let $t_1 = dt_N$. We now repeat the argument for f_N but removing dt_N from the S sets. Continuing in this way, we derive a strictly decreasing sequence $\{t_k\}$. If the number of reductions is infinite, this sequence is infinite, since we never run out of possibilities. But again by Lemma 1, any strictly decreasing sequence must be finite. □

Spurious zeroes: It is possible that pseudo-reduction of f with respect to F may lead to a spurious zero. This occurs when for some $f_i \in F, \mathsf{Sep}(f_i)$ pseudo-reduces to zero with respect to other members of F. The algorithm Reduceall outputs a set in which no element pseudo-reduces any other element at all, (such a set is then called *auto-reduced*, following Kolchin [30].) It ensures the auto-reduced set generates, as far as possible, the same ideal as the original set F; the output set generates an ideal slightly smaller than the input set. Reduceall is easily adapted to output a set in which no element pseudo-reduces any other element's separant.

Definition 2 ($M(X)$). If X is a finite set of d.p.s, define $M(X)$ to be the multiplicative set generated by factors of the elements of X. (A set M is multiplicative if $a, b \in M$ implies $ab \in M$.)

In forming $\mathsf{normal}^{\mathsf{p}}(f_k, \{f_1, ..., f_{k-1}\})$ we collect in a set denoted $X(f_k, \{f_1, ..., f_{k-1}\})$ all the factors with which f_k is multiplied in sucessive pseudo-reductions.

ALGORITHM: REDUCEALL

INPUT: a set F of differential polynomials
a term ordering
OUTPUT: sets $F' = \mathsf{reduceall}(F), X = X(\mathsf{reduceall}(F))$
the set F' is auto-reduced and the generators of F appear in $I(F')$
multiplied by factors of the elements of X.

$F' := F$
$z := 0$
$X := \{\}$
while $z = 0$ do
sort F' into increasing order $(f'_1 < f'_2 < ... < f'_r)$
for k from 2 to $|F'|$
$f''_k = \mathsf{normal}^{\mathsf{p}}(f'_k, \{f'_1, \ldots, f'_{k-1}\})$
if $f''_k = f'_k$ then $z := 1$ else $F' := F'$ minus $\{f'_k\}$ union $\{f''_k\}$
$X := X$ union $X(f'_k, \{f'_1, ..., f'_{k-1}\})$
$k := 1$
break
end

The set X is minimized if no member of F reduces (algebraically or differentially) any other member.

Lemma 4. *The algorithm "REDUCEALL" terminates.*

Proof. Suppose not. Then at least one of the original equations would be the first in an infinite strictly decreasing sequence in $R_{n,m}$. But any such sequence must terminate. □

We now show some properties of pseudo-reduction (cf [8] for equivalent properties of reduction.)

Definition 3 ($S(G)$). For G in $R_{n,m}$ let $S(G)$ be the multiplicative set in $R_{n,m}$ generated by the set of factors of all the highest coefficients and separants of the g in G. (A set S is a multiplicative set if $a, b \in S$ implies $ab \in S$.) We assume that $1, -1 \in S$.

Definition 4 ($\sim_G$). Let $\sim_G$ denote the equivalence relation generated by pseudo-reduction. That is, $f \sim_G g$ if there exists a sequence $h_1, h_2, ..., h_k$ such that $f = h_1$, $g = h_k$, and either $h_i \rightarrow_{G,p} h_{i+1}$ or $h_{i+1} \rightarrow_{G,p} h_i$.

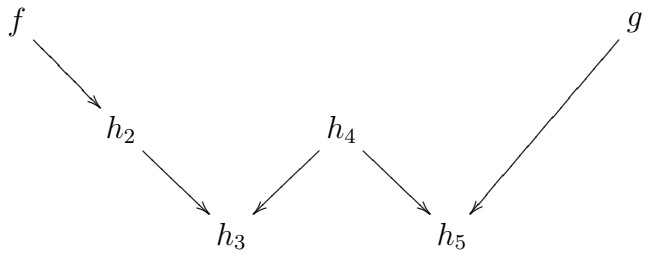


Figure 2.1:
Each arrow represents pseudo-reduction. In the diagram $f \sim g$.

Definition 5 ($f \downarrow_G g$). Let $f \downarrow_G g$ denote the fact that there exists an h such that $f \rightarrow_{G,p} h$ and $g \rightarrow_{G,p} h$, i.e. f and g have a common successor.
If $f \downarrow_G g$ then $f \sim_G g$.

We note the following properties for an arbitrary set G:
PR1 if $f \rightarrow_{G,p} g$ then $h.f \rightarrow_{G,p} h.g$ for all $h \in R_{n,m}$
PR2 if $f - g$ pseudo-reduces in one step to h, then there exist $s, s', s'' \in S(G)$ and d.p.'s f' and g' such that $f \rightarrow_{G,p} f', g \rightarrow_{G,p} g'$ and $sh = s'f' - s''g'$.

PR3 if $f - g \rightarrow_{G,p} 0$ then $s'f \downarrow_G s''g$ for some $s, s'' \in S(G)$.
PR4 if $f \rightarrow_{G,p} h$ then there exists an $s \in S(G)$ such that $s.f - h \in I$.
PR5 if $f \rightarrow_{G,p} 0$ then $h.f \rightarrow_{G,p} 0$ for all $h \in R_{n,m}$.

We prove property PR3, the others following directly from the formulae. The proof follows induction on the number of steps used to pseudo-reduce $f-g$ to zero. If $f = g$ then clearly $f \downarrow_G g$. Suppose the result is true if the pseudo-reduction uses k steps, and consider the case where the pseudo-reduction takes $k+1$ steps. Let the first step be h_1. By property PR2, there exist $s, s', s'' \in S(G)$ and d.p.'s f' and g' such that $f \rightarrow_{G,p} f', g \rightarrow_{G,p} g'$ and $sh_1 = s'f' - s''g'$. By property PR5, $sh_1 \rightarrow_{G,p} 0$ in k steps, so by the inductive step $s'f' \downarrow_G s''g'$. Hence $s'f \downarrow_G s''g$, using property PR1.□

Definition 6 ($f \equiv_G g$)**.** If $f - g \in I(G)$ then we write $f \equiv_G g$.

Lemma 5. *If $f \equiv_G g$ then $f \sim_G g$. Conversely, if $f \sim_G g$ then there exist $s_1, s_2 \in S$ such that $s_1 f \equiv_G s_2 g$.*

The proof of Lemma 5 follows that of Lemma 1 in [2].

2.6 The differential S polynomials

In direct analogy to the algebraic case, we wish to find a basis with respect to which every member of the ideal pseudo-reduces to zero. We showed in Chapter 1 that it was easy to find an example of a basis which does not satisfy this criterion merely by choosing two polynomials whose S polynomial was non-zero, and taking the ideal generated by them. Converting the example to a differential one by converting multiplication by x_i to $\dfrac{\partial}{\partial x_i}$, one can see that the following formulae are a direct generalization of the formula for the algebraic S polynomial (cf the first example following.)

Let f_1 and f_2 be two d.p.'s with the same highest unknown. Take the two multi-indices

of least degree, α^1 and α^2 such that

$D^{\alpha^1}\mathsf{HDT}(f_1) = D^{\alpha^2}\mathsf{HDT}(f_2)$.

Let $Z = \mathsf{gcd}(\mathsf{Hcoeff}(D^{\alpha^1} f_1), \mathsf{Hcoeff}(D^{\alpha^2} f_2))$.

If both $\alpha^1, \alpha^2 \neq 0$, then define

$$\mathsf{diffSpoly}(f_1, f_2) = \frac{(\mathsf{Hcoeff}(D^{\alpha^1} f_1).D^{\alpha^2} f_2 - \mathsf{Hcoeff}(D^{\alpha^2} f_2).D^{\alpha^1} f_1)}{Z}.$$

If $\alpha^1 = 0$ and $\alpha^2 \neq 0$, then

$$\mathsf{diffSpoly}(f_1, f_2) = \frac{(\mathsf{Hcoeff}(f_1)\mathsf{HDT}(f_1)^{(\mathsf{Hp}(f_1)-1)} D^{\alpha^2} f_2 - \mathsf{Hcoeff}(D^{\alpha^2} f_2) f_1)}{Z}$$

and similarly if $\alpha^1 \neq 0$ and $\alpha^2 = 0$.

If $\alpha^1 = \alpha^2 = 0$ so that $\mathsf{HDT}(f_1) = \mathsf{HDT}(f_2)$, or if f_1 and f_2 have different highest unknowns, then the differential S polynomial is defined to be

$$\mathsf{diffSpoly}(f_1, f_2) = \frac{\mathsf{Head}(f_2) f_1 - \mathsf{Head}(f_1) f_2}{\mathsf{gcd}(\mathsf{Head}(f_1), \mathsf{Head}(f_2))}$$

Calculations equivalent to differential S polynomials appear in [30, p. 136 and p. 167].

Example 4 (differential S polynomials).

(1) In the case where the differential polynomials are linear, in one unknown and with constant coefficients, the diffSpoly *calculation mimics the algebraic one, since in this case differentiation mimics multiplication by* $\dfrac{\partial}{\partial x_i}$.

Take $f_1 = u_{xxy} + u_y$

$f_2 = u_{xyy} + u$.

Then $\mathsf{diffSpoly}(f_1, f_2) = \dfrac{\partial}{\partial x_1} f_2 - \dfrac{\partial}{\partial x_2} f_1$
$= u_x - u_{yy}$

(2) The next level of generality is that of linear equations with variable coefficients.

Take $f_1 = u_{xxy} + yu_y$

$f_2 = yu_{xyy} + u$

Then $\mathsf{diffSpoly}(f_1, f_2) = \dfrac{\partial}{\partial x} f_2 - y\dfrac{\partial}{\partial y} f_1$
$= u_x - yu_y - y^2 u_{yy}$

More general examples will be given later.

A trick due to Drach ([53]) exists which converts a pde system in m unknowns $\{u^j \mid j = 1, ..., m\}$ and n variables $\{x_i \mid i = 1, ..., n\}$ to an isomorphic system in one unknown and $n + m$ variables. We take extra variables $x_{n+1}, x_{n+2}, ..., x_{n+m}$ and define the new unknown u to be

$$u = x_{n+1}.u^1 + x_{n+2}.u^2 + ... + x_{n+m}.u^m$$

so that $u^i \dfrac{\partial u}{\partial x_i}, i = n + 1, \ldots, n + m$. We then add to the system the equations

$$\frac{\partial^2 u}{\partial x_i \partial x_j} = 0 \quad \text{for } i, j \in \{n + 1, n + 2, \ldots, n + m\} \qquad (*)$$

For this system to have an ordering equivalent to the original system, it is necessary to adopt a weighted ordering. It is desirable that the given differential S polynomial formulae be compatible in the following sense: in the case of two d.p.'s in the first system having different highest unknowns, the definition of the differential S polynomial utilizes an algebraic formula whereas the isomorphic polynomials in the second system have only one unknown and hence the formula used is the differential one. The definitions above yield compatible results.

2.7 Differential Gröbner Bases

Many of the properties of Gröbner bases for polynomial ideals listed in Chapter 1 either apply directly to differential ideals or have differential analogues.

Systems that are linear, with constant coefficients and in one unknown, can be regarded as polynomials in the operators $\left\{\frac{\partial}{\partial x_i}\right\}$. Examining such systems leads us to conjecture that replacing Spolynomials with differential Spolynomials, and algebraic reduction with differential reduction in Buchberger's algorithm will yield a "differential Gröbner basis". In fact, this is only true for linear systems, or systems where the highest coefficient of every polynomial given or generated is a constant.

In systems where a highest coefficient contains a derivative term, the analogous procedure may not terminate in general. The reason is that the product rule dictates that the coefficients become differentiated while the HDT does not, and thus these terms will not reduce away in general. Thus the result of performing differential Spolynomials and reducing them will lead in general to a polynomial that is higher in rank than the ones given. This problem compounds upon iteration.

The proof of termination of Buchberger's algorithm relies on the fact that finitely generated polynomial ideals are noetherian. This means that any ascending sequence of ideals

$$I_0 \subseteq I_1 \subseteq \cdots \subseteq I_n \subseteq \cdots \subseteq R$$

in the polynomial ring R is essentially finite i.e. $\exists N$ such that $n > N$ implies $I_n = I_N$.

Differential polynomial rings are not noetherian, since they are generated algebraically by infinitely many indeterminates. However, Ritt has proved ([43]) that ascending sequences of perfect or radical ideals terminate. Hence we do not expect termination of an algorithm using reduction for systems that generate non-perfect ideals. Forsman [18] has conjectured that the algorithm will terminate, using reduction, in

radical (or perfect) ideals.

To overcome the difficulties associated with reduction, we resort to pseudo-reduction. We shall see that this compromise involves a loss of information. Nevertheless, for a large number of examples, the algorithm using pseudo-reduction yields sufficient information to answer the kinds of questions Gröbner bases answer. Moreover, for linear systems, pseudo-reduction is the same as reduction so that the same code will suffice.

The loss of information entailed in pseudo-reduction is contained, for a system G, in the set $S(G)$, which we defined earlier in this chapter. We repeat the definition here for convenience:

Definition 7 ($S(G)$). For $G \subset R_{n,m}$ let $S(G)$ be the multiplicative set in $R_{n,m}$ generated by the set of factors of all the highest coefficients and separants of the elements of G. (A set S is a multiplicative set if $a, b \in S$ implies $ab \in S$.) We assume that $1, -1 \in S$.

Property One below shows an example of this "loss of information".

The use of pseudo-reduction is not new. In his book "Differential Algebra" J.F. Ritt defined a *chain* to be an increasing sequence $\{A_n\}_{n=1}^{N}$ of elements of the differential ideal such that each A_n is pseudo-reduced with respect to $\{A_1, ..., A_{n-1}\}$. (What Ritt called reduction is today called pseudo-reduction.)
Given two chains $\mathbf{A} = \{A_n\}_{n=1}^{N}$ and $\mathbf{B} = \{B_n\}_{n=1}^{M}$, he declared $\mathbf{A} > \mathbf{B}$ if either there existed a $k < \min(N, M)$ such that $\text{rank}(A_i) = \text{rank}(B_i)$ for $i < k$ and $\text{rank}(A_k) > \text{rank}(B_k)$, or $N > M$ and rank $(A_i) = \text{rank}(B_i)$ for $i \leq M$. If neither $\mathbf{A} > \mathbf{B}$ nor $\mathbf{A} < \mathbf{B}$ then he defined the two chains to be of equal rank.

A *characteristic set* is a chain that is least in the set of chains.

Definition 8 (auto-reduced). A set G is called an *auto-reduced* basis if no element

of G pseudo-reduces any other element of G.

A characteristic set is auto-reduced.

Lemma ([43, p.5]). *A chain is a characteristic set if and only if every member of the ideal pseudo-reduces to zero with respect to it.*

This property of a characteristic set, when compared to Buchberger's original definition of a Gröbner basis, is strikingly similar. Removing the cumbersome definition of a chain, we define:

Definition 9 (differential Gröbner basis). A **differential Gröbner basis** of the differential ideal I is a basis of I with respect to which every element f of I has a unique $\mathsf{normal}^{\mathsf{p}}$ form, zero. Note that a differential Gröbner basis need not be auto-reduced while a characteristic set need not be a basis. Examples of differential Gröbner bases for given ideals are discussed in Chapter 3.

We now state and prove two important properties of differential Gröbner bases. Other important properties are discussed in this and subsequent chapters.

PROPERTY ONE

Let f_0 be the least element of the differential ideal $I(G)$ with respect to some term ordering. A differential Gröbner basis with respect to that term ordering contains an element of the form sf_0 for some $s \in S(G)$.

Proof: If not, then no other element of the differential Gröbner basis would be able to pseudo-reduce f_0 to zero, contradicting the definition of a differential Gröbner basis.

PROPERTY TWO

The system Σ is inconsistent if and only if 1 is an element of any differential Gröbner

basis for $I(\Sigma)$.

Proof: If 1 is in a differential Gröbner basis for $I(\Sigma)$, then the equations in Σ imply 1=0, which is a contradiction. Conversely, suppose the system Σ is inconsistent. Then some combination of the equations in Σ implies 1=0. But then $1 \in I(\Sigma)$, which must pseudo-reduce with respect to some element of any differential Gröbner basis for $I(\Sigma)$. But only 1 can pseudo-reduce 1. Therefore a differential Gröbner basis for any order must contain 1.

These properties show that not every basis is a differential Gröbner basis.

2.8 The main results

Buchberger proved that a basis of an algebraic ideal is a Gröbner basis if and only if every S polynomial of the basis elements reduces to zero (cf Chapter 1.). His algorithm for generating a Gröbner basis consists of computing all the Spolynomials, reducing them to normal form, adding the non-zero normal forms to the list, and ite-rating. Those Spolynomials that do not reduce to zero are precisely the obstructions to the list of polynomials being a Gröbner basis.
We now proceed to ask the question, what differential polynomials generated by members of a basis do not pseudo-reduce to zero with respect to that basis? We begin by examining the pseudo-reductions of differential Spolynomials; we shall see that the condition that all differential Spolynomials pseudo-reduce to zero is insufficient to ensure a differential Gröbner basis.

Example 5 (pseudo-reduction of a diffSpolynomial). *Let f_1 and f_2 be defined by*
$f_1 = u_y u_{xxy} + u_{xy}$
$f_2 = u_x u_{xyy} + u_{xy}$

In the lexicographic ordering with $y > x, \mathsf{HDT}(f_1) = u_{xxy}$ *and* $\mathsf{HDT}(f_2) = u_{xyy}$.

Then $\mathsf{diffSpoly}(f_1, f_2) = u_x \dfrac{\partial}{\partial y} f_1 - u_y \dfrac{\partial}{\partial x} f_2$

$$= \{u_x u_{yy} - u_y\} u_{xxy} + \{u_x - u_y u_{xx}\} u_{xyy}.$$

Reduction with respect to $\{f_1, f_2\}$ *yields* $u_x u_{yy} u_{xxy} - u_y u_{xx} u_{xyy}$, *which is greater than both* f_1 *and* f_2. *Pseudo-reducing the result with respect to* $\{f_1, f_2\}$ *results in*

$$\mathsf{normal}^{\mathsf{p}}(\mathsf{diffSpoly}(f_1, f_2), \{f_1, f_2\}) = u_{xy}\{u_y^2 u_{xx} - u_x^2 u_{yy}\}$$

which is less than either f_1 *or* f_2. *Thus, the equation generated cannot be pseudo-reduced to zero with respect to* $\{f_1, f_2\}$.

The following lemma gives an upper bound for a differential analogue for Buchberger's algorithm, replacing Spolynomial calculations with diffSpolynomial calculations and reduction with pseudo-reduction. Its proof shows how the algorithm produces a series of differential polynomials all less than the elements of the original set.

Definition 10 (the map δ). We define the map $\delta : \{\{f_i, f_j\} \mid f_i, f_j \in R_{n,m}\} \to \mathbb{N}^n$. If $\mathsf{HDT}(f_1) = p^j_{\alpha^1}$, $\mathsf{HDT}(f_2) = p^j_{\alpha^2}$, and γ^1 and γ^2 are the smallest multi-indices possible such that $D^{\gamma^1}(\mathsf{HDT}(f_1)) = D^{\gamma^2}(\mathsf{HDT}(f_2))$ then define the map δ to be $\delta(\{f_1, f_2\}) = \alpha^1 + \gamma^1 = \alpha^2 + \gamma^2$.
If $\mathsf{Hu}(f_1) \neq \mathsf{Hu}(f_2)$ then $\delta(\{f_1, f_2\}) = 0$.

The multi-indices γ^1 and γ^2 are the multi-indices used to calculate the differential S polynomial of f_1 and f_2.

Lemma 6. *For* $f_1, f_2 \in R_{n,m}$, *and the lexicographic order, or if* $\mathsf{Hu}(f_1) \neq \mathsf{Hu}(f_2)$ *or if* $\mathsf{HDT}(f_1) = \mathsf{HDT}(f_2)$, *we have*
$\mathsf{normal}^{\mathsf{p}}(\mathsf{diffSpoly}(f_1, f_2), \{f_1, f_2\}) < \max\{f_1, f_2\}$.
With the total degree ordering and $\mathsf{Hu}(f_1) = \mathsf{Hu}(f_2) = u^j$ *(say),*

$\mathsf{normal}^{\mathsf{p}}(\mathsf{diffSpoly}(f_1, f_2)), \{f_1, f_2\}) < p^j_\delta$ *where* $\delta = \delta(\{f_1, f_2\})$.
Furthermore, for $g = \mathsf{normal}^{\mathsf{p}}(\mathsf{diffSpoly}(f_1, f_2), \{f_1, f_2\})$, *we have* $\mathsf{diffSpoly}(f_1, g)$, *when pseudo-reduced with respect to* $\{f_1, f_2, g\}$ *has the same upper bounds for its derivative terms.*

Proof. If $\mathsf{Hu}(f_1) \neq \mathsf{Hu}(f_2)$ or if $\mathsf{HDT}(f_1) = \mathsf{HDT}(f_2)$, the result follows directly from the definition of the diffSpolynomial for these cases. So assume $\mathsf{Hu}(f_1) = \mathsf{Hu}(f_2)$ and $\mathsf{HDT}(f_1) \neq \mathsf{HDT}(f_2)$. Let a derivative term A occur to some power r in $g = \mathsf{normal}^{\mathsf{p}}(\mathsf{diffSpoly}(f_1, f_2), \{f_1, f_2\})$. If the power r is greater than 1, then A occurs to some power in either f_1 or f_2, so that $A^r < \max\{\mathsf{HDT}(f_1)^{\mathsf{Hp}(f_1)}, \mathsf{HDT}(f_2)^{\mathsf{Hp}(f_2)}\}$. So, let A (to the power 1) occur in g. Then there exists a derivative term B occurring to some power in say f_1, and an index $\beta \in \mathbb{N}^n$ such that $D^\beta(B) = A$.
Indices can be regarded as vectors in $\mathbb{N}^n$ and can be summed as vectors, componentwise. For a given multi-index α, the set $\alpha + \mathbb{N}^n = \{\varepsilon \mid \alpha \text{ is a summand of } \varepsilon\}$. If α^i is the multi-index for $\mathsf{HDT}(f_i)$, the sets $\alpha^1 + \mathbb{N}^n, \alpha^2 + \mathbb{N}^n$ in $\mathbb{N}^n$ are the sets of those multi-indices that can be pseudo-reduced by f_1 and f_2 respectively (see Figure 2.8.) The smallest point of intersection is the index $\delta = \delta(\{f_1, f_2\})$. From the formulae for differential S polynomials and pseudo-reduction it must be that β is a summand of γ^1 or γ^2. If $B = p^j_\sigma$, then $Q = \{\beta + \sigma \mid \beta \text{ is a summand of } \gamma^1\}$ contains the index associated with the term A. Note that $\sigma < \max\{\alpha^1, \alpha^2\}$. If A cannot be reduced by f_1 or f_2, then it must be less than one of the $\mathsf{HDT}(f_i)$ in the lexicographic order, since the set Q cannot lie in that part of $\mathbb{N}^n$ that is greater than $\max\{\alpha^1, \alpha^2\}$.
In the total degree ordering, it is possible for $|\beta + \sigma|$ to have greater magnitude than $|\alpha^1|$ or $|\alpha^2|$, and not be reducible. Nevertheless we obtain that the set Q for some A occurring in g must lie in that part of $\mathbb{N}^n$ with magnitude less than $|\delta|$.
The final statement of the lemma follows from the same considerations. □

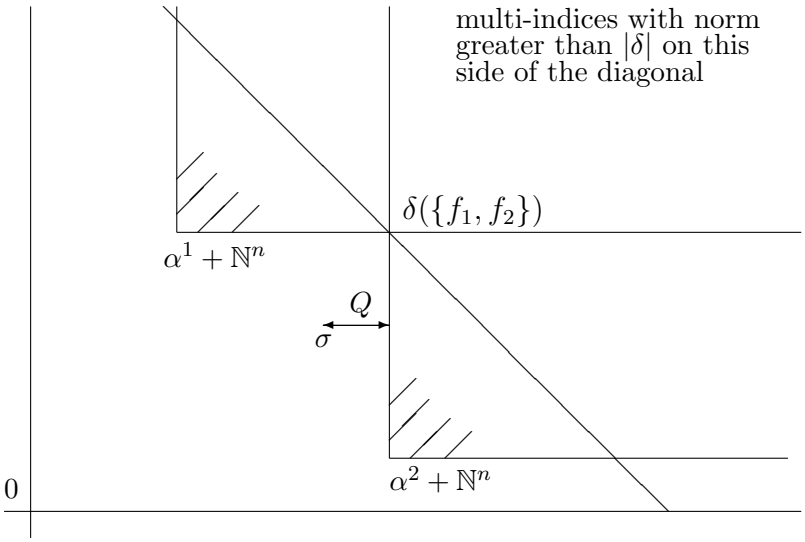


Figure 2.2:
The multi-index $\delta = \delta(f_1, f_1)$, where $\mathsf{HDT}(f_i) = \alpha^i$

Changing the example before Lemma 6, we obtain an example which shows why we need different bounds for the different orderings. Set

$f_1 = u_y u_{xxy} + u_{xy}$

$f_2 = u_x u_{xyy} + u_{xx}$

In total degree ordering the HDT's are the same as before, but we now observe that

$$\mathsf{diffSpoly}(f_1, f_2) = u_{yy} u_x u_{xxy} + u_{xyy}\{u_x - u_y u_{xx}\} - u_y u_{xxx}$$

The highest derivative term of the $\mathsf{normal}^{\mathrm{p}}$-form with respect to $\{f_1, f_2\}$ is $u_{xxx} < u_{xxyy}$ where $(2,2) = \delta(\{f_1, f_2\})$. (Recall $u_{xxyy} = p_{(2,2)}$.)

We now come to examining the result analogous to Buchberger's (Theorem 1, Chapter 1.) The replacement of Spolynomial calculations with diffSpolynomial calculations, and reductions with pseudo-reductions, "almost" yields a set that pseudo-reduces every element of the ideal to zero. In fact, in the general case, we obtain that

for every element f of the ideal $I(G)$, there is an element s of $S(G)$ such that the product $s.f$ pseudo-reduces to zero, provided $S(G) \cap I = \phi$. For a linear system, the set $S(G)$ lies in $\mathbb{F}[x_1, ..., x_n]$, so that a differential Gröbner basis is achieved.

The second and third parts of Lemma 7 below introduce two extra conditions on the set of generators G. If the first condition is satisfied (in addition to all diffSpolynomials pseudo-reducing to zero and $S(G) \cap I = \phi$), then G is a DGB. We will use this part of Lemma 7 in example 5, Chapter 3, an example which is both non-linear and non-prime. The second condition is trivially satisfied if G is auto-reduced. It gives a decomposition result for any element of the ideal that does not pseudo-reduce to zero, (again assuming that all diffSpolynomials pseudo-reduce to zero.) This decomposition result shows that if G is also a Gröbner basis for the *algebraic* ideal generated by G, then G is a DGB for $I(G)$.

Definition 11 (indets(G)). For a finite set of d.p.s G, let $\mathsf{indets}(G)$ be the set of derivative terms and variables that occur to some power in the elements of G.

Definition 12 ($I_{\mathsf{alg}}(G)$). For a finite set $G \subset R_{n,m}$, let $I_{\mathsf{alg}}(G)$ be the algebraic ideal generated by G considered as polynomials in the polynomial ring $\mathbb{F}[\mathsf{indets}(G)]$.

Definition 13 (coherent). If for all $f_i, f_k \in G$, $\mathsf{diffSpoly}(f_i, f_k) \rightarrow_{G,p} 0$, we say the set G is **coherent** ([30]).

Lemma 7. *For a set G of d.p.s, suppose*

$$(\mathsf{CNI}) \qquad \begin{cases} \mathsf{diffSpoly}(f_i, f_k) \rightarrow_{G,p} 0 \quad \forall\ f_1, f_k \in G \\ S(G) \cap I(G) = \phi. \end{cases}$$

Then (1) $\forall f \in I(G), \exists s \in S(G)$ such that $s.f \rightarrow_{G,p} 0$.

(2) if in addition to (CNI) *the condition*

$$(\mathsf{SPR}) \qquad \textit{for all} \quad s \in S(G),\ s = \mathsf{normal}^{\mathsf{p}}(s, G)$$

is satisfied, then $f \rightarrow_{G,p} 0$ for all $f \in I(G)$.

(3) if in addition to (CNI) *the condition*
(GAC) *for $f, g \in G$, if g pseudo-reduces f at the derivative term $\mathsf{DT} = D^{\alpha}\mathsf{HDT}(g)$, and $\mathsf{DT} \neq \mathsf{HDT}(f)$ if $\mathsf{Hp}(f) = 1$, then $D^{\alpha}g \in I_{\mathsf{alg}}(G)$*

is satisfied, then for all $f \in I(G), f \not\to_{G,p} 0 \Rightarrow \mathsf{normal}^{\mathsf{p}}(f) = f_0 + \sum d_i f_i$, where $f_0, f_i \in I_{\mathsf{alg}}(G)$, the d_i are in normal^p-form and $\mathsf{indets}(d_i) \cap \mathsf{indets}(G) = \phi$.

If the set G is auto-reduced, the property (GAC) is satisfied trivially.

The notation:

CNI stands for Coherent with Null Intersection,

SPR stands for S set is Pseudo- Reduced

GAC stands for G set is Almost " Complete". (if we do not require $\mathsf{DT} \neq \mathsf{HDT}(f)$ if $\mathsf{Hp}(f) = 1$, we say G is complete, or GC holds.)
The difference between GC and GAC is the following: firstly, we only need GAC, while secondly, in the DIFFGBASIS algorithm, if we complete G to satisfy GC instead of GAC, then DIFFGBASIS will not terminate in general (cf Example 5, Chapter 3.)

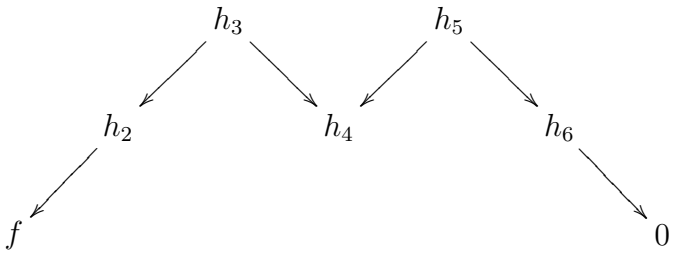
Proof. **(1)** We model the proof of this result on the proof of G3 $\Rightarrow$ G1 in [2]. Consider the condition (*):

(*) Let $f \in I(G)$. Then any two pseudo-reductions of f, to h_1 and h_2 (say), have a common successor. That is, there exist $s_1, s_2 \in S(G)$ and $k \in I$ such that $s_1 h_1 \to_{G,p} k$, and $s_2 h_2 \to_{G,p} k$.

We show that for all $f \in I(G)$, there exists an $s \in S(G)$ such that $s.f \to_{G,p} 0$.

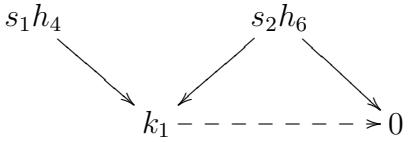
Since $f \in I(G)$, we have $f \sim 0$. That is, there exist $h_1, h_2, ..., h_n$ such that $h_1 = f, h_n = 0$ and either $h_i \to_{G,p} h_{i+1}$ or $h_{i+1} \to_{G,p} h_i$. We give an example in the

following figure:

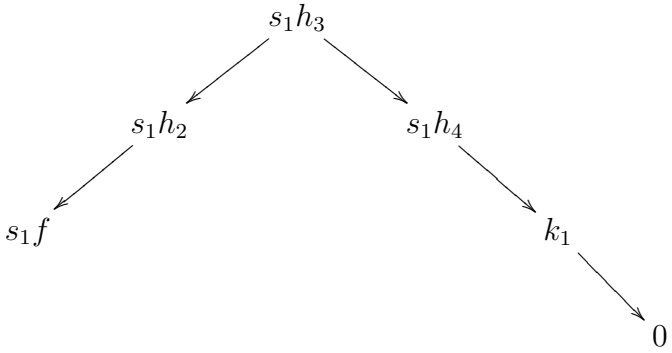


We show the argument for the example in the diagram.

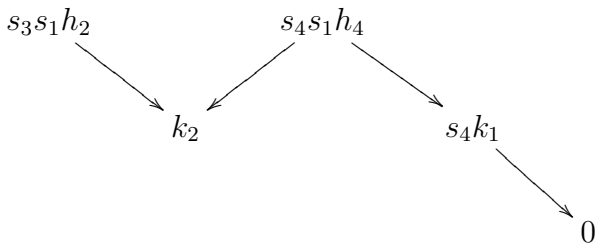
The element h_5 has two pseudo-reductions to h_4 and h_6. We apply the condition (*) and obtain s_1, s_2 and k_1 such that $s_1h_4 \rightarrow_{G,p} k_1$ and $s_2h_6 \rightarrow_{G,p} k_1$. Now we also have $s_2h_6 \rightarrow_{G,p} 0$, so applying condition (*) again we see that $s'k_1$ and 0 have a common successor, which must be 0. Reassign to s_1 the value s_1s'. This is shown schematically in the following diagram:



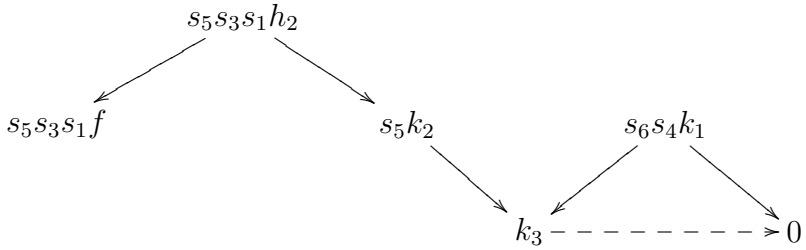
We now have the following situation:



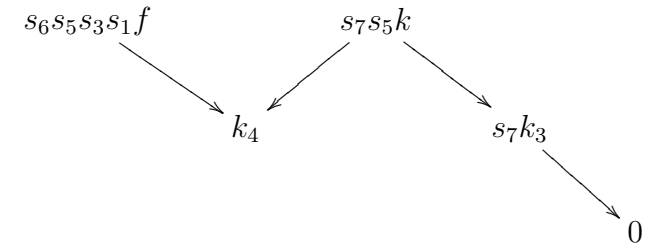
The element s_1h_3 has two successors s_1h_2 and s_1h_4, so we apply (*) to obtain:

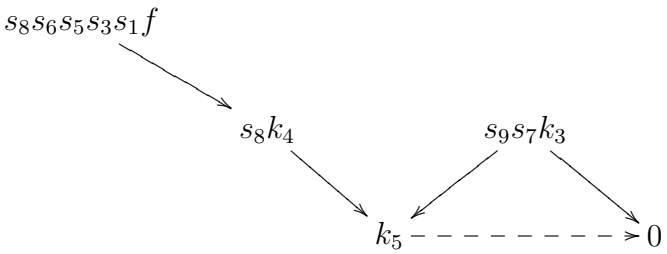


Now $s_4s_1h_4$ has two successors, leading to the diagram



where as before $s''k_3$ pseudo-reduces to zero. Continuing in this fashion, we obtain the following sequence of diagrams:





But this last diagram provides $s = s_8s_6s_5s_3s_1$ such that $s.f$ pseudo-reduces to zero. We now show that the condition (*) holds; that is, for two pseudo-reductions of $f \in I$ to h_1 and h_2, we shall show that $sh_1 \downarrow_G s'h_2$, for some $s, s' \in S(G)$.

Case 1: h_1 and h_2 are pseudo-reductions via different terms of f in different summands of f. For $f_1, f_2 \in G$ suppose f_1 reduces the term $\mathsf{DT}_1^{p_1}$, and f_2 reduces the term $\mathsf{DT}_2^{p_2}$. We have

$s_1 h_1 = \mathsf{Hcoeff}(D^{\gamma^1} f_1) f - \mathsf{coeff}(f, \mathsf{DT}_1^{p_1}) \mathsf{DT}_1^{j_1} D^{\gamma^1} f_1$, and

$s_2 h_2 = \mathsf{Hcoeff}(D^{\gamma^2} f_2) f - \mathsf{coeff}(f, \mathsf{DT}_2^{p_2}) \mathsf{DT}_2^{j_2} D^{\gamma^2} f_2$, where the index j_1 is either $p_1 - 1$ if $\gamma^1 \neq 0$ or $p_1 - \mathsf{Hp}(f_1)$ if $\gamma^1 = 0$, and similarly for j_2, while the s_i's are the relevant gcd's.

Reducing $s_1 h_1$ via the term $\mathsf{DT}_2^{p_2}$ using $D^{\gamma^2} f_2$ yields

$$s_3 s_1 h_1 = \mathsf{Hcoeff}(D^{\gamma^2} f_2) \mathsf{Hcoeff}(D^{\gamma^1} f_1) f -$$

$$\mathsf{Hcoeff}(D^{\gamma^2} f_2) \mathsf{coeff}(f, \mathsf{DT}_1^{p_1}) \mathsf{DT}_1^{j_1} D^{\gamma^1} f_1 -$$

$$\mathsf{Hcoeff}(D^{\gamma^1} f_1) \mathsf{coeff}(f, \mathsf{DT}_2^{p_2}) \mathsf{DT}_2^{j_2} D^{\gamma^2} f_2 +$$

$$\mathsf{coeff}(\mathsf{coeff}(f, \mathsf{DT}_1^{p_1}) \mathsf{DT}_1^{j_1} D^{\gamma^1} f_1, \mathsf{DT}_2^{p_2}) \mathsf{DT}_2^{j_2} D^{\gamma^2} f_2$$

where s_3 is the relevant gcd. The formula for the pseudo-reduction of $s_2 h_2$ via $\mathsf{DT}_1^{p_1}$ using $D^{\gamma^1} f_1$ inverts the indices 1 and 2. It can be seen that the first three summands are symmetric in the indices 1 and 2. The last term can be reduced away using $D^{\gamma^2} f_2$ or $D^{\gamma^1} f_1$, respectively.
Hence we have that $s h_1 \downarrow_G s' h_2$, for some $s, s' \in S(G)$.

Case 2: h_1 and h_2 are reductions of f via different terms in the same summand of f, which we write as

$$A.\mathsf{DT}_1^{p_1}.\mathsf{DT}_2^{p_2}.$$

As before we have $\mathsf{HDT}(D^{\gamma^1} f_1) = \mathsf{DT}_1, \mathsf{HDT}(D^{\gamma^2} f_2) = \mathsf{DT}_2$. We assume without loss of generality that $\mathsf{DT}_1 > \mathsf{DT}_2$, and that A contains no powers of DT_1 or DT_2. If neither DT_1 divides $\mathsf{Hcoeff}(D^{\gamma^2} f_2)$ nor DT_2 divides $\mathsf{Hcoeff}(D^{\gamma^1} f_1)$, then the proof

that $sh_1 \downarrow_G s'h_2$, for some $s, s' \in S(G)$ mirrors that of Case 1. So suppose (letting red stand for reductum) that

$$D^{\gamma^1} f_1 = B_1.\mathsf{DT}_2^{k_1}.\mathsf{DT}_1^q + \mathsf{red}(D^{\gamma^1} f_1)$$

$$D^{\gamma^2} f_2 = B_2.\mathsf{DT}_1^{q'}.\mathsf{DT}_2^{k_2} + \mathsf{red}(D^{\gamma^2} f_2)$$

Since $\mathsf{HDT}(D^{\gamma^2} f_2) = DT_2, q' = 0$. We show the calculation for $k_1 < k_2$, the case $k_1 \geq k_2$ being similar. Furthermore, since $\mathsf{DT}_2 \in S(G)$ and $S(G) \cap G = \phi$, then $\mathsf{red}(D^{\gamma^2} f_2) \neq 0$. Since $k_2 > k_1 \geq 1$, we have $\gamma^2 = 0$.

Finally let

$$\begin{aligned} & f = A.\mathsf{DT}_1^{p_1}.\mathsf{DT}_2^{p_2} + \mathsf{rest}(f) \\ & s_1 = \mathsf{gcd}(B_1, A) \\ \text{and} \quad & s_2 = \mathsf{gcd}(B_2, A) \end{aligned}$$

Then

$$\begin{aligned} & s_1 h_1 = B_1 f - A.\mathsf{DT}_2^{(p_2 - k_1)} \mathsf{DT}_1^{(p_1 - q)} D^{\gamma_1} f_1 \\ \text{and} \quad & s_2 h_2 = B_2 f - A.\mathsf{DT}_2^{(p_2 - k_2)} \mathsf{DT}_1^{p_1}.f_2 \end{aligned}$$

so that

$$B_2 s_1 h_1 - B_1 s_2 h_2 = -A.\mathsf{DT}_1^{(p_1 - q)} \mathsf{DT}_2^{(p_2 - k_2)}.$$

$$[B_2 \mathsf{DT}_2^{(k_2 - k_1)} D^{\gamma^1} f_1 - B_1.\mathsf{DT}_1^q f_2].$$

Set $g = [B_2 \mathsf{DT}_2^{(k_2 - k_1)} D^{\gamma^1} f_1 - B_1.\mathsf{DT}_1^q f_2]$.
(If the B_i are monomials, then g is proportional to the algebraic Spolynomial of $D^{\gamma^1} f_1$ and f_2.)

We have

$$g = B_2 \mathsf{DT}_2^{(k_2 - k_1)} \mathsf{red}(D^{\gamma^1} f_1) - B_1.\mathsf{DT}_1^q \mathsf{red}(f_2).$$

Recall that $\mathsf{red}(f_2) \neq 0$. Furthermore, DT_1 does not occur in f_2, since $\mathsf{HDT}(f_2) = \mathsf{DT}_2$ and $\mathsf{DT}_1 > \mathsf{DT}_2$. Pseudo-reducing g with respect to f_1 at the term DT_1^q yields

$$(B_2 \mathsf{DT}_2^{k_2} + \mathsf{red}(f_2)) \mathsf{red}(D^{\gamma_1} f_1).$$

Regardless of whether $\mathsf{red}(D^{\gamma^1} f_1)$ contains any powers of DT_2 or not, this last polynomial pseudo-reduces to 0 with respect to f_2. Hence we have that

$$B_2 s_1 h_1 - B_1 s_2 h_2 \rightarrow_{G,p} 0.$$

Since the $B_i \in S(G)$, we have by property $\mathsf{PR3}$ that $sh_1 \downarrow_G s'h_2$, for some $s, s' \in S(G)$, as required.

Case 3: h_1 and h_2 are reductions of f via the same term DT^p. In this case we have $\mathsf{HDT}(D^{\gamma^1} f_1) = \mathsf{HDT}(D^{\gamma^2} f_2) = \mathsf{DT}$. From the formulae above for $s_1 h_1, s_2 h_2$ we have that

$$\mathsf{Hcoeff}(D^{\gamma^2} f_2) s_1 h_1 - \mathsf{Hcoeff}(D^{\gamma^1} f_1) s_2 h_2$$
$$= s\ \mathsf{coeff}(f, \mathsf{DT}^p) \mathsf{DT}^k \mathsf{diffSpoly}(D^\alpha f_1, D^\alpha f_2)$$

where $s = \mathsf{gcd}(\mathsf{Hcoeff}(D^{\gamma^1} f_1), \mathsf{Hcoeff}(D^{\gamma^2} f_2))$, and

$$k = \begin{cases} p - 1 & \gamma^1, \gamma^2 \neq 0 \\ p - \mathsf{Hp}(f_1) & \gamma^1 = 0, \gamma^2 \neq 0 \\ p - (\mathsf{Hp}(f_1) - \mathsf{Hp}(f_2)) & \gamma^1, \gamma^2 = 0, \mathsf{Hp}(f_1) \geq \mathsf{Hp}(f_2) \end{cases}$$

while $\alpha \in \mathbb{N}^n$. The multi-index α is non-zero in the case $\gamma^1, \gamma^2 \neq 0$ only. We now show that condition (CNI) implies that $\mathsf{diffSpoly}(D^\alpha f_1, D^\alpha f_2)$ must pseudo-reduce to zero for all $\alpha \in \mathbb{N}^n$; then we can use property $\mathsf{PR3}$ to show that $sh_1 \downarrow_G s'h_2$, for some $s, s' \in S(G)$.

We recall the following definition:

Definition. We define the map $\delta : \{\{f_i, f_j\} \mid f_i, f_j \in R_{n,m}\} \rightarrow \mathbb{N}^n$. If $\mathsf{HDT}(f_1) = p^j_{\alpha^1}$, $\mathsf{HDT}(f_2) = p^j_{\alpha^2}$, and γ^1 and γ^2 are the indices of least degree possible such that $D^{\gamma^1}(\mathsf{HDT}(f_1)) = D^{\gamma^2}(\mathsf{HDT}(f_2))$ then $\delta(\{f_1, f_2\}) = \alpha^1 + \gamma^1 = \alpha^2 + \gamma^2$.
If $\mathsf{Hu}(f_1) \neq \mathsf{Hu}(f_2)$ then $\delta(\{f_1, f_2\}) = 0$.

Since $\mathsf{HDT}(D^{\gamma^1} f_1) = \mathsf{HDT}(D^{\gamma^1} f_1)$, we have $\mathsf{Hu}(D^{\gamma^1} f_1) = \mathsf{Hu}(D^{\gamma^2} f_2)$. Let $\delta_{ij} = \delta(\{f_i, f_j\})$. Repeating the calculations above for $f = \mathsf{diffSpoly}(D^{\alpha^1} f_{i_1}, D^{\alpha^1} f_{j_1})$, with

$f_{i_1}, f_{j_1} \in G$, with the DT we are reducing with respect to $f_{i_2}, f_{j_2} \in G$ having associated multi-index $\varepsilon \in \mathbb{N}^n$, the 'difference' of the pseudo-reductions contains $\mathsf{diffSpoly}(D^{\alpha^2} f_{i_2}, D^{\alpha^2} f_{j_2})$ for some index α^2. Since f is a diffSpolynomial, the term with index $\alpha^1 + \delta_{i_1 j_1}$ has cancelled, so that ε is strictly less than $\alpha^1 + \delta_{i_1 j_1}$. But $\varepsilon = \alpha^2 + \delta_{i_2 j_2}$. Now using induction on α and the $\{\delta_{ij} \mid f_i, f_j \in G\}$.

Proof of Lemma 7 (2): For $f \in I(G)$, such that $f \not\to_{G,p} 0$, there exists $s \in S(G)$ such that $s.f \to_{G,p} 0$. We can assume that f is in normal$^{\mathrm{p}}$-form. Look at a pseudo-reduction of sf at the term DT^p, using $g_0 \in G$. There are two possibilities:

(i) DT^p occurs in s

(ii) DT occurs to some power in both s and f.

Suppose condition (SPR) is satisfied. Then the case (1) cannot occur. But neither can case (2), since then a suitable power of s, which is also an element of $S(G)$, would pseudo-reduce. Thus we arrive at a contradiction.

Proof of Lemma 7 (3): For $f \in I(G)$, such that $f \not\to_{G,p} 0$, there exists an $s \in S(G)$ such that $s.f \to_{G,p} 0$. It cannot be that $s \to_{G,p} 0$, for then $\exists s' \in S(G)$ such that $s'.s \in I(G)$ (by $\mathsf{PR4}$), which contradicts $S(G) \cap I(G) = \phi$. We can assume that f is in normal$^{\mathrm{p}}$-form.

Look at a pseudo-reduction of $s.f$ at the term DT^p in some summand of $s.f$, using $g_0 \in G$. We have that $\mathsf{DT} = D^{\alpha}\mathsf{HDT}(g_0)$. There are two possibilities:

(i) DT^p occurs in s

(ii) DT occurs to some power in both f and s.

Suppose the condition (GAC) holds, and consider the possibility (i). If DT^p occurs in some $\mathsf{Hcoeff}(g)$ or $\mathsf{Sep}(g)$ for some $g \in G$, then g_0 pseudo-reduces that g, so that by (GAC), $D^{\alpha} g_0 \in I_{\mathsf{alg}}(G)$. Otherwise DT occurs in some $\mathsf{Hcoeff}(g)$ or $\mathsf{Sep}(g)$, but only to powers less than in g_0. Thus $\mathsf{HDT}(g_0) = \mathsf{DT}$. Either way, the pseudo-reduction of sf has the form $h_1 = s'sf - \mathsf{coeff}(sf, \mathsf{DT}^p)\mathsf{DT}^k g'$ for some $g' \in I_{\mathsf{alg}}(G), k \in \mathbb{N}$. Now consider the second possibility (ii). In this case, DT occurs in f but too small a power to be pseudo-reduced by g_0. In this possibility, the pseudo-reduction of sf has the

form

$$h_1 = s'sf - \mathsf{coeff}(sf, \mathsf{DT}^p)\mathsf{DT}^k g_0, \qquad k \in \mathbb{N}.$$

Now consider the second step in the pseudo-reduction of sf to zero. This time there is a third possibility, namely our new DT satisfies

(iii) DT^p occurs in g_0 or g' (both elements of $I_{\mathsf{alg}}(G)$, so that $\mathsf{DT} \in \mathsf{indets}(G)$).

Note we do not need DT to be $\mathsf{HDT}(g_0)$ or $\mathsf{HDT}(g')$ if the highest power is one. By the condition (GAC), and using similar reasoning as above, a pseudo-reduction of such a term leads to the second pseudo-reduction of sf having the form

$$h_2 = s''\, h_1 - \mathsf{coeff}(h_1, \mathsf{DT}^p)\; g'' \quad g'' \in I_{\mathsf{alg}}(G).$$

Continuing until sf is pseudo-reduced to zero, we obtain an "expansion" of sf, namely, $s'sf = f_0 + \sum d_i f_i$, where $f_0, f_i \in I_{\mathsf{alg}}(G)$, the d_i are in normal$^{\mathrm{p}}$-form and $\mathsf{indets}(d_i) \cap \mathsf{indets}(G) = \phi$. (Recall that $\forall s \in S(G), \mathsf{indets}(s) \subseteq \mathsf{indets}(G)$, so that $g' \in I_{\mathsf{alg}}(G)$ implies $sg' \in I_{\mathsf{alg}}(G)$.)

We now show that the expansion of $s'sf$ and the fact $f \in I(G)$ implies that f has a similar expansion. So suppose not, i.e. suppose that to obtain f we need to differentiate elements of G (derivatives not contained in $I_{\mathsf{alg}}(G)$). Consider the highest derivative term of one of the differentiated elements of G. This derivative term cannot appear in f since it does not appear in $s'sf$ and $\mathsf{indets}(f) \subseteq \mathsf{indets}(s'sf)$. Thus it must cancel with another derivative term, i.e. the expansion of f involves differential S polynomials and their pseudo-reductions. But all differential S polynomials pseudo-reduce to zero. Since f is in normal$^{\mathrm{p}}$-form, we have a contradiction. □

Example 6 (a coherent system that is not a DGB). *Consider the system* Σ *generated by*

$$f_1 = u_x^2 - 1$$
$$f_2 = u_y^2 - 1$$
$$f_3 = (u_x + u_y)u_z - 1$$

in the lexicographic ordering with $z > y > x$. *Then* $S(G) = M\{u_x, u_y, u_x + u_y\}$. *The three generators of* Σ *form an auto-reduced set, and all diffSpolynomials pseudo-reduce to zero. Now* $u_y f_3 - u_z f_2 - u_x f_3 + u_z f_1 = u_x - u_y \in I(F)$, *but* $u_x - u_y$ *does not*

pseudo-reduce to zero. However, there exists an element s of S(G) such that $s(u_x - u_y)$ *does pseudo-reduce to zero, namely* $s = u_x + u_y$.

Theorem 1. *Let G be a finite set of differential polynomials. Suppose that*
(i) $\mathsf{diffSpoly}(f_i, f_k) \rightarrow_{G,p} 0 \quad \forall f_i, f_k \in G$
(ii) G is a Gröbner basis for $I_{\mathsf{alg}}(G)$ *(i.e. every element of* $I_{\mathsf{alg}}(G)$ *reduces (algebraically) to zero with respect to G.) and either:*
(SPR) *for all* $s \in S(G)$, $s = \mathsf{normal}^{\mathsf{p}}(s, G)$
or
(GAC) *for* $f, g \in G$, *if g pseudo-reduces f at the derivative term* $\mathsf{DT} = D^{\alpha}\mathsf{HDT}(g)$, $(\mathsf{DT} \neq \mathsf{HDT}(f)$ *if* $\mathsf{Hp}(f) = 1)$, *then* $D^{\alpha}g \in I_{\mathsf{alg}}(G)$, *and* $S(G) \cap I(G) = \phi$.
Then G is a differential Gröbner basis for $I(G)$.

Notes:
(1) If G is auto-reduced, condition (GAC) holds trivially.
(2) The condition $S(G) \cap I(G) = \phi$ is necessary. An example appears in Chapter 5 which violates this condition and for which the set is not a DGB.
(3) A close examination of the proof of Lemma 7 shows that one can replace the condition $S(G) \cap I(G) = \phi$ with the condition $\mathsf{normal}^{\mathsf{p}}(s, G) \neq 0 \; \forall s \in S(G)$.
(4) Schwarz [48] considers **orthomonic** systems (following Janet and Riquier.) Such systems can be written $\mathsf{HDT}(f) + ... = 0$, where the remainders of all the equations in the system do not contain any highest derivative term or any derivative of them. For such systems, coherence will guarantee the system is a DGB, since they are automatically Gröbner bases for the algebraic ideal they generate, and the condition SPR holds.

Proof. We first show that the conditions of being coherent, a Gröbner basis for the algebraic ideal, and SPR are sufficient to guarantee $S(G) \cap I(G) = \phi$. Suppose not. Let $s \in S(G) \cap I(G)$. Now SPR implies that

$$\mathsf{indets}(S(G)) \cap \{D^{\alpha}(\mathsf{HDT}(g)) \mid \alpha \in \mathbb{N}^n, g \in G\} = \phi.$$

Hence the expansion of s involves cancelling of the highest terms of the elements of G, either algebraically or differentially. But that implies that there is either an algebraic or differential S polynomial that does not pseudo-reduce to zero, a contradiction.

Applying Lemma 5, $\forall f \in I(G)$, either $f \rightarrow_{G,p} 0$, or $\mathsf{normal}^{\mathrm{p}}(f) = f_0 + \Sigma d_i f_i$, where $f_0, f_i \in I_{\mathsf{alg}}(G)$, the d_i are in normal$^{\mathrm{p}}$-form and $\mathsf{indets}(d_i) \cap \mathsf{indets}(G) = \phi$. But G is a Gröbner basis for $I_{\mathsf{alg}}(G)$, so $f \rightarrow_G 0$. But if f reduces to zero, it pseudo-reduces to zero. Thus, G pseudo-reduces every element of $I(G)$ to zero, and hence it is a differential Gröbner basis for $I(G)$. □

2.9 The Algorithms

We now present three algorithms. The first is analogous to Buchberger's, and was first written down by Carrà-Ferro [12] , who called it the Kolchin-Ritt algorithm. As noted above, this algorithm generates a DGB where the input equations are linear.

ALGORITHM KOLCHIN-RITT

INPUT: a finite basis $F = \{f_1, f_2, ..., f_N\}$ for a differential ideal I
a term ordering
OUTPUT: sets $F' = \mathsf{reduceall}(F), X = X(\mathsf{reduceall}(F))$
a set G =Kolchin-Ritt(F) such that

$$S(G) \cap I(G) = \phi \Longrightarrow \forall g \in I(G), \exists s \in S(G) \text{ such that } sg \rightarrow_{G,p} 0$$

$G := F$

pairset:= $\{\{f_i, f_k\} \mid f_i, f_k \in G\}$
while pairset$\neq \{\}$
for $\{f_i, f_k\}$ in pairset do
pairset:=pairset minus $\{\{f_i, f_k\}\}$
$m :=$ $\mathsf{normal}^{\mathsf{p}}(\mathsf{diffSpoly}(\{f_i, f_k\}), G)$
if $m \neq 0$ do
pairset:=pairset union $\{\{f_i, m\} \mid f_i \in G\}$
$G := G$ union $\{m\}$

end

We need the condition $S(G) \cap I(G) = \phi$ not only in order to use Lemma 7, but also because spurious zeroes can result when pseudoreducing with a polynomial whose highest coefficient or separant pseudo-reduces to zero (so that $S(G) \cap I(G) = \phi$ is violated).

Proof of termination of Kolchin-Ritt:

Let the basis after the nth iteration be G_n, and let g_n be the least element of G_n. Consider the sequence $\{g_n\}$. Since $G_n \supset G_{n-1}$, this sequence is decreasing and hence terminates, at N_1, say. Denote the terminal value by h_1. Now iterate the argument for $n > N_1$, on $G_n \backslash \{h_1\}$. Continuing in this way, we produce an increasing sequence $\mathcal{H} = \{h_m\}$. Now every element of $G_N \backslash G_{N-1}$ is pseudo-reduced with respect to every element of G_{N-1}, and hence in the sequence $\mathcal{H}$, h_m is pseudo-reduced with respect to $\{h_1, ..., h_{m-1}\}$. If the sequence $\mathcal{H}$ is infinite, the sequence $\{\mathsf{Hu}(h_m)\}$, will be infinite for at least one unknown u^j, and we consider the subsequence of $\mathcal{H}$ consisting of those elements with highest unknown u^j. Examining the sequence $\mathcal{H}I = \{x^{\alpha^m} | \mathsf{HDT}(h_m) = p^j_{\alpha^m}\}$, we obtain by Dickson's Lemma for polynomial ideals that $\exists M$ such that for $m > M, x^{\alpha^m}$ has a divisor in one of the $\{x^{\alpha^1}, ..., x^{\alpha^{M-1}}\}$. This contradicts the fact that the sequence is pseudo-reduced. Thus for some $M_1, m > M_1 \Rightarrow \mathsf{HDT}(h_m) =$

$\mathsf{HDT}(h_{m_1})$. But in a pseudo-reduced sequence, if the HDT's terminate, so does the sequence. □

We now show an algorithm that "Almost Completes" a set of d.p.'s to a new set that does satisfy GAC.

ALGORITHM GAC

INPUT: a set F of d.p.'s
OUTPUT: a set $G \supset F$ such that G satisfies GAC

$G := F$
$H := F$;
while $H \neq \{\}$
  $H := \{\}$
  for g in G
  for f in F
    for DT^p occurring in g
      if $\mathsf{DT} = \mathsf{HDT}(g)$ and $\mathsf{Hp}(g) = 1$ then next
      if $\mathsf{DT} = D^\alpha\mathsf{HDT}(f)$ for some α and $D^\alpha f \notin I_{\mathsf{alg}}(G)$
        then $H := H$ union $\{D^\alpha f\}$
  $G := G$ union H

Termination of GAC:

Denote by F_n the set H at the end of the nth iteration, $F_0 = F$. We show $\exists N$ such that $F_n = \{\}$ for $n > N$.
The set F_n consists of those polynomials of the form $D^\alpha f_i$, which do not reduce to zero with respect to F_{n-1}, for some $f_i \in F$ such that $D^\alpha\mathsf{HDT}(f_i)$ occurs in an element of F_{n-1}. Note $F_n \cap F_{n-1} = \phi$. Suppose the sequence $\{F_n\}$ is infinite. Pick the highest

element of F_n, $t_n = D^\sigma f_j$, where $\sigma = \sigma(n), j = j(n)$, with $D^\sigma \mathsf{HDT}(f_j)$ occurring in some element s_n of F_{n-1}, and $D^\sigma \mathsf{HDT}(f_j) \neq \mathsf{HDT}(s_n)$ if $\mathsf{Hp}(s_n) = 1$. Let $\mathcal{S} = \{s_n\}$. Now by construction, $t_{n-1} \geq s_{n-1} > t_n$, so that $t_{n-1} > t_n$. (Note: if $\mathsf{Hp}(s_n) > 1$, then any derivative of f_j such that $D^\alpha \mathsf{HDT}(f_j) = \mathsf{HDT}(s_n)$ will be less than s_n. If we do not need to differentiate f_j to obtain $\mathsf{HDT}(f_j) = \mathsf{HDT}(s_n)$, then since f_j is in F it is not added to H.) Thus $\{t_n\}$ is a strictly decreasing sequence, which terminates by Lemma 2. □

Proof of correctness of GAC:

Suppose that a derivative term DT occurs in some element t_n of F_n, and an element t_{n-1} of F_{n-1} pseudo-reduces t_n at DT. Now $t_{n-1} = D^\alpha \mathsf{HDT}(f_i)$ for some element f_i of F, so that f_i pseudo-reduces t_n at DT. □

Finally, a simple check will determine if a set G of D.P.'s satisfies SPR. We first check that no element of G pseudo-reduces any other element's highest coefficient or separant. We then check that no HDT occurs in any other element's highest coefficient or separant. Finally, we check that no HDT occurs to any power other than one. (Any system containing a polynomial whose HDT occurs to a power higher than 1 will never satisfy SPR.) If the check holds, we write $\mathsf{SPR}(G)$ = true, otherwise we write $\mathsf{SPR}(G)$ = false.

Definition 14. ($\mathsf{GB}_{\mathsf{alg}}(G$,termorder)).
For a set of d.p.s G, denote by $\mathsf{GB}_{\mathsf{alg}}(G$,termorder) the Gröbner basis for $I_{\mathsf{alg}}(G)$ generated by Buchberger's algorithm (using algebraic reduction with respect to the given termorder.)

ALGORITHM DIFFGBASIS

INPUT: a set F of d.p.s
a term ordering

OUTPUT: sets G such that $I(G) = I(F)$,
(1) G is coherent
(2) G satisfies SPR or GAC

Thus if $S(G) \cap I(G) = \phi$, then G is a differential Gröbner basis for $I(F)$.

$G := \{\}$

$H := F$

while $G \neq H$

$G := H$

$H :=$Kolchin-Ritt(G)

if $\mathsf{SPR}(H)$ then $G := H$, end

$H := \mathsf{GB}_{\mathsf{alg}}(H)$

$H := \mathsf{GAC}(H)$

Notes (1): the set of differential coefficients $S(G)$ will be minimized if G is converted to an algebraically reduced set (i.e. the output of the Gröbner basis algorithm is reduced.)

(2): The proof of Lemma 7 (1) Case 3 shows that if a set F is coherent, then $\mathsf{diffSpoly}(D^\alpha f_i, D^\beta f_k) \rightarrow_{F,p} 0$ for all $\alpha, \beta \in \mathbb{N}^n$. Hence we can reduce the number of pairs considered in Kolchin-Ritt after the first iteration. Such a reduction may not improve the efficiency of the algorithm, as experimental evidence shows. It appears that for the Maple symbolic algebra programme in which these algorithms have been implemented, keeping the outputs of previous iterations in memory causes a significant increase in running time.

Proof of termination of DIFFGBASIS:

Let F_n be the output of the algorithm after the nth iteration. We have $F_m \supset F_{m-1}$. Let h_m be the maximum element of $F_m \backslash F_{m-1}$. As in the proof of termination of the Kolchin-Ritt algorithm we consider for the sequence $\mathcal{H} = \{h_m\}$, the sequence

$\mathcal{H}I = \{x^{\alpha^m} \mid \mathsf{HDT}(h_m) = p^j_{\alpha^m}\}$, (if necessary for a suitable sub-sequence of $\mathcal{H}$, all with the same highest unknown u^j). We obtain by Dickson's Lemma for polynomial ideals that $\exists M$ such that for $m > M, x^{\alpha^m}$ has a divisor in one of the $\{x^{\alpha^1}, ..., x^{\alpha^{M-1}}\}$. Let $m > M$. Now the output of Kolchin-Ritt is pseudo-reduced with respect to F_M, while the Gröbner basis algorithm does not alter the list of derivative terms occurring in H, so there is an d.p. t_m, of the output of GAC in F_m or F_{m-1}, containing the highest derivative term of h_m. The d.p. t_m has its highest derivative term occurring in a d.p. in $F_{m-1} \backslash F_{m-2}$ or in $F_{m-2} \backslash F_{m-3}$. Hence for $m > M, \mathsf{HDT}(h_m) \leq HDT(t_m) \leq \mathsf{HDT}(h_{m-1})$ or $\mathsf{HDT}(h_{m-2})$. Hence the sequence $\{\mathsf{HDT}(h_m)\}$ terminates. Consider next the sequence $\mathcal{HP} = \{\mathsf{Hp}(h_m)\}$. No calculations performed in either Kolchin-Ritt, GB or GAC lead to higher Highest powers, so $\mathcal{HP}$ also terminates at $m = M$.

Thus for $m > M$, the h_m all have the same highest derivative term raised to the same power. The algorithm GAC will not output a d.p. with the same $\mathsf{HDT}^{\mathsf{Hp}}$ as h_M, as it outputs only d.p.'s whose HDT's occur to some power in the separants and tails of existing d.p.'s, while the output of Kolchin-Ritt is pseudo-reduced (Kolchin-Ritt will not output another dp with the same HDT as h_{m-1}), so we obtain that h_m is output by GB. Thus h_m is the normal form of an Spolynomial. It is indeed possible to obtain increasing higher coefficients, as the following calculation shows:

$$f_1 = \mathsf{HC}_1\mathsf{HDT}(h_m) + \mathsf{tail}_1$$
$$f_2 = \mathsf{HC}_2\mathsf{HDT}_2 + \mathsf{tail}_2$$

where $\mathsf{HDT}_2 = \mathsf{HDT}(f_2) \neq \mathsf{HDT}(h_m)$.

Then

$$\mathsf{Spoly}(f_1, f_2) = \frac{\mathsf{HC}_1\mathsf{HDT}(h_m)\mathsf{tail}_2 - \mathsf{HC}_2\mathsf{HDT}_2\mathsf{tail}_1}{\mathsf{gcd}(\mathsf{HC}_1, \mathsf{HC}_2)}.$$

So all we require is that $\mathsf{tail}_2 > \mathsf{HC}_1$ and $\mathsf{gcd}(\mathsf{HC}_1, \mathsf{HC}_2) \neq 1$, so that the Spoly does not reduce to zero.

Consider the sequence $\mathcal{HC} = \{\mathsf{Hcoeff}(h_m), m > M\}$. We show the sequence $\mathcal{HC}$ must terminate. Suppose the sequence $\mathcal{HC}$ increases indefinitely. We follow the same

argument as for $\mathcal{H}$ above on the sequence $\{\mathsf{HDT}(\mathsf{Hcoeff}(h_m)) : m > M\}$, to obtain a d.p. t_m output by GAC that contains the DT, $\mathsf{HDT}(\mathsf{Hcoeff}(h_m))$ for $m > M_0$ (say). We have $t_m = D^{\alpha^m}(g_m)$ for some $\alpha^m \in \mathbb{N}^n$, where the g_i are output by GB or Kolchin-Ritt. The DT, $\mathsf{HDT}(\mathsf{Hcoeff}(h_m))$ will be in the tail of $D^{\alpha^m}(g_m)$ (by the calculation of the Spoly above). Comparing g_{M_0+1} with g_{M_0+2} we have that if $\mathcal{H}C$ increases, the tail of g_{M_0+2} is higher than that of g_{M_0+1} . By considering the sequence $\{\mathsf{HDT}(\mathsf{tail}(g_i))\}$ and applying the Dickson's Lemma argument, we have that for large enough i, the g_i are output by GB. Since the GB algorithm does not alter the list of DT's in its input, we obtain a d.p. output by GAC in the previous iteration of DIFFGBASIS containing the $\mathsf{DT}, \mathsf{HDT}(\mathsf{tail}(g_i))$. In this way, we see that indefinite increasing in the sequence $\mathcal{H}C$ is caused by successive differentiation of existing d.p.s in the GAC algorithm and forming Spolynomials of the h_i with this output of GAC. But the output of GAC is always lower than its input d.p.'s, so that any such succession must lead to a decreasing $\mathsf{Hcoeff}(h_m)$, a contradiction. The same argument shows that the sequence $\{\mathsf{Hcoeff}(\mathsf{Hcoeff}(h_m))\}$ must terminate. Finally for sufficiently high m, $\mathsf{Hmon}(h_m) = \mathsf{Hmon}(h_{m+1})$. Now none of GB, Kolchin-Ritt or GAC will output a d.p. with the same highest monomial as an existing d.p., so that the sequence $\{h_m\}$ terminates. □

There is another way to achieve GAC, namely by converting bases to be auto-reduced. This method causes the output ideal to be smaller than the input ideal, with a smaller solution set. In some examples, the output ideal has only the trivial solution, as shown in Example 5, Chapter 3.

2.10 Chapter 2, Conclusion

We have defined a differential Gröbner basis to be a basis with respect to which every element of the ideal pseudo-reduces to zero, and we have proved a characterisation

theorem for such a basis.

The algorithm to generate a differential Gröbner basis is seen to require both the algebraic version of Buchberger's algorithm, and the differential analogue of Buchberger's algorithm, the Kolchin-Ritt algorithm. In addition, a completion algorithm is required. All conditions necessary to ensure the output is a differential Gröbner basis are guaranteed to hold, bar one: if the output is G (say), then we do not check whether $S(G) \cap I(G) = \phi$ holds in general.

Chapter 3

PRACTICE IS EASIER THAN THEORY

This chapter demonstrates the algorithm on several types of systems, and the effects of using different orderings is discussed. Further examples are to be found in Chapter 4, where resolvent systems and elimination ideals are calculated, and in Chapter 5, where several extensions to the algorithm are given.

The first example is that of a linear system in one unknown function with constant coefficients. This class of examples can be viewed as polynomials in the operators $\left\{\frac{\partial}{\partial x_i}\right\}$, so the algebraic theory can be used for these examples. We show that the differential theory yields exactly equivalent results to the algebraic algorithm for this class of system.

We then discuss a linear example with variable coefficients. Thirdly, the well-known calculations for the Korteweg-de Vries equations are shown to be an example of the algorithm.

The last two systems are non-linear systems. It is in these systems that the conditions for Theorem 1 need to be checked carefully.

It is not hard to see from these examples that the algorithm is used to generate from the given equations more equations that are in some sense simpler. That is, they involve fewer unknowns and variables. One then solves, if possible, from the simplest equations up. This phenomenon is the content of the "elimination ideals" which are discussed in the next chapter. Obviously, finding the "right" coordinates and the right ordering is vital both to efficiency and to the utility of the output.

A major problem with both the algebraic theory and the differential theory is that seemingly simple input equations can generate expressions involving hundreds of terms. An interesting paper by D. Lazard [31] indicates another method, albeit less intuitive, which contains the possibility that control of the S-sets can be made part of the theory.

3.1 Example 1: Linear, constant coefficients

The system has one unknown u, and five variables $\{x, y, z, w, t\}$, and is generated by

$$\begin{cases} f_1 = u_{wt} - u_{xx} \\ f_2 = u_{zt} - u_{xw} \end{cases}$$

Assume the lexicographic ordering based on $t > w > z > y > x$, so that $\mathsf{HDT}(f_1) = u_{wt}$, and $\mathsf{HDT}(f_2) = u_{zt}$. Then

$$\mathsf{diffSpoly}(f_1, f_2) = \frac{\partial}{\partial w} f_2 - \frac{\partial}{\partial z} f_1 = u_{xxz} - u_{xww}.$$

This equation does not reduce with respect to either f_1 or f_2, so it must be added to our basis:

$$f_3 = u_{xxz} - u_{xww}.$$

We now iterate the algorithm on the system $F = \{f_1, f_2, f_3\}$. Clearly $\mathsf{diffSpoly}(f_1, f_2)$ now reduces to zero with respect to F. We calculate

$$\begin{aligned} f_1 S f_3 &= \frac{\partial}{\partial y} f_3 - \frac{\partial^2}{\partial x \partial w} f_1 \\ &= u_{xxzt} - u_{xxxw} \\ &= \frac{\partial^2}{\partial x^2} f_2 \end{aligned}$$

so this diffSpoly reduces to zero. Similarly, $f_2 S f_3$ reduces to zero, so that the output of the Kolchin-Ritt algorithm is

$$\mathsf{newbasis} = \{f_1, f_2, f_3\}.$$

We now note that the conditions for Theorem 1 apply, so that newbasis is a differential Gröbner basis for the ideal $I = \langle f_1, f_2 \rangle_F$. Where the equations are linear, the output of the Kolchin-Ritt algorithm is always a differential Gröbner basis.

Linear systems in one unknown and with constant coefficients can be written

$$\left(\sum_{\alpha} c_{\alpha,i} D^{\alpha} \right) u = 0 \qquad i = 1, \ldots, r \ \text{ and } \ c_{\alpha,i} \in \mathbb{F}.$$

Such systems are equivalent to algebraic polynomials in the operators $\left\{ \dfrac{\partial}{\partial x_i} \right\}$ and the differential Gröbner basis can be calculated with either the algebraic algorithm on the operator polynomials or with the Kolchin-Ritt algorithm. The results will be the same.

Let us now calculate the Gröbner basis for the equivalent algebraic system, which is obtained by translating $D^{\alpha} u$ into x^{α}:

$$\left\{ \begin{array}{l} f_1 = wt - x^2 \\ f_2 = zt - xw \end{array} \right. \qquad (*)$$

Then $\mathsf{Spoly}(f_1, f_2) = xw^2 - x^2 z$, which is the translation of the differential S polynomial obtained above. The iteration and termination of the algebraic algorithm is a translation of the calculations above, yielding a Gröbner basis for $(*)$, namely

$$\{f_1, f_2, x^2 z - xw^2\}.$$

3.2 Example 2: Linear systems, variable coefficients

The second example is a system of linear equations with variable coefficients ([38, Ex.13, p.135]) in one unknown function depending on three variables, $\{x, y, z\}$.

Let

$$\begin{cases} f_1 = u_{zz} - yu_{xx} \\ f_2 = u_{yy} \end{cases}$$

Assume the inverse-lexicographic ordering. This is the lexicographic ordering based on $z > y > x$. Then

$$\begin{aligned} \mathsf{HDT}(f_1) &= u_{zz}, \\ \mathsf{HDT}(f_2) &= u_{yy}, \end{aligned}$$

and

$$\begin{aligned} \mathsf{diffSpoly}(f_1, f_2) &= \frac{\partial^2}{\partial y^2} f_1 - \frac{\partial^2}{\partial z^2} f_2 \\ &= -yu_{xxyy} - 2u_{xxy}. \end{aligned}$$

This does not pseudo-reduce with respect to f_1, but pseudo-reducing with respect to f_2 yields a new equation which we add to our basis, namely

$$f_3 = u_{xxy}.$$

(We do not need to keep the constant coefficient.)

After one iteration of the algorithm, our basis is

$$L = \begin{cases} f_1 = u_{zz} - yu_{xx} \\ f_2 = u_{yy} \\ f_3 = u_{xxy} \end{cases}$$

Now $\mathsf{diffSpoly}(f_2, f_3) = 0$, (since they both consist of one term), but

$$\mathsf{diffSpoly}(f_1, f_3) = \frac{\partial^3}{\partial x^2 y} f_1 - \frac{\partial^2}{\partial z^2} f_3$$

$$= -u_{xxxx} - yu_{xxxxy}.$$

The only equation among $\{f_1, f_2, f_3\}$ to (pseudo-)reduce $\mathsf{diffSpoly}(f_1, f_3)$ is f_3, yielding a new equation to add to our basis, namely

$$f_4 = u_{xxxx}.$$

Trivially,

$$\mathsf{diffSpoly}(f_2, f_4) = \mathsf{diffSpoly}(f_3, f_4) = 0,$$

while

$$\begin{aligned}\mathsf{diffSpoly}(f_1, f_4) &= \frac{\partial^4}{\partial x^4} f_1 - \frac{\partial^2}{\partial z^2} f_4 \\ &= -yu_{(6,0,0)}.\end{aligned}$$

This (pseudo-)reduces to zero with respect to $\{f_4\}$. Now the $\mathsf{diffSpoly}(f_i, f_j)$, for $i, j \in \{1, 2, 3, 4\}$ are either identically zero or reduce to zero or an element of the basis $\{f_1, f_2, f_3, f_4\}$, which means that they all reduce to zero with respect to that basis.

Thus after two iterations the algorithm terminates yielding the output

$$\mathsf{newbasis} = \begin{cases} f_1 = u_{zz} - yu_{xx} \\ f_2 = u_{yy} \\ f_3 = u_{xxy} \\ f_4 = u_{xxxx} \end{cases}$$

Once again all the conditions for Theorem 1 hold, and we conclude that newbasis is a differential Gröbner basis.

After the first iteration, the highest variable, z, was eliminated, and after two iterations we have an equation involving only x, the lowest variable. In a lexicographic ordering, the algorithm produces successive eliminations; this feature is discussed fully in Chapter 4. With respect to the inverse-lexicographic ordering, the equation f_4 is the least member of the ideal generated by $\{f_1, f_2\}$, since the least member of the differential Gröbner basis is the least member of the ideal generated by that basis.

Other orderings yield different bases. The output of the algorithm using the reverse-lexicographic ordering is

$$\mathsf{newbasis}_2 = \begin{cases} f_1 = u_{zz} - yu_{xx} \\ f_2 = u_{yy} \\ f_3 = yu_{yzz} - u_{zz} \\ f_4 = u_{zzzz} \end{cases}$$

It is easier to solve the original system using the output obtained with the inverse-lexicographic ordering. Solving

$$u_{xxxx} = 0$$

yields

$$u = a_3x^3 + a_2x^2 + a_1x + a_0,$$

where the a_i are functions of y and z. Next use

$$u_{xxy} = 0$$

to obtain

$$6\left(\frac{\partial}{\partial y}a_3\right)x + 2\frac{\partial}{\partial y}a_2 = 0$$

or

$$\frac{\partial}{\partial y}a_3 = 0 \quad \text{and} \quad \frac{\partial}{\partial y}a_2 = 0.$$

From

$$u_{yy} = 0$$

is obtained

$$a_1 = b_1y + b_0, \quad a_0 = c_1y + c_0,$$

so that

$$u = a_3x^3 + a_2x^2 + b_1xy + b_0x + c_1y + c_0$$

with b_1, b_0, c_1 and c_0 being functions of z only, as are a_3 and a_2.
From

$$u_{zz} - yu_{xx} = 0$$

is obtained

$$\frac{\partial^2}{\partial z^2}(a_3x^3 + a_2x^2 + b_1xy + b_0x + c_1y + c_0) - 6a_3xy - 2a_2y = 0.$$

Comparing coefficients of like monomials yields

$$\begin{cases} \dfrac{\partial^2}{\partial z^2}a_3 = 0 & \dfrac{\partial^2}{\partial z^2}a_2 = 0 \\ \dfrac{\partial^2}{\partial z^2}b_2 = 6a_3 & \dfrac{\partial^2}{\partial z^2}b_0 = 0 \\ \dfrac{\partial^2}{\partial z^2}c_1 = 2a_2 & \dfrac{\partial^2}{\partial z^2}c_0 = 0 \end{cases}$$

Finally u is a polynomial in $\{x, y, z\}$ depending on 12 arbitrary constants. As Pommaret remarks, such a solution is not apparent from the outset. The method used to solve the system is not unlike the method used to solve linear systems, namely, converting to echelon form first and then solving from the "bottom up".

Linear systems with variable coefficients have the form

$$\left(\sum_{\alpha,\beta,i} c_{\alpha,\beta,i}x^\beta D^\alpha\right) u^i = 0 \qquad i = 1, \ldots, r.$$

Such equations are also referred to as elements in the Weyl algebra. As well as the methods outlined in this thesis, there are several other methods for calculating differential Gröbner bases for such systems. Galligo [19] discusses them from a geometric viewpoint. In the case of one unknown, this case is also an example of the work of Apel and Lassner [1] who generalized Buchberger's algorithm to enveloping algebras of finitely generated Lie algebras. For the linear case with variable coefficients, the Lie algebra is

$$\langle x_i, \frac{\partial}{\partial x_i} \mid i = 1, \ldots, n\rangle_{\mathbb{F}}$$

with enveloping algebra, the so-called Weyl algebra, $\mathbb{F}\left[x_i, \dfrac{\partial}{\partial x_i} \mid i = 1, \ldots, n\right]$.

There is an extensive literature on the Weyl algebra, whose ideals have been studied from many points of view.

3.3 Example 3: A system with two unknowns

The third example shows elimination, not of differentiations with respect to certain variables, but of certain unknowns. The equations are the Bäcklund equations for the Korteweg-de Vries (KdV) equation and the modified KdV equation. There are two unknowns $\{u, v\}$ and two variables $\{x, y\}$. Take

$$F = \begin{cases} f_1 = 2u + v_x + v^2 \\ f_2 = u_{xx} + 2uv^2 + 4u^2 - u_x v - \frac{1}{2} v_y. \end{cases}$$

With the ordering being the lexicographical one based on $v > u$ and $y > x$,

$$\mathsf{HDT}(f_1) = v_x$$

and

$$\mathsf{HDT}(f_2) = v_y.$$

Then

$$\begin{aligned} &\mathsf{diffSpoly}(f_1, f_2) \\ &= -\frac{1}{2}\frac{\partial}{\partial y} f_1 - \frac{\partial}{\partial x} f_2 \\ &= -u_y - v v_y - u_{xxx} - 2u_x v^2 - 4uvv_x - 8uu_x + 2u_{xx} v + u_x v_x. \end{aligned}$$

This can be pseudo-reduced at the terms containing v_x and v_y using f_1 and f_2 respectively. The result is, after elimination of irrelevant constant factors,

$$f_3 = u_y + u_{xxx} + 12uu_x,$$

that is, a form of the KdV equation. The unknown function v has been eliminated. The set $\{f_1, f_2, f_3\}$ forms a differential Gröbner basis for $I(F)$.

By using the ordering $u > v$, the output of the algorithm is, in addition to f_1 and f_2,

$$f_3 = v_y + v_{xxx} - 6v^2 v_y.$$

that is, the modified KdV equation. The unknown u has been eliminated.

It will be seen in Chapter 4 that differential Gröbner bases solve the Bäcklund problem ([39, p.644], [40]), which is to find all conditions on the separate unknowns in the problem.

3.4 Example 4: A non-linear system

Let us now do an example where the coefficient of the highest derivative term is not in $\mathbb{F}[x_1, \ldots, x_n]$. This system has one unknown function and three variables:

$$\begin{cases} f_1 = u_z - uu_x \\ f_2 = u_{yy}. \end{cases}$$

Take the lexicographic ordering, with $x > y > z$. Then

$$\mathsf{diffSpoly}(f_1, f_2) = u_{yyz} - u_{yy}u_x - 2u_y u_{xy} - uu_{xyy}.$$

which pseudo-reduces to

$$f_3 = uu_y u_{yz} - u_y^2 u_z.$$

Now $\mathsf{HDT}(f_3) = u_{yz}$. The $\mathsf{diffSpoly}(f_2, f_3)$ pseudo-reduces with respect to f_2 to zero, while

$$f_4 = \mathsf{normal}^{\mathsf{p}}(\mathsf{diffSpoly}(f_1, f_3), \{f_1, f_2, f_3\}) = u_y^3 u^2(-u_z^2 + 2uu_{zz}).$$

Now $\mathsf{HDT}(f_4) = u_y$, occuring to a power greater than one, as a factor of f_4. So we cannot conclude that any output G containing f_4 is a differential Gröbner basis since

$$f_4 \in S(G) \cap I(G).$$

Changing the order is clearly indicated. We show the output of the Kolchin-Ritt algorithm for both orders that place y as the lowest variable:

In the lexicographic order with $x > z > y$, we obtain

$$G = \text{Kolchin-Ritt}(f_1, f_2) = \{u_{yy}, -uu_yu_{zy} + u_y^2u_z, -u^2u_yu_{zz} + 2uu_y^2u_z, u_z - uu_x\}$$

Now $S(G) = M(\{u, u_y\})$, and in the lexicographic order based on $x > z > y$, no element of S(G) pseudo-reduces. Thus condition (SPR) of Theorem 1 in Chapter 2 holds.

In the lexicographic ordering with $z > x > y$, the output of the Kolchin-Ritt algorithm is

$$\mathsf{newbasis} = \{u_z - uu_x, u_y^2u_{xx}, u_yu_{xy}, u_{yy}\}$$

Now newbasis is a differential Gröbner basis for $I(f_1, f_2)$; since $S(\mathsf{newbasis}) = M(\{u_y\})$ and no element of this set pseudo-reduces i.e condition (SPR) holds and since newbasis is a Gröbner basis for $I_{\mathsf{alg}}(G)$.
Using newbasis, we can find all solutions to $f_1 = 0, f_2 = 0$ that satisfy $u_y \neq 0$. We begin with the least element of newbasis, namely

$$u_{yy} = 0.$$

This yields

$$u = F(x, z) + G(x, z)y.$$

The second lowest element of newbasis is

$$u_yu_{xy} = 0.$$

Since $u_y \neq 0$, we have

$$u = F(x, z) + G(z)y.$$

Next we use the equation

$$u_y^2u_{xx} = 0.$$

This yields

$$u = K(z)x + H(z) + G(z)y.$$

Finally we use the equation

$$u_z - uu_x = 0$$

to obtain

$$u = \frac{-x + by + c}{z + a},$$

where a, b, c are arbitrary constants.

In this example, the ordering used clearly makes a difference to the ease of solving the equations.

3.5 Example 5: A non-prime system

This example shows that by choosing the condition GC to hold, rather than GAC, the algorithm will not terminate.

The example

$$F = \begin{cases} v_x - 2vu = 0 \\ v_y + v(u^2 + 2u_x) = 0 \end{cases}$$

yields after one iteration of the algorithm (using $v > u$)

$$G = \begin{cases} v_x - 2vu \\ v_y + v(u^2 + 2u_x) \\ v(u_y + uu_x + u_{xx}) \end{cases}$$

and $S(G) = M(\{u_y + uu_x + u_{xx}\})$.

It is easily verified that G is a differential Gröbner basis, since the condition (SPR) of Theorem 1, Chapter 2 holds, and since G is a Gröbner basis of $I_{\mathsf{alg}}(G)$.

Attempting to complete the set G to make the condition (GC) hold and to simultaneously be a Gröbner basis for $I_{\mathsf{alg}}(G)$, leads to an infinite set, containing all elements of the form $vD^{\alpha}(u_y + uu_x + u_{xx}), \alpha \in \mathbb{N}^n$.

If instead of completing we convert the set to be pseudo-reduced (thus ensuring GC, GAC are trivially satisfied), we obtain only the equation $\{v(u_y + uu_x + u_{xx})\}$. Since we cannot within the theory allow $S(G) \cap I(G) = \phi$, we have $u_y + uu_x + u_{xx} \neq 0$. Thus we obtain only the trivial condition $v = 0$. Here we see the difference between completing and insisting on auto-reduced sets.

If one wants to consider the equation $u_y + uu_x + u_{xx} = 0$ in addition to the first two (i.e. $v \neq 0$), one must run the algorithm again with the input

$$F' = \{v_x - 2vu, v_y + v[(u)^2 + 2u_x], u_y + uu_x + u_{xx}\}.$$

The set F' is a differential Gröbner basis for $I(F')$ in the order $v > u$.

Examples such as Example 5 above lead one to suspect that an ideal may not contain a differential Gröbner basis that is also auto-reduced, if the ideal is not prime. (The ideal generated by $G = \{v(u_y + uu_x + u_{xx})\}$ is also not perfect, since $(v_x(u_y + uu_x + u_{xx}))^2 \in I(G)$ but $v_x(u_y + uu_x + u_{xx}) \notin I(G)$.) This example can be converted to a prime one by taking $w = \ln(v)$, and writing the equations in terms of w and u.

Chapter 4

RESOLVENT SYSTEMS AND ELIMINATION IDEALS

This chapter contains an application of differential Gröbner bases to calculate resolvent systems and elimination ideals. Examples are discussed. A comparison of the Janet resolution of a system of PDE's and the projective syzygy resolution of a polynomial ideal is given.

4.1 Resolvent Systems

A system Σ can be written using general notation as $\mathcal{D}(u) = 0$, where $\mathcal{D}$ is a (non-linear) operator, and u represents a vector of unknown functions $(u^1, \ldots, u^m)$. Let $v = (v^1, \ldots, v^k)$ be in the range of $\mathcal{D}$, i.e. there exists a u so that $\mathcal{D}(u) = v$. In general, the range of an operator is not the whole of $(C^\infty(\mathbb{R}))^k$ It is necessary for v to satisfy various compatibility conditions, written $\mathcal{D}^{(1)}(v) = 0$, also denoted by $\sum^{(1)}$; this system is called the resolvent system (for the meaning of the index, see the next

section, the Janet Resolution.) While the compatibility conditions $\mathcal{D}^{(1)}(v) = 0$ are necessary conditions for v to be in the range of $\mathcal{D}$, they are by no means sufficient. A famous example by H. Lewy gives a single equation $\mathcal{D}(u) = v$ where $\mathcal{D}$ is linear, v is C^∞ and there is no solution u. ([29, p.235-9], see also [53], [15, Vol II p. 54, §4b] and references there.)

The first example is a well-known result.

Example 1 (Resolvent system of the curl operator). *In this example,* $u^i \in C^\infty(U, \mathbb{R})$*, where* $U \subset \mathbb{R}^3$*,*

$$D \begin{bmatrix} u^1 \\ u^2 \\ u^3 \end{bmatrix} = \begin{bmatrix} u^3_y - u^2_z \\ u^1_z - u^3_x \\ u^2_x - u^1_y \end{bmatrix} \in (C^\infty(U, \mathbb{R}))^3$$

We seek the compatibility conditions on $\begin{bmatrix} v^1 \\ v^2 \\ v^3 \end{bmatrix}$ *such that*

$$D \begin{bmatrix} u^1 \\ u^2 \\ u^3 \end{bmatrix} = \begin{bmatrix} v^1 \\ v^2 \\ v^3 \end{bmatrix}$$

We input the following equations into the algorithm with any lexicographic ordering such that $u^i > v^j$*, all* i, j*.*

$$\begin{cases} u^3_y - u^2_z - v^1 \\ u^1_z - u^3_x - v^2 \\ u^2_x - u^1_y - v^3 \end{cases}$$

The output contains the equation

$$v^1_x + v^2_y + v^3_z = 0.$$

This is the only equation in the output where all the u^i *have been eliminated. Since the equations are linear, the output is a differential Gröbner basis for the input ideal. By Theorem 3 later in this chapter, the equation* $v^1_x + v^2_y + v^3_z = 0$ *generates the ideal of compatibility conditions.*

Example 2 (Resolvent system of a differential ideal). *(cf Example 2, Chapter 3, [39, p.636]) Consider the system* Σ *in* $\mathbb{R}_{3,1}$ *generated by*

$$\begin{aligned} u_{zz} - yu_{xx} &= 0 \\ u_{yy} &= 0. \end{aligned}$$

We seek to find the resolvent system, i.e. the equations that must be satisfied by unknown functions v *and* w *in the new system* Σ^*

$$\begin{aligned} u_{zz} - yu_{xx} &= v \\ u_{yy} &= w \end{aligned}$$

if a solution u *is to exist. Here* v *and* w *are functions of the variables* $\{x, y, z\}$*. Then with the lexicographic ordering based on* $x < y < z$*, the output of the algorithm is*

$$\begin{aligned} & u_{zz} - yu_{xx} - v = 0 \\ & u_{yy} - w = 0 \\ & 2u_{xxy} - w_{zz} + v_{yy} + yw_{xx} = 0 \\ & 2u_{xxxx} - w_{zzzz} + v_{yyzz} + 2yw_{xxzz} \\ & +2v_{xxy} - yv_{xxyy} - y^2 w_{xxxx} = 0 \\ & -w_{yzz} + v_{yyy} + 3w_{xx} + yw_{xxy} = 0 \\ & -w_{(0,0,6)} + v_{(0,2,4)} + 3yw_{(2,0,4)} + 2v_{(2,1,2)} \\ & -2yv_{(2,2,2)} - 3y^2 w_{(4,0,2)} + 2v_{(4,0,0)} - 2yv_{(4,1,0)} \\ & +y^2 v_{(4,2,0)} + y^3 w_{(6,0,0)} = 0. \end{aligned}$$

The final two equations involve only v *and* w*. Thus these equations are necessary conditions on* v *and* w *in order for a solution* u *to exist. It is a result of Theorem 3 that the final two equations generate the resolvent system.*

In his book "Differential Galois Theory", Pommaret [39, p.636] writes "How could we obtain $\mathcal{D}^{(1)}$ from the knowledge of $\mathcal{D}$? . . . this problem is a difficult one ... [and] involves *necessarily* diagram chasing." The method used here is conceptually and practically simpler than that of Pommaret, and involves no diagram chasing.

The resolvent systems in the examples above were calculated by selecting those equations in the output of the algorithm that involved only derivatives of the image functions, the v^i. For the calculation, the ordering on the unknowns must be $u^i > v^j$ for all i, j.

More generally, if one chooses a lexicographic ordering on the x^i and the u^j, say $x_{i_1} < x_{i_2} < \cdots < x_{i_n}$ and $u^{j_1} < u^{j_2} < \cdots < u^{j_m}$, then those equations in a differential Gröbner basis for the ideal containing only $\{u^{j_1}, \ldots, u^{j_s}\}$ and derivatives with respect to $\{x_{i_1}, \ldots, x_{i_r}\}$ generate the differential ideal

$$I \cap \mathbb{R}_{\mathsf{diff}}[x_{i_1}, \ldots, x_{i_r}, u^{j_1}, \ldots, u^{j_s}].$$

This result is Theorem 4, which is the analogue of Trinks' Corollary [54, p. 484, Chapter 1].

The term resolvent system has been used by Pommaret in this elimination sense: in a system with more than one unknown, the equations satisfied by certain subsets of the unknowns are also called resolvent systems.

Theorem 3. *Assume a lexicographic ordering. Let* $\Sigma = \{f_i \mid i = 1, \ldots, N\}$ *be the generators of a differential ideal* I *of* $R_{n,m}$. *Take* N *new unknowns* $\{v^i \mid i = 1, \ldots, N\}$ *with some ordering, and consider the associated system* $\Sigma^* = \{f_i - v^i \mid i = 1, \ldots, N\}$. *Add to the ordering* $u^j > v^i$ *all* i *and* j . *Those equations in the output of the algorithm involving only the* $\{v^j\}$ *forms a set of generators for the resolvent system.*

The proof follows from Theorem 4. It is interesting to note that this method of generating the dual of the syzygy module has been used by Buchberger to give the implicitization of a parametric system (Chapter 1 and [9]).

4.2 The Janet Resolution

Iterating the process of forming the resolvent system leads to the Janet resolution of the system. Let $\mathcal{S}$ be the solution space of the equation $\mathcal{D}(u) = 0$ where $u \in \mathcal{R}^{i_0}$ (a suitable function space) . Let the resolvent system be denoted $\mathcal{D}^{(1)} : \mathcal{R}^{i_1} \to \mathcal{R}^{i_2}$, and let the resolvent system of the resolvent system be denoted $\mathcal{D}^{(2)}$, and so on. Then we have the following sequence of maps:

$$0 \longrightarrow \mathcal{S} \xrightarrow{\mathsf{inc}} \mathcal{R}^{i_0} \xrightarrow{\mathcal{D}} \mathcal{R}^{i_1} \xrightarrow{\mathcal{D}^{(1)}} \mathcal{R}^{i_2} \xrightarrow{\mathcal{D}^{(2)}} \mathcal{R}^{i_3} \xrightarrow{\mathcal{D}^{(3)}} \cdots$$

The map inc is the inclusion map. In this sequence, we have the composition of consecutive maps is zero:

$$\mathcal{D}^{(n)}\mathcal{D}^{(n+1)} = 0$$

In standard algebraic theory, a resolution must also be exact. By this is meant, that $\ker\mathcal{D}^{(n+1)} = \mathrm{im}\mathcal{D}^{(n)}$. In the Janet resolution, we have only that $\ker\mathcal{D}^{(n+1)} \supset \mathrm{im}\mathcal{D}^{(n)}$.

Example 3 (Janet resolution of exterior differentiation operator.). *A familiar example of a resolution is the Poincaré d-sequence. Let U be an open set in $\mathbb{R}^n, \Lambda^k(U)$ the set of exterior k-forms on U, and let d be the usual exterior derivative. Then the sequence*

$$0 \longrightarrow \Lambda^0(U) \xrightarrow{d} \Lambda^1(U) \xrightarrow{d} \cdots \xrightarrow{d} \Lambda^n(U) \longrightarrow 0$$

is a resolution for the operator d. In the case U is homeomorphic to the unit ball $B^3 = \{x \in \mathbb{R}^3 \mid |x| \leq 1\}$, this particular Janet resolution is a resolution in the algebraic sense: $du = v$ has a solution if and only if $dv = 0$.
Let us look at this sequence in co-ordinates in the case n is 3. We have $\Lambda^0(U) = \{f : U \to \mathbb{R}^3\}$, and

$$df = \frac{\partial f}{\partial x_1}dx_1 + \frac{\partial f}{\partial x_2}dx_2 + \frac{\partial f}{\partial x_3}dx_3.$$

Now suppose $df = v$*, so that*

$$(*) \quad \begin{cases} \dfrac{\partial f}{\partial x_1} = v_1 \\ \dfrac{\partial f}{\partial x_2} = v_2 \\ \dfrac{\partial f}{\partial x_3} = v_3 \end{cases}$$

From the fact that partial derivatives commute, we have that

$$(**) \quad \begin{cases} \dfrac{\partial v_1}{\partial x_2} - \dfrac{\partial v_2}{\partial x_1} = 0 \\ \dfrac{\partial v_3}{\partial x_2} - \dfrac{\partial v_2}{\partial x_3} = 0 \\ \dfrac{\partial v_1}{\partial x_3} - \dfrac{\partial v_3}{\partial x_1} = 0. \end{cases}$$

The equations $(**)$ *are the equations* v *must satisfy in order for an* f *to exist such that* $df = v$*, and this is the resolvent system for* $d|_{\Lambda^0(U)}$*. In the notation of exterior differentiation, they are written* $dv = 0$*.*

If one takes as the input to the DIFFGBASIS *algorithm the equations* $(*)$*, then the output will be the equations* $(*)$ *and the equations* $(**)$*.*

Continuing, we have for $d|_{\Lambda^1(U)}$*, that* $dv = w$ *implies*

$$(\bullet) \quad \begin{cases} \dfrac{\partial v_2}{\partial x_1} - \dfrac{\partial v_1}{\partial x_2} = w_3 \\ \dfrac{\partial v_3}{\partial x_2} - \dfrac{\partial v_2}{\partial x_3} = w_2 \\ \dfrac{\partial v_1}{\partial x_3} - \dfrac{\partial v_3}{\partial x_1} = w_1. \end{cases}$$

With the equations $(\bullet)$ *as the input to the* DIFFGBASIS *algorithm, the output will be the equations* $(\bullet)$ *and the equation*

$$(\bullet\bullet) \quad \frac{\partial w_1}{\partial x_1} + \frac{\partial w_2}{\partial x_2} + \frac{\partial w_3}{\partial x_3} = 0$$

We now turn to another example where the result is not known in advance.

Example 4 (The Janet resolution of Example §2, Chapter 3.). *The system* $\Sigma^{(0)}$ *is*

$$f_1^{(0)} = u_{zz} - yu_{xx}$$
$$f_2^{(0)} = u_{yy}.$$

The first resolvent system $\Sigma^{(1)}$ *was calculated in Example 2 of the first section of this chapter. This is*

$$\begin{aligned} f_1^{(1)} = - \quad & v^2_{yzz} + v^1_{yyy} + 3v^2_{xx} + yv^2_{xxy} \\ f_2^{(1)} = - \quad & v^2_{(0,0,6)} + v^1_{(0,2,4)} + 3yv^2_{(2,0,4)} + 2v^1_{(2,1,2)} \\ & -2yv^1_{(2,2,2)} - 3(y)^2v^2_{(4,0,2)} + 2v^1_{(4,0,0)} \\ & -2yv^1_{(4,1,0)} + (y)^2v^1_{(4,2,0)} + (y)^3v^2_{(6,0,0)} \end{aligned}$$

The next step is to calculate the output of the algorithm for the system $\{f_1^{(1)} - w^1, f_2^{(1)} - w^2\}$. *The output will be* $f_1^{(1)} - w^1, f_2^{(1)} - w^2$, *the resolvent system* $\Sigma^{(2)}$, *and possibly some other equations if the ordering chosen is different from the one used here. Taking the lexicographic ordering based on* $w^2 < w^1 < v^2 < v^1$ *and* $z > y > x$ *we obtain one equation in* w^1 *and* w^2*:*

$$f_1^{(2)} = w^1_{zzzz} - 2yw^1_{xxzz} + (y)^2w^1_{xxxx} - w^2_y.$$

A system generated by only one equation has a null resolvent system, and so the Janet resolution of $\Sigma^{(0)}$ *terminates after three steps.*

In the early part of this century (1920), Janet ([28]) proved that if the original system Σ was composed of linear differential equations (that is to say, linear as differential equations), then the resolution must terminate by at most n steps, where n is the number of variables. The termination of the Janet resolution for a system consisting of arbitrary differential polynomials is, I believe, not known in general. The case of linear

equations with constant coefficients is equivalent to the termination of the syzygy resolution of a polynomial ideal (see later this chapter), which was demonstrated by Hilbert [24] in 1892.

4.3 Elimination Ideals

Theorem 4. *Assume the lexicographic ordering. Let G be a differential Gröbner basis for an ideal I contained in $R_{n,m}$, with the ordering on the unknowns being $u^m > u^{m-1} > \cdots > u^1$ and on the variables $x_n > x_{n-1} > \cdots > x_1$. Let $R_{k,j}$ be the differential subring generated by $\{u^1, u^2, \ldots, u^k, x_1, x_2, \ldots, x_j\}$. Then $G \cap R_{k,j}$ is a differential Gröbner basis for $I \cap R_{k,j}$.*

Proof. Let $G \cap R_{k,j} = G'$ and $G \backslash G' = G''$. Let $I' = I \cap R_{k,j}$. Suppose $g \in I'$ but that g is not an element of the ideal $I(G')$, generated by G'. Note that G' is a differential Gröbner basis for $I(G')$. Let g be pseudo-reduced with respect to G'. Since $g \neq 0$, $g \in I(G'')$. But all the elements of G'' have highest terms involving unknowns and variables that are not in I'; such terms must have cancelled out so that g must be expressible as diffSpolynomials of elements in $I(G'')$ and their pseudo-reductions. Now g is not pseudo-reducible with respect to G'' since no highest term of any element of G'' reduces any term of g, and g has already been pseudo-reduced with respect to G', so we have a contradiction. □

Example 5 (Kadomtsev-Petviashvili equations ([47])). *These equations are the 3 dimensional analogue of the Bäcklund equations for the Korteweg-de Vries equations. The system is similar to Example 3 of Chapter 3, in that the principal part is linear for all orderings. This means that this example is also tractable by methods*

that first convert the system to a system of exterior differential forms [7].

$$F = \left\{ \begin{array}{r} u_x + \frac{1}{2}v_{xx} + \frac{1}{4}v_x^2 + v_y = 0 \\ u_y - \frac{1}{6}v_z - \frac{1}{6}v_{xxx} + \frac{1}{2}v_{xy} + \frac{1}{12}v_x^3 + \frac{1}{2}v_x v_y = 0 \end{array} \right.$$

We first take the lexicographic ordering based on $u > v, z > y > x$, and we obtain one extra condition, from which u has been eliminated:

$$6v_{yy} + 2v_{xz} + 2v_{xxxx} - 3v_x^2 v_{xx} - 6v_{xx}v_y = 0.$$

Taking the ordering based on $v > u$, we obtain one extra condition, from which v has been eliminated:

$$u_{xz} + 3u_{yy} + u_{xxxx} + 6u_{xx}u_x = 0.$$

The leading terms have coefficients in the field, and so the output is a differential Gröbner basis. Hence

$$I(F) \cap \mathbb{R}_{\mathsf{diff}}[x, y, z; u] = I(u_{xz} + 3u_{yy} + u_{xxxx} + 6u_{xx}u_x),$$

and

$$I(F) \cap \mathbb{R}_{\mathsf{diff}}[x, y, z; v] = I(6v_{yy} + 2v_{xz} + 2v_{xxxx} - 3v_x^2 v_{xx} - 6v_{xx}v_y).$$

Example 6 (elimination ideals, a system with a non-linear principal part). *This system has a non-linear principal part, and thus cannot so easily be tackled by algorithms that first convert to a system of exterior differential forms, or which use Riquier's method. Let*

$$F = \left\{ \begin{array}{l} u_y v_x - u_x = 0 \\ u_x v_y - u_y = 0 \end{array} \right.$$

Performing the algorithm in the lexicographic order with $v > u$, and $y > x$ we obtain one extra condition, denoted g (say):

$$-u_x u_y^2 u_{xy} + u_y u_x^2 u_{xy} + u_y^3 u_{xx} - u_x^3 u_{yy} = 0.$$

which has for its HDT*, u_{yy}. We have for the output $G = F \cup \{g\}$, that $S(G) = M(\{u_x, u_y\})$ so that* SPR *holds. It is clear that $S(G) \cap I(G) = \phi$, so G is a differential Gröbner basis, and $I(F) \cap \mathbb{R}_{\mathsf{diff}}[x, y; u] = I(g)$.*

Performing the algorithm with $u > v$, and $y > x$ we obtain one new condition denoted h (say):

$$u_x(v_x v_y - 1) = 0$$

Thus we have not entirely eliminated u. The output $G = F \cup \{h\}$ has $S(G) = M(\{v_x v_y - 1, v_x\})$. Thus SPR *holds. Insisting that $S(G) \cap I(G) = \phi$ (i.e. $v_x v_y - 1 \neq 0$) leads to the conclusion that $u_x = 0$, a trivial solution. It is better to run the algorithm again adding the equation $v_x v_y - 1 = 0$ to the input. We then would obtain for the augmented system $F' = F \cup \{v_x v_y - 1\}$ that $I(F') \cap \mathbb{R}_{\mathsf{diff}}[x, y; v] = I(v_x v_y - 1)$.*

Example 7 (elimination ideals). *Our third example shows that one can obtain more than one condition from which one of the unknowns has been eliminated. Set*

$$F = \begin{cases} v_y u_y - v_x = 0 \\ v_{xy} u_x - u = 0 \end{cases}$$

Performing the algorithm in the lexicographic ordering, with $v > u$ and $y > x$, we obtain four new conditions, with two conditions in u only, denoted by g_1 and g_2, (say). The equation g_1 has 33 summands, while g_2 has 39 summands. We have:

$\mathsf{HDT}(g_1) = u_{xyyy}$, $\mathsf{Hp}(g_1) = 1$, *and*

$\mathsf{Hcoeff}(g_1) =$

$$u_x^5 u_y \{u u_y u_{xx} + u u_x u_y u_{yy} - u u_y^2 u_{xy} + u u_x u_{xy} - u_y u_x^2 + u_x u_y^3\}$$

while

$\mathsf{HDT}(g_2) = u_{xxyy}, \mathsf{Hp}(g_2) = 1$, *and* $\mathsf{Hcoeff}(g_2) = \mathsf{Hcoeff}(g_1)$.

Equations with so many terms are difficult to solve. Yet the fact that there exist such equations implied by the given set may have implications for the choice of method of numerical solution. Moreover, in combination with other methods such as use of symmetries, the use of elimination ideals could be extremely effective.

APPLICATIONS

The major applications of the elimination ideals are in non-linear control theory with distributed parameters, where one wishes to establish a hierarchy of control, and to separate out the conditions that must be satisfied by the input and output variables respectively. ([42, 40] , [17])

Another application is where one wishes to discover if any of the unknowns in the system satisfies what is effectively an ODE with respect to some variable, that is, all differentiations are with respect to the same variable. If the ODE can be solved, that variable can be eliminated, simplifying the system. The use of different orderings on the variables to find all ODE's in the ideal is discussed in the second example of Chapter 3, where it is shown that the ideal generated by $\{u_{zz} - yu_{xx}, u_{yy}\}$ contains the ODE's $\{u_{yy}, u_{xxxx}, u_{zzzz}\}$.

4.4 Formal Duality of Resolvent Systems and Syzygies for Linear Systems

We compare the syzygy resolution for an algebraic set of polynomials, and the Janet resolution for the corresponding differential ideal, obtained by identifying x_i with $\dfrac{\partial}{\partial x_i}$; both the algebraic and differential resolutions ontained are well-known.

Let us consider the syzygy resolution of the ideal

$$A = \langle x, y, z \rangle_{\mathbb{R}} \subset \mathbb{R}[x, y, z].$$

We write the generators of A as a vector U, viz (x, y, z), (assume all vectors are row vectors) and seek the set of vectors V (whose components are polynomials in $\mathbb{R}[x, y, z]$) such that

$$VU^T = 0.$$

Then the syzygy module $S(A)$ is generated by

$$\begin{cases} V_1 = (y, -x, 0) \\ V_2 = (z, 0, -x) \\ V_3 = (0, z, -y) \end{cases}$$

(cf Chapter 1.) Continuing, we write the generators of $S(A)$ as a row vector V, and seek those vectors W such that

$$WV^T = 0.$$

Then the second syzygy module $S^{(2)}(A)$ is generated by

$$W = (x, y, z).$$

We have the exact sequence

$$0 \longrightarrow \mathbb{R}[x,y,z] \xrightarrow{M^{(2)}} \mathbb{R}[x,y,z]^3 \xrightarrow{M^{(1)}} \mathbb{R}[x,y,z]^3 \xrightarrow{M^{(0)}} \mathbb{R}[x,y,z] \longrightarrow \mathbb{R} \longrightarrow 0$$

where

$$M^{(0)} \begin{bmatrix} p_1 \\ p_2 \\ p_3 \end{bmatrix} = xp_1 + yp_2 + zp_3$$

$$M^{(1)} \begin{bmatrix} p_1 \\ p_2 \\ p_3 \end{bmatrix} = \begin{bmatrix} -yp_3 + zp_2 \\ +xp_3 - zp_1 \\ -xp_2 + yp_1 \end{bmatrix}$$

and

$$M^{(2)}(p) = \begin{bmatrix} xp \\ yp \\ zp \end{bmatrix}.$$

We have $\ker M^{(i)} = S^{(i)}(A)$. Note that $S^{(0)}(A) = A$, and $\mathbb{R} = \mathbb{R}[x,y,z]/A$.

Let us now consider the differential system

$$(*) \quad \begin{cases} \dfrac{\partial u}{\partial x} = 0 \\ \dfrac{\partial u}{\partial y} = 0 \\ \dfrac{\partial u}{\partial z} = 0 \end{cases}$$

This is the translation, under the identification $x^\alpha \leftrightarrow \dfrac{\partial^{|\alpha|}}{\partial x^\alpha} u$ of the ideal A to a differential ideal. (We insert the dummy argument u to the differential operators.) We have already calculated the resolution of this ideal, (it is in fact the same as the Poincaré sequence), in Example 3 of this chapter.

Let $\Re$ be a suitable function space. Let $\mathbb{R}$ stand for the constant functions. We can write the resolution in the following way:

$$0 \longrightarrow \mathbb{R} \longrightarrow \Re \xrightarrow{D^{(0)}} \Re^3 \xrightarrow{D^{(1)}} \Re^3 \xrightarrow{D^{(2)}} \Re \longrightarrow 0$$

where

$$D^{(0)}(u) = \begin{bmatrix} u_x \\ u_y \\ u_z \end{bmatrix}$$

$$D^{(1)}(u) = \begin{bmatrix} v^1 \\ v^2 \\ v^3 \end{bmatrix} = \begin{bmatrix} v^3_y - v^2_z \\ v^1_z - v^3_x \\ v^2_x - v^1_y \end{bmatrix}$$

$$D^{(2)}(u) = \begin{bmatrix} w^1 \\ w^2 \\ w^3 \end{bmatrix} = w^1_x + w^2_y + w^3_z.$$

It is not hard to see that replacing x with $\dfrac{\partial}{\partial x}$ the maps $D^{(i)}$ are the transpose of the maps $M^{(i)}$, and that replacing $\mathbb{R}[x, y, z]$ with $\Re$, the two exact sequences are formally dual. In fact, we have an algorithm for obtaining the Janet resolution of a system

of linear equations, with one unknown and constant coefficients, from the syzygy resolution of the corresponding polynomial ideal, by considering the system as a set of polynomials in the operators $\{\frac{\partial}{\partial x}\}$. That is, we replace $\mathbb{R}[x_i]$ with $\mathfrak{R}$, replace x with $\frac{\partial}{\partial x}$, take the transpose of the maps and send the arrows in the opposite direction. The final space in the syzygy resolution is $\mathbb{R}[x_i]/A$, while the first non-zero space in the Janet resolution is the solution space to $\mathcal{D}(u) = 0$.

In view of the Lewy example we cannot say that the Janet resolution is exact even for linear systems; the two sequences are only "formally" dual. Restricting the function spaces to be analytic spaces, we obtain exactness ([53], see also Goldschmidt [21] who proves an existence theorem for analytic systems.)

Chapter 5

COMPARISONS AND EXTENSIONS

5.1 Algebraic vs differential Gröbner bases

Given a set of d.p.'s $\Sigma = \{f_i \mid i = 1, \ldots, N\}$ we can form the r-prolongation

$$\Sigma^{(r)} = \{D^\alpha f_i \mid i = 1, \ldots, N, |\alpha| \leq r\}.$$

Let $M = \max\{|\alpha| \mid p^j_\alpha$ occurs to some power in any of the $f_i\}$. One can form the non-differential ring $\mathcal{A}_{m,n,t} = F[x_i, u^j, p^j_\alpha \mid |\alpha| \leq t]$. Let $I_{\mathsf{alg}}(\Sigma^{(r)})$ denote the non-differential ideal generated by $\Sigma^{(r)}$ in $\mathcal{A}_{m,n,r+M}$. Take the ordering on the derivative terms as determining the order on the indeterminants in $\mathcal{A}_{m,n,r+M}$, with $u^i > x_j$, and then assume lexicographic ordering on monomials in $\mathcal{A}_{m,n,r+M}$.

Theorem 4. *For sufficiently large r, a Gröbner basis B of $I_{\mathsf{alg}}(\Sigma^{(r)})$ satisfies $I_{\mathsf{alg}}(B) \supset I_{\mathsf{alg}}(\text{DIFFGBASIS}(\Sigma))$.*

Proof. For a sufficiently large r, all the $D^\alpha f_i$ used in the calculation of the

DIFFGBASIS algorithm will be in $I_{\mathsf{alg}}(\Sigma^{(r)})$. It can be seen from the formulae that the diffSpolynomial formulae reduce to algebraic formulae when the differentiations are already performed. Where the separants or highest coefficients contain more than one summand, repeated calculation of algebraic Spolynomials result in the diffSpolynomial calculation. □

Ritt proves an equivalent result in terms of characteristic sets in the case where the ideals are prime ([43, Chapter V].) The iteration of prolongation and Gröbner basis calculation has been discussed by Carrà-Ferro [12] and Ollivier [37, 36]. They have both shown that in general such an iteration (using differential reduction) will not terminate.

In general, the algebraic calculation in $I_{\mathsf{alg}}(\Sigma^{(r)})$ will be far larger than that of the differential Gröbner basis. Consider the case of Example 2, Chapter 3, which has three variables, one unknown and starts with two equations. The highest derivative used in the calculation is of order five. To use the algebraic algorithm, the two equations are prolonged to be of order five, yielding 20 equations in 25 indeterminates (3 variables, one unknown and 21 derivative terms.). The first iteration requires the calculation of 190 Spolynomials. The complete algebraic calculation is beyond the capacity of even top-range personal computers (as at 1990), while the differential Gröbner basis calculation was completed in minutes on a Macintosh Plus, using an implementation of the differential algorithm as a package in MAPLE.

5.2 A branching algorithm

In his book, Ritt ([43]) is concerned with the prime decomposition of a differential ideal. He proves that every perfect differential ideal has a prime decomposition. (An ideal I is prime if $a.b \in I$ implies $a \in I$ or $b \in I$. The ideal I is said to be perfect

if an $a^n \in I$ implies $a \in I$.) The calculation of the prime decomposition of an algebraic ideal is now algorithmic, due to the work of Gianni, Trager and Zacharias [20]. The prime decomposition is important because one then has a listing of the solution varieties, and the equations involved will be in some sense simpler, having all factors removed. There is a complication in the case of differential ideals, which is that an irreducible d.p. may have a derivative that factors. We give an example of this at the end of this section. In some cases it is sufficient to take account of the factors as they appear in the algorithm, a process that concerns us in this section. This process has also been discussed by Melenk [33].

In seeking a solution to a system of partial differential equations one can take the algorithm a step further: after each iteration of the algorithm the new conditions obtained can be factored. Suppose each new condition obtained has $n(i)$ factors. Then there are $N = \prod n(i)$ factors. Form N new lists, each consisting of the previous list plus one factor from each new condition created, upon which to iterate the algorithm. Instead of a sequence

$$\{F_0, F_1, \ldots, \mathsf{newbasis}\}$$

of lists, a tree of lists is generated. Such a tree is illustrated in Figure 5.1.

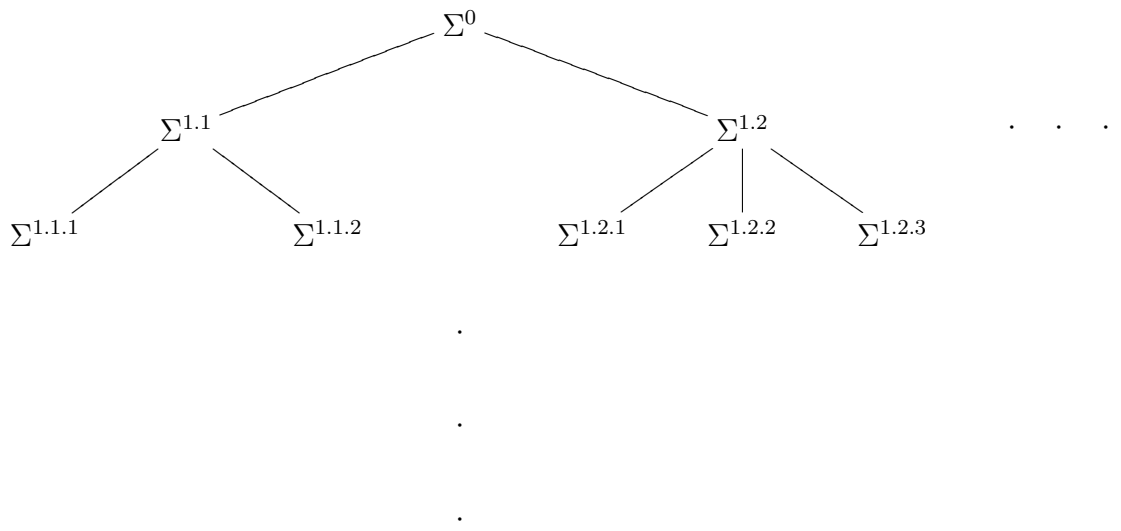


Figure 5.1:
A tree of systems

It is straightforward to show that this branched algorithm will also terminate.

Lemma 1. *The branching algorithm terminates.*

Proof. Suppose not. Then there is a path $P = [\Sigma^0, \Sigma^{1.i_1}, \Sigma^{1.i_1.i_2}, \ldots]$ in the tree that is infinite. Now repeat the argument for the termination of the non-branching algorithm, but on the list of systems in the path rather than on the systems obtained after successive iterations. □

A solution to the original system will be a solution to one of the resulting systems. The converse is false: a solution to one of the resulting systems will not in general be a solution to the original system. For example, a solution to one of the resulting

systems may only be a solution to the original system for certain values or subsets of the constants of integration. Furthermore, the resulting lists will not in general be bases for the ideal generated by the original list. Presumably the differential ideals generated by the resultant lists form some kind of "decomposition" or "cover" of the initial ideal. Ritt [43] proves that a perfect ideal has a prime decomposition, that is, can be expressed as the intersection of finitely many prime ideals. That a differential ideal be prime is a very strong condition: a differential ideal generated by a single irreducible d.p. is not necessarily prime, primary or perfect. Consider the example of an ideal I in $\mathbb{R}_{1,1}$ generated by

$$f = \left(\frac{du}{dx}\right)^2 + \frac{du}{dx} + 2u + x.$$

Then $\dfrac{df}{dx} \in I$. But $\dfrac{df}{dx} = \left(2\dfrac{du}{dx} + 1\right)\left(\dfrac{d^2u}{dx^2} + 1\right)$ and neither factor, nor any power of either of them, is in I, so I is neither prime nor primary. Furthermore,

$$\left(\left(2\frac{du}{dx} + 1\right)\frac{d^3u}{dx^3}\right)^2 \in I, \quad \text{but}$$

$$\left(2\frac{du}{dx} + 1\right)\frac{d^3u}{dx^3} \notin I,$$

so I is not perfect. Other examples, where one must differentiate to higher orders and then substitute in order to obtain factors are in [43, Chapter II].

Example (Branching Algorithm). *Consider the system in* $\mathbb{R}_{1,3}$ *generated by*

$$f_1 = u_{zz} - u_z u_x,$$
$$f_2 = u_{yy}.$$

With the lexicographic ordering based on $z > y > x$*, the first iteration of the algorithm yields*

$$f_3 = u_{yz} u_{xy}.$$

Hence we iterate the algorithm on two sets of generators,

$\Sigma^{1.1}$	$\Sigma^{1.2}$
$f_1 = u_{zz} - u_z u_x,$	$f_1 = u_{zz} - u_z u_x,$
$f_2 = u_{yy},$	$f_2 = u_{yy},$
$f_3 = u_{yz}.$	$f_3 = u_{xy}.$

Iterating the algorithm on $\Sigma^{1.1}$ *yields the new basis element* $f_4 = u_z u_{xy}$. *Hence two new systems* $\Sigma^{1.1.1}$ *and* $\Sigma^{1.1.2}$ *are formed, which are respectively*

$\Sigma^{1.1.1}$	$\Sigma^{1.1.2}$
$f_1 = u_z$	$f_1 = u_{zz} - u_z u_x,$
$f_2 = u_{yy}.$	$f_2 = u_{yy},$
	$f_3 = u_{yz},$
	$f_4 = u_{xy}.$

These two bases are now differential Gröbner bases, i.e. the algorithm terminates at this step. Iterating the algorithm on the system $\Sigma^{1.2}$ *yields the new basis element* $f_4 = u_{yz} u_{xx}$. *Hence two new systems are formed,* $\Sigma^{1.2.1}$ *and* $\Sigma^{1.2.2}$.

$\Sigma^{1.2.1}$	$\Sigma^{1.2.2}$
$f_1 = u_{zz} - u_z u_x,$	$f_1 = u_{zz} - u_z u_x,$
$f_2 = u_{yy},$	$f_2 = u_{yy},$
$f_3 = u_{xy},$	$f_3 = u_{xy},$
$f_4 = u_{yz}.$	$f_4 = u_{xx}.$

The algorithm terminates for both these systems with no new factors being discovered. It can be seen that $\Sigma^{1.2.1}$ *and* $\Sigma^{1.1.2}$ *are the same system and hence three distinct systems are the output of the branching algorithm. Their solutions are as follows:*

$\Sigma^{1.1.1} : u = f(x)y + g(x)$ *where* f *and* g *are arbitrary functions,*

$\Sigma^{1.2.1} : u = ky + g(x, z)$ *where* k *is a constant and*

$$\frac{\partial^2}{\partial z^2}g - \left(\frac{\partial}{\partial z}g\right)\left(\frac{\partial}{\partial x}g\right) = 0.$$

This equation has among its solutions the functions

$$g(x, z) = -\frac{b}{a}\ln\left(-\frac{a}{b}k_1(ax + bz) + k_2\right)$$

$$g(x, z) = \frac{2s}{k}(kx + r)\tanh^{-1}\left(\sqrt{\frac{ks}{2}}z + t\right)$$

$$g(x, z) = \sqrt{\frac{2}{r}}\tan^{-1}\left(\frac{z}{x\sqrt{2r}}\right) + t$$

where $k_1, k_2, k, s, t, r, a, b$ *are arbitrary constants. These solutions are found by the usual means of converting a PDE into ODE's. The first is found by looking for a solution that is a function of a linear combination of the two variables, while the third is found by looking for a solution that is a function of the quotient of the two variables. The reason one looks for these particular solutions is that the equation is invariant under translations and dilations. The second solution is found by the method of separable variables. Of course, one can always declare* g *to be independent of one of its variables, and obtain trivial solutions!*

$$\Sigma^{1.2.2} : u = g(z)x + f(z)y + h(z) \quad \textit{where}$$

$$\frac{d^2}{dz^2}g - g\left(\frac{d}{dz}g\right) = 0,$$

$$\frac{d^2}{dz^2}f - g\left(\frac{d}{dz}f\right) = 0,$$

$$\frac{d^2}{dz^2}h - g\left(\frac{d}{dz}h\right) = 0.$$

Note that both f and h satisfy the same equation. The equation in g has as its solution

$$g(z) = \sqrt{2\kappa}\tan\left(\sqrt{\frac{\kappa}{2}}z + \rho\right)$$

where κ and ρ are arbitrary constants.

The equations for the functions f and h have as solution

$$f, h = \gamma_1\sqrt{\frac{2}{\kappa}}\tan\left(\sqrt{\frac{\kappa}{2}}z + \rho\right) + \gamma_2.$$

where γ_1 and γ_2 are arbitrary constants. Hence u depends on six arbitrary constants.

It is easily seen in this example that any solution of the resulting systems is a solution to the original system.

5.3 Non-polynomial functions of the unknowns

A very desirable extension of the algorithm would be to systems whose equations contain functions of the unknowns, for example, the Sine-Gordon equations, and equations for metric components in general relativity which can have terms involving e^U, where U is some potential.

If the system contains powers of $\sin(u)$ or $\cos(u)$, we can add two unknowns to the system, v^1 and v^2, substitute v^1 for $\sin(u)$, v^2 for $\cos(u)$, and add in the equations

$$\frac{\partial v^1}{\partial x_i} - v^2\frac{\partial u}{\partial x_i} = 0$$
$$\frac{\partial v^2}{\partial x_i} - v^1\frac{\partial u}{\partial x_i} = 0$$

for $i = 1, \ldots, n$. The system will now be of the required type for the algorithm to be correct and to terminate. A similar procedure can be employed for e^u, $1/u$, $\tan(u)$ and $\sec(u)$, $\cot(u)$ and $\mathrm{cosec}(u)$.

However suppose we have an arbitrary function of an unknown.

Example 8. (system with an arbitrary function of an unknown).

$$(u_x)^2 - (u_t)^2 = 1$$
$$u_{xx} - u_{tt} = f(u)$$

where f is an arbitrary function of u, to be determined.

Using the ordering $u > f(u)$, in this case the DIFFGBASIS algorithm terminates yielding an equation in f in order for a solution u to exist, namely

$$\frac{df}{du} + f^2 = 0.$$

We input to Kolchin-Ritt

$$F = \begin{cases} (u_x)^2 - (u_t)^2 - 1 \\ u_{xx} - u_{tt} - f(u) \end{cases}$$

where f is an arbitrary function of u, to be determined.

Using the ordering $u > f(u)$, in this case the Kolchin-Ritt algorithm terminates yielding

$$G = \begin{cases} u_x^2 - u_t^2 - 1 \\ u_{xx} + f u_x^2 - f \\ u_{xx} - u_{tt} - f \\ (u_x^2 - 1)\left(\dfrac{df}{du} + f^2\right)\left(\dfrac{d^2 f}{du^2} + 2f\dfrac{df}{du}\right) \\ (u_x^2 - 1)^2\left(\dfrac{df}{du} + f^2\right) \end{cases}$$

The fifth equation is in $S(G) \cap I(G)$, so the output is not a DGB. In fact the equation $\dfrac{df}{du} + f^2 = 0$ is in $I(F)$. This can be shown in several ways, for example by changing

to characteristic coordinates, $s = x + t$, $r = x - t$, and computing the algorithm. In characteristic co-ordinates, the system is

$$F_c = \begin{cases} u_r u_s - 1 \\ u_{rs} - f(u) \end{cases}$$

The Kolchin-Ritt algorithm then yields $u_s^4 \left(\dfrac{df}{du} + f^2 \right) = 0$. *Multiplying the second equation by* u_r^4 *yields* $\dfrac{df}{du} + f^2 = 0$. *Another way of finding this equation in the ideal is to prolong and then do the algebraic Gröbner basis algorithm. This was done in Chapter 1, Example 4. Inputting the set* F_c, *the DIFFGBASIS algorithm terminates yielding*

$$K_{(\mathsf{lex}, r>s)} = \begin{cases} u_s u_r - 1 \\ \dfrac{df}{du} + f^2 \\ u_{sr} - f \\ u_{ss} + u_s^2 f(u) \end{cases}$$

Now $S(K) \cap I(K) = M\{u_r\}$ *so the set* K *is a DGB.*

(The time taken for this example ranges from 19 minutes on a MacPlus, to 1.3 minutes on an Apollo Workstation.)

The solution of this system is now easy to derive, it is:

$$f = \frac{1}{u + k} \qquad\qquad k \in \mathbb{R}$$

$$u = 2\sqrt{rs + cs + c'r + cc'} - k \qquad\qquad c, c' \in \mathbb{R}$$

The algorithms presented in this paper will terminate on examples containing arbitrary functions of the unknowns as well. To see this, in the proof of termination of the Kolchin-Ritt algorithm, split the output of the algorithm after each iteration into two sets, one whose highest derivative terms involve the unknown functions $\{u^1, \ldots, u^m\}$, and one whose highest derivative terms involve the arbitrary functions $\{b^1, \ldots, b^r\}$

of the unknowns. Since $u^j > b^k$ for all j, k, the second set contains equations that involve only the arbitrary functions. Then the argument can be applied to the two sets separately.

5.4 Chapter 5, Conclusion

This concludes the second part of the thesis, comprising Chapters 3, 4 and 5, which is concerned with the effects of computing the algorithm, and its variations, on different types of systems, and with different orderings. A truly effective theory would also take into account known symmetries of the system. Nevertheless, even in their present state the algorithms outlined in this thesis can be a valuable tool for studying systems of partial differential equations.

Chapter 6

INVOLUTIVITY AND INTEGRABILITY

This chapter is published as

E.L.Mansfield, *Simple Criterion for Involutivity*, Journal of the London Math Society, vol. 54, pp. 323–345, 1996.

Bibliography

[1] Apel and Lassner, *An Extension of Buchberger's Algorithm and Calculations in Enveloping Fields of Lie Algebras*, J. Symbolic Calculation. **6** (1988), 361–370.

[2] Bachmair and Buchberger, *A Simplified Proof of the Characterization Theorem for Gröbner Bases*, ACM SIGSAM Bulletin **40** (1976), 19–24.

[3] Bayer, *Computational Algebraic Geometry Part One: Basic Tools*, Columbia University, Lecture Notes, Conference on "Computers and Mathematics", Stanford University, August, 1986.

[4] Bayer and Stillman, *A Criterion for Detecting m-regularity*, Invent. Math. **87** (1987), 1–.

[5] ———, *A Theorem on refining division orders by the reverse-lexicographic order*, Duke Math J. **55** (1987), no. 2, 321–.

[6] Bott and Tu, *Differential forms in Algebraic Topology*, Springer-Verlag, 1982.

[7] Bryant, Chern, Gardner, Goldschmidt, and Griffiths, *Exterior Differential Systems*, Math. Sci. Res. Inst. Pub. 18, Springer Verlag, 1991.

[8] Buchberger, *A Theoretical Basis for the Reduction of Polynomials to Canonical Forms*, ACM SIGSAM Bulletin **39** (1976), 19–29.

[9] ———, *A Survey on the Method of Gröbner bases for Solving Problems in Connection with Systems of Multi-variate Polynomials*, Symbolic and Algebraic Computation by Computers (N. Inada and T. Soma, eds.), World Scientific Pub. Co., 1985.

[10] ———, *Applications of Gröbner Bases in non-linear Computational Geometry*, Mathematical Aspects of Scientific Software (J. Rice, ed.), Springer Verlag, 1988, also in Trends in Computer Algebra, Lecture Notes in Computer Science, no. 296, ed. R. Janssen, Springer Verlag, 1988.

[11] B. Buchberger, G. Collins, and B. Kutzler, *Algebraic Methods for Geometric Reasoning*, Ann. Rev. Comput. Sci. **3** (1988), 85–119.

[12] G. Carrà-Ferro, *Gröbner bases and differential ideals*, Proc. AAECC5, Springer Verlag, Menorca, Spain, 1987, pp. 129–140.

[13] Y. Choquet-Bruhat and C. DeWitt-Morette, *Analysis, Manifolds and Physics*, North-Holland(Revised Edition), 1982.

[14] C. Conley, *Lectures in Dynamical Systems*, University of Wisconsin-Madison, 1983-4.

[15] Courant and Hilbert, *Methods of Mathematical Physics*, Interscience Publishers, John Wiley, 1962.

[16] Faugère, Gianni, Lazard, and Mora, *Efficient computation of zero-dimensional Gröbner bases by change of ordering*, Preprint, 1989.

[17] M. Fleiss, *Décomposition en cascade des sytémes automatiques et feuilletages invariants*, Bull. Soc. Math. France **113** (1985), 285–293.

[18] K. Forsman, *Private communication.*

[19] Galligo, *Some algorithmic questions on ideals of differential operators*, Proc. EUROCAL '85, L.N.C.S. 204.

[20] P. Gianni, B. Trager, and G. Zacharias, *Gröbner bases and Primary Decomposition of Polynomial Ideals*, J. Symbolic Alg. **6** (1988), 149–167.

[21] H. Goldschmidt, *Integrability Criteria for Systems of non-linear partial differential equations*, J. Differential Geometry **1** (1967), 269–307.

[22] Hartley and Tucker, *A constructive implementation of the Cartan-Kähler Theory of exterior differential systems*, Preprint, Dept. Physics, University of Lancaster.

[23] R. Hartshorne, *Algebraic Geometry*, Springer Verlag, 1977.

[24] D. Hilbert, *Ueber die Theorie der algebraischen Formen.*, Math. Ann. (1890), 473–534.

[25] Hilton and Stammbach, *A Course in Homological Algebra*, Springer Verlag, 1971.

[26] M. Hirsch, *Differential Topology*, Springer Verlag, 1976.

[27] A. Hudson, *Symbolic Computation of Involutivity of PDEs.*, Masters Thesis, University of Sydney, 1987.

[28] M. Janet, *Sur les Systèmes d'Équations aux Dérivées Partielles*, J. Math. Pure Appl. **3** (1920), 65–151.

[29] F. John, *Partial Differential Equations*, Springer-Verlag, 1982.

[30] Kolchin, *Differential algebra and algebraic groups*, Pure and Applied Mathematics, 54, Academic Press, Inc., Orlando, FL, 1973.

[31] Lazard, *A new method for solving algebraic systems of positive dimension*, Preprint, LITP, Paris VII, no. 89–77.

[32] R. McGehee, *Triple collisions in the collinear three-body problem*, Invent. Math. (1974), 191–227.

[33] Melenk, *Solving Polynomial Equation Systems by Gröbner Type Methods*, CWI Quarterly **3** (1990), 121–136.

[34] Möller and Mora, *New Constructive Methods in Classical Ideal Theory*, J. Algebra **100** (1986), 138–178.

[35] C.A. Neff, *Decomposing Algebraic varieties using Gröbner bases*, Preprint IBM Research, T.J. Watson Research Center.

[36] F. Ollivier, *Canonical Bases: Relations with Standard Bases, Finiteness Conditions and Application to Tame Automorphisms*, Research Report LIX/RR/90/14, École polytechnique, Laboratoire d'Informatique.

[37] ———, Thesis, École Polytechnique, 1990.

[38] J.F. Pommaret, *Systems of Partial Differential Equations and Lie pseudogroups*, Gordon & Breach Science, London, 1978.

[39] ———, *Differential Galois Theory*, Gordon & Breach Science, London, 1983.

[40] ———, *Géometrie différentielle algébrique et théorie du contrôle - Note*, C.R.Acad. Sci. Paris 302 Série I (1986), no. 15, 547–550.

[41] ———, *Lie Pseudogroups and Mechanics*, Gordon & Breach Science, London, 1988.

[42] ———, *Problèmes formels en théorie du contrôle aux dérivées partielles*, C.R.Acad. Sci. Paris 308 Série I (1989), 457–460.

[43] Ritt, *Differential Algebra*, A.M.S. Colloquium Lectures **33** (1950).

[44] L. Robbiano, *Term orderings on the polynomial ring*, EUROCAL 85, Springer LNCS 204, 1985, pp. 513–517.

[45] J. Rotman, *An Introduction to Homological Algebra*, Academic Press, 1979.

[46] F.O. Schreyer, *Diplomarbeit am Fachbereit Mathematik der Universität Hamburg*, 1980.

[47] F. Schwarz, *Symmetries and Involution Systems: Some Experiments in Computer Algebra*, Topics in Soliton Theory and exaclty solvable equations (B. Fuchssteiner M. Ablowitz and M. Kruskal, eds.), World Scientific Pub., 1987, pp. 290–299.

[48] F. Schwarz, *Monomial Orderings and Gröbner bases*, SIGSAM Bulletin **25** (1991), no. 1, 10–23.

[49] W. Sit, *Some comments on Term-ordering in Gröbner basis calculations*, ACM SIGSAM Bulletin **23** (1989), no. 2, 34–38.

[50] D. Spear, *A Constructive Approach to Commutative Ring Theory*, Proc. the 1977 MACSYMA User's Conference, Univ. California-Berkeley. NASA CP- 2012.

[51] D. Spencer, *Overdetermined systems of linear partial differential equations*, Bull. Am. Math. Soc **75** (1969), 179–239.

[52] N. Steenrod, *Fibre bundles*, Prentice-Hall, 1957.

[53] O. Stormark, *Formal and local solvability of partial differential equations*, TRITA-MAT **11** (1988).

[54] Trinks, *über B. Buchbergers Verfahren, Systeme algebraisher Gleichungen zu lösen*, J. Number Theory **10** (1978), 475–488.

[55] R. Walker, *Algebraic Curves*, Springer Verlag, 1978.

[56] V. Weispfenning, *Admissible Orders and Linear Forms*, ACM SIGSAM Bulletin **5** (1987), 16–18.

[57] F. Winkler, *Solution of Equations I: Polynomial Ideals and Gröbner Bases*, Lecture Notes, Conference on "Computers and Mathematics", Stanford University, August, 1986.

[58] Zariski and Samuel, *Commutative Algebra*, vol. I and II, Van Nostrand, 1958, Springer Verlag 1975.

Appendix 1–3 USER'S MANUAL FOR DIFFGROB

In the original version of the thesis there were 3 appendices:

Appendix 1. User's manual for DIFFGROB;

Appendix 2. Description of procedures;

Appendix 3. The Code.

These appendices are omitted because they are superseded by diffgrob2 manual.

Further information: http://www.kent.ac.uk/IMS/personal/elm2/

Online demo: http://centaur.maths.qmw.ac.uk/CATHODE/DiffGrob2_demo.html

Appendix 4 RESEARCH DIRECTIONS

This appendix contains various avenues for further research. Other unsolved problems can be found in the Appendix of [43].

1) IMPROVE THE EFFICIENCY OF THE ALGORITHM
One of the costliest parts of the algorithm are the procedures involving pseudo-reduction and reduction. To lessen the number of differential S polynomials to be calculated and hence pseudo-reduced can possibly be achieved in a number of ways:

(i) are there any theoretical grounds on which one can guarantee a diffSpoly pseudo-reduces to zero?

(ii) see also problems 2, 9

(iii) find the fastest path to a normal form for a given term ordering

2) EFFICACIOUS TERM ORDERINGS
Find the fastest term orderings for a particular system. Similar to this problem is that of finding the term ordering from which it is easiest to solve the system.

3) PRIME DECOMPOSITION OF DIFFERENTIAL IDEALS
This problem has been solved in the algebraic case by Gianni et al, so it is natural to try to solve the differential analogue. Ritt, Ollivier and Kolchin discuss at length

prime differential ideals. The complication in the differential case is that one must know how many times to differentiate before one reduced the problem to the algebraic one. See also [31].

4) NON-COMMUTATIVE DIFFERENTIAL OPERATORS

One can generalize the derivations used here to derivations in Lie Algebras other than $\langle \frac{\partial}{\partial x_i} \mid i = 1, \ldots, n \rangle$. One should be able to use the work of Apel and Lassner in the differential setting. Note that their work does not apply directly, since polynomials of operators are not equivalent to polynomials of operated on functions.

5) INVERSE BÄCKLUND PROBLEM

This is the opposite of elimination. Suppose that we have a problem in two unknowns u and v, and we know the elimination ideals $I \cap \mathbb{R}_{\mathsf{diff}}[x_1, \ldots, x_n; u]$ and $I \cap \mathbb{R}_{\mathsf{diff}}[x_1, \ldots, x_n; v]$. Find a basis for I.

6) PERTURBATION OF SYSTEMS

If a system is perturbed in a certain way, for example, to make the equations transverse, or if the equations depend on a certain parameter, how does a differential Gröbner basis perturb?

7) GLOBALIZE TO SYSTEMS ON MANIFOLDS

Extend the theory to systems on spaces other than $\mathbb{R}^n$.

8) THE BRANCHING ALGORITHM

Implement the branching algorithm and describe more precisely the relationship of its output to the output of the non-branching algorithm.

9) SYMMETRIES AND DGB'S

One should be able to take advantage of a known symmetry structure to make the algorithm more efficient, i. e. terminate within the available memory. This problem would rely on problem 4 begin solved, i. e. having a generalization of the algorithm

to non-commutative operators. Is there any connection between such a generalization and differential Galois theory ([39])?

10) GENERAL COEFFICIANTS

The theory should generalize to coefficients other than $\mathbb{R}$ or $\mathbb{C}$. Perhaps spurious factor could be "divided out" as part of the coefficient ring.

11) USE OF REDUCTION IN RADICAL IDEALS

The algorithm using reduction, not pseudo-reduction may terminate for systems that generate perfect or radical ideals, since Ritt proved that ascending chains of perfect ideals terminate (i.e. differential ideals are noetherian with respect to radical ideals.)

12) TERMINATION OF THE JANET RESOLUTION

The theorems in Chapter 6 should go a long way to proving that the Janet resolution of non-linear systems terminates, since all systems are eventually (with sufficient prolongation) involutive, meaning that all syzygies of the symbol equations are eventually of degree 1.

13) EFFICACIOUS CO-ORDINATES

The final example of Chapter 5 shows that a change of co-ordinates can lead to massive variations in time to terminate, and utility of the output. Are there any algorithmic methods which lead to "better" co-ordinates.

14) USE OF THE JANET RESOLUTION TO CONSTRUCT SOLUTIONS

If the Janet resolution is exact, it may be possible to construct a homotopy operator on the resolution, allowing a solution to be constructed.

15) DO SYSTEMS THAT GENERATE PRIME IDEALS HAVE LOCI THAT ARE MANIFOLDS IN THE JET BUNDLE, AND VICE VERSA?

Pommaret [39, p.246] has a criterion for an ideal to be prime. Systems that generate a prime ideal do not yield new factors upon differentiation.

Appendix 5 SOME DEFINITIONS AND RESULTS

This appendix contains some basic definitions and results for fibre bundles and for homological algebra, as they needed in Chapter 6. This thesis does not require any global theory. Further references are [52], [6], [13], [26], [25].

The third part of this Appendix contains the proof of a criterion for involutivity used to corroborate certain examples in Chapter 6

A5.1 Fibre Bundles

These notes are compiled from [13], [38], lecture notes in Differential Topology given at the University of Sydney, 1979 by Dr. M. J. Field and at the University of Wisconsin, 1982-3 by Dr. D. Stowe.

A **bundle** is a triple (E, B, π) consisting of two topological spaces E and B and a continuous onto mapping $\pi : E \to B$. The space B is called the **base**. The simplest example is the cartesian bundle $(M \times B, B, \pi)$ where the projection π is given by $\pi(m, b) = b$.

A **fibre bundle** (E, B, π, G) is a bundle (E, B, π) together with a fibre F such that $\pi^{-1}(x)$ (denoted F_x) is homeomorphic to F for all $x \in B$, a topological group of homeomorphisms, G, of F onto itself, and a covering of B by a family of open sets $\{U_\alpha : \alpha \in A\}$ such that:

(1) locally the bundle is a **trivial bundle**, i. e. for each α, $\pi^{-1}(U_\alpha)$ is homeomorphic to $U_\alpha \times F$. The homeomorphism has the form

$$\varphi_\alpha : \pi^{-1}(U_\alpha) \to U_\alpha \times F, \quad \varphi_\alpha(p) = (\pi(p), \phi_\alpha(p))$$

Let $x \in B$. Then $\phi_{\alpha,x} = \phi_\alpha|_{\pi^{-1}(x)}$ is a homeomorphism of F_x onto F.

(2) Let $x \in U_\alpha \cap U_\beta$. Then $\phi_{\alpha,x}\phi_{\beta,x}^{-1} : F \to F$ is an element of the group G.

(3) The induced mappings $g_{\alpha\beta} : U_\alpha \cap U_\beta \to G$ given by $g_{\alpha\beta}(x) = \phi_{\alpha,x}\phi_{\beta,x}^{-1}$ are continuous. They are called the **transition functions**, and satisfy the relation $g_{\alpha\beta}(x)g_{\beta\gamma}(x) = g_{\alpha\gamma}(x)$.

A **vector bundle** is a fibre bundle where the fibre is a vector space of dimension n (say), and the group G is a subgroup of the general linear group $GL(n)$. Similarly, if the fibre is an affine space and G is the group of linear transformations and translations, the bundle is an **affine bundle**. More precisely, if $\{U_\alpha\}$ are the trivialising patches on the affine bundle $\mathcal{F}$, for $(x, y) \in \pi^{-1}(U_\alpha \cup U_\beta)$,

$\mathrm{pr}_2\varphi_\alpha\varphi_\beta^{-1} : U_\alpha \cap U_\beta \times F \to F$ is given by

$(x, y) \to A_{\alpha\beta}(x) + B_{\alpha\beta}(x)$

where pr_2 is projection onto the second factor, and $A_{\alpha\beta}(x)$ is an element of $GL(F)$ and $B_{\alpha\beta}(x) \in F$. Note F is an affine space so linear transformations and translations are defined. It is possible to consider a related vector bundle whose translation functions are given by the $\{A_{\alpha\beta(x)}\}$; the fibre may be smaller than F depending on the $\{A_{\alpha\beta(x)}\}$. In this case, we say the affine bundle is **modelled** on the related vector bundle.

The **tangent vector** to a manifold M at a point x is defined to be an equivalence class of differential curves; curves are maps $\gamma : I \subset \mathbb{R} \to M$ such that $\gamma(0) = x$. Two

curves γ_1, γ_2 are equivalent if, under every mapping f taking a neighbourhood of x to $\mathbb{R}$, which is differentiable at x, then

$$\frac{d}{dt}|_{t=0} f \circ \gamma_1 = \frac{d}{dt}|_{t=0} f \circ \gamma_2.$$

(Recall a map $f : U_\alpha \to \mathbb{R}$ is differentiable at a point x if, when composed with the inverse of a co-ordinate chart map, $\phi_\alpha^{-1} : \mathbb{R}^n \to U_\alpha$, it is differentiable as a map $\mathbb{R}^n \to \mathbb{R}$ (where $n = \dim M$) at $\phi_\alpha^{-1}(x)$.)

If the maps f are co-ordinate charts composed with a projection to a coordinate hyperplane in $\mathbb{R}^n$, we obtain that all components of the tangent vector are well-defined.
Since locally M has co-ordinates that look like $\mathbb{R}^n$, it makes sense that locally we can add curves, and multiply them by constants. Such operations take equivalence classes to equivalence classes in a well-defined way. Hence the union of all equivalence classes of curves γ such that $\gamma(0) = x$ is a vector space; it is denoted $T_x(M)$. The **tangent bundle** is the union $\cup_{x \in M} T_x(M)$.

This definition has an advantage in proving theorems, since to produce a tangent vector at x we take a curve γ on the manifold such that $\gamma(0) = x$, compose with a local co-ordinate chart, and consider its derivative at $t = 0$.

If $\{U_\alpha, \phi_\alpha : U_\alpha \to \mathbb{R}^n\}$ is an atlas for M, the transition functions of the tangent bundle at x are the jacobians of the maps $\{\phi_\alpha \phi_\beta^{-1} : \mathbb{R}^n \to \mathbb{R}^n\}$ at x, since the trivialising maps for $T(M)$ are the tangent maps of the $\{\phi_\alpha : U_\alpha \to \mathbb{R}^n\}$. (This is one way of defining the tangent bundle.)

The dual $T_x^*(M)$ to the tangent vector space $T_x(M)$ is the space of linear maps $T_x(M) \to \mathbb{R}$; it is a vector space whose elements are called co-tangent vectors. Forming the union over all $x \in M$ yields the cotangent bundle $T^*(M)$. If $\{U_\alpha, \phi_\alpha : U_\alpha \to \mathbb{R}^n\}$ is an atlas for M, the transition functions of the cotangent bundle at x are the adjoints of the jacobians of the maps $\{\phi_\alpha \phi_\beta^{-1} : \mathbb{R}^n \to \mathbb{R}^n\}$ at x.

Given a map $g : N \to M$ and a bundle (E, M, π), we define the **pullback bundle** $(g^{-1}(E), N, p) : g^{-1}(E) = \{y \in N \times E \mid g\mathrm{pr}_1(y) = \pi\mathrm{pr}_2(y)\}$ where pr_i is the projection onto the i^{th} factor.

$$\begin{array}{ccc} g^{-1}(E) & \xrightarrow{\mathrm{pr}_2} & E \\ \downarrow{\scriptstyle \mathrm{pr}_1} & & \downarrow{\scriptstyle \pi} \\ N & \xrightarrow{g} & M \end{array}$$

Given two bundles over the same base $(\mathcal{F}, B, \pi)$ and $(\mathcal{L}, B, \tau)$, whose fibres have a linear structure over the same coefficient ring, we can form the **tensor product** bundle $\mathcal{F} \otimes \mathcal{L}$. The total space of the tensor bundle is the union $\cup_{x \in M} \pi^{-1}(x) \otimes \tau^{-1}(x)$. We take a cover of B that is sub-ordinate to the corves that trivialize the bundles $\mathcal{F}$ and $\mathcal{L}$, and take appropriate restrictions to the trivialising maps for $\mathcal{F}$ and $\mathcal{L}$. Then the trivialising maps for $\mathcal{F} \otimes \mathcal{L}$ is the tensor product of the trivialising maps for $\mathcal{F}$ and $\mathcal{L}$.

To form the bundles $S^k T^*(M)$ and $\Lambda^k T^*(M)$, we take the tensor product of the cotangent bundle $T^*(M)$ with itself k times (the fibres have a linear structure over $\mathbb{R}$), and then take the symmetric and anti-symmetric subsets respectively.

Given the bundle (M, B, π), it is not necessary that all the fibres be homeomorphic. Let M be a manifold of dimension $k + n$, with base space of dimension k. Suppose M has an open covering by open sets $\{U_\alpha : \alpha \in A\}$, with co-ordinate maps $\varphi_\alpha : U_\alpha \to \mathbb{R}^{n+k}$ and $\{\pi(U_\alpha) = V_\alpha : \alpha \in A\}$ is a covering of B, with $\psi_\alpha : \pi(U_\alpha) \to \mathbb{R}^k$ the co-ordinate charts for B. We say M is a **fibred manifold** with base B if the diagram:

$$\begin{array}{ccc} U_\alpha & \xrightarrow{\varphi_\alpha} & \mathbb{R}^n \times \mathbb{R}^k \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \mathrm{pr}_2} \\ V_\alpha & \xrightarrow{\psi_\alpha} & \mathbb{R}^k \end{array}$$

commutes, where pr_2 is the projection onto the second factor.

A5.2 Homological Algebra

These notes are from lectures in Algebraic Topology given at the University of Sydney in 1979 by Dr. R. Eyland.

A graded group is a family $\{G_\alpha : \alpha \in \mathbb{Z}\}$ of commutative groups indexed by the integers. Without loss of generality, the group operation is assumed to be addition.
A chain complex is a pair (C, ∂) consisting of a graded group and an endomorphism $\partial : C \to C$ such that $\partial\partial = 0$ and ∂ has degree -1. This means the map ∂ consists of maps $\{\partial_n : C_n \to C_{n-1}\}$ such that $\partial_{n-1}\partial_n = 0$, $\partial(c+d) = \partial(c) + \partial(d)$, and $\partial(-c) = -\partial(c)$.
A chain map $\tau : (C, \partial) \to (C', \partial')$ is a set of maps $\tau_n : C_n \to C'_n$ which satisfy $\tau(c+d) = \tau(c)+\tau(d)$, $\tau(-c) = -\tau(c)$ (i.e. τ is a homomorphism), and $\tau_n\partial'_n = \partial_n\tau_{n-1}$ (τ commutes with ∂).
A subcomplex of a chain complex C is a chain complex $C' = \{C'_n\}$ such that for each n, C'_n is a subgroup of C_n and $\partial'_n = \partial_n|_{C'_n}$. For each subcomplex, there is a quotient complex C/C' where $(C/C')_n = (C_n)/C'_n$ and the differential is the induced map $c + C'_n \to \partial(c) + C'_{n-1}$.
For a chain complex C, we defined the graded group of cycles $Z(C) = \ker\partial$, i.e. $Z_n = \ker\partial_n$, and the graded group of boundaries $B(C) = \text{im}\ \partial$, i.e. $B_n = \text{im}\ \partial_n$. We define the homology graded group $H(C) = Z(C)/B(C)$; $H_n = Z_n/B_n$. The equivalence class of $z \in Z_n$ is denoted $\{z\}$.
If the deferential is of degree $+1$, so that $\partial_n : C_n \to C_{n+1}$, the corresponding homology groups are called cohomology groups, the cycles cocycles and the boundaries, coboundaries. Theorems proved for homology have corresponding theorems in cohomology.

A short exact sequence of chain complexes is a sequence of chain maps

$$\mathcal{C}: \quad 0 \longrightarrow C' \xrightarrow{\alpha} C \xrightarrow{\beta} C'' \longrightarrow 0$$

such that for all n, $\ker \beta_n = \text{im } \alpha_n$, the maps α_n are 1-1 and the maps β_n are onto. So $\mathcal{C}$ corresponds to a commutative diagram of abelian groups:

$$\begin{array}{ccccccccc}
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & C'_{n+1} & \xrightarrow{\alpha_{n+1}} & C_{n+1} & \xrightarrow{\beta_{n+1}} & C''_{n+1} & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \partial'_{n+1}} & & \downarrow{\scriptstyle \partial_{n+1}} & & \downarrow{\scriptstyle \partial''_{n+1}} & & \\
0 & \longrightarrow & C'_{n} & \xrightarrow{\alpha_{n}} & C_{n} & \xrightarrow{\beta_{n}} & C''_{n} & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \partial'_{n}} & & \downarrow{\scriptstyle \partial_{n}} & & \downarrow{\scriptstyle \partial''_{n}} & & \\
0 & \longrightarrow & C'_{n-1} & \xrightarrow{\alpha_{n-1}} & C_{n-1} & \xrightarrow{\beta_{n-1}} & C''_{n-1} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & &
\end{array}$$

in which all rows are exact and the composite of any two vertical maps is trivial. Short exact sequences arise naturally when one considers a subcomplex C' of a chain complex C:

$$0 \longrightarrow C' \xrightarrow{\alpha} C \xrightarrow{\beta} C/C' \longrightarrow 0$$

where α is the inclusion and β the natural projection.
Let H' denote the homology graded group of C' and H'' the homology graded group of C''.

Chain maps naturally induce maps on the homology classes. If a homology class $x = \{z\}$ (say) i.e. the class x is represented by z, then the homology map $\alpha_* : H(C') \to H(C)$ induced by $\alpha : C' \to C$, is given by $\alpha_* x = \{\alpha z\}$. Since $\alpha\partial = \partial'\alpha$, the map α_* is well-defined.

Lemma A5.1 (The snake or connecting homomorphism Δ_*). *Let a short exact sequence $\mathcal{C}$ be given, and let α_* and β_* be the maps induced by α, β on homology groups. There is homomorphism $\Delta_* : H'' \to H$ of degree -1 i.e. $\Delta_n : H''_n \to H_{n-1}$, so that the sequence*

$$\mathcal{L} : \qquad \longrightarrow H_{n+1}(C'') \xrightarrow{\Delta_*} H_n(C') \xrightarrow{\alpha_*} H_n(C) \xrightarrow{\beta_*} H_n(C'') \xrightarrow{\Delta_*} H_{n-1}(C') \longrightarrow$$

is exact.

Proof. Definition of Δ_* : Let $x \in H_{n+1}(C'')$, so that x is an equivalence class of elements in C''_{n+1}, $x = \{z\}$ or $z + B''_{n+1}$, and $\partial''(z) = 0$. By exactness β is onto and so $z = \beta(w)$ for some $w \in C_n$. Now $\beta\partial w = \partial''\beta w = \partial'' z = 0$. By exactness, $\ker\beta = \text{im }\alpha$, and α is 1-1, so there is a unique $u \in C'_{n-1}$ such that $\alpha u = \partial w$. The element $u = \Delta_*(z)$: we need to show that Δ is well-defined on the equivalence class of x, that is, if we take any other representative of the class x, we obtain an element in the same equivalence class as u. Suppose $w_1 \in C_n$ is another element such that $\beta w_1 \in x$ (i.e. $x = w_1 + B''_{n+1}$) Then $\beta(w - w_1) \in B_n(C')$ i.e. $\beta(w - w_1) = \partial'' v$ for some $v \in C''_{n+1}$. Since β is onto, $v = \beta y$, some $y \in C_{n+1}$. So $\beta(w - w_1) = \partial''\beta y = \beta\partial y$ or $\beta(w - w_1 - \partial y) = 0$. Again by exactness , $w - w_1 - \partial y = \alpha t$, some $t \in C'_n$. Then $\partial w_1 = \partial w - \partial\partial y - \partial\alpha t = \alpha u - \alpha\partial' t = \alpha(u - \partial' t)$, i.e. $\Delta_*(\beta w_1) = u - \partial' t$. But $u - \partial' t + B_{n-1}(C') = u + B_{n-1}(C')$. In other words, Δ_{*n} assigns to the homology class x the homology class of $\alpha^{-1}\partial\beta^{-1}x$.

We now show the sequence $\mathcal{L}$ is exact.

We have

$$\begin{cases} \Delta_*\beta_* x = \{\alpha^{-1}\partial\beta^{-1}\beta x\} = \{\alpha^{-1}\partial x\} = \{\alpha^{-1}0\} = 0 \\ \beta_*\alpha_* x = (\beta\alpha)_* x = 0 \\ \alpha_*\Delta_* x = \{\alpha\alpha^{-1}\partial\beta^{-1}x\} = \{\partial\beta^{-1}x\} = 0 \end{cases}$$

so

$$\begin{cases} \text{im }\beta_* \subset \ker\Delta_* \\ \text{im }\alpha_* \subset \ker\beta_* \\ \text{im }\Delta_* \subset \ker\alpha_* \end{cases}$$

Let $x \in \ker\Delta_*$ and let $z \in x$, $z \in C'_n$. Then, as above, $z = \beta y$ and $\alpha^{-1}\partial y \in B_{n-1}(C')$ (α is 1-1 by exactness.) So $\alpha^{-1}\partial y = \partial' u$ for some $u \in C'_n$. Then $y - \alpha u \in C_n$ and $\partial(y - \alpha u) = \partial y - \partial\alpha u = \partial y - \alpha\partial' u = 0$. So $y - \alpha u \in Z_n(C)$. Then $\beta_*\{y - \alpha u\} = \{\beta y - \beta\alpha u\} = \{z\} = x$.

So $\ker\Delta_* \subset \text{im }\beta_*$.

Let $x \in \ker \beta_*$, $z \in x$. Then $z \in C_n$ and $\beta z \in B_n(C'')$. So $\beta z = \partial' y$ for some $y \in C''_{n+1}$. Since β is onto, $y = \beta u$ some $u \in C_{n+1}$. Thus $\beta z = \partial' \beta u = \beta \partial u$. So $\beta(z - \partial u) = 0$. So $z - \partial u = \alpha v$ for some $v \in C'_n$. Now $\alpha \partial' v = \partial z - \partial \partial u = 0$. So $v \in Z_n(C')$. Then $\alpha_*\{v\} = \{\alpha v\} = \{z - \partial u\} = \{z\} = x$.

So $\ker \beta_* \subset \text{im } \alpha_*$.

Let $x \in \ker \alpha_*$, $z \in x$. Then $z \in C'_n$ and $\alpha z = \partial y$ for some $y \in C_{n+1}$. Then $z \in \{\alpha^{-1}\partial\beta^{-1}\beta y\}$. So $x = \Delta_*\{\beta y\}$, while $\beta y \in Z_n(C'')$ since $\partial''\beta y = \beta \partial y = \beta\alpha z = 0$.

So $\ker \alpha_* \subset \text{im } \Delta_*$. □

Using the long exact sequence, we show what happens if $H_n(C) \equiv 0$, that is, the middle column of the large commutative diagram above, corresponding to the short exact sequence, is exact. From the long exact sequence derived from the short exact sequence using the snake homomorphism, we have

$$\mathcal{L}' : \quad 0 \longrightarrow H_{n+1}(C'') \xrightarrow{\Delta_*} H_n(C') \xrightarrow{\alpha_*} 0 \xrightarrow{\beta_*} H_n(C'') \xrightarrow{\Delta_*} H_{n-1}(C') \longrightarrow 0 \ldots$$

Thus the maps α_* and β_* are the zero maps. By exactness, the maps Δ_* are both onto and 1-1, that is, they are isomorphisms.
Hence $H_n(C'') \approx H_{n-1}(C')$ for all n.

A5.3 A criterion for involutivity

The results in this section appear in [38, pp.10–4]. Proofs given here are those of the author.
They concern a criterion for involutivity obtained by grading the Spencer δ-operator lexicographically; the δ-operator is already graded by the degree on Λ^n, so we have a double grading of δ. The result is used to corroborate the involutivity of certain systems discussed in Chapter 6.

For the definitions of g_r, τ_r, S^kT^*, $V(\mathcal{E})$, $dx^{(\nu)}$ and δ, refer to Chapter 6.

Define the operators δ_i as follows:

$$\delta_i(dx^{(\nu)}) = \begin{cases} dx^{(\nu-1_i)} & \nu_i > 0 \\ 0 & \text{otherwise} \end{cases}$$

and set $(S^kT^*)^i = \{w \in S^kT^* \mid \delta_1(w) = 0, \delta_2(w) = 0, \ldots, \delta_i(w) = 0\}$. The elements of $(S^kT^*)^i$ are those symmetric forms that involve no components in the $x_1, x_2, \ldots, x_i$ directions and

$$0 = (S^kT^*)^n \subset (S^kT^*)^{n-1} \subset \ldots \subset (S^kT^*)^2 \subset (S^kT^*)^0 = S^kT^*$$

It is trivial to check that $\delta = \sum_i dx_i \wedge \delta_i$ (up to a constant!)

The vector space g_{q+r} are graded the same way as the $(S^kT^*)^i$:

$$(g_{q+r})^i = g_{q+r} \cap \left(S^{q+r}T^* \otimes V(\mathcal{E})\right)^i.$$

Lemma A5.2. *The symbol maps τ_r commute with the δ_i, and thus respect the grading on S^kT^*.*

Proof. Spencer [51] proves that the following diagram commutes (Pommaret uses σ_r for the symbol map; we have used this notation for the symbol of an equation, and hence use τ_r to represent the actual linear map between the symmetric bundles)

$$\begin{array}{ccc} S^{q+r+1}T^* \otimes V(\mathcal{E}) & \xrightarrow{\tau_{r+1}} & S^{r+1}T^* \otimes V(\mathcal{E}') \\ \downarrow \delta & & \downarrow \delta \\ T^* \otimes S^{q+r}T^* \otimes V(\mathcal{E}) & \xrightarrow{\mathrm{id}_{T^*} \otimes \tau_r} & T^* \otimes S^rT^* \otimes V(\mathcal{E}') \end{array}$$

which is equivalent to the statement, $dx_i \otimes \delta_i\tau_{r+1} = dx_i \otimes \tau_r\delta_i$. Therefore $\delta_i\tau_{r+1} = \tau_r\delta_i$. It then follows that

$$\tau_{r+1} : \left(S^{q+r+1}T^* \otimes V(\mathcal{E})\right)^i \to \left(S^{r+1}T^* \otimes V(\mathcal{E}')\right)^i.$$

□

By definition, the two sequences

$$0 \longrightarrow (g_{q+r+1})^{i-1} \longrightarrow \big(S^{q+r+1}T^* \otimes V(\mathcal{E})\big)^{i-1} \xrightarrow{\tau_{r+1}}$$

$$\tau_{r+1}\Big(\big(S^{q+r+1}T^* \otimes V(\mathcal{E})\big)^{i-1}\Big) \longrightarrow 0$$

and

$$0 \longrightarrow \big(S^{q+r+1}T^* \otimes V(\mathcal{E})\big)^{i} \longrightarrow \big(S^{q+r+1}T^* \otimes V(\mathcal{E})\big)^{i-1} \xrightarrow{\delta_i}$$

$$\big(S^{q+r}T^* \otimes V(\mathcal{E})\big)^{i-1} \longrightarrow 0$$

are exact. Define

$$\big(\tau_r\big(S^{q+r}T^* \otimes V(\mathcal{E})\big)\big)^i = \tau_r\big(S^{q+r}T^* \otimes V(\mathcal{E})\big) \cap \big(S^rT^* \otimes V(\mathcal{E}')\big)^i.$$

Notation: write T^k for $S^kT^* \otimes V(\mathcal{E})$.

Lemma A5.2 implies that $\tau_{r+1}((T^{q+r+1})^i) \subset (\tau_{r+1}((T^{q+r+1})^{i-1}))^i$. The two exact sequences for δ_i and τ_r can be "enmeshed" in the following commutative and exact diagram (arrows in outline are inclusions):

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & (g_{q+r+1})^i & \longrightarrow & (T^{q+r+1})^i & \longrightarrow & \big(\tau_{r+1}((T^{q+r+1})^{i-1})\big)^i & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & (g_{q+r+1})^{i-1} & \longrightarrow & (T^{q+r+1})^{i-1} & \longrightarrow & \tau_{r+1}((T^{q+r+1})^{i-1}) & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \delta_i} & & \downarrow{\scriptstyle \delta_i} & & \downarrow{\scriptstyle \delta_i} & & \\
0 & \longrightarrow & (g_{q+r})^{i-1} & \longrightarrow & (T^{q+r})^{i-1} & \longrightarrow & \tau_r((T^{q+r})^{i-1}) & \longrightarrow & 0 \\
 & & & & \downarrow & & \downarrow & & \\
 & & & & 0 & & 0 & &
\end{array}$$

Lemma A5.3. *The maps*

$$\tau_{r+1} : \big(S^{q+r+1}T^* \otimes V(\mathcal{E})\big)^i \to \big(\tau_{r+1}(S^{q+r+1}T^* \otimes V(\mathcal{E}))\big)^i$$

(all $r \geq 0$, $i \geq 0$) are surjective if and only if the maps $\delta_i(g_{q+r+1})^{i-1} \to (g_{q+r})^{i-1}$ (all $r \geq 0$, $i \geq 1$) are surjective. ([38, p. 104])

Lemma A5.4. *$H(\Lambda^p T^* \otimes (g_{q+r})^{n-1}) = 0$ for all $p \geq 0$, $r \geq 0$.*

Proof. The vector space $(g_{q+r})^{n-1} \subset \left(S^{q+r}T^* \otimes V(\mathcal{E})\right)^{n-1} = \langle dx_n^{(q+r)} \otimes e^k \mid k = 1, \ldots, m \rangle$. If $(g_{q+r})^{n-1} = 0$, there is nothing to prove. Now
$0 = \delta(\alpha \otimes dx_n^{(q+r)}) = \alpha \wedge dx_n \otimes dx_n^{(q+r-1)}$
$\Rightarrow \quad \alpha \wedge dx_n = 0$
$\Rightarrow \quad \alpha = \alpha' \wedge dx_n$
$\Rightarrow \quad \alpha \otimes dx_n^{(q+r)} = \delta(\alpha' \otimes dx_n^{(q+r+1)})$. The space $(g_{q+r})^{n-1}$ is several copies of $\langle dx_n^{(q+r)} \rangle$; the preceding argument applies to each copy, since $dx_n^{(q+r)} \otimes e^k \in (g_{q+r})^{n-1} \Rightarrow dx_n^{(q+r+1)} \otimes e^k \in (g_{q+r+1})^{n-1}$. □

Theorem A5.5 (CRITERION FOR INVOLUTIVITY). *If the maps $\delta_i : (g_{q+r+1})^{i-1} \to (g_{q+r})^{i-1}$ for all $r \geq 0$ and $i \geq 1$ are surjective, then g_q is an involutive symbol.*

Proof. Let $w \in \Lambda^p T^* \otimes g_{q+r}$ be such that $\delta(w) = 0$. Separate w into two terms, one consisting of the summands of w with dx_1 in their anti-symmetric part, and one, denoted w_1, consisting of the summands of w without dx_1 in their anti-symmetric part, so that

$$w = w_1 + \sum_k \alpha_k \wedge dx_1 \otimes s_k$$

where $s_k \in g_{q+r}$, $\alpha_k \in \Lambda^{p-1}T^*$ and α_k has no term containing dx_1 in its anti-symmetric part. Now $\delta_1 : g_{q+r+1} \to g_{q+r}$ is surjective, so for all k, there is a $t_k \in g_{q+r+1}$ such that $\delta_1(t_k) = s_k$. Let $w_2 = \sum \alpha_k \otimes t_k$, and let $w^{(1)} = w - \delta(w_2) = w_1 - \sum_{k,j>1} \alpha_k \wedge dx_j \otimes \delta_j t_k$. Now $\delta w^{(1)} = \delta(w - \delta(w_2)) = \delta w = 0$ and no summand of $w^{(1)}$ has dx_1 in its anti-symmetric part. There two facts together imply that $w \in \Lambda^p T^* \otimes (g_{q+r})^1$. Now use the fact that $\delta_2 : (g_{q+r+1})^1 \to (g_{q+r})^1$ is surjective. Repeating the argument yields an

element

$$w^{(2)} = w^{(1)} - \delta w_2^{(1)} = w - \delta(w_2) - \delta w_2^{(1)} \in \Lambda^p T^* \otimes (g_{q+r})^2,$$

with $\delta w^{(2)} = 0$. Continuing in this way, we obtain an element $w^{(n-1)}$ in $\Lambda^p T^* \otimes (g_{q+r})^{n-1}$, with $\delta w^{(n-1)} = 0$, and $w^{(n-1)} = w - \delta(\phi)$ for some $\phi \in \Lambda^{p-1} T^* \otimes g_{q+r+1}$. However $H(\Lambda^p T^* \otimes (g_{q+r})^{n-1}) = 0$ by Lemma 6.8, implying that $w^{(n-1)} = \delta(k)$ for some $k \in \Lambda^{p-1} T^* \otimes (g_{q+r+1})^{n-1}$. This implies that w itself is in the image of δ, implying that $H(\Lambda^p T^* \otimes g_{q+r}) = 0$ for all $r \geq 0$ and p, which is to say, g_q is an involutive symbol. □

It is clear from the proof that grading the spaces according to the ordering $x_n < x_{n-1} < \ldots < x_2 < x_1$ is irrelevant. One can restate the result as follows:

Theorem A5.5 (BIS). *Let $x_{i_n} < x_{i_{n-1}} < \ldots < x_{i_1}$ be an ordering on the variables and define $(g_{q+r+1})^{i_j}$ to be the space $\{w \in g_{q+r+1} \mid \delta_{i_1} w = 0, \ldots, \delta_{i_j} w = 0\}$. If the maps $\delta_{i_j} : (g_{q+r+1})^{i_{j-1}} \to (g_{q+r})^{i_{j-1}}$ (all $r \geq 0$, $i \geq 1$) are surjective, then g_q is an involutive symbol. The ordering may depend on the level of prolongation r.*

Example A5.6 (an involutive system). *Let $X = \mathbb{R}^2$, $\mathcal{E} = X \times \mathbb{R}$ and*

$$\mathcal{R}_2 = \begin{cases} u_{xy} - u_{xx} = 0 \\ u_{yy} - u_{xy} = 0 \end{cases}$$

so that $g_2 = \langle v_{xx} + v_{xy} + v_{yy} \rangle$. Hence

$$\mathcal{R}_3 = \begin{cases} u_{xxy} - u_{xxx} = 0 \\ u_{xyy} - u_{xxy} = 0 \\ u_{yyy} - u_{xyy} = 0 \end{cases}$$

and $g_3 = \langle v_{xxx} + v_{xxy} + v_{xyy} + v_{yyy} \rangle$.

Then $\delta_1(g_3) = g_2$ so δ_1 is surjective, while $(g_3)^1 = 0$, $(g_2)^1 = 0$.

Prolonging,

$$\mathcal{R}_n = \begin{cases} u_{(n-1,1)} - u_{(n,0)} = 0 \\ u_{(n-2,2)} - u_{(n-1,1)} = 0 \\ \vdots \\ u_{(0,n)} - u_{(1,n-1)} = 0 \end{cases}$$

and

$$g_n = \langle \sum_{i,j:\ i+j=n} v_{(i,j)} \rangle.$$

Then $\delta_1 : g_{n+1} \to g_n$ *is surjective while* $(g_n)^1 = 0$, *so that the conditions of Theorem A5.5 are satisfied implying* g_2 *is an involutive symbol. Let*

$$u_{xy} - u_{xx} = f^1$$
$$u_{yy} - u_{xy} = f^2$$

Then using the basis $\langle v_{xxx}, v_{xxy}, v_{xyy}, v_{yyy} \rangle$ *for* $S^3T^* \otimes V(\mathcal{E})$ *and the basis* $\langle f^1_x, f^1_y, f^2_x, f^2_y \rangle$ *for* $S^1T^* \otimes V(\mathcal{E}')$, *the map* τ_1 *has the matrix form*

$$\begin{vmatrix} -1 & 1 & 0 & 0 \\ 0 & -1 & 1 & 0 \\ 0 & -1 & 1 & 0 \\ 0 & 0 & -1 & 1 \end{vmatrix}$$

Then $\tau_1((T^3)^1) = \langle f^2_y \rangle$

$\tau_1(T^3) = \langle f^1_x, f^1_y + f^2_x, f^2_y \rangle$

and $(\tau_1(T^3))^1 = \langle f^2_y \rangle$.

Thus $\tau_1 : (T^3)^1 \to (\tau_1(T^3))^1$ *is surjective.*

This example shows how syzygies (in this case, $f^1_y = f^2_x$*), lowers the dimensions of the spaces* $(\tau_{r+1}(T^{q+r+1}))^i$. *Since*

$$\dim(T^{q+r+1})^{n-1} = \#\textit{unknown functions},$$

and $\dim(S^{r+1}T^* \otimes V(\mathcal{E}'))^{n-1} = \#$*equations in the system, if the system is overdetermined the map* τ_{r+1} *can never be surjective without the presence of degree* 1 *syzygies.*

In this example, a syzygy of the system will be a syzygy of the symbol, but this will not be true in general where an equation has terms of more the one degree.

Example A5.7 (Ex 6.6, Ch 6 revisited). *Recall*

$$g_2 = \langle v_{yz} + v_{xx}, v_{xy}, v_{yy}, v_{zz} + v_{xz} \rangle,$$

$$g_3 = \langle v_{yyz} + v_{xxy}, v_{xyy}, v_{yyy}, \textit{sum of other basis elements} \rangle.$$

In fact, for $2 + r \geq 3$,

$$g_{2+r} = \langle v_{(0,2+r-1,1)} + v_{(2+r-1,1,0)}, v_{(1,2+r-1,0)}, v_{(0,2+r,0)}, \textit{sum of the rest} \rangle$$

Now $\delta_1(g_{2+r+1})$ *misses* $v_{(0,2+r-1,1)} + v_{(2+r-1,1,0)}$, *because differentiating the equation* $u_{(0,2+r-1,1)} - u_{(2+r-1,1,0)} = 0$ *(i.e.* $\left(\frac{\partial}{\partial y}\right)^{2+r-2} (u_{yz} - u_{xx})$*) with respect to* x, *yields an equation which has a term in common with a derivative of the other original equation* $u_{zz} - u_{xz} = 0$. *This causes the basis element of* g_{2+r+1} *containing the terms* $v_{(1,2+r-1,1)}$ *and* $v_{(2+r,1,0)}$, *to not be of the form* $v_{(1,2+r-1,1)} + v_{(2+r,1,0)} +$ *an element of* $\{w \mid \delta_1 w = 0\}$. *For no prolongation is* $\delta_1(g_{2+r+1}) = g_{2+r}$. *However, for* $2 + r \geq 3$, $\delta_2(g_{2+r+1}) = g_{2+r}$ *while* $\{w \mid \delta_2 w = 0\} = \emptyset$. *Hence the conditions for Theorem A5.5 bis are satisfied, and* g_3 *is an involutive symbol.*