# Introduction to Computational Differential Algebra, I

William Sit, City College of New York

October 14 and 28, 2005
First of two lectures as part of Graduate Center Series
For Kolchin Seminar in Differential Algebra, 2005–6

**Abstract**

Under both Ritt and Kolchin, basic differential algebra was developed from a constructive view point and the foundation they built has been advanced and extended to become applicable in symbolic computation. In the first talk, we begin with a study of the division algorithm and how it may be modified and used to perform reductions in polynomial rings, ordinary and then partial differential polynomial rings. The abstract notions of (partial) differential rings, fields, and differential polynomials will be covered and no prerequisite is necessary. We will use examples to illustrate how differential polynomials may be ordered and manipulated algebraically using Euclidean-like division. The goal is to apply the reduction algorithms for ideal membership decisions, when possible, and to "simplify" a given system of algebraic differential equations like reducing the order, degree, and number of unknowns, or breaking the system up into "simpler" systems. We will compare this with the analogous operations on algebraic systems. More formally, we will cover the concepts of term-ordering and ranking, partial reduction and reduction, autoreduced sets, Grobner basis and characteristic sets.

In the second talk, we will discuss methods to compute Grobner basis and characteristic sets and the role they play in computational differential algebra: Are there constructive methods, though not necessarily efficient, to solve basic decidability problems? Each algebraic problem has a differential version simply by adding the word "differential" to appropriate places. The ideal membership problem, "Can we tell if a given (differential) polynomial ideal contains a given (differential) polynomial?" will be revisited. Other questions to be discussed are: Can we tell if a given (differential) polynomial ideal is prime? or radical? Does a (differential) polynomial ideal have a finite basis? How do the algebraic and differential analogs differ?

Both this talk and the October 28 talk will be informal and aimed at beginning graduate students. More rigorous treatment is available from my tutorial paper.

Perhaps the simplest and most familiar algorithm is that of long division.[1]

```
                  7 * * * *
              --------------

* * * ) * 7 * * 7 * *
        * * *
        -----
          * * * 7
            * * *
          -------
              * * *
              * * *
              -----
              * * * *
              * * * 7
              -------
                    7
```

Given two positive numbers $m$ and $n$, we can divide $m$ by $n$ to get a **unique quotient** $q$ and a **unique remainder** $r$ such that

$$m = qn + r, \qquad r < n.$$

We observe that if $r = 0$, then $n \mid m$, in other words, $m$ belongs to the ideal generated by $n$ in the ring $\mathbb{Z}$. **And conversely.** The division algorithm thus provides a **test for ideal membership**. For this test, the quotient is not important. From the equation: $m = qn + r$, we know that if a number $p$ divides $n$, then $p$ will divide $m$ if and only if it divides $r$. **Thus the remainder $r$ is a simplification of $m$ as far as divisibility is concerned.**

[1] In the above division, * denotes a digit not equal to 7. You should be able to recover all the digits. This is a variation of a puzzle taken from *Fun with Figures*, by L. Harwood Clarke, 2nd ed., William Heinemann Ltd, 1956.

What is really required of this algorithm? A brief moment of reflection suggests the following:

1. We need to **represent $m$ in some base $b$** (say 10). This means we actually write $m$ as a polynomial in $b$ with coefficients that are between 0 and $b-1$. In particular, as a linear combination of powers of $b$. And similarly for $n, q$, and $r$.

$$m = m_k b^k + \cdots + m_0$$

$$n = n_\ell b^\ell + \cdots + n_0$$

$$q = q_h b^h + \cdots + q_0$$

$$r = r_g b^g + \cdots + r_0$$

2. Obviously, we need to **order the digits** (terms) in this representation in decreasing powers of the base (by means of place-value).

3. If $n > m$ (**order the numbers**), we simply let $q = 0$ and $r = m$ and stop.

4. Otherwise, we use a **recursive procedure** that begins by

   (a) Deciding the most significant digit $q_h$ of the quotient $q$, including its place-value $h$.

   (b) Multiply $n$ by $q_h b^h$

   (c) Subtract the result in (b) from $m$ to get $m'$

5. Repeat Steps 3 and 4 using $m'$ instead of $m$

6. For divisibility, test $r = 0$ (**Equality test, zero test**)

In short, we need a **data representation**, and perhaps independent of the data representation, an **ordering of the terms** (digits), an **ordering of the numbers**, **equality testing**, **zero-testing**, and a **recursive procedure** to reduce the "size" of dividend $m$. The step (4) above may be called a **reduction step** and $m'$ called the **reductum** of $m$ by $n$.

**What happens if we want to continue to divide $r$ by another divisor?**

Suppose we want to divide 29 by both 15 and 10. We can either divide 29 first by 15, get a remainder 14 and then divide 14 by 10 to get a remainder 4, or we can divide 29 first by 10, get a remainder 9 and then divide by 15 to get a remainder 9. The final remainder is no longer unique and depends on the order in which division is performed. However, in each case:

**If the divisors are $n_1$ and $n_2$, we get *some* quotients $q_1, q_2$ and *some* remainder $r$ such that**

$$m = q_1 n_1 + q_2 n_2 + r$$

**and while $r$ is not unique, we can still say that $m$ is in the ideal generated by $n_1, n_2$ if $r = 0$.**

**What about the converse?**

**What happens if we "mix" the reduction steps?**

Let's divide 3275 by 15 and 10 in two way. First:

1. 3275 = 200*15 + 275
2. 275 = 20*10 + 75
3. 75 = 5*15 + 0

Second:

1. 3275 = 300*10 + 275
2. 275 = 10*15 + 125
3. 125 = 10*10 + 25
4. 25 = 2*10 + 5

Now we get **two different** remainders, **one zero, the other not**. So **the converse is not true**, and **the "mixed" reduction algorithm is not useful for testing ideal membership**: it may miss.

But still, the equation $m = q_1 n_1 + q_2 n_2 + r$ is valid, and a number $p$ that divides both $n_1$ and $n_2$ will divide $m$ if and only if it divides $r$. **So $r$ is still a simplification of $m$ for divisibility.**

**To make the algorithm work, we need to find a specific ordering of all the divisors and a specific order in the reduction steps that would guarantee the converse: if $m$ is in the ideal $(n_1, n_2)$, then the computed remainder must be zero.**

As far as the ideal membership problem goes, we don't really care about $n_1, n_2$. Perhaps we can replace them by another set of generators that will have the uniqneness-of-remainder property. For the ring of integers, this is obtained by using the gcd since $\mathbb{Z}$ is a PID (principal ideal domain). In the example, if we use the single divisor 5 (gcd of 15, 10), the remainder will be zero if and only if $m$ is in the ideal $(10, 15) = (5)$.

It is clear that the division algorithm works equally well (in fact easier) with minor modification in a polynomial ring $K[x]$ in one variable over a field $K$. In **univariate polynomial division**, we want to remove the **leading term** (that is, term with the highest degree in $x$) of the dividend only. We will still obtain a relationship $M(x) = Q(x)N(x) + R(x)$ which will tell us that a zero of $N(x)$ will be a zero of $M(x)$ if and only if it is a zero of $R(x)$. (**Remainder Theorem**)

The rest of this talk simply generalizes the ideas here for polynomial rings and then differential polynomial rings. The methods of **Gröbner basis** and **characteristic set** are two approaches to solve this problem in the polynomial world.

**What happens if the coefficient domain is not a field but just an integral domain?**

Take an example for division in $\mathbb{Z}[x]$. Suppose we divide

$$M = 6x^4 + 4x^2 + 3x$$

by

$$N = 4x^2 + 1.$$

Unlike integer division of 60430 by 401, which gives $60430 = 150 \times 401 + 280$, we cannot divide $4x^2$ into $6x^4$ exactly and we can't use the other lower terms to help either. In a way, this simplifies the algorithm! What we need is to **multiply the dividend** by 4 before dividing. So we have, applying the reduction step twice, the following:

1. $4M = 24x^4 + 16x^2 + 12x$ (**pre-multiplication**)
2. $4M = 6x^2N + (10x^2 + 12x)$ (normal reduction step)
3. $M' = 10x^2 + 12x$ (first pseudo-remainder)
4. $4M' = 40x^2 + 48x$ (pre-multiplication)
5. $4M' = 10N + (48x - 10)$ (normal reduction step)
6. $M'' = 48x - 10$ (second pseudo-remainder)

The entire process is called **pseudo-division**, and each reduction step (steps 1, 2 or steps 4, 5 in the example) is called a **pseudo-reduction**. The final remainder $M''$ is called a **pseudo-remainder**. The coefficient of the leading term of the divisor $N$ (4 in the example) is called the **initial** of $N$.

If the initial of the divisor $N$ is denoted by $I$, then we have

$$I^e M = QN + R$$

where $e$ is some natural number called a **pseudo-exponent**, $Q$ is a **pseudo-quotient** and $R$ is a pseudo-remainder. The pseudo-quotient and pseudo-remainder are of course unique for each fixed pseudo-exponent. We can always choose $e = \max(\deg M - \deg N + 1, 0)$, which need not be minimal (for example, when $M = N$). **A zero of $N$ which does not annihilate its initial will be a zero of $M$ if and only if it is a zero of $R$.**

Note: If $R = 0$, we no longer know that $M \in (N)$, only that $I^e M \in (N)$ for some $e$.

The **saturation ideal** of an ideal $J$ by an element $I$ in a ring is defined as

$$J : I^\infty = \{\, M \mid I^e M \in J \text{ for some e} \in \mathbb{N} \,\}$$

When $J$ is a **principal ideal**, say $J = (N)$, the triple $(e, Q, R)$ is unique for any $M \in (N) : I^\infty$ **when $e$ is minimally chosen**. We have:

$$R = 0 \text{ if and only if } M \in (N) : I^\infty$$

**whether $e$ is minimal or not**.

If you have not noticed already, it is not always necessary to pre-multiply the dividend by the **entire** initial. In the example, it suffices to premultiply $M$ and $M'$ by 2, a factor of the initial. There is a trade-off between extra computation and controlling the **growth of the coefficients** in pseudo-division. For this talk, we do not consider efficiency issues. This subject involves GCD computations and is still under research.

We next look at the algorithm for **multivariate polynomial rings** $K[x_1, \ldots, x_n]$, where $K$ may be a field, or just an integral domain. We can have two different views.

**The first is to view multivariate polynomials as they are.** We need to order monomials. A **term-ordering** is a total ordering of the set of all monomials, or power products, in the variables $x_1, \ldots, x_n$ such that

$$1 < M \text{ for all monomials } M, \text{ and}$$

$$M_1 < M_2 \Longrightarrow x_i M_1 < x_i M_2 \text{ for all monomials } M_1, M_2 \text{ and } 1 \leq i \leq n.$$

This is the **Gröbner basis** approach.

In $K[x, y]$, the monomials look like $x^i y^j$ and we may order two monomials $M_1 = x^{i_1} y^{j_1}$ and $M_2 = x^{i_2} y^{j_2}$ by saying $M_1 < M_2$ if $i_1 < i_2$, or if $i_1 = i_2$ and $j_1 < j_2$. Thus $x^2 y^3 < x^3 y^k$ for any $k$. This is an example of a **purely lexicographic** (or **pure lex** for short) term ordering. A pure lex term-ordering is determined once we have ordered the variables themselves.

So **pure lex with $x > y > z$ in $K[x, y, z]$ means that the exponent for $x$ is compared before the exponent of $y$, which is compared before the exponent of $z$.**

Another term-ordering commonly used is the **degree-lexicographic** ordering, where **deg-lex with** $x > y$ means we first compare the total degree, then the exponent of $x$, followed by the exponent of $y$.

**The second way to view multivariate polynomials is to treat them as univariate polynomials in some main variable with coefficients that are polynomials in the remaining variables.** In practice, we usually rank[2] the indeterminates, and single out one, usually, one with the highest rank, as the main variable. This is the **characteristic set** approach. In this view, there is no need for an explicit term-ordering since the monomials (powers of the main variable) are naturally ordered by degree in the main variable.

[2] Abstractly as orderings on sets, a **ranking** is a generalization of a term-ordering. Here, we need only a linear order (permutation induced) on the indeterminates. In general, we distinguish ranking from term-ordering.

Suppose the coefficient field is $\mathbb{Q}$, the field of rational numbers. **Using pure lex with $x > y$ term-ordering**, we will carry out the reduction steps in the following example.

Say we want to divide $M$ by $N$, where

$$M = \mathbf{5x^3y^2} - 10xy^3 \qquad\qquad N = \mathbf{2x^2y} + x^2 + xy^3.$$

Both $M$ and $N$ are already arranged with their terms in decreasing order with their **leading terms** in blue. In each reduction step, we highlight in red the highest term among those that can be reduced (called the **head term**). **A head term need not be the leading term, and it depends on $N$.**

1. $M = (\frac{5}{2}xy)N + M_1$ where $M_1 = \mathbf{-\frac{5}{2}x^3y} - \frac{5}{2}x^2y^4 - 10xy^3$
2. $M_1 = (-\frac{5}{4}x)N + M_2$ where $M_2 = \frac{5}{4}x^3\mathbf{-\frac{5}{4}x^2y^4} + \frac{5}{4}x^2y^3 - 10xy^3$
3. $M_2 = (-\frac{5}{4}y^3)N + M_3$ where $M_3 = \frac{5}{4}x^3 + \mathbf{\frac{5}{2}x^2y^3} + \frac{5}{4}xy^6 - 10xy^3$
4. $M_3 = (\frac{5}{4}y^2)N + M_4$ where $M_4 = \frac{5}{4}x^3\mathbf{-\frac{5}{4}x^2y^2} + \frac{5}{4}xy^6 - \frac{5}{4}xy^5 - 10xy^3$
5. $M_4 = (-\frac{5}{8}y)N + M_5$ where $M_5 = \frac{5}{4}x^3 + \mathbf{\frac{5}{8}x^2y} + \frac{5}{4}xy^6 - \frac{5}{4}xy^5 + \frac{5}{8}xy^4 - 10xy^3$
6. $M_5 = (-\frac{5}{16})N + M_6$ where $M_6 = \frac{5}{4}x^3 - \frac{5}{16}x^2 + \frac{5}{4}xy^6 - \frac{5}{4}xy^5 + \frac{5}{8}xy^4 - \frac{165}{16}xy^3$

Notice that $M_6$ contains no monomial divisible by the leading monomial of $N$. The sequence of head terms in the remainders $M_1, \ldots, M_6$ is strictly decreasing, which is one of the reasons why the procedure terminates.

**If the coefficient domain $K$ is not a field, say $K = \mathbb{Z}$ instead of $K = \mathbb{Q}$, the division will be replaced by pseudo-division.** In the pure-lex example, $N = \mathbf{2x^2y} + x^2 + xy^3$ and at each step, the pseudo-remainder will be premultiplied by the initial $\mathbf{2}$ whenever needed.

1. $\mathbf{2}M = (5xy)N + M_1$ where $M_1 = \mathbf{-5x^3y} - 5x^2y^4 - 20xy^3$
2. $\mathbf{2}M_1 = (-5x)N + M_2$ where $M_2 = 5x^3\mathbf{-10x^2y^4} + 5x^2y^3 - 40xy^3$
3. $M_2 = (-5y^3)N + M_3$ where $M_3 = 5x^3 + \mathbf{10x^2y^3} + 5xy^6 - 40xy^3$
4. $M_3 = (5y^2)N + M_4$ where $M_4 = 5x^3\mathbf{-5x^2y^2} + 5xy^6 - 5xy^5 - 40xy^3$
5. $\mathbf{2}M_4 = (-5y)N + M_5$ where $M_5 = 10x^3 + \mathbf{5x^2y} + 10xy^6 - 10xy^5 + 5xy^4 - 80xy^3$
6. $\mathbf{2}M_5 = (-5)N + M_6$ where $M_6 = 20x^3 - 5x^2 + 20xy^6 - 20xy^5 + 10xy^4 - 165xy^3$

By dividing $M_6$ by $\mathbf{2}^4$, we can recover the remainder when the coefficient field is $\mathbb{Q}$. Thus it is more efficient to perform pseudo-division over $\mathbb{Z}$ and then put back the necessary denominators. In theory, it is easier to deal with fields, but in computation, it is easier to deal with the underlying integral domain if the field is a quotient field.

**The remainder computed this way depends on the term-ordering.**

Using **deg-lex with $x > y$** (recall this means we first compare the total degree, then the exponent of $x$, followed by the exponent of $y$) to perform the reduction for the same example, we are done in one step.

$$M = \mathbf{5x^3y^2 - 10xy^3}, \qquad N = \mathbf{xy^3} + 2x^2y + x^2.$$

1. $M = (-10)N + M_1$ where $M_1 = 5x^3y^2 + 20x^2y - 10x^2$ (remainder)

Note that in this step, the term (in red) of $M$ that is reduced is not the leading term.

Again $M_1$ **contains no monomial divisible by the leading monomial of** $N$. Such a polynomial is said[3] to be **Gröbner-reduced with respect to** $N$.

**Viewing multivariate polynomials as univariate polynomials in some main variable**:

We may, for example, view $K[x, y]$ as $K[y][x]$, using $x$ as the main variable. In our example,

$$M = 5y^2\mathbf{x^3} - 10y^3\mathbf{x}$$

$$N = (\mathbf{2y + 1})\mathbf{x^2} + y^3\mathbf{x}$$

The initial of $N$ is $\mathbf{2y + 1}$. The reduction is done by pseudo-division since the coefficient domain is now $K[y]$. **The remainder will be of lower degree in the main variable than the divisor**. Such a remainder is said to be **algebraically reduced** with respect to $N$ and its main variable.

1. $(\mathbf{2y + 1})M = (5y^2)\mathbf{x}N + M_1$ where $M_1 = -5y^5\mathbf{x^2} - (20y^4 + 10y^3)\mathbf{x}$
2. $(\mathbf{2y + 1})M_1 = 5y^5N + M_2$ where $M_2 = (5y^8 - 40y^5 - 40y^4 - 10y^3)\mathbf{x}$

[3] In the literature, the term "reduced" is used without any qualifiers and is potentially a source of confusion.

Now we are ready for differential polynomials. We need to recall what differential rings, and differential ideals are, and some notations. Let's do the **ordinary** case first, that is, rings equipped with only one derivation.

A **derivation on a ring** $K$ (**always assumed commutative with unit**) is simply a linear map $\delta : K \longrightarrow K$ satisfying the product rule:

$$\delta(ab) = a\delta(b) + \delta(a)b$$

A ring equipped with a single derivation is called an **ordinary differential ring**. Differentiation is often denoted by the $'$ notation, that is $a' = \delta(a)$. An ideal $J$ of $K$ is a **differential ideal** if $a' \in J$ whenever $a \in J$. **The intersection of an arbitrary family of differential ideals is a differential ideal.** The **differential ideal generated by a set of elements** $a_1, \ldots, a_k$ is denoted by $[a_1, \ldots, a_k]$ and is the smallest differential ideal containing $a_1, \ldots, a_k$.

The **differential polynomial ring** over $K$ in the **differential indeterminates** $y_1, \ldots, y_n$, denoted by $K\{ y_1, \ldots, y_n \}$, is constructed as the polynomial ring over $K$ over a family of (algebraic) indeterminates $\mathbf{y} = \{ y_{i,j} \}_{1 \leq i \leq n, j \in \mathbb{N}}$ and we make $K[\mathbf{y}] = K[\{ y_{i,j} \}]$ into an ordinary differential ring by extending the derivation $\delta$ on $K$:

$$\delta(y_{i,j}) = y_{i,j+1} \text{ for all } i, j.$$

We identify $y_{i,0}$ with $y_i$, and will also write $y_{i,j}$ as $y_i^{(j)}$ or $\delta^j(y_i)$. These are called **derivatives**. Any family of derivatives are algebraically independent over $K$.

An **ordinary differential polynomial** $P$ is just an element of $K\{ y_1, \ldots, y_n \}$. Any such $P$ can involve only finitely many derivatives $v_1, \ldots, v_r$ and hence $P$ lives in a polynomial ring $K[v_1, \ldots, v_r]$ with finitely many algebraic indeterminates. Even after a finite number of algebraic and differentiation operations, the result will still live in a polynomial ring with finitely many algebraic indeterminates.

So we can apply the previously discussed division algorithms to differential polynomials.

Let's see what a differential polynomial $P$ looks like: that depends on what view we take. Whether we treat $P$ as a multivariate polynomial in the derivatives that appear in $P$ or as a univariate polynomial using some derivative that appears in $P$ as the main variable, we need a way to order the derivatives, that is, to **rank** the derivatives.

A **ranking** of the differential indeterminates $y_1, \ldots, y_n$ is a total ordering of the set of derivatives $\mathbf{Y} = \{ y_{i,j} \mid 1 \leq i \leq n, j \in \mathbb{N} \}$ such that

$$v < \delta(v) \text{ for all derivatives } v, \text{ and}$$

$$v_1 < v_2 \Longrightarrow \delta(v_1) < \delta(v_2) \text{ for all derivatives } v_1, v_2.$$

A ranking in particular is a total order on the $n$ disjoint sets

$$\mathbf{Y}_i = \{ y_{i,j} \mid j \in \mathbb{N} \}$$

and when viewed as a relation on the disjoint union of $\mathbf{Y}_i$, it is possible to include some not so intuitive subsets of $\mathbf{Y}_i \times \mathbf{Y}_j$.

The **order** of a derivative $y_{i,j}$ is defined to be the integer $j$. For ordinary differential polynomial rings, a commonly used ranking is an **orderly ranking**, which requires that

$$\text{order}(v_1) < \text{order}(v_2) \Longrightarrow v_1 < v_2.$$

An orderly ranking **for an ordinary differential ring** is completely decided once the order on the differential indeterminates is fixed. In this case, $y_{i,j} < y_{i',j'}$ if either $j < j'$ or if $j = j'$ and $y_i < y_{i'}$. For $n = 2$, we may list the derivatives in order of increasing rank:

$$y_1 < y_2 < y_1' < y_2' < y_1'' < y_2'' < \cdots$$

A different ranking, called an **unmixed ranking**, is obtained by defining $y_{i,j} < y_{i',j'}$ if $i < i'$ or if $i = i'$ and $j < j'$. The unmixed ranking is induced by the lexicographic order on the pairs $(i, j)$. Every derivative of $y_1$ is of lower rank than every derivative of $y_2$. Listed in order of increasing rank for $n = 2$:

$$y_1 < y_1' < y_1'' < \cdots < y_2 < y_2' < y_2'' < \cdots$$

Suppose we have selected a ranking. A differential polynomial is a linear combination (over the coefficient domain $K$) of **differential monomials**, which are monomials in the derivatives. A differential monomial looks like this:

$$M = \prod_{1 \le i \le n, j \in \mathbb{N}} y_{i,j}^{e_{i,j}}$$

where all but a finite number of $e_{i,j} \in \mathbb{N}$ are zero. If $M$ involves only $k$ derivatives, say

$$v_1 = y_{i_1,j_1},\ v_2 = y_{i_2,j_2},\ \ldots,\ v_k = y_{i_k,j_k}$$

where the pairs $(i_\ell, j_\ell)$ are all distinct, then we may write

$$M = v_1^{e_1} \cdots v_k^{e_k} = y_{i_1,j_1}^{e_1} \cdots y_{i_k,j_k}^{e_k} = (\delta^{j_1} y_{i_1})^{e_1} \cdots (\delta^{j_k} y_{i_k})^{e_k}.$$

This multitude of notations provides us the convenience to suppress the amount of details as we please. We can then write a differential polynomial $P$ as simply:

$$P = a_1 M_1 + a_2 M_2 + \cdots a_r M_r \qquad (a_1, \ldots, a_r \in K)$$

if $P$ has $r$ terms, where each $M_t$ is a differential monomial as above, and we can "zoom-in" for the details if we like.

With this multivariate view, we are ready to perform reduction by multivariate division. Or are we?

**We need a term-ordering!** A term-ordering is more complicated to define for a polynomial ring in infinitely many indeterminates, but since any finite set of polynomials live in a polynomial ring with a finite number of indeterminates, that is not too difficult. If we are not concerned with differentiation, we certainly can use any term-ordering that is compatible with the underlying ranking on the derivatives. **Two commonly used ones are the pure-lex and degree-lex term-ordering induced by the ranking.**

Suppose in $K\{\, y_1, y_2 \,\}$, where we rank $y_1$ higher than $y_2$ in an orderly ranking, we want to divide

$$F = 5(y_1')^2(y_2'')^3 - 10(y_1')^3 y_2''$$

by

$$G = (y_1')^3 y_2'' + 2y_1'(y_2'')^2 + (y_2'')^2.$$

If we examine these two differential polynomials more carefully, we will see that they only involve two derivatives: $y_1'$ and $y_2''$ and the rank of $y_2''$ is higher than the rank of $y_1'$ because the ranking is orderly. Now with a simplified notation, using $x$ for $y_2''$ and $y$ for $y_1'$, then we have

$$F = 5x^3y^2 - 10xy^3, \qquad G = xy^3 + 2x^2y + x^2$$

which are exactly the $M$ and $N$ we had before. So you should be convinced that we can carry out the divisions, either using the multivariate view or the univariate view.

**But what if we are not so lucky? what if in $F$, one of the $y_2''$ is actually $y_2'''$?**

**We should be able to differentiate $G$ to reduce $F$!**

So, how does one differentiate a differential polynomial?

The **structure of the derivative of a differential polynomial** $P$ is best understood from the univariate view point. We shall choose the **derivative of the highest rank that appears in** $P$ as the main variable. This derivative is called the **leader** of $P$ and usually denoted by $u_P$. In this view, we can write $P$ as a univariate polynomial in $u_P$ with coefficients in $K[\mathbf{Y}\backslash\{u_P\}]$, that is, the coefficients are differential polynomials not involving $u_P$.

$$P = \mathbf{I_d u_P^d} + I_{d-1}\mathbf{u_P^{d-1}} + \cdots I_1 \mathbf{u_P} + I_0$$

Notice in this representation, all the "coefficients" $I_d, I_{d-1}, \ldots, I_0$ **involve only derivatives of lower rank than** $P$. We call $I_d$ the **initial** of $P$ and denote this by $I_P$.

Applying the product and chain rules, we have

$$\begin{aligned}\delta(P) = P' &= (\mathbf{d} I_d \mathbf{u_P^{d-1}} + (\mathbf{d-1}) I_{d-1}\mathbf{u_P^{d-2}} + \cdots + I_1)\delta\mathbf{u_P} + \\ &\quad \delta(I_d)u_P^d + \delta(I_{d-1})u_P^{d-1} + \cdots + \delta(I_1)u_P + \delta(I_0)\end{aligned}$$

**The leader of** $\delta P$ **is** $\delta u_P$ since $v < u_P \Longrightarrow \delta v < \delta u_P$ for any derivative $v$ that appears in $I_j$. Since $\delta P$ is linear in $\delta u_P$, the initial of $\delta P$ is

$$I_{\delta P} = \mathbf{d} I_d \mathbf{u_P^{d-1}} + (\mathbf{d-1}) I_{d-1}\mathbf{u_P^{d-2}} + \cdots + I_1 = \frac{\partial P}{\partial u_P}.$$

We call this initial the **separant** of $P$ and denote it by $S_P$.

We summarize this property by writing:

$$\delta P = S_P \delta u_P + \text{ terms involving lower derivatives.}$$

Back to the question:

**But what if we are not so lucky? what if in $F$, one of the $y_2''$ is actually $y_2'''$? We should be able to differentiate $G$ to reduce $F$!**

So let's do that. Let

$$F = 5(y_1')^2(\mathbf{y_2'''})^3 - 10(y_1')^3 y_2''$$

Here is the derivative of $G$:

$$\begin{aligned}
G &= (y_1')^3 y_2'' && + 2y_1'(y_2'')^2 && + (y_2'')^2 \\
\delta(G) = G' &= (\mathbf{y_1'})^{\mathbf{3}}\mathbf{y_2'''} + 3(y_1')^2 y_1'' y_2'' && +\mathbf{4y_1'y_2''y_2'''} + 2y_1''(y_2'')^2 && +\mathbf{2y_2''y_2'''} \\
&= ((\mathbf{y_1'})^{\mathbf{3}} + \mathbf{4y_1'y_2''} + \mathbf{2y_2''})\mathbf{y_2'''} + 3(y_1')^2 y_1'' y_2'' + 2y_1''(y_2'')^2 \\
&= S_G\mathbf{y_2'''} + T, \text{ where } T \text{ is a sum of terms involving lower derviatives}
\end{aligned}$$

Now since $G'$ is **linear** in $y_2'''$, instead of the usual pseudo-division of $F$ by $G'$ as univariate polynomials in $u_{G'} = \mathbf{y_2'''}$ (which would result in remainders that do not involve $y_2'''$), we can, equivalently, **eliminate** $u_{G'}$ in $F$ by **substituting**

$$\mathbf{y_2'''} = \frac{\delta(G) - (\mathbf{3(y_1')^2 y_1'' y_2'' + 2y_1''(y_2'')^2})}{\mathbf{(y_1')^3 + 4y_1'y_2'' + 2y_2''}} = \frac{\delta G - \mathbf{T}}{\mathbf{S_G}}$$

and then clearing the denominators. So we have

$$(\mathbf{S_G})^3 F = Q\delta(G) + 5(y_1')^2(\mathbf{-T})^3 - 10(y_1')^3 y_2''(\mathbf{S_G})^3$$

This is simply performing a regular univariate division in $K(\mathbf{Y}\backslash u_{G'})[u_{G'}]$ over a field, and then clearing denominators in the resulting equation $M = QN + R$.

The previous reduction may be called **differential reduction** in contrast to the earlier **algebraic reduction**. The "official" name is **partial reduction**. So we can summarize partial reduction this way.

When working to partially reduce $F$ by $G$, suppose a **proper** derivative of $u_G$ appears in $F$, say $\delta^j u_G$ appears, where $j \geq 1$ is the highest possible. We differentiate $G$ up to that order, obtaining:

$$\begin{aligned} \delta G &= S_G \delta u_G + T_1 \\ \delta^2 G &= S_G \delta^2 u_G + T_2 \\ &\vdots \\ \delta^j G &= S_G \delta^j u_G + T_j \end{aligned}$$

where each $T_\ell$ is a sum of terms involving derivatives that are lower than $\delta^\ell u_G$. We then perform substitutions and clear denominators that are always powers of $S_G$ (equivalently, perform univariate pseudo-divisions of $F$ by $\delta^j G, \delta^{j-1} G, \ldots, \delta G$, in that order). We will get

$$S_G^s F = Q_1 \delta(G) + Q_2 \delta^2(G) + \cdots Q_j \delta^j(G) + \widetilde{F}$$

where $\widetilde{F}$ will not contain any proper derivatives of $u_G$. We call $\widetilde{F}$ the **partial remainder** of $F$ with respect to $G$. **A differential polynomial $P$ is said to be partially reduced with respect to $G$ if $P$ does not contain any proper derivatives of $u_G$.**

Observe that we can continue to (algebraically) reduce $\widetilde{F}$ using unvariate pseudo-division by $G$ so that if the leader $u_G$ of $G$ appears in the remainder, it will be of lower degree than the degree of $u_G$ in $G$. Combining, the complete reduction of $F$ by $G$ results in an equation of the form:

$$I_G^i S_G^s F = Q_0 G + Q_1 \delta(G) + Q_2 \delta^2(G) + \cdots Q_j \delta^j(G) + F_0$$

The remainder $F_0$ has the property that it is both partially reduced and algebraically reduced with respect to $G$. It is called the **Ritt-Kolchin remainder** and is obtained using a specific sequence of reductions as described.

It is fairly straight forward to generalize all the previous algorithms to the partial differential polynomial ring. A **partial differential ring** is a ring $K$ equipped with a number of commuting derivations $\delta_1, \ldots, \delta_m$ (that is, $\delta_i \delta_j a = \delta_j \delta_i a$ for all $i, j$ and all $a \in K$). The set of these specific derivations is denoted by $\Delta$. The **partial differential polynomial ring in the differential indeterminates** $y_1, \ldots, y_n$ is denoted by $K\{ y_1, \ldots, y_n \}$ and is constructed as the polynomial ring in the family $\{ y_{i,\vec{k} \in \mathbb{N}^m} \}$ of (algebraic) indeterminates over $K$, where the given derivations of $K$ are extended by defining:

$$\delta_j y_{i,(k_1,\ldots,k_j,\ldots,k_m)} = y_{i,(k_1,\ldots,k_j+1,\ldots,k_m)} \text{ for all } i, j, k_1, \ldots, k_m$$

We identify $y_{i,(0,\ldots,0)}$ with $y_i$ and write $\theta y_i$ for $y_{i,(k_1,\ldots,k_m)}$ where $\theta = \delta_1^{k_1} \cdots \delta_m^{k_m}$. We call any such $\theta$ a **derivative operator**, and any such $\theta y_i$ a **derivative** of $y_i$. The set of derivative operators is denoted by $\Theta$ and the set of derivatives by $\mathbf{Y}$.

A **ranking** is a total ordering of $\mathbf{Y}$ such that

$$v < \delta v \text{ for all derivatives } v, \text{ and}$$

$$v_1 < v_2 \Longrightarrow \delta(v_1) < \delta(v_2) \text{ for all derivatives } v_1, v_2 \text{ and all } \delta \in \Delta.$$

A ranking in particular is a total order on the union of $n$ disjoint sets

$$\mathbf{Y}_i = \{ y_{i,(k_1,\ldots,k_m)} \mid (k_1, \ldots, k_m) \in \mathbb{N}^m \}$$

When restricted to $\mathbf{Y}_i$ for a fixed $i$, it is equivalent to a term-ordering on the formal polynomial ring $K[\delta_1, \ldots, \delta_m]$ when the derivative $\delta_1^{k_1} \cdots \delta_m^{k_m} y_i$ is identified with the monomial $\delta_1^{k_1} \cdots \delta_m^{k_m}$.

The **order** of a derivative $y_{i,(k_1,\ldots,k_m)}$ is defined to be the sum of the integers $k_j$. A commonly used ranking is an **orderly ranking**, which requires that

$$\text{order}(v_1) < \text{order}(v_2) \Longrightarrow v_1 < v_2.$$

An orderly ranking example is one induced by the lexicographic order on $(k_1 + \cdots + k_m, i, k_1, \ldots, k_{m-1})$.

As for the ordinary case, a **differential monomial** $M$ is a monomial in the derivatives. If $M$ involves only $\ell$ derivatives

$$v_1 = \theta_1 y_{i_1}, \quad v_2 = \theta_2 y_{i_2}, \quad \ldots, \quad v_\ell = \theta_\ell y_{i_\ell}$$

where the pairs $(i_\nu, \theta_\nu)$ are distinct, we may write

$$M = v_1^{e_1} \cdots v_\ell^{e_\ell} = (\theta_1 y_{i_1})^{e_1} \cdots (\theta_\ell y_{i_\ell})^{e_\ell}.$$

A **differential polynomial** is again a linear combination of differential monomials with coefficients in $K$. Any differential polynomial $P$ involves only finitely many derivatives, and the one with the highest rank is called its **leader** and denoted by $u_P$. **initial** and **separant** are defined exactly the same way as the ordinary case and we again have:

$$\delta P = S_P \delta u_P + T, \qquad \text{where } T \text{ is a sum of terms involving lower derivatives}$$

More generally, for any derivative operator $\theta \in \Theta$, we have

$$\theta P = S_P \theta u_P + T, \qquad \text{where } T \text{ is a sum of terms involving lower derivatives}$$

A **term-ordering** can be induced using either pure-lex or degree-lex and be compatible with a given ranking, and hence Gröbner reduction (multivariate view), algebraic reduction (univariate pseudo-division) can be performed as before. For partial reduction, suppose $F$ involves a proper derivative of the leader $u_G$ of $G$, say the derivative is $v = \theta u_G$ where $\theta \neq 1$. Choose $v$ such that it is of highest possible rank. We can then eliminate $v$ from $F$ by the substitution of $v = \frac{\theta G - T}{S_G}$ and then clear denominator. Repeat the same for the pseudo-remainder thus obtained until $F$ is partially reduced.

Again, a complete reduction of a differential polynomial $F$ by another $G$ results in an equation of the form:

$$I_G^i S_G^s F \equiv F_0 \pmod{[G]}$$

We now return to the **ideal membership problem**. Recall (p. 6):

**We need to find a specific ordering of all the divisors and a specific order in the reduction steps that would guarantee the converse: if $m$ is in the ideal $(n_1, n_2)$, then the computed remainder must be zero.**

Just as for integer divisions, for both polynomial and differential polynomial reductions, we are concerned only that if $F$ belongs to an ideal, then its remainder should be zero. The actual divisors used are not important. In the polynomial ring (over a field) case, **a basis G of an ideal $J$ such that every element $F \in J$ is Gröbner-reduced to zero** is called a **Gröbner basis** of $J$. There is an algorithm, called the **Buchberger algorithm**, that, given any basis of $J$, computes a Gröbner basis of $J$, which is always finite. With a Gröbner basis, the remainder obtained by Gröbner reduction is unique and independent of the reduction steps and hence Gröbner reduction provides a test for ideal membership. End of story.

In the differential polynomial ring case, a differential ideal need not be finitely generated. Moreover, because of pseudo-division, even if the differential ideal is finitely generated, say by $A_1, \ldots, A_r$, the Ritt-Kolchin remainder $F_0$ of a differential polynomial $F$ only satisfies the following relation:

$$I_{A_1}^{i_1} \cdots I_{A_r}^{i_r} S_{A_1}^{s_1} \cdots S_{A_r}^{s_r} F \equiv F_0 \pmod{[A_1, \ldots, A_r]}$$

The vanishing of $F_0$ only says that

$$I_{A_1}^{i_1} \cdots I_{A_r}^{i_r} S_{A_1}^{s_1} \cdots S_{A_r}^{s_r} F \in [A_1, \ldots, A_r]$$

or $F \in [A_1, \ldots, A_r] : H^\infty$ where

$$H = I_{A_1} \cdots I_{A_r} S_{A_1} \cdots S_{A_r}$$

which is often known as **the product of initials and separants of $A_1, \ldots, A_r$**. Moreover, we have not yet specified the order of partial reductions steps and algebraic reductions steps when more than one divisor is involved.

It is time to introduce the notion of an **autoreduced set**. Suppose we are given a finite set of polynomials (or differential polynomials) $A_1, \ldots, A_r$. Given a reduction procedure of a polynomial $F$ by another $G$, we have associated with it a notion of **being reduced**.

For **Gröbner reduction**, $F$ is Gröbner reduced with respect to $G$ if $F$ contains no monomials which is a multiple of the leading monomial of $G$ (p. 12).

For **algebraic reduction**, $F$ is algebraically reduced with respect to $G$ if the degree of the main variable in $F$ is lower than that in $G$.

For **partial reduction**, $F$ is partially reduced with respect to $G$ if no proper derivative of the leader of $G$ appears in $F$. Note that being partially reduced is to be algebraically reduced with respect to each derivative $\theta G$ when the main variable is $\theta u_G$ (and hence $\theta u_G$ does not appear at all in $F$, for all $\theta \neq 1$).

For **Ritt-Kolchin reduction**, $F$ is reduced with respect to $G$ if it is both partially reduced and algebraically reduced when the main variable is $u_G$.

A set $A_1, \ldots, A_r$ is (Gröbner, algebraic, partial, or Ritt-Kolchin) **autoreduced** if each $A_i$ is (resp. Gröbner, algebraic, partial, Ritt-Kolchin) reduced with respect to every other $A_j$.

We note that by definition, an empty set is autoreduced and a set consisting of a single polynomial not in $K$ is autoreduced.

Perhaps we should also consider the **numerical reduction** (division): A natural number $m$ is (numerical) reduced with respect to another natural number $n$ if $m < n$. Then a numerical autoreduced set of natural numbers must be a singleton. In fact, given a finite set of natural numbers $n_1, \ldots, n_r$, then the ideal generated by $n_1, \ldots, n_r$ has a unique **autoreduced** subset which is simply the set consisting of only the GCD $n$ of $n_1, \ldots, n_r$, which is obtained by autoreducing the given set (the Euclidean GCD algorithm). Obviously we have $(n) = (n_1, \ldots, n_r)$ and any $m$ in the ideal must have a remainder 0 when divided by $n$ and conversely.

With each type of reduction, we start with some kind of total order $\leq$ on some set $\mathcal{T}$. Indeed, the total order is a well-ordering, and we can define a map that associates to every polynomial (differential polynomial) $F$ that is not in the coefficient domain $K$ an element of $\mathcal{T}$ called the **rank** of $F$. We can then induce a **pre-order**[4] $\preceq$ on all such polynomials by saying that $F \preceq G$ **if** $\operatorname{rank} F \leq \operatorname{rank} G$; and we say in case $F \prec G$ that $F$ **has lower rank than** $G$ or $F$ **is lower than** $G$. Of course, two distinct differential polynomials may have the same rank. We can further extend this preorder to the entire polynomial (differential polynomial) ring by defining every element of the coefficient domain $K$ is lower than every polynomial not in $K$.

For **Gröbner reduction**, we have a term-ordering on the set of monomials, and all term-orderings are well-orderings. We can define the **Gröbner rank** of $F$ to be the leading monomial of $F$, relative to the given term-ordering.

For **algebraic reduction**, we have the well-ordering on $\mathbb{N}$, which may be identified with the set of powers of the main variable. We can define the **algebraic rank** of $F$ to be the degree of the main variable in $F$. For **numerical reduction**, the **numerical rank** of $n$ is $n$ itself.

For **partial reduction**, we have a ranking on the set $\mathbf{Y}$ of all the derivatives, and every ranking is a well-ordering. We can define the **partial rank** of $F$ to be the leader $u_F$ of $F$.

For **Ritt-Kolchin reduction**, we have a total ordering on the set of powers of the derivatives using the lexicographic order on $(v, j)$ after identifying it with $v^j$. This total ordering is a well-ordering. We can define the **Ritt-Kolchin rank** of $F$ to be the pair $(u_F, d_F)$ where $u_F$ is the leader of $F$ and $d_F$ is the degree of $u_F$ in $F$.

**If $F$ is lower than $G$, then $F$ is reduced with respect to $G$ (in all cases).**

**The converse is true only for the algebraic or numerical reduction case.**

[4]Recall that a preorder is defined as a reflexive and transitive relation.

**Every autoreduced set is finite.**

Given two autoreduced sets $\mathbf{A} : A_1, \ldots, A_r$ and $\mathbf{B} : B_1, \ldots, B_s$, and suppose each is arranged in non-decreasing order of rank. Then since the sets are autoreduced, they are actually in increasing order of rank. We can now extend the preorder induced by rank to autoreduced sets as follows:

We say **A has lower rank than B** if either there exists an index $t$, $1 \leq t < \min(r, s)$ such that $\operatorname{rank} A_i = \operatorname{rank} B_i$ for $1 \leq i \leq t$ and $\operatorname{rank} A_{t+1} < \operatorname{rank} B_{t+1}$, or $r > s$ and $\operatorname{rank} A_i = \operatorname{rank} B_i$ for $1 \leq i \leq s$.

**In every non-empty set of autoreduced sets, there exists an autoreduced set of lowest rank.**

**Something to think about:**

Every polynomial ideal $J$ contains a Gröbner-autoreduced subset $G$ of lowest Gröbner rank. Is $G$ a Gröbner basis for $J$, that is, will every $F \in J$ be Gröbner-reduced to zero by $G$?

Every polynomial ideal $J$ contains an algebraic-autoreduced subset $C$ of lowest algebraic rank. What does it mean? Is $C$ an (algebraic) **characteristic set**, that is, will every $F \in J$ be algebraic-reduced to zero by $C$?

Every differential polynomial ideal $J$ contains a partial-autoreduced subset $P$ of lowest partial-rank. What does it mean?

Every proper differential polynomial ideal $J$ contains a Ritt-Kolchin autoreduced subset $\mathbf{A}$ of lowest Ritt-Kolchin rank. It is called a **characteristic set** of $J$. Every element $F \in J$ that is Ritt-Kolchin reduced with respect to $\mathbf{A}$ must be zero and hence every $F \in J$ will be Ritt-Kolchin reduced to zero by $\mathbf{A}$.

Let $\mathfrak{R} = K\{\, y, z \,\}$ be an ordinary differential polynomial ring.

Suppose the **ranking is orderly and satisfies** $z < y$. Let

$$A_1 = y^2 + z, \quad A_2 = y' + y.$$

Then

$$\mathbf{\Gamma}\colon A_1 < A_2$$

is **algebraic autoreduced** as a subset of polynomials in $\mathfrak{S} = K[z, y, y']$ and is of lowest algebraic rank for the ideal $J = (A_1, A_2)$ of $\mathfrak{S}$, which is prime. However, $\mathbf{\Gamma}$ is **not partial autoreduced**, because $A_2$ is not partially reduced with respect to $A_1$.

The differential ideal $\mathfrak{a} = [A_1, A_2]$, while also prime, has a **Ritt-Kolchin characteristic set**

$$\mathbf{A}\colon A_1 < A_3$$

where

$$A_3 = A_1' + 2A_1 - 2yA_2 = z' + 2z.$$

**A has lower Ritt-Kolchin rank than $\mathbf{\Gamma}$.**

We have $\mathfrak{a} = [\mathbf{A}]\colon 2y$ where $2y$ is the product of initials and separants of $\mathbf{A}$. **Thus an algebraic characteristic set of a prime ideal need not be a Ritt-Kolchin characteristic set of the differential ideal it generates**. The ideal $J$, being a subset of $\mathfrak{a}$, is does not contain any non-zero element Ritt-Kolchin reduced with respect to $\mathbf{A}$, but contains $A_2$ which is algebraic-reduced with respect to $\mathbf{A}$ as a polynomial in $K[z, y, z', y']$. Also, $A_3$ is a non-zero differential polynomial which is Ritt-Koclhin reduced with respect to $\mathbf{\Gamma}$.

What's next?

Characteristic sets are used to study prime differential ideals and radical differential ideals. There is a algorithm to compute a characteristic set of a prime differential ideal and then it can be used to test membership in prime differential ideals.

There is also an algorithm to decompose a radical differential ideal into its prime differential components. Thus we can also test membership in radical differential ideals.

These algorithms depend heavily on a property called the Rosenfeld property, which is implied if an autoreduced set is coherent. This property allows one to push problems in differential polynomial algebra to problems in polynomial algebra.

There is the Ritt-Raudenbush Basis Theorem, which states that every radical differential ideal is the smallest radical differential ideal containing a certain finite set of differential polynomials.

There are two theorems on the components of a single differential polynomial. The first concerns the general component of an irreducible differential polynomial, and the second states that each component is the general component of some irreducible differential polynomial.

There are more deep theorems.

There are the Buchberger algorithm and applications of Gröbner basis.

Introduction to Computational Differential Algebra, II

William Sit, City College of New York

October 14 and 28, 2005
Second of two lectures as part of Graduate Center Series
For Kolchin Seminar in Differential Algebra, 2005–6

**Abstract**

Under both Ritt and Kolchin, basic differential algebra was developed from a constructive view point and the foundation they built has been advanced and extended to become applicable in symbolic computation. In the first talk, we begin with a study of the division algorithm and how it may be modified and used to perform reductions in polynomial rings, ordinary and then partial differential polynomial rings. The abstract notions of (partial) differential rings, fields, and differential polynomials will be covered and no prerequisite is necessary. We will use examples to illustrate how differential polynomials may be ordered and manipulated algebraically using Euclidean-like division. The goal is to apply the reduction algorithms for ideal membership decisions, when possible, and to "simplify" a given system of algebraic differential equations like reducing the order, degree, and number of unknowns, or breaking the system up into "simpler" systems. We will compare this with the analogous operations on algebraic systems. More formally, we will cover the concepts of term-ordering and ranking, partial reduction and reduction, autoreduced sets, Grobner basis and characteristic sets.

In the second talk, we will discuss methods to compute Grobner basis and characteristic sets and the role they play in computational differential algebra: Are there constructive methods, though not necessarily efficient, to solve basic decidability problems? Each algebraic problem has a differential version simply by adding the word "differential" to appropriate places. The ideal membership problem, "Can we tell if a given (differential) polynomial ideal contains a given (differential) polynomial?" will be revisited. Other questions to be discussed are: Can we tell if a given (differential) polynomial ideal is prime? or radical? Does a (differential) polynomial ideal have a finite basis? How do the algebraic and differential analogs differ?

Both this talk and the October 28 talk will be informal and aimed at beginning graduate students. More rigorous treatment is available from my tutorial paper.

**Dickson's Lemma**,[5] is a result on the **product order of $\mathbb{N}^m$**. There are many versions. For ease of exposition, given a lattice point $p$ in $\mathbb{N}^m$, let $C_p$ be the translate $p + \mathbb{N}^m$ based at $p$ and we call this the **cone at $p$**. If $q \in C_p$, we also say **$p$ divides $q$** ($p \leq q$ in the product order).

**1. In any infinite sequence of points $p_1, p_2, \ldots$, there is a subsequence $p_{k_1}, p_{k_2}, \ldots$ such that $p_{k_i}$ divides $p_{k_{i+1}}$ ($p_{k_i} \leq p_{k_{i+1}}$).**

**Proof**: If $m = 1$, this is clear. Suppose $m > 1$. Let $p'_1, p'_2, \ldots$ be the sequence obtained by projecting each point to $\mathbb{N}^{m-1}$ by removing the first coordinates. By induction, there is a subsequence $p'_{k_1}, p'_{k_2}, \ldots$ such that $p'_{k_i}$ divides $p'_{k_{i+1}}$ for every $i$. There is a further subsequence of $p_{k_1}, p_{k_2}, \ldots$ that is non-decreasing.

**2. Any union of cones is a finite union of cones.**

**1. implies 2.** Let $P$ be a union of cones. Let $p_1$ be in $P$. If possible, let $p_2$ be an element of $P \backslash C_{p_1}$. In general, if possible, let $p_k$ be an element of the complement in $P$ of the union of the cones at $p_1, \ldots, p_{k-1}$. If this process stops, then $P$ is a finite union of cones. If not, we obtain an infinite sequence where no member is in the union of the cones of earlier members. This contradicts 1. (or 3., 4.)

**3. In any infinite sequence of points $p_1, p_2, \ldots$, there exists a natural number $N \in \mathbb{N}$ such that for all $j > N$, $p_i$ divides $p_j$ for some $i \leq N$.**

**2. implies 3.** Let $P$ be the union of the cones based at $p_k$, $k \geq 1$. Then $P$ is a finite union of cones and hence of cones based at some $p_{j_1}, \ldots, p_{j_s}$. Take $N = \max\{ j_1, \ldots, j_s \}$.

**4. In any infinite sequence of points $p_1, p_2, \ldots$, there exist indices $i < j$ such that $p_i$ divides $p_j$.**

**3. implies 4.** Trivial.

**5. Any sequence of points $p_1, p_2, \ldots$ such that $p_{i+1}$ properly divides $p_i$ ($p_i > p_{i+1}$) for all $i$ is finite. (There are no infinite strictly decreasing sequences: the product order is well-founded.)**

**4. implies 5.** If the sequence were infinite, there would be some $i < j$ such that $p_i$ divides $p_j$, but $p_j$ properly divides $p_i$ by hypothesis.

[5] Cox, Little and O'Shea: Theorem 5 of Chapter 2; Kolchin: Lemma 15 of Chapter 0.

**Any term-ordering of the set of monomials in $m$ algebraic indeterminates is a well-ordering. Any ranking of the set of derivatives Y is a well-ordering.**

**Proof**: A term-ordering respects the product order (that is, if $p \leq q$, then $X^p \leq X^q$ where $X^p$ stands for $x_1^{p_1} \cdots x_m^{p_m}$). Hence a sequence of monomials strictly decreasing with respect to a term-ordering, if infinite, corresponds to an infinite sequence of lattice points, which must have an infinite subsequence, non-decreasing with respect to the product order and hence with respect to the term-ordering, a contradiction.

Similarly for a ranking. Any sequence of derivatives strictly decreasing with respecst to a ranking must be finite because for any differential indeterminate $y_j$, the strictly decreasing subsequence consisting of terms that are derivatives of $y_j$ must be finite.

As corollaries:

**Hilbert Basis Theorem**. Every ideal in $K[x_1, \ldots, x_m]$ is finitely generated.

**Proof**: Fix a term-ordering. The set of Gröbner ranks (leading monomials) of all elements in a polynomial ideal $I$ corresponds to a union $P$ of cones in $\mathbb{N}^m$, which is a finite union of cones. Let the bases of these cones correspond to the Gröbner ranks of $G_1, \ldots, G_s$, with $G_i \in I$. Then $I$ is generated by $G_1, \ldots, G_s$. Indeed, **the $G_i$ form a Gröbner basis**: Let $F \in I$. Performing successive Gröbner reductions yields a relation of the form:

$$F = Q_1 G_1 + \cdots + Q_s G_s + R$$

where $R$ is Gröbner-reduced with respect to every $G_i$. If $R \neq 0$, the Gröbner rank of $R$ would correspond to a point in $P$, which would mean that $R$ is not Gröbner reduced with respect to some $G_i$.

**A linear differential ideal is finitely generated (as a differential ideal).**

**Proof**: Similar, using Ritt-Kolchin reduction (but much simplified) instead of Gröbner reduction.

Let's see how we can expand a given set to an autoreduced set. Let $F_1, \ldots, F_r$ be a given set of polynomials or differential polynomials, as the case may be. If $r = 0$ or $r = 1$, then the set is autoreduced. Suppose $r > 1$. We arrange $F_1, \ldots, F_r$ in order of non-decreasing rank. For simplicity, assume the coefficient domain $K$ is a (differential) field.

For **algebraic reduction** Any two polynomials with different main variables are algebraic autoreduced. If the main variables are the same, we can reduce the one with higher rank (degree) by the one with lower rank using pseudo-division. This is analogous to the Euclidean algorithm for GCD. Let $M$ and $N$ be such a pair among the given polynomials with common main variable $v$. Writing:

$$A_0 = M = I_0 v^{d_0} + \cdots, \qquad A_1 = N = I_1 v^{d_1} + \cdots$$

where $d_1 \leq d_0$, we obtain a pseudo-division triple when we divide $A_0$ by $A_1$:

$$I_1^{e_1} A_0 = Q_1 A_1 + A_2$$

where $A_2 = I_2 v^{d_2} + \cdots$ has the property that $d_2 < d_1$. If $d_2 > 0$, we continue and divide $A_1$ by $A_2$ and so on, yielding a finite sequence $A_0, A_1, A_2, \ldots, A_r$ when $A_r$ no longer involves $v$.

$$I_j^{e_j} A_{j-1} = Q_j A_j + A_{j+1} \qquad (1 \leq j \leq r-1)$$

It is easy to see that $A_j \in (M, N)$ for all $j$. **If** $A_r = 0$, then $A_{r-1} \in (M, N)$, $A_{r-1}$ has lower degree in $v$ than $d_0$, $A_{r-2} \in (A_{r-1}) : I_{r-1}$, but we do not know about $M$ and $N$. **We need to reduce $M, N$ by $A_{r-1}$.**

**If** $A_r \neq 0$, then $A_r$ does not involve $v$, $A_r \in (M, N)$ and the main variable of $A_r$ is lower than $v$. **Again, we need to reduce $M, N$ with respect to $A_r$ with a new main variable.**

From this, we see that **for each variable $v$, there can be at most one polynomial with $v$ as main variable in an autoreduced set. Thus every algebraic autoreduced set is finite.**

**Example**. Let $M = 5y^2\mathbf{x^3} - 10y^3\mathbf{x}$, $N = (\mathbf{2y+1})\mathbf{x^2} + y^3\mathbf{x}$. We have

$$\begin{aligned}(\mathbf{2y+1})^2 M &= (5y^2(2y+1)\mathbf{x} - 5y^5)N + A_2,\\ (\mathbf{5y^8 - 40y^5 - 40y^4 - 10y^3})N &= ((2y+1)\mathbf{x} + y^3)A_2\end{aligned}$$

where $A_2 = (\mathbf{5y^8 - 40y^5 - 40y^4 - 10y^3})\mathbf{x}$.
Note that $N \in (A_2) : (\mathbf{5y^8 - 40y^5 - 40y^4 - 10y^3})^\infty$.
but **also** $M \in (A_2) : (\mathbf{5y^8 - 40y^5 - 40y^4 - 10y^3})^\infty$.
So the singleton set $A_2$ is the lowest autoreduced subset (or **characteristic set**) of $(M, N)$ and

$$(M, N) \subset (A_2) : (\mathbf{5y^8 - 40y^5 - 40y^4 - 10y^3})^\infty.$$

For example, $\mathbf{x} \notin (M, N)$.
**Example**. Let $M = 5y^2\mathbf{x^2} - 10y^3$, $N = (\mathbf{2y+1})\mathbf{x} + y^3$. We now only have

$$(\mathbf{2y+1})^2 M = (5y^2(2y+1)\mathbf{x} - 5y^5)N + A_2$$

where $A_2 = \mathbf{5y}^8 - 40\mathbf{y}^5 - 40\mathbf{y}^4 - 10\mathbf{y}^3$
with a new main variable $y$. Note that since $N$ is reduced with respect to $A_2$, and

$$M \in (N, A_2) : (\mathbf{2y+1})^\infty$$

the set $\{ N, A_2 \}$ forms an autoreduced set and is lowest.

## Buchberger's Algorithm

**Input**: A term ordering, polynomials $A_1, \ldots, A_r$ (assumed not in $K$).
**Output**: A Gröbner basis $G_1, \ldots, G_s$ for the ideal $(A_1, \ldots, A_r)$.

**Step 1** Let $G$ be the set $\{ A_1, \ldots, A_r \}$

**Step 2** Form the set $B$ of all pairs $(A_i, A_j)$, $1 \leq i < j \leq r$

**Step 3** While $B$ is not empty, pick a pair, say $(M, N)$. Delete this from $B$. Let $X_M$ be the Gröbner rank of $M$ and similarly for $X_N$. Compute the LCM $X_{M,N}$ of $X_M, X_N$. Let $c_M$ be the coefficient for $X_M$ in $M$, and similarly let $c_N$ be the coefficient for $X_N$ in $N$. Compute the **$S$-polynomial**

$$S(M,N) = \frac{1}{c_M}\frac{X_{M,N}}{X_M}M - \frac{1}{c_N}\frac{X_{M,N}}{X_N}N.$$

Gröbner reduce $S(M,N)$ by the set $G$. Let the remainder be $R$.

**Step 4** If $R \neq 0$, adjoin the pairs $(F, R)$ for every $F \in G$, and adjoin $R$ to $G$.

**Step 5** Repeat Steps 3 and 4 until $B$ is empty, at which point, $G$ is a Gröbner basis.

**Proof**: First, the algorithm terminates because at each iteration, we add to $G$ possibly an element $R$ whose rank (leading monomial) corresponds to a point in $\mathbb{N}^m$ outside the union of cones based at points corresponding to the ranks of $G$. If the algorithm does not terminate, this produces an infinite sequence of points where each point is not divisible by any of the preceding points. This contradicts Dickson's Lemma.

When the algorithm stops, all $S$-polynomials of pairs in $B$ are reduced to zero.

**Theorem. A set $G_1, \ldots, G_s$ is a Gröbner basis of the ideal it generates if and only if all $S$-polynomials $S(G_i, G_j)$ reduces to 0.**

Let $\mathfrak{R} = K[t,x,y,z]$ and we use the pure lex term ordering with respect to $t > x > y > z$. Let

$$A_1 = \mathbf{xz} + y, \qquad A_2 = \mathbf{x} - yz, \qquad A_3 = \mathbf{tz} - 1.$$

Let $S_{i,j}$ denote $S(A_i, A_j)$ and let $\xrightarrow{A}$ denote a Gröbner reduction by $A$. Then

$$\begin{aligned} S_{1,2} &= A_1 - zA_2 = \mathbf{yz^2} + y =: A_4 \\ S_{2,3} &= tzA_2 - xA_3 = -\mathbf{tyz^2} + x \xrightarrow{A_3} \mathbf{x} - yz \xrightarrow{A_2} 0 \end{aligned}$$

Observe that in general, **if $X_M, X_N$ are relatively prime, then $X_{M,N} = X_M X_N$ and $S(M,N) \xrightarrow{M,N} 0$.**

$$\begin{aligned} S(M,N) &= \frac{1}{c_M} X_N (c_M X_M + T_M) - \frac{1}{c_N} X_M (c_N X_N + T_N) \\ &= \frac{1}{c_M} X_N T_M - \frac{1}{c_N} X_M T_N \\ &\xrightarrow{N} \frac{1}{c_M}(-\frac{1}{c_N} R_N) T_M - \frac{1}{c_N} X_M T_N \\ &\xrightarrow{M} \frac{1}{c_M}(-\frac{1}{c_N} R_N) T_M - \frac{1}{c_N}(-\frac{1}{c_M} R_M) T_N = 0 \end{aligned}$$

$$\begin{aligned} S_{1,3} &= tA_1 - xA_3 = \mathbf{ty} + x \xrightarrow{A_2} \mathbf{ty} + yz =: A_5 \\ S_{1,4} &= yzA_1 - xA_4 = \mathbf{y^2 z} - xy \xrightarrow{A_2} y^2 z - y^z = 0 \\ S_{1,5} &\xrightarrow{A_1, A_5} 0, \quad S_{2,4} \xrightarrow{A_2, A_4} 0, \quad S_{2,5} \xrightarrow{A_2, A_5} 0 \\ S_{3,4} &= yzA_3 - tA_4 = -\mathbf{ty} - yz \xrightarrow{A_5} 0 \\ S_{3,5} &= yA_3 - zA_5 = -\mathbf{yz^2} - y \xrightarrow{A_4} 0 \\ S_{4,5} &= tA_4 - z^2 A_5 = \mathbf{ty} - yz^3 \xrightarrow{A_5} -\mathbf{yz^3} + yz \xrightarrow{A_4} yz - yz = 0 \end{aligned}$$

So $A_1, A_2, A_3, A_4, A_5$ form a Gröbner basis.

Here're **some computational problems from algebraic geometry solvable by Gröbner basis methods**. Let $G_1, \ldots, G_r$, and $F, F_1, F_2$ be polynomials in $\mathfrak{R} = K[x_1, \ldots, x_m]$. Let $J = (G_1, \ldots, G_r)$.

1. **Congruence** Decide if $F_1 \equiv F_2 \pmod{J}$.
2. **Ideal Membership**. Decide if $F$ belongs to the ideal $J$.
3. **Syzygies**. Compute a fundamental set of $r$-tuples of polynomials $A_1, \ldots, A_r$ such that $\sum_{i=1}^{r} A_i G_i = 0$.
4. **Free Resolution**. Compute a finite free resolution of the ideal $J$.
5. **Radical Ideal Membership**. Decide whether $F \in \sqrt{J}$. If the coefficient domain is an algebraically closed field $K$, by the Nullstellensatz, this is equivalent to deciding whether the algebraic set consisting of common zeros of $G_1, \ldots, G_r$ is contained in the hypersurface $F = 0$. This problem reduces to an ideal membership problem whether $1 \in (G_1, \ldots, G_r, Fz - 1)$ for the polynomial ring $K[x_1, \ldots, x_m, z]$. Special case when $F = 1$: decide whether there are any common zeros.
6. **Common zeros**. Decide if the set of common zeros is finite or infinite. If finite, find the polynomial of minimal degree in $J \cap K[x_1]$.
7. **Ideal Intersection**. Given two polynomial ideals $J_1, J_2$ by ideal generators, find a set of generators for $J_1 \cap J_2$. Special case: find the projection ideal $J \cap K[x_1, \ldots, x_s]$ where $1 \leq s \leq m$.
8. **Saturation Ideal** Compute the saturation ideal $J : F^{\infty}$.
9. **Radical Ideal**. Compute a basis for $\sqrt{J}$.
10. **Primary and Prime Decompositions**. Compute a primary decomposition of $J$ and a prime decomposition of $\sqrt{J}$.
11. **Primality Test**. Decide whether $J$ is prime, and if not, find $F_1, F_2$ such that $F_1 F_2 \in J$ but $F_1, F_2 \notin J$.
12. **Radicality Test**. Decide whether $J$ is radical, and if not, find a polynomial $F$ and a natural number $e$ such that $F^e \in J$ but $F \notin J$.
13. **Hypersurface Test**. Decide whether $J$ is a principal ideal or not.

14. **Hilbert Function and Poincare Series** If $G_1, \ldots, G_r$ are homogeneous, compute the Hilbert function

$$H_{\mathfrak{R}/J}(n) = \dim_K(\mathfrak{R}/J)_n$$

which, for sufficiently large $n$, is a polynomial in $n$, and compute the Poincare Series (generating function for $H$)

$$P_{\mathfrak{R}/J}(z) = \sum_n H_{\mathfrak{R}/J}(n) z^n = \frac{Q(z)}{(1-z)^d}$$

where $d$ is the degree of the Hilbert polynomial and $d = \dim J$.

15. **Basis** If $G_1, \ldots, G_r$ are homogeneous, compute a basis of $\mathfrak{R}/J$ as a $K$-vector space and a multiplication table for $\mathfrak{R}/J$.

16. **Canonical Simplifier**. If $F \equiv F_0 \pmod J$, what is the "simpliest" form of $F_0$ and how to compute it?

17. **Solving Congruence**. If $\mathfrak{R}/J$ is finite dimensional, and given $F_1, F_2$, decide if there is an $F$ such that $F_1 F \equiv F_2 \pmod J$ and if yes, find $F$.

18. **Invertibility Test**. Special case of solving a congruence: If $\mathfrak{R}/J$ is finite dimensional, decide whether $F$ is invertible mod $J$. Equivalently, whether $1 \in (G_1, \ldots, G_r, F)$.

19. **Rationalize expressions involving surds**. For example, find the inverse of $x + \sqrt{2} + \sqrt[3]{3^2}$ (as a polynomial in $x$, $\sqrt{2}$, and $\sqrt[3]{3}$).

**The Rosenfeld Property**

An autoreduced set $\mathbf{A}$ of differential polynomials is said to have the **Rosenfeld Property** if every differential polynomial $F$ in the differential ideal $\mathfrak{a} = [\mathbf{A}] : H_{\mathbf{A}}^{\infty}$ that is partially reduced with respect to $\mathbf{A}$ is already in the ideal $J = (\mathbf{A}) : H_{\mathbf{A}}^{\infty}$.

**For A to have the Rosenfeld property, it is sufficient that all differential $S$-polynomials**

$$\Delta(A, A', v) := S_{A'}\theta_A A - S_A \theta_{A'} A' \xrightarrow{\mathbf{A}} 0$$

**whenever $A, A' \in \mathbf{A}$ has a least common derivative $v = \theta_A u_A = \theta_{A'} u_{A'}$**

If $\mathbf{A}$ has the Rosenfeld property, then:

- $\mathfrak{a}$ is prime if and only if $J$ is prime.
- $\mathfrak{a}$ is radical if and only if $J$ is radical.
- $\mathfrak{a}$ has the property that there is no non-zero differential polynomial in $\mathfrak{a}$ that is reduced with respect to $\mathbf{A}$ if and only if $J$ has the property. This property is called the **zero-reduced** property.

**If A has the Rosenfeld property and if $J$ is prime and zero-reduced, then A is a characteristic set of $\mathfrak{a}$ (and $\mathfrak{a}$ is prime). A differential polynomial $F$ belongs to $\mathfrak{a}$ if and only if the Ritt-Kolchin remainder of $F$ with respect to A is zero.**

With the help of the Rosenfeld property, some important properties of the differential ideal $[\mathbf{A}] : H_{\mathbf{A}}^{\infty}$ can be decided by corresponding properties of the ideal $J = (\mathbf{A}) : H_{\mathbf{A}}^{\infty}$ in $\mathfrak{R}\, K\{ y_1, \ldots, y_n \}$. However, we need to place $J$ into a polynomial ring with finitely many indeterminates to use Gröbner base techniques. Fortunately, these properties do not depend on which polynomial ring $J$ lives as long as all the derivatives appearing in $\mathbf{A}$ are there.

**Invertibility of Initials**

Let $\mathbf{A} : A_1 < \cdots < A_r$ be an autoreduced set. Suppose $v_k$ is the leader of $A_k$. Let $V$ be the set of derivatives appearing in $\mathbf{A}$ and consider the polynomial ring $K[V] = \mathfrak{S}_0[v_1, \ldots, v_r]$ where $\mathfrak{S}_0 = K[V \backslash \{ v_1, \ldots, v_r \}]$. Let $\mathfrak{S}_k = \mathfrak{S}_0[v_1, \ldots, v_k]$. For any differential polynomial $F \in \mathfrak{S}_k$, the following are equivalent:

1. $F$ **is invertible modulo** $(A_1, \ldots, A_k) \cdot \mathfrak{S}_k$
2. **There exist** $L \in \mathfrak{S}_0$, $L \neq 0$, **and** $M \in \mathfrak{S}_k$ **such that** $L = MF \bmod (A_1, \ldots, A_k)$.
3. $\mathfrak{S}_0 \cap (A_1, \ldots, A_k, F) \cdot \mathfrak{S}_k \neq (0)$.

By 3., clearly **invertibility is decidable** by using Gröbner basis in $K_0[v_1, \ldots, v_k]$ where $K_0$ is the quotient field of $\mathfrak{S}_0$.

We say $\mathbf{A}$ **has invertible initials** if each initial $I_k$ of $A_k$ is invertible as a polynomial in $\mathfrak{S}_{k-1}$. If $r = 1$, then $I_1$ is always invertible. If $\mathbf{A}$ has invertible initials, then we have a number of nice properties:

- $\mathfrak{S}_k \cdot (A_1, \ldots, A_k) \cap \mathfrak{S}_0 = (0)$.
- $K_0[v_1, \ldots, v_r]/(\mathbf{A})$ **is a non-trivial finite dimensional vector space over** $K_0$.
- $F$ **is invertible if and only if** $F \notin (\mathbf{A})$ **and** $F$ **is not a zero-divisor modulo** $(\mathbf{A})$.

These properties provide a linear algebra method to test invertibility of $F$ and if $F$ is not invertible, we can compute a $G \in \mathfrak{S}_r$ such that $G$ is algebraically reduced with respect to $\mathbf{A}$ and $GF \in (\mathbf{A})$ but $G \notin (\mathbf{A})$.

**Algorithm $\mathcal{A}(W)$**

**Input:** A differential polynomial ring $\mathfrak{R} = K\{ y_1, \ldots, y_n \}$ with a ranking on $\mathbf{Y}$ and a non-empty finite set $W \subset \mathfrak{R}$

**Output:** A finite, possibly empty, set $\mathcal{A} = \mathcal{A}(W)$ of autoreduced sets of $\mathfrak{R}$ such that for each $\mathbf{A} \in \mathcal{A}$, $\mathfrak{q}_{\mathbf{A}} = [\mathbf{A}]\colon H_{\mathbf{A}}^{\infty}$ is prime with characteristic set $\mathbf{A}$, and $\{ W \} = \cap_{\mathbf{A} \in \mathcal{A}}\ \mathfrak{q}_{\mathbf{A}}$.

[Step 1: ] **If $W$ contains a non-zero element of $K$, Return $\emptyset$.**

Ignore the case when the radical differential ideal is the unit ideal.

[Step 2: ] **$\mathbf{A}$ := autoreduced subset of $W$ of lowest rank**

A brute force way would be to form all subsets of $W$ and verify if any is autoreduced. Among those that are, pick the one with lowest rank.

[Step 3: ] **For all $F \in W, F \notin \mathbf{A}$ do**

[Step 3a: ] $F_0$ := **Ritt-Kolchin remainder of $F$ with respect to $\mathbf{A}$**

[Step 3b: ] **If $F_0 \neq 0$, Return $\mathcal{A}(W + F_0)$.**[6]

Adjoin $F_0$ to $W$ if we get a lower rank differential polynomial and start over. If all other elements of $W$ are reduced to zero, we have $W \subset [\mathbf{A}] : H_{\mathbf{A}}^{\infty}$.

[6] Here, $W + F_0$ means $F_0$ is adjoined to $W$.

[Step 4: ] **For all $A, A' \in \mathbf{A}$ do**

[Step 4a: ] **If $u_A, u_{A'}$ has a least common derivative $v = \theta_A u_A = \theta_{A'} u_{A'}$**

[Step 4a.1: ] $F := \Delta(A, A', v) = S_{A'}\theta_A A - S_A \theta_{A'} A'$

This is the differential version of the $S$-polynomial. It has a rank strictly lower than $v$. We are checking coherence here.

[Step 4a.2: ] $F_0 :=$ **Ritt-Kolchin remainder of** $F$

[Step 4a.3: ] **If $F_0 \neq 0$, Return $\mathcal{A}(W + F_0)$.**

Again, if we get something of lower rank and reduced, adjoin it and start over. Otherwise, **A** is coherent.

[Step 5: ] **Sort $\mathbf{A}$: $A_1 < \ldots < A_p$ by rank.**
**$V :=$ the set of derivatives $\theta y_j$ appearing in $\mathbf{A}$**
**$\mathcal{S}_0 := K[V \backslash \{ v_1, \ldots, v_p \}]$, where $v_k$ is leader of $A_k$**

We are now in a finite polynomial ring. All the differential algebra is done. All differential polynomials are partially reduced with respect to $\mathbf{A}$ by the choice of $V$ since $\mathbf{A}$ is autoreduced.

[Step 5a: ] **For $k = 2, \ldots, p$ do**

[Step 5a.1: ] **If the initial $I_k$ of $A_k$ is not invertible with respect to $\mathbf{A}_{k-1} : A_1 < \cdots < A_{k-1}$,**

[Step 5a.1.1: ] **find a non-zero $G_k \in \mathcal{S}_0[v_1, \ldots, v_{k-1}]$, $G_k \notin (\mathbf{A}_{k-1})$,**
**$G_k$ reduced with respect to $\mathbf{A}_{k-1}$ and $G_k I_k \in (\mathbf{A}_{k-1})$**

[Step 5a.1.2: ] **Return $\mathcal{A}(W + I_k) \cup \mathcal{A}(W + G_k)$.**

If the initials are not invertible, we split because something in the ideal factors. We can test invertibility using linear algebra or Gröbner basis. The linear algebra method provides $G_k$ when the answer is negative.

[Step 6: ] **Let $I := \prod_{k=1}^{p} I_k$ and $J_I^V := (\mathbf{A}) : I^\infty$ (compute a Gröbner basis of $J_I^V$)**

[Step 6a: ] **If $J_I^V = (1)$, Return the union of $\mathcal{A}(W + I_k)$ for all $1 \leq k \leq p$.**

If $J_I^V$ is the unit ideal, then some power of $I$ belongs to $(W)$ and we need to split again.

[Step 6b: ] **If $J_I^V$ is not prime**

[Step 6b.1: ] **Find non-zero $F, F' \in \mathcal{S}_0[v_1, \ldots, v_p]$ such that $FF' \in J_I^V$, $F, F' \notin J_I^V$**

This is also effective by Gröbner basis method since we can compute a Gröbner basis for the radical ideal $\sqrt{J_I^V}$ and test if $\sqrt{J_I^V} \subset J_I^V$ to see if $J_I^V$ is radical. If yes, a prime decomposition can be computed to see if it is prime. If there are more than one component, we can use ideal membership tests to find the $F, F'$.

[Step 6b.2: ] $F_0 :=$ **Ritt-Kolchin remainder of $F$**

[Step 6b.3: ] $F_0' :=$ **Ritt-Kolchin remainder of $F'$**

[Step 6b.4: ] **Return the union of $\mathcal{A}(W + I_k)$ for all $1 \leq k \leq p$, and $\mathcal{A}(W + F_0)$, $\mathcal{A}(W + F_0')$.**

If the ideal is not prime, we need to split and start over.

[Step 7: ] **If $S := \prod_{k=1}^{p} S_k \in J_I^V$**

[Step 7a: ] **Return the union of $\mathcal{A}(W + I_k)$ and $\mathcal{A}(W + S_k)$ for all $1 \leq k \leq p$.**

If $S \in J_I^V$, then since $J_I^V$ is prime, it means some factor of $S$ is in $J_I^V$ and since separants are lower, we need to split and start over. Alternatively, $S \in J_I^V$ means $SI \in (W)$.

[Step 8: ] **Return the union of $\mathcal{A}(W + I_k)$ and $\mathcal{A}(W + S_k)$ for all $1 \leq k \leq p$, and the set with the singleton A.**

Now $\mathbf{A}$ is a characteristic set of for $[\mathbf{A}] : H_{\mathbf{A}}^{\infty} = \{ W \} : H_{\mathbf{A}}$. This is related to the radical differential ideal $\{ W \}$ by the equation:

$$\{ W \} = \{ W \} : H_{\mathbf{A}} \cap \{ W + H \}$$

We found one prime and the others can be found by repeating the procedure on $W$ with $H_{\mathbf{A}}$ adjoined.