

Chapter 7

Techniques of symbolic computation via Gröbner bases

7.1 Solving systems of polynomial equations

The critical point equations, (9.4) and (9.5) below, are algebraic equations whose solution is one step in the process of producing asymptotics for $a_{\mathbf{r}}$. Even when F is rational, these algebraic points are specified only as common solutions to sets of polynomial equations, so what does it mean to “find” them? One could at this point include a discussion of numerical methods. I am not an expert in these, and besides, there is a different point to be made here. The point $\mathbf{z}(\mathbf{r})$ determines the exponential growth rate, but computations of the exact leading term require further computations for which $\mathbf{z}(\mathbf{r})$ is an input. It is good practice to maintain analytic forms for the inputs through as much of the computation as possible in order to take advantage of algebraic simplifications. (This can be especially important when taking large powers of algebraic numbers less than 1.) Even if one is content to remain at the level of exponential growth rates, it would be desirable to maintain analytic expressions such as $\mathbf{z}(\mathbf{r})$ in order to do calculus on them.

As algebraic geometers have long known, the best way to keep track of algebraic numbers is via the ideals of polynomials that annihilate them. In the last twenty years, a field of computational algebra has burgeoned, providing algorithms for manipulating these ideals and settling questions such as ideal membership and equality of ideals. During the latter part of this period, these results have been implemented, so that packages for manipulating polynomial ideals are now available in many different computing platforms. The present section is devoted to explaining how to use these in the context of computing multivariate asymptotics for the coefficients of rational generating functions. The computations are only truly effective if the coefficients are finitely specificiable. Thus the remainder of this section will work over $\mathbb{Q}[\mathbf{z}]$ instead of $\mathbb{C}[\mathbf{z}]$, though most of the theory is equally valid over any field of characteristic zero.

I have concentrated on the platform with which I am most familiar, namely Maple (version 11.0). The Gröbner basis package must be loaded with the command `with(Groebner)`. I gather that serious computational algebraists use more powerful packages such as Singular and Macaulay, but Maple has a more friendly user interface and is more versatile and widespread. Those who get in so deeply that they need greater power can consult up to date references such as <http://www.google.com>. The remainder of this section explains term orders, Gröbner bases, and their use in computations over zero-dimensional ideals. The exposition somewhat follows [CLO98, Chapter 1].

Term orders

The univariate polynomial division algorithm for $p(z)/q(z)$ produces a quotient and a remainder: $p = aq + r$. The remainder, r , always has degree less than the degree of q . This works because one can divide the leading term of q into the leading term of p so as to find a multiple of q whose subtraction will cancel the leading term, and this may be continued until the leading term of the remainder is so small that it is not divisible by the leading term of q .

To duplicate this feat in several variables, one needs to extend the natural partial order on monomials to a total order. The extension must be compatible with multiplication and there must be no infinite descents. Thus we define

Definition 7.1. *A monomial ordering on $\mathbb{Q}[\mathbf{z}]$ is any relation $>$ on the set of monomials \mathbf{z}^α satisfying:*

- (i) $>$ is a total ordering
- (ii) $>$ is a well ordering
- (iii) if $\alpha, \beta, \gamma \in (\mathbb{Z}^+)^d$ and $\mathbf{z}^\alpha > \mathbf{z}^\beta$ then $\mathbf{z}^{\alpha+\gamma} > \mathbf{z}^{\beta+\gamma}$.

One common term order is the **lexicographic** term order, where $\mathbf{z}^\alpha > \mathbf{z}^\beta$ if and only if for some $j \leq d$, $\alpha_j > \beta_j$ while $\alpha_i = \beta_i$ for all $i < j$. Another is the total degree order, in which $\alpha > \beta$ if and only if either the degree of α is greater than the degree of β or the degrees are equal and $\alpha > \beta$ in the lexicographic order.

Definition 7.2. *Let $>$ be any monomial order. For $f \in \mathbb{Q}[\mathbf{z}]$, let $\text{LT}(f)$ denote the leading term of f with respect to the order $>$.*

Monomial orders do what they were intended to do: given a polynomial p , a set of polynomials $[q_1, \dots, q_k]$ and monomial order $>$, there is an algorithm to produce a representation $p = \sum a_i q_i + r$ with $\text{LT}(r)$ not divisible by any $\text{LT}(q_i)$. One such algorithm is implemented in Maple as `normalf(p, [q1, ..., qk], order)`, where `order` is an order such as `plex[x,y]` or `tdeg[y,z,x]` from a list of implemented monomial orders.

Gröbner bases

Let I be an ideal in $\mathbb{Q}[\mathbf{z}]$ and let $>$ be a monomial order.

Definition 7.3. A **Gröbner basis** for the ideal I with respect to the monomial order $>$ is a basis $\{g_1, \dots, g_k\}$ for I with the property that for any nonzero $f \in I$, $\text{LT}(f)$ is divisible by $\text{LT}(g_i)$ for some i . The basis is called **reduced** if no monomial of g_i is divisible by $\text{LT}(g_j)$ for any distinct i, j .

It turns out that reduced Gröbner bases are unique (see [CLO92, Proposition 6 of 2.7]), they are algorithmically computable, and they have been implemented in Maple as well via the command `Basis([p1, ..., pk], order)`.

The choice of monomial order has effects on computation time that are not fully understood. It also has important effects on the composition of the resulting Gröbner basis. The following proposition gives an example of this.

Proposition 7.4. Let I be an ideal in $\mathbb{Q}[\mathbf{z}]$. The following conditions are equivalent.

- (i) The set $V(I)$ of common solutions to all polynomials in I is a finite subset of \mathbb{C}^d .
- (ii) $\mathbb{C}[\mathbf{z}]/I$ is a finite dimensional vector space over \mathbb{C} .
- (iii) Given a monomial order, there are finitely many monomials not divisible by a leading term of the Gröbner basis for I .

Furthermore, if these conditions are met, then there is a univariate polynomial in I whose roots are precisely the values of z_d of the last coordinates of the roots \mathbf{z} of I .

PROOF: Assume (i). Let S be the set of last coordinates of points in $V(I)$ and let $f = \prod_{a \in S} (z_d - a)$ be the univariate polynomial vanishing precisely at points of S . Then f vanishes on I so by Hilbert's Nullstellensatz, some power of f is in the ideal generated over \mathbb{C} by I . Using the lexicographic Gröbner basis, \mathcal{B} over \mathbb{C} , this means some power of z_d is divisible by the leading term of some element of \mathcal{B} , hence \mathcal{B} contains a polynomial in z_d alone. But the question as to whether g is in the span of all products of elements of I up to degree N is a question of linear algebra in the coefficients, so if the answer for some N is “yes” over \mathbb{C} then it is “yes” over \mathbb{Q} . Therefore some power of f is in $\mathbb{Q}[z_d]$, and taking the radical derives the final conclusion of the proposition from (i).

For each $z_j, 1 \leq j \leq d$, the same argument shows that some power of z_j is a leading term of an element of \mathcal{B} , although for $j < d$ it does not follow that \mathcal{B} contains a polynomial in z_j alone. This is, however, good enough to imply (iii), which implies (ii): the dimension of the vector space $\mathbb{C}[\mathbf{z}]/I$ is equal to the number of such monomials and in fact these are a basis for $\mathbb{C}[\mathbf{z}]/I$ over \mathbb{C} .

Finally, to show that (ii) implies (i), consider the set T_j of monomials $\{z_j^k : k = 0, 1, 2, \dots\}$. By (ii), these are linearly dependent in $\mathbb{C}[\mathbf{z}]/I$, hence some finite linear combination vanishes in $\mathbb{C}[\mathbf{z}]/I$, or equivalently, there is a polynomial $g_j(z_j) \in I$. Then g_j annihilates the j^{th} coordinate of

every $\mathbf{z} \in V(I)$, hence the number of possible values for the j^{th} coordinate of a point of $V(I)$ is at most $\deg(g_j)$ for each j , and there are at most $\prod_j \deg(g_j)$ points in $V(I)$. \square

The lexicographic basis, while not in practice very computationally efficient, has the property that it contains a polynomial $f \in \mathbb{Q}[z_d]$ whenever I is zero-dimensional. We call f the **elimination polynomial** for z_d .

Computing modulo a zero-dimensional ideal: elimination method

A computation we will need to do again and again is to compute an algebraic function of a quantity \mathbf{x} which is itself algebraic. To see what is involved, let us consider a simple univariate example.

Example 7.5 (algebraic function of an algebraic number). Suppose x is a root of the polynomial

$$P(x) := x^3 - x^2 + 11x - 2 = 0$$

and we need to compute $g(x) := x^5/(120x^4 - 1)$. Because x is the root of a cubic, we could solve for radicals. Not only is this messy, but when plugging into g , the resulting expression would be simplified by Maple only to N/D where

$$N = - \left(\left(172 + 36\sqrt{1641} \right)^{2/3} - 128 - 2\sqrt[3]{172 + 36\sqrt{1641}} \right)^5$$

and

$$\begin{aligned} D = & 15552\sqrt[3]{172 + 36\sqrt{1641}} \left(-1778217 \left(172 + 36\sqrt{1641} \right)^{2/3} \right. \\ & + 40749 \left(172 + 36\sqrt{1641} \right)^{2/3} \sqrt{1641} - 284577144 \\ & \left. - 6707112\sqrt{1641} + 5144692\sqrt[3]{172 + 36\sqrt{1641}} + 1076796\sqrt[3]{172 + 36\sqrt{1641}}\sqrt{1641} \right). \end{aligned}$$

This is far from the simplest expression for this quantity. Also it evaluates in Maple to 0.1935445... which is off in the sixth place.

We do much better if we realize that $y := g(x)$ must itself be algebraic. In fact, the pair (x, y) solves the system $\{P(x) = 0, (867x^4 - 1)y - x^5 = 0\}$. The command

```
Basis ([P , y*(867 *x^4 - 1) - x^5], plex(x,y));
```

produces a basis whose first element is the elimination polynomial

$$\theta(y) := 11454803y^3 - 2227774y^2 + 2251y - 32. \quad (7.1)$$

This expresses y as the root of a cubic. Solving this in floating point will now be accurate to more than six places. It can also be expressed as the simpler radical:

$$\frac{1}{393637535306427} \sqrt[3]{A + B\sqrt{C}} + \frac{4885622710417}{3} \frac{1}{\sqrt[3]{A + B\sqrt{C}}} + \frac{2227774}{34364409}$$

where A, B and C are integers of many digits each.

More generally, now, let us suppose that the vector \mathbf{x} is the solution to $\{p_1(\mathbf{x}, \mathbf{z}) = \cdots = p_d(\mathbf{x}, \mathbf{z}) = 0\}$, where \mathbf{z} is a vector of parameters and the ideal $J := \langle p_1, \dots, p_d \rangle$ is zero-dimensional over the ring $\mathbb{C}(\mathbf{z})[\mathbf{x}]$ of polynomials in \mathbf{x} whose coefficients are rational functions of the parameters \mathbf{z} . We wish to compute a general algebraic function $A(\mathbf{x})$. In the simple example we had a rational function $y(\mathbf{x}) = Q(x)/R(x)$, resulting in the polynomial equation $R(x)y - Q(x) = 0$; in the general case we will simply have an implicit polynomial relation $Q(A, \mathbf{x}) = 0$ for some polynomial $Q \in \mathbb{C}[s, x_1, \dots, x_d]$. Since \mathbf{x} may be a multi-valued function of \mathbf{z} and A may be a multivalued function of \mathbf{x} , the best we can hope for algebraically is to find the minimal polynomial for $A(\mathbf{x})$ in terms of the parameters \mathbf{z} . The solution to this will be a collection of algebraic conjugates, from among which one must choose based on specified choices of branches for \mathbf{x} and A .

At this level, the computation is very short: the ideal $J \cup \{A\}$ has solutions $\{(x_1, \dots, x_d, A(\mathbf{x}))\}$ as \mathbf{x} varies over solutions to J .

Example 7.6 (multivariate). Suppose that (x, y) solves the equations $rx + r^2xy + sy^2 - rsx = 0 = sx - ry$. Let $A(x, y)$ solve $A = xA^2 + y$. The the Maple code

```
p1 := x*r + x*y*r^2 + y^2*s - x*r*s;
p2 := x*s - y*r;
Q := x*A^2 - A + y;
Basis([p1, p2, Q], plex(x,y,A));
```

produces a basis whose first element is the elimination polynomial

$$-A^3r^3 + A^3r^3s - A^2s^3 - A^2r^3s - r^2sA + s^2r^2A.$$

This expresses A in the minimal way as an algebraic function of r and s .

While this is straightforward, we have sometimes had trouble getting the computation to halt. The in-principle complexity of a Gröbner basis computation is doubly exponential, and while in practice it is usually much faster, the run times can be unpredictable. The following alternative method in the case where A is a rational function is guaranteed to take only polynomial time once a Gröbner basis for J has been computed.

Matrix method

Let J be a zero-dimensional ideal and Q be a polynomial. We return to the problem of computing $P(\mathbf{z})/Q(\mathbf{z})$ where $\mathbf{z} \in V(J)$ is a solution to J and P and Q are polynomials. Since \mathbf{z} is algebraic,

so is $P(\mathbf{z})/Q(\mathbf{z})$, therefore there are polynomials in $\mathbb{Q}[\mathbf{z}]$ that annihilate $P(\mathbf{z})/Q(\mathbf{z})$ and we take the computation of such a polynomial to be the goal. Note that this will not distinguish for which \mathbf{z} the quantity $P(\mathbf{z})/Q(\mathbf{z})$ has been computed - for irreducible varieties, these are all algebraically conjugate and satisfy the same polynomials.

Pick a Gröbner basis \mathcal{B} and enumerate the monomials not divisible by a leading term of any member of the basis. This results in a list $A := \{\mathbf{z}^{\mathbf{r}} : \mathbf{r} \in \mathcal{A}\}$ for some set \mathcal{A} whose cardinality is the complex vector space dimension of $\mathbb{C}[\mathbf{z}]/J$. If $\mathbf{r}, \mathbf{s} \in \mathcal{A}$ then either $\mathbf{r} + \mathbf{s} \in \mathcal{A}$ or else $\mathbf{z}^{\mathbf{r}+\mathbf{s}}$ may be reduced, via the Maple command `normalf(zr+s, B, order)` to a linear combination of elements of A . In other words, the vector space W spanned by A over \mathbb{C} has an algebra structure and we know how to determine coefficients $\{c_{\mathbf{n},\mathbf{m}} : \mathbf{n} \in (\mathbb{Z}^d), \mathbf{m} \in A\}$ with $c_{\mathbf{n},\mathbf{m}} = \delta_{\mathbf{n},\mathbf{m}}$ when $\mathbf{n} \in A$ and such that

$$\mathbf{z}^{\mathbf{r}} \cdot \mathbf{z}^{\mathbf{s}} = \sum_{\mathbf{m} \in A} c_{\mathbf{r}+\mathbf{s},\mathbf{m}} \mathbf{z}^{\mathbf{m}}.$$

A matrix representation for this algebra (in terms of multiplication on the right) is obtained by mapping each $\mathbf{z}^{\mathbf{r}}$ to the operator of multiplication by $\mathbf{z}^{\mathbf{r}}$. Thus $\mathbf{z}^{\mathbf{r}}$ maps to $M(\mathbf{r})$ where $M(\mathbf{r})$ is a square matrix indexed by \mathcal{A} and

$$M(\mathbf{r})_{\mathbf{s},\mathbf{m}} := c_{\mathbf{r}+\mathbf{s},\mathbf{m}}$$

is the coefficient of $\mathbf{z}^{\mathbf{m}}$ in $\mathbf{z}^{\mathbf{r}+\mathbf{s}}$.

Once we compute $M(\mathbf{r})$ for each $\mathbf{r} \in A$, we may add, subtract and multiply these matrices to obtain a matrix for multiplication by any polynomial $P(\mathbf{z})$. Furthermore, we may invert a matrix $M(Q(\mathbf{z}))$ to obtain a matrix representing division by $Q(\mathbf{z})$. Thus the matrix $M := M(P(\mathbf{z})) [M(Q(\mathbf{z}))]^{-1}$ represents multiplication by $P(\mathbf{z})/Q(\mathbf{z})$ where $\mathbf{z} \in V(J)$. Let L be any univariate polynomial. Then $L(P(\mathbf{z})/Q(\mathbf{z})) = 0$ for all $\mathbf{z} \in V(J)$ if and only if $L(M)$ is the zero matrix. The minimal polynomial satisfied by $P(\mathbf{z})/Q(\mathbf{z})$ for all $\mathbf{z} \in V(J)$ is the minimal polynomial for M , which may be computed by Maple's `minpoly` command. If $V(J)$ is irreducible, this is the minimal polynomial for each $P(\mathbf{z})/Q(\mathbf{z})$. If $V(J)$ is not irreducible then of course to get the minimal polynomial for a particular $P(\mathbf{z})/Q(\mathbf{z})$ one must specify a component of $V(J)$.

Example 7.5 continued: The monomials $\{1, x, x^2\}$ form a basis for $\mathbb{C}[x]/P$. Multiplication by x is a matrix already in rational canonical form:

$$M(x) = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 2 & -11 & 1 \end{bmatrix}.$$

The matrix representing $y = g(x)$ is given by $T := M^5 / (120M^4 - I)$. The Maple code

```
MinimalPolynomial(T,y);
```

then returns the polynomial $\theta(y)$ from (7.1).

7.2 Examples of Gröbner basis computation

It will be more interesting to do examples later once we have more complicated formulæ such as Theorem 10.17 which estimates $a_{\mathbf{r}}$ up to a factor of $(1 + o(1))$ in the “smooth point” case, where the geometry of $\{H = 0\}$ is the simplest (here H is the denominator of a rational generating function of interest). For now, however, there is plenty we can learn about computing the locations of the critical points themselves. Let \mathcal{V} denote the set $\{H = 0\}$. Peeking ahead to Section 9.3, we find that smooth critical points (those where ∇H does not vanish) are given by the equations $H = 0$ along with $\nabla H \parallel \mathbf{r}$. Here, the positive real vector parameter \mathbf{r} matters only up to scalar multiples and represents the direction of indices in which asymptotics are desired. The equation $\nabla H \parallel \mathbf{r}$ is really $d - 1$ independent equations $r_1 \partial H / \partial x_j = r_j \partial H / \partial x_1$ for $2 \leq j \leq d$.

When $H = \prod_{j=1}^k H_j$ is a product of square free factors whose varieties intersect transversely at \mathbf{x} , we call \mathbf{x} an **arrangement point**. If all points of \mathcal{V} are arrangement points, then the critical point equations are $H(\mathbf{x}) = 0$ along with the requirement that \mathbf{r} be in the span of $\{\nabla H_j(\mathbf{x})\}$ where j runs over only those values for which $H_j(\mathbf{x}) = 0$. [Check that this reduces to the stated equations in the case $k = 1$ of smooth points!] A quick dimension check shows that on each stratum of \mathcal{V} (a stratum being determined by the subset of functions H_j that vanish), we expect a zero-dimensional set of solutions.

Let us consider an illuminating special case. Suppose that $H = H_1 H_2$. When looking for smooth critical points, should we look separately on the components H_j or should we forge ahead with the critical point equations (9.4)? Observe that where H_1 vanishes, the gradient of H

$$\nabla H = H_1 \nabla H_2 + H_2 \nabla H_1 = H_2 \nabla H_1$$

is parallel to the gradient of H_1 . Theoretically, therefore, it does not make a difference. Computationally, however, removing the extraneous factor of H_2 can only speed up the computation of smooth critical points on H_1 . Thus it is better, though not necessary, to recognize when H factors.

Example 7.7 (simplifying quadratics). In Chapter 14 we will discuss the generating function for the number a_{nk} of distinct subsequences of length k of the string of length n that cyclically repeats the letters $1, \dots, d$. The generating function is given in [FHS04, equation (7)] as

$$F(x, y) = \sum a_{nk} x^k y^n = \frac{1}{1 - y - xy(1 - y^d)}.$$

We will compute the case $d = 3$, so $F = 1/(1 - y - xy(1 - y^3))$. Fix $1 < \lambda < (d + 1)/2$. Let us compute coefficients in the direction $n/k = \lambda$, that is, $\bar{\mathbf{r}} = (1, \lambda)$.

Suppose we forget to check whether H factors. First, if we check for singularities, we will find one at $(1, 1)$. Secondly, we solve the critical point equations for a smooth point $\mathbf{z}(\lambda) = (x(\lambda), y(\lambda))$ given by (9.4):

$$\begin{aligned} 1 - y - xy(1 - y^3) &= 0; \\ g := ky(-1 - x(1 - y^3) + 3xy^3) + nxy(1 - y^3) &= 0. \end{aligned}$$

The Maple command `Basis([H, g], plex(x, y))` returns a basis $\{g_1^*, g_2^*\}$, where

$$g_1^*(y) := (1 - y)^2[(n - 3k)y^2 + (n - 2k)y + (n - k)]$$

and g_2^* has leading term x^1y^0 . The factorization of g_1^* is another tip that H may factor. Going back and checking, we find that H does indeed factor into $(1 - y)$ and $(1 - xy(1 - y^d)/(1 - y))$. It is easy to see that there are no smooth critical points on the component $y = 1$, so we compute on the other component. Re-doing the computation for $1 - xy(1 - y^d)/(1 - y)$ yields the basis $\mathcal{B} := \{g_1, g_2\}$ where $g_1 = [(n - 3k)y^2 + (n - 2k)y + (n - k)]$ g_2 still has a pure x term. Before continuing, observe several points:

- (i) In Chapter 10 we will see how to arrive at this more transparently.
- (ii) In this case y is quadratic over the rationals and one could use the quadratic formula to solve by radicals. When $d \geq 6$, however, and in practice when $d \geq 4$, one cannot do this.
- (iii) Even in the present case, $d = 3$, solving by radicals and plugging into the polynomial for x as a function of y will yield an expression that is correct but difficult for Maple to simplify¹.

Accordingly, we continue without solving for y . The leading terms of \mathcal{B} are y^2 and x . There are exactly two monomials not divisible by one of these, namely 1 and y . In the basis $\{1, y\}$ for $\mathbb{C}[x, y]/\langle \mathcal{B} \rangle$, multiplication by y is particularly simple: 1 goes to y and y goes to

$$y^2 = (\lambda - 1)/(3 - \lambda) + y(\lambda - 2)/(3 - \lambda).$$

Thus

$$M(y) = \begin{bmatrix} 0 & 1 \\ \frac{\lambda-1}{3-\lambda} & \frac{\lambda-2}{3-\lambda} \end{bmatrix}.$$

Using `minpoly` we may verify that the minimal polynomial for this is g_1 . What about x ? From the equation $H = 0$ we know that

$$x = \frac{1}{y(1 + y + y^2)} = \frac{(3 - \lambda)^2}{(4 - \lambda)y + (\lambda - 1)}.$$

Computing $(3 - \lambda)^2[(4 - \lambda) * M(y) + (\lambda - 1) * \text{Id}]^{-1}$ gives

$$M(x) = \begin{bmatrix} 1/3 \frac{-10\lambda+11+2\lambda^2}{\lambda-1} & 1/3 \frac{(-4+\lambda)(-3+\lambda)}{\lambda-1} \\ 4/3 - 1/3\lambda & -1 + 1/3\lambda \end{bmatrix}$$

and computing the minimal polynomial p_x for x in an indeterminate, t , gives

$$p_x(t) = 3t^2 - \frac{14 - 14\lambda + 3\lambda^2}{\lambda - 1}t + \frac{(3 - \lambda)^3}{\lambda - 1}.$$

¹By hand, one can force Maple to repeatedly multiply parts of the expression by their algebraic conjugates.

Now it is permitted to solve for radicals in order to express the exponential order of a_{nk} as a function of n and k :

$$x(\lambda) = \frac{3\lambda^2 - 14\lambda + 14 + \sqrt{-3\lambda^4 + 36\lambda^3 - 152\lambda^2 + 256\lambda - 128}}{6\lambda - 6}$$

$$y(\lambda) = \frac{\lambda - 2 + \sqrt{-8 + 12\lambda - 3\lambda^2}}{6 - 2\lambda}$$

$$a_{nk} \approx x \binom{n}{k}^{-k} y \binom{n}{k}^{-n}.$$

Example 7.8 (an arrangement point). Suppose that the denominator H of the generating function F factors as $H = H_1H_2H_3$ where

$$\begin{aligned} H_1 &= 1 - x - y - xy \\ H_2 &= 1 - 2x - xy - y^2 \\ H_3 &= 1 - \frac{1}{4}x - \frac{3}{2}y - \frac{1}{4}y^2. \end{aligned}$$

Let us see what we can determine about \mathcal{V} . First we check whether the divisors H_j are all smooth. We may check the smoothness of H_j by computing

```
Basis([H_j , diff(H_j,x) , diff(H_j,y)] , tdeg(x,y));
```

here, we are free to use the term order `tdeg` that is fastest for computation, since all we want to know is whether the ideal in each case is equal to `[1]` (that is, whether the intersection of the three equations is empty). We see that it is. Next, we check for a common intersection point. The command

```
gb := Basis([H_1, H_2, H_3], plex(y, x))
```

returns `gb := [1-4x-x^2, 1-2y-x]`. Here we used the term order `plex(y, x)` to get an elimination basis, which we stored in `gb` for later use. We see from this that there are two common intersection points, whose x -values are the two roots $-2 \pm \sqrt{5}$ of the quadratic $1 - 4x - x^2$ and whose y -coordinate is $(1+x)/2$, that is, respectively $(-1 \pm \sqrt{5})/2$. We let `p` denote the solution in the positive quadrant and `q` the solution in the negative quadrant.

Next, we check whether `p` is an arrangement point. One way to check transversality of the three intersections at `p` is to check that the gradients are pairwise linearly independent there. Execute the commands

```
u_j := [diff(H_j,x), diff(H_j,y)];
```

for $j = 1, 2, 3$, followed by

```
Dij := ui [1] * uj [2] - uj [1] * ui [2];
```

for $(i, j) = (1, 2), (1, 3), (2, 3)$. To check linear dependence of the first two curves at \mathbf{p} , we need to evaluate D_{12} at \mathbf{p} . In this case we have an explicit expression for \mathbf{p} but in general we may not, however we may always evaluate by reducing D_{12} modulo the ideal of \mathbf{p} :

```
NormalForm(D12, gb, plex(y, x));
```

If $D_{12}(\mathbf{p}) = 0$ then reducing modulo a Gröbner basis for the ideal defined by \mathbf{p} , with respect to the same term order, must return zero. The value returned is $-(1 + 3x)/2$ so we see that the first two curves intersect transversely at \mathbf{p} . Incidentally, since \mathbf{q} is the algebraic conjugate of \mathbf{p} , the computation at \mathbf{q} is identical and transversality at one implies transversality at the other.

The results of Chapter 11 require that we find a linear relation for H_1, H_2 and H_3 over the analytic functions in a neighborhood of \mathbf{p} . Unfortunately, when the `NormalForm` command is used to compute the reduction, R , of f modulo g_1, \dots, g_n , the package is not set up to return h_1, \dots, h_n for which $R = f - \sum h_j g_j$. Until this is corrected, you must write your own subroutine to do this. Let us assume you have written such a routine, call it `ReduceWitness` (see Exercise 7.1). If H_1 were in $\langle H_2, H_3 \rangle$, then computing `gb23 := Basis([H2, H3], plex(y, x));` and `ReduceWitness(H1, gb23, plex(t, x));` would find g_2 and g_3 for which $H_1 - g_2 H_2 - g_3 H_3 = 0$.

In the local ring at \mathbf{p} , it is indeed true that $H_1 \in \mathcal{I} := \langle H_2, H_3 \rangle$, but this can and does fail in the polynomial ring because \mathcal{I} is not prime there. In fact, the curves \mathcal{V}_2 and \mathcal{V}_3 intersect in four points, only two of which are in \mathcal{V}_1 . To see this, load the `PolynomialIdeals` package and compute

```
gb23 := Basis([H1, H2], plex(y, x));
extra23 := Quotient(gb23, PolynomialIdeal(gb));
elimpoly := extra23 [2];
```

This returns the ideal of the “extra” points:

```
extra23 :=  $\langle 3x - 8 - 2y, x^2 - 8x + 20 \rangle$ ;
```

The generators for this ideal are nonvanishing on \mathbf{p} and multiplying H_1 by any of these, say the elimination polynomial $x^2 - 8x + 20$, produces a polynomial that vanishes wherever H_2 and H_3 vanish, hence is in the ideal `gb23`. Then, computing

```
ReduceWitness(elimpoly * H1, gb, plex(y, x))
```

produces g_2 and g_3 such that `elimpoly` $H_1 - g_2 H_2 - g_3 H_3 = 0$ as desired.

7.3 D-modules: computing with D-finite functions

In Chapter 2 we saw that several classes of generating functions are closed under addition and multiplication. One such class is the algebraic functions. If $F, G \in \mathbb{C}[[z_1, \dots, z_d]]$ are algebraic over $\mathbb{C}[z_1, \dots, z_d]$ then the fact that $F + G$ and FG are algebraic is in fact an effective fact in the following sense. We must be given algebraic functions F and G in some canonical form. Given that these are supposed to be algebraic, it makes sense to take as inputs definitions that witness the algebraicity of F and G . Specifically, let us take as inputs a polynomial $P \in \mathbb{C}[z_1, \dots, z_d][x]$ for which $P(F) = 0$ and a polynomial $Q \in \mathbb{C}[z_1, \dots, z_d][x]$ for which $Q(G) = 0$. Then we may use Gröbner basis computations to find a polynomial in $\mathbb{C}[z_1, \dots, z_d][x]$ annihilating $F + G$ and another one annihilating FG (see Exercises 7.2 and 7.3).

When it comes to D-finite functions, one may similarly ask whether operations known to preserve D-finiteness may be carried out effectively. The answer is yes, although the implementation is still evolving so I will not describe this in depth. To make sense of this, let us specify the problem as follows. By analogy with the case of algebraic functions, we should take the inputs to be D-finite functions, specified in a form which bears witness to their being D-finite. Unfortunately, the definition of D-finiteness for multivariate functions is that their derivatives generate a finite dimensional vector space. We would like a more effective definition, such as the univariate definition, which gives a linear differential equation (2.8). In the multivariate case, a D-finite function F does satisfy such a differential equation, but one typically needs F to satisfy more than one such equation in order to guarantee that F is D-finite and to compute differential equations satisfied by expressions involving F . We are led to consider an algebraic structure on all possible differential equations.

Consider $2d$ operations on $\mathbb{C}[[z_1, \dots, z_d]]$: the first d of these are multiplication by z_1, \dots, z_d respectively; the second d are differentiation $(\partial/\partial z_1), \dots, (\partial/\partial z_d)$ respectively. Denote the first d by x_1, \dots, x_d and the last d by $\partial_1, \dots, \partial_d$. Every commutation relation among these $2d$ operators is trivial except for the commutation relation

$$\partial_j x_j = x_j \partial_j + 1.$$

This motivates the following definition, which may be found in [Cou95, Chapter 1].

Definition 7.9 (Weyl algebra). Let U_d denote the free algebra over \mathbb{C} generated by the symbols $x_1, \dots, x_d, \partial_1, \dots, \partial_d$ and let A_d denote the quotient of this by the two-sided ideal generated by the set

$$\{[x_i, x_j], [\partial_i, \partial_j], [x_i, \partial_j], [x_i, \partial_i] - 1 : i \neq j\}$$

where $[u, v]$ denotes the commutator $uv - vu$. The algebra A_d is called the Weyl algebra and is isomorphic to the ring of differential operators on $\mathbb{C}[z_1, \dots, z_d]$ that are linear over $\mathbb{C}(z_1, \dots, z_d)$ (which we then extend to view as linear operators on $\mathbb{C}[[z_1, \dots, z_d]]$).

Suppose that $P, Q \in A_d$ annihilate $F \in \mathbb{C}[[z_1, \dots, z_d]]$. Then $\alpha P + \beta Q$ annihilate F for $\alpha, \beta \in \mathbb{C}$ and RP annihilates F for any $R \in A_d$. Consequently, the annihilator, \mathcal{I} , of F in A_d is a left ideal

of A_d . There is a condition on the annihilator of F , which we will not define here, which implies D-finiteness of F . An ideal is said to be **holonomic** if a certain quotient that may be constructed forms a finite dimensional vector space; see [SST00, Definition 1.4.8] for the full definition. The annihilator of F is holonomic if and only if F is D-finite. Furthermore, holonomicity is algorithmically checkable (Algorithm 1.4.17 of [SST00]).

It turns out that the theory of Gröbner bases may be adapted almost without alteration for certain cases where non-commutativity is limited, and these include the Weyl algebra. This is laid out in Sections 1.1 – 1.2 of [SST00], and apparently originated with [Cas84, Gal85]. Another treatment, in the slightly more general context of **Ore algebras**, appears in [CS98] and is attributed to [KRW90, Kre93].

The implementation of Gröbner basis techniques for non-commutative algebras is more complete in systems other than Maple, such as Singular and CoCoA. I do not want to get into those systems here! Maple 10 does have a package called `Ore_algebra`, which can apparently do the computations necessary, for example, to find a basis for the annihilator of $F + G$ given bases for the annihilators of F and G . An example of how to do this is given in [CS98, Section2.2].

Notes

The fact that the annihilator in the Weyl algebra of a function is holonomic if and only if the function is D-finite seems to have been proved first by Kashiwara [Kas78]; I quoted it from [CS98, Section 2]. For ideals that are not the annihilator of a function, the notions of holonomy and D-finiteness do not exactly correspond.

Exercises

Exercise 7.1 (witnessing $f = R \pmod{\mathcal{I}}$). Implement the algorithm described in [CLO92, Chapter 2, Section 3] for producing the quotients g_1, \dots, g_n as well as the remainder R such that $f = R + \sum_{j=1}^n g_j h_j$ where the polynomials f and h_1, \dots, h_n are given. You may assume h_1, \dots, h_n are a Gröbner basis for the ideal \mathcal{I} they generate, since you can always pass to that case by a single Maple computation. It is up to you whether to allow the term order to be input or simply to work with respect to a single term order such as `plex`. Some helpful pseudocode is given on page 62 of [CLO92].

Exercise 7.2 (effective addition of algebraic functions). The `Basis` command in Maple's `Groebner` package, if given a term ordering `plex(a, b)` and inputs in variables a, b, c, d, \dots , will treat this as a computation over $\mathbb{C}(c, d, \dots)[a, b]$, that is polynomials in a and b with coefficients in a rational function field. Use the substitution $F = (s + d)/2$ and $G = (s - d)/2$ and the `Basis` command to find a polynomial annihilating $F + G$.

Exercise 7.3 (effective multiplication of algebraic functions). Can you repeat Exercise 7.2 but for multiplication rather than addition?