Rational Expression Simplification with Polynomial Side Relations

by

Roman Pearce

B.Sc., Simon Fraser University, 2001

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

MASTER OF SCIENCE

In the Department
of
Mathematics

SIMON FRASER UNIVERSITY

August 2005

Approval

Name:	Roman Pearce
Degree:	Master of Science
Title of Thesis:	Rational Expression Simplification with Polynomial Side Relations
Examining Committee:	Dr. Petr Lisonek Assistant Professor Chair
	Dr. Michael Monagan Associate Professor Senior Supervisor
	Dr. Imin Chen Assistant Professor
	Dr. Marc Rybowicz External Examiner l'Université de Limoges 33, rue François Mitterrand 87032 Limoges Cedex 01, France
Date Approved:	August 4, 2005

SIMON FRASER UNIVERSITY

PARTIAL COPYRIGHT LICENCE

Abstract

The goal of this thesis is to develop generic algorithms for computing in polynomial quotient rings and their fields of fractions. We present two algorithms for simplifying rational expressions over $k[x_1, \ldots, x_n]/I$. The first algorithm uses Groebner bases for modules to compute an equivalent expression whose largest term is minimal with respect to a given monomial order. The second algorithm solves systems of linear equations to find equivalent expressions and conducts a brute force search to find an expression of minimal total degree.

Dedication

To my wife Sarah,

whose tolerance and support exceeded all reasonable bounds.

Acknowledgements

I would like to thank my supervisor Dr. Michael Monagan. His insights and outlook have influenced me far more than I would care to admit, and all for the better. The algorithm of Section 2.5 and the suggestion to use ideal quotients are his. I am also indebted for his unwaivering support and seemingly infinite patience, even when I didn't deserve it.

Contents

Approval Page ii

Abstract iii

Dedication iv

Acknowledgements v

Table of Contents vi

1 Preliminaries 1
- 1.1 Introduction . . . 1
- 1.2 Definitions . . . 3
- 1.3 Gröbner Bases . . . 6
- 1.4 Ideal Operations . . . 14
- 1.5 Homogenization . . . 18
- 1.6 Modules . . . 21

2 Quotient Rings 28
- 2.1 Arithmetic in $k[x_1, \ldots, x_n]/I$ . . . 28
- 2.2 Polynomial Division . . . 29
- 2.3 Rational Expressions I . . . 33
- 2.4 Rational Expressions II . . . 37
- 2.5 Rational Expressions III . . . 44

A Implementation 51
- A.1 PolynomialIdeals in Maple 10 . . . 51
- A.2 Inverses and Exact Division . . . 58
- A.3 Rational Expression Simplification . . . 61

Chapter 1

Preliminaries

1.1 Introduction

The manipulation of polynomials is a fundamental goal of computer algebra. It was the purpose for which many of the first computer algebra systems were written, and it remains an area of active research today. Presently, we have good algorithms to factor polynomials and simplify rational expressions over the rational numbers, finite fields, and over algebraic number fields.

The direction of our work has been somewhat different. Our goal is to develop generic algorithms for polynomial division and rational expression simplification in the presence of algebraic side relations. More precisely, we want to compute in polynomial quotient rings and their fields of fractions.

The cornerstone of any approach will be Gröbner bases. Invented by Bruno Buchberger in 1965, Gröbner bases are primarily used for ideal-theoretic com-

putations and for simplifying elements of a quotient ring to a canonical form. They can also be used to solve linear equations modulo an ideal, which we will use to invert elements and perform exact division.

In this thesis we present two solutions to the problem of rational expression simplification. This is a problem which arises quite naturally in computer algebra, often in relatively simple contexts. Consider the expression below.

$$\frac{\sin(x)+1}{\sin^4(x)-\cos^4(x)+\sin(x)}$$

This is a rational expression in $\sin(x)$ and $\cos(x)$, where the functions themselves satisfy the polynomial relation $\sin(x)^2+\cos(x)^2=1$. We would like to simplify the fraction so as to minimize the total degree of both the numerator and denominator in the result. We demonstrate using an ad-hoc method. Letting $s=\sin(x)$ and $c=\cos(x)$, we can rewrite the denominator as follows.

$$\begin{aligned}(s^4-c^4)+s &= (s^2-c^2)(s^2+c^2)+s \\ &= (s^2-(1-s^2))(1)+s \\ &= 2s^2+s-1 \\ &= (2s-1)(s+1)\end{aligned}$$

From this we can cancel the numerator and obtain $1/(2\sin(x)-1)$. This fraction must have minimal total degree because the expression is not a constant.

There are a number of problems confronting ad-hoc methods, not the least of which is that factorizations may not be unique. Another more profound difficulty is that some fractions can be simplified in a way that does not cor-

respond to the cancellation of a common divisor. This was noted by Monagan and Mulholland in for fractions over $\mathbb{Q}[s,c]/\langle s^2+c^2-1\rangle$ [Mul01].

What is needed is a general method; this is the topic of Chapter two. The rest of this chapter introduces the machinery of Gröbner bases and the ideal theoretic operations upon which our methods rely. This thesis is largely the result of computer experiments performed using the Maple computer algebra system and some of our own software. A sample session demonstrating this software is contained in the appendix.

1.2 Definitions

We begin with some basic definitions. Recall from the previous section that we had a polynomial relation $s^2+c^2-1=0$. In general we may have a number of such relations, so let S be the set of all polynomials which are equivalent to zero. The set S is clearly closed under addition, and any product involving an element of S is also in S.

Definition 1.1. Let R be a commutative ring. A set $I \subseteq R$ is an *ideal* if

i) $f+g \in I$ for all $f,g \in I$

ii) $fh \in I$ for all $f \in I$ and $h \in R$

We will restrict ourselves to computing with multivariate polynomials over a field, so that in our case $R = k[x_1,\ldots,x_n]$, the polynomial ring in n variables over the field k. A *generating set* or *basis* for an ideal I is a set of elements

$\{f_1, \ldots, f_s\}$ such that every element in I can be expressed in terms of the f_i. In our previous example the generating set consisted of a single element: s^2+c^2-1. In general we write $\langle f_1, \ldots, f_s \rangle$ to denote the ideal generated by $\{f_1, \ldots, f_s\}$.

Lemma 1.2. *Let $I \subsetneq R$ be an ideal where R is a commutative ring with identity. Define a relation $\sim$ on the elements of R by $a \sim b \Leftrightarrow a - b \in I$. Then $\sim$ is an equivalence relation.*

Proof $a - a = 0 \in I$ so $\sim$ is reflexive. If $a \sim b$ then $a - b \in I$ so $b - a = (-1)(a - b) \in I$ and $\sim$ is symmetric. Now suppose $a \sim b$ and $b \sim c$. Then $a - c = (a - b) + (b - c) \in I$ and $\sim$ is transitive. $\square$

If $a-b \in I$ we say that a and b are *congruent modulo I* and write $a \equiv b \mod I$. The congruence relation partitions the elements of R into equivalence classes, where everything in I is equivalent to zero.

Definition 1.3. Let $I \subsetneq R$ be an ideal where R is a commutative ring with identity. The *quotient ring R/I* is the ring whose elements are the equivalence classes of R modulo I, under the ring operations of R.

Example 1.4. From the earlier example with polynomials in $\mathbb{Q}[s, c]$:

$$\begin{aligned} s^4 - c^4 + s &= 2s^2 + s - 1 + (s^2 - c^2 - 1)(s^2 + c^2 - 1) \\ &\equiv 2s^2 + s - 1 \mod \langle s^2 + c^2 - 1 \rangle \end{aligned}$$

Thus $s^4 - c^4 + s$ and $2s^2 + s - 1$ are in the same equivalence class modulo $\langle s^2 + c^2 - 1 \rangle$. In the quotient ring $\mathbb{Q}[s, c]/\langle s^2 + c^2 - 1 \rangle$ they correspond to the

same element.

In addition to computing in $k[x_1, \ldots, x_n]/I$ we would like to simplify elements of its *field of fractions*. Fractions over $k[x_1, \ldots, x_n]/I$ can be represented as ordered pairs (a, b) where $b \notin I$, so that two fractions (a, b) and (c, d) are equivalent if $ad \equiv bc \mod I$. The binary operations are $(a, b) + (c, d) = (ad + bc, bd)$ and $(a, b) \cdot (c, d) = (ac, bd)$.

The definition above admits a troublesome possibility. Let $I = \langle x^2 - 1 \rangle$ and consider $1/(x-1) + 1/(x+1) = 2x/(x^2-1)$. Since $x^2 - 1 \equiv 0 \mod I$ the result is not a valid fraction. This problem arises whenever two non-zero elements multiply to give zero; such elements are called *zero-divisors*. Notice that a and b are zero-divisors of $k[x_1, \ldots, x_n]/I$ if and only if $ab \in I$ and $a, b \notin I$.

Definition 1.5. An ideal $I \subsetneq R$ is *prime* if $ab \in I \Rightarrow a \in I$ or $b \in I$.

Definition 1.6. A commutative ring with identity is an *integral domain* if it does not contain zero-divisors.

It should be clear that $k[x_1, \ldots, x_n]/I$ is an integral domain if and only if I is a prime ideal. In our approach to simplifying rational expressions we will assume that I is prime so as to avoid the problems caused by zero-divisors.

1.3 Gröbner Bases

Gröbner bases are a fundamental tool of algebraic geometry. They generalize the ideas behind the Euclidean algorithm and Gaussian elimination to systems of multivariate polynomials and provide canonical representatives for elements of a quotient ring. This allows us simplify expressions and detect zero.

A key ingredient of linear algebra and univariate polynomial computations is that an order is imposed on the monomials which may appear. In Gaussian elimination the monomials are variables, ordered a priori or incrementally by a pivoting strategy. In the Euclidean algorithm powers of a single variable are ordered by their degree. The definition below generalizes both of these concepts.

Definition 1.7. A *monomial order* is a relation $<$ such that

i) $<$ is a total order on the monomials of $k[x_1, \ldots, x_n]$

ii) $a < b \implies ac < bc$ for monomials a, b, and c

iii) 1 is the smallest monomial under $<$

Example 1.8. In *lexicographic order* with $x_1 > x_2 > \cdots > x_n$ monomials are compared first by their degree in x_1, then by their degree in x_2, and so on, continuing as long as there is a tie.

Example 1.9. In *graded lexicographic order* with $x_1 > x_2 > \cdots > x_n$ monomials are first compared by their total degree with ties broken by lexicographic

order as above. To illustrate we have written the terms of the polynomial below in descending graded-lexicographic order with $x > y > z$.

$$f(x, y, z) = x^3 + x^2z + xy^2 + x^2 + xy + xz + y^2 + x + y + z + 1$$

Example 1.10. In *graded-reverse lexicographic order* with $x_1 > x_2 > \cdots > x_n$ monomials are again compared first by their total degree but ties are broken by preferring monomials with least degree in the smallest variables. We have rewritten the polynomial above so that its terms are in descending graded-reverse lexicographic order with $x > y > z$.

$$f(x, y, z) = x^3 + xy^2 + x^2z + x^2 + xy + y^2 + xz + x + y + z + 1$$

Observe that x^3 is again the largest monomial, only this time because its degree in z and then y is smallest among its competitors. For the same reason, xy^2 is now greater than x^2z and y^2 is greater than xz.

Example 1.11. In an *elimination order* with $\{x_1, \ldots, x_{i-1}\} \gg \{x_i, \ldots, x_n\}$ monomials are first compared using a monomial order on $\{x_1, \ldots, x_{i-1}\}$, with ties broken by a second order on $\{x_i, \ldots, x_n\}$. As a result, the monomials containing $\{x_1, \ldots, x_{i-1}\}$ are all greater than the monomials involving only $\{x_i, \ldots, x_n\}$. Elimination orders can also have multiple groups of variables. The extreme case where $\{x_1\} \gg \{x_2\} \gg \cdots \gg \{x_n\}$ is lexicographic order.

Definition 1.12. Let $f \in k[x_1, \ldots, x_n]$. The *leading term* of f, denoted $\mathrm{LT}(f)$, is the term whose monomial is greatest with respect to a monomial order. The coefficient and monomial of this term are called the *leading coefficient* and *leading monomial* respectively.

Monomial orders lead to a natural generalization of polynomial division. Here a single polynomial is divided by a set of polynomials producing a remainder and optionally a sequence of quotients. When our choice of monomial order is clear we write $f \div G \rightarrow r$ to denote the division of a polynomial f by a list of polynomials G producing a remainder r.

Algorithm 1.13 (The Division Algorithm).

Input a polynomial f, a list of polynomials G, a monomial order $<$

Output a polynomial r where no term of r is divisible by an $\mathrm{LT}(G_i)$, (optionally) a list of polynomials Q with $f - \sum_{i=1}^{|G|} Q_i G_i = r$

$(p, r) \leftarrow (f, 0)$

$Q \leftarrow (0, \ldots, 0)$

while $p \neq 0$ **do**

  select the first G_i where $\mathrm{LT}(G_i)$ divides $\mathrm{LT}(p)$

  if no such G_i exists move $\mathrm{LT}(p)$ to the remainder

    $r \leftarrow r + \mathrm{LT}(p)$

    $p \leftarrow p - \mathrm{LT}(p)$

  else cancel $\mathrm{LT}(p)$ using G_i

    $Q_i \leftarrow Q_i + (\mathrm{LT}(p)/\mathrm{LT}(G_i))$

    $p \leftarrow p - (\mathrm{LT}(p)/\mathrm{LT}(G_i))G_i$

  end if

end loop

return r, Q

We would like to use the division algorithm to test for membership in an ideal, but doing so poses a problem. Consider $I = \langle x^2 + 1, xy + 1 \rangle$. The polynomial $x(xy+1) - y(x^2+1) = x - y$ is clearly a member of the ideal, however it can not be reduced by either $x^2 + 1$ or $xy + 1$ using any monomial order. The problem is remedied by the following condition.

Definition 1.14. Let $I \subseteq k[x_1, \ldots, x_n]$ be an ideal and let $<$ be a monomial order. A set G is a *Gröbner basis* for I with respect to $<$ if for every $f \in I$, $\mathrm{LT}(f)$ is divisible by $\mathrm{LT}(g)$ for some $g \in G$.

Example 1.15. Let $I = \langle x^3 - 1, x^2 - x \rangle$ in $\mathbb{Q}[x]$. From the Extended Euclidean algorithm we obtain $\gcd(x^3-1, x^2-x) = (1)(x^3-1) - (x+1)(x^2-x) = x-1 \in I$. Every element of I is of the form $p(x^3-1) + q(x^2-x)$ which is divisible by $x-1$ so $I = \langle x - 1 \rangle$ and $\{x - 1\}$ is a Gröbner basis.

Theorem 1.16. *Let G be a Gröbner basis for $I \subseteq k[x_1, \ldots, x_n]$. Then*

i) $f \div G \to r$ *implies* $f \equiv r \mod I$

ii) $f \equiv g \mod I$ *and* $f \div G \to r$ *implies* $g \div G \to r$

Proof (i) By Algorithm 1.13 we have $f - r = \sum_{i=1}^{|G|} Q_i G_i \equiv 0 \mod I$. (ii) If $f \div G \to r$ and $g \div G \to r'$ then no term of r (respectively r') is divisible by a leading term of G. Then no term of $r - r'$ is divisible by a leading term of G, and since $r - r' \in I$ and G is a Gröbner basis this implies $r - r' = 0$. $\square$

Corollary 1.17.

i) $f \div G \to 0$ *if and only if* $f \in I$

ii) if $f \div G \to r$ *then the remainder* r *is unique*

For a given monomial order, Theorem 1.16 associates each equivalence class of $k[x_1, \ldots, x_n]/I$ with a unique remainder, called a *normal form*, which can be computed by division with a Gröbner basis for I. Thus we can perform addition and multiplication in $k[x_1, \ldots, x_n]/I$ using the operations of $k[x_1, \ldots, x_n]$, followed by a reduction to the normal form.

Having demonstrated the usefulness of Gröbner bases we turn now to their construction. Previously we discovered $x - y \in \langle x^2 + 1, xy + 1 \rangle$ by inducing a cancellation of the leading terms of $x^2 + 1$ and $xy + 1$. This is called a *syzygy*, and to compute a Gröbner basis for an arbitrary ideal it will suffice to compute these syzygies one at a time and add them, when necessary, to the generating set.

Definition 1.18. Let f and g be polynomials and let $<$ be a monomial order. The *syzygy polynomial* of f and g is

$$\mathrm{S}(f, g) = \frac{\mathrm{LT}(g)f - \mathrm{LT}(f)g}{\gcd(\mathrm{LT}(f), \mathrm{LT}(g))}$$

Theorem 1.19 (Buchberger's Syzygy Criterion). *Let* I *be an ideal with generating set* G *and let* $<$ *be a monomial order.* G *is a Gröbner basis for* I *with respect to* $<$ *if and only if* $\mathrm{S}(f, g) \div G \to 0$ *for all* $f, g \in G$.

Proof See [Cox96].

We present a crude version of Buchberger's algorithm based on Theorem 1.19. The algorithm terminates when $\mathrm{S}(f,g) \div G \to 0$ has been verified for all $f, g \in G$. This is guaranteed to happen by the *ascending chain condition*; every strictly increasing sequence of ideals in $k[x_1, \ldots, x_n]$ is finite. Observe that when a non-zero remainder r is added to G the ideal of leading monomials of G is strictly enlarged. The ACC also implies that every ideal of $k[x_1, \ldots, x_n]$ has a finite set of generators, so that Algorithm 1.20 implies the existence of Gröbner bases.

Algorithm 1.20 (Buchberger's Algorithm).

Input a set of generators F, a monomial order $<$

Output a Gröbner basis G with respect to $<$

$G \leftarrow F$

$P \leftarrow \{(f,g) \mid f, g \in F\}$

while $|P| > 0$ do

  select a pair $(f,g) \in P$

  $P \leftarrow P \setminus \{(f,g)\}$

  $r \leftarrow \mathrm{S}(f,g) \div G$

  if $r \neq 0$

    $P \leftarrow P \cup \{(h,r) \mid h \in G\}$

    $G \leftarrow G \cup \{r\}$

  end if

end loop

return G

Example 1.21. We compute a Gröbner basis for $\langle xy+1, x^2+1\rangle \subseteq \mathbb{Q}[x,y]$ using lexicographic order with $x > y$. Our initial basis consists of just these polynomials, but we have a syzygy.

$$S(xy+1, x^2+1) = x(xy+1) - y(x^2+1) = x - y$$

This polynomial can not be reduced by either x^2+1 or $xy+1$ so we add it to the basis unchanged and two new syzygies are created.

$$S(x^2+1, x-y) = (x^2+1) - x(x-y) = xy+1$$
$$S(xy+1, x-y) = (xy+1) - y(x-y) = y^2+1$$

The first polynomial is already in the basis and thus reduces to zero. The second one doesn't reduce, so it is added to the basis and its syzygies are constructed.

$$\begin{aligned} S(x^2+1, y^2+1) &= y^2(x^2+1) - x^2(y^2+1) = -x^2+y^2 \\ S(xy+1, y^2+1) &= y(xy+1) - x(y^2+1) \quad = -x+y \\ S(x-y, y^2+1) &= y^2(x-y) - x(y^2+1) \quad = -x-y^3 \end{aligned}$$

One can easily verify that all of these syzygies reduce to zero. The algorithm terminates with $\{xy+1, x^2+1, x-y, y^2+1\}$ which is a Gröbner basis.

Observe that the initial generators $xy+1$ and x^2+1 in Example 1.21 are no longer needed in the final Gröbner basis. To see this, we can sort the basis into descending order and divide each element by its successors using Algorithm 1.13. We find that $x^2+1 = x(x-y) + (xy+1)$ and $xy+1 = y(x-y) + (y^2+1)$, so $\{x-y, y^2+1\}$ is also a Gröbner basis.

Definition 1.22. Let G be a Gröbner basis, G is *reduced* if $0 \notin G$ and each $g \in G$ is in normal form with respect to $G \setminus \{g\}$.

A particularly useful property of reduced Gröbner bases is that their elements are unique up to a constant multiple [Cox96]. Starting from the output of Buchberger's algorithm one can construct a reduced Gröbner basis by dividing as above, although more efficient methods exist. Some variants of Buchberger's algorithm also partially reduce the basis as new polynomials are added [Geb88].

With regards to a practical implementation Algorithm 1.20 is dreadfully slow. In practice it is not necessary to consider every $S(f, g)$ and criteria have been developed to omit superfluous ones [Buc79][Geb88]. Still the vast majority of time in Buchberger's algorithm is spent reducing syzygies to zero [Buc85]. Subsequent algorithms by J.C. Faugère improve on this by considering several syzygies at once [Fau99][Fau02].

One redeeming property of Algorithm 1.20 is that we can easily modify it to express the resulting Gröbner basis elements in terms of the initial generators. The idea is to attach a vector C to each $g \in G$ with the property that

$$g = \sum_{i=1}^{|F|} C_i F_i$$

Whenever polynomial arithmetic is performed, the vectors are updated with the analogous operation. We illustrate the technique by repeating Example 1.21.

Example 1.23. Let $F = [xy + 1, x^2 + 1] \subset \mathbb{Q}[x, y]$ be our generating set, again using lexicographic order with $x > y$. We begin by attaching the identity vectors $[1, 0]$ and $[0, 1]$ to $xy + 1$ and $x^2 + 1$. The first syzygy

$$S(xy + 1, x^2 + 1) = x(xy + 1) - y(x^2 + 1) = x - y$$

is assigned the vector $x[1,0] - y[0,1] = [x, -y]$. Continuing, we assign

$$\begin{aligned} \mathrm{S}(xy+1, x-y) &= y^2+1 & 1[1,0] - y[x,-y] &= [1-xy, y^2] \\ \mathrm{S}(x^2+1, x-y) &= xy+1 & 1[0,1] - x[x,-y] &= [-x^2, 1+xy] \end{aligned}$$

Were we to reduce these polynomials we would have to update their vectors in Algorithm 1.13 as well, but for now we are done. The remaining syzygies all reduce to zero and $[xy+1, x^2+1, x-y, y^2+1]$ is a Gröbner basis. From the vectors we obtain the following relations.

$$\begin{aligned} xy+1 &= 1\,(xy+1) + 0\,(x^2+1) \\ x^2+1 &= 0\,(xy+1) + 1\,(x^2+1) \\ x-y &= x\,(xy+1) - y\,(x^2+1) \\ y^2+1 &= (1-xy)\,(xy+1) + y^2\,(x^2+1) \end{aligned}$$

1.4 Ideal Operations

In addition to membership testing, Gröbner bases also can be used to compute many ideal-theoretic operations. Because surveys of this area usually constitute a volume, we present a minimum amount of material and defer to [Cox96] and [BW93] for additional treatment. We begin with the intersection of an ideal and a subring of $k[x_1, \ldots, x_n]$.

Theorem 1.24 (The Elimination Theorem). *Let $I \subseteq k[x_1, \ldots, x_n]$ be an ideal and let G be a Gröbner basis for I with respect to an elimination order $<$ with $\{x_1, \ldots, x_{i-1}\} \gg \{x_i, \ldots, x_n\}$. Then $G \cap k[x_i, \ldots, x_n]$ is a Gröbner basis for $I \cap k[x_i, \ldots, x_n]$ under the restriction of $<$ to $\{x_i, \ldots, x_n\}$.*

Proof Note that $G \cap k[x_i, \ldots, x_n] \subset I \cap k[x_i, \ldots, x_n]$ since $G \subset I$. Now for $f \in I \cap k[x_i, \ldots, x_n]$ we have $f \div G \to 0$ under $<$ but no term of f contains $\{x_1, \ldots, x_{i-1}\}$ so only elements of $G \cap k[x_i, \ldots, x_n]$ can be used in the division. The same argument applied to $\{S(g_i, g_j) : g_i, g_j \in G \cap k[x_i, \ldots, x_n]\}$ shows that $G \cap k[x_i, \ldots, x_n]$ is a Gröbner basis. □

Example 1.25. In Example 1.21 we found that $\{x^2 + 1, xy + 1, y - x, y^2 + 1\}$ is a Gröbner basis for $I = \langle x^2 + 1, xy + 1\rangle \subset \mathbb{Q}[x, y]$ under lexicographic order with $x > y$. Since this is an elimination order $I \cap \mathbb{Q}[y] = \langle y^2 + 1\rangle$.

Definition 1.26. Let $I = \langle f_1, \ldots, f_s\rangle$ and $J = \langle g_1, \ldots, g_t\rangle$. Then

i) The *ideal sum* $I + J = \langle f_1, \ldots, f_s, g_1, \ldots, g_t\rangle$.

ii) The *ideal product* $IJ = \langle f_1 g_1, \ldots, f_i g_j, \ldots, f_s g_t\rangle$

iii) The *intersection* $I \cap J = \{f : f \in I \text{ and } f \in J\}$

A clever trick reduces the computation of ideal intersections to the subring intersection of Theorem 1.24. Let $I \subseteq k[x_1, \ldots, x_n]$ be an ideal and let t be an extra variable. We let tI denote the ideal product of $\langle t\rangle$ and I in $k[x_1, \ldots, x_n, t]$.

Lemma 1.27. *Let I and J be ideals of $k[x_1, \ldots, x_n]$. Then $I \cap J = (tI + (1 - t)J) \cap k[x_1, \ldots, x_n]$.*

Proof Suppose $f \in I \cap J \subseteq k[x_1, \ldots, x_n]$. Then $tf \in tI$ and $(1 - t)f \in (1 - t)J$ so $f = tf + (1 - t)f \in (tI + (1 - t)J) \cap k[x_1, \ldots, x_n]$. Now let $f \in (tI + (1 - t)J) \cap k[x_1, \ldots, x_n]$. Then $\langle tf\rangle \subseteq (tI + (1 - t)J)$ so we can add

$\langle 1-t\rangle$ to both sides and obtain $f \in \langle tf, 1-t\rangle \subseteq I + \langle 1-t\rangle$ and intersect with $k[x_1, \ldots, x_n]$ to get $f \in I$. A similar argument shows $f \in J$. $\square$

Example 1.28. Let $I = \langle x-1, y-1\rangle$ and $J = \langle x-1, y+1\rangle$. We eliminate t from $\{t(x-1), t(y-1), (1-t)(x-1), (1-t)(y+1)\}$ using a lexicographic Gröbner basis with $t > x > y$. The Gröbner basis is $\{y^2-1, x-1, 2t-y-1\}$ so $I \cap J = \langle y^2-1, x-1\rangle$.

The most important task of this section is to describe the quotient operation for ideals. Analogous to cancelling out a GCD, it forms the basis of one of our methods for simplifying rational expressions over $k[x_1, \ldots, x_n]/I$.

Definition 1.29. Let $I, J \subseteq k[x_1, \ldots, x_n]$ be ideals. The *ideal quotient* $I : J$ is the set $\{f \in k[x_1, \ldots, x_n] : fh \in I \text{ for all } h \in J\}$.

We show that $I : J$ is an ideal. Note that it trivially contains I. If $f, g \in I : J$ and $h \in J$ then $(f+g)h = fh + gh \in I$ so $(f+g) \in I : J$. Likewise if $f \in I : J$, $h \in J$ and $g \in k[x_1, \ldots, x_n]$ then $fgh \in I$ since $fh \in I$, so $fg \in I : J$.

Example 1.30. Let $I = \langle x^2 - y^2\rangle$ and $J = \langle x-y\rangle$. Then $I : J = \langle x+y\rangle$.

Example 1.31. Let $f, g \in k[x]$. The quotient $\langle f\rangle : \langle g\rangle$ contains all polynomials whose product with g is a multiple of f. In particular, a minimal element is $\operatorname{lcm}(f,g)/g = f/\gcd(f,g)$ which also generates the ideal.

The properties below are noted by Cox et al [Cox96]. The third property combined with the subsequent lemma provides an algorithm to compute $I : J$.

Lemma 1.32. *Let I, J, and K be ideals of $k[x_1, \ldots, x_n]$. Then*

i) $I : J = k[x_1, \ldots, x_n]$ *if and only if* $J \subseteq I$

ii) $IJ \subseteq K$ *if and only if* $I \subseteq K : J$

iii) $I : (\sum_{i=1}^{s} J_i) = \bigcap_{i=1}^{s} (I : J_i)$

Proof See [Cox96].

Lemma 1.33. *Let G be a Gröbner basis for $I \cap \langle f \rangle$. Then $\{g/f : g \in G\}$ is a Gröbner basis for $I : \langle f \rangle$ with respect to the same monomial order.*

Proof First observe $g_i \in \langle f \rangle$ so each g_i/f is a polynomial. Then $g_i/f \in I : \langle f \rangle$ since $(g_i/f)f = g_i \in I$. Now let $h \in I : \langle f \rangle$. We know $\mathrm{LT}(fh)$ is divisible by some $\mathrm{LT}(g_i)$ since $\{g_1, \ldots, g_t\}$ is a Gröbner basis. Then $\mathrm{LT}(h)$ is divisible by $\mathrm{LT}(g_i/f)$, and since h was arbitrary $\{g_1/f, \ldots, g_t/f\}$ is a Gröbner basis. □

Example 1.34. Let $I = \langle x^2, y^2 - 1 \rangle$ and $J = \langle x, y - 1 \rangle$ in $\mathbb{Q}[x, y]$. Then $I \cap \langle x \rangle = \langle x^2, x(y^2 - 1) \rangle$ and $I \cap \langle y - 1 \rangle = \langle x^2(y - 1), y^2 - 1 \rangle$ so

$$\begin{aligned} I : J &= (I : \langle x \rangle) \cap (I : \langle y - 1 \rangle) \\ &= \langle x, y^2 - 1 \rangle \cap \langle x^2, y + 1 \rangle \\ &= \langle x^2, x(y + 1), y^2 - 1 \rangle \end{aligned}$$

1.5 Homogenization

Next we present a few interesting results about homogeneous Gröbner bases from [Fro97]. A generalization to arbitrary gradings appears in §10.2 of [BW93].

Definition 1.35. A polynomial $f \in k[x_1, \ldots, x_n]$ is *homogeneous* if all of its non-zero terms have the same total degree.

Lemma 1.36. *Let f and $G = [g_1, \ldots, g_t]$ be homogeneous polynomials. If we compute $f \div G \longrightarrow r$ using Algorithm 1.13, then the remainder r and all of the quotients are also homogeneous.*

Proof Upon entering the main loop p (which is initially f) is homogeneous and we take one of two actions. If $\mathrm{LT}(p)$ is divisible by some $\mathrm{LT}(g_i)$ then we subtract $p_{new} \leftarrow p - (\mathrm{LT}(p)/\mathrm{LT}(g_i))g_i$. Since g_i is homogeneous p_{new} is homogeneous and $\deg(p_{new}) = \deg(p)$ if $p_{new} \neq 0$. Otherwise we move the leading term of p to the remainder r. Because the degree of p is invariant while $p \neq 0$ the terms of r all have degree $\deg(f)$. Similarly, the non-zero terms of each quotient Q_i must have degree $\deg(f) - \deg(g_i)$. □

Lemma 1.37. *Let I be an ideal generated by homogeneous polynomials. Then a reduced Gröbner basis for I with respect to any monomial order consists of homogeneous polynomials.*

Proof Observe that syzygies of homogeneous polynomials are homogeneous and by Lemma 1.36 so are their remainders. Thus the Buchberger algorithm

adds only homogeneous polynomials to the generating set. To reduce a Gröbner basis it suffices to divide each $g \in G$ by $G \setminus \{g\}$ and remove zero. Again by Lemma 1.36 the result is a set of homogeneous polynomials. □

An ideal with homogeneous generators is said to be homogeneous also. Note that the class of homogeneous ideals is closed under the operations of Section 1.4, although we have omitted some of the requisite details.

Definition 1.38. Let $f \in k[x_1, \ldots, x_n]$ and let y be a new variable. The *homogenization* of f in y is the polynomial $f^{(y)} = y^{\deg(f)} f(x_1/y, \ldots, x_n/y)$.

Example 1.39. Let $f = x^3 + x + 1 \in \mathbb{Q}[x]$. We introduce y to homogenize f. Applying Definition 1.38 we obtain $f^{(y)} = x^3 + xy^2 + y^3$.

Homogenization is an injective map from $k[x_1, \ldots, x_n]$ to $k[x_1, \ldots, x_n, y]$ which can be inverted by evaluating $y = 1$. It is not a ring homomorphism since $(f+g)^{(y)} \neq f^{(y)} + g^{(y)}$ when f and g have different total degree. Nevertheless, using Gröbner basis theory we can recover some of the results for homogeneous polynomials, provided we accept the following condition.

Definition 1.40. Let $<$ be a monomial order on $k[x_1, \ldots, x_n]$ and let y be a new variable. We say that $<'$ is a *good extension* of $<$ to $k[x_1, \ldots, x_n, y]$ if $\mathrm{LT}_<(f) = \mathrm{LT}_{<'}(f^{(y)})$ for all $f \in k[x_1, \ldots, x_n]$.

Example 1.41. Let $<$ and $<'$ denote graded lexicographic order with $x > y$ and $x > y > z$ respectively. We show that $<'$ is *not* a good extension of $<$. Let

$f = x + y^2$. Then $\mathrm{LT}_<(f) = y^2$ but $\mathrm{LT}_{<'}(f^{(z)}) = \mathrm{LT}_{<'}(xz + y^2) = xz$.

Example 1.42. Let $<$ and $<'$ denote graded reverse lexicographic order with $x_1 > x_2 > \ldots x_n$ and $x_1 > x_2 > \cdots > x_n > y$ respectively. We show that $<'$ is a good extension of $<$. If $f^{(y)}$ is the homogenization of $f \in k[x_1, \ldots, x_n]$ then all of its terms have degree $\deg(f)$ and to compute $\mathrm{LT}_{<'}(f^{(y)})$ we first select the terms with lowest degree in y. These terms have degree zero in y and degree $\deg(f)$ in $\{x_1, \ldots, x_n\}$ so they are initially selected by $<$ as well. Then $\mathrm{LT}_{<'}(f^{(y)}) = \mathrm{LT}_<(f)$ since subsequent ties are broken in an identical manner.

Not all monomial orders have good extensions. In fact, $\mathrm{LT}_<(f) = \mathrm{LT}_{<'}(f^{(y)})$ requires $\deg(\mathrm{LT}_<(f)) = \deg(f)$ for all f so only *graded* orders can be extended. The purpose of good extensions is simple: as we will see in the following theorem, the property of being a Gröbner basis is preserved under homogenization and dehomogenization. This has numerous applications in projective geometry, see [Cox96] for examples.

Definition 1.43. Let $I \subseteq k[x_1, \ldots, x_n]$ be an ideal. The *homogenization* of I in y is the ideal $I^{(y)}$ generated by $\{f^{(y)} : f \in I\}$ in $k[x_1, \ldots, x_n, y]$.

Example 1.44. Let $I = \langle y - 1, xy - 1 \rangle$. If we homogenize $y - 1$ and $xy - 1$ using a new variable z we obtain $I' = \langle y - z, xz - z^2 \rangle$. However $x - 1 \in I$ so $x - z \in I^{(z)}$ but $x - z \notin I'$. This shows that we can not simply homogenize the generators of I to obtain $I^{(z)}$.

Theorem 1.45. *Let $I \subseteq k[x_1, \ldots, x_n]$ be an ideal, and let G be a reduced Gröbner basis for I with respect to a monomial order $<$. If y is a new variable and $<'$ is a good extension of $<$ to $\{x_1, \ldots, x_n, y\}$, then $G^{(y)} = \{g^{(y)} : g \in G\}$ is a reduced Gröbner basis for $I^{(y)}$ under $<'$.*

Proof See [Fro97].

Example 1.46. Let $I = \langle y - 1, xy - 1 \rangle$ as in Example 1.44. We homogenize I using graded reverse lexicographic order with $x > y > z$, which is a good extension of the same order with $x > y$. A reduced Gröbner basis for I is $\{y-1, x-1\}$ so a reduced Gröbner basis for $I^{(z)}$ is $\{y-z, x-z\}$ by Theorem 1.45.

1.6 Modules

For our final section of preliminary material, we introduce Gröbner bases for modules. Modules over rings are similar to vector spaces over fields, although our presentation focuses entirely on developing Gröbner basis techniques. For a more comprehensive treatment of modules refer to [Cox98].

Definition 1.47. Let R be a ring with unity. A *module over R* or *R-module* is a set M together with operations for addition and scalar multiplication satisfying

i) $(M, +)$ is an Abelian group

ii) $1f = f$ for all $f \in M$

iii) $(ab)f = a(bf) \in M$ for all $a, b \in R$ and $f \in M$

iv) $(a+b)f = af + bf$ for all $a, b \in R$ and $f \in M$

v) $a(f+g) = af + ag$ for all $a \in R$ and $f, g \in M$

When R is not commutative the definition above is that of a *left R-module*, however we are only concerned with the case $R = k[x_1, \ldots, x_n]$. In fact, we will only consider modules which are a subset of R^m. These are *submodules* of R^m, since R^m is itself an R-module.

Example 1.48. Let $R = k[x, y]$ and consider the set of all possible combinations of $\begin{bmatrix} x \\ 1 \end{bmatrix}$ and $\begin{bmatrix} y \\ 0 \end{bmatrix}$ in R^2. For example, $\begin{bmatrix} 0 \\ y \end{bmatrix} = y \begin{bmatrix} x \\ 1 \end{bmatrix} - x \begin{bmatrix} y \\ 0 \end{bmatrix}$ is in the set while $\begin{bmatrix} y \\ 1 \end{bmatrix}$ is not. It is easy to see that this set is a module over R and thus a submodule of R^2.

Observe that submodules of R^1 correspond to ideals. With this in mind it is natural to ask whether Gröbner basis techniques can be extended to work with submodules of R^m. The only suprising fact is that it all works out so easily.

Our first task is to extend monomial orders to elements of R^m. Following [Cox98], we write $f \in R^m$ as a linear combination of monomials in R and standard basis vectors $\mathbf{e_i}$. For example:

$$\begin{bmatrix} x^2 + y \\ 2y \end{bmatrix} = \begin{bmatrix} x^2 \\ 0 \end{bmatrix} + \begin{bmatrix} y \\ 0 \end{bmatrix} + \begin{bmatrix} 0 \\ 2y \end{bmatrix} = x^2 \mathbf{e_1} + y \mathbf{e_1} + 2y \mathbf{e_2}$$

Then monomials of R^m are all of the form $\alpha \mathbf{e_i}$ where α is a monomial in R. Given a monomial order $<$ on $R = k[x_1, \ldots, x_n]$ there are two natural ways to

extend it to a monomial order on R^m [AL94].

Definition 1.49. Let $<$ be a monomial order on R. The *position over term* monomial order $<_{POT}$ is defined by $a\,\mathbf{e_i} >_{POT} b\,\mathbf{e_j}$ if $i < j$ or $i = j$ and $a > b$.

Definition 1.50. Let $<$ be a monomial order on R. The *term over position* monomial order $<_{TOP}$ is defined by $a\,\mathbf{e_i} >_{TOP} b\,\mathbf{e_j}$ if $a > b$ or $a = b$ and $i < j$.

Example 1.51. Let $<$ denote graded lexicographic order with $x > y$ and let $f = xy\,\mathbf{e_1} + x^2\,\mathbf{e_2} + x^2\,\mathbf{e_3} = \begin{bmatrix} xy & x^2 & x^2 \end{bmatrix}^T$. Then the largest (or leading) monomial of f is $xy\,\mathbf{e_1}$ under $<_{POT}$ and $x^2\,\mathbf{e_2}$ under $<_{TOP}$.

All that remains is to define division and syzygies for monomials of R^m before we can run the algorithms of Section 1.3 unchanged. Quite naturally, if a monomial $a\,\mathbf{e_i}$ divides $b\,\mathbf{e_j}$ we expect to find q with $b\,\mathbf{e_j} = qa\,\mathbf{e_i}$. This is possible if and only if $i = j$ and a divides b in R. Similarly, one constructs syzygies by inducing a cancellation of the leading terms.

Definition 1.52. Let $f, g \in R^m$ with leading terms $a\,\mathbf{e_i}$ and $b\,\mathbf{e_j}$ respectively. The *syzygy vector* of f and g is $\mathrm{S}(f,g) = \dfrac{bf - ag}{\gcd(a,b)}$ if $i = j$ or $\mathbf{0} \in R^m$ otherwise.

Example 1.53. Let $f = x\,\mathbf{e_1} + \mathbf{e_2}$ and $g = y\,\mathbf{e_1}$ from Example 1.48. We use $<_{TOP}$ extending graded lexicographic order with $x > y$. The leading monomials are $x\,\mathbf{e_1}$ and $y\,\mathbf{e_1}$, so $\mathrm{S}(f,g) = yf - xg = y\,\mathbf{e_2}$.

Example 1.54. Building on the previous example, we apply Algorithm 1.13 to divide $p = (xy + y)\,\mathbf{e_1} + x\,\mathbf{e_2}$ by $G = \{x\,\mathbf{e_1} + \mathbf{e_2}, y\,\mathbf{e_1}, y\,\mathbf{e_2}\}$ using $<_{TOP}$. The leading monomial of p is $xy\,\mathbf{e_1}$, which is reducible by G_1. We subtract

$$p \leftarrow \begin{bmatrix} xy + y \\ x \end{bmatrix} - y \begin{bmatrix} x \\ 1 \end{bmatrix} = \begin{bmatrix} y \\ x - y \end{bmatrix}$$

Since we are using a term over position order the new leading term of p is $x\,\mathbf{e_2}$. This is not divisible by any element of G, so we move it to the remainder. The next term of p is $y\,\mathbf{e_1}$, which is reducible by G_2 so

$$p \leftarrow \begin{bmatrix} y \\ -y \end{bmatrix} - \begin{bmatrix} y \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ -y \end{bmatrix}$$

Finally the leading term $-y\,\mathbf{e_2}$ is cancelled by adding G_3 and we obtain zero. The algorithm terminates, returning the remainder $r = x\,\mathbf{e_2}$ and optionally the list of quotients $Q = [-y, -1, 1]$.

The characterization of Gröbner bases is the same for modules as it is for polynomial ideals, and one can show that Buchberger's criterion (Theorem 1.19) carries over as well [Cox98]. That is, a set G is a Gröbner basis if and only if $\mathrm{S}(f, g) \div G \to 0$ for all $f, g \in G$. Observe that this condition is satisfied by the set G of Example 1.54, and that it was obtained by running the Buchberger algorithm in Example 1.53.

Similarly Lemma 1.2, Theorem 1.16, and Corollary 1.17 all continue to hold when ideals $I \subseteq R$ are replaced by modules $M \subseteq R^m$. As a result, Gröbner bases can be used to test for membership in submodules of R^m. This is illustrated in Example 1.54, where $p = (xy + y)\,\mathbf{e_1} + x\,\mathbf{e_2}$ was found not to be an element of the module $\langle x\,\mathbf{e_1} + \mathbf{e_2}, y\,\mathbf{e_1}\rangle$.

We conclude with two interesting applications of Gröbner bases for modules. First we show how a module computation can express a Gröbner basis for an ideal $I \subseteq k[x_1, \ldots, x_n]$ in terms of the generators, like the extended Buchberger algorithm of Section 1.3. We demonstrate using Example 1.23.

Example 1.55. Let $F = [xy + 1, x^2 + 1]$ and let $<$ denote lexicographic order with $x > y$. We compute a Gröbner basis for $\langle F_1 \mathbf{e_1} + \mathbf{e_2}, F_2 \mathbf{e_1} + \mathbf{e_3} \rangle$ using $<_{POT}$. Our initial basis is $G = \{(xy + 1)\mathbf{e_1} + \mathbf{e_2}, (x^2 + 1)\mathbf{e_1} + \mathbf{e_3}\}$ and

$$\mathrm{S}(G_1, G_2) = xG_1 - yG_2 = (x - y)\mathbf{e_1} + x\mathbf{e_2} + (-y)\mathbf{e_3}$$

Written in $<_{POT}$ order, the monomials are $x\mathbf{e_1}$, $-y\mathbf{e_1}$, $x\mathbf{e_2}$, and $-y\mathbf{e_3}$. None of them are reducible by G_1 or G_2, so we add this element unchanged as G_3 and construct its syzygies

$$\mathrm{S}(G_1, G_3) = G_1 - yG_3 = (y^2 + 1)\mathbf{e_1} + (-xy + 1)\mathbf{e_2} + y^2\mathbf{e_3}$$

$$\mathrm{S}(G_2, G_3) = G_2 - xG_3 = (xy + 1)\mathbf{e_1} + (-x^2)\mathbf{e_2} + (xy + 1)\mathbf{e_3}$$

The latter is reducible by G_1, and we add $G_4 = (y^2 + 1)\mathbf{e_1} + (-xy + 1)\mathbf{e_2} + y^2\mathbf{e_3}$ and $G_5 = (-x^2 - 1)\mathbf{e_2} + (xy + 1)\mathbf{e_3}$ to the basis. There are no syzygies involving G_5 at this point because no other G_i has a leading monomial in $\mathbf{e_2}$. The remaining syzygies are

$$\begin{aligned}
\mathrm{S}(G_1, G_4) &= (-x + y)\mathbf{e_1} + (x^2y - x + y)\mathbf{e_2} + (-xy^2)\mathbf{e_3} \\
\mathrm{S}(G_2, G_4) &= (-x^2 + y^2)\mathbf{e_1} + (x^3y - x^2)\mathbf{e_2} + (-x^2y^2 + y^2)\mathbf{e_3} \\
\mathrm{S}(G_3, G_4) &= (-x - y^3)\mathbf{e_1} + (x^2y + xy^2 - x)\mathbf{e_2} + (-xy^2 - y^3)\mathbf{e_3}
\end{aligned}$$

all of which reduce to zero. The elements of G are written in vector form below.

$$G = \left\{ \begin{bmatrix} xy+1 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} x^2+1 \\ 0 \\ 1 \end{bmatrix}, \begin{bmatrix} x-y \\ x \\ -y \end{bmatrix}, \begin{bmatrix} y^2+1 \\ 1-xy \\ y^2 \end{bmatrix}, \begin{bmatrix} 0 \\ -x^2-1 \\ xy+1 \end{bmatrix} \right\}$$

Notice that the first row of G contains a Gröbner basis for $\langle F \rangle$ and the remaining rows express this basis in terms of F. Compare this to Example 1.23.

Finally we show how Gröbner bases for modules can be used to compute an ideal quotient $I : \langle g \rangle$. This technique (from [CT98]) is substantially faster than the method of Section 1.4 because it avoids the construction of $I \cap \langle g \rangle$. By Lemma 1.33 the generators of the intersection are a factor of g larger than those of the quotient.

Lemma 1.56. *Let $R = k[x_1, \ldots, x_n]$, let $g \in R$, and let $I \subseteq R$ be an ideal. If $M = \langle I\mathbf{e_1}, I\mathbf{e_2}, g\,\mathbf{e_1} + \mathbf{e_2} \rangle \subseteq R^2$ then $I : \langle g \rangle = M \cap \mathbf{e_2}$.*

Proof We first show $M \cap \mathbf{e_2} \subseteq I : \langle g \rangle$. Every element $a\,\mathbf{e_1} + b\,\mathbf{e_2} \in M$ satisfies $a - bg \equiv 0 \mod I$ so if $b \in M \cap \mathbf{e_2}$ then $bg \equiv 0 \mod I$ and $b \in I : \langle g \rangle$. Now let $f \in I : \langle g \rangle$. Then $fg \in I$ so $fg = q_1 f_1 + \cdots + q_s f_s$ for some $\{q_i\} \subset R$ and

$$\begin{bmatrix} 0 \\ f \end{bmatrix} = f \begin{bmatrix} g \\ 1 \end{bmatrix} - q_1 \begin{bmatrix} f_1 \\ 0 \end{bmatrix} - q_2 \begin{bmatrix} f_2 \\ 0 \end{bmatrix} - \ \ldots \ - q_s \begin{bmatrix} f_s \\ 0 \end{bmatrix}$$

expresses f as an element of $M \cap \mathbf{e_2}$.

Example 1.57. Let $I = \langle y^2 - x, x^2 - xy \rangle$ and let $g = y$. We use $<_{POT}$ where $<$ is graded-reverse lexicographic order with $x > y$. The module $\langle I\,\mathbf{e_1}, I\,\mathbf{e_2}, y\,\mathbf{e_1} + \mathbf{e_2} \rangle$

is generated by

$$G = \left\{ \begin{bmatrix} y^2 - x \\ 0 \end{bmatrix}, \begin{bmatrix} x^2 - xy \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ y^2 - x \end{bmatrix}, \begin{bmatrix} 0 \\ x^2 - xy \end{bmatrix}, \begin{bmatrix} y \\ 1 \end{bmatrix} \right\}$$

The pairs $\{\mathrm{S}(G_1, G_2), \mathrm{S}(G_3, G_4), \mathrm{S}(G_1, G_5), \mathrm{S}(G_2, G_5)\}$ are the only syzygies which are not identically zero under Definition 1.52. However $\mathrm{S}(G_1, G_2)$ and $\mathrm{S}(G_3, G_4)$ must reduce to zero since $\{y^2 - x, x^2 - xy\}$ is a Gröbner basis for I with respect to $<$. Thus we compute

$$\begin{aligned} \mathrm{S}(G_1, G_5) &= (y^2 - x)\,\mathbf{e_1} - y(y\,\mathbf{e_1} + \mathbf{e_2}) &&= -x\,\mathbf{e_1} - y\,\mathbf{e_2} \\ \mathrm{S}(G_2, G_5) &= y(x^2 - xy)\,\mathbf{e_1} - x^2(y\,\mathbf{e_1} + \mathbf{e_2}) &&= -xy^2\,\mathbf{e_1} - x^2\,\mathbf{e_2} \end{aligned}$$

The first syzygy doesn't reduce so it is added to the basis as G_6. The second reduces to $(-xy + x)\,\mathbf{e_2}$ following the steps below.

$$\begin{aligned} -xy^2\,\mathbf{e_1} - x^2\,\mathbf{e_2} &\xrightarrow{+xG_1} -x^2\,\mathbf{e_1} - x^2\,\mathbf{e_2} \\ &\xrightarrow{+xG_2} -xy\,\mathbf{e_1} - x^2\,\mathbf{e_2} \\ &\xrightarrow{+xG_5} (-x^2 + x)\mathbf{e_2} \\ &\xrightarrow{+G_4} (-xy + x)\mathbf{e_2} \end{aligned}$$

So $(-xy + x)\,\mathbf{e_2}$ is added to the basis as G_7. The remaining syzygies all reduce to zero so G is a Gröbner basis for $\langle I\,\mathbf{e_1}, I\,\mathbf{e_2}, y\,\mathbf{e_1} + \mathbf{e_2} \rangle$ with respect to $<_{POT}$. In vector form the elements of G are

$$\begin{bmatrix} y^2 - x \\ 0 \end{bmatrix}, \begin{bmatrix} x^2 - xy \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ y^2 - x \end{bmatrix}, \begin{bmatrix} 0 \\ x^2 - xy \end{bmatrix}, \begin{bmatrix} y \\ 1 \end{bmatrix}, \begin{bmatrix} -x \\ -y \end{bmatrix}, \begin{bmatrix} 0 \\ -xy + x \end{bmatrix}$$

Then $I : \langle g \rangle = G \cap \mathbf{e_2} = \langle y^2 - x, x^2 - xy, -xy + x \rangle$, which is also a Gröbner basis with respect to $<$.

Chapter 2

Quotient Rings

2.1 Arithmetic in $k[x_1, \ldots, x_n]/I$

Recall Theorem 1.16 and Corollary 1.17; using Algorithm 1.13 and a Gröbner basis for I we can simplify polynomials to a unique representative of their equivalence class modulo I. Thus we can add and multiply in $k[x_1, \ldots, x_n]/I$ using the operations of $k[x_1, \ldots, x_n]$, reducing to a canonical form as desired.

Example 2.1. Let $I = \langle x^2 + y, y^2 + 1 \rangle$. We use graded lexicographic order with $x > y$. Observe that the generators of I are already a Gröbner basis since $\mathrm{S}(x^2 + y, y^2 + 1) = y^2(x^2 + y) - x^2(y^2 + 1) = y^3 - x^2$ reduces to zero. Let $f = xy + 1$ and let $g = x + y$. Then $f + g = xy + x + y + 1$ and

$$\begin{aligned} fg &= x^2y + xy^2 + x + y \\ &\equiv (-y)y + x(-1) + x + y \mod I \\ &\equiv y + 1 \mod I \end{aligned}$$

Our first interesting task is the computation of inverses in $k[x_1, \ldots, x_n]/I$. This method is from §6.1 of [BW93]. Let f be an element of $k[x_1, \ldots, x_n]/I$. Then f is invertible if and only if there exists an $f^{-1} \in k[x_1, \ldots, x_n]$ with $ff^{-1} \equiv 1 \mod I$, or equivalently $1 = ff^{-1} + h$ for some $h \in I$.

The key observation is that this is equivalent to $1 \in \langle f \rangle + I \subseteq k[x_1, \ldots, x_n]$, where $\langle f \rangle + I$ is the ideal generated by f together with the generators of I. Then $\{1\}$ is a reduced Gröbner basis for $\langle f \rangle + I$ and we can compute the inverse using the extended Buchberger algorithm of Section 1.3.

Example 2.2. Let $I = \langle x^2 + y, y^2 + 1 \rangle$ and let $f = x$. To compute the inverse of f modulo I we run the extended Buchberger algorithm on $\langle x, x^2 + y, y^2 + 1 \rangle$ using graded lexicographic order with $x > y$. We assign vectors $[1, 0, 0]$, $[0, 1, 0]$, and $[0, 0, 1]$ to x, $x^2 + y$, and $y^2 + 1$, respectively, and compute the syzygies

$$\begin{aligned} \mathrm{S}(x, x^2 + y) &= x(x) - 1(x^2 + y) &&= -y \quad \text{assigned} \quad [x, -1, 0] \\ \mathrm{S}(-y, y^2 + 1) &= y(-y) + 1(y^2 + 1) = 1 && \text{assigned} \quad [xy, -y, 1] \end{aligned}$$

Then $1 = (xy)(x) + (-y)(x^2 + y) + 1(y^2 + 1)$. Since $x^2 + y$ and $y^2 + 1$ are in I $1 \equiv (xy)(x) \mod I$ and $x^{-1} = xy \mod I$.

2.2 Polynomial Division

We can extend the method of computing inverses in $k[x_1, \ldots, x_n]/I$ to describe polynomial division modulo I in general. Once again we exploit the connection between representatives $f \in k[x_1, \ldots, x_n]/I$ and ideals $\langle f \rangle + I \subseteq k[x_1, \ldots, x_n]$,

which we denote by $\langle f, I \rangle$. Our approach is based on two lemmas.

Lemma 2.3. *Let f be a polynomial and let I be an ideal. If $\{g_1, \ldots, g_t\}$ is a Gröbner basis for $\langle f, I \rangle$ then there exist $q_i \in k[x_1, \ldots, x_n]$ with $g_i \equiv q_i f \mod I$.*

Proof The statement is actually trivial, but our goal is to compute the q_i. Let $I = \langle h_1, \ldots, h_s \rangle$. From the extended Buchberger algorithm we obtain quotients expressing each g_i in terms of $\{f, h_1, \ldots, h_s\}$, i.e.:

$$g_i = q_{i0} f + q_{i1} h_1 + q_{i2} h_2 + \ldots q_{is} h_s$$

Since all of the h_i are equivalent to zero we have $g_i \equiv q_{i0} f \mod I$. □

Example 2.4. Let $f = xy + 1$ and let $I = \langle x^2 + 1 \rangle \subset \mathbb{Q}[x, y]$. In Example 1.23 we computed a Gröbner basis for $\langle f, I \rangle$ using lexicographic order with $x > y$. We obtained the basis $\{xy + 1, x^2 + 1, x - y, y^2 + 1\}$ and the relations

$$\begin{aligned} xy + 1 &= 1\,(xy + 1) + 0\,(x^2 + 1) \\ x^2 + 1 &= 0\,(xy + 1) + 1\,(x^2 + 1) \\ x - y &= x\,(xy + 1) - y\,(x^2 + 1) \\ y^2 + 1 &= (1 - xy)\,(xy + 1) + y^2\,(x^2 + 1) \end{aligned}$$

Then $x - y \equiv xf \mod I$ and $y^2 + 1 \equiv (1 - xy)f \mod I$.

Example 2.5. We illustrate how to do the computation of Lemma 2.3 using Gröbner bases for modules. Let $<$ be a monomial order and let $I = \langle h_1, \ldots, h_s \rangle$.

If we compute a Gröbner basis for the module

$$M = \left\langle \begin{bmatrix} h_1 \\ 0 \end{bmatrix}, \ldots, \begin{bmatrix} h_s \\ 0 \end{bmatrix}, \begin{bmatrix} f \\ 1 \end{bmatrix} \right\rangle$$

using $<_{POT}$ we will obtain a Gröbner basis for $\langle f, I \rangle$ in the first coordinate. The second coordinate must contain the desired relations $\{q_i\}$, because every element $[a, b] \in M$ satisfies $a \equiv bf \mod I$.

Lemma 2.6. *Let f and g be elements of $k[x_1, \ldots, x_n]/I$ and suppose $g \in \langle f, I \rangle$. Then there exists some $q \in k[x_1, \ldots, x_n]$ with $g \equiv qf \mod I$, and we say that f divides g in $k[x_1, \ldots, x_n]/I$.*

Proof Let $G = \{g_1, \ldots, g_t\}$ be a Gröbner basis for $\langle f, I \rangle$ with respect to some monomial order. Then $g \div G \to 0$ using Algorithm 1.13 and we obtain a set of quotients $\{c_i\}$ with $g = \sum_{i=1}^{t} c_i g_i$. Let $\{q_1, \ldots, q_s\}$ be the polynomials from Lemma 2.3 with $g_i \equiv q_i f \mod I$. Then $g \equiv (\sum_{i=1}^{t} c_i q_i) f \mod I$. □

Example 2.7. Let $g = 4sc^2 - s - 4c^2 + 2$ and $f = 2s - 1$ in $\mathbb{Q}[s, c]/\langle s^2 + c^2 - 1 \rangle$. We will divide g by f using lexicographic order with $s > c$. Our first task is to compute a Gröbner basis for $\langle f, I \rangle$ expressed in terms of f and $s^2 + c^2 - 1$. From the extended Buchberger algorithm (see Example 1.23) we obtain the basis $\{4c^2 - 3, f\}$ and the relation

$$4c^2 - 3 = (-2s - 1)f + 4(s^2 + c^2 - 1)$$

Next we apply Algorithm 1.13 to write g in terms of this basis.

$$g = (s - 1)(4c^2 - 3) + (1)(f)$$

Since the normal form of g is zero, we know that f divides g modulo I. We substitute for $4c^2 - 3$ to obtain

$$\begin{aligned} g &\equiv (s-1)(-2s-1)f + f \mod I \\ &\equiv (-2s^2 + s + 2)f \mod I \end{aligned}$$

The quotient $-2s^2 + s + 2$ is not reduced modulo I. It reduces to $s + 2c^2$.

Note that f divides g modulo I if and only if $\langle g, I\rangle \subseteq \langle f, I\rangle$. We say that f is a *proper divisor* of g if $\langle f, I\rangle$ is proper and the containment is strict. A natural question to ask is whether this also implies $\deg(g) > \deg(f)$. As we will see in the next example, the somewhat suprising answer is *no*.

Example 2.8. Let $f = xy^3 + x + 1$ and let $I = \langle xy^5 - x - y\rangle$. We use graded lexicographic order with $x > y$. The element $y^2 f \equiv xy^2 + y^2 + x + y \mod I$ has total degree three, however $\langle y^2 f, I\rangle \subset \langle f, I\rangle \subset \mathbb{Q}[x, y]$ strictly.

From the examples in this section we see that when f divides g we can not say anything about the degree of the quotient. However, if f, g, and I are all homogeneous then we have the following result.

Lemma 2.9. *Let I be a homogeneous prime ideal and let f and g be homogeneous polynomials with $g \notin I$. If $g \equiv qf \mod I$ then the normal form of q with respect to any monomial order is also homogeneous with degree* $\deg(g) - \deg(f)$.

Proof Let $q = q_1 + q_2$ where q_1 consists of precisely the terms of degree $\deg(g) - \deg(f)$. Then $g - q_1 f - q_2 f \equiv 0 \mod I$ implies $q_2 f \equiv 0 \mod I$ since

the terms of $q_2 f$ can not be cancelled by any terms of $g - q_1 f$. Finally I prime and $f \notin I$ implies $q_2 \in I$, so the normal form of q is equal to the normal form of q_1. This is homogeneous with degree $\deg(g) - \deg(f)$ by Lemma 1.36. □

Example 2.10. In general the requirement that I is prime in Lemma 2.9 can not be dropped. Let $I = \langle (x-y)(x^2+y^2) \rangle$, $f = x^2 + y^2$ and $q = x^2 + x - y$. Then q is reduced modulo I but $g = x^2y^2 + y^4 \equiv qf \mod I$. It is true that there exist homogeneous q with $g \equiv qf \mod I$ and $\deg(q) = \deg(g) - \deg(f)$. For instance, $q = x^2$ or $q = y^2$ in this example.

2.3 Rational Expressions I

Finally we consider the problem of rational expression simplification over $k[x_1, \ldots, x_n]/I$. Our goal is simple: given a fraction a/b compute c/d with $ad \equiv bc \mod I$ and $\deg(c) + \deg(d)$ minimal. In this section we show how to construct equivalent fractions using the ideal quotient operation. We will assume that I is prime.

We proceed as follows. Let $c \notin I$ be an element of $\langle a, I \rangle : \langle b \rangle$. Then $bc \in \langle a, I \rangle$ by Definition 1.29 so a divides bc in $k[x_1, \ldots, x_n]/I$. If d is the quotient from Lemma 2.6 then $bc \equiv ad \mod I$ and a/b is equivalent to c/d. Our first lemma shows that every equivalent fraction can be obtained in this way.

Lemma 2.11. *If* $a/b \equiv c/d \mod I$ *then* $c \in \langle a, I \rangle : \langle b \rangle$ *and* $d \in \langle b, I \rangle : \langle a \rangle$.

Proof It suffices to show $bc \in \langle a, I\rangle$ and $ad \in \langle b, I\rangle$. Since $bc \equiv ad \mod I$ we have $bc = ad + h$ for some $h \in I$, and the right hand side expresses bc as an element of $\langle a, I\rangle$. Likewise $ad = bc - h$ expresses ad as an element of $\langle b, I\rangle$. □

Example 2.12. We illustrate with an example from [Mul01]. Consider

$$\frac{sc - c^2 + s + 1}{c^4 - 2c^2 + s + 1} \quad \text{over} \quad \mathbb{Q}[s, c]/\langle s^2 + c^2 - 1\rangle$$

We first compute $\langle sc - c^2 + s + 1, s^2 + c^2 - 1\rangle : \langle c^4 - 2c^2 + s + 1\rangle = \langle s, c + 1\rangle$ using Lemmas 1.27 and 1.33 or alternatively Lemma 1.56. Our numerator is chosen from this ideal, so we pick $s + c + 1$ following [Mul01]. Next we divide $(s + c + 1)(c^4 - 2c^2 + s + 1)$ by $sc - c^2 + s + 1$ modulo $\langle s^2 + c^2 - 1\rangle$ and obtain the quotient $s - sc^2 + 1$ from Lemma 2.6. Then

$$\frac{sc - c^2 + s + 1}{c^4 - 2c^2 + s + 1} \to \frac{s + c + 1}{s - sc^2 + 1} \mod \langle s^2 + c^2 - 1\rangle$$

Of course it was not necessary to choose the numerator $s + c + 1$, we can choose any $f \in \langle s, c + 1\rangle$ which is not a multiple $s^2 + c^2 - 1$. The following fractions were obtained from choosing $f = s$ and $f = c + 1$ respectively:

$$\frac{-2s}{sc^2 - c^3 - sc - s + 2c - 1} \qquad \frac{-2(c + 1)}{sc^2 + c^3 + sc - s - 2c - 1}$$

Example 2.13. To better understand the method we examine it in a more familiar setting. Let $a, b \in k[x]$ and let $I = \langle 0\rangle$. Then $\langle a, I\rangle : \langle b\rangle = \langle a/\gcd(a, b)\rangle$ (see Example 1.31) and choosing $c = a/\gcd(a, b)$ we obtain the denominator $d = bc/a = b/\gcd(a, b)$, effectively cancelling a greatest common divisor.

Monagan and Mulholland observed that fractions over $\mathbb{Q}[s, c]/\langle s^2 + c^2 - 1\rangle$ can be simplified in a way that does not correspond to the cancellation of a

common divisor [Mul01]. This phenomenon actually occurs quite frequently in general, as in the following example.

Example 2.14. Let $a = y^5+x+y$, $b = x-y$, and $I = \langle xy^5-x-y\rangle \subset \mathbb{Q}[x,y]$. We simplify $a/b \mod I$ using graded lexicographic order with $x > y$. A Gröbner basis for $\langle a, I\rangle : \langle b\rangle$ is $\{x^2+xy+x+y, y^5+x+y, xy^4+y^4\}$, and if we select $c = x^2+xy+x+y$ we obtain $d = x^2-xy$ from Lemma 2.6. Then

$$\frac{y^5+x+y}{x-y} \to \frac{x^2+xy+x+y}{x^2-xy} \mod \langle xy^5-x-y\rangle$$

We show that c does not divide a and d does not divide b in $\mathbb{Q}[x,y]/I$. A Gröbner basis for $\langle c, I\rangle$ is $\{x^2+xy+x+y, y^6+xy+y^2, xy^5-x-y\}$, and by examining the leading terms we see that $a \notin \langle c, I\rangle$. Likewise a Gröbner basis for $\langle d, I\rangle$ is $\{xy-y^2, x^2-y^2, y^6-x-y\}$ and it is easy to see that $b \notin \langle d, I\rangle$.

So why does this happen? Notice how we have used a correspondence between ideals $J \subseteq k[x_1,\ldots,x_n]/I$ and ideals $J+I \subseteq k[x_1,\ldots,x_n]$. See §5.2 of [Cox96] for more details. By Lemma 1.32 $\langle a, I\rangle : \langle b\rangle = \langle a, I\rangle : \langle b, I\rangle$ so our method computes $\langle a\rangle : \langle b\rangle$ in $k[x_1,\ldots,x_n]/I$. We make two remarks. First, although we started with principal ideals $\langle a\rangle$ and $\langle b\rangle$ in $k[x_1,\ldots,x_n]/I$ we have no guarantee that their quotient is principal. Second, even if it were and $\langle a\rangle : \langle b\rangle = \langle f\rangle$, extracting f from a basis of $\langle f, I\rangle$ is a non-trivial problem. Thus we should expect to find $c \in \langle a, I\rangle : \langle b\rangle$ with $\langle a, I\rangle \not\subseteq \langle c, I\rangle$, producing the situation above.

So far we have simplified fractions a/b by choosing a numerator $c \in \langle a, I\rangle : \langle b\rangle$ with minimal total degree. However this strategy may not produce c/d with $\deg(c) + \deg(d)$ minimal, as illustrated in the next example.

Example 2.15. Consider Example 2.14 again, only this time we will attempt to simplify b/a. A Gröbner basis for $\langle b, I\rangle : \langle a\rangle$ is $\{x - y, y^5 - 2\}$, so choosing a numerator of minimal degree simply reconstructs the original fraction. This fraction has total degree six, however in Example 2.14 we constructed one with total degree four.

We mention one important case where choosing a numerator with minimal degree does produce a fraction with minimal degree.

Theorem 2.16. *Let I be a homogeneous prime ideal and suppose $a, b \notin I$ are homogeneous polynomials. Let G be a reduced Gröbner basis for $\langle a, I\rangle : \langle b\rangle$ with respect to a graded monomial order $<$. If we choose $c \in G$, $c \notin I$ with* $\deg(c)$ *minimal and compute $d = bc/a \mod I$, then c/d is equivalent to a/b and* $\deg(c) + \deg(d)$ *is minimal.*

Proof Observe that c is homogeneous by Lemma 1.37 and d is homogeneous with degree $\deg(b)+\deg(c)-\deg(a)$ by Lemma 2.9. Now since $a \notin I$ the normal form of a has degree $\deg(a)$ by Lemma 1.36, so any homogeneous $a' \equiv a \mod I$ has $\deg(a') = \deg(a)$. Similarly for b, so that $\deg(a)$ and $\deg(b)$ are fixed. Then $\deg(c)$ minimal implies $\deg(d) = \deg(b) + \deg(c) - \deg(a)$ is minimal as well.

Example 2.17. Let $a = x^3 + x^2y$, $b = 2xy + y^2$, and let $I = \langle x^3 + xy^2 + y^3\rangle$. We use graded lexicographic order with $x > y$. A Gröbner basis for $\langle a, I\rangle : \langle b\rangle$ is $\{xy, x^2 - y^2, y^3\}$, so if we let $c = xy$ and compute $d = b\,c/a \equiv -x + y \mod I$

using Lemma 2.6 then

$$\frac{x^3+x^2y}{2xy+y^2} \rightarrow \frac{xy}{-x+y} \mod I$$

Alternatively, we could choose $c = x^2 - y^2$ and compute $d = x + 2y$ so that

$$\frac{x^3+x^2y}{2xy+y^2} \rightarrow \frac{x^2-y^2}{x+2y} \mod I$$

Similarly, a Gröbner basis for $\langle b, I\rangle : \langle a\rangle$ is $\{y, x\}$. If we choose $d = y$ then we obtain $c = (x^2 + xy - y^2)/3$ and

$$\frac{x^3+x^2y}{2xy+y^2} \rightarrow \frac{x^2+xy-y^2}{3y} \mod I$$

Finally if $d = x$ then $c = (x^2 - 2xy - y^2)/3$ and

$$\frac{x^3+x^2y}{2xy+y^2} \rightarrow \frac{x^2-2xy-y^2}{3x} \mod I$$

Example 2.18. We homogenize Example 2.14 using a new variable z and graded reverse lexicographic order with $x > y > z$. Our goal is to simplify

$$\frac{y^5+xz^4+yz^4}{x-y} \mod \langle xy^5 - xz^5 - yz^5\rangle$$

A Gröbner basis for the quotient $\langle y^5 + xz^4 + yz^4, xy^5 - xz^5 - yz^5\rangle : \langle x - y\rangle$ is $\{y^5+xz^4+yz^4, x^2z^4+xyz^4+xz^5+yz^5, xy^4z^4+y^4z^5\}$, indicating that the original fraction has minimal total degree. This is in sharp contrast to Example 2.14, and it suggests that there is little hope of using homogenization to extend Theorem 2.16 to non-homogeneous problems.

2.4 Rational Expressions II

In this section we will use Gröbner bases for modules to reduce fractions over $k[x_1, \ldots, x_n]/I$ to a minimal canonical form. The result is analogous to

the normal form for ordinary polynomials produced by Theorem 1.16. Observe that if a/b is a fraction over $k[x_1, \ldots, x_n]/I$ then the set of pairs $[x, y]$ satisfying $bx - ay \equiv 0 \mod I$ is a module over $k[x_1, \ldots, x_n]$.

Lemma 2.19. *Let $I = \langle h_1, \ldots, h_s \rangle$ be a prime ideal and let a/b be a fraction over $k[x_1, \ldots, x_n]/I$. If $\langle a, I \rangle : \langle b \rangle = \langle c_1, \ldots, c_t \rangle$ and $d_i = bc_i/a \mod I$ then*

$$\left\{ \begin{bmatrix} c_1 \\ d_1 \end{bmatrix}, \ldots, \begin{bmatrix} c_t \\ d_t \end{bmatrix}, \begin{bmatrix} 0 \\ h_1 \end{bmatrix}, \ldots, \begin{bmatrix} 0 \\ h_s \end{bmatrix} \right\}$$

generates $M = \{[x, y] : bx - ay \equiv 0 \mod I\}$ as a $k[x_1, \ldots, x_n]$-module.

Proof By construction, the generators above all satisfy $bx - ay \equiv 0 \mod I$. Let $[f, g] \in M$. By Lemma 2.11 $f \in \langle c_1, \ldots, c_t \rangle$ so $f = p_1 c_1 + \cdots + p_t c_t$ for some $p_i \in k[x_1, \ldots, x_n]$. Then

$$a(g - (p_1 d_1 + \cdots + p_t d_t)) \equiv b(f - (p_1 c_1 + \cdots + p_t c_t)) \equiv 0 \mod I$$

and since I is prime $g - (p_1 d_1 + \cdots + p_t d_t) \equiv 0 \mod I$. Then there exist $q_i \in k[x_1, \ldots, x_n]$ with

$$g - (p_1 d_1 + \cdots + p_t d_t) = q_1 h_1 + \cdots + q_s h_s$$

$$\text{and } \begin{bmatrix} f \\ g \end{bmatrix} = p_1 \begin{bmatrix} c_1 \\ d_1 \end{bmatrix} + \cdots + p_t \begin{bmatrix} c_t \\ d_t \end{bmatrix} + q_1 \begin{bmatrix} 0 \\ h_1 \end{bmatrix} + \cdots + q_s \begin{bmatrix} 0 \\ h_s \end{bmatrix}. \quad \square$$

Our approach is to compute a reduced Gröbner basis for this module using a term over position monomial order. Then we will select the smallest $[c, d]$ under the module order with $c, d \notin I$ to be our simplified fraction. This minimizes the largest monomial appearing in c/d under the original monomial order. We call

this monomial the *leading monomial* of c/d.

Example 2.20. We repeat Example 2.15 using this new method. Let $a = x-y$ and $b = y^5+x+y$, and consider a/b modulo $I = \langle xy^5-x-y\rangle$. We let $<$ be graded lexicograpghic order with $x > y$. A Gröbner basis for $\langle a, I\rangle : \langle b\rangle$ is $\{x-y, y^5-2\}$ and from Lemma 2.6 we obtain the denominators $\{y^5+x+y, -y^9-y^5+y^4\}$. We construct the module

$$\left\langle \begin{bmatrix} x-y \\ y^5+x+y \end{bmatrix}, \begin{bmatrix} y^5-2 \\ -y^9-y^5+y^4 \end{bmatrix}, \begin{bmatrix} 0 \\ xy^5-x-y \end{bmatrix} \right\rangle$$

and compute a Gröbner basis using $<_{TOP}$

$$\left\{ \begin{bmatrix} x^2-xy \\ x^2+xy+x+y \end{bmatrix}, \begin{bmatrix} x-y \\ y^5+x+y \end{bmatrix}, \begin{bmatrix} xy^4-2 \\ xy^4+y^4 \end{bmatrix} \right\}$$

The elements of this basis are all valid fractions because their numerators and denominators are not in I. We conclude that $(x^2-xy)/(x^2+xy+x+y)$ has the smallest leading monomial among all fractions equivalent to a/b.

Example 2.21. We repeat Example 2.12 where the goal was to simplify

$$\frac{sc-c^2+s+1}{c^4-2c^2+s+1} \mod I = \langle s^2+c^2-1\rangle$$

We use graded lexicographic order with $s > c$. A reduced Gröbner basis for $\langle sc-c^2+s+1, s^2+c^2-1\rangle : \langle c^4-2c^2+s+1\rangle$ is $\{s, c+1\}$, so the module is generated by $[s, -\frac{1}{2}(sc^2-c^3-sc-s+2c-1)]$, $[c+1, -\frac{1}{2}(sc^2+c^3+sc-s-2c-1)]$, and $[0, s^2+c^2-1]$. Note that the first two elements are the fractions constructed for s and $c+1$ at the end of Example 2.12. A Gröbner basis for the module is

$$\left\{ \begin{bmatrix} 0 \\ s^2+c^2-1 \end{bmatrix}, \begin{bmatrix} s^2+c^2-1 \\ 0 \end{bmatrix}, \begin{bmatrix} s-c-1 \\ c^3+sc-2c \end{bmatrix}, \begin{bmatrix} -s-c-1 \\ sc^2-s-1 \end{bmatrix} \right\}$$

so $(s-c-1)/(c^3+sc-2c)$ has a minimal leading monomial with respect to $<$.

Unfortunately having a minimal leading monomial does not guarantee that the fraction itself has minimal total degree, even when a graded order is used.

Example 2.22. Let $I = \langle x^5+xy-1\rangle$, $a = x^3y^3-x^4+x-1$, and $b = x^2-y^2+1$. We use graded lexicographic order with $x > y$. A Gröbner basis for the module of Lemma 2.19 with respect to $<_{TOP}$ is

$$\left\{ \begin{bmatrix} xy^4-x^3-x^2y-y^3+x^2+x \\ -x^4+x^2y^2-x^2 \end{bmatrix}, \begin{bmatrix} 0 \\ x^5+xy-1 \end{bmatrix}, \begin{bmatrix} x^5+xy-1 \\ 0 \end{bmatrix}, \right.$$
$$\left. \begin{bmatrix} x^3y^3-x^4+x-1 \\ x^2-y^2+1 \end{bmatrix}, \begin{bmatrix} -x^2y^3+x^4+x^3+y-1 \\ x^4y^2-x^4+y^3-x-y \end{bmatrix} \right\}$$

The first element has the smallest leading term, however its numerator is degree five and its denominator is degree four. This compares poorly with the original fraction, which has degrees six and two, respectively.

Another possible objection to this method is that it does not detect when the denominator is invertible or when it divides the numerator. In those cases we might prefer to get a polynomial of higher degree instead of a fraction.

Example 2.23. Let $I = \langle xy^2-1\rangle$ and consider the fraction $(x+1)/x^2$. One can easily verify that $x^2y^4 \equiv 1 \mod I$ so that the inverse of x^2 is y^4. Then $(x+1)/x^2 \equiv (x+1)y^4 \mod I$ which reduces to y^4+y^2. However, we will

compute $\langle x+1, xy^2-1\rangle : \langle x^2\rangle = \langle x+1, y^2+1\rangle$ and construct the module

$$\left\langle \begin{bmatrix} x+1 \\ x^2 \end{bmatrix}, \begin{bmatrix} y^2+1 \\ x \end{bmatrix}, \begin{bmatrix} 0 \\ xy^2-1 \end{bmatrix} \right\rangle$$

whose generators are already a Gröbner basis with respect to term over position graded lexicographic order with $x > y$. The smallest valid fraction is $(y^2+1)/x$.

At this point we need to offer a solution. One possibility is to minimize the leading term of the denominator rather than the largest term in the entire fraction. This computation does not require modules at all. To simplify a/b modulo I one can simply choose $d \in \langle b, I\rangle : \langle a\rangle$, $d \notin I$ minimal and compute $c \equiv ad/b \mod I$, inverting the method of Section 2.3. Whenever b is invertible or b divides a modulo I we will obtain $d = 1$ and $c \equiv a/b \mod I$.

An alternative solution is to adapt the method of this section to detect this case and deal with it at no extra cost. We can invert Lemma 2.19 so that we compute $\langle b, I\rangle : \langle a\rangle = \langle d_1, \ldots, d_t\rangle$ and $c_i = ad_i/b \mod I$. If b is invertible or if b divides a modulo I we will obtain $\langle b, I\rangle : \langle a\rangle = \langle 1\rangle$ and $c_1 = a/b \mod I$. Otherwise we can proceed with the computation for modules. As a pleasant side effect we can extend Lemma 2.19 to the case where I is not prime.

Lemma 2.24. *Let $I = \langle h_1, \ldots, h_s\rangle$ be an ideal and let a/b be a fraction over $k[x_1, \ldots, x_n]/I$ where b is not a zero-divisor. If $\langle b, I\rangle : \langle a\rangle = \langle d_1, \ldots, d_t\rangle$ and $c_i = ad_i/b \mod I$ then*

$$\left\{ \begin{bmatrix} c_1 \\ d_1 \end{bmatrix}, \ldots, \begin{bmatrix} c_t \\ d_t \end{bmatrix}, \begin{bmatrix} h_1 \\ 0 \end{bmatrix}, \ldots, \begin{bmatrix} h_s \\ 0 \end{bmatrix} \right\}$$

generates $M = \{[x, y] : bx - ay \equiv 0 \mod I\}$ *as a* $k[x_1, \ldots, x_n]$*-module.*

Proof Again by construction, all of the generators satisfy $bx - ay \equiv 0 \mod I$. Let $[f, g] \in M$. By Lemma 2.11 $g \in \langle d_1, \ldots, d_t \rangle$ so $g = p_1 d_1 + \cdots + p_t d_t$ for some $p_i \in k[x_1, \ldots, x_n]$. Then

$$b(f - (p_1 c_1 + \cdots + p_t c_t)) \equiv a(g - (p_1 d_1 + \cdots + p_t d_t)) \equiv 0 \mod I$$

and since b is not a zero-divisor $f - (p_1 c_1 + \cdots + p_t c_t) \equiv 0 \mod I$. Then there exist $q_i \in k[x_1, \ldots, x_n]$ with

$$f - (p_1 c_1 + \cdots + p_t c_t) = q_1 h_1 + \cdots + q_s h_s$$

$$\text{and } \begin{bmatrix} f \\ g \end{bmatrix} = p_1 \begin{bmatrix} c_1 \\ d_1 \end{bmatrix} + \cdots + p_t \begin{bmatrix} c_t \\ d_t \end{bmatrix} + q_1 \begin{bmatrix} h_1 \\ 0 \end{bmatrix} + \cdots + q_s \begin{bmatrix} h_s \\ 0 \end{bmatrix}. \quad \square$$

Example 2.25. Let $a = 4sc^2 - s - 4c^2 + 2$ and $b = 2s - 1$ in $\mathbb{Q}[s, c]/\langle s^2 + c^2 - 1 \rangle$ from Example 2.7. We will simplify a/b using lexicographic order with $s > c$. We first compute a Gröbner basis for $\langle b, I \rangle : \langle a \rangle = \langle 1 \rangle$ using Lemma 1.56. This indicates that b divides a modulo I, so we take 1 to be the denominator and compute $s + 2c^2 \equiv a/b \mod I$.

We present this modified method in the form of an algorithm, which computes a reduced canonical form for a fraction over $k[x_1, \ldots, x_n]/I$ with respect to a given monomial order. The total degree of the output may not be minimal, however the monomials which appear will be as small as possible under the ordering. As a corollary, the algorithm must cancel any common divisor.

Algorithm 2.26 (Rational Expression Normal Form).

Input $I = \langle h_1, \ldots, h_s \rangle$ a prime ideal of $k[x_1, \ldots, x_n]$,
a/b with $a, b \notin I$, and a monomial order $<$

Output (optionally) a quotient $c = a/b$ if b divides a modulo I
c/d with $ad \equiv bc \mod I$, c and d are reduced, and the
largest monomial in c/d minimal with respect to $<$

$\{d_1, \ldots, d_t\} \leftarrow$ a reduced Gröbner basis for $\langle b, I \rangle : \langle a \rangle$ (Lemma 1.56)

$\{c_1, \ldots, c_t\} \leftarrow$ the quotients $ad_i/b \mod I$ (Lemma 2.6)

(optional) **if** $\{d_1, \ldots, d_t\} = \{1\}$ then **return** the normal form of c_1

$M \leftarrow$ the module $\langle [c_1, d_1], \ldots, [c_t, d_t], [h_1, 0], \ldots, [h_s, 0] \rangle$

$G \leftarrow$ a reduced Gröbner basis for M with respect to $<_{TOP}$

return the smallest $[f, g] \in G$ with respect to $<_{TOP}$ with $f, g \notin I$

Additional examples are given in the appendix. We will conclude this section with a remark on the difficulties of extending this method to work with fractions over non-integral domains. Lemma 2.24 poses no problem, however we must be careful that in simplifying $a/b \rightarrow c/d$ we do not choose d to be a zero-divisor.

Lemma 2.27. *$f \notin I$ is a zero-divisor modulo I if and only if $I : \langle f \rangle \not\subseteq I$.*

Proof Let f be a zero-divisor modulo I. Then $fq \in I$ for some $q \notin I$ and $q \in I : \langle f \rangle$. Now let $I : \langle f \rangle = \langle q_1, \ldots, q_s \rangle \not\subseteq I$. Then some $q_i \notin I$ but $fq_i \in I$ by Definition 1.29.

Observe that we can test for zero-divisors efficiently using Lemma 1.56. To compute $I : \langle f \rangle$, we will compute a Gröbner basis for $M = \langle I\,\mathbf{e_1}, I\,\mathbf{e_2}, f\,\mathbf{e_1} + \mathbf{e_2} \rangle$

using a position over term monomial order $<_{POT}$. However, if the generators for I are a Gröbner basis with respect to $<$ then we can identify zero-divisors by a remainder r with leading monomial in $\mathbf{e_2}$ being added to the basis for M.

Example 2.28. Let $I = \langle x^2 - y, y^2 - x, xy - 1\rangle$ and $f = x + y + 1$. Let $<$ denote graded lexicographic order with $x > y$, since the generators of I are already a Gröbner basis with respect to that order. A Gröbner basis for the module $\langle I\,\mathbf{e_1}, I\,\mathbf{e_2}, f\,\mathbf{e_1} + \mathbf{e_2}\rangle$ with respect to $<_{POT}$ is

$$\left\{\begin{bmatrix} 0 \\ y-1 \end{bmatrix}, \begin{bmatrix} 0 \\ x-1 \end{bmatrix}, \begin{bmatrix} x+y+1 \\ 1 \end{bmatrix}, \begin{bmatrix} y^2+y+1 \\ 1 \end{bmatrix}\right\}$$

We can see by inspection that $I : \langle f\rangle = \langle y-1, x-1\rangle \not\subseteq I$ so f is a zero-divisor. One might also note that $I = \langle y-1, x-1\rangle \cap \langle x+y+1, y^2+y+1\rangle$, where the generating sets are Gröbner bases with respect to $<$.

Although we can detect zero-divisors in the denominator using Lemma 2.27, it is not at all clear what our algorithm should do when this actually happens. We leave this as a topic for future research.

2.5 Rational Expressions III

We conclude this chapter with an alternative method for simplifying rational expressions over $k[x_1, \ldots, x_n]/I$ which is guaranteed to produce an expression with minimal total degree. Given a/b with $a, b \notin I$, we will conduct a global search for equivalent expressions with lower total degree. At each step we set c and d to be linear combinations of monomials with undetermined coefficients

and attempt to solve $ad - bc \equiv 0 \mod I$ with $c, d \not\equiv 0 \mod I$. We will use a Gröbner basis for I with respect to a graded monomial order.

Lemma 2.29. *Let $I \subseteq k[x_1, \ldots, x_n]$ be an ideal and let $a, b \in k[x_1, \ldots, x_n]$ with $a, b \notin I$. If $c = \sum_{i=1}^{s} c_i \mathbf{x_i}$ and $d = \sum_{j=1}^{t} d_j \mathbf{x_j}$, where $\mathbf{x_i}$ and $\mathbf{x_j}$ are monomials of $k[x_1, \ldots, x_n]$ and the c_i and d_j are unknowns, then the coefficients of the normal form of $ad - bc \mod I$ with respect to any monomial order are homogeneous linear polynomials in the c_i and d_j.*

Proof The coefficients of bc and ad are multiples of c_i and d_j respectively, so the coefficients of $ad - bc$ are linear and homogeneous in c_i and d_j. Now consider what happens in Algorithm 1.13. In a reduction step we will subtract $p_{new} \leftarrow p - (\mathrm{LT}(p)/\mathrm{LT}(g))\, g$. If p has linear homogeneous coefficients in c_i and d_j then $(\mathrm{LT}(p)/\mathrm{LT}(g))\, g$ and p_{new} will have this property also. Moving $\mathrm{LT}(p)$ to the remainder r retains this property for both p and r, so the coefficients of the remainder are linear and homogeneous in c_i and d_j as well.

Example 2.30. From Example 2.14 let $a = y^5 + x + y$, $b = x - y$, and let $I = \langle xy^5 - x - y \rangle$. We will attempt to construct $c/d \equiv a/b \mod I$ using monomials of up to degree two. Let $c = c_1 + c_2 y + c_3 x + c_4 y^2 + c_5 xy + c_6 x^2$ and $d = d_1 + d_2 y + d_3 x + d_4 y^2 + d_5 xy + d_6 x^2$. The normal form of $ad - bc$ under graded lexicographic order with $x > y$ is

$$\begin{aligned} &d_4 y^7 + d_2 y^6 + d_1 y^5 + (d_6 - c_6)x^3 + (d_5 + d_6 - c_5 + c_6)x^2 y + (c_5 - c_4 + d_4 + d_5)xy^2 \\ &\quad + (d_4 + c_4)y^3 + (d_6 + d_3 - c_3)x^2 + (d_5 + c_3 + d_2 - c_2 + d_6 + d_3)xy \\ &\quad + (d_5 + c_2 + d_2)y^2 + (d_1 - c_1 + d_3)x + (c_1 + d_1 + d_3)y \end{aligned}$$

Equating each coefficient to zero, we obtain a 12×12 system of homogeneous

linear equations with the general solution $c_1 = 0$, $c_2 = t$, $c_3 = t$, $c_4 = 0$, $c_5 = t$, $c_6 = t$, $d_1 = 0$, $d_2 = 0$, $d_3 = 0$, $d_4 = 0$, $d_5 = -t$, $d_6 = t$. For any $t \neq 0$ we can substitute these values into c/d an obtain $(x^2 + xy + x + y)/(x^2 - xy)$.

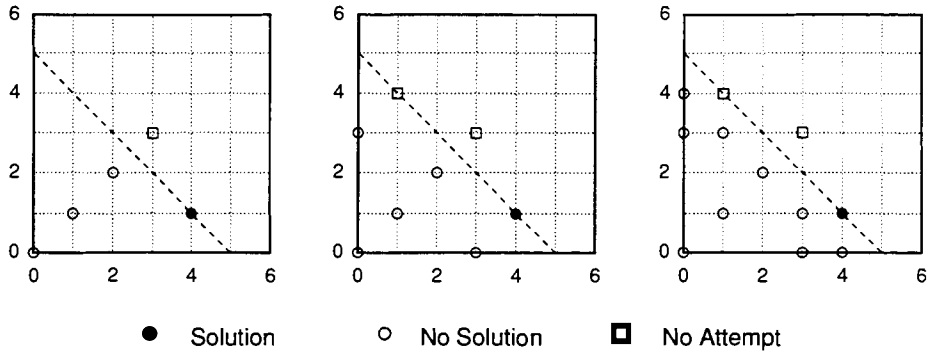
Example 2.31. Let $a/b = y^2/(x^2 - y) \mod I = \langle xy^2 - 1 \rangle$. We will attempt to construct an equivalent fraction c/d wit $\deg(c) = 2$ and $\deg(d) = 1$. Let $c = c_1 + c_2y + c_3x + c_4y^2 + c_5xy + c_6x^2$ and $d = d_1 + d_2y + d_3x$. The normal form of $ad - bc \mod I$ under graded lexicographic order with $x > y$ is

$$-c_6x^4 - c_5x^3y - c_3x^3 + (c_6 - c_2)x^2y + (d_2 + c_4)y^3 - c_1x^2$$
$$+ c_3xy + (d_1 + c_2)y^2 - c_4x + c_1y + (d_3 + c_5)$$

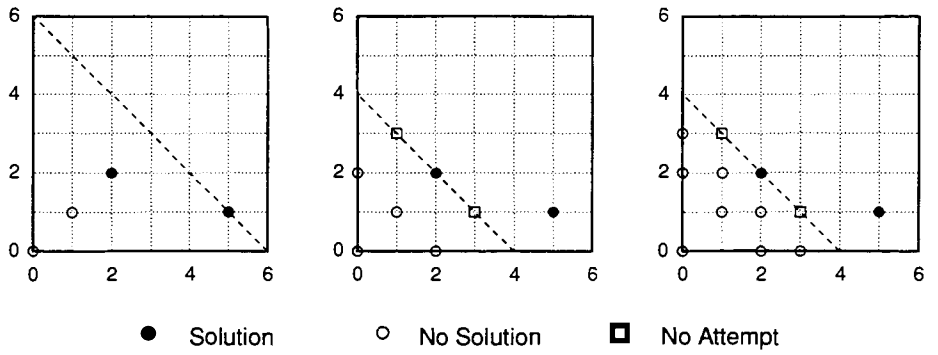
We can see by inspection that the linear system has only the trivial solution.

Having described a single step of the algorithm we turn now to the overall strategy. The idea is to walk up through the degrees of the numerator and denominator until either a solution is found or the total degree becomes greater than or equal to the current minimal solution. When this happens we backtrack recursively to examine the remaining possibilities.

Example 2.32. Suppose we are given a fraction a/b with $\deg(a) = 4$ and $\deg(b) = 1$ which can not be simplified. We first try to construct c/d with $(\deg(c), \deg(d)) = (0, 0)$ and when that fails we will try $(1, 1)$ and $(2, 2)$, as illustrated in the first figure below. The total degree of the next step, $(3, 3)$, is too high to be minimal so we split the computation (see figure 2) and continue searching from $(3, 0)$ and $(0, 3)$. The empty circles in the final figure show all of the cases which are eventually checked.



Example 2.33. Let $a = y^5 + x + y$, $b = x - y$, and $I = \langle xy^5 - x - y \rangle$. To simplify $a/b \mod I$ we will try to construct c/d with $(\deg(c), \deg(d)) = (0,0)$ and $(1,1)$, both of which fail, before we succeed at $(2,2)$ (see Example 2.30). We must now backtrack and check $(2,0)$ and $(0,2)$ (see figure 2) since a solution at either of those points would produce a solution at $(2,2)$.



Walking from $(2,0)$ we arrive at $(3,1)$, however it would be redundant to test this point since we already have a solution of total degree four. We backtrack to test $(3,0)$ and $(2,1)$ before abandoning this path. From $(0,2)$ we walk to $(1,3)$ which is also redundant, and backtrack to test $(1,2)$ and $(0,3)$. Neither point has a solution, so we can conclude that our solution at $(2,2)$ has minimal total degree. Then $(y^5+x+y)/(x-y) \to (x^2+xy+x+y)/(x^2-xy) \mod \langle xy^5-x-y \rangle$.

We make some quick remarks before describing the algorithm in full. First, in our ansatz for c/d we can omit monomials which are reducible by the Gröbner basis for I and thus construct the normal forms of c and d directly. Second, if a simpler fraction is found it can be used in place of a/b in subsequent steps of the algorithm. In particular, the normal form computation of $ad - bc \mod I$ will involve polynomials lower degree so that fewer reduction steps may be needed. One would then expect the resulting linear systems to be sparser, since their complexity depends on the number of reduction steps.

Algorithm 2.34 (Rational Expression Simplification).

Input a non-zero fraction a/b, a Gröbner basis G for a prime ideal I with respect to some a monomial order $<$
(when called recursively) an initial $(N, D) = (\deg(c), \deg(d))$

Output c/d with $ad \equiv bc \mod I$ and $\deg(c) + \deg(d)$ minimal

if (N, D) was not specified **then**
  $(N, D) \leftarrow (0, 0)$
end if
$(c, d) \leftarrow (a, b)$
$numsteps \leftarrow 0$
while $N + D < \deg(a) + \deg(b)$ **do**
  $M_1 \leftarrow \{\mathbf{x} \in k[x_1, \ldots, x_n] : \deg(\mathbf{x}) \leq N \text{ and } \mathbf{x} \text{ not reducible by } G\}$
  $M_2 \leftarrow \{\mathbf{x} \in k[x_1, \ldots, x_n] : \deg(\mathbf{x}) \leq D \text{ and } \mathbf{x} \text{ not reducible by } G\}$
  $\bar{c} \leftarrow \sum_{\mathbf{x_i} \in M_1} c_i \, \mathbf{x_i}$
  $\bar{d} \leftarrow \sum_{\mathbf{x_j} \in M_2} d_j \, \mathbf{x_j}$
  $r \leftarrow NormalForm(a\bar{d} - b\bar{c}, G, <)$

$S \leftarrow$ the set of coefficients of r as a polynomial in $\{x_1, \ldots, x_n\}$

if S has a non-trivial solution λ **then**

$(c, d) \leftarrow$ substitute λ into $(\bar{c}, \bar{d})$

break loop

end if

$(N, D) \leftarrow (N + 1, D + 1)$

$numsteps \leftarrow numsteps + 1$

end loop

if $numsteps > 0$ **then**

$(c, d) \leftarrow RatSimplify(c/d, G, <, N, D - numsteps)$

$(c, d) \leftarrow RatSimplify(c/d, G, <, N - numsteps, D)$

end if

return c/d

We show that in the worst case scenario (when the fraction doesn't reduce) the algorithm terminates in $O(d \log_2(d))$ steps, where $d = \deg(a) + \deg(b)$. From $(0, 0)$ we require $\lceil d/2 \rceil$ steps to reach the border, at which point the computation splits into two paths of approximately half the original length. If we follow all of the paths simultaneously, this branching can occur at most $\log_2(d) + 1$ times before the length of each path becomes $d/(2^{\log_2(d)+1}) < 1$. Then the total number of steps is bounded by

$$\sum_{i=1}^{\log_2(d)+2} 2^{i-1} d/2^i = \frac{d}{2}(\log_2(d) + 2) \in O(d \log_2(d))$$

Note however that the size of the linear systems can not be controlled. In general there are $\frac{1}{n!} \prod_{i=0}^{n-1} (d + i)$ monomials in n variables with degree less than

d, and potentially all of them can appear in each linear system along the border. When d is large relative to n this number is proportional to d^n, so the method becomes impractical for problems of high degree. It is for precisely this reason that we start at $(0,0)$ and walk up, as opposed to some other approach. In the event that a/b simplifies to c/d, the size of the linear systems which we encounter will depend on $\deg(c) + \deg(d)$ instead of $\deg(a) + \deg(b)$.

Appendix A

Implementation

A.1 PolynomialIdeals in Maple 10

We have written a new Maple 10 package for ideal theoretic computations called PolynomialIdeals which we have used extensively to experiment with algorithms and to develop examples for this thesis. We have implemented a data-structure for ideals of $k[x_1, \ldots, x_n]$, new routines for Gröbner bases, and various ideal-theoretic operations, including all of the operations of Section 1.4.

In this section we introduce the package and show how it can be used to perform all of the computations in Chapter 1. In the later sections we use these routines to implement the algorithms of Chapter 2. To begin, we first load the package using Maple's *with* command. This allows us to construct ideals using an angled-bracket notation. The ideal J below is assumed to lie in the ring $\mathbb{Q}[x, y, z]$ by default.

```
> with(PolynomialIdeals):
Warning, the assigned name <,> now has a global binding
Warning, the protected name subset has been redefined and unprotected
> J := <x*y-z, x^2+z>;
```

$$J := \langle xy - z, x^2 + z \rangle$$

Note that Maple reserves the capital letter I for the imaginary unit, so we will use the letters J and K to represent ideals. To compute Gröbner bases it is necessary understand how Maple represents monomial orders. They appear as functions of the ring variables given as an argument to the Gröbner basis command. For example, lexicographic order with $x > y > z$ is specified as $plex(x, y, z)$ in Maple syntax below.

```
> PolynomialIdeals:-GroebnerBasis(J,plex(x,y,z));
```

$$[z^2 + y^2 z, yz + xz, xy - z, x^2 + z]$$

The other term orders are represented similarly: 'grlex' is graded lexicographic order and 'tdeg' is graded reverse lexicographic order. Below we compute a Gröbner basis for J using graded reverse lexicographic order with $z > x > y$. We first alias PolynomialIdeals:-GroebnerBasis to GroebnerBasis so that we don't have to type as much.

```
> GroebnerBasis := PolynomialIdeals:-GroebnerBasis:  # alias
> GroebnerBasis(J,tdeg(z,x,y));
```

$$[xy - z, x^2 + z, yz + xz, z^2 + y^2 z]$$

The 'prod' order constructs an elimination order as a product of monomial orders. In the computation below, we compare monomials first using graded lexicographic order with $x > y$ with ties broken by lexicographic order on z.

```
> GroebnerBasis(J,prod(grlex(x,y),plex(z)));
```

$$[yz + xz, z^2 + y^2z, xy - z, x^2 + z]$$

Maple's Gröbner basis commands return the unique reduced Gröbner basis which is primitive and fraction-free, sorted in the monomial order. We will use the internal PolynomialIdeals command, since it implements new functionality not yet available in the standard command. For example, to run the extended Buchberger algorithm we can use the following syntax.

```
> G, C := GroebnerBasis([x*y-z, x^2+z], tdeg(z,x,y), method=extended);
```

$$G, C := [xy - z, x^2 + z, yz + xz, z^2 + y^2z], [[1, 0], [0, 1], [-x, y], [-xy - z, y^2]]$$

The output is two lists, the first of which is the sorted reduced Gröbner basis. The second list defines the rows of a transformation matrix whose dot product with the vector of generators gives the Gröbner basis, as shown below.

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \\ -x & y \\ -xy - z & y^2 \end{bmatrix} \begin{bmatrix} xy - z \\ x^2 + z \end{bmatrix} = \begin{bmatrix} xy - z \\ x^2 + z \\ yz + xz \\ z^2 + y^2z \end{bmatrix}$$

To compute normal forms we will also use an internal command which can compute a list of quotients (see Algorithm 1.13) and assign them to an optional

fourth argument. Below we compute $f \div G \to r$ and assign the quotients to Q.

```
> NormalForm := PolynomialIdeals:-NormalForm:  # alias
> f := x^3-x*y^2+x*z+y*z;
```

$$f := x^3 - xy^2 + xz + yz$$

```
> r := NormalForm(f, G, tdeg(z,x,y), 'Q'); Q;
```

$$r := 0$$

$$[-y, x, 0, 0]$$

```
> 'f' = Q[1]*G[1] + Q[2]*G[2] + 'r'; # don't evaluate f and r
```

$$f = -y(xy - z) + x(x^2 + z) + r$$

```
> evalb(expand(%)); # evaluate and test the equation
```

$$true$$

The package implements all of the algorithms of Section 1.4. For example, to intersect the ideals of Example 1.28 one would type:

```
> Intersect(<x-1,y-1>, <x-1,y+1>);
```

$$\langle x - 1, y^2 - 1 \rangle$$

The Quotient command computes ideal quotients. In Example 1.34 we computed $\langle x^2, y^2 - 1 \rangle : \langle x, y - 1 \rangle$ as the intersection of $\langle x^2, y^2 - 1 \rangle : \langle x \rangle$ and $\langle x^2, y^2 - 1 \rangle : \langle y - 1 \rangle$. We can do this in Maple as follows.

```
> Q1 := Quotient(<x^2, y^2-1>, x);
```

$$Q1 := \langle x, y^2 - 1 \rangle$$

```
> Q2 := Quotient(<x^2, y^2-1>, y-1);
```

$$Q1 := \langle y+1, x^2 \rangle$$

```
> Intersect(Q1,Q2);
```

$$\langle x^2, xy+x, y^2-1 \rangle$$

Of course, the Quotient command can also perform these steps automatically.

```
> Quotient(<x^2, y^2-1>, <x,y-1>);
```

$$\langle x^2, xy+x, y^2-1 \rangle$$

To compute Gröbner bases for modules we will employ a useful trick. Consider the module from Example 1.57 whose generators are given below. We will compute a Gröbner basis for this module using position over term graded-reverse lexicographic order with $x > y$.

$$M = \left\langle \begin{bmatrix} y^2-x \\ 0 \end{bmatrix}, \begin{bmatrix} x^2-xy \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ y^2-x \end{bmatrix}, \begin{bmatrix} 0 \\ x^2-xy \end{bmatrix}, \begin{bmatrix} y \\ 1 \end{bmatrix} \right\rangle$$

The trick is to introduce dummy variables for each module position, such as $\{e_1, e_2, \dots\}$, and the polynomials $e_i e_j = 0$ for all $i \neq j$. The dummy variables prevent the different components from interacting, while $e_i e_j = 0$ ensures that $\mathrm{S}(f,g) = 0$ if f and g have leading monomials in distinct components.

```
> M := [[(y^2-x),0], [(x^2-x*y),0], [0,(y^2-x)], [0,(x^2-x*y)], [y,1]];
```

$$M := [[(y^2-x),0],[(x^2-xy),0],[0,(y^2-x)],[0,(x^2-xy)],[y,1]]$$

```
> J := <e[1]*e[2], map(inner, M, [e[1],e[2]])>;
```

$$J := \langle e_1e_2, (y^2-x)e_1, (x^2-xy)e_1, (y^2-x)e_2, (x^2-xy)e_2, ye_1+e_2 \rangle$$

Next we compute the Gröbner basis for this ideal. We can emulate TOP or POT using a product order, placing the original variables first or last, respectively. It does not matter what order is chosen for the dummy variables.

```
> G := GroebnerBasis(J, prod(plex(e[1],e[2]), tdeg(x,y))); # POT order
```

$$G := [e_2y^2 - e_2x, e_2xy - e_2x, e_2x^2 - e_2x, ye_1 + e_2, e_1x + ye_2, e_2^2, e_1e_2]$$

Finally we discard polynomials which are not linear in the e_i. The result is a Gröbner basis for the module, which we will convert into vector form. The basis differs with that of Example 1.57 only because it has been reduced.

```
> G := remove(a -> degree(a, {e[1],e[2]}) > 1, G);
```

$$G := [e_2y^2 - e_2x, e_2xy - e_2x, e_2x^2 - e_2x, ye_1 + e_2, e_1x + ye_2]$$

```
> GV := map(a->map2(coeff, a, [e[1],e[2]]), G);
```

$$GV := [[0, y^2 - x], [0, xy - x], [0, x^2 - x], [y, 1], [x, y]]$$

```
> map(Vector, GV);
```

$$\left[\begin{bmatrix} 0 \\ y^2 - x \end{bmatrix}, \begin{bmatrix} 0 \\ xy - x \end{bmatrix}, \begin{bmatrix} 0 \\ x^2 - x \end{bmatrix}, \begin{bmatrix} y \\ 1 \end{bmatrix}, \begin{bmatrix} x \\ y \end{bmatrix}\right]$$

We write a short Maple program to perform these steps automatically. It takes as arguments a list of module elements, a monomial order, and either 'TOP' or 'POT' for term over position or position over term order, respectively.

```
ModuleGB := proc(M::list(list), tord, ordertype)
  local N, e, i, j, V, J, G, mtord;
```

```
  N := nops(M[1]);
  V := [seq(e[i], i=1..N)];
  J := [op(map(inner, M, V)), seq(seq(e[i]*e[j], j=1..i-1), i=2..N)];
  if ordertype='POT' then
    mtord := 'prod'('plex'(op(V)), tord);
  else
    mtord := 'prod'(tord, 'plex'(op(V)));
  end if;
  G := GroebnerBasis(J, mtord);
  G := remove(a->degree(a,{op(V)}) > 1, G);
  G := map(a->map2(coeff, a, V), G);
end proc:
```

We test the command on the previous example.

```
> ModuleGB(M, tdeg(x,y), POT);
```

$$[[0, y^2 - x], [0, xy - x], [0, x^2 - x], [y, 1], [x, y]]$$

This computation comes from Example 2.20. We compute a Gröbner basis using term over position graded lexicographic order with $x > y$.

```
> M := [[x-y, y^5+x+y], [y^5-2, -y^9-y^5+y^4], [0, x y^5-x-y]]:
> map(Vector,M);
```

$$\left[\begin{bmatrix} x-y \\ y^5+x+y \end{bmatrix}, \begin{bmatrix} y^5-2 \\ -y^9-y^5+y^4 \end{bmatrix}, \begin{bmatrix} 0 \\ xy^5-x-y \end{bmatrix}\right]$$

```
> G := ModuleGB(M, grlex(x,y), TOP):
```

```
> map(Vector, G);
```

$$\left[\left[\begin{array}{c} x^2 - xy \\ x + y + x^2 + xy \end{array}\right], \left[\begin{array}{c} x - y \\ y^5 + x + y \end{array}\right], \left[\begin{array}{c} xy^4 - 2 \\ xy^4 + y^4 \end{array}\right]\right]$$

A.2 Inverses and Exact Division

Recall from Section 2.1 how we can compute inverses in $k[x_1, \ldots, x_n]/I$ using the extended Buchberger algorithm. Given $f \in k[x_1, \ldots, x_n]/I$, we compute a Gröbner basis G for $\langle f, I \rangle$ using any monomial order. If $1 \in G$ then f is invertible, and we can write 1 as a multiple of f modulo I. We demonstrate using $f = x$ and $I = \langle x^2 + y, y^2 + 1 \rangle$ from Example 2.2. The Generators command is used to get the set of generators for the ideal.

```
> f := x;
```

$$f := x$$

```
> J := <x^2+y, y^2+1>;
```

$$J := \langle x^2 + y, y^2 + 1 \rangle$$

```
> F := [f, op(Generators(J))];
```

$$F := [x, x^2 + y, y^2 + 1]$$

```
> G, C := GroebnerBasis(F, grlex(x,y), method=extended);
```

$$G, C := [1], [[xy, 1, -y]]$$

```
> finv := C[1][1];
```

$$finv := xy$$

```
> NormalForm(f*finv, J, grlex(x,y)); # check
```

$$1$$

The general case of polynomial division is not much more complicated. Let $f = xy^3 + x + 1$ and $I = \langle xy^5 - x - y \rangle$ from Example 2.8. We divide $g = xy^3+y^3+xy+y^2$ by f modulo I using graded lexicographic order with $x > y$.

```
> f := x*y^3+x+1;
```

$$f := xy^3 + x + 1$$

```
> g := x*y^3+y^3+x*y+y^2
```

$$g := xy^3 + y^3 + xy + y^2$$

```
> J := <x*y^5-x-y>;
```

$$J := \langle xy^5 - x - y \rangle$$

```
> F := [f, op(Generators(J))];
```

$$F := [xy^3 + x + 1, xy^5 - x - y]$$

```
> G,C := GroebnerBasis(F, grlex(x,y), method=extended):  G;
```

$$[2x^2 + 3xy + y + 3x + 2, y^3 + xy + y^2 - x - 1, xy^2 + y^2 + x + y]$$

```
> C;
```

$$[[2 + x - xy^3 + xy - y^4x + y + xy^2, xy + xy^2 - x], [-1 + y^3, -y], [y^2, -1]]$$

```
> r := NormalForm(g, G, grlex(x,y), 'Q'); Q;
```

$$r = 0$$

$$[-\tfrac{1}{2}y + \tfrac{1}{2}, x + 1, \tfrac{1}{2}]$$

At this point we have the matrix equation $g = QCF$, where Q and F are row and column vectors, respectively. We verify the relation in Maple.

```
> expand(Vector[row](Q).Matrix(C).Vector(F));
```

$$xy^3 + y^3 + xy + y^2$$

The quotient for g/f is the first component of QC.

```
> q := NormalForm((Vector[row](Q).Matrix(C))[1], J, grlex(x,y));
```

$$q := y^3$$

```
> NormalForm(g - q*f, J, grlex(x,y));
```

$$0$$

Once again we write a short Maple program to automate the steps above. However we will do a dot product of Q with the first column of C and avoid the rest of the matrix multiplication.

```
Div := proc(g, f, J, tord)
  local F, G, C, Q, q, i;

   F := [f, op(Generators(J))];
   G, C := GroebnerBasis(F, tord, method=extended);
   if NormalForm(g, G, tord, 'Q')=0 then
     q := add(Q[i]*C[i][1], i=1..nops(Q));
     NormalForm(q, J, tord);
   else
     FAIL # f does not divide g mod J
   end if;
end proc;
```

To compute the inverse of f we can simply divide 1 by f. We test the program on the previous examples.

```
> Div(g, f, J, grlex(x,y));
```

$$y^3$$

```
> Div(1, x, <x^2+y, y^2+1>, grlex(x,y));
```

$$xy$$

A.3 Rational Expression Simplification

The tools we have developed make it easy to implement the algorithms for rational expression simplification. Below we have implemented Algorithm 2.26.

```
RatNF := proc(a, b, J, tord)
  local d, c, M, G, i;

   d := GroebnerBasis(Quotient(<b,op(Generators(J))>, a), tord);
   c := [seq(Div(a*i,b,J,tord), i=d)];
   M := [seq([c[i],d[i]], i=1..nops(c)), seq([i,0], i=Generators(J))];
   G := ModuleGB(M, tord, TOP);
   G := remove(a->member(0, map(NormalForm, a, J, tord)), G);
   if nops(G)=0 then 0 else G[1][1]/G[1][2]; end if;
end proc:
```

We verify the program on Examples 2.20 and 2.22.

```
> RatNF(x-y, y^5+x+y, <x*y^5-x-y>, grlex(x,y));
```

$$\frac{x^2 - xy}{x^2 + xy + x + y}$$

```
> RatNF(x^3*y^3-x^4+x-1, x^2-y^2+1, <x^5+x*y-1>, grlex(x,y));
```

$$\frac{y^4x - y^3 - x^3 + x^2 - x^2y + x}{-x^4 + x^2y^2 - x^2}$$

Note that Algorithm 2.26 is a normal form algorithm which can be run using any monomial order. Below we re-run Example 2.20, this time minimizing the largest term of the fraction with respect to lexicographic order with $x > y$.

```
> RatNF(x-y, y^5+x+y, <x*y^5-x-y>, plex(x,y));
```

$$\frac{-y^5 + 2}{y^9 + y^5 - y^4}$$

Algorithm 2.34 is a little more complicated. We will use a subroutine to generate the set of monomials of degree less than or equal to d which are not reducible by a given Gröbner basis.

```
GenMon := proc(vars, d::nonnegint, G, tord)
  local L, M, v, m, i;

   L := map(PolynomialIdeals:-LeadingMonomial, G, tord);
   M := {1};
   for v in vars do
     M := {seq(seq(m*v^i, i=0..d-degree(m)), m=M)};
     M := remove(m->member(true, map2(divide, m, L)), M);
   end do;
end proc:
```

```
RatSimp := proc(a, b, J, tord, N1, D1)
  local N, D, c, d, G, vars, M1, M2, cbar, dbar, r, S, L, numsteps;

   if nargs = 6 then N,D := N1,D1; else N,D := 0,0; end if;
   c,d := a,b;
   numsteps := 0:
   G := GroebnerBasis(J, tord);
   vars := indets(tord, 'name');
   while N + D < degree(a)+degree(b) do
     printf("%a ",[N,D]); # print the steps
     M1 := GenMon(vars, N, G, tord);
     M2 := GenMon(vars, D, G, tord);
     cbar := add(cat('c',i)*M1[i], i=1..nops(M1));
     dbar := add(cat('d',i)*M2[i], i=1..nops(M2));
     r := NormalForm(a*dbar-b*cbar, G, tord);
     S := coeffs(r, vars);
     L := solve(S, indets(S) minus vars);
     cbar,dbar := op(subs(L, [cbar, dbar]));
     if cbar <> 0 and dbar <> 0 then
       # substitute any left over ci or di equal to 1
       S := seq(i=1, i=indets([cbar,dbar]) minus vars);
       c,d := op(subs(S, [cbar,dbar]));
       break;
     end if;
     N,D := N+1,D+1;
     numsteps := numsteps + 1;
```

```
  end do;
  if numsteps > 0 then
    (c,d) := RatSimp(c, d, J, tord, N, D-numsteps);
    (c,d) := RatSimp(c, d, J, tord, N-numsteps, D);
  end if;
  c,d;
end proc:
```

Here is a quick example to demonstrate what the subroutine does.

```
> GenMon({x,y}, 3, [x*y-1], plex(x,y));
```

$$\{1, x, y, x^2, y^2, x^3, y^3\}$$

Here is the algorithm running Example 2.33.

```
> c,d := RatSimp(y^5+x+y, x-y, <x*y^5-x-y>, grlex(x,y)):
[0, 0] [1, 1] [2, 2] [2, 0] [3, 0] [2, 1] [0, 2] [1, 2] [0, 3]
> c/d;
```

$$\frac{x^2 + xy + x + y}{x^2 - xy}$$

In Example 2.22 we started with a fraction of total degree eight, and the normal form algorithm produced a fraction of higher total degree. We verify that the original fraction had minimal total degree.

```
> c,d := RatSimp(x^3*y^3-x^4+x-1, x^2-y^2+1, <x^5+x*y-1>, grlex(x,y)):
[0, 0] [1, 1] [2, 2] [3, 3] [4, 0] [5, 1] [6, 0] [7, 0] [6, 1] [4, 2]
```

```
[5, 2] [4, 3] [0, 4] [1, 5] [2, 4] [3, 4] [2, 5] [0, 6] [1, 6] [0, 7]
> c/d;
```

$$\frac{x^3y^3 - x^4 + x - 1}{x^2 - y^2 + 1}$$

Bibliography

[AL94] W. Adams, P. Loustaunau. *An Introduction to Gröbner Bases.* AMS, Providence, 1994.

[Buc79] B. Buchberger. *A criterion for detecting unnecessary reductions in the construction of Gröbner bases.* Lecture Notes in Computer Science, 72, pp. 3-21, 1979.

[Buc85] B. Buchberger. *Gröbner Bases: An algorithmic method in polynomial ideal theory.* in Multidimensional systems theory, pp. 184-232, Reidel, 1985.

[BW93] T. Becker, V. Weispfenning. *Gröbner Bases : A Computational Approach to Commutative Algebra.* Springer-Verlag, New York Berlin Heidelberg, 1993.

[CT98] M. Caboara, C. Traverso. *Efficient Algorithms for Ideal Operations (Extended Abstract).* ISSAC 1998 Proceedings, pp. 147-152, 1998.

[Cox96] D. Cox, J. Little, D. O'Shea. *Ideals, Varieties, and Algorithms.* Second Edition. Springer-Verlag, New York Berlin Heidelberg, 1996.

[Cox98] D. Cox, J. Little, D. O'Shea. *Using Algebraic Geometry.* Springer-Verlag, New York Berlin Heidelberg, 1998.

[Fau99] J.C. Faugère. *A New Efficient Algorithm for Computing Gröbner Bases (F_4)*. Journal of Pure and Applied Algebra, 139, 1-3, pp. 61-88, 1999.

[Fau02] J.C. Faugère. *A New Efficient Algorithm for Computing Gröbner Bases Without Reduction to Zero (F_5)*. ISSAC 2002 Proceedings, pp. 75-83, 2002.

[Geb88] R. Gebauer, H. Möller. *On an installation of Buchberger's algorithm.* Journal of Symbolic Computation, 6, pp. 275-286, 1988.

[Fro97] R. Fröberg. *An Introduction to Gröbner Bases.* Wiley & Sons, West Sussex, 1997.

[Mul01] J. Mulholland, M. Monagan. *Algorithms for Trigonometric Polynomials.* ISSAC 2001 Proceedings, pp. 245-252, 2001.