Rational Simplification Modulo a Polynomial Ideal *

Michael Monagan
Department of Mathematics
Simon Fraser University
Burnaby, B.C. Canada.
mmonagan@cecm.sfu.ca.

Roman Pearce
Department of Mathematics
Simon Fraser University
Burnaby, B.C. Canada.
rpearcea@cecm.sfu.ca.

ABSTRACT

We present two algorithms for simplifying rational expressions modulo an ideal of the polynomial ring $k[x_1, \ldots, x_n]$. The first algorithm generates the set of equivalent expressions as a module over $k[x_1, \ldots, x_n]$ and computes a reduced Gröbner basis. From this we obtain a canonical form for the expression up to our choice of monomial order. The second method constructs equivalent expressions by solving linear systems over k, and conducts a global search to minimize the total degree of the result. Depending on the ideal, the algorithms may or may not cancel all common divisors. We also provide some timings comparing the efficiency of the algorithms in Maple.

1. INTRODUCTION

Let k be a field and let $I \subset k[x_1, \ldots, x_n]$ be an ideal. We will assume that I is prime so that the quotient ring $k[x_1, \ldots, x_n]/I$ is an integral domain [4]. In this paper we show how to simplify fractions over $k[x_1, \ldots, x_n]/I$ which permits effective computation in that domain. Otherwise arithmetic with fractions produces "blow up".

For example, let $I = \langle xy - 1 \rangle \subset \mathbb{Q}[x, y]$ and consider

$$\frac{x}{x-y} + \frac{y}{y-1} \equiv \frac{x+y^2-2}{x+y^2-y-1} \mod I$$

where we have used the relation $xy = 1$ to reduce the right hand side. The algorithms presented in this paper produce the simplification

$$\frac{x+y^2-2}{x+y^2-y-1} \longrightarrow \frac{x-y-1}{x-y} \mod I$$

reducing the total degree of the fraction from 4 to 2.

Specific instances of this problem have been considered before, notably the case of trigonometric polynomials [7, 9]. The idea behind the methods of [7, 9] is to use a parameterization of $V = \mathbf{V}(I)$ as an injective homomorphism from $k[V]$ to a rational function field $k(t)$, where the problem is solved by computing and cancelling a polynomial gcd in $k[t]$. We illustrate the technique on an example from [9].

Example 1. *Consider*

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

A parameterization of $\mathbf{V}(s^2 + c^2 - 1)$ *is* $\{s = 2t/(1+t^2),\ c = (1-t^2)/(1+t^2)\}$. *Substituting into* a/b *we obtain the following simplified expression in* $\mathbb{Q}(t)$.

$$\frac{f(t)}{g(t)} = \frac{2t^4 + 4t^2 + 2}{t^5 - t^4 + 4t^3 + 4t^2 - t + 1}$$

To invert the map we use the implicitization method of [4]. Since $1 + t^2$ *does not vanish over* $\mathbb{Q}$ *we can eliminate* t *from*

$$J = \langle f(t)\,\mathbf{e_1} + g(t)\,\mathbf{e_2}, (1+t^2)s - 2t, (1+t^2)c - (1-t^2) \rangle$$

We find that $(s - c - 1)\,\mathbf{e_1} + (c^3 + sc - 2c)\,\mathbf{e_2}$ *is a minimal element of* $J \cap \mathbb{Q}[s, c]$ *with respect to graded lexicographic order with* $s > c$. *This gives the simplification*

$$\frac{sc - c^2 + s + 1}{c^4 - 2c^2 + s + 1} \longrightarrow \frac{s - c - 1}{c^3 + sc - 2c} \mod \langle s^2 + c^2 - 1 \rangle$$

which reduces the total degree of the expression from 6 to 4.

A fundamental limitation of this approach is that many affine varieties can not be parameterized. Irreducible curves in two variables must have genus zero [8], so for example fractions over $\mathbb{Q}[x, y]/\langle y^2 - x^3 + x \rangle$ could not be handled. A similar condition exists for surfaces [11], and we know of no algorithms to parameterize higher dimensional objects.

In this paper we present two algebraic methods for simplifying fractions over $k[x_1, \ldots, x_n]/I$. The first is a Gröbner basis method which computes a reduced canonical form. This method requires additional material from the theory of Gröbner bases which we present in Section 2. The algorithm and a proof of its correctness are given in Section 3. In Section 4 we present the second algorithm which is a dense method that minimizes total degree. We end with a section comparing the performance of the two algorithms in the Maple computer algebra system.

It turns out that for some ideals the methods do not cancel all common divisors. In fact, both methods may introduce common divisors. This was a surprise to us. In Section 2 we give a general condition on the ideal I and its monomial order which, if met, guarantees that no common divisors are present in the output of either algorithm.

*Supported by NSERC of Canada and the MITACS NCE of Canada

2. PRELIMINARIES

In this section we will review some known results about Gröbner bases in preparation for the sequel. Good references for this material are [1, 2, 5].

First recall how Gröbner bases for polynomials in $R = k[x_1, \ldots, x_n]$ can be generalized to vectors of polynomials in R^m, which define a *submodule* of R^m (submodules of R^1 correspond to ideals). To run the Buchberger algorithm one must extend monomial orders on R to vectors over R as well. We adopt the definitions and terminology of [1].

DEFINITION 1. *Let $<$ be a monomial order on $k[x_1, \ldots, x_n]$. 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 2. *Let $<$ be a monomial order on $k[x_1, \ldots, x_n]$. 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 $i < j$.*

Position over term orders behave like lexicographic order with respect to the vector components. Polynomials in the first component are eliminated, producing the intersection of the module with the lower components, and so on, until a Gröbner basis is obtained. Similarly, term over position orders resemble total degree orders for ordinary polynomials. They do not have any elimination properties, however, the largest monomial appearing in any component is minimized.

EXAMPLE 2. *Let $<$ denote graded lexicographic order with $x > y$. We will compute Gröbner bases for the module*

$$M = \left\langle \begin{bmatrix} y \\ x \end{bmatrix}, \begin{bmatrix} 1 \\ xy - 1 \end{bmatrix} \right\rangle \subset \mathbb{Q}[x, y]^2$$

using $<_{POT}$ and $<_{TOP}$. For $<_{POT}$ the respective leading monomials are $y\,\mathbf{e_1}$ and $1\,\mathbf{e_1}$, so we construct the syzygy

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

This new element has a leading monomial in $\mathbf{e_2}$, which can not be cancelled with monomials in $\mathbf{e_1}$. There are no other syzygies, so $\{y\,\mathbf{e_1} + x\,\mathbf{e_2}, 1\,\mathbf{e_1} + xy\,\mathbf{e_2}, (-xy^2 + x + y)\,\mathbf{e_2}\}$ is a Gröbner basis for M with respect to $<_{POT}$. For $<_{TOP}$ the leading monomials are $x\,\mathbf{e_2}$ and $xy\,\mathbf{e_2}$, respectively. Their syzygy is

$$y \begin{bmatrix} y \\ x \end{bmatrix} - \begin{bmatrix} 1 \\ xy - 1 \end{bmatrix} = \begin{bmatrix} y^2 - 1 \\ 1 \end{bmatrix}$$

This element has a leading monomial in $\mathbf{e_1}$, so there are no syzygies between it and the other module elements. Then $\{y\,\mathbf{e_1} + x\,\mathbf{e_2}, 1\,\mathbf{e_1} + xy\,\mathbf{e_2}, (y^2 - 1)\,\mathbf{e_1} + 1\,\mathbf{e_2}\}$ is a Gröbner basis for M with respect to $<_{TOP}$.

LEMMA 1. *Let f be a polynomial and let I be an ideal of $k[x_1, \ldots, x_n]$. If $\{g_1, \ldots, g_t\}$ is a Gröbner basis for $\langle f \rangle + I$ then there exist $\{q_1, \ldots, q_t\}$ with $g_i \equiv q_i f \mod I$ for each i.*

The quotients q_i comprise a column of the transformation matrix for $\{g_1, \ldots, g_t\}$. One can compute them using the extended Buchberger algorithm [2], or using a module computation as follows. Let $I = \langle h_1, \ldots, h_s \rangle$. If we compute a reduced Gröbner basis for the module

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

using a position over term order $<_{POT}$ then we obtain

$$G = \left\{ \begin{bmatrix} 0 \\ p_1 \end{bmatrix}, \ldots, \begin{bmatrix} 0 \\ p_u \end{bmatrix}, \begin{bmatrix} g_1 \\ q_1 \end{bmatrix}, \ldots, \begin{bmatrix} g_t \\ q_t \end{bmatrix} \right\}$$

where the g_i are a reduced Gröbner basis for $\langle f \rangle + I$ with respect to $<$ and the q_i are reduced modulo I. This method is quite effective at controlling intermediate expression swell, and in practice, one can use a Gröbner basis for I and omit the syzygies among the h_i.

LEMMA 2. *Let $f, g \in k[x_1, \ldots, x_n]$ and $g \in \langle f \rangle + I$. Then there exists $q \in k[x_1, \ldots, x_n]$ satisfying $g \equiv qf \mod I$, and we say that f* divides *g modulo I.*

PROOF. Let $\{g_1, \ldots, g_t\}$ be a Gröbner basis for $\langle f \rangle + I$ and let $\{q_1, \ldots, q_t\}$ be the quotients from Lemma 1. Then there exists $\{c_1, \ldots, c_t\}$ by the normal form algorithm with $g = \sum_{i=1}^{t} c_i g_i \equiv \sum_{i=1}^{t} c_i q_i f \equiv \left(\sum_{i=1}^{t} c_i q_i\right) f \mod I$ □

A more general version of Lemma 2 appears in [2] in the context of solving linear equations over $k[x_1, \ldots, x_n]/I$. Next we define the quotient operation for ideals, which is the basis of our first simplification algorithm.

DEFINITION 3. *Let $I, J \subseteq k[x_1, \ldots, x_n]$ be ideals. The* ideal quotient *$I : J$ is the set $\{f \in k[x_1, \ldots, x_n] : fh \in I \text{ for all } h \in J\}$.*

For our purposes it will suffice to compute quotients of the form $I : \langle f \rangle$ where $f \in k[x_1, \ldots, x_n]$. The most efficient way of doing this is the "tag variable algorithm variant" [3].

LEMMA 3. *Let $I = \langle h_1, \ldots, h_s \rangle$ and let f be a polynomial. If $M = \langle f\,\mathbf{e_1} + \mathbf{e_2}, I\mathbf{e_1}, I\mathbf{e_2} \rangle$ then $I : \langle f \rangle = M \cap \mathbf{e_2}$.*

PROOF. Let $b \in M \cap \mathbf{e_2}$. Every $a\,\mathbf{e_1} + b\,\mathbf{e_2} \in M$ satisfies $a - bf \equiv 0 \mod I$ so $bf \equiv 0 \mod I$ and $b \in I : \langle f \rangle$. Now let $b \in I : \langle f \rangle$. Then $bf \in I$ so $bf = q_1 h_1 + \cdots + q_s h_s$ for some $\{q_i\} \subset k[x_1, \ldots, x_n]$ and

$$\begin{bmatrix} 0 \\ b \end{bmatrix} = b \begin{bmatrix} f \\ 1 \end{bmatrix} - \left(q_1 \begin{bmatrix} h_1 \\ 0 \end{bmatrix} + \cdots + q_s \begin{bmatrix} h_s \\ 0 \end{bmatrix} \right)$$

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

EXAMPLE 3. *Let $I = \langle x + y^2 - y - 1, xy - 1 \rangle$ and $J = \langle x + y^2 - 2 \rangle$ in $\mathbb{Q}[x, y]$. To compute $I : J$ we construct the module $M = \langle [\,x + y^2 - 2, 1\,], [\,x + y^2 - y - 1, 0\,], [\,xy - 1, 0\,], [\,0, x + y^2 - y - 1\,], [\,0, xy - 1\,] \rangle$ and compute a reduced Gröbner basis with respect to a position over term monomial order.*

We will employ a trick to compute this result using only the Buchberger algorithm for ordinary polynomials. We first write each module element $[\,a, b\,]$ as $a\,\mathbf{e_1} + b\,\mathbf{e_2}$ and add the relations $\mathbf{e_i}\,\mathbf{e_j} = 0$ for $1 \le i, j \le 2$ to the generating set. To simulate a position over term order, we use a product order which compares first using lexigraphic order on $\{\mathbf{e_1}, \mathbf{e_2}\}$ and second using a monomial order on $\{x, y\}$. Finally we discard any polynomials whose degree in $\{\mathbf{e_1}, \mathbf{e_2}\}$ is greater than one from the resulting Gröbner basis.

Using lexicographic order and $\mathbf{e_1} > \mathbf{e_2} > x > y$ we obtain

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

Then $I : J = \langle y^2 - 1, x - y \rangle$.

3. REDUCED CANONICAL FORMS

Our approach to computing reduced canonical forms for fractions modulo I is actually quite simple. Given a/b we will construct the module $\{[\,c,d\,] : ad - bc \equiv 0 \mod I\}$ and compute a reduced Gröbner basis using a term over position order. From this we extract the smallest $[\,c,d\,]$ with $c,d \notin I$, minimizing the largest monomial in c/d. Uniqueness follows from our use of reduced Gröbner bases. In the results that follow we will denote ideals of the form $\langle a\rangle + I$ by $\langle a, I\rangle$. Recall Definition 3 for ideal quotients given above.

LEMMA 4. *Let I be an ideal of $k[x_1,\ldots,x_n]$ and suppose $a/b \equiv c/d \mod I$. Then $c \in \langle a, I\rangle : \langle b\rangle$ and $d \in \langle b, I\rangle : \langle a\rangle$.*

PROOF. Since $ad - bc \equiv 0 \mod I$ we have $ad - bc = h$ for some $h \in I$. Then $bc = ad - h$ expresses c as an element of $\langle a, I\rangle : \langle b\rangle$, while $ad = bc + h$ expresses d as an element of $\langle b, I\rangle : \langle a\rangle$. □

LEMMA 5. *Let $a, b \in k[x_1,\ldots,x_n]$ where b is not a zero-divisor modulo $I = \langle h_1,\ldots,h_s\rangle$. If $\langle b, I\rangle : \langle a\rangle = \langle d_1,\ldots,d_t\rangle$ and $c_i = ad_i/b \mod I$ for $i = 1\ldots t$ 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 $M = \{[x,y] : ay - bx \equiv 0 \mod I\}$ as a module over $k[x_1,\ldots,x_n]$.

PROOF. By construction each generator $[\,x,y\,]$ satisfies $ay - bx \equiv 0 \mod I$ so suppose $[\,x,y\,] \in M$. By Lemma 4 $y \in \langle d_1,\ldots,d_t\rangle$ so $y = p_1d_1 + \cdots + p_td_t$ for some $\{p_i\} \subset k[x_1,\ldots,x_n]$. Then

$$\begin{aligned} b(x - (p_1c_1 + \cdots + p_tc_t)) &\equiv a(y - (p_1d_1 + \cdots + p_td_t)) \\ &\equiv a \cdot 0 \mod I \end{aligned}$$

and since b is not a zero-divisor

$$x - (p_1c_1 + \cdots + p_tc_t) \equiv 0 \mod I$$

Then there exists $\{q_i\} \subset k[x_1,\ldots,x_n]$ with

$$x - (p_1c_1 + \cdots + p_tc_t) = q_1h_1 + \cdots + q_sh_s$$

and $\begin{bmatrix} x \\ y \end{bmatrix} = \sum_{i=1}^{t} p_i \begin{bmatrix} c_i \\ d_i \end{bmatrix} + \sum_{i=1}^{s} q_i \begin{bmatrix} h_i \\ 0 \end{bmatrix}$ □

EXAMPLE 4. *Let $a/b = (x+y^2-2)/(x+y^2-y-1)$ modulo $I = \langle xy-1\rangle$ from the introduction. From Example 3 we have $\langle b, I\rangle : \langle a\rangle = \langle x - y, y^2 - 1\rangle$. From Lemma 2 we obtain*

$$\begin{aligned} x - y - 1 &\equiv (x-y)a/b \mod I \\ y^2 + y - 1 &\equiv (y^2-1)a/b \mod I \end{aligned}$$

Next we construct the module

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

The generators of M are almost a Gröbner basis with respect to term over position graded lexicographic order with $x > y$, one only needs to flip the last element. The algorithm will select $c/d = (x-y-1)/(x-y)$.

In the previous example we can apply Lemma 2 to find that $a = (y-1)\,c \mod I$ and $b = (y-1)\,d \mod I$, thus the algorithm cancelled a common factor of $y - 1$. An obvious question is whether the simplification of fractions always corresponds to the cancellation of common divisors and the answer is *no*. This was already noted by Mulholland and Monagan for fractions over $\mathbb{Q}[s,c]/\langle s^2 + c^2 - 1\rangle$ [9], and Example 1 in the introduction demonstrates an instance of it. The next example was a surprise however.

EXAMPLE 5. *Let $a/b = (y^5 + x + y)/(x - y)$ modulo $I = \langle xy^5 - x - y\rangle \subset \mathbb{Q}[x,y]$. Then $\langle b, I\rangle : \langle a\rangle = \langle x - y, y^5 - 2\rangle$ using Lemma 3 and we construct the module*

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

using Lemmas 2 and 5. Using term over position graded lexicographic order with $x > y$, the smallest element in a reduced Gröbner basis is $[\,x^2+xy+x+y, x^2-xy\,]$. Neither polynomial is in I so

$$\frac{y^5+x+y}{x-y} \longrightarrow \frac{x^2+xy+x+y}{x^2-xy} \mod I$$

We can check with Lemma 2 that the new numerator and denominator do not divide the old ones. In fact,

$$\begin{aligned} x^2+xy+x+y &\equiv x(y^5+x+y) \mod I \\ \text{and} \quad x^2-xy &\equiv x(x-y) \mod I. \end{aligned}$$

So a common factor of x was added to the numerator and denominator to simplify the fraction! Note that x is not a unit of $\mathbb{Q}[x,y]/I$. If it were we would have computed its inverse already during the check with Lemma 2.

It's worth examining why a common factor was added in Example 5 since this does not happen over other domains, like the trigonometric polynomial ring $\mathbb{Q}[s,c]/\langle s^2 + c^2 - 1\rangle$ [9]. The reason is that in the trigonometric polynomial ring we have a "degree sum formula", $\deg(pq) = \deg(p) + \deg(q)$, where p, q and pq are in normal form modulo $\langle s^2 + c^2 - 1\rangle$. This implies that common factors only increase total degree. In Lemma 8 we state a sufficient condition for this formula to hold for arbitrary ideals, but to prove it we will need two well-known results.

LEMMA 6. *Let f be a homogeneous polynomial and let G be a set of homogeneous polynomials. If $f \div G \to r$ then r is homogeneous and if $r \neq 0$, $\deg(r) = \deg(f)$.*

PROOF. See [6], or [2]. □

DEFINITION 4. *The* initial form *of a polynomial f, $init(f)$, is the sum of the terms with degree $\deg(f)$. For example, $init(x^2 + xy + x + y) = x^2 + xy$.*

LEMMA 7. *If G is a Gröbner basis with respect to a graded monomial order $<$ then $init(G) = \{init(g) \mid g \in G\}$ is a Gröbner basis with respect $<$ as well.*

PROOF. Suppose not. Then there exists $g_i, g_j \in G$ with $S(init(g_i), init(g_j)) \div init(G) \to r \neq 0$. Then $S(g_i, g_j)$ could not reduce to zero modulo G since the leading terms of G and $init(G)$ are the same. □

LEMMA 8 (DEGREE SUM). *Let G be a Gröbner basis for a prime ideal I with respect to a graded monomial order. If $\langle init(G)\rangle$ is also prime then for all $p, q \in k[x_1,\ldots,x_n]/I$ $\deg(pq) = \deg(p) + \deg(q)$ after reduction to normal form.*

PROOF. We can assume p and q are already in normal form so $init(p)$ and $init(q)$ are not reducible by $init(G)$. Then $init(pq) = init(p)\,init(q) \div init(G) \rightarrow r \neq 0$ since $\langle init(G)\rangle$ is prime. Terms of r must appear in the normal form of pq since they can not be reduced by the leading terms of G. Then $\deg(r) = \deg(init(pq)) = \deg(p) + \deg(q)$ by Lemma 6. □

We show that when a graded monomial order is used and the hypotheses of Lemma 8 are satisfied the simplification algorithm does not return fractions with common divisors. Let $M = \{[x, y] : ay - bx \equiv 0 \mod I\}$. If $[pc, pd] \in M$ then $[c, d] \in M$ since I is prime and $\deg(c) < \deg(pc)$ and $\deg(d) < \deg(pd)$ by Lemma 8. This implies that $[c, d]$ has a smaller leading term than $[pc, pd]$, so $[pc, pd]$ would be eliminated from a reduced Gröbner basis for M.

EXAMPLE 6. *Consider $\mathbb{Q}[s, c]/\langle s^2 + c^2 - 1\rangle$. The initial form of $s^2 + c^2 - 1$ is $s^2 + c^2$ which is irreducible over $\mathbb{Q}$. We conclude that the simplification algorithm removes all common divisors from fractions over this domain.*

EXAMPLE 7. *Consider $\mathbb{Q}[s, c]/\langle s^2 - c^2 + 1\rangle$ and observe that $\langle init(G)\rangle = \langle s^2 - c^2\rangle$ is not prime. Let $p = s + c - 1$ and $q = s - c + 1$. Then $pq = s^2 - c^2 + 2c - 1 \equiv 2c - 2 \mod I$ and the fraction*

$$\frac{pq}{(p-3)q} \equiv \frac{2c-2}{-3s+5c-5} \mod I$$

is already in canonical form. We can use Lemma 2 to verify that p, q, and $p-3$ are all non-units of $\mathbb{Q}[s, c]/\langle s^2 - c^2 + 1\rangle$.

We can generalize Lemma 8 to allow for *weighted degree orders*, where the variables are graded with respect to a vector of positive weights (see §10.2 of [2]). The definitions of degree and initial form are similarly adjusted, providing a measure of control over $\langle init(G)\rangle$. We illustrate this below.

EXAMPLE 8. *Let $f = y^2 - x^3 + x \in \mathbb{Q}[x, y]$. With ordinary total degree $init(f) = x^3$ and Lemma 8 can not be applied. However using the weight vector $\omega = [2, 3]$ on $[x, y]$ we find $\deg_\omega(f) = 6$ and $init_\omega(f) = y^2 - x^3$ is irreducible. Now Lemma 8 can be applied!*

Example 8 shows how a carefully chosen weighted degree order can make the simplification algorithm remove common divisors. Note that a parameterization method could not be used for that domain since the genus of f is 1.

We can also ask how good the output of the simplification algorithm is when a total degree order is used. The next example shows that the algorithm may increase total degree.

EXAMPLE 9. *Consider $a/b = (x^2y^4 - y)/(x^2 - y^2 + 1)$ modulo $I = \langle x^3 + xy - 1\rangle \subset \mathbb{Q}[x, y]$. Note that we can not apply Lemma 8 since $init_\omega(I) \in \{x^3, xy, x^3 + xy\}$ for any weight vector ω. Worse, if we run the standard algorithm using graded lexicographic order with $x > y$, the only valid fractions in the module Gröbner basis are*

$$\frac{xy^4 - x^2y - y^2}{-x^2y^2 - y^3 + x^2 + x + y} \quad \textit{and}$$

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

The original fraction had total degree $\deg(a) + \deg(b) = 8$, while both "simplified" fractions have total degree 9.

We prove that the total degree of a reduced canonical form is within a factor of two of the minimum total degree in this case. Let a/b be in canonical form with respect to a graded monomial order. Then $\max(\deg(a), \deg(b))$ is minimal and

$$\begin{aligned} \deg(a) + \deg(b) &\leq 2\max(\deg(a), \deg(b)) \\ &\leq 2\max(\deg(c), \deg(d)) \\ &\leq 2(\deg(c) + \deg(d)) \end{aligned}$$

for any $c/d \equiv a/b \mod I$.

Finally we mention an improvement for an important special case of the algorithm. Suppose I be homogeneous. Then $init(G) = G$ so if I is prime Lemma 8 is satisfied. We show that if a and b are also homogeneous then one can skip the construction of the module M and its Gröbner basis computation entirely.

LEMMA 9. *Let I and J be homogeneous ideals. Then the quotient $I : J$ is generated by homogeneous polynomials.*

PROOF. See [6]. □

LEMMA 10. *Let I be a homogeneous prime ideal and let f and g be homogeneous polynomials, $g \notin I$. If $g = qf \mod I$ and q is in normal form then q is also homogeneous and $\deg(q) = \deg(g) - \deg(f)$.*

PROOF. Let $q = q_1 + q_2$ where q_1 consists of 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 its terms can not be cancelled by Lemma 6, and I is prime implies $q_2 \equiv 0 \mod I$. □

Our modified approach computes a reduced Gröbner basis for $\langle b, I\rangle : \langle a\rangle$ with respect to a graded monomial order. We select the smallest $d \notin I$ for the denominator, and compute the numerator $c \equiv ad/b \mod I$ using Lemma 2. Since I is prime, c is unique, and $\deg(c) = \deg(a) + \deg(d) - \deg(b)$ by Lemma 10. Since $\deg(d)$ is minimal, our choice of d thus produces a canonical form with minimal total degree.

EXAMPLE 10. *Let $a/b = (x^3 + x^2y)/(2xy + y^2)$ modulo $I = \langle x^3 + xy^2 + y^3\rangle$. We first compute $\langle b, I\rangle : \langle a\rangle = \langle x, y\rangle$ using Lemma 3 and any graded monomial order. If $x > y$ we choose $d = y$ and compute $c \equiv ad/b \equiv (x^2 + xy - y^2)/3 \mod I$ using Lemma 2. Then*

$$\frac{x^3 + x^2y}{2xy + y^2} \longrightarrow \frac{x^2 + xy - y^2}{3y} \mod \langle x^3 + xy^2 + y^3\rangle$$

cancelling a common factor of $(2x + y)/3$.

Our improved algorithm for the homogeneous case can also be used when a, b, and I are homogeneous with respect to a vector of weights, although it is much harder to choose weights (as in Example 8) since they depend on a and b.

We conclude this section with some additional remarks. First one might wonder why we compute $\langle b, I\rangle : \langle a\rangle$ and not $\langle a, I\rangle : \langle b\rangle$. The reason is that if the denominator is invertible modulo I or if it divides the numerator exactly then we have the option of returning a polynomial. Both the standard and the homogeneous method will compute a reduced Gröbner basis for $\langle b, I\rangle : \langle a\rangle = \langle 1\rangle$, find $d = 1$, and compute $c \equiv a/b \mod I$. The standard algorithm can be halted before the module Gröbner basis computation. The homogeneous method requires no modification.

Second, notice that computing $\langle b, I\rangle : \langle a\rangle$ allows us to run the algorithm even when I is not prime. Unfortunately

zero-divisors can appear in the denominators of the module Gröbner basis and it is not entirely clear what we should do. We leave this question to future research.

4. MINIMAL TOTAL DEGREE

The algorithm of Section 3 is appropriate for computing in fields of fractions of $k[x_1,\ldots,x_n]/I$, but Example 9 and others like it suggest the need for a different approach to the simplification problem. Our goal should be to minimize total degree, and not necessarily force expressions into a canonical form. To this end we present a global search algorithm which can be made reasonably efficient in practice.

The idea of this method is to walk up through the degrees of the numerator and denominator and at each step attempt to solve $ad-bc\equiv 0 \mod I$ using an ansatz for c and d. We demonstrate a solving step below.

EXAMPLE 11. *Let* $a/b = (y^5+x+y)/(x-y)$ *modulo* $I=\langle xy^5-x-y\rangle$. *Assuming* $\deg(c)=\deg(d)=2$ *we set*

$$\begin{aligned} c &= c_1+c_2y+c_3x+c_4y^2+c_5xy+c_6x^2 \\ d &= d_1+d_2y+d_3x+d_4y^2+d_5xy+d_6x^2 \end{aligned}$$

The normal form of $ad-bc \mod I$ *is*

$$\begin{aligned} &d_4y^7+d_2y^6+d_1y^5+(d_6-c_6)x^3+(d_5+d_6-c_5+c_6)x^2y \\ &+(c_5-c_4+d_4+d_5)xy^2+(d_4+c_4)y^3+(d_6+d_3-c_3)x^2 \\ &+(d_5+c_3+d_2-c_2+d_6+d_3)xy+(d_5+c_2+d_2)y^2 \\ &+(d_1-c_1+d_3)x+(c_1+d_1+d_3)y \end{aligned}$$

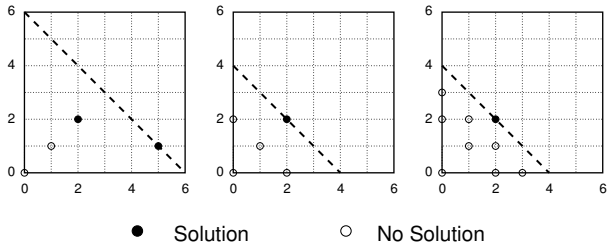
Equating each coefficient to zero, we obtain a 12×12 *homogeneous linear system with general solution*

$$\begin{array}{llllll} c_1=0 & c_2=t & c_3=t & c_4=0 & c_5=t & c_6=t \\ d_1=0 & d_2=0 & d_3=0 & d_4=0 & d_5=-t & d_6=t \end{array}$$

For any $t\neq 0$ *we can substitute this solution into* c/d *and obtain* $(x^2+xy+x+y)/(x^2-xy)$.

To search efficiently we start from $(\deg(c),\deg(d))=(0,0)$ and increase both $\deg(c)$ and $\deg(d)$ by one in each step. When either a solution is found or $\deg(c)+\deg(d)$ becomes larger than the total degree of the current minimal solution we recurse to examine the remaining possibilities.

EXAMPLE 12. *Let* $a/b=(y^5+x+y)/(x-y)$ *modulo* $I=\langle xy^5-x-y\rangle$. *We first try to construct* $c/d\equiv a/b$ *with* $(\deg(c),\deg(d))=(0,0)$ *and* $(1,1)$, *which fail, before we succeed at* $(2,2)$, *as shown in the first figure below.*



We recurse to check $(2,0)$ *and* $(0,2)$ *since solutions at one of those points would produce a solution at* $(2,2)$. *From* $(2,0)$ *we walk to* $(3,1)$, *however it would be redundant to test this point since we already have a solution with 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* $(0,3)$. *No other solutions are found, so we conclude that the* $(2,2)$ *solution has minimal total degree. This result may not be unique however, since the points* $(0,4)$, $(1,3)$, $(3,1)$, *and* $(4,0)$ *were never tested.*

We present the simplification algorithm below. Note that in practice one should build up multiplication matrices [5] for a and b instead of computing the normal form of $ad-bc$ directly in each iteration.

ALGORITHM 1 (RATIONAL SIMPLIFICATION).

Input *a Gröbner basis* G *for a prime ideal* I, a/b *with* $b\not\equiv 0 \mod I$, $(N,D)=(\deg(c),\deg(d))$ *if called recursively*
Output c/d, $ad\equiv bc \mod I$, $\deg(c)+\deg(d)$ *minimal*

if (N,D) *not specified* ***then*** $(N,D)\leftarrow(0,0)$ ***end if***
$(c,d)\leftarrow(a,b)$
steps $\leftarrow 0$
while $N+D<\deg(a)+\deg(b)$ ***do***
  $M_1\leftarrow\{$*monomials* $\mathrm{x}^\alpha\notin\langle LM(G)\rangle, \deg(\mathrm{x}^\alpha)\le N\}$
  $M_2\leftarrow\{$*monomials* $\mathrm{x}^\alpha\notin\langle LM(G)\rangle, \deg(\mathrm{x}^\alpha)\le D\}$
  $\hat{c}\leftarrow\sum_{\mathrm{x_i}\in M_1} c_i\,\mathrm{x_i}$
  $\hat{d}\leftarrow\sum_{\mathrm{x_j}\in M_2} d_j\,\mathrm{x_j}$
  $r\leftarrow NormalForm(a\hat{d}-b\hat{c},G)$
  $S\leftarrow$ *the set of coefficients of* r
  if S *has a non-trivial solution* λ ***then***
    $(c,d)\leftarrow$ *substitute* λ *into* $(\hat{c},\hat{d})$
    break loop
  end if
  $(N,D)\leftarrow(N+1,D+1)$
  steps $\leftarrow$ *steps* $+1$
end loop
if *steps* >0 ***then***
  $(c,d)\leftarrow Simplify(c/d,G,N,D-steps)$
  $(c,d)\leftarrow Simplify(c/d,G,N-steps,D)$
end if
return c/d

LEMMA 11. *Let* I *be an ideal of* $k[x_1,\ldots,x_n]$ *and suppose* $a/b\equiv c/d \mod I$ *where* $D=\deg(c)+\deg(d)$ *is minimal. Then Algorithm 1 terminates in* $O(D\log_2(D))$ *steps.*

PROOF. The algorithm requires at most D steps to find the first solution, at which point the search splits into two paths of approximately half the original length. This can occur at most $\log_2(D)+1$ times before the length of each path becomes $D/(2^{\log_2(D)+1})<1$, bounding the number of steps by

$$\sum_{i=0}^{\log_2(D)+1} 2^iD/2^i = D(\log_2(D)+2)\in O(D\log_2(D))$$

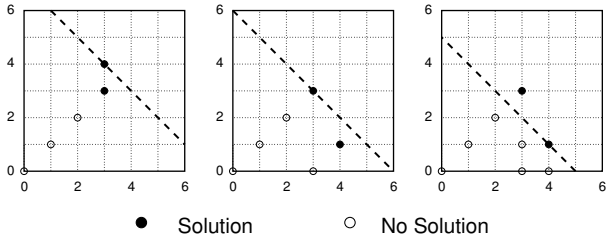
□

The $O(D\log_2(D))$ steps of Algorithm 1 improves on the $O(D^2)$ steps for a naive approach, however the size of the linear systems grows rapidly. There are $\binom{D+n-1}{n-1}$ monomials in n variables with degree D, and potentially all of them can appear in the linear systems for $(D,0)$ or $(0,D)$. Worse, if $\deg(a)+\deg(b)>2D$ we can check (D,D) as well, which has the equations from both points.

EXAMPLE 13. *Let* $I = \langle x^5 y + 1 \rangle \subset \mathbb{Q}[x, y]$, $f = x^2 y + 1$, *and* $g = x^3 - y$. *The fraction* $1/f$ *already has minimal total degree, so we expect*

$$h = \frac{x^3 - y}{x^3 - x^2 y^2 - y - 1} \equiv \frac{g}{fg} \mod I$$

to simplify to a fraction with total degree 3. Algorithm 1 checks $(0,0)$, $(1,1)$, *and* $(2,2)$ *before finding its first solution at* $(3,3)$. *It recurses to check* $(3,0)$ *and* $(4,1)$, *where it finds a solution with total degree 5, and recurses again for* $(4,0)$ *and* $(3,1)$. *We illustrate these steps in the diagrams below.*



Recursing from $(3,3)$ *again, the algorithm checks* $(0,3)$ *and finds* $1/f$. *It terminates, since there is nowhere else to go. The table below summarizes the linear systems encountered.*

Point	*Size*	*Density*
$(0,0)$	3×2	*.833*
$(1,1)$	9×6	*.296*
$(2,2)$	18×12	*.157*
$(3,3)^*$	25×20	*.114*
$(3,0)$	14×11	*.143*

Point	*Size*	*Density*
$(4,1)^*$	20×18	*.100*
$(4,0)$	20×16	*.100*
$(3,1)$	13×13	*.125*
$(0,3)^*$	11×11	*.112*

* *solution found*

Example 13 almost captures the worst-case of our search strategy. The result has total degree D, yet we check the point (D, D) and fill in half of a border with total degree $5D/3 - 1 \approx 2D$. Each linear system contains all possible monomials, since the generator for I has a leading monomial of degree $2D$. To construct versions of this example with higher degree one can substitute $(x, y) \to (x^k, y^k)$ for $k > 1$.

5. TIMINGS

So far we have presented two algorithms for simplifying fractions modulo a polynomial ideal. The goal of this section is to provide insight into their performance.

We implemented both algorithms in Maple 10 using the Gröbner basis routines of the PolynomialIdeals package. To compute Gröbner bases for modules we use Buchberger's algorithm and the trick from Example 3. To compute ideal quotients $I : f$ we use Lemma 3 and a Gröbner basis for I, omitting syzygies among the Gröbner basis elements.

For most problems we report the total degree of the input (deg) and the result (res). For the reduced canonical form algorithm (cform) and its homogeneous variant (hform) we report the total time. For the minimal degree algorithm (mindeg) and a homogeneous version (hdeg) we report only the time required to solve the linear systems using Maple's SolveTools[Linear] command. Optimized implementations of those algorithms should produce similar results. We ran the tests on a 32-bit 1.4GHz Athlon PC with 1GB of RAM.

EXAMPLE 14. *An extremely sparse problem derived from Example 13 and the substitution* $(x, y) \to (x^k, y^k)$. *Simplify*

$$\frac{y^k - x^{3k}}{x^{2k} y^{2k} - x^{3k} + y^k + 1} \mod \langle x^{5k} y^k + 1 \rangle$$

Both algorithms output $1/(x^{2k} y^k + 1)$, *reducing the total degree from* $7k$ *to* $3k$. *The canonical form algorithm runs in constant time while the minimal degree algorithm has bad asymptotic performance. The largest linear system and total number of steps for the mindeg algorithm are also recorded.*

k	*cform*	*mindeg*	*steps*	$(3k, 3k)$	*density*
1	*.166*	*.013*	*9*	25×20	*.114*
2	*.169*	*.061*	*17*	79×56	*.0359*
3	*.168*	*.174*	*23*	160×110	*.01767*
4	*.169*	*.492*	*35*	268×182	*.01052*
5	*.170*	*1.101*	*41*	403×272	*.006979*
6	*.169*	*2.120*	*49*	565×380	*.004970*
7	*.171*	*3.698*	*55*	754×506	*.003719*
8	*.170*	*7.888*	*75*	970×650	*.002888*

EXAMPLE 15. *Let* $a/b = (y^5 + x + y)/(x - y)$ *modulo* $I = \langle xy^5 - x - y \rangle \subset \mathbb{Q}[x, y]$. *From Examples 5 and 12 we know that* a/b *simplifies to* $(x^2 + xy + x + y)/(x^2 - xy) \mod I$ *using either algorithm. In this example we will simplify*

$$\frac{a\,(ab)^k}{b\,(ab)^k} \equiv \frac{a}{b} \mod I$$

where $a(ab)^k$ *and* $b(ab)^k$ *are first reduced to normal form. The output is always* $(x^2 + xy + x + y)/(x^2 - xy)$. *We also test a parameterization method using* $\{x = t/(t^5 - 1), y = t\}$ *and Buchberger's algorithm for implicitization. This requires a slight modification from Example 1, see §3.3 of [4].*

k	*deg*	*cform*	*mindeg*	*param*
1	*6*	*.098*	*.012*	*.018*
2	*18*	*.191*	*.014*	*.018*
3	*30*	*.414*	*.017*	*.020*
4	*42*	*1.068*	*.024*	*.022*
5	*54*	*2.187*	*.032*	*.025*
6	*66*	*3.260*	*.040*	*.036*
7	*78*	*6.223*	*.044*	*.043*
8	*90*	*10.934*	*.053*	*.050*

As expected, the canonical form algorithm is a poor choice when the answer has low total degree. A comparison can be drawn with univariate rational expressions, where one can choose between computing and cancelling out a gcd versus constructing a result with dense interpolation. Note that the ideal quotient computation (Lemma 3) is essentially the extended Euclidean algorithm with one cofactor in this case.

EXAMPLE 16. *Let* $a/b = (y^5 + x + y)/(x - y)$ *modulo* $I = \langle xy^5 - x - y \rangle$. *We simplify* $a^k/b^k \mod I$ *where* a^k *and* b^k *are first reduced to normal form. The algorithms all produce results with the same total degree.*

k	*deg*	*res*	*cform*	*mindeg*	*param*
1	*6*	*4*	*.099*	*.013*	*.027*
2	*12*	*8*	*.306*	*.117*	*.074*
3	*18*	*10*	*.530*	*.240*	*.180*
4	*24*	*13*	*.924*	*.800*	*.455*
5	*30*	*16*	*1.653*	*2.390*	*.810*
6	*36*	*20*	*2.852*	*6.221*	*1.852*
7	*42*	*22*	*4.628*	*8.297*	*3.626*
8	*48*	*26*	*7.549*	*15.237*	*6.556*
9	*54*	*29*	*11.347*	*30.362*	*12.017*
10	*60*	*30*	*14.652*	*30.469*	*17.123*

Although the canonical form algorithm is initially the slowest, it eventually beats the minimal degree algorithm and the parameterization method on Example 16. Almost all of the time in the parameterization algorithm is spent

implicitizing the result, so improved Gröbner basis routines should benefit both algorithms proportionately. In our next example we compare a specialized algorithm for a particular domain which does not compute Gröbner bases.

EXAMPLE 17. *A trigonometric example from [9]. Let*

$$\frac{a}{b} = \frac{5c^3 + 21c^2 + 4cs + 23c + 12s + 15}{7c^3 - sc^2 + 31c^2 + 2sc + 15s + 37c + 21}$$

In this test we simplify a^k/b^k modulo $\langle s^2 + c^2 - 1\rangle$ using our algorithms and the algorithm of [9], which parameterizes $\mathbb{V}(s^2 + c^2 - 1)$ using the tan half-angle formula and recovers an expression in $\{s, c\}$ using a resultant. It is implemented as 'trig/ratpoly/simplify' in Maple 10.

k	*deg*	*res*	*cform*	*mindeg*	*param*
5	*30*	*6*	*.336*	*.093*	*.051*
10	*60*	*10*	*.891*	*.619*	*.138*
15	*90*	*16*	*1.887*	*4.599*	*.340*
20	*120*	*20*	*3.474*	*10.074*	*.673*
25	*150*	*26*	*5.472*	*30.506*	*1.967*
30	*180*	*30*	*9.046*	*52.614*	*2.952*
35	*120*	*36*	*12.081*	*140.187*	*5.153*
40	*240*	*40*	*17.797*	*228.333*	*7.666*
45	*270*	*46*	*24.207*	*453.586*	*11.531*
50	*300*	*50*	*34.797*	*707.379*	*16.420*

We find Example 17 encouraging, despite the fact that we were unable to beat the parameterization method of [9]. The canonical form algorithm had good asymptotic performance, and it seems reasonable to suggest that faster Gröbner basis routines would make it competitive. The minimal degree algorithm performed poorly due to the high degrees and the density of the linear systems encountered. The systems were 80-95% non-zero during the initial walks from $(0, 0)$ and 30-50% non-zero thereafter.

EXAMPLE 18. *This problem is homogeneous. Let*

$$\frac{a}{b} = \frac{x^4 + y^2z^2 + 2xz^3}{y^2z^2 + 2yz^3 + z^4}$$

We will simplify $a^k/b^k \mod \langle xy + z^2\rangle$ using the canonical form and minimal degree algorithms and their homogeneous variants. All four methods reduce the total degree from $8k$ to $6k$. We stopped testing the mindeg algorithm at $k = 5$.

k	*deg*	*res*	*hform*	*cform*	*hdeg*	*mindeg*	*steps*
1	*8*	*6*	*.106*	*.147*	*.025*	*.048*	*12*
2	*16*	*12*	*.275*	*.408*	*.134*	*.790*	*29*
3	*24*	*18*	*.588*	*1.142*	*.493*	*7.061*	*52*
4	*32*	*24*	*1.268*	*2.366*	*1.092*	*32.096*	*69*
5	*40*	*30*	*1.989*	*4.679*	*1.915*	*108.412*	*80*
6	*48*	*36*	*3.103*	*8.594*	*4.360*	–	*121*
7	*56*	*42*	*4.952*	*16.769*	*6.856*	–	*136*
8	*64*	*48*	*7.191*	*29.196*	*12.787*	–	*161*

The homogeneous minimal degree algorithm performed quite well on Example 18. Much of this can be attributed to having only three variables and an ideal generator that eliminates a lot of monomials. Our remarks about the size of the linear systems apply equally to the homogeneous case of the algorithm. Thus we can expect to see systems with up to $\binom{d+n-1}{n-1}$ rows and columns where n is the number of variables and d is the total degree of the result. When n is fixed this number is $O(d^{n-1})$. When d is fixed it is $O(n^d)$.

6. CONCLUSION

We presented two methods for simplifying fractions over $k[x_1, \ldots, x_n]/I$ when I is prime. The first method produces a canonical form and is appropriate for computing in the field of fractions. It performs well enough to be recommended generally, and in some cases a monomial order can be chosen so that all common divisors are cancelled. A homogeneous variant is also available which is faster, cancels all common divisors, and produces an expression with minimal total degree.

Our second method is better suited to simplification since it always constructs an expression with minimal total degree. It is essentially a dense interpolation. It performs poorly on sparse problems when the output has moderately high total degree. A variant of the algorithm for homogeneous problems has much better performance, although only for a small number of variables.

The output of both methods may have common divisors present between the numerator and denominator. This depends on the ideal and the monomial order. For some ideals one can choose a monomial order to force the output of the first method to have no common divisor.

Where applicable, we expect parametrization methods to have the best overall performance. The difficulty is in the implicitization step, where Buchberger's algorithm should not be used directly. Alternatives include resultants [5] and Buchberger's algorithm followed by the Gröbner Walk [12]. Our algorithms might also be of use to someone developing faster methods for a specific domain.

7. REFERENCES

[1] W. Adams, P. Loustaunau. An Introduction to Gröbner Bases. AMS, 1996.

[2] T. Becker and V. Weispfenning. Gröbner Bases. Springer-Verlag, 1993.

[3] M. Caborara, C. Traverso. Efficient algorithms for ideal operations (extended abstract). ISSAC 1998 Proceedings, pp. 147-152, 1998.

[4] D. Cox, J. Little, D. O'Shea. Ideals, Varieties, and Algorithms. Second Edition. Springer-Verlag, 1996.

[5] D. Cox, J. Little, D. O'Shea. Using Algebraic Geometry. Second Edition. Springer-Verlag, 2005.

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

[7] J. Gutierrez, T. Recio. Advances on the simplification of sine-cosine equations. J. Symb. Comput. 26(1), pp. 31-70, 1998.

[8] M. van Hoeij. Rational Parametrizations of Algebraic Curves using a Canonical Divisor. J. Symb. Comput. 23, pp. 209-227, 1997.

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

[10] R. Pearce. Rational Expression Simplification with Polynomial Side Relations. M.Sc. Thesis, Simon Fraser University, 2005.

[11] J. Schicho. Rational Parametrization of Real Algebraic Surfaces. ISSAC 1998 Proceedings, pp. 302-308, 1998.

[12] Q. Tran. Efficient Groebner Walk Conversion for Implicitization of Geometric Objects. Computer Aided Geometric Design, 21(9), pp. 837-857, 2004.