Rational Simplification Modulo a Polynomial Ideal

Roman Pearce   Michael Monagan

Simon Fraser University

July 2006

The Problem

Our goal is to simplify fractions modulo an ideal of polynomial relations. For example, suppose $xy - 1 = 0$. Consider

$$\frac{x}{x-y} + \frac{y}{y-1} = \frac{2xy - x - y^2}{(x-y)(y-1)}$$

Using the relation $xy = 1$ to reduce terms we obtain

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

But this is not simplified. We could obtain

$$\frac{x + y^2 - 2}{x + y^2 - y - 1} \equiv \frac{x - y - 1}{x - y} \mod \langle xy - 1 \rangle$$

Example: Trigonometric Polynomials

"Simplify":

$$\frac{\sin(x)\cos(x) - \cos^2(x) + \sin(x) + 1}{\cos^4(x) - 2\cos^2(x) + \sin(x) + 1}$$

Let $s = \sin(x)$ and $c = \cos(x)$. The problem becomes

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

Previous Work:

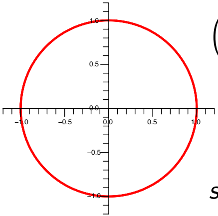
- J. Gutierrez, T. Recio. JSC 26-1, 1998
- J. Mulholland, M. Monagan. ISSAC 2001

Trigonometric Simplification

Map the problem into one variable.

$$\sin(x) \rightarrow \frac{2\tan(x/2)}{1+\tan^2(x/2)}$$

$$\cos(x) \rightarrow \frac{1-\tan^2(x/2)}{1+\tan^2(x/2)}$$



$$\left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right)$$

$$s^2 + c^2 - 1 = 0$$

$$\frac{sc - c^2 + s + 1}{c^4 - 2c^2 + s + 1} \rightarrow \boxed{\begin{array}{c}\text{cancel}\\ \text{univariate}\\ \text{gcd}\end{array}} \rightarrow \frac{2(t^4 + 2t^2 + 1)}{t^5 - t^4 + 4t^3 + 4t^2 - t + 1}$$

Finally we *implicitize* to recover an expression in $\{s, c\}$.

Parameterization Methods

In general:

- given $I \subset k[x_1, \ldots, x_n]$ (prime), parameterize $\mathbb{V}(I)$ to map $k[x_1, \ldots, x_n]/I \to k(y_1, \ldots, y_m)$
- cancel common divisors using a gcd
- implicitize to recover a result

Problems:

- finding parameterizations can be hard
- implicitization of fractions requires some thought
- many affine varieties can not be parameterized

Conclusion: this is not going to work very well in general

Fractions over $k[x_1, \ldots, x_n]/I$

- Two fractions $\frac{a}{b}$ and $\frac{c}{d}$ are equivalent if $ad - bc \equiv 0 \mod I$
- $M = \{[x, y] \mid ay - bx \equiv 0 \mod I\}$ is a module over $k[x_1, \ldots, x_n]$
- Our approach is to construct the module M and extract the minimal non-zero element from a reduced Gröbner basis.

Ideal quotients: $J : \langle f \rangle = \{h \mid hf \in J\}$

Example: Let $a = (x-1)(x+1)$ and $b = (x-1)(x^2+x+1)$
Then $\langle a \rangle : \langle b \rangle = \langle x+1 \rangle = \langle a/\gcd(a,b) \rangle$

In general: Given $a/b \mod I$, the ideal quotient $\langle a, I \rangle : \langle b \rangle$ contains the numerators of all equivalent fractions

Constructing Equivalent Fractions

Given $a/b \mod I$ where $I = \langle h_1, \ldots, h_s \rangle$

- compute $\langle a, I \rangle : \langle b \rangle = \langle c_1, \ldots, c_t \rangle$
- solve for denominators $d_i \equiv c_i b/a \mod I$
- the module of equivalent fractions is generated by

$$\left\{ \left[\begin{array}{c} c_1 \\ d_1 \end{array} \right], \ldots, \left[\begin{array}{c} c_t \\ d_t \end{array} \right], \left[\begin{array}{c} 0 \\ h_1 \end{array} \right], \ldots, \left[\begin{array}{c} 0 \\ h_s \end{array} \right] \right\}$$

Example: $(x+y^2-2)/(x+y^2-y-1) \mod \langle xy-1 \rangle$

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

$$\begin{array}{rcl} x-y & \equiv & (x-y-1)(x+y^2-y-1)/(x+y^2-2) \mod \langle xy-1 \rangle \\ y^2-1 & \equiv & (y^2+y-1)(x+y^2-y-1)/(x+y^2-2) \mod \langle xy-1 \rangle \end{array}$$

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

Gröbner Bases for Modules

(Adams & Loustaunau) To compute leading monomials we can:

- choose the largest monomials, break ties by component (term-over-position – TOP)
- from first non-zero component, select largest monomial (position-over-term – POT)

Graded lexicographic order with $x > y$ (TOP or POT):

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

So this is a Gröbner basis (Buchberger's first criterion)

We will use TOP order to construct a "small" fraction, i.e., the largest monomial in the result will be minimal.

Examples: Reduced Canonical Form

By computing a reduced Gröbner basis, we get a canonical form.

- $$\frac{sc - c^2 + s + 1}{c^4 - 2c^2 + s + 1} \longrightarrow \frac{s - c - 1}{c^3 + sc - 2c} \mod \langle s^2 + c^2 - 1 \rangle$$
- $$\frac{y^5 + x + y}{x - y} \longrightarrow \frac{x^2 + xy + x + y}{x^2 - xy} \mod \langle xy^5 - x - y \rangle$$
- $$\frac{x^2y^4 - y}{x^2 - y^2 + 1} \longrightarrow \frac{xy^4 - x^2y - y^2}{-x^2y^2 - y^3 + x^2 + x + y} \mod \langle x^3 + xy - 1 \rangle$$

In the last example the algorithm reduced x^2y^4 at the expense of everything else. This is bad for simplification. The algorithm can output a result with up to twice the minimum total degree.

Common Divisors

Returning to the second example:

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

The algorithm *added* a common factor of x:

$$\begin{aligned} x(y^5+x+y) &\equiv x^2+xy+x+y \mod \langle xy^5-x-y\rangle \\ x(x-y) &\equiv x^2-xy \mod \langle xy^5-x-y\rangle \end{aligned}$$

But this *never* happens over $\mathbb{Q}[s,c]/\langle s^2+c^2-1\rangle$ – why ?

Answer: to reduce we use $s^2=1-c^2$ or $c^2=1-s^2$, either one preserves total degree.

In general: we also use the fact that s^2+c^2 is irreducible.

Degree Sum Lemma

With respect to a graded order:

We want $\deg(\overline{pq}) = \deg(p) + \deg(q)$ for $p, q \in k[x_1, \ldots, x_n]/I$
(p, q, and $\overline{pq}$ are in normal form)

- common factors will increase the degree of both the numerator and denominator
- the module GB computation will remove these factors to obtain the smallest leading monomial

Condition: $init(I) = \langle init(f) \,|\, f \in I \rangle$ is prime
($init(f)$ is the initial form of f, ie: the terms of maximal degree)

Note: this condition is both necessary and sufficient

- there is no hope for $\mathbb{Q}[x, y]/\langle xy^5 - x - y \rangle$

Closing Remarks

Also in the paper:

- mention generalization to *weighted degrees*: $deg_\omega(f)$, $init_\omega(f)$
- choose weights to make the algorithm remove common factors

Example: $\mathbb{Q}[x,y]/\langle x^3 - y^2 - x\rangle$, choose $\omega = [2,3]$ on $[x,y]$
so that $init(x^3 - y^2 - x) = x^3 - y^2$ is prime

- homogeneous variant (output has minimal total degree)
- dedicated algorithm for simplification ($n\log(n)$ global search) where $n = \deg(c) + \deg(d)$, the total degree of the result
- basic timings and analysis of performance