Propositon 7.20

Let $p, q \in k[x_1, \dots, x_n]$ s.t. $LM(p)$ and $LM(q)$ coprime:

$$\mathrm{lcm}(LM(p), LM(q)) = LM(p) \cdot LM(q)$$

Then $\overline{S(p,q)}^{(p,q)} = 0$

Proof

We may assume $LC(p) = LC(q) = 1$

(since the leading coefficient is cancelled out in $S(p,q)$)

Write

$$p = LM(p) + \tilde{p} \quad , \quad q = LM(q) + \tilde{q}.$$

Then

$$S(p,q) = LM(q)p - LM(p)q = (q - \tilde{q})p - (p - \tilde{p})q$$
$$= \tilde{p}q - \tilde{q}p$$

Claim: $\operatorname{multideg} S(p,q) = \max(\operatorname{multideg} \tilde{p}q, \operatorname{multideg} \tilde{q}p)$

Proof of claim: If not, the leading terms in $\tilde{p}q - \tilde{q}p$ cancel, so

$$LM(\tilde{p})\, LM(q) = LM(\tilde{p}q) = LM(\tilde{q}p) = LM(\tilde{q})\, LM(p)$$

Since $LM(p)$, $LM(q)$ are coprime it follows that

$$LM(p) \mid LM(\tilde{p})$$

But this is impossible since $LM(p) > LM(\tilde{p})$

Hence $LM(S(p,q)) = LM(\tilde{p})LM(q)$ or

$$LM(S(p,q)) = LM(\tilde{q})LM(p)$$

but not both!

So in the division algorithm we have a division step

$$g = S(p,q) - LT(\tilde{p})q$$
$$= \tilde{p}q - \tilde{q}p - LT(\tilde{p})q$$
$$= (\tilde{p} - LT(\tilde{p}))q - \tilde{q}p \quad =: \tilde{\tilde{p}}q - \tilde{q}p$$

or $g = \tilde{p}q - (\tilde{q} - LT(\tilde{q}))p =: \tilde{p}q - \tilde{\tilde{q}}p$

Repeating the argument, we see that the division algorithm gives a unique sequence of reductions

$$\begin{array}{ccccccc} \tilde{p} & \rightsquigarrow & \tilde{\tilde{p}} & \rightsquigarrow & \tilde{\tilde{\tilde{p}}} & \rightsquigarrow & \cdots \\ \shortparallel & & \shortparallel & & \shortparallel & & \\ p_1 & & p_2 & & p_3 & & \end{array}$$

with $LM(p_1) > LM(p_2) > LM(p_3) > \dots$

and similarly $LM(q_1) > LM(q_2) > LM(q_3) > \dots$

By the well ordering property these sequences must terminate at $p_N = 0$ and $q_M = 0$ for some N, M. Hence the division algorithm gives

$$\overline{S(p,q)}^{(p,q)} = 0 \qquad \square$$

Corollary 7.21

If $G = \{g_1, \dots, g_s\} \subset k[x_1, \dots, x_n]$ is a finite set such that all $g_i, g_j \in G$, $g_i \neq g_j$ have coprime leading terms, then G is a Gröbner basis.

Proof

In Buchberger's criterion (Thm 7.14) the order of the tuple G is arbitrary. By Proposition 7.20 we have for all g_i, g_j

$$\overline{S(g_i, g_j)}^{(g_i, g_j, g_1, \dots, \hat{g}_i, \dots, \hat{g}_j, \dots, g_s)} = 0 \qquad \square$$

g_i omitted $\quad$ g_j omitted

Example 7.22

Reordering the tuple is important:

If $G = (yz + y, x^3 + y, z^4)$ in deglex order then $S(x^3 + y, z^4) = yz^4$ but division algorithm with the tuple G uses $LT(yz + y) = yz$ to compute

$$yz^4 = (z^3 - z^2 + z - 1)(yz + y) + 0 \cdot (x^3 + y) + 0 \cdot z^4 + y$$

Hence

$$\overline{yz^4}^{G} = y \neq 0, \qquad \overline{yz^4}^{(x^3+y, z^4, yz+y)} = 0$$

Polynomial computations in SageMath

Try it online: sagecell.sagemath.org

Polynomial rings

```
P.<x,y> = PolynomialRing(QQ, order='deglex')
```

polynomials

```
p1 = 2*x^3 - 4*x*y
p2 = x^2*y - 2*y^2 + x
```

ideals

```
I = P.ideal(p1, p2)
```

leading terms | leading monomials | leading coefficients

```
p1.lt()    p1.lm()    p1.lc()
```

pre-implemented Buchberger

```
from sage.rings.polynomial.toy_buchberger import *
set_verbose(1)
buchberger(I)
```

S-polynomials

```
p3=spol(p1, p2)
```

lcm

```
lcm(p1, p2)
```

polynomial reduction (not necessarily polynomial division)

```
p3.reduce([p1,p2])
```

more efficient Gröbner basis computation

```
I.groebner_basis()
```

tab-completion substitute in sagecell: `dir(I)`

Example 7.23

$I = \langle p_1, p_2 \rangle \subset \mathbb{Q}[x,y,z]$ with degrevlex order

$p_1 = xz - y^2 \qquad p_2 = x^3 - z^2$

A Gröbner basis is $G = \{p_1, p_2, p_3, p_4, p_5\}$

$p_3 = x^2y^2 - z^3$ from $S(p_1, p_2)$

$p_4 = -xy^4 + z^4$ from $S(p_1, p_3)$

$p_5 = -y^6 + z^5$ from $S(p_1, p_4)$

Hence

$\langle LT(I) \rangle = \langle LT(G) \rangle = \langle y^6, x^3, x^2y^2, xz, xy^4 \rangle$

Consider

$f = -4x^2y^2z^2 + y^6 + 3z^5$

$g = xy - 5z^2 + x$

Then $LT(g) = xy \notin \langle LT(G) \rangle \Rightarrow g \notin I$

$LT(f) = -4x^2y^2z^2 \in \langle LT(G) \rangle$ so possibly $f \in I$.

Polynomial division show

$\overline{f}^G = 0 \Rightarrow f \in I$

Example 7.24

Find the minimum and maximum values of

$$f = x^3 + 2xyz - z^2 \in \mathbb{R}[x,y,z]$$

restricted to the sphere

$$g = x^2+y^2+z^2-1 = 0$$

Method of Lagrange multipliers:

Consider critical points of $\nabla f - \lambda \nabla g$

$$p_1 = 3x^2 + 2yz - 2\lambda x = 0$$

$$p_2 = 2xz - 2\lambda y = 0$$

$$p_3 = 2xy - 2z - 2\lambda z = 0$$

$$g = x^2 + y^2 + z^2 - 1 = 0$$

Compute a Gröbner basis for

$I = \langle p_1, p_2, p_3, g \rangle \subset \mathbb{R}[\lambda, x, y, z]$ in the lex order.

We obtain $G = \{g_0, \dots, g_7\}$ including

$$g_7 = z^7 - \frac{1763}{1152} z^5 + \frac{655}{1152} z^3 - \frac{11}{288} z$$

$$= z(z-1)(z+1)\left(z-\frac{2}{3}\right)\left(z+\frac{2}{3}\right)\left(z^2 - \frac{11}{128}\right)$$

$\Rightarrow$ Any $(x,y,z) \in V(I)$ has $z \in \{0, \pm 1, \pm \frac{2}{3}, \pm\sqrt{\frac{11}{128}}\}$

Substituting these values for z and solving the remaining system $g_0 = \dots = g_6 = 0$, we find

$V(I) = \{10 \text{ points}\}$ and can evaluate min f, max f

Warning: Gröbner computations may take unreasonable amounts of memory and/or time, even with state-of-the-art methods.

Example 7.25 (Gröbner degree >> input degree)

$I = \langle x^{n+1} - yz^{n-1}w,\ xy^{n-1} - z^n,\ x^n z - y^n w \rangle,\ n \geq 1$

in degrevlex order.

The reduced Gröbner basis contains for example

$$z^{n^2+1} - y^{n^2} w$$

Even worse pathological behavior can be found from combinatorial word problems (Mayr–Meyer 1982):

$\exists\, I_n = \langle p_{k,1}, \ldots, p_{k,9} : 1 \leq k \leq n \rangle \subset \mathbb{Q}[x_{i,1}, \ldots, x_{i,14}, 1 \leq i \leq n]$

$p_{k,i} = x^{\alpha_{k,i}} - x^{\beta_{k,i}}, \quad \deg p_{k,i} \leq 5$

such that a Gröbner basis contains elements of degree $\approx 2^{2^n}$