The division algorithm

October 22, 2021 9:45 AM

CLO 2.3 A division algorithm for $k[x_1,\dots,x_n]$.

Given $f_1,\dots,f_s \in k[x_1,\dots,x_n]\setminus\{0\}$, $f \in k[x_1,\dots,x_n]$, to divide $f \div \{f_1,\dots,f_s\}$ we want to write

$$f = a_1 f_1 + \dots + a_s f_s + r \quad \text{for } a_1,\dots,a_s, r \in k[x_1,\dots,x_n].$$

quotients ($a_1,\dots,a_s$) remainder (r).

Context $I = \langle f_1,\dots,f_s\rangle$. Is $f \in \langle f_1,\dots,f_s\rangle$.
If $r=0 \Rightarrow f \in I$.

Example Suppose $f_1 = xy+1$, $f_2 = 1+y$, $f = -x+xy^2$.
Suppose we use $<_{lex}$ with $x>y$. $\Rightarrow f = xy^2 - x$

$f_1 = xy+1$
$f_2 = y+1$

$a_1 = y$
$a_2 = -1$

$\boxed{r = -x+1}$

$$\begin{array}{l}
xy^2 - x = f = p_1 \\
-(xy^2 + y) \\
-x - y = p_2 \\
-y = p_3 \\
-1\cdot f_2 \quad -(-y-1) \\
1 = p_4 \\
0
\end{array}$$

$f = a_1f_1 + a_2f_2 + r$?

No term in r is divisible by $LT(f_i)$.

Notice $\boxed{xy^2 > x > y > 1}$

Does $r \neq 0$ mean $f \notin \langle f_1, f_2\rangle$?

$f_2 = y+1$
$f_1 = xy+1$

$a_2 = xy - x$
$a_1 = 0$

$r = 0$.

$$\begin{array}{l}
xy^2 - x = f \\
-(xy^2 + xy) \\
-xy - x \\
-xf_1 \quad -(-xy-x) \\
0
\end{array}$$

$f \in \langle f_1, f_2\rangle$.

The output depends on the order of f_i.
If $f \in \langle f_1,\dots,f_s\rangle$ division may not produce a 0 remainder.
The problem is the basis $\{f_1,\dots,f_s\}$ for I not the $\div$ alg.

Proof of termination

Claim Each time round the loop $LM(P_{NEW}) < LM(P_{OLD})$ or $P_{NEW}=0$.

CASE 1. Is $p-LT(p)=0$ or $LM(\underbrace{p-LT(p)}_{P_{NEW}}) < LM(\underbrace{p}_{P_{OLD}})$. $\cancel{xy^2}+xy+y^2$

CASE 2. Is $LM(\underbrace{p-tf_i}_{P_{NEW}}) < LM(\underbrace{p}_{P_{OLD}})$ or $p-tf_i=0$.

$$LM(p-tf_i)$$

$$= LM\left(LT(p)+(p-LT(p)) - \underbrace{\frac{LT(p)}{LT(f_i)}}_{t}\cdot\left(LT(f_i)+(f_i-LT(f_i))\right)\right)$$

$$= LM\Big(LT(p) + \underbrace{p-LT(p)}_{<LT(p)} - \big[LT(p) - \underbrace{t(f_i-LT(f_i))}_{<LT(p) \text{ by (ii)}}\big]\Big).$$

$p-$

Letting $p_1, p_2, \dots$ denote the values of p at the i'th step of the $\div$ alg, i.e., $p_1=p$. then

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

Since $>$ is a well ordering, Lemma 2 says such a strictly decreasing sequence cannot continue indefinitely, hence $p=0$, and the $\div$ alg terminates.