Computational Algebra

4. Reductions or Rewrite rules

A closer look to what happens during the Algorithm Multivariate Division is that we use the polynomials $g_1, \dots, g_s$ to rewrite monomials of a polynomial f as other polynomials (that are "smaller" in the sense of the given term order). In other words, we think of the g_i as <u>rewrite rules</u> of the form

$$LM_{\leq}(g_i) \longrightarrow g_i - LM_{\leq}(g_i)$$

Multivariate Division hence performs a series of <u>reductions</u>, or <u>rewriting</u>, according also to the order in which $g_1, \dots, g_s$ are listed. We saw that the order, in general, matters, hence if we performed the reductions in any order we would not, in general, obtain the same result. However, formulating the procedure in terms of rewrite rules points out the condition that would solve the problem, namely, <u>confluence</u>.

<u>Def</u>: let $g_1, \dots, g_s \in k[x_1, \dots, x_n]$, let $\leq$ be a term order and suppose that all the $g_1, \dots, g_s$ are nonzero, let $G := \{g_1, \dots, g_s\}$

a. let $f_1 \in k[x_1, \dots, x_n]$ and suppose that for some $t \in \mathbb{T}^n$, we have that $t \cdot LT_{\leq}(g_i) \in \operatorname{supp}(f_1)$ for some $i \in \{1, \dots, s\}$; then, let $c \in k$

be such that $c \cdot t \cdot LM_{\leq}(g_i)$ is a monomial in f_1, and set $f_2 := f_1 - c \cdot t \cdot g_i$; then we say that f_1 reduces to f_2 modulo g_i / using g_i in one step; passing from f_1 to f_2 is called a reduction step; we write $f_1 \xrightarrow{g_i} f_2$

b. the transitive closure of the relations $\xrightarrow{g_1}, \ldots, \xrightarrow{g_s}$ is called the reduction using G, or the rewrite relation defined by G and it is denoted by $\xrightarrow{G}$; hence, we have $f_1 \xrightarrow{G} f_2$ if and only if $f_1 \xrightarrow{g_{i_1}} h_1 \xrightarrow{g_{i_2}} \ldots \xrightarrow{g_{i_k}} h_k \xrightarrow{g_{i_{k+1}}} f_2$ for some polynomials $h_1, \ldots, h_k$ and indices $i_1, \ldots, i_{k+1}$

c. a polynomial f_1 such that there exists no $i \in \{1, \ldots, s\}$ and no f_2 such that $f_1 \xrightarrow{G} f_2$ is called irreducible with respect to $\xrightarrow{G}$

d. the equivalence relation defined by $\xrightarrow{G}$ is denoted $\xleftrightarrow{G}$ (recall that if R is a relation on a set X, then the equivalence relation $\sim_R$ induced by R is the intersection of all equivalence relations containing R; notice that $X \times X$ is an equivalence relation, so the intersection is not on an empty index; more concretely, we have that if $x, y \in X$, then $x \sim_R y$ if and only if there exist $z_0 = x, z_1, \ldots, z_k, z_{k+1} = y$ in X such that for every i, we have $(z_i, z_{i+1}) \in R$ or $(z_{i+1}, z_i) \in R$)

<u>Remark</u>: by choosing $c = 0$, we can always write that $f \xrightarrow{g} f$.

<u>Prop.</u>: let $g_1, \dots, g_s$ be non-zero polynomials in $k[x_1, \dots, x_n]$ and set $G :=$
$= \{g_1, \dots, g_s\}$; the following hold.

a. if $f_1 \xrightarrow{G} f_2$ and $f_2 \xrightarrow{G} f_1$, then $f_1 = f_2$

b. if $f_1 \xrightarrow{G} f_2$, then for every $t \in \mathbb{T}^n$, we have $t \cdot f_1 \xrightarrow{G} t \cdot f_2$

c. every chain $f_1 \xrightarrow{G} f_2 \xrightarrow{G} \dots$ is eventually ~~st~~stationary

d. if $f_1 \xrightarrow{g_i} f_2$ and if $f_3 \in k[x_1, \dots, x_n]$, then there exists a polynomial $f_4 \in k[x_1, \dots, x_n]$ such that $f_1 + f_3 \xrightarrow{g_i} f_4$ and $f_2 + f_3 \xrightarrow{g_i} f_4$

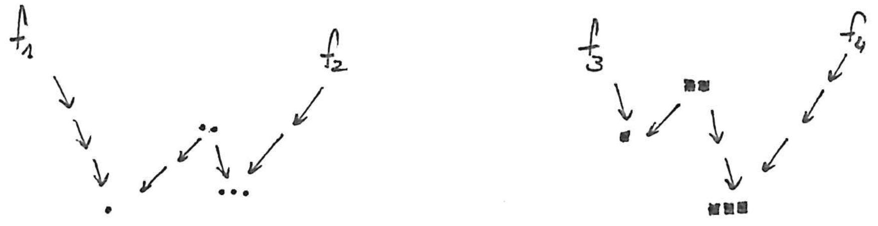
e. if $f_1 \xleftrightarrow{G} f_2$ and $f_3 \xleftrightarrow{G} f_4$, then $f_1 + f_3 \xleftrightarrow{G} f_2 + f_4$

f. if $f_1 \xleftrightarrow{G} f_2$ and $\tilde{f} \in P$, then $\tilde{f} \cdot f_1 \xleftrightarrow{G} \tilde{f} \cdot f_2$

g. $f \xleftrightarrow{G} 0$ se e solo se $f \in (g_1, \dots, g_s)$

h. $f_1 \xleftrightarrow{G} f_2$ se e solo se $f_1 - f_2 \in (g_1, \dots, g_s)$

<u>Proof</u>: first of all, we notice that it suffices to prove a., b., c., d., g.
in fact, e. follows from d., since if we have



then $f_1 + f_3 \xleftrightarrow{G} \bullet + f_3 \xleftrightarrow{G} \bullet\bullet + f_3 \xleftrightarrow{G} \bullet\bullet\bullet + f_3 \xleftrightarrow{G} f_2 + f_3$

$f_2 + f_3 \xleftrightarrow{G} \blacksquare + f_2 \xleftrightarrow{G} \blacksquare\blacksquare + f_2 \xleftrightarrow{G} \blacksquare\blacksquare\blacksquare + f_2 \xleftrightarrow{G} f_2 + f_4$

moreover, f. follows from b. and from e. by writing $\tilde{f}$ as a sum of monomials; finally, h. follows from e. and g. once we notice that $f_1 \xleftrightarrow{G} f_2$ if and only if $f_1 - f_2 \xleftrightarrow{G} 0$

so, let us prove the missing properties

a. let us consider the full chain of reductions of $f_1 \xrightarrow{G} f_2 \xrightarrow{G} f_1$:

$$f_1 = f'_0 \xrightarrow{g_{i_1}} f'_1 \xrightarrow{g_{i_2}} \dots \xrightarrow{g_{i_t}} f'_t = f_1$$

for some index $k \in \{0, \dots, t\}$ we have $f'_k = f_2$; now, let t be the largest term that gets reduced in this chain; by construction and by the definition of reduction this is a term that is present in f_1, but then gets reduced and can never appear again, but this contradicts the fact that we have again f_1 at the end of the chain; therefore every reduction must be a trivial reduction, namely $f_1 = f_2$

b. this is true since $t \cdot f_1 \xrightarrow{g_i} t \cdot f_2$ is implied by $f_1 \xrightarrow{g_i} f_2$

c. suppose that there exists a chain $f_1 \xrightarrow{g_{i_1}} f_2 \xrightarrow{g_{i_2}} \dots$ that does not become stationary; first of all, notice that every f_i must have a term in its support that eventually reduces; otherwise, in fact, from a certain point on all reductions would be trivial; then for each $i \in \mathbb{N}$, there exists a term $t_i \in \operatorname{supp}(f_i)$ which is the largest term that gets eventually reduced; however then we have $t_1 \geq t_2 \geq \dots$ and by Dickson's lemma this chain must eventually get stationary, which is in contradiction with the fact that each of the t_i gets reduced.

d. we suppose that $f_1 \xrightarrow{g_i} f_2$, and we write $f_2 = f_1 - c\cdot t\cdot g_i$ with $c \in k$ and $t \in \mathbb{T}^n$; we may assume that $c \neq 0$, otherwise the result follows immediately; we set c' to be the coefficient of $t\cdot LT_\leq(g_i)$ in the polynomial f_3 and we distinguish two scenarios

i. $c' = -c$, then $f_1 + f_3 = f_2 + f_3 + c\cdot t\cdot g = f_2 + f_3 - c'\cdot t\cdot g_i$

now, the coefficient of $t\cdot LT_\leq(g_i)$ is zero in $f_2 + f_3 - c' t\cdot g_i$,

so $f_2 + f_3 \xrightarrow{g_i} f_1 + f_3$, so we can choose $f_4 := f_1 + f_3$

ii. $c' \neq -c$, we define

$$f_4 := f_1 + f_3 - (c+c')t g_i = f_2 + f_3 - c' t\cdot g_i$$

then again the coefficient of $t\cdot LT_\leq(g_i)$ vanishes in f_4, so the claim follows

g. suppose that $f \xleftrightarrow{G} 0$, then we have a diagram of the form

$$\begin{tikzcd} f \arrow[dr] & & f_2 \arrow[dl] \arrow[dr] & \\ & f_1 & & 0 \end{tikzcd}$$

then following the diagram, we have

$$\left.\begin{aligned} f &= f_1 + \sum \lambda_i g_i \\ f_2 &= f_1 + \sum \mu_i g_i \\ f_2 &= 0 + \sum \nu_i g_i \end{aligned}\right\} \Rightarrow \begin{aligned} f = \sum \lambda_i g_i + \\ + \sum \nu_i g_i - \\ - \sum \mu_i g_i \end{aligned}$$

so we can always write $f = \sum f_i g_i$, namely $f \in (g_1, \dots, g_s)$

conversely, suppose that $f = \sum f_i g_i$, then if we prove that for all $i \in \{1, \dots, s\}$ we have $f_i g_i \xleftrightarrow{G} 0$, then by e. we conclude;

now, $g_i \xleftrightarrow{G} 0$ and using f. we have $f_i g_i \xleftrightarrow{G} 0$

Unfortunately, property g. cannot be used to algorithmically check ideal membership, since the arrows in the needed reductions might point in the "wrong" direction.

<u>Prop</u>: let $g_1, \dots, g_s \in k[x_1, \dots, x_n]$ be nonzero polynomials, let $G := \{g_1, \dots, g_s\}$, and let $I := (g_1, \dots, g_s)$; the following conditions are equivalent:

C1. $f \xrightarrow{G} 0$ if and only if $f \in I$

C2. if f is irreducible with respect to $\xrightarrow{G}$ and $f \in I$, then $f = 0$

C3. for every $f_1 \in k[x_1, \dots, x_n]$ there exists a unique $f_2 \in k[x_1, \dots, x_n]$ such that $f_1 \xrightarrow{G} f_2$ and f_2 is irreducible with respect to the relation $\xrightarrow{G}$

C4. if $f_1 \xrightarrow{G} f_2$ and $f_1 \xrightarrow{G} f_3$, then there exists $f_4 \in k[x_1, \dots, x_n]$ such that $f_2 \xrightarrow{G} f_4$ and $f_3 \xrightarrow{G} f_4$

$$\begin{tikzcd} & f_2 \arrow[dr, dashed] & \\ f_1 \arrow[ur, "G"] \arrow[dr, "G"'] & & f_4 \\ & f_3 \arrow[ur, dashed] & \end{tikzcd}$$

we say in this case that $\xrightarrow{G}$ is <u>confluent</u>

Proof. $C_1 \Rightarrow C_2$ suppose that $f \in I$, then by C_1, $f \xrightarrow{G} 0$; since f is supposed to be irreducible then $f = 0$

$C_2 \Rightarrow C_3$ let $f_1 \in k[x_1, \dots, x_n]$; we already know that there exists f_2 with $f_1 \xrightarrow{G} f_2$ and f_2 is irreducible (since chains of reductions eventually stabilize); suppose now that there exists another polynomial f_2' with the same properties, then $f_2 - f_2' \in I$

since $f_2 - f_2' \xleftrightarrow{G} 0$; moreover, the polynomial $f_2 - f_2'$ is irreducible with respect to $\xrightarrow{G}$ by construction of f_2 and f_2', because no element in $supp(f_2) \cup supp(f_2')$ is a multiple of one of $LT_\leq(g_1), \dots, LT_\leq(g_s)$; hence by C_2 $f_2 - f_2' = 0$, so we get the uniqueness in the statement

$C_3 \Rightarrow C_4$. notice that we can get to the situation

$$\begin{tikzcd} & f_2 \arrow[r, "G"] & f_2' \\ f_1 \arrow[ur, "G"] \arrow[dr, "G"'] & & \\ & f_3 \arrow[r, "G"'] & f_3' \end{tikzcd}$$

with both f_2' and f_3' irreducible with respect to $\xrightarrow{G}$

but then $f_1 \xrightarrow{G} f_2'$ and $f_1 \xrightarrow{G} f_3'$ with f_2' and f_3' irreducible, so by C_3 we have $f_2' = f_3'$

$C_4 \Rightarrow C_1$. we know that $f \in I$ if and only if $f \xleftrightarrow{G} 0$, so in order to prove C_1 we need to show $f \xleftrightarrow{G} 0$ if and only if $f \xrightarrow{G} 0$, which hence amounts to proving $f \xrightarrow{G} 0$ knowing $f \xleftrightarrow{G} 0$; let then $f_1, \dots, f_t$, where $f_1 = f$ and $f_t = 0$ a 'roof" that witnesses $f \xleftrightarrow{G} 0$, namely, $f_i \xrightarrow{G} f_{i+1}$ or $f_{i+1} \xrightarrow{G} f_i$; let $l \in \{1, \dots, t-2\}$ be the largest index such that $f_{l+1} \xrightarrow{G} f_l$; then $f_{l+1} \xrightarrow{G} 0$ and $f_{l+1} \xrightarrow{G} f_l$, which implies by C_4 that $f_l \xrightarrow{G} 0$; then we can replace the sequence $f_1, \dots, f_t$ by the sequence $f_1, \dots, f_l, 0$ and proceed by induction.

Our goal is now to show that properties $G_1, \dots, G_4$ are actually equivalent to the condition of being a Gröbner basis. The first step we take is to prove that $G_1, \dots, G_4$ are equivalent to (given $I = (g_1, \dots, g_s)$)

A_2. for every $f \in I$, there are $f_1, \dots, f_s \in k[x_1, \dots, x_n]$ such that

$$f = \sum_{i=1}^{s} f_i g_i \quad \text{and} \quad LT_{\leq}(f) = \max\{LT_{\leq}(f_i g_i) : i \in \{1, \dots, s\},\ f_i g_i \neq 0\}$$

The key to this is provided by the following lemma.

<u>Lemma</u>: let $g_1, \dots, g_s$ be non-zero polynomials, let $G := \{g_1, \dots, g_s\}$ and $I := (g_1, \dots, g_s)$

assume that some $f \in I \setminus \{0\}$ satisfies $f \xrightarrow{G} 0$

a. there exists $\alpha \in \{1, \dots, s\}$ and $t \in \mathbb{T}^n$ such that

$$LT_{\leq}(f) = t \cdot LT_{\leq}(g_\alpha)$$

b. there are $f_1', \dots, f_s' \in k[x_1, \dots, x_n]$ such that

$$f - \frac{LC_{\leq}(f)}{LC_{\leq}(g_\alpha)} \cdot t \cdot g_\alpha = \sum_{i=1}^{s} f_i' g_i$$

with $LT_{\leq}(f) > LT_{\leq}(f_i' g_i)$ for all i with $f_i' g_i \neq 0$

c. if we set $f_i := f_i'$ for $i \neq \alpha$ and $f_\alpha = f_\alpha' + \frac{LC_{\leq}(f)}{LC_{\leq}(g_\alpha)} \cdot t$,

then $f = \sum_{i=1}^{s} f_i g_i$ and $LT_{\leq}(f) = \max\{LT_{\leq}(f_i g_i) : f_i g_i \neq 0\}$

Proof: a. this is true since $LM_{\leq}(f)$ must be reduced in some step

b. let us write

$$f = f_1 \xrightarrow{g_{i_1}} \dots \xrightarrow{g_{i_t}} m_t \longrightarrow 0$$

then by a. there exists a step in the reduction when $LT_{\leq}(f)$ is reduced, and this step is unique, since the reduction substitutes $LM_\leq(f)$ with smaller monomials in the term order; so there exists some $g_\alpha \in G$ and some step $l \in \{1, \dots, t-1\}$ such that

$$f_l - \frac{LC_\leq(f)}{LC_\leq(g_\alpha)} \cdot t \cdot g_\alpha = f_{l+1}$$

when $LM_\leq(f)$ gets reduced; then

$$f - \frac{LC_\leq(f)}{LC_\leq(g_\alpha)} \cdot t \cdot g_\alpha = f - (f_l - f_{l+1})$$

$$= \underbrace{\sum_{i=1}^{l-1} (m_i - m_{i+1}) + \sum_{i=l+1}^{t} (m_i - m_{i+1})}_{\text{this is of the form } \sum_j f_j' g_j}$$

now, the polynomials $\{f_j'\}$ are obtained by collecting all contributions of the form $c_\beta \cdot t_\beta \cdot g_\beta$ that appear in the reductions; however, we know that if $m_i - m_{i+1} = c_\beta t_\beta g_\beta$, then by the definition of reduction it holds $LT_\leq(m_i) \geq t_\beta \cdot LT_\leq(g_\beta)$, so since $LT_\leq(f)$ is eliminated exactly once, we get that

$$LT_\leq(f_j' g_j) < LT_\leq(f) \quad \forall j$$

c. this follows from b. by construction.

We are ready to prove the equivalence.

Prop.: let $g_1, \dots, g_s \in k[x_1, \dots, x_n]$ be non-zero polynomials, let $G = \{g_1, \dots, g_s\}$ and let $I := (g_1, \dots, g_s)$; then conditions C_1, C_2, C_3 and C_4 are equivalent to condition A_2

Proof: $A_2 \Rightarrow C_2$ suppose that there exists a nonzero $f \in I$ that is irreducible with respect to $\xrightarrow{G}$, by A_2, we can write

$$f = \sum_{i=1}^{s} f_i g_i \quad \text{with} \quad LT_\leq(f) = \max\{LT_\leq(f_i g_i) : f_i g_i \neq 0\}$$

let $t \cdot LT_\leq(g_i)$ the term that achieves the maximum, then if we set $f' := f - \frac{LC_\leq(f)}{LC_\leq(g_i)} \cdot t \cdot g_i$ we have that $f \xrightarrow{G} f'$ and $f' \neq f$, which is a contradiction to the irreducibility of f.

$C_2 \Rightarrow A_2$ follows immediately from part c. of the previous lemma.

Property A_2 is equivalent to another one that seems weaker.

Prop: let $I \subseteq k[x_1, \dots x_n]$ be an ideal, let $g_1, \dots g_s \in k[x_1, \dots, x_n]$ be non-zero polynomials; the following are equivalent

A_1. for every $f \in I$, we can write $f = \sum f_i g_i$ with

$$LT_\leq(f) \geq LT_\leq(f_i g_i) \quad \text{for all } i \text{ s.t. } f_i g_i \neq 0$$

A_2. for every $f \in I$, we can write $f = \sum f_i g_i$ with

$$LT_\leq(f) = \max\{LT_\leq(f_i g_i) : f_i g_i \neq 0\}$$

Proof: $A_2 \Rightarrow A_1$ follows by definition

$A_1 \Rightarrow A_2$, by A_1 we have that $LT_\leq(f) \leq \max\{LT_\leq(f_i g_i) : f_i g_i \neq 0\}$ while the other inequality simply follows from the properties of the leading term with respect to the sum.

We are finally ready to show that Gröbner bases solve the confluence problem:

We have already proven the following statement.

<u>Prop</u>: let $I \subseteq k[x_1, \dots, x_n]$ be an ideal, let $g_1, \dots g_s \in k[x_1, \dots, x_n]$ be non-zero polynomials, then the following are equivalent:

B_1. $\{LT_{\leq}(g_1), \dots, LT_{\leq}(g_s)\}$ generates $LT_{\leq}\{I\}$ ($\mathbb{T}^n$ - mono ideal)

B_2: $\{LT_{\leq}(g_1), \dots, LT_{\leq}(g_s)\}$ generates $LT_{\leq}(I)$, (ideal)

(i.e., $G = \{g_1, \dots g_s\}$ is a Gröbner basis for I)

Here comes the final equivalence

<u>Prop</u>: let $I \subseteq k[x_1, \dots, x_n]$ and let $g_1, \dots g_s \in I$ be nonzero polynomials; then conditions A_1 and A_2 are equivalent to conditions B_1 and B_2

Proof: $A_2 \Rightarrow B_1$ in fact, suppose $t \in LT_{\leq}(I)$; this means that there exists $f \in I$ such that $LT_{\leq}(f) = t$; by A_2 we have that $f = \sum f_i g_i$ with $LT_{\leq}(f)$ being the maximum of $LT_{\leq}(f_i g_i)$; but then $t = t' \cdot LT_{\leq}(g_i)$ for some $i \in \{1, \dots, s\}$

$B_1 \Rightarrow A_1$ suppose that there exists $f \in I \setminus \{0\}$ that cannot be written in the form $f = \sum f_i g_i$ with $LT_{\leq}(f_i g_i) \leq LT_{\leq}(f)$; since $\leq$ is a well-order, there exists an element in $I \setminus \{0\}$ that satisfies this property and has minimal leading term; by B_1, we have $LT_{\leq}(f) = t \cdot LT_{\leq}(g_i)$ for some $i \in \{1, \dots, s\}$; then $f - \frac{LC_{\leq}(f)}{LC_{\leq}(g_i)} \cdot t \cdot g_i \neq 0$, because $f = \frac{LC_{\leq}(f)}{LC_{\leq}(g_i)} \cdot t \cdot g_i$ would satisfy A_1; then this new element has smaller leading term, so it satisfies A_1, but then also f satisfies A_1, a contradiction