In the proof of Buchberger's Criterion (Theorem 7.14) the key part was the deduction

$$\overline{S(g_i, g_j)}^G = 0 \implies S(g_i, g_j) = \sum q_k g_k \text{ where}$$
$$\text{multideg}(q_k g_k) \leq \text{multideg } S(g_i, g_j)$$
$$< \text{multideg lcm}(LM(g_i), LM(g_j))$$

This is also the only part where we used $\overline{S(g_i, g_j)}^G = 0$.
This observation leads to two useful variants of the criterion.

Definition 7.26

Let $P = \{p_1, \ldots, p_s\} \subset k[x_1, \ldots, x_n]$
A sum expression
$$S = \sum_{k=1}^{s} q_k p_k$$
is a

(i) standard representation if
$$\text{multideg}(q_k p_k) \leq \text{multideg } S \quad \text{when } q_k p_k \neq 0$$
(ii) lcm representation of $S = S(p_i, p_j)$ if
$$\text{multideg}(q_k p_k) < \text{multideg lcm}(LM(p_i), LM(p_j))$$
when $q_k p_k \neq 0$.

Theorem 7.27

A basis $G = \{g_1, \dots, g_s\}$ of an ideal I is a Gröbner basis

$\iff \overline{S(g_i, g_j)}^G = 0 \quad \forall i \forall j$ (Buchberger's Criterion)

$\iff S(g_i, g_j)$ has a standard representation $\forall i \forall j$

$\iff S(g_i, g_j)$ has a lcm representation $\forall i \forall j$

Proof

Repeat the proof of Buchberger's Criterion. For "$\Rightarrow$" observe that $\overline{S(g_i, g_j)}^G = 0$ implies that polynomial division gives both a standard and lcm representation. $\square$

Example 7.28

lcm rep $\overset{(1)}{\not\Rightarrow}$ standard rep $\overset{(2)}{\not\Rightarrow}$ zero remainder:

(1) Consider $p_1 = xz+1$, $p_2 = yz+1$, $p_3 = xz - x + y + 1$ in lex:

$$S(p_1, p_2) = -x + y = -1 \cdot p_1 + 0 \cdot p_2 + 1 \cdot p_3$$

Then $LM(q_1 p_1) = LM(q_3 p_3) = xz$

and $xz < xyz = lcm(LM(p_1), LM(p_2))$

but $xz > x = LM(S(p_1, p_2))$

(2) Follows from Example 7.22.

Moral: lcm $\Leftrightarrow$ standard $\Leftrightarrow$ zero remainder

ONLY FOR GRÖBNER BASES

8. ELIMINATION THEORY

In Example 7.24 $p_1 = p_2 = p_3 = g = 0$ was solved as follows:

- Define the ideal $I = \langle p_1, p_2, p_3, g \rangle \subset \mathbb{R}[\lambda, x, y, z]$
- <u>Elimination step</u>: find $g_7 \in I$ with fewer variables, $g_7 \in \mathbb{R}[z]$
- Solve the simpler problem $g_7 = 0$
- <u>Extension step</u>: Extend solutions of $g_7 = 0$ to solutions of the whole problem

Goal: Formalize this as a general method.

<u>Definition 8.1</u>

Let $I < K[x_1, \ldots, x_n]$ be an ideal.
The l-th elimination ideal of I is

$$I_l := I \cap K[x_{l+1}, \ldots, x_n]$$

<u>Remark</u>

- in Example 7.24, $g_7 \in \mathbb{R}[z]$ is in the third elimination ideal $I_3 = I \cap \mathbb{R}[z]$.
- $I = I_0$ is the zero-th elimination ideal
- each I_l is an ideal in $K[x_{l+1}, \ldots, x_n]$ (but not in $K[x_1, \ldots, x_n]$)

Theorem 8.2 (Elimination Theorem)
Let $I \subset K[x_1, \ldots, x_n]$ be an ideal and $G \subset I$ a Gröbner basis in the lex order.
Then for every $0 \leq l \leq n$,

$$G_l := G \cap K[x_{l+1}, \ldots, x_n]$$

is a Gröbner basis of the l-th elimination ideal I_l.

Proof

Since $G \subset I$, we have $G_l \subset I_l$
so in order to prove $\langle LT(G_l)\rangle = \langle LT(I_l)\rangle$.
we need to show :

$$\forall f \in I_l \quad \exists g \in G_l : \quad LT(g) \mid LT(f)$$

Let $f \in I_l \subset I$. G is a Gröbner basis of I, so $LT(g) \mid LT(f)$ for some $g \in G$.

Claim: $g \in I_l$.

Proof of claim: Since $f \in K[x_{l+1}, \ldots, x_n]$, any monomial x^α that contains any of $x_1, \ldots, x_l$ would satisfy $x^\alpha > LT(f)$ in lex.
Since $LT(g) \mid LT(f)$, we have $LT(g) \leq LT(f)$ and hence $g \in K[x_{l+1}, \ldots, x_n]$ $\square$

Example 8.3

Consider the polynomial system

$$xy = 1$$
$$xz = 1$$

in $\mathbb{R}[x,y,z]$.

Define $I = \langle xy-1, xz-1 \rangle$

A single S-polynomial computation gives

$$S(xy-1, xz-1) = y - z$$

and we find a reduced Gröbner basis in the lex order:

$$G = \{ xz-1, y-z \}$$

Here $LT(y-z) \mid LT(xy-1)$ so $xy-1$ is redundant.

From G, we deduce the elimination ideals

$$I = I_0 = \langle xz-1, y-z \rangle$$
$$I_1 = I \cap \mathbb{R}[y,z] = \langle y-z \rangle$$
$$I_2 = I \cap \mathbb{R}[z] = \{0\}$$

Consider the variety

$$V(I) = \{ (a_1, a_2, a_3) \in \mathbb{R}^3 \quad a_1 a_3 - 1 = a_2 - a_3 = 0 \}$$

From $I_1 = \langle y-z \rangle \subset \mathbb{R}[y,z]$ we obtain <u>partial solutions</u>:

$$(a_2, a_3) \in V(I_\ell) \iff a_2 = a_3$$

so

$$V(I_\ell) = \{ (a,a) : a \in \mathbb{R} \}$$

We want to extend partial solutions $(a,a) \in V(I_1)$ to complete solutions $(a_1, a, a) \in V(I)$, $a_1 \in \mathbb{R}$.

Problem: this is not possible for all (a,a).

$(0,0) \in V(I_1)$ but for $p = xz - 1$ we have

$$p(a_1, 0, 0) = a_1 \cdot 0 - 1 = -1 \neq 0.$$

For $a \neq 0$, we instead find

$$p(a_1, a, a) = a_1 \cdot a - 1 = 0 \iff a_1 = 1/a$$

so we get the solution $(1/a, a, a) \in V(I)$.

<u>Theorem 8.4</u> (Extension Theorem)

Let K be an algebraically closed field and $I = \langle p_1, \dots, p_s \rangle \subset K[x_1, \dots, x_n]$.

Give each generator p_i a <u>x_1-decomposition</u>:

$$p_i = c_i \cdot x_1^{N_i} + r_i, \quad \text{where}$$

N_i = largest exponent of x_1 appearing in p_i,

$c_i \in K[x_2, \dots, x_n]$, $c_i \neq 0$,

all monomials of r_i include x_1^m with $0 \leq m < N_i$.

Let $(a_2, \dots, a_n) \in V(I_1)$ be a partial solution in the first elimination ideal.

If $(a_2, \dots, a_n) \notin V(c_1, \dots, c_s)$,

then $\exists a_1 \in K$ s.t. $(a_1, a_2, \dots, a_n) \in V(I)$.

Example 8.5

(1) In Example 8.3 we had

$$p_1 = xz - 1 = z \cdot x^1 - 1 \qquad c_1 = z$$
$$p_2 = xy - 1 = y \cdot x^1 - 1 \qquad c_2 = y$$

so $V(c_1, c_2) = \{(a_2, a_3) : a_2 = a_3 = 0\} = \{(0,0)\}$

(2) Algebraically closed is necessary:

For $I = \langle x^2 - y, x^2 - z \rangle \subset \mathbb{R}[x,y,z]$

$I_1 = \langle y - z \rangle$

so again we have the partial solutions

$V(I_1) = \{(a,a) : a \in \mathbb{R}\}$

but $x^2 - a$ has solutions $x \in \mathbb{R}$ only for $a \geq 0$.

Corollary 8.6

Let K be algebraically closed and $I = \langle p_1, \ldots, p_s \rangle \subset K[x_1, \ldots, x_n]$.

Suppose in the x_1-decompositions $p_i = c_i \cdot x^{N_i} + r_i$, one of the generators has a constant $c_i \in K$, $c_i \neq 0$.

Then all partial solutions $(a_2, \ldots, a_n) \in V(I_1)$ extend to complete solutions $(a_1, \ldots, a_n) \in V(I)$

Proof

$V(c_1, \ldots, c_s) \subset V(c_i) = \{a \in K^{n-1} : c_i = 0\} = \emptyset$ $\square$

The strategy to prove Theorem 8.4 will be

- take a lex Grobner basis $G = \{g_1, \ldots, g_t\}$
- for $\bar{a} = (a_2, \ldots, a_n) \in V(I_1)$, consider the ideal

$J := I_{(x_2, \ldots, x_n) = \bar{a}} := \{ f(x_1, \bar{a}) : f \in I\} \subset k[x_1]$

- univariate ideals are principal.

  Show that $\exists g \in G$ such that

  $J = \langle g(x_1, \bar{a}) \rangle$ (the hard part!)

- choose $a_1 \in k$ as a root of $g(x_1, \bar{a}) \in k[x_1]$

For $f \in k[x_1, \ldots, x_n]$ nonzero write the x_1-decomposition as

$$f = c_f \cdot x_1^{N_f} + r_f$$

with $c_f = c_f(x_2, \ldots, x_n) \in k[x_2, \ldots, x_n]$, $N_f \geq 0$.

We will denote

$$\deg(f, x_1) := N_f$$

When $f = 0$, set $c_f = 0$.

<u>Lemma 8.7</u>

Let $S = \sum_{i=1}^{t} q_i g_i$ be a standard representation for lex order. Then

(i) $\deg(S, x_1) \geq \deg(q_i g_i, x_1)$ whenever $q_i g_i \neq 0$

(ii) $$c_S = \sum_{\deg(q_i g_i, x_1) = \deg(f, x_1)} c_{q_i} \cdot c_{g_i}$$

Proof

(i) In the standard representation $S = \sum q_i g_i$

we have $LM(q_i g_i) \leq LM(S)$ whenever $q_i g_i \neq 0$.

By definition of lex order we obtain

$$\deg(q_i g_i, x_1) \leq \deg(S, x_1)$$

(ii) Consider the x_1-decompositions

$$q_i = c_{q_i} x^{N_{q_i}} + r_{q_i}$$

$$g_i = c_{g_i} x^{N_{g_i}} + r_{g_i}$$

$$S = c_S x^{N_S} + r_S$$

Then

$$q_i g_i = c_{q_i} c_{g_i} x^{N_{q_i} + N_{g_i}} \underbrace{+ c_{q_i} x^{N_{q_i}} r_{g_i} + c_{g_i} x^{N_{g_i}} r_{q_i} + r_{q_i} r_{g_i}}_{\text{terms with } x_1\text{-degree smaller than } N_{q_i} + N_{g_i}}$$

Hence

$$c_S = \sum_{N_{q_i} + N_{g_i} = N_S} c_{q_i} c_{g_i} \qquad \square$$