Theorem 7.14 (Buchberger's criterion)

Let $I \subset k[x_1, \dots, x_n]$ be an ideal and $G = \{g_1, \dots, g_s\}$ a basis of I.
Then G is a Gröbner basis of I if and only if
the remainder $\overline{S(g_i, g_j)}^G$ is zero for all i, j.

Proof

"$\Rightarrow$" Since $S(g_i, g_j) \in I$, Corollary 7.9 $\Rightarrow$ $\overline{S(g_i, g_j)}^G = 0$

"$\Leftarrow$" Let $0 \neq f \in I$. Need to show $LT(f) \in \langle LT(g_1), \dots, LT(g_s) \rangle$.

Since G is a basis

$$f = \sum_{i=1}^{s} h_i g_i, \quad h_1, \dots, h_s \in k[x_1, \dots, x_n]$$

however $h_1, \dots, h_s$ are not unique.

Choose $h_1, \dots, h_s$ such that

$$\delta := \max\{\text{multideg}(h_i g_i) : 1 \leq i \leq s\}$$

is minimal. (possible by the well-order property)

By Lemma 5.8 we have

$$\text{multideg}(f) \leq \delta$$

If $\text{multideg}(f) = \delta = \text{multideg}(h_i g_i)$ then by Lemma 5.8

$$LM(f) = LM(h_i) LM(g_i)$$

So $LT(f) \in \langle LT(g_1), \dots, LT(g_s) \rangle$ and we are done.

We will next show that $\text{multideg}\, f < \delta$
would contradict the assumption $\overline{S(g_i, g_j)}^G = 0$.

Suppose multideg $f < \delta$. Split

$$\{1, \dots, s\} = A \sqcup B,$$

where $A = \{ i : \text{multideg}(h_i g_i) = \delta \}$, $B = \{1, \dots, s\} \setminus A$

Then $f = \sum_{i=1}^{s} h_i g_i = \sum_{i \in A} h_i g_i + \sum_{i \in B} h_i g_i$

$$(*) \quad = \underbrace{\sum_{i \in A} LT(h_i) g_i}_{\text{multideg} = \delta} + \underbrace{\sum_{i \in A} (h_i - LT(h_i)) g_i + \sum_{i \in B} h_i g_i}_{\text{multideg} < \delta}$$

Set $p_i := LT(h_i) g_i$.

Since multideg $f < \delta$, we have

$$\text{multideg}\left(\sum_{i \in A} p_i \right) < \delta, \qquad \text{multideg}(p_i) = \delta \quad \forall i \in A$$

By Lemma 7.13. $\sum_{i \in A} p_i$ is a K-linear combination of $S(p_i, p_j)$, $i, j \in A$.

By construction $LT(p_i) = LT(h_i) LT(g_i)$ and multideg p_i = multideg $p_j = \delta$ for $i, j \in A$. Hence

$$\text{lcm}(LM(p_i), LM(p_j)) = x^\delta \text{ and}$$

$$S(p_i, p_j) = \frac{x^\delta}{LT(p_i)} p_i - \frac{x^\delta}{LT(p_j)} p_j$$

$$= \frac{x^\delta}{\cancel{LT(h_i)} LT(g_i)} \cancel{LT(h_i)} g_i - \frac{x^\delta}{\cancel{LT(h_j)} LT(g_j)} \cancel{LT(h_j)} g_j$$

$$= x^{\delta - \gamma_{ij}} S(g_i, g_j), \quad \gamma_{ij} := \text{lcm}(LM(g_i), LM(g_j))$$

By assumption $\overline{S(g_i, g_j)}^{G} = 0$, so the division algorithm gives

$$S(g_i, g_j) = \sum_{k=1}^{s} q_k g_k, \quad \text{multideg}(q_k g_k) \le \text{multideg } S(g_i, g_j)$$

Hence

$$S(p_i, p_j) = \sum_{k=1}^{s} x^{\delta - \gamma_{ij}} q_k g_k$$

and $\text{multideg}(x^{\delta-\gamma_{ij}} q_k g_k) \le \text{multideg } S(p_i, p_j) \overset{\text{Lemma 7.13(1)}}{<} \delta$.

Putting everything together, we are able to write $\sum_{i \in A} p_i$ as a K-linear combination of polynomials $x^{\delta - \gamma_{ij}} q_k g_k$ with multideg $< \delta$.

By $\circledast$ we have $f = \sum_{i=1}^{s} \tilde{h}_i \cdot g_i$, $\text{multideg}(\tilde{h}_i \cdot g_i) < \delta$, which contradicts the choice of δ. $\square$

Example 7.15

$p_1 = -t + x - 1 \quad p_2 = -t^2 + y + 1 \quad f = x^2 - 2x - y$

1) In lex order on $\mathbb{Q}[t,x,y]$, $G = \{p_1, f\}$ is a Gröbner basis:

Example 7.12 $\Rightarrow$ $S(p_1, f) = 2tx + ty - x^3 + x^2$

Apply the division algorithm to $S(p_1, f)$ by (p_1, f)

g	r	q_1	q_2
$2tx + ty - x^3 + x^2$	0	0	0
$ty - x^3 + 3x^2 - 2x$	0	$-2x$	0
$-x^3 + 3x^2 + xy - 2x - y$	0	$-2x - y$	0
$x^2 - 2x - y$	0	$-2x - y$	$-x$
0	0	$-2x - y$	$-x + 1$

Buchberger's criterion $\Rightarrow$ $\{p_1, f\}$ is a Gröbner basis.

2) Example 6.13 $\Rightarrow$ $\{p_1, p_2\}$ is not a Gröbner basis

Example 7.12 $\Rightarrow$ $S(p_1, p_2) = -tx + t + y + 1$

Applying the division algorithm to $S(p_1, p_2)$ by (p_1, p_2) gives

g	r	q_1	q_2
$-tx + t + y + 1$	0	0	0
$t - x^2 + x + y + 1$	0	x	0
$-x^2 + 2x + y$	0	$x - 1$	0
0	$-x^2 + 2x + y$	$x - 1$	0

$\rightsquigarrow$ we reconstruct f using $S(p_1, p_2)$.

Theorem 7.16 (Buchberger's algorithm)

Let $I = \langle p_1, \dots, p_s \rangle$ be an ideal.

Apply the following algorithm:

1. Set $G := \{p_1, \dots, p_s\}$
2. Set $G' := G$
3. For each pair $\{p, q\} \subset G'$, $p \neq q$:
   Compute $r := \overline{S(p,q)}^{G'}$
   If $r \neq 0$, set $G := G \cup \{r\}$
4. If $G \neq G'$, go back to step 2.

Then after finitely many steps $G = G'$ and G is a Gröbner basis of I.

Proof

If $G \subset I$, then for any $p, q \in I$ also $S(p,q) \in I$ and $\overline{S(p,q)}^G \in I$.

Hence $\langle G \rangle \subset I = \langle p_1, \dots, p_s \rangle \subset \langle G \rangle$,

so G is a basis of I throughout the algorithm.

If the algorithm stops, then $\overline{S(p,q)}^G = 0$ for all $p, q \in G$, so G is a Gröbner basis by Buchberger's criterion.

So it remains to show that the algorithm stops after finitely many steps.

Consider the sets G', G after the loop in step 3.
Since $G' \subset G$, we have $\langle LT(G') \rangle \subset \langle LT(G) \rangle$.
If $G' \neq G$, then $\exists r = \overline{S(p,q)}^{G'} \in G \setminus G'$.
Division algorithm $\Rightarrow$ terms of r not divisible by $LT(g)$, $g \in G'$. Hence

$$LT(r) \notin \langle LT(G') \rangle \text{ but } LT(r) \in \langle LT(G) \rangle$$

so $\langle LT(G') \rangle \subsetneq \langle LT(G) \rangle$.

By the ACC (Theorem 7.5) after finitely many steps we must have $\langle LT(G') \rangle = \langle LT(G) \rangle$ so eventually $G = G'$ and the algorithm stops. $\square$

Example 7.17

Let $p_1 = x^3 - 2xy$ in $\mathbb{Q}[x,y]$ with deglex order

$p_2 = x^2y - 2y^2 + x$

Then $S(p_1, p_2) = -x^2$ and $\overline{S(p_1,p_2)}^{(p_1,p_2)} = -x^2 =: p_3$

$S(p_1, p_3) = -2xy$ $\quad \overline{S(p_1,p_3)}^{(p_1,p_2,p_3)} = -2xy =: p_4$

$S(p_2, p_3) = -2y^2 + x$ $\quad \overline{S(p_2,p_3)}^{(p_1,p_2,p_3)} = -2y^2 + x =: p_5$

The S-polynomials among $p_1, \ldots, p_5$ are

	p_1	p_2	p_3	p_4	p_5
p_1	$-$	p_3	p_4	$-2xy^2$	$\frac{1}{2}x^4 - 2xy^3$
p_2		$-$	p_5	$-2y^2 + x$	$\frac{1}{2}x^3 - 2y^3 + xy$
p_3			$-$	0	$\frac{1}{2}x^3$
p_4				$-$	$\frac{1}{2}x^2$

Here $\overline{S(p_i, p_j)}^{(p_1, \ldots, p_5)} = 0$ for all $1 \le i < j \le 5$

so $p_1, \ldots, p_5$ is a Gröbner basis.

Definition 7.18

A reduced Gröbner basis of an ideal $I \subset k[x_1, \ldots, x_n]$ is a Gröbner basis $G \subset I$ such that for all $g \in G$

(i) $LC(g) = 1$

(ii) No monomial of g is in $\langle LT(G \setminus \{g\}) \rangle$

Theorem 7.19

Let $I \neq \{0\}$ ideal. Fix a monomial order.
Then I has a unique reduced Gröbner basis.

Proof

Proposition 6.10 $\Rightarrow$ the monomial ideal $\langle LT(I) \rangle$ has a unique minimal basis

$$\langle LT(I) \rangle = \langle x^{\alpha_1}, \ldots, x^{\alpha_s} \rangle \qquad (*)$$

Start with a Gröbner basis $G = \{g_1, \ldots, g_s\}$, $LT(g_i) = x^{\alpha_i}$ and construct a reduced Gröbner basis as follows:

- For $g_1 \in G$ compute the remainder $r_1 := \overline{g_1}^{G \setminus \{g_1\}}$
  By minimality of $(*)$, $LT(g_i) = x^{\alpha_i} \nmid x^{\alpha_1} = LT(g_1)$ for $i \neq 1$, so $LT(r_1) = LT(g_1) = x^{\alpha_1}$
  $\Rightarrow \langle LT(r_1), LT(g_2), \ldots, LT(g_s) \rangle = \langle LT(g_1), \ldots, LT(g_s) \rangle = \langle LT(I) \rangle$
  So $\{r_1, g_2, \ldots, g_s\}$ is also a Gröbner basis of I.

- Repeat the construction to obtain

$$r_2 := \overline{g_2}^{(r_1, g_3, \dots, g_s)}$$
$$r_3 := \overline{g_3}^{(r_1, r_2, g_4, \dots, g_s)}$$
$$\vdots$$
$$r_s := \overline{g_s}^{(r_1, r_2, \dots, r_{s-1})}$$

Then $LT(r_i) = LT(g_i) = x^{\alpha_i}$, so we have

(i) $\{r_1, \dots, r_s\}$ is a Gröbner basis of I

(ii) $LC(r_i) = 1$

(iii) No term of r_i is divisible by any of
$$LT(r_1), \dots, LT(r_{i-1}), \underset{LT(r_{i+1})}{\underset{\shortparallel}{LT(g_{i+1})}}, \dots, \underset{LT(r_s)}{\underset{\shortparallel}{LT(g_s)}}$$

Hence $\{r_1, \dots, r_s\}$ is a reduced Gröbner basis.

To show uniqueness, let $G = \{r_1, \dots, r_s\}$ and $\tilde{G} = \{\tilde{r}_1, \dots, \tilde{r}_s\}$ be two reduced Gröbner bases.

Reordering elements if necessary, by uniqueness of $\circledast$
$$LT(r_i) = x^{\alpha_i} = LT(\tilde{r}_i)$$

Hence $r_i - \tilde{r}_i$ has no x^{α_i} term,

and also cannot have any $x^{\alpha_j} = LT(r_j) = LT(\tilde{r}_j)$ term

since G and $\tilde{G}$ are reduced. Hence
$$\overline{r_i - \tilde{r}_i}^{G} = r_i - \tilde{r}_i$$

and Corollary 7.9 $\Rightarrow$ $r_i - \tilde{r}_i = 0$ since $r_i - \tilde{r}_i \in I$. $\square$