Buchberger Algorithm Formalization

Sanghyeok0

October 24, 2025

Chapter 1

Finset

1.1 Piecewise

Lemma 1 (prod ite not mem)**.** *Let s, t be finite sets of indices in ι, and let $f : \iota \to M$. Then*

$$\prod_{x \in s} \begin{cases} 1, & \text{if } x \in t, \\ f(x), & \text{otherwise} \end{cases} = \prod_{x \in s \setminus t} f(x).$$

Proof. We split the product over the disjoint union $s = (s \setminus t) \cup (s \cap t)$.

$$\begin{aligned} \prod_{x \in s} \begin{cases} 1, & \text{if } x \in t \\ f(x), & \text{otherwise} \end{cases} &= \left(\prod_{x \in s \setminus t} f(x) \right) \cdot \left(\prod_{x \in s \cap t} 1 \right) \\ &= \prod_{x \in s \setminus t} f(x). \end{aligned}$$

The first equality holds because for any $x \in s \setminus t$, the term is $f(x)$, while for any $x \in s \cap t$, the term is 1. The product of ones is one. □

Lemma 2 (sum ite not mem)**.** *Let s, t be finite sets of indices in ι, and let $f : \iota \to A$ be a function to an additive commutative monoid. Then*

$$\sum_{x \in s} \begin{cases} 0, & \text{if } x \in t, \\ f(x), & \text{otherwise} \end{cases} = \sum_{x \in s \setminus t} f(x).$$

Proof. We split the sum over the disjoint union $s = (s \setminus t) \cup (s \cap t)$.

$$\begin{aligned} \sum_{x \in s} \begin{cases} 0, & \text{if } x \in t \\ f(x), & \text{otherwise} \end{cases} &= \left(\sum_{x \in s \setminus t} f(x) \right) + \left(\sum_{x \in s \cap t} 0 \right) \\ &= \sum_{x \in s \setminus t} f(x). \end{aligned}$$

The first equality holds because for any $x \in s \setminus t$, the term is $f(x)$, while for any $x \in s \cap t$, the term is 0. The sum of zeros is zero. □

Chapter 2

Orders and Abstract Reduction Relations

2.1 Monomial Ideals and Dickson's Lemma

Definition 3. Let r be a relation on M. Then r is called

1. **reflexive** if $\Delta(M) \subseteq r$,
2. **symmetric** if $r \subseteq r^{-1}$,
3. **transitive** if $r \circ r \subseteq r$,
4. **antisymmetric** if $r \cap r^{-1} \subseteq \Delta(M)$,
5. **connex** if $r \cup r^{-1} = M \times M$,
6. **irreflexive** if $\Delta(M) \cap r = \varnothing$,
7. **strictly antisymmetric** if $r \cap r^{-1} = \varnothing$,
8. an **equivalence relation** on M if r is reflexive, symmetric, and transitive,
9. a **quasi-order** (**preorder**) on M if r is reflexive and transitive,
10. a **partial order** on M if r is reflexive, transitive and antisymmetric,
11. a **(linear) order** on M if r is a connex partial order on M, and
12. a **linear quasi-order** on M if r is a connex quasi-order on M.

Definition 4. Let r be a relation on M with strict part r_s, and let $N \subseteq M$.

1. Then an element a of N is called *r-minimal* (*r-maximal*) in N if there is no $b \in N$ with $b\, r_s\, a$ (with $a\, r_s\, b$). For $N = M$ the reference to N is omitted.
2. A *strictly descending* (*strictly ascending*) r-chain in M is an infinite sequence $\{a_n\}_{n\in\mathbb{N}}$ of elements of M such that $a_{n+1}\, r_s\, a_n$ (such that $a_n\, r_s\, a_{n+1}$) for all $n \in \mathbb{N}$.

3. The relation r is called **well-founded** (**noetherian**) if every non-empty subset N of M has an r-minimal (an r-maximal) element. r is a **well-order** on M if r is a well-founded linear order on M.

Definition 5 (The "Antisymmetrization" of M)**.** Let $(M, \leq)$ be a preordered set. Define an equivalence relation

$$\sim : M \times M \to \text{Prop}, \qquad a \sim b \iff (a \leq b \wedge b \leq a).$$

We write $[a]$ for the equivalence class of a, and denote the quotient by

$$\text{Quot}(M, \sim) = \{\, [a] \mid a \in M\}.$$

Definition 6 (Minimal elements and min–classes)**.** Let $N \subseteq M$. An element $b \in N$ is called *minimal in* N if

$$\forall\, y \in N,\ y \leq b \implies b \leq y.$$

We denote by

$$\text{Minimal}(N) = \{\, b \in N \mid \forall\, y \in N,\ y \leq b \to b \leq y\}$$

the set of all minimal elements of N. The *min–classes* of N are then

$$\text{minClasses}(N) = \{\, [b] \in \text{Quot}(M, \sim) \mid b \in \text{Minimal}(N)\}.$$

Definition 7. Let $\preceq$ be a quasi-order on M and let $N \subseteq M$. Then a subset B of N is called a **Dickson basis**, or simply **basis** of N w.r.t. $\preceq$, if for every $a \in N$ there exists some $b \in B$ with $b \preceq a$.

1. We say that $\preceq$ has the **Dickson property**, or is a **well-quasi-order**(wqo), if every subset N of M has a finite basis w.r.t. $\preceq$.

2. A **well partial order**, or a wpo, is a wqo that is a proper ordering relation, i.e., it is antisymmetric.

Proposition 8. *Let $\preceq$ be a quasi-order on M with associated equivalence relation $\sim$. Then the following are equivalent:*

1. *$\preceq$ is a well-quasi-order.*

2. *Whenever $\{a_n\}_{n\in\mathbb{N}}$ is a sequence of elements of M, then there exist $i < j$ with $a_i \preceq a_j$.*

3. *For every nonempty subset N of M, the number of min-classes in N is finite and non-zero.*

Proof. □

Proposition 9. *Let $\preceq$ be a well- quasi-order on M, and let $\{a_n\}_{n\in\mathbb{N}}$ be a sequence of elements of M. Then there exists a strictly ascending sequence $\{n_i\}_{i\in\mathbb{N}}$ of natural numbers such that $a_{n_i} \preceq a_{n_j}$ for all $i < j$.*

Proof. We define the sequence $\{n_i\}_{i\in\mathbb{N}}$ recursively, and by simultaneous induction on i we verify the following properties:

1. $a_{n_i} \preceq a_{n_{i+1}}$ for all $i \in \mathbb{N}$, and

2. for all $i \in \mathbb{N}$, the set $\{n \in \mathbb{N} \mid a_{n_i} \preceq a_n\}$ is infinite.

For $i = 0$, let $\{b_1, \dots, b_k\}$ be a finite basis of the set $\{a_n \mid n \in \mathbb{N}\}$, and for each j with $1 \leq j \leq k$, set

$$B_j = \{n \in \mathbb{N} \mid b_j \preceq a_n\}.$$

Then $\bigcup_{j=1}^{k} B_j = \mathbb{N}$ by the choice of B. Since the union of finitely many finite sets is finite, we can find a B_j which is infinite. Moreover, $b_j = a_m$ for some $m \in \mathbb{N}$, and we set $n_0 = m$. For $i + 1$, we consider the set

$$U_i = \{a_n \mid a_{n_i} \preceq a_n, n_i < n\}.$$

By condition (ii) for i, the set $\{n \in \mathbb{N} \mid a_n \in U_i\}$ is infinite. Choosing some finite basis of U_i, we can, as before, find an element a_m in this basis such that $a_m \preceq a_n$ for infinitely many different $n \in \mathbb{N}$, and we take $n_{i+1} = m$. Conditions (i) and (ii) obviously continue to hold. It now follows easily from condition (i) and the transitivity of $\preceq$ that $\{n_i\}_{i \in \mathbb{N}}$ has the desired property. □

Lemma 10. *Let $f, g \in k[x_1, \dots, x_n]$ be nonzero polynomials. Then:*

1. $\text{multideg}(fg) = \text{multideg}(f) + \text{multideg}(g)$.
2. *If $f + g \neq 0$, then* $\text{multideg}(f + g) \leq \max(\text{multideg}(f), \text{multideg}(g))$. *If, in addition,* $\text{multideg}(f) \neq \text{multideg}(g)$, *then equality occurs.*

Lemma 11. *Let ι be an index set and $s \subset \iota$ a finite subset. For each $i \in s$, let $h_i \in k[x_1, \dots, x_n]$. Then the following inequality holds:*

$$\text{multideg}\left(\sum_{i \in s} h_i\right) \leq \max_{i \in s} \{\text{multideg}(h_i)\}$$

where the max *is taken with respect to the monomial order.*

Proof. Let $M = \max_{i \in s}\{\text{multideg}(h_i)\}$. Any monomial x^b appearing in the sum $\sum_{i \in s} h_i$ must be a monomial in at least one of the summands, say h_{i_0} for some $i_0 \in s$. By definition, the multidegree of any such term is bounded by the multidegree of the polynomial it belongs to, so $b \leq \text{multideg}(h_{i_0})$. Also by definition, $\text{multideg}(h_{i_0}) \leq M$. Therefore, $b \leq M$ for any monomial x^b in the sum. This implies that the multidegree of the sum itself cannot exceed M. □

Lemma 12. *Let $I = \langle x^\alpha \mid \alpha \in A \rangle$ be a monomial ideal. Then a monomial x^β lies in I if and only if x^β is divisible by x^α for some $\alpha \in A$.*

Proof. If x^β is a multiple of x^α for some $\alpha \in A$, then $x^\beta \in I$ by the definition of ideal. Conversely, if $x^\beta \in I$, then $x^\beta = \sum_{i=1}^{s} h_i x^{\alpha(i)}$, where $h_i \in k[x_1, \dots, x_n]$ and $\alpha(i) \in A$. If we expand each h_i as a sum of terms, we obtain

$$x^\beta = \sum_{i=1}^{s} h_i x^{\alpha(i)} = \sum_{i=1}^{s} \left(\sum_j c_{i,j} x^{\beta(i,j)}\right) x^{\alpha(i)} = \sum_{i,j} c_{i,j} x^{\beta(i,j)} x^{\alpha(i)}.$$

□

Theorem 13. *Let $(\mathbb{N}^n, \leq')$ be the direct product of n copies of the natural numbers $(\mathbb{N}, \leq)$ with their natural ordering. Then $(\mathbb{N}^n, \leq')$ is a Dickson partially ordered set. More explicitly, every subset $S \subseteq \mathbb{N}^n$ has a finite subset B such that for every $(m_1, \dots, m_n) \in S$, there exists $(k_1, \dots, k_n) \in B$ with*

$$k_i \leq m_i \quad \text{for } 1 \leq i \leq n.$$

Proof. □

Theorem 14 (Dickson's Lemma (MvPolynomial))**.** *Let $I = \langle x^\alpha | \alpha \in A \rangle \subseteq k[x_1, \dots, x_n]$ be a monomial ideal. Then I can be written in the form $I = \langle x^{\alpha(1)}, \dots, \alpha(s) \rangle$, where $\alpha(1), \dots, \alpha(s) \in A$. In particular, I has a finite basis.*

Proof. □

Chapter 3

Gröbner Bases

3.1 Polynomial Reductions

Theorem 15 (Division Algorithm for Multivariate Polynomials)**.** *Let P be a subset of $K[X]$ and $f \in K[X]$. Then there exists a normal form $g \in K[X]$ of f modulo P and a family $\mathcal{F} = \{q_p\}_{p\in P}$ of elements of $K[X]$ with*

$$f = \sum_{p\in P} q_p\, p + g \quad \textit{and} \quad \max\{\mathrm{LT}(q_p p) \mid p \in P,\ q_p p \neq 0\} \leq \mathrm{LT}(f).$$

If P is finite, the ground field is computable, and the term order on T is decidable, then g and $\{q_p\}_{p\in P}$ can be computed from f and P.

Proof. □

3.2 Gröbner Bases-Existence and Uniqueness

Definition 16 (Initial Ideal)**.** Let $I \subseteq k[x_1, \ldots, x_n]$ be an ideal other than $\{0\}$, and fix a monomial ordering on $k[x_1, \ldots, x_n]$. Then:

1. We denote by
$$\mathrm{LT}(I) = \{\, c\, x^\alpha \mid \exists\, f \in I \setminus \{0\} \text{ with } \mathrm{LT}(f) = c\, x^\alpha\}.$$
2. We denote by $\langle \mathrm{LT}(I)\rangle$ the ideal generated by the elements of $\mathrm{LT}(I)$.

Theorem 17. *Let $I \subseteq k[x_1, \ldots, x_n]$ be an ideal different from $\{0\}$.*

1. *$\langle \mathrm{LT}(I)\rangle$ is a monomial ideal.*
2. *There are $g_1, \ldots, g_t \in I$ such that $\langle \mathrm{LT}(I)\rangle = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t)\rangle$.*

Proof. 1. The leading monomials $\mathrm{LM}(g)$ of elements $g \in I \setminus \{0\}$ generate the monomial ideal $\langle \mathrm{LM}(g) \mid g \in I \setminus \{0\}\rangle$. Since $\mathrm{LM}(g)$ and $\mathrm{LT}(g)$ differ by a nonzero constant, this ideal equals $\langle \mathrm{LT}(g) \mid g \in I \setminus \{0\}\rangle = \langle \mathrm{LT}(I)\rangle$. Thus, $\langle \mathrm{LT}(I)\rangle$ is a monomial ideal.

2. Since $\langle \mathrm{LT}(I)\rangle$ is generated by the monomials $\mathrm{LM}(g)$ for $g \in I \setminus \{0\}$, Dickson's Lemma tells us that $\langle \mathrm{LT}(I)\rangle = \langle \mathrm{LM}(g_1), \ldots, \mathrm{LM}(g_t)\rangle$ for finitely many $g_1, \ldots, g_t \in I$. Since $\mathrm{LM}(g_i)$ differs from $\mathrm{LT}(g_i)$ by a nonzero constant, it follows that $\langle \mathrm{LT}(I)\rangle = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t)\rangle$. This completes the proof.

□

Definition 18. Fix a monomial order $>$ on the polynomial ring $k[x_1, \dots, x_n]$. A finite subset $G = \{g_1, \dots, g_t\}$ of an ideal $I \subseteq k[x_1, \dots, x_n]$ different from $\{0\}$ is said to be a **Gröbner basis** (or **standard basis**) for I if the ideal generated by the leading terms of the elements in G is equal to the ideal generated by the leading terms of all elements in I. That is,

$$\langle \mathrm{LT}(g_1), \dots, \mathrm{LT}(g_t) \rangle = \langle \mathrm{LT}(I) \rangle,$$

where $\mathrm{LT}(I) = \{\mathrm{LT}(f) \mid f \in I \setminus \{0\}\}$. Using the convention that $\langle \varnothing \rangle = \{0\}$, we define the empty set $\varnothing$ to be the Gröbner basis of the zero ideal $\{0\}$.

Proposition 19. *Let $I \subseteq k[x_1, \dots, x_n]$ be an ideal and let $G = \{g_1, \dots, g_t\}$ be a Gröbner basis for I. Then given $f \in k[x_1, \dots, x_n]$ there is a unique $r \in k[x_1, \dots, x_n]$ with the following two properties:*

1. *No term of r is divisible by any of $\mathrm{LT}(g_1), \dots, \mathrm{LT}(g_t)$.*
2. *There is $g \in I$ such that $f = g + r$.*

In particular, r is the remainder on division of f by G no matter how the elements of G are listed when using the division algorithm.

Proof. The division algorithm gives $f = q_1 g_1 + \cdots + q_t g_t + r$, where r satisfies (i). We can also satisfy (ii) by setting $g = q_1 g_1 + \cdots + q_t g_t \in I$. This proves the existence of r. To prove uniqueness, suppose $f = g + r = g' + r'$ satisfy (i) and (ii). Then $r - r' = g' - g \in I$, so that if $r \neq r'$, then $\mathrm{LT}(r - r') \in \langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(g_1), \dots, \mathrm{LT}(g_t) \rangle$. By Lemma 12, it follows that $\mathrm{LT}(r - r')$ is divisible by some $\mathrm{LT}(g_i)$. This is impossible since no term of r, r' is divisible by one of $\mathrm{LT}(g_1), \dots, \mathrm{LT}(g_t)$. Thus $r - r'$ must be zero, and uniqueness is proved. The final part of the proposition follows from the uniqueness of r. □

Corollary 20 (Ideal Membership Problem)**.** *Let $G = \{g_1, \dots, g_t\}$ be a Gröbner basis for an ideal $I \subseteq k[x_1, \dots, x_n]$ (with respect to a given monomial order $>$) and let $f \in k[x_1, \dots, x_n]$. Then $f \in I$ if and only if the remainder on division of f by G is zero.*

$$f \in I \iff \mathrm{rem}(f, G) = 0.$$

Proof. If the remainder is zero, then we have already observed that $f \in I$. Conversely, given $f \in I$, then $f = f + 0$ satisfies the two conditions of Proposition 19. It follows that 0 is the remainder of f on division by G. □

Definition 21. We will write $\overline{f}^F$ for the remainder(normalform) on division of f by the ordered s-tuple

$$F = (f_1, \dots, f_s).$$

If F is a Gröbner basis for the ideal $\langle f_1, \dots, f_s \rangle$, then by Proposition 1 we may regard F as a set (without any particular order).

Definition 22. Let $f, g \in k[x_1, \dots, x_n]$ be nonzero polynomials.

1. If $\mathrm{multideg}(f) = \alpha$ and $\mathrm{multideg}(g) = \beta$, then let

$$\gamma = (\gamma_1, \dots, \gamma_n), \quad \gamma_i = \max(\alpha_i, \beta_i) \quad \text{for each } i.$$

We call x^γ the *least common multiple* of $\mathrm{LM}(f)$ and $\mathrm{LM}(g)$, written

$$x^\gamma = \mathrm{lcm}(\mathrm{LM}(f), \mathrm{LM}(g)).$$

2. The S-polynomial of f and g is the combination

$$S(f,g) \;=\; \frac{x^\gamma}{\mathrm{LT}(f)}\, f \;-\; \frac{x^\gamma}{\mathrm{LT}(g)}\, g.$$

Lemma 23. *Suppose we have a sum $\sum_{i=1}^s p_i$, where $\mathrm{multideg}(p_i) = \delta \in \mathbb{Z}^n_{\geq 0}$ for all i. If $\mathrm{multideg}\Big(\sum_{i=1}^s p_i\Big) < \delta$, then $\sum_{i=1}^s p_i$ is a linear combination, with coefficients in k, of the S-polynomials $S(p_j, p_l)$ for $1 \leq j, l \leq s$. Furthermore, each $S(p_j, p_l)$ has multidegree $< \delta$.*

Proof. Let $d_i = \mathrm{LC}(p_i)$, so that $d_i x^\delta$ is the leading term of p_i. Since the sum $\sum_{i=1}^s p_i$ has strictly smaller multidegree, it follows easily that $\sum_{i=1}^s d_i = 0$.

Next observe that since p_i and p_j have the same leading monomial, their S-polynomial reduces to

$$S(p_i, p_j) = \frac{1}{d_i} p_i - \frac{1}{d_j} p_j. \tag{1}$$

It follows that

$$\begin{aligned} \sum_{i=1}^{s-1} d_i S(p_i, p_s) &= d_1 \left(\frac{1}{d_1} p_1 - \frac{1}{d_s} p_s \right) + d_2 \left(\frac{1}{d_2} p_2 - \frac{1}{d_s} p_s \right) + \cdots \\ &= p_1 + p_2 + \cdots + p_{s-1} - \frac{1}{d_s}(d_1 + \cdots + d_{s-1}) p_s. \end{aligned} \tag{2}$$

However, $\sum_{i=1}^s d_i = 0$ implies $d_1 + \cdots + d_{s-1} = -d_s$, so that (2) reduces to

$$\sum_{i=1}^{s-1} d_i S(p_i, p_s) = p_1 + \cdots + p_{s-1} + p_s.$$

Thus, $\sum_{i=1}^s p_i$ is a sum of S-polynomials of the desired form, and equation (1) makes it easy to see that $S(p_i, p_j)$ has multidegree $< \delta$. The lemma is proved. □

Lemma 24. *Suppose that $p_i = c_i x^{\alpha^{(i)}} g_i$ and $p_j = c_j x^{\alpha^{(j)}} g_j$ have the same multidegree δ. Then*

$$S(p_i, p_j) = x^{\delta - \gamma_{ij}} S(g_i, g_j),$$

where $x^{\gamma_{ij}} = \mathrm{lcm}(\mathrm{LM}(g_i), \mathrm{LM}(g_j))$.

Proof. By hypothesis, $\mathrm{multideg}(p_i) = \mathrm{multideg}(p_j) = \delta$, which implies $\delta = \alpha^{(i)} + \mathrm{multideg}(g_i)$ and $\delta = \alpha^{(j)} + \mathrm{multideg}(g_j)$. The leading terms are $\mathrm{LT}(p_i) = c_i \,\mathrm{LC}(g_i) x^\delta$ and $\mathrm{LT}(p_j) = c_j \,\mathrm{LC}(g_j) x^\delta$. Let γ_{ij} be the exponent of $\mathrm{lcm}(\mathrm{LM}(g_i), \mathrm{LM}(g_j))$.

On the one hand, the left-hand side simplifies to:

$$\begin{aligned} S(p_i, p_j) &= \frac{x^\delta}{\mathrm{LT}(p_i)} p_i - \frac{x^\delta}{\mathrm{LT}(p_j)} p_j \\ &= \frac{x^\delta}{c_i \,\mathrm{LC}(g_i) x^\delta} (c_i x^{\alpha^{(i)}} g_i) - \frac{x^\delta}{c_j \,\mathrm{LC}(g_j) x^\delta} (c_j x^{\alpha^{(j)}} g_j) \\ &= \frac{1}{\mathrm{LC}(g_i)} x^{\alpha^{(i)}} g_i - \frac{1}{\mathrm{LC}(g_j)} x^{\alpha^{(j)}} g_j. \end{aligned}$$

On the other hand, the right-hand side expands to:

$$\begin{aligned} x^{\delta-\gamma_{ij}} S(g_i, g_j) &= x^{\delta-\gamma_{ij}} \left(\frac{x^{\gamma_{ij}}}{\mathrm{LT}(g_i)} g_i - \frac{x^{\gamma_{ij}}}{\mathrm{LT}(g_j)} g_j \right) \\ &= \frac{x^{\delta}}{\mathrm{LC}(g_i) x^{\mathrm{multideg}(g_i)}} g_i - \frac{x^{\delta}}{\mathrm{LC}(g_j) x^{\mathrm{multideg}(g_j)}} g_j \\ &= \frac{1}{\mathrm{LC}(g_i)} x^{\delta - \mathrm{multideg}(g_i)} g_i - \frac{1}{\mathrm{LC}(g_j)} x^{\delta - \mathrm{multideg}(g_j)} g_j \\ &= \frac{1}{\mathrm{LC}(g_i)} x^{\alpha^{(i)}} g_i - \frac{1}{\mathrm{LC}(g_j)} x^{\alpha^{(j)}} g_j. \end{aligned}$$

The two sides are equal, which completes the proof. □

Theorem 25 (Buchberger's Criterion)**.** *Let I be a polynomial ideal in $k[x_1, \ldots, x_n]$. Then a basis $G = \{g_1, \ldots, g_t\}$ of I is a Gröbner basis for I (with respect to a given monomial order $>$) if and only if for all pairs $i \neq j$, the remainder on division of the S-polynomial $S(g_i, g_j)$ by G (listed in some order) is zero.*

$$\forall i \neq j, \quad \mathrm{rem}(S(g_i, g_j), G) = 0.$$

Proof. $\Rightarrow$: If G is a Gröbner basis, then since $S(g_i, g_j) \in I$, the remainder on division by G is zero by Corollary 20.

$\Leftarrow$: Let $f \in I$ be nonzero. We will show that $\mathrm{LT}(f) \in \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t) \rangle$ as follows. Write

$$f = \sum_{i=1}^{t} h_i g_i, \quad h_i \in k[x_1, \ldots, x_n].$$

From Lemma 10, it follows that

$$\mathrm{multideg}(f) \leq \max(\mathrm{multideg}(h_i g_i) \mid h_i g_i \neq 0). \tag{3}$$

The strategy of the proof is to pick the most efficient representation of f, meaning that among all expressions $f = \sum_{i=1}^{t} h_i g_i$, we pick one for which

$$\delta = \max(\mathrm{multideg}(h_i g_i) \mid h_i g_i \neq 0)$$

is minimal. The minimal δ exists by the well-ordering property of our monomial ordering. By (3), it follows that $\mathrm{multideg}(f) \leq \delta$.

If equality occurs, then $\mathrm{multideg}(f) = \mathrm{multideg}(h_i g_i)$ for some i. This easily implies that $\mathrm{LT}(f)$ is divisible by $\mathrm{LT}(g_i)$. Then $\mathrm{LT}(f) \in \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t) \rangle$, which is what we want to prove.

It remains to consider the case when the minimal δ satisfies $\mathrm{multideg}(f) < \delta$. We will use $S(g_i, g_j) \longrightarrow^{G} 0$ for $i \neq j$ to find a new expression for f that decreases δ. This will contradict the minimality of δ and complete the proof.

Given an expression $f = \sum_{i=1}^{t} h_i g_i$ with minimal δ, we begin by isolating the part of the sum where multidegree δ occurs:

$$\begin{aligned} f &= \sum_{\mathrm{multideg}(h_i g_i) = \delta} h_i g_i + \sum_{\mathrm{multideg}(h_i g_i) < \delta} h_i g_i \qquad (4) \\ &= \sum_{\mathrm{multideg}(h_i g_i) = \delta} \mathrm{LT}(h_i) g_i + \sum_{\mathrm{multideg}(h_i g_i) = \delta} (h_i - \mathrm{LT}(h_i)) g_i + \sum_{\mathrm{multideg}(h_i g_i) < \delta} h_i g_i. \end{aligned}$$

The monomials appearing in the second and third sums on the second line all have multidegree $< \delta$. Then $\text{multideg}(f) < \delta$ means that the first sum on the second line also has multidegree $< \delta$.

The key to decreasing δ is to rewrite the first sum in two stages: use Lemma 23 to rewrite the first sum in terms of S-polynomials, and then use $S(g_i, g_j) \text{---}^G\!\!\to 0$ to rewrite the S-polynomials without cancellation.

To express the first sum on the second line of (4) using S-polynomials, note that

$$\sum_{\text{multideg}(h_i g_i)=\delta} \text{LT}(h_i) g_i \tag{5}$$

satisfies the hypothesis of Lemma 23 since each $p_i = \text{LT}(h_i)g_i$ has multidegree δ and the sum has multidegree $< \delta$. Hence, the first sum is a linear combination with coefficients in k of the S-polynomials $S(p_i, p_j)$. In Exercise 24, you will verify that

$$S(p_i, p_j) = x^{\delta - \gamma_{ij}} S(g_i, g_j),$$

where $x^{\gamma_{ij}} = \text{lcm}(\text{LM}(g_i), \text{LM}(g_j))$. It follows that the first sum (5) is a linear combination of $S(g_i, g_j)$ for certain pairs (i, j).

Consider one of these S-polynomials $S(g_i, g_j)$. Since $S(g_i, g_j) \text{---}^G\!\!\to 0$, the division algorithm (Theorem 3 of §3) gives an expression

$$S(g_i, g_j) = \sum_{l=1}^{t} A_l g_l, \tag{6}$$

where $A_l \in k[x_1, \dots, x_n]$ and

$$\text{multideg}(A_l g_l) \leq \text{multideg}(S(g_i, g_j)) \tag{7}$$

when $A_l g_l \neq 0$. Now multiply each side of (6) by $x^{\delta - \gamma_{ij}}$ to obtain

$$x^{\delta - \gamma_{ij}} S(g_i, g_j) = \sum_{l=1}^{t} B_l g_l, \tag{8}$$

where $B_l = x^{\delta - \gamma_{ij}} A_l$. Then (7) implies that when $B_l g_l \neq 0$, we have

$$\text{multideg}(B_l g_l) \leq \text{multideg}(x^{\delta - \gamma_{ij}} S(g_i, g_j)) < \delta \tag{9}$$

since $\text{LT}(S(g_i, g_j)) < \text{lcm}(\text{LM}(g_i), \text{LM}(g_j)) = x^{\gamma_{ij}}$ by Exercise 7.

It follows that the first sum (5) is a linear combination of certain $x^{\delta - \gamma_{ij}} S(g_i, g_j)$, each of which satisfies (8) and (9). Hence we can write the first sum as

$$\sum_{\text{multideg}(h_i g_i)=\delta} \text{LT}(h_i) g_i = \sum_{l=1}^{t} \tilde{B}_l g_l \tag{10}$$

with the property that when $\tilde{B}_l g_l \neq 0$, we have

$$\text{multideg}(\tilde{B}_l g_l) < \delta. \tag{11}$$

Substituting (10) into the second line of (4) gives an expression for f as a polynomial combination of the g_i's where *all* terms have multidegree $< \delta$. This contradicts the minimality of δ and completes the proof. □

Definition 26. Fix a monomial order and let $G = \{g_1, \dots, g_t\} \subseteq k[x_1, \dots, x_n]$. Given $f \in k[x_1, \dots, x_n]$, we say that f **reduces to zero modulo** G, written $f \xrightarrow{G} 0$, if f has a **standard representation**

$$f = A_1 g_1 + \cdots A_t g_t, \ A_i \in k[x_1, \dots, x_n],$$

which means that whenever $A_i g_i \neq 0$, we have

$$\deg(f) \geq \deg(A_i g_i).$$

Theorem 27 (Buchberger's Algorithm)**.** *Let $I = \langle f_1, \dots, f_s \rangle \neq \{0\}$ be a polynomial ideal. Then a Gröbner basis for I can be constructed in a finite number of steps by the following algorithm:*

Input : $F = (f_1, \dots, f_s)$

Output : A Gröbner basis $G = (g_1, \dots, g_t)$ for I, with $F \subseteq G$

$G := F$

REPEAT

$G' := G$

FOR each pair $\{p, q\}$, $p \neq q$ in G' **DO**

$r := \overline{S(p,q)}^{G'}$

IF $r \neq 0$ **THEN** $G := G \cup \{r\}$

UNTIL $G = G'$

RETURN G

Proof. We begin with some frequently used notation. If $G = \{g_1, \dots, g_t\}$, then $\langle G \rangle$ and $\langle \mathrm{LT}(G) \rangle$ will denote the following ideals:

$$\langle G \rangle = \langle g_1, \dots, g_t \rangle, \qquad \langle \mathrm{LT}(G) \rangle = \langle \mathrm{LT}(g_1), \dots, \mathrm{LT}(g_t) \rangle.$$

Turning to the proof of the theorem, we first show that $G \subseteq I$ holds at every stage of the algorithm. This is true initially, and whenever we enlarge G, we do so by adding the remainder $r = \overline{S(p,q)}^{G'}$ for $p, q \in G' \subseteq G$. Thus, if $G \subseteq I$, then $p, q \in I$ and, hence, $S(p,q) \in I$, and since we are dividing by $G' \subseteq I$, we get $G \cup \{r\} \subseteq I$. We also note that G contains the given basis F of I, so that G is actually a basis of I.

The algorithm terminates when $G = G'$, which means that $r = \overline{S(p,q)}^{G'} = 0$ for all $p, q \in G$. Hence G is a Gröbner basis of $\langle G \rangle = I$ by Theorem 6 of §6.

It remains to prove that the algorithm terminates. We need to consider what happens after each pass through the main loop. The set G consists of G' (the old G) together with the nonzero remainders of S-polynomials of elements of G'. Then

$$\langle \mathrm{LT}(G') \rangle \subseteq \langle \mathrm{LT}(G) \rangle. \tag{3.1}$$

Since $G' \subseteq G$. Furthermore, if $G' \neq G$, we claim that $\langle \mathrm{LT}(G') \rangle$ is strictly smaller than $\langle \mathrm{LT}(G) \rangle$. To see this, suppose that a nonzero remainder r of an S-polynomial has been adjoined to G. Since r is a remainder on division by G', $\mathrm{LT}(r)$ is not divisible by the leading terms of elements of G', and thus $\mathrm{LT}(r) \notin \langle \mathrm{LT}(G') \rangle$ by Lemma 2 of §4. Yet $\mathrm{LT}(r) \in \langle \mathrm{LT}(G) \rangle$, which proves our claim.

By (1), the ideals $\langle \mathrm{LT}(G') \rangle$ from successive iterations of the loop form an ascending chain of ideals in $k[x_1, \ldots, x_n]$. Thus, the ACC (Theorem 7 of §5) implies that after a finite number of iterations the chain will stabilize, so that $\langle \mathrm{LT}(G') \rangle = \langle \mathrm{LT}(G) \rangle$ must happen eventually. By the previous paragraph, this implies that $G' = G$, so that the algorithm must terminate after a finite number of steps. □

Lemma 28. *Let G be a Gröbner basis of $I \subseteq k[x_1, \ldots, x_n]$. Let $p \in G$ be a polynomial such that $\mathrm{LT}(p) \in \langle \mathrm{LT}(G \setminus \{p\}) \rangle$. Then $G \setminus \{p\}$ is also a Gröbner basis for I.*

Proof. We know that $\langle \mathrm{LT}(G) \rangle = \langle \mathrm{LT}(I) \rangle$. If $\mathrm{LT}(p) \in \langle \mathrm{LT}(G \setminus \{p\}) \rangle$, then we have $\langle \mathrm{LT}(G \setminus \{p\}) \rangle = \langle \mathrm{LT}(G) \rangle$. By definition, it follows that $G \setminus \{p\}$ is also a Gröbner basis for I. □

Chapter 4

The State Polytope

4.1 Basic Concepts of Polyhedral Geometry

In the first half of this chapter we review some basic concepts from polyhedral geometry. In the second half we introduce the state polytope of an ideal I. It has the property that its vertices are in a natural bijection with the distinct initial ideals $\text{in}_<(I)$.

Definition 29 (Polyhedron)**.** A *polyhedron* is a finite intersection of closed half-spaces in $\mathbb{R}^n$. Thus a polyhedron P can be written as $P = \{\mathbf{x} \in \mathbb{R}^n : A \cdot \mathbf{x} \leq \mathbf{b}\}$, where A is a matrix with n columns.

If $\mathbf{b} = 0$ then there exist vectors $\mathbf{u}_1, \ldots, \mathbf{u}_m \in \mathbb{R}^n$ such that

$$P = \text{pos}(\{\mathbf{u}_1, \ldots, \mathbf{u}_m\}) := \{\lambda_1 \mathbf{u}_1 + \cdots + \lambda_m \mathbf{u}_m : \lambda_1, \ldots, \lambda_m \in \mathbb{R}_+\}. \tag{4.1}$$

Definition 30 (Polyhedral Cone)**.** A polyhedron of the form (4.1) is called a *(polyhedral) cone*.

Here and throughout this book $\mathbb{R}_+$ denotes the non-negative reals. The *polar* of a cone C is defined as

$$C^* = \{\omega \in \mathbb{R}^n : \omega \cdot \mathbf{c} \leq 0 \text{ for all } \mathbf{c} \in C\}.$$

Definition 31 (Polytope)**.** A polyhedron Q which is bounded is called a *polytope*. Every polytope Q can be written as the convex hull of a finite set of points

$$Q = \text{conv}(\{\mathbf{v}_1, \ldots, \mathbf{v}_m\}) := \left\{ \sum_{i=1}^m \lambda_i \mathbf{v}_i : \lambda_1, \ldots, \lambda_m \in \mathbb{R}_+, \sum_{i=1}^m \lambda_i = 1 \right\}. \tag{4.2}$$

Here are two examples of 3-dimensional polytopes: The cube and the octahedron.