# INTRODUCTION TO GRÖBNER BASES

TAKAYUKI HIBI AND HIDEFUMI OHSUGI

Let $S = K[x_1, \ldots, x_n]$ denote the polynomial ring in $n$ variables over a field $K$ with $\deg x_i = 1$ for $i = 1, 2, \ldots, n$, and let

$$\mathrm{Mon}(S) = \{x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n} : a_i \in \mathbb{Z}_+, i = 1, 2, \ldots, n\},$$

be the set of monomials of $S$, where $\mathbb{Z}_+$ is the set of nonnegative integers. In particular $1 \in \mathrm{Mon}(S)$. For monomials $\mathbf{x}^{\mathbf{a}} = x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}$ and $\mathbf{x}^{\mathbf{b}} = x_1^{b_1} x_2^{b_2} \cdots x_n^{b_n}$ of $S$, we say that $\mathbf{x}^{\mathbf{b}}$ *divides* $\mathbf{x}^{\mathbf{a}}$ if $b_i \leq a_i$ for $i = 1, 2, \ldots, n$. We write $\mathbf{x}^{\mathbf{b}} \mid \mathbf{x}^{\mathbf{a}}$ if $\mathbf{x}^{\mathbf{b}}$ divides $\mathbf{x}^{\mathbf{a}}$. Let $\mathcal{M}$ be a nonempty subset of $\mathrm{Mon}(S)$. A monomial $\mathbf{x}^{\mathbf{a}} \in \mathcal{M}$ is said to be a *minimal element* of $\mathcal{M}$ with respect to divisibility if whenever $\mathbf{x}^{\mathbf{b}} \mid \mathbf{x}^{\mathbf{a}}$ with $\mathbf{x}^{\mathbf{b}} \in \mathcal{M}$, then $\mathbf{x}^{\mathbf{b}} = \mathbf{x}^{\mathbf{a}}$. Let $\mathcal{M}^{\min}$ denote the set of minimal elements of $\mathcal{M}$.

**Theorem 1** (Dickson's lemma). *Let $\mathcal{M}$ be a nonempty subset of* $\mathrm{Mon}(S)$. *Then $\mathcal{M}^{\min}$ is a finite set.*

*Proof.* We prove Dickson's lemma by using induction on $n$, the number of variables of $S = K[x_1, x_2, \ldots, x_n]$. Let $n = 1$. If $d$ is the smallest integer for which $x_1^d \in \mathcal{M}$, then $\mathcal{M}^{\min} = \{x_1^d\}$. Thus $\mathcal{M}^{\min}$ is a finite set.

Let $n \geq 2$ and $B = K[\mathbf{x}] = K[x_1, x_2, \ldots, x_{n-1}]$. We use the notation $y$ instead of $x_n$. Thus $S = K[x_1, x_2, \ldots, x_{n-1}, y]$. Let $\mathcal{M}$ be a nonempty subset of $\mathrm{Mon}(S)$. Write $\mathcal{N}$ for the subset of $\mathrm{Mon}(B)$ which consists of those monomials $\mathbf{x}^{\mathbf{a}}$, where $\mathbf{a} \in \mathbb{Z}_+^{n-1}$, such that $\mathbf{x}^{\mathbf{a}} y^b \in \mathcal{M}$ for some $b \geq 0$. Our induction hypothesis says that $\mathcal{N}^{\min}$ is a finite set. Let $\mathcal{N}^{\min} = \{u_1, u_2, \ldots, u_s\}$. By the definition of $\mathcal{N}$, for each $1 \leq i \leq s$, there is $b_i \geq 0$ with $u_i y^{b_i} \in \mathcal{M}$. Let $b = \max\{b_1, b_2, \ldots, b_s\}$. Now, for each $0 \leq \xi < b$, define the subset $\mathcal{N}_\xi$ of $\mathcal{N}$ to be

$$\mathcal{N}_\xi = \{\mathbf{x}^{\mathbf{a}} \in \mathcal{N} : \mathbf{x}^{\mathbf{a}} y^\xi \in \mathcal{M}\}.$$

Again, our induction hypothesis says that, for each $0 \leq \xi < b$, the set ${\mathcal{N}_\xi}^{\min}$ is finite. Let ${\mathcal{N}_\xi}^{\min} = \{u_1^{(\xi)}, u_2^{(\xi)}, \ldots, u_{s_\xi}^{(\xi)}\}$. We now show that each monomial belonging to $\mathcal{M}$ is divisible by one of the monomials which appear in the following list:

$$\begin{gathered} u_1 y^{b_1}, u_2 y^{b_2}, \ldots, u_s y^{b_s}, \\ u_1^{(0)}, u_2^{(0)}, \ldots, u_{s_0}^{(0)}, \\ u_1^{(1)} y, u_2^{(1)} y, \ldots, u_{s_1}^{(1)} y, \\ \cdots\cdots \\ u_1^{(b-1)} y^{b-1}, u_2^{(b-1)} y^{b-1}, \ldots, u_{s_{b-1}}^{(b-1)} y^{b-1}. \end{gathered}$$

*JST CREST GRÖBNER SCHOOL*, Kobe University, September 14–18, 2009.

In fact, since, for each monomial $w = \mathbf{x}^{\mathbf{a}} y^{\gamma} \in \mathcal{M}$ with $\mathbf{x}^{\mathbf{a}} \in \mathrm{Mon}(B)$, one has $\mathbf{x}^{\mathbf{a}} \in \mathcal{N}$, it follows that if $\gamma \geq b$, then $w$ is divisible by one of the monomials $u_1 y^{b_1}, u_2 y^{b_2}, \ldots, u_s y^{b_s}$, and that if $0 \leq \gamma < b$, then $w$ is divisible by one of the monomials $u_1^{(\gamma)} y^{\gamma}, u_2^{(\gamma)} y^{\gamma}, \ldots, u_{s_\gamma}^{(\gamma)} y^{\gamma}$. Clearly, the monomials listed above are in $\mathcal{M}$. Hence $\mathcal{M}^{\min}$ is a subset of the set of monomials listed above. Thus $\mathcal{M}^{\min}$ is finite, as desired. □

A *monomial order* on $S$ is a total order $<$ on $\mathrm{Mon}(S)$ such that

- $1 < u$ for all $1 \neq u \in \mathrm{Mon}(S)$;
- if $u, v \in \mathrm{Mon}(S)$ and $u < v$, then $uw < vw$ for all $w \in \mathrm{Mon}(S)$.

**Example 2.** (a) Let $\mathbf{a} = (a_1, a_2, \ldots, a_n)$ and $\mathbf{b} = (b_1, b_2, \ldots, b_n)$ be vectors belonging to $\mathbb{Z}_+^n$. We define the total order $<_{\mathrm{lex}}$ on $\mathrm{Mon}(S)$ by setting $\mathbf{x}^{\mathbf{a}} <_{\mathrm{lex}} \mathbf{x}^{\mathbf{b}}$ if either (i) $\sum_{i=1}^n a_i < \sum_{i=1}^n b_i$, or (ii) $\sum_{i=1}^n a_i = \sum_{i=1}^n b_i$ and the left-most nonzero component of the vector $\mathbf{a} - \mathbf{b}$ is negative. It follows that $<_{\mathrm{lex}}$ is a monomial order on $S$, which is called the *lexicographic order* on $S$ induced by the ordering $x_1 > x_2 > \cdots > x_n$.

(b) Let $\mathbf{a} = (a_1, a_2, \ldots, a_n)$ and $\mathbf{b} = (b_1, b_2, \ldots, b_n)$ be vectors belonging to $\mathbb{Z}_+^n$. We define the total order $<_{\mathrm{rev}}$ on $\mathrm{Mon}(S)$ by setting $\mathbf{x}^{\mathbf{a}} <_{\mathrm{rev}} \mathbf{x}^{\mathbf{b}}$ if either (i) $\sum_{i=1}^n a_i < \sum_{i=1}^n b_i$, or (ii) $\sum_{i=1}^n a_i = \sum_{i=1}^n b_i$ and the right-most nonzero component of the vector $\mathbf{a} - \mathbf{b}$ is positive. It follows that $<_{\mathrm{rev}}$ is a monomial order on $S$, which is called the *reverse lexicographic order* on $S$ induced by the ordering $x_1 > x_2 > \cdots > x_n$.

For example, $x_2 x_3 <_{\mathrm{lex}} x_1 x_4$ and $x_1 x_4 <_{\mathrm{rev}} x_2 x_3$ in $K[x_1, x_2, x_3, x_4]$. Among the monomials of degree 2 of $K[x_1, x_2, x_3]$, one has

$$x_3^2 <_{\mathrm{lex}} x_2 x_3 <_{\mathrm{lex}} x_2^2 <_{\mathrm{lex}} x_1 x_3 <_{\mathrm{lex}} x_1 x_2 <_{\mathrm{lex}} x_1^2$$

and

$$x_3^2 <_{\mathrm{rev}} x_2 x_3 <_{\mathrm{rev}} x_1 x_3 <_{\mathrm{rev}} x_2^2 <_{\mathrm{rev}} x_1 x_2 <_{\mathrm{rev}} x_1^2.$$

**Exercise 3.** List the 10 monomials of degree 3 of $K[x_1, x_2, x_3]$ with respect to each of $<_{\mathrm{lex}}$ and $<_{\mathrm{rev}}$.

**Lemma 4.** *Let $<$ be a monomial order on $S$. Let $u, v \in \mathrm{Mon}(S)$ with $u \neq v$ and suppose that $u$ divides $v$. Then $u < v$.*

*Proof.* Write $v = uw$ with $w \in \mathrm{Mon}(S)$. Since $w \neq 1$, one has $1 < w$. Thus $1 \cdot u < w \cdot u$. Hence $u < v$, as desired. □

We will work with a fixed monomial order $<$ on $S$. Let $f = \sum_{u \in \mathrm{Mon}(S)} a_u u$ be a nonzero polynomial of $S$ with each $a_u \in K$. The *support* of $f$ is the finite set

$$\mathrm{supp}(f) = \{u \in \mathrm{Mon}(S) : a_u \neq 0\}.$$

The *initial monomial* of $f$ with respect to $<$ is the biggest monomial with respect to $<$ among the monomials belonging to $\mathrm{supp}(f)$.

Recall that an ideal of $S$ is a nonempty subset $I$ of $S$ such that

- if $f, g \in I$, then $f \pm g \in I$;
- if $f \in I$ and $h \in S$, then $fh \in I$.

Given a subset $\{f_\lambda\}_{\lambda\in\Lambda}$ of $S$, we write $(\{f_\lambda\}_{\lambda\in\Lambda})$ for the set of polynomials of the form $\sum_{\lambda\in\Lambda} h_\lambda f_\lambda$, where $\{\lambda \in \Lambda : h_\lambda \neq 0\}$ is finite. Then $(\{f_\lambda\}_{\lambda\in\Lambda})$ is an ideal of $S$, which is called the ideal of $S$ *generated by* $\{f_\lambda\}_{\lambda\in\Lambda}$. When $\Lambda$ is finite, say, $\Lambda = \{1, 2, \ldots, s\}$, we write $(f_1, f_2, \ldots, f_s)$ instead of $(\{f_1, f_2, \ldots, f_s\})$. Conversely, given an ideal $I$ of $S$, there exists a subset $(\{f_\lambda\}_{\lambda\in\Lambda})$ of $S$ with $I = (\{f_\lambda\}_{\lambda\in\Lambda})$. We call $\{f_\lambda\}_{\lambda\in\Lambda}$ *a system of generators* of $I$. We say that an ideal $I$ of $S$ is *finitely generated* if $I$ possesses a system of generators consisting of a finite number of polynomials. Later, we will see that every ideal of $S$ is finitely generated (Corollary 9).

A *monomial ideal* is an ideal which is generated by a set of monomials. Let $I \subset S$ be a monomial ideal. It follows that $I$ is generated by a subset $\mathcal{N} \subset \mathrm{Mon}(S)$ if and only if $(I \cap \mathrm{Mon}(S))^{\min} \subset \mathcal{N}$. Hence $(I \cap \mathrm{Mon}(S))^{\min}$ is a *unique* minimal system of monomial generators of $I$. Dickson's lemma guarantees that $(I \cap \mathrm{Mon}(S))^{\min}$ is finite. Thus in particular every monomial ideal is finitely generated.

Let $I$ be a nonzero ideal of $S$. The *initial ideal* of $I$ with respect to $<$ is the monomial ideal of $S$ which is generated by $\{\mathrm{in}_<(f) : 0 \neq f \in I\}$. We write $\mathrm{in}_<(I)$ for the initial ideal of $I$. Thus

$$\mathrm{in}_<(I) = (\{\mathrm{in}_<(f) : 0 \neq f \in I\}).$$

Since $(\mathrm{in}_<(I) \cap \mathrm{Mon}(S))^{\min}$ is a minimal system of monomial generators of $\mathrm{in}_<(I)$, and since $\mathrm{in}_<(I) \cap \mathrm{Mon}(S) = (\{\mathrm{in}_<(f) : 0 \neq f \in I\})$, there exists a finite number of nonzero polynomials $g_1, g_2, \ldots, g_s$ belonging to $I$ such that $\mathrm{in}_<(I)$ is generated by the set $\{\mathrm{in}_<(g_1), \mathrm{in}_<(g_2), \ldots, \mathrm{in}_<(g_s)\}$ of their initial monomials.

**Definition 5.** Let $I$ be a nonzero ideal of $S$. A finite set $\{g_1, g_2, \ldots, g_s\}$ of nonzero polynomials with each $g_i \in I$ is said to be a *Gröbner basis* of $I$ with respect to $<$ if the initial ideal $\mathrm{in}_<(I)$ of $I$ is generated by the set $\{\mathrm{in}_<(g_1), \mathrm{in}_<(g_2), \ldots, \mathrm{in}_<(g_s)\}$ of their initial monomials.

A Gröbner basis of $I$ with respect to $<$ exists. If $\mathcal{G}$ is a Gröbner basis of $I$ with respect to $<$, then every finite set $\mathcal{G}'$ with $\mathcal{G} \subset \mathcal{G}' \subset I$ is also a Gröbner basis of $I$ with respect to $<$. If $\mathcal{G} = \{g_1, \ldots, g_s\}$ is a Gröbner basis of $I$ with respect to $<$ and if $f_1, \ldots, f_s$ are nonzero polynomials belonging to $I$ with each $\mathrm{in}_<(f_i) = \mathrm{in}_<(g_i)$, then $\{f_1, \ldots, f_s\}$ is also a Gröbner basis of $I$ with respect to $<$.

**Example 6.** Let $S = K[x_1, x_2, \ldots, x_7]$ and $I = (f, g)$, where $f = x_1x_4 - x_2x_3$ and $g = x_4x_7 - x_5x_6$. Let $<_{\mathrm{lex}}$ the lexicographic order on $S$ induced by $x_1 > x_2 > \cdots > x_7$. One has $\mathrm{in}_{<_{\mathrm{lex}}}(f) = x_1x_4$ and $\mathrm{in}_{<_{\mathrm{lex}}}(g) = x_4x_7$. We claim that $\{f, g\}$ is not a Gröbner basis of $I$ with respect to $<_{\mathrm{lex}}$. In fact, the polynomial $h = x_7 f - x_1 g = x_1x_5x_6 - x_2x_3x_7$ belongs to $I$, but its initial monomial $\mathrm{in}_{<_{\mathrm{lex}}}(h) = x_1x_5x_6$ can be divided by neither $\mathrm{in}_{<_{\mathrm{lex}}}(f)$ nor $\mathrm{in}_{<_{\mathrm{lex}}}(g)$. Hence $\mathrm{in}_{<_{\mathrm{lex}}}(h) \notin (\mathrm{in}_{<_{\mathrm{lex}}}(f), \mathrm{in}_{<_{\mathrm{lex}}}(g))$. Thus $\mathrm{in}_{<_{\mathrm{lex}}}(I) \neq (\mathrm{in}_{<_{\mathrm{lex}}}(f), \mathrm{in}_{<_{\mathrm{lex}}}(g))$. In other words, $\{f, g\}$ is not a Gröbner basis of $I$ with respect to $<_{\mathrm{lex}}$. Later, we will show that $\{f, g, h\}$ is a Gröbner basis of $I$ with respect to $<_{\mathrm{lex}}$ (Example 16).

**Lemma 7.** *Let $<$ be a monomial order on $S = K[x_1, \ldots, x_n]$. Then, for any monomial $u$ of $S$, there is no infinite descending sequence of the form*

$$u = u_0 > u_1 > u_2 > \cdots . \qquad (1)$$

*Proof.* Suppose, on the contrary, that one has an infinite descending sequence (1) and write $\mathcal{M}$ for the set of monomials $\{u_0, u_1, u_2, \ldots\}$. It follows from Dickson's lemma that $\mathcal{M}^{\min}$ is a finite set, say $\mathcal{M}^{\min} = \{u_{i_1}, u_{i_2}, \ldots, u_{i_s}\}$ with $i_1 < i_2 < \cdots < i_s$. Then the monomial $u_{i_s+1}$ is divided by $u_{i_j}$ for some $1 \leq j \leq s$. Thus by Lemma 4 one has $u_{i_j} < u_{i_s+1}$, which contradicts $i_j < i_s + 1$. □

**Theorem 8.** *Let $I$ be a nonzero ideal of $S = K[x_1, \ldots, x_n]$ and $\mathcal{G} = \{g_1, \ldots, g_s\}$ a Gröbner basis of $I$ with respect to a monomial order $<$ on $S$. Then $I = (g_1, \ldots, g_s)$. In other words, every Gröbner basis of $I$ is a system of generators of $I$.*

*Proof.* (Gordan) Let $0 \neq f \in I$. Since $\text{in}_<(f) \in \text{in}_<(I)$ and since $\mathcal{G}$ is a Gröbner basis of $I$, i.e., $\text{in}_<(I) = (\text{in}_<(g_1), \ldots, \text{in}_<(g_s))$, it follows that there is $g_{i_0}$ such that $\text{in}_<(g_{i_0})$ divides $\text{in}_<(f)$. Let $\text{in}_<(f) = w_0 \,\text{in}_<(g_{i_0})$ with $w_0 \in \text{Mon}(S)$. Let $h_0 = f - c_{i_0}^{-1} c_0 w_0 g_{i_0}$, where $c_0$ is the coefficient of $\text{in}_<(f)$ in $f$ and where $c_{i_0}$ is the coefficient of $\text{in}_<(g_{i_0})$ in $g_{i_0}$. Then $h_0 \in I$. Since $\text{in}_<(w_0 g_{i_0}) = w_0 \,\text{in}_<(g_{i_0})$ it follows that $\text{in}_<(h_0) < \text{in}_<(f)$. If $h_0 = 0$, then $f \in (g_1, \ldots, g_s)$.

Let $h_0 \neq 0$. Then the same technique as we used for $f$ can be applied for $h_0$. Thus $h_1 = f - c_{i_1}^{-1} c_1 w_1 g_{i_1} - c_{i_0}^{-1} c_0 w_0 g_{i_0}$, where $c_1$ is the coefficient of $\text{in}_<(h_0)$ in $h_0$ and where $c_{i_1}$ is the coefficient of $\text{in}_<(g_{i_1})$ in $g_{i_1}$. Then $h_1 \in I$ and $\text{in}_<(h_1) < \text{in}_<(h_0)$. If $h_1 = 0$, then $f \in (g_1, \ldots, g_s)$.

If $h_1 \neq 0$, then we proceed as before. Lemma 7 guarantees that this procedure must terminate. Thus we obtain an expression of the form $f = \sum_{q=0}^{N} c_{i_q}^{-1} c_q w_q g_{i_q}$. In particular, $f$ belongs to $(g_1, g_2, \ldots, g_s)$. Thus $I = (g_1, g_2, \ldots, g_s)$, as desired. □

**Corollary 9** (Hilbert basis theorem). *Every ideal of the polynomial ring $S = K[x_1, \ldots, x_n]$ is finitely generated.*

It is natural to ask if the converse of Theorem 8 is true or false. That is to say, if $I = (f_1, f_2, \ldots, f_s)$ is an ideal of $S = K[x_1, \ldots, x_n]$, then does there exist a monomial order $<$ on $S$ such that $\{f_1, f_2, \ldots, f_s\}$ is a Gröbner basis of $I$ with respect to $<$ ?

**Example 10** ([4]). Let $S = K[x_1, x_2, \ldots, x_{10}]$ and $I$ the ideal of $S$ generated by

$$f_1 = x_1x_8 - x_2x_6, \quad f_2 = x_2x_9 - x_3x_7, \quad f_3 = x_3x_{10} - x_4x_8,$$
$$f_4 = x_4x_6 - x_5x_9, \quad f_5 = x_5x_7 - x_1x_{10}.$$

We claim that there exists *no* monomial order $<$ on $S$ such that $\{f_1, \ldots, f_5\}$ is a Gröbner basis of $I$ with respect to $<$.

Suppose, on the contrary, that there exists a monomial order $<$ on $S$ such that $\mathcal{G} = \{f_1, \ldots, f_5\}$ is a Gröbner basis of $I$ with respect to $<$. First, note that each of the five polynomials

$$x_1x_8x_9 - x_3x_6x_7,\ x_2x_9x_{10} - x_4x_7x_8,\ x_2x_6x_{10} - x_5x_7x_8,$$
$$x_3x_6x_{10} - x_5x_8x_9,\ x_1x_9x_{10} - x_4x_6x_7$$

belongs to $I$. Let, say, $x_1x_8x_9 > x_3x_6x_7$. Since $x_1x_8x_9 \in \text{in}_<(I)$, there is $g \in \mathcal{G}$ such that $\text{in}_<(g)$ divides $x_1x_8x_9$. Such $g \in \mathcal{G}$ must be $f_1$. Hence $x_1x_8 > x_2x_6$. Thus $x_2x_6 \notin \text{in}_<(I)$. Hence there exists no $g \in \mathcal{G}$ such that $\text{in}_<(g)$ divides $x_2x_6x_{10}$. Hence $x_2x_6x_{10} < x_5x_7x_8$. Thus $x_5x_7 > x_1x_{10}$. Continuing these arguments, we obtain

$$x_1x_8x_9 > x_3x_6x_7, \quad x_2x_9x_{10} > x_4x_7x_8, \quad x_2x_6x_{10} < x_5x_7x_8,$$
$$x_3x_6x_{10} > x_5x_8x_9, \quad x_1x_9x_{10} < x_4x_6x_7$$

and

$$x_1x_8 > x_2x_6, \;\; x_2x_9 > x_3x_7, \;\; x_3x_{10} > x_4x_8,$$
$$x_4x_6 > x_5x_9, \;\; x_5x_7 > x_1x_{10}.$$

Hence

$$(x_1x_8)(x_2x_9)(x_3x_{10})(x_4x_6)(x_5x_7) > (x_2x_6)(x_3x_7)(x_4x_8)(x_5x_9)(x_1x_{10}). \tag{2}$$

The opposite relation in (2) occurs in case of $x_1x_8x_9 < x_3x_6x_7$. However, both sides of the inequality (2) coincide with $x_1x_2\cdots x_{10}$.

In high school mathematics, we learn that, given polynomials $f$ and $g \neq 0$ in one variable $x$, there exist unique polynomials $q$ and $r$ such that $f = gq+r$, where either $r = 0$ or $\deg r < \deg g$. The division algorithm generalizes this well-known result.

**Theorem 11** (Division algorithm). *Let $S = K[x_1, \ldots, x_n]$ denote the polynomial ring in $n$ variables over a field $K$ and fix a monomial order $<$ on $S$. Let $g_1, g_2, \ldots, g_s$ be nonzero polynomials of $S$. Then, given a polynomial $0 \neq f \in S$, there exist polynomials $f_1, f_2, \ldots, f_s$ and $f'$ of $S$ with*

$$f = f_1g_1 + f_2g_2 + \cdots + f_sg_s + f' \tag{3}$$

*such that the following conditions are satisfied:*

(i) *if $f' \neq 0$ and if $u \in \mathrm{supp}(f')$, then none of $\mathrm{in}_<(g_1), \ldots, \mathrm{in}_<(g_s)$ divides $u$, i.e., no $u \in \mathrm{supp}(f')$ belongs to $(\mathrm{in}_<(g_1), \ldots, \mathrm{in}_<(g_s))$;*

(ii) *if $f_i \neq 0$, then*
$$\mathrm{in}_<(f_ig_i) \leq \mathrm{in}_<(f).$$

The right hand side of equation (3) is said to be a *standard expression* for $f$ with respect to $g_1, g_2, \ldots, g_s$, and the polynomial $f'$ is called a *remainder* of $f$ with respect to $g_1, g_2, \ldots, g_s$.

Instead of giving a detailed proof of Theorem 11, we discuss a typical example which clearly explains the procedure to obtain a standard expression.

**Example 12.** Let $<_{\mathrm{lex}}$ denote the lexicographic order on $S = K[x, y, z]$ induced by $x > y > z$. Let $g_1 = x^2 - z, g_2 = xy - 1$ and $f = x^3 - x^2y - x^2 - 1$. Each of

$$\begin{aligned} f &= x^3 - x^2y - x^2 - 1 = x(g_1 + z) - x^2y - x^2 - 1 \\ &= xg_1 - x^2y - x^2 + xz - 1 = xg_1 - (g_1 + z)y - x^2 + xz - 1 \\ &= xg_1 - yg_1 - x^2 + xz - yz - 1 = xg_1 - yg_1 - (g_1 + z) + xz - yz - 1 \\ &= (x - y - 1)g_1 + (xz - yz - z - 1) \end{aligned}$$

and

$$\begin{aligned} f &= x^3 - x^2y - x^2 - 1 = x(g_1 + z) - x^2y - x^2 - 1 \\ &= xg_1 - x^2y - x^2 + xz - 1 = xg_1 - x(g_2 + 1) - x^2 + xz - 1 \\ &= xg_1 - xg_2 - x^2 + xz - x - 1 = xg_1 - xg_2 - (g_1 + z) + xz - x - 1 \\ &= (x - 1)g_1 - xg_2 + (xz - x - z - 1) \end{aligned}$$

is a standard expression of $f$ with respect to $g_1$ and $g_2$, and each of $xz - yz - z - 1$ and $xz - x - z - 1$ is a remainder of $f$.

Example 12 says that a remainder of a nonzero polynomial may not be unique. However, we have the following fact.

**Lemma 13.** *If $\mathcal{G} = \{g_1, \ldots, g_s\}$ is a Gröbner basis of $I = (g_1, \ldots, g_s)$, then for any nonzero polynomial $f$ of $S$, there is a unique remainder of $f$ with respect to $g_1, \ldots, g_s$.*

*Proof.* Suppose there exist remainders $f'$ and $f''$ with respect to $g_1, \ldots, g_s$ with $f' \neq f''$. Since $0 \neq f' - f'' \in I$, the initial monomial $w = \mathrm{in}_<(f' - f'')$ must belong to $\mathrm{in}_<(I)$. However, since $w \in \mathrm{supp}(f') \cup \mathrm{supp}(f'')$, none of the monomials $\mathrm{in}_<(g_1), \ldots, \mathrm{in}_<(g_s)$ divides $w$. Hence $\mathrm{in}_<(I) \neq (\mathrm{in}_<(g_1), \ldots, \mathrm{in}_<(g_s))$. □

Given nonzero polynomials $f$ and $g$ of $S$, the notation $\mathrm{lcm}(\mathrm{in}_<(f), \mathrm{in}_<(g))$ stands for the least common multiple of $\mathrm{in}_<(f)$ and $\mathrm{in}_<(g)$. Let $c_f$ denote the coefficient of $\mathrm{in}_<(f)$ in $f$ and $c_g$ the coefficient of $\mathrm{in}_<(g)$ in $g$. The polynomial

$$S(f, g) = \frac{\mathrm{lcm}(\mathrm{in}_<(f), \mathrm{in}_<(g))}{c_f \, \mathrm{in}_<(f)} f - \frac{\mathrm{lcm}(\mathrm{in}_<(f), \mathrm{in}_<(g))}{c_g \, \mathrm{in}_<(g)} g$$

is called the *$S$-polynomial* of $f$ and $g$.

We say that $f$ *has remainder* 0 with respect to $g_1, g_2, \ldots, g_s$ if, in the division algorithm, there is a standard expression (3) of $f$ with respect to $g_1, g_2, \ldots, g_s$ with $f' = 0$.

**Lemma 14.** *Let $f$ and $g$ be nonzero polynomials and suppose that $\mathrm{in}_<(f)$ and $\mathrm{in}_<(g)$ are relatively prime, i.e., $\mathrm{lcm}(\mathrm{in}_<(f), \mathrm{in}_<(g)) = \mathrm{in}_<(f) \, \mathrm{in}_<(g)$. Then $S(f, g)$ has remainder 0 with respect to $f, g$.*

*Proof.* To simplify notation we will assume that each of the coefficients of $\mathrm{in}_<(f)$ in $f$ and $\mathrm{in}_<(g)$ in $g$ is equal to 1. Let $f = \mathrm{in}_<(f) + f_1$ and $g = \mathrm{in}_<(g) + g_1$. Since $\mathrm{in}_<(f)$ and $\mathrm{in}_<(g)$ are relatively prime, it follows that

$$\begin{aligned} S(f, g) &= \mathrm{in}_<(g) f - \mathrm{in}_<(f) g \\ &= (g - g_1) f - (f - f_1) g \\ &= f_1 g - g_1 f. \end{aligned}$$

We claim $(\mathrm{in}_<(f_1) \, \mathrm{in}_<(g) =) \, \mathrm{in}_<(f_1 g) \neq \mathrm{in}_<(g_1 f) \; (= \mathrm{in}_<(g_1) \, \mathrm{in}_<(f))$. In fact, if $\mathrm{in}_<(f_1) \, \mathrm{in}_<(g) = \mathrm{in}_<(g_1) \, \mathrm{in}_<(f)$, then, since $\mathrm{in}_<(f)$ and $\mathrm{in}_<(g)$ are relatively prime, it follows that $\mathrm{in}_<(f)$ must divide $\mathrm{in}_<(f_1)$. However, since $\mathrm{in}_<(f_1) < \mathrm{in}_<(f)$, this is impossible. Let, say, $\mathrm{in}_<(f_1) \, \mathrm{in}_<(g) < \mathrm{in}_<(g_1) \, \mathrm{in}_<(f)$. Then $\mathrm{in}_<(S(f, g)) = \mathrm{in}_<(g_1 f)$ and $S(f, g) = f_1 g - g_1 f$ turns out to be a standard expression of $S(f, g)$ in terms of $f$ and $g$. Hence $S(f, g)$ has remainder 0 with respect to $f$ and $g$, and similarly for $\mathrm{in}_<(g_1) \, \mathrm{in}_<(f) < \mathrm{in}_<(f_1) \, \mathrm{in}_<(g)$. □

We now come to the most fundamental theorem in the theory of Gröbner bases.

**Theorem 15** (Buchberger criterion)**.** *Let $I$ be a nonzero ideal of $S$ and $\mathcal{G} = \{g_1, g_2, \ldots, g_s\}$ a system of generators of $I$. Then $\mathcal{G}$ is a Gröbner basis of $I$ if and only if the following condition is satisfied:*

($*$) *For all $i \neq j$, $S(g_i, g_j)$ has remainder 0 with respect to $g_1, \ldots, g_s$.*

We refer the reader to a standard textbook on Gröbner bases, e.g., [1], [2] and [3] for a proof of the Buchberger criterion. However, for a (general) Gröbner basis "user," it may not be required to understand a detailed proof of the Buchberger criterion.

In Example 6, by using Lemma 14 together with the Buchberger criterion, it follows immediately that the set $\{f, g\}$ is a Gröbner basis of $I = (f, g)$ with respect to the reverse lexicographic order $<_{\text{rev}}$ induced by $x_1 > x_2 > \cdots > x_7$.

The Buchberger criterion supplies an algorithm to compute a Gröbner basis starting from a system of generators of an ideal.

Let $\{g_1, g_2, \ldots, g_s\}$ be a system of generators of a nonzero ideal $I$ of $S$ and suppose that $\{g_1, g_2, \ldots, g_s\}$ is *not* a Gröbner basis of $I$. The Buchberger criterion then guarantees that there is an $S$-polynomial $S(g_i, g_j)$ such that *no* remainder of $S(g_i, g_j)$ with respect to $g_1, g_2, \ldots, g_s$ is 0. Let $h_{ij} \in I$ be a remainder of a standard expression of $S(g_i, g_j)$ with respect to $g_1, g_2, \ldots, g_s$. Then $\text{in}_<(h_{ij})$ can be divided by none of the monomials $\text{in}_<(g_1), \text{in}_<(g_2), \ldots, \text{in}_<(g_s)$. In other words, the inclusion

$$(\text{in}_<(g_1), \text{in}_<(g_2), \ldots, \text{in}_<(g_s)) \subset (\text{in}_<(g_1), \text{in}_<(g_2), \ldots, \text{in}_<(g_s), \text{in}_<(h_{ij})).$$

is strict. With setting $g_{s+1} = h_{ij}$, suppose that $\{g_1, g_2, \ldots, g_s, g_{s+1}\}$ is not a Gröbner basis of $I$. Again, by using the Buchberger criterion, there is a $S$-polynomial $S(g_k, g_\ell)$ such that no remainder of $S(g_k, g_\ell)$ with respect to $g_1, g_2, \ldots, g_s, g_{s+1}$ is 0. Let $h_{k\ell} \in I$ be a remainder of $S(g_k, g_\ell)$ with respect to $g_1, g_2, \ldots, g_s, g_{s+1}$. Then the inclusion

$$(\text{in}_<(g_1), \text{in}_<(g_2), \ldots, \text{in}_<(g_s), \text{in}_<(g_{s+1})) \subset (\text{in}_<(g_1), \text{in}_<(g_2), \ldots, \text{in}_<(g_s), \text{in}_<(g_{s+1}), \text{in}_<(h_{k\ell})).$$

is strict. By virtue of Dickson's lemma, these procedures must terminate after a finite number of steps, and a Gröbner basis of $I$ can be obtained.

The above algorithm to find a Gröbner basis starting from a system of generators of an ideal is said to be the *Buchberger algorithm*.

**Example 16.** We continue Example 6. Let $S = K[x_1, x_2, \ldots, x_7]$ and $<_{\text{lex}}$ the lexicographic order on $S$ induced by $x_1 > x_2 > \cdots > x_7$. Let $f = x_1x_4 - x_2x_3$ and $g = x_4x_7 - x_5x_6$. Thus $\text{in}_{<_{\text{lex}}}(f) = x_1x_4$ and $\text{in}_{<_{\text{lex}}}(g) = x_4x_7$. Let $I = (f, g)$. Then $\{f, g\}$ is not a Gröbner basis of $I$ with respect to $<_{\text{lex}}$. Now, as a remainder of $S(f, g) = x_7f - x_1g = x_1x_5x_6 - x_2x_3x_7$ with respect to $f$ and $g$, we choose $S(f, g)$ itself. Let $h = x_1x_5x_6 - x_2x_3x_7$ with $\text{in}_{<_{\text{lex}}}(h) = x_1x_5x_6$. Then $\text{in}_{<_{\text{lex}}}(g)$ and $\text{in}_{<_{\text{lex}}}(h)$ are relatively prime. On the other hand, $S(f, h) = x_2x_3(x_4x_7 - x_5x_6)$ has remainder 0 with respect to $f, g, h$. It follows from the Buchberger criterion that $\{f, g, h\}$ is a Gröbner basis of $I$ with respect to $<_{\text{lex}}$.

The following theorem is called *Elimination Theorem* and plays an important role when solving a system of equations.

**Theorem 17.** *Let $S' = K[x_{i_1}, \ldots, x_{i_m}]$ be the subring of $S = K[x_1, \ldots, x_n]$ where $1 \leq i_1 < \cdots < i_m \leq n$ and let $<$ a monomial order on $S$ (and $S'$). Let $\mathcal{G}$ denote a Gröbner basis of a nonzero ideal $I$ of $S$ with respect ot $<$. If $<$ satisfies the condition*

$$(\sharp) \quad g \in \mathcal{G}, \ \text{in}_<(g) \in S' \implies g \in S'$$

*then $\mathcal{G} \cap S'$ is a Gröbner basis of $I \cap S'$ with respect to $<$.*

*Proof.* Let $u$ be a monomial belonging to $\mathrm{in}_<(I \cap S')$. Then there exists a polynomial $(0 \neq)$ $f \in I \cap S'$ such that $\mathrm{in}_<(f) = u$. Since $f \in I$, the initial monomial $u$ belongs to $\mathrm{in}_<(I)$. Hence there exists $g \in \mathcal{G}$ such that $\mathrm{in}_<(g)$ devides $u$. Then $\mathrm{in}_<(g)$ belongs to $S'$. Thanks to the condition ($\sharp$), we have $g \in S'$ and hence $g \in \mathcal{G} \cap S'$. Thus $\mathrm{in}_<(I \cap S')$ is generated by $\{\mathrm{in}_<(g) \ : \ g \in \mathcal{G} \cap S'\}$ as desired. □

**Example 18.** Let $\mathbf{a} = (a_1, a_2, \ldots, a_n)$ and $\mathbf{b} = (b_1, b_2, \ldots, b_n)$ be vectors belonging to $\mathbb{Z}_+^n$. We define the total order $<_{\mathrm{plex}}$ on $\mathrm{Mon}(S)$ by setting $\mathbf{x}^{\mathbf{a}} <_{\mathrm{plex}} \mathbf{x}^{\mathbf{b}}$ if the left-most nonzero component of the vector $\mathbf{a} - \mathbf{b}$ is negative. It follows that $<_{\mathrm{plex}}$ is a monomial order on $S$, which is called the *purely lexicographic order* on $S$ induced by the ordering $x_1 > x_2 > \cdots > x_n$. If $S' = K[x_m, x_{m+1}, \ldots, x_n]$ is a subring of $S = K[x_1, \ldots, x_n]$, then the condition ($\sharp$) in Theorem 17 holds for a Gröbner basis $\mathcal{G}$ of an arbitrary ideal $I$ of $S$ with respect to $<_{\mathrm{plex}}$.

Let $f_1, \ldots, f_s, g_1, \ldots, g_t \in S$. It is easy to see that, if $(f_1, \ldots, f_s) = (g_1, \ldots, g_t)$ holds, then the set of solutions of $f_1 = \cdots = f_s = 0$ equals to that of $g_1 = \cdots = g_t = 0$. Thus, one can eliminate the variables $x_1, \ldots, x_{m-1}$ from $f_1 = \cdots = f_s = 0$ by computing a system of generators of $I \cap K[x_m, x_{m+1}, \ldots, x_n]$. Thanks to Theorem 8, we can apply Elimination Theorem to eliminate variables from a system of equations.

**Example 19** ([3])**.** Let $f_1 = x^2 + y + z - 1$, $f_2 = x + y^2 + z - 1$ and $f_3 = x + y + z^2 - 1$ and consider the system of equations $f_1 = f_2 = f_3 = 0$. Let $I = (f_1, f_2, f_3)$. Then $\{x + y + z^2 - 1, y^2 - y - z^2 + z, 2yz^2 + z^4 - z^2, z^6 - 4z^4 + 4z^3 - z^2\}$ is a Gröbner basis of $I$ with respect to $<_{\mathrm{plex}}$ induced by $x > y > z$. Thus, thanks to Theorem 17,

$$\begin{aligned} I \cap \mathbb{C}[z] &= (z^6 - 4z^4 + 4z^3 - z^2) \\ I \cap \mathbb{C}[y, z] &= (y^2 - y - z^2 + z, 2yz^2 + z^4 - z^2, z^6 - 4z^4 + 4z^3 - z^2) \end{aligned}$$

Note that $z^6 - 4z^4 + 4z^3 - z^2 = z^2(z-1)^2(z^2 + 2z - 1)$.

## References


[1] W. Adams and P. Loustaunau, "An Introduction to Gröbner Bases," Amer. Math. Soc., Providence, RI, 1994.

[2] T. Becker and V. Weispfenning, "Gröbner Bases," Springer–Verlag, Berlin, Heidelberg, New York, 1993.

[3] D. Cox, J. Little and D. O'Shea, "Ideals, Varieties and Algorithms," Springer–Verlag, Berlin, Heidelberg, New York, 1992.

[4] H. Ohsugi and T. Hibi, Toric ideals generated by quadratic binomials, *J. Algebra* **218** (1999), 509–527.



Takayuki Hibi, Department of Pure and Applied Mathematics, Graduate School of Information Science and Technology, Osaka University, Toyonaka, Osaka 560-0043, Japan.

*E-mail address*: `hibi@math.sci.osaka-u.ac.jp`

Hidefumi Ohsugi, Department of Mathematics, College of Science, Rikkyo University, Toshima-ku, Tokyo 171-8501, Japan

*E-mail address*: `ohsugi@rkmath.rikkyo.ac.jp`