2.3 The notion of a Gröbner basis

The material of this chapter is largely taken from
F.Winkler,
Polynomial Algorithms in Computer Algebra,
Springer-Verlag, Wien New York (1996)
where also proofs of theorems are given.

Before we start with the technical details, let us briefly review the historical development leading to the concept of Gröbner bases. In his seminal paper of 1890 D. Hilbert gave a proof of his famous Basis Theorem as well as of the structure and length of the sequence of syzygy modules of a polynomial system. Implicitly he also showed that the Hauptproblem, i.e. the problem whether $f \in I$ for a given polynomial f and polynomial ideal I, can be solved effectively. Hilbert's solution of the Hauptproblem (and similar problems) was reinvestigated by G. Hermann in 1926. She counted the field operations required in this effective procedure and arrived at a double exponential upper bound in the number of variables. In fact, Hermann's, or for that matter Hilbert's, algorithm always actually achieves this worst case double exponential complexity. The next important step came when B. Buchberger, in his doctoral thesis of 1965 advised by W. Gröbner, introduced the notion of a Gröbner basis (he did not call it that at this time) and also gave an algorithm for computing it. Gröbner bases are very special and useful bases for polynomial ideals. In subsequent publications Buchberger exhibited important additional applications of his Gröbner bases method, e.g. to the solution of systems of polynomial equations. In the worst case, Buchberger's Gröbner bases algorithm is also double exponential in the number of variables, but in practice there are many interesting examples which can be solved in reasonable time. But still, in the worst case, the double exponential behaviour is not avoided. And, in fact, it cannot be avoided by any algorithm capable of solving the Hauptproblem, as was shown by E.W. Mayr and A.R. Meyer in 1982.

When we are solving systems of polynomial (algebraic) equations such as

$$f_1(x_1, \ldots, x_n) \;=\; \cdots \;=\; f_m(x_1, \ldots, x_n) = 0 \;,$$

the important parameters are the number of variables n and the degree d

of the polynomials $f_1, \ldots, f_m$. The Buchberger algorithm for constructing Gröbner bases is at the same time a generalization of Euclid's algorithm for computing the greatest common divisor (GCD) of univariate polynomials (the case $n = 1$) and of Gauss' triangularization algorithm for linear systems (the case $d = 1$). Both these algorithms are concerned with solving systems of polynomial equations, and they determine a canonical basis (either the GCD of the inputs or a triangularized form of the system) for the given polynomial system. Buchberger's algorithm can be seen as a generalization to the case of arbitrary n and d.

Let K be a computable field and $K[X] = K[x_1, \ldots, x_n]$ the polynomial ring in n indeterminates over K. A subset I of $K[X]$ is a *(polynomial) ideal* of $K[X]$, iff it is closed under the formation of linear combinations; i.e., for $m \in \mathbb{N}$, $f_1, \ldots, f_m \in I$ and $p_1, \ldots, p_m \in K[X]$, also

$$\sum_{i=1}^{m} p_i f_i \ \in I \ .$$

If F is any subset of $K[X]$ we write $\langle F \rangle$ or ideal(F) for the ideal generated by F in $K[X]$.

$$\langle F \rangle \ = \ \{ \sum_{i=1}^{m} p_i f_i \mid m \in \mathbb{N}, \ f_i \in F, \ p_i \in K[X] \}$$

i.e. $\langle F \rangle$ consists of all linear combinations (also the empty linear combination $0 = \sum_{i=1}^{0} p_i f_i$) of F over $K[X]$.
F is called a *basis* or *generating set* of $\langle F \rangle$.

By $[X]$ we denote the monoid (under multiplication) of *power products* $x_1^{i_1} \cdots x_n^{i_n}$ in $x_1, \ldots, x_n$. $1 = x_1^0 \ldots x_n^0$ is the unit element in the monoid $[X]$. $\mathrm{lcm}(s, t)$ denotes the least common multiple of the power products s, t.

Commutative rings with 1 in which the *basis condition* holds, i.e. in which every ideal has a finite basis, are usually called *Noetherian rings*. This notation is motivated by the following lemma.

Lemma 2.3.1. *In a Noetherian ring there are no infinitely ascending chains of ideals.* □

Theorem 2.3.2. (Hilbert's Basis Theorem) *If R is a Noetherian ring then also the univariate polynomial ring $R[x]$ is Noetherian.*

Hilbert's Basis Theorem implies that the multivariate polynomial ring $K[X]$ is Noetherian, if K is a field. So every ideal I in $K[X]$ has a finite basis, and if we are able to effectively compute with finite bases then we are dealing with all the ideals in $K[X]$.

We will define a Gröbner basis of a polynomial ideal via a certain reduction relation for polynomials. A Gröbner basis will be a basis with respect to which the corresponding reduction relation is confluent. Before we can define the reduction relation on the polynomial ring, we have to introduce an ordering of the power products with respect to which the reduction relation should be decreasing.

Definition 2.3.3. Let $<$ be an ordering on $[X]$ that is compatible with the monoid structure, i.e.
(i) $1 = x_1^0 \dots x_n^0 < t$ for all $t \in [X] \setminus \{1\}$, and
(ii) $s < t \Longrightarrow su < tu$ for all $s, t, u \in [X]$.
We call such an ordering $<$ on $[X]$ an *admissible ordering.* □

Example 2.3.4. We give some examples of frequently used admissible orderings on $[X]$.
(a) The *lexicographic ordering* with $x_{\pi(1)} > x_{\pi(2)} > \dots > x_{\pi(n)}$, π a permutation of $\{1, \dots, n\}$:
$x_1^{i_1} \dots x_n^{i_n} <_{lex,\pi} x_1^{j_1} \dots x_n^{j_n}$ iff there exists a $k \in \{1, \dots, n\}$ such that for all $l < k$ $i_{\pi(l)} = j_{\pi(l)}$ and $i_{\pi(k)} < j_{\pi(k)}$.
If $\pi = \mathrm{id}$, we get the usual lexicographic ordering $<_{lex}$.
(b) The *graduated lexicographic ordering* w.r.t. the permutation π and the weight function $w : \{1, \dots, n\} \to \mathbb{R}^+$:
for $s = x_1^{i_1} \dots x_n^{i_n}, t = x_1^{j_1} \dots x_n^{j_n}$ we define $s <_{glex,\pi,w} t$ iff

$$\Big(\sum_{k=1}^{n} w(k) i_k < \sum_{k=1}^{n} w(k) j_k\Big) \quad \text{or}$$

$$\Big(\sum_{k=1}^{n} w(k) i_k = \sum_{k=1}^{n} w(k) j_k \quad \text{and} \quad s <_{lex,\pi} t\Big).$$

We get the usual graduated lexicographic ordering $<_{glex}$ by setting $\pi = \mathrm{id}$ and $w = 1_{const}$.

(c) The *graduated reverse lexicographic ordering*:
we define $s <_{grlex} t$ iff

$$\deg(s) < \deg(t) \quad \text{or}$$

$$(\deg(s) = \deg(t) \text{ and } t <_{lex,\pi} s, \text{ where } \pi(j) = n - j + 1).$$

(d) The *product ordering* w.r.t. $i \in \{1, \ldots, n-1\}$ and the admissible orderings $<_1$ on $X_1 = [x_1, \ldots, x_i]$ and $<_2$ on $X_2 = [x_{i+1}, \ldots, x_n]$:
for $s = s_1 s_2, t = t_1 t_2$, where $s_1, t_1 \in X_1, s_2, t_2 \in X_2$, we define $s <_{prod,i,<_1,<_2} t$ iff

$$s_1 <_1 t_1 \quad \text{or} \quad (s_1 = t_1 \text{ and } s_2 <_2 t_2). \qquad \square$$

Lemma 2.3.5. *Let $<$ be an admissible ordering on $[X]$.*
(i) If $s, t \in [X]$ and s divides t then $s \leq t$.
(ii) $<$ (or actually $>$) is Noetherian, i.e. there are no infinite chains of the form $t_0 > t_1 > t_2 > \ldots$, and consequently every subset of $[X]$ has a smallest element.

Proof: Winkler, *Computer Algebra*, Lemma 8.2.3. $\square$

Throughout this chapter let R be a commutative ring with 1, K a field, X a set of variables, and $<$ an admissible ordering on $[X]$.

Whenever a set M is equipped with a Noetherian relation $\longrightarrow$ we can apply the **Principle of Noetherian Induction** [1] for proving that a predicate P holds for all $x \in M$:
if for all $x \in M$

$$\big[\forall y \in M : (x \longrightarrow y) \Longrightarrow P(y)\big] \implies P(x)$$

then

$$\forall x \in M : P(x) \ .$$

[1] see P.M. Cohn, *Algebra*, Wiley, New York (1974)

Definition 2.3.6. Let s be a power product in $[X]$, f a non-zero polynomial in $R[X]$, F a subset of $R[X]$.
By $\mathrm{coeff}(f,s)$ we denote the coefficient of s in f.
$\mathrm{lpp}(f) := \max_<\{t \in [X] \mid \mathrm{coeff}(f,t) \neq 0\}$ (*leading power product* of f),
$\mathrm{lc}(f) := \mathrm{coeff}(f, \mathrm{lpp}(f))$ (*leading coefficient* of f),
$\mathrm{in}(f) := \mathrm{lc}(f)\mathrm{lpp}(f)$ (*initial* of f),
$\mathrm{red}(f) := f - \mathrm{in}(f)$ (*reductum* of f),
$\mathrm{lpp}(F) := \{\mathrm{lpp}(f) \mid f \in F \setminus \{0\}\}$,
$\mathrm{lc}(F) := \{\mathrm{lc}(f) \mid f \in F \setminus \{0\}\}$,
$\mathrm{in}(F) := \{\mathrm{in}(f) \mid f \in F \setminus \{0\}\}$,
$\mathrm{red}(F) := \{\mathrm{red}(f) \mid f \in F \setminus \{0\}\}$. □

If I is an ideal in $R[X]$, then $\mathrm{lc}(I) \cup \{0\}$ is an ideal in R. However, $\mathrm{in}(F) \cup \{0\}$ in general is not an ideal in $R[X]$.

Definition 2.3.7. Any admissible ordering $<$ on $[X]$ induces a partial ordering $\ll$ on $R[X]$, the *induced ordering*, in the following way:

$$
\begin{aligned}
f \ll g \text{ iff } \quad & f = 0 \text{ and } g \neq 0 \text{ or} \\
& f \neq 0,\ g \neq 0 \text{ and } \mathrm{lpp}(f) < \mathrm{lpp}(g) \text{ or} \\
& f \neq 0,\ g \neq 0,\ \mathrm{lpp}(f) = \mathrm{lpp}(g) \text{ and } \mathrm{red}(f) \ll \mathrm{red}(g).
\end{aligned}
$$

Lemma 2.3.8. *$\ll$ (or actually $\gg$) is a Noetherian partial ordering on $R[X]$.*

Proof: We have to show that every sequence $f_1 \gg f_2 \gg \ldots$ is finite. This is achieved by Noetherian induction on $\mathrm{lpp}(f_1)$ w.r.t. $>$. □

One of the central notions of the theory of Gröbner bases is the concept of polynomial reduction.

Definition 2.3.9. Let $f, g, h \in K[X]$, $F \subseteq K[X]$. We say that g *reduces to h w.r.t. f* ($g \longrightarrow_f h$) iff there are power products $s, t \in [X]$ such that s has a non–vanishing coefficient c in g ($\mathrm{coeff}(g,s) = c \neq 0$), $s = \mathrm{lpp}(f) \cdot t$, and

$$h = g - \frac{c}{\mathrm{lc}(f)} \cdot t \cdot f.$$

If we want to indicate which power product and coefficient are used in the

reduction, we write

$$g \longrightarrow_{f,b,t} h, \qquad \text{where } b = \frac{c}{lc(f)}.$$

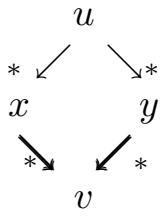
We say that g *reduces to* h *w.r.t.* F ($g \longrightarrow_F h$) iff there is $f \in F$ such that $g \longrightarrow_f h$. □

Example 2.3.10. Let $F = \{\ldots, f = x_1x_3 + x_1x_2 - 2x_3, \ldots\}$ in $\mathbb{Q}[x_1, x_2, x_3]$, and $g = x_3^3 + 2x_1x_2x_3 + 2x_2 - 1$. Let $<$ be the graduated lexicographic ordering with $x_1 < x_2 < x_3$.
Then $g \longrightarrow_F x_3^3 - 2x_1x_2^2 + 4x_2x_3 + 2x_2 - 1 =: h$, and in fact $g \longrightarrow_{f,2,x_2} h$.
□

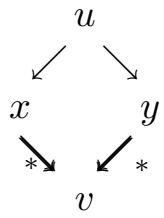
Definition 2.3.11. Let $\longrightarrow$ be a reduction relation, i.e. a binary relation, on a set M.

- $x \longrightarrow$ means x is *reducible*, i.e. $x \longrightarrow y$ for some y;
- $\underline{x}\!\!\not\longrightarrow$ means x is *irreducible* or *in normal form* w.r.t. $\longrightarrow$. We omit mentioning the reduction relation if it is clear from the context;
- $x \downarrow y$ means that x and y have a *common successor*, i.e. $x \longrightarrow z \longleftarrow y$ for some z;
- $x \uparrow y$ means that x and y have a *common predecessor*, i.e. $x \longleftarrow z \longrightarrow y$ for some z;
- x *is a* $\longrightarrow$*–normal form* of y iff $y \longrightarrow^* \underline{x}$. □

Definition 2.3.12. (a) $\longrightarrow$ is *Noetherian* or has the *termination property* iff every reduction sequence terminates, i.e. there is no infinite sequence $x_1, x_2, \ldots$ in M such that $x_1 \longrightarrow x_2 \longrightarrow \ldots$.
(b) $\longrightarrow$ is *Church–Rosser* or has the *Church–Rosser property* iff $a \longleftrightarrow^* b$ implies $a \downarrow_* b$.
(c) $\longrightarrow$ is *confluent* iff $x \uparrow^* y$ implies $x \downarrow_* y$, or graphically every diamond of the following form can be completed:



(d) $\longrightarrow$ is *locally confluent* iff $x \uparrow y$ implies $x \downarrow_* y$, or graphically every diamond of the following form can be completed:



□

As a consequence of the Noetherianity of admissible orderings we get that $\longrightarrow_F$ is Noetherian for any set of polynomials $F \subset K[X]$. So, in contrast to the general theory of rewriting, termination is not a problem for polynomial reductions. But we still have to worry about the Church-Rosser property.

Theorem 2.3.13. (a) $\longrightarrow$ is Church–Rosser if and only if $\longrightarrow$ is confluent.
(b) (Newman Lemma) Let $\longrightarrow$ be Noetherian. Then $\longrightarrow$ is confluent if and only if $\longrightarrow$ is locally confluent.
(c) (Refined Newman Lemma) Let $\longrightarrow$ be a reduction on M and $<$ a partial Noetherian ordering on M s.t. $\longrightarrow \subseteq >$. Then $\longrightarrow$ is confluent if and only if for all $x, y, z \in M$:

$$x \longleftarrow z \longrightarrow y \quad \text{implies} \quad x \longleftrightarrow^*_{(<z)} y$$

i.e. all intermediate elements w in the chain $x \longleftrightarrow^* y$ satisfy $w < z$. In this case we say *x and y are connected w.r.t. $\longrightarrow$ below z.*

Proof: For (a) and (b) see Theorem 8.1.2 in [Winkler 1996].
For (c) see Theorem 8.1.3 in [Winkler 1996]. □

As an immediate consequence of the previous definitions we get that the reduction relation $\longrightarrow$ is (nearly) compatible with the operations in the polynomial ring. Moreover, the reflexive–transitive–symmetric closure of the reduction relation $\longrightarrow_F$ is equal to the congruence modulo the ideal generated by F.

Lemma 2.3.14. *Let $a \in K^*$, $s \in [X]$, $F \subseteq K[X]$, $g_1, g_2, h \in K[X]$.*
(a) $\longrightarrow_F \subseteq \gg$,
(b) $\longrightarrow_F$ is Noetherian,

(c) if $g_1 \longrightarrow_F g_2$ *then* $a \cdot s \cdot g_1 \longrightarrow_F a \cdot s \cdot g_2$,
(d) if $g_1 \longrightarrow_F g_2$ *then* $g_1 + h \downarrow_F^* g_2 + h$.

Proof: [Winkler 1996] Exercise 8.2(2). □

Theorem 2.3.15. *Let* $F \subseteq K[X]$. *The ideal congruence modulo* $\langle F \rangle$ *equals the reflexive–transitive–symmetric closure of* $\longrightarrow_F$, *i.e.* $\equiv_{\langle F \rangle} = \longleftrightarrow_F^*$.

Proof: [Winkler 1996] Exercise 8.2(3). □

So the congruence $\equiv_{\langle F \rangle}$ can be decided if $\longrightarrow_F$ has the Church–Rosser property. Of course, this is not the case for an arbitrary set F. Such distinguished sets (bases for polynomial ideals) are called Gröbner bases.

Definition 2.3.16. A subset F of $K[X]$ is a *Gröbner basis* (for $\langle F \rangle$) iff $\longrightarrow_F$ is Church–Rosser. □

A Gröbner basis of an ideal I in $K[X]$ is by no means uniquely defined. In fact, whenever F is a Gröbner basis for I and $f \in I$, then also $F \cup \{f\}$ is a Gröbner basis for I.

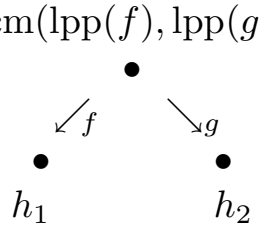
For testing whether a given basis F of an ideal I is a Gröbner basis it suffices to test for local confluence of the reduction relation $\longrightarrow_F$. This, however, does not yield a decision procedure, since there are infinitely many situations $f \uparrow_F g$. However, Buchberger has been able to reduce this test for local confluence to just testing a finite number of sitations $f \uparrow_F g$ [Buchberger 1965]. For that purpose he has introduced the notion of subtraction polynomials, or S–polynomials for short.

Definition 2.3.17. Let $f, g \in K[X]^*$, $t = \mathrm{lcm}(\mathrm{lpp}(f), \mathrm{lpp}(g))$. Then

$$\mathrm{cp}(f,g) = \left(t - \frac{1}{\mathrm{lc}(f)} \cdot \frac{t}{\mathrm{lpp}(f)} \cdot f,\ t - \frac{1}{\mathrm{lc}(g)} \cdot \frac{t}{\mathrm{lpp}(g)} \cdot g\right)$$

is the *critical pair* of f and g. The difference of the elements of $\mathrm{cp}(f,g)$ is the *S–polynomial* $\mathrm{spol}(f,g)$ of f and g. □

If $\mathrm{cp}(f,g) = (h_1, h_2)$ then we can depict the situation graphically in the following way:



The critical pairs of elements of F describe exactly the essential branchings of the reduction relation $\longrightarrow_F$.

Theorem 2.3.18. (Buchberger's Theorem) *Let F be a subset of $K[X]$.*
(a) F is a Gröbner basis if and only if $g_1 \downarrow_F^* g_2$ for all critical pairs (g_1, g_2) of elements of F.
(b) F is a Gröbner basis if and only if $\mathrm{spol}(f,g) \longrightarrow_F^* 0$ for all $f, g \in F$.

Proof: ([Winkler 1996] Theorem 8.3.1)
(a) Obviously, if F is a Gröbner basis then $g_1 \downarrow_F^* g_2$ for all critical pairs (g_1, g_2) of F.

On the other hand, assume that $g_1 \downarrow_F^* g_2$ for all critical pairs (g_1, g_2). By the Refined Newman Lemma (Theorem 2.3.13(c)) it suffices to show $h_1 \longleftarrow\!\!\!\longrightarrow_{F(\ll h)}^* h_2$ for all h, h_1, h_2 such that $h_1 \longleftarrow_F h \longrightarrow_F h_2$.
Let s_1, s_2 be the power products that are eliminated in the reductions of h to h_1 and h_2, respectively. I.e. there are polynomials $f_1, f_2 \in F$, coefficients $c_1 = \mathrm{coeff}(h, s_1) \neq 0$, $c_2 = \mathrm{coeff}(h, s_2) \neq 0$, and power products t_1, t_2 such that

$$s_1 = t_1 \mathrm{lpp}(f_1), \quad h_1 = h - \frac{c_1}{\mathrm{lc}(f_1)} t_1 f_1 \quad \text{and}$$
$$s_2 = t_2 \mathrm{lpp}(f_2), \quad h_2 = h - \frac{c_2}{\mathrm{lc}(f_2)} t_2 f_2.$$

We distinguish two cases, depending on whether or not $s_1 = s_2$.
Case $s_1 \neq s_2$: w.l.o.g. assume $s_1 > s_2$. Let $a = \mathrm{coeff}(-(c_1/\mathrm{lc}(f_1))t_1 f_1, s_2)$. Then $\mathrm{coeff}(h_1, s_2) = c_2 + a$ and therefore

$$h_1 \longrightarrow_F h_1 - \frac{c_2 + a}{\mathrm{lc}(f_2)} t_2 f_2 = h - \frac{c_1}{lc(f_1)} t_1 f_1 - \frac{c_2 + a}{\mathrm{lc}(f2)} t_2 f_2.$$

On the other hand

$$h_2 \longrightarrow_F h_2 - \frac{c_1}{\mathrm{lc}(f_1)} t_1 f_1 \longrightarrow_F h_2 - \frac{c_1}{\mathrm{lc}(f_1)} t_1 f_1 - \frac{a}{\mathrm{lc}(f_2)} t_2 f_2 =$$
$$h - \frac{c_1}{lc(f_1)} t_1 f_1 - \frac{c_2 + a}{\mathrm{lc}(f2)} t_2 f_2.$$

Thus, $h_1 \longleftrightarrow^*_{F(\ll h)} h_2$, in fact $h_1 \downarrow^*_F h_2$.
Case $s_1 = s_2$: let $s = s_1 = s_2$, $c = \mathrm{coeff}(h, s)$ and $h' = h - cs$. So for some power product t we have $s = t \cdot \mathrm{lcm}(\mathrm{lpp}(f_1), \mathrm{lpp}(f_2))$, and $h_1 = h' + c \cdot t \cdot g_1$, $h_2 = h' + c \cdot t \cdot g_2$, where $(g_1, g_2) = \mathrm{cp}(f_1, f_2)$. By assumption $g_1 \downarrow^*_F g_2$, i.e. there are $p_1, \ldots, p_k$ and $q_1, \ldots, q_l$ such that

$$g_1 = p_1 \longrightarrow_F \ldots \longrightarrow_F p_k = q_l \longleftarrow_F \ldots \longleftarrow_F q_1 = g_2.$$

So, by Lemma 2.3.14(c),

$$ctg_1 = ctp_1 \longrightarrow_F \ldots \longrightarrow_F ctp_k = ctq_l \longleftarrow_F \ldots \longleftarrow_F ctq_1 = ctg_2.$$

Applying Lemma 2.3.14(d) we get

$$h_1 = h' + ctp_1 \downarrow^*_F \ldots \downarrow^*_F h' + ctp_k = h' + ctq_l \downarrow^*_F \ldots \downarrow^*_F h' + ctq_1 = h_2.$$

All the intermediate polynomials in these reductions are less than h w.r.t. $\ll$. Thus, $h_1 \longleftrightarrow^*_{F(\ll)} h_2$.

(b) Every S–polynomial is congruent to 0 modulo $\langle F \rangle$. So by Theorem 2.3.15 $\mathrm{spol}(f, g) \longleftrightarrow^*_F 0$. If F is a Gröbner basis, this implies $\mathrm{spol}(f, g) \longrightarrow^*_F 0$.

On the other hand assume that $\mathrm{spol}(f, g) \longrightarrow^*_F 0$ for all $f, g \in F$. We use the same notation as in (a). In fact, the whole proof is analogous to the one for (a), except for the case $s_1 = s_2 = s$. So for $h_1 = h' + ctg_1 \longleftarrow_F h \longrightarrow_F h' + ctg_2 = h_2$ we have to show $h_1 \longleftrightarrow^*_{F(\ll h)} h_2$.
$g_1 - g_2$ is the S–polynomial of $f_1, f_2 \in F$, so by the assumption $g_1 - g_2 \longrightarrow^*_F 0$. By Lemma 2.3.14 also $h_1 - h_2 = ct(g_1 - g_2) \longrightarrow^*_F 0$, i.e. for some $p_1, \ldots, p_k$ we have

$$h_1 - h_2 = p_1 \longrightarrow_F \ldots \longrightarrow_F p_k = 0.$$

Again by Lemma 2.3.14 we get

$$h_1 = p_1 + h_2 \downarrow^*_F \ldots \downarrow^*_F p_k + h_2 = h_2,$$

and therefore $h_1 \longleftrightarrow^*_{F(\ll h)} h_2$. □

Buchberger's theorem suggests an algorithm for checking whether a given finite basis is a Gröbner basis: reduce all the S–polynomials to normal forms and check whether they are all 0. In fact, by a simple extension we get an algorithm for constructing Gröbner bases.

---

algorithm GRÖBNER_B(**in:** F**; out:** G)**;**
[Buchberger algorithm for computing a Gröbner basis.
F is a finite subset of $K[X]^*$;
G is a finite subset of $K[X]^*$, such that
$\langle G\rangle = \langle F\rangle$ and G is a Gröbner basis.]
(1) $G := F$**;**
$C := \{\{g_1, g_2\} \mid g_1, g_2 \in G, g_1 \neq g_2\}$**;**
(2) **while** not all pairs $\{g_1, g_2\} \in C$ are marked **do**
{choose an unmarked pair $\{g_1, g_2\}$**;**
mark $\{g_1, g_2\}$**;**
$h :=$ normal form of $\mathrm{spol}(g_1, g_2)$ w.r.t. $\longrightarrow_G$**;**
if $h \neq 0$
then$\{C := C \cup \{\{g, h\} \mid g \in G\}$**;**
$G := G \cup \{h\}$ **};**
};
return □

Every polynomial h constructed in GRÖBNER_B is in $\langle F\rangle$, so $\langle G\rangle = \langle F\rangle$ throughout GRÖBNER_B. Thus, by Theorem 1.8 GRÖBNER_B yields a correct result if it stops. The termination of GRÖBNER_B is a consequence of Dickson's Lemma which implies that in $[X]$ there is no infinite chain of elements $s_1, s_2, \ldots$ such that $s_i \not| \; s_j$ for all $1 \leq i < j$. The leading power products of the polynomials added to the basis form such a sequence in $[X]$, so this sequence must be finite.

Theorem 2.3.19. (Dickson's Lemma) *Every $A \subseteq [X]$ contains a finite subset B, such that every $t \in A$ is a multiple of some $s \in B$.*

Proof: [Winkler 1996] 8.3.2. □

The termination of GRÖBNER_B also follows from Hilbert's Basis

Theorem applied to the initial ideals of the sets G constructed in the course of the algorithm, i.e. $\langle \mathrm{in}(G) \rangle$.

The algorithm GRÖBNER_B provides a constructive proof of the following theorem.

Theorem 2.3.20. *Every ideal I in $K[X]$ has a Gröbner basis.* □

Example 2.3.21. Let $F = \{f_1, f_2\}$, with $f_1 = x^2y^2 + y - 1$, $f_2 = x^2y + x$. We compute a Gröbner basis of $\langle F \rangle$ in $\mathbb{Q}[x, y]$ w.r.t. the graduated lexicographic ordering with $x < y$. The following describes one way in which the algorithm GRÖBNER_B could execute (recall that there is a free choice of pairs in the loop):

(1) $\mathrm{spol}(f_1, f_2) = f_1 - yf_2 = -xy + y - 1 =: f_3$ is irreducible, so $G := \{f_1, f_2, f_3\}$.
(2) $\mathrm{spol}(f_2, f_3) = f_2 + xf_3 = xy \longrightarrow_{f_3} y - 1 =: f_4$, so $G := \{f_1, f_2, f_3, f_4\}$.
(3) $\mathrm{spol}(f_3, f_4) = f_3 + xf_4 = y - x - 1 \longrightarrow_{f_4} -x =: f_5$, so $G := \{f_1, \ldots, f_5\}$.

All the other S–polynomials now reduce to 0, so GRÖBNER_B terminates with

$$G = \{x^2y^2 + y - 1, x^2y + x, -xy + y - 1, y - 1, -x\}.$$ □

In addition to the original definition and the ones given in Theorem 2.3.18, there are many other characterizations of Gröbner bases. We list only a few of them.

Theorem 2.3.22. *Let I be an ideal in $K[X]$, $F \subseteq K[X]$, and $\langle F \rangle \subseteq I$. Then the following are equivalent.*

(a) F is a Gröbner basis for I.
(b) $f \longrightarrow_F^* 0$ for every $f \in I$.
(c) $f \longrightarrow_F$ for every $f \in I \setminus \{0\}$.
(d) For all $g \in I, h \in K[X]$: if $g \longrightarrow_F^* \underline{h}$ then $h = 0$.
(e) For all $g, h_1, h_2 \in K[X]$: if $g \longrightarrow_F^* \underline{h_1}$ and $g \longrightarrow_F^* \underline{h_2}$ then $h_1 = h_2$.
(f) $\langle \mathrm{in}(F) \rangle = \langle \mathrm{in}(I) \rangle$.

Proof: [Winkler 1996] Theorem 8.3.4. □

The Gröbner basis G computed in Example 2.3.21 is much too complicated. In fact, $\{y - 1, x\}$ is a Gröbner basis for the ideal. There is a general

procedure for simplifying Gröbner bases.

Theorem 2.3.23. *Let G be a Gröbner basis for an ideal I in $K[X]$. Let $g, h \in G$ and $g \neq h$.*
(a) If $\mathrm{lpp}(g) \mid \mathrm{lpp}(h)$ then $G' = G \setminus \{h\}$ is also a Gröbner basis for I.
(b) If $h \longrightarrow_g h'$ then $G' = (G \setminus \{h\}) \cup \{h'\}$ is also a Gröbner basis for I.

Proof: [Winkler 1996] Theorem 8.3.5. □

Observe that the elimination of basis polynomials described in Theorem 2.3.23(a) is only possible if G is a Gröbner basis. In particular, we are not allowed to do this during a Gröbner basis computation. Based on Theorem 2.3.23 we can show that every ideal has a unique Gröbner basis after suitable pruning and normalization.

Definition 2.3.24. Let G be a Gröbner basis in $K[X]$.
G is *minimal* iff $\mathrm{lpp}(g) \not| \ \mathrm{lpp}(h)$ for all $g, h \in G$ with $g \neq h$.
G is *reduced* iff for all $g, h \in G$ with $g \neq h$ we cannot reduce h by g.
G is *normed* iff $\mathrm{lc}(g) = 1$ for all $g \in G$. □

From Theorem 2.3.23 we obviously get an algorithm for transforming any Gröbner basis for an ideal I into a normed reduced Gröbner basis for I. No matter from which Gröbner basis of I we start and which path we take in this transformation process, we always reach the same uniquely defined normed reduced Gröbner basis of I.

Theorem 2.3.25. *Every ideal in $K[X]$ has a unique finite normed reduced Gröbner basis.*

Proof: [Winkler 1996] Theorem 8.3.6. □

Observe that the normed reduced Gröbner basis of an ideal I depends, of course, on the admissible ordering $<$. Different orderings can give rise to different Gröbner bases. However, if we decompose the set of all admissible orderings into sets which induce the same normed reduced Gröbner basis of a fixed ideal I, then this decomposition is finite. This leads to the consideration of universal Gröbner bases. A universal Gröbner basis for I is a basis for I which is a Gröbner basis w.r.t. any admissible ordering of

the power products.

If we have a Gröbner basis G for an ideal I, then we can compute in the vector space $K[X]_{/I}$ over K. The irreducible power products (with coefficient 1) modulo G form a basis of $K[X]_{/I}$. We get that $\dim(K[X]_{/I})$ is the number of irreducible power products modulo G. Thus, this number is independent of the particular admissible ordering.

Example 2.3.26. Let $I = \langle x^3y - 2y^2 - 1, x^2y^2 + x + y\rangle$ in $\mathbb{Q}[x, y]$. Let $<$ be the graduated lexicographic ordering with $x > y$. Then the normed reduced Gröbner basis of I has leading power products x^4, x^3y, x^2y^2, y^3. So there are 9 irreducible power products.

If $<$ is the lexicographic ordering with $x > y$, then the normed reduced Gröbner basis of I has leading power products x and y^9. So again there are 9 irreducible power products.

In fact, $\dim(\mathbb{Q}[x, y]_{/I}) = 9$. □