Gröbner Technology

Teo Mora

1 Notation and Definitions

$\mathbb{F}$ denotes an arbitrary field, $\overline{\mathbb{F}}$ denotes its algebraic closure and $\mathbb{F}_q$ denotes a finite field of size q (so q is implicitly understood to be a power of a prime) and $\mathcal{P} := \mathbb{F}[X] := \mathbb{F}[x_1, \ldots, x_n]$ the polynomial ring over the field $\mathbb{F}$.

For any ideal $\mathfrak{I} \subset \mathcal{P}$ and any extension field $\mathbb{E}$ of $\mathbb{F}$, let $\mathcal{V}_{\mathbb{E}}(\mathfrak{I})$ denote the set of the rational points of $\mathfrak{I}$ over $\mathbb{E}$. We also write $\mathcal{V}(\mathfrak{I}) = \mathcal{V}_{\overline{\mathbb{F}}}(\mathfrak{I})$.

Let $\mathcal{T}$ be the set of terms in $\mathcal{P}$, *id est*

$$\mathcal{T} := \{x_1^{a_1} \cdots x_n^{a_n} : (a_1, \ldots, a_n) \in \mathbb{N}^n\},$$

which is a multiplicative version of the additive semigroup $\mathbb{N}^n$, the relation between these notations being obvious: given

$$\alpha := (a_1, \ldots, a_n), \qquad \beta := (b_1, \ldots, b_n), \qquad \gamma := (c_1, \ldots, c_n)$$

and the terms

$$\tau_a := X^\alpha = x_1^{a_1} \cdots x_n^{a_n}, \qquad \tau_b := X^\beta = x_1^{b_1} \cdots x_n^{b_n}, \qquad \tau_c := X^\gamma = x_1^{c_1} \cdots x_n^{c_n},$$

we have

$$\begin{aligned} &\tau_a \cdot \tau_b = \tau_c \iff a_i + b_i = c_i \quad \text{for each } i \iff \alpha + \beta = \gamma, \\ &\tau_a \mid \tau_b \iff a_i \le b_i \quad \text{for each } i \iff \alpha \le_P \beta, \end{aligned}$$

where $<_P$ is the natural partial ordering over $\mathbb{N}^n$.

The assignment of a finite set of terms

$$G := \{\tau_1, \ldots, \tau_\nu\} \subset \mathcal{T}, \quad \tau_i = x_1^{a_1^{(i)}} \cdots x_n^{a_n^{(i)}}$$

—or, equivalently of a finite set of integer vectors

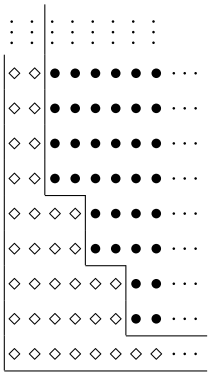
$$\{a^{(1)}, \ldots, a^{(\nu)}\} \subset \mathbb{N}^n, \quad a^{(i)} = (a_1^{(i)}, \ldots, a_n^{(i)}) \in \mathbb{N}^n,$$

defines a partition of $\mathcal{T}$ (resp. $\mathbb{N}^n$) in two parts (see Fig. 1 where $G := \{x_1^6 x_2, x_1^4 x_2^3, x_1^2 x_2^5\} \subset \mathcal{T}$):

T. Mora
DIMA and DISI, Università di Genova, Genova, Italy
e-mail: theomora@dima.unige.it

M. Sala et al. (eds.), *Gröbner Bases, Coding, and Cryptography*,
DOI 10.1007/978-3-540-93806-4_2,

Fig. 1 A Gröbner escalier



- $T := \{\tau\tau_i : \tau \in \mathcal{T}, 1 \le i \le \nu\} \cong \{\alpha + a^{(i)} : \alpha \in \mathbb{N}^n, 1 \le i \le \nu\} =: \Sigma$ which is a *semigroup ideal*, *id est* a subset $T \subset \mathcal{T}$ (resp. $\Sigma \subset \mathbb{N}^n$) such that

$$\tau \in \mathcal{T}, t \in T \Longrightarrow \tau t \in T, \text{resp. } a \in \Sigma, b \in \mathbb{N}^n, a \le_P b \Longrightarrow b \in \Sigma;$$

- $N := \mathcal{T} \setminus T \cong \mathbb{N}^n \setminus \Sigma =: \Delta$ which is an *order ideal*, *id est* a subset $N \subset \mathcal{T}$ (resp. $\Delta \subset \mathbb{N}^n$) such that

$$\tau \in \mathcal{T}, t \in N, \tau \mid t \Longrightarrow \tau \in N, \text{resp. } a \in \Delta, b \in \mathbb{N}^n, a \ge_P b \Longrightarrow b \in \Delta.$$

Remark that the assignment of

- a finite monomial set $G \subset \mathcal{T}$,
- a semigroup ideal $T \subset \mathcal{T}$,
- an order ideal $N \subset \mathcal{T}$

uniquely characterizes the other data: in fact

– N and T are related by their being complementary in $\mathcal{T}$,
– each semigroup ideal $T \subset \mathcal{T}$ has a unique minimal basis $G \subset T$ such that $T := \{\tau\tau_i : \tau \in \mathcal{T}, \tau_i \in G\}$; the fact, whose proof is quite involved, that G is finite is known as Dickson's lemma but actually was already proved by Gordan (1900).

We recall that the well-orderings on $\mathcal{T}$ which are a *semigroup ordering*, *id est* satisfy

$$\tau_1 < \tau_2 \quad \Longrightarrow \quad \tau\tau_1 < \tau\tau_2 \quad \text{for each } \tau, \tau_1, \tau_2 \in \mathcal{T}$$

are called *term orderings*, even if the old-fashioned notion of *admissible ordering* can still be found somewhere.

For a free-module $\mathcal{P}^m$, $m \in \mathbb{N}$, we denote by $\{\mathbf{e}_1, \ldots, \mathbf{e}_m\}$ its canonical basis,

$$\begin{aligned}\mathcal{T}^{(m)} &= \{t\mathbf{e}_i, t \in \mathcal{T}, 1 \le i \le m\} \\ &= \{x_1^{a_1} \cdots x_n^{a_n}\mathbf{e}_i, (a_1, \ldots, a_n) \in \mathbb{N}^n, 1 \le i \le m\}\end{aligned}$$

denotes its monomial $\mathbb{F}$-basis and $\prec$ denotes a well-ordering on $\mathcal{T}^{(m)}$ which is compatible with the term-ordering $\prec$ on $\mathcal{T}$, that is, satisfying

$$\tau_1 \preceq \tau_2, \qquad \mathsf{t}_1 \preceq \mathsf{t}_2, \quad \Longrightarrow \quad \tau_1\mathsf{t}_1 \preceq \tau_2\mathsf{t}_2$$

for each $\tau_1, \tau_2 \in \mathcal{T}, \mathsf{t}_1, \mathsf{t}_2 \in \mathcal{T}^{(m)}$.

Note that $\mathcal{T}^{(1)} = \mathcal{T}$.

For each $f = \sum_{\tau\in\mathcal{T}^{(m)}} \mathsf{c}(f,\tau)\tau \in \mathcal{P}^m$, its *support* is

$$\mathrm{supp}(f) := \{\tau \in \mathcal{T}^{(m)} : \mathsf{c}(f,\tau) \neq 0\},$$

its *leading term* is the term $\mathbf{T}_\prec(f) := \max_\prec(\mathrm{supp}(f))$, its *leading coefficient* is $\mathrm{lc}_\prec(f) := \mathsf{c}(f, \mathbf{T}_\prec(f))$ and its *leading monomial* is $\mathbf{M}_\prec(f) := \mathrm{lc}_\prec(f)\mathbf{T}_\prec(f)$.

When $\prec$ is understood we will drop the subscript, as in $\mathbf{T}(f) = \mathbf{T}_\prec(f)$.

For any set $F \subset \mathcal{P}^m$, write

- $\mathbf{T}\{F\} := \mathbf{T}_\prec\{F\} := \{\mathbf{T}(f) : f \in F\}$;
- $\mathbf{M}\{F\} := \mathbf{M}_\prec\{F\} := \{\mathbf{M}(f) : f \in F\}$;
- $\mathbf{T}(F) := \mathbf{T}_\prec(F) := \{\tau\mathbf{T}(f) : \tau \in \mathcal{T}, f \in F\}$, a *monomial module*[1];
- $\mathbf{N}(F) := \mathbf{N}_\prec(F) := \mathcal{T}^{(m)} \setminus \mathbf{T}_\prec(F)$, an *order module*[2];
- $\mathbb{I}(F) = \langle F\rangle$ the module generated by F.

Remark that, if $m = 1$, the assignment of $\mathbf{T}\{F\}$ gives the partition $\mathcal{T} = \mathbf{T}(F) \sqcup \mathbf{N}(F)$ discussed above, that the related semigroup ideal $\mathbf{T}(F)$ is also denoted $\Sigma(F)$ while the related order ideal $\mathbf{N}(F)$ is also denoted $\Delta(F)$ and labelled *Δ-set* or *footprint*. When F is the Gröbner basis of the module $\mathbb{I}(F)$ it generates, $\mathbf{N}(F)$ is called the *Gröbner éscalier* (Galligo 1974) of $\mathbb{I}(F)$.

We can now induce a finer partition of $\mathcal{T}^{(m)}$ in terms of a module $\mathsf{M} \subset \mathcal{P}^m$ and a term-ordering $\prec$, by defining (see Fig. 2 where this time we have set $\mathsf{M} := \mathbb{I}(x_1^6, x_1^4x_2^3, x_2^5) \subset \mathcal{P}$)

- $\diamond$ $\mathbf{N}_\prec(\mathsf{M}) = \mathcal{T}^{(m)} \setminus \mathbf{T}_\prec(\mathsf{M})$ its *Gröbner éscalier*;
- $\circ$ $\mathbf{B}_\prec(\mathsf{M}) := \{x_h\tau : 1 \leq h \leq n, \tau \in \mathbf{N}_\prec(\mathsf{M})\} \setminus \mathbf{N}_\prec(\mathsf{M})$, its *border set*;
- $\bullet$ $\mathbf{J}_\prec(\mathsf{M}) := \mathbf{T}_\prec(\mathsf{M}) \setminus \mathbf{B}_\prec(\mathsf{M})$,
- $*$ $\mathbf{G}_\prec(\mathsf{M}) \subset \mathbf{B}_\prec(\mathsf{M})$ the unique minimal basis of $\mathbf{T}_\prec(\mathsf{M})$,
- $\cdot$ $\mathbf{C}_\prec(\mathsf{M}) := \{\tau \in \mathbf{N}_\prec(\mathsf{M}) : x_h\tau \in \mathbf{T}_\prec(\mathsf{M}), \forall h\}$ its *corner set*.

Under this notation, the following properties are trivially satisfied:

Lemma 1 *It holds*

1. $\mathbf{T}_\prec(\mathsf{M}) = \{\tau \in \mathcal{T} : \exists g \in \mathsf{M} : \mathbf{T}_\prec(g) = \tau\}$;
2. $\mathbf{J}_\prec(\mathsf{M}) = \{\tau \in \mathbf{T}_\prec(\mathsf{M}) : x_i \mid \tau \Longrightarrow \frac{\tau}{x_i} \in \mathbf{T}_\prec(\mathsf{M})\}$;
3. $\mathbf{B}_\prec(\mathsf{M}) = \{\tau \in \mathbf{T}_\prec(\mathsf{M}) : \exists x_i \mid \tau, \frac{\tau}{x_i} \in \mathbf{N}_\prec(\mathsf{M})\}$;

[1] *Id est* a subset $T \subset \mathcal{T}^{(m)}$ such that $\tau \in \mathcal{T}, \mathsf{t} \in T \Longrightarrow \tau\mathsf{t} \in T$.

[2] *Id est* a subset $N \subset \mathcal{T}^{(m)}$ such that $\tau \in \mathcal{T}, \tau\mathsf{t} \in N \Longrightarrow \mathsf{t} \in N$.

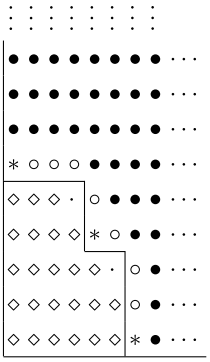


Fig. 2 A refined Gröbner escalier

4. $\mathbf{G}_\prec(\mathsf{M}) = \{\tau \in \mathbf{T}_\prec(\mathsf{M}) : \forall x_i \mid \tau, \frac{\tau}{x_i} \in \mathbf{N}_\prec(\mathsf{M})\}$;
5. $\mathbf{C}_\prec(\mathsf{M}) = \{\tau \in \mathbf{N}_\prec(\mathsf{M}) : \forall i, x_i\tau \in \mathbf{B}_\prec(\mathsf{M})\}$;
6. $\mathbf{N}_\prec(\mathsf{M}) = \{\tau \in \mathcal{T} : \nexists g \in \mathsf{M} : \mathbf{T}_\prec(g) = \tau\}$;
7. $\mathbf{C}_\prec(\mathsf{M}) \cup \mathbf{T}_\prec(\mathsf{M})$ *is a monomial module*;
8. $\mathbf{N}_\prec(\mathsf{M}) \cup \mathbf{G}_\prec(\mathsf{M})$ *and* $\mathbf{N}_\prec(\mathsf{M}) \cup \mathbf{B}_\prec(\mathsf{M})$ *are order modules*.
9. $\tau \in \mathbf{J}_\prec(\mathsf{M}) \iff \forall x_i \mid \tau, \frac{\tau}{x_i} \in \mathbf{T}_\prec(\mathsf{M})$;
10. $\tau \in \mathbf{B}_\prec(\mathsf{M}) \setminus \mathbf{G}_\prec(\mathsf{M}) \iff \exists h, H : \frac{\tau}{x_h} \in \mathbf{N}_\prec(\mathsf{M}), \frac{\tau}{x_H} \in \mathbf{B}_\prec(\mathsf{M}) \subset \mathbf{T}_\prec(\mathsf{M})$;
11. $\tau \in \mathbf{B}_\prec(\mathsf{M}) \setminus \mathbf{G}_\prec(\mathsf{M}) \Longrightarrow \forall x_i \mid \tau, \frac{\tau}{x_i} \in \mathbf{N}_\prec(\mathsf{M}) \cup \mathbf{B}_\prec(\mathsf{M})$;
12. $\tau \in \mathbf{N}_\prec(\mathsf{M}) \cup \mathbf{G}_\prec(\mathsf{M}) \iff \forall x_i \mid \tau, \frac{\tau}{x_i} \in \mathbf{N}_\prec(\mathsf{M})$;
13. $\tau \in \mathbf{T}_\prec(\mathsf{M}) \cup \mathbf{C}_\prec(\mathsf{M}) \iff \forall i, x_i\tau \in \mathbf{T}_\prec(\mathsf{M})$;
14. $\tau \in \mathbf{N}_\prec(\mathsf{M}) \setminus \mathbf{C}_\prec(\mathsf{M}) \iff \exists h : x_h\tau \in \mathbf{N}_\prec(\mathsf{M})$.

Lemma 2 *Let* N *be a finitely generated* $\mathcal{P}$*-module,* $\Phi : \mathcal{P}^m \mapsto \mathsf{N}$ *be any surjective morphism and set* $\mathsf{M} := \ker(\Phi)$. *Then*

1. $\mathcal{P}^m \cong \mathsf{M} \oplus \mathrm{Span}_{\mathbb{F}}(\mathbf{N}(\mathsf{M}))$;
2. $\mathsf{N} \cong \mathrm{Span}_{\mathbb{F}}(\mathbf{N}(\mathsf{M}))$;
3. *for each* $f \in \mathcal{P}^m$, *there is a unique* $g := \mathrm{Can}(f, \mathsf{M}, \prec) \in \mathrm{Span}_{\mathbb{F}}(\mathbf{N}(\mathsf{M}))$ *such that* $f - g \in \mathsf{M}$.
   Such g *is called the* canonical form *of* f *w.r.t.* M *and satisfies also*:
   (a) $\mathrm{Can}(f_1, \mathsf{M}, \prec) = \mathrm{Can}(f_2, \mathsf{M}, \prec) \iff f_1 - f_2 \in \mathsf{M}$;
   (b) $\mathrm{Can}(f, \mathsf{M}, \prec) = 0 \iff f \in \mathsf{M}$.

Definition 3 Let N be a finitely generated $\mathcal{P}$-module, $\Phi : \mathcal{P}^m \mapsto \mathsf{N}$ be any surjective morphism and set $\mathsf{M} := \ker(\Phi)$.

Let $G \subset \mathsf{M}$, $f, h, f_1, f_2 \in \mathcal{P}^m$. Then

1. G will be called a *Gröbner basis* of M if

$$\mathbf{T}(G) = \mathbf{T}(\mathsf{M}),$$

that is, $\mathbf{T}\{G\} := \{\mathbf{T}(g) : g \in G\}$ generates $\mathbf{T}(\mathsf{M}) = \mathbf{T}\{\mathsf{M}\}$.

2. For each $f_1, f_2 \in \mathcal{P}^m$ such that

$$\mathbf{T}(f_1) = t_1 \mathbf{e}_{l_1}, \qquad \mathbf{T}(f_2) = t_2 \mathbf{e}_{l_2},$$

the *S-polynomial of* f_1 *and* f_2 exists only if $\mathbf{e}_{l_1} = \mathbf{e}_{l_2} := \epsilon$, in which case it is

$$S(f_1, f_2) := \mathrm{lc}(f_2)^{-1} \frac{\delta(f_1, f_2)}{t_2} f_2 - \mathrm{lc}(f_1)^{-1} \frac{\delta(f_1, f_2)}{t_1} f_1,$$

where $\delta := \delta(f_1, f_2) := \mathrm{lcm}(t_1, t_2)$; $\delta\epsilon$ is called the *formal term* of $S(f_1, f_2)$.

3. f has a *Gröbner representation* $\sum_{i=1}^{\mu} p_i g_i$ in terms of G if [3]

$$f = \sum_{i=1}^{\mu} p_i g_i, \quad p_i \in \mathcal{P},\ g_i \in G, \qquad \mathbf{T}(p_i)\mathbf{T}(g_i) \preceq \mathbf{T}(f), \quad \text{for each } i.$$

4. f has the *(strong) Gröbner representation* $\sum_{i=1}^{\mu} c_i t_i g_i$ in terms of G if

$$f = \sum_{i=1}^{\mu} c_i t_i g_i, \quad c_i \in \mathbb{F} \setminus \{0\},\ t_i \in \mathcal{T},\ g_i \in G,$$

with $\mathbf{T}(f) = t_1 \mathbf{T}(g_1) \succ \cdots \succ t_i \mathbf{T}(g_i) \succ \cdots$.

5. f has the *weak Gröbner representation* $\sum_{i=1}^{\mu} c_i t_i g_i$ in terms of G if

$$f = \sum_{i=1}^{\mu} c_i t_i g_i, \quad c_i \in \mathbb{F} \setminus \{0\}, t_i \in \mathcal{T}, g_i \in G,$$

with $\mathbf{T}(f) = t_1 \mathbf{T}(g_1) \succeq \cdots \succeq t_i \mathbf{T}(g_i) \succeq \cdots$.

6. For any $f_1, f_2 \in \mathcal{P}^m$, whose S-polynomial exists and has $\delta\epsilon$ as formal term, we say that $S(f_1, f_2)$ has a *quasi-Gröbner representation* in terms of G if it can be written as $S(g, f) = \sum_{k=1}^{\mu} p_k g_k$, with $p_k \in \mathcal{P}$, $g_k \in G$ and $\mathbf{T}(p_k)\mathbf{T}(g_k) \prec \delta\epsilon$ for each k.

7. $h := \mathrm{NF}_{\prec}(f, G)$ is called a *normal form* of f w.r.t. G, if

- $f - h \in \mathbb{I}(G)$ has a strong Gröbner representation in terms of G and
- $h \neq 0 \Longrightarrow \mathbf{T}(h) \notin \mathbf{T}(G)$.

8. The *reduced Gröbner basis* of M wrt $\prec$ is the set

$$\{\tau - \mathrm{Can}(\tau, \mathsf{M}, \prec) : \tau \in \mathbf{G}_{\prec}(\mathsf{M})\}.$$

9. The *border basis* of M w.r.t. $\prec$ is the set

$$\{\tau - \mathrm{Can}(\tau, \mathsf{M}, \prec) : \tau \in \mathbf{B}_{\prec}(\mathsf{M})\}.$$

[3] Note that here, unlike in (4), we are not assuming $i \neq j \Longrightarrow \mathbf{T}(p_i)\mathbf{T}(g_i) \neq \mathbf{T}(p_j)\mathbf{T}(g_j)$; moreover both here, in (4) and in (5) a same element of G can repeatedly appear.

10. A *Gröbner representation* of M is the assignment of

- a linearly independent set $\mathbf{q} = \{q_1, \ldots, q_s\}$ $(q_1 = 1)$, where $s = \#(\mathbf{N}(\mathsf{M}))$, such that $\mathcal{P}^m/\mathsf{M} = \mathrm{Span}_{\mathbb{F}}(\mathbf{q})$,
- the set

$$\mathcal{M} = \mathcal{M}(\mathbf{q}) := \left\{ \left(a_{lj}^{(h)}\right) \in \mathbb{F}^{s^2}, 1 \le h \le n \right\}$$

of the $s \times s$ square matrices $(a_{lj}^{(h)})$ defined by the equalities

$$x_h q_l = \sum_j a_{lj}^{(h)} q_j, \quad \forall l, j, h, 1 \le l, j \le s, 1 \le h \le n$$

in $\mathcal{P}^m/\mathsf{M} = \mathrm{Span}_{\mathbb{F}}(\mathbf{q})$.

11. For each $f \in \mathcal{P}$ the *Gröbner description* of f in terms of a Gröbner representation $(\mathbf{q}, \mathcal{M})$ is the unique vector

$$\mathbf{Rep}(f, \mathbf{q}) := (\gamma(f, q_1, \mathbf{q}), \ldots, \gamma(f, q_s, \mathbf{q})) \in \mathbb{F}^s$$

such that $f - \sum_j \gamma(f, q_j, \mathbf{q}) q_j \in \mathsf{M}$.

12. The *linear representation* of M w.r.t. $\prec$ is the Gröbner representation $(\mathbf{N}_\prec(\mathsf{M}), \mathcal{M}(\mathbf{N}_\prec(\mathsf{M})))$ where $\mathbf{q} = \mathbf{N}_\prec(\mathsf{M})$.

With these definitions, if $\mathbf{N}_\prec(\mathsf{M}) = \{\tau_1, \ldots, \tau_s\}$, *the Gröbner description*

$$\mathbf{Rep}(f, \mathbf{N}_\prec(\mathsf{M})) := (\gamma(f, \tau_1, \mathbf{N}_\prec(\mathsf{M})), \ldots, \gamma(f, \tau_s, \mathbf{N}_\prec(\mathsf{M})))$$

of f in terms of the linear representation of M *w.r.t.* $\prec$ is a convoluted synonym of the notion of canonical form

$$\mathrm{Can}(f, \mathsf{M}, \prec) = \sum_{j=1}^{s} \gamma(f, \tau_j, \prec)\tau_j = \sum_{j=1}^{s} \gamma(f, \tau_j, \mathbf{N}_\prec(\mathsf{M}))\tau_j$$

of f in terms of $\prec$.

2 Term-Orderings: Classification and Representation

Definition 4 A *weight function* $v_{\mathsf{w}} : \mathcal{T} \mapsto \mathbb{R}$ on $\mathcal{T}$ and $\mathcal{P}$ is the assignment of a vector $\mathsf{w} := (w_1, \ldots, w_n) \in \mathbb{R}^n$, $w_i \ge 0$, so that $v_{\mathsf{w}}(X^a) = \mathsf{w} \cdot a = \sum_i w_i a_i$.

Theorem 5 (Erdös 1956) *Each semigroup ordering $\prec$ on $\mathcal{T}$ is characterized by assigning $r \le n$ linearly independent vectors*

$$\mathsf{w}_1, \ldots, \mathsf{w}_j := (w_{j1}, \ldots, w_{jn}), \ldots, \mathsf{w}_r \in \mathbb{R}^n$$

—or equivalently an $r \times n$ matrix $(w_{ji}) \in \mathbb{R}^{rn}$ of maximal rank—so that for each $\tau_a := X^a$, $\tau_b := X^b$ in $\mathcal{T}$, we have

$$\tau_a < \tau_b \iff \exists j\colon \quad \mathsf{w}_j \cdot a < \mathsf{w}_j \cdot b \quad \textit{and} \quad \mathsf{w}_i \cdot a = \mathsf{w}_i \cdot b \quad \textit{for } i < j.$$

Moreover, such an ordering is a well-ordering iff, for each i, $X_i > 1$, that is iff, for each i, $w_{ji} > 0$, where j denotes the minimal value for which $w_{ji} \neq 0$.

Finally, if M_1, M_2 are two $r \times n$ matrices, then they characterize the same ordering $<$ iff there is an invertible r-square matrix $A = (a_{ij})$ such that

$$M_1 = AM_2 \quad \textit{and} \quad a_{ij} = \begin{cases} 0 & \textit{if } i < j, \\ 1 & \textit{if } i = j. \end{cases}$$

Among the term-orderings we will quote those which have common and practical use, also for applications.

- The **lexicographical** (lex) ordering induced by $X_1 < X_2 < \cdots < X_n$ is defined by

$$X_1^{a_1} \cdots X_n^{a_n} < X_1^{b_1} \cdots X_n^{b_n} \iff \exists j\colon \quad a_j < b_j \quad \text{and} \quad a_i = b_i \quad \text{for } i > j;$$

  it has good elimination properties since it allows to compute all the elimination ideals $I \cap \mathbb{F}[X_1, \ldots, X_i]$:

  Fact 6 If G is the Gröbner basis of $I \subset \mathbb{F}[X_1, \ldots, X_n]$ w.r.t. lex then, for each $i \leq n$, $G \cap \mathbb{F}[X_1, \ldots, X_i]$ is the Gröbner basis of $I \cap \mathbb{F}[X_1, \ldots, X_i]$ w.r.t. lex.

- Note that the lexicographical ordering depends on a chosen ordering imposed on the variables; recently many authors prefer using the lexicographical ordering induced by $X_1 > X_2 > \cdots > X_n$ which is defined by

$$X_1^{a_1} \cdots X_n^{a_n} < X_1^{b_1} \cdots X_n^{b_n} \iff \exists j\colon \quad a_j < b_j \quad \text{and} \quad a_i = b_i \quad \text{for } i < j.$$

- The **reverse lexicographical** (rev-lex) ordering induced by $X_1 < X_2 < \cdots < X_n$ is defined by

$$X_1^{a_1} \cdots X_n^{a_n} < X_1^{b_1} \cdots X_n^{b_n} \iff \exists j\colon \quad a_j > b_j \quad \text{and} \quad a_i = b_i \quad \text{for } i < j;$$

  it is not a well-ordering since $\cdots < X_i^{d+1} < X_i^d < \cdots < X_1 < 1$.

- The **deg-rev-lex**[4] (degree reverse lexicographical) ordering induced by $X_1 < X_2 < \cdots < X_n$ is the one where terms are first compared by their degree and the ties are solved using rev-lex: it is defined by

$$X^a < X^b \iff \text{exists } j\colon \quad a_j > b_j \quad \text{and} \quad a_i = b_i \quad \text{for } 0 \leq i < j,$$

  where we set $a_0 := -\sum_i a_i$, $b_0 := -\sum_i b_i$ and has the following property

[4] Often shorthanded as *drl*.

Fact 7 Denoting, for each $i \le n$, $\pi_i : \mathcal{T} \mapsto \mathcal{T} \cap \mathbb{F}[X_1, \ldots, X_i]$ the projection[5] defined by

$$\pi_i(X_j) := \begin{cases} X_j & \text{if } j > i \\ 1 & \text{if } j \le i \end{cases}$$

then any two terms $t_1, t_2 \in \mathcal{T}$ satisfy

$$t_1 < t_2 \iff \text{exists } j\text{:} \quad d_{j1} < d_{j2}, \quad \text{and} \quad d_{i1} = d_{i2} \quad \text{for each } i < j$$

where we have set $d_{ji} := \deg(\pi_j(t_i))$.

- Naturally, also the definitions of the rev-lex and deg-rev-lex orderings depend on a chosen ordering imposed on the variables; thus, the deg-rev-lex ordering induced by $X_1 > X_2 > \cdots > X_n$ is defined as

$$X^a < X^b \iff \exists j\text{:} \quad a_j > b_j \quad \text{and} \quad a_i = b_i \quad \text{for } n+1 \ge i > j,$$

where we set $a_{n+1} := -\sum_i a_i, b_{n+1} := -\sum_i b_i$.
- More in general, given an ordering $<$ on $\mathcal{T}$ its **degree extension** is the ordering $\prec$ defined as

$$t_1 \prec t_2 \iff \deg(t_1) < \deg(t_2) \quad \text{or} \quad \deg(t_1) = \deg(t_2), \quad t_1 < t_2.$$

- If we have a weight vector $\mathsf{w} := (w_1, \ldots, w_n) \in \mathbb{R}^n \setminus \{\mathbf{0}\}$ and a term ordering $<$, the construction leading to the degree extension of $<$ can be performed to lead to the **weight extension** $\prec$ of $<$ (or the *refinement of* v_w with $<$) defined as

$$t \prec T \iff v_\mathsf{w}(t) < v_\mathsf{w}(T) \quad \text{or} \quad v_\mathsf{w}(t) = v_\mathsf{w}(T), \quad t < T.$$

Bayer and Stillman (1987) proved that the rev-lex ordering is the 'most efficient' refinement of a weight function v_w.

Given a term-ordering $<$ on $\mathcal{T}$, a $<$-compatible well-ordering $\prec$ on $\mathcal{T}^{(m)}$ can be defined in different ways; we limit ourselves to quote the more standard constructions referring to Carrà Ferro and Sit (1994), Caboara and Silvestri (1999) for a more general treatment: setting an ordering $\lessdot$ on the canonical basis $\{\mathbf{e}_1, \ldots, \mathbf{e}_m\}$,

- the **TOP** (term over position) ordering is defined as

$$t_1\mathbf{e}_{l_1} \prec t_2\mathbf{e}_{l_2} \iff t_1 < t_2 \quad \text{or} \quad t_1 = t_2, \mathbf{e}_{l_1} \lessdot \mathbf{e}_{l_2};$$

- the **POT** (position over term) ordering is defined as

$$t_1\mathbf{e}_{l_1} \prec t_2\mathbf{e}_{l_2} \iff \mathbf{e}_{l_1} \lessdot \mathbf{e}_{l_2} \quad \text{or} \quad \mathbf{e}_{l_1} = \mathbf{e}_{l_2}, t_1 < t_2.$$

[5] Obviously π_0 is just the identity.

$(g, \sum_{i=1}^{\mu} c_i t_i g_i) := \mathbf{NormalForm}(f, G)$
$g := f, i := 0,$
While $\mathbf{T}(g) \in \mathbf{T}(G)$ **do**
  Let $t \in \mathcal{T}, \gamma \in G : t\mathbf{T}(\gamma) = \mathbf{T}(g),$
  $i := i + 1, c_i := \frac{\mathrm{lc}(g)}{\mathrm{lc}(\gamma)}, t_i := t, g_i := \gamma, g := g - c_i t_i g_i.$
$\mu := i$

Fig. 3 Buchberger normal form algorithm

3 Buchberger's Theorem and Algorithm

The *Buchberger Normal Form Algorithm* (Buchberger 1965, 1970, 1998, 2006) (see Fig. 3) is a Gaussian-like linear algebra reduction which, given a finite set $F \subset \mathcal{P}^m$ and an element $f \in \mathcal{P}^m$, returns a normal form g of f w.r.t. F and a strong Gröbner representation[6] $\sum_{i=1}^{\mu} c_i t_i g_i$ of $f - g$ in terms of F; extending it we obtain the *Buchberger Canonical Form Algorithm* (Buchberger 1965, 1970, 1998, 2006) (see Fig. 4) which, if F is assumed to be a Gröbner basis, returns the canonical form $g := \mathrm{Can}(f, \mathsf{M}, \prec) \in \mathrm{Span}_{\mathbb{F}}(\mathbf{N}(\mathsf{I}))$ and strong Gröbner representation $\sum_{i=1}^{\mu} c_i t_i g_i$ of $f - g$ in terms of F.

Corollary 8 *Let* N *be a finitely generated* $\mathcal{P}$*-module,* $\Phi : \mathcal{P}^m \to \mathsf{N}$ *be any surjective morphism and set* $\mathsf{M} := \ker(\Phi)$*. Let* G *be a Gröbner basis of* M *w.r.t.* $\prec$*. Then*

1. *For each* $f \in \mathcal{P}^m$, $f - \mathrm{Can}(f, \mathsf{M})$ *has a strong Gröbner representation in terms of* G;
2. *The* reduced Gröbner basis *of* M *w.r.t.* $\prec$ *is the unique set* $G \subset \mathsf{M}$ *such that*[7]
   (a) $\mathbf{T}_{\prec}\{G\}$ *is an irredundant basis of* $\mathbf{T}_{\prec}(\mathsf{M})$;
   (b) *for each* $g \in G$, $\mathrm{lc}(g) = 1$;
   (c) *for each* $g \in G$, $g - \mathbf{T}(g) \in \mathrm{Span}_{\mathbb{F}}(\mathbf{N}(\mathsf{M}))$.

On each free module $\mathcal{P}^s$ ($\{\mathsf{e}_1, \ldots, \mathsf{e}_s\}$ denotes its canonical basis) one can impose a valuation $v : \mathcal{P}^s \to \mathcal{T}$ by fixing s terms $\tau_1, \ldots, \tau_s$ and defining for each i $v(\mathsf{e}_i) := \tau_i$, so that, for each $f := (h_1, \ldots, h_s) = \sum_i h_i \mathsf{e}_i$ we have $v(f) := \max_{\prec}\{\mathbf{T}_{\prec}(h_i)\tau_i\}$; by definition, its *leading form* $\mathcal{L}(f)$ is the homogeneous component (of degree $v(f)$) $(\nu_1, \ldots, \nu_m)$ where

$$\nu_i = \begin{cases} \mathbf{M}(h_i) & \text{iff } \mathbf{T}(t_i)\tau_i = v(f) \\ 0 & \text{otherwise.} \end{cases}$$

[6] The reason why *strong* Gröbner representations are pinned up among Gröbner representations of a polynomial is that the output of Buchberger Form Algorithms is necessarily *strong*.

The notion of weak Gröbner representation (Definition 3.5) has a similar rôle in the more esoteric theory of Gröbner bases for polynomials over a ring, for which the reader is directed to Byrne and Mora (2009).

[7] A basis which satisfies only conditions (a) and (b), but not necessarily (c), is called a *minimal Gröbner basis*.

$(g, \sum_{i=1}^{\mu} c_i t_i g_i) := \mathbf{CanonicalForm}(f, G)$
$h := f, i := 0, g := 0,$
While $h \neq 0$ **do**
$\%\%\ f = g + \sum_{i=1}^{\mu} c_i t_i g_i + h,$
$\%\%\ \mathbf{T}(f-g) \geq \mathbf{T}(h);$
$\%\%\ i > 0 \implies \mathbf{T}(f-g) = t_1\mathbf{T}(g_1) > t_2\mathbf{T}(g_2) > \cdots > t_i\mathbf{T}(g_i) > \mathbf{T}(h);$
  If $\mathbf{T}(h) \in \mathbf{T}(G)$ **do**
    Let $t \in \mathcal{T}, \gamma \in G : t\mathbf{T}(\gamma) = \mathbf{T}(h)$
    $i := i+1, c_i := \frac{\mathrm{lc}(h)}{\mathrm{lc}(\gamma)}, t_i := t, g_i := \gamma, h := h - c_i t_i g_i.$
  Else
    $\%\%\ \mathbf{T}(h) \in \mathbf{N}(\mathsf{M})$
    $h := h - \mathbf{M}(h), g := g + \mathbf{M}(h)$
$\mu := i$

Fig. 4 Buchberger canonical form algorithm

Such valuation is of course compatible with the natural valuation of $\mathcal{P}$ and an element $\sum_i h_i \mathsf{e}_i$ is homogeneous of degree τ iff, for each i

$$h_i \neq 0 \implies h_i = \mathbf{M}(h_i) \quad \text{and} \quad \mathbf{T}(h_i)\tau_i = \tau.$$

Definition 9 Denoting, for each set $F \subset \mathcal{P}^s$,

$$\mathcal{L}\{F\} := \{\mathcal{L}(f) : f \in F\}, \qquad \mathcal{L}(F) := \mathbb{I}(\mathcal{L}\{F\}),$$

given a module $\mathsf{E} \subset \mathcal{P}^s$, the homogeneous module $\mathcal{L}(\mathsf{E})$ is called the *leitmodul* of E. Any set $B \subset \mathsf{E}$ such that $\mathcal{L}(B) = \mathcal{L}(\mathsf{E})$ is called a *standard basis* of E and is a basis of it.

Fixed a set $\{g_1, \ldots, g_s\} := G \subset \mathsf{M}$, with $\mathbf{M}(g_j) := c_j \tau_j \mathbf{e}_{l_j}$, for each j, I will freely use the shorthand

$$\mathbf{T}(l_1, l_2, \ldots, l_r) := \mathrm{lcm}(\tau_i : i \in \{l_1, i_2, \ldots, l_r\})\varepsilon$$

for each set $\{l_1, l_2, \ldots, l_r\} \subseteq \{1, \ldots, s\}$ satisfying $\mathbf{e}_{l_1} = \cdots = \mathbf{e}_{l_r} =: \varepsilon$; in particular for $i, j, k, 1 \leq i, j, k \leq s$, $\mathbf{e}_{l_i} = \mathbf{e}_{l_j} = \mathbf{e}_{l_k} =: \varepsilon$, we have

$$\mathbf{T}(i) = \mathbf{T}(g_i), \qquad \mathbf{T}(i,j) := \mathrm{lcm}(\tau_i, \tau_j)\varepsilon, \qquad \mathbf{T}(i,j,k) := \mathrm{lcm}(\tau_i, \tau_j, \tau_k)\varepsilon;$$

for each pair $\{i, j\}$, $1 \leq i < j \leq s$ for which $\mathbf{e}_{l_i} = \mathbf{e}_{l_j} =: \varepsilon$, I will also use the shorthand $S(i, j)$ to denotes $S(g_i, g_j)$, $\omega(i, j) := \mathbf{T}(i, j)\varepsilon$ to denote its formal term and

$$s(i,j) := c_j^{-1} \frac{\mathbf{T}(i,j)}{\tau_j} \mathsf{e}_j - c_i^{-1} \frac{\mathbf{T}(i,j)}{\tau_i} \mathsf{e}_i.$$

If, with the current notation, we impose on the module $\mathcal{P}^s$ the valuation v defined by $v(\mathsf{e}_j) := \tau_j$, we have that if $f := \sum_j h_j \mathsf{e}_j \in \mathcal{P}^s$ satisfies $\sum_j h_j g_j = 0$

necessarily, denoting

$$\tau\varepsilon := \max_{\prec}\{\mathbf{T}_<(h_i)\mathbf{T}_\prec(g_i)\} \quad \text{and} \quad I := \{i, 1 \le i \le s : \mathbf{T}(h_i)\mathbf{T}(g_i) = \tau\varepsilon\}$$

the homogeneous element $\mathcal{L}(f) := \sum_j v_j \mathsf{e}_j \in \mathcal{P}^s$ of degree τ satisfies

- $0 \neq v_j \Longrightarrow j \in I$ and $v_j = \mathbf{M}(h_j) =: d_j\omega_j$,
- $\sum_{j=1}^s v_j \mathbf{M}_<(g_j) = \sum_{j\in I}(d_j\omega_j)\cdot(c_j\tau_j\mathbf{e}_{l_j}) = (\sum_{j\in I}(d_jc_j)\cdot(\tau_j\omega_j))\varepsilon = 0$,
- $\sum_{j\in I} d_j \operatorname{lc}(g_j) = 0$ and $\omega_j\mathbf{T}_<(g_j) = \tau\varepsilon$ for each $j \in I$.

Definition 10 Given a finite set $G := \{g_1, \ldots, g_s\} \subset \mathcal{P}^m$, $\mathbf{M}(g_j) := c_j\tau_j\mathbf{e}_{l_j}$, and denoting $\mathfrak{S} : \mathcal{P}^s \to \mathcal{P}$ the map defined by $\sum_{i=1}^s p_i\mathsf{e}_i \mapsto \sum_{i=1}^s p_i g_i$:

1. each element of $\ker(\mathfrak{S}) \subset \mathcal{P}^s$ is called a *syzygy* of G;
2. the *syzygy module* of G is the module

$$\ker(\mathfrak{S}) := \{(p_1, \ldots, p_s) : \sum_{i=1}^s p_i g_i = 0\} \subset \mathcal{P}^s;$$

3. the *natural* valuation v on $\mathcal{P}^s$ is the one defined by $v(\mathsf{e}_j) := \tau_j$.

Remark 11

1. if $f := (p_1, \ldots, p_s)$ is a syzygy of G, then $\mathcal{L}(f) := \sum_j v_j\mathsf{e}_j \in \mathcal{P}^s$ is a homogeneous syzygy of $\mathbf{M}\{G\}$;
2. for each homogeneous syzygy $\phi := \sum_j d_j\omega_j\mathsf{e}_j \in \mathcal{P}^s$ of $\mathbf{M}\{G\}$ the element $h := \mathfrak{S}(\phi) = \sum_j d_j\omega_j g_j \in \mathcal{P}^m$, if is not zero, satisfies

$$\mathbf{T}(h) < v(\phi) = \omega_j\tau_j \quad \text{for each } j;$$

   therefore if $h = \sum_j p_j g_j$ is a Gröbner representation in terms of G, then

$$f := \phi - h = \phi - \sum_j p_j\mathsf{e}_j = \sum_j (d_j\omega_j - p_j)\mathsf{e}_j \in \ker(\mathfrak{S})$$

   is a syzygy and satisfies $v(f) = v(\phi)$ and $\mathcal{L}(f) = \phi$;
3. for each $i, j, 1 \le i < j \le s$, for which $S(i, j)$ exists and has $\omega(i, j) := \mathbf{T}(i, j)\varepsilon$ as formal term, it holds $\mathcal{L}(S(i, j)) = s(i, j)$ which is a homogeneous element of degree $\mathbf{T}(i, j)$;
4. conversely $S(i, j) = \mathfrak{S}(s(i, j))$;
5. denoting $\mathfrak{B} := \{\{i, j\} : 1 \le i < j \le s, S(i, j) \text{ exists}\}$, $\{s(i, j) : \{i, j\} \in \mathfrak{B}\}$ is a homogeneous basis of the syzygy module of $\mathbf{M}\{G\}$.

Lemma 12 (Buchberger's First Criterion 1979) *With the present notation, under the assumption that* M *is an ideal, it holds*

$$\mathbf{T}(i)\mathbf{T}(j) = \mathbf{T}(i, j) \quad \Longrightarrow \quad \mathrm{NF}(S(i, j), G) = 0.$$

Lemma 13 (Buchberger's Second Criterion 1979) *For $i, j, 1 \leq i < j \leq s$, $\mathbf{e}_{l_i} = \mathbf{e}_{l_j} =: \varepsilon$, if there is $k, 1 \leq k \leq s$: $\mathbf{T}(k) \mid \mathbf{T}(i, j)$,—so that in particular $\mathbf{e}_{l_k} = \varepsilon$,—and $S(i, k)$ and $S(k, j)$ have a quasi-Gröbner representation in terms of G, then also $S(i, j)$ has a quasi-Gröbner representation.*

Definition 14 (Gebauer and Möller 1985, 1988) Denoting $\mathfrak{B} := \{\{i, j\} : 1 \leq i < j \leq s, S(i, j) \text{ exists}\}$ and

$$\mathfrak{B}_1 := \begin{cases} \{\{i, j\} : \mathbf{T}(i)\mathbf{T}(j) = \mathbf{T}(i, j)\} & \text{iff } \mathsf{M} \text{ is an ideal,} \\ \emptyset & \text{otherwise} \end{cases}$$

a subset $\mathfrak{GM} \subset \mathfrak{B} \setminus \mathfrak{B}_1$ is called a *Gebauer–Möller set* for G iff the set $\{s(i, j) : \{i, j\} \in \mathfrak{GM} \cup \mathfrak{B}_1\}$ is a homogeneous basis of the syzygy module of $\mathbf{M}\{G\}$.

Theorem 15 (Buchberger) *Let $\mathsf{M} \subset \mathcal{P}^m$ be a sub-module, and $\{g_1, \ldots, g_s\} =: G \subset \mathsf{M}$, with $\mathbf{T}(g_j) := \tau_j \mathbf{e}_{l_j}$ and wlog $\mathrm{lc}(g_j) = 1$ for each j; denoting $\mathfrak{B}$ and $\mathfrak{B}_1$ as in Definition 14 and $\mathfrak{GM} \subset \mathfrak{B} \setminus \mathfrak{B}_1$ any Gebauer–Möller set for G, the following conditions are equivalent*:

1. *G is a Gröbner basis of M;*
2. *$f \in \mathsf{M} \iff$ it has a Gröbner representation in terms of G;*
3. *$f \in \mathsf{M} \iff$ it has a strong Gröbner representation in terms of G;*
4. *for each $f \in \mathcal{P}^m \setminus \{0\}$ and any normal form $h := \mathrm{NF}(f, G)$ of f w.r.t. G, $f \in \mathsf{M} \iff h = 0$;*
5. *for each $f \in \mathcal{P} \setminus \{0\}$, $f - \mathrm{Can}(f, \mathsf{M})$ has a strong Gröbner representation in terms of G;*
6. *for each $i, j, 1 \leq i < j \leq s$, the S-polynomial $S(i, j)$ (if it exists) has a quasi-Gröbner representation in terms of G.*
7. *for each homogeneous basis $\mathcal{B}$ of the syzygy module of $\mathbf{M}\{G\}$ and for each element $\phi \in \mathcal{B}$, there is a syzygy $f_\phi \in \ker(\mathfrak{S})$ of G, such that $\mathcal{L}(f_\phi) = \phi$;*
8. *for each $\{i, j\} \in \mathfrak{GM}$, the S-polynomial $S(i, j)$ has a quasi-Gröbner representation in terms of G.*
9. *for each $\{i, j\} \in \mathfrak{GM}$ the S-polynomial $S(i, j)$ has a Gröbner representation in terms of G.*

Corollary 16 *With the present notation and under the equivalent conditions of Theorem 15, the set*

$$\{f_\phi : \phi \in \mathfrak{GM}\} \cup \left\{ c_j^{-1} \frac{\mathbf{T}(i, j)}{\tau_j} \mathsf{e}_j - c_i^{-1} \frac{\mathbf{T}(i, j)}{\tau_i} \mathsf{e}_i : (i, j) \in \mathfrak{B}_1 \right\}$$

is a standard basis of $\ker(\mathfrak{S})$.

Lemma 17 (Möller 1988) *For each $i, j, k : 1 \leq i, j, k \leq s$, $\mathbf{e}_{l_i} = \mathbf{e}_{l_j} = \mathbf{e}_{l_k}$, it holds*

$$\frac{\mathrm{lcm}(\tau_i, \tau_j, \tau_k)}{\mathrm{lcm}(\tau_i, \tau_k)} S(i, k) - \frac{\mathrm{lcm}(\tau_i, \tau_j, \tau_k)}{\mathrm{lcm}(\tau_i, \tau_j)} S(i, j) + \frac{\mathrm{lcm}(\tau_i, \tau_j, \tau_k)}{\mathrm{lcm}(\tau_k, \tau_j)} S(k, j) = 0.$$

Corollary 18 (Gebauer and Möller 1985, 1988) (*Compare Lemma 13*)
Under the assumption of Lemma 17 if the equivalent conditions $\mathbf{T}(i,j,k) = \mathbf{T}(i,j)$ *and* $\mathbf{T}(k) \mid \mathbf{T}(i,j)$ *are satisfied and both* $S(i,k)$ *and* $S(k,j)$ *have a quasi-Gröbner representation in terms of* G, *then also* $S(i,j)$ *has a quasi-Gröbner representation.*

Proposition 19 (Gebauer and Möller 1985, 1988) *With the present notation, denote*

$\mathfrak{GM}_* \subset \{\{i,j\}, 1 \le i < j < s\}$ *a Gebauer–Möller set for* $\{g_1, \ldots, g_{s-1}\}$
$\mathfrak{B}_2 := \{\{i,j\} \in \mathfrak{GM}_* : \mathbf{T}(i,j,s) = \mathbf{T}(i,j), \mathbf{T}(i,s) \neq \mathbf{T}(i,j) \neq \mathbf{T}(j,s)\}.$

Let $\mathsf{T} := \{\mathbf{T}(j,s) : 1 \le j < s\}$ *and* $\mathsf{T}' \subset \mathsf{T}$ *be the set of the elements* $\tau \in \mathsf{T}$ *such that either*

- *exists* $\tau' \in \mathsf{T} : \tau' \mid \tau \neq \tau'$ *or*
- (*in case* M *is an ideal*) *exists* $i_\tau : 1 \le i_\tau < s, \mathbf{T}(i_\tau)\mathbf{T}(s) = \mathbf{T}(i_\tau, s) = \tau$;

for each $\tau \in \mathsf{T} \setminus \mathsf{T}'$ *choose* $i_\tau, 1 \le i_\tau < s$, *such that* $\mathbf{T}(i_\tau, s) = \tau$ *and define*

$$\mathfrak{B}_3(G) := \{\{i_\tau, s\} : \tau \in \mathsf{T} \setminus \mathsf{T}'\}.$$

Then $(\mathfrak{GM}_* \setminus \mathfrak{B}_2) \cup \mathfrak{B}_3(G)$ *is a Gebauer–Möller set for* G

Thus, given a finite basis $F := \{g_1, \ldots, g_s\} \subset \mathsf{M}$, the Buchberger Algorithm (Fig. 5) returns a Gröbner basis G of M by iteratively forcing condition (9) of Theorem 15 and applying Proposition 19 in order to efficiently remove the so called *useless pairs*, *id est* those which are known, for theoretical reasons (Lemmas 12 and 13, Corollary 18), having 0 as normal form.

$(G) := \mathbf{GröbnerBasis}(F)$
where
  $F := \{g_1, \ldots, g_s\} \subset \mathcal{P} \setminus \{0\}$,
  G is a Gröbner basis of the ideal $\mathbb{I}(F)$;
$G := \{g_1, g_2\}, B := \emptyset$
If $\mathbf{T}(1)\mathbf{T}(2) \neq \mathbf{T}(1,2)$ **then** $B := B \cup \{\{1,2\}\}$
For each $r, 3 \le r \le s$ **do**
  $G := G \cup \{g_r\}$
  $\mathfrak{B}_2 := \{\{i,j\} \in B : \mathbf{T}(r) \mid \mathbf{T}(i,j), \mathbf{T}(i,r) \neq \mathbf{T}(i,j) \neq \mathbf{T}(j,r)\}$
  $B := (B \setminus \mathfrak{B}_2) \cup \mathfrak{B}_3(G)$
While $B \neq \emptyset$ **do**
  Choose $\{i,j\} \in B$, $B := B \setminus \{\{i,j\}\}$, $h := S(i,j)$
  $(h, \sum_{i=1}^{\mu} c_i t_i g_i) := \mathbf{NormalForm}(h, G)$
  If $h \neq 0$ **then**
    $s := s+1, g_s := h, G := G \cup \{g_s\}$
    $\mathfrak{B}_2 := \{\{i,j\} \in B : \mathbf{T}(s) \mid \mathbf{T}(i,j), \mathbf{T}(i,s) \neq \mathbf{T}(i,j) \neq \mathbf{T}(j,s)\}$
    $B := (B \setminus \mathfrak{B}_2) \cup \mathfrak{B}_3(G)$

Fig. 5 Buchberger's algorithm (sketch)

Figure 5 is a poor sketch of the standard implementation, whose description can be found in Giovini et al. (1991) and which is mainly based on Traverso's analysis (Traverso and Donato 1989); the reader is suggested to consider the recently proposed new implementation (Brickenstein 2005) of Buchberger's algorithm, Faugère's algorithms F_4 (Faugére 1999) and F_5 (Faugère 2002) which compute Gröbner basis by a strongly improved version of Macaulay's algorithms (Macaulay 1913, 1916) and Gerdt–Blinkov (Zarkov 1996; Gerdt and Blinkov 1998a, 1998b) algorithm which computes Gröbner basis via an adaptation of Janet's notion of *complete bases* and his corresponding algorithm to compute them (Janet 1920).

Since often a lex Gröbner basis computation is either infeasible or time-consuming, it is efficient to deduce the required lex Gröbner basis from the feasible degrevlex one via elementary linear algera (see Mora 2009).

Acknowledgements For their comments and suggestions, the author thanks all the authors of this book and especially M. Sala.

References

D. Bayer and M. Stillman, *A theorem on refining division orders by the reverse lexicographic order*, Duke Math. J. **55** (1987), nos. 2, 321–328.

M. Brickenstein, *Gröbner bases with slim polynomials*, Reports in Comp. Alg. 35, Univ. Kaiserslautern, Kaiserslautern, 2005, http://www.mathematik.uni-kl.de/.

B. Buchberger, *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal*, Ph.D. thesis, Innsbruck, 1965.

B. Buchberger, *Ein algorithmisches Kriterium für die Lösbarkeit eines algebraischen Gleichungssystems*, Aequationes Math. **4** (1970), 374–383.

B. Buchberger, *A criterion for detecting unnecessary reductions in the construction of Gröbner-bases*, Symbolic and algebraic computation (EUROSAM 1979), LNCS, vol. **72**, Springer, Berlin, 1979, pp. 3–21.

B. Buchberger, *An algorithmical criterion for the solvability of algebraic systems of equations*, London Math. Soc. LNS **251** (1998), 535–545.

B. Buchberger, *Bruno Buchberger's PhD thesis 1965: An algorithm for finding the basis elements of the residue class ring of a zero dimensional polynomial ideal*, J. Symb. Comput. **41** (2006), nos. 3–4, 475–511.

E. Byrne and T. Mora, *Gröbner bases over commutative rings and applications to coding theory*, this volume, 2009, pp. 239–261.

M. Caboara and M. Silvestri, *Classification of compatible module orderings*, J. Pure Appl. Algebra **142** (1999), nos. 1, 13–24.

G. Carrà Ferro and W. Y. Sit, *On term-orderings and rankings*, Computational algebra (Fairfax, VA, 1993), Lecture Notes in Pure and Appl. Math., vol. **151**, Dekker, New York, 1994, pp. 31–77.

J. Erdös, *On the structure of ordered real vector spaces*, Publ. Math. Debrecen **4** (1956), 334–343.

J. C. Faugére, *A new efficient algorithm for computing Gröbner bases* (F_4), J. Pure Appl. Algebra **139** (1999), nos. 1–3, 61–88.

J. C. Faugère, *A new efficient algorithm for computing Gröbner bases without reduction to zero* (F_5), Proc. of ISSAC 2002, ACM, New York, 2002, pp. 75–83.

A. Galligo, *À propos du théorème de-préparation de Weierstrass*, Fonctions de plusieurs variables complexes, Springer, Berlin, 1974, pp. 543–579. LNM. 409.

R. Gebauer and H. M. Möller, *A fast variant of Buchberger's algorithm*, preprint, 1985.

R. Gebauer and H. M. Möller, *On an installation of Buchberger's algorithm*, J. Symb. Comput. **6** (1988), nos. 2–3, 275–286.

V. P. Gerdt and Y. A. Blinkov, *Involutive bases of polynomial ideals*, Math. Comput. Simulation **45** (1998a), nos. 5–6, 519–541.

V. P. Gerdt and Y. A. Blinkov, *Minimal involutive bases*, Math. Comput. Simulation **45** (1998b), nos. 5–6, 543–560.

A. Giovini, T. Mora, G. Niesi, L. Robbiano and C. Traverso, *"One Sugar cube, please" or selection strategies in the Buchberger algorithm*, Proceedings of ISSAC 1991, ACM, New York, 1991, pp. 49–54.

P. Gordan, *Les invariants des formes binaries*, Journal de Mathématiques Pure et Appliés **6** (1900), 141–156.

M. Janet, *Sur les systèmes d'équations aux dérivées partielles*, Journal de Mathématiques Pure et Appliés **3** (1920), 65–151.

F. S. Macaulay, *On the resolution of a given modular system into primary systems including some properties of Hilbert numbers*, Math. Ann. **74** (1913), no. 1, 66–121.

F. S. Macaulay, *The Algebraic Theory of Modular Systems*, Cambridge University Press, Cambridge, 1916.

H. M. Möller, *On the construction of Gröbner bases using syzygies*, J. Symb. Comput. **6** (1988), nos. 2–3, 345–359.

T. Mora, *The FGLM problem and Moeller's algorithm on zero-dimensional ideals*, this volume, 2009, pp. 1–100.

C. Traverso and L. Donato, *Experimenting the Gröbner basis algorithm with AlPI system*, Proc. of ISSAC 1989, ACM, New York 1989, pp. 192–198.

A. Y. Zarkov, *Solving zero-dimensional involutive systems*, Proc. of MEGA 1994, Birkhäuser, Basel, 1996, pp. 389–399.

http://www.springer.com/978-3-540-93806-4

Gröbner Bases, Coding, and Cryptography
Sala, M.; Mora, T.; Perret, L.; Sakata, S.; Traverso, C. (Eds.)
2009, XVI, 430 p.,
ISBN: 978-3-540-93806-4