PART SIX

Algebraic Solving

And I beheld when he opened the sixth seal, and, lo, there was a great earthquake; and the sun become black as sackcloth of hair, and the moon became as blood;

And the stars of heaven fell unto the earth, even as a fig tree casteth her untimely figs, when she is shaken of a mighty wind.

Revelation (Authorized Version)

The things depending from Sun: spirituality, gold, carbuncle, heliotrope, lion, phoenix, seal.

E.C. Agrippa, *De Occulta Phylosophia*

So, according to the wil and meaning of *Fra.* C. R. C., we his brethren request again all the learned in Europe who shall read (sent forth in five languages) this our *Fama* and *Confessio*, that it would please them with good deliberation to ponder this our offer, and to examine most nearly and sharply their arts, and behold the present time with all diligence, and to declare their minde, either *communicato consilio*, or *singulatim* by print.

And although at this time we make no mention either of our names or meetings, yet nevertheless every one's opinion shall assuredly come to our hands, in what language so ever it be, nor any body shal fail, whoso gives but his name, to speak with some of us, either by word of mouth, or else, if there be some lett, in writing. And this we say for a truth, that whosoever shal earnestly, and from his heart, bear affection unto us, it shal be beneficial to him in goods, body, and soul; but he that is false-hearted, or onely greedy of riches, the same first of all shal not be able in any manner of wise to hurt us, but bring himself to utter ruine and destruction. Also our building, although one hundred thousand people had very near seen and beheld the same, shal for ever remain untouched, undestroyed, and hidden to the wicked world.

Sub umbra alarum tuarum, Jehova.

Fama Fraternitatis

39

Trinks

The first paper applying Buchberger's Algorithm being Trinks' proposal of an algorithm for solving polynomial equation systems, Trinks' Algorithm is the natural choice for opening this section on algebraic solving.

Trinks' Algorithm is essentially an effective reformulation of Gröbner's proof of Hilbert's Nullstellensatz (Section 20.3): given a zero-dimensional ideal $\mathsf{J} \subset \mathcal{Q} := K[Z_1, \ldots, Z_r]$, then Trinks' Algorithm, for each root $\alpha \in \mathsf{K}^{i-1}$ of $\mathsf{J} \cap K[Z_1, \ldots, Z_{i-1}]$, computes iteratively and solves $\gcd(h(\alpha, Z_i) : h \in G_i) \in \mathsf{K}[Z_i]$ where G_i denotes a basis of the ideal $\mathsf{J} \cap K[Z_1, \ldots, Z_i]$; the rôle of Gröbner bases consists in allowing the computation of such a basis of the elimination ideals.

The main improvement to Trinks' Algorithm, apart from the use of FGLM (see Sections 29.1 and 29.2) in order to efficiently deduce the needed lex Gröbner basis of J, is the Gianni–Kalkbrener proposal to use their Theorem 34.6.3; the evaluation at α of all polynomials in G_i and the computation of their gcd is thus reduced to the evaluation at α of the leading polynomials of some elements in G_i and of the first element whose leading polynomial does not vanish at α.

After recalling in Section 39.1 the basic tools provided by Gröbner bases w.r.t. solving, I present Trinks' Algorithm, in Section 39.2, and the Gianni–Kalkbrener Algorithm, in Section 39.3, and conclude with some comments which aim to read these algorithms in the setting of Kronecker–Duval Philosophy (Section 39.4). Finally, in Section 39.5, I discuss a solver from 1913 which already explicitly applies the main property of the lex term ordering and anticipates Macaulay's Lemma.

39.1 Recalling Gröbner

Let us consider

- an infinite, perfect field k,[1] where, if $p := \mathrm{char}(k) \neq 0$, it is possible to extract pth roots,
- the algebraic closure k of k,

[1] While the techniques discussed here apply in this general setting, we are mainly thinking of the case $k = \mathbb{Q}$, $\mathsf{k} := \mathbb{C}$; nevertheless, technically we need to (and we can) solve over $\mathbb{Q}(V_1, \ldots, V_d)$.

- the universal field $\Omega(k)$ over k (Definition 9.4.1),
- the polynomial ring $\mathcal{P} := k[X_1, \ldots, X_n]$,
- its k-basis $\mathcal{T} := \{X_1^{a_1} \cdots X_n^{a_n} : (a_1, \ldots, a_n) \in \mathbb{N}^n\}$,
- an ideal $\mathsf{I} := (F) := \mathbb{I}(F) := \left\{\sum_{i=1}^{u} h_i f_i : h_i \in \mathcal{P}\right\} \subset \mathcal{P}$ given by[2]
- a finite basis $F := \{f_1, \ldots, f_u\} \subset \mathcal{P}$,
- the algebraic affine variety $\mathcal{Z}(\mathsf{I}) := \{\mathsf{a} \in \mathsf{k}^n : f(\mathsf{a}) = 0, \text{ for each } f \in F\} \subset \mathsf{k}^n$.

Each polynomial $f \in k[X_1, \ldots, X_n]$ is therefore a unique linear combination

$$f = \sum_{t \in \mathcal{T}} c(f, t)t$$

of the terms $t \in \mathcal{T}$ with coefficients $c(f, t)$ in k; the support

$$\operatorname{supp}(f) := \{t \in \mathcal{T} : c(f, t) \neq 0\}$$

of f being finite, once a term ordering $<$ on $\mathcal{T}$ is fixed,[3] f has a unique representation as an ordered linear combination of terms:

$$f = \sum_{i=1}^{s} c(f, t_i)t_i : c(f, t_i) \in k \setminus \{0\}, \quad t_i \in \mathcal{T}, \quad t_1 > \cdots > t_s;$$

the *maximal term* of f is $\mathbf{T}(f) := t_1$, its *leading cofficient* is $\operatorname{lc}(f) := c(f, t_1)$ and its *maximal monomial* is $\mathbf{M}(f) := c(f, t_1)t_1$.

For any set $F \subset \mathcal{P}$ we denote

- $\mathbf{T}_<\{F\} := \{\mathbf{T}(f) : f \in F\}$,
- $\mathbf{T}_<(F) := \{\tau\mathbf{T}(f) : \tau \in \mathcal{T}, f \in F\}$,
- $\mathbf{N}_<(F) := \mathcal{T} \setminus \mathbf{T}_<(F)$,
- $k[\mathbf{N}_<(F)] := \operatorname{Span}_k(\mathbf{N}_<(F))$;

we will usually omit the dependence on $<$ if there is no ambiguity. Recall that

Definition 39.1.1 (Buchberger). *A subset $G \subset \mathsf{I}$ will be called a* Gröbner basis *of I w.r.t. $<$ (Definition 22.2.1) if $\mathbf{T}(G) = \mathbf{T}\{\mathsf{I}\}$, that is, $\mathbf{T}\{G\}$ generates the monomial ideal $\mathbf{T}(\mathsf{I}) = \mathbf{T}\{\mathsf{I}\}$.*

For each $f \in \mathcal{P}$ the canonical form *of f w.r.t. I (Definition 22.2.13) is the unique polynomial*

$$g := \operatorname{Can}(f, \mathsf{I}, <) = \sum_{t \in \mathbf{N}(\mathsf{I})} \gamma(f, t, <)t \in k[\mathbf{N}(\mathsf{I})]$$

such that $f - g \in \mathsf{I}$. ⊙

Let us fix any term ordering $<$ on $\mathcal{T}$ and compute a Gröbner basis $G \subset \mathsf{I}$ of I w.r.t. $<$.

[2] Throughout the book I will use the notation $\mathbb{I}(F) \subset \mathcal{R}$ to denote the ideal generated by the basis F in the ring $\mathcal{R}$; when there is no ambiguity $\mathcal{R}$ will be not specified.

[3] Recall that (cf. Definition 22.1.2) a well-ordering $<$ on $\mathcal{T}$ that is also a semigroup ordering, that is, if

$$t_1 < t_2 \implies tt_1 < tt_2 \quad \text{for each } t, t_1, t_2 \in \mathcal{T}$$

is called a term ordering.

Then the following hold (cf. Remark 27.12.4):

- $\mathcal{Z}(\mathsf{I}) = \emptyset \iff 1 \in \mathsf{I} \iff 1 \in G$;
- $\mathcal{Z}(\mathsf{I})$ is infinite iff $\mathbf{N}(\mathsf{I})$ is infinite $\iff$ there exists i such that, for each $d \in \mathbb{N}$, $X_i^d \notin \mathbf{T}(G) = \mathbf{T}(\mathsf{I})$;
- $\mathcal{Z}(\mathsf{I})$ is finite iff $\mathbf{N}(\mathsf{I})$ is finite $\iff$ for each i there exists $d_i \in \mathbb{N} : X_i^{d_i} \in \mathbf{T}\{G\} \subset \mathbf{T}(\mathsf{I})$; moreover, in this case and under the assumption that I is radical, we have $\#\mathcal{Z}(\mathsf{I}) = \#\mathbf{N}(\mathsf{I})$.

The Kredel–Weispfenning Algorithm (Corollary 27.11.9) allows us to deduce from $\mathbf{T}(\mathsf{I})$ the dimension $d := \dim(\mathsf{I})$, the rank $r := n - d := r(\mathsf{I})$ of I and a maximal set of independent variables (Definition 27.11.4) $\{X_{i_1}, \ldots, X_{i_d}\}$ such that $\mathsf{I} \cap k[X_{i_1}, \ldots, X_{i_d}] = (0)$.

Then, we can re-enumerate and relabel the variables as follows:

$$\{X_1, \ldots, X_n\} = \{V_1, \ldots, V_d, Z_1, \ldots, Z_r\}, \quad \{X_{i_1}, \ldots, X_{i_d}\} = \{V_1, \ldots, V_d\},$$

so that

$$\mathsf{I} \cap k[V_1, \ldots, V_d] = (0),$$

and consider

the field $K := k(V_1, \ldots, V_d)$,
its algebraic closure K
and its universal field $\Omega(K) = \Omega(k)$,
the polynomial ring $\mathcal{Q} := K[Z_1, \ldots, Z_r]$,
its K-basis $\mathcal{W} := \{Z_1^{a_1} \cdots Z_r^{a_r} : (a_1, \ldots, a_r) \in \mathbb{N}^r\}$,
the zero-dimensional ideal $\mathsf{J} := \mathsf{I}^e := \mathsf{I}K[Z_1, \ldots, Z_r]$[4]
and the unmixed ideal $\mathsf{J}^c := \mathsf{J} \cap \mathcal{P}$.

Then, if $\mathsf{I} = \cap_{i=1}^{\mathsf{t}} \mathfrak{q}_i$ denotes any irredundant primary representation in $\mathcal{P}$ and we wlog assume that the primaries are ordered in such a way that, for a suitable value $1 \le \mathsf{r} \le \mathsf{t}$,

$$\{X_{i_1}, \ldots, X_{i_d}\} \text{ is a maximal set of independent variables for } \mathfrak{q}_i \iff i \le \mathsf{r}$$

then Corollary 27.5.19 grants that

$$\mathsf{J} := \mathsf{I}^e = \bigcap_{i=1}^{\mathsf{r}} \mathfrak{q}_i^e = \bigcap_{i=1}^{\mathsf{r}} \mathfrak{q}_i \mathcal{Q}$$

is an irredundant primary representation in $\mathcal{Q}$ and

$$\mathsf{J}^c := \mathsf{I}^{ec} = \bigcap_{i=1}^{\mathsf{r}} \mathfrak{q}_i \subset \mathcal{P}$$

is an irredundant primary representation.

[4] For this notation see Section 27.5.

Moreover, the Gianna–Trager–Zacharias (GTZ), Alonso, Raimondo, Giusti and Heintz (ARGH) and Caborah, Conti and Traverso (CCT) schemes (Chapter 35) allow us to compute unmixed ideals $\mathfrak{a}_j \subset \mathcal{P}$, giving a decomposition

$$\sqrt{\mathsf{I}} = \sqrt{\mathsf{J}^c} \bigcap \left(\bigcap_j \sqrt{\mathfrak{a}_j} \right).$$

Thus solving the ideal $\mathsf{I} \subset \mathcal{P}$ is reduced, via the Gröbner technique, to solving each unmixed GTZ, ARGH or CCT component and, in turn, solving each such component is reduced to solving the related zero-dimensional extension ideal.

39.2 Trinks' Algorithm

Thus we are reduced to consider a zero-dimensional ideal

$$\mathsf{J} \subset \mathcal{Q} := K[Z_1, \ldots, Z_r],$$

which we assume to be given via a Gröbner basis $G_\prec$ w.r.t. the lexicographical ordering $\prec$ induced on $\mathcal{W}$ by $Z_1 \prec Z_2 \prec \cdots \prec Z_r$:

$$Z_1^{a_1} \cdots Z_r^{a_r} \prec Z_1^{b_1} \cdots Z_r^{b_r} \iff \text{there exist } j : a_j < b_j \text{ and } a_i = b_i \text{ for } i > j.$$

Then, if we denote, for i, $1 \leq i < r$,

$\mathsf{J}_i := \mathsf{J} \cap K[Z_1, \ldots, Z_i]$,
$\pi_i : \mathsf{K}^r \to \mathsf{K}^i$ as the canonical projection $\pi_i(a_1, \ldots, a_r) = (a_1, \ldots, a_i)$,
$G_i := G_\prec \cap K[Z_1, \ldots, Z_i]$,

we have, for each i,

(1) $\mathcal{Z}(\mathsf{J}_i) = \pi_i(\mathcal{Z}(\mathsf{J})) = \{(a_1, \ldots, a_i) : (a_1, \ldots, a_r) \in \mathcal{Z}(\mathsf{J})\}$,
(2) G_i is the reduced lexicographical Gröbner basis of J_i (Corollary 26.2.4).

In particular, there is a unique monic polynomial $f(Z_1) \in K[Z_1]$ such that

$$\mathsf{J}_1 = \mathbb{I}(f) \quad \text{and} \quad \{f\} = G_\prec \cap K[Z_1].$$

For each $\alpha := (a_1, \ldots, a_{i-1}) \in \mathsf{K}^{i-1}$, denote as $\Phi_\alpha : K[Z_1, \ldots, Z_i] \to \mathsf{K}[T]$ the projection defined by

$$\Phi_\alpha(f) = f(a_1, \ldots, a_{i-1}, T) \quad \text{for each } f \in K[Z_1, \ldots, Z_i].$$

Theorem 39.2.1 (Trinks). *Let $\alpha := (a_1, \ldots, a_{i-1}) \in \mathcal{Z}(\mathsf{J}_{i-1})$ and let $f \in \mathsf{K}[T]$ be a generator of the principal ideal $\Phi_\alpha(\mathsf{J}_i) \subset \mathsf{K}[T]$. Then, for each $b \in \mathsf{K}$,*

$$(a_1, \ldots, a_{i-1}, b) \in \mathcal{Z}(\mathsf{J}_i) \iff f(b) = 0.$$

Proof. Let $h(Z_1, \ldots, Z_i) \in \mathsf{J}_i$ be any polynomial such that

$$f(T) = \Phi_\alpha(h) = h(a_1, \ldots, a_{i-1}, T).$$

$\mathsf{Z} :=$ **Solve**(F, L)
where
$F := \{f_1, \ldots, f_u\} \subset \mathcal{Q} := K[Z_1, \ldots, Z_r]$,
$L \supset K$ is a field extension of K,
$\mathsf{J} \subset \mathcal{Q}$ is the zero-dimensional ideal generated by F,
$\mathsf{Z} := \{\alpha_1, \ldots, \alpha_\mathsf{s}\} = \mathcal{Z}(\mathsf{J}) \cap L^r$.
Compute the reduced lexicographical Gröbner basis G of $(f_1, \ldots, f_u)$.
Let $p(Z_1)$ be the unique element in $G \cap K[Z_1]$,
$\mathsf{Z}_1 := \{a \in L : p(a) = 0\}$.
For $i = 2, \ldots, r$ **do**
$\mathsf{Z}_i := \emptyset$.
For each $(a_1, \ldots, a_{i-1}) \in \mathsf{Z}_{i-1}$ **do**
$H := \{g(a_1, \ldots, a_{i-1}, Z_i) : g \in G_i \setminus G_{i-1}\}$,
$p := \gcd(H)$,
$\mathsf{Z} := \{a \in L : p(a) = 0\}$,
$\mathsf{Z}_i := \mathsf{Z}_i \cup \{(a_1, \ldots, a_{i-1}, a) : a \in \mathsf{Z}\}$.
$\mathsf{Z} := \mathsf{Z}_r$.

Figure 39.1. Trinks' Algorithm

Then

$$(a_1, \ldots, a_{i-1}, b) \in \mathcal{Z}(\mathsf{J}_i) \implies f(b) = h(a_1, \ldots, a_{i-1}, b) = 0.$$

Conversely, for any $b \in \mathsf{K} : f(b) = 0$ and for any $g(Z_1, \ldots, Z_i) \in \mathsf{J}_i$, it holds that $\Phi_\alpha(g) \in \Phi_\alpha(\mathsf{J}_i)$, so that

$$g(a_1, \ldots, a_{i-1}, b) = \Phi_\alpha(g)(b) = 0 \quad \text{for each } g \in \mathsf{J}_i$$

and $(a_1, \ldots, a_{i-1}, b) \in \mathcal{Z}(\mathsf{J}_i)$. ⊡

Algorithm 39.2.2 (Trinks). Trinks' Algorithm (Figure 39.1) for "solving" a zero-dimensional ideal is based on the theorem above and consists in iteratively computing $\mathcal{Z}(\mathsf{J}_i)$ by "solving", for each $\alpha \in \mathcal{Z}(\mathsf{J}_{i-1})$, the univariate polynomial generating the principal ideal $\Phi_\alpha(\mathsf{J}_i)$. ⊡

Example 39.2.3. To illustrate Trinks' Algorithm let us consider the zero-dimensional ideal $\mathsf{J} \subset \mathbb{Q}[Z_1, Z_2, Z_3]$ discussed in Example 33.2.6 whose lex Gröbner basis is $G := \{g_i, 1 \le i \le 8\}$, where (Examples 33.5.1 and 33.5.2)[5]

$$\begin{aligned}
g_1 &:= \mathbf{1}Z_1^3 - 3Z_1^2 + 2Z_1,\\
g_2 &:= (\mathbf{Z_1^2} - \mathbf{Z_1})Z_2,\\
g_3 &:= \mathbf{Z_1}Z_2^2 - Z_1Z_2,\\
g_4 &:= \mathbf{1}Z_2^3 - 3Z_2^2 + 2Z_2,\\
g_5 &:= (\mathbf{Z_1^2} - \mathbf{3Z_1} + \mathbf{2})Z_3 - 3Z_2^2 - 6Z_2Z_1 + 9Z_2 - Z_1^2 + 3Z_1 - 2,\\
g_6 &:= (\mathbf{Z_2} + \mathbf{Z_1} - \mathbf{2})Z_3 + 3Z_2^2 + Z_2Z_1 - 7Z_2 - 2Z_1^2 + 3Z_1 + 2,
\end{aligned}$$

[5] The *leading polynomial* (see below) $\mathrm{Lp}(g_i)$ is indicated in **bold**.

$$g_7 := (\mathbf{Z_1} - \mathbf{2})Z_3^2 - 4Z_3Z_1 + 8Z_3 - 15Z_2^2 - 30Z_2Z_1 + 45Z_2 + 3Z_1 - 6,$$
$$g_8 := \mathbf{1}Z_3^3 - 3Z_3^2 + 3Z_3Z_1 - 4Z_3 - 3Z_2^2 - 6Z_2Z_1 + 9Z_2 - 3Z_1 + 6,$$

and whose roots are $\mathcal{Z}(\mathsf{J}) = \{\mathsf{b}_j, 1 \le j \le 9\}$, with

$$\begin{array}{lllllllll} \mathsf{b}_1 & = & (0,0,1). & \mathsf{b}_2 & = & (0,1,-2), & \mathsf{b}_3 & = & (2,0,2), \\ \mathsf{b}_4 & = & (0,2,-2), & \mathsf{b}_5 & = & (1,0,3), & \mathsf{b}_6 & = & (1,1,3), \\ \mathsf{b}_7 & = & (1,1,1), & \mathsf{b}_8 & = & (2,0,1), & \mathsf{b}_9 & = & (2,0,0). \end{array}$$

Then we have:

$$\begin{array}{ll} p(Z_1) := & g_1, \quad \mathsf{Z}_1 := \{0,1,2\}; \\ \alpha = (0): & \Phi_\alpha(g_2) = \Phi_\alpha(g_3) = 0; \quad \Phi_\alpha(g_4) = T^3 - 3T^2 + 2T; \\ & \mathsf{Z} := \{0,1,2\}, \quad \mathsf{Z}_2 := \{(0,0),(0,1),(0,2)\}; \\ \alpha = (1): & \Phi_\alpha(g_2) = 0; \quad \Phi_\alpha(g_3) = T^2 - T; \quad \Phi_\alpha(g_4) = T^3 - 3T^2 + 2T; \\ & \gcd(\Phi_\alpha(g_3), \Phi_\alpha(g_4)) = T^2 - T; \\ & \mathsf{Z} := \{0,1\}, \quad \mathsf{Z}_2 := \{(0,0),(0,1),(0,2),(1,0),(1,1)\}; \\ \alpha = (2): & \Phi_\alpha(g_2) = 2T; \quad \Phi_\alpha(g_3) = 2T^2 - 2T; \quad \Phi_\alpha(g_4) = T^3 - 3T^2 + 2T; \\ & \gcd(\Phi_\alpha(g_i), 2 \le i \le 4) = T; \\ & \mathsf{Z} := \{0\}, \quad \mathsf{Z}_2 := \{(0,0),(0,1),(0,2),(1,0),(1,1),(2,0)\}; \\ \alpha = (0,0): & \Phi_\alpha(g_5) = 2T - 2; \quad \Phi_\alpha(g_6) = -2T + 2; \\ & \Phi_\alpha(g_7) = -2T^2 + 8T - 6; \quad \Phi_\alpha(g_8) = T^3 - 3T^2 - 4T + 6; \\ & \gcd(\Phi_\alpha(g_i), 5 \le i \le 8) = T - 1; \\ & \mathsf{Z} := \{1\}, \quad \mathsf{Z}_2 := \{(0,0,1)\}; \\ \alpha = (0,1): & \Phi_\alpha(g_5) = 2T + 4; \quad \Phi_\alpha(g_6) = -T - 2; \\ & \Phi_\alpha(g_7) = -2T^2 + 8T + 24; \quad \Phi_\alpha(g_8) = T^3 - 3T^2 - 4T + 12; \\ & \gcd(\Phi_\alpha(g_i), 5 \le i \le 8) = T + 2; \\ & \mathsf{Z} := \{-2\}, \quad \mathsf{Z}_2 := \mathsf{Z}_2 \cup \{(0,1,-2)\}; \\ \alpha = (0,2): & \Phi_\alpha(g_5) = 2T + 4; \quad \Phi_\alpha(g_6) = 0; \\ & \Phi_\alpha(g_7) = -2T^2 + 8T + 24; \quad \Phi_\alpha(g_8) = T^3 - 3T^2 - 4T + 12; \\ & \gcd(\Phi_\alpha(g_i), 5 \le i \le 8) = T + 2; \\ & \mathsf{Z} := \{-2\}, \quad \mathsf{Z}_2 := \mathsf{Z}_2 \cup \{(0,2,-2)\}; \\ \alpha = (1,0): & \Phi_\alpha(g_5) = 0; \quad \Phi_\alpha(g_6) = -T + 3; \\ & \Phi_\alpha(g_7) = -T^2 + 4T - 3; \quad \Phi_\alpha(g_8) = T^3 - 3T^2 - T + 3; \\ & \gcd(\Phi_\alpha(g_i), 6 \le i \le 8) = T - 3; \\ & \mathsf{Z} := \{3\}, \quad \mathsf{Z}_2 := \mathsf{Z}_2 \cup \{(1,0,3)\}; \\ \alpha = (1,1): & \Phi_\alpha(g_5) = 0; \quad \Phi_\alpha(g_6) = 0; \\ & \Phi_\alpha(g_7) = -T^2 + 4T - 3; \quad \Phi_\alpha(g_8) = T^3 - 3T^2 - T + 3; \\ & \gcd(\Phi_\alpha(g_i), 7 \le i \le 8) = T^2 - 4T + 3; \\ & \mathsf{Z} := \{1,3\}, \quad \mathsf{Z}_2 := \mathsf{Z}_2 \cup \{(1,1,3),(1,1,1)\}; \\ \alpha = (2,0): & \Phi_\alpha(g_5) = \Phi_\alpha(g_6) = \Phi_\alpha(g_7) = 0; \quad \Phi_\alpha(g_8) = T^3 - 3T^2 + 2T; \\ & \gcd(\Phi_\alpha(g_i), 7 \le i \le 8) = T^3 - 3T^2 + 2T; \\ & \mathsf{Z} := \{0,1,2\}, \quad \mathsf{Z}_2 := \mathsf{Z}_2 \cup \{(2,0,0),(2,0,1),(2,0,2)\}. \end{array}$$

39.3 Gianni–Kalkbrener Algorithm

Apart from the FGLM proposal of indirectly producing the needed lexicographical Gröbner basis via linear algebra from the Gröbner bases w.r.t. an easier-to-compute term ordering, the most relevant improvement on Trinks' Algorithm is based on a deeper analysis performed by Gianni and Kalkbrener on the structure of the lexicographical Gröbner basis of a zero-dimensional ideal.

Remarking that each polynomial $f \in K[Z_1, \ldots, Z_i]$ can be uniquely expressed as

$$f = \sum_{j=0}^{D} h_j(Z_1, \ldots, Z_{i-1}) Z_i^j, \quad h_D \neq 0,$$

we recall that the degree of f in the variable Z_i is denoted

$$\deg_{Z_i}(f) := \deg_i(f) := D$$

and that $\mathrm{Lp}(f) := h_d$ is named the *leading polynomial* of f; we observe that, for the lexicographical ordering $\prec$, we have $\mathbf{T}(f) = \mathbf{T}(\mathrm{Lp}(f)) Z_i^{\deg_i(f)}$.

We also denote, for each i, $1 \leq i \leq r$, $\delta \in \mathbb{N}$,

$$G_{i\delta} := \{g \in G, g \in K[Z_1, \ldots, Z_i], \deg_i(g) \leq \delta\}$$

and remark that each $G_{i\delta}$ is a section of both $G_{i\delta+1}$ and G_i and that the obvious inclusions hold:

$$G_{11} \subseteq G_{12} \subseteq \cdots \subseteq G_1 \subseteq \cdots \subseteq G_{i-1} \subseteq \cdots \subseteq G_{i\delta} \subseteq G_{i\delta+1} \subseteq \cdots \subseteq G_i \subseteq \cdots .$$

For each i, $1 \leq i \leq r$, $\delta \in \mathbb{N}$, and each $F \subset \mathcal{Q}$, we also write

$$\mathrm{Lp}_{i\delta}(F) := \{\mathrm{Lp}(g), g \in F \cap K[Z_1, \ldots, Z_i], \deg_i(g) \leq \delta\}.$$

Theorem 39.3.1 (Gianni–Kalkbrener). *Let $\mathsf{J} \subset \mathcal{Q}$ be an ideal and $\prec$ be the lexicographical ordering induced by $Z_1 \prec \cdots \prec Z_r$.*

Let $G := \{g_1, \ldots, g_v\}$ be a Gröbner basis of J w.r.t. $\prec$, enumerated in such a way that

$$\mathbf{T}(g_1) \prec \mathbf{T}(g_2) \prec \cdots \prec \mathbf{T}(g_{v-1}) \prec \mathbf{T}(g_v).$$

Then, with the notation above:

- *for each i, $i \leq r$, G_i is a Gröbner basis of J_i;*
- *for each i, $1 \leq i \leq r$, $\delta \in \mathbb{N}$, $\mathrm{Lp}_{i\delta}(G)$ is a Gröbner basis of $\mathrm{Lp}_{i\delta}(\mathsf{J})$;*
- *for each i, $1 \leq i \leq r$, and each $\alpha := (b_1, \ldots, b_{i-1}) \in \mathcal{Z}(\mathsf{J}_{i-1})$, denoting as*
  σ the minimal value such that $\Phi_\alpha(\mathrm{Lp}(g_\sigma)) \neq 0$ and
  j, δ the values such that

$$g_\sigma = \mathrm{Lp}(g_\sigma) Z_j^{\delta+1} + \cdots \in K[Z_1, \ldots, Z_j] \setminus K[Z_1, \ldots, Z_{j-1}],$$

it holds that

(a) $j = i$,

(b) *for each* $g \in G_{i-1}$, $\Phi_\alpha(g) = 0$,

(c) *for each* $g \in G_{i\delta}$, $\Phi_\alpha(g) = 0$,

(d) $\Phi_\alpha(g_\sigma) = \gcd(\Phi_\alpha(g) : g \in G_i) \in \mathsf{K}[T]$,

(e) for each $b \in \mathsf{K}$,

$$(b_1, \ldots, b_{i-1}, b) \in \mathcal{Z}(\mathsf{J}_i) \iff \Phi_\alpha(g_\sigma)(b) = 0.$$

Proof. See Sections 26.2 and 34.6. ⊙

Algorithm 39.3.2 (Gianni–Kalkbrener). The Gianni–Kalkbrener improvement to Trinks' Algorithm allows us to avoid, for each $\alpha := (a_1, \ldots, a_{i-1}) \in \mathsf{Z}_{i-1}$, both a complete evaluation $\Phi_\alpha(g)$ of all $g \in G_i \setminus G_{i-1}$ and also the computation of their gcd, reducing this step to the evaluation of the leading polynomials of a suitable subset of such elements (Figure 39.2). ⊙

Example 39.3.3. In Example 39.2.3, the Gianni–Kalkbrener Algorithm computes

$$\begin{aligned} & \mathsf{Z}_1 := \{0, 1, 2\}; \\ \alpha = (0) : \quad & \Phi_\alpha(\mathrm{Lp}(g_2)) = \Phi_\alpha(\mathrm{Lp}(g_3)) = 0; \quad \Phi_\alpha(\mathrm{Lp}(g_4)) = 1; \\ & \Phi_\alpha(g_4) = T^3 - 3T^2 + 2T; \\ & \mathsf{Z} := \{0, 1, 2\}, \quad \mathsf{Z}_2 := \{(0, 0), (0, 1), (0, 2)\}; \end{aligned}$$

$\mathsf{Z} :=$ **Solve**(F, L),
where
$F := \{f_1, \ldots, f_u\} \subset \mathcal{Q} := K[Z_1, \ldots, Z_r]$,
$L \supset K$ is a field extension of K,
$\mathsf{J} \subset \mathcal{Q}$ is the zero-dimensional ideal generated by F,
$\mathsf{Z} := \{\alpha_1, \ldots, \alpha_\mathsf{s}\} = \mathcal{Z}(\mathsf{J}) \cap L^r$.
Compute the reduced lexicographical Gröbner basis G of $(f_1, \ldots, f_u)$.
Sort $G := \{g_1, \ldots, g_v\}$ by increasing maximal terms.
$\mathsf{Z}_1 := \{a \in L : g_1(a) = 0\}$,
%% g_1 is the unique element in $G \cap K[Z_1]$.
For $i = 2, \ldots, r$ **do**
  $\mathsf{Z}_i := \emptyset$;
  $g := \min(g \in G_i \setminus G_{i-1})$.
  For each $(a_1, \ldots, a_{i-1}) \in \mathsf{Z}_{i-1}$ **do**
    $h := g$.
    While $\mathrm{Lp}(h)(a_1, \ldots, a_{i-1}) = 0$ **do** $h :=$ **Next**(h, G),
    $p := h(a_1, \ldots, a_{i-1}, Z_i)$,
    %% $h(a_1, \ldots, a_{i-1}, Z_i) \neq 0$,
    %% $p = \gcd(H)$ for $H := \{g(a_1, \ldots, a_{i-1}, Z_i) : g \in G_i \setminus G_{i-1}\}$,
    $\mathsf{Z} := \{a \in L : p(a) = 0\}$,
    $\mathsf{Z}_i := \mathsf{Z}_i \cup \{(a_1, \ldots, a_{i-1}, a) : a \in \mathsf{Z}\}$.
$\mathsf{Z} := \mathsf{Z}_r$.

Figure 39.2. Trinks' Algorithm, Gianni–Kalkbrener Improvement