J. Symbolic Computation (1999) **11**, 1–000

Basic Algorithms for Specialization in Gröbner Bases

A. MONTES †

† *Dep. Matemàtica Aplicada 2., Universitat Politècnica de Catalunya, E.*

(Received 28 January 1999)

Weispfenning (1992) proves the existence of comprehensive Gröbner bases that specialize for any values of the parameters, and provides an algorithm to compute one of them. But when using this algorithm for the discussion of polynomial systems, a large set of cases is often obtained, many of them representing repeated and/or inconsistent cases.

The aim of our work is to obtain a new algorithm for dealing with Gröbner bases with parameters which outputs only the properly different reduced Gröbner bases, or in any case a reduced set of cases.

In this paper, the basic algorithms used in the new approach are given. The complete algorithm is studied in a forthcoming paper.

1. Introduction.

Let $F = \{f_1, \dots, f_s\} \subseteq R[x_1, \dots, x_n; a_1, \dots, a_m] = R[\overline{x}, \overline{a}]$ be a set of polynomials in the variables $\overline{x}$ and the parameters $\overline{a}$, where R is a unique factorization domain (UFD) with unity. We can consider F as a polynomial set in the variables $\overline{x}$ with coefficients in $R[\overline{a}]$.

In many applications it is required to determine the reduced Gröbner basis of the ideal $\langle F \rangle$ when the parameters $\overline{a}$ are substituted in some extension field K of R, for different concrete values $\overline{a}_0 \in K^m$. For example, in order to determine the conditions for a family of curves to have a singular point, to determine conditions on the magnitudes of a robot configuration with certain degrees of freedom, to obtain a formula to solve the load-flow problem for a given network and any injected power (Montes, 1995; Montes, 1998) in automatic theorem proving, and so on.

This problem has been studied and solved by Weispfenning (1992) who introduced the concept of comprehensive Gröbner basis $\mathrm{CGB}(\langle F \rangle)$, and gave an algorithm to compute one. A $\mathrm{CGB}(\langle F \rangle)$ is a Gröbner basis for F embedded in $R(\overline{a})[\overline{x}]$, that continues to be a Gröbner basis in $K[\overline{x}]$ for every substitution of the parameters $\overline{a} \to \overline{a}_0 \in K^m$, in F. The algorithm also determines sets of conditions on the parameters and the corresponding Gröbner bases. Its goal is a CGB, and the output is not easy to be analyzed for discussing systems in applications, as it consists of a large set of cases many of them not compatible or non disjoint. This algorithm has been implemented by V. Weispfenning and M. Pesch.

I am grateful to V. Weispfenning for his remark about the convenience of using his

† Partially supported by Proyecto DGES-MEC PB96-0005-C02-02

0747–7171/90/000000 + 00 $03.00/0

algorithm and software for the load-flow problem (Montes, 1995). His comments induced me to work on the improvement of the algorithm.

For this purpose, instead of focusing our interest on the CGB –it is not the important object in applications– we are concerned with obtaining the essential different reduced Gröbner basis, without repetition of cases.

Under this perspective, a case is a set of polynomial equalities and inequalities over the parameters $\overline{a}$. It would be desirable to distinguish cases only when its corresponding reduced Gröbner bases have different leading monomials sets in the variables $\overline{x}$. This is perhaps an excessive requirement, but we have this target in mind.

The problem of specialization of Gröbner bases has been actually studied by many authors. The general basic problem can be formulated in the following way. Let R, R' be Noetherian commutative rings with identity, and $\sigma : R \to R'$ be a ring homomorphism. When does a Gröbner basis of an ideal $I \subseteq R[\overline{x}]$ map to a Gröbner basis of $\langle \sigma(I) \rangle$ under the natural extension $\sigma : R[\overline{x}] \to R'[\overline{x}]$. Given a monomial order $\succ$, obviously it suffices to have

$$\langle \sigma(\mathrm{lm}(I)) \rangle = \langle \mathrm{lm}(\sigma(I)) \rangle \tag{1.1}$$

In (Kalkbrener, 1997) are reviewed conditions obtained by different authors for this question (Gianni, 1987; Bayer, Galligo, Stillman, 1991; Pauer, 1992; Gräbe, 1993; Assi, 1994). Kalkbrener (1997) also proves a necessary and sufficient condition for 1.1 when R' is a field. Let $\{g_1, \ldots, g_s\}$ be a Gröbner basis of $I \subseteq R[\overline{x}]$ with respect to a monomial order $\succ$, and assume that the $g_i's$ are ordered in such a way that $\mathrm{lc}(g_1), \ldots \mathrm{lc}(g_r) \notin \ker(\sigma)$. Then (1.1) holds for $I, \succ$ iff the the polynomials $\sigma(g_{r+1}), \ldots, \sigma(g_s)$ can be reduced to 0 modulo $\{\sigma(g_1), \ldots, \sigma(g_r)\}$. In formula

$$\sigma(g_i) \longrightarrow_{\{\sigma(g_1),\ldots,\sigma(g_r)\}} 0 \quad \text{for} \quad r < i \leq s \tag{1.2}$$

The practical interesting case in which we are interested occurs when we take as original ring a polynomial ring $R[\overline{a}]$ over a domain R with unity and for R' some extension field K of R. The variables $\overline{a}$ are considered as parameters. We restrict ourselves to this case. In this case $R[\overline{a}]$ can be embedded in the quotient field $R(\overline{a})$ and we do not need the general algorithm for computing Gröbner basis over rings given in (Möller, 1988), but only the classical Buchberger algorithm over fields. When doing so, we cannot use the sufficient condition obtained from (1.2) for $r = s$, as we can extend σ to act on the local ring $R[\overline{a}]_{\ker(\sigma)}$ but not on $R(\overline{a})$. Acting so we must compute Gröbner basis in the local ring and we want to avoid it.

In this paper, the basic tools for improving Weispfenning algorithm in the restricted case, working in $R(\overline{a})[\overline{x}]$, are given. The complete algorithm is given in a forthcoming paper.

First of all, we prove that the ordinary division algorithm specializes when all the leading coefficients of the divisors do not become zero, and we give a specific NORMALFORM algorithm that outputs polynomials without denominators on the parameters. We then construct Gröbner basis of $\langle F \rangle$ in $R(\overline{a})[\overline{x}]$ for which we are able to give a sufficient condition on the parameters that ensures automatic specialization. The algorithm PGB0 outputs such a Gröbner basis from which we immediately obtain the sufficient condition in the form of a variety W, that we call the *singular variety*, outside of which the Gröbner basis specializes. This singular variety consists of the union of irreducible varieties defined by one polynomial. We minimize and reduce it and obtain the reduced Gröbner basis that specializes outside W. But the singular variety W obtained is not determined by the input ideal and depends on the path followed by PGB0 algorithm. In order to minimize the singular variety where specialization does not hold, we introduce a new generalized Gaussian elimination algorithm GGE that transforms a given basis of an ideal into a particular triangular form with the minimum number of leading coefficients containing parameters. We apply GGE algorithm before PGB0 to minimize the singular variety. We include all these steps in the algorithm PGB. It outputs a reduced singular variety W and the unique reduced Gröbner basis in $R(\overline{a})[\overline{x}]$ that surely specializes outside W. Finally we provide some illustrative examples.

We use the following notations. A power product in the variables $\overline{x}$ is denoted x^α. A monomial is a product of a coefficient in the coefficient ring or field and a power product of the variables. Given a monomial order $\succ$ the leading monomial, coefficient and power product are denoted:

$$\mathrm{lm}_{\overline{x}}(f) = c\, x^\alpha, \quad \mathrm{lc}_{\overline{x}}(f) = c, \quad \mathrm{lpp}_{\overline{x}}(f) = x^\alpha.$$

The subindex $_{\overline{x}}$ will be omitted when it clearly refers to the set of variables $\overline{x}$, as this is the most usual case in this paper.

2. Specialization and Buchberger algorithm

We restrict ourselves to specializations coming from replacement of parameters. The corresponding ring homomorphism is:

$$\sigma : R[\overline{a}] \longrightarrow K \tag{2.1}$$

where K is any field extension of R (a UFD) and $\sigma|R = Id$. To provide a specialization is equivalent to choose $\overline{a}_0 \in K^m$, and setting $\sigma(\overline{a}) = \overline{a}_0$. We will denote also by σ the natural extension $\sigma' : R[\overline{a}][\overline{x}] \longrightarrow K[\overline{x}]$ which is the identity on $\overline{x}$.

Sometimes (see section 3) we extend σ for certain elements of $R(\overline{a})$ (more precisely to the local ring $R[\overline{a}]_{\ker(\sigma)}$). When we say that $\sigma(f)$ makes sense for $f \in R(\overline{a})[\overline{x}]$ it has to be understood that $f \in R[\overline{a}]_{\ker(\sigma)}[\overline{x}]$.

Let us denote $F_0 = \sigma(F) \subset K[\overline{x}]$ the polynomial set where the specialization is performed.

As the coefficients of F can be embedded in the fraction field $R(\overline{a})$, we can use classical Buchberger's algorithm to compute its Gröbner basis. We shall modify it in order to obtain a "well normalized" polynomial set G without denominators in $R[\overline{a}]$. Thus, the resulting G belongs to $R[\overline{a}][\overline{x}]$. We can also use the algorithm to compute a Gröbner basis of F_0, its coefficients being in the field K. As it is well known, the specialization of G, say $G_0 = \sigma(G)$, has not to be necessarily a Gröbner basis of $\langle F_0 \rangle$.

Weispfenning's C.G.B. commutes with specialization in the sense that $\sigma(\mathrm{C.G.B.}(\langle F \rangle))$ is also a Gröbner basis of $\langle F_0 \rangle$. Instead, our first objective is determining for which specializations σ we cannot ensure that the reduced Gröbner basis commutes with the specialization. Our goal is to compute a sufficient set of conditions on $\overline{a}_0$, that make the algorithm acting on F to be automatically translatable by specialization into the algorithm acting on F_0, and consequently ensuring that, if G is any Gröbner basis of $\langle F \rangle$, then G_0 is a Gröbner basis of $\langle F_0 \rangle$.

As we shall see, the sufficient condition can be described by a variety $W \subset K^m$ which is the union of a set of $m-1$ dimensional varieties irreducible in $\mathrm{Quot}(R)$, outside of which specialization commutes.

In what follows we assume that an $\overline{x}$ monomial order $\succeq$ is given. In some algorithms we need also a monomial order involving all variables $[\overline{x},\overline{a}]$. Then we must use a compatible elimination product order (Bayer and Stillman, 1987) $\succ_{[\overline{x},\overline{a}]}$, in which all $\overline{x}$ are greater than all $\overline{a}$. More precisely, if we denote by $\succ_{\overline{x}}$ and $\succ_{\overline{a}}$ the restriction of the ordering to the $\overline{x}$ variables (resp. to the $\overline{a}$ variables), then $\succ_{[\overline{x},\overline{a}]}$ has to satisfy the following condition: For all $\alpha,\gamma\in\mathbb{Z}^n_{\geq 0}$ and $\beta,\delta\in\mathbb{Z}^m_{\geq 0}$

$$\overline{x}^\alpha\overline{a}^\beta \succ_{[\overline{x},\overline{a}]} \overline{x}^\gamma\overline{a}^\delta \Longleftrightarrow \left\{\overline{x}^\alpha \succ_{\overline{x}} \overline{x}^\gamma \quad \text{or} \quad \left(\overline{x}^\alpha = \overline{x}^\gamma \quad \text{and} \quad \overline{a}^\beta \succ_{\overline{a}} \overline{a}^\delta\right)\right\}.$$

We want to modify Buchberger's algorithm acting on F in order to provide the variety $W\subset K^m$ outside of which specialization works. We also intend to produce only polynomials with coefficients in $R[\overline{a}]$, without denominators.

Denominators of $R[\overline{a}]$ appear in the ordinary algorithm when computing S-polynomials and by performing divisions.

For the purpose we begin redefining S-polynomials without denominators as follows:

$$S(f,g)=\frac{\Gamma\, x^\gamma}{\mathrm{lm}(f)}\, f-\frac{\Gamma\, x^\gamma}{\mathrm{lm}(g)}\, g \tag{2.2}$$

where

$$\begin{aligned}\Gamma &= \mathrm{lcm}(\mathrm{lc}(f),\mathrm{lc}(g))\\ x^\gamma &= \mathrm{lcm}(\mathrm{lpp}(f),\mathrm{lpp}(g))\end{aligned}$$

with a slightly different normalization than usual, which does not affect its nature but produces a result in $R[\overline{a}][\overline{x}]$. (Compare with the modification given by Weispfenning (1992), which uses as Γ the product instead of the less common multiple. We use that R is an UFD).

3. Modified division algorithm: NORMALFORM

We now study division under specialization and prove the following

PROPOSITION 3.1. *Let $f,g_1,...,g_s\in R[\overline{a}][\overline{x}]$. Let $\succ$ be an $\overline{x}$-monomial order and σ a specialization (2.1), satisfying the conditions*

$$\sigma(\mathrm{lc}(g_i))\neq 0 \quad \textit{for all} \quad 1\leq i\leq s.$$

Let $q_1,\dots,q_s\in R(\overline{a})[\overline{x}]$ and $r\in R(\overline{a})[\overline{x}]$ be the quotients and remainder of the division of f by $g_1,\dots,g_s$ in $R(\overline{a})[\overline{x}]$. Then $\sigma(q_1),\dots,\sigma(q_s)$ and $\sigma(r)$ make sense and they are the corresponding quotients and remainders for the division of $\sigma(f)$ by $\sigma(g_1),\dots,\sigma(g_s)$ in $K[\overline{x}]$.

In other words, considering the division of f by $g_1,...,g_s$, if no leading coefficients of the divisors vanish under the specialization, then division and specialization commute properly. This condition is equivalent to the fact that the leading monomials $\mathrm{lpp}(g_i)$ and $\mathrm{lpp}(\sigma(g_i))$ are the same.

PROOF. We prove the result by induction on the division step. Call $(p^{(j)},{q_1}^{(j)},\dots,{q_s}^{(j)})$ and $(p'^{(k)},{q'_1}^{(k)},\dots,{q'_s}^{(k)})$ the partial (remainders, quotients) at steps j and k respectively of the divisions in $R(\overline{a})[\overline{x}]$ and in $K[\overline{x}]$. We want to prove that for each j there is some k

so that $\sigma(p^{(j)}) = p'^{(k)}$ and $\sigma(q_i^{(j)}) = q_i'^{(k)}$ for $i = 1, \ldots, s$. It is true, by construction for $j = 0$ by picking $k = 0$. Suppose we are at some step j in the division in $R(\overline{a})[\overline{x}]$, and assume induction hypothesis. Let i_j be the first index for which $\mathrm{lpp}(g_{i_j})$ divides $\mathrm{lpp}(p^{(j)})$. The new partial quotient to add and the new partial remainder will be

$$\begin{aligned} \psi_{i_j} &= \frac{\mathrm{lm}(p^{(j)})}{\mathrm{lm}(g_{i_j})} \\ p^{(j+1)} &= p^{(j)} - \psi_{i_j} g_{i_j}. \end{aligned} \tag{3.1}$$

Observe that by hypothesis, σ makes sense on ψ_{i_j} and $p^{(j+1)}$. So, specializing, two cases can occur:

Case 1: $\sigma(\mathrm{lc}(p^{(j)})) = 0$. In this case, also $\sigma(\psi_{i_j}) = 0$ and $\sigma(p^{(j+1)}) = \sigma(p^{(j)})$, and the same is true for the partial quotients. So the same k applies to $j + 1$.

Case 2. $\sigma(\mathrm{lc}(p^{(j)})) \neq 0$. Then $\sigma(\psi_{i_j}) \neq 0$. As by hypothesis all $\mathrm{lpp}(g_i)$ remain stable under specialization, i_j is the first index for which $\mathrm{lpp}(\sigma(g_{i_j}))$ divides $\mathrm{lpp}(p'^{(k)})$, so

$$\begin{aligned} \psi'_{i_j} &= \frac{\mathrm{lm}(p'^{(k)})}{\mathrm{lm}(\sigma(g_{i_j}))} \\ p'^{(k+1)} &= p'^{(k)} - \psi'_{i_j} \sigma(g_{i_j}). \end{aligned}$$

Using the induction hypothesis for j and specializing equations (3.1) yields:

$$\begin{aligned} \sigma(\psi_{i_j}) &= \frac{\sigma(\mathrm{lm}(p^{(j)}))}{\sigma(\mathrm{lm}(g_{i_j}))} = \frac{\mathrm{lm}(p'^{(k)})}{\mathrm{lm}(\sigma(g_{i_j}))} = \psi'_{i_j} \\ \sigma(p^{(j+1)}) &= p'^{(k)} - \psi'_{i_j} \sigma(g_{i_j}) = p'^{(k+1)}, \end{aligned}$$

so in this case we pick $k + 1$. Note that the partial quotients also remain stable. □

The division in $R(\overline{a})[\overline{x}]$ introduces coefficients with denominators in $R[\overline{a}]$. But these denominators arise only from leading coefficients of the divisors $g_1, \ldots, g_s$, and are divisors of a product of powers of them. Under the hypothesis of proposition 3.1, we can still multiply f by a convenient factor μ in $R[\overline{a}]$. This will only change the normalization of f by a non-vanishing factor under specialization. Let

$$\mu = \mathrm{lcm}(\mathrm{LC}(\mathrm{denom}(q_1)), \ldots, \mathrm{LC}(\mathrm{denom}(q_s)), \mathrm{LC}(\mathrm{denom}(r))).$$

Writing $q_i' = \mu\, q_i$ and $r' = \mu\, r$, we have

$$\mu\, f = \sum_{i=1}^{s} q_i' g_i + r'. \tag{3.2}$$

The result will be a division with quotients q_i' and remainder r' in $R[\overline{a}][\overline{x}]$. This algorithm is usually denoted as NORMALFORM.

If the condition on the leading monomials is satisfied, proposition (3.1) guarantees that NORMALFORM can be specialized automatically and $\sigma(\mu) \neq 0$.

In general we are not interested in the quotients and we only need that the remainder is in $R[\overline{a}][\overline{x}]$. So we can take $\mu = \mathrm{denom}(r)$.

Moreover, if the content, $\mathrm{cont}_{\overline{x}}(r') \in R[\overline{a}]$, is not 1, we can further reduce the division. Let λ be the maximum divisor of $\mathrm{cont}(r')$ that is also a product of powers of divisors of some $\mathrm{lc}(g_i)$. As, by hypothesis, these factors do not cancel in the specialization, the result can be modified dividing the remainder r, and correspondingly the quotients $q_1, \ldots, q_s$ and μ by λ. This will be our version of NORMALFORM. Finally

$$\mu = \frac{\mathrm{denom}(r)}{\lambda}.$$

With this value of μ the quotients can be in $R(\overline{a})[\overline{x}]$ instead then in $R[\overline{a}][\overline{x}]$, and also μ can be in $R(\overline{a})$ instead then in $R[\overline{a}]$, but the remainder is still in $R[\overline{a}][\overline{x}]$.

In actual programming, we can eliminate denominators at each division step in order to only operate with polynomials without denominators.

4. The lc-condition and PGB0 algorithm

We are now able to give a modified Buchberger's algorithm. Given $F \subset R[\overline{a}][\overline{x}]$, it outputs a Gröbner basis $G \subset R[\overline{a}][\overline{x}]$ of $\langle F_{R[\overline{a}]}\rangle$, the ideal generated by F in $R(\overline{a})[\overline{x}]$. Then we define the *singular variety*

$$W := \bigcup_{g \in G} \mathbb{V}(\mathrm{lc}(g)). \tag{4.1}$$

Outside W specialization is certainly allowed. The algorithm is almost the same as the classical one (Cox, Little & O'Shea, 1992) except that S-polynomials are defined by equation (2.2) and divisions are performed by NORMALFORM.

4.1. Modified Buchberger algorithm, PGB0

Input: $F = \{f_1, \ldots, f_s\} \subset R[\overline{a}][\overline{x}]$,
$\succ$: an $\overline{x}$-monomial order.
Output: $G = \{g_1, \ldots, g_t\}$, a Gröbner basis of $\langle F\rangle$, with $F \subset G$
  $G := F$; $G' = \phi$
  WHILE $G \neq G'$
    $G' := G$
    FOR each pair $\{p, q\}$, $p \neq q$ in G' DO
      $S := \overline{S(p,q)}^{G'}$ **(using definition (2.2) and** NORMALFORM**)**
      IF $S \neq 0$ THEN
        $G := G \cup \{S\}$.

We claim the following

Proposition 4.1. *Let G be the output of* PGB0, *and W given by equation* (4.1). *Then*

(i) *$G =$ is a Gröbner basis of $\langle F_{R(\overline{a})}\rangle$, the ideal generated by F in $R(\overline{a})[\overline{x}]$, with $F \subset G$.*
(ii) $G \subset R[\overline{a}][\overline{x}]$
(iii) *If σ is determined by $\overline{a}_0$, and $\overline{a}_0 \notin W$, then $\sigma(G)$ is a Gröbner basis of $\langle \sigma(F)\rangle$.*

We refer to the condition in (iii) as the lc-condition. Observe that if we decompose every $\mathrm{lc}(g)$, for $g \in G$ in irreducible factors, W may be written as the union of the varieties defined by each one of the irreducible factors, and this provides the decomposition of W into irreducible components when we factor in the algebraic closure of K.

Proof. (i) is obvious, as the only changes with respect to the classical GB algorithm are multiplication by factors in $R[\overline{a}]$, which are elements of the coefficient field $R(\overline{a})$.

(ii) is true by the definition (2.2) of S-polynomials and NORMALFORM.

(iii) Finally we prove that lc-condition is a sufficient condition to ensure that $\sigma(G)$ is a Gröbner basis of $\sigma(\langle F\rangle)$. lc-condition (iii) is also "necessary" in the sense that otherwise we cannot guarantee automatic translation: if F is at the depart a Gröbner basis and lc-condition is not satisfied, then F and $F_0 = \sigma(F)$ will not have the same set of leading monomials. So translation is not automatic, even if specialization can possibly hold. On the other side, by (i)

$$\langle \mathrm{lpp}(\langle F\rangle)\rangle = \langle \mathrm{lpp}(g_1), \ldots, \mathrm{lpp}(g_t)\rangle$$

and if lc-condition is satisfied, then

$$\langle \mathrm{lpp}(g_1), \ldots, \mathrm{lpp}(g_t)\rangle = \langle \mathrm{lpp}(\sigma(g_1)), \ldots, \mathrm{lpp}(\sigma(g_t))\rangle.$$

We need only to prove now that

$$\langle \mathrm{lpp}(\sigma(g_1)), \ldots, \mathrm{lpp}(\sigma(g_t))\rangle = \langle \mathrm{lpp}(\langle \sigma(F)\rangle)\rangle = \langle \mathrm{lpp}(\langle F_0\rangle)\rangle$$

in order to finish the proof of (iv).

Let us write $G = \{f_1, \ldots, f_s, g_{s+1}, \ldots, g_t\}$. So the first s elements of $\sigma(G)$ are the elements of $\sigma(F)$, and if lc-condition holds, they have the same leading monomials. The remaining elements, $s+1$ till t, are the specialization of the non-vanishing residues of the S-polynomials of any two previous elements of G.

We now follow the steps of the algorithm. Take any S-polynomial $S(g_i, g_j)$ of two elements in G'. If lc-condition is satisfied until this step, then $\sigma(S(g_i, g_j))$ is equal to the ordinary S-polynomial $S(\sigma(g_i), \sigma(g_j))$ up to non-vanishing K factors (constants), as the definitions of S-polynomials only involves leading terms. By proposition 3.1, if the residue $\overline{S(g_i, g_j)}^{G'}$ using NORMALFORM vanishes, then the ordinary residue $\overline{\sigma(S(g_i, g_j))}^{\sigma(G')}$ vanishes too. If it doesn't vanish it will be added to the list. But if lc-condition still holds, then $S(\sigma(g_i), \sigma(g_j))$ doesn't vanish either, as its leading monomial coincides, up to K factors, with that of $\sigma(S(g_i, g_j))$. So the algorithm continues to be translatable by specialization. As a consequence G specializes to a Gröbner basis of F_0. □

5. Minimal and reduced Gröbner basis

It is now very simple to prove that under the lc-conditions the Gröbner basis obtained can be minimized and reduced. The classical improvements of Buchberger's algorithm are also easily proved in our case. Nevertheless, the singular variety cannot be reduced by considering only the leading coefficients of the minimal or of the reduced basis. For this purpose we shall use a different technique.

Minimal Gröbner basis is obtained by discarding from a Gröbner basis those polynomials whose leading monomials can be divided by the leading monomial of any other polynomial in the basis. If G is a Gröbner basis, it is a basis of the ideal, and so, if $p \in G$ is such that $\mathrm{lm}(p) \in \langle \mathrm{lm}(G - \{p\})\rangle$, then $\langle \mathrm{lm}(G-\{p\})\rangle = \langle \mathrm{lm}(G)\rangle$. It follows that is $G - \{p\}$ is also a Gröbner basis of $\langle F\rangle$. The minimal Gröbner basis G' so obtained will continue to specialize outside the variety W obtained by PGB algorithm, and $\mathrm{lpp}(G') \subset \mathrm{lpp}(G)$.

The minimal Gröbner basis G' can also be reduced and continue to specialize outside W, as the leading coefficients of the actual G' do not become zero by specialization outside W, and so we can divide each polynomial p in G' by $G' - \{p\}$, and the result will be a reduced Gröbner basis G". We only need to normalize it adequately.

Finally we normalize the polynomials. As $\mathrm{cont}(p)$ is always a divisor of $\mathrm{lc}(p)$ and for $a_0 \notin W$ it does not vanish by specialization, we can divide p by its content. The polynomial obtained has only a R-unity ambiguity. If R is $\mathbb{Z}$, we can drop this ambiguity by taking positive $\mathrm{lc}_{\overline{x}\overline{a}}(p)$. The resulting reduced Gröbner basis is unique in $R[\overline{x}, \overline{a}]$, and specializes to a reduced Gröbner basis in $K[\overline{x}]$ outside W, except that it has to be normalized after specializing.

6. Reduction of the singular variety: generalized Gaussian elimination GGE and PGB

If we compute the singular variety of an ideal using PGB0, and then minimize, reduce and normalize the basis, it is clear, that the resulting reduced Gröbner basis is unique. But the computed singular variety depends on the development of PGB0 algorithm and is not uniquely determined by the ideal, as the algorithm can follow different paths. In any case, we obtain a sufficient condition for the Gröbner basis to specialize, but this condition is algorithm depending (see Example 1). It is very important to reduce the variety so much as possible.

For this purpose we introduce a generalized Gaussian elimination algorithm (GGE) to transform the initial basis F of the ideal to a more simple basis F'.

6.1. Generalized Gaussian Elimination, GGE

Input: $F = [f_1, \ldots, f_s] \subset R[\overline{x}, \overline{a}]$, ($\overline{x}$ and $\overline{a}$ as variables)
$\succ_{[\overline{x},\overline{a}]}$: a compatible $[\overline{x}, \overline{a}]$ elimination order.
Output: F' a new basis of $\langle F \rangle$.

```
G := F; G' = φ
WHILE G ≠ G'
    FOR i from 1 to #G DO
        G' := G
        G := φ
        FOR k from 1 to #G' DO
            IF k ≠ i THEN
                f := NORMALFORM(g'_k, [g'_i], [x̄, ā], ≻_[x̄,ā]) (ordinary division)
                G := G ∪ [f]
            ELSE G := G ∪ [g'_i]
F' := G/cont_[x̄,ā](G).
```

The idea of the algorithm comes from ordinary Gaussian elimination.

Taking F' as input for PGB0, the algorithm is simplified and we expect that only the strict real special cases will occur in the singular variety when an adequate order of the variables is chosen. In the examples it is shown that we are able to achieve this goal. Nevertheless, the process is sensitive to the variable order chosen, and we cannot ensure, in general, complete minimality of the singular variety obtained. It is important to choose the variables in an order for which there are leading terms in $[\overline{x}, \overline{a}]$ not containing the parameters, and dividing other leading terms.

We defined GGE algorithm considering all variables $\overline{x}$ and parameters $\overline{a}$ as variables.

More generally we can define the algorithm separating them. In this case it is necessary to consider as divisors only those polynomials with constant leading coefficients. But the best elimination is obtained using all $[\overline{x},\overline{a}]$ as variables.

PROPOSITION 6.1. *Let $F \subset R[\overline{a}][\overline{x}]$, and $F' := \mathrm{GGE}\,(F,[\overline{x},\overline{a}],\succ_{[\overline{x},\overline{a}]})$, where $\succ_{[\overline{x},\overline{a}]}$ is a compatible $[\overline{x},\overline{a}]$ elimination order, i.e. using $\overline{x}$ and $\overline{a}$ as variables in the divisions. Then*

(i) *F' is a new basis of $\langle F\rangle \subset \mathrm{Quot}(R)[\overline{x},\overline{a}]$ that has less or equal number of elements than F. Moreover $\langle \mathrm{lpp}_{[\overline{x},\overline{a}]}(F)\rangle \subset \langle \mathrm{lpp}_{[\overline{x},\overline{a}]}(F')\rangle$, and also $\langle \mathrm{lpp}_{\overline{x}}(F)\rangle \subset \langle \mathrm{lpp}_{\overline{x}}(F')\rangle$.*
(ii) *F' specializes, i.e. $\sigma(F')$ is also a basis of $\langle \sigma(F)\rangle$.*
(iii) *The algorithm terminates.*
(iv) *Each $p \in F'$, is the residue of dividing p by $F' - \{p\}$ with respect to the given $[\overline{x},\overline{a}]$-order. We say that F' is reduced for this order.*

PROOF. (i) At each division in the algorithm we substitute in a given F-basis two polynomials in $R[\overline{a}][\overline{x}]$, say $\{f,g\}$ by $\{g,r\}$, where $f = g\,h + r$. As we can express f and g as a linear combination of g and r with coefficients in $\mathrm{Quot}(R)$, then $\{g,r\}$ is a new basis of $\langle f,g\rangle$, and consequently $\{g,r\}$ can substitute $\{f,g\}$ to form a new basis of F. This is the only repeated action in computing the GGE. Observe also, that the final number of polynomials is less or equal than the number of polynomials in F, as we substitute at each step two polynomials by two or one (when the residue is 0) polynomials. The proposition when we only consider the $\overline{x}$ as variables is a consequence of $\succ_{[\overline{x},\overline{a}]}$ being a compatible elimination order.

(ii) Note that even if the algorithm is used considering the $\overline{a}$ as parameters, no denominators of $R[\overline{a}]$ appear, as we only divide by polynomials with constant leading coefficients in R.

(iii) We have to prove that the algorithm finishes. Let F_i be the base after the i^{th} loop. Define

$$d_i = \sum_{f\in F_i} \mathrm{multideg}_{[\overline{x},\overline{a}]}(f).$$

As $\#F_i \leq \#F_{i-1}$ and for every division in the algorithm, whenever the leading term is divisible, the multideg of the remainder is strictly smaller then that of the dividend, necessarily $d_i \preceq_{[\overline{x},\overline{a}]} d_{i-1}$. If $d_i = d_{i-1}$ then no leading monomial has changed in the loop i. So, no monomial of a $f \in F_i$ is divisible by any leading monomial of an element of F_i (with constant leading coefficient, when we only consider the $\overline{x}$ as variables), as all possible divisions have been performed in loop i. So the algorithm stops in this case. As $\succ_{[\overline{x},\overline{a}]}$ is a well-order, d_i necessarily stabilize, and the algorithm effectively terminates. GGE works in the direction of the reduced Gröbner basis, even if it need not reach it, as not all S-polynomials are constructed and tested.

(iv) As all leading coefficients are constants of R, all polynomials in F' have been considered as divisors of the others, and no polynomial will be divisible by the remaining. (iv) is the triangulation property of GGE. It only applies when variables and parameters are taken as variables. $\square$

We incorporate GGE as a previous step of PGB algorithm, before calling PGB0, in order to transform the initial basis. The resulting singular variety will now be smaller, and if we choose a suitable order of the variables, in practice we are often able to obtain the minimal singular variety.

GGE algorithm is remarkable for being used with linear systems with parameters. If we apply it only with respect to the variables, but not to the parameters, it reduces to the ordinary Gaussian elimination carried out with care, i.e. using only pivots not depending on the parameters. But if we apply it with respect to variables and parameters, it goes further, and provides a perfect first step for a reduced case discussion, as can be seen in the example in the next section.

Let us give finally the PGB algorithm:

6.2. PGB algorithm

Input: $F = \{f_1, \ldots, f_s\} \subset R[\overline{x}, \overline{a}]$,
$\succ_{[\overline{x},\overline{a}]}$: a compatible elimination $[\overline{x}, \overline{a}]$-monomial order.
Output: G the reduced Gröbner basis of $\langle F \rangle$, with respect to $[\overline{x}]$.
W: The singular variety outside of which the basis specializes.

$G_1 := \mathrm{GGE}(F, [\overline{x}, \overline{a}], \succ_{[\overline{x},\overline{a}]})$
$G_2 := \mathrm{PGB0}(G_1, [\overline{x}], \succ_{\overline{x}})$
$W := \bigcup_{g \in G_2} \mathbb{V}(\mathrm{lc}_{\overline{x}}(g))$
$G_3 := \mathrm{Minimal}(G_2, [\overline{x}], \succ_{\overline{x}})$
$G_4 := \mathrm{Reduce}(G_3, [\overline{x}], \succ_{\overline{x}})$
$G := \mathrm{Normalize}(G_4, [\overline{x}], [\overline{a}], \succ_{[\overline{x},\overline{a}]})$.

7. Examples

Example 1. Consider the following linear system in the variables $\{x, y, z, u\}$ with the parameters $\{a, b\}$.

$$\begin{aligned} F \quad := \quad & [a\,x + 2\,y + 3\,z + u - 6, x + 3\,y - z + 2\,u - b, \\ & 3\,x - a\,y + z - 2, 5\,x + 4\,y + 3\,z + 3\,u - 9] \end{aligned}$$

We take F to be the basis of an ideal in $\mathbb{Z}[x, y, z, u, a, b]$ and compute the a new basis with the GGE algorithm given in section 6, relative to all the variables and parameters $[x, y, z, u, a, b]$ in lex order. The result is:

$$\begin{aligned} F' \quad := \quad & \mathrm{GGE}(F, \mathrm{lex}(x, y, z, u, a, b)) \\ & [756\,x - 39\,a\,b - 4\,b - 155 - 117\,a + (117\,a + 51)\,u, \\ & -189\,y - 6\,a\,b + 107 + 43\,b - 18\,a + (18\,a - 123)\,u, \\ & -756\,z + 1439 - 236\,b - 99\,a - 33\,a\,b + (-15 + 99\,a)\,u, \\ & (30\,a - 21 - 9\,a^2)\,u + 9\,a^2 + 3\,a^2\,b - 11\,a\,b - 22\,a + 49 - 28\,b,] \end{aligned}$$

As we see, the new basis is completely Gaussian reduced:

The new basis is triangular: each leading monomial is different when we consider as variables all x, y, z, u, a, b. In this case, it is also true if we consider only as variables x, y, z, u.

The pivots (leading coefficients) of the variables x, y, z are constants and only the last leading coefficient in the variable u is a polynomial in the parameters and is essentially the singular variety: $30\,a - 21 - 9\,a^2 = -3\,(a-1)\,(3\,a-7)$, or the value of the determinant.

Instead, the variable u is not eliminated in the equations giving x, y, z.

In this form, the system is very simple to be discussed.

The result is, in this case, a minimal Gröbner basis, but not the reduced one.

Moreover, in this example, F' is itself a comprehensive Gröbner basis.

Now we compute the reduced Gröbner basis using PGB algorithm and obtain

$$\begin{array}{rcl} G & := & \mathrm{PGB}(F', \mathrm{lex}(x,y,z,u), \mathrm{lex}(a,b), 'W') = \\ & & (9\,a^2 - 30\,a + 21)\,x - 6\,a\,b + 9\,a - 2\,b - 1, \\ & & (9\,a^2 - 30\,a + 21)\,y + 3\,a\,b + 20 - 23\,b, \\ & & (9\,a^2 - 30\,a + 21)\,z + 53\,a - 5\,a\,b - 18\,a^2 + 3\,a^2\,b - 39 + 6\,b, \\ & & (9\,a^2 - 30\,a + 21)\,u - 9\,a^2 - 3\,a^2\,b + 11\,a\,b + 22\,a - 49 + 28\,b] \end{array}$$

and the singular variety

$$W = \mathbb{V}(a-1) \cup \mathbb{V}(3\,a-7)$$

that, in this example, is the minimal variety where the linear system has different kinds of solutions. We do not go deeper in the general discussion of all cases as this is the object of a forthcoming paper.

If we compute the Gröbner basis using PGB algorithm without previous reduction of F to F', the basis G is the same, but the variety becomes $W_1 = \mathbb{V}(a) \cup \mathbb{V}(a^2+35) \cup \mathbb{V}(3\,a-2) \cup \mathbb{V}(a-1) \cup \mathbb{V}(3\,a-7)$.

It is interesting to compare G and F'. It is not true, in general, that F' is a Gröbner basis, but it is triangular in x, y, z, u, a, b. The reduced Gröbner basis G is now triangular with respect to the variables x, y, z, u. Instead, its leading coefficients are not constants, though all variables are isolated (u does not appear in the equations defining x, y, z).

Note: If we compute the GGE with respect only to the variables and not to the parameters, the result is the ordinary Gaussian elimination using constant pivots, and the singular variety increases. The result is in this case:

$$\begin{array}{rcl} F' & := & \mathrm{GGE}(F, \mathrm{lex}(x,y,z,u)) = \\ & & [11\,x + 13\,z + u + 4\,b - 27, -11\,y + 8\,z - 7\,u - 9 + 5\,b, \\ & & (-3-a)\,u + (49 - 13\,a)\,z - 4\,a\,b + 27\,a + 10\,b - 84, \\ & & (-3 + 7\,a)\,u + (-28 - 8\,a)\,z - 5\,a\,b + 9\,a - 12\,b + 59 \end{array}$$

Example 2. Take now the general cubic in Weierstrass form given by

$$f := y^2 + a_1\,x\,y + a_3\,y - x^3 - a_2\,x^2 - a_4\,x - a_6$$

and search the conditions for f to have singular points. The system is given by:

$$\begin{array}{rcl} H & := & [y^2 + a_1\,x\,y + a_3\,y - x^3 - a_2\,x^2 - a_4\,x - a_6, \\ & & a_1\,y - 3\,x^2 - 2\,a_2\,x - a_4, 2\,y + a_1\,x + a_3] \end{array}$$

Applying GGE we obtain:

$$\begin{array}{rcl} H_1 & := & \mathrm{GGE}(H, \mathrm{lex}(y, x, a_6, a_2, a_4, a_3, a_1)) = \\ & & [(16\,a_2^2 + 8\,a_1^2\,a_2 + a_1^4 - 24\,a_1\,a_3 - 48\,a_4)\,x \\ & & -72\,a_6 - 18\,a_3^2 + 8\,a_2\,a_4 + 4\,a_1\,a_2\,a_3 + 2\,a_1^2\,a_4 + a_1^3\,a_3, \\ & & 6\,x^2 - (-4\,a_2 - a_1^2)\,x + 2\,a_4 + a_1\,a_3, 2\,y + a_1\,x + a_3]. \end{array}$$

Computing the PGB we obtain $G = [1]$ and the singular variety $W = \mathbb{V}(f_1) \cup \mathbb{V}(f_2)$, where

$$
\begin{aligned}
f_1 \;=\;& 12\,a_2\,a_1^4\,a_6 - 16\,a_2^2\,a_4^2 + 64\,a_4^3 - 36\,a_2\,a_1\,a_3^3 + 432\,a_6^2 - 288\,a_2\,a_4\,a_6 + 64\,a_2^3\,a_6 \\
& +27\,a_3^4 - 16\,a_1\,a_4\,a_2^2\,a_3 + 96\,a_1\,a_4^2\,a_3 - 8\,a_4^2\,a_2\,a_1^2 - a_4^2\,a_1^4 + a_2\,a_1^4\,a_3^2 + 8\,a_1^2\,a_2^2\,a_3^2 \\
& +30\,a_1^2\,a_4\,a_3^2 - 72\,a_2\,a_4\,a_3^2 + 216\,a_3^2\,a_6 - 36\,a_1^3\,a_6\,a_3 - a_1^5\,a_4\,a_3 - 8\,a_2\,a_1^3\,a_4\,a_3 \\
& -144\,a_1\,a_6\,a_2\,a_3 + 48\,a_1^2\,a_6\,a_2^2 + 16\,a_2^3\,a_3^2 + a_1^6\,a_6 - 72\,a_1^2\,a_6\,a_4 - a_1^3\,a_3^3
\end{aligned}
$$

$$
f_2 \;=\; 16\,a_2^2 + 8\,a_1^2\,a_2 + a_1^4 - 24\,a_1\,a_3 - 48\,a_4
$$

The singular variety provides a very simply discussion of the solutions. As we shall see in the next paper, where the general discussion for polynomial systems will be provided, $f_1 = 0$ reveals itself as the condition for the existence of solutions of G, i.e. for the existence of singular points. The condition $f_2 = 0$ is responsible for the nature of the Gröbner basis, i.e., for the nature of the singular points. In this example, if we do not use GGE, we also obtain bigger singular varieties.

References

Adams, W.W., Boyle, A.K. (1992). Some Results on Gröbner Bases over Commutative Rings. *Jour. Symb. Comp.* **13**, 473-484.

Assi A. (1994). On Flatness of Generic Projections. *Jour. Symb. Comp.* **18**, 447-462.

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

Bayer, D., Galligo, A., Stillman, M. (1991). Gröbner Bases and extension of scalars. Computational algebraic geometry and commutative algebra (Cortona, 1991) p 198-215. *Sympos. Math, XXXIV*, Cambridge Univ. Press, Cambridge, 1993.

Becker, T. (1994). On Gröbner bases under specialization. *Appl. Algebra Engrg. Comm. Comput,* **5**, num. 1, 1-8.

Cox, D., Little, J., O'Shea, D. (1992). Ideals, Varieties and Algorithms. Springer. New-York.

Gebauer, R., Möller, H.M., (1987). On an installation of Buchberger's Algorithm. Springer.

Gianni, P. (1987). Properties of Gröbner Bases under Specializations, in EUROCAL'87 A theorem on refining division orders by the reverse lexicographic order. J.H. Davenport Ed., Springer LNCS vol 378, 293-297.

Gianni, P., Mora T. (1987). Algebraic Solutions of Systems of Polynomial Equations using Gröbner Bases. *Applied algebra, algebraic algorithms and error-correcting Codes.* (Menorca,1987), p. 247-257. . *Lecture Notes in Comut. Sci, 356*, Springer, Berlin, 1989.

Gianni, P., Trager, B., Zacharias, G. (1988). Gröbner Bases and Primary Decomposition of Polynomial Ideals. *Jour. Symb. Comp.* **6**, 149-167.

Gräbe, H.G. (1993). On Lucky Primes. *Jour. Symb. Comp.* **15**, 199-209.

Kalkbrener, M. (1987). Solving systems of algebraic aquations by using Gröbner Bases. In: Davenport, J.H. (ed.) EUROCAL'87, European Conference on Computer Algebra. Lecture Notes in Computer Science, 378, p 282-292. Springer.

Kalkbrener, M. (1997). On the stability of Gröbner Bases under specializations. *Jour. Symb. Comp.* **24**, num. 1, 51-58.

Miller, J.L. (1996). Analogs of Gröbner Bases in Polynomial Rings over a Ring. *Jour. Symb. Comp.* **21**, 139-153.

Möller, H.M. (1988). On the construction of Gröbner Bases using syzygies. *Jour. Symb. Comp.* **6**/2,3, p. 345-359.

Montes, A. (1995). Solving the load flow problem using Gröbner bases, *SIGSAM Bull.* **29**, 1-13.

Montes, A. (1998). Algebraic solution of the load-flow problem for a 4-nodes electrical network, *Math. and Comp. in Simul.* **45**, 163-174.

Pauer, F. (1992). On Lucky Ideals for Gröbner Basis Computations. *Jour. Symb. Comp.* **14**, 471-482.

Weispfenning V. (1992). Comprehensive Gröbner Bases. *Jour. Symb. Comp.* **14**, 1-29.