Konrad-Zuse-Zentrum für Informationstechnik Berlin

H. Michael Möller*

On Decomposing Systems of Polynomial Equations With Finitely Many Solutions

* FB Mathematik
FernUniversität Hagen
Postfach 940
W-5800 Hagen
Germany

Fellow of the Konrad–Zuse–Zentrum Berlin

Preprint SC 92–15 (June 1992)

Contents

Abstract

This paper deals with systems of m polynomial equations in n unknown, which have only finitely many solutions. A method is presented which decomposes the solution set into finitely many subsets, each of them given by a system of type

$$f_1(x_1) = 0,\ f_2(x_1, x_2) = 0, \ldots, f_n(x_1, \ldots, x_n) = 0.$$

The main tools for the decomposition are from ideal theory and use symbolical manipulations. For the ideal generated by the polynomials which describe the solution set, a lexicographical Gröbner basis is required. A particular element of this basis allows the decomposition of the solution set. A recursive application of these decomposition techniques gives finally the triangular subsystems. The algorithm gives even for non-finite solution sets often also usable decompositions.

Keywords: Algebraic variety decomposition, Gröbner bases, systems of nonlinear equations.

1. Introduction

We deal with the problem of solving a system of m equations

$$f_1(x_1, \ldots, x_n) = 0, \ldots, f_m(x_1, \ldots, x_n) = 0, \qquad (1)$$

where $f_1, \ldots, f_m$ are n-variate polynomials with coefficients in a field $I\!K$. Here, solving means finding the solution set, i. e. the set of all $(x_1, \ldots, x_n) \in \overline{I\!K}^n$ satisfying (1), where $\overline{I\!K}$ is a suitable algebraic extension of $I\!K$.

There are two major point of views on what "finding" means in this context. The first one is the more algebraic concept of elimination. The second is a numerical one, the approximate calculation of the n-tuples $(x_1, \ldots, x_n) \in \overline{I\!K}^n$ satisfying (1).

Numerically, the solution set can be described, when there are only finitely many solutions, all of them in $\mathbb{C}^n$. Then approximations of prescribed exactness can be found in the floating point analogue to $\mathbb{C}^n$ for each of the solution points. But it seems, that only under the restrictive condition $m = n$ methods for solving numerically (1) exists, e. g. Auzinger & Stetter [1], Li [6], Ortega & Rheinboldt [10], Schwetlick [12]. Therefore, underdetermined systems, i. e. systems (1) with $m < n$, having an infinite solution set, can only be treated numerically, when fixed numerical values are assigned to "free" parameters. And an overdetermined system, $m > n$, seems to be only solvable after a preprocessing, i.e. by reducing it to (a system of) n equations in n variables.

Algebraically, the set

$$\{(x_1, \ldots, x_n) \in \overline{I\!K}^n \mid f_i(x_1, \ldots, x_n) = 0,\ i = 1, \ldots, m\}, \qquad (2)$$

is a variety, representing the common zeros of the polynomials in the ideal $A = (f_1, \ldots, f_m)$. The computation of the elimination ideals $A_k := A \cap I\!K[x_1, \ldots, x_k]$ seem to be a feasible way for solving (1). Trinks [13] proposed the computation of the lexicographical Gröbner basis of A, which contains for every k a (again lexicographical Gröbner) basis of A_k. Solving numerically the univariate problem in A_1, then after substituting the numerical approximations into A_2, the problem of finding the zeros in A_2 is a univariate one. Substituting these approximations into A_3, again a univariate problem arises, etc. This was for a long time considered to be the right concept for solving algebraically systems of equations.

However, when in the elimination ideal A_k the first $k-1$ variables are replaced by numerical values, there might be more than one basis polynomial remain nonzero after the substitution. Then there is the question, which of these polynomials shall be used for the (univariate) zero computation. And because all numerical values are only approximations, polynomials which should be zero after substitution may become nonzero and might be used unfortunately for zero computation... We can overcome all these numerical problems, when we have a method for splitting a set (2) into a finite union of sets of type (2) each with $m = n$.

Lazard [5] presented a method of decomposing a finite variety (2) into irreducible ones, and showed that each of them has a minimal generating set, with $m = n$ polynomials, of triangular type

$$\begin{array}{lcl} f_1(x_1) & = & x_1^{d_1} + \sum_{j=1}^{d_1-1} g_{1,j} x_1^j, \\ f_2(x_1,x_2) & = & x_2^{d_2} + \sum_{j=1}^{d_2-1} g_{2,j}(x_1) x_2^j, \\ & \cdots & \\ f_n(x_1,\ldots,x_n) & = & x_n^{d_n} + \sum_{j=1}^{d_n-1} g_{n,j}(x_1,\ldots,x_{n-1}) x_n^j. \end{array} \tag{3}$$

Numerical methods for solving equations are considerably simple when applied to systems (3). For instance, the iteration step in Newton's method for obtaining the $k+1$-st improved approximation $x^{(k+1)}$,

$$x^{(k+1)} := x^{(k)} - F'(x^{(k)})^{-1} F(x^{(k)}),$$

where $F := (f_1,\ldots,f_n)^T$ and $x^{(k)}$ is the k-th approximation, requires the solving of a set of linear equations, $F'(x^{(k)})h = F(x^{(k)})$ (and $x^{(k+1)} := x^{(k)} - h$). Here, the Jacobian $F'(x^{(k)})$ is triangular, such that the values of h are easily found by only successive substitutions. For achieving this favourable decomposition, Lazard recommends the computation of a Gröbner basis of $(f_1,\ldots,f_m)$ and polynomials factorization in algebraic extension fields by D. Duval's D5-techniques.

Starting point for this paper was the observation that, having a lexicographical Gröbner basis for $A = (f_1,\ldots,f_m)$, a decomposition for the finite variety (2) is obtained easily, and polynomial factorization is not necessary (but if cheap, then useful). By an iterative application of such decompositions, finitely many disjoint sets (3) are constructed. The needed lexicographical Gröbner bases can often be read off from already known Gröbner bases, cf. lemma 7, such that their computation costs no arithmetical operation. The only difficulty in the recursion is to calculate lexicographical Gröbner bases for ideal quotients $A : g$ and ideal sums $A + (g)$, when a Gröbner basis for A is given. Here we propose either Buchberger's algorithm (for $A + (g)$) and, in section 3, a modification of a method by Gianni et al. [3] (for $A : g$) or, if we already know, that the variety of A is finite, we may use linear techniques. In this case, it is sufficient to have an arbitrary Gröbner basis of A and to transform it to a lexicographical one by linear techniques like the FGLM-method, see Marinari et al. [7], and lexicographical Gröbner bases for $A : g$ and $A + (g)$ can be computed similarly costing at most $O(s^3)$ arithmetical operations, where s is the dimension of the $\mathbb{K}$-vector space $\mathbb{K}[x_1,\ldots,x_n]/A$.

An early version of the algorithm is already installed as procedure GROEPOSTPROC in the Gröbner package of the Computer Algebra System REDUCE, release 3.4, Melenk et al. [8]. For a successful application of this package including the decomposition procedure see for instance Hietarinta [4].

2. Ideals and decompositions

Let us first summarize some elementary notions and facts on ideals and varieties. More details and proofs can be found in textbooks on algebra and ideal theory, like [11] or [14].

Only polynomials in a ring $\mathcal{P} := I\!\!K[x_1, \ldots, x_n]$ are considered, where $I\!\!K$ is a field. The set of all points which are common zeros of given polynomials $f_1, \ldots, f_r$ is called their *variety,* briefly $V(f_1, \ldots, f_r)$. Since these points are the common zeros of all polynomials of the ideal A generated by $f_1, \ldots, f_r$, $A = \{\sum_{i=1}^{r} g_i f_i \mid g_i \in \mathcal{P}\}$, the variety is also called the variety of A, $V(A)$. As usual we write in this context $A = (f_1 \ldots, f_r)$. For determining $V(A)$, it is irrelevant, what basis $\{f_1, \ldots, f_r\}$ of A we have chosen. $V(A)$ is empty iff $1 \in A$, i.e. iff $\mathcal{P} = A$. If $V(A)$ consists of only finitely many points, then A is called *zero-dimensional* , briefly $dim(A) = 0$. The variety is contained in $\overline{I\!\!K}^n$, where $\overline{I\!\!K}$ denotes an algebraic field extension of $I\!\!K$.

The sum and the quotient of two ideals A and B, $A + B := \{a + b \mid a \in A, b \in B\}$, $A : B := \{p \mid p \cdot b \in A \text{ for all } b \in B\}$ as well as the intersection $A \cap B$ are also ideals. For short $A : b$ instead of $A : (b), b \in \mathcal{P}$. The *radical* of an ideal A, $\sqrt{A}$ for short, is the ideal $\{f \in \mathcal{P} \mid \exists \sigma \in I\!\!N : f^\sigma \in A\}$. By the Hilbert Nullstellensatz, $\sqrt{A} = \{f \in \mathcal{P} \mid f(y) = 0 \; \forall y \in V(A)\}$. Hence $V(A) = V(\sqrt{A})$. The product $A \cdot B$ is the least ideal containing all $a \cdot b$, $a \in A, b \in B$. Writing $A^1 := A$, we define recursively A^m by $A^m := A^{m-1} \cdot A$.

An ideal P is called a *zero-dimensional prime ideal,* if there exists a $y \in \overline{I\!\!K}^n$ such that $f(y) = 0 \Rightarrow f \in P$. Obviously $y \in V(P)$, but every point in $V(P)$ can be taken as such y defining membership for P. A zero-dimensional ideal Q is called *primary* or *P-primary,* if $P^\sigma \subseteq Q \subseteq P$ for a $\sigma \in I\!\!N$ and a zero-dimensional prime ideal P. Then $P = \sqrt{Q}$ and especially $V(Q) = V(P)$. Every zero-dimensional ideal A has a so called *primary decomposition,* which means, that there are finitely many distinct zero-dimensional prime ideals P_i and P_i-primary ideals Q_i with $A = \bigcap Q_i$. These P_i and Q_i are uniquely determined by A. It follows $V(A) = \bigcup V(P_i)$.

Lemma 1. *For ideals A and B and arbitrary $m \in I\!\!N$*

$$A \subseteq B \Longrightarrow A \subseteq B \cap (A : B^m) \subseteq \sqrt{A}. \tag{4}$$

If A is a radical, then $A = B \cap (A : B)$ and $A : B = A : B^m$ for all integer $m > 1$.

Proof. Since $A \subseteq A : B^m$ by definition of ideal quotients, and since $A \subseteq B$, we get the first inclusion in (4). Let $g \in B \cap (A : B^m)$. Then $g \in B$ and $g \in A : B^m$. Hence $g^m \in B^m$ and therefore $g^{m+1} \in A$, implying $g \in \sqrt{A}$. Hence (4).
If $A = \sqrt{A}$, then $A = B \cap A : B^m$ by (4). If $g \in A : B^m$, then $g \cdot b^m \in A$ for all $b \in B$. Therefore $g^m b^m \in A$ and hence $g \cdot b \in \sqrt{A} = A$ implying $g \in A : B$. On the other hand $A : B \subseteq A : B^m$. Hence $A : B = A : B^m$.

Lemma 2. *If B and $A \subseteq B$ are ideals with $dim(A) = 0$ and if $m \in I\!\!N$ is* *sufficiently large, then* $V(A)$ *is the disjoint union* $V(A) = V(B) \cup V(A : B^m)$ *with*

$$\begin{aligned} V(B) &= \{y \in V(A) \mid \ \forall b \in B : b(y) = 0\}, \\ V(A : B^m) &= \{y \in V(A) \mid \ \exists b \in B : b(y) \neq 0\}. \end{aligned} \tag{5}$$

Proof. $A \subseteq B \Longrightarrow V(B) \subseteq V(A)$. Hence $V(B) = \{y \in V(A) \mid \ \forall b \in B : b(y) = 0\}$. Let us consider the primary decompositions of A,

$$A = \bigcap Q_i, \text{ with } P_i\text{-primary } Q_i.$$

Then, see for instance Renschuch,[11, p.58], $A : B^m = \bigcap Q_i : B^m$, and, Renschuch [11, p.79ff] $Q_i : B^m$ equals Q_i, if $B^m \not\subseteq P_i$, equals $\mathcal{P}$, if $B^m \subseteq Q_i$, and equals an other P_i-primary ideal in the remaining cases, i. e. in the cases $B^m \subseteq P_i$, $B^m \not\subseteq Q_i$. But $B^m \subseteq P_i$ iff $B \subseteq P_i$ by definition of (zero-dimensional) prime ideals and $B \subseteq P_i$ implies $B^m \subseteq Q_i$ for $m \geq \sigma$, where $P_i^\sigma \subseteq Q_i$. Therefore $Q_i : B^m = Q_i$, if $B \not\subseteq P_i$, and $= \mathcal{P}$, if $B \subseteq P_i$. Hence $V(A : B^m) = \bigcup_{B \not\subseteq P_i} V(P_i) = \{y \in \bigcup V(P_i) \mid \ \exists b \in B : b(y) \neq 0\}$. The assertion follows by $V(A) = \bigcup V(P_i)$.

Lemma 3. *Let* $dim(A) = 0$ *and* $A \subseteq B = (g_1, \ldots, g_s)$. *Then for sufficiently large* $m, m_1, \ldots, m_s \in \mathbb{N}$:

$$V(A : B^m) = \bigcup_{i=1}^{s} V((A + (g_1, \ldots, g_{i-1})) : g_i^{m_i}) \tag{6}$$

with $V((A+(g_1, \ldots, g_{i-1})) : g_i^{m_i}) = \{y \in V(A) \mid g_1(y) = \ldots = g_{i-1}(y) = 0 \neq g_i(y)\}$. *If* A *is in addition a radical, then (6) holds for all positive* $m, m_1, \ldots, m_s$.

Proof. By lemma 2 $V(A : B^m) = \{y \in V(A) \mid \ \exists b \in B : b(y) \neq 0\}$. Therefore, using $B = (g_1, \ldots, g_s)$,

$$\begin{aligned} V(A : B^m) &= \{y \in V(A) \mid \exists i \leq s : g_i(y) \neq 0\} \\ &= \textstyle\bigcup_{i=1}^{s} \{y \in V(A) \mid g_1(y) = \ldots = g_{i-1}(y) = 0 \neq g_i(y)\}. \end{aligned}$$

Since $A \subseteq A + (g_1, \ldots, g_{i-1})$, we get by lemma 2 (with $A + (g_1, \ldots, g_{i-1})$ in place of B)

$$V(A + (g_1, \ldots, g_{i-1})) = \{y \in V(A) \mid g_k(y) = 0 \text{ for all } 1 \leq k \leq i-1\}$$

and (with $A + (g_1, \ldots, g_{i-1})$ in place of A and $A + (g_1, \ldots, g_i)$ in place of B implying $A : B^{m_i} = A : g_i^{m_i}$)

$$V((A + (g_1, \ldots, g_{i-1})) : g_i^{m_i}) = \{y \in V(A + (g_1, \ldots, g_{i-1})) \mid g_i(y) \neq 0\}$$

Hence the varieties $V((A + (g_1, \ldots, g_{i-1})) : g_i^{m_i})$ are disjoint and their union equals $V(A : B^m)$.
If $A = \sqrt{A}$, then $A + (g_1, \ldots, g_{i-1})$ is a radical, too. Hence all applications of lemma 2 can by lemma 1 already done with arbitrary positive integers $m, m_1, \ldots, m_s$.

3. Ideal quotients and Gröbner bases

In section 2 we described the decomposition of a variety into varieties of ideals of type $A : g^m$, m sufficiently large. Since the ascending chain

$$A \subset A : g \subset A : g^2 \subset \ldots$$

terminates ($\mathcal{P}$ is Noetherian), there is a least k with $A : g^{k-1} \subset A : g^k = A : g^{k+1}$. (By arguments from ideal theory this implies $A : g^k = A : g^{k'}$ for all $k' > k$.) m sufficiently large means $m \geq k$. We will call this $A : g^k$ the *saturation of* $A : g$ and k its *saturation index.*

We need the computation of bases for the saturations of $(A+(g_1, \ldots, g_{i-1})) : g_i$, $i = 1, \ldots, s$. This computation is easier, when a Gröbner basis for $A + (g_1, \ldots, g_{i-1})$ is already known. Therefore, we prefer to have an algorithm which, given a Gröbner basis of an ideal A_i, computes simultaneously a Gröbner basis for the next $A_{i+1} := A_i + (g_i)$ and a Gröbner basis of the saturation of $A_i : g_i$, where with respect to the application in section 2, we are content of getting a basis of the saturation instead of a Gröbner basis. Having a careful look at a method proposed by Gianni et al. [3], we will see that a minor modification of this method satisfies our requirements.

First we want to remind the most important notions of Gröbner basis techniques, by which many problems like membership problem, ideal equality, etc. can be decided constructively cf. Buchberger [2]. We need some of these techniques slightly more generalized. Therefore, we formulate them in terms of modules in $\mathcal{P}^s$ as in [9], including the polynomials case [2] as a subcase. Denoting by T the set of terms $x_1^{i_1} \cdots x_n^{i_n}$, $i_1, \ldots, i_n$ nonnegative integers, the set of module-terms $T^{(s)}$ is the set of all te_i, $t \in T$, e_i the i-th canonical unit vector of $\mathcal{P}^s$. Having T equipped with a so called *admissible* order $<_T$, i. e. an order, which is compatible with multiplication and with $1 \leq_T t$ for all terms t, then we can introduce an order in $T^{(s)}$ with $te_i < ue_i$ if $t <_T u$ and $vte_i < vue_j$ if $te_i < ue_j$. Every nonzero s-tuple $f \in \mathcal{P}^s$ has a maximal module-term (w.r.t.$<$), the leading module-term, $lt(f)$. Its coefficient is the leading coefficient, $lc(f)$. The modular generalization of an S-polynomial is for two nonzero $f, g \in \mathcal{P}^s$ defined by

$$S(f,g) := \frac{l.c.m.\{lt(f), lt(g)\}}{lt(f)lc(f)} f - \frac{l.c.m.\{lt(f), lt(g)\}}{lt(g)lc(g)} g.$$

It is defined only for those f, g for which $lt(f) = te_i$ and $lt(g) = t'e_j$ with $i = j$, because only in this case their leading terms have a least common multiple.

The reduction of $0 \neq f \in \mathcal{P}^s$ modulo a given set of s-tuples $F := \{f_1, \ldots, f_r\}$, $0 \notin F$, is defined by $f \longrightarrow_F g := f - \frac{lt(f)}{lc(f_i)lt(f_i)} f_i$ if $f_i \in F$ and $lt(f_i)$ divides $lt(f)$. By $\longrightarrow_F^*$ we denote the transitive reflexive closure of $\longrightarrow_F$. Every module $A \subseteq \mathcal{P}^s$ has a *Gröbner basis* which is a set $F := \{f_1, \ldots, f_r\}$, $0 \notin F \subset A$, such that the leading term of every $0 \neq f \in A$ is a multiple of an $lt(f_i)$, $f_i \in F$. A Gröbner basis

F is called *reduced*, if no $lt(f_i)$ divides an other $lt(f_j)$, $f_i, f_j \in F$. (The definition of Gröbner bases shows, that a reduced Gröbner basis is obtained from a Gröbner basis simply by cancelling elements with a leading term being a multiple of an other one.)

An equivalent definition for Gröbner bases is, that for every $f \in \mathcal{P}^s$ there exists a uniquely (by f and $<_T$) determined $g \in \mathcal{P}^s$ with $f \longrightarrow_F^* g$ and g irreducible, i. e. $g \longrightarrow_F^* h$ implies $g = h$. In this context, g is called the *normalform* of f, $NF(f, <_T)$ for short. Another equivalent definition for Gröbner bases is that $S(f,g) \longrightarrow_F^* 0$ for all $f, g \in F$. On this condition Buchberger's algorithm for polynomial ideals and its generalization to modules is based. It computes from a given module basis a Gröbner basis w.r.t. the preassigned order $<$ by calculating the $S(f,g)$ for the pairs (f,g) from the actual set F and reducing it modulo F until no further reduction modulo F can be performed. If the result is a nonzero s-tuple h, then the algorithm is continued with $F' := F \cup \{h\}$ as new F, i.e. with the calculation of the $S(f,g)$, $f, g \in F'$, and their reduction modulo F'. The algorithm terminates and the final F is a Gröbner basis.

Lemma 4. *Let* $A = (a_1, \ldots, a_r)$ *be an ideal and* $0 \neq g \in \mathcal{P}$. *Then*

$$M := \{(u,v) \in \mathcal{P}^2 \mid u + g \cdot v \in A\}$$

is a module with basis $\{(a_1, 0), \ldots, (a_r, 0), (g, -1)\}$. *If* $\pi_i : M \longrightarrow \mathcal{P}$ *denotes the canonical projection on its i-th component,* $i = 1, 2$, *then*

$$\pi_1(M) = A + (g), \quad \pi_2(ker\pi_1) = A : g. \tag{7}$$

Proof. Obviously $(a_i, 0) \in M$ and $(g, -1) \in M$. Let $(u,v) \in M$. Then there are $h_1, \ldots, h_r \in \mathcal{P}$ with $u + g \cdot v = \sum h_i a_i$. Therefore,

$$(u,v) = \sum h_i \cdot (a_i, 0) + (-v) \cdot (g, -1).$$

This is the basis property. Considering the projection of the basis elements, we get $\pi_1(M) = A + (g)$, and using $(0,v) \in M \Leftrightarrow gv \in A \Leftrightarrow v \in A : g$, we get $\pi_2(ker\pi_1) = A : g$.

Algorithm for Gröbner bases computation of $A + (g)$ and $A : g$.

Input: A basis $\{a_1, \ldots, a_r\}$ of A, a $0 \neq g \in \mathcal{P}$ and an admissible order $<_T$.

Output: A Gröbner basis G_1 of $A + (g)$ and G_2 of $A : g$, both w.r.t. $<_T$.

Step 1: Define for module-terms in $\mathcal{P}^2$ an order $<$ by $te_i < t'e_j$, if $i = 2, j = 1$ or $i = j \in \{1, 2\}$, $t <_T t'$.

Step 2: Compute a Gröbner basis G w.r.t. $<$ for the module M generated by $(a_1, 0), \ldots, (a_r, 0), (g, -1)$.

Step 3: Let $\pi_i : M \longrightarrow \mathcal{P}$ be the canonical projection on the i-th component, $i = 1, 2$, then $G_1 := \pi_1(G)$ and $G_2 := \pi_2(\{(u, v) \in G \mid u = 0\})$.

The correctness follows easily from the observation $lt(u, v) = lt(u)$ if $u \neq 0$, and $lt(0, v) = lt(v)$ if $v \neq 0$.

The Gröbner basis of $A : g$ can be used as new input, giving Gröbner bases of $A : g^2$ and $A : g + (g)$. Then using the Gröbner basis of $A : g^2$ as input, the alg. gives Gröbner bases for $A : g^3$ and $A : g^2 + (g)$, etc. This procedure can be iterated until we get $A : g^k = A : g^{k+1}$, i.e. until the saturation and its index are found. There are two observations which accelerate this recursive Gröbner basis computation. If $\{a'_1, \ldots, a'_{s'}\}$ is the obtained Gröbner basis for $A : g^i$, then in the next application of Buchberger's algorithm, we know that all $(0, a'_i)$ belong to the actual module M. Hence we may use as input all $(a'_i, 0)$, all $(0, a'_i)$ and $(g, -1)$. And at the beginning of the next loop only the "S-polynomials" $S((a'_i, 0), (g, -1))$ have to be built and reduced, because the "S-polynomials" $S((a'_i, 0), (a'_j, 0))$ and $S((0, a'_i), (0, a'_j))$ reduce to $(0, 0)$, since the a'_i are a Gröbner basis.

Introducing a new variable x_o and using the bijection $(u, v) \longleftrightarrow x_o \cdot u + v$, the Gröbner basis calculation in step 2 of the algorithm can be seen in principle as Buchberger's algorithm applied to $x_o a_1, \ldots, x_o a_r, x_o g - 1$, where although the input polynomials belong to $I\!K[x_o, \ldots, x_n]$ only multiplications with terms of $T \subset I\!K[x_1, \ldots, x_n]$ in the S-polynomial computations and in the reductions are admitted, i.e. only those $S(f_i, f_j)$ are considered, where f_i, f_j either both contain x_0 or both don't, and in $f \longrightarrow_F g := f - \frac{lt(f)}{lc(f_i)lt(f_i)} f_i$ the term $\frac{lt(f)}{lt(f_i)}$ does not contain x_0. Using the output Gröbner basis $\{a'_1, \ldots, a'_{s'}\}$ as input for the computation of a Gröbner basis for $A : g^2$ means in the same way multiplication of all a'_i by x_o and then using them together with $x_o g - 1$ as input for the modified Buchberger algorithm.

The connection of this procedure to the method in [3] is now apparent. In [3], Buchberger's algorithm is applied to $a_1, \ldots, a_s, x_o g - 1$ in $I\!K[x_o, \ldots, x_n]$. At first, the S-polynomial computations for the pairs $(x_o g - 1, a_i)$ require multiplication of all a_i by x_o, since $S(a_i, x_o g - 1) = S(x_o a_i, x_o g - 1)$. At termination, the Gröbner basis elements not depending on x_o are a Gröbner basis for the saturation of $A : g$, w.r.t. $<_T$, if the order $<$ for terms in $x_o, x_1, \ldots, x_n$ satisfies $x_o^{i_o} t < x_o^{j_o} t'$ if $i_o < j_o$ or ($i_o = j_o$ and $t <_T t'$) for terms $t, t' \in T$. Hence, in contrast to our variant, multiplications with x_o are allowed without restrictions. Therefore, both methods are essentially the same, differing only by the book-keeping to what $A : g^i$ or $A : g^i + (g)$ the actually considered polynomial belong.

The presented computation of a Gröbner basis for $A : g$ holds for ideals A of arbitrary dimension. There is also a linear method, which is applicable, when A is zero-dimensional and is given by a Gröbner basis (w.r.t. an arbitrary admissible order $<_1$.) Then $\mathcal{P}/A$ is an s-dimensional $I\!K$-vector space and the equivalence classes consists of all polynomials f having the same normalform $NF(f, <_1)$.

Take the terms $t \in T$ in increasing order $<_T$. Denote this ordered set S. Calculate $NF(t \cdot g, <_1)$ until the first $t \in S$ is found such that $NF(t \cdot g, <_1)$ depends linearly on preceding normalforms $NF(t' \cdot g, <_1)$, $t' \in S$, i.e. $NF(t \cdot g, <_1) = \sum c(t')NF(t' \cdot g, <_1)$. Then $t - \sum c(t')t' \in A : g$. Modify S by removing this t and all its multiples. Then look again for the first $t \in S$, such that $NF(t \cdot g, <_1)$ depends linearly on some preceding $NF(t' \cdot g, <_1)$, $t' \in S$. This gives an additional $t - \sum c(t')t' \in A : g$. Then this t and its multiples are removed from S etc. This procedure terminates, since otherwise the monomial ideal generated by all t which are once removed from S has no finite basis. And by construction, there is no $f \in A : g$ having a leading term (w.r.t. $<_T$) which is no multiple of the leading term of a $t - \sum c(t')t'$ found in the algorithm. This means that these $t - \sum c(t')t'$ constitute a Gröbner basis of $A : g$ w.r.t. $<_T$. For a more detailed exposition and proof of this algorithm, readers are referred for instance to [7], where the FGLM-method is discussed which is the special instance $g = 1$ of the method presented here. The additional computational amount of this FGLM-generalization stems from dealing with normalforms $NF(t \cdot g, <_1)$ instead of $NF(t, <_1)$. The complexity analysis of the FGLM-method in [7] uses heavily a recursion relation $NF(x_k t, <_1) = NF(x_k NF(t, <_1), <_1)$, but apart of $NF(1, <_1) = 1$ the authors of [7] never used special simplifications arising from the fact $t \in T$. Therefore only the initial computation of $NF(1 \cdot g, <_1)$ could give a complexity surpassing $O(s^3)$. But in most applications, like the algorithm of the next section, $g = NF(g, <_1)$ holds, which means no additional amount to the $O(s^3)$-complexity.

A method, similar to those in [7], can be used for the computation of a lexicographical Gröbner basis of $A + (g)$, when a lexicographical Gröbner basis for the ideal A with $dim(\mathcal{P}/A) = s$ is given. It requires first the computation of a generalization of a Gröbner basis, a so called border basis. Such basis consists of $b \leq n \cdot s$ elements and contains the given Gröbner basis. A careful analysis shows that the calculation of a border basis of $A + (g)$ requires at most $s^2(n + 2)(b + s) = O(s^3)$ additions and multiplications.

4. Decomposition into triangular systems

Definition 1. Let $\{y_1, \ldots, y_r\}$ and $\{z_1, \ldots, z_s\}$ be disjoint subsets of $\{x_1, \ldots, x_n\}$. Then $\{y_1, \ldots, y_r\}$ will be called *lexicographically in front of* $\{z_1, \ldots, z_s\}$ *with respect to* $<_T$, if for arbitrary terms the following implication holds.

$$y_1^{i_1} \cdots y_r^{i_r} <_T y_1^{j_1} \cdots , y_r^{j_r} \Longrightarrow y_1^{i_1} \cdots y_r^{i_r} z_1^{k_1} \cdots z_s^{k_s}. <_T y_1^{j_1} \cdots y_r^{j_r} z_1^{l_1} \cdots z_s^{l_s} \qquad (8)$$

This definition is useful for combining orders which order sets of terms for disjoint sets of variables. A special instance is the lexicographical order, where every $\{x_i\}$

is in front of $\{x_1, \ldots, x_{i-1}\}$, $i = 2, \ldots, n$. For deriving special properties of this lexicographical order, we show the following result.

Lemma 5. *Let x_n be lexicographically in front of $\{x_1, \ldots, x_{n-1}\}$ w.r.t. $<_T$ and let $deg_{x_n}(f)$ denote the degree of f in x_n. The the following assertions hold.*

i) If $f_1, \ldots, f_r$ are polynomials with $deg_{x_n}(f_i) \leq d$, $i = 1, \ldots, r$, then $(f_1, \ldots, f_r)$, has a Gröbner basis w.r.t. $<_T$, where every element f satisfies $deg_{x_n}(f) \leq d$.

ii) If $F := \{f_1, \ldots, f_r\}$ is a Gröbner basis w.r.t. $<_T$, then $F_k := F \cap \{f \in \mathcal{P} \mid deg_{x_n}(f) < k\}$ is a Gröbner basis (w.r.t. $<_T$) for all positive integers k.

iii) Let $f_i := \sum_{j=0}^{d_i} \tilde{g}_{ij}(x_1 \ldots, x_{n-1}) x_n^{d_i - j}$ with nonzero polynomials $\tilde{g}_{io}$, $i = 1, \ldots, r$. If $F := \{f_1, \ldots, f_r\}$ is a Gröbner basis w.r.t. $<_T$, then $G := \{\tilde{g}_{1o}, \ldots, \tilde{g}_{ro}\}$ is a Gröbner basis (w.r.t. $<_T$).

Proof. Using F as input for Buchberger's algorithm, we observe, that if no polynomial in the input has a degree in x_n greater than d, then this holds true for all polynomials in the algorithm. This follows from $deg_{x_n}(f) = deg_{x_n}(lt(f))$ and therefore $deg_{x_n}(S(f,g)) \leq \max\{deg_{x_n}(f), deg_{x_n}(g)\}$. And in the reduction $f \longrightarrow_F g := f - \frac{lt(f)}{lc(f_i) lt(f_i)} f_i$ also $deg_{x_n}(g) \leq deg_{x_n}(f)$ holds because $g = lc(f) \cdot S(f, f_i)$ and $lt(f_i)$ divides $lt(f)$. This proves i).
If F is a Gröbner basis, then $S(f,g) \longrightarrow_F^* 0$ for all $f, g \in F_k$. But every f_i involved in the reduction of $S(f,g)$ to 0 satisfies $deg_{x_n}(f_i) < k$ by the same arguments as before. Hence $S(f,g) \longrightarrow_{F_k}^* 0$, i.e. F_k is already a Gröbner basis. This proves ii).
If F is a Gröbner basis, then observing only the reduction of terms of highest degree in x_n in $S(f_i, f_j) \longrightarrow_F^* 0$, we get $S(\tilde{g}_{io}, \tilde{g}_{jo}) \longrightarrow_G^* 0$. This proves iii).

This lemma shows that, having one lexicographical Gröbner basis $F := \{f_1, \ldots, f_r\}$, we can read off many other lexicographical Gröbner bases from F. For instance, when the f_i are ordered by $lt(f_j) <_T lt(f_i)$, if $i > j$, and when, for a given s, f_i is the only polynomial in $F \cap I\!\!K[x_1, \ldots, x_k]$ with $deg_{x_k}(f_i) = s$, then $\{f_i, f_{i+1}, \ldots, f_r\}$ and $\{f_{i+1}, \ldots, f_r\}$ are both lexicographical Gröbner bases.

Example 1. Let $\mathbb{Q}$ be the field of rationals, $\mathcal{P} := \mathbb{Q}[x_1, x_2, x_3, x_4]$, and $<_T$ the lexicographical order with $x_1 <_T x_2 <_T x_3 <_T x_4$. A lexicographical Gröbner basis of an ideal, introduced by A. Björck and called "Arnborg4", is $\{f_1, \ldots, f_6\}$ with

$$\begin{aligned}
f_1 &:= x_4 + x_3 + x_2 + x_1, \\
f_2 &:= x_3^2 + 2x_3x_1 + x_1^2, \\
f_3 &:= x_3x_2 - x_3x_1 + x_2^2x_1^4 + x_2x_1 - 2x_1^2, \\
f_4 &:= x_3x_1^4 - x_3 + x_1^5 - x_1, \\
f_5 &:= x_2^3x_1^2 + x_2^2x_1^3 - x_2 - x_1, \\
f_6 &:= x_2^2x_1^6 - x_2^2x_1^2 - x_1^4 + 1.
\end{aligned} \tag{9}$$

Then $\{f_2, f_3, f_4, f_5, f_6\}$, $\{f_3, f_4, f_5, f_6\}$, $\{f_5, f_6\}$ and $\{f_6\}$ are also Gröbner bases by lemma 5ii). Applying lemma 5iii) on these five bases gives in addition lexicographical (not-reduced) Gröbner bases, which are after reduction $\{1\}$ (from $\{f_1, \ldots, f_6\}$ and $\{f_2, \ldots, f_6\}$), $\{x_2 - x_1, x_1^4 - 1\}$ (from $\{f_3, f_4, f_5, f_6\}$,) $\{x_1^2\}$, and $\{x_1^6 - x_1^2\}$.

Example 2. Let $\mathcal{P} := \mathbb{Q}[x_1, x_2, x_3]$, and $<_T$ the lexicographical order with $x_1 <_T x_2 <_T x_3$. The set $\{f_1, f_2, f_3, f_4\}$ with

$$\begin{aligned} f_1 &:= x_3^2 + x_3 + x_2 - 1, \\ f_2 &:= x_3x_2 + x_3x_1 + x_3 + x_2x_1 + x_1 + 2, \\ f_3 &:= x_2^2 + 2x_2 - 1, \\ f_4 &:= x_1^2 - 2, \end{aligned} \tag{10}$$

is a lexicographical Gröbner basis. Then, by lemma 5ii), $\{f_2, f_3, f_4\}$, $\{f_3, f_4\}$, and $\{f_4\}$ are lexicographical Gröbner bases, too, and by lemma 5iii) after reduction, $\{1\}$, and $\{x_2 + x_1 + 1, x_1^2 - 2\}$ (from $\{f_2, f_3, f_4\}$) as well.

Lemma 6. *Let A be a zero-dimensional ideal and G a Gröbner basis of A. Then there exists for every $i = 1, \ldots, n$ an $f_i \in G$ and an integer $k_i > 0$, such that $lt(f_i) = x_i^{k_i}$.*

Proof. As zero-dimensional ideal, A contains for every x_i a polynomial univariate in x_i. Its leading term, a pure power of x_i, is a multiple of the leading term of an $f_i \in G$ by the definition of Gröbner bases.

Lemma 7. *Let $G = \{f_1, \ldots, f_r\}$ be a reduced Gröbner basis with respect to an order $<_T$, where x_n is lexicographically in front of$\{x_1, \ldots, x_{n-1}\}$,*

$$f_i := \sum_{j=0}^{d_i} \tilde{g}_{ij}(x_1, \ldots, x_{n-1}) x_n^{d_i - j} \tag{11}$$

with nonzero polynomials $\tilde{g}_{io}$, $i = 1, \ldots, r$, and $lt(f_r) <_T \ldots <_T lt(f_1)$. If g_{1o} is constant, then $(f_2, \ldots, f_r) : f_1$ has the Gröbner basis (w.r.t.$<_T$) $\{\tilde{g}_{2o}, \ldots, \tilde{g}_{ro}\}$ and $f_1 \notin (f_2, \ldots, f_r)$.

Remark. If $\{f_1, \ldots, f_r\}$ generate a zero-dimensional ideal, then $\tilde{g}_{1o}$ is a constant, because by lemma 6 there is an f_i with $lt(f_i) = x_n^{k_i}$ which is f_1 by the numbering of the polynomials.

Proof. Let $\tilde{g}_{1o} = 1$. Because of the numbering of the f_i and because G is reduced, $d_1 > \max\{d_2, \ldots, d_r\}$ holds. Consider $h_i := \tilde{g}_{io} \cdot f_1 - x_n^{d_1 - d_i} f_i$, $1 < i \leq r$. Because of $lt(h_i) <_T lt(f_1)$ and $h_i \in (f_1 \ldots, f_r)$, the leading term is a multiple of an $lt(f_j), j > 1$. Hence for a suitable $p_i \in \mathcal{P}$: $h_i' := h_i - p_i f_j$ is in $(f_1, \ldots, f_r)$ and $lt(h_i') <_T lt(h_i) <_T lt(f_1)$. Analogously with h_i' in place of h_i we find an $h_i'' \in (f_1, \ldots, f_r)$, $lt(h_i'') <_T lt(h_i') <_T lt(h_i) <_T lt(f_1)$, etc. This reduction procedure terminates, since $\mathcal{P}$ is Noetherian, with 0. The difference of every two consecutive members of this reduction chain are in $(f_2, \ldots, f_r)$, the last one being 0.

Hence $h_i \in (f_2, \ldots, f_r)$. Therefore also $\tilde{g}_{io} \cdot f_1 \in (f_2, \ldots, f_r)$. This implies

$$(\tilde{g}_{2o}, \ldots, \tilde{g}_{ro}) \subseteq (f_2, \ldots, f_r) : f_1.$$

Take now a $g \cdot f_1 \in (f_2, \ldots, f_r)$, $0 \neq g \in \mathcal{P}$. It has a leading term, which is a multiple of an $lt(f_i)$, $i > 1$, since $\{f_2, \ldots, f_r\}$ is a Gröbner basis by lemma 5ii), i.e.

$$lt(g) x_n^{d_1} \in (lt(\tilde{g}_{2o}) x_n^{d_2}, \ldots, lt(\tilde{g}_{ro}) x_n^{d_r}).$$

Therefore, $lt(g) lt(f_1)$ is a t-fold multiple, $t \in T$, of an $lt(\tilde{g}_{io}) lt(f_1)$, $1 < i \leq r$. Hence, for a suitable $c \in I\!\!K$, $g' f_1 := g f_1 - c \cdot t \cdot \tilde{g}_{io} f_1$, such that $g' f_1 \in (f_2, \ldots, f_r)$ and $lt(g') <_T lt(g)$ or $g' = 0$, allowing again an inductive argument. Therefore

$$g f_1 \in (\tilde{g}_{2o} f_1, \ldots, \tilde{g}_{ro} f_1). \tag{12}$$

This means $g \in (\tilde{g}_{2o}, \ldots, \tilde{g}_{ro})$ if $g \in (f_2, \ldots, f_r) : f_1$. In other words $(f_2, \ldots, f_r) : f_1 = (\tilde{g}_{2o}, \ldots, \tilde{g}_{ro})$, where by lemma 5iii) $\{\tilde{g}_{2o}, \ldots, \tilde{g}_{ro}\}$ is a lexicographical Gröbner basis.
$\{f_2, \ldots, f_r\}$ is Gröbner basis by lemma 5ii), and $lt(f_1)$ is no multiple of an $lt(f_i)$, $i > 1$.
Therefore $f_1 \notin (f_2, \ldots, f_r)$.

For formulating the main algorithm, we need two technical definitions. By $<_k$ we will denote the lexicographical order of terms in $x_1, \ldots, x_k$ with $x_1 <_k \ldots <_k x_k$. And $\mathrm{SAT}(G, g, <_k)$ denotes the saturation of $A : g$, where G is a Gröbner basis w.r.t. $<_k$ and A the ideal generated by G.

Algorithm for decomposing zero-dimensional varieties.

Input: $(\{f_1, \ldots, f_r\}; <_n)$, where $\{f_1, \ldots, f_r\}$ is a reduced Gröbner basis w.r.t. $<_n$ of a zero-dimensional ideal A.

Output: A set Z of finitely many polynomial sets $\{g_1, \ldots, g_n\}$ of triangular type (3), such that $V(A)$ is the union of the disjoint sets $V(g_1, \ldots, g_n)$, $\{g_1, \ldots, g_n\} \in Z$.

Step 1: Let $lt(f_j) <_n lt(f_i)$ for $i > j$. Let $\tilde{f}_i := lc_{x_n}(f_i) \in I\!\!K[x_1, \ldots, x_{n-1}]$ denote the leading coefficient of f_i considered as polynomial in x_n, $i > 1$. Let $G_1 := \{f_1, \ldots, f_r\}$. Reduce the lexicographical Gröbner basis $\{\tilde{f}_2, \ldots, \tilde{f}_r\}$ to a Gröbner basis G.

Step 2: Call the alg. with input $(G; <_{n-1})$, resulting in a set Z' of finitely many sets $\{\tilde{g}_1, \ldots, \tilde{g}_{n-1}\}$. Let then Z denote the set of all polynomials $\{\tilde{g}_1, \ldots, \tilde{g}_{n-1}, \frac{1}{lc(f_1)} f_1\}$, $\{\tilde{g}_1, \ldots, \tilde{g}_{n-1}\} \in Z'$.

Step 3: For $i = 2, \ldots, r$ do while $\tilde{f}_i \notin A$:
Compute a Gröbner basis G_i' of $\mathrm{SAT}(G_{i-1}, \tilde{f}_i, <_n)$ and a Gröbner basis G_i of $(f_1, \ldots, f_r, \tilde{f}_2, \ldots, \tilde{f}_i)$, both w.r.t. the order $<_n$, call then the algorithm with input $(G_i'; <_n)$, and enlarge Z by the resulting triangular sets.

For proving correctness and termination of this alg., let $B := (f_2, \ldots, f_r) : f_1 + (f_1)$. Since $f_i \in (f_2, \ldots, f_r) \subseteq (f_2, \ldots, f_r) : f_1,\ i = 2, \ldots, r$, we have $A \subseteq B$. By lemma 7, $\{f_1, \tilde{f}_2, \ldots, \tilde{f}_r\}$ generates B and the $\tilde{f}_i,\ i > 1$, depend only on $x_1, \ldots, x_{n-1}$ and constitute a lex. Gröbner basis. Using $V(B) = V(f_1) \cap V(\tilde{f}_2, \ldots, \tilde{f}_r) = V(f_1) \cap V(G)$, G a reduced Gröbner basis of $(\tilde{f}_2, \ldots, \tilde{f}_r)$, and assuming that correctness and termination are already proved for the $n-1$-variate algorithm, we see that in step 2 the required decomposition is performed for $V(B)$.

By lemma 3, the variety of the saturation of $A : B$ is the disjoint union of the varieties

$$V(A : f_1^{m_1}),\ V((A + (f_1)) : \tilde{f}_2^{m_2}), \ldots, V((A + (f_1, \tilde{f}_2, \ldots, \tilde{f}_{r-1})) : \tilde{f}_r^{m_r})$$

again with sufficiently large $m_i, i = 1, \ldots, r$. Because of $f_1 \in A$, the first variety is empty, and $A + (f_1) = A$. Hence $V(A : B^m)$ is the disjoint union of

$$V(A : \tilde{f}_2^{m_2}),\ V((A + (\tilde{f}_2)) : \tilde{f}_3^{m_3}), \ldots, V((A + (\tilde{f}_2, \ldots, \tilde{f}_{r-1})) : \tilde{f}_r^{m_r}),$$

where empty varieties may be omitted. For instance $(A + (\tilde{f}_2, \ldots, \tilde{f}_{i-1})) : \tilde{f}_i^{m_i}$ is $\mathcal{P}$ with an empty variety, if $\tilde{f}_i \in A$. By construction, $\tilde{f}_i$ belongs to A, if and only if $deg_{x_n}(f_i) = 0$. The ordering of the f_i in step 1 implies then that there is a k, such that $\tilde{f}_i \notin A$ if and only if $i \leq k$. Therefore, in step 3 all nontrivial varieties are computed, such that their union is $V(A : B^m)$.

For termination, we remark that A is a proper subset of the saturation of $A : B$. This follows from the disjoint union $V(A) = V(B) \cup V(A : B^m)$ and $V(B)$ not empty because otherwise $1 \in (f_2, \ldots, f_r) : f_1$ in contradiction to $f_1 \notin (f_2, \ldots, f_r)$ by lemma 7. Hence A is a proper subset of all $\mathrm{SAT}(G_{i-1}, \tilde{f}_i, <_n) \supseteq A : B^m$. If we know, that the algorithm terminates when applied to ideals in $I\!\!K[x_1, \ldots, x_{n-1}]$ and to ideals which contain properly A, then an inductive argument proves termination of the algorithm applied to A, since $I\!\!K[x_1, \ldots, x_n] = \mathcal{P}$ is Noetherian.

The result of the algorithm can be summarized in the following.

Theorem. *Let $f_1, \ldots, f_r$ be polynomials in $I\!\!K[x_1, \ldots, x_n]$ with only finitely many common zeros. Then the set $V(f_1, \ldots, f_r)$ of these zeros is the disjoint union of finitely many sets $V(g_1, \ldots, g_n)$, obtained by the decomposition algorithm, where*

$$\begin{array}{rll} g_1 = & x_1^{d_1} + \sum_{j=1}^{d_1-1} a_j x_1^j & \in I\!K[x_1], \\ g_2 = & x_2^{d_2} + \sum_{j=1}^{d_2-1} g_{2,j}(x_1) x_2^j & \in I\!K[x_1, x_2], \\ & \cdots & \\ g_n = & x_n^{d_n} + \sum_{j=1}^{d_n-1} g_{n,j}(x_1, \ldots, x_{n-1}) x_n^j & \in I\!K[x_1, \ldots, x_n]. \end{array} \tag{13}$$

5. Examples

Termination and correctness of the algorithm is only shown here for zero-dimensional ideals. For A with $dim(A) \neq 0$ we may decompose $V(A)$ by lemma 1 into $V(B) \cup V(A : B^m)$ where (as in the algorithm for decomposing zero-dimensional ideals) $B := (f_2, \ldots, f_r) : f_1 + (f_1)$ and $\{f_1, \ldots, f_r\}$ a lexicographical Gröbner basis of A with $lt(f_i) <_T lt(f_1)$ for $i > 1$. Sometimes this decomposition is an improper one, $V(A) = V(A : B^m)$. We have installed an early version of this algorithm in REDUCE 3.4 as procedure GROEPOSTPROC, see Melenk et al. [8]. There we allow lexicographical Gröbner bases of arbitrary ideals as input and interrupt the algorithm, when we arrive at an improper decomposition. Then we choose a different lexicographical order, i.e. we renumber the variables, and start the algorithm anew. After a finite number of trials, we get in any case a proper decomposition. The reason for this successful decomposition is roughly said that, when we start with an order where the first d variables constitute a maximal set of independent variables, then the ideal A can be considered as a zero-dimensional ideal in $I\!K(x_1, \ldots, x_d)[x_{d+1}, \ldots, x_n]$. However, a detailed description and proof of this procedere goes beyond the aim of this paper.

Let us finally consider how the decomposition algorithm works, when applied on the bases considered in the examples 1 and 2.

Example 1 (cont.) As before, we have

$$\begin{array}{rcl} f_1 & := & x_4 + x_3 + x_2 + x_1, \\ f_2 & := & x_3^2 + 2x_3x_1 + x_1^2, \\ f_3 & := & x_3x_2 - x_3x_1 + x_2^2x_1^4 + x_2x_1 - 2x_1^2, \\ f_4 & := & x_3x_1^4 - x_3 + x_1^5 - x_1, \\ f_5 & := & x_2^3x_1^2 + x_2^2x_1^3 - x_2 - x_1, \\ f_6 & := & x_2^2x_1^6 - x_2^2x_1^2 - x_1^4 + 1. \end{array}$$

Although the input ideal is no radical, $f_2 = (x_3 + x_1)^2$, in the algorithm all saturation indices turn out to be equal to 1.
The first call of the algorithm is with input $(\{f_1, \ldots, f_6\}, <_4)$:

STEP 1 (No calculation, only application of lemma 7): $\tilde{f}_i = f_i,\ i = 2, \ldots, 6.$

STEP 2 Call the alg. with $(\{f_2, \dots, f_6\}, <_3)$ and append f_1 to all resulting triang. sets.

STEP 3 Empty loop.

The call with input $(\{f_2, \dots, f_6\}, <_3)$ gives

STEP 1 (No calculation, only application of lemma 7): $\{\tilde{f}_3, \dots, \tilde{f}_6\} = \{x_2 - x_1, x_1^4 - 1, f_5, f_6\}$. Reduction of this Gröbner basis (=cancellation of redundant polynomials) to $\{x_2 - x_1, x_1^4 - 1\}$.

STEP 2 Call the alg. with input $(\{x_2 - x_1, x_1^4 - 1\}, <_2)$ resulting in $\{\{x_1^4 - 1, x_2 - x_1\}\}$. Append f_2. This gives $\{\{x_1^4 - 1, x_2 - x_1, x_3^2 + 2x_3x_1 + x_1^2\}\}$.

STEP 3 Because of $(f_2, \dots, f_6) : (x_2 - x_1) = (2x_3 - x_2^2x_1^3 + 3x_1, f_5, f_6)$, the algorithm is called with $(\{2x_3 - x_2^2x_1^3 + 3x_1, f_5, f_6\}, <_3)$. Then $(f_2, \dots, f_6, x_2 - x_1) : (x_1^4 - 1) = (1)$ with no call (empty variety).

The call with input $(\{2x_3 - x_2^2x_1^3 + 3x_1, f_5, f_6\}, <_3)$ gives in analogy to the first call a call with input $(\{f_5, f_6\}, <_2)$, where $2x_3 - x_2^2x_1^3 + 3x_1$ is appended to all resulting triangular sets.

The call with input $(\{f_5, f_6\}, <_2)$:

STEP 1 Lemma 7 not applicable since $lt_{x_2}(f_5) = x_1^3$. This step computes B. We get here $B = (f_5, x_1^4 - 1)$ because $(f_6) : f_5 = (x_1^4 - 1)$.

STEP 2 Since $\{x_1^4 - 1\}$ is already ”triangular”, this step returns $\{x_1^4 - 1, f_5\}$.

STEP 3 $(f_5, f_6) : (x_1^4 - 1) = (x_2^2x_1^2 - 1)$. Here no further decomposition is possible. Hence $\{x_2^2x_1^2 - 1\}$ is returned unchanged.

In total the algorithm returns $\{S_1, S_2, S_3\}$ with

$$\begin{aligned}
S_1 &:= \{x_1^4 - 1, x_2 - x_1, x_3^2 + 2x_3x_1 + x_1^2, x_4 + x_3 + x_2 + x_1\},\\
S_2 &:= \{x_1^4 - 1, x_2^3x_1^2 + x_2^2x_1^3 - x_2 - x_1, x_3^2 + 2x_3x_1 + x_1^2, x_4 + x_3 + x_2 + x_1\},\\
S_3 &:= \{x_2^2x_1^2 - 1, x_3^2 + 2x_3x_1 + x_1^2, x_4 + x_3 + x_2 + x_1\}.
\end{aligned}$$

It should mentioned however, that in REDUCE 3.4 the call of GROEBNERF, which uses the early version of the algorithm, returns the much nicer sets

$$\{x_4 + x_2, x_3 + x_1, x_2x_1 + 1\},$$
$$\{x_4 + x_2, x_3 + x_1, x_2x_1 - 1\},$$

because in GROEBNERF all polynomials from input, such as $f_2 = (x_3 + x_1)^2$, and polynomials obtained by reducing S-polynomials are factorized and for each factor the Groebner basis calculation is continued separately.

Example 2 (cont.) Here, f_1, f_2, f_3, f_4 are

$$\begin{aligned} f_1 &:= x_3^2 + x_3 + x_2 - 1, \\ f_2 &:= x_3x_2 + x_3x_1 + x_3 + x_2x_1 + x_1 + 2, \\ f_3 &:= x_2^2 + 2x_2 - 1, \\ f_4 &:= x_1^2 - 2. \end{aligned}$$

The input ideal is a radical, therefore all saturation indices are equal to 1. The first call of the algorithm is with input $(\{f_1, f_2, f_3, f_4\}, <_3)$:

STEP 1 (No calculation, only application of lemma 7) $\tilde{f}_2 = x_2 + x_1 + 1,\ \tilde{f}_3 = f_3,\ \tilde{f}_4 = f_4$. Cancellation of redundant Gröbner basis elements gives $\{x_2 + x_1 + 1, x_1^2 - 2\}$.

STEP 2 Since the input $\{x_2 + x_1 + 1, x_1^2 - 2\}$ is already triangular, the alg. with input $(\{x_2+x_1+1, x_1^2-2\}, <_2)$ returns this triang. set unchanged. Appending f_1 gives the first triangular set for the ideal (f_1, f_2, f_3, f_4).

STEP 3 The loop is only used once, because $x_1^2 - 1 = f_4$ belongs to (f_1, f_2, f_3, f_4). Then $(f_1, f_2, f_3, f_4) : (x_2 + x_1 + 1) = (x_3 + x_1, x_2 - x_1 + 1, f_4)$. But this is again already triangular. Therefore the algorithm returns $\{f_4, x_2 - x_1 + 1, x_3 + x_1\}$.

In total the algorithm returns the set $\{S_1, S_2\}$ with

$$\begin{aligned} S_1 &:= \{x_1^2 - 2, x_2 + x_1 + 1, x_3^2 + x_3 + x_2 - 1\}, \\ S_2 &:= \{x_1^2 - 2, x_2 - x_1 + 1, x_3 + x_1\}. \end{aligned}$$

Acknowledgement

The work leading to the version of the decomposition algorithm which is already installed in REDUCE 3.4 was done while the author was fellow of the Konrad–Zuse–Zentrum für Informationstechnik in Berlin. He wishes also to express his thanks to Herbert Melenk for discussions and for implementing the early version.

References

1. W. Auzinger and H. J. Stetter: An elimination algorithm for the computation of all zeros of a system of multivariate polynomial equations. ISNM 86, Birkhäuser Verlag, 1988.

2. B. Buchberger: Gröbner bases – an algorithmic method in polynomial ideal theory. In: Progress, direction and open problems in multidimensional systems theory (ed.: N. K. Bose), D. Reidel Publ. Comp., 1985, pp. 184–232.

33 P. Gianni, B. M. Trager, G. Zacharias: Gröbner bases and primary decomposition of polynomial ideals, J. Symb. Comp. 6, 1988, pp. 15–33.

4. J. Hietarinta: Solving the Young-Baxter equation in 2 dimensions with massive use of factorizing Gröbner basis computation. Proceedings of ISSAC '92, to appear.

5. D. Lazard: Solving zero-dimensional algebraic systems. J. Symb. Comp. 13, 1992, pp. 117–131.

6. T. Y. Li: Solving polynomial systems. The Math. Intelligencer 9, 1987, pp. 33–39.

7. M. G. Marinari, H. M. Möller, and T. Mora: Gröbner bases of ideals given by dual bases. Proceedings of ISSAC '91, acm press, pp. 55–63.

8. H. Melenk, H. M. Möller, and W. Neun: GROEBNER, A package for Calculating Groebner Bases. Manual, distributed with REDUCE 3.4, RAND Corporation, 1991.

9. H. M. Möller and T. Mora: New constructive methods in classical ideal theory. J. Algebra 100, 1986, pp. 138–178.

10. J. N. Ortega and W. C. Rheinboldt: Iterative solution of nonlinear equations in several variables. Academic Press, 1970.

11. B. Renschuch: Elementare und praktische Idealtheorie, MfL 16, VEB Deutscher Verlag der Wissenschaften, Berlin, 1976.

12. H. Schwetlick: Numerische Lösung nichtlinearer Gleichungen. Oldenbourg Verlag, 1979.

13. W. Trinks: Über B. Buchbergers Verfahren, Systeme algebraischer Gleichungen zu lösen. J. Number Th. 10, 1978, pp. 475–488.

14. B. L. van der Waerden: Moderne Algebra. Vol. I and II, Springer Verlag, 1966 and 1967.