J. Symbolic Computation (1997) **11**, 1–000

Comprehensive Gröbner Bases

VOLKER WEISPFENNING

Universität Passau, D-8390 Passau, Germany

(Received 5 March 1990)

Let K be an integral domain and let S be the polynomial ring $K[U_1, .., U_m; X_1, .., X_n]$. For any finite $F \subseteq S$, we construct a comprehensive Gröbner basis of the ideal $Id(F)$, i.e. a finite ideal basis of $Id(F)$ that is a Gröbner basis of $Id(F)$ in $K'[X_1, \ldots, X_n]$ for every specialization of the parameters $U_1, \ldots, U_m$ in an arbitrary field K'. We show that this construction can be performed with the same worst case degree bounds in the main variables X_i as for ordinary Gröbner bases ; moreover, examples computed in an ALDES/SAC-2 implementation show that the construction is of practical value. Comprehensive Gröbner bases admit numerous applications to parametric problems in algebraic geometry; in particular, they yield a fast elimination of quantifier-blocks in algebraically closed fields.

1. Introduction

The method of Gröbner bases (or standard bases) is meanwhile well established as one of the fundamental algorithmic tools in polynomial algebra and algebraic geometry (see Buchberger (1985, 1987), Gianni & Mora (1988), Kredel & Weispfenning (1988), Möller & Mora (1986)) It has also been extended to certain non-commutative algebras (see Apel & Lassner (1988), Mora (1985), Mora (1988), Kandri-Rody & Weispfenning (1990), Kredel & Weispfenning (1990). In its basic version, it deals with multivariate polynomials over a field K. It assigns to any finite set $F \subseteq R = K[X_1, ..., X_n]$ another such set G (a **Gröbner basis**) such that G and F generate the same ideal $Id(G) = Id(F)$ in R, and such that many problems related to $Id(F)$ and its zeros in an algebraically closed extension field $\overline{K}$ can be solved algorithmically using G. Thus the computation of G serves as a preprocessing step (of potentially high complexity) in the solution of these problems. The construction of G depends on F and on a **term-order** $<$ on R (see Robbiano (1985), Weispfenning (1987)). If G is taken minimal in a suitable sense (i.e. G is a **reduced Gröbner basis**), then G is even uniquely determined by the ideal $Id(F)$ and by $<$.

The dependence of G on the term-order $<$ is considerable, in particular as far as the complexity of the computation of G is concerned. This dependence can, however, (at least theoretically) be eliminated by the construction of a **universal Gröbner basis** or a **Gröbner fan** (see Mora & Robbiano (1988), Schwartz (1988), Weispfenning (1989a) Schemmel (1989)).

In the present paper we study the dependence of a Gröbner basis G of $Id(F)$ on the coefficients of the polynomials in F with the goal of eliminating any non-uniformity in

0747–7171/90/000000 + 00 $03.00/0

this dependence. Regarded both from an algebraic and a numerical point of view (i.e. with respect to the Zariski topology on K and the topology on $K = \mathbf{C}$ induced by the absolute value, respectively), the construction is extremely unstable under variation of these coefficients. Consider e.g. $G = \{X+1, UY+X\} \subseteq \mathbf{Q}[U,X,Y]$. In $\mathbf{Q}(U)[X,Y]$, G forms a Gröbner basis for any term order with $X < Y$; under the specialization $U = 0$, this property is lost, however. As a consequence, GBs are unable to solve *parametric* problems in algebraic geometry: Let e.g. G be as above; then G is a Gröbner basis in $\mathbf{Q}[U,X,Y]$ as well for any term order with $U < X < Y$. Nevertheless, G does not tell us, for which values of U, G has a common complex zero. This is the case for $U \neq 0$, but not for $U = 0$.

On the other hand, it is known (see Weispfenning (1988) and for special cases (see Gianni (1989), Kalkbrener (1989)) that the construction of G remains uniform when the coefficients are varied only within a certain constructible subset of the coefficient space, that can be determined in principle algorithmically from F and the given term-order. Moreover, for given F, there are only finitely many such constructible subsets (see Weispfenning (1988), compare also Ferro & Gallo (1988). So these facts seem to analyze the given problem in principle.

On closer scrutiny, however, a number of important issues are left unresolved by these results:

1 They do not explicitly describe algorithms for the construction of these constructible sets and the Gröbner bases corresponding to these sets.
2 Even if problem 1 was resolved, the resulting Gröbner bases would not be contained in the original ideal $Id(F)$. So this type of solution does not constitute an analogue of a Universal Gröbner basis in the sense that **one** finite set $G \subset Id(F)$ is simultaneously a Gröbner basis in all specializations of the indeterminate coefficients.

The main result of this paper is an **explicit algorithmic construction** of a **comprehensive Gröbner basis** G from any finite set of polynomials $F \subseteq S = K[U_1,...,U_m,X_1,...,X_n]$, where K is a field, $X_1,...,X_n$ are the main variables and $U_1,...,U_m$ are the parameters. The finite set G is a comprehensive Gröbner basis in the sense that $G \subseteq Id(F)$ and for any specialization σ of the parameters $U_1,...,U_m$ in any extension field K' of K, the image $\sigma[G]$ of G is a Gröbner basis of the ideal generated by $\sigma[F]$. More generally, the construction is also valid for the case that K is an integral domain and σ is an arbitrary ring homomorphism from $K[U_1,\dots,U_m]$ into some field K'. So even if no parameters U_i are present, a comprehensive Gröbner basis comprises in general more information than an ordinary Gröbner basis. This is e.g. the case for $R = \mathbf{Z}$; here a comprehensive Gröbner basis G in S constitutes not only a Gröbner basis in $\mathbf{Q}[\mathbf{X}]$, but also in $\mathbf{F}_p[\mathbf{X}]$ for all finite prime fields $\mathbf{F}_p$.

A comprehensive Gröbner basis G does not explicitly contain any information on a constructible partition of the parameter space; the coefficients of the polynomials in G are polynomial functions of the coefficients of the polynomials in the input system F. Thus G is a perfect analogue of a universal Gröbner basis . Of course, the construction of G can also be combined with the construction of a universal Gröbner basis to yield the ultimate totally invariant object, a **universal comprehensive Gröbner basis** .

The construction of a comprehensive Gröbner basis follows in principle the construction of a suitable constructible partition of the parameter space together with corresponding partial Gröbner bases . There is, however, one crucial difference to the line of reasoning sketched above: The construction of a partial Gröbner basis G corresponding to a constructible subset of the parameter space is schizophrenic in so far as it uses for its definition the constructible set in question, but simultaneously is defined in S in such a way that G remains inside the ideal $Id(F)$. This fact allows us to completely discard the construction of the constructible partition of the parameter space after it has been completed and to retain only the union of all "modified" Gröbner bases constructed along the way as a comprehensive Gröbner basis .

A comprehensive Gröbner basis G is rich enough in information so that a suitable constructible partition of the parameter space together with corresponding Gröbner bases (**a Gröbner system**) can be easily recovered from G. On the other hand, its size is usually much smaller than that of a corresponding Gröbner system. So it contains the same information in a more condensed form.

The number of applications of comprehensive Gröbner bases is large and manifold; it comprises most basic parametric problems in polynomial algebra and algebraic geometry that have been inaccessible to Gröbner basis methods so far. These include:

1 The study of parametric varieties, their size- and their dimension-functions; in particular one-parameter varieties and algebraic bifurcation problems.
2 Parametric ideal membership and parametric modules of syzygies.
3 The study of deformations of finitely generated commutative algebras.
4 A new method for the fast elimination of quantifier blocks in algebraically closed fields of arbitrary characteristic; besides comprehensive Gröbner bases the method uses for efficiency recent results on bounds in Hilbert's Nullstellensatz (see Fitchas & Galligo (1990)).

The algorithms of this paper have been implemented in ALDES/SAC-2 by E. Schönfeld (see Schönfeld (1991)) and in AXIOM/SCRATCHPAD II by W. Faas (see Faas (1992)) at the University of Passau. Both show – contrary to a priori expectations and in accordance with the worst-case bounds proved below – that the method is indeed of practical value. A detailled case study concerning practicability will be given in a subsequent paper.

In a different direction, comprehensive Gröbner bases open the way for numeric Gröbner basis calculations with certified accuracy using numeric arithmetic on the coefficients (see Rump (1987)).

The **plan of the paper** is as follows:

Section 2 presents the basic definitions and characterizations of comprehensive Gröbner bases and a non-constructive proof for their existence.

Section 3 describes the algorithms for the construction of comprehensive Gröbner bases and Gröbner systems.

Section 4 treats the construction of reduced comprehensive Gröbner bases and reduced Gröbner systems.

Section 5 computes upper worst case complexity bounds for the construction of comprehensive Gröbner bases in comparison to "classical" Gröbner bases and introduces partial comprehensive Gröbner bases that are important for fast quantifier elimination in algebraically closed fields.

Section 6 describes some immediate applications of comprehensive Gröbner bases : Elimination of quantifier-blocks in algebraically closed fields, computation of quantifier-free formulas determining parametric ideal membership and parametric dimension of varieties, computation of generators for parametric modules of syzygies, and deformation of residue algebras, in particular the isomorphism problem for different parameter values.

Section 7 illustrates the method by 4 examples computed using the implementation in Schönfeld (1991).

Section 8 sketches the construction of universal comprehensive Gröbner bases and discusses extensions of the method to specializations in other ground rings and to certain non-commutative polynomial rings.

The construction of comprehensive Gröbner bases and their application to quantifier elimination was first presented at a workshop on computer algebra organized by Prof. Loos at the University of Tübingen in September 1988. The contents of the full paper was presented at the CoCoa II conference, Genova, May 1989. Some related ideas and conjectures concerning a uniform description of the coefficients of the polynomials in a Gröbner basis appear in a preliminary form in Buchberger (1988).

2. Comprehensive Gröbner Bases - Existence

Throughout the paper, a **ring** will be a commutative ring with 1, a ring homomorphism will have to preserve the unit 1, and in any field or integral domain $0 \neq 1$. Let K be an integral domain, let $R = K[\mathbf{U}] = K[U_1, ..., U_m]$ be the polynomial ring over K in the indeterminates $U_1, ..., U_m$ and let $S = R[\mathbf{X}] = R[X_1, ..., X_n] = K[\mathbf{U}, \mathbf{X}]$ be the polynomial ring over R in the indeterminates $X_1, ..., X_n$. We regard $U_1, ..., U_m$ as **parameters** and $X_1, ..., X_n$ as the **main variables** of S; accordingly, we regard the polynomials $f(\mathbf{U}, \mathbf{X})$ in S as distributive polynomials in the main variables with coefficients $g(\mathbf{U}) \in R$ that are distributive polynomials in the parameters. T denotes the set of all **terms** of S in the main variables; so any $t \in T$ is a power-product of $X_1, ..., X_n$. M denotes the set of all **monomials** in S, i.e. of all products $m = g \cdot t$ with $g = g(\mathbf{U}) \in R$ and $t = t(\mathbf{X}) \in T$.

A **specialization** σ of S is a ring-homomorphism $\sigma : R \longrightarrow K'$ into some field K'. So whenever K is a field, then $\sigma \mid K$ is an embedding of K into K', and so we may regard K' as an extension field of K and assume that $\sigma \mid K = id_K$. A specialization σ is uniquely determined by its restriction to K and the images $\sigma(U_i)$ of the parameters in R. Conversely suppose we are given a ring homomorphism $\varphi : K \longrightarrow K'$ and an arbitrary map $\psi : \{U_1, ..., U_m\} \longrightarrow K'$. Then there exists a unique specialization $\sigma : R \longrightarrow K'$, such that $\sigma \mid K = \varphi$ and $\sigma \mid \{U_1, ..., U_m\} = \psi$. A specialization $\sigma : R \longrightarrow K'$ has a canonical extension to a ring-homomorphism $\overline{\sigma} : S \longrightarrow K'[X_1, ..., X_n]$. For $f = \sum_{i \in I} a_i(\mathbf{U}) \cdot t_i$ with $a_i(\mathbf{U}) \in R$, $t_i \in T$, $\overline{\sigma}(f) = \sum_{i \in I} \sigma(a_i(U)) \cdot t_i$. In the following, we denote this extension $\overline{\sigma}$ by σ as well. For a subset F of $K'[\mathbf{X}]$, $I(F)$ denotes the ideal generated by F in $K'[\mathbf{X}]$.

Throughout this section, we fix a term-order $\leq$ on T.

Let G be a finite subset of S. Then G is a **comprehensive Gröbner basis** (with respect to $\leq$), if for all fields K' and all specializations $\sigma : R \longrightarrow K'$ of S, $\sigma(G)$ is a Gröbner basis in $K'[\mathbf{X}]$ (with respect to the term-order $\leq$).

Notice that the definition of a comprehensive Gröbner basis refers to two proper classes of objects: All fields K' and all specializations $\sigma : R \longrightarrow K'$. In a first lemma we will restrict K' to fields determined by the image of σ. This will allow us to characterize comprehensive Gröbner bases in terms of the set $Spec(R)$ of all prime ideals of R.

LEMMA 2.1. *[Stability of Gröbner bases under field extensions] Let K'' be an extension field of a field K', let $S'' = K''[X_1, ..., X_n]$, $S' = K'[X_1, ..., X_n]$, and let G be a Gröbner basis with respect to $\leq$ in S'. Then G is also a Gröbner basis with respect to $\leq$ in S''.*

Proof. Let f, g be two different non-zero polynomials in G and let h be the S-polynomial of f and g. Then $h \in S'$ and $h \xrightarrow[G]{*} 0$ in S' and hence in S''. □

Call a specialization $\sigma : R \longrightarrow K' \supseteq K$ **epi**, if $K' = Quot(\sigma(R))$, where $Quot(R')$ denotes the quotient field of a ring R'. Then we may conclude from the lemma:

COROLLARY 2.2. *Let G be a finite subset of S. Then G is a comprehensive Gröbner basis with respect to $\leq$ iff for all epi specializations $\sigma : R \longrightarrow K'$, $\sigma(G)$ is a Gröbner basis in $K'[\mathbf{X}]$ with respect to $\leq$.*

The **spectrum** of R, $Spec(R)$, is the set of all prime ideals of R. For $f \in S$, we let $M(f)$ and $T(f)$ denote the set of all monomials and of all terms, respectively, that occur in f with non-vanishing coefficient. For $\pi \in Spec(R)$, we let $M_\pi(f)$ ($T_\pi(f)$) be the set of all $m \in M(f)$ ($t \in T(f)$) such that the coefficient of m (the coefficient of t in f) is not in π. $HM_\pi(f)$ ($HT_\pi(f)$) denotes the maximal element of $M_\pi(f)$ (of $T_\pi(f)$) with respect to the given term-order. $HC_\pi(f) \in R$ is the coefficient of $HM_\pi(f)$. If $T_\pi(f) = \emptyset$, then $HT_\pi(f)$, $HM_\pi(f)$, and $HC_\pi(f)$ are undefined.

So for $\pi = \{0\}$, $HM_\pi(f)$, $HT_\pi(f)$ and $HC_\pi(f)$ are just the usual **head-monomial**, **head-term** and **head-coefficient** of f. If $F \subseteq S$, then $HT_\pi(F) = \{HT_\pi(f) : f \in F\}$; similar for $HM_\pi(F)$ and $HC_\pi(F)$.

For every specialization σ of S, $ker(\sigma) \in Spec(R)$. Conversely, every $\pi \in Spec(R)$ determines an epi specialization σ_π with kernel π : Let $K_\pi = Quot(R/\pi)$; then σ_π is the canonical homomomorphism from R into K_π.

LEMMA 2.3. *Let I be an ideal of S, and let G be a finite subset of I. Let $\sigma : R \longrightarrow K'$ be an epi specialization of S with $ker(\sigma) = \pi \in Spec(R)$. Then $\sigma(G)$ is a Gröbner basis of $Id(\sigma(I))$ in $K'[\mathbf{X}]$ iff for all $f \in I$ such that $HT_\pi(f)$ is defined, there exists $g \in G$ such that $HT_\pi(g) \mid HT_\pi(f)$.*

Proof. "$\Longrightarrow$" : Since $0 \neq \sigma(f) \in \sigma(Id(G))$, there exists $g \in G$ with $HT_\pi(g) = HT(\sigma(g)) \mid HT(\sigma(f)) = HT_\pi(f)$.

"$\Longleftarrow$": Let $f \in S$ with $0 \neq \sigma(f) \in Id(\sigma(I))$. Then there exists $c \in R \setminus \pi$ and $h \in I$ with $\sigma(c \cdot f) = \sigma(h)$. So $HT_\pi(h) = HT(\sigma(h)) = HT(\sigma(f))$. By hypothesis, there exists $g \in G$ such that $HT_\pi(g)$ divides $HT_\pi(h)$, and hence $HT(\sigma(f))$. This shows that $\sigma(G)$ is a Gröbner basis of $Id(\sigma(I))$ in $K'[\mathbf{X}]$. □

Let I be an ideal of S and let G be a finite subset of I. Then we say G is a **comprehensive Gröbner basis of** I, if for all specializations $\sigma : R \longrightarrow K'[\mathbf{X}]$, $\sigma(G)$ is a Gröbner basis of the ideal $Id(\sigma(I))$ in $K'[\mathbf{X}]$; in other words G is a comprehensive Gröbner basis included in I and for all specializations $\sigma : R \longrightarrow K' \supseteq K$, $Id(\sigma(G)) = Id(\sigma(I))$ in $K'[\mathbf{X}]$. By corollary 2.2, one may restrict this condition equivalently to epi specializations. So by lemma 2.3, it can be expressed in terms of prime ideals in $Spec(R)$ as follows:

THEOREM 2.4. *Let G be a finite subset of an ideal I of S. Then the following assertions are equivalent:*

(i) G is a comprehensive Gröbner basis of I with respect to $\leq$.
(ii) For all $\pi \in Spec(R)$ and all $t \in HT_\pi(I)$, there exists $g \in G$ with $HT_\pi(g) \mid t$.

Proof. Combine corollary 2.2 and lemma 2.3. □

Specializing in the theorem $I = Id(G)$, we obtain the following characterization of comprehensive Gröbner bases:

COROLLARY 2.5. *Let G be a finite subset of S. Then the following assertions are equivalent:*

(i) G is a comprehensive Gröbner basis with respect to $\leq$.
(ii) For all $\pi \in Spec(R)$ and all $t \in HT_\pi(Id(G))$ there exists $g \in G$ with $HT_\pi(g) \mid t$.

Before giving an explicit construction of comprehensive Gröbner bases, we show the existence of these bases for arbitrary ideals I in S.

For an ideal I of S the equivalence relation $\sim_I$ on $Spec(R)$ is defined by $\pi \sim_I \pi' \iff HT_\pi(I) = HT_{\pi'}(I)$.

Let I be an ideal of S and let $\pi \in Spec(R)$. Then for any finite $G \subseteq I$ such that $\sigma_\pi(G)$ is a reduced Gröbner basis of $I(\sigma_\pi(I))$ in $K_\pi[\mathbf{X}]$, $\sigma_\pi(G)$ and hence $HT_\pi(G) = HT(\sigma_\pi(G))$ is uniquely determined by I and π independent of the choice of G. We denote the finite subset $HT_\pi(G)$ of $HT_\pi(I)$ by $HT'_\pi(I)$. Notice that $HT_\pi(G)$ is in fact the unique minimal Dickson basis of $HT_\pi(I)$ with respect to divisibility in T. Consequently, the equivalence relation $\sim_I$ on $Spec(R)$ can be characterized in a finitary way:

LEMMA 2.6. *Let I be an ideal of S and let $\pi, \pi' \in Spec(R)$. Then $\pi \sim_I \pi'$ iff $HT'_\pi(I) = HT'_{\pi'}(I)$.*

Proof. Obvious. □

THEOREM 2.7. *Let I be an ideal in S.*

(i) The equivalence relation $\sim_I$ has only finitely many equivalence classes.
(ii) There exists a comprehensive Gröbner basis G of I.

Proof. The proof given here is non-constructive and depends on the results in Weispfenning (1988); an independent constructive proof is given in section 3. (i) Let F be a finite basis for the ideal I. Then one can construct from F a finite partition of $Spec(R)$ into constructible subsets (given by case distinctions on the vanishing or non-vanishing of certain coefficients with respect to the main variables), such that for each specialization σ_π, where π is in one of these subsets, the reduced Gröbner basis G_π for $Id(\sigma_\pi(F))$ is given uniformly in F; in particular, the coefficients of the polynomials $g \in G_\pi$ are rational functions of the coefficients of the polynomials in F (with integer coefficients), whose denominators do not vanish under σ_π. (The details of this argument are carried out in Weispfenning (1988)). This means in particular, that for all π in this subset, $HT(G_\pi)$ is the same. So by lemma 2.6 , this finite partition refines the partition of $Spec(R)$ induced by $\sim_I$.

(ii) Pick representatives $\pi_1, ..., \pi_r$ for the equivalence classes of $\sim_I$ in $Spec(R)$, and put $H_i = HT_{\pi_i}(I)$ for $1 \leq i \leq r$. Then by Dickson's lemma, each H_i has a finite basis B_i (in the sense that for every $t \in H_i$ there exists $s \in B_i$ with $s \mid t$). For every $t \in H_i$ we can pick $f_t \in I$ with $HT_{\pi_i}(f_t) = t$. Let $G_i = \{f_t : t \in B_i\}$; then G_i is a finite subset of I such that $HT_{\pi_i}(G_i) = B_i$. We claim that $G = \bigcup_{i=1}^r G_i$ is a comprehensive Gröbner basis of I. Indeed $G \subseteq I$; whenever $\pi \in Spec(R)$ and $t \in HT_\pi(I)$, then $\pi \sim_I \pi_i$ for some $1 \leq i \leq r$, and so there exists $g \in G_i$ with $HT_\pi(g) = HT_{\pi_i}(g) \mid t \in HT_{\pi_i}(I)$. So by theorem 2.4 G is a comprehensive Gröbner basis. □

Before we start with the construction of comprehensive Gröbner bases , we remark that in principle this task can always be reduced to a generic construction in the following sense: For any given degree bound d on an input system F of size $\#F \leq k$, it suffices to compute one single "generic" comprehensive Gröbner basis from which all others (over an arbitrary integral domain K) are simply obtained by specialization. Since, however, a "generic" input system F has a huge number of indeterminate coefficients, this may not be of any practical value for computations.

Let $1 \leq d \leq \mathbf{N}$ and put $T_d = \{t \in T : deg_{X_i}(t) < d \text{ for } 1 \leq i \leq d\}$. We consider the most general polynomial f in the main variables $X_1, ..., X_n$ with $deg_{X_i}(f) < d$ for $1 \leq i \leq n$. Since $\#T_d = d^n$, f consists of the sum of all d^n terms in T_d, each multiplied with an indeterminate coefficient. More generally, if $F = \{f_1, ..., f_k\}$ is a finite set of independent "generic" polynomials f with $deg_{X_i}(f) < d$ for $1 \leq i \leq n$, then $F \subseteq S_r = \mathbf{Z}[V_1, ..., V_r; X_1, ..., X_n]$, where $V_1, ..., V_r,\ r = k \cdot d^n$, are the indeterminate coefficients of $f_1, ..., f_k$. We denote the corresponding ring $\mathbf{Z}[V_1, ..., V_r]$ by R_r.

PROPOSITION 2.8. *Let $F \subseteq S_r$ be as above and let G be a comprehensive Gröbner basis for $Id(F)$ with respect to a term order $\leq$ on T. Let $\rho : R_r \longrightarrow R = K[U_1, ..., U_m]$ be a ring homomorphism and denote the canonical extension of ρ mapping S_r into $S = K[U_1, ..., U_m; X_1, ..., X_n]$ also by ρ. Then $\rho(G)$ is a comprehensive Gröbner basis for $Id(\rho(F))$ with respect to $\leq$.*

Proof. Let $\sigma : R \longrightarrow K' \supseteq K$ be a specialization of R. Then $\sigma \circ \rho : R_r \longrightarrow K'$ is a specialization of R_r, and so $(\sigma \circ \rho)(G)$ is a Gröbner basis for $Id((\sigma \circ \rho)(F))$ in $K'[X_1, ..., X_n]$, and so $\sigma(\rho(G))$ is a Gröbner basis for $Id(\sigma(\rho(F)))$. This shows that $\rho(G)$ is a comprehensive Gröbner basis for $Id(\rho(F))$. □

3. Comprehensive Gröbner Bases - Construction

In this section, we describe some algorithms that - taken together - provide an explicit construction of a comprehensive Gröbner basis for $Id(F)$ from any finite $F \subseteq S$ via the intermediate concept of a **Gröbner system**. Since all polynomial algorithms in S involve of course computations in the ground ring K, we shall from now on tacitly assume that K **is a computable ring**. This means that the elements of K are represented in such a way that the arithmetic operations on K are computable and that the equality of any two given elements is decidable. Moreover, we assume (unless mentioned otherwise) that all the term orders on T under consideration are decidable.

The strategy will be as follows: Starting from a finite basis F of the ideal I, we construct a finite partition of $Spec(R)$ into constructible subsets and simultaneously for each block of this partition a finite set of polynomials G with $F \subseteq G \subseteq Id(F)$, such that for all π in the corresponding block, $\sigma_\pi(G)$ is a Gröbner basis and $HT_\pi(G) = HT'_\pi(I)$ is fixed. Consequently, $HT(\sigma_\pi(I)) = HT_\pi(I)$ is fixed for all π in one block, and so this partition refines the partition induced by $\sim_I$.

The collection of all pairs consisting of polynomial conditions on the U_i defining such a block together with the corresponding basis G will form a **Gröbner system**. From this Gröbner system a comprehensive Gröbner basis is simply obtained by uniting all G's and deleting all the polynomial conditions.

In order to describe the construction in a concise way, we need the following **definitions**:

A **condition** γ is a finite set of polynomial equations $g(\mathbf{U}) = 0$ and polynomial inequalities $g(\mathbf{U}) \neq 0$ in the parameters $\mathbf{U}$. Any condition determines a constructible subset Sp_γ of $Spec(R)$: $Sp_\gamma = \{\pi \in Spec(R) : g \in \pi$ for $g(\mathbf{U}) = 0$ in γ, and $g' \notin \pi$ for $g'(U) \neq 0$ in $\gamma\}$. Notice that Sp_γ may be empty. A finite set Γ of conditions is a **case distinction**, if for $\gamma \neq \gamma' \in \Gamma$, Sp_γ and $Sp_{\gamma'}$ are disjoint. Γ is a **cover** of a condition δ, if Γ is a case distinction and $\bigcup_{\gamma\in\Gamma} Sp_\gamma = Sp_\delta$; Γ is a **cover** of a case distinction Δ, if Γ is of the form $\Gamma = \bigcup_{\delta\in\Delta} \Gamma_\delta$, where each Γ_δ is a cover of δ. Γ is a **complete case distinction**, if it covers the empty condition. In particular $\Gamma = \{\emptyset\}$ is a complete case distinction, since $Sp_\emptyset = Spec(R)$. Whenever Γ is a complete case distinction, $g \in R$, $\Gamma_1 = \{\gamma \cup \{g = 0\} : \gamma \in \Gamma\}$, $\Gamma_2 = \{\gamma \cup \{g \neq 0\} : \gamma \in \Gamma\}$, then $\Gamma_1 \cup \Gamma_2$ is a complete case distinction that **refines** Γ; similar for covers. We refer to the conditions $\gamma \cup \{g = 0\}$ and $\gamma \cup \{g \neq 0\}$ as **successors** of the condition γ. This is in accordance with the attitude of viewing the set of all conditions as a **tree** under the inclusion relation with root $\emptyset$.

A **colouring** of R is a map *col* which assigns to every element a of R - given as a specific integral-rational expression in the parameters and the elements of K - one of the colours *white*, *green*, *red* in such a way that 0 is coloured in *green* and all invertible elements of K are coloured in *red*. Any condition γ determines a colouring of the ring R in the following way: Let $a \in R$ be given as a specific integral-rational expression in the parameters and the elements of K (which may differ from its normal form as distributive polynomial in $U_1, ..., U_m$). Then $col(a)$ is defined recursively as follows:

$col(0) = green$, $col(a) = red$, if a is invertible in K,

$col(a) = green$, if the equation $a = 0$ is in γ,

$col(a) = red$, if the inequality $a \neq 0$ is in γ,

$col(-a) = col(a)$,

$col(a \cdot b) = red$, if both a and b are coloured *red*,

$col(a \cdot b) = green$, if a or b is coloured *green*,

$col(a + b) = red$, if a is coloured *red* and b is coloured *green* or vice versa,

$col(a + b) = green$, if both a and b are coloured *green*,

In all other cases, $col(a) = white$.

Informally, a is coloured in *green* or *red*, if the question $a = 0$ is decided by γ in an obvious manner; otherwise a is coloured in *white*. So the colour of a in its given (e.g. factored) form may be *green* or *red*, while the colour of a in its distributive polynomial form may be *white*.

For any $f \in S$ such a colouring of R induces a **colouring of** $T(f)$: A term $t \in T(f)$ inherits the colour of its coefficient in f. The sets of terms in f coloured in green, red and white by γ are denoted by $T_{green,\gamma}(f)$, $T_{red,\gamma}(f)$ and $T_{white,\gamma}(f)$, respectively. For $t \in T(f)$, t is called the **head-term of f with respect to** γ (**notation** $t = HT_\gamma(f)$), if $t \in T_{red,\gamma}(f)$ and for all $t' \in T(f)$ with $t' > t$, $t' \in T_{green,\gamma}(f)$. So $HT_\gamma(f)$ may be undefined for certain f and γ. If $HT_\gamma(f)$ is defined, then $HC_\gamma(f)$ is the coefficient a of $HT_\gamma(f)$ in f and $HM_\gamma(f)$ is the monomial $a \cdot HT_\gamma(f)$.

At this point we need to recall some concepts related to the construction of Gröbner bases in a polynomial ring $K'[\mathbf{X}]$ over a field K', such as **reduction of polynomials** with respect to a finite set of polynomials, the **S-polynomial** $\mathrm{SPol}(f, g)$ of two polynomials f, g, and the concept of a **reduced finite set** of polynomials (compare Buchberger (1985)). Usually, these concepts involve division of coefficients in the ground field K'. For the purpose of this paper, we need to avoid division; so we use a slightly modified notion of reduction and S-polynomials: We say f **reduces to f' modulo** p (**notation**

$f \underset{p}{\longrightarrow} f'$) if $f, f', p \in K'[\mathbf{X}]$, $p \neq 0$, f contains a monomial $a \cdot t$ ($0 \neq a \in K'$) such that $HT(p)$ divides t, say $HT(p) \cdot s = t$ for $s \in T$, if $f' = HC(p) \cdot f - a \cdot s \cdot p$. (So in the usual sense this means $HC(p) \cdot f \underset{p}{\longrightarrow} f'$.) Let $f, g \in K'[\mathbf{X}]$ and let $HM(f) = a \cdot s$, $HM(g) = b \cdot t$ with $0 \neq a, b \in K'$. Let $t' = u \cdot s = v \cdot t$ be the least common multiple of s and t in T. Then $\mathrm{SPol}(f, g) = b \cdot u \cdot f - a \cdot v \cdot g$. The remaining concepts are defined in terms of these modified ones in the usual manner.

Next, we relativize this form of reduction and S-polynomial with respect to a condition γ: We say f **reduces to** f' **modulo** p **relative to** γ (**notation** $f \underset{p}{\longrightarrow} f' \quad [\gamma]$) if $HT_\gamma(p)$ is defined and there exists some monomial $a \cdot t$ in f with $t \in T_{red,\gamma}(f) \cup T_{white,\gamma}(f)$ such that for some $s \in T$, $HT_\gamma(p) \cdot s = t$ and $f' = HC_\gamma(p) \cdot f - a \cdot s \cdot p$. If this is the case, we say f **is reducible modulo** p **relative to** γ. Reduction and reducibility modulo a set P of polynomials and iterated reduction modulo P relative to γ (denoted by $\overset{*}{\underset{P}{\longrightarrow}} [\gamma]$) are defined in the obvious way. Notice that $f \underset{P}{\longrightarrow} f' \quad [\gamma]$ does in general not imply $f' < f$. So Noetherianity of this reduction relation for fixed P and γ does not follow in the usual manner. Instead, we define the γ-**part**, $\mathrm{PART}(\gamma, f)$, of a polynomial $f \in S$ with respect to a condition γ as the polynomial resulting from f by deleting all monomials of f, whose coefficient is coloured in *green* by γ. Then we may conclude:

LEMMA 3.1. *(i)* $f \underset{P}{\longrightarrow} f' \ [\gamma]$ *implies* $\mathrm{PART}(\gamma, f') < \mathrm{PART}(\gamma, f)$.

(ii) For fixed P *and* γ, *the reduction relation* $\underset{P}{\longrightarrow} [\gamma]$ *is Noetherian.*

(iii) If f *is irreducible modulo* P *relative to* γ, *then* f *is also irreducible modulo* P *relative to* δ *for every condition* δ *extending* γ.

Proof. (i) By definition of f', there exists $t \in T_{red,\gamma}(f) \cup T_{white,\gamma}(f) \setminus T(f')$, such that for all $t' \in T(f') \setminus T(f)$ with $t' > t$, it follows that $t' \in T_{green,\gamma}(f')$. (ii) is an immediate consequence of (i) and the well-foundedness of the quasi-order $<$ on S. (iii) follows from the fact that $\delta \supseteq \gamma$ implies $T_{red,\delta}(f) \cup T_{white,\delta}(f) \subseteq T_{red,\gamma}(f) \cup T_{white,\gamma}(f)$. □

If f, g are polynomials such that $HM_\gamma(f) = a \cdot s$ and $HM_\gamma(g) = b \cdot t$ are defined and if $t' = u \cdot s = v \cdot t$ is the least common multiple of s and t, then the **S-polynomial of** f **and** g **relative to** γ is the polynomial $\mathrm{SPol}_\gamma(f, g) = b \cdot u \cdot f - a \cdot v \cdot g$.

The relation between the absolute and relativized notions is as follows:

LEMMA 3.2. *Let* γ *be a condition such that* $Sp_\gamma \neq \emptyset$ *and let* $\pi \in Sp_\gamma$, $P \subseteq S$. *Then*

(i) $f \underset{P}{\longrightarrow} f' \ [\gamma]$ *implies* $\sigma_\pi(f) \underset{\sigma_\pi(P)}{\longrightarrow} \sigma_\pi(f')$ *or* $\sigma_\pi(f) = \sigma_\pi(f')$.

(ii) $f \overset{*}{\underset{P}{\longrightarrow}} f' \ [\gamma]$ *implies* $\sigma_\pi(f) \overset{*}{\underset{\sigma_\pi(P)}{\longrightarrow}} \sigma_\pi(f')$.

(iii) If f *is irreducible modulo* P *relative to* γ, *then* $\sigma_\pi(f)$ *is irreducible modulo* $\sigma_\pi(P)$ *in* $K_\pi[\mathbf{X}]$.

(iv) $\sigma_\pi(\mathrm{SPol}_\gamma(f, g)) = \mathrm{SPol}(\sigma_\pi(f), \sigma_\pi(g))$.

Proof. Obvious. □

Let Γ be a finite set of conditions and let F be a finite set of polynomials in S. Then we say Γ **determines** F, if for every $\gamma \in \Gamma$ and every $f \in F$, either $HT_\gamma(f)$ is defined or $T(f) = T_{green,\gamma}(f)$. If $\Gamma = \{\gamma\}$ and Γ determines F, then we say γ determines F.

LEMMA 3.3. *For a condition γ and a given finite subset F of S one can construct a cover Δ of γ that determines F.*

Proof. There is an obvious algorithm **DET** that satisfies the following specification:

Algorithm **DET** (γ, F)
Input: A condition γ and $F = \{f_1, ..., f_m\} \subseteq S$.
Output: A cover Δ of γ that determines F.

The algorithm simply adds to γ the finitely many equations and inequalities on the coefficients of polynomials in F necessary to determine F. Notices that this does not require that *each* coefficient of a polynomial in F is coloured in *red* or in *green*. □

Let P be a finite set of polynomials in S and let γ be a condition that determines P. Then we define a **normal form** of a polynomial f with respect to P relative to γ as a pair (g, c) with $g \in S, c \in R$ such that

(i) $f \xrightarrow[P]{*} g\ [\gamma]$ and g is irreducible modulo P relative to γ.
(ii) $cf - g \in Id(P)$.
(iii) c is coloured in *red* by γ.

The following simple algorithm computes a (not necessarily unique) normal form of a polynomial:

Algorithm **NORMALFORM** (γ, f, P)
Input: A condition γ, $f, \in S$, and a finite set $P \subseteq S$ such that $\{\gamma\}$ determines P.
Output: A normal form (g, c) of f modulo P relative to γ.
BEGIN
    $g := f;\quad c := 1;$
    WHILE g is reducible modulo P relative to γ DO
        g' := some element of S such that $g \xrightarrow[p]{} g'\ [\gamma]$ for some $p \in P$;
        $c := c \cdot HC_\gamma(p);\quad g := g';$
    END
    Return (g, c)
END

Partial correctness is obvious; termination follows from lemma 3.1(ii). □

Let B be a case distinction. Then a **Gröbner system** for an ideal I of S over B is a finite set GS of pairs (γ, G) such that:

(i) G is a finite subset of I determined by the condition γ.
(ii) $\Gamma = \{\gamma : (\gamma, G) \in GS\}$ is a cover of B.
(iii) For every $\pi \in Sp_\gamma$, $\sigma_\pi(G)$ is a Gröbner basis of $I(\sigma_\pi(I))$ in $K_\pi[\mathbf{X}]$.

A **comprehensive Gröbner basis of** I **over** B is a finite subset G of I such that for all $\pi \in \bigcup_{\beta \in \mathrm{B}} Sp_\beta$, $\sigma_\pi(G)$ is a Gröbner basis of $I(\sigma_\pi(I))$. So for $\mathrm{B} = \{\emptyset\}$, G is a comprehensive Gröbner basis of I; in this case, we call GS simply a Gröbner system for I.

The use of a comprehensive Gröbner basis of I over B recommends itself when one is interested only in certain specializations that are specified in advance by the case distinction B and wants to reduce the complexity of the construction of a full comprehensive Gröbner basis .

Any Gröbner system GS for I (over B) determines a comprehensive Gröbner basis G' of I (over B) and vice versa:

PROPOSITION 3.4. *(i) Let GS be a Gröbner system for I over* B*, and put $G' = \bigcup\{G : (\gamma, G) \in GS\}$. Then G' is a comprehensive Gröbner basis of I over* B.

(ii) Let G be a comprehensive Gröbner basis of I over B*, and let $\Gamma = \bigcup_{\beta\in \mathrm{B}} \mathbf{DET}(\beta, G)$. Then $GS = \{(\gamma, G) : \gamma \in \Gamma\}$ is a Gröbner system for I over* B*. Moreover, for any further Gröbner system GS' for I over* B*, such that $(\delta, G') \in GS'$ implies $G' = G$, there exists $(\gamma, G) \in GS$ such that $Sp_\delta \subseteq Sp_\gamma$.*

Proof. (i) is obvious from the fact that any extension $G' \subseteq Id(G)$ of a Gröbner basis G is again a Gröbner basis for $Id(G)$, and the fact that $\bigcup\{Sp_\gamma : (\gamma, G) \in GS\} = \bigcup\{Sp_\beta : \beta \in \mathrm{B}\}$.

(ii) The first claim follows from the fact that Γ is a cover of B. Next let $(\delta, G) \in GS'$, and suppose $\pi \in Sp_\delta$. Pick $(\gamma, G) \in GS$ with $\pi \in Sp_\gamma$. Then both δ and γ determine G, and so by the definition of Γ, $Sp_\delta \subseteq Sp_\gamma$. □

Starting from any comprehensive Gröbner basis for I one is now in a position to compute the equivalence relation $\sim_I$ on $Spec(R)$ in an effective way: For $T' \subseteq T$, we put $\mathrm{Mult}(T') = \{t \in T : \exists s \in T' \text{ with } s \mid t\}$.

COROLLARY 3.5. *Let G be a comprehensive Gröbner basis for I, let Γ and GS be as in the preceeding proposition (with $\mathrm{B} = \emptyset$), and call $\gamma, \delta \in \Gamma$ associated, if $\mathrm{Mult}HT_\gamma(G) = \mathrm{Mult}HT_\delta(G)$. Then for $\pi, \pi' \in Spec(R)$, $\pi \sim_I \pi'$ iff there exist $\gamma, \delta \in \Gamma$ such that γ and δ are associated and $\pi \in Sp_\gamma$, $\pi' \in Sp_\delta$.*

Proof. Notice that for any $\gamma \in \Gamma$, $\pi \in Sp_\gamma$, $HT_\pi(I) = \mathrm{Mult}HT_\gamma(G)$. □

As a further application, we can now specify an algorithm **GRÖBNERTEST** that determines for a given finite subset G of S those specializations σ for which $\sigma(G)$ is a Gröbner basis .

Algorithm **GRÖBNERTEST** (G)
Input: A finite $G \subseteq S$
Output:A case distinction Γ such that for every $\pi \in Spec(R)$,
$\sigma_\pi(G)$ is a Gröbner basis in $K_\pi[\mathbf{X}]$ iff $\pi \in Sp_\gamma$ for some $\gamma \in \Gamma$.

BEGIN
  $\Gamma := \mathbf{DET}(\emptyset, G)$;
  $P := \{(\gamma, f, g) : \gamma \in \Gamma,\ f, g \in G\ ,\ f \neq g\}$;
  WHILE $P \neq \emptyset$ DO
    $(\gamma, f, g) :=$ some element of P; $\Gamma := \Gamma \setminus \{\gamma\}$;
    $P := P \setminus \{(\gamma, f, g)\}$; $h := \mathrm{SPol}_\gamma(f, g)$;
    $(k, c) := \mathbf{NORMALFORM}(\gamma, h, G)$;
    $\Gamma := \Gamma \cup \{\delta \in \mathbf{DET}(\gamma, k) : T_{green,\delta}(k) = T(k)\}$;
  END
END

Termination of the algorithm is obvious by the fact that $\#P$ decreases in each run of the while-loop. Correctness follows from lemma 3.2 together with the well-known Buchberger criterion for Gröbner bases in terms of S-polynomials. □

Notice that this algorithm yields a decision procedure for the problem whether G is a comprehensive Gröbner basis of $Id(G)$ over a given case distinction: For this purpose, it suffices to check, whether $\bigcup_{\beta \in \mathrm{B}} Sp_\beta \subseteq \bigcup_{\gamma \in \Gamma} Sp_\gamma$. This can be achieved by computing "classical" Gröbner bases and applying Hilbert's Nullstellensatz together with the well-known Rabinowich trick in the parameter ring R. (compare Buchberger (1987)).

We also remark that the constructible set $C = \bigcup_{\gamma \in \Gamma} Sp_\gamma$ of all $\pi \in Spec(R)$, for which $\sigma_\pi(G)$ is a Gröbner basis , is in general neither closed nor open in the Zariski topology of $Spec(R)$. Example: Let $G = \{Y+1, UX+VY\} \subseteq \mathbf{Q}[U,V;X,Y]$ with the lexicographic order on $T(X,Y)$; then $C = \{\pi : U \in \pi \implies V \in \pi\}$.

Next, we proceed to the construction of comprehensive Gröbner bases via Gröbner systems. In contrast to the test above, this construction will not involve any Gröbner basis computation on the parameters. In fact, any comprehensive Gröbner basis G constructed in this way will always have the property that **GRÖBNERTEST**(G) will yield an obviously complete case distinction Γ, so that no further Gröbner basis computation in the parameter ring R is required.

THEOREM 3.6. (CONSTRUCTION OF GRÖBNER SYSTEMS) *For a finite $F \subseteq S$ and a given case distinction* B *one can construct a Gröbner system GS for $I(F)$ over* B.

Proof. GS is constructed by the algorithm **GRÖBNERSYSTEM** below. Notice that properties (i) and (ii) of the definition of a Gröbner system are invariant of the while-loop; another invariant of this loop is the property that for every (γ, G, f, g) with $(\gamma, G) \in GS$ and f, g different elements of G, and $(\gamma, G, f, g) \notin P$, $\mathrm{SPol}_\gamma(f,g)$ has a normal form (k, c) with respect to G relative to some subcondition of γ, such that all terms of k are coloured in *green* by γ. Upon termination, P will be empty. So every pair (γ, G) in GS will have the following property: Whenever f, g are two different elements in G, then there exist $k \in S$ and a subcondition γ' of γ such that $\mathrm{SPol}_\gamma(f,g) \xrightarrow[G]{*} k\ [\gamma']$, and with $T(k) = T_{green,\gamma}(k)$. So by lemma 3.2, $\mathrm{SPol}(\sigma_\pi(f), \sigma_\pi(g)) \xrightarrow[\sigma_\pi(G)]{*} 0$ for every $\pi \in Sp_\gamma$. In addition $G \supseteq F$. So we may conclude that property (iii) of the definition of a Gröbner system holds as well.

To prove termination, we apply König's tree lemma : The set of all quadruples (γ, G, f, g) obtained in the course of the algorithm forms a tree, when the successor of a quadruple (γ, G, f, g) is defined as any quadruple $(\delta, G \cup \{k\}, f', g')$ or (δ, G, f', g') produced from (γ, G, f, g) in one run of the while-loop. This tree is finitely branching. So it suffices to show that any branch b of this tree is finite: Notice to begin with that whenever (δ, G, f', g') follows (γ, G, f, g) in the branch b, then $f, g, f', g' \in G$ and $\{f, g\} \neq \{f', g'\}$. So b cannot contain infinitely many quadruples with the same second component. If $(\delta, G \cup \{k\}, f', g')$ follows (γ, G, f, g) in b and $t = HT_\delta(k)$, then t is not divided by any $HT_\gamma(g) = HT_\delta(g)$ with $g \in G$. So if b were infinite, we would get an infinite sequence of terms $\{t_i\}_{i \in \mathbf{N}}$ such that t_i does not divide t_j for $i < j$. This contradicts Dickson's lemma. □

Algorithm **GRÖBNERSYSTEM** (F, B)
Input: A finite $F \subseteq S$ and a case distinction B.
Output: A finite set GS of pairs (γ, G) forming a Gröbner system for $Id(F)$ over B.
BEGIN
  $\Gamma := \bigcup\{\mathbf{DET}(\beta, F) : \beta \in \mathrm{B}\}$;
  $GS := \{(\gamma, F) : \gamma \in \Gamma\}$;
  $P := \{(\gamma, F, f, g) : \gamma \in \Gamma,\ f, g \in F\ ,\ f \neq g\}$;
  WHILE $P \neq \emptyset$ DO
    $(\gamma, G, f, g) :=$ some element of P;
    $GS := GS \setminus \{(\gamma, G)\}$;
    $P := P \setminus \{(\gamma, G, f, g)\}$;
    $h := \mathrm{SPol}_\gamma(f, g)$;
    $(k, c) := \mathbf{NORMALFORM}(\gamma, h, G)$;
    $\Delta := \mathbf{DET}(\gamma, \{k\})$;
    $\Delta' := \{\delta \in \Delta : T_{red,\delta}(k) \neq \emptyset\}$;
    IF $\Delta' = \emptyset$ THEN $GS := GS \cup \{(\gamma, G)\}$;
    ELSE
    $GS := GS\ \cup\ \{(\delta, G \cup \{k\}) : \delta \in \Delta'\} \cup\ \{(\delta, G) : \delta \in \Delta \setminus \Delta'\}$;
    $P := (P \setminus \{(\gamma, G, f', g') : (\gamma, G, f', g') \in P\})\ \cup\ \{(\delta, G \cup \{k\}, f', k) :$
      $f' \in G, \delta \in \Delta'\}\ \cup\ \{(\delta, G, f', g') : (\gamma, G, f', g') \in P, \delta \in \Delta\}$;
  END
END

4. Reduced Gröbner Systems

Recall that a finite set F of polynomials in some polynomial ring $K'[\mathbf{X}]$ is **reduced** (or **autoreduced**), if every $f \in F$ is non-zero irreducible modulo $F \setminus \{f\}$. The natural relativization of this definition to a condition γ, reads as follows: Suppose γ determines F. Then we say F **is reduced relative to** γ, if in addition for every $f \in F$, f is irreducible modulo $F \setminus \{f\}$ relative to γ, and $T_{red,\gamma}(f) \neq \emptyset$.

LEMMA 4.1. *For a condition γ and a given finite set $F \subseteq S$ one can construct a finite set* RED *of pairs (δ, G) such that*

(i) G is a finite subset of S such that for all $\pi \in Sp_\gamma$, $Id(\sigma_\pi(G)) = Id(\sigma_\pi(F))$.
(ii) δ is a condition that determines G.
(iii) $\Delta = \{\delta : (\delta, G) \in \mathrm{RED}\}$ is a cover of γ.
(iv) G is reduced relative to δ.

Moreover, if for every $\pi \in SP_\gamma$, $\sigma_\pi(F)$ is a Gröbner basis of $Id(\sigma_\pi(I))$, then $\sigma_\pi(G)$ is a reduced Gröbner basis of $Id(\sigma_\pi(I))$ for every $\pi \in Sp_\delta$.

Proof. RED is computed from (γ, F) by the algorithm **REDUCTION** below. Partial correctness for properties $(i)-(iv)$ follows readily from the following respective invariants of the REPEAT-loop:

(i) $G \cup U$ is a finite subset of S such that for all $\pi \in Sp_\gamma$, $Id(\sigma_\pi(G \cup U)) = Id(\sigma_\pi(F))$.
(ii) δ is a condition that determines $G \cup U$.
(iii) $\{\delta : (\delta, G) \in RD\}$ is a cover of γ.
(iv) Every $f \in G$ is irreducible modulo $(G \cup U) \setminus \{f\}$ relative to δ.

Next assume $\sigma_\pi(F)$ is a Gröbner basis of $Id(\sigma_\pi(I))$ for all $\pi \in Sp_\gamma$. We claim that for every triple (δ, G, U) produced in the course of the algorithm and every $\pi \in Sp_\delta$, $\sigma_\pi(G \cup U)$ is a Gröbner basis of $Id(\sigma_\pi(I))$. This will complete the proof of partial correctness. For the initial values of (δ, G, U) this is true by hypothesis. Next let (δ', G', U') be a successor of (δ, G, U) obtained by one run of the repeat-loop. We use the criterion established in lemma 2.3: Let $\pi \in Sp_\delta$, and let $t \in HT_\pi(I)$; then by the induction assumption, there exists $g \in G \cup U$ such that $HT_\pi(g)$ divides t. If $HT_\pi(h)$ divides $HT_\pi(g)$ for some $h \in G' \cup U'$, we are done. Assume this is not the case. Let $(k, c) =$ NORMALFORM$(\delta, g, G \cup U)$; then some step in the iterated reduction relative to δ leading from g to k has eliminated $HT_\pi(g)$, since $HT_\pi(g)$ has been coloured in red by δ. So there exists $h \in G \cup U$ such that $HT_\pi(h)$ divides $HT_\pi(g)$, a contradiction. Termination is proved again by an application of König's lemma to the finitely branching tree of all triples (δ, G, U) produced in the course of the algorithm. If b is a branch of this tree and (δ', G', U') is a successor of (δ, G, U) in b, then either $\#(U') < \#(U)$ or $min(U') < min(U)$. So b must be finite. □

Algorithm **REDUCTION**(γ, F)
Input: A condition γ and a finite subset F of S.
Output: A finite set RED of pairs (δ, G) that satisfies the assertions of the lemma.

```
BEGIN
    Δ := DET(γ, F);
    RD := {(δ, ∅, U) : δ ∈ Δ, U := {f ∈ F : T_{red,δ}(f) ≠ ∅}
    REPEAT
        (δ, G, U) := some element of RD with U ≠ ∅;
        RD := RD \ {(δ, G, U)};
        f := some minimal element of U;
        (k, c) := NORMALFORM(δ, f, (G ∪ U) \ {f})
        IF k = f THEN RD := RD ∪ {(δ, G ∪ {f}, U \ {f})}
        ELSE
        BEGIN
            Δ := DET(δ, {k});
            RD := RD ∪ {(ε, ∅, (U \ {f})  ∪ G ∪ {k}) :  ε ∈ Δ with T_{red,ε}(k) ≠ ∅}
            ∪ {(ε, G, (U \ {f}) :  ε ∈ Δ with T_{red,ε}(k) = ∅}
        END
    UNTIL for all (δ, G, U) ∈ RD , U = ∅ ;
    RED := {(δ, G) : (δ, G, ∅) ∈ RD, }
END
```

A **reduced Gröbner system** for an ideal I of S (over a case distinction B) is a Gröbner system GS for I (over B) such that for each $(\gamma, G) \in GS$ and every $\pi \in Sp_\gamma$, $\sigma_\pi(G)$ is a **reduced** Gröbner basis of $Id(\sigma_\pi(I))$ in $K_\pi[\mathbf{X}]$.

By combining the algorithms **GRÖBNER SYSTEM** and **REDUCTION**, we are now in a position to construct reduced Gröbner systems:

Corollary 4.2. *For a finite $F \subseteq S$ (and a given case distinction B) one can construct a reduced Gröbner system GS for $Id(F)$ (over B).*

Proof. Let GS be a Gröbner system for $Id(F)$ over B, and let

$$GS' = \bigcup_{(\gamma,G)\in GS} \mathbf{REDUCTION}(\gamma, G).$$

Then by lemma 4.1, GS' is a reduced Gröbner system for $Id(F)$ over B. □

As a byproduct, we can now determine the equivalence classes of $\sim_I$ for an ideal I of S from a reduced Gröbner system for I more easily than in corollary 3.5.

Corollary 4.3. *Let F be a finite subset of S, let GS be a reduced Gröbner system for the ideal $Id(F)$, and let $\Delta = \{\delta : (\delta, G) \in GS\}$. Then $\{Sp_\delta : \delta \in \Delta\}$ refines the equivalence classes of Spec(R) with respect to $\sim_{I(F)}$. Moreover, for $(\delta, G), (\delta', G') \in GS$, Sp_δ and $Sp_{\delta'}$ are subsets of the same equivalence class iff $HT_\delta(G) = HT_{\delta'}(G')$.*

Proof. This is an immediate consequence of the characterization of $\sim_{Id(F)}$ given in lemma 2.6. □

Using the concept of a reduced Gröbner system, it is now natural to define a **reduced comprehensive Gröbner basis** (over a case distiction B) as any set G' of the form $G' = \bigcup\{G : (\gamma, G) \in GS\}$, where GS is a reduced Gröbner system (over B).

It is well-known that a "classical" reduced Gröbner basis G in a polynomial ring $K'[\mathbf{X}]$ is uniquely determined (up to multiplicative constants) by the ideal $Id(G)$; moreover, it has the smallest number of elements among all Gröbner bases of $Id(G)$. For reduced comprehensive Gröbner bases this is not the case. Example: Let $S = \mathbf{Q}[U, V; X, Y]$, and let $f = UX + 1$, $g = VY$. Then both $GS = \{(\{U = 0\}, f), (\{U \neq 0\}, \{f, g\})\}$ and $GS' = \{(\{V = 0\}, f + g), (\{V \neq 0, U = 0\}, \{f\}), (\{V \neq 0, U \neq 0\}, \{f, g\})\}$ are reduced Gröbner systems and $Id(f, g) = Id(f, g, f + g)$. So both $\{f, g\}$ and $\{f, g, f + g\}$ are reduced comprehensive Gröbner bases for the same ideal.

In fact, a reduced comprehensive Gröbner basis will frequently comprise many more polynomials than a non-reduced comprehensive Gröbner basis . So in order to reduce the number of polynomials in comprehensive Gröbner bases as much as possible, the following concept of a **globally reduced comprehensive Gröbner basis** is more useful:

Let $f, f' \in S$, $P \subseteq S$, and suppose $f' = f - mp$ for some $m \in M$, $p \in P$ such that $m \cdot \mathrm{HM}(p)$ is a monomial in f and $\mathrm{HC}(p)$ is a unit in K. Then we say f **reduces globally to f' modulo** P. We say P is **globally reduced**, if no $p \in P$ is globally reducible modulo $P \setminus \{p\}$.

By a slight modification of the usual non-parametric reduction algorithm (compare Buchberger (1985)), one can now specify an algorithm **GLOBAL REDUCTION**(F), that transforms a given finite $F \subseteq S$ into a globally reduced finite $G \subseteq S$ such that $Id(F) = Id(G)$. Moreover, if F is a comprehensive Gröbner basis , so is G. Since a global reduction is a reduction under every specialization, a reduced set F is, in particular, globally reduced. The converse fails to be true as example 7.2 will show.

Similar as before, the concept of **global reduction relative to a given case distinction** can be defined.

5. Some Complexity Bounds

The great generality of a comprehensive Gröbner basis suggests that the construction of a comprehensive Gröbner basis is by far more complicated than that of an ordinary, non-parametric Gröbner basis . The purpose of this section is to show that in the asymptotic worst case comparison to ordinary Gröbner bases , this construction is not as costly as one might expect. For upper complexity bounds on the construction of a comprehensive Gröbner basis it suffices, by proposition 2.8, to consider the generic case of an input system $F = \{f_1, ..., f_k\} \subseteq S_r$ of k "generic" polynomials of degree $deg_{\mathbf{X}}(f_j) = d$ with independent indeterminate coefficients $V_1, ..., V_r$ in $R_r = \mathbf{Z}[V_1, ..., V_r]$, $r = k \cdot d^n$. (Here and in the following $deg_{\mathbf{X}}(f)$ denotes the total degree of a polynomial $f \in S$ with respect to the main variables $\mathbf{X}$.) We want to study the influence on F of the two types of transformations in $S_r = R_r[X_1, \ldots, X_n]$ that lead from F to a comprehensive Gröbner basis G for $Id(F)$, viz. formation of S-polynomials and reduction with respect to a condition.

We begin by studying the transformation of *arbitrary* coefficients $U_1, \ldots, U_m$ of parametric polynomials: Let

$$g \in S = K[U_1, ..., U_m; X_1, ..., X_n].$$

Then we call g **U-homogeneous** of **U-degree** D, if all the coefficients of g are homogeneous polynomials in $U_1, ..., U_m$ of the same degree D.

LEMMA 5.1. *Let $f, g \in S$ be $\mathbf{U}$-homogeneous of $\mathbf{U}$-degree D_f and D_g, respectively, and let γ be a condition. Then*

- *(i) Let $h = \mathrm{SPol}_\gamma(f, g)$; then $h = 0$ or h is $\mathbf{U}$-homogeneous of $\mathbf{U}$-degree $D_h = D_f + D_g$.*
- *(ii) If $f \underset{g}{\longrightarrow} h\ [\gamma]$, then h is $\mathbf{U}$-homogeneous of $\mathbf{U}$-degree $D_h = D_f + D_g$.*

Proof. Let $HM_\gamma(f) = a \cdot s$ and $HM_\gamma(g) = b \cdot t$. Then $h = b \cdot u \cdot f - a \cdot v \cdot g$ for some $u, v \in T$. Then for arbitrary monomials $c \cdot s \in M(f)$, $c' \cdot s' \in M(g)$, we have $deg(b \cdot c) = D_g + deg(a) = D_g + D_f = deg(b) + D_f = deg(c' \cdot a)$. So all the coefficients of h are homogeneous of degree $D_f + D_g$.

Next let $f \underset{g}{\longrightarrow} h\ [\gamma]$ with $h = b \cdot f - e \cdot w \cdot g$, where $e \cdot w \cdot t \in M(f)$. Then for $c \cdot s$ and $c' \cdot s'$ as above, the coefficients of h are of the form $b \cdot c - e \cdot c'$. Since $deg(e \cdot c') = deg(a \cdot c')$, this entails that $b \cdot c - e \cdot c'$ is homogeneous of degree $D_f + D_g$. □

COROLLARY 5.2. *Let $G \subseteq S$ be a finite set of $\mathbf{U}$-homogeneous polynomials of U-degrees $\leq D$. Let $h \in S$ be obtained from polynomials in G by at most q successive formations of S-polynomials and reductions with respect to some conditions in arbitrary order. Then h is $\mathbf{U}$-homogeneous of $\mathbf{U}$-degree $\leq D \cdot 2^q$.*

Proof. Induction on q. □

Notice that all the generic polynomials $f_i \in F$ above are $\mathbf{U}$-homogeneous of $\mathbf{U}$-degree 1. So corollary 5.2 can be applied to $G = F$, i.e. the case polynomials in S_r with "generic" coefficients $V_1, \ldots, V_r$:

COROLLARY 5.3. *Let $F \subseteq S_r$ be as above and let G be a comprehensive Gröbner basis for $Id(F)$ in S_r. If the construction of G involves performing the operation of either forming an S-polynomial or performing a reduction with respect to some condition at most q times, then each $g \in G$ is $\mathbf{V}$-homogeneous of $\mathbf{V}$-degree $\leq 2^q$.*

Next, we study the growth of the degree in the main variables during the computation of a comprehensive Gröbner basis . For this purpose, it is convenient to restrict our attention to input polynomials that are **homogeneous in the main variables**. This restriction is inessential as the following proposition shows:

PROPOSITION 5.4. *Let $F \subseteq S_r$ be as above, let $<$ be an arbitrary term order on T, let Z be a new (homogenizing) variable, let $S_r^* = S[Z]$ with T^* as the set of terms. Extend $<$ to a term order on T^* by putting $Z^j < X_i$ for $j \in \mathbf{N}$, $1 \leq i \leq n$. Let f_i^* denote the homogenization of f_i and let $F^* = \{f_1^*, ..., f_k^*\}$. Let G be a comprehensive Gröbner basis for $Id(F^*)$ constructed from F^* as in section 3. Then every $g \in G$ is homogeneous in the main variables and $\mathbf{V}$-homogeneous in the parameters.*

Next, let $G_* = \{g_* : g \in G\} \subseteq S_r$ be the set of all dehomogenizations of polynomials in G. Then G_* is a comprehensive Gröbner basis for $Id(F)$ in S_r with respect to $<$.

Proof. By definition, the formation of S-polynomials and the reduction of polynomials with respect to some condition preserves homogeneity in the main variables and by corollary 5.3 also the $\mathbf{V}$-homogeneity of all f_i^*. Moreover, by the fact that Z is lexicographically small with respect to all X_i, $HT_\psi(g_*) = (HT_\psi(g))_*$ for an arbitrary $\psi \in Spec(R_r)$ and $g \in G$.

In order to show that G_* is a comprehensive Gröbner basis for $Id(F)$, we check the criterion of lemma 2.3: Let $f \in Id(F)$, $\psi \in Spec(R_r)$ such that $HT_\psi(f)$ is defined. Then for some $j, j' \in \mathbf{N}$, $f^* Z^j \in Id(F^*)$ and $HT_\psi(f^* Z^j) = Z^{j'} \cdot HT_\psi(f)$. So by hypothesis, $HT_\psi(g) \mid HT_\psi(f^* \cdot Z^j)$ for some $g \in G$, and hence $HT_\psi(g_*) = (HT_\psi(g))_* \mid (HT_\psi(f^* \cdot Z^j))_* = HT_\psi((f^*)_*) = HT_\psi(f)$. □

For the rest of this section we will change our notation slightly in order to adapt it to the homogeneous case: $F = \{f_1, ..., f_k\} \subset S_r$ will now be a system of "generic" **homogeneous** polynomials with independent indeterminate coefficients $V_1, ..., V_r$ such that $deg_{\mathbf{X}}(f_j) \leq d$ for $1 \leq j \leq k$.

THEOREM 5.5. *Fix a term order $<$ on T. Let $D = D(n, d, k)$ be a worst-case bound for the $\mathbf{X}$-degrees of all polynomials occuring in a computation of a Gröbner basis G' for $Id(F')$ with respect to $<$ for some system $F' \subseteq K[\mathbf{X}]$ of k homogeneous polynomials of degrees $\leq d$ following some specific selection strategy for the choice of S-polynomials. Let $Q = Q(n, d, k)$ be a worst-case bound for the number of formations of S-polynomials and of reductions occuring in such a computation. Then the same upper bound D on the $\mathbf{X}$-degrees applies to a computation of a comprehensive Gröbner basis G for $Id(F)$ with respect to $<$ from $F \subseteq S_r$, (where F is as above) following the same selection strategy. All polynomials $g \in G$ are $\mathbf{V}$-homogeneous of $\mathbf{V}$-degree $\leq 2^Q$. The total number of formations of S-polynomials and of reductions used in the computation of G is bounded by $D^{2(Q+1)}$.*

Proof. Fix one branch b of the computation tree of the comprehensive Gröbner basis G from F. In b cancel all monomials that are coloured green by their corresponding condition. Then the resulting computation is a computation of a Gröbner basis G' for $Id(\sigma(F))$ for some specialization σ of R_r, following the same selection strategy for S-polynomials. So the $\mathbf{X}$-degrees of all these modified polynomials are bounded by D. By the homogeneity in $\mathbf{X}$ of all the polynomials in b (guaranteeed by proposition 5.4), the same degree bound applies to all the unmodified polynomials in b.

Moreover, the number of formations of S-polynomials and of reductions occuring in b is bounded by Q. So by corollary 5.3, every polynomial in b is $\mathbf{V}$-homogeneous of $\mathbf{V}$-degree $\leq 2^Q$.

If in the whole computation tree of G only the formation of S-polynomials and the reductions are counted as vertices, then the tree has depth Q and branching order $\leq D^2$ (by the definition of the algorithm **DET**). So the total number of these steps in the tree is bounded by $D^{2(Q+1)}$. □

Next, we study the complexity of testing the triviality of $Id(\sigma(F))$ for $F \subseteq S$ and an arbitrary specialization σ of R via the computation of a comprehensive Gröbner basis. Here the bound of d^n in the effective Hilbert Nullstellensatz (obtained in Fitchas & Galligo (1990)) plays a decisive role. It allows us to replace the construction of a full comprehensive Gröbner basis by that of a partial comprehensive Gröbner basis of much lower complexity.

PROPOSITION 5.6. *Let $d \in \mathbf{N}$, let $S' = K'[X_1, ..., X_n]$, let $<$ be a fixed term order on T, let I be an ideal in S, and let G be a finite set of homogeneous polynomials of degree $\leq d$ in I. Then the following assertions are equivalent:*

(i) For all $0 \neq f \in I$ that are homogeneous of degree $\leq d$, there exists $g \in G$ with $HT(g) \mid HT(f)$.

(ii) For all $f \in I$ that are homogeneous of degree $\leq d$, $f \xrightarrow[G]{*} 0$.

(iii) $I = Id(G)$ and for all $f, g \in G$, such that $deg(\mathrm{SPol}(f,g)) \leq d$, $\mathrm{SPol}(f,g) \xrightarrow[G]{*} 0$.

*If these equivalent conditions are satisfied, we call G a d-**partial homogeneous Gröbner basis of** I with respect to $<$.*

Proof. This is obvious by relativizing the "classical" Gröbner basis theory to homogeneous polynomials of degree $\leq d$ (compare Giusti (1984), Möller & Mora (1984)). □

Let us call $G \subseteq S = K[U_1, ..., U_m;\ X_1, ..., X_n]$ a d-**partial homogeneous comprehensive Gröbner basis** of an ideal $I \subseteq S$ (with respect to $<$), if G consists of polynomials that are homogeneous of degree $\leq d$ in the main variables, and if for all specializations $\sigma : R \longrightarrow K'$, $\sigma(G)$ is a d-partial homogeneous Gröbner basis of $Id(\sigma(I))$ with respect to $<$. Next, let $F \subseteq S$, let F^* denote the homogenization of F as in proposition 5.4, let G be a d-partial homogeneous comprehensive Gröbner basis of $Id(F^*)$, and let G_* be the dehomogenization of G as defined in proposition 5.4. Then we call G_* a d-**partial comprehensive Gröbner basis** of $Id(F)$. Then the effective Nullstellensatz of Fitchas & Galligo (1990) yields the parametric test for the triviality of ideals:

THEOREM 5.7. *Let $F = \{f_1, \ldots, f_k\} \subseteq S$, and assume $deg_{\mathbf{X}}(f_i) \leq d$ for $1 \leq i \leq k$. Put*

$$D' = D'(n,d) = \begin{cases} d^n & \text{if } d \geq 3,\ n \geq 2 \\ 3^n & \text{if } d < 3,\ n \geq 2 \\ d+1 & \text{if } n = 1 \end{cases}$$

Let G be a D'-partial comprehensive Gröbner basis (or an arbitrary comprehensive Gröbner basis) of $Id(F)$. For $g \in G$, let $abs_g(\mathbf{U})$ denote the coefficient of the constant term 1 in g and let $C(g)$ denote the set of all non-vanishing coefficients $c(\mathbf{U})$ of terms $1 \neq t \in T$ in g. Then the following assertions are equivalent for every $\pi \in Spec(R)$:

(i) $1 \notin Id(\sigma_\pi(F))$

(ii) $Id(\sigma_\pi(F))$ has a common zero in some extension field of $\sigma_\pi(S)$.

(iii) $Id(\sigma_\pi(F))$ *has a common zero in all algebraically closed extension fields of* $\sigma_\pi(S)$.
(iv) For all $g \in G$, $\bigwedge_{c\in C(g)} \sigma_\pi(c) = 0 \implies \sigma_\pi(abs_g) = 0$

Proof. The equivalence between (i), (ii) and (iii) is the content of Hilbert's Nullstellensatz.

(ii) $\implies$ (iv): Put $\sigma_\pi(\mathbf{U}) = \mathbf{a} \in K'^m$, and let $\mathbf{b}$ be an n-tuple in K'^n such that $f_i(\mathbf{a},\mathbf{b}) = 0$ for $1 \leq i \leq m$. Then $g(\mathbf{a},\mathbf{b}) = 0$ for all $g \in G$, since $G \subseteq Id(F)$. So if $c(\mathbf{a}) = 0$ for all $c(\mathbf{U}) \in C(g)$, then $abs_g(\mathbf{a}) = 0$.

(iv) $\implies$ (i): Suppose $1 \in Id(f_1(\mathbf{a},\mathbf{X}), ..., f_k(\mathbf{a},\mathbf{X}))$, where the ideal is taken in $K_\pi[\mathbf{X}]$.

First, we consider the case that G is a comprehensive Gröbner basis of $Id(F)$. Then by theorem 2.4, there exists $g \in G$ such that $HT_\pi(g)$ divides 1. So $\sigma_\pi(c(\mathbf{U})) = c(\mathbf{a}) = 0$ for all $c \in C(g)$, but $\sigma_\pi(abs_g(\mathbf{U})) = abs_g(\mathbf{a}) \neq 0$.

Next, suppose G is a D'-partial comprehensive Gröbner basis of $Id(F)$. Then G is of the form $G = H_*$ for a D'-partial homogeneous comprehensive Gröbner basis H of $Id(F^*)$. By the effective Nullstellensatz in Fitchas & Galligo (1990), $1 = \sum_{i=1}^k h_i\sigma_\pi(f_i)$ for some polynomials $h_i \in K_\pi[\mathbf{X}]$ such that $deg(h_i f_i) \leq D'$. By homogenizing, we obtain an equation $Z^{D'} = \sum_{i=1}^k h_i'(\mathbf{X},Z) f_i^*(\mathbf{a},\mathbf{X},Z)$, where $\mathbf{a} = \sigma_\pi(\mathbf{U})$, and h_i' homogeneous polynomials in $K_\pi[\mathbf{X},Z]$. with $deg(h_i' f_i) \leq D'$. Since $\sigma_\pi(H)$ is a D'-partial homogeneous Gröbner basis of $Id(\sigma_\pi(F^*))$, we find $h \in H$ such that $HT(\sigma_\pi(h)) = HT_\pi(h) \mid Z^{D'}$. After dehomogenization, this means that $HT_\pi(h_*) \mid 1$, where $h_* \in G$. So $c(\mathbf{a}) = 0$ for all $c \in C(g)$, but $abs_g(\mathbf{a}) \neq 0$. □

Recall from Möller & Mora (1986) that the degree bound $D(n,d,k)$ in theorem 5.5 concerning the $\mathbf{X}$-degrees occuring during the construction of a (comprehensive) Gröbner basis from a set F of homogeneous polynomials is doubly exponential in n. By way of contrast, the parametric testing of ideal triviality by means of a $D'(n,d)$-partial comprehensive Gröbner basis requires only polynomials of $\mathbf{X}$-degrees simply exponential in n:

Corollary 5.8. *Let* $F = \{f_1,\ldots,f_k\} \subseteq S_r$ *be a "generic" system of polynomials, and fix a term order* $<$ *on* T. *Let* $D' = D'(n,d)$ *be defined as in theorem 5.7. Let* $Q' = Q'(n,d,k)$ *be a worst-case bound for the number of formation of* S*-polynomials and of reductions occuring in a computation of a* D'*-partial homogeneous Gröbner basis G' for* $Id(F')$ *with respect to* $<$ *for some system* $F' \subseteq K[\mathbf{X}]$ *of* k *homogeneous polynomials of degrees* $\leq d$ *following some specific selection strategy for the choice of* S*-polynomials. Then the same upper bound* D' *on the* $\mathbf{X}$*-degrees applies to a computation of a* D'*-partial comprehensive Gröbner basis* G *for* $Id(F)$ *with respect to* $<$ *from* $F \subseteq S_r$, *(where* F *is as above) following the same selection strategy. All polynomials* $g \in G$ *are* $\mathbf{V}$*-homogeneous of* $\mathbf{V}$*-degree* $\leq 2^{Q'}$. *The total number of formations of* S*-polynomials and of reductions used in the computation of* G *is bounded by* $D'^{2(Q'+1)}$.

Proof. Let F^* be the homogenization of F in the sense of proposition 5.4. Then F^* is a system of generic homogeneous polynomials in the $n+1$ main variables. Let H be a D'-partial homogeneous comprehensive Gröbner basis of $Id(F^*)$ computed from F^* according to the given selection strategy. Then by proposition 5.6 (iii), the computation of H from F^* does not involve polynomials of $\mathbf{X}$-degrees greater than D'. G is obtained from H by a simple dehomogenization. So the proof of theorem 5.5 is valid with D and Q replaced by D' and Q'. □

6. Applications

Elimination of quantifier-blocks in algebraically closed fields. Let $K = \mathbf{Z}$, and let R, S be defined as before. A **quantifier-free formula** is a boolean combination of polynomial equations $g(\mathbf{U}) = 0$ in the parameters. An **existential formula** is an expression of the form $\exists X_1 ... \exists X_n \varphi(\mathbf{U}, \mathbf{X})$, where $\varphi(\mathbf{U}, \mathbf{X})$ is an $\wedge$-$\vee$-combination of polynomial equations $f(\mathbf{U}, \mathbf{X}) = 0$ and inequalities $f(\mathbf{U}, \mathbf{X}) \neq 0$. A **primitive formula** is an expression of the form $\exists X_1 ... \exists X_n \varphi(\mathbf{U}, \mathbf{X})$, where $\varphi(\mathbf{U}, \mathbf{X})$ is a conjunction of polynomial equations $f(\mathbf{U}, \mathbf{X}) = 0$ and inequalities $f(\mathbf{U}, \mathbf{X}) \neq 0$. A **positive primitive formula** is a primitive formula that contains no inequalities. The problem is to find an algorithm that assigns to each existential formula $\varphi(\mathbf{U})$ a quantifier-free formula $\varphi'(\mathbf{U})$ that is equivalent to $\varphi(\mathbf{U})$ in every algebraically closed field K', i.e. determines the same constructible subset of K'^m as $\varphi(\mathbf{U})$ (compare Rabin (1977)). It suffices to consider the problem for positive primitive φ: In a first step an existential formula may equivalently be rewritten as a disjunction of primitive formulas. Subsequently, any conjunction of polynomial inequalities in the resulting formula may be replaced by a single inequality by forming a product of polynomials. Finally, a single inequality $f(\mathbf{U}, \mathbf{X}) \neq 0$ can be replaced equivalently in any field by the equation $\exists X_{n+1}((f(\mathbf{U}, \mathbf{X}) \cdot X_{n+1} - 1) = 0)$ containing the additional variable X_{n+1}.

Recall that we regard elements f of S as polynomials in $\mathbf{X}$ with coefficients in R. As in theorem 5.7, we let $abs_f(\mathbf{U}) \in R$ be the coefficient of the constant term 1 in f (whether this coefficient is zero or not), and let $C(f)$ denote the set of all non-zero coefficients of f except abs_f.

Theorem 6.1. *Let $F = \{f_1, ..., f_k\} \subseteq S$ and suppose $deg\mathbf{X}(f_i) \leq d$ for $1 \leq i \leq k$, let $D' = D'(n, d)$ be defined as in theorem 5.7, and let G be a D'-partial comprehensive Gröbner basis of $Id(F)$ (or an arbitrary comprehensive Gröbner basis of $Id(F)$). Then the positive primitive formula $\exists X_1 ... \exists X_n (\bigwedge_{i=1}^k f_i(\mathbf{U}, \mathbf{X}) = 0)$ is equivalent to $\epsilon_G(\mathbf{U})$ in every algebraically closed field K', where ϵ_G is the quantifier-free formula*

$$\bigwedge_{g \in G} (abs_g(\mathbf{U}) = 0 \vee \bigvee_{c \in C(g)} c(\mathbf{U}) \neq 0)$$

Proof. This is an immediate consequence of the equivalence $(iii) \iff (iv)$ in theorem 5.7. $\square$

The formula $\epsilon_G(\mathbf{U})$ may be viewed as an affine system of resultants for $F = \{f_1, \ldots, f_k\}$ (compare van der Waerden (1940), section 80).

Membership in ideals depending upon parameters. The negation of the quantifier-free formula ϵ_G constructed in theorem 6.1 may be viewed as a test for the parametric triviality problem for the ideal $Id(F)$. Our goal is now to specify more generally quantifier-free formulas that test the parametric ideal membership. More specifically, given $f \in S$ and a finite $F \subseteq S$, we want to construct a quantifier-free formula $\varphi(\mathbf{U})$, such that in all fields K' and for all $\mathbf{a} \in K'^m$, $f(\mathbf{a}, \mathbf{X}) \in Id(F(\mathbf{a}, \mathbf{X})) \iff \varphi(\mathbf{a})$ holds in K'.

This can be achieved as follows: Let G be a comprehensive Gröbner basis of $Id(F)$ and let $\Gamma = \mathbf{DET}(\emptyset, G)$, and let

$\Delta = \{\delta : \exists\gamma \in \Gamma$ such that $\delta \in \mathbf{DET}(\gamma, \{k\})$ and $T(k) = T_{green,\delta}(k)$ for $(k, c) = \mathbf{NORMALFORM}(\gamma, f, G)\}$.

Let $\overline{\delta}$ denote the conjunction of all polynomial equations and inequalities in δ: Then we put

$$\varphi_{G,f}(\mathbf{U}) \;:=\; \bigvee_{\delta\in\Delta} \overline{\delta}$$

THEOREM 6.2. *For all fields K' and all $\mathbf{a} \in K'^m$, $\varphi_{G,f}(\mathbf{a})$ holds in K' iff $f(\mathbf{a}, \mathbf{X}) \in Id(F(\mathbf{a}, \mathbf{X}))$ (where the ideal is taken in $K'[\mathbf{X}]$).*

Proof. Let σ be the specialization of R mapping $\mathbf{U}$ onto $\mathbf{a}$. If $\sigma(f) \in Id(\sigma(F))$, pick $\gamma \in \Gamma$, $\delta \in \mathbf{DET}(\gamma, \{k\})$ with $ker(\sigma) \in Sp_\delta$, where $(k, c) = \mathbf{NORMALFORM}(\gamma, f, G)$. Then $\sigma(k) \in Id(\sigma(F))$, since $cf - k \in Id(F)$ and $\sigma(c) \neq 0$. So $T(k) = T_{green,\delta}(k)$, and so $\delta \in \Delta$, and so $\overline{\delta}(\mathbf{a})$ and hence $\varphi_{G,f}(\mathbf{a})$ holds in K'.

Conversely, assume $\varphi_{G,f}(\mathbf{a})$ holds in K'; then $ker(\sigma) \in Sp_\delta$ for some $\delta \in \Delta$, and so $f \xrightarrow[G]{*} f'$ $[\delta]$ for some f' with $T(f') = T_{green,\delta}(f')$, and so $\sigma(f') = 0$, and so $\sigma(f) \in Id(\sigma(G)) = Id(\sigma(F))$. □

Finally, we remark that for any parameter-value $\mathbf{a} \in K'$, for which some fixed $\overline{\delta}(\mathbf{a})$ holds in K', $cf(\mathbf{a}, \mathbf{X})$ has in fact a uniform representation as a linear combination of polynomials in $F(\mathbf{a}, \mathbf{X})$, which can be read from a reduction chain $f \xrightarrow[G]{*} f'$ $[\delta]$.

Dimension of varieties depending upon parameters. The quantifier-free formula ϵ_G constructed in theorem 6.1 may also be viewed as a test for the parametric variety $V(F)$ to be of dimension -1. Our goal is now to specify more generally quantifier-free formulas that for a given number d describe those parameter-values for which the variety $V(F)$ has dimension d.

Let, as before, F be a finite subset of S, and let G be a comprehensive Gröbner basis of $Id(F)$ with respect to some fixed term order on T. Put $\Gamma = \mathbf{DET}(\emptyset, G)$ and put $HT_\gamma(G) = \{HT_\gamma(g) : g \in G\}$ for $\gamma \in \Gamma$. For any subset $\mathcal{V}$ of $\mathcal{X} = \{X_1, \ldots, X_n\}$, let $T(\mathcal{V})$ be the set of all $t \in T$ that involve only variables from $\mathcal{V}$. Then we define $\psi_{\mathcal{V},G}(\mathbf{U})$ as the quantifier-free formula

$$\bigvee\{\overline{\gamma} : \gamma \in \Gamma,\ T(\mathcal{V}) \cap HT_\gamma(G) = \emptyset\}$$

For $-1 \leq d \leq n$, we define quantifier-free formulas $\psi_G^d(\mathbf{U})$ as follows:

$\psi_G^n := \psi_G^{\leq n} := \psi_{\mathcal{X},G}$, $\psi_G^{-1} := \neg\epsilon_G$, where ϵ_G is as in theorem 6.1.

For $0 \leq d < n$, we let $\psi_G^{\leq d} := \bigvee\{\psi_{\mathcal{V},G} : \mathcal{V} \subseteq \mathcal{X},\ \#\mathcal{V} = d\}$, $\psi_G^d := \psi_G^{\leq d} \wedge \neg\psi_G^{\leq d+1}$.

THEOREM 6.3. *Let K' be an algebraically closed field and let $\mathbf{a} \in K'^m$. Then the following assertions hold:*

(i) $\psi_G^{\leq d}(\mathbf{a})$ holds in K' iff $V(F(\mathbf{a}, \mathbf{X}))$ has dimension $\leq d$.

(ii) $\psi_G^d(\mathbf{a})$ holds in K' iff $V(F(\mathbf{a}, \mathbf{X}))$ has dimension d.

Proof. This is an immediate consequence of the following facts proved in Kredel & Weispfenning (1988): For a Gröbner basis G of a proper ideal in $K'[\mathbf{X}]$, $\mathcal{V}$ is a set of strongly independent variables in $V(G)$ iff $T(\mathcal{V}) \cap HT(G) = \emptyset$; moreover, the greatest number of elements in such a set $\mathcal{V}$ determines the dimension of $V(G)$. □

Modules of syzygies depending upon parameters. For the classical case of polynomials over a field, it is well-known, how to compute a generating set B for the module M of syzygies for a finite set F of polynomials: First, one passes to a Gröbner basis G of $Id(F)$, next one gets a generating set B' of the module M' of syzygies corresponding to G from "standard representations" of all S-polynomials of members of G, and finally B' is linearly tranformed into a generating set B of the module of syzygies corresponding to F using the tranformations between F and G (see Buchberger (1985)).

For the present parametric situation, we proceed analogously in a semi-global manner: Given a finite $F \subseteq S$, we compute a comprehensive Gröbner basis G with $Id(G) = Id(F)$ and the back-and forth transformations beween F and G. Let $G = \{g_1, \ldots, g_s\}$. Then we want to find a complete case distinction Γ and for every $\gamma \in \Gamma$ a finite subset B_γ of S^s such that for every $\pi \in Sp_\gamma$, $\sigma_\pi(B)$ generates the module $M_\pi = \{\mathbf{p} \in K_\pi[\mathbf{X}]^s : \sum_{k=1}^s p_k \sigma_\pi(g_k) = 0\}$ of all syzygies of $\sigma_\pi(G)$, where $K_\pi = Quot(R/\pi)$. If this is the case, then we call the family $\{B_\gamma\}_{\gamma\in\Gamma}$ a **finite generating system for the pointwise modules of syzygies of G.**

The construction proceeds as follows: We put $\Gamma = \mathbf{DET}(\emptyset, G)$. For every $\gamma \in \Gamma$ and all $1 \leq i < j \leq s$, we let $h_{ij\gamma} = \mathrm{SPol}_\gamma(g_i, g_j) = m_{ij\gamma} g_i + m'_{ij\gamma} g_j$, where $m_{ij}, m'_{ij} \in M$. For every $(h'_{ij\gamma}, c_{ij\gamma}) = \mathbf{NORMALFORM}(\gamma, h_{ij\gamma}, G)$, we have

$$c_{ij\gamma} h_{ij\gamma} - h'_{ij\gamma} \in Id(G),\ T(h'_{ij\gamma}) = T_{green,\gamma}(h'_{ij\gamma}) \text{ and } h_{ij\gamma} \xrightarrow[G]{*} h'_{ij\gamma}\ [\gamma].$$

This yields a representation

$$c_{ij\gamma} h_{ij\gamma} = \sum_{k=1}^{s} f_{ijk\gamma} g_k \ + \ h'_{ij\gamma},$$

where $f_{ijk\gamma} \in S,\ HT_\gamma(f_{ijk\gamma} g_k) \leq HT_\delta(h_{ij\gamma})$.
So, with

$$p_{ijk\gamma} = \begin{cases} f_{ijk\gamma} & \text{for } k \neq i, j \\ f_{ijk\gamma} - c_{ij\gamma} m_{ij\gamma} & \text{for } k = i \\ f_{ijk\gamma} - c_{ij\gamma} m'_{ij\gamma} & \text{for } k = j \end{cases}$$

we get $\sum_{k=1}^s p_{ijk\gamma} g_k = h'_{ij\gamma}$.
As a consequence, we find that, for every $\pi \in Sp_\gamma,\ \gamma \in \Gamma$,

$$\sum_{k=1}^{s} \sigma_\pi(p_{ijk\gamma}) \sigma_\pi(g_k) = 0$$

represents a nontrivial syzygy over $K_\pi(R)$, i.e. by taking the above formula pointwise, one imitates exactly the pattern of the usual construction of a generating set of the module of syzygies of $\sigma_\pi(G)$ (compare Buchberger (1985)). Hence we can define the family $\{B_\gamma\}_{\gamma\in\Gamma}$ as follows:

For $\gamma \in \Gamma$, we put

$$B_\gamma = \{(p_{ij1\gamma}, \ldots, p_{ijs\gamma}) : 1 \leq i < j \leq s\}$$

So we have the following result:

THEOREM 6.4. *The family* $\{B_\gamma\}_{\gamma\in\Gamma}$ *is a finite generating system for the pointwise modules of syzygies of* G.

Deformation of residue algebras. Let F be a finite set of polynomials in S, and put as before $K_\pi = Quot(R/I)$ for $\pi \in Spec(R)$. The problem is to determine how the properties of the residue algebras $A_\pi = S/Id(\sigma_\pi(F))$ vary, when π ranges over all prime ideals in $Spec(R)$. For many properties this problem can be solved algorithmically, once a reduced Gröbner system for $Id(F)$ has been computed. In fact, for most of these properties the set of prime ideals π, where they hold for A_π can be described by a quantifier-free formula obtained directly from a comprehensive Gröbner basis of $Id(F)$.

To begin with, we desribe a quantifier-free formula that determines the dimension of A_π as a K_π-linear space. Let G be a comprehensive Gröbner basis of $Id(F)$, and let $\Gamma = \mathbf{DET}(\emptyset, G)$. For any $\gamma \in \Gamma$, we put $RT_\gamma(G) = \{t \in T : \forall\ g \in G \text{ not } HT_\gamma(g) \mid t\}$. Let $\overline{\gamma}$ be defined as in theorem 6.2. Then we let $\tau_d(\mathbf{U})$ be the quantifier-free formula

$$\bigvee\{\overline{\gamma} : \gamma \in \Gamma,\ \#\ RT_\gamma(G) = d\}$$

for $d \in \mathbf{N}$.

THEOREM 6.5. *(i) For every* $\pi \in Spec(R)$, $dim_{K_\pi}(A_\pi) = d \iff \tau_d(\sigma_\pi(\mathbf{U}))$ *holds in* K_π.

(ii) Let $\pi \in Spec(R)$ *be such that* $Id(\sigma_\pi(F))$ *is a radical ideal, and let* $V(\sigma_\pi(F))$ *denote the variety of* $\sigma_\pi(F)$ *in the algebraic closure of* K_π. *Then*

$$\#\ V(\sigma_\pi(F)) = d \iff \tau_d(\sigma_\pi(\mathbf{U}))\textit{holds in } K_\pi.$$

(iii) For all $\pi \in Spec(R)$, $dim_{K_\pi}(A_\pi)$ *is positive and finite iff* $\psi^0_G(\mathbf{U})$ *holds in all fields. If this is the case, then* $T' = \bigcup_{\gamma\in\Gamma} RT_\gamma(G)$ *contains a basis of* A_π *for all* π, *and so* $dim_{K_\pi}(A_\pi)$ *is bounded by* D^n, *where* $D = max(deg_{X_i}(t) : t \in T')$.

Proof. (i) For any $\gamma \in \Gamma$, $\pi \in Sp_\gamma$, $RT_\gamma(G) = \{t \in T : \forall\ g \in G \text{ not } HT(\sigma_\pi(g)) \mid t\}$. So by a well-known result (see Buchberger (1985)), the residues modulo $\sigma_\pi(I)$ of RT_γ are in $1-1$-correspondence with RT_γ and form a basis of A_π as K_π-linear space.

(ii) Recall that for a radical ideal $Id(\sigma_\pi(F))$, A_π is the coordinate ring of the variety $V(\sigma_\pi(F))$. So $dim_{K_\pi}(A_\pi)$ is the number of points of this variety, provided this number is finite.

(iii) is an immediate consequence of (i) and theorem 6.3. □

COROLLARY 6.6. *Let* GS *be a reduced Gröbner system for* $Id(F)$ *and let* $(\gamma, G) \in GS$. *Let* $\pi, \pi' \in Sp_\gamma$, *and suppose* j *is an isomorphism from* K'_π *onto* $K'_{\pi'}$, *such that* $j(\sigma_\pi(a)) = \sigma_{\pi'}(a)$ *for all coefficients* a *of polynomials in* G. *Then* j *extends canonically to an isomorphism from* A_π *onto* $A_{\pi'}$.

Proof. By the above, the residues of the elements of RT_γ form a basis of A_π as linear space over K'_π for all $\pi \in Sp_\gamma$. We claim that for all $\pi, \pi' \in Sp_\gamma$ the identity map on RT_γ together with j induces an isomorphism of the K_π-algebra A_π onto the $K_{\pi'}$-algebra $A_{\pi'}$. It suffices to show that the structure constants of A_π and $A_{\pi'}$ with respect to the basis RT_γ have the same representatives in R. These structure constants in turn are determined by the representation of any product $t \cdot X_i$ $(1 \le i \le n, t \in RT_\gamma)$ as a linear combination of terms in RT_γ. If $t \cdot X_i \in RT_\gamma$, the representation is the obvious one; if this is not the case, then there exists a unique $g \in G$ with $HT_\gamma(g) = t \cdot X_i$, and so $g - t \cdot X_i$ is the representation of $t \cdot X_i$ as a linear combination of terms in RT_γ in any algebra A_π with $\pi \in Sp_\gamma$. □

Notice that the characterization of the equivalence relation $\sim_{Id(F)}$ in corollary 3.5, $\pi \sim_{Id(F)} \pi'$ implies that A_π and $A_{\pi'}$ have a common subset T' of T as a basis over K_π and $K_{\pi'}$, respectively. So we may conclude:

PROPOSITION 6.7. *Let $\pi, \pi' \in Spec(R)$ and suppose $\pi \sim_{Id(F)} \pi'$. Then $dim_{K_\pi}(A_\pi) = dim_{K_{\pi'}}(A_{\pi'})$.*

Finally, we present quantifier-free formulas that solve the general isomorphism and embedding problem between parametric residue algebras over a fixed algebraically closed field.

We need the following definitions: Let $\mathbf{U}' = (U'_1, \ldots, U'_m)$, let F be a finite subset of S, and let GS be a reduced Gröbner system for $Id(F)$. Consider $1 \le d, d' \in \mathbf{N}$ and $(\gamma, G), (\gamma', G') \in GS$ such that $\#RT_\gamma(G) = d$, $\#RT_{\gamma'}(G') = d'$, and let $\mathbf{Y} = (Z_{ij})$ be a $(d \times d')$-matrix of new indeterminate parameters. Recall from the proof of corollary 6.6 that for all $\pi \in Sp_\gamma$ the structure constants of A_π are determined uniformly by G as polynomials in $\mathbf{U}$. Similar for $\pi' \in Sp_{\gamma'}$. So it is now straighforward to write down a quantifier-free formula $\mu_{d,d',\gamma,\gamma'}(\mathbf{U}, \mathbf{U}')$ that expresses in every field $K' \supseteq K_\pi \cup K_{\pi'}$ the fact that the K'-linear map $A_\pi \longrightarrow A_{\pi'}$ given by the matrix $\mathbf{Y}$ with respect to the K'-linear bases RT_γ of A_π and $RT_{\gamma'}$ of $A_{\pi'}$ is compatible with the structure constants of A_π and $A_{\pi'}$ in such a way that the map is a homomorphism of K'-algebras.

Next, let $\rho(\mathbf{Y})$ be a quantifier-free formula expressing the assertion that $det(\mathbf{Y}) \neq 0$, and let $\iota_d(\mathbf{U}, \mathbf{U}', \mathbf{Y})$ be the quantifier-free formula

$$\bigvee\{\overline{\gamma} \wedge \overline{\gamma'} \wedge \mu_{d,d,\gamma,\gamma'}(\mathbf{U}, \mathbf{U}') \wedge \rho(\mathbf{Y}) \ :$$

$$(\gamma, G), (\gamma', G') \in GS, \ \#RT_\gamma(G) = d, \ \#RT_{\gamma'}(G') = d\}.$$

Using determinants of quadratic submatrices of $\mathbf{Y}$, we can also write down a quantifier-free formula $\rho_r(\mathbf{Y})$ that expresses the fact that $\operatorname{rank}(\mathbf{Y}) = r$ $(0 \le r \le \min(d, d'))$. We let $\iota_{d,d'}(\mathbf{U}, \mathbf{U}', \mathbf{Y})$ be the formula

$$\bigvee\{\overline{\gamma} \wedge \overline{\gamma'} \wedge \mu_{d,d',\gamma,\gamma'}(\mathbf{U}, \mathbf{U}') \wedge \rho_d(\mathbf{Y}) \ :$$

$$(\gamma, G), (\gamma', G') \in GS, \ \#RT_\gamma(G) = d, \ \#RT_{\gamma'}(G') = d'\}$$

for $d \le d'$. Finally, we let $\varphi_d(\mathbf{U}, \mathbf{U}')$ and $\varphi_{d,d'}(\mathbf{U}, \mathbf{U}')$ $(d \le d')$ be quantifier-free formulas equivalent to

$$\exists \mathbf{Y} \ \iota_d(\mathbf{U}, \mathbf{U}', \mathbf{Y}) \quad \text{and} \quad \exists \mathbf{Y} \ \iota_{d,d'}(\mathbf{U}, \mathbf{U}', \mathbf{Y})$$

respectively, by the elimination of the quantifier-block in algebraically closed fields described above. Then by construction, we have the following result:

THEOREM 6.8. *Let K' be an algebraically closed field, let $\mathbf{a}, \mathbf{a}' \in K'^m$, and let $\pi, \pi' \in Spec(R)$ be the kernels of the specializations $\mathbf{U} \mapsto \mathbf{a}$, $\mathbf{U}' \mapsto \mathbf{a}'$. Then the following holds:*

(i) $\varphi_d(\mathbf{a}, \mathbf{a}')$ holds in K' iff the residue algebras A_π and $A_{\pi'}$ are isomorphic as K'-algebras.

(ii) $\varphi_{d,d'}(\mathbf{a}, \mathbf{a}')$ holds in K' iff $dim_{K'}(A_\pi) = d$, $dim_{K'}(A_{\pi'}) = d'$ and A_π is embeddable into $A_{\pi'}$ as a K'-algebra.

7. Examples

In this section we illustrate the method of comprehensive Gröbner bases and its applications by a few simple examples that have been computed using the implementation of the algorithms above by E. Schönfeld (Schönfeld (1991)) in the computer algebra system ALDES/SAC-2. All CPU-timings below refer to an IBM 9370 under VM/CMS; CASES refers to the number of conditions in the Gröbner system that is constructed. The term order is invers-lexicographic in all examples except for example 7.3, where it is lexicographic.

EXAMPLE 7.1. We consider two "generic" quadratic univariate polynomials $f = a_0X^2 + a_1X + a_2$, $g = b_0X^2 + b_1X + b_2$ in the ring $S = \mathbf{Q}[a_0, a_1, a_2, b_0, b_1, b_2; X]$. Let $F = \{f, g\}$; then the following set $G = \{f, g, h_1, h_2, h_3, h_4, h_5, h_6\}$ is a comprehensive Gröbner basis of $Id(F)$:

$h_1 = (a_0b_1 - b_0a_1)X^2 \;+\; (a_2b_1 - a_1b_2)$,
$h_2 = (-a_0a_1b_0)X^3 \;+\; (a_0a_2b_0 - a_0a_1b_1)X^2 \;+\; (a_2^2b_0 - a_1a_2b_1 - a_1^2b_2)$,
$h_3 = (-b_0b_1a_0)X^3 \;+\; (b_0b_2a_0 - b_0b_1a_1)X^2 \;+\; (b_2^2a_0 - b_1b_2a_1 - b_1^2a_2)$,
$h_4 = (a_1b_0 - b_1a_0)X \;+\; (a_2b_0 - b_2a_0)$,
$h_5 = a_0 \cdot R(g, f)$, $h_6 = b_0 \cdot R(f, g)$, where R(g,f) denotes the resultant of g and f.

Notice the symmetry between h_2, h_3 and between h_5, h_6; moreover the homogeneity of the coefficients of all h_i in the parameters, and the fact that the degree in the main variable X has increased in the passage from F to G. G is a reduced comprehensive Gröbner basis as well. Moreover, since none of the highest coefficients of these polynomials is in $\mathbf{Q}$, G is also globally reduced (TIME = 2.2 sec, CASES = 23).

Under the hypothesis of the cases distinction $B = \{\{a_0 \neq 0, b_0 \neq 0\}\}$, the computed comprehensive Gröbner basis consists of f, g, h_4, h_5, h_6 only; the computed quantifier-free formula equivalent to $\exists x(f = 0 \wedge g = 0)$ is easily seen to be equivalent to $R(f, g) = 0$ (TIME= 0.7 sec; CASES = 5).

EXAMPLE 7.2. Let $F = \{f, g\} \subseteq \mathbf{Q}[u, v; X, Y]$ be given by $f = vXY + uX^2 + X$, $g = uY^2 + X^2$. Then the following is a comprehensive Gröbner basis G for $Id(F)$:

$G = \{f, g, h_1\}$, where $h_1 = (u^3 + v^2)X^3 \;+\; 2u^2X^2 \;+\; uX$,

Inspection of the highest coefficients shows that G is also globally reduced. The possible dimensions of the variety $V(F)$ can now easily be determined as follows:

$$dimV(F) = \begin{cases} 1 & \text{if } u = 0 \\ 0 & \text{otherwise} \end{cases}$$

In the case $u \neq 0$, where $V(F)$ has finitely many elements, these elements can easily be computed from G. A reduced comprehensive Gröbner basis G' for $Id(F)$ contains in addition the following polynomials:

$h_2 = 2u^3Y^2 - (v^2 + u^3)X^3 - uX$,

$h_3 = u^2Y^2 - vXY - X$,
$h_4 = u^2Y^2 - (v^2 + u^3)X^4 - 2u^2X^3$,
$h_5 = 2uvXY - (v^2 + u^3)X^3 + uX$
(TIME = 1.2 sec; CASES = 6).

Our next example is taken from Böge et al. (1986); it is due to Raksanyi and Walter and describes a chemical equilibrium.

EXAMPLE 7.3. $F = \{f_1, f_2, f_3, f_4\} \subseteq \mathbf{Q}[a_1, a_2, a_3, a_4; X_1, X_2, X_3, X_4]$ with
$f_1 = X_4 - (a_4 - a_2)$,
$f_2 = X_1 + X_2 + X_3 + X_4 + (a_1 + a_3 + a_4)$,
$f_3 = X_1X_3 + X_1X_4 + X_2X_3 + X_3X_4 - (a_1a_4 + a_1a_3 + a_3a_4)$,
$f_4 = X_1X_3X_4 - a_1a_3a_4$.
The following set $G = \{f_1, h_1, h_2, h_3, h_4, h_5\}$ is a comprehensive Gröbner basis of $Id(F)$:
$h_1 = X_1 + X_2 + X_3 - (a_3 + a_2 + a_1)$,
$h_2 = (a_3a_4^2 + a_2a_4^2 + a_1a_4^2 - 2a_2a_3a_4 - 2a_2^2a_4 - 2a_1a_2a_4 + a_2^2a_3 + a_2^3 + a_1a_2^2)X_2X_3^2 - (a_3^2a_4^2 + 2a_2a_3a_4^2 + a_1a_3a_4^2 + a_2^2a_4^2 + 2a_1a_2a_4^2 + a_1^2a_4^2 - 2a_2a_3^2a_4 - 4a_2^2a_3a_4 - 3a_1a_2a_3a_4 - 2a_2^3a_4 - 4a_1a_2^2a_4 - 2a_1^2a_2a_4 + a_2^2a_3^2 + 2a_2^3a_3 + 2a_1a_2^2a_3 + a_2^4 + 2a_1a_2^3 + a_1^2a_2^2)X_2X_3 + (a_3^2a_4^3 + 2a_2a_3a_4^3 + 2a_1a_3a_4^3 + a_2^2a_4^3 + 2a_1a_2a_4^3 + a_1^2a_4^3 - 3a_2a_3^2a_4^2 - 6a_2^2a_3a_4^2 - 6a_1a_2a_3a_4^2 - 3a_2^3a_4^2 - 6a_1a_2^2a_4^2 - 3a_1^2a_2a_4^2 + 3a_2^2a_3^2a_4 + 6a_2^3a_3a_4 + 6a_1a_2^2a_3a_4 + 3a_2^4a_4 + 6a_1a_2^3a_4 + 3a_1^2a_2^2a_4 - a_2^3a_3^2 - 2a_2^4a_3 - 2a_1a_2^3a_3 - a_2^5 - 2a_1a_2^4 - a_1^2a_2^3)X_2 + (a_3a_4^3 + a_2a_4^3 + a_1a_4^3 - 3a_2a_3a_4^2 + a_1a_3a_4^2 - 3a_2^2a_4^2 - 3a_1a_2a_4^2 + 3a_2^2a_3a_4 - a_1a_2a_3a_4 + 3a_2^3a_4 + 3a_1a_2^2a_4 - a_2^3a_3 - a_2^4 - a_1a_2^3)X_3^2 - (a_3^2a_4^3 + a_2a_3a_4^3 + 2a_1a_3a_4^3 + a_1a_2a_4^3 + a_1^2a_4^3 - 2a_2a_3^2a_4^2 + a_1a_3^2a_4^2 - 2a_2^2a_3a_4^2 - 3a_1a_2a_3a_4^2 + a_1^2a_3a_4^2 - 2a_1a_2^2a_4^2 - 2a_1^2a_2a_4^2 + a_2^2a_3^2a_4 - 2a_1a_2a_3^2a_4 + a_2^3a_3a_4 - 2a_1^2a_2a_3a_4 + a_1a_2^3a_4 + a_1^2a_2^2a_4 + a_1a_2^2a_3^2 + a_1a_2^3a_3 + a_1^2a_2^2a_3)X_3 - (a_2a_3^2a_4^3 - a_1a_3^2a_4^3 + 2a_2^2a_3a_4^3 + a_1a_2a_3a_4^3 - a_1^2a_3a_4^3 + a_2^3a_4^3 + 2a_1a_2^2a_4^3 + a_1^2a_2a_4^3 - a_2a_3^3a_4^2 - 5a_2^2a_3^2a_4^2 - a_1a_2a_3^2a_4^2 - a_1^2a_3^2a_4^2 - 7a_2^3a_3a_4^2 - 8a_1a_2^2a_3a_4^2 - a_1^2a_2a_3a_4^2 - 3a_2^4a_4^2 - 7a_1a_2^3a_4^2 - 5a_1^2a_2^2a_4^2 - a_1^3a_2a_4^2 + 2a_2^2a_3^3a_4 + a_1a_2a_3^3a_4 + 7a_2^3a_3^2a_4 + 7a_1a_2^2a_3^2a_4 + 2a_1^2a_2a_3^2a_4 + 8a_2^4a_3a_4 + 14a_1a_2^3a_3a_4 + 7a_1^2a_2^2a_3a_4 + a_1^3a_2a_3a_4 + 3a_2^5a_4 + 8a_1a_2^4a_4 + 7a_1^2a_2^3a_4 + 2a_1^3a_2^2a_4 - a_2^3a_3^3 - a_1a_2^2a_3^3 - 3a_2^4a_3^2 - 5a_1a_2^3a_3^2 - 2a_1^2a_2^2a_3^2 - 3a_2^5a_3 - 7a_1a_2^4a_3 - 5a_1^2a_2^3a_3 - a_1^3a_2^2a_3 - a_2^6 - 3a_1a_2^5 - 3a_1^2a_2^4 - a_1^3a_2^3)$,
$h_3 = (a_4 - a_2)X_2X_3 + (a_4 - a_2)X_3^2 - (a_3a_4 + a_2a_4 + a_1a_4 - a_2a_3 - a_2^2 - a_1a_2)X_3 + a_1a_3a_4$,
$h_4 = (a_4 - a_2)X_2 + X_3^2 - (a_3 + a_2 + a_1)X_3 - (a_2a_4 - a_2a_3 - a_1a_3 - a_2^2 - a_1a_2)$,
$h_5 = X_3^3 - (a_4 + a_3 + a_1)X_3^2 + (a_3a_4 + a_1a_4 + a_1a_3)X_3 - a_1a_3a_4$
Moreover, G is globally reduced.
As an application, the possible dimensions of the variety $V(F)$ are obtained as $-1, 0, 1$ with explicit quantifier-free formulas describing these three cases. In particular $dim V(F) = 0 \iff (a_4 - a_2) \neq 0$. (TIME = 16.4 sec; CASES = 7).

Our final example shows that comprehensive GBs can sometimes also be used for quantifier elimination in real closed fields. It has been presented in Davenport & Heintz (1988) as an example, where real quantifier elimination by the Collins method of cylindrical algebraic decomposition runs into enormous difficulties.

EXAMPLE 7.4. Consider the following formula:

$$\exists c \forall b \forall a (((a = d \wedge b = c) \vee (a = c \wedge b = 1)) \Longrightarrow a^2 = b)$$

By eliminating the universal quantifiers in favour of existential quantifiers and negations and computing two comprehensive Gröbner bases (the first with b, a as main variables and c, d as parameters, the second with c as main variable and d as parameter) one finds the quantifier-free formula $d^4 - 1 = 0$ to be equivalent to the formula above in every algebraically closed field of characteristic zero. Simple inspection of these elimination steps shows moreover that this equivalence is valid in the field of reals as well (TIME = 1.2 sec).

8. Some Generalizations

We have shown that the basic constructions and applications of Gröbner bases in polynomial rings over fields can be performed globally for polynomial rings with parameters that admit arbitrary specializations in fields.

This raises the question, to what an extent this method can be applied to more general Gröbner basis constructions.

First, let us consider universal Gröbner bases , i.e. Gröbner bases that have this property simultaneously for all term orders (see Mora & Robbiano (1988), Schwartz (1988), Weispfenning (1989a), Schemmel (1989)) Here, a combination of both algorithms is straightforward and presents no problems. As a result, one can compute a **universal comprehensive Gröbner basis** , i.e. an ideal basis that has the Gröbner property with respect to all term orders and all specializations of parameters in arbitrary fields.

A considerable extension of the construction of comprehensive Gröbner bases - and in fact of universal comprehensive Gröbner bases - is possible for non-commutative polynomial rings of solvable type (see Kandri-Rody & Weispfenning (1990)). This is of considerable interest for computations in algebras arising in quantum physics that frequently depend on parameters. An outline of this theory has been presented in Kredel & Weispfenning (1990).

For commutative parametric polynomial rings, where we admit specializations in more general commutative ground rings, comprehensive Gröbner bases do not exist in general. This applies in particular to specializations in the ring **Z** of integers:

THEOREM 8.1. *Comprehensive Gröbner bases do not exist for arbitrary ideals in* $\mathbf{Z}[U; X]$*, with respect to specializations in* **Z**.

Proof. Let $S = \mathbf{Z}[U; X]$, let $f = 2X,\ g = UX + 1$, and assume for a contradiction that $I = Id(\{f, g\})$ has a comprehensive Gröbner basis G with respect to specializations in **Z**. Then $1 \in I$, if we specialize U to an even number and $1 \notin I$, if we specialize U to an odd number. So G must contain some polynomial $g(U, X)$ such that $g(a, X) = \pm 1$, if a is even, and $g(a, X) \neq \pm 1$, if a is odd. This is impossible, since the coefficients of G with respect to X are univariate polynomials in U, and hence take on two given values only finitely many times, unless they are constant. □

This argument can easily be generalized to show that comprehensive Gröbner bases do not exist for arbitrary ideals with respect to specializations in a fixed commutative principal ideal domain that is not a field or a valuation ring.

References

Apel J., Lassner W. (1988), An extension of Buchberger's algorithm and calculations in enveloping fields of Lie algebras, J. Symb. Comp. 6, 361-370.

Böge W., Gebauer R., Kredel H. (1986), Some examples for solving systems of algebraic equations by calculating Gröbner bases , J. Symb. Comp. 1, 83-98.

Buchberger B.(1985), Gröbner bases: An algorithmic method in polynomial ideal theory, chap. 6 in *Recent Trends in Multidimensional System Theory*, N. K. Bose Ed., Reidel Publ. Comp..

Buchberger B. (1987), Applications of Gröbner bases in non-linear computational geometry, in *Trends in Computer Algebra*, R. Janssen Ed., Springer LNCS vol. 296, pp 52-80.

Buchberger B. (1988), Gröbner bases and generalized Sylvester matrices, unpublished notes, Universität Linz.

Computer Algebra, Symbolic and Algebraic Computation, B.Buchberger, G. E. Collins, R. Loos Eds., Springer Verlag 1982/83.

Davenport J.H., Heintz J. (1988), Real quantifier elimination is doubly exponential, J. Symb. Comp. 5, 29-36.

Faas W. (1992), Implementierung eines Algorithmus zur Berechnung umfassender Gröbnerbasen unter Scratchpad II, Diploma thesis, University of Passau.

Ferro A., Gallo G. (1988), Gröbner bases, Ritt's algorithm and decision procedures for algebraic theories, in *Proc. AAECC-5, Menorca, 1987,* L. Huguet, A. Poli Eds., Springer LNCS vol. 356, pp. 230-237.

Fitchas N., Galligo A. (1990), Nullstellensatz effectif et conjecture de Serre (theoreme de Quillen-Suslin) pour le calcul formel, Mathem. Nachrichten 149, 231-253.

Gianni P. (1989), Properties of Gröbner bases under specialization, in *EUROCAL '87*, J.H.Davenport Ed., Springer LNCS vol. 378, pp. 293-297.

Gianni P., Mora T. (1988), Algebraic solution of systems of polynomial equations using Gröbner bases, in *Proc. AAECC-5, Menorca, 1987,* L. Huguet, A. Poli Eds., Springer LNCS vol. 356, pp. 247-257.

Giusti M. (1984), Some effectivity problems in polynomial ideal theory, in *EUROSAM' 84*, J. Fitch Ed., Springer LNCS vol. 174, pp. 159-171.

Kalkbrener M., Solving systems of algebraic equations by using Gröbner bases, in *EUROCAL '87*, J.H.Davenport Ed., Springer LNCS vol. 378, pp. 282-292.

Kandri-Rody A., Weispfenning V. (1990), Non-commutative Gröbner bases in algebras of solvable type, J. Symb. Comp. 9, 1-26.

Kredel H., Weispfenning V. (1988), Computing dimension and independent sets for polynomial ideals, J. Symb. Comp. 6, 231-248.

Kredel H., Weispfenning V. (1990), Parametric Gröbner bases in rings of solvable type, Proc. IV. International Conference on Computer Algebra in Physical Research, Joint Institute for Nuclear Research Dubna, USSR, May 1990; World Scientific, Singapore, 1991, pp. 236-244.

Möller H.M., Mora T. (1984), Upper and lower bounds for the degree of Gröbner bases , in *EUROSAM 84*, J. Fitch Ed., Springer LNCS vol. 174, pp.172-183.

Möller H.M., Mora T. (1986), New constructive methods in classical ideal theory, J. of Algebra 100, 138-178.

Mora T.,(1986) Gröbner bases for non-commutative polynomial rings, in *Proc. AAECC-3, Grenoble, 1985,* J. Calmet Ed., Springer LNCS vol. 229, pp. 353-362.

Mora T. (1988), Standard bases and non-Noetherianity: Non-commutative polynomial rings, in *Proc. AAECC-4, Karlsruhe, 1986,* Th. Beth, M. Clausen Eds., Springer LNCS vol. 307, pp. 98-109.

Mora T., Robbiano L. (1988), The Gröbner Fan of an ideal, J Symb. Comp. 6, 183 - 208.

Rabin M.O. (1977), Decidable theories, in *Handbook of Mathematical Logic*, J. Barwise Ed., North–Holland, pp. 595-630.

Robbiano L. (1985), Term orderings on the polynomial ring, in *EUROCAL '85*, B.F.Caviness Ed., Springer LNCS vol. 204, pp. 513-517.

Rump S.M. (1987), Algebraic computation, numerical computation and verified inclusions, in *Trends in Computer Algebra*, R. Janssen Ed., Springer LNCS vol. 296, pp. 177-197..

Schemmel K.-P.(1989), An extension of Buchberger's algorithm to compute all reduced Gröbner bases of a polynomial ideal, in *EUROCAL '87*, J.H.Davenport Ed., Springer LNCS vol. 378, pp. 300-310.

Schönfeld E. (1991), Parametrische Gröbnerbasen im Computeralgebra System ALDES/SAC-2, Diploma thesis, University of Passau.

Schwartz N. (1988), Stability of Gröbner bases, J. pure and appl. Algebra 53, 171 - 186.

van der Waerden,B.L. (1940), *Moderne Algebra*, Teil II, Springer Verlag.

Weispfenning V. (1987), Admissible orders and linear forms, ACM SIGSAM Bulletin 21,2, 16-18.

Weispfenning V. (1988), Some bounds for the construction of Gröbner bases, 1987, in *Proc. AAECC-4, Karlsruhe, 1986,* Th. Beth, M. Clausen Eds., Springer LNCS vol. 307, pp. 195 -201.

Weispfenning V. (1989a), Constructing Universal Gröbner bases, in *Proc. AAECC-5, Menorca, 1987,* L. Huguet, A. Poli Eds., Springer LNCS vol. 356, pp. 408-417.

Weispfenning V. (1989), Gröbner bases in polynomial rings over commutative regular rings, in *EUROCAL '87*, J.H.Davenport Ed., Springer LNCS vol. 378, pp. 336-347.