Canonical Comprehensive Gröbner Bases

Volker Weispfenning
Fakultät für Mathematik und Informatik
Universität Passau
D-94030 Passau, Germany

e-mail: `weispfen@uni-passau.de`

MIP-0201
January, 2002

Abstract

Comprehensive Gröbner bases for parametric polynomial ideals were introduced, constructed, and studied by the author in 1992. Since then the construction has been implemented in the computer algebra systems ALDES/SAC-2, MAS, REDUCE and MAPLE. A comprehensive Gröbner basis is a finite subset G of a parametric polynomial ideal I such that $\sigma(G)$ constitutes a Gröbner basis of the ideal generated by $\sigma(I)$ under all specializations σ of the parameters in arbitrary fields. This concept has found numerous applications. In contrast to reduced Gröbner bases, however, no concept of a canonical comprehensive Gröbner basis was known that depends only on the ideal and the term order. In this note we find such a concept under very general assumptions on the parameter ring. After proving the existence and essential uniqueness of canonical comprehensive Gröbner bases in a non-constructive way, we provide a corresponding construction for the classical case, where the parameter ring is a multivariate polynomial ring. It proceeds via the construction of a canonical faithful Gröbner system. Some simple examples illustrate the features of canonical comprehensive Gröbner bases. Besides their theoretical importance, canonical comprehensive Gröbner bases are also of potential interest for efficiency reasons as indicated by the research of A. Montes.

1 Introduction

Let Q be an integral domain, let R be the polynomial ring $Q[U_1, \ldots, U_m]$ in the parameters $U_1, \ldots, U_m$, and let S be the polynomial ring $R[X_1, \ldots, X_n]$ over the parameter ring R in the variables $X_1, \ldots, X_n$. Fix a term order $<$ on the set $T = T(X_1, \ldots, X_n)$ of terms in the variables $X_1, \ldots, X_n$. Then it is well-known [Wei92, BWK98] that in general a Gröbner basis in S with respect to the variables $X_1, \ldots, X_n$ will no longer remain a Gröbner basis in $K'[X_1, \ldots, X_n]$ when the parameters $U_1, \ldots, U_m$ are specialized to some values in a field K'. Special cases, where Gröbner bases are specialization-invariant have been studied in [Bec94, Kal97, FGT01].

This fact motivates the following definition: For any finite parametric polynomial set $F \subseteq S$, a comprehensive Gröbner basis of the ideal $Id(F)$ generated by F is a finite ideal basis G of $Id(F)$ that is a Gröbner basis of the ideal generated by $Id(F)$ in $K'[X_1, \ldots, X_n]$ for every specialization of the parameters $U_1, \ldots, U_m$ in an arbitrary field K'.

The existence of comprehensive Gröbner bases was shown in [Wei92]; the paper provided moreover a construction of a comprehensive Gröbner basis G from F and a given term order on the variables $X_1, \ldots, X_n$ via a Gröbner system together with experimental results in an implementation by E. Schönfeld [Sch91] in ALDES/SAC-2. Subsequent implementations of variants of this construction in SCRATCHPAD by W. Faas [Faa92], in MAS by M. Pesch [Pes94] (see http://www.fmi.uni-passau.de/algebra/projects/mas.php3), in REDUCE by A. Dolzmann and T. Sturm (see http://www.fmi.uni-passau.de/ reduce/cgb/), and in LISP by Marek Rychlik (see http://alamos.math.arizona.edu/CGB/latex-doc/manual/node4.html) followed. Roughly speaking, comprehensive Gröbner bases provide parametric generalizations of all immediate algebraic and geometric applications of Gröbner bases including parametric ideal and syzygy problems, parametric ideal dimension, and quantifier elimination for algebraically closed fields. The practical importance of comprehensive Gröbner bases was underlined by a series of papers providing significant applications in diverse scientific areas [KW91, RE93, RE95, Wei95, Mon95, Mon98, PSWZ98].

A considerable improvement in the practical efficiency of computing a Gröbner system was obtained by A. Montes in [Mon99, Mon01] by a detailed analysis of the necessary case distinctions concerning specializations of the parameters. While this paper contains good heuristics for computing a small number of case distinctions, and thus a small resulting Gröbner system, it fails to define in an algorithm-independent way, what the weakest conditions on the generic case for parameter specializations should be. This in turn is the nucleus for finding small systems of cases deviating from this generic case. The next problem is then to iterate these approach for all non-generic cases; this is completely left open in [Mon99, Mon01].

Inspired by the practical approach of Montes, I was encouraged to reconsider the natural theoretical problem that has bothered me since the discovery of comprehensive Gröbner bases 10 years ago: Given a parametric ideal I in the ring S; is there a purely structural concept of a *canonical comprehensive Gröbner basis* for I that always exists and is sufficiently uniquely determined by the ideal I and the chosen term order on T.

For "ordinary" non-parametric Gröbner bases the corresponding canonical object is of course the unique reduced Gröbner basis of I (see [BWK98]). In a first attempt to mimic reduced Gröbner bases for the parametric case, I defined and constructed in [Wei92] *globally reduced comprehensive Gröbner bases*; but these are still far from being unique. Similarly the concepts introduced in [Mon99, Mon01] come closer towards a "canonical" Gröbner system but are still only algorithm dependent approximations of this goal. So the concept of a canonical Gröbner system and a canonical comprehensive Gröbner basis remained elusive.

In the following this problem is solved both in a platonistic and a constructive manner. The solution requires among others an extension of the concept of Gröbner systems and comprehensive Gröbner bases to more general parameter rings besides multivariate polynomial rings over integral domains or fields. We consider instead arbitrary Noetherian domains equipped with a well-quasi-order as parameter rings R. In fact, if we restrict ourselves from the outset to the study of finitely generated ideals, then we can drop the assumption of Noetherianity. We define two kinds of canonical Gröbner systems: Faithful Gröbner systems in the spirit of [Wei92] leading to canonical comprehensive Gröbner bases, and non-faithful Gröbner systems in the spirit of [Mon01], where the conditions describing the various cases concerning specialization of parameter are essential and cannot be dropped. For the classical case, where the parameter ring is a polynomial ring over a field we outline a construction of a (faithful) Gröbner system and a canonical comprehensive Gröbner basis from a finite ideal basis and a term order. Several simple examples illustrate the concepts and the constructions.

2 Generic Gröbner bases

We use the notation of [BWK98]. Let R be a Noetherian domain with quotient field K. We denote the polynomial ring $R[X_1, \ldots, X_n]$ by S and the polynomial ring $K[X_1, \ldots, X_n]$ by S'. The set of terms in the indeterminates

$X_1, \ldots, X_n$ is denoted by T. A *specialization* of R is a homomorphism $\sigma : R \longrightarrow K'$, where K' is a field. So for every specialization σ of R the image $\sigma(R)$ is an integral domain, and hence the kernel $ker(\sigma)$ of σ is a prime ideal in R. Conversely for every prime ideal P of R there exists a specialization σ_P of R with $ker(\sigma_P) = P$; it suffices to take as the canonical homomorphism $\sigma : R \longrightarrow K'$, where $\sigma(r) = r + P$ and K' is the quotient field of R/P.

Every specialization $\sigma : R \longrightarrow K'$ of R extends canonically to a homomorphism $\sigma : S \longrightarrow K'[X_1, \ldots, X_n]$ by applying σ coefficientwise.

We let $<$ be a term order on T. Then every ideal I of S extends canonically to an ideal $I' = KI$ in S'. The extended ideal I' has a reduced Gröbner basis G wrt. $<$ in S'. G is uniquely determined by I' and $<$, and hence also uniquely determined by I and $<$. All polynomials in G are monic. We call any set H of the form $H = \{a_g g \mid g \in G, 0 \neq a_g \in K\}$ a *minimal Gröbner basis* of I'. So for any minimal Gröbner basis H of I', $|H| = |G|$ and $G = \{HC(h)^{-1}h \mid h \in H\}$.

In order to get sufficient uniqueness for the generic Gröbner bases we want to find, we consider the following additional conditions on the ring R: We call a linear quasi-order $\preceq$ on $R^* = R \setminus \{0\}$ a *well-quasi-order (wqo)* on R, if every non-empty subset M of R contains a $\preceq$-minimal element. We denote the equivalence relation induced by $\preceq$ by $\sim$; so we have

$$a \sim b \iff a \preceq b \text{ and } b \preceq a.$$

The equivalence class of a wrt. $\sim$ is denoted by a .

Let now $\preceq$ be a wqo on R and let $<$ be a term order on T. Denote the set of all monomials at with $0 \neq a \in R$, $t \in T$ in S by M. Then $\preceq$ extends to a wqo of M by a "lexicographic" combination of $<$ and $\preceq$:

$$at \preceq a't' \iff t < t' \text{ or } (t = t' \text{ and } a \preceq a')$$

In a next step $\preceq$ extends to a wqo on $S \setminus \{0\}$: Denote the set of monomials of $f \in S$ by $M(f)$. Then we put

$$f \preceq g \iff \text{by comparing the respective monomials of}$$

$$f \text{ and } g \text{ in decreasing order until two non-equivalent}$$

$$\text{monomials } m \in M(f), m' \in M(g) \text{ occur with } m \preceq m'.$$

This is analogous to the extension of a term order to non-zero polynomials in [BWK98]. An analogous proof shows that $\preceq$ is indeed a wqo on $S \setminus \{0\}$. The equivalence relation $\sim$ on $S \setminus \{0\}$ is defined in the same way as on $R \setminus \{0\}$.

Next we define for each $g \in G$ a subset J_g of R as follows:

$$J_g = \{a \in R \mid ag \in I\}$$

Then one easily verifies that J_g is a non-zero ideal of R.

We call a specialization σ of R *essential for* $(I,<)$, if for some $g \in G$ $ker(\sigma) \supseteq J_g$; otherwise we call σ of R *inessential for* $(I,<)$.

We let J_0 be the ideal product of all J_g with $g \in G$, and put $J = rad(J_0)$. Then we get the following characterization of J :

Theorem 2.1 $J =$

$$\bigcap\{ker(\sigma) \mid \sigma \text{ is an essential specialization of } R \text{ for } (I,<)\}$$

Proof. Since for every specialization σ of R $ker(\sigma)$ is a prime ideal of R, we see that σ is essential for $(I,<)$ iff $ker(\sigma) \supseteq J_0$. Consequently,

$$J = rad(J_0) = \bigcap\{P \mid J_0 \subseteq P \text{ is prime ideal of } R\} =$$

$$\bigcap\{ker(\sigma) \mid \sigma \text{ is an essential specialization of } R \text{ for } (I,<)\}$$

□

If P is a prime ideal of R we denote by R_P the localization of R wrt. P inside the quotient field K; so $R_P = \{ab^{-1} \mid a \in R, b \in R \setminus P\}$. Recall that every specialization $\sigma : R \longrightarrow K'$ extends canonically to specialization $\sigma : R_P \longrightarrow K'$ by putting $\sigma(ab^{-1}) = \sigma(a)(\sigma(b))^{-1}$, where $P = ker(\sigma)$. Again this extension $\sigma : R_P \longrightarrow K'$ extends canonically by coefficientwise application to a homomorphism $\sigma : R_P[X_1,\dots,X_n] \longrightarrow K'[X_1,\dots,X_n]$. Hence we say for a polynomial $f \in S'$ that $\sigma(f)$ is defined in $K'[X_1,\dots,X_n]$, if $f \in R_P[X_1,\dots,X_n]$ for $P = ker(\sigma)$. Similar for sets of polynomials in S'.

The importance of inessential specializations results from the following fact:

Theorem 2.2 *Let $\sigma : R \longrightarrow K'$ be an inessential specialization for $(I,<)$. Then*

1. *$\sigma(G)$ is defined and for every $g \in G$, $HT(\sigma(g)) = HT(g)$.*
2. *$\sigma(G)$ is the reduced Gröbner basis of the ideal I'' generated by $\sigma(I)$ in $K'[X_1,\dots,X_n]$ wrt. the term order $<$.*

Proof. (i) Since σ is inessential for $(I,<)$, we find for every $g \in G$ some $a_g \in J_g \setminus ker(\sigma)$. Then $a_g g \in I$, and so $\sigma(a_g g) \in \sigma(I)$ and $\sigma(a_g) \neq 0$. So $\sigma(g) = \sigma(a_g g)(\sigma(a_g))^{-1}$ is defined and an element of I''. Consequently

$\sigma(G)$ is defined and $\sigma(G) \subseteq I''$. Moreover, for every $g \in G$, $HT(\sigma(g)) = HT(\sigma(a_g g)) = HT(a_g g) = HT(g)$.

(ii) In order to show that $\sigma(G)$ is a Gröbner basis of I'' in $K'[X_1, \ldots, X_n]$, it suffices to show that every $h \in I''$ is reducible in finitely many steps to zero wrt. $\sigma(G)$. $\square$

We call any product $a_g g$ with $0 \neq a_g \in J_g$ a *lifting* of g. If a_g is $\preceq$-minimal in $J_g \setminus \{0\}$, we call $a_g g$ a *minimal lifting* of g. Similarly we call any set $G' := \{ag \mid 0 \neq a \in J_g, g \in G\}$ a *lifting* of G, and we call $G' := \{a_g g \mid a_g \text{minimal in } J_g \setminus \{0\}, g \in G\}$ a *minimal lifting* of G.

Summarizing we have for given ideal I in S and term order $<$ on T obtained a uniquely determined non-zero radical ideal J of R and a minimal lifting G' of the reduced Gröbner basis G of I' such that for all inessential specializations $\sigma : R \longrightarrow K'$ $\sigma(G')$ is a minimal Gröbner basis of the ideal I'' generated by $\sigma(I)$ in $K'[X_1, \ldots, X_n]$. The polynomial set G' is uniquely determined up to the equivalence $\sim$ on its elements.

We call G' the *generic Gröbner basis* of I and J the *generic ideal* of R associated with I wrt. the term order $<$.

3 Canonical Gröbner Systems

In this section we iterate the approach that led us to the generic Gröbner basis and the generic ideal for all "singular cases". We keep the notation of the previous section. As noted above the generic ideal J of R associated with the ideal I of S and the term order $<$ is a non-zero radical ideal. If $J = R$, then every specialization of R is inessential wrt $(I, <)$, and so $\sigma(G')$ is a minimal Gröbner basis for all specializations σ of R, and hence a comprehensive Gröbner basis of $(I, <)$. In this case we call G' the canonical comprehensive Gröbner basis of $(I, <)$.

Next suppose $J \neq R$. Then the fact that R is a Noetherian domain implies that J is the intersection (equivalently the product) of the uniquely determined finitely many isolated prime ideals of J (see [ZS58], Part I, Chapter IV, Theorem 10, or [BWK98], Section 8.5). Let $\mathcal{P}_J$ be the finite set of all isolated prime ideals of J. Then for each $P \in \mathcal{P}_J$ R/P is again a Noetherian domain. Let $\preceq$ be a wqo on R and define for each $P \in \mathcal{P}_J$ a relation $\preceq_P$ on R/P by

$$a + P \preceq_P b + P \iff a \preceq b,$$

where a has been chosen $\preceq$-minimal in the residue class $a + P$, and b has been chosen $\preceq$-minimal in the residue class $b + P$. Then it is easy to verify that each of these relations $\preceq_P$ is well-defined and also a wqo on R/P.

We put $S_P := (R/P)[X_1, \ldots, X_n]$, let K_P be the quotient field of R/P, and put $S'_P := K_P[X_1, \ldots, X_n]$. We let κ_p denote the canonical epimorphism from R to R/P and also its natural coefficientwise extension $\kappa_p : S \longrightarrow S_P$. For an ideal I in S the image ideal $\kappa_p(I)$ is denoted by I_P.

With these notations all the assumptions and conclusions of the previous section carry over from R, S a term order $<$ on T, and an ideal I of S to the corresponding objects $R/P, S_P, <$, and I_P. Hence we obtain for every $P \in \mathcal{P}_J$ a generic Gröbner basis $G_P \subseteq S_P$ and the corresponding generic ideal $\{0\} \neq J_P \subseteq R/P$ for the ideal I_P and the term order $<$.

Next we pass to preimages wrt. κ_P : We put $J'_P = \kappa_P^{-1}(J_P)$ and $I'_P = \kappa_P^{-1}(I_P)$. So J'_P is a proper extension of J_P, and I'_P is obtained by extension and contraction wrt κ_P and we have $I \subseteq I'_P$, but equality fails in general. Hence we have two natural choices for preimages of elements $f \in I_P$: Either we take $g \in I$ minimal with $\kappa_P(g) = f$ or we take $h \in I'_P$ minimal with $\kappa_P(h) = f$. Then $h \preceq g$, but equivalence may fail. We call h a *minimal preimage* of f and g a *minimal faithful preimage* of f wrt. κ_P. We let G_P^- be the set of all $g \in G_P$ that have no preimage under κ_P in G'. We denote the finite set obtained from G_P^- by taking minimal faithful preimages wrt κ_P by G'_P. The finite set obtained from G_P^- by taking minimal preimages wrt κ_P is denoted by G''_P.

Now we can define canonical partial Gröbner systems: All elements of such a system will be triples (J, J', G), where $J \subset J'$ are radical ideals in R and G is a finite subset of S.

The faithful partial Gröbner system of $(I, <)$ of level 0 and the partial Gröbner system of $(I, <)$ of level 0 are both $\{(\{0\}, J, G')\}$. The faithful partial Gröbner system of $(I, <)$ of level 1 and the partial Gröbner system of $(I, <)$ of level 1 are both empty if $J = R$; otherwise the faithful partial Gröbner system of $(I, <)$ of level 1 is $\{(J, J'_P, G'_P) \mid P \in \mathcal{P}_J\}$, and the partial Gröbner system of $(I, <)$ of level 1 is $\{(J, J'_P, G''_P) \mid P \in \mathcal{P}_J\}$.

Let now $\sigma : R \longrightarrow K'$ be a specialization that is essential wrt. $(I, <)$. Then $ker(\sigma) \supseteq J$, and so for some $P \in \mathcal{P}_J$, we have $ker(\sigma) \supseteq P$. So by the homomorphism theorem, σ induces a uniquely determined specialization $\sigma_P : R/P \longrightarrow K'$ defined by $\sigma_P(\kappa_P(a)) = \sigma(a)$. In particular we have $ker(\sigma) = \kappa_P^{-1}(ker(\sigma_P))$.

It should now be obvious, how to define recursively faithful partial Gröbner systems of $(I, <)$ and partial Gröbner systems of $(I, <)$ of every natural number level n. This is done by iterating the definition of R/P, $S_P, <$, I_P, and σ_P from R, S, a term order $<$ on T, an ideal I of S and a specialization σ of R. This leads to a finitely branching tree of triples (J, J', G), such that the set of all triples of a given level n is a (faithful) partial Gröbner system of $(I, <)$ of level n. In every branch of this tree the first components form a strictly increasing chain of radical ideals in R; so by the Noetherianity of R every branch is finite. Hence by König's tree lemma the whole tree is finite. We call the resulting finite tree the *canonical (faithful) Gröbner tree* of $(I,<)$, and the set of all triples in the respective tree the *canonical (faithful) Gröbner system* of $(I,<)$. Then the elements of both Gröbner systems are uniquely determined by $(I,<)$ up to equivalence of the polynomials in the third entry of each triple.

For every specialization σ of R there is at least one triple (J,J',G) in the (faithful) Gröbner system $(I,<)$, such that $ker(\sigma) \supseteq J$ and $ker(\sigma) \not\supseteq J'$. If this is the case, we call σ an *inessential* specialization of R wrt. the triple (J,J',G). Thus an inessential specialization of R in the previously defined sense is inessential for the unique triple $\{(\{0\},J,G')\}$ of level zero of the (faithful) canonical Gröbner system. Whenever σ is inessential wrt. a triple (J,J',G), then $\sigma(G)$ is a minimal Gröbner basis of the ideal generated by $\sigma(I)$ in $K'[X_n,\dots,X_n]$ wrt. the term order $<$.

4 Canonical Comprehensive Gröbner Bases

Suppose that GS is the canonical faithful Gröbner system for $(I,<)$. Then all the third entries of triples in GS are polynomials in I. We define the set

$$H := \bigcup\{G \mid \text{ there exist radical ideals}$$

$$J \subset J' \text{ of } R \text{ with } (J,J',G) \in GS\}$$

as the *canonical comprehensive Gröbner basis* for $(I,<)$. Then H is a finite subset of I and the elements of H are uniquely determined up to equivalence in S. In particular the number of polynomials in a comprehensive Gröbner basis H and for each $h \in H$ the set of terms $T(h)$ are uniquely determined by $(I,<)$.

At this point it is absolutely essential that we use the *faithful* canonical Gröbner system, since for the non-faithful canonical Gröbner system the third entries are in general not subsets of the ideal I.

Notice that H is indeed a comprehensive Gröbner basis for $(I,<)$: Whenever $\sigma : R \longrightarrow K'$ is a specialization of R, then there exists a triple $(J,J',G) \in GS$, such that σ is inessential wrt. (J,J',G), and so $\sigma(G)$ is a minimal Gröbner basis of the ideal generated by $\sigma(I)$ in $K'[X_1,\dots,X_n]$ wrt. the term order $<$. Since by definition $G \subseteq H \subseteq I$, it follows that $\sigma(G) \subseteq \sigma(H) \subseteq \sigma(I)$; hence $\sigma(H)$ is also a Gröbner basis of the ideal generated by $\sigma(I)$ in $K'[X_1,\dots,X_n]$.

Notice that we can not expect that the number of polynomials in a canonical comprehensive Gröbner basis for $(I,<)$ is the smallest compared with all other comprehensive Gröbner bases for $(I,<)$. Indeed it may be possible that two preimages of polynomials taken at different nodes in the (faithful) Gröbner tree yield the same polynomial modulo the relevant prime ideals at these nodes. In this case one of these polynomials is superfluous in the resulting canonical comprehensive Gröbner basis. By our definition of a faithful canonical Gröbner system this cannot happen between two nodes, where one is a descendent of the other. It may, however, happen in other cases, at two nodes in the same level. In this case there is no natural preference about the order in which one handles these cases; any selection of polynomials avoiding common preimages would require a non-canonical user-defined order among the isolated prime ideals associated with a given radical ideal in the relevant domain R/P. Hence the resulting objects would no longer be canonical. For an easy example of this type see example 7.2 below.

As an alternative one could treat all immediate successor nodes of a given node simultaneously searching for common preimages of polynomials for large subsets of these nodes in the spirit of the Chinese remainder construction [BW91] in order to minimize the number of polynomials. But again this would involve non-canonical choicec in the case of incomparable large subsets of nodes each having a common preimage of polynomials occuring at these nodes.

5 Generalizations and Variations

Our hypothesis so far has been that R is a Noetherian domain that admits a wqo $\preceq$. How essential are these assumptions?

Firstly let us drop the Noetherianity of the domain R : For algorithmic considerations it is obviously sufficient to consider only finitely generated ideals I in S. If F is a finite basis for I, let $R^\wedge$ be the subring of R generated by the coefficients of all polynomials in F. Then $R^\wedge$ is a homomorphic image of a polynomial ring in finitely many indeterminates over the ring of integers, and hence Noetherian. Let $I^\wedge$ be the ideal generated by F in $S^\wedge = R^\wedge[X_1, \ldots, X_n]$. Any wqo $\preceq$ on R restricts to a wqo on $R^\wedge$. Let $<$ be a term order on T. Then any canonical (faithful) Gröbner system and any canonical comprehensive Gröbner basis for $I^\wedge$ will constitute a canonical (faithful) Gröbner system and a canonical comprehensive Gröbner basisfor I by the fact that Gröbner bases remain stable under ground field extensions (see[BWK98], Corollary 5.51).

Hence the Noetherianity of R can be dropped, if one restricts attention to finitely generated ideals I in S.

What happens if we drop the existence of a wqo $\preceq$ on R? Of course our choices of minimal elements satisfying certain requirements are no longer possible; instead on has to make arbitrary choices. Hence the uniqueness assertions on the elements of a canonical comprehensive Gröbner basis and the elements of the last entries of a (faithful) canonical Gröbner system break down. We can, however, still assert that any two canonical comprehensive Gröbner bases contain the same number of polynomials. Similarly for (faithful) canonical Gröbner systems.

Recall that a reduced Gröbner basis of a polynomial ideal wrt. a given term order remains stable under ground field extensions (see [BWK98], Corollary 5.51), since all constructions involved are invariant under ground field extensions. In contrast to this situation the definition of a canonical Gröbner system involves primary decomposition of ideals in the parameter ring R. If R is a polynomial ring $Q[U_1, \ldots, U_m]$ over a non-algebraically-closed ground field Q, then clearly primary decomposition of ideals in R changes under extension of the ground field Q. Example 7.3 below provides an instance of this phenomenon.

For some applications only specializations of the parameter ring R in a special field K' are of interest. If K' is the field of real numbers (or an arbitrary real-closed field), then all concepts introduced above can be modified accordingly, e. g by restricting attention to real prime ideals only in place of the arbitrary prime ideals arising in Gröbner systems.

6 Algorithmic Aspects

The classical standard example of a Noetherian domain R with a wqo $\preceq$ is a multivariate polynomial ring of the type $R = Q[U_1, \ldots, U_m]$ over a field or Noetherian domain Q with the wqo $\preceq$ on R induced by a term order $\ll$ on the set of terms $T(U_1, \ldots, U_m)$ in the parameters $U_1, \ldots, U_m$. Since from the algorithmic viewpoint we restrict our attention to ideals in S given by a finite basis F, we may moreover drop the Noetherianity condition on R and hence on Q, as remarked above. Two elements a, b of R are equivalent iff they have the same set of terms in $T(U_1, \ldots, U_m)$. This is the situation considered in [Wei92], except that there no term order $\ll$ was taken into account.

Let $<$ be a term order on $T = T(X_1, \ldots, X_n)$. Then the extension of $\preceq$ to S is identical to the wqo induced by the block term order $\preceq'$ on S regarded as $Q[U_1, \ldots, U_m, X_1, \ldots, X_n]$, where all U_i are lexicographically smaller than all X_j. This corresponds to the setting considered in [Mon01].

The homomorphic images of R occuring in the construction of (faithful)

Gröbner systems and comprehensive Gröbner bases are then domains of the form $Q'[u_1, \ldots, u_m]$ obtained by adjunction of finite set to Q', where Q' is a homomorphic image of Q.

Let us now assume that Q is a computable domain (compare [BWK98]), and that the term oders $\ll$ and $<$ are decidable. Then the wqos $\preceq$ on R and on S are decidable, and $R,\ K,\ S,\ S'$ are computable domains.

In order to compute a generic Gröbner basis for $(I, <)$ we first compute from F and $<$ the reduced Gröbner basis G of I' (see e. g. [BWK98]). Next we need to compute for every $g \in G$ a finite basis of the ideal J_g and a minimal non-zero element of J_g. If these tasks are completed, then we have computed the generic Gröbner basis G' for $(I, <)$. Moreover the product ideal J_0 and its radical J can be computed by well-known techniques (compare [BWK98, EHV92]). Thus we have completed level zero of a (faithful) canonical Gröbner system for $(I, <)$.

For level 1, we first need to compute all isolated prime ideals $P \in \mathcal{P}_J$. This is achieved via a primary decomposition of J_0 (see [BWK98, EHV92]). Next for each $P \in \mathcal{P}_J$ all constructions at level 0 have to be repeated with R replaced by R/P and I by the ideal I_P of S_P that has as a basis $F_P := \{f + P \mid f \in F\}$. Notice that by Gröbner basis theory R/P and S_P are again computable domains, and the relations $\preceq_P$ is again a decidable wqo on R/P. This leads to a construction of G_P and J_P. Finally we need to compute $J'_P = \kappa_P^{-1}(J_P)$ and minimal κ_P-preimages of certain elements of G_P in I or in S, in order to get G'_P and G''_P, respectively.

For higher levels of the Gröbner tree no essentially new algorithmic tasks arise.

Next we study the different basic tasks arising in an algorithmic construction of a (faithful) canonical Gröbner system in more detail:

The first open task arising above is to compute for a given polynomial $g \in I'$ a finite basis of the ideal J_g in R and a minimal non-zero element of J_g.

Suppose the first subtask has been solved, i. e, we have a finite basis D of J_g. Then we can compute from D the reduced Gröbner basis E of J_g wrt. the term order $\ll$. It is now obvious that the smallest polynomial in E is a minimal non-zero element of J_g.

For the first subtask we recall that $g \in I'$ is given with coefficients in K represented by reduced quotients of elements of R. Let d be the product of the denominators of the coefficients of g. For the polynomial $dg \in S$ we have then $J_g = ((dI) : (dg)) \cap R$. Using this equation one can compute a finite basis of J_g using standard Gröbner basis methods in $S = K[U_1, \ldots, U_m, X_1, \ldots, X_n]$ (see [BWK98]).

The next task to be performed above for level one and higher levels of the Gröbner system is to compute $J'_P = \kappa_P^{-1}(J_P)$ and to compute minimal κ_P-preimages of given elements of G_P in I or in S from a given finite basis $\kappa(H_P)$ of J_P and M of P. Then clearly J'_P is the ideal generated by $H_P \cup M$ in R. Next let $g \in S$ with $\kappa_P(g) \in G_P$. We want to find a minimal polynomial $h \in I$ and $k \in S$ with $h \in g+P,\ k \in g+P$. This is an instance of the "Chinese remainder problem" of computing minimal elements in a finite intersection of residue classes wrt. several polynomial ideals solved algorithmically in [BW91], compare also [BWK98].

Thus we have completed all basic algorithmic tasks required in the construction of a canonical comprehensive Gröbner basis.

7 Examples

Example 7.1 *This simple example shows that in general the generic ideal J may not be a principal ideal. Thus its variety may be different from the "singular variety" studied in [Mon01] which is always a hypersurface.*

Let $R = \mathbb{Q}[U,V],\ S = R[X],\ F = \{f,g\} \subset S$ with $f = UX,\ g = VX$, let I be the ideal generated by F in S, and let $\preceq$ be the wqo on R induced by the lexicographical term order on $T(U,V)$ with $V > U$, and let $<$ be the unique term order on T. Then $G = \{X\}$ is the reduced Gröbner basis of I'. Consequently $\{f\}$ is a generic Gröbner basis for $(I,<)$. $J = J_0 = J_X$ is the ideal generated by $\{U,V\}$ in R. This is not a principal ideal in R.

Example 7.2 *The following example illustrates the fact that the canonical comprehensive Gröbner basis may not be a minimal comprehensive Gröbner basis.*

Let $R = \mathbb{Q}[U,V],\ S = R[X,Y,Z],\ F = \{f,g\} \subset S$ with $f = UY + X,\ g = VZ + X + 1$, let I be the ideal generated by F in S, and let $<$ be the lexicographical term order on T with $Z > Y > X$. We let the wqo $\preceq$ on R be induced by the lexicographical term order on $T(U,V)$ with $V > U$. Then by the first Buchberger criterion (see [BWK98], Lemma 5.66), $\{f/U, g/UV\}$ is the reduced Gröbner basis of I', and so F is a generic Gröbner basis for $(I,<)$. Hence $J_{f/U} = RU,\ J_{g/UV} = RV$, and so $J = J_0 = RUV$. The isolated prime ideals of J are $P := RU$ and $Q := RV$. A minimal Gröbner basis of I_P in S_P is $G_P := \{X+P, VZ+1+P\}$, and a minimal Gröbner basis of I_Q in S_Q is $G_Q := \{X+1+P, UY-1+P\}$. Hence we get $G'_P = \{f,h\}, G''_P = \{X, VZ+1\}$, $G'_Q = \{g,-h\}, G''_P = \{X+1, UY-1\}$, where $h = VZ-UY+1$. So a canonical comprehensive Gröbner basis for $(I,<)$ will involve both h and $-h$ which is clearly superfluous.

Example 7.3 *The final example shows the explicit dependence of canonical Gröbner systems on the ground field of the parameter ring R.*

Let $R = Q[U]$, $S = R[X, Y, Z]$, $F = \{f, g\} \subset S$ with $f = (U^2 + 1)Y + X^3 - 1$, $g = (U^2 + 1)Z + X^2 - 1$, let I be the ideal generated by F in S, and let $<$ be the lexicographical term order on T with $Z > Y > X$. We let the wqo $\preceq$ on R be induced by the degree-order on $T(U)$. Then by the first Buchberger criterion (see [BWK98], Lemma 5.66), F is a generic Gröbner basis for $(I, <)$.

In case Q contains a root of U^2+1, e. g. $Q = \mathbb{C}$, then $J = J_0 = R(U^2+1)$, and this ideal has $P1 := R(U - i)$, $P_2 := R(U + i)$ as associated isolated prime ideals. In both factor-rings R_{P_j}, we have $f + P_j = X^3 - 1 + P_j$, $g + P_j = X^2 - 1 + P_j$. Hence we obtain in both cases $\{X - 1 + P_j\}$ as reduced Gröbner basis of I_{P_j}. A minimal preimage of $X - 1 + P_j$ in I is in both cases $h := (U^2 + 1)(Y - XZ) + X - 1$. So we obtain $F \cup \{h\}$ as a canonical comprehensive Gröbner basis for $(I, <)$.

If, however, Q is a subfield of the reals, then the polynomial $U^2 + 1$ is irreducible, and so $J = R(U^2 + 1)$ is prime ideal, and so R/J is the field $Q[i]$. So as above we see that $\{X - 1 + J\}$ is the reduced Gröbner basis of I_J. So we obtain as before $F \cup \{h\}$ as a canonical comprehensive Gröbner basis for $(I, <)$. Notice, however, that in this case the faithful Gröbner system for $(I, <)$ differs from that in the previous case.

8 Conclusions

Comprehensive Gröbner bases form an adequate generalization of Gröbner bases in rings of polynomials with parametric coefficients. In Gröbner basis theory reduced Gröbner bases are canonical objects determined uniquely by a polynomial ideal I and a term order $<$, independently of any algorithm for their construction. In the theory of comprehensive Gröbner bases no additional structural conditions on a comprehensive Gröbner basis were known that would guarantee existence and sufficient uniqueness in analogy with reduced Gröbner bases in Gröbner basis theory. All special types of comprehensive Gröbner bases considered in the literature were dependent on an algorithm for their construction and would yield essentially different results on variations of the algorithm.

In this note we have presented a purely structural definition of a canonical comprehensive Gröbner basis and an associated canonical (faithful) Gröbner systems for a given parametric polynomial ideal I and a term order $<$. We have shown the existence of a canonical comprehensive Gröbner basis for any given pair $(I, <)$. If the parameter ring R is a Noetherian domain provided with a well-quasi-ordering $\preceq$, then a comprehensive Gröbner basis of $(I, <)$ is uniquely determined up to the equivalence induced by $\preceq$. If one restricts attention to finitely generated ideals I, then the Noetherianity condition on R can even be dropped. In the classical case, where the parameter ring R is a polynomial ring in the parameters over a field Q, we have also described an algorithm for the construction of a canonical (faithful) Gröbner system and a resulting canonical comprehensive Gröbner basis from a finite ideal basis of I and a term order $<$. The experience gained by the heuristic approach of A. Montes to approximative canonial Gröbner systems shows that this algorithm may also be interesting from the viewpoint of efficiency.

References

[Bec94] Thomas Becker. Gröbner bases versus d-Gröbner bases, and Gröbner bases under specialization. *AAECC*, 5:1–8, 1994.

[BW91] Th. Becker and V. Weispfenning. The chinese remainder problem, multivariate interpolation and gröbner bases. In S.M. Watt, editor, *ISSAC'91*, pages 64–69, 1991.

[BWK98] Thomas Becker, Volker Weispfenning, and Heinz Kredel. *Gröbner Bases, a Computational Approach to Commutative Algebra*, volume 141 of *Graduate Texts in Mathematics*. Springer, New York, corrected second printing edition, 1998.

[EHV92] D. Eisenbud, C. Huneke, and W. Vasconcelos. Direct methods for primary decomposition. *Invent. Math.*, 110:207–235, 1992.

[Faa92] W. Faas. Konstruktion umfassender Gröbner Basen in SCRATCHPAD II. Diploma thesis, Universität Passau, März 1992.

[FGT01] E. Fortuna, P. Gianni, and B. Trager. Degree reduction under specialization. *J. pure and applied alebra*, 164(1-2):153–164, 2001. Proceedings MEGA 2000.

[Kal97] M. Kalkbrener. On the stability of Gröbner bases under specializations. *J. Symb. Computation*, pages 51–58, 1997.

[KW91] H Kredel and V. Weispfenning. Parametric Gröbner bases in rings of solvable type. In *Proceedings: IV. Intern. Conference on Computer Algebra in Physical Research (Joint Institute for Nuclear*

Research Dubna, USSR, May 1990), pages 236–244, Singapore, 1991. World Scientific.

[Mon95] A. Montes. Solving the load-flow problem using Gröbner bases. *SIGSAM Bulletin*, 29:1–13, 1995.

[Mon98] A. Montes. Algebraic solution of the load-flow problem for a four nodes electrical network. *Math. and Comp. in Simulation*, 45:163–174, 1998.

[Mon99] A. Montes. Basic algorithm for specialization in Gröbner bases. In I. Bermejo, editor, *Actas de EACA-99*, pages 215–228, Tenerife, 1999. Universidad de La Laguna.

[Mon01] A. Montes. A new algorithm for discussing Gröbner bases with parameters. *J. Symb. Comp.*, (to appear), 2001.

[Pes94] Michael Pesch. Computing Comprehensive Gröbner Bases using MAS. User Manual, September 1994.

[PSWZ98] A. Pethö, J. Stein, T. Weis, and H. G. Zimmer. Computing the torsion group of elliptic curves by the method of Gröbner bases. In Manuel Bronstein, Johannes Grabmeier, and Volker Weispfenning, editors, *Symbolic Rewriting Techniques*, volume 15 of *Progress in Computer Science and Applied Logic*, pages 245–265. Birkhäuser Verlag, 1998.

[RE93] M.-F. Roy and T. van Effelterre. Aspect graphs of algebraic surfaces. In M. Bronstein, editor, *ISSAC'93*, pages 135–143. ACM Press, 1993.

[RE95] M.-F. Roy and T. van Effelterre. Aspect graphs of algebraic surfaces. Technical report, IRMAR, University of Rennes, 1995. available at URL: http://www.riaca.win.tue.nl/CAN/Research_Areas/AI/Vision/Aspect_graphs/Kiev_Last/Kiev_Last.html.

[Sch91] Elke Schönfeld. Parametrische Gröbnerbasen im Computeralgebrasystem ALDES/SAC-2. Diploma thesis, Universität Passau, D-94030 Passau, Germany, May 1991.

[Wei92] Volker Weispfenning. Comprehensive Gröbner bases. *Journal of Symbolic Computation*, 14:1–29, July 1992.

[Wei95] Volker Weispfenning. Solving parametric polynomial equations and inequalities by symbolic algorithms. In *Proceeding of the workshop:"Computer Algebra in Science and Engineering", Bielefeld, Aug'94*, pages 163–179, Singapore, 1995. World Scientific.

[ZS58] O. Zariski and P. Samuel. *Commutative Algebra I, II.* Van Nostrand Reinhold Company, New York, 1958.