PARAMETRIC GRÖBNER BASES FOR NON-COMMUTATIVE POLYNOMIALS

H. Kredel, V. Weispfenning
Universität Passau
D - 8390 Passau, FR Germany

Introduction. It was shown in [KRW] that the Gröbner basis technique with all its immediate applications (see [B]) can be extended from commutative polynomials to a large class of non-commutative polynomial rings over fields. More precisely, the method works for one- **and** two-sided ideals in **solvable algebras**, a class of rings that comprises e.g. enveloping algebras of finitely dimensional Lie algebras, Weyl algebras and iterated Ore-extensions of fields (compare also [K]). So the method is a strong generalization of the results in [AL].

On the other hand, it is well-known that for commutative polynomials with parametric coefficients, Gröbner bases are extremely unstable under specialization of the parameters. This problem was overcome by the second author by the construction of **comprehensive Gröbner bases**, i.e. bases for commutative polynomial ideals that are Gröbner bases in every specialization of the parametric coefficients (presented at the CoCoa-II conference, Genova 1989, see [W2]).

In this paper, we outline

1. the construction of parametric solvable algebras that may serve as "universal objects" for large classes of solvable algebras.

2. the construction of comprehensive Gröbner bases in parametric solvable algebras, where both the coefficients of the polynomials in question and the commutator relations defining the algebra are parametric.

This has the following far-reaching consequence: Let $d, k \in \mathbb{N}$ be given bounds; then for all solvable algebras S' over a suitable class of fields and with commutator relations below the degree bound d, and for all finite polynomial systems F in S' with $|F| \leq k$ and $deg(F) \leq d$, the computation of Gröbner bases for the left, right, or two-sided ideal generated by F can be reduced to a single computation of a comprehensive Gröbner basis G in a single parametric solvable algebra S, from which all the desired Gröbner bases in the algebras S' can be obtained simply by specialization. The same applies to all the applications of one- and two-sided Gröbner bases in solvable algebras indicated in [KRW] and [AL] and [W2]. Moreover, the construction of G can be performed for a fixed term-order or even an arbitrary class of term-orders; in the latter case one arrives at a **universal comprehensive Gröbner basis** (compare [W1]).

1 Parametric Solvable Algebras

Solvable algebras were introduced in [KRW] as a wide class of non-commutative algebras, in which most of the Gröbner basis theory for commutative polynomial rings (compare [B]) is valid for one- and two-sided ideals.

Parametric solvable algebras arise from solvable algebras when the ground field is replaced by a quotient ring of a multivariate polynomial ring over an integral domain, so that the commutator relations of the algebra may involve parameters. More precisely, let K be an integral domain, let $K[U_1, ..., U_m]$ be the (commutative) polynomial ring in $U_1, ..., U_m$, let I be an ideal in $K[U_1, ..., U_m]$ with $I \cap K = \{0\}$, and let $R = K[U_1, ..., U_m]/I$, so that $R = K[u_1, ..., u_m]$ with $u_i = U_i + I$. Next let $S = R[X_1, ..., X_n]$ be the polynomial ring in $X_1, ..., X_n$ over R, and let $<$ be a term-order on the set T of all terms (power-products) in $X_1, ..., X_n$. Let $*$ be a new, possibly non-commutative, multiplication on S such that the following conditions are satisfied:

Definition 1.1 *(i)* $(S, 0, 1, +, -, *)$ *is an associative ring extending* R.

(ii) For all $a, b \in R$, $1 \leq h \leq i \leq j \leq k \leq n$, $t \in T(X_i, ..., X_j)$, $a * bt = bt * a = abt$, $X_h * bt = bX_h t$, $bt * X_k = btX_k$.

(iii) For all $1 \leq i < j \leq n$ *there exist* $0 \neq c_{ij} \in R$, $p_{ij} \in S$ *such that* $X_j * X_i = c_{ij}X_iX_j + p_{ij}$ *and* $p_{ij} < X_iX_j$ *in the quasi-order on* S *induced by the term-order on* T*. Moreover, if* $C = \{c_{ij} : 1 \leq i < j \leq n\}$ *and* C' *is the multiplicative subset generated by* C *in* R*, then* $0 \notin C'$.

Then we call $(S, *)$ *a* **parametric solvable algebra over** R *and denote it by* $R\{X_1, ..., X_n\}$*. The special case of a* **solvable algebra over** K *is obtained by specializing* K *to a field and taking* $m = 0$*. We put* $P = \{p_{ij} : 1 \leq i < j \leq n\}$.

The following lemma shows that the multiplication $*$ of $S = R\{X_1, ..., X_n\}$ is uniform in the parameters $u_1, ..., u_m$.

Lemma 1.2 *Let* K *be an integral domain* $m \geq 1$, $R = K[u_n, ..., u_m]$*; let* $S = R\{X_1, ..., X_n\}$ *be a parametric solvable algebra satisfying 1.1; let* $0 \neq f, g \in S$*. Then we can compute* $c \in C'$ *and* $p \in S$ *such that* $f * g = c \cdot f \cdot g + p$ *and* $p < f \cdot g$*.* c *and* p *are uniquely determined by these properties, and the coefficients of* p *in* R *are* *polynomials in all c_{ij}, the coefficients in R of all p_{ij} and of f, g. Furthermore these polynomials are formed uniformly, independently of the ring R.*

Moreover, if for some $1 \leq i \leq n$, $f \in R\{X_1, ..., X_i\}$ and $g \in R\{X_i, ..., X_n\}$, then $f * g = f \cdot g$.

Proof. By analyzing the proof of lemmas 1.3 and 1.4 in [KRW]. □

Left reduction $f \underset{H}{\longrightarrow} f'$ for $f, f' \in S$, $H \subseteq S$ is defined similar as in the commutative case except that we avoid division in R; so $d \cdot f - f'$ is in the left ideal $I_L(H)$ generated by H for some $0 \neq d \in R$. A similar convention applies to the **left S-polynomial** $SPol(f, g)$ of $0 \neq f, g \in S$ (see [KRW] and [W2] for details).

Corollary 1.3 *Let $S = R\{X_1, ..., X_n\}$ be a parametric solvable algebra, let $0 \neq f, g \in S$, $H \subseteq S$. Then the following hold:*

(i) If $f \underset{H}{\longrightarrow} f'$ in S, then coefficients of f' in R are polynomials in the coefficients in R of the polynomials in $\{f\} \cup H \cup C \cup P$. Moreover, $f' < f$.

(ii) The coefficients in R of $h = SPol(f, g)$ are polynomials in the coefficients in R of the polynomials in $\{f, g\} \cup C \cup P$.

A **specialization** of $R = K[u_1, ..., u_m]$ is a ring homomorphism $\sigma : R \longrightarrow K'$, where K' is a field. Let $S = R\{X_1, ..., X_n\}$ be a parametric solvable algebra over R given as above, and let $S' = K'\{X_1, ..., X_n\}$ be a solvable algebra over K' such that for $1 \leq i < j \leq n$, $X_j * X_i = c'_{ij} X_i X_j + p'_{ij}$ with $0 \neq c'_{ij} \in K'$, $p'_{ij} \in S'$, $p'_{ij} < X_i X_j$. Let $\overline{\sigma} : S \longrightarrow K'[X_1, ..., X_n]$ be the natural extension of σ obtained by applying σ coefficientwise. Then we call σ **admissible for** S and S', if for $1 \leq i < j \leq n$, $\sigma(c_{ij}) = c'_{ij}$ and $\overline{\sigma}(p_{ij}) = p'_{ij}$.

Lemma 1.4 *Let $\sigma : R \longrightarrow K'$ be a specialization of R that is admissible for $S = R\{X_1, ..., X_n\}$ and $S' = K'\{X_1, ..., X_n\}$. Then $\overline{\sigma} : S \longrightarrow S'$ is a ring homomorphism (with respect to the new multiplication $*$). So whenever $0 \neq f, g \in S$, and $f * g = c \cdot f \cdot g + p$ and $\overline{\sigma}(f) * \overline{\sigma}(g) = c' \cdot \overline{\sigma}(f) \cdot \overline{\sigma}(g) + p'$ are as in 1.2, then $c' = \sigma(c)$ and $p' = \overline{\sigma}(p)$.*

Proof. Immediate from 1.2. □

Let $K'\{X_1, ..., X_n\}$ be a solvable algebra over an arbitrary field K', let $T'_{ij} (1 \leq i < j \leq n)$ be finite subsets of T and put $T' = \{T'_{ij}\}_{1 \leq i < j \leq n}$. Then we say, $K'\{X_1, ..., X_n\}$ **is of type** T', if all terms occuring in some polynomial p_{ij} $(1 \leq i < j \leq n)$ of definition 1.1 (iii) are elements of T'.

As an application of the preceeding lemmas, we can now show that for fixed T', every solvable algebra of type T' over an arbitrary field K' can be obtained from a single parametric solvable algebra by specializations:

Theorem 1.5 *Let $T' = \{T'_{ij}\}_{1 \le i < j \le n}$ be a family of finite subsets of T and let $<$ be a term-order on T such that $t < X_iX_j$ for every $t \in T_{ij}$ $(1 \le i < j \le n)$. Let K be an integral domain. Then there exists a ring $R = K[u_1, ..., u_m] = K[U_1, ..., U_m]/I$ (where $K[\mathrm{U}]$ is a polynomial ring over K) and a parametric solvable algebra $S = R\{X_1, ..., X_n\}$ such that for all fields K', all solvable algebras $S' = K'\{X_1, ..., X_n\}$ of type T' and all ring homomorphisms $\varphi : K \longrightarrow K'$, φ has an extension to a specialization $\sigma : R \longrightarrow K'$ that is admissible for S and S'. If σ is surjective, then we have in particular $S' = \overline{\sigma}(S)$.*

Proof. For all $1 \le i < j \le n$, we let c_{ij} be an indeterminate and p_{ij} the most general polynomial with indeterminate coefficients containing all terms in T'_{ij}. Let $(U_1, ..., U_m)$ be a list of these indeterminates. For every pair of terms $s, t \in T$ let c_{st} and p_{st} be determined by 1.2 in such a way that

$$(1) \quad s * t = c_{s,t}st + p_{s,t} \text{ and } c_{st} \in C',\ p_{s,t} < st$$

in every parametric solvable algebra $S = R\{X_1, ..., X_n\}$, satisfying 1.1, where $R = K[u_1, ..., u_n]$.

Then (1) together with 1.1 (ii) determines the structure constants in R of S with respect to the basis T of S. By [J], proposition 1, page 4, there exists a set Q of quadratic polynomials in these structure constants with the following property: $q(u_1, ..., u_m) = 0$ for all $q \in Q$ iff the algebra on the free R-module with basis T and multiplication $*$ defined by (1) is associative. Let now I be the ideal generated by Q in the polynomial ring $K[U_1, ..., U_m]$. Then $I \cap K = \{0\}$, (since there exists the solvable algebra $K'[X_1, ..., X_n]$ over $K' = Quot(K)$). Put $R = K[U_1, ..., U_m]/I = K[u_1, ..., u_m]$ and define the R-algebra S with basis T over R by (1). Then by construction, S is associative and hence a parametric solvable algebra over R satisfying 1.1.

Let now $S' = K'\{X_1, ..., X_n\}$ be a solvable algebra of type T' over a field K' satisfying for $1 \le i < j \le n$

$$X_j * X_i = c'_{ij}X_iX_j + p'_{ij} \text{ with } 0 \ne c'_{ij} \in K',\ p'_{ij} \in S', p'_{ij} < X_iX_j.$$

Let $v_1, ..., v_m$ be the m-tuple consisting of c'_{ij} and the coefficients of the p'_{ij} listed in the same order as the m-tuple $(U_1, ..., U_m)$ for the c_{ij} and p_{ij}. Let $\varphi : K \longrightarrow K'$ be a ring-homomorphism and let $\overline{\varphi} : K[U_1, ..., U_m] \longrightarrow K'$ be its canonical extension with $\overline{\varphi}(U_i) = v_i$. Then by definition of Q, $\overline{\varphi}(q(U_1, ..., U_m)) = 0$ for all $q \in Q$. Consequently $ker(\overline{\varphi}) \supseteq I$, and so $\overline{\varphi}$ induces a specialization $\sigma : R \longrightarrow K'$ with $\sigma(u_i) = v_i$. By construction σ is admissible for S and S', and so by 1.4 $\overline{\sigma} : S \longrightarrow S'$ is a ring-homomorphism. Moreover $\overline{\sigma}$ is surjective, if σ is surjective. □

To indicate the scope of this theorem we mention the following special case:

Let $1 \le n \in \mathrm{N}$ be fixed and let K be a field. Let $\mathcal{U}_n$ be the class of all universal enveloping algebras of some n-dimensional Lie-Algebra $\mathcal{A}$ over K with basis $X_1, ...X_n$

(see [J]). Every $S \in \mathcal{U}_n$ is a solvable algebra $S = K\{X_1, ..., X_n\}$ over K such that for $1 \le i < j \le n$, $X_j * X_i = X_i X_j + p_{ij}$ where p_{ij} is a linear form in $X_1, ..., X_n$ and the term-order ist e.g. total-degree-lexicographical. Then the theorem yields:

Corollary 1.6 *There exists a parametric solvable algebra $S = R\{X_1, ..., X_n\}$, where $R = K[u_1, ..., u_m]$ and $m = \frac{1}{2}n^2(n-1)$ such that for every $S' \in \mathcal{U}_n$ there exists a specialization $\sigma : R \longrightarrow K$ that is admissible for S and S' such that $\sigma \mid K = id$ and $S' = \overline{\sigma}(S)$.*

2 Comprehensive Gröbner Bases

Let $S = R\{X_1, ..., X_n\}$ be a parametric solvable algebra over $R = K[u_1, ..., u_m]$ with respect to a fixed term-order $<$ on T as in 1.1.. For $F \subseteq S$ we let $I_L(F)$, $I_R(F)$, $I(F)$ denote the left, right, and two-sided ideal generated by F in S, respectively. For the definition and characterizations of left, right, and two-sided Gröbner bases for an ideal, we refer the reader to [KRW].

Definition 2.1 *Let I be a left (right, two-sided) ideal in S and let G be a finite subset of I. Then G is a* **comprehensive left (right, two-sided) Gröbner basis of** *I, if for all solvable algebras $S' = K'\{X_1, ..., X_n\}$ over a field K' and all specializations $\sigma : R \longrightarrow K'$ that are admissible for S and S', $\overline{\sigma}(G)$ is a left (right, two-sided) Gröbner basis of the left (right, two-sided) ideal $I_L(\overline{\sigma}(I))$, $(I_R(\overline{\sigma}(I)),\ I(\overline{\sigma}(I)))$ in S'. (Here and in the following, $\overline{\sigma}$ is the canonical extension of σ to a ring-homomorphism $\overline{\sigma} : S \longrightarrow S'$.)*

Our main result is the following:

Theorem 2.2 *Let $S = R\{X_1, ..., X_n\}$ be a parametric solvable algebra as above and let F be a finite subset of S. Then one can construct a comprehensive left (right, two-sided) Gröbner basis G of $I_L(F)$, $(I_R(F)$, $I(F))$ in S. The construction is algorithmic relative to the term-order $<$ on T and computations in the ground ring R.*

The **proof** combines the constructions in [KRW] and [W2] with the uniformity results on parametric solvable algebras. All these constructions taken together form a large and fairly complicated system of interrelated algorithms. Moreover, in the present situation, any specialization σ of the parameters $(u_1, ..., u_n)$ of R changes not only the construction of Gröbner bases, but even the computation of products in $\sigma[R]$. So, in addition, these algorithms have to be interlocked. Hence we can present here only an outline of the ideas and steps involved.

Very roughly speaking, the argument follows a pattern of folding and unfolding: In the folding phase one constructs a Gröbner system and in the unfolding phase one extracts a comprehensive Gröbner basis from the Gröbner system by deleating all information on case distinctions.

A **left (right, two-sided) Gröbner system** GS **for** F is a finite tree, whose vertices are pairs (γ, G) with the following properties:

(i) γ is a condition, i.e. finite set of polynomial equations and inequations in the parameters $(u_1, ..., u_m)$ of the ring R.

(ii) G is a finite subset of $I_L(F)$ (of $I_R(F)$, of $I(F)$) extending F.

(iii) The root of GS is $(\emptyset, F)$.

(iv) Any leaf (γ, G) of GS has the following property: Whenever $\sigma : R \longrightarrow K'$ is a specialization that is admissible for S and S' (where $S = K'\{X_1, ..., X_n\}$ is a solvable algebra) and is compatible with the condition γ, then G is a left (right, two-sided) Gröbner basis of $I_L(F)$ (of $I_R(F)$, of $I(F)$) in S'.

From any such Gröbner system, a left (right, two-sided) comprehensive Gröbner basis G of $I_L(F)$ ($I_R(F)$, $I(F)$) can be extracted by "forgetting" all the conditions γ in the leaves of GS and uniting all the corresponding polynomial sets G; in other words

$$G = \bigcup \{G : (\gamma, G) \text{ is a leaf of } GS\}.$$

Next we discuss the construction of a left and a two-sided Gröbner system for F.

First, we recall from [KRW] the steps involved in the construction of a left (two-sided) Gröbner basis from a finite polynomial system F in a solvable algebra $S' = K'\{X_1, ..., X_n\}$:

(i) Formation of left S-polynomials $h = SPol(f, g)$ for $f \neq g$.

(ii) Successive left reduction of h to a normal form.

(iii) (in the case of two-sided Gröbner bases). Formation of products $g * X_i$ $(1 \leq i \leq n)$ and successive left reduction of these products to a normal form.

We want to perform the analogous steps in the parametric solvable algebra S in such a way that they remain valid under every admissible specialization of R. This forces us to adjoin to each step a case distinction on the vanishing or non-vanishing of certain coefficients that are relevant to this step. In this way a single step is transformed into a finite fan of single steps with associated conditions. Iterating this transformation, one may expect to arrive at a tree that forms Gröbner system for F.

This is, however, not the case for the following reason: If one follows a path trough this tree, the computation steps are performed according to the associated conditions. This means e.g. that by certain polynomial equations in a condition, certain monomials of a polynomial in S have to be cancelled. This in turn means that the corresponding computation step - regarded as a computation in R - will lead outside of the ideal $I_L(F)$ (or $I(F)$, respectively). So property (ii) of a Gröbner system will be violated.

The way out of this problem is as follows:
Each computation step in the tree to be constructed is performed in a "schizophrenic" manner. Instead of cancelling a monomial m according to a condition γ, we "colour" the monomial m according to γ: m is coloured green (red, white) if γ "says" that m should be zero (γ "says" that m should be non-zero, γ leaves m undetermined). In no case, however, a monomial is cancelled. Instead the computation step is guided by the colours, where care has to be taken that all monomials relevant to the step have been coloured green or red before.

In other words, the **definition** of the step is guided by the specializations compatible with the condition in question: its **formal computation** is, however, done in S in such a way that it never leads outside the ideal $I_L(F)$ (or $I(F)$, respectively).

Finally, one has to guarantee that the modified tree constructed in this way is indeed finite. To show this, let B be a branch of this tree T. Modify the branch by cancalling all monomials that have been coloured green by their corresponding condition. Then the modified branch B' constitutes a correct left (two-sided) Gröbner basis computation with respect to any admissible specialization $\overline{\sigma} : S \longrightarrow S'$ that is compatible with all conditions in the branch B'. So by the results of [KRW], B' is finite, and hence B is finite. Thus we know that every branch of T is finite. Moreover, by construction, T is finitely branching in every vertex; so by König's tree lemma, the whole tree T is finite.

This completes our proof sketch. □

Next we indicate an extension of theorem 2.2 that concerns comprehensive Gröbner bases in S that have this property for **all** term-orders, as far as they are compatible with the solvability of the algebra S.

Recall from [W1] that a finite subset G of a solvable algebra $S' = K'\{X_1, ..., X_n\}$ is a **universal left (right, two-sided) Gröbner basis**, if G is a left (right, two-sided) Gröbner basis for all term-orders $<$ on T that are compatible with 1.1 (iii). In an analogous way, we define a finite subset G of S to be a **universal comprehensive left (right, two-sides) Gröbner basis**, if G is a comprehensive left (right, two-sided) Gröbner basis for all term-orders $<$ on T that are compatible with 1.1 (iii).

We denote this class of term-orders by $Ord(S)$.

Let us now revisit the proof sketch above with the goal of constructing a **universal** comprehensive left (or two-sided) Gröbner basis of $I_L(F)$ (of $I(F)$). We modify the construction of a Gröbner system to that of a **universal Gröbner system**:
We extend conditions to include finitely many inequalities $s < t$ for $s, t \in T$. At each vertex of the tree, we distinguish cases (by constructing finitely many new conditions in the extended sense) in such a way that, besides the vanishing or non-vanishing of coefficients, we also take into account the possible order relations between the terms under consideration for term-orders compatible with the extended condition at the given vertex. Then the remaining arguments are still valid.
So we obtain:

Theorem 2.3 *Let $S = R\{X_1, ..., X_n\}$ be a parametric solvable algebra as above and let F be a finite subset of S. Then one can construct a universal comprehensive left (right, two-sided) Gröbner basis G of $I_L(F)$, ($I_R(F)$, $I(F)$) in S. The construction is algorithmic relative to computations in the ground ring R.*

3 Applications and Conclusions

We have shown in the preceedings sections that the Gröbner basis theory in solvable algebras can be performed in a very uniform, parametric way. This suggests a number of applications both of theoretical and practical interest.

1. Gröbner basis calculations in non-commutative solvable algebras tend to be costly due to the great number of $*$-products of terms that has to be computed. In part, this problem can be overcome by storing all the values of products that occur during a specific computation and updating the list of products as necessary (see [K]). By theorem 1.5, these computations have to be performed only once for every solvable algebra S' of given type T'. The same applies to Gröbner bases computations in S' for polynomial systems of bounded degree by 2.1.

2. The following applications of comprehensive Gröbner bases in commutative polynomial rings in [W2] can be carried over to parametric solvable algebras with only minor changes:

(i) Parametric ideal membership
(see [W2], theorem 6.2).

(ii) Parametric modules of syzygies
(see [W2], theorem 6.4).

(iii) Deformation of residue spaces and residue algebras (see [W2], theorem 6.8).

Example: Let $n, d \in \mathbf{N}$ be fixed. Consider the problem of transforming a right fraction ab^{-1} into a left fraction $c^{-1}d$ in the enveloping field of an arbitrary n-dimensional Lie algebra **A** and arbitrary polynomials a, b of degree $\leq d$ (see [AL]). Then the problem can be solved by the computation of a **single** comprehensive Gröbner basis in a suitable parametric solvable algebra and a **single** computation of a finite generating system for the pointwise modules of syzygies (see [W2], section 6).

3. In commutative polynomial rings, comprehensive Gröbner bases provide also a "fast" method for quantifier elimination in algebraically closed fields (see [W2], theorem 6.1). In a modified and somewhat restricted sense, such a method can also be obtained for existentially closed skewfields, using comprehensive Gröbner bases in parametric solvable algebras. Research on this topic is not yet completed and will be presented in a subsequent report.

References

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

[B] B. Buchberger, 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., 1985.

[J] N. Jacobson, *Lie algebras*, Interscience Publishers, 1962.

[KRW] A. Kandri-Rody, V.Weispfenning, Non-commutative Gröbner bases in algebras of solvable type, 1986, J. Symb. Comput. 9 (1990), pp. 1 - 26.

[K] H. Kredel, Computing in polynomial rings of solvable type, this volume.

[W1] V. Weispfenning, Constructing Universal Gröbner Bases, in Proc. AAECC-5, Springer LNCS col 356, pp. 195 - 201.

[W2] V.Weispfenning, Comprehensive Gröbner bases, preprint March 1990, University of Passau, MIP-9003.