# Reduction of everywhere convergent power series with respect to Gröbner bases ${ }^{1}$ 

J. Apel ${ }^{\text {a, },}$, J.Stückrad ${ }^{\text {a }}$, P. Tworzewski ${ }^{\text {b }}$, T.Winiarski ${ }^{\text {b }}$<br>${ }^{\mathrm{a}}$ Leipzig, Fakultät für Mathematik und Informatik, Universität Leipzig, Augustusplatz 10-11, D-04109 Leipzig, Germany<br>${ }^{6}$ Cracow, Instytut Matematyki, Uniwersytet Jagielloński, Reymonta 4, 30-059 Kraków, Poland

Communicated by M.-F. Roy; received 1 September 1994; revised 15 April 1995


#### Abstract

We introduce a notion of Gröbner reduction of everywhere convergent power series over the real or complex numbers with respect to ideals generated by polynomials and an admissible term ordering. The presented theory is situated somewhere between the known theories for polynomials and formal power series. Our main theorem states the existence of a formula for the division of everywhere convergent power series over the real or complex numbers by a finite set of polynomials. If the set of polynomials is a Gröbner basis then the remainder of that division depends only on the equivalence class of the power series modulo the ideal generated by the polynomials. When the power series which shall be divided is a polynomial the division formula leads to a usual Gröbner representation well known from polynomial rings. Finally, the results are applied to prove the closedness of ideals generated by polynomials in the ring of everywhere convergent power series and to give a very simple proof of the affine version of Serre's graph theorem.


1991 Math. Subj. Class.: 13105, 46A04, 13P10

## 1. Introduction

In this paper, we introduce a notion of Gröbner reduction of everywhere convergent power series over the real or complex numbers with respect to ideals generated by polynomials and an admissible term ordering. The presented theory is situated somewhere between the known theories for polynomials and formal power series. The paper

[^0]results from the cooperation of authors working on different fields of mathematics. So, we hope that the subject of the paper will be intcresting for scientists belonging to a wide spectrum of research areas, too. For the sake of selfcompleteness we start with a short introduction into the well-known theories of admissible term orderings and Gröbner bases for polynomial ideals in Section 2. For a comprehensive overview we refer to [3]. Section 3 contains the main theorem which says that there is a formula for the division of everywhere convergent power series over the real or complex numbers by a finite set of polynomials. If the set of polynomials is a Gröbner basis then the remainder of that division depends only on the equivalence class of the power series modulo the ideal generated by the Gröbner basis. In case the power series which shall be divided is also a polynomial, the division formula gives a G-representation.

Finally, in Section 4 we apply the results to prove the closedness of ideals generated by polynomials in the ring of everywhere convergent power series and to give a very simple proof of the affine version of Serre's graph theorem.

## 2. Gröbner bases and admissible orderings

The basic algebraic structures involved in this paper are the polynomial ring $R=$ $\mathbb{K}[X]$, the ring $S=\mathbb{K}[[X]]$ of formal power series, and the ring $E=\{f \in S \mid f$ is convergent in $\left.\mathbb{K}^{n}\right\}$, where $X=\left(X_{1}, \ldots, X_{n}\right)$ is the list of indeterminates. Since we are interested in convergence, we restrict ourself to the fields of complex $(\mathbb{C})$ or real $(\mathbb{R})$ numbers. Nevertheless, the results connected only with polynomials are valid with respect to an arbitrary coefficient field. Clearly, there are the inclusions $R \subset E \subset S$. In this paper convergency of power series always means convergency at the entire space $\mathbb{K}^{n}$.

For $f=\sum_{\alpha \in \mathbb{N}^{n}} c_{\alpha} X^{\alpha} \in S$ we define the support $\operatorname{supp} f=\left\{\alpha \mid c_{\alpha} \neq 0\right\}$ of $f$. For sets $F \subset S$ we set $\operatorname{supp} F=\bigcup_{f \in F} \operatorname{supp} f$. The elements of $R$ are just these of finite support. For the use of Gröbner techniques it is necessary to order the monomials $X^{\alpha}$ in such a way that the multiplication is (strong) monotone with respect to the ordering. Such orderings are called admissible term orderings (cf. [6]). Considering only the exponents $\alpha$ the investigation of these orderings can be done in $\mathbb{N}^{n}$. The orderings induced in $\mathbb{N}^{n}$ will be also called admissible term orderings.

The description of admissible term orderings in $\mathbb{N}^{n}$ requires considerations in $\mathbb{R}^{n}$. Any linear form $L=\sum_{i=1}^{n} l_{i} X_{i}$, where $l_{i} \in \mathbb{R}$, defines a partial ordering $\sqsubset_{L}$ in $\mathbb{N}^{n}$ by

$$
\begin{equation*}
\alpha \sqsubset_{L} \beta \Longleftrightarrow L(\alpha)<L(\beta) . \tag{1}
\end{equation*}
$$

Obviously, the partial ordering $\sqsubset_{L}$ is monotone with respect to the addition in $\mathbb{N}^{n}$. Using a second linear form $L^{\prime}$ we may refine $\square_{L}$ to a new monotone partial ordering $\sqsubset_{\left(L, L^{\prime}\right)}$ by comparing first with respect to $\sqsubset_{L}$ and if this gives no decision then with respect to $\sqsubset_{L^{\prime}}$. Iterating this process using only proper refinements, finally, after at most $n$ steps, we come to an admissible term ordering. On the contrary, any term ordering
can be given by such a sequence of linear forms of $\mathbb{R}^{n}$. A detailed description and classification of the admissible term orderings can be found in [14].

Dealing with polynomial rings, term well-orderings are used. This provides finiteness of the reduction procedure. In rings of power series, often non-noetherian orderings are used. Otherwise, even initial terms cannot be defined. In this paper we are working somewhere in between. We use Gröbner basis theory in $R$ but afterwards we apply it to elements of $E$. The reason is that in contrast to earlier works connected with Gröbner reductions for power series (cf. [12,13]) we are considering a different topology.

In this paper, from now on, ordering will always mean admissible term well-ordering. An example for an ordering is the lexicographical ordering $\prec_{\text {lex }}$ defined by $\alpha \prec_{\text {lex }} \beta$ if and only if the first non-zero component of $\alpha-\beta$ is negative.

Let us emphasize the importance of orderings which are given by a sequence of linear forms which have only natural number coefficients. These orderings can be described by the formula

$$
\begin{equation*}
\alpha \prec_{\mathfrak{U}} \beta \Longleftrightarrow \alpha \mathfrak{U} \prec_{\text {lex }} \beta \mathfrak{U}, \tag{2}
\end{equation*}
$$

where $\mathfrak{H}$ is a regular $n \times n$ - matrix with natural number entries.
The orderings of that type are exactly these term well-orderings which Robbiano called of lexicographical type in [14]. There it is also shown that we need exactly $n$ linear forms and that the $i$ th column of $\mathfrak{A}$ may be chosen as the coefficients of the $i$ th linear form. A linear form $L$ with real coefficients defines an oriented hyperplane of $\mathbb{R}^{n}$ crossing the origin. Considering only a bounded area of $\mathbb{R}^{n}$ there exists always a second oriented hyperplane of $\mathbb{R}^{n}$ crossing the origin which has only integer coordinates such that there is no lattice point of $\mathbb{N}^{n}$ lying between both hyperplanes (with respect to the orientation). As an easy conclusion we get from this fact, is that for an arbitrary term well-ordering $\prec$ and any finite subset $M \subset \mathbb{N}^{n}$ there exists an ordering $\prec_{\mathfrak{2}}$ of type (2) such that $\prec_{M}=\left.\prec_{\mathfrak{M}}\right|_{M}$.

Some of the investigations in Section 3 will require a more restricted type of term orderings having the property that for any given element of $\mathbb{N}^{n}$ there exists only a finite number of smaller vectors. An ordering has this property if and only if its first linear form has only positive coefficients.

The following lemma is due to Bayer [2] and shows how any ordering may be approximated by an ordering of this type.

Lemma 2.1. Let $\prec$ be a term ordering and $M \subset \mathbb{N}^{n}$ a finite set. There exists a linear form

$$
\begin{equation*}
L=\sum_{i=1}^{n} l_{i} X_{i} \quad\left(0<l_{i} \in \mathbb{N}\right) \tag{3}
\end{equation*}
$$

such that the restrictions of the partial orderings $\sqsubset_{L}$ and $\prec$ to $M$ coincide.

Proof. The proof will be given by constructing a suitable linear form $L$. First of all we find an approximation $\prec_{\mathfrak{U}}$ of type (2) such that $\prec_{M}=\left.\prec_{\mathfrak{A}}\right|_{M}$. If $\prec_{\mathfrak{N}}$ is the lexicographical ordering, everything is easy. For instance, Bayer's linear form $L=$ $\sum_{i=1}^{n} t^{n-i} X_{i}$ may be used, where $t \in \mathbb{N}$ is greater than the degree of any monomial $X^{\alpha}$ for $\alpha \in M$. By setting

$$
M_{\mathfrak{U}}:=\{\alpha \mathfrak{U} \mid \alpha \in M\}
$$

the problem of the ordering described by the matrix $\mathfrak{A}$ may be transformed into this for the lexicographical one. Let $L_{\text {lex }}$ be a suitable linear form for $M_{\mathscr{A}}$ and $\prec_{\text {lex }}$, i.e. $L_{\text {lex }}$ has positive integer coefficients and $\sqsubset_{L_{\text {lex }}}$ coincides with $\prec_{\text {lex }}$ on $M_{\mathfrak{Q}}$, then we set $L:=\mathfrak{N} L_{\text {lex }}$ where $L$ and $L_{\text {lex }}$ are considered as the column vectors of their coefficients. It is obvious that the $L$ so-defined is of type (3) and that $\square_{L}$ and $\prec$ coincide on $M$.

Any term ordering which is a refinement of $\sqsubset_{L}$, e.g. the ordering

$$
\alpha \prec_{L} \beta \Longleftrightarrow\left\{\begin{array}{l}
L(\alpha)<L(\beta) \quad \text { or }  \tag{4}\\
L(\alpha)=L(\beta) \wedge \alpha \prec \beta
\end{array}\right.
$$

will coincide on $M$ with $\prec$.
For some applications the weaker condition to $L$, namely, that only the refinement $\prec_{L}$ of $\sqsubset_{L}$ defined in (4) has to coincide with $\prec$ on $M$ is also sufficient. The notions below depend on the chosen ordering. Sometimes, if different orderings are involved, we will index the notions by the corresponding ordering in order to avoid confusion. Otherwise, we assume that we are working with respect to a fixed term ordering and neglect the index.

Let $\prec$ be a fixed ordering. The maximal (with respect to $\prec$ ) vector $\alpha$ appearing in supp $f$ of a non-zero polynomial $f \in R$ is called the exponent $\exp f$ of $f$. Furthermore, the coefficient of $X^{\exp f}$ in $f$ is called the leading coefficient $\operatorname{lc} f$, the monomial inf $:=$ lc $f X^{\exp f}$ the initial term, and tail $f:=f-\operatorname{in} f$ the tail of $f$.

The notions of initial term and exponent will be extended to sets of polynomials in the usual way in $F=\{\operatorname{in} f \mid f \in F \backslash\{0\}\}$ and $\exp F=\{\exp f \mid f \in F \backslash\{0\}\}$. If $F$ contains at least one non-zero polynomial then the monoid ideal $\exp F+\mathbb{N}^{n}$ will be denoted by $\Delta_{F}$ and the complement $\mathbb{N}^{n} \backslash \Delta_{F}$ by $\mathcal{D}_{F}$. If $F \subseteq\{0\}$ then, by definition, $\Delta_{F}=\emptyset$.

In what follows we consider only non-zero ideals $I$ and sets $F$ of polynomials containing at least one non-zero polynomial.

A power series $g \in E$ is called reducible with respect to a set $F \subset R$ if $\operatorname{supp} g \cap \Delta_{F} \neq$ $\emptyset$. Otherwise, $g$ is said to be reduced with respect to $F$. Obviously, $g$ is reduced with respect to $F$ if and only if $\operatorname{supp} g \subset \mathfrak{D}_{F}$. This fact will be abbreviated by writing $g \in$ $E\left(\mathfrak{D}_{F}\right)$ or if $g$ is even a polynomial also by $g \in R\left(\mathfrak{D}_{F}\right)$. The definitions are restricted to convergent power series since, in general, reducibility introduced in this paper makes no sense for formal power series.

We say, that $g \in R$ reduces to $g^{\prime} \in R$ with respect to $F \subset R$ (denoted by $g \xrightarrow{F} g^{\prime}$ ) if there is an equation

$$
\begin{equation*}
g^{\prime}=g-c_{\gamma} X^{\gamma} f \tag{5}
\end{equation*}
$$

where $f \in F, \gamma \in \mathbb{N}^{n}, c_{\gamma} \in \mathbb{K} \backslash\{0\}, \gamma+\exp f \in \operatorname{supp} g$ and $\gamma+\exp f \notin \operatorname{supp} g^{\prime}$.
Since we are working over a field, for any $g$ which is reducible with respect to $F$ there exists a $g^{\prime}$ such that $g \xrightarrow{F} g^{\prime}$. By the noetherianess of $\prec$ the reduction process can be iterated only finitely many times, i.e. for any polynomial $g$ there is a (not necessarily unique) reduced polynomial $g_{\mathrm{red}}$ which satisfies $g \xrightarrow{F}{ }^{*} g_{\mathrm{red}}$ where $*$ marks the reflexive, transitive closure of the reduction relation. The polynomials $g_{\text {red }}$ will be also called reduced forms of $g$ with respect to $F$. There may be distinguished one of the reduced forms of $g$ with respect to a finite basis $F$ and an ordering $\prec$ by fixing a reduction strategy, i.e. we have to use a stronger definition of reduction which ensures that there is at most one polynomial $g^{\prime}$ such that $g$ may be reduced in the stronger sense to $g^{\prime}$ with respect to a fixed set $F$ and a fixed term ordering $\prec$. The simplest case where different reduced forms could be obtained occurs when a monomial has to be reduced which is divisible by more than one leading term of the polynomials from $F$. This reflects Buchberger's main idea for the construction of S-polynomials (cf. [6]). In order to get uniqueness for a single reduction step for monomials we fix an enumeration of the elements of $F$ and always use for the reduction the first possible element according to this enumeration (cf. [10]). On reducing polynomials consisting of more than one monomial, the reduced form could depend on the choice of the next monomial to be reduced. At the moment we will complete the strategy for polynomials by requiring that the largest reducible exponent from the support should be treated first. Following Definition 2.2 we will show that the reduced form is already unique without using this second part of the strategy.

If we need to emphasize that reduced forms of polynomials are obtained by applying a fixed unique reduction strategy we will call $g_{\text {red }}$ a normal form of $g$ and denote it by $\mathrm{Nf} g$.

Definition 2.2. Let $g \in R, F \subset R$, and $\prec$ be a term ordering. A representation

$$
g=\sum_{f \in F} h_{f} f+g_{\mathrm{rem}}
$$

where $g_{\text {rem }} \in R\left(\mathfrak{D}_{F}\right), h_{f} \in R$, and for any $f \in F$ we have either $h_{f}=0$ or $\exp h_{f}+\exp f \preceq \exp g$, is called a $G$-representation of $g$ with respect to $F$ and $\prec$. The polynomial $g_{\text {rem }}$ is called a G-remainder of $g$ with respect to $F$ and $\prec$. Furthermore, the representation is called strong $G$-representation with respect to $F$ and $\prec$ if in addition all the vectors $\alpha+\exp f$, where $f \in F$ and $\alpha \in \operatorname{supp} h_{f}$, are pairwise distinct.

The strong G-representations are these G-representations with respect to finite sets $F$ which can be constructed by iterated reduction in an algorithmic way. In this case the G-remainders are reduced forms of $g$. In contrast, a G-remainder of $g$ is not
necessarily a reduced form of $g$ with respect to $F$. For any unique reduction strategy, the normal form operator Nf is linear. For polynomials $g$ and $g^{\prime}$ consider associated normal forms $\mathrm{Nf} g$ and $\mathrm{Nf} g^{\prime}$ with respect to $F$, respectively. There exist strong Grepresentations $g=\sum_{f \in F} h_{f} f+\mathrm{Nf} g$ and $g^{\prime}=\sum_{f \in F} h_{f}^{\prime} f+\mathrm{Nf} g^{\prime}$. We want to show that $\sum_{f \in F}\left(h_{f}+h_{f}^{\prime}\right) f+\mathrm{Nf} g+\mathrm{Nf} g^{\prime}$ is a strong G-representation of $g+g^{\prime}$ and that $\mathrm{Nf}\left(g+g^{\prime}\right)=\mathrm{Nf} g+\mathrm{Nf} g^{\prime}$ with respect to the fixed reduction strategy. Suppose, there is a situation, such that $\alpha_{1}+\exp f_{1}=\alpha_{2}+\exp f_{2}=\beta$, where $\alpha_{i} \in \operatorname{supp}\left(h_{f_{i}}+h_{f_{i}}^{\prime}\right)$ ( $i=1,2$ ). Since the strong G-representations of $g$ and $g^{\prime}$ are constructed according to a selection strategy which determinates the $f$ to be used for the reduction of a monomial, we must have $f_{1}=f_{2}$ and, consequently, $\alpha_{1}=\alpha_{2}$. Taking into account $\mathrm{Nf} g+\mathrm{Nf} g^{\prime} \in R\left(\mathfrak{D}_{F}\right)$, we have proven that we have a strong G-representation of $g+g^{\prime}$ with respect to $F$. Consequently, $\mathrm{Nf}\left(g+g^{\prime}\right)=\mathrm{Nf} g+\mathrm{Nf} g^{\prime}$ with respect to our unique reduction strategy, including selection of the next monomial to be reduced.

During the construction of the strong G-representation of $g+g^{\prime}$ we did not use the second part of the reduction strategy. Suppose, $g^{\prime}=-g$ and that the normal form strategies for $\mathrm{Nf} g$ and $\mathrm{Nf} g^{\prime}$ coincide only in the first part. According to the above ideas the difference of the strong G-representations provides a strong G-representation for $g+g^{\prime}=0$, therefore, $h_{f}+h_{f}^{\prime}=0$ for all $f \in F$ and $\mathrm{Nf} g=-\mathrm{Nf} g^{\prime}$, i.e. the normal form of $g$ does not depend on the second part of the reduction strategy.

There still remains an open gap, namely the reduction of convergent power series. This gap will be closed in Section 3. Now we give a short introduction to the theory of Gröbner bases [5] which turned out to be a very powerful tool in constructive commutative algebra (cf. $[6,8]$ ).

Definition 2.3. A subset $F \subset I$ of the ideal $I \subset R$ such that $\operatorname{in} F R=\operatorname{in} I R$ is called a Gröbner basis of $I$ (with respect to $\prec$ ).

This is the most common Gröbner basis definition which can be used also in more general situations (c. [ $15,13,4,1]$ ). In the case of polynomial rings over a field there are different equivalent conditions: some of them will be listed below.

Lemma 2.4. For a subset $F \subset I$ of a non-zero ideal I the following conditions are equivalent:
(i) $F$ is a Gröbner basis of $I$,
(ii) $\Delta_{F}=\Delta_{I}$,
(iii) any $g \in I \backslash\{0\}$ is reducible with respect to $F$,
(iv) any $g \in I$ has a G-representation with respect to $F$ with $g_{\mathrm{rem}}=0$,
(v) $F$ generates $I$ and the remainder $g_{\mathrm{rem}}$ appearing in $G$-representations of $g \in R$ with respect to $F$ is uniquely determined.

Proof. (i) $\Rightarrow$ (ii), (ii) $\Rightarrow$ (iii), and (iii) $\Rightarrow$ (iv) are obvious.
To prove (iv) $\Rightarrow$ (v) we consider two remainders of $g$ with respect to $F$. Clearly, we have $k:=g_{\mathrm{rem}}-g_{\mathrm{rem}}^{\prime} \in I \cap R\left(\mathfrak{D}_{F}\right)$. Consider the G-representation $k=\sum_{f \in F} h_{f} f+k_{\text {rem }}$.

For any $f \in F$ we must have either $h_{f}=0$ or $\exp h_{f}+\exp f \prec \exp k$ since equality would yield $\exp k \notin \mathfrak{D}_{F}$. In conclusion either $k=k_{\text {rem }}=0$ or $\exp k_{\text {rem }}-\exp k$ for any G-representation of $k$ with respect to $F$. From (iv) it follows $g_{\text {rem }}-g_{\text {rem }}^{\prime}=0$, which completes the proof.

It remains to show (v) $\Rightarrow$ (i). Suppose that there is an element $g \in I \backslash\{0\}$, such that in $g \notin \operatorname{in} F R$. Since we are working over a field this means $\exp g \notin \Delta_{F}$. Without loss of generality we may assume $\operatorname{supp} g \subset \mathfrak{D}_{F}$. For $F$ generating $I$, there is a representation $g=\sum_{f \in F} h_{f} f$. Let $f^{\prime} \in F$ and $\alpha \in \mathbb{N}^{n}$ such that $\exp h_{f}+\exp f \prec \alpha+\exp f^{\prime}$ for all $f \in F$. Both $g$ and 0 are remainders in a G-representation of $X^{\alpha} f^{\prime}+g$ with respect to $F$. This contradicts the assumption (v).

Above we have stated the difference between G-remainders and reduced forms of $g$ with respect to $F$. According to condition (v) we have coincidence for Gröbner bases. Analogous formulations of the conditions (iv) and (v) using strong G-representations would also yield equivalent conditions. It should be mentioned that there is a very important equivalence to the conditions of the lemma which is similar to (iv) but requires zero-remainders only for a finite number of special ideal elements, the so-called S-polynomials (cf. [6]). This condition is fundamental for the algorithmic construction of Gröbner bases. The results presented in this paper are rather existential than constructive since for any of the cases we are not yet able to give an algorithmic solution of the reduction problem for convergent power series. According to our topology, even the question truncated results makes no sense.

The existence of a (finite) Gröbner basis $F$ of an arbitrary ideal $I \subset R$ with respect to a given ordering is obvious. For polynomial rings it makes sense to define reduced Gröbner bases (cf. [6]) by

Definition 2.5. $F$ is called reduced Gröbner basis if lc $f=1$ and $\operatorname{supp} f \cap \Delta_{F \backslash\{f\}}=\emptyset$ for all $f \in F$.

## Proposition 2.6. The reduced Gröbner basis of an ideal $I \subset R$ is finite and unique.

Proof. The finiteness of the reduced Gröbner basis follows from the fact that $\Delta_{I}$ as monoid ideal of the noetherian monoid $\mathbb{N}^{n}$ is finitely generated.

Let $G$ and $G^{\prime}$ be two reduced Gröbner bases of $I$. According to condition (iii) of Lemma 2.4 any element $g$ of $G$ must be reducible with respect to $G^{\prime}$, i.e. there exists a $g^{\prime} \in G^{\prime}$ such that $\exp g \in \Delta_{\left\{g^{\prime}\right\}}$. On the other hand, we have $\exp g^{\prime} \in \Delta_{G}$ and $\exp g \notin \Delta_{G \backslash\{g\}}$, therefore, $\exp g^{\prime} \in \Delta_{\{g\}}$. Consequently, $\exp g^{\prime}=\exp g$ and ing $g^{\prime}=\operatorname{ing}$. It follows $\operatorname{supp}\left(g-g^{\prime}\right) \subseteq\left(\operatorname{supp} g \cup \operatorname{supp} g^{\prime}\right) \backslash\{\exp g\}$. Since $g-g^{\prime} \in I$ it has to be zero or reducible with respect to both $G$ and $G^{\prime}$ according to condition (iii). The second case is impossible by the definition of the reduced Gröbner basis. Consequently, we have $g=g^{\prime}$ and $G \subseteq G^{\prime}$. In the same way, we get the other inclusion. This completes the proof.

Proposition 2.7. For a Gröbner basis $F$ of the ideal I the set $B:=\left\{X^{\alpha} \mid \alpha \in \mathfrak{D}_{F}\right\}$ forms a vector space basis of $R / I$.

The assertion follows immediately from conditions (iv) and (v) of Lemma 2.4.
Proposition 2.8. Let $F \subset I$ be a Gröbner basis with respect to the ordering $\prec$. Let $\prec^{\prime}$ be an ordering such that $\exp _{\prec} f=\exp _{\prec^{\prime}} f$ for all $f \in F$. Then $F$ is also Gröbner basis of I with respect to $\prec^{\prime}$.

Proof. By construction it is $\Delta_{F, \prec}=\Delta_{F, \prec^{\prime}}$. Therefore, $g$ is reducible with respect to $F^{\prime}$ and $\prec$ if and only if it is reducible with respect to $F$ and $\prec^{\prime}$. According to condition iii) of Lemma 2.4 the claim will follow.

Since $\operatorname{supp} G$ is finite for a (reduced) Gröbner basis $G$ of the ideal $I$ with respect to an arbitrary ordering $\prec^{\prime}$ we find an ordering $\prec$ described by a regular matrix with natural number entries such that $G$ is also (reduced) Gröbner basis with respect to the new ordering. Furthermore, the class of orderings of type (2) is large enough to find for any application of Gröbner bases a convenient ordering within the class.

By Lemma 2.1 the class of orderings could be restricted even more. It would be sufficient to consider only orderings of type (4). Unfortunately, for some applications as, e.g. the computation of elimination ideals, the construction of a suitable linear form $L$ requires that a Gröbner basis with respect to another ordering not of type (4) or at least some bound for its support is known in advance. On the other hand, for our applications in Section 3 it is already enough to know that for a given Gröbner basis there always exists an ordering of type (4) which gives rise to the same Gröbner basis.

At the end of this section we will present a well-known proposition which allows to construct elimination ideals. This proposition will be applied to Serre's graph theorem in the last section.

Proposition 2.9. Consider the polynomial ring $R=\mathbb{K}[Y, Z]$ in two groups $Y$ and $Z$ of indeterminates. Let $\prec$ be an elimination ordering for $Y$, i.e. we have $\exp Z^{\alpha} \prec$ $\exp \left(Y^{\beta_{1}} Z^{\beta_{2}}\right)$ for any non-zero vector $\beta_{1}$ and arbitrary vectors $\beta_{2}$ and $\alpha$. Furthermore, let $F \subset I$ be a Gröbner basis of the ideal $I \subset R$ with respect to $\prec$. Then $F \cap \mathbb{K}[Z]$ is a Gröbner basis of $I \cap K[Z]$ with respect to the ordering $\prec_{Z}$ induced by $\prec$ in $\mathbb{N}^{k}$ where $k$ is the number of indeterminates contained in $Z$.

Proof. Any element $g \in I$ has a G-representation $g=\sum_{f \in F} h_{f} f$ with respect to $F$ and $\prec$. Clearly, $F \cap \mathbb{K}[Z] \subset I \cap \mathbb{K}[Z]$. Consider $g \in I \cap \mathbb{K}[Z]$. By definition of $\prec$ it follows ing $\in \mathbb{K}[Z]$ if and only if $g \in \mathbb{K}[Z]$. According to the exponent condition for Grepresentations all polynomials $h_{f}$ for $f \notin \mathbb{K}[Z]$ have to be zero. In the case $f \in \mathbb{K}[Z]$ it must be $h_{f} \in \mathbb{K}[Z]$, too. Consequently, the above sum is also a G-representation of $g$ in the ring $\mathbb{K}[Z]$ w.r.t. $F \cap \mathbb{K}[Z]$ and $\prec_{Z}$. According to condition (iv) of Lemma 2.4 the claim will follow.

Remark. Assume we are given two arbitrary orderings $\prec_{Y}$ and $\prec_{Z}$ acting on monomials depending only on $Y$ and $Z$, respectively. Then there exists an elimination ordering $\prec$ for $Y$ as defined in Proposition 2.9 which coincides with $\prec_{Y}$ or $\prec_{Z}$ for monomials depending only on $Y$ or $Z$, respectively. For example the ordering $\prec$ defined by

$$
\left(\alpha_{1}, \alpha_{2}\right) \prec\left(\beta_{1}, \beta_{2}\right) \Longleftrightarrow\left\{\begin{array}{l}
\alpha_{1} \prec_{Y} \beta_{1} \text { or } \\
\alpha_{1}=\beta_{1} \wedge \alpha_{2} \prec_{Z} \beta_{2}
\end{array}\right.
$$

fulfills this condition.
Furthermore, if $Y$ are the first $m$ indeterminates of $X$, and $Z$ are the remaining $n-m$ ones, then, e.g., the lexicographical ordering can be used for the elimination of $Y$ from $I$.

## 3. Reduction of convergent power series

In Section 2 we left the gap regarding the result of the reduction of a reducible convergent power series. Clearly, a procedure similar to polynomials would not terminate in general. That, of course, is a problem also arising during the reduction of formal power series (cf. [13]). But, in that case, one may define reduction strategies which ensure that any truncation of the reduced power series may be computed exactly. Such a strategy cannot be applied to our problem, since a power series has no highest term with respect to an admissible term well-ordering. We could start the reduction with the smallest occurring monomial. But, in this case, any later reduction may change any of the already considered terms and we have to start from the very beginning in any step. What we get are series for the coefficients of the resulting power series. To answer the questions for convergence or even limits of this coefficient series is far from being easy.

We avoid this problem by defining a one-step reduction. On the one hand we lose some constructivity of the reduction by this approach. But, on the other hand, we can solve many existence problems, e.g. we prove the convergence of the above mentioned coefficient series.

Definition 3.1. Let $g=\sum_{\alpha \in \mathbb{N}^{n}} c_{\alpha} X^{\alpha} \in E$ be a convergent power series, $F \subset R$ a finite set of polynomials, and $\prec$ an admissible term well-ordering. We say that $g$ reduces to $g_{\text {red }}$ with respect to $F$ (denoted by $g \xrightarrow{F} g_{\text {red }}$ ) if $g_{\text {red }}=\sum_{a \in \mathbb{N}^{n}} c_{\alpha} X_{\text {red }}^{\alpha}$ for some reduced forms $X_{\text {red }}^{\alpha}$ with respect to $F$ and $\prec$ of $X^{\alpha}$, for all $\alpha \in \mathbb{N}^{n}$.

First of all, we have to justify our definition by proving the convergence of $g_{\text {red }}$. As a by-product we will obtain that $g_{\text {red }}$ is reduced with respect to $F$. Therefore, $g_{\text {red }}$ will be again called a reduced form of $g$ with respect to $F$. Using normal forms with respect to a fixed reduction strategy, instead of only reduced forms of the $X^{\alpha}$, we also obtain a unique normal form for $g_{\text {red }}$ which we will call as the normal form and denote by $\mathrm{N} f g$. The normal form operator is again linear. If $g$ is a polynomial, the above normal form and the normal form from Section 2 coincide.

Let $g=\sum_{\alpha \in \mathbb{N}^{n}} c_{\alpha} X^{\alpha} \in S$ and let $r=\left(r_{1}, \ldots, r_{n}\right)$ be an $n$-tuple of positive real numbers. Following [9] we define the norm

$$
\|g\|_{r}:=\sum_{\alpha \in \mathbb{N}^{n}}\left|c_{\alpha}\right| r^{\alpha}
$$

and the set $B_{r}:=\left\{g \in S \mid\|g\|_{r}<+\infty\right\}$ of formal power series of finite norm. Clearly, we have $E \subseteq B_{r}$ for any $r$. We shall always consider the space $E$ as a Frechet space with the topology determined by the system of seminorms (norms) $\|\cdot\|_{r}$ corresponding to all $r$. Let us fix $\mathfrak{D} \subseteq \mathbb{N}^{n}$ and set $B_{r}(\mathfrak{D}):=B_{r} \cap S(\mathcal{D})$. The space $B_{r}$ is a Banach algebra (cf. [9]), $B_{r}(\mathcal{D})$ as a closed subspace of $B_{r}$ is a Banach space and $E(\mathcal{D})$ is a closed subspace of $E$.

From this and from elementary facts concerning power series we may deduce the following lemma.

Lemma 3.2. Let $r_{v}=\left(r_{1 v}, \ldots, r_{n v}\right), v=1,2, \ldots$ be a sequence of $n$-tuples of positive real numbers such that

$$
r_{j v} \rightarrow+\infty \quad \text { when } v \rightarrow \infty, \quad \text { for } j=1,2, \ldots, n
$$

If $g_{\alpha} \in E(\mathbb{D})$, for $\alpha \in \mathbb{N}^{n}$, and

$$
\sum_{\alpha \in \mathbb{N}^{n}}\left\|g_{\alpha}\right\|_{r_{v}}<+\infty, \quad \text { for } v=1,2, \ldots
$$

then the series $\sum_{\alpha \in \mathbb{N}^{n}} g_{\alpha}$ is convergent in $E$ and its sum $g \in E(\mathbb{D})$.

Remark. Let $g_{\alpha}=\sum_{\beta \in \mathbb{N}^{n}} g_{\alpha \beta} X^{\beta}$, for $\alpha \in \mathbb{N}^{n}$. Since the assumptions of Lemma 3.2 imply that the family $\left(c_{\alpha \beta} x^{\beta}\right)_{\alpha, \beta \in \mathbb{N}^{n}}$ is absolutely summable, for any $x \in \mathbb{K}^{n}$, $\sum_{\alpha, \beta \in \mathbb{N}^{n}} c_{\alpha \beta} X^{\beta}$ is independent of ordering of summation.

Before we apply this convergence criterion to our reduced power series we need a norm estimation in connection with the reduction process of polynomials.

Lemma 3.3. Let $F \subset R$ be a finite set and $\prec$ an admissible term well-ordering. There exists a sequence $r_{v}$ as in Lemma 3.2 such that

$$
\left\|g^{\prime}\right\|_{r_{v}}+\left\|c_{\gamma} X^{\gamma}\right\|_{r_{v}} \leq\|g\|_{r_{v}}, \quad \text { for } v=1,2, \ldots
$$

for any simple reduction step $g^{\prime}=g-c_{\gamma} X^{\gamma} f$ where $g$ and $g^{\prime}$ are polynomials and $c_{\gamma}, X^{\gamma}$, and $f$ are as in formula (5).

Proof. By Lemma 2.1 there exists a linear form $L=\sum_{i=1}^{n} l_{i} X_{i}$ such that $\left.\sqsubset_{L}\right|_{\operatorname{supp} F}=$ $\left.\prec\right|_{\text {supp } F}$.

Set $\rho_{v}=\left(v^{l_{1}}, \ldots, v^{l_{n}}\right)$. Since $F$ is finite there exists $v_{0} \in \mathbb{N}$ such that

$$
\left\|\mathrm{in}_{\prec_{L}} f\right\|_{\rho_{v}}=\left\|\mathrm{c}_{\prec_{1}} f| |^{L\left(\exp _{\alpha_{L}} f\right)} \geq\right\| \operatorname{tail}_{\Omega_{L}} f \|_{\rho_{v}}+1, \quad \text { for all } f \in F \text { and } v \geq v_{0}
$$

where $\prec_{L}$ is the refinement (4) of $\sqsubset_{L}$.

Since $\operatorname{in}_{<} f=\operatorname{in}_{\alpha_{L}} f$ and $\operatorname{tail}_{<} f=\operatorname{tail}_{\alpha_{L}} f$ for any polynomial $f \in F$, the sequence $r_{\nu}=\rho_{v+v_{0}}, \quad v=1,2, \ldots$ satisfies the conditions assumed in Lemma 3.2 and

$$
\begin{equation*}
\left\|\mathrm{in}_{\prec} f\right\|_{r_{v}} \geq\left\|\operatorname{tail}_{\prec} f\right\|_{r_{v}}+1, \quad \text { for all } f \in F \text { and } v=1,2, \ldots \tag{6}
\end{equation*}
$$

We set $\alpha:=\gamma+\exp _{\prec} f$. Then $g$ can be decomposed in the form $g=c_{\alpha} X^{\alpha}+p$ such that $\alpha \notin \operatorname{supp} p$ and $c_{\alpha}=c_{\gamma}$ lc $c_{\prec} f$. Consequently, $\|g\|_{r_{v}}=\|p\|_{r_{v}}+\left\|c_{\alpha} X^{\alpha}\right\|_{r_{v}}=$ $\|p\|_{r_{v}}+\left\|c_{\gamma} X^{\gamma_{i n}} f_{i_{v}}=\right\| p\left\|_{r_{v}}+\right\| c_{\gamma} X^{\gamma}\left\|_{r_{v}}\right\| \operatorname{in}_{\alpha} f \|_{r_{v}}(v=1,2, \ldots)$. By (6) it follows

$$
\begin{equation*}
\|g\|_{r_{v}} \geq\|p\|_{r_{v}}+\left\|c_{\gamma} X^{\gamma}\right\|_{r_{v}}\left(\left\|\operatorname{tail}_{\prec} f\right\|_{r_{v}}+1\right) \quad(v=1,2, \ldots) \tag{7}
\end{equation*}
$$

Applying the triangular inequality to the equation

$$
g^{\prime}=g-c_{\gamma} X^{\gamma} f=p+c_{\alpha} X^{\alpha}-c_{\gamma} X^{\gamma} \mathrm{in}_{\prec} f-c_{\gamma} X^{\gamma} \text { tail }_{\prec} f=p-c_{\gamma} X^{\gamma} \text { tail }_{\prec} f
$$

and then using the estimation (7) yields

$$
\left\|g^{\prime}\right\|_{r_{v}} \leq\|p\|_{r_{v}}+\| c_{\gamma} X^{\gamma} \text { tail }_{\alpha} f\left\|_{r_{v}}=\right\| p\left\|_{r_{v}}+\right\| c_{\gamma} X^{\gamma}\left\|_{r_{v}}\right\| \text { tail }_{\alpha} f\left\|_{r_{v}} \leq\right\| g\left\|_{r_{v}}-\right\| c_{\gamma} X^{\gamma} \|_{r_{v}}
$$

for $v=1,2, \ldots$, which completes the proof.
Proposition 3.4. Let $F \subset R$ be a finite set of polynomials, $\prec$ an admissible term wellordering and $r_{y}$ the sequence from Lemma 3.3. Then for any strong $G$-representation

$$
g=\sum_{f \in F} h_{f} f+g_{\mathrm{red}}
$$

of $g \in R$ with respect to $F$ and $\prec$ the following the conditions are satisfied:
(i) $\left\|g_{\text {red }}\right\|_{r_{v}}+\sum_{f \in F}\left\|h_{f}\right\|_{r_{v}} \leq\|g\|_{r_{v}}$,
(ii) $\left\|g_{\text {red }}\right\|_{r_{v}} \leq\|g\|_{r_{v}}$,
(iii) $\left\|h_{f}\right\|_{r_{v}} \leq\|g\|_{r_{v}}$ for all $f \in F$, for all $v=1,2, \ldots$.

Proof. Since the given G-representation of $g$ is strong it can be rewritten in the form

$$
g=\sum_{\mu=1}^{m} c_{\mu} X^{\alpha_{\mu}} f_{\mu}+g_{\mathrm{red}}
$$

providing a reduction sequence

$$
g \xrightarrow{F} g-c_{1} X^{\alpha_{1}} f_{1} \xrightarrow{F} g-\sum_{\mu=1}^{2} c_{\mu} X^{\alpha_{\mu}} f_{\mu} \xrightarrow{F} \cdots \xrightarrow{F} g-\sum_{\mu=1}^{m} c_{\mu} X^{\alpha_{\mu}} f_{\mu}=g_{\mathrm{rcd}}
$$

Condition (i) follows by applying Lemma 3.3 to each step of the reduction sequence. The conditions (ii) and (iii) are trivial consequences from (i).

As the next proposition will show, the important property (ii) of Proposition 3.4 is not only valid for polynomials but also for convergent power series.

Proposition 3.5. Let $F$, $\prec$ and $r_{v}$ be as in Proposition 3.4. Furthermore, let $g=$ $\sum_{\alpha \in \mathbb{N}^{n}} c_{\alpha} X^{\alpha} \in E$. Then we have the following properties:
(i) the series $g_{\text {red }}=\sum_{\alpha \in \mathbb{N}^{n}} c_{\alpha} X_{\text {red }}^{\alpha}$ is convergent in $E\left(\mathfrak{D}_{F}\right)$,
(ii) $\left\|g_{\text {red }}\right\|_{r_{v}} \leq\|g\|_{r_{v}}$, for $v=1,2, \ldots$.

Proof. (i) follows from condition (ii) of Proposition 3.4 and Lemma 3.2 since $X_{\text {red }}^{\alpha} \in$ $R\left(\mathfrak{D}_{F}\right) \subset E\left(\mathfrak{D}_{F}\right)$.
(ii) follows from

$$
\left\|g_{\text {red }}\right\|_{r_{v}} \leq \sum_{\alpha \in \mathbb{N}^{n}}\left\|c_{\alpha} X_{\text {red }}^{\alpha}\right\|_{r_{v}} \leq \sum_{\alpha \in \mathbb{N}^{n}}\left\|c_{\alpha} X^{\alpha}\right\|_{r_{v}}=\|g\|_{r_{v}}
$$

Two very useful results we may conclude from this proposition are:
Lemma 3.6. Let $F$ be a finite subset of $R$ and Nf a (power series) normal form operator with respect to $F$ and an admissible term well-ordering $\prec$. Then:
(i) The operator $\mathrm{Nf}: E \longrightarrow E\left(\mathfrak{D}_{F}\right)$ is continuous.
(ii) If $F$ is Gröbner basis of some ideal $I \subset R$ then $\mathrm{Nf} g=0$ for any element $g \in I E$.

Proof. (i) follows immediately from condition (ii) of Proposition 3.5 and the linearity condition of Nf .
(ii) There exists a sequence of polynomials $g_{\mu} \in I, \mu=1,2, \ldots$ such that $\lim _{\mu \rightarrow \infty}$ $g_{\mu}=g$. From Lemma 2.4 and the assumption that $F$ is a Gröbner basis, we obtain $\mathrm{Nf} g_{\mu}=0$ for the polynomials $g_{\mu} \in I$. Since Nf is a continuous operator it follows

$$
\mathrm{Nf} g=\lim _{\mu \rightarrow \infty} \mathrm{Nf} g_{\mu}=0
$$

The following main theorem of this paper states that there is a division formula for convergent power series modulo an ideal $I$ generated by polynomials. Furthermore, the remainder of $g$ with respect to a Gröbner basis of $I$ is the only element of $E\left(\mathcal{D}_{I}\right)$ which is congruent to $g$ modulo $I E$.

Theorem 3.7. Let $I \subset R$ be a polynomial ideal generated by the finite set $F$ and $\prec a$ term ordering. For $g \in E$ and $g_{\mathrm{red}} \in E\left(\mathfrak{D}_{F}\right)$ such that $g \xrightarrow{F, \longrightarrow} g_{\mathrm{red}}$ we have:
(i) There exists a division formula

$$
\begin{equation*}
g=\sum_{f \in F} h_{f} f+g_{\mathrm{red}} \tag{8}
\end{equation*}
$$

where $h_{f} \in E$. In case $g$ is a polynomial the division formula is a $G$-representation.
(ii) Let $F$ be a Gröbner basis of I with respect to $\prec$. Then for any power series $g^{\prime} \in E\left(\mathfrak{D}_{F}\right)$ such that $g-g^{\prime} \in I E$ we have $g^{\prime}=g_{\text {red }}$.

Proof. (i) Let $g=\sum_{\alpha \in \mathbb{N} n} c_{\alpha} X^{\alpha}$. According to Definition 3.1 there are strong Grepresentations

$$
X^{\alpha}=\sum_{f \in F} h_{f, \alpha} f+X_{\mathrm{red}}^{\alpha}
$$

such that $g_{\text {red }}=\sum_{\alpha \in \mathbb{N} n} c_{\alpha} X_{\text {red }}^{\alpha}$. Therefore,

$$
g=\sum_{\alpha \in \mathbb{N}^{n}} \sum_{f \in F} h_{f, \alpha} f+g_{\mathrm{red}} .
$$

Set $h_{f}:=\sum_{\alpha \in \mathbb{N}^{n}} h_{f, \alpha}$. Using condition (iii) of Proposition 3.4 and Lemma 3.2 it will follow immediately that the power series $h_{f}$ are absolutely, locally uniformly convergent in $\mathbb{K}^{n}$. The G-representation property is obvious.
(ii) By condition (i) it follows $g_{\mathrm{red}} \in I E$. Therefore, $g^{\prime}-g_{\mathrm{red}} \in I E \cap E\left(\mathfrak{D}_{F}\right)$. According to Lemma 3.6, for any normal form operator we must have $\mathrm{Nf}\left(g^{\prime}-g_{\text {red }}\right)=0$. But since $g^{\prime}-g_{\text {red }}$ is reduced this implies $g^{\prime}-g_{\text {red }}=0$ and this completes the proof of part (ii).

Note, that the notion of reduction introduced in Section 2 for polynomials could be used also for convergent power series. Obviously, a power series obtained by a reduction of a convergent power series would be also convergent and also congruent to the first power series modulo the ideal generated by $F$. But in general, after a finite number of reductions nothing of interest is produced, i.e. we do not gain constructivity. Therefore, we decided to start with the reduction notion of Definition 3.1, which provides immediately a useful result.

The theorem shows that the vector space basis of $R / I$ defined by a Gröbner basis of $I$ has the preferable property that the image of any convergent power series modulo $I E$ represented in terms of this basis is convergent, too. The following example shows that this property is not a matter of course for an arbitrary vector space basis of $R / I$.

Example: Consider the ideal $I=(y-1) R \subset R=\mathbb{K}[X, Y]$. The monomials $\left\{X^{k} Y^{k!} \mid k \in\right.$ $\mathbb{N}\}$ give a basis of the vector space $R / I$. But $\sum_{k=0}^{\infty} X^{k} / k$ ! takes the representation $\sum_{k=0}^{\infty}$ $X^{k} Y^{k!} / k!$ in terms of the above basis which is not convergent in $\mathbb{K}^{2}$.

During the final preparations of this paper we got information about a very interesting paper of Djakov and Mitiagin ([7]). There, a division algorithm is presented for a convergent power series modulo polynomial ideals with respect to the degreewise lexicographical term ordering. Since the authors did not apply the theory of Gröbner bases in [7], their results are less constructive than it is here. Furthermore, the restriction of the term ordering will restrict also the possible applications. For instance, the proof of the affine version of Serre's graph theorem given in the next section requires the use of an elimination ordering.

## 4. Applications of reduction

Very often the theory of Gröbner basis is applied to algorithmic solutions of computational tasks. In this section we will show that this theory may be also applied to prove hard theorems.

Theorem 4.1. Let $I$ be an ideal of $R$. Then $I E-\overline{I E}$, where over bar denotes the closure relative to the topology of the Frechet space E.

Proof. Let $g \in \overline{I E}$, i.e. there exists a sequence $\left(g_{\mu}\right)_{\mu=1,2, \ldots .}$ of series $g_{\mu} \in I E$ converging to $g$, i.e. $\lim _{\mu \rightarrow \infty} g_{\mu}=g$. Let $F$ be a reduced Gröbner basis of $I$ and Nf a normal form operator with respect to $F$. From the condition (ii) of Lemma 3.6 it follows $\mathrm{Nf} g_{\mu}=0$, for $\mu=1,2, \ldots$, and so the condition (i) of Lemma 3.6 implies $\mathrm{Nf} g=0$. By condition (i) of Theorem 3.7 there exists a representation

$$
g=\sum_{f \in F} h_{f} f+0
$$

where $h_{f} \in E$, for $f \in F$. This implies $g \in I E$ and completes the proof.
In the complex case, i.e. $\mathbb{K}=\mathbb{C}$, our topology coincides with the topology of local uniform convergence. Therefore, in this situation our theorem gives a closedness of the ideal $I E$ in the topology of local uniform convergence in $\mathbb{C}^{n}$ (cf. [16, Theorem 4.4]).

Now we come to a second application. Let $V$ be an algebraic subset of $\mathbb{K}^{n}$ and $f \in E$ such that $f \mid V: V \rightarrow \mathbb{K}$ has algebraic graph. If $\mathbb{K}=\mathbb{C}$ then (by Serre's graph theorem [18]) there exists a polynomial $g$ such that $g|V=f| V$ (for some more details we refer to $[17,11]$ ).

Now we present a different proof of this fact (also for $\mathbb{K}=\mathbb{R}$ ) together with a construction of $g$.

Theorem 4.2. Let $I \subset R$ be the ideal of the set $V$. If $f \in E$ has algebraic graph on $V$ then $f_{\text {red }}$ with respect to any Gröbner basis of $I$ is a polynomial.

Proof. Let us consider the reduction with respect to the Gröbner basis $F$ of $I$ with respect to the ordering $\prec$. We introduce a new variable $Y$ and consider the ring $R_{Y}:=$ $R[Y]=\mathbb{K}[X, Y]$ and choose an ordering $\prec_{Y}$ convenient for the elimination of $Y$ (see Proposition 2.9) which coincides with $\prec$ for monomials depending only on $X$. Analogously, $E_{Y}$ denotes the ring of power series convergent in the entire space $\mathbb{K}^{n+1}$.

By assumption the graph $W=V\left((Y-f) E_{Y}+I E_{Y}\right)$ is algebraic. Therefore, there exists an ideal $J \subset R_{Y}$ defining the same variety, i.e. $V(J)=W$.

Let $G$ be a Gröbner basis of $J$ with respect to $\prec_{r}$. Consequently, $G \cap R$ is a Gröbner basis of $J \cap R$ with respect to $\prec$ and any polynomial belonging to $G$ but not to $R$ has an initial term depending on $Y$. Note, that a polynomial or convergent power series has a unique reduced form with respect to a Gröbner basis, therefore, the terminology "the reduced form", which will be used in the remaining proof, is justified. Since $Y-f$
vanishes on $W$ the reduced forms of $Y$ and $f$ with respect to $G$ have to be the same according to our main Theorem 3.7.

On the one hand, $f$ depends only on the indeterminates $X$ and therefore the reduced form of $f$ with respect to $G$ is the same as with respect to $G \cap R$. But the reduced form of $f$ with respect to $G \cap R$ lies in $E$ and is independent of $Y$. On the other hand, $Y$ is a polynomial and its reduced form with respect to $G$ is again a polynomial.

Combining both results we get $f_{\text {red }} \in R$, where the reduction is performed with respect to $G \cap R$. According to the construction of $W$ all elements of $I$ vanish on $W$. Therefore, $I R_{Y} \subseteq J$ and $I \subseteq J \cap R$. Conversely, let us consider the projection $\Pi(W)$ of $\mathbb{K}^{n+1}$ to $\mathbb{K}^{n}$ parallel to the $Y$-axis. Then $V(J \cap R)=\overline{\Pi( }(W)=V(I)=V$. By definition, $I$ contains all polynomials from $R$ vanishing on $V$, therefore, $J \cap R \subseteq I$. In conclusion $I=J \cap R$ and $f_{\text {red }}$ is the polynomial we were looking for.

From the theorem we may deduce that a convergent power series has algebraic graph on an algebraic set $V$ if and only if the power series reduces to a polynomial with respect to an arbitrary Gröbner basis of the ideal defined by $V$. That gives a criterion to decide whether or not the graph of a given convergent power series is algebraic on a given algebraic set $V$. First of all we choose an ordering and compute the Gröbner basis of the ideal of $V$ with respect to this ordering. If we may prove that the result of the reduction of the power series with respect to the Gröbner basis has only finite support then we may conclude that the graph is algebraic. Contrary to this, if we may show that the support is infinite then we have proved that the graph is not algebraic. In order to facilitate the above task it should be stressed that we have the free choice of the ordering and may try to find a convenient one.

Of course, the above criterion often will not lead to a decision. If the reduction of convergent power series would be algorithmic all could be solved. Indeed, this is not the case but note also that the question for finiteness of the support may be much easier to answer than finding the reduced power series.

We will close the section with an example.
Example. Consider the ideal $I \subset R=\mathbb{K}[X, Y, Z]$ generated by the polynomials

$$
\begin{aligned}
F=\{ & X^{2} Z^{2}+3 Y Z^{3}+6 Z^{4}+X^{2} Y+6 Z^{3}+6 Z^{2}+9 Z \\
& 12 Y Z^{4}+3 Y^{4}+12 Y Z^{3}+12 Y Z^{2}+18 Y Z \\
& \left.3 Z^{5}+X^{2} Z^{2}+3 Y Z^{3}+X^{2} Y\right\}
\end{aligned}
$$

and the convergent power series

$$
g=\sum_{i, j=0}^{\infty} \frac{Y^{i} Z^{j}}{i!j!}
$$

Probably, it is not obvious from the first view whether or not $g$ has an algebraic graph over $V(I)$. But computing the reduced Gröbner basis $G_{\mathrm{d}}$ of $I$ with respect to
the degreewise lexicographical ordering gives

$$
\begin{aligned}
G_{d}=\{ & Z^{4}+1 / 3 X^{2} Z, Y Z^{3}+1 / 3 X^{2} Y, \\
& X^{2} Z^{2}-2 X^{2} Z+6 Z^{3}+6 Z^{2}+9 Z \\
& X^{2} Y Z-3 / 4 Y^{4}+X^{2} Y-3 Y Z^{2}-9 / 2 Y Z \\
& Y^{4} Z-3 Y^{4}+2 Y Z^{2}-6 Y Z \\
& X^{4} Z+54 X^{2} Z-171 Z^{3}-162 Z^{2}-162 Z \\
& X^{4} Y+27 / 2 Y^{4}-9 Y Z^{2}+27 Y Z \\
& X^{2} Y^{4}+165 / 2 Y^{4}-2 X^{2} Y+6 Y Z^{2}+171 Y Z, \\
& \left.Y^{7}+492 Y^{4}-4 Y Z^{2}+984 Y Z\right\}
\end{aligned}
$$

Reducing the power series $g$ will give a result containing all three indeterminates. Nevertheless, looking carefully, one realizes that the number of reduced monomials which are not pure powers of $X$ is finite and that the support of the reduced form of $g$ does not contain pure powers of $X$, i.e. the graph of $G$ is algebraic on $V$. Using the reduced Gröbner basis

$$
\begin{aligned}
G_{l}=\{ & Z^{5}-2 Z^{4}-2 Z^{3}-2 Z^{2}-3 Z \\
& Y^{4}+4 Y Z^{4}+4 Y Z^{3}+4 Y Z^{2}+6 Y Z \\
& \left.X^{2} Z+3 Z^{4}, X^{2} Y+3 Y Z^{3}\right\}
\end{aligned}
$$

of $I$ with respect to the lexicographical ordering this is much more obvious. One may immediately see, that $I \cap \mathbb{K}[Y, Z]$ is zero-dimensional, and therefore, the reduced form of the power series $g$ with respect to $G_{l}$ must be a polynomial in $Y$ and $Z$ since also $g$ depends only on $Y$ and $Z$.

## References

[1] J. Apel, A relationship between Gröbner bases of ideals and vector modules of G-algebras, Contemp. Math. 131 (1992) 195-204.
[2] D. Bayer, The division algorithm and the Hilbert Scheme, Ph.D. Thesis, Harvard University, 1982.
[3] T. Becker and V. Weispfenning, Gröbner Bases, a Computational Approach to Commutative Algebra (Springer, Berlin, 1993).
[4] P. Beckmann and J. Stückrad, The concept of Gröbner algebras, J. Symbolic. Comput. 10 (1990) 465-479.
[5] B. Buchberger, Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal, Ph.D. Thesis, Univ. Innsbruck, 1965.
[6] B. Buchberger, An algorithmic method in polynomial ideal theory, in: N.K. Bose, ed., Recent Trends in Multidimensional System Theory (Reidel, Dordrecht, 1984) chapter 6.
[7] P.B. Djakov and B.S. Mitiagin, The structure of polynomial ideals in the algebra of entire functions, preprint 123, Polish Academy of Sciences, 1977.
[8] P. Gianni, B. Trager and G. Zacharias, Gröbner bases and primary decomposition of polynomial ideals, J. Symbolic. Comput. 6 (1988) 149-167.
[9] H. Grauert and R. Remmert, Analytische Stellenalgebren (Springer, Berlin, 1971).
[10] M. Lejeune-Jalabert, Effectivité de Calculus Polynomiaux, Cours de D.E.A., Université de Grenoble, Grenoble, 1986.
[11] S. Eojasiewicz, Introduction to Complex Analytic Geometry (Birkhäuser, Basel, 1991 ).
[12] T. Mora, An algorithm to compute the equations of tangent cones, Lecture Notes in Computer Science, Vol. 144, (Springer, Berlin, 1982) 158-165.
[13] T. Mora, Seven variations on standard bases, preprint, Univ. di Genova, Dip. di Mathematica, N. 45, 1988.
[14] L. Robbiano, Term orderings on the polynomial ring, Lecture Notes in Computer Science, Vol. 204 (Springer, Berlin, 1985) 513-517.
[15] L. Robbiano, On the theory of graded structures, J. Symbolic. Comput. 2 (1986) 139-170.
[16] W. Rudin, A geometric criterion for algebraic varieties, J. Math. Mech. 17 (1968) 671-683.
[17] W. Rusek and T. Winiarski, Criteria for regularity of holomorphic mappings, Bull. Polon. Acad. Sci. 28 (1980) 471-475.
[18] J.P. Serre, Géométrie algébraique et géométrie analytique, Ann. de L' Inst. Fourier 6 (1955-1956) 1-42.


[^0]:    ${ }^{1}$ This research was partially supported by KBN Grant Nr. 210779101 and by DAAD.
    *Corresponding author.

