Intersections of Sequences of Ideals Generated by Polynomials†

Dedicated to Professor Stanisław Lojasiewicz on his 70th birthday.

J. Apel, J. Stückrad, P. Tworzewski, T. Winiarski

Mathematics Subject Classification: 13P10, 41A05, 30E05

ABSTRACT

We present a method for determining the reduced Gröbner basis with respect to a given admissible term order of order type ω of the intersection ideal of an infinite sequence of polynomial ideals.

As an application we discuss the Lagrange type interpolation on algebraic sets and the "approximation" of the ideal I of an algebraic set by zero dimensional ideals, whose affine Hilbert functions converge towards the affine Hilbert function of I.

1 Introduction

Infinite descending ideal sequences are used for the definition of algebraic topologies (c.f. [ZS2]). The ideals will constitute a basis of neighbourhoods of 0. In order to obtain a Hausdorff space the intersection of the ideal family must be the zero-ideal. It is a well-known result (Theorem of Chevalley, c.f. [ZS2]) for complete semi-local rings that the powers of the intersection of all maximal ideals define the weakest algebraic topology such that the ring becomes a Hausdorff space. Furthermore, the Chevalley Theorem and the Krull Theorem (c.f. [ZS1]) state that the intersection of a descending ideal sequence is the zero ideal if and only if for each natural number r there exists an ideal in the sequence which is contained in the r-th power of the maximal ideal.

†This research was partially supported by KBN Grant Nr. 2 P03A 061 08 and by DAAD

In this paper we will discuss intersections of descending ideal sequences in rings of polynomials, germs, and entire functions. Due to the lack of completeness and for some rings also semi-locality we can not simply extend the ideas of Krull and Chevalley. However, at least in the case of polynomial functions we can give a satisfactory answer by means of Gröbner bases (cf. [B] and [BWK]).

Theorem 1 *Let $I_1 \supseteq I_2 \supseteq \ldots$ be a descending sequence of ideals of the polynomial ring $R = \mathbb{K}[X]$. Furthermore, for each $\nu = 1, 2, \ldots$ let G_ν be the reduced Gröbner basis of I_ν with respect to a fixed order $\prec$ of order type ω. Then the set $G = \bigcap_{\nu=\mu}^{\infty} G_\nu$ is the reduced Gröbner basis of the intersection ideal $I = \bigcap_{\nu=1}^{\infty} I_\nu$ with respect to $\prec$, for sufficiently large μ. In particular,*

$$\mathrm{lt}\left(\bigcap_{i=1}^{\infty} I_i\right) = \bigcap_{i=1}^{\infty} \mathrm{lt}(I_i)\,.$$

In Section 2 we will observe that the restriction to order type ω is essential.

The situation becomes much more complicated in rings lying between the polynomial ring and the ring of formal power series, e.g. the ring of entire functions. We have the two trivial marginal cases that the intersection is zero if we lift the ideals to the ring of formal power series or that the intersection is non-zero if we contract the ideals to the polynomial ring, where, of course, the decisions carry over.

The following example will illustrate that everything can happen in the area between these both marginal cases.

Example 1 *Let $R, E, \mathcal{O}_0$ be the rings of polynomials, entire functions and germs of analytic functions at 0, respectively, and let S be the ring of formal power series in the variables X and Y over the coefficient field $\mathbb{C}$. Furthermore, let (ρ_μ) be a sequence of positive integers satisfying the inequalities*

$$\rho_{\mu+1} > \mu\rho_\mu \quad (\mu \geq 1) \tag{1}$$

and let (c_μ) be an arbitrary sequence of non-zero complex numbers.
Consider the sequence

$$Q_\nu = \left(X - \sum_{\mu=1}^{\nu-1} c_\mu Y^{\rho_\mu},\, Y^{\rho_\nu}\right) R, \quad \nu = 1, 2, \ldots$$

of polynomial ideals. Set $f := X - \sum_{\mu=1}^{\infty} c_\mu Y^{\rho_\mu}$. If A denotes one of the rings $R, E, \mathcal{O}_0$, or S, then :

i) $Q_\nu A$ *is primary ideal with associated prime* $\mathfrak{m}_A = (X,Y)A$ *and* $Q_{\nu+1}A \subset Q_\nu A \not\subset \mathfrak{m}_A{}^2$ *for all* $\nu = 1, 2, \ldots,$

ii) $f \in A$ *implies that* $\bigcap_{\nu=1}^\infty Q_\nu A = fA,$

iii) $\bigcap_{\nu=1}^\infty Q_\nu A = (fS) \cap A,$

iv) $\bigcap_{\nu=1}^\infty Q_\nu R = \{0\},$

v) $f \notin \mathcal{O}_0$ *implies that* $\bigcap_{\nu=1}^\infty Q_\nu \mathcal{O}_0 = (\bigcap_{\nu=1}^\infty Q_\nu E)\, \mathcal{O}_0 = \{0\}.$

The results of Theorem 1 on the intersection of infinite ideal families in polynomial rings will be applied to interpolation problems. The corresponding main result is (for definitions c.f. Section 3):

Theorem 2 *Let* $V \subset \mathbb{K}^n$ *be an infinite algebraic set,* $I = I(V)$ *the ideal of* V*, and* $\prec$ *be an admissible term order of order type* ω*. Furthermore, let* $P_1, P_2, \ldots$ *be a sequence of points of* V *such that* $\mathcal{P}_r = \{P_1, \ldots, P_r\}$ *is admissible for interpolation w.r.t.* $\prec$ *for all* $r \geq 1$*. Then:*

i) The sequence of affine Hilbert functions [1] *of* $I_{\mathcal{P}_r}$ *is pointwise convergent towards the affine Hilbert function of* I*.*

ii) $I = \bigcap_{i=1}^\infty I_{\mathcal{P}_i}$*.*

iii) There exists r_0 *such that* $G_I \subseteq G_{I_{\mathcal{P}_r}}$ *for all* $r \geq r_0$*, where* G_I *and* $G_{I_{\mathcal{P}_r}}$ *are the reduced Gröbner bases (w.r.t.* $\prec$*) of* I *and* $I_{\mathcal{P}_r}$*, respectively.*

We note that the statement of this Theorem holds also for more general orders. But it depends on V which generalizations are allowed, see our remarks in Section 4.

The paper is organized as follows: In Section 2 we prove Theorem 1 and some related results. Moreover, we prove the statements of Example 1. In Section 3 we apply the results on intersections to the solution of interpolation problems. In particular, we prove Theorem 2. Finally, we discuss the relationship to the classical Lagrange interpolation and we give an outlook on interpolation of entire functions in Section 4.

[1] For the definition of the affine (or cumulative) Hilbert function see [CLO], Def. 2, p.428.

2 Intersection of families of polynomial ideals

Notations. We use the following notations: $R := \mathbb{K}[X]$, $S := \mathbb{K}[[X]]$, $\mathcal{O}_0 := \mathbb{K}\{X\} = \{f \in S | f \text{ is convergent in some neighbourhood of } 0\}$, and $E := \{f \in S | f \text{ is convergent in } \mathbb{K}^n\}$, where $X = (X_1, \ldots, X_n)$ is a list of indeterminates. Although, in the case of polynomial rings and rings of formal power series the results will not depend on the field $\mathbb{K}$, we will assume $\mathbb{K} = \mathbb{C}$ or $\mathbb{K} = \mathbb{R}$ if we consider convergent power series. The set of terms generated by X will be denoted by $T(X)$. A total order $\prec$ on $T(X)$ is said to be admissible if it satisfies the following two conditions

i) $1 \prec X^\alpha$ for each $\alpha \in \mathbb{N}^n \backslash \{0\}$

ii) $X^\alpha \prec X^\beta \Longrightarrow X^{\alpha+\gamma} \prec X^{\beta+\gamma}$, for all $\alpha, \beta, \gamma \in \mathbb{N}^n$.

An admissible term order $\prec$ is called of order type ω if for any term $t \in T(X)$ the set $\{s | s \prec t\}$ is finite. The support $\operatorname{supp}(f)$ of an element $f \in S$ is defined to be the set of all terms appearing in f with non-zero coefficient. If the term t is maximal with respect to $\prec$ amongst all elements of $\operatorname{supp}(f)$ then t is called the leading term $\operatorname{lt}_\prec(f)$ of f (w.r.t. $\prec$). The coefficient of $\operatorname{lt}_\prec(f)$ is called the leading coefficient of f (w.r.t. $\prec$) and denoted by $\operatorname{lc}_\prec(f)$. Clearly, 0 has no leading term. Power series with infinite support need not to have an leading term. The notion of leading term is extended to subsets $F \subset S$ by defining $\operatorname{lt}_\prec(F) := \{\operatorname{lt}_\prec(f) | f \in F, f \text{ posses a leading term}\}$. Furthermore, we introduce the notations $\Delta_\prec(F) := (\operatorname{lt}_\prec F) \cdot T(X)$ and $\mathcal{D}_\prec(F) := T(X) \backslash \Delta_\prec(F)$ for the monoid ideal generated by all leading terms of elements of F in the monoid of terms and its complement, respectively. By the ring inclusions $R \subset E \subset \mathcal{O}_0 \subset S$ the same definitions apply to the corresponding rings. Since, in general, it will be clear from the context which order is meant we will omit the index $\prec$ and we write e.g. $\operatorname{lt}(f)$ instead of $\operatorname{lt}_\prec(f)$.

Gröbner bases. Let F be a subset of an ideal $I \subset R$. Then F is called a Gröbner basis of I w.r.t. $\prec$ iff $\Delta(F) = \Delta(I)$. If, in addition, $\operatorname{supp}(f) \subseteq \mathcal{D}(F \setminus \{f\})$ and $\operatorname{lc}(f) = 1$ for all elements $f \in F$, then F is called reduced Gröbner basis. The reduced Gröbner basis of an ideal I w.r.t. $\prec$ is uniquely determined. Often, the monomial ideal $\operatorname{In}(F) = \operatorname{lt}(F) \cdot R$ of initial monomials of the elements of F is used instead of the monoid ideal $\Delta(F)$. Actually, such an approach allows to consider more general situations, e.g. polynomial rings over integral domains. In our situation, i.e. over coefficient fields, both considerations are equivalent. A well-known property of Gröbner bases is that the residue classes of the elements of $\mathcal{D}(F)$ form a vector space basis of the quotient ring R/I. Hence, for each polynomial $g \in R$ there exists a uniquely determined polynomial $g_{I,red}$ satisfying $g - g_{I,red} \in F \cdot R$ and $\mathrm{supp}(g_{I,red}) \subseteq \mathcal{D}(F)$. The polynomial $g_{I,red}$ can be considered as the remainder of the division of g by I. It can be computed using a reduction algorithm by Gröbner bases. An obvious property which will be applied in subsequent proofs is that $\mathrm{lt}(g) \in \mathcal{D}(I)$ implies $\mathrm{lt}(g_{I,red}) = \mathrm{lt}(g)$, and hence, $g \notin I$. Lifting I to the ring E of entire functions an appropriate division procedure can be applied also to arbitrary entire functions $g \in E$ (see [ASTW]) leading to a reduced form also denoted by $g_{I \cdot E,red}$. For a comprehensive introduction to the theory of Gröbner bases of ideals of polynomial rings we refer to [BWK] and [CLO].

Intersections. We consider an infinite sequence of ideals $I_\nu \subset R$, $\nu = 1, 2, \ldots$, and ask for an algorithm computing a generating set of $I = \bigcap_{\nu=1}^{\infty} I_\nu$. Using the results of Gianni, Trager, Zacharias on the intersection of a finite number of polynomial ideals ([GTZ], see also [BWK], [CLO]) the problem can be reduced to descending ideal sequences $(I_\nu)_{\nu=1,2,\ldots}$. In this situation Theorem 1 shows how to obtain the reduced Gröbner basis of I with respect to an admissible term order of order type ω.

Proof of Theorem 1. Set $G^{(\mu)} := \bigcap_{\nu=\mu}^{\infty} G_\nu$ for $\mu = 1, 2, \ldots$ and $\Delta := \bigcap_{\nu=1}^{\infty} \Delta(I_\nu)$. Trivially, $G^{(\mu)} \cdot R \subseteq I$ for all $\mu \geq 1$. Hence, it remains to prove $I \subseteq G^{(\mu)} \cdot R$, for suitable μ.

Consider the case $\Delta = \emptyset$ and assume that there exists $0 \neq f \in I$. From $\Delta = \emptyset$ we deduce the existence of $\nu_0 \geq 1$ such that $\mathrm{lt}(f) \notin \Delta(I_{\nu_0})$. Hence, $f_{I_{\nu_0},red} \neq 0$ and $f \notin I_{\nu_0}$ which contradicts $f \in I$. Consequently, $\Delta = \emptyset$ implies $I = \{0\} \subseteq G^{(\mu)} \cdot R$ for $\mu = 1, 2, \ldots$.

Now, let us consider the case $\Delta \neq \emptyset$. Then Δ is a monoid ideal of $T(X)$. Let $\{t_1, \ldots, t_m\}$ be its minimal basis. We will show that for any $i \in \{1, 2, \ldots, m\}$ there exist a positive integer μ_i and a polynomial g_i such that $\mathrm{lt}(g_i) = t_i$ and $g_i \in G^{(\mu)}$ for $\mu \geq \mu_i$.

Let us fix i. Each of the reduced Gröbner bases G_ν $(\nu = 1, 2, \ldots)$ will contain a polynomial $g_{i,\nu} \in G_\nu$ whose leading term divides $t_i \in \Delta \subseteq \Delta(I_\nu)$. Since $\mathrm{lt}(g_{i,\nu}) \in \Delta(I_\mu)$ for all $\mu \leq \nu$ we can additionally assume that $\mathrm{lt}(g_{i,\mu})$ divides $\mathrm{lt}(g_{i,\nu})$. Because t_i has only finitely many divisors the sequence $(\mathrm{lt}(g_{i,\nu}))_{\nu=1,2,\ldots}$ will eventually stabilize. By the assumption that t_i belongs to the minimal basis of Δ we deduce that there exists μ_i' such that $\mathrm{lt}(g_{i,\nu}) = t_i$ for all $\nu \geq \mu_i'$. Let $f_{\nu_1,\nu_2} = g_{i,\nu_1} - g_{i,\nu_2}$ be the difference of two of the above polynomials, where $\mu_i' \leq \nu_1 < \nu_2$. Assume, $f_{\nu_1,\nu_2} \neq 0$. We have $f_{\nu_1,\nu_2} \in I_{\nu_1}$ and, hence, $\mathrm{lt}(f_{\nu_1,\nu_2}) \in \Delta(I_{\nu_1})$. Furthermore, it follows $\mathrm{lt}(f_{\nu_1,\nu_2}) \notin \mathrm{supp}(g_{i,\nu_1})$, $\mathrm{lt}(f_{\nu_1,\nu_2}) \in \mathrm{supp}(g_{i,\nu_2})$ and $\mathrm{lt}(f_{\nu_1,\nu_2}) \notin \Delta(I_{\nu_2})$ from the assumption that G_{ν_1} and G_{ν_2} are reduced Gröbner bases. Taking into account also $\mathrm{lt}(f_{\nu_1,\nu_2}) \prec t_i$ we can summarize $\mathrm{lt}(f_{\nu_1,\nu_2}) \in (\Gamma_i \cap \Delta(I_{\nu_1})) \setminus \Delta(I_{\nu_2}) \subseteq (\Gamma_i \cap \Delta(I_{\nu_1})) \setminus \Delta$, where Γ_i is defined as the set $\{t \in T(X) \mid t \prec t_i\}$ of all terms smaller than t_i (w.r.t. $\prec$). One easily verifies $\bigcap_{\nu=1}^{\infty} (\Gamma_i \cap \Delta(I_\nu)) \setminus \Delta = \emptyset$. Each of the sets $(\Gamma_i \cap \Delta(I_\nu)) \setminus \Delta$ is finite since Γ_i is finite due to the assumption that $\prec$ is of order type ω. Hence, there exists $\mu_i \geq \mu_i'$ such that $(\Gamma_i \cap \Delta(I_\nu)) \setminus \Delta = \emptyset$ for all $\nu \geq \mu_i$. Consequently, $f_{\nu_1,\nu_2} = 0$ for all $\mu_i \leq \nu_1 < \nu_2$ and $g_i := g_{i,\mu_i} \in G^{(\mu_i)} = \bigcap_{\nu=\mu_i}^{\infty} G_\nu$. Combining the results for all $i = 1, 2, \ldots, m$ we obtain $\{g_1, \ldots, g_m\} \subseteq \bigcap_{\nu=\mu}^{\infty} G_\nu$ where $\mu := \max(\mu_1, \ldots, \mu_m)$. Finally, from

$$\Delta = (\mathrm{lt}(g_1), \ldots, \mathrm{lt}(g_m)) \cdot T(X) \subseteq \Delta\left((g_1, \ldots, g_m) \cdot R\right) \subseteq \Delta(I) \subseteq \Delta$$

and $(g_1, \ldots, g_m) \cdot R \subseteq I$ it follows that $G = \{g_1, \ldots, g_m\}$ is a Gröbner basis of I. Since G is subset of some other reduced Gröbner basis it is reduced, too. □

A trivial consequence of Theorem 1 is:

Corollary 1 *Let $R = \mathbb{K}[X]$ be the polynomial ring in the variables $X = \{X_1, \ldots, X_n\}$ over the field $\mathbb{K}$ and let $\prec$ be an admissible term order of order type ω. Then the intersection $I = \bigcap_{\nu=1}^{\infty} I_\nu$ of a sequence of ideals satisfying*

$$I_{\nu+1} \subseteq I_\nu \subset R \quad (\nu = 1, 2, \ldots)$$

is the zero ideal if and only if

$$\bigcap_{\nu=1}^{\infty} \Delta(I_\nu) = \emptyset\,.$$

Remark: If $\mathbb{K}$ is one of the fields $\mathbb{R}$ or $\mathbb{C}$ then we can use the following alternative proof for Corollary 1 by applying only analytic arguments.

Proof: Assume $\Delta := \bigcap_{\nu=1}^{\infty} \Delta(I_\nu) \neq \emptyset$. Since Δ is non-empty intersection of monoid ideals it is a monoid ideal of $T(X)$, too. Therefore, it possesses a finite and uniquely determined minimal basis $\{t_1, \ldots, t_m\}$. Using this basis we try to construct a non-zero polynomial f belonging to the intersection $I = \bigcap_{\nu=1}^{\infty} I_\nu$. We take polynomials $f_\nu \in I_\nu$ such that $\mathrm{lt}(f_\nu) = t_1$ for $\nu = 1, 2, \ldots$. The union $\bigcup_{\nu=1}^{\infty} \mathrm{supp} f_\nu$ of the supports of these polynomials is finite. Hence, all polynomials f_ν belong to a finite dimensional vector space V over $\mathbb{K}$. We may multiply the polynomials f_ν by suitable $c_\nu \in \mathbb{K}$ such that $\|c_\nu f_\nu\| = 1$ with respect to the norm $\|\cdot\|$ defined by

$$\| \sum_{\alpha \in \mathbb{N}^n} d_\alpha X^\alpha \| = \sqrt{\sum_{\alpha \in \mathbb{N}^n} |d_\alpha|^2} \quad .$$

The infinite sequence $c_\nu f_\nu$ belongs to a (compact) unit sphere in our finite dimensional vector space V, and, consequently, has at least one accumulation point. Fixing a natural number $\nu_0 \geq 1$ then any polynomial $c_\nu f_\nu$ such that $\nu \geq \nu_0$ belongs to I_{ν_0}. Since polynomial ideals are closed in the topology defined by the norm $\|\cdot\|$ any accumulation point f of the sequence belongs to I_{ν_0}, too. Finally, $f \in I$, $\|f\| = 1$ and, therefore, $f \neq 0$. $\square$

Proof of the statements contained in Example 1. Obviously, $Q_{\nu+1} \subset Q_\nu$. All ideals Q_ν have the same radical $\text{Rad } I_\nu = (X, Y)R$ $(\nu \geq 1)$. Since this radical is a maximal ideal $\mathfrak{m}_R$ in R we can deduce that all Q_ν are primary ideals with associated prime ideal $\mathfrak{m}_R$. From the given bases we can immediately read off that $Q_\nu \not\subset {\mathfrak{m}_R}^2$ for all $\nu = 1, 2, \ldots$. The same remains true if we lift the ideals of both sides to the ring $E, \mathcal{O}_0$, or S, respectively. This proves property i).

The basic idea to verify the properties ii) and iii) is to consider isomorphic images of the Q_ν. Note, that for any formal power series $p \in \mathbb{C}[[Y]]$ which does not contain a constant term the mapping $X \mapsto X + p$ and $Y \mapsto Y$ defines a homomorphism $\Phi_p : S \to S$. The mapping Φ_p is invertible with inverse Φ_{-p}, hence it is an automorphism. One checks easily that $p \in A$ implies that the restriction $\Phi_p|_A$ of Φ_p to A is an automorphism of A.

In order to prove property ii) we set $p := \sum_{\mu=1}^{\infty} c_\mu Y^{\rho_\mu} = X - f$. Note, with $f \in A$ we have also $p \in A$. Hence, $\Phi_p|_A\,(Q_\nu A) = (X, Y^{\rho_\nu})A$ for all $\nu = 1, 2, \ldots$ and

$$\Phi_p|_A(\bigcap_{\nu=1}^{\infty} Q_\nu A) = \bigcap_{\nu=1}^{\infty} (X, Y^{\rho_\nu})A = XA \, .$$

Applying the inverse mapping yields property ii).

Now, we will prove property iii). Set $p_\nu := \sum_{\mu=1}^{\nu-1} c_\mu Y^{\rho_\mu}$ for all $\nu = 1, 2, \ldots$. Since $p_\nu \in R \subseteq A$ we have

$$\Phi_{p_\nu}|_A(Q_\nu A) = (X, Y^{\rho_\nu})A = ((X, Y^{\rho_\nu})S) \cap A = \Phi_{p_\nu}(Q_\nu S) \cap A$$

for all rings A under consideration.

Applying the inverse mapping, computing the intersection, and using ii) for $A = S$ yields

$$\bigcap_{\nu=1}^{\infty} Q_\nu A = \left(\bigcap_{\nu=1}^{\infty} Q_\nu S\right) \cap A = (fS) \cap A$$

The properties ii) and iii) show that $f \in A$ will imply $fA = (fS) \cap A$. Now, we will consider the intersection ideal $(fS) \cap A$ in some particular cases when $f \notin A$.

Clearly, for any possible values of the coefficients c_μ we have $f \notin R$. But for each other ring A under consideration there exist suitable coefficients c_μ such that A is the smallest ring containing f among all considered rings A, e.g. $c_\mu = \frac{1}{\rho_\mu!}$ implies $f \in E \backslash R$, $c_\mu = 1$ yields $f \in \mathcal{O}_0 \backslash E$, and finally $f \in S \backslash \mathcal{O}_0$ for $c_\mu = \rho_\mu!$.

It follows the proof of property iv). Assume that there exists a non-zero polynomial $g \in \bigcap_{\nu=1}^{\infty} Q_\nu$. Then g can be written in the form

$$g = h_s X^s + \cdots + h_1 X + h_0 \,,$$

where h_i $(0 \leq i \leq s)$ are polynomials depending only on Y and $h_s \neq 0$.

The given bases G_ν of the ideals Q_ν are Gröbner bases with respect to the lexicographical order defined by $Y < X$. Therefore, g lies in the intersection of the Q_ν if and only if the reduction of g with respect to G_ν leads to the zero polynomial for all $\nu = 1, 2, \ldots$. Such a reduction consists of the substitution of X by $\sum_{\mu=1}^{\nu-1} c_\mu Y^{\rho_\mu}$ and the deletion of all powers of Y higher than ρ_ν. Replacement of X in g yields a sum of products of polynomials in Y. The degree of the products is bounded above by

$$\max_{1 \leq i \leq s} \left(i\rho_{\nu-1} + \deg h_i\right) \,.$$

For sufficiently large $\nu > \nu_0$ this maximum will be reached exactly in the case $i = s$. By formula 1 it follows immediately that there exists a sufficiently large ν_1 such that $s\rho_{\nu-1} + \deg h_s < \rho_\nu$ for all $\nu \geq \nu_1$. In conclusion $\deg g_{Q_\nu, red} = s\rho_{\nu-1} + \deg h_s$ for $\nu \geq \max(\nu_0, \nu_1)$ which contradicts the assumption $g \in \bigcap_{\nu=1}^{\infty} Q_\nu$.

Note, that we have

$$\bigcap_{\nu=1}^{\infty} \Delta(Q_\nu) = X \cdot T(X, Y) \,.$$

So, we observe as a by-product that the order type ω is essential in Theorem 1 and Corollary 1.

Finally, we prove property v). Consider coefficients c_μ such that $f \in S \backslash \mathcal{O}_0$. Furthermore, assume that there exists a non-zero element $g \in (fS) \cap \mathcal{O}_0$, Both, $\mathcal{O}_0$ and S, are unique factorization domains. Since f is irreducible in S there exists an irreducible factor g' of g in $\mathcal{O}_0$ which is divisible by f in S. Since the constant term of $X - f \in \mathbb{C}[Y]$ is equal to zero, $f(X-f, Y) = 0$, and f (formally) divides g', we have $g'(X-f, Y) = 0$, i.e. $X - f$ is a (formal) solution of the analytic equation $g'(X,Y) = 0$. According to Artin's Theorem ([A], see also [T]) there exists also a convergent series solution $X(Y) \in \mathbb{C}\{Y\}$ of the equation $g'(X,Y) = 0$. Since g' is irreducible in $\mathcal{O}_0$ it will follow $X - X(Y) = g'u$ for some unit $u \in \mathcal{O}_0$. Consequently, f divides $X - X(Y)$ in S. Hence, $f = X - X(Y)$ which contradicts $f \notin \mathcal{O}_0$. Therefore, $((fS) \cap E)\mathcal{O}_0 = (fS) \cap \mathcal{O}_0 = \{0\}$. $\square$

3 Admissible interpolation systems

Notation. Let $\mathcal{F} = \{F_1, \dots, F_\mu\}$ be a system of μ functions and $\mathcal{P} = \{P_1, \dots, P_\mu\}$ be a system of μ points then by definition:

$$det(\mathcal{F}, \mathcal{P}) := det\,(F_i(P_j))_{i,j=1,\dots,\mu}\ .$$

Writing $det(\mathcal{F}, \mathcal{P}) \neq 0$ without explicitly claiming the enumeration of $\mathcal{F}$ and $\mathcal{P}$ we will understand that according to an arbitrary enumeration, which makes sense since the enumeration can influence only the sign.

About interpolation. Interpolation means, that we are looking for a function from a given class which takes prescribed values at given points. Usually, we expect the class of functions and the set of points to be fixed and the interpolation function to be uniquely determined by the prescribed values. Interpolation by polynomials can be considered from two points of view. Firstly, we fix a system $\mathcal{P} = \{P_1, \dots, P_\mu\}$ and ask for an "optimal" system $M \subset T(X)$ of μ terms such that for any data $b_1, \dots, b_\mu \in \mathbb{K}$ there exists a unique polynomial $F \in Lin(M)$, where $Lin(M)$ is the linear subspace of $\mathbb{K}[X]$ spanned by M, such that $F(P_j) = b_j$ for $j = 1, \dots, \mu$. Secondly, an "optimal" system $M \subset T(X)$ is given and we are looking for "good" nodes $\mathcal{P}$. Note, that $\mathcal{P}$ and M give unique interpolation solutions if and only if $det(M, \mathcal{P}) \neq 0$.

The use of Gröbner bases for solving interpolation problems is not new. So, Becker and Weispfenning applied Gröbner basis techniques in order to solve the following problem: Find a minimal polynomial which takes prescribed values and derivatives on points or parameterized hypersurfaces in

$\mathbb{K}^n$ (see [BW]). It can happen that the problem is unsolvable, but the algorithm will realize that.

The question under consideration in this paper is different and can be roughly described as follows: Assume that it is possible to determine the value of the function at an arbitrary point. What is a good choice of a sequence of points such that the successive interpolation functions will converge towards the original function? In particular, polynomial functions shall be reconstructed after finitely many steps. In the multivariate case the question is clearly non-trivial since a bad choice of points could lead, for instance, to only univariate polynomials. In fact, we will deal with the problem in a more general setting. We are considering not only functions with domain $\mathbb{K}^n$ but also such defined on algebraic sets.

Interpolation via Gröbner bases. Let $V \subset \mathbb{K}^n$ be an algebraic set. We consider the corresponding vanishing ideal $I = I(V)$ in $K[X]$ and fix an admissible term order $\prec$. Since the residue classes $X^\alpha + I$ corresponding to $X^\alpha \in \mathcal{D}(I)$ form a basis of $\mathbb{K}[X]/I$ it is natural to consider for interpolation only polynomials with supports in $\mathcal{D}(I)$.

Let $\mathcal{P}$ be a system of μ pairwise different points of V and let $I(\mathcal{P})$ be the corresponding polynomial ideal. Then $\dim_{\mathbb{K}} \mathbb{K}[X]/I(\mathcal{P}) = \mu$ and, hence, $\mathcal{D}(I(\mathcal{P}))$ consists of exactly μ elements of $\mathcal{D}(I)$. (Note, that $I \subseteq I(\mathcal{P})$ implies $\mathcal{D}(I(\mathcal{P})) \subseteq \mathcal{D}(I)$.) Different systems $\mathcal{P}' \subseteq V$ of μ points can lead to different sets $\mathcal{D}(I(\mathcal{P}'))$. But there is a unique set $\mathcal{D} \subset \mathcal{D}(I)$ consisting of μ terms such that $\mathcal{D}(I(\mathcal{P})) = \mathcal{D}$ for a non-empty Zariski open set in the set of μ-tuples of pairwise different points of V, namely the set $\mathcal{D}(I)^{(\mu)}$ of the μ smallest (w.r.t. $\prec$) terms of $\mathcal{D}(I)$. This is a direct consequence of the following

Theorem 3 *Let $I = I(V) \subseteq \mathbb{K}[X_1, \ldots, X_n] = \mathbb{K}[X]$ be the ideal defined by the algebraic set $V \subseteq \mathbb{K}^n$. Furthermore, let $\mathcal{P} = \{P_1, \ldots, P_\mu\}$ be a system of μ pairwise different points of V and $I(\mathcal{P}) \subseteq \mathbb{K}[X]$ be the ideal corresponding to $\mathcal{P}$. Then for any admissible term order $\prec$ we have:*

$$\mathcal{D}(I(\mathcal{P})) = \mathcal{D}(I)^{(\mu)} \Longleftrightarrow det\left(\mathcal{D}(I)^{(\mu)}, \mathcal{P}\right) \neq 0$$

Proof: ($\Longrightarrow$) $\mathcal{D}(I)^{(\mu)}$ is basis of $\mathbb{K}[X]/I(\mathcal{P})$ by construction. Hence, the determinant has to be unequal zero.

($\Longleftarrow$) The condition on the determinant implies that $\mathcal{D}(I)^{(\mu)}$ is linearly independent modulo $I(\mathcal{P})$ and according to its cardinality it is a basis of $\mathbb{K}[X]/I(\mathcal{P})$. By construction $\mathcal{D}(I(\mathcal{P})) \subseteq \mathcal{D}(I)$. Suppose there exists $X^\alpha \in$

$\mathcal{D}(I(\mathcal{P}))\setminus\mathcal{D}(I)^{(\mu)}$. Then $X^\alpha + I(\mathcal{P}) = l(X) + I(\mathcal{P})$, where $l(X)$ is a linear combination of the elements of $\mathcal{D}(I)^{(\mu)}$. Hence, $X^\alpha - l(X)$ is a polynomial of $I(\mathcal{P})$ having leading term X^α which contradicts the choice of X^α. $\square$

This observation justifies

Definition 1 *Let $V \subset \mathbb{K}^n$ be an algebraic set, $I = I(V)$ the ideal of V, and $\prec$ be an admissible term order. A set $\mathcal{P}$ of μ pairwise different points of V is called* admissible for interpolation *(w.r.t. $\prec$) if $\mathcal{D}(I(\mathcal{P})) = \mathcal{D}(I)^{(\mu)}$.*

Lemma 1 *Let V be an algebraic set and I be the ideal of V. Then for any given sequence of pairwise different terms $t_1, t_2, \ldots \in \mathcal{D}(I)$ there is a sequence $P_1, P_2, \ldots \in V$ such that*

$$det(\{t_1, t_2, \ldots, t_r\}, \{P_1, P_2, \ldots, P_r\}) \neq 0 \text{ for all } r \geq 1\,.$$

Proof: We construct $P_1, P_2, \ldots, P_r$ inductively on r.

$r = 1$: Since $t_1 \notin I$ we have $V \not\subseteq V(t_1)$, i.e. there exists $P_1 \in V$ such that $t_1(P_1) \neq 0$ and we are done in this case.

$r > 1$: Assume that $P_1, \ldots, P_{r-1}$ are already constructed then consider the polynomial

$$F := det(\{t_1, t_2, \ldots, t_r\}, \{P_1, P_2, \ldots, P_{r-1}, X\})$$

which has support contained in $\mathcal{D}(I)$. F is non-zero since the coefficient of t_r is equal to

$$det(\{t_1, t_2, \ldots, t_{r-1}\}, \{P_1, P_2, \ldots, P_{r-1}\}) \neq 0\,.$$

In conclusion, $F \notin I$. Hence, $V \not\subseteq V(F)$ and the existence of $P_r \in V$ such that $F(P_r) \neq 0$ follows. $\square$

As an obvious consequence we have

Corollary 2 *Each infinite algebraic subset V of $\mathbb{K}^n$ contains a sequence of points $P_1, P_2, \ldots$ such that $P_1, \ldots, P_r$ is admissible for interpolation, for all $r \geq 1$.*

Applying the results on ideal intersections from the preceding section we obtain our main theorem on interpolation as follows:

Proof of Theorem 2. Fix $d_0 \in \mathbb{N}$ and let $T^{(d_0)}$ be the set of all terms of total degree smaller or equal d_0. Furthermore, let s be the maximal element of $T^{(d_0)}$ with respect to $\prec$ and r_{d_0} the number of terms contained in $\mathcal{D}_I$ which are smaller or equal than s w.r.t. $\prec$. Note, that r_{d_0} is finite since $\prec$ is of order type ω.

Then

$$\mathcal{D}(I)^{(r_{d_0})} \cap T^{(d_0)} = \mathcal{D}(I) \cap T^{(d_0)}.$$

Since $\mathcal{P}_{r_{d_0}} = \{P_1, \ldots P_{r_{d_0}}\}$ is admissible for interpolation w.r.t. $\prec$ we have

$$\mathcal{D}(I(\mathcal{P}_{r_{d_0}})) = \mathcal{D}(I)^{(r_{d_0})}$$

Hence,

$$\mathcal{D}(I(\mathcal{P}_r)) \cap T^{(d_0)} = \mathcal{D}(I) \cap T^{(d_0)} \text{ for } r \geq r_{d_0}$$

Consequently, the affine Hilbert function of $I(\mathcal{P}_r)$ and I are equal at any point $d \leq d_0$ for $r \geq r_{d_0}$.

ii) The inclusion $I \subseteq \bigcap_{i=1}^{\infty} I_{\mathcal{P}_i}$ is trivial. Taking into account that the initial ideals of both sides are equal according to i) the above inclusion has to be equality.

iii) Follows by Theorem 1. $\square$

4 Concluding remarks.

Recall, that we were looking for "optimal" sets M of terms such that the linear space spanned by M defines the space of interpolation functions and we were looking for "good" nodes $\mathcal{P}$ such that $\mathcal{P}$ and M give unique interpolation solutions for any prescribed values at $\mathcal{P}$.

A set M consisting of μ terms is "optimal" in our theory if it consists of the μ smallest terms with respect to a fixed admissible term order which are not contained in the monoid ideal generated by the leading terms of the ideal defined by the algebraic set V which is the domain of the functions to be interpolated. So, in the particular case of $V = \mathbb{K}^n$, a degree compatible admissible term order $\prec$ and $\mu = \binom{\nu+n}{n}$ the set M will consist exactly of all terms having degree smaller or equal ν. This is the same notion of optimality as applied in classical Lagrange interpolation.

By definition the systems $\mathcal{P}$ which are admissible for interpolation are "good" nodes. In the non-trivial case of infinite algebraic sets V we proved that it is always possible to construct an infinite sequence of points such that each finite initial segment is admissible for interpolation. Moreover, each system of nodes which is admissible for interpolation can be prolonged by adding a new point.

So, actually we can find "optimal" M and "good" $\mathcal{P}$ for arbitrary admissible term orders. But using e.g. a lexicographical order on $V = \mathbb{K}^n$ all systems M will contain only powers of the smallest variable. Hence, each interpolation polynomial will be univariate. So, using more and more nodes will not provide better and better interpolation functions converging towards the original one. In order to have a convergence property, we need at least that enlarging M will exhaust $\mathcal{D}(I(V))$. Each admissible order of order type ω ensures such a behaviour since we can enumerate the elements of the vector space basis according to $\prec$ and then each set M containing at least as many elements as the number of a given term will contain that term, too. Note, that for particular V also some admissible orders which are not of order type ω can have the property that the enlargement of M exhausts the vector space basis. All statements formulated here for order type ω easily carry over also to such orders.

Theorem 2 proves that interpolation with respect to an order of order type ω has the property that interpolation of a polynomial function provides a sequence of interpolation polynomials converging towards the original function.[2] It would be nice to have a similar result also for entire functions. But in this case, convergence would require more than only exhausting M and $\mathcal{P}$ admissible for interpolation. In fact, it is necessary to find infinite sequences of nodes such that each initial segment is admissible for interpolation and such that, in addition, $I(V) \cdot E = \bigcap_{i=1}^{\infty} I_{\mathcal{P}_i} \cdot E$. The latter is far from being self-evident as Example 1 shows.

REFERENCES

[ASTW] J. Apel, J. Stückrad, P. Tworzewski, T. Winiarski, Reduction of everywhere convergent power series with respect to Gröbner bases. *J. Pure Appl. Algebra* **110**, S. 113–129, 1995.

[A] M. Artin, On the Solutions of Analytic Equations. *Invent. Math.* **5**, pp. 277–291, 1968.

[BW] T.Becker, V.Weispfenning, The Chinese Remainder Problem, Multivariate Interpolation, and Gröbner Bases. Proc. ISSAC'91, Bonn, ACM Press, S. 64 – 69, 1991.

[2] Moreover, polynomial functions are even reconstructed after finite many steps.

[BWK] T.Becker, V.Weispfenning, H.Kredel, Gröbner Bases, A Computational Approach to Commutative Algebra. Springer, 1993.

[B] B. Buchberger, Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal. Ph.D. Thesis, Univ. Innsbruck, 1965.

[CLO] D. Cox, J. Little, D. O'Shea, Ideals, Varieties, and Algorithms, Springer, 1992.

[GTZ] P. Gianni, B. Trager, G. Zacharias, Gröbner Bases and Primary Decomposition of Polynomial Ideals. *J.Symb.Comp.* **6**, pp. 149–167, 1988.

[T] J.Cl. Tougeron, Idéaux de fonctions différentiable, Springer, 1972.

[ZS1] O. Zariski, P. Samuel, Commutative Algebra. (Volume I), Springer, 1975.

[ZS2] O. Zariski, P. Samuel, Commutative Algebra. (Volume II), Springer, 1975.

Authors addresses.

J. Apel, J. Stückrad
Fakultät für Mathematik und Informatik, Universität Leipzig,
Augustusplatz 10–11, D-04109 Leipzig, Germany

apel@informatik.uni-leipzig.de stueckrad@mathematik.uni-leipzig.de

P. Tworzewski, T. Winiarski
Instytut Matematyki, Uniwersytet Jagielloński, Reymonta 4,
30-059 Kraków, Poland

tworzews@im.uj.edu.pl winiarsk@im.uj.edu.pl