A Sparse Effective Nullstellensatz

Martín Sombra [1]

Departamento de Matemática, Universidad Nacional de La Plata,
Calle 50 y 115, 1900 La Plata, Argentina.
E-mail: sombra@mate.unlp.edu.ar

Abstract.

We present bounds for the sparseness in the Nullstellensatz. These bounds can give a much sharper characterization than degree bounds of the monomial structure of the polynomials in the Nullstellensatz in case that the input system is sparse. As a consequence we derive a degree bound which can substantially improve the known ones in case of a sparse system.

In addition we introduce the notion of algebraic degree associated to a polynomial system of equations. We obtain a new degree bound which is sharper than the known ones when this parameter is small. We also improve the previous effective Nullstellensätze in case the input polynomials are quadratic.

Our approach is completely algebraic, and the obtained results are independent of the characteristic of the base field.

Keywords. Cohen–Macaulay ring, effective Nullstellensatz, Newton polytope, degree of a polynomial system of equations.

AMS Subject Classification. 13P10.

Introduction

Let k be a field and $\overline{k}$ be its algebraic closure. We denote the affine n–space over $\overline{k}$ by $\mathbb{A}^n$. For a given polynomial system $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$ without common zeros in $\mathbb{A}^n$, the classical Hilbert's Nullstellensatz states that there exist $g_1, \ldots, g_s \in k[x_1, \ldots, x_n]$ satisfying the Bézout equation

$$1 = g_1 f_1 + \cdots + g_s f_s. \tag{1}$$

Let d denote the maximum degree of the polynomials $f_1, \ldots, f_s$ and assume that $n \geq 2$. Then there exist polynomials $g_1, \ldots, g_s$ satisfying the degree bound

$$\deg g_i f_i \leq \max\{3, d\}^n.$$

This result is due to Kollár [21]. This bound is optimal for $d \geq 3$ because of the well–known example due to Mora–Lazard–Masser–Philippon–Kollár

$$f_1 := x_1^d,\ f_2 := x_1 x_n^{d-1} - x_2^d,\ \ldots,\ f_{n-1} := x_{n-2} x_n^{d-1} - x_{n-1}^d,\ f_n := x_{n-1} x_n^{d-1} - 1$$

[1] Partially supported by CONICET PID 3949/92, UBA CyT EX. 001 and Fundación Antorchas.

It is easy to verify that in this case $\deg g_1 f_1 \geq d^n$ for any solution system $g_1, \ldots, g_n$ of the Bézout equation.

We note that such a degree bound allows us, given polynomials $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$, to determine whether the equation (1) is solvable or not. If it is solvable, we can then actually find a solution, as it reduces the original problem to solving a k–linear system of equations.

The study of this Bézout identity is the object of much research, due to both its theoretical and practical importance, mainly in the context of computational algebraic geometry and diophantine approximation. Thus it has been approached from many points of view and with different objectives. In this respect we refer to the research papers [2], [4], [6], [8], [13], [15], [17], [22], [27], [30], [31], [32]. We also refer to the surveys [3], [26], [36] for a broad introduction to the history of this problem, main results and open questions.

For a Laurent polynomial $f = \sum_{i \in \mathbb{Z}^n} a_i \, x^i \in k[x_1, \ldots, x_n, x_1^{-1}, \ldots, x_n^{-1}]$, the *support* of f is defined as the set $\{i : a_i \neq 0\}$ and more generally, the support of a *family* of Laurent polynomials $f_1, \ldots, f_s$ is defined as the set of exponents of all the nonzero monomials of all the f_i. The *Newton polytope* $\mathcal{N}(f_1, \ldots, f_s)$ is defined as the convex hull of the support of $f_1, \ldots, f_s$. The *unmixed volume* $\mathcal{U}(f_1, \ldots, f_s)$ of the *family* of Laurent polynomials $f_1, \ldots, f_s$ is defined as $\rho!$ times the volume of the polytope $\mathcal{N}(f_1, \ldots, f_s)$, where ρ denotes the dimension of this polytope.

The degree of a polynomial is bounded by a nonnegative integer d if and only if its Newton polytope is contained in $d\,\Delta$, where Δ denotes the standard simplex $\mathrm{conv}(0, e_1, \ldots, e_n)$ in $\mathbb{R}^n$. Thus the notion of Newton polytope gives a sharper characterization of the monomial structure of a polynomial than just degree. This concept was introduced in the context of root counting by Bernshtein [5] and Kushnirenko [24], and is now in the basis of sparse elimination theory. Within this theory, algorithms for elimination problems are designed to try to exploit the sparseness of the involved polynomials, and sparseness is then usually measured in terms of the Newton polytope of these polynomials. This is the point of view introduced by Sturmfels in his foundational work [34] and further explored in [9], [20], [28], [29], [37] to name a few references.

The sparse aspect in the Nullstellensatz has also been considered by Canny and Emiris, who obtained a sparse effective Nullstellensatz but only for the case of $n+1$ *generic* n–variate Laurent polynomials [9]. Here, generic can be interpreted in the following sense: If one restricts the support of each f_i to lie in a fixed set $\mathcal{A}_i$ — thus restricting which monomials are allowed to appear — the coefficient values for which the Canny–Emiris Nullstellensatz *fails* lies in a codimension ≥ 1 subvariety of the coefficient space. This follows easily from recognizing that the failure of their sparse resultant–based derivation depends on the existency of roots at toric infinity. It should also be pointed out that when its genericity assumptions hold, the Canny–Emiris Nullstellensatz gives bounds at least as good as any result stated in the present paper.

We obtain the following result, which in this context can be seen as a bound for the sparseness of the output polynomials in terms of the sparseness of the input system.

Theorem 1. *Let $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$ be polynomials without common zeros in $\mathbb{A}^n$. Let $\mathcal{N}$ denote the Newton polytope of the polynomials $x_1, \ldots, x_n, f_1, \ldots, f_s$, and let $\mathcal{U}$*

denote the unmixed volume of this polytope. Then there exist $g_1, \dots, g_s \in k[x_1, \dots, x_n]$ *satisfying*

$$1 = g_1 f_1 + \cdots + g_s f_s,$$

with $\mathcal{N}(g_i f_i) \subseteq \; n^{n+3} \mathcal{U} \, \mathcal{N}$ *for* $i = 1, \dots, s$.

Let $d := \max_i \deg f_i$. We readily derive from the previous result the degree bound

$$\deg g_i f_i \le n^{n+3} \, d \, \mathcal{U}.$$

We obtain from this the worst–case bound $\deg g_i f_i \le n^{n+2} \, d^{n+1}$, as the unmixed volume of the polynomials $x_1, \dots, x_n, f_1, \dots, f_n$ is always bounded by d^n. We show however that our degree bound can considerably improve the usual one in case that the input system is sparse and $d \ge n$ (Example 2.12).

We also obtain an analogous result for the case of Laurent polynomials.

Theorem 2. *Let* $f_1, \dots, f_s \in k[x_1, \dots, x_n, x_1^{-1}, \dots, x_n^{-1}]$ *be Laurent polynomials without common zeros in* $(\overline{k}^*)^n$. *Let* $\mathcal{N}$ *denote the Newton polytope of* $f_1, \dots, f_s$, *and let* $\mathcal{U}$ *denote the unmixed volume of this polytope. Then there exist* $a \in \mathbb{Z}^n$ *and* $g_1, \dots, g_s \in k[x_1, \dots, x_n, x_1^{-1}, \dots, x_n^{-1}]$ *satisfying*

$$1 = g_1 f_1 + \cdots + g_s f_s,$$

with $a \in \; n^{2n+3} \mathcal{U}^2 \, \mathcal{N}$ *and* $\mathcal{N}(g_i f_i) \subseteq \; n^{2n+3} \mathcal{U}^2 \, \mathcal{N} - a$ *for* $i = 1, \dots, s$.

The proof of both results is similar. It takes as its first step the translation of the original system of equations over the affine space or the torus into a system of linear equations over an appropriate toric variety. The resulting system is then solved by appealing to an effective Nullstellensatz for linear forms in a Cohen–Macaulay graded ring. This key lemma is proved following for the most part the lines of a previous paper [33] which in turn is based on previous work of Dubé [11] and Almeida [1]. We introduce at this time some simplifications into the proofs and techniques involved. In particular we eliminate the use of estimates for the Hilbert function.

As a by–product, we obtain an effective Nullstellensatz which holds not only for linear forms, but for arbitrary homogeneous elements in a Cohen–Macaulay graded ring (Theorem 1.8).

In addition we apply these arguments in two other situations. First we consider the usual effective Nullstellensatz. Let $f_1, \dots, f_s \in k[x_1, \dots, x_n]$ be polynomials without common zeros in $\mathbb{A}^n$. Let $d_i := \deg f_i$ and assume that $d_1 \ge \cdots \ge d_s$ holds. We obtain the following improved degree bound:

$$\deg g_i f_i \le 2 \, d_s \prod_{j=1}^{\min\{n,s\}-1} d_j$$

for the polynomials $g_1, \dots, g_s$ satisfying the Bézout equation.

For the case when the polynomials $f_1, \dots, f_s$ are quadratic the best previous known bound is $\deg g_i f_i \le n \, 2^{n+2}$, which is due to Sabia and Solernó [30]. Our estimate improves this bound to $\deg g_i f_i \le 2^{n+1}$, which is very close to the expected 2^n.

Finally, we obtain another bound for the degrees in the Nullstellensatz. We introduce the notion of *algebraic degree* of a polynomial system. Roughly speaking it measures the degree of the ideals succesively cutted out by the equations $f_1, \ldots, f_s$. It is the algebraic analogue of the notion of geometric degree of a system of equations of Giusti et al. [16], Krick, Sabia and Solernó [23] and Sombra [33]. We refer to Section 3 for the precise description and comparison between both notions.

Degree bounds have been obtained for the polynomials in the Nullstellensatz which mainly depend on the geometric degree [15], [23], [33]. We show that a similar bound holds by replacing the geometric degree of the input polynomial system by the algebraic degree.

Theorem 3. *Let $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$ be polynomials without common zeros in $\mathbb{A}^n$. Let $d := \max_i \deg f_i$ and let δ denote the algebraic degree of this polynomial system. Then there exist $g_1, \ldots, g_s \in k[x_1, \ldots, x_n]$ satisfying*

$$1 = g_1 f_1 + \cdots + g_s f_s,$$

with $\deg g_i f_i \leq \min\{n, s\}^2 \, d \, \delta$ *for* $i = 1, \ldots, s$.

Let $d_i := \deg f_i$ and assume that $d_1 \geq \cdots \geq d_s$ holds. Then the Bézout bound $\delta(f_1, \ldots, f_s) \leq d_s \prod_{i=1}^{\min\{n,s\}-2} d_i$ holds, and therefore we essentially recover from this result the known bounds for the degrees in the Nullstellensatz. The algebraic degree is bounded by the geometric degree, and so we also recover the known degree bounds in the Nullstellensatz which depend on the geometric degree. We show however that the algebraic degree is much smaller than the geometric degree in some particular instances, and by force, than the Bézout bound d^{n-1} (Example 3.20). We conclude that the obtained degree bound is much sharper in these cases than the known ones.

The outline of the paper is as follows. In Section 1 we obtain the effective Nullstellensatz for linear forms in a Cohen–Macaulay graded ring. In Section 2 we prove both Theorems and and we derive some of their consequences. Section 3 is devoted to degree bounds in the usual Nullstellensatz.

1. An Effective Nullstellensatz over Cohen–Macaulay Graded Rings

Throughout this paper we denote by k be an infinite field and by $\overline{k}$ its algebraic closure. All the rings to be considered are Noetherian commutative, and more precisely, finitely generated k–algebras. The polynomial ring $k[x_0, \ldots, x_n]$ is alternatively denoted by S.

For a homogeneous ideal J in the polynomial ring $k[x_0, \ldots, x_n]$, $\dim J$ denotes the Krull dimension of $k[x_0, \ldots, x_n]/J$, and $\deg J$ denotes $(\dim J - 1)!$ times the leading coefficient of the Hilbert polynomial of the graded k–algebra $k[x_0, \ldots, x_n]/J$.

A graded ring A is *Cohen–Macaulay* if it contains a regular sequence of homogeneous elements of length equal to the dimension of A. In particular A is unmixed, and its quotient with respect to any regular sequence of homogeneous elements is Cohen–Macaulay.

Let I be a homogeneous Cohen–Macaulay ideal in the polynomial ring $k[x_0, \ldots, x_n]$, that is, the quotient ring $k[x_0, \ldots, x_n]/I$ is Cohen–Macaulay. Let $r := \dim I$ and let $V(I) \subseteq \mathbb{P}^n$ be the variety defined by I in the projective n–space.

Let $p \in S/I$ be a homogeneous element which is not a zero–divisor. Let $\eta_1, \ldots, \eta_s \in S/I$ be homogeneous elements of degree one — or for short, linear forms — which define the empty variety in the open set $\{p \neq 0\}$ of $V(I)$. In this situation, Hilbert's Nullstellensatz implies that p belongs to the radical of the ideal $(\eta_1, \ldots, \eta_s)$, that is, $p \in \sqrt{(\eta_1, \ldots, \eta_s)}$. Equivalently we have that 1 lies in the ideal $(\overline{\eta}_1, \ldots, \overline{\eta}_s)$ spanned by $\overline{\eta}_1, \ldots, \overline{\eta}_s$ in the ring $(S/I)_p$.

We are going to give a bound for the minimal $D \in \mathbb{N}$ such that p^D falls into the ideal $(\eta_1, \ldots, \eta_s)$. We state here the main result of this section, and then we derive it from a series of lemmas.

Main Lemma 1.1 *Let $I \subseteq k[x_0, \ldots, x_n]$ be a homogeneous Cohen–Macaulay ideal of dimension r. Let $p \in k[x_0, \ldots, x_n]/I$ be a homogeneous element and $\eta_1, \ldots, \eta_s \in k[x_0, \ldots, x_n]/I$ be linear forms such that p lies in the radical of the ideal $(\eta_1, \ldots, \eta_s)$ and p is not a zero–divisor. Then*

$$p^D \in (\eta_1, \ldots, \eta_s)$$

holds, with $D := \min\{r, s\}^2 \deg I$.

Particular cases of this result were obtained by Caniglia, Galligo and Heintz [8, Proposition 10] and Smietanski [32, Lemma 1.44]. As a consequence of this result we derive an effective Nullstellensatz for Cohen–Macaulay graded rings (Theorem 1.8 and Corollary 1.9).

Let A be a ring and let $\alpha_1, \ldots, \alpha_t$ be elements of A. Then $\alpha_1, \ldots, \alpha_t$ is called a *weak regular sequence* if $\overline{\alpha}_i$ is not a zero–divisor in the ring $A/(\alpha_1, \ldots, \alpha_{i-1})$ for $i = 1, \ldots, t$. We note that this definition differs from usual notion of regular sequence only in one point, namely that it allows $\overline{\alpha}_t$ to be a unit in $A/(\alpha_1, \ldots, \alpha_{t-1})$.

By considering generic k–linear combinations of the given linear forms we reduce to the case when $\overline{\eta}_1, \ldots, \overline{\eta}_s$ is a weak regular sequence in $(S/I)_p$ and $s \leq r$. We assume this from now on. Next we are going to show that $\eta_1, \ldots, \eta_s$ can be replaced by polynomials of controlled degree which form a regular sequence in S/I (Corollary 1.3). The following lemma is a generalization of [19, Remark 4].

Lemma 1.2 *Let $K \subseteq k[x_0, \ldots, x_n]$ be a homogeneous unmixed ideal and let $\xi_1, \ldots, \xi_m \in \mathbb{P}^n$ be points lying outside of $V(K)$. Then there exists a homogeneous polynomial g in K such that* $\deg g \leq \deg K$ *and* $g(\xi_i) \neq 0$ *for all* i.

Proof. For each associated prime ideal P of K we take a homogeneous polynomial g_P such that $\deg g_P \leq \deg P$ and $g_P(\xi_i) \neq 0$ for $i = 1, \ldots, m$. This is clear from a generic projection. Let Q_P be the corresponding P–primary ideal in the decomposition of K. Let $l(Q_P)$ denote the length of Q_P, that is, the length of $(S/Q_P)_P$ as a S/P–module. Let

$$g := \prod_P g_P^{\,l(Q_P)},$$

where the product is taken over all the associated prime ideals of K. Then $g(\xi_i) \neq 0$ for $i = 1, \ldots, m$, and we have also that the polynomial g lies in the ideal K by [7, Lemma 1]. The degree bound $\deg g \leq \sum_P l(Q_P) \deg P = \deg K$ holds by [38, Proposition 1.49]. $\square$

In the sequel we shall denote by J_i the contraction to the ring S/I of the ideal $(\overline{\eta}_1, \ldots, \overline{\eta}_i) \subseteq (S/I)_p$ and by δ_i the degree of the homogeneous ideal J_i for $i = 1, \ldots, s$.

Corollary 1.3 *With the notation of Main Lemma 1.1, there exist homogeneous elements $h_1, \ldots, h_s \in S/I$ satisfying the following conditions:*

i) $h_i \equiv p^{c_i} \eta_i \mod J_{i-1}$ *for some* $c_i \geq 0$,

ii) $h_1, \ldots, h_s$ *is a regular sequence,*

iii) $\deg h_i \leq \deg J_{i-1} + \deg p - 1$,

for $i = 1, \ldots, s$.

Proof. We proceed by induction on i. By assumption p is not a zero–divisor in S/I so that the canonical morphism $S/I \to (S/I)_p$ is injective. The fact that $\overline{\eta}_1$ is not a zero–divisor in $(S/I)_p$ implies then that η_1 is not a zero–divisor in S/I.

Now let $i \geq 2$ and assume that the elements $h_1, \ldots, h_{i-1}$ are already constructed. Let H_{i-1} denote the ideal spanned by $h_1, \ldots, h_{i-1}$ in S/I. Let $H_{i-1} = (\cap_j Q_j) \cap (\cap_l R_l)$ be the primary decomposition of H_{i-1}, with $p \notin \sqrt{Q_j}$ and $p \in \sqrt{R_l}$. Our aim is to find a homogeneous element h_i in S/I lying outside of all the associated primary ideals of H_{i-1}.

We recall that the ideal H_{i-1} has no imbedded component as it is spanned by a regular sequence in a Cohen–Macaulay ring. On the other hand the ideal J_{i-1} has the primary decomposition $\cap_j Q_j$ and so it follows that $V(R_l) \not\subseteq V(J_{i-1})$ holds for each l. We choose a point $\xi_l \in V(R_l) - V(J_{i-1})$ and a homogeneous element $g \in J_{i-1}$ such that $\deg g \leq \deg J_{i-1}$ and $g(\xi_l) \neq 0$ for each l. The existence of g is guaranteed by the previous lemma. By eventually multiplying g with linear forms we can suppose without loss of generality that $\deg g = c_i \deg p + 1$ holds for some $c_i \geq 0$. In particular we can assume that $\deg g \leq \deg J_{i-1} + \deg p - 1$ holds. Finally we set

$$h_i := ag + p^{c_i} \eta_i$$

for some $a \in k$ to be determined. Then h_i is homogeneous and $h_i \equiv p^{c_i} \eta_i \mod J_{i-1}$ holds. Therefore h_i does not belong to $\sqrt{Q_j}$, as both p and η_i are not zero–divisors modulo J_{i-1}. We have also that $h_i(\xi_l) = a\, g(\xi_l) + (p^{c_i} \eta_i)(\xi_l) \neq 0$ for a generic choice of a, which forces $h_i \notin \sqrt{R_l}$. $\square$

We fix the following notation. Let $h_1, \ldots, h_s \in S/I$ be the homogeneous polynomials introduced in Corollary 1.3, and let $H_i := (h_1, \ldots, h_i)$ and $L_i := (\eta_1, \ldots, \eta_i)$ denote the homogeneous ideals successively generated by $h_1, \ldots, h_s$ and $\eta_1, \ldots, \eta_s$ respectively.

Let us write $h_i = l_i + p^{c_i}\, \eta_i$ for some $l_i \in J_{i-1}$ and $c_i \geq 0$. Then set $\gamma_i := \delta_{i-1} - \delta_i$, and let $\lambda_i := \sum_{j=1}^{i} (\gamma_j + c_j)$ and $\mu_i := \sum_{j=1}^{i} ((i - j + 1)\gamma_j + (i - j) c_j)$ for $i = 1, \ldots, s$.

For an ideal K of S/I we denote by K^u the unmixed part of K, that is, the unmixed ideal given as the intersection of the primary components of K of maximal dimension.

Lemma 1.4 *Let $q \in J_i$ for some $1 \leq i \leq s$. Then $p^{\gamma_i} q \in (J_{i-1}, \eta_i)^u$.*

Proof. Let $(\cap_j Q_j) \cap (\cap_l R_l)$ be the primary decomposition of the ideal $(J_{i-1}, \eta_i)^u$, with $p \notin \sqrt{Q_j}$ and $p \in \sqrt{R_l}$. Then $\cap_j Q_j$ is the primary decomposition of J_i. Let $K_i := \cap_l R_l$ be the intersection of the other primary components. Then K_i is an unmixed ideal which lies in the hypersurface $\{p = 0\}$.

The ideals $(J_{i-1}, \eta_i)^u$ and (J_{i-1}, η_i) have the same degree because they only differ in an ideal of codimension at least $i+1$. Then $\deg(J_{i-1}, \eta_i) = \delta_{i-1}$, as η_i is not a zero–divisor mod J_{i-1}, and so $\deg K_i = \gamma_i = \delta_{i-1} - \delta_i$. Therefore p^{γ_i} lies in the ideal K_i [7, Lemma 1] and we conclude that $p^{\gamma_i} q \in (\cap_j Q_j) \cap (\cap_l R_l) = (J_{i-1}, \eta_i)^u$ as stated. □

The following two statements (Lemmas 1.5 and 1.6) are simple extensions of [11, Lemmas 6.1 and 6.2].

Lemma 1.5 *Let $q \in J_i$ for some $1 \le i \le s$. Then $p^{\lambda_i} q \in H_i$.*

Proof. We proceed by induction on i. First $p^{\gamma_1} q \in (\eta_1)^u$ by Lemma 1.4. We have also that $(\eta_1)^u = (\eta_1)$ and so the assertion is true for $i = 1$.

Let $i \ge 2$ and assume that the statement holds for $i - 1$. By Lemma 1.4, $p^{\gamma_i} q \in (J_{i-1}, \eta_i)^u$, that is, $p^{\gamma_i} q$ belongs to the intersection of the primary components of dimension $r - i$ of the ideal (J_{i-1}, η_i). The intersection of the other primary components is an ideal of codimension at least $i + 1$. Then there exists a regular sequence $w_1, \ldots, w_{i+1}$ in this ideal, as S/I is a Cohen–Macaulay ring. We have that $w_j\, p^{\gamma_i}\, q \in (J_{i-1}, \eta_i)$ and so there exist $u_j \in J_{i-1}$ and $v_j \in S/I$ such that $w_j\, p^{\gamma_i}\, q = u_j + v_j \eta_i$ for $j = 1, \ldots, i+1$. Then

$$w_j\, p^{\gamma_i + c_i}\, q = p^{c_i}\, u_j + p^{c_i}\, v_j\, \eta_i = p^{c_i} u_j + v_j(h_i - l_i) = (p^{c_i} u_j - v_j l_i) + v_j h_i.$$

Therefore $p^{\gamma_i + c_i} u_j - v_j l_i \in J_{i-1}$ and by the inductive hypothesis $p^{\lambda_{i-1}}(p^{\gamma_i + c_i} u_j - v_j l_i)$ lies in the ideal H_{i-1}. Then $w_j\, p^{\lambda_i}\, q \in H_i$ holds for $j = 1, \ldots, i+1$, as $\lambda_i = \lambda_{i-1} + \gamma_i - c_i$.

The ideal H_i is spanned by a regular sequence $h_1, \ldots, h_i$ and so it is an unmixed ideal of dimension $r - i$. Thus for each associated prime ideal P of H_i there exists some j such that $w_j \notin P$. We conclude that $p^{\lambda_i} q \in H_i$. □

Lemma 1.6 *Let $q \in J_i$ for some $1 \le i \le s$. Then $p^{\mu_i} q \in L_i$.*

Proof. We shall proceed by induction on i. The case $i = 1$ follows in the same way as in the preceding lemma because $L_1 = H_1$ and $\mu_1 = \lambda_1$.

Let $i \ge 2$. Then $p^{\lambda_i} q$ lies in H_i by Lemma 1.5. Let us write $p^{\lambda_i} q = u + v\, h_i$ for some $u \in H_{i-1}$ and $v \in S/I$. Therefore $p^{\lambda_i} q - v\, h_i \in H_{i-1}$ and thus $p^{\lambda_i} q - p^{c_i}\, v\, \eta_i$ lies in the ideal J_{i-1} because $H_{i-1} \subseteq J_{i-1}$ and $h_i \equiv p^{c_i}\, \eta_i \mod J_{i-1}$. This implies in turn that $p^{\lambda_i - c_i} q - v\, \eta_i \in J_{i-1}$.

From the inductive hypothesis we get that $p^{\mu_{i-1}}(p^{\lambda_i - c_i}\, q - v\, \eta_i)$ lies in L_{i-1} and so $p^{\mu_{i-1} + \lambda_i - c_i} q \in L_i$. The statement follows from the observation that $\mu_i = \mu_{i-1} + \lambda_i - c_i$. □

Proof of Main Lemma 1.1. We can suppose without loss of generality that $\overline{\eta}_1 \ldots, \overline{\eta}_s$ is a weak regular sequence in $(S/I)_p$ and that $s \le r$. After Lemma 1.6 it only remains to bound μ_s. We make use of the estimates $\gamma_i, c_i \le \delta_{i-1}$ and we get the bound

$$\begin{aligned} \mu_s &= \textstyle\sum_{j=1}^{s}((s - j + 1)\gamma_j + (s - j)c_j) \\ &\le \textstyle\sum_{j=1}^{s}((s - j + 1)\delta_{j-1} + (s - j)\delta_{j-1}) \le s^2 \deg I. \end{aligned}$$

□

The rest of the section is devoted to the extension of the previous result to the case when we consider homogeneous elements of arbitrary degree instead of linear forms. First we establish some generalities about the Veronese imbedding.

Let us denote by N the integer $\binom{n+d}{d} - 1$ and let $a_0, \ldots, a_N$ denote the exponents of the different monomials of degree d in S. Let

$$v_d : \mathbb{P}^n \to \mathbb{P}^N, \qquad x := (x_0 : \cdots : x_n) \mapsto (x^{a_0} : \cdots : x^{a_N})$$

be the Veronese map. This is a regular morphism of projective varieties and so its image is a closed subvariety of $\mathbb{P}^N$. This variety is called the Veronese variety and it is denoted by $v_{n,d}$. Let $I(v_{n,d})$ be its defining ideal and let us denote by $S^{(d)} := k[y_0, \ldots, y_N]/I(v_{n,d})$ its homogeneous coordinate ring. The Veronese map induces an inclusion of k–algebras $i_d : S^{(d)} \hookrightarrow S$ defined by $y_j \mapsto x^{a_j}$ for $j = 0, \ldots, N$.

Let J be an ideal of S and $J^{(d)}$ be its contraction to the ring $S^{(d)}$. Identifying the quotient ring $S^{(d)}/J^{(d)}$ with its image in S/J through the inclusion $i_d : S^{(d)}/J^{(d)} \hookrightarrow S/J$ we obtain the decomposition in graded parts

$$S^{(d)}/J^{(d)} = \oplus_j \, (S/J)_{d\,j}.$$

Let $h_{J^{(d)}}$ and h_J denote the Hilbert functions of $J^{(d)}$ and J respectively. Then $h_{J^{(d)}}(m) = h_J(d\,m)$ for $m \in \mathbb{N}$. It follows that the ideals $J^{(d)}$ and J have the same dimension and that their degrees are related by the formula $\deg J^{(d)} = d^{\,\dim J - 1} \deg J$.

Lemma 1.7 *Let J be a homogeneous Cohen–Macaulay ideal in S and let $J^{(d)}$ denote its contraction to the ring $S^{(d)}$. Then $J^{(d)}$ is a Cohen–Macaulay ideal.*

Proof. Let us denote by A and B the quotient rings $S^{(d)}/J^{(d)}$ and S/J respectively. We identify A with its image in B through the inclusion i_d. We shall exhibit a regular sequence of homogeneous elements in A of length equal to the dimension of A.

Let e denote the dimension of the ring B, which is also the dimension of A. Let $\beta_1, \ldots, \beta_e$ be a regular sequence in B of homogeneous elements. Let $\alpha_i := \beta_i^d$ for $i = 1, \ldots, e$. Then $\alpha_1, \ldots, \alpha_e$ are elements of A which form a regular sequence in B, by [25, Theorem 16.1]. We assert that they also form a maximal regular sequence in A. We need only to prove that α_i is not a zero–divisor in $A/(\alpha_1, \ldots, \alpha_{i-1})$ for $i = 1, \ldots, e$. Let $\zeta \in A$ be an element such that $\zeta\, \alpha_i \in (\alpha_1, \ldots, \alpha_{i-1})$. Then there exist homogeneous elements $\zeta_1, \ldots, \zeta_{i-1} \in B$ such that $\zeta = \zeta_1 \alpha_1 + \cdots + \zeta_{i-1}\alpha_{i-1}$ because $\alpha_1, \ldots, \alpha_{i-1}$ is a regular sequence in B. An easy verification shows that $\zeta_1, \ldots, \zeta_{i-1}$ can be chosen to lie in A, from which it follows that $\zeta \in (\alpha_1, \ldots, \alpha_{i-1})$. $\square$

Theorem 1.8 *Let $I \subseteq k[x_0, \ldots, x_n]$ be a homogeneous Cohen–Macaulay ideal. Let $f_1, \ldots, f_s \in k[x_0, \ldots, x_n]/I$ and $p \in k[x_1, \ldots, x_n]/I$ be homogeneous elements such that p lies in the radical of the ideal $(f_1, \ldots, f_s)$ and p is not a zero–divisor. Let $r := \dim I$ and $d := \max_i f_i$. Then*

$$p^D \in (f_1, \ldots, f_s)$$

holds, with $D := r^2\, d^r \deg I$.

Proof. First we note that the zero locus in $V(I)$ of the polynomials $\{f_i\}_i$ equals the zero locus in $V(I)$ of the polynomials $\{x_j^{d-\deg f_i} f_i\}_{ij}$. We have also that $x_j^{d-\deg f_i} f_i$ lies in the ideal $(f_1, \dots, f_s)$ for all i and j. Therefore we can suppose without loss of generality that f_i is a homogeneous polynomial of degree d for $i = 1, \dots, s$. We note however that the number of input polynomials have been enlarged in this preparative step.

Let $i_d : S^{(d)} \hookrightarrow S$ be the inclusion of k–algebras induced by the Veronese map and let $I^{(d)}$ denote the contraction of the ideal I to the ring $S^{(d)}$. Then we have the inclusion $i_d : S^{(d)}/I^{(d)} \hookrightarrow S/I$ and the decomposition in graded parts $i_d(S^{(d)}/I^{(d)}) = \oplus_j (S/I)_{dj}$. We take a linear form $\eta_i \in S^{(d)}/I^{(d)}$ such that $i_d(\eta_i) = f_i$ for $i = 1, \dots, s$, which exists as the inclusion i_d is a bijection in degree one. We take also a homogeneous element $q \in S^{(d)}/I^{(d)}$ such that $i_d(q) = p^d$.

The map $v_d : V(I) \to V(I^{(d)})$ is a dominant regular map of projective varieties and so it is surjective. Therefore the zero locus of the linear forms $\eta_1, \dots, \eta_s$ lies in the image of the zero locus of the polynomials $f_1, \dots, f_s$. The common zeros of $f_1, \dots, f_s$ lie in the hypersurface $\{p^d = 0\}$ of $V(I)$ and we have in addition that $v_d(\{p^d = 0\}) = \{q = 0\}$. Then the subvariety of $V(I^{(d)})$ defined by $\eta_1, \dots, \eta_s$ lies in the hypersurface $\{q = 0\}$.

By Lemma 1.7 the ideal $I^{(d)}$ is Cohen–Macaulay, and we have also that q is not a zero–divisor modulo $I^{(d)}$. Then we are in the hypothesis of the Main Lemma 1.1. As a consequence we obtain that

$$q^{\,r^2 \,\deg I^{(d)}} \in (\eta_1, \dots, \eta_s)$$

holds. Finally we apply the morphism i_d to the previous expression and we get that

$$p^{d\,r^2\,(d^{\,r-1}\deg I)} \in (f_1, \dots, f_s)$$

holds, as $\deg I^{(d)} = d^{r-1} \deg I$. □

Corollary 1.9 *Let $I \subseteq k[x_1, \dots, x_n]$ be an ideal such that its homogenization I^h in the ring $k[x_0, \dots, x_n]$ is Cohen-Macaulay. Let $f_1, \dots, f_s \in k[x_1, \dots, x_n]$ be polynomials without common zeros in the affine variety $V(I)$. Then there exist $g_1, \dots, g_s \in k[x_1, \dots, x_n]$ such that*

$$1 \equiv g_1 f_1 + \cdots + g_s f_s \pmod{I}$$

holds, with $\deg g_i f_i \le (r+1)^2\, d^{r+1} \deg I^h$ *for $i = 1, \dots, s$.*

Proof. By assumption the ideal I^h is a Cohen–Macaulay homogeneous ideal of dimension $r+1$. We have also that x_0 is not a zero–divisor modulo I^h.

Let f_i^h denote the homogenization of f_i for $i = 1, \dots, s$. The homogeneous polynomials $f_1^h, \dots, f_s^h$ have no common zero in $V(I^h)$ outside the hyperplane $\{x_0 = 0\}$. By Theorem 1.8 there exist homogeneous polynomials $v_1, \dots, v_s \in S$ such that

$$x_0^{(r+1)^2\, d^{r+1}} = v_1 f_1^h + \ldots + v_s f_s^h \pmod{I^h}$$

holds, with $\deg v_i f_i^h = (r+1)^2\, d^{r+1}$. The corollary then follows by evaluating $x_0 := 1$. □

Let the notation be as in Corollary 1.9. In the case when I is the zero ideal, that is, in the setting of the classic effective Nullstellensatz, we get the degree bound

$$\deg g_i f_i \le (r+1)^2\, d^{r+1}.$$

2. Sparse Effective Nullstellensätze

This section is devoted to our sparse effective Nullstellensätze (Theorems and) and the derivation of some of their consequences.

First we introduce notation and state some basic facts from polyhedral geometry and toric varieties. We refer to the books [14] and [35] for the proofs of these facts and for a more general background on these subjects.

Let $\mathcal{A} \subseteq \mathbb{Z}^n$ be a finite set of integer vectors. The convex hull of $\mathcal{A}$ as a subset of $\mathbb{R}^n$ is denoted by $\mathrm{conv}(\mathcal{A})$. The cone over $\mathrm{conv}(\mathcal{A})$ is denoted by $\mathrm{pos}(\mathcal{A})$, that is $\mathrm{pos}(\mathcal{A}) := \mathbb{R}_{\geq 0}\,\mathrm{conv}(\mathcal{A})$. The set $\mathcal{A}$ is *graded* if there exists an integer vector $\omega \in \mathbb{Z}^n$ such that $< a, \omega >= 1$ holds for every $a \in \mathcal{A}$, that is, when the set $\mathcal{A}$ lies in an affine hyperplane which does not contain the origin.

Let $\mathbb{Z}\mathcal{A}$ denote the $\mathbb{Z}$–module generated by $\mathcal{A}$. Let $\mathbb{R}\mathcal{A}$ denote the linear space spanned by $\mathcal{A}$, so that $\mathbb{Z}\mathcal{A}$ is a lattice in $\mathbb{R}\mathcal{A}$. Let ρ denote the dimension of this linear space. Then we consider the euclidian volume form in $\mathbb{R}A$, normalized in such a way that each primitive lattice simplex has unit volume. The normalized *volume* $\mathrm{Vol}(\mathcal{A})$ of the set $\mathcal{A}$ is defined as the volume of its convex hull with respect to this volume form.

We get readily from the definition the bound

$$\mathrm{Vol}(\mathcal{A}) \leq \rho!\,\mathrm{vol}\,(\mathrm{conv}(\mathcal{A})),$$

where $\mathrm{vol}\,(\mathrm{conv}(\mathcal{A}))$ denotes the volume of the convex hull of $\mathcal{A}$ with respect to the usual non–normalized volume form of $\mathbb{R}^n$. Let $\mathbb{N}\mathcal{A}$ denote the semigroup spanned by $\mathcal{A}$. This semigroup is always contained in the semigroup $\mathrm{pos}(\mathcal{A}) \cap \mathbb{Z}\mathcal{A}$. The set $\mathcal{A}$ is said to be *normal* or *saturated* if the equality $\mathbb{N}\mathcal{A} = \mathrm{pos}(\mathcal{A}) \cap \mathbb{Z}\mathcal{A}$ holds. A polytope $\mathcal{P}$ is said to be *integral* if it is the convex hull of a finite set of integer vectors.

An integral simplex is called *unimodular* if its interior contains no integral vector. Let $\mathcal{P}$ be an integral polytope. A subdivision of $\mathcal{P}$ is said to be *unimodular* if it consists solely of unimodular integral simplices. For an integral polytope $\mathcal{P}$ in $\mathbb{R}^n$, we denote by $\mathcal{A}(\mathcal{P})$ the set $\{1\} \times (\mathcal{P} \cap \mathbb{Z}^n)$, which is a graded set of integral vectors in $\mathbb{Z}^{n+1}$. We note that the set $\mathcal{A}(\mathcal{P})$ is normal in the case when $\mathcal{P}$ admits a unimodular subdivision.

With respect to toric geometry, we shall follow the lines of [35]. This point of view differs from the usual one in algebraic geometry. It is more combinatorial and suits better for our purposes. Let $\mathcal{A} = \{a_1, \ldots, a_N\}$ in $\mathbb{Z}^n$ be again a finite set of integer vectors. We associate to the set $\mathcal{A}$ the morphism

$$\varphi_{\mathcal{A}} : k[y_1, \ldots, y_N] \to k[x_1, \ldots, x_n, x_1^{-1}, \ldots, x_n^{-1}], \qquad y_i \to x^{a_i}.$$

The kernel of this map is a prime ideal $I_{\mathcal{A}}$ of $k[y_1, \ldots, y_N]$, called the *toric ideal* associated to the set $\mathcal{A}$. This ideal defines an *affine toric variety* $X_{\mathcal{A}}$ as its zero locus in $\mathbb{A}^N$. This variety is irreducible and its dimension equals the rank of the $\mathbb{Z}$–module $\mathbb{Z}\mathcal{A}$.

The k–algebra $k[x_1, \ldots, x_n, x_1^{-1}, \ldots, x_n^{-1}]$ is the coordinate ring of the torus $(\overline{k}^*)^n$. Thus the map $\varphi_{\mathcal{A}}$ induces a dominant map $(\overline{k}^*)^n \to X_{\mathcal{A}}$. The image of this map is called the *torus* $T_{\mathcal{A}}$ of the affine toric variety $X_{\mathcal{A}}$. This torus equals the open set $\{y_1 \cdots y_N \neq 0\}$ of $X_{\mathcal{A}}$.

The ideal $I_{\mathcal{A}}$ is homogeneous if and only if the set $\mathcal{A}$ is graded. In this case the set $\mathcal{A}$ defines a *projective toric variety* $Y_{\mathcal{A}}$ as the zero locus of the ideal $I_{\mathcal{A}}$ in the projective space $\mathbb{P}^{N-1}$. The dimension of $Y_{\mathcal{A}}$ equals then the rank of $\mathbb{Z}\mathcal{A}$ minus one, and its degree equals the normalized volume of the set $\mathcal{A}$.

Let $\mathcal{A} = \{a_1, \ldots, a_N\} \subseteq \mathbb{Z}^n$ be a graded set. The intersection of the projective variety $Y_{\mathcal{A}}$ with the affine chart $\{y_i \neq 0\} \cong \mathbb{A}^{N-1}$ equals the affine toric variety associated to the set

$$\mathcal{A} - a_i := \{a_1 - a_i, \ldots, a_{i-1} - a_i, a_{i+1} - a_i, \ldots, a_N - a_i\}.$$

In fact $Y_{\mathcal{A}}$ is irredundantly covered by the affine varieties $X_{\mathcal{A}-a_i}$, where a_i runs over the vertices of the polytope $\mathrm{conv}(\mathcal{A})$.

The k–algebra $k[y_1, \ldots, y_N]/I_{\mathcal{A}}$ is isomorphic to the semigroup algebra $k[\mathbb{N}\mathcal{A}]$. This algebra is normal if and only if the set $\mathcal{A}$ is normal. We recall Hochster's theorem that the k–algebra $k[\mathbb{N}\mathcal{A}]$ is a Cohen–Macaulay domain when the set $\mathcal{A}$ is normal [10].

Let $\mathcal{P}$ be an integral polytope of $\mathbb{R}^n$. This polytope determines a fan $\Delta_{\mathcal{P}}$ and a complete toric variety $X_{\mathcal{P}} = X(\Delta_{\mathcal{P}})$. This variety comes equipped with an ample Cartier divisor $D_{\mathcal{P}}$. This Cartier divisor defines then a map $\varphi_{\mathcal{P}} : X_{\mathcal{P}} \to \mathbb{P}^{N-1}$, where N denotes the cardinality of the set $\{\mathcal{P} \cap \mathbb{Z}^n\}$. The image of this map is the projective variety $Y_{\mathcal{A}(\mathcal{P})}$, where the set $\mathcal{A}(\mathcal{P})$ is defined as before as $\{1\} \times (\mathcal{P} \cap \mathbb{Z}^n)$ [14, Section 3.4]. The divisor $(n-1)D_{\mathcal{P}}$ is very ample [12], and so the graded set $\mathcal{A}((n-1)\,\mathcal{P})$ is normal.

Theorem 2.10 *Let $p, f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$ be polynomials such that p lies in the radical of the ideal $(f_1, \ldots, f_s)$. Let $\mathcal{P}$ be an integral polytope which contains the Newton polytope of the polynomials $1, x_1, \ldots, x_n, f_1, \ldots, f_s$. Assume furthermore that $\mathcal{A}(\mathcal{P})$ is a* normal *set of integer vectors in $\mathbb{Z}^{n+1}$. Then there exist $D \in \mathbb{N}$ and $g_1, \ldots, g_s \in k[x_1, \ldots, x_n]$ such that*

$$p^D = g_1 f_1 + \cdots + g_s f_s$$

holds, with $D \leq n! \min\{n+1, s\}^2 \operatorname{vol}(\mathcal{P})$ and $\mathcal{N}(g_i f_i) \subseteq (1 + \deg p)\, n! \min\{n+1, s\}^2 \operatorname{vol}(\mathcal{P})\ \mathcal{P}$ for $i = 1, \ldots, s$.

Proof. Let $\mathcal{B} = \{b_0, \ldots, b_N\}$ denote the set of integer vectors $\mathcal{P} \cap \mathbb{Z}^n$, so that $\mathcal{A}(\mathcal{P}) = \{1\} \times \mathcal{B}$. Assume that $b_0 = (0, \ldots, 0)$. We consider the morphism of k–algebras

$$\psi : k[y_1, \ldots, y_N] \to k[x_1, \ldots, x_n], \qquad y_i \mapsto x^{b_i}.$$

The kernel of this morphism is the defining ideal $I_{\mathcal{B}-b_0}$ of the affine toric variety $X_{\mathcal{B}-b_0}$. This affine variety is the intersection of the projective toric variety $Y_{\mathcal{A}(\mathcal{P})}$ with the affine cart $\{y_0 \neq 0\}$ of $\mathbb{P}^N$. In addition the map ψ induces an isomorphism $\mathbb{A}^n \to X_{\mathcal{B}-b_0}$.

Let ζ_i be a polynomial of degree one in $k[y_1, \ldots, y_N]$ such that $\psi(\zeta_i) = f_i$ for $i = 1, \ldots, s$. We take also a polynomial q in $k[y_1, \ldots, y_N]$ of degree less or equal to the degree of p such that $\psi(q) = p$. Then $\zeta_1, \ldots, \zeta_s$ have no common zero in $X_{\mathcal{B}-b_0}$ outside the hypersurface $\{q = 0\}$.

Let $\eta_1, \ldots, \eta_s, u$ denote the homogenization of $\zeta_1, \ldots, \zeta_s, q$ in $k[y_0, \ldots, y_N]$ respectively. Then the linear forms $\eta_1, \ldots, \eta_s$ have no common zero in $Y_{\mathcal{A}(\mathcal{P})}$ outside the hypersurface $\{y_0\, u = 0\}$.

By assumption the set $\mathcal{A}(\mathcal{P})$ is normal, and so $I_{\mathcal{A}(\mathcal{P})}$ is a Cohen–Macaulay prime homogeneous ideal of $k[y_0, \ldots, y_N]$ of dimension less or equal that $n+1$. We have also that $y_0\, u$ is not a zero–divisor modulo $I_{\mathcal{A}(\mathcal{P})}$. Then we are in the hypothesis of the Main Lemma 1.1. Let D denote the integer $\min\{n+1,s\}^2 \deg Y_{\mathcal{A}(\mathcal{P})}$. We obtain that there exist homogeneous elements $\alpha_1,\ldots,\alpha_s \in k[y_0,\ldots,y_N]/I_{\mathcal{A}(\mathcal{P})}$ of degree $(1+\deg u)\, D-1$ satisfying

$$(y_0\, u)^D = \alpha_1\eta_1+\cdots+\alpha_s\eta_s.$$

Finally we evaluate $y_0 := 1$ and we apply the map ψ to the preceding identity. We get

$$p^D = g_1 f_1+\cdots+g_s f_s,$$

where we have set $g_i(x) := \alpha_i(1, x^{b_1},\ldots,x^{b_N})$ for $i=1,\ldots,s$. We have the estimates $\deg u \le \deg p$ and $\deg Y_{\mathcal{A}(\mathcal{P})} \le n!\,\mathrm{vol}\,(\mathcal{P})$. We conclude that $D \le\ n!\, \min\{n+1,s\}\,\mathrm{vol}\,(\mathcal{P})$ and that the polytope $\mathcal{N}(f_i g_i)$ is contained in $((1+\deg p)\, n!\, \min\{n+1,s\}^2\, \mathrm{vol}\,(\mathcal{P}))\ \mathcal{P}$ for $i=1,\ldots,s$. □

We derive from the previous theorem the following degree bound.

Corollary 2.11 *Let the notation be as in Theorem 2.10 and $d := \max_i f_i$. Then there exist $D \in \mathbb{N}$ and $g_1,\ldots,g_s \in k[x_1,\ldots,x_n]$ such that*

$$p^D = g_1 f_1+\cdots+g_s f_s$$

holds, with $D \le\ n!\, \min\{n+1,s\}^2\, \mathrm{vol}\,(\mathcal{P})$ and $\deg g_i f_i \le\ d\,(1+\deg p)\, n!\, \min\{n+1, s,\}^2\, \mathrm{vol}\,(\mathcal{P})$ for $i=1,\ldots,s$.

□

We are going to show with an example that this degree bound can be much more precise than the usual one in case of a sparse input system.

Example 2.12 Let

$$f_i := a_{i0}+a_{i1}x_1+\cdots+a_{in}x_n+b_{i1}x_1\cdots x_n+\cdots+b_{id}(x_1\cdots x_n)^d$$

for $i=1,\ldots,s$ be polynomials without common zeros in $\mathbb{A}^n$. Let $\mathcal{P}_d := \mathrm{conv}(0,e_1,\ldots,e_n,d\,(e_1+\cdots+e_n))$ so that $\mathcal{P}_d$ contains the Newton polytope of the polynomials $1,x_1,\ldots,x_n,f_1,\ldots,f_s$. We have the decomposition

$$\mathcal{P}_d = \cup \mathcal{Q}_{ij}$$

with $\mathcal{Q}_{ij} := ((j-1)\,(e_1+\cdots+e_n), e_1,\ldots,\widehat{e_i},\ldots,e_n, j\,(e_1+\cdots+e_n))$ for $i=1,\ldots,n$ and $j=1,\ldots,d$. Then $\mathcal{P}_d$ is unimodular and so the set $\mathcal{A}(\mathcal{P})$ is normal. Thus we are in the hypothesis of Corollary 2.11 and we conclude that there exist $g_1,\ldots,g_s \in k[x_1,\ldots,x_n]$ such that

$$1 = g_1 f_1+\cdots+g_s f_s$$

holds, with $\mathcal{N}(g_i f_i) \subseteq n\, d\, \min\{n+1,s\}^2\, \mathcal{P}_d$, as the volume of $\mathcal{P}_d$ equals $d/(n-1)!$. In particular we get the degree bound $\deg g_i f_i \le (n+1)^4\, d^2$, which is much sharper than the estimate $\deg g_i f_i \le n^n\, d^n$ which follows from direct application of the usual degree bound.

Let notation be again as in Theorem 2.10. Let $\mathcal{N}$ denote the Newton polytope of the polynomials $1, x_1, \ldots, x_n, f_1, \ldots, f_s$ and let $\mathcal{U}$ denote the unmixed volume of this polytope. Assume that $n \geq 2$. In this situation we can then take the polytope $\mathcal{P}$ to be $(n-1)\,\mathcal{N}$. Then we get the bounds

$$D \leq n^{n+2}\,\mathcal{U}, \qquad \mathcal{N}(g_i f_i) \subseteq ((1+\deg p)\, n^{n+3}\,\mathcal{U})\,\mathcal{N}.$$

It is easy to check that these bounds hold also when $n = 1$. Thus Theorem follows from this observation in the particular case $p = 1$. We observe that in this case the condition $0 \in \mathcal{P}$ is redundant.

We remark that the naive notion of sparseness, based on counting the number of nonzero monomials in each polynomial, does not yield better bounds for the degrees in the Nullstellensatz than the usual ones, in view of the Mora–Lazard–Masser–Philippon–Kollár example.

We obtain a similar result in the case of Laurent polynomials.

Theorem 2.13 *Let $p, f_1, \ldots, f_s \in k[x_1^{-1}, \ldots, x_n^{-1}, x_1, \ldots, x_n]$ be Laurent polynomials such that p lies in the radical of the ideal $(f_1, \ldots, f_s)$. Let $\mathcal{P}$ be an integral polytope which contains the Newton polytope of $p, f_1, \ldots, f_s$. Let ρ denote its dimension. Assume furthermore that $\mathcal{A}(\mathcal{P})$ is a normal set of integer vectors in $\mathbb{Z}^{n+1}$. Then there exist $D \in \mathbb{N}$, $a \in \mathbb{Z}^n$ and $g_1, \ldots, g_s \in k[x_1, \ldots, x_n, x_1^{-1}, \ldots, x_n^{-1}]$ such that*

$$p^D = g_1 f_1 + \cdots + g_s f_s$$

holds, with $D \leq \rho!\, \min\{n+1, s\}^2 \operatorname{vol}(\mathcal{P})$, $a \in (\rho!\, \min\{n+1, s\} \operatorname{vol}(\mathcal{P}))^2 \mathcal{P}$ and $\mathcal{N}(g_i f_i) \subseteq (\rho!\, \min\{n+1, s\} \operatorname{vol}(\mathcal{P}))^2\ \mathcal{P} - a$ for $i = 1, \ldots, s$.

Proof. As before, we denote by $\mathcal{B} = \{b_0, \ldots, b_N\}$ the set of integer vectors $\mathcal{P} \cap \mathbb{Z}^n$. Assume for the moment that $b_0 = (0, \ldots, 0)$. We consider the morphism

$$\psi : k[y_1, \ldots, y_N] \to k[x_1, \ldots, x_n, x_1^{-1}, \ldots, x_n^{-1}], \qquad y_i \mapsto x^{b_i}.$$

The kernel of this morphism is the defining ideal $I_{\mathcal{B}-b_0}$ of the affine toric variety $X_{\mathcal{B}-b_0}$. Let T denote the torus of this toric variety. Then we have that $X_{\mathcal{B}-b_0}$ equals the intersection of the projective variety $Y_{\mathcal{A}(\mathcal{P})}$ with the affine cart $\{y_0 \neq 0\}$ of $\mathbb{P}^N$, and that T is also the torus of $Y_{\mathcal{A}(\mathcal{P})}$. We recall that this torus equals the open set $\{y_0 \cdots y_N = 0\}$ of $Y_{\mathcal{A}(\mathcal{P})}$.

The map ψ induces a surjection $(\overline{k}^*)^n \to T$. Let $\zeta_1, \ldots, \zeta_s, q$ be elements of degree one in $k[y_1, \ldots, y_N]$ such that $\psi(\zeta_i) = f_i$ for $i = 1, \ldots, s$ and $\psi(q) = p$. Then $\zeta_1, \ldots, \zeta_s$ have no common zero in T outside the hyperplane $\{q = 0\}$.

Let $\eta_1, \ldots, \eta_s, u$ denote the homogenization of $\zeta_1, \ldots, \zeta_s, q$ in $k[y_0, \ldots, y_N]$ respectively. Then the linear forms $\eta_1, \ldots, \eta_s$ have no common zero in $Y_{\mathcal{A}(\mathcal{P})}$ outside the hypersurface $\{y_0 \cdots y_N\, u = 0\}$.

Let $V(\eta_1, \ldots, \eta_s)$ denote the subvariety of $Y_{\mathcal{A}(\mathcal{P})}$ defined by the linear forms $\eta_1, \ldots, \eta_s$. By Bézout's inequality [19], the number of irreducible components of $V(\eta_1, \ldots, \eta_s)$ does not exceed the degree of $Y_{\mathcal{A}(\mathcal{P})}$. Let us denote by δ the degree of $Y_{\mathcal{A}(\mathcal{P})}$, so that $\delta \leq \rho! \operatorname{vol}(\mathcal{P})$ holds. In our situation this implies that $V(\eta_1, \ldots, \eta_s)$ lies in the union of at most δ hyperplanes. These hyperplanes are defined by variables $y_{i_1}, \ldots, y_{i_l}$, and eventually also by the linear form u, depending on whether $\eta_1, \dots, \eta_s$ have a common zero in T in the hyperplane $\{u = 0\}$ or not. Let Π denote the product of these equations, which is a polynomial of degree less or equal that δ.

By assumption the set $\mathcal{A}(\mathcal{P})$ is normal and so $I_{\mathcal{A}(\mathcal{P})}$ is a Cohen–Macaulay prime homogeneous ideal of $k[y_0, \dots, y_N]$. We have also that Π is not a zero–divisor modulo this ideal. Thus we are again in the hypothesis of the Main Lemma 1.1. Let E denote the integer $\min\{n+1, s\}^2 \deg Y_{\mathcal{A}(\mathcal{P})}$. Then there exist homogeneous elements $\alpha_1, \dots, \alpha_s \in k[y_0, \dots, y_N]/I_{\mathcal{A}(\mathcal{P})}$ of degree $(\deg \Pi) \cdot E - 1$ such that

$$\Pi^E = \alpha_1 \eta_1 + \cdots + \alpha_s \eta_s$$

holds. We evaluate $y_0 := 1$ and we apply the map ψ to the preceding identity. We get

$$p^D = g_1 f_1 + \cdots + g_s f_s,$$

where we have set $g_i(x) := (x^{b_{i_1}} \cdots x^{b_{i_l}})^{-1} \alpha_i(1, x^{b_1}, \dots, x^{b_N})$ for $i = 1, \dots, s$ and $D := E$ in the case when u appears as a factor of Π and $D := 1$ in the other case. Then $D \leq \rho! \min\{n+1, s\}^2 \operatorname{vol}(\mathcal{P})$ holds and the polytope $\mathcal{N}(g_i f_i)$ is contained in $(\rho! \operatorname{vol}(\mathcal{P})\, E - 1)\, \mathcal{P} - (b_{i_1} + \cdots + b_{i_l})$ for $i = 1, \dots, s$. We have that $\deg \Pi \leq \deg Y_{\mathcal{A}(\mathcal{P})} \leq \rho! \operatorname{vol}(\mathcal{P})$ and that $i_1 + \ldots + i_k \in \deg Y_{\mathcal{A}(\mathcal{P})}\, \mathcal{P}$.

Now we consider the general case. Let b_0 be any integer vector in $\mathcal{P}$, and let $\mathcal{Q}$ denote the polytope $\mathcal{P} - b_0$. By the previous considerations there exist $D \in \mathbb{N}$, $a_0 \in \mathbb{Z}^n$ and $g_1, \dots, g_s \in k[x_1, \dots, x_n, x_1^{-1}, \dots, x_n^{-1}]$ such that

$$p^D = g_1 f_1 + \cdots + g_s f_s$$

holds, with $D \leq \rho! \min\{n+1, s\}^2 \operatorname{vol}(\mathcal{Q})$, $a_0 \in \rho! \operatorname{vol}(\mathcal{Q})\, \mathcal{Q}$ and $\mathcal{N}(g_i f_i) \subseteq (\rho! \min\{n+1, s\} \operatorname{vol}(\mathcal{Q}))^2\, \mathcal{Q} - a_0$ for $i = 1, \dots, s$.

Let a be the integer vector $a_0 + (\rho! \min\{n+1, s\} \operatorname{vol}(\mathcal{P}))^2\, b_0$. Then a lies in the polytope $(\rho! \min\{n+1, s\} \operatorname{vol}(\mathcal{P}))^2\, \mathcal{P}$ and we have also that $\mathcal{N}(g_i f_i) \subseteq (\rho! \min\{n+1, s\} \operatorname{vol}(\mathcal{P}))^2\, \mathcal{P} - a$ holds for $i = 1, \dots, s$ as stated. □

Let notation be as in Theorem 2.13. Let $\mathcal{N}$ denote the Newton polytope of $p, f_1, \dots, f_s$ and let $\mathcal{U}$ denote the unmixed volume of this polytope. Assume in addition that $n \geq 2$. In this situation we can then take the polytope $\mathcal{P}$ to be $(n-1)\mathcal{N}$. We get the bounds

$$D \leq n^{n+2}\, \mathcal{U}, \qquad \mathcal{N}(g_i f_i) \subseteq (n^{2n+3}\, \mathcal{U})\, \mathcal{N} - a.$$

for some $a \in (n^{2n+3}\, \mathcal{U})\, \mathcal{N}$. As before, it is easy to verify that the same bounds hold also when $n = 1$. Thus Theorem follows from this observation in the particular case $p = 1$.

Let $q = f/g \in k(x_1, \dots, x_n)$ be a rational function given as the quotient of two polynomials without common factors. Then the *degree* of q is defined as $\deg q := \max\{\deg f, \deg g\}$.

We derive from Theorem 2.13 the following degree bound.

Corollary 2.14 *Let notation be as in Theorem 2.13 and $d := \max_i \deg f_i$. Then there exist $D \in \mathbb{N}$ and $g_1, \dots, g_s \in k[x_1, \dots, x_n, x_1^{-1}, \dots, x_n^{-1}]$ such that*

$$p^D = g_1 f_1 + \cdots + g_s f_s$$

holds, with $D \leq \rho! \min\{n+1, s\}^2 \operatorname{vol}(\mathcal{P})$, $a \in (\rho! \min\{n+1, s\} \operatorname{vol}(\mathcal{P}))^2 \mathcal{P}$ and $\deg(g_i f_i) \leq d\, ((1 + \deg p) \rho! \min\{n+1, s\} \operatorname{vol}(\mathcal{P}))^2$ for $i = 1, \dots, s$.

□

3. Improved Bounds for the Degrees in the Nullstellensatz

In this section we consider the degree bounds in the Nullstellensatz. We shall apply the methods used in Section 1 in a direct way — without any reference to the Veronese map — in the setting of the classic effective Nullstellensatz. The proof follows closely the same lines and so we shall skip some verifications in order to avoid unnecessary repetitions.

Assume that we are given homogeneous polynomials $f_1, \ldots, f_s$ in $k[x_0, \ldots, x_n]$ without common zeros in the hyperplane $\{x_0 = 0\}$. In this situation we are going to give a bound for the minimal $D \in \mathbb{N}$ such that $x_0^D \in (f_1, \ldots, f_s)$.

We shall assume without loss of generality that $s \leq n+1$ and that $\overline{f}_1, \ldots, \overline{f}_s$ is a weak regular sequence in $k[x_0, \ldots, x_n]_{x_0}$. Let $d_i := \deg f_i$, and we suppose that $d_2 \geq \cdots \geq d_s$ and that $d_s \geq d_1$ hold. As before these polynomials can be obtained as linear combinations of the original polynomials, eventually multiplied by powers of x_0.

Let us denote by J_i the contraction to the ring S of the ideal $(\overline{f}_1, \ldots, \overline{f}_i) \subseteq S_{x_0}$ for $i = 1, \ldots, s$. We make the convention $J_0 := (0)$.

Lemma 3.15 *Following the preceding notation, there exist homogeneous polynomials $h_1, \ldots, h_s \in k[x_0, \ldots, x_n]$ satisfying the following conditions:*

i) $h_i \equiv x_0^{c_i} f_i \mod J_{i-1}$ *for some* $c_i \in \mathbb{N}$,

ii) $h_1, \ldots, h_s$ *is a regular sequence,*

iii) $\deg h_i \leq \max\{\deg J_{i-1}, \deg f_i\}$,

for $i = 1, \ldots, s$.

□

We introduce the following notation. Let δ_i denote the degree of the homogeneous ideal J_i for $i = 0, \ldots, s$. We recall the Bézout bound $\delta_i \leq \prod_{j=1}^{i} d_j$. Then let $\gamma_i = d_i\, \delta_{i-1} - \delta_i$ for $i = 1, \ldots, \min\{n, s\}$ and $\gamma_{n+1} := \delta_n + d_{n+1} - 1$. We also let $\delta := \max\{\delta_i : i = 1, \ldots, s-1\}$ and $d := \max\{d_i : i = 1, \ldots, s-1\}$. For an ideal I of S we denote by I^u its unmixed part.

Lemma 3.16 *Let $q \in J_i$ for some $1 \leq i \leq s$. Then $x_0^{\gamma_i}\, q \in (J_{i-1}, \eta_i)^u$.*

Proof. The case $i \leq n$ is exactly as in Lemma 1.4. Thus we only consider the case $i = n+1$.

The ideal J_n is has dimension one and its degree is δ_n. Then $(J_n, f_{n+1})_m = S_m$ for $m \geq \delta_n + d_{n+1} - 1$ as f_{n+1} is not a zero–divisor modulo J_n [33, Theorem 2.23]. It follows that $x_0^{\gamma_{n+1}} \in (J_n, f_{n+1})$ and in particular $x_0^{\gamma_{n+1}}\, q \in (J_n, f_{n+1})^u$. □

Now let $h_1, \ldots, h_s$ be the homogeneous polynomials introduced in Lemma 3.15. We set $\mu_i := \sum_{j=2}^{i} ((i-j+1)\, \gamma_j + (i-j)\, c_j)$ for $i = 1, \ldots, \min\{n, s\}$ and $\mu_{n+1} := \mu_n + \gamma_{n+1}$, where c_i denotes the integer $\deg h_i - \deg f_i$.

We denote by L_i the homogeneous ideal $(f_1, \ldots, f_i)$ for $i = 1, \ldots, s$.

Lemma 3.17 *Let $q \in J_i$ for some $1 \le i \le s$. Then $x_0^{\mu_i} q \in L_i$.*

Proof. The case $i \le n$ is exactly as in Lemma 1.6. Thus we only consider the case $i = n+1$.

By the previous lemma $x_0^{\gamma_{n+1}}\, q \in (J_n, f_{n+1})^u = (J_n, f_{n+1})$ and so $x_0^{\gamma_{n+1}}\, q - u\, f_{n+1} \in J_n$ for some polynomial $u \in S$. We apply then the inductive hypothesis and we obtain that $x_0^{\mu_n}\, (x_0^{\gamma_{n+1}}\, q - u\, f_{n+1}) \in L_n$ from which it follows that $x_0^{\mu_{n+1}}\, q \in L_{n+1}$. $\square$

Thus it only remains to bound μ_s. We shall be concerned with two different types of bounds. One depends as usual on the number of variables and on the degrees of the input polynomials, and the other depends also on the degree of some ideals associated to these polynomials.

Lemma 3.18 *Let notation be as before. Then $\mu_s \le \min\{n, s\}^2\, d\, \delta$. In case $\deg f_i \ge 2$ for $i = 1, \ldots, s$ we have that $\mu_s \le 2 \prod_{j=1}^{\min\{n,s\}} d_j$.*

Proof. We decompose the integer μ_s in two terms and we estimate them separately. First we consider the term $\sum_{j=2}^{s} (s-j)\, c_j$. We have that $c_i \le \max\{\delta_{i-1} - d_i, 0\}$. In particular $c_2 = 0$ as $\delta_1 = d_1$ and $d_1 \le d_2$. Then

$$\begin{aligned}
\textstyle\sum_{j=2}^{s} (s-j)\, c_j &\le \textstyle\sum_{j=3}^{s-1} (s-j)\, (d_1 \cdots d_{j-1} - d_j) \\
&\le \textstyle(\sum_{j=3}^{s-1} (s-j)/d_j \cdots d_{s-2})\, d_1 \cdots d_{s-2} - \sum_{j=2}^{s-1} (s-j)\, d_j \\
&\le 4\, d_1 \cdots d_{s-2} - d_{s-1},
\end{aligned}$$

under the assumption $d_i \ge 2$ for $i = 1, \ldots, s$. We have also $\sum_{j=2}^{s-1} (s-j)\, c_j \le \sum_{j=2}^{s-1} (s-j)\, \delta = \frac{1}{2}\, (s-2)(s-1)\, \delta$.

Now we estimate the other term. We consider first the case $s \le n$. Then

$$\begin{aligned}
\textstyle\sum_{j=2}^{s} (s-j+1)\, \gamma_j &= \textstyle\sum_{j=2}^{s} (s-j+1)\, (d_j\, \delta_{j-1} - \delta_j) \\
&= \textstyle(s-1)\, d_2\, \delta_1 + \sum_{j=3}^{s} ((s-j+1)\, d_j - (s-j))\, \delta_{j-1} - \delta_n \\
&\le d_1 \cdots d_s - \delta_s,
\end{aligned}$$

from which we obtain the bound $\mu_s = \sum_{j=2}^{s} (s-j+1)\, \gamma_j + \sum_{j=2}^{s-1} (s-j)\, c_j \le (d_1 \cdots d_s - \delta_s) + (4\, d_1 \cdots d_{s-2} - d_{s-1}) \le 2\, d_1 \cdots d_s$. In the case $s = n+1$ we have that $\mu_{n+1} = \mu_n + \gamma_{n+1}$ which implies that $\mu_{n+1} \le (2\, d_1 \cdots d_n - \delta_n - d_{n-1}) + (\delta_n + d_{n+1} - 1) \le 2\, d_1 \cdots d_n$. On the other hand we have also the estimate $\sum_{j=2}^{s} (s-j+1)\, \gamma_j \le \frac{1}{2}\, (s-1)\, s\, d\, \delta$ from where we conclude that $\mu_s \le \frac{1}{2}\, (s-1)\, s\, d\, \delta + \frac{1}{2}\, (s-2)\, (s-1)\, \delta \le (s-1)^2\, d\, \delta$ holds, as stated. $\square$

Theorem 3.19 *Let $f_1, \ldots, f_s \in k[x_0, \ldots, x_n]$ be homogeneous polynomials such that x_0 lies in the radical of the ideal $(f_1, \ldots, f_s)$. Let $d_i := \deg f_i$ for $i = 1, \ldots, s$ and assume that $d_1 \ge \cdots \ge d_s$ holds. Then*

$$x_0^D \in (f_1, \ldots, f_s)$$

holds, with $D := 2\, d_s \prod_{i=1}^{\min\{n,s\}-1} d_i$.

Proof. After Lemmas 3.17 and 3.18 it only remains to consider the case when some f_i has degree one.

By assumption $f_1, \ldots, f_s$ are ordered in such a way that $d_1 \geq \cdots \geq d_s$ holds. Let r be maximum such that $d_r \geq 2$, so that the polynomials $f_{r+1}, \ldots, f_s$ have all degree one. We can assume without loss of generality that they are k–linearly independent. We can also suppose that neither 1 nor x_0 lie in the k–linear space spanned by $f_{r+1}, \ldots, f_s$ as if this is the case the statement is trivial.

Let $y_0, \ldots, y_{n+r-s-1} \in S$ be polynomials of degree one which complete $f_{r+1}, \ldots, f_s$ to a linear change of variables. We suppose in addition that $y_0 = x_0$. Then the natural inclusion $k[y_0, \ldots, y_{n+r-s-1}] \hookrightarrow k[x_0, \ldots, x_n]/(f_{r+1}, \ldots, f_s)$ is an isomorphism. Let v_i be an homogeneous polynomial in $k[y_0, \ldots, y_{n+r-s-1}]$ such that $v_i \equiv f_i \mod (f_{r+1}, \ldots, f_s)$ for $i = 1, \ldots, r$. Then x_0 lies in the radical of the ideal $(v_1, \ldots, v_r)$ of $k[y_0, \ldots, y_{n+r-s-1}]$ and $\deg v_i \leq d_i$ holds for $i = 1, \ldots, r$.

Let E denote the integer $2 \prod_{i=1}^{r} \deg v_i$ so that $E \leq D := 2\, d_s \prod_{i=1}^{\min\{n,s\}-1} d_i$. Then $x_0^D \in (v_1, \ldots, v_r)$ from where it follows that $x_0^D \in (f_1, \ldots, f_s)$ as stated. □

Then the degree bound announced in the Introduction follows from this result by homogenizing the input polynomials and by considering the degree of the polynomials in a representation of x_0^D.

Now we are going to prove Theorem . We introduce the notion of algebraic degree of a polynomial system.

Let $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$ be polynomials without common zeros in $\mathbb{A}^n$. Let $\lambda = (\lambda_{ij})_{ij} \in \overline{k}^{s \times s}$ be an arbitrary $s \times s$ matrix with entries in $\overline{k}$. We note by $h_i(\lambda)$ the linear combinations $\sum_j \lambda_{ij} f_j$ induced by the matrix λ for $i = 1, \ldots, s$.

Consider the set Γ of $s \times s$ matrices such that for any λ in Γ the polynomials $h_1(\lambda), \ldots, h_{t-1}(\lambda)$ form a regular sequence in $\overline{k}[x_1, \ldots, x_n]$ and $1 \in (h_1(\lambda), \ldots, h_t(\lambda))$ for some $t = t(\lambda) \leq \min\{n, s\}$. This set is nonempty, and in fact it contains a nonempty open set of $\overline{k}^{s \times s}$.

For each $\lambda \in \Gamma$ and $i = 1, \ldots, t-1$ we denote by $J_i(\lambda) \subseteq k[x_0, \ldots, x_n]$ the homogenization of the ideal $(h_1(\lambda), \ldots, h_i(\lambda))$. Then let $\delta(\lambda)$ denote the maximum degree of the homogeneous ideal $J_i(\lambda)$ for $i = 1, \ldots, t-1$.

The *algebraic degree* of the polynomial system $f_1, \ldots, f_s$ is defined as

$$\delta(f_1, \ldots, f_s) := \min\{\delta(\lambda) : \lambda \in \Gamma\}.$$

The notion of geometric degree of [23] and [33] is defined in an analogous way as the minimum of $\delta(\lambda)$ for $\lambda \in \Gamma$, with the additional hypothesis in the definition of Γ that the ideals $J_i(\lambda)$ are radical for $i = 1, \ldots, t-1$. Another difference is that in the case when the characteristic of k is positive the polynomials $h_j(\lambda)$ are taken as linear combinations of the polynomials $\{x_j\, f_i\}_{ij}$.

The notion of geometric degree of [16] is similar to that of [23], [33], the only difference is that it is not defined as a minimum but as the value of $\delta(\lambda)$ for a generic choice of λ.

Thus the algebraic degree is bounded by the geometric degree, whichever version of the later one we consider. The following example shows that in fact it can be much smaller. It is a variant of [23, Example 3].

Example 3.20 Let us consider the polynomial system

$$f_1 := 1 - x_1 x_2^d,\ f_2 := x_2 - x_3^d,\ \ldots,\ f_{n-1} := x_{n-1} - x_n^d,\ f_n := x_n^2$$

for some $d \geq 2$. It is easy to check that these polynomials have no common zero in $\mathbb{A}^n$. We are going to compute both the geometric degree δ_g — in the sense of [23], [33] — and the algebraic degree δ_a for this particular example. We obtain $\delta_g = d^{n-1}$ and $\delta_a = 2$ and thus we show that δ_a can be much smaller than δ_g in some particular instances.

First we consider the geometric degree. The polynomials $f_1, \ldots, f_n$ form a weak regular sequence, $1 \in (f_1, \ldots, f_n)$ and the ideal $(f_1, \ldots, f_i)$ is radical for $i = 1, \ldots, n-1$. Then $\deg V(f_1, \ldots, f_i) = d^i$ for $i = 1, \ldots, n-1$, from where it follows $\delta_g \leq d^{n-1}$.

Let $h_i := \sum_j \lambda_{ij} f_j$ be $\overline{k}$–linear combinations of $f_1, \ldots, f_n$ for $i = 1, \ldots, l$. Assume that $1 \in (h_1, \ldots, h_n)$ and that $(h_1, \ldots, h_i)$ is a radical ideal of dimension $n-i$ for $i = 1, \ldots, l-1$. We are going to show that $l = n$ and that $\deg V(h_1, \ldots, h_{n-1}) \geq d^{n-1}$.

We can assume without loss of generality that the linear combinations h_i are in staircase form in the sense of linear algebra. By this we mean $h_i = f_{n(i)} + \sum_{j>n(i)} a_{ij} f_j$ with $n(1) < \cdots < n(l)$. For our particular polynomial system, this allows us to eliminate the variables $x_{n(1)}, \ldots, x_{n(l)}$ into the equations $h_1, \ldots, h_l$, as each variable x_i does not appear in f_j for $j > i$. Thus when $l \leq n-1$ the variety defined by $h_1, \ldots, h_l$ can be parametrized by expressing these variables as rational functions of the other ones. It follows that $(h_1, \ldots, h_l)$ has dimension at least $n - l$. We deduce that $l = n$ and that $(h_1, \ldots, h_{n-1})$ is a radical ideal of dimension one.

Next suppose first that $h_1, \ldots h_{n-1}$ are invertible linear combinations of $f_1, \cdots, \hat{f}_i, \ldots, f_n$ for some $1 \leq i \leq n-1$. Then $(h_1, \ldots h_{n-1}) = (f_1, \ldots, \hat{f}_i, \ldots, f_n)$ which is not radical, and thus contradicting our assumptions. Then $h_i = f_i + a_i f_n$ for some $a_i \in \overline{k}$, if we assume again that the linear combinations $h_1, \ldots, h_{n-1}$ are in reduced form. We deduce that the curve $V(h_1, \ldots, h_{n-1})$ is parametrized by a rational map $t \mapsto \varphi(t) = (\varphi_1(t), \ldots, \varphi_n(t))$, where $\varphi_i \in \overline{k}(t)$ is a rational function of degree d^{n-i} for $i = 1, \ldots, n$. We get that $\deg V(h_1, \ldots, h_{n-1}) = d^{n-1}$ from where we deduce the lower bound $\delta_g \geq d^{n-1}$. Combining this with the previous estimate we conclude $\delta_g = d^{n-1}$.

Now we consider the algebraic degree. The polynomials $f_n, \ldots, f_1$ form a weak regular sequence and $1 \in (f_n, \ldots, f_1)$. We have that $(f_n, \ldots, f_{n-i+1}) = (x_n^2, x_{n-1}, \ldots, x_{n-i+1})$ for $i = 1, \ldots, n$ from where it follows that $\delta_a \leq 2$. In addition, any nontrivial linear combination h of $f_1, \ldots, f_n$ has degree at least two and so $\delta_a \geq \deg h \geq 2$. We conclude that $\delta_a = 2$.

We obtain the following degree bound by direct application of Lemmas 3.17 and 3.18.

Theorem 3.21 *Let $f_1, \ldots, f_s \in k[x_0, \ldots, x_n]$ be homogeneous polynomials such that x_0 lies in the radical of the ideal $(f_1, \ldots, f_s)$. Let f_i^a denote the affinization of f_i for $i = 1, \ldots, s$. Let $d := \max_i \deg f_i$ and let δ denote the degree of the polynomial system $f_1^a, \ldots, f_s^a$. Then*

$$x_0^D \in (f_1, \ldots, f_s)$$

holds, with $D := \min\{n, s\}^2\, d\, \delta$.

□

Then Theorem follows from this result in the same way we derived the previous degree bound from Theorem 3.19

If we apply this degree bound to the previous example we obtain that there exist $g_1, \dots, g_n \in k[x_1, \dots, x_n]$ satisfying

$$1 = g_1 f_1 + \cdots + g_n f_n,$$

with $\deg g_i f_i \le 2\, n^2\, d$ for $i = 1, \dots, s$. In fact we have the identity

$$1 = f_1 + x_1\, x_2^{d-1}\, f_2 + x_1\, x_2^{d-1}\, x_3^{d-1}\, f_3 + \cdots + x_1\, x_2^{d-1} \cdots x_{n-1}^{d-1}\, x_n^{d-2}\, f_n$$

Acknowledgements. This work originated in several conversations with Bernd Sturmfels. He motivated me to think about the sparse Nullstellensatz and suggested me several lines to approach it. Special thanks are due to him. I am also grateful to Alicia Dickenstein and Joos Heintz for helpful discussions and suggestions, and to Pablo Solernó for providing me a counterexample to a conjecture in an early version of this paper. I also thank the referees for helpful suggestions, in particular Example 2.12.

I thank the Departments of Mathematics of the Universities of Alcalá and of Cantabria, Spain, where part of this paper was written during a stay in the spring of 1997.

References

[1] M. S. Almeida, *Función de Hilbert de álgebras graduadas y Nullstellensatz afín efectivo*, Tesis de Licenciatura, Univ. Buenos Aires, 1995.

[2] F. Amoroso, *On a conjecture of C. Berenstein and A. Yger*, in L. González–Vega and T. Recio, eds., Algorithms in algebraic geometry and applications, Proceedings MEGA'94, Birkhäuser Progress in Math. **143**, Bikhäuser, Basel, 1996, pp. 17–28.

[3] C. A. Berenstein, D. C. Struppa, *Recent improvements in the complexity of the effective Nullstellensatz,* Linear Alg. Appl. **157** (1991), pp. 203–215.

[4] C. A. Berenstein, A. Yger, *Effective Bézout identities in* $\mathbb{Q}[x_1, \dots, x_n]$, Acta Math. **166** (1991), pp. 69–120.

[5] D. N. Bernshtein, *The number of roots of a system of equations,* Funcional Analysis and its Applications **9** (1975), pp. 183–185 (translated from Russian).

[6] W. D. Brownawell, *Bounds for the degrees in the Nullstellensatz,* Ann. of Math. **126** (1987), pp. 577–591.

[7] W. D. Brownawell, D. W. Masser, *Multiplicity estimates for analytic functions II,* Duke J. Math. **47** (1980), pp. 273–295.

[8] L. Caniglia, A. Galligo, J. Heintz, *Some new effectivity bounds in computational geometry,* in T. Mora, ed, Proceedings AAECC–6, Lect. Notes in Comput. Sci. 357, Springer, Berlin, 1989, pp. 131–151.

[9] J. Canny, I. Emiris, *A subdivision–based algorithm for the sparse resultant,* Preprint, 1996.

[10] V. I. Danilov, *The geometry of toric varieties,* Russian Math. Surveys **33** (1978), pp. 97–154.

[11] T. W. Dubé, *A combinatorial proof of the effective Nullestellensatz,* J. Symb. Comp. **15** (1993), pp. 277–296.

[12] G. Ewald, U. Wessels, *On the ampleness of invertible sheaves in complete toric varieties,* Results Math. **25** (1991), pp. 275–278.

[13] N. Fitchas, A. Galligo, *Nullstellensatz effectif et conjecture de Sèrre (théorème de Quillen–Suslin) pour le Calcul Formel,* Math. Nachr. **149** (1990), pp. 231–253.

[14] W. Fulton, *Introduction to toric varieties,* Ann. Math. Studies **131**, Princeton Univ. Press, 1993.

[15] M. Giusti, K. Hägele, J. Heintz, J. L. Montaña, J. E. Morais, L. M. Pardo, *Lower bounds for diophantine approximation,* J. Pure Appl. Algebra **117 & 118** (1997), pp. 277–317.

[16] M. Giusti, J. Heintz, J. E. Morais, J. Morgenstern, L. M. Pardo, *Straight–line programs in geometric elimination theory,* J. Pure Appl. Algebra **124** (1998), pp. 101–146.

[17] K. Hägele, J. E. Morais, L. M. Pardo, M. Sombra, *On the intrinsic complexity of the arithmetic Nullstellensatz,* Preprint, 1997.

[18] J. Harris, *Algebraic geometry: a first course,* Graduate Texts in Math. 133, Springer, Berlin, 1992.

[19] J. Heintz, *Definability and fast quantifier elimination in algebraically closed fields,* Theoret. Comput. Sci. **24** (1983), pp. 239-277.

[20] B. Huber, B. Sturmfels, *A polyhedral method for solving sparse polynomial systems,* Math. Comp. **64** (1995), pp. 1541–1555.

[21] J. Kollár, *Sharp effective Nullstellensatz,* J. Amer. Math. Soc. **1** (1988), pp. 963–975.

[22] T. Krick, L. M. Pardo, *A computational method for diophantine approximation,* in L. González–Vega and T. Recio, eds., Algorithms in algebraic geometry and applications, Proceedings MEGA'94, Birkäuser Progress in Math. **143**, Bikhäuser, Basel, 1996, pp. 193–253.

[23] T. Krick, J. Sabia, P. Solernó, *On intrinsic bounds in the Nullstellensatz,* AAECC Journal **8** (1997), pp. 125–134.

[24] A. G. Kushnirenko, *Newton polytopes and the Bézout theorem,* Functional Analysis and its Applications **10** (1976), pp. 82–83 (translated from Russian).

[25] H. Matsumura, *Commutative ring theory,* Cambridge Univ. Press, 1986.

[26] L. M. Pardo, *How upper and lower bounds meet in elimination theory,* in G. Cohen, M. Giusti and T. Mora, eds., Proceedings AAECC–11, Lect. Notes. Comput. Sci. **948**, pp. 33–69, Springer, Berlin, 1995.

[27] P. Philippon, *Dénominateurs dans le théorème des zeros de Hilbert,* Acta Arith. **58** (1990), pp. 1–25.

[28] J. M. Rojas, *Toric generalized characteristic polynomials,* Preprint, 1997.

[29] J. M. Rojas, *Toric laminations, sparse generalized characteristic polynomials, and a refinement of Hilbert's tenth problem,* in F. Cucker and M. Shub, eds., Foundations of Computational Mathematics, Springer–Verlag, 1997.

[30] J. Sabia, P. Solernó, *Bounds for traces in complete intersections and degrees in the Nullstellensatz,* AAECC Journal **6** (1995), pp. 353–376.

[31] B. Shiffman, *Degree bounds for the division problem in polynomial ideals,* Michigan Math. J. **36** (1989), pp. 163–171.

[32] F. Smietanski, *Quelques bornes effectives pour le théoreme des zeros avec parametres,* These, Univ. Nice–Sophia Antipolis, 1994.

[33] M. Sombra, *Bounds for the Hilbert function of polynomial ideals and for the degrees in the Nullstellensatz,* J. Pure Appl. Algebra **117 & 118** (1997), pp. 565–599.

[34] B. Sturmfels, *Sparse elimination theory,* in D. Eisenbud and L. Robbiano, eds., Proceedings of the Cortona conference on computational algebraic geometry and commutative algebra, Symposia Matematica XXXIV, Ist. Naz. di Alta Matematica, Cambridge Univ. Press, 1993, pp. 377–396.

[35] B. Sturmfels, *Gröbner bases and convex polytopes,* Univ. Lect. Series **8**, Amer. Math. Soc., 1996.

[36] B. Teissier, *Résultats récents d'algèbre commutative effective,* Sém. Bourbaki 718, Astérisque 189–190, pp. 107–131, Soc. Math. France, 1991.

[37] J. Verschelde, P. Verlinden, R. Cools, *Homotopies exploiting Newton polytopes for solving sparse polynomial systems,* SIAM J. Numer. Anal. **31** (1994), pp. 915–930.

[38] W. Vogel, *Lectures on results on Bézout theorem,* Tata Lect. Notes **74**, Springer, Berlin, 1984.

[39] O. Zariski, P. Samuel, *Commutative algebra, 2 vols.,* Van Nostrand, New York, 1958, 1960.