Degree Bounds for Gröbner Bases of Low-Dimensional Polynomial Ideals

Ernst W. Mayr
Technische Universität München
Boltzmannstr. 3
D-85748 Garching
mayr@in.tum.de

Stephan Ritscher
Technische Universität München
Boltzmannstr. 3
D-85748 Garching
ritsches@in.tum.de

ABSTRACT

Let $\mathbb{K}[X]$ be a ring of multivariate polynomials with coefficients in a field $\mathbb{K}$, and let $f_1, \dots, f_s$ be polynomials with maximal total degree d which generate an ideal I of dimension r. Then, for every admissible ordering, the total degree of polynomials in a Gröbner basis for I is bounded by $2\left(\frac{1}{2}d^{n-r} + d\right)^{2^r}$. This is proved using the cone decompositions introduced by Dubé in [5]. Also, a lower bound of similar form is given.

Categories and Subject Descriptors

I.1.1 [**Symbolic and Algebraic Manipulation**]: Expressions and Their Representation—*Representations (general and polynomial)*; G.2.1 [**Dicrete Mathematics**]: Combinatorics—*Counting problems*

General Terms

Theory

Keywords

multivariate polynomial, Gröbner basis, polynomial ideal, ideal dimension, complexity

1. INTRODUCTION

Gröbner bases are a very powerful tool in computer algebra which was introduced by Buchberger [2]. Many problems that can be formulated in the language of polynomials can be easily solved once a Gröbner basis has been computed. This is because Gröbner bases allow quick ideal consistency checks, ideal membership tests, and ideal equality tests, among others.

Unfortunately, the computation of a Gröbner basis can be very expensive. The problem is exponential space complete, which was shown in [13] and [11]. Interestingly, both the upper and the lower bound are obtained by considering polynomials of high degree in the ideal. So knowing good bounds for the degrees of polynomials in the Gröbner basis means also knowing the complexity of its calculation.

In [13] and [14] it was shown that, in the worst case, the degree of polynomials in a Gröbner basis is at least doubly exponential in the number of indeterminates of the polynomial ring. [1], [7], and [14] provide a doubly exponential upper degree bound as explained in the introduction of [5]. [5] gives a combinatorial proof of an improved upper bound.

For zero-dimensional ideals, the bounds are smaller by a magnitude. The well-known theorem of Bézout (cf. [16]) immediately implies a singly exponential upper degree bound. For graded monomial orderings the degrees are even bounded polynomially, as proved in [12]. Both bounds are exact, and the examples providing lower bounds are folklore (cf. [14]).

This suggests that also ideals with small non-zero dimension permit better degree bounds than in the general case. Furthermore, in [9] an ideal membership test was provided with space complexity exponential only in the dimension of the ideal. This result anticipated a degree bound of the form shown in this paper.

The remainder of the paper is organized as follows. In the second section notation for polynomial ideals and Gröbner bases will be fixed. We do not give proofs or comprehensive explanations. For a detailed introduction and accompanying proofs we refer to the literature. The third chapter contains the main result of this paper, the upper degree bound depending on the ideal dimension. Since the proof uses cone decompositions as defined by Dubé in [5], we first review these techniques. Then we explain how to adapt this approach to get a dependency on the ideal dimension and derive the upper degree bound. Finally we demonstrate how to use the results from [13] and [14] to obtain a lower bound of similar form.

Credits

We wish to thank the referees for their detailed feedback. Particular thanks are due to one of them for showing how to tighten our bound.

2. NOTATION

In this chapter, we define the notation that will be used throughout the paper. For a more detailed introduction to polynomial algebra, the reader may consult [3] and [4].

2.1 Polynomial Ideals

Consider the ring $\mathbb{K}[X]$ of polynomials in the variables $X = \{x_1, \dots, x_n\}$. The *(total) degree* of a monomial is $\deg(x_1^{e_1} \cdots x_n^{e_n}) = e_1 + \dots + e_n$. A polynomial is called

ISSAC 2010, 25–28 July 2010, Munich, Germany.

homogeneous if all its monomials have the same degree. Every polynomial $f \neq 0$ permits a unique representation $f = f_0 + \ldots + f_d$, $f_d \neq 0$, with f_k being homogeneous of degree k, the so-called *homogeneous components* of f. The *homogenization* of f with respect to a new variable x_{n+1} is defined by ${}^h f = x_{n+1}^d f_0 + x_{n+1}^{d-1} f_1 + \ldots + f_d$. A set $S \subset \mathbb{K}[X]$ is called *homogeneous* if for every polynomial $f \in S$ also its homogeneous components f_k are elements of S.

Throughout the paper we assume some arbitrary but fixed *admissible* monomial ordering (cf. [5], §2.1). Therefore we won't keep track of it in the notation. The largest monomial occuring in a polynomial f is called *leading monomial* and denoted by $\mathrm{LM}(f)$.

$\langle f_1, \ldots, f_s \rangle$ denotes the *ideal* $\{\sum_{i=1}^s a_i f_i : a_i \in \mathbb{K}[X]\}$ generated by $F = \{f_1, \ldots, f_s\}$. G is a *Gröbner basis* of the ideal I if $\langle G \rangle = I$ and $\langle \mathrm{LM}(G) \rangle = \langle \mathrm{LM}(I) \rangle$.

$\mathrm{nf}_I(f)$ denotes the *normal form* of f, which, for a fixed monomial ordering, is the unique irreducible polynomial fulfilling $\mathrm{nf}_I(f) \equiv f \mod I$. The set of all normal forms is denoted by N_I. Since the normal forms are unique, we have the direct sum $\mathbb{K}[X] = I \oplus N_I$. For details see [5], §2.1.

Unless stated differently, we will consider an ideal I generated by homogeneous polynomials $f_1, \ldots, f_s$ with degrees $d_1 \geq \ldots \geq d_s$.

2.2 Hilbert Functions

Let $T \subset \mathbb{K}[X]$ be homogeneous and $T_z = \{f \in T : f$ homogeneous with $\deg(f) = z$ or $f = 0\}$ the homogeneous polynomials of T of degree z. Then the *Hilbert function* of T is defined as

$$\varphi_T(z) = \dim_{\mathbb{K}}(T_z),$$

i.e. the vector space dimension of T_z over the field $\mathbb{K}$. It easily follows from the dimension theorem for direct sums that

$$\varphi_{S \oplus T}(z) = \varphi_S(z) + \varphi_T(z).$$

It is well-known that, for large values of z, the Hilbert functions $\varphi_I(z)$ and $\varphi_{N_I}(z)$ of a homogeneous ideal I and its normal forms N_I are polynomials. These polynomials, known as *Hilbert polynomials*, will be denoted by $\overline{\varphi}_I(z)$ and $\overline{\varphi}_{N_I}(z)$, respectively.

2.3 Ideal Dimension

The *dimension* of an homogeneous ideal can be defined in many equivalent ways (cf. [3], §9). The following definition turns out to be the most suitable for our purpose.

$$\dim(I) = \deg(\overline{\varphi}_{N_I}) + 1$$

with $\deg(0) = -1$. We add 1 to the degree in order to obtain the affine instead of the projective dimension. This simplifies the presentation which is inherently affine.

Since we will have to deal with ideal dimensions and vector space dimensions, we will write $\dim(I)$ for the former and $\dim_{\mathbb{K}}(I)$ for the latter in order to avoid confusion.

2.4 Regular Sequences

A sequence $(g_1, \ldots, g_t)$ with $g_k \in \mathbb{K}[X]$ is called *regular sequence* (cf. [6]) if

- g_k is a nonzerodivisor in $\mathbb{K}[X]/\langle g_1, \ldots, g_{k-1} \rangle$, for all $1 \leq k \leq t$, and
- $\mathbb{K}[X] \neq \langle g_1, \ldots, g_t \rangle$.

A nice, well-known property of regular sequences is that their Hilbert polynomial only depends on the degrees of the polynomials and the number of indeterminates.

Proposition 2.1. *Let $(g_1, \ldots, g_t)$ with $g_k \in \mathbb{K}[X]$ be a homogeneous regular sequence with degrees $d_1 \geq \ldots \geq d_t$ and $J = \langle g_1, \ldots, g_t \rangle$. Then $N_J \cong \mathbb{K}[X]/J$ have (for any term ordering) a Hilbert function which only depends on n, t, and $d_1, \ldots, d_t$. The Hilbert function and the Hilbert polynomial are equal for $z > d_1 + \ldots + d_t - n$.*

Proof. See [10], §5.2B and §5.4B. $\square$

We are given now an ideal I of dimension r and want to embed a regular sequence which is as long as possible. It turns out that the length of this sequence is always $n - r$.

Proposition 2.2 (cf. Schmid 1995). *Let $\mathbb{K}$ be an infinite field and $I \subsetneq \mathbb{K}[X]$ an ideal generated by homogeneous polynomials $f_1, \ldots, f_s$ with degrees $d_1 \geq \ldots \geq d_s$ and $\dim(I) \leq r$. Then there are a permutation σ of $\{1, \ldots, s\}$ and homogeneous $a_{k,i} \in \mathbb{K}[X]$ such that*

$$g_k = \sum_{i=\sigma(k)}^{s} a_{k,i} f_i$$

for $k = 1, \ldots, n-r$ form a regular sequence of homogeneous polynomials, and $\deg(g_k) = d_{\sigma(k)}$.

Proof. See [15], Lemma 2.2. It's an extension to the homogeneous case. Since in the ring $\mathbb{K}[X]$ any permutation of a regular sequence is regular, one can choose $\sigma = \mathrm{id}$. $\square$

3. UPPER DEGREE BOUND

3.1 Cone Decompositions

The upper degree bound presented in this paper is based on the concept of cone decompositions introduced in [5]. This section will summarize the results that will be used leaving out the proofs which can be found in the original paper [5].

For a homogeneous polynomial h and a set of variables $U \subset X$, the corresponding *cone* is denoted by $C = C(h, U) = h\mathbb{K}[U]$. For succinctness, by the *degree* of a cone C we mean the degree of its apex, i.e., $\deg(C) = \deg(h)$. Similarly, we call the cardinality of U the *dimension* of the cone, i.e. $\dim(C) = \#U$. Note that h and U are uniquely determined by C as a set. Since we will not describe algorithms as in [5], we don't need to talk about pairs of h and U as a representation of the cone.

One of the most important reasons for working with cones is that their Hilbert functions can be easily calculated. For a cone C of dimension 0, we have

$$\varphi_C(z) = \begin{cases} 0 & \text{for } z \neq \deg(C) \\ 1 & \text{for } z = \deg(C) \end{cases},$$

for cones of dimension greater than zero

$$\varphi_C(z) = \begin{cases} 0 & \text{for } z < \deg(C) \\ \binom{z - \deg(C) + \dim(C) - 1}{\dim(C) - 1} & \text{for } z \geq \deg(C) \end{cases}.$$

Since we can handle the Hilbert functions of direct sums, we want to express the spaces we deal with as direct sums of cones.

Definition 3.1 (Dubé 1990). *Let T be a vector space and $T = \bigoplus_{i=1}^{l} C_i$ a direct decomposition into cones C_i. Then we call $P = \{C_i : i = 1, \ldots, l\}$ a* cone decomposition *of T. We will use the notation $\deg(P) = \max\{\deg(C) : C \in P\}$.*

Obviously

$$\overline{\varphi}_T(z) = \sum_{C \in P} \overline{\varphi}_C(z).$$

In a slight abuse of notation we also write $\varphi_P(z)$ for $\varphi_T(z)$ (respectively $\overline{\varphi}_P(z)$ for $\overline{\varphi}_T(z)$) if P is a cone decomposition of T. Our final interest will not be the Hilbert function of a cone decomposition but its Hilbert polynomial. Therefore we define $P^+ = \{C \in P : \dim(C) > 0\}$, the subset of cones with dimension greater 0. One can easily check that the polynomial part of zero-dimensional cones is 0. Therefore

$$\overline{\varphi}_P(z) = \overline{\varphi}_{P^+}(z) = \sum_{C \in P^+} \overline{\varphi}_C(z).$$

Here

$$\begin{aligned} \overline{\varphi}_C(z) &= \binom{z - \deg(C) + \dim(C) - 1}{\dim(C) - 1} \\ &= \frac{(z - \deg(C) + \dim(C) - 1) \cdots (z - \deg(C) + 1)}{(\dim(C) - 1) \cdots 1}. \end{aligned}$$

We want to consider cone decompositions whose Hilbert polynomial has a nice representation which is interlinked with the maximal degree of a reduced Gröbner basis. The first step towards this is the following definition.

Definition 3.2 (Dubé 1990). *A cone decomposition P is* k-standard *for some $k \in \mathbb{N}$ if*

- *$C \in P^+$ implies $\deg(C) \geq k$ and*
- *for all $C \in P^+$ and for all $k \leq d \leq \deg(C)$, there exists a cone $C^{(d)} \in P$ with degree d and dimension at least $\dim(C)$.*

Note that P is k-standard for all k if and only if $P^+ = \emptyset$. Otherwise it can be k-standard for at most one k, namely the minimal degree of the cones in P^+. Furthermore, the union of k-standard decompositions is k-standard, again.

Lemma 3.3 (Dubé 1990). *Every k-standard cone decomposition P may be refined into a $(k+1)$-standard cone decomposition P' with $\deg(P) \leq \deg(P')$ and $\deg(P^+) \leq \deg(P'^+)$.*

Proof. See [5], Lemma 3.1. □

Dubé was able to construct such cone decompositions for the set of normal forms of an ideal.

Proposition 3.4 (Dubé 1990). *For any homogeneous ideal $I \subset \mathbb{K}[X]$ and any monomial ordering $\prec$, there is a 0-standard cone decomposition Q of N_I such that $\deg(Q) + 1$ is an upper bound on the degrees of polynomials required in a Gröbner basis of I.*

Proof. See [5], Theorem 4.11. □

The next step in [5] is a worst case construction. The question that arises is: How large can the degrees of the cones in Q and thus the degrees in the Gröbner basis be? We know that a k-standard cone decomposition P contains at least one cone in each degree between k and the maximal degree. So in the worst case there would be exactly one cone in each degree.

Definition 3.5 (Dubé 1990). *A k-standard cone decomposition P is* k-exact *if $\deg(C) \neq \deg(C')$ for all $C \neq C' \in P^+$.*

Since k-exact cone decompositions are also k-standard, the cones of higher degrees have lower dimensions, i.e., $C, C' \in P, \deg(C) > \deg(C')$ implies $\dim(C) \leq \dim(C')$.

Since one can split a cone into a cone of dimension 0 and same degree and cones of higher degrees, one can refine a k-standard cone decomposition such that it becomes k-exact. Dubé gives an algorithmic proof herefore.

Lemma 3.6 (Dubé 1990). *Every k-standard cone decomposition P may be refined into a k-exact cone decomposition P' with $\deg(P) \leq \deg(P')$ and $\deg(P^+) \leq \deg(P'^+)$.*

Proof. See [5], Lemma 6.3. □

A nice side effect of this worst case construction is that we can easily calculate the Hilbert polynomial of an exact cone decomposition P of some space T. Herefore we need the following notion.

Definition 3.7 (Dubé 1990). *Let P be a k-exact cone decomposition. If $P^+ = \emptyset$, let $k = 0$. Then the* Macaulay constants *of P are defined as*

$$a_i = \max\{k, \deg(C) + 1 : C \in P^+, \dim(C) \geq i\}$$

for $i = 0, \ldots, n+1$.

Note that the definition looks slightly different from the one given in [5], but is equivalent to it. This definition implies $\max\{k, \deg(P^+)\} = a_0 \geq \ldots \geq a_n \geq a_{n+1} = k$. Now

$$\overline{\varphi}_T(z) = \sum_{i=1}^{n} \sum_{c=a_{i+1}}^{a_i - 1} \binom{z - c + i - 1}{i - 1}.$$

Some lengthy calculations in [5] finally yield

Lemma 3.8 (Dubé 1990). *Given a k-exact decomposition P of some space T, the Hilbert polynomial of T is given by*

$$\overline{\varphi}_T(z) = \binom{z - k + n}{n} - 1 - \sum_{i=1}^{n} \binom{z - a_i + i - 1}{i}. \quad (1)$$

The Macaulay constants (except a_0) may be deduced from Hilbert polynomial and thus depend only on $\overline{\varphi}_T$ and not on the chosen decomposition.

Proof. See [5], Lemma 7.1. □

We are going to apply this result to an ideal generated by an exact sequence.

Corollary 3.9. *If P is a k-exact decomposition of N_J for an ideal J generated by a homogeneous regular sequence $g_1, \ldots, g_t$ of degrees $d_1, \ldots, d_t$. Then the Macaulay constants (except a_0) depend only on n, t, and $d_1, \ldots, d_t$, and neither on the chosen monomial ordering nor on the generators of J.*

Proof. This is a direct consequence of Proposition 2.1 and Lemma 3.8. □

3.2 A New Decomposition

In order to bound the Macaulay constants of a homogeneous ideal $I = \langle f_1, \ldots, f_s\rangle$, Dubé uses the direct decompositions

$$\mathbb{K}[X] = I \oplus N_I$$

and

$$I = \langle f_1\rangle \oplus \bigoplus_{i=2}^{s} f_i \cdot N_{\langle f_1,\ldots,f_{i-1}\rangle : f_i},$$

where $H : g = \{f : fg \in H\}$ is a special case of the ideal quotient. The Hilbert functions of $\mathbb{K}[X]$ and $\langle f_1\rangle$ are easily determined, and for all other summands one can calculate exact cone decompositions using the theory explained in the previous section. In Dubé's construction, the Macaulay constants achieve their worst case bound in the zero-dimensional case. Therefore we are going to use a slightly different decomposition.

So let I be an r-dimensional ideal generated by homogeneous polynomials $f_1, \ldots, f_s$ with degrees $d_1 \geq \ldots \geq d_s$. According to Proposition 2.2, there is a regular sequence $g_1, \ldots, g_{n-r} \in I$ with $\deg(g_k) = d_k$. First we prove a decomposition along the lines of Dubé, but starting from $J = \langle g_1, \ldots, g_{n-r}\rangle$ instead of $\langle f_1\rangle$.

Lemma 3.10. *With the stated hypotheses,*

$$I = J \oplus \bigoplus_{i=1}^{s} \mathrm{nf}_J(f_i) \cdot N_{J_i : \mathrm{nf}_J(f_i)} \tag{2}$$

with $J_k = \langle g_1, \ldots, g_{n-r}, f_1, \ldots, f_{k-1}\rangle$.

Proof. To prove this, we inductively show

$$J_{k+1} = J \oplus \bigoplus_{i=1}^{k} \mathrm{nf}_J(f_i) \cdot N_{J_i : \mathrm{nf}_J(f_i)}$$

for $k = 0, \ldots, s-1$. The equality $I = J_s$ then yields the stated result.

The "$\supset$"-inclusion is clear since $f_j, g_j \in I$. For the other inclusion, the case $k = 0$ is trivial. So assume $k > 0$. Let $f \in J_{k+1}$ and thus $f = f' + a \cdot f_k = (f' + a \cdot (f_k - \mathrm{nf}_J(f_k))) + a \cdot \mathrm{nf}_J(f_k)$ with $f', a \cdot (f_k - \mathrm{nf}_J(f_k)) \in J_k$. We rewrite

$$a = (a - \mathrm{nf}_{J_k : \mathrm{nf}_J(f_k)}(a)) + \mathrm{nf}_{J_k : \mathrm{nf}_J(f_k)}(a),$$

which yields

$$a \cdot \mathrm{nf}_J(f_k) \in (J_k : \mathrm{nf}_J(f_k)) \cdot \mathrm{nf}_J(f_k) + N_{J_k : \mathrm{nf}_J(f_k)} \cdot \mathrm{nf}_J(f_k).$$

Since $(J_k : \mathrm{nf}_J(f_k)) \cdot \mathrm{nf}_J(f_k) \subset J_k$, we get $f \in J_k + \mathrm{nf}_J(f_k) \cdot N_{J_k : \mathrm{nf}_J(f_k)}$ and inductively J_{k+1} of the stated form. It remains to show that the sum is direct. But this is clear since

$$J_k \cap \mathrm{nf}_J(f_k) \cdot N_{J_k : \mathrm{nf}_J(f_k)} \subset J_k \cap N_{J_k} = \{0\}.$$

$\square$

Now we are going to construct cone decompositions for the parts of (2).

Proposition 3.11. *With the stated hypotheses, any 0-standard decomposition Q of N_I may be completed into a d_1-standard decomposition P of N_J such that* $\deg(Q) \leq \deg(P)$.

Proof. By Proposition 3.4, we can construct 0-standard cone decompositions Q_k of $N_{J_k : \mathrm{nf}_J(f_k)}$. Then $f_k \cdot Q_k$ are d_k-standard cone decompositions of $f_k \cdot N_{J_k : \mathrm{nf}_J(f_k)}$. By Lemma 3.3, $Q, Q_1, \ldots, Q_s$ can be refined into d_1-standard cone decompositions $Q', Q'_1, \ldots, Q'_s$. Since

$$\mathbb{K}[X] = J \oplus \bigoplus_{i=1}^{s} \mathrm{nf}_J(f_i) \cdot N_{J_i : \mathrm{nf}_J(f_i)} \oplus N_I,$$

the union

$$P' = Q' \cup Q'_1 \cup \ldots \cup Q'_s$$

is a d_1-standard cone decomposition of N_J. By Lemma 3.6, this can be refined to a d_1-exact cone decomposition P of N_J with maximal degree $\deg(Q) \leq \deg(P)$. Thus the maximal degree of cones in P is also an upper bound on the Gröbner basis degree. $\square$

All Macaulay constants of a cone decomposition P of N_J except $a_0 = \deg(P)$ are determined by the Hilbert polynomial. But, because of Proposition 3.4 and 3.11, $\deg(P)$ is what we are actually interested in. Thus we want to bound a_0 using the other Macaulay constants which can be determined from the Hilbert polynomial (Corollary 3.9).

Lemma 3.12. *Let J be the ideal generated by the regular sequence $g_1, \ldots, g_{n-r}$ with degrees $d_1, \ldots, d_{n-r}$, P be a cone decomposition of N_J and $a_0, \ldots, a_{n+1}$ the corresponding Macaulay constants. Then*

$$a_0 \leq \max\{a_1, d_1 + \ldots + d_{n-r} - n\}.$$

Proof. Consider

$$\mathbb{K}[X] = J \oplus \bigoplus_{C \in P} C.$$

We know that the Hilbert functions (Hilbert polynomials) of the left hand and the right hand side agree. Furthermore, for z large enough (by Proposition 2.1, $z > d_1 + \ldots + d_{n-r} - n$ suffices) $\varphi_{\mathbb{K}[X]}(z) = \overline{\varphi}_{\mathbb{K}[X]}(z)$ and $\varphi_J(z) = \overline{\varphi}_J(z)$. This yields for $a_1 \leq z < a_0$:

$$\begin{aligned}\#\{C \in P : \dim(C) = 0, \deg(C) = z\} &= \varphi_P(z) - \overline{\varphi}_P(z) \\ &= (\varphi_{\mathbb{K}[X]}(z) - \varphi_J(z)) - (\overline{\varphi}_{\mathbb{K}[X]}(z) - \overline{\varphi}_J(z)) = 0\end{aligned}$$

Thus there are no cones with degree greater or equal $\max\{a_1, d_1 + \ldots + d_{n-r} - n\}$ which implies the statement. $\square$

As a consequence of Proposition 3.11, Corollary 3.9 and Lemma 3.12, we can choose a nice ideal J for the further considerations - independent of I.

Corollary 3.13. *Let Q be a 0-standard cone decomposition of N_I for some ideal I and some fixed admissible monomial ordering. If I has dimension r and is generated by homogeneous polynomials $f_1, \ldots, f_s$ of degrees $d_1 \geq \ldots \geq d_s$, then*

$$\deg(Q) \leq \max\{\deg(P^+), d_1 + \ldots + d_{n-r} - n\}$$

where P is a d_1-exact cone decomposition of N_J and J is the ideal $\left\langle x_{r+1}^{d_1}, \ldots, x_n^{d_{n-r}}\right\rangle$.

Proof. By Proposition 3.11, we can extend a 0-standard cone decomposition Q of N_I to an d_1-exact cone decomposition P' of $N_{J'}$ with $\deg(Q) \leq \deg(P')$ for $J' \subset I$ being generated by a homogeneous regular sequence of length $n-r$ and degrees $d_1, \ldots, d_{n-r}$. By Lemma 3.12, $\deg(P') = a_0$ can be bounded by $\deg(P'^+) = a_1$. By Corollary 3.9, the Macaulay constants a_k of P' (except a_0) only depend on

$n, n-r$, and $d_1, \ldots, d_{n-r}$. The ideal $J = \left\langle x_{r+1}^{d_1}, \ldots, x_n^{d_{n-r}} \right\rangle$ is obviously a r-dimensional ideal generated by a homogeneous regular sequence with the same degrees. Thus a d_1-exact cone decomposition of N_J (which exists by Proposition 3.4) has the same Macaulay constants (except a_0) and thus $\deg(P'^+) = \deg(P^+)$.
□

Example 3.14. *Before we continue the proof and bound the Macaulay constants in the next section, we want to illustrate that the Macaulay constants are independent of the ideals I and J. We will work in the ring $\mathbb{K}[x_1, x_2, x_3]$ for this example, i.e., $n = 3$. First we consider the very simple ideal $I = \langle x_1^2 \rangle$ (i.e., $d_1 = 2$), which has dimension $r = 2$, and the regular sequence $g_1 = x_1^2$. Using the concepts of this section and the algorithms from [5], implemented in Singular [8], we obtain an exact cone decomposition P of $N_{\langle g_1 \rangle}$. Due to its size we only list the cones of positive dimension:*

$$P^+ = \{C(x_2^2, \{x_2, x_3\}), C(x_1x_2^2, \{x_2, x_3\}, C(x_2x_3^3, \{x_3\}), C(x_3^5, \{x_3\}), C(x_1x_2x_3^4, \{x_3\}), C(x_1x_3^6, \{x_3\})\}$$

Now we do the same for $I' = \langle x_1^2 - x_1x_2, x_1x_2 + x_1x_3 \rangle$ and the regular sequence $g_1' = x_1^2 - x_2x_3$.

$$P'^+ = \{C(x_2^2, \{x_2, x_3\}), C(x_1x_2^2 + x_1x_2x_3, \{x_2, x_3\}), C(x_2x_3^3, \{x_3\}), C(x_3^5, \{x_3\}), C(x_1x_3^5, \{x_3\}), C(x_1x_2x_3^5 + x_1x_3^6, \{x_3\})\}$$

Both P and P' are exact cone decompositions with the same parameters n, r, d_1 and thus - as expected - have the same Macaulay constants:

$$a_0 = 8, a_1 = 8, a_2 = 4, a_3 = 2.$$

3.3 Macaulay Constants

By Corollary 3.13, it suffices to bound the Macaulay constant a_1 of a d_1-exact cone decomposition of N_J for the ideal $J = \left\langle x_{r+1}^{d_1}, \ldots, x_n^{d_{n-r}} \right\rangle$, which will be fixed for the remainder of this section.

The special shape of this ideal allows to dramatically simplify the corresponding proof in Dubé's paper which does not make any assumption on the ideal, except that it is generated by monomials. Nevertheless the bound we will obtain applies to any ideal by preceding corollary.

From $r = \dim(J) = \deg(\overline{\varphi}_J)+1$, one immediately deduces:

Lemma 3.15. *$a_n = \ldots = a_{r+1} = d_1$.*

In order to determine the remaining Macaulay constants, we have to determine N_J. For the ideal J we chose, this is

$$N_J = T_r \otimes \mathbb{K}[x_1, \ldots, x_r],$$

where the vector space T_r is given by

$$T_r = \operatorname{span}_{\mathbb{K}} \left\{ m \in \mathbb{K}[x_{r+1}, \ldots, x_n] : m \text{ monomial}, \; x_i^{d_{i-r}} \nmid m \text{ for } i = r+1, \ldots, n \right\} \quad (3)$$

and $A \otimes B$ denotes the tensor product of A and B, i.e., the vector space generated by $\{ab : a \in A, b \in B\}$. we need the following observation:

Lemma 3.16. *Any cone decomposition P_k of a vector space $T_k \otimes \mathbb{K}[x_1, \ldots, x_k]$, T_k generated by monomials, has exactly $\dim_{\mathbb{K}}(T_k)$ cones of dimension k.*

Proof. The key is to look at the Hilbert polynomials. We easily see that, for a monomial basis $\{t_1, \ldots, t_l\}$ of T_k,

$$T_k \otimes \mathbb{K}[x_1, \ldots, x_k] = t_1\mathbb{K}[x_1, \ldots, x_k] \oplus \ldots \oplus t_l\mathbb{K}[x_1, \ldots, x_k]$$

and

$$\overline{\varphi}_{T_k \otimes \mathbb{K}[x_1,\ldots,x_k]}(z) = \sum_{i=1}^{l} \binom{z - \deg(t_i) + k - 1}{k-1}.$$

On the other hand, the Hilbert polynomial of the cone decomposition P_k is

$$\overline{\varphi}_{P_k}(z) = \sum_{C \in P_k} \binom{z - \deg(C) + \dim(C) - 1}{\dim(C) - 1}.$$

Since P_k is a cone decomposition of $T_k \otimes \mathbb{K}[x_1, \ldots, x_k]$, we have $\overline{\varphi}_{T_k \otimes \mathbb{K}[x_1,\ldots,x_k]}(z) = \overline{\varphi}_{P_k}(z)$. Now compare the coefficients of z^{k-1} of both polynomials. Since P_k only contains cones of dimension at most k, this yields

$$\sum_{i=1}^{l} \frac{1}{(k-1)!} = \sum_{\substack{C \in P \\ \dim(C)=k}} \frac{1}{(k-1)!}$$

and thus $\#\{C \in P : \dim(C) = k\} = l = \dim_{\mathbb{K}}(T_k)$. □

Looking at the explicit formula (3) for T_r, one obtains $\dim(T_r) = d_1 \cdots d_{n-r}$ and thus:

Lemma 3.17. *$a_r = d_1 \cdots d_{n-r} + d_1$.*

Now we construct a d_1-exact cone decomposition with a special form. This allow us to bound the further Macaulay constants.

Lemma 3.18. *There exist a d_1-exact cone decomposition P of N_J ($J = \left\langle x_{r+1}^{d_1}, \ldots, x_n^{d_{n-r}} \right\rangle$) and subspaces T_k of N_J such that $P_{\leq k} = \{C \in P : \dim(C) \leq k\}$ is a cone decomposition of $T_k \otimes \mathbb{K}[x_1, \ldots, x_k]$ and $T_k \subset \mathbb{K}[x_{k+1}, \ldots, x_n]$ has a monomial basis for all $k = 1, \ldots, r$. Furthermore $a_k \leq \frac{1}{2}a_{k+1}^2$ for $k = 1, \ldots, r-1$.*

Proof. We construct P inductively. Let $P_{>k} = \{C \in P : \dim(C) > k\}$ and consider $k = r$. Since P cannot contain cones with dimension greater than r, $P_{>r} = \emptyset$ and $P_{\leq r}$ is a cone decomposition of $N_J = T_r \otimes \mathbb{K}[x_1, \ldots, x_r]$ with the monomial basis given in (3).

Now we assume that all cones of $P_{>k}$ have been constructed and that we already chose T_k such that

$$N_J = T_k \otimes \mathbb{K}[x_1, \ldots, x_k] \oplus \bigoplus_{C \in P_{>k}} C.$$

We want to construct $P_{\leq k}$ inductively such that it is a cone decomposition of $T_k \otimes \mathbb{K}[x_1, \ldots, x_k]$. By Lemma 3.16, P must contain exactly $\dim_{\mathbb{K}}(T_k)$ cones of dimension k. $P_{>k}$ is already constructed, so that $a_n, \ldots, a_{k+1}$ are fixed. Since P shall be d_1-exact, the cones of dimension k must have the degrees $a_{k+1}, a_{k+1}+1, a_{k+1}+2, \ldots$. Let $\{t_1, \ldots, t_l\}$ be a monomial basis of T_k with $\deg(t_1) \leq \ldots \leq \deg(t_l)$. Then we choose

$$C_i = t_i x_k^{a_{k+1}+i-\deg(t_i)-1}\mathbb{K}[x_1, \ldots, x_k] \text{ with } i = 1, \ldots, l$$

as cones of dimension k. It is easy to see that $\deg(C_i) = a_{k+1} + i - 1$ and $\dim(C_i) = k$. Thus we do not violate the definition of exact cone decompositions. Since $T_k \subset \mathbb{K}[x_{k+1}, \ldots, x_n]$, furthermore

$$T_k \otimes \mathbb{K}[x_1, \ldots, x_k] = C_1 \oplus \ldots \oplus C_l \oplus (T_{k-1} \otimes \mathbb{K}[x_1, \ldots, x_{k-1}])$$

with

$$\begin{aligned} T_{k-1} = \operatorname{span}_{\mathbb{K}} \{ & t_i x_k^e : i = 1, \ldots, l, \\ & e = 0, \ldots, a_{k+1} + i - \deg(t_i) - 2\} \subset \mathbb{K}[x_k, \ldots, x_n]. \end{aligned}$$

Inductively, this yields

$$N_J = (T_{k-1} \otimes \mathbb{K}[x_1, \ldots, x_{k-1}]) \oplus \bigoplus_{C \in P_{>k-1}} C.$$

So it only remains to bound a_{k-1}.

$$\begin{aligned} a_{k-1} - a_k = \dim_{\mathbb{K}}(T_{k-1}) &= \sum_{i=1}^{l} (a_{k+1} + i - \deg(t_i) - 1) \\ &\leq \sum_{i=1}^{l} (a_{k+1} + i - 1) = l a_{k+1} + \frac{1}{2} l(l-1) \end{aligned}$$

With $l = \dim_{\mathbb{K}}(T_k) = a_k - a_{k+1}$, we get by induction

$$\begin{aligned} a_{k-1} &\leq a_k + (a_k - a_{k+1}) a_{k+1} + \frac{1}{2}(a_k - a_{k+1})(a_k - a_{k+1} - 1) \\ &= \frac{1}{2}\left(a_k^2 - a_{k+1}^2 + a_k + a_{k+1}\right) \\ &\leq \frac{1}{2}\left(a_k^2 - a_{k+1}^2 + \frac{1}{2} a_{k+1}^2 + a_{k+1}\right) \leq \frac{1}{2} a_k^2 \end{aligned}$$

□

Corollary 3.19. *$a_k \leq 2\left[\frac{1}{2}(d_1 \cdots d_{n-r} + d_1)\right]^{2^{r-k}}$ for $k = 1, \ldots, r$.*

Finally we remember that a_1 bounds the Gröbner basis degree and state our main theorem.

Theorem 3.20. *Let $I = \langle f_1, \ldots, f_s \rangle$ be an ideal in the ring $\mathbb{K}[X] = \mathbb{K}[x_1, \ldots, x_n]$ generated by homogeneous polynomials of degrees $d_1 \geq \ldots \geq d_s$. Then for any admissible ordering $\prec$, the degree required in a Gröbner basis for I with respect to $\prec$ is bounded by $2\left[\frac{1}{2}(d_1 \cdots d_{n-r} + d_1)\right]^{2^{r-1}}$, where $r > 0$ is the (affine) dimension of I.*

Proof. Corollary 3.19 gives a bound on a_1. Since this bound is greater than $d_1 + \ldots + d_{n-r} - n$, Corollary 3.13 and Proposition 3.4 finish the proof. □

Just like Dubé, we can lift this result to non-homogeneous ideals by introducing an additional homogenization variable x_{n+1}. This implies

Corollary 3.21. *Let $I = \langle f_1, \ldots, f_s \rangle$ be an ideal in the ring $\mathbb{K}[X] = \mathbb{K}[x_1, \ldots, x_n]$ generated by arbitrary polynomials of degrees $d_1 \geq \ldots \geq d_s$. Then for any admissible ordering $\prec$, the degree required in a Gröbner basis for I with respect to $\prec$ is bounded by $2\left(\frac{1}{2} d_1 \cdots d_{n-r} + d_1\right)^{2^r}$, where r is the dimension of I.*

If we consider an arbitrary non-trivial ideal, its dimension r is at most $n-1$. For $r = n-1$, the bound given in this paper simplifies to $2\left(\frac{d_1^2}{2} + d_1\right)^{2^{n-2}}$. This is exactly Dubé's bound in [5], Theorem 8.2.

However our bound bridges the gap to the case of zero-dimensional ideals. It is well-known that the Gröbner basis of I in this case can be at most the vector space dimension of $\mathbb{K}[X]/I$, which is bounded by $d_1 \cdots d_n$ according to the theorem of Bézout. Our bound (though not proved for $r = 0$) specializes to $d_1 \cdots d_n + d_1$ which is close to the perfect bound. For $0 < r < n-1$ the bound is new to the best knowledge of the authors.

4. LOWER DEGREE BOUND

Finally we want to give a lower bound of similar form. Mayr, Meyer [13] and Möller, Mora [14] gave a lower bound for H-bases.

An H-basis of an ideal I is an ideal basis H such that $\langle \{h_{\deg(h)} : h \in H\} \rangle = \langle \{f_{\deg(f)} : f \in I\} \rangle$ (here $h_{\deg(h)}$ and $f_{\deg(f)}$ are the homogeneous components of highest degree). Consider a *graded* monomial ordering, i.e. $\deg(m) < \deg(m')$ implies $m \prec m'$ for all monomials m, m'. Then it is easy to see that any Gröbner basis with respect to $\prec$ is also an H-basis.

So we can reformulate the result as follows.

Proposition 4.1 (Mayr, Meyer 1982). *There is a family of ideals $J_n \subset \mathbb{K}[X]$ with $n = 14(k+1), k \in \mathbb{N}$, of polynomials in n variables of degree bounded by d such that each Gröbner basis with respect to a graded monomial ordering contains a polynomial of degree at least $\frac{1}{2} d^{2^{\left(\frac{n}{14}-1\right)}} + 4$.*

We are going to embed this ideal in a larger ring as follows. Define

$$J_{r,n} = \langle J_r, x_{r+1}, \ldots, x_n \rangle \subset \mathbb{K}[X].$$

Obviously $\dim(J_{r,n}) < r$.

Theorem 4.2. *There is a family of ideals $J_{r,n} \subset \mathbb{K}[X]$ with $r = 14(k+1) \leq n, k \in \mathbb{N}$ of polynomials in n variables of degree bounded by d with dimension less than r such that each Gröbner basis with respect to a graded monomial ordering contains a polynomial of degree at least $\frac{1}{2} d^{2^{\frac{r}{14}-1}} + 4$.*

The constant $\frac{1}{14}$ in the exponent could be improved by applying the techniques of [14] to the improved construction in [17]. Furthermore it would be interesting to give a non-trivial upper bound on the dimension of the ideals J_n (resp. $J_{r,n}$). To the best of the authors' knowledge, only the lower bound $\dim(J_n) \geq \frac{3}{14} n + 12$ (cf. [14]) is known.

5. REFERENCES

[1] D. Bayer. The division algorithm and the Hilbert scheme. 1982.

[2] B. Buchberger. *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal.* PhD thesis, Universität Innsbruck, 1965.

[3] D. Cox, J. Little, and D. O'Shea. *Ideals, Varieties, and Algorithms.* Springer New York, 1992.

[4] D. Cox, J. Little, and D. O'Shea. *Using Algebraic Geometry.* Springer Verlag, 2005.

[5] T. Dubé. The Structure of Polynomial Ideals and Gröbner Bases. *SIAM Journal on Computing*, 19:750, 1990.

[6] D. Eisenbud. *Commutative algebra with a view toward algebraic geometry*. Springer, 1995.

[7] M. Giusti. Some effectivity problems in polynomial ideal theory. In *Eurosam*, volume 84, pages 159–171. Springer, 1984.

[8] G.-M. Greuel, G. Pfister, and H. Schönemann. SINGULAR 3.1.0 — A computer algebra system for polynomial computations. 2009. http://www.singular.uni-kl.de.

[9] M. Kratzer. *Computing the dimension of a polynomial ideal and membership in low-dimensional ideals*. Bachelor's thesis, Technische Universität München, 2008.

[10] M. Kreuzer and L. Robbiano. Computational commutative algebra 2. 2005.

[11] K. Kühnle and E. Mayr. Exponential space computation of Gröbner bases. In *Proceedings of the 1996 international symposium on Symbolic and algebraic computation*, pages 63–71. ACM New York, NY, USA, 1996.

[12] D. Lazard. Gröbner bases, Gaussian elimination and resolution of systems of algebraic equations. In *Proc. EUROCAL*, volume 83, pages 146–156. Springer, 1983.

[13] E. Mayr and A. Meyer. The complexity of the word problems for commutative semigroups and polynomial ideals. *Advances in Mathematics*, 46(3):305–329, 1982.

[14] H. Möller and F. Mora. *Upper and Lower Bounds for the Degree of Groebner Bases*. Springer-Verlag London, UK, 1984.

[15] J. Schmid. On the affine Bezout inequality. *manuscripta mathematica*, 88(1):225–232, 1995.

[16] I. Shafarevich. *Basic Algebraic Geometry*. Springer-Verlag, 1994.

[17] C. Yap. A new lower bound construction for commutative Thue systems with applications. *J. Symbolic Comput*, 12(1), 1991.