Degree Bounds for Gröbner Bases in Algebras of Solvable Type

Matthias Aschenbrenner
University of California, Los Angeles

(joint with Anton Leykin)

UCLA

- … introduced by Kandri-Rody & Weispfenning (1990);
- … form a class of associative algebras over fields which generalize
  - commutative polynomial rings;
  - Weyl algebras;
  - universal enveloping algebras of f. d. Lie algebras;
- … are sometimes also called *polynomial rings of solvable type* or *PBW-algebras* (Poincaré-Birkhoff-Witt).

Systems of linear PDE with polynomial coefficients can be represented by left ideals in the *Weyl algebra*

$$A_n(\mathbb{C}) = \mathbb{C}\langle x_1, \ldots, x_n, \partial_1, \ldots, \partial_n \rangle,$$

the $\mathbb{C}$-algebra generated by the x_i, ∂_j subject to the relations:

$$x_j x_i = x_i x_j, \qquad \partial_j \partial_i = \partial_i \partial_j$$

and

$$\partial_j x_i = \begin{cases} x_i \partial_j & \text{if } i \neq j \\ x_i \partial_j + 1 & \text{if } i = j. \end{cases}$$

The Weyl algebra acts naturally on $\mathbb{C}[x_1, \ldots, x_n]$:

$$(\partial_i, f) \mapsto \frac{\partial f}{\partial x_i}, \qquad (x_i, f) \mapsto x_i f.$$

Let $\mathfrak{g}$ be a Lie algebra over a field K. The *universal enveloping algebra* $U(\mathfrak{g})$ of $\mathfrak{g}$ is the K-algebra obtained by imposing the relations

$$g \otimes h - h \otimes g = [g, h]_{\mathfrak{g}}$$

on the tensor algebra of the K-linear space $\mathfrak{g}$.

Poincaré-Birkhoff-Witt Theorem: the canonical morphism

$$\mathfrak{g} \to U(\mathfrak{g})$$

is injective, and $\mathfrak{g}$ generates the K-algebra $U(\mathfrak{g})$.

If $\mathfrak{g}$ corresponds to a Lie group G, then $U(\mathfrak{g})$ can be identified with the algebra of left-invariant differential operators on G.

Affine Algebras and Monomials

Let R be a K-algebra, and $x = (x_1, \ldots, x_N) \in R^N$. Write

$$x^\alpha := x_1^{\alpha_1} \cdots x_N^{\alpha_N} \qquad \text{for a multi-index } \alpha = (\alpha_1, \ldots, \alpha_N) \in \mathbb{N}^N.$$

We say that R is affine with respect to x if the family $\{x^\alpha\}$ of monomials in x is a basis of R as K-linear space.

Suppose R is affine w.r.t. x. Each $f \in R$ can be uniquely written

$$f = \sum_\alpha f_\alpha x^\alpha \qquad (f_\alpha \in K, \text{ with } f_\alpha = 0 \text{ for all but finitely many } \alpha).$$

Hence we can talk about the degree of non-zero $f \in R$.

We also have a monoid structure on the set $x^\diamond$ of monomials:

$$x^\alpha * x^\beta := x^{\alpha+\beta}.$$

A monomial ordering of $\mathbb{N}^N$ is a total ordering of $\mathbb{N}^N$ compatible with $+$ in $\mathbb{N}^N$ with smallest element 0.

Example

The *lexicographic* and *reverse lexicographic* orderings:

$$\alpha <_{\text{rlex}} \beta : \qquad \alpha \neq \beta \text{ and } \alpha_i > \beta_i \text{ for the last } i \text{ with } \alpha_i \neq \beta_i.$$

A monomial ordering $\leqslant$ of $\mathbb{N}^N$ yields an ordering of $x^\diamond$:

$$x^\alpha \leqslant x^\beta \qquad \Longleftrightarrow \qquad \alpha \leqslant \beta$$

Hence we can talk about the leading monomial $\operatorname{lm}(f) = x^\lambda$ of a non-zero element $f \in R$:

$$f = f_\lambda x^\lambda + \sum_{\alpha<\lambda} f_\alpha x^\alpha, \qquad f_\lambda \neq 0.$$

Examples

- $K[x]$ is affine with respect to $x = (x_1, \ldots, x_N)$.
- $A_n(K)$ is affine with respect to $(x_1, \ldots, x_n, \partial_1, \ldots, \partial_n)$.
- $U(\mathfrak{g})$ is affine with respect to a basis $(x_1, \ldots, x_N)$ of $\mathfrak{g}$.

These affine algebras are specified by a *commutation system* $\mathcal{R} = (R_{ij})$ in the free K-algebra $K\langle X \rangle$:

$$R_{ij} = X_j X_i - c_{ij} X_i X_j - P_{ij}$$

$$\text{where } 0 \neq c_{ij} \in K \text{ and } P_{ij} \in \bigoplus_{\alpha} K X^{\alpha} \text{ for } 1 \leqslant i < j \leqslant N.$$

Definition

The K-algebra R is of solvable type with respect to x and $\leqslant$ if

1. R is affine with respect to x, and
2. for $1 \leqslant i < j \leqslant N$ there are $0 \neq c_{ij} \in K$ and $p_{ij} \in R$ with

$$x_j x_i = c_{ij} x_i x_j + p_{ij} \quad \text{and} \quad \text{lm}(p_{ij}) < x_i x_j.$$

We call the K-algebra R of solvable type quadric if $\deg(p_{ij}) \leqslant 2$ for all i, j and homogeneous if $p_{ij} = 0$ or $\deg(p_{ij}) = 2$ for all i, j.

Key Property of Solvable Type Algebras

$$\text{lm}(f \cdot g) = \text{lm}(f) * \text{lm}(g) \qquad \text{for non-zero } f, g \in R.$$

In particular, R is an integral domain.

Quadric algebras of solvable type can be *homogenized*:

Example (Homogenization of the Weyl Algebra)

$$A_n^*(K) = K\langle x_1, \dots, x_n, \partial_1, \dots, \partial_n, t\rangle$$

with relations

$$\begin{array}{lll} x_j x_i = x_i x_j, & \partial_j \partial_i = \partial_i \partial_j, & \\ \partial_j x_i = x_i \partial_j & & \text{if } i \neq j, \\ \partial_i x_i = x_i \partial_i + t^2, & & \\ x_i t = t x_i, & \partial_i t = t \partial_i, & \end{array}$$

is homogeneous of solvable type w.r.t. the lexicographic product of any monomial ordering of $\mathbb{N}^{2n}$ and the usual ordering of $\mathbb{N}$.

Examples of homogeneous algebras of solvable type include all Clifford algebras.

Suppose R is a homogeneous algebra of solvable type.
Then R is naturally graded:

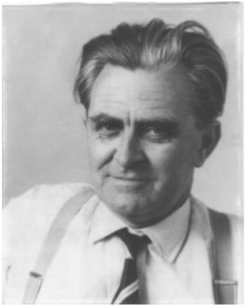
$$R = \bigoplus_{d} R_{(d)} \qquad \text{where } R_{(d)} = \bigoplus_{|\alpha|=d} Kx^{\alpha}.$$

For a homogeneous K-linear subspace $V = \bigoplus_{d} V_{(d)}$ of R, the Hilbert function $H_V \colon \mathbb{N} \to \mathbb{N}$ of V is defined by

$$H_V(d) := \dim_K V_{(d)} \qquad \text{for each } d.$$

If I is a homogeneous ideal of R, then there is a polynomial $P \in \mathbb{Q}[T]$ such that $H_I(d) = P(d)$ for all $d \gg 0$, called the Hilbert polynomial of I.

Gröbner basis theory . . .



- . . . provides a general method for computing with polynomials in several indeterminates, which has emerged in the last 40 years;
- . . . subsumes well-known algorithms for polynomials (Gaussian elimination, Euclidean algorithm, etc.);
- . . . is usually developed for commutative polynomial rings, but generalizes to algebras of solvable type.

Gröbner Bases in Algebras of Solvable Type

General Idea

Let R be an algebra of solvable type.

$$F = \{f_1, \ldots, f_n\} \subseteq R \qquad \text{(input set)}$$

$$\Big\downarrow \text{ Buchberger's algorithm}$$

$$G = \{g_1, \ldots, g_m\} \subseteq R \qquad \text{(output set)}$$

The sets F and G generate the same (left) ideal of R.

Reduction of Elements of R

$f \underset{g}{\longrightarrow} h$ if h is obtained from f by subtracting a multiple $cx^\beta g$ of the non-zero element $g \in R$ which cancels a non-zero term of f.

We say that f is reducible with respect to G if $f \underset{G}{\longrightarrow} h$ for some h, and reduced w.r.t. G otherwise. Each chain

$$f_0 \underset{G}{\longrightarrow} f_1 \underset{G}{\longrightarrow} \cdots \qquad (f_i \neq 0)$$

is finite. So for every f there is some r such that $f \underset{G}{\overset{*}{\longrightarrow}} r$ and r is reduced w.r.t. G, called a G-normal form of f.

Gröbner Bases in Algebras of Solvable Type

Definition

A finite subset G of an ideal I of R is called a Gröbner basis of I if every element of R has a unique G-normal form $\mathrm{nf}_G(f)$.

Suppose G is a Gröbner basis of I. Then the map $f \mapsto \mathrm{nf}_G(f)$ is K-linear, and $R = I \oplus \mathrm{nf}_G(R)$. A basis of $\mathrm{nf}_G(R)$: all $w \in x^\diamond$ which are not $*$-multiples of some $\mathrm{lm}(g)$ with $g \in G \setminus \{0\}$.

Each ideal I of R has a Gröbner basis. In fact, there exists an

- effective characterization of Gröbner bases (*Buchberger's criterion*), and
- an algorithm to obtain a Gröbner basis from a given finite set of generators for I (*Buchberger's algorithm*).

Applications of Gröbner Bases

- decide ideal membership:

$$f \in I \quad \Longleftrightarrow \quad f \xrightarrow[G]{*} 0$$

- construct generators for solutions to homogeneous equations:

$$y_1 f_1 + \cdots + y_n f_n = 0$$

- … many more (in *D*-module theory), e.g.:
  - talk by Anton Leykin (computing local cohomology);
  - book by Saito-Sturmfels-Takayama (computing hypergeometric integrals).

Some authors prefer the term *Janet basis* if $R = A_m(K)$.

Suppose $R = K[x_1, \ldots, x_N]$ is commutative. Fix a monomial ordering of $\mathbb{N}^N$. Let $f_1, \ldots, f_n \in R$ be of maximal degree d, and $I = (f_1, \ldots, f_n)$.

Lower Degree Bound (Mayr & Meyer, 1982)

One can choose the f_i such that every Gröbner basis of I contains a polynomial of degree $\geqslant d^{2^{O(N)}}$.

Upper Degree Bound (Bayer, Möller & Mora, Giusti, 1980s)

Suppose K has characteristic zero. There is a Gröbner basis of I all of whose elements are of degree $\leqslant d^{2^{O(N)}}$.

Strategy of the Proof

1. Homogenize: $R \rightsquigarrow R^* = K[x, t]$, $I \rightsquigarrow I^* = (f_1^*, \ldots, f_n^*)$.
2. Place I^* into *generic coordinates.*
3. In generic coordinates, the degrees of polynomials in a Gröbner basis of I^* w.r.t. revlex ordering are $\leqslant (2d)^{2^N}$.
4. This bound also serves as a bound on the *regularity* of I^*. (A homogeneous ideal J has regularity r if for every degree r homogeneous polynomial f, the ideal (J, f) has different Hilbert polynomial.)
5. A homogeneous ideal of R^* with regularity r has its *Macaulay constant* b_1 bounded by $(r + 2N + 4)^{(2N+4)^{N+1}}$.
6. For any monomial ordering, the degree of polynomials in a Gröbner basis of I^* is bounded by $\max\{r, b_1\}$.
7. Specialize I^* back to I by setting $t = 1$.

It was generally believed that that in the case of Weyl algebras, a similar upper bound should hold: the *associated graded algebra* of $R = A_m(K)$,

$$\operatorname{gr} R = \bigoplus_d (\operatorname{gr} R)_{(d)} \qquad \text{where } (\operatorname{gr} R)_{(d)} = R_{(\leqslant d)}/R_{(<d)},$$

is commutative:

$$\operatorname{gr} R = K[y_1, \ldots, y_m, \delta_1, \ldots, \delta_m] \qquad \text{where } y_i = \operatorname{gr} x_i,\ \delta_i = \operatorname{gr} \partial_i.$$

In fact, for degree-compatible $\leqslant$ there is a close connection between Gröbner bases of I and Gröbner bases of

$$\operatorname{gr} I = \{\operatorname{gr} f : f \in I\}.$$

But:

$$I = (f_1, \ldots, f_n) \not\Rightarrow \operatorname{gr} I = (\operatorname{gr} f_1, \ldots, \operatorname{gr} f_n).$$

The technique of using generic coordinates also seems problematic.

However, using entirely with combinatorial tools (*cone decompositions*, sometimes called *Stanley decompositions*) one can show (no assumptions on char K):

Theorem (Dubé, 1990)

Suppose $R = K[x_1, \ldots, x_N]$ *and* $f_1, \ldots, f_n$ *are as above. There is a Gröbner basis for* $I = (f_1, \ldots, f_n)$ *which consists of polynomials of degree at most*

$$D(N, d) = 2\left(\frac{d^2}{2} + d\right)^{2^{N-1}}.$$

Main Result

Suppose R is a quadric K-algebra of solvable type with respect to $x = (x_1, \ldots, x_N)$ and $\leqslant$. Let $f_1, \ldots, f_n \in R$ be of degree $\leqslant d$.

Theorem

The ideal $I = (f_1, \ldots, f_n)$ has a Gröbner basis whose elements have degree at most $D(N, d)$.

A similar result was independently and simultaneously proved for $R = A_m(K)$ by Chistov & Grigoriev.

A general (non-explicit) uniform degree bound for Gröbner bases in algebras of solvable type had earlier been established by Kredel & Weispfenning (1990).

Corollary 1

Suppose $\leqslant$ is degree-compatible.

1. *If there are $y_1, \ldots, y_n \in R$ such that*

$$y_1 f_1 + \cdots + y_n f_n = f,$$

then there are such y_i of degree at most $\deg(f) + D(N, d)$.

2. *The left module of solutions to the homogeneous equation*

$$y_1 f_1 + \cdots + y_n f_n = 0$$

is generated by solutions of degree at most $3D(N, d)$.

For $R = K[x]$, this is due to G. Hermann (1926), corrected by Seidenberg (1974). For $R = A_m(K)$, part (1) generalizes a result of Grigoriev (1990).

Corollary 2

Suppose $\leqslant$ is degree-compatible. If there are a finite index set J and $y_{ij}, z_{ij} \in R$ such that

$$f = \sum_{j \in J} y_{1j} f_1 z_{1j} + \cdots + \sum_{j \in J} y_{nj} f_n z_{nj}$$

then there are such J and y_{ij}, z_{ij} with

$$\deg(y_{ij}), \deg(z_{ij}) \leqslant \deg(f) + D(2N, d).$$

There is also a notion of Gröbner basis of two-sided ideals, with a corresponding degree bound. Note that $A_m(K)$ is simple.

Holonomic Ideals

Return to $R = A_m(K)$, and assume char $K = 0$. Then

$$m \leqslant \dim R/I < 2m \qquad (\textit{Bernstein Inequality}).$$

Here, $\dim R/I = 1 +$ degree of the Hilbert polynomial of R/I.

Ideals I with $\dim R/I = m$ are called *holonomic.*

In analogy with 0-dimensional ideals in $K[x]$, one would expect a single-exponential degree bound for Gröbner bases of holonomic ideals. (Known in special cases.)

There is a close connection

$$\text{holonomic ideals of } R \leftrightarrow \text{0-dim. ideals of } R_m(K) = K(x) \otimes_{K[x]} R.$$

Only a doubly-exponential bound on the leading coefficient of the Kolchin polynomial of $R_m(K)/R_m(K)I$ is known. (Grigoriev, 2005)

Cone Decompositions

Suppose R is a homogeneous algebra of solvable type and M a homogeneous K-linear subspace of R.

- Monomial cone: a pair (w, y) with $w \in x^\diamond$ and $y \subseteq x$.

$$C(w, y) := K\text{-linear span of } w * y^\diamond.$$

- $\mathcal{D}$ is a monomial cone decomposition of M if $C(w, y) \subseteq M$ for every $(w, y) \in \mathcal{D}$ and

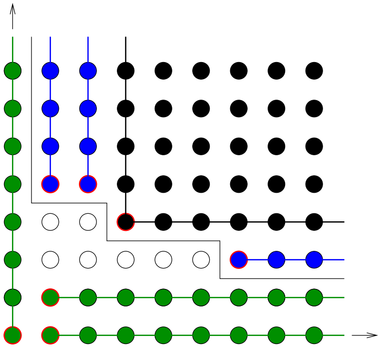
$$M = \bigoplus_{(w,y)\in\mathcal{D}} C(w, y).$$

- Cone: a triple (w, y, h), where $h \in R$ is homogeneous.

$$C(w, y, h) := C(w, y)h = \{gh : g \in C(w, y)\} \subseteq R.$$

- $\mathcal{D}$ is a cone decomposition of M if $C(w, y, h) \subseteq M$ for every $(w, y, h) \in \mathcal{D}$ and $M = \bigoplus_{(w,y,h)\in\mathcal{D}} C(w, y, h)$.

For an ideal I of R with Gröbner basis G, one can construct a monomial cone decomposition for $\mathrm{nf}_G(R)$. (Stanley, Sturmfels & White ...) In fact:

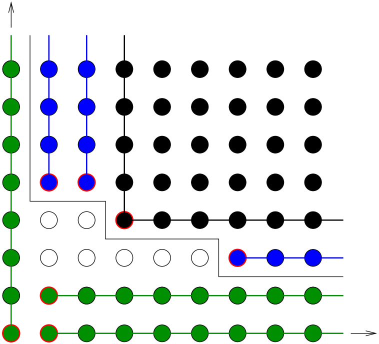


$$\mathcal{D}^+ := \{(w, y, h) \in \mathcal{D} : y \neq \emptyset\}$$

$\mathcal{D}$ is *d*-standard if $\forall (w, y, h) \in \mathcal{D}^+$:

- $\deg(w) + \deg(h) \geqslant d$;
- if $d \leqslant d' \leqslant \deg(w) + \deg(h)$, then there is some $(w', y', h') \in \mathcal{D}^+$ with $\deg(w') + \deg(h') = d'$ and $\#y' \geqslant \#y$.

For an ideal I of R with Gröbner basis G, one can construct a monomial cone decomposition for $\mathrm{nf}_G(R)$. (Stanley, Sturmfels & White . . .) In fact:

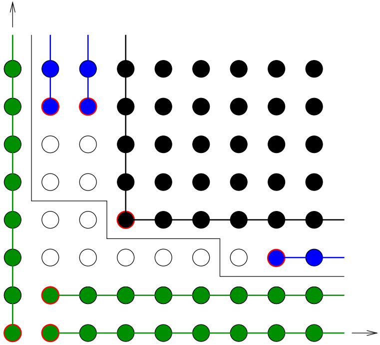


$\mathrm{nf}_G(R)$ admits a 0-standard monomial cone decomposition $\mathcal{D}$ with the property that the $g \in G$ with

$$\deg(g) \leqslant 1 + \deg(\mathcal{D})$$

are still a Gröbner basis of I. (Dubé)

A cone decomposition $\mathcal{D}$ is exact if $\mathcal{D}$ is d-standard for some d and for every d' there is *at most one* $(w, y, h) \in \mathcal{D}^+$ with $\deg(w) + \deg(h) = d'$.



Given a d-standard cone decomposition $\mathcal{D}$ of M, one can construct an exact d-standard decomposition $\mathcal{D}'$ of M with $\deg(\mathcal{D}') \geqslant \deg(\mathcal{D})$.

Suppose $I = (f_1, \ldots, f_n)$ where the f_i are homogeneous of degree at most $d = \deg(f_1)$. Then I also admits a d-standard cone decomposition: Write

$$I = (f_1) \oplus \mathrm{nf}_{G_2}(R) f_2 \oplus \cdots \oplus \mathrm{nf}_{G_n}(R) f_n,$$

where G_i is a Gröbner basis of $\big((f_1, \ldots, f_{i-1}) : f_i\big)$.

Let $\mathcal{D}$ be a cone decomposition of M which is d-standard for some d, and let $d_{\mathcal{D}}$ be the smallest such d.

- The Macaulay constants $b_0 \geqslant \cdots \geqslant b_{N+1} = d_{\mathcal{D}}$ of $\mathcal{D}$:

$$b_i := \min\left\{d_{\mathcal{D}}, 1 + \deg \mathcal{D}_i\right\} = \begin{cases} d_{\mathcal{D}} & \text{if } \mathcal{D}_i = \emptyset \\ 1 + \deg \mathcal{D}_i & \text{otherwise.} \end{cases}$$

  where $\mathcal{D}_i := \left\{(w, y, h) \in \mathcal{D} : \#y \geqslant i\right\}$.
- For $M = \mathrm{nf}_G(R)$, where G is a Gröbner basis of I, the Macaulay constants of all 0-standard decompositions are the same; for $d \geqslant b_0$:

$$H_M(d) = \binom{d - b_{N+1} + N}{N} - 1 - \sum_{i=1}^{N} \binom{d - b_i + i - 1}{i}.$$

Macaulay Constants

Theorem

Suppose $f_1, \ldots, f_n \in R$ are homogeneous of degree at most d. Then $I = (f_1, \ldots, f_n)$ has a Gröbner basis G whose elements have degree at most

$$D(N-1, d) = 2\left(\frac{d^2}{2} + d\right)^{2^{N-2}}.$$

Let

$$a_i = \text{Macaulay constants for a 0-standard exact cone decomposition of } \mathrm{nf}_G(R).$$

$$b_i = \text{Macaulay constants for a } d\text{-standard cone decomposition of } I.$$

Theorem

Suppose $f_1, \ldots, f_n \in R$ are homogeneous of degree at most d. Then $I = (f_1, \ldots, f_n)$ has a Gröbner basis G whose elements have degree at most

$$D(N-1, d) = 2\left(\frac{d^2}{2} + d\right)^{2^{N-2}}.$$

Using that

$$H_I(d) + H_{\mathrm{nf}_G(R)}(d) = H_R(d) = \binom{d+N-1}{N-1},$$

one may show

$$a_j + b_j \leqslant D(N-j, d) \qquad \text{for } j = 1, \ldots, N-2.$$

Theorem

Suppose $f_1, \dots, f_n \in R$ are homogeneous of degree at most d. Then $I = (f_1, \dots, f_n)$ has a Gröbner basis G whose elements have degree at most

$$D(N-1,d) = 2\left(\frac{d^2}{2} + d\right)^{2^{N-2}}.$$

In particular,

$$a_1 + b_1 \leqslant D := D(N-1,d).$$

Degrees of elements in G are bounded by a_0, but another argument shows

$$\max\{a_0, b_0\} = \max\{a_1, b_1\} \leqslant D. \quad \square$$