Computing the minimal number of equations defining an affine curve ideal-theoretically

Hans Schoutens

Department of Mathematics
Ohio State University
Columbus, OH 43210 (USA)

Abstract

There is an algorithm which computes the minimal number of generators of the ideal of a reduced curve C in affine n-space over an algebraically closed field K, provided C is not a local complete intersection.

The existence of such an algorithm follows from the fact that given $d \in \mathbb{N}$, there exists $d' \in \mathbb{N}$, such that if $\mathfrak{a}$ is a height $n-1$ radical ideal in $K[X_1, \dots, X_n]$, generated by polynomials of degree at most d, then $\mathfrak{a}$ admits a set of generators of minimal cardinality, with each generator having degree at most d', except possibly when $K[X_1, \dots, X_n]/\mathfrak{a}$ is an (unmixed) local complete intersection.

Key words: number of generators, local complete intersection, curve

1 Introduction

Determining the minimal number of generators of an ideal $\mathfrak{a}$ in a Noetherian ring A can be a hard problem if the ring is not local; in contrast, if A is local, then Nakayama's Lemma reduces the problem to determining the vector space dimension of $\mathfrak{a} \otimes k$ over the residue field k. Even if A is finitely generated over a field K, the existence of an effective procedure to calculate the minimal number of generators is far from obvious. For instance, Schmidt in [4, Remark 1.10] shows that for A the coordinate ring of an elliptic curve over an algebraically closed field K, there is some $d \in \mathbb{N}$ and a collection of principal ideals $\mathfrak{a}_1, \mathfrak{a}_2, \dots$ in A, such that each $\mathfrak{a}_n$ is generated by the image of two polynomials f_n, g_n of degree at most d, but no polynomial of degree at most n generates $\mathfrak{a}_n$.

Email address: `schoutens@math.ohio-state.edu` (Hans Schoutens).
URL: `http://www.math.ohio-state.edu/~schoutens` (Hans Schoutens).

Preprint submitted to Elsevier Science *11.03.2002*

As far as I know, there is no example in a polynomial ring over a field K with the properties of SCHMIDT's example. Put differently, present knowledge does not exclude the existence of a bound d' depending only on d and n, such that any ideal $\mathfrak{a}$ in $K[X_1, \ldots, X_n]$ generated by polynomials of degree d admits a generating set of minimal cardinality of degree at most d' (in this form, the problem was originally posed by VAN DEN DRIES in [11]). In this paper, I will treat the case of a reduced curve C over an algebraically closed field, that is to say, the case where the defining ideal of C is a height $n-1$ radical ideal $\mathfrak{a}$. More precisely, I will prove the existence of an algorithm which computes the minimal number of generators of a radical ideal $\mathfrak{a}$ of height $n-1$ in the polynomial ring $A = K[X_1, \ldots, X_n]$ over an algebraically closed field K, provided that $\mathfrak{a}$ is not locally generated by $n-1$ elements. Note that in any case, by KRULL's Principal Ideal Theorem, $\mathfrak{a}$ is locally generated by at least $n-1$ elements. If locally the number of generators of $\mathfrak{a}$ is equal to $n-1$ (which is for instance the case if $\mathfrak{a}$ defines a smooth curve), then we say that $\mathfrak{a}$ defines an *unmixed locally complete intersection.* In that case, the minimal number of generators of $\mathfrak{a}$ is either $n-1$ (the *complete intersection* case) or n, but the algorithm that I will describe here cannot discern which.

Uniform bounds. The main result of this paper is the following uniformity result.

Theorem 1 *There exists a integer valued computable function $D(d, n)$, defined on pairs of positive integers (d, n), with the following property. Let K be an algebraically closed field and let $A = K[X]$ for some n-tuple of variables X. If a height $n-1$ ideal $\mathfrak{a}$ in A is generated by polynomials of degree at most d and if $A/\mathfrak{a}$ is generically but not locally a complete intersection, then there exists a generating set of $\mathfrak{a}$ of minimal cardinality, with each generator of degree at most $D(d, n)$.*

For the remainder of this introduction, let A denote the polynomial ring $K[X]$ with K an algebraically closed field and X an n-tuple of variables. Let $\mathfrak{a} = (f_1, \ldots, f_s)A$ be an ideal of A with each f_i of degree at most d. We will obtain a slightly more general result than stated in Theorem 1. Namely, we will prove Theorem 1 under the following assumptions on $\mathfrak{a}$:

(i) $\mathfrak{a}$ has height $n-1$;

(ii) the unmixed part of $\mathfrak{a}$ is generically a complete intersection, that is to say, $A/\mathfrak{a}$ is a complete intersection locally at each minimal prime which is not a maximal ideal;

(iii) $\mathfrak{a}$ is not an unmixed local complete intersection, that is to say, locally at some maximal ideal, $\mathfrak{a}$ requires at least n generators.

In other words, $A/\mathfrak{a}$ is one-dimensional, $\mu(\mathfrak{a}A_{\mathfrak{p}})$ equals $n-1$, for all height $n-1$ prime ideals $\mathfrak{p}$ containing $\mathfrak{a}$, and $\mu(\mathfrak{a}A_{\mathfrak{m}})$ is at least n, for some maximal ideal $\mathfrak{m}$ (see for instance [3, Theorem 21.2]; recall that a local ring R is called a *complete intersection*, if its completion is a homomorphic image of a regular local ring modulo a regular sequence). Clearly, any radical ideal is generically a complete intersection whence satisfies Condition (ii). The key observation is now that Conditions (i)–(iii) imply that the minimal number of generators of $\mathfrak{a}$ is equal to the minimal number of generators locally at some maximal ideal of A. This follows from the EE-Conjecture proven by Mohan-Kumar; see Lemma 9. Theorem 1 then follows by a compactness argument.

The algorithm. In the course of the proof of Theorem 1 we will show the following result on the first order definability of the minimal number of generators.

Corollary 2 *Let $U = (U_1, \dots, U_m)$ and $X = (X_1, \dots, X_n)$ be variables and let $I = (F_1, \dots, F_s)\mathbb{Z}[U, X]$ be an ideal in $\mathbb{Z}[U, X]$. For each $t \in \mathbb{N}$, there exists a constructible set $Z_t \subset \mathbb{A}^m_{\mathbb{Z}}$ with the following property. For each algebraically closed field K, the set of K-rational points of Z_t consists precisely of those tuples $\mathbf{c} \in K^m$ for which the ideal $I(\mathbf{c}) := (F_1(\mathbf{c}, X), \dots, F_s(\mathbf{c}, X))K[X]$ satisfies Conditions* (i)–(iii) *and is minimally generated by t elements. Moreover, there is an effective way to determine the equations of Z_t from the given ideal I.*

This means, with the terminology of [8–10], that for ideals satisfying Conditions (i)–(iii), the property of having a prescribed minimal number of generators is *definable in families* (note that in the older papers [6,7], the term *asymptotically definable* was used instead of definable in families). This also shows the algorithmic nature of determining the minimal number of generators of a given ideal satisfying Conditions (i)–(iii): simply write $\mathfrak{a}$ as a *fiber* $I(\mathbf{c})$ of some ideal I in $\mathbb{Z}[U, X]$, calculate the constructible sets Z_t and determine to which Z_t the tuple $\mathbf{c}$ belongs.

Why complete intersections are problematic. It might come as a surprise that the local complete intersection case eludes our methods. This, however, ties in with the equally different problem of checking whether a module is free, as I will explain now. Firstly, due to the homological nature of being projective, we can check algorithmically whether a finitely generated module M (presented as a cokernel of some matrix) over an affine ring A is projective; in fact, being projective is definable in families. On the other hand, as an example in [4] shows, the property of being free is in general not definable in families–it is definable in families though over a polynomial ring over a field, since then being free is the same as being projective by the Suslin-Quillen Theorem.

Suppose now that A is a polynomial ring and that I is an unmixed height $n-1$ ideal in A which is locally a complete intersection. By a result of Mohan-Kumar (see Corollary 7 below), I is either generated by $n-1$ elements (whence a complete intersection) or by n elements. The issue is how to determine whether I is a complete intersection. The fact that I is a complete intersection precisely when the *conormal bundle* I/I^2 (or, if $n = 3$, the canonical module $\operatorname{Ext}^2_A(A/I, A)$) is free as an A/I-module, is of no use, since A/I is in general not a polynomial ring. In view of the previous observations, the following problem therefore may be hard.

Problem 3 *Is there for each pair of positive integers d and n, a bound d', such that if the ideal I of a reduced complete intersection curve in $\mathbb{A}^n_K$ is generated by polynomials of degree at most d, then there are polynomials $f_1, \dots, f_{n-1}$ of degree at most d' generating I?*

2 Local-Global Principles

Throughout this paper $X = (X_1, \dots, X_n)$ will always denote an n-tuple of variables and K an algebraically closed field.

Definition 4 *We will denote the minimal number of generators of an ideal $\mathfrak{a}$ in a (not necessarily local) Noetherian A by $\mu_A(\mathfrak{a})$, or simply, by $\mu(\mathfrak{a})$. For a prime ideal $\mathfrak{p}$ of A, we set*

$$\mathrm{FS}_{\mathfrak{p}}(\mathfrak{a}) := \dim(A/\mathfrak{p}) + \mu_{A_{\mathfrak{p}}}(\mathfrak{a}A_{\mathfrak{p}}).$$

The main local-global principle for the number of generators is undoubtedly the Forster-Swan Theorem. For our purposes, we need also a sharper version due to Mohan-Kumar, which has come to be known as the *EE-Conjecture*; I will state both results only for ideals. Note that for the first estimate, we do need to take into account minimal primes, but no so for the second.

Theorem 5 (Forster-Swan Theorem; [1]) *Let $\mathfrak{a}$ be an ideal in a Noetherian ring A. If D is the maximum of all $\mathrm{FS}_{\mathfrak{p}}(\mathfrak{a})$ for $\mathfrak{p}$ running over all prime ideals of A, then $\mu_A(\mathfrak{a}) \leq D$.*

Theorem 6 (EE-Conjecture; [2]) *Let $\mathfrak{a}$ be an ideal in $A = K[X]$, where K is a field and X a finite tuple of variables. If D is the maximum of all $\mathrm{FS}_{\mathfrak{p}}(\mathfrak{a})$ for $\mathfrak{p}$ running over all non-zero prime ideals of A, then $\mu_A(\mathfrak{a}) \leq D$.*

Corollary 7 *Let $\mathfrak{a}$ be a height $n-1$ ideal of $K[X]$. If $\mathfrak{a}$ is locally a complete intersection, then $\mu(\mathfrak{a})$ is either $n-1$ or n. In fact, if $\mathfrak{a}$ is not unmixed, then $\mu(\mathfrak{a}) = n$.*

PROOF. Put $A = K[X]$. Recall that $\mathfrak{a}$ not unmixed means in the present situation that some maximal ideal $\mathfrak{m}$ is a minimal prime of $\mathfrak{a}$. Since $\mathfrak{a}A_\mathfrak{m}$ has therefore height n, our assumption implies that it is minimally generated by n elements. Therefore, the second statement follows from the first, since in any case $\mu(\mathfrak{a}A_\mathfrak{m}) \leq \mu(\mathfrak{a})$.

To prove the first statement, note that $n-1 \leq \mu(\mathfrak{a})$ by Krull's Principal Ideal Theorem. For every prime ideal $\mathfrak{p}$ of A, our assumption implies that $\mu(\mathfrak{a}A_\mathfrak{p})$ is either at most the height of $\mathfrak{p}$ or one (according to whether $\mathfrak{p}$ contains $\mathfrak{a}$ or not). Therefore, $\mathrm{FS}_\mathfrak{p}(\mathfrak{a}) \leq n$, for all non-zero prime ideals $\mathfrak{p}$. The conclusion now follows from Theorem 6. □

Apart from these local-global principles, we will also make use of the following easy observation on faithfully flat descent.

Lemma 8 *Let $R \to S$ be a faithfully flat homomorphism between local rings. For any ideal $\mathfrak{a}$ of R, we have that $\mu_R(\mathfrak{a}) = \mu_S(\mathfrak{a}S)$.*

PROOF. Let $x_1, \dots, x_n$ generate $\mathfrak{a}$ minimally. By Nakayama's Lemma we can renumber in such way that $x_1, \dots, x_m$ generate $\mathfrak{a}S$ minimally. In other words, if $I = (x_1, \dots, x_m)R$, then $\mathfrak{a}S = IS$. Therefore, by faithful flatness $\mathfrak{a} = \mathfrak{a}S \cap R = IS \cap R = I$, showing that $m = n$. □

3 Degree bounds on generating sets of minimal cardinality

Lemma 9 (Key Lemma) *If $\mathfrak{a}$ is an ideal of $K[X]$ satisfying Conditions* (i)–(iii) *form the Introduction, then there is a maximal ideal $\mathfrak{m}$ such that $\mu(\mathfrak{a}) = \mu(\mathfrak{a}K[X]_\mathfrak{m})$.*

PROOF. Put $A = K[X]$ (for this result, it is not necessary that K be algebraically closed). By Krull's Principal Ideal Theorem, we always have that $n-1 \leq \mu(\mathfrak{a})$. Let v be the maximum of all $\mu(\mathfrak{a}A_\mathfrak{m})$, where $\mathfrak{m}$ runs over all maximal ideals of A. By Condition (iii), we must have $n \leq v$. If $\mathfrak{p}$ is a non-zero prime ideal of A not containing $\mathfrak{a}$, then $\mu_{A_\mathfrak{p}}(\mathfrak{a}A_\mathfrak{p}) = 1$ whence $\mathrm{FS}_\mathfrak{p}(\mathfrak{a}) = \dim A/\mathfrak{p} + 1 \leq n$. If $\mathfrak{p}$ is a height $n-1$ prime ideal containing $\mathfrak{a}$, then $\mu(\mathfrak{a}A_\mathfrak{p}) = n-1$ by Condition (ii), and hence $\mathrm{FS}_\mathfrak{p}(\mathfrak{a}) = n$. In conclusion, since $n \leq v$, the maximum of all $\mathrm{FS}_{\mathfrak{p}}(\mathfrak{a})$ is equal to v. By the EE-Conjecture (Theorem 6), we have that $\mathfrak{a}$ is generated by at most v elements. Since clearly $v \leq \mu(\mathfrak{a})$, we get that $v = \mu(\mathfrak{a})$, as required. □

Proof of Theorem 1. Fix a pair of natural numbers (d, n). I claim that Conditions (i)–(iii) are first order definable in the following sense (in the terminology of [9,10], we would say that these conditions are *definable in families*; in the older papers [6,7], the term *asymptotically definable* was used). Namely, there exists a constructible subset $A^{(d,n)}$ in some affine space over $\mathbb{Z}$ (or, equivalently, a first order formula $\alpha^{(d,n)}$ without parameters), with the following property. Let K be an algebraically closed field and set $A = K[X]$. Let $\mathfrak{a}$ be an ideal in A generated by polynomials $f_1, \dots, f_s$ of degree at most d. Let $\mathbf{c}_{\mathfrak{a}}$ be the tuple in K of all coefficients of the f_i in a once and for all fixed order. Note that since the vector space of all polynomials in n variables of degree at most d over a field is finite dimensional, we can choose the number of these generators $s = s(d, n)$ independent from $\mathfrak{a}$. We refer to $\mathbf{c}_{\mathfrak{a}}$ as a *code* of $\mathfrak{a}$. First order definability then amounts to the assertion that $\mathbf{c}_{\mathfrak{a}}$ is a K-rational point of $A^{(d,n)}$ (or, equivalently, $\alpha^{(d,n)}(\mathbf{c}_{\mathfrak{a}})$ holds in K) if, and only if, Conditions (i)–(iii) hold for the ideal $\mathfrak{a}$. The existence of such a constructible set follows from the uniformity results in [6, Proposition 5.1 and Theorem 5.3] (see also [5,7]). Note that by the Nullstellensatz, any maximal ideal in A is of the form $(X_1 - a_1, \dots, X_n - a_n)A$ for some tuple $(a_1, \dots, a_n)$ in K. This fact is needed in order to express Condition (iii) and is one of the reasons why we can currently only prove Theorem 1 for algebraically closed fields. It is also needed, in conjunction with Nakayama's Lemma, to construct for each $t \in \mathbb{N}$, a $\mathbb{Z}$-constructible set $B_t^{(d,n)}$ (that is to say, a first order formula $\beta_t^{(d,n)}$ without parameters) with the property that $\mathbf{c}_{\mathfrak{a}}$ is a K-rational point of $B_t^{(d,n)}$ if, and only if, t is the maximum of all $\mu(\mathfrak{a}A_{\mathfrak{m}})$, where $\mathfrak{m}$ runs over all maximal ideals of A. Finally, let $C_{t,e}^{(d,n)}$ be a $\mathbb{Z}$-constructible set (that is to say, a first order formula $\gamma_{t,e}^{(d,n)}$ without parameters) with the property that $\mathbf{c}_{\mathfrak{a}}$ is a K-rational point of $C_{t,e}$ if, and only if, $\mathfrak{a}$ is generated by t polynomials of degree at most e (the existence of such a constructible set follows from the uniform bounds on linear equations proven in [5]).

Lemma 9 now asserts that whenever a code $\mathbf{c}_{\mathfrak{a}}$ of an ideal $\mathfrak{a}$ belongs to $A^{(d,n)} \cap B_t^{(d,n)}$, then $\mu(\mathfrak{a}) = t$. From this, the Corollary in the introduction is immediate. Moreover, below I will argue that there is an effective method to obtain the equations of these constructible sets, so that we do get an effective algorithm (albeit hopelessly inefficient) to calculate the minimal number of generators. Let me first though finish the proof of Theorem 1. Since a generating set of minimal cardinality has some finite degree, we get that

$$A^{(d,n)} \cap B_t^{(d,n)} \subset \bigcup_{e \geq 0} C_{t,e}^{(d,n)}$$

(as constructible sets). Therefore, compactness (which amounts in the logic setup to first order compactness) shows that for each triple (d, n, t), there is some $e(d, n, t)$ such that

$$A^{(d,n)} \cap B_t^{(d,n)} \subset C_{t,e(d,n,t)}^{(d,n)}. \tag{1}$$

Let $D(d, n)$ be the maximum of all $e(d, n, t)$, for $0 \leq t \leq s(d, n)$. I claim that $D(d, n)$ has the properties proclaimed in Theorem 1. Indeed, let $\mathfrak{a}$ be an ideal generated by polynomials of degree at most d satisfying Conditions (i)–(iii) and let $\mathbf{c}_{\mathfrak{a}}$ be a code of $\mathfrak{a}$. Choose t such that $\mathbf{c}_{\mathfrak{a}}$ belongs to $B_t^{(d,n)}$. Clearly, $t \leq s(d, n)$ and by the argument above, $t = \mu(\mathfrak{a})$. Therefore, by (1), we have that $\mathfrak{a}$ admits t generators of degree at most $e(d, n, t) \leq D(d, n)$, as claimed.

To prove the computability of the function D, and hence the effective nature of the constructible sets, we use some arguments from logic. Namely, let $\Phi_{d,n,e}$ be the sentence

$$\bigwedge_{t \leq s(d,n)} (\forall \mathbf{x})[\alpha^{(d,n)}(\mathbf{x}) \wedge \beta_t^{(d,n)}(\mathbf{x}) \rightarrow \gamma_{t,e}^{(d,n)}(\mathbf{x})].$$

Since $\Phi_{d,n,D(d,n)}$ is true in any algebraically closed field, it is provable from the theory of algebraically closed fields by the Gödel Completeness Theorem. Since the theory of algebraically closed fields is recursive, we can list all its first order theorems effectively (using for instance a theorem generator). For each pair (d, n), let $\bar{D}(d, n)$ be the first e such that a theorem of the form $\Phi_{d,n,e}$ appears in this list (so that in particular $\bar{D}(d, n) \leq D(d, n)$). It follows that $\bar{D}$ is a computable function. □

4 A generalization to affine schemes

In this section, I will discuss how the above method can be used in case the polynomial ring is replaced by one of its homomorphic images.

Theorem 10 *For each d, there is a (computable) bound d' with the following property. Let K be an algebraically closed field, X a tuple of at most d variables and $I \subset J$ ideals in $K[X]$ generated by polynomials of degree at most d. Put $A := K[X]/I$ and $\mathfrak{a} := JA$. Suppose A has (Krull) dimension n and $\mathfrak{a}$ is a radical ideal of height $n - 1$ satisfying the following two additional conditions.*

(i) Each minimal prime ideal of $\mathfrak{a}$ lies in the regular locus of A.
(ii) For each maximal ideal $\mathfrak{m}$ of A, we have that $\mu(\mathfrak{a}A_{\mathfrak{m}}) \geq n + 1$.

If $t = \mu_A(\mathfrak{a})$, then there exist $f_1, \dots, f_t \in K[X]$ of degree at most d', such that $\mathfrak{a} = (f_1, \dots, f_t)A$.

PROOF. With some minor modifications, the same proof as for Theorem 1 applies. In fact, by the same arguments, it suffices to show that $\mu(\mathfrak{a})$ is equal to the maximum v of all $\mu(\mathfrak{a}A_{\mathfrak{m}})$, where $\mathfrak{m}$ runs over all maximal ideals of A. By (ii), we have $n+1 \leq v$. To prove that $v = \mu_A(\mathfrak{a})$, we calculate again the various $\mathrm{FS}_{\mathfrak{p}}(\mathfrak{a})$, for $\mathfrak{p}$ a prime ideal of A. If $\mathfrak{p}$ does not contain $\mathfrak{a}$, we have that $\mathrm{FS}_{\mathfrak{p}}(\mathfrak{a}) = \dim A/\mathfrak{p} + 1 \leq n+1$; a less optimal bound than in the polynomial case since we can no longer ignore the contribution of the minimal primes of A. If $\mathfrak{p}$ is a height $n-1$ minimal prime of $\mathfrak{a}$, then $\mathfrak{a}A_{\mathfrak{p}} = \mathfrak{p}A_{\mathfrak{p}}$, since $\mathfrak{a}$ is radical. Since $A_{\mathfrak{p}}$ is regular by (i), we get that $\mathfrak{a}A_{\mathfrak{p}}$ is generated by $n-1$ elements so that $\mathrm{FS}_{\mathfrak{p}}(\mathfrak{a}) = n < v$. By the FORSTER-SWAN Theorem (Theorem 5), it follows that $\mu(\mathfrak{a}) \leq v$ so that necessarily $v = \mu(\mathfrak{a})$, as required. □

References

[1] O. Forster, *Über die Anzahl der Erzeugenden eines Ideal in einem Noetherschen Ring*, Math. Z. **84** (1964), 80–87.

[2] N. Mohan Kumar, *On two conjectures about polynomial rings*, Invent. Math. **46** (1978), 225–236.

[3] H. Matsumura, *Commutative ring theory*, Cambridge University Press, Cambridge, 1986.

[4] K. Schmidt, *Bounds and definability over fields*, J. Reine Angew. Math. **377** (1987), 18–39.

[5] K. Schmidt and L. van den Dries, *Bounds in the theory of polynomial rings over fields. A non-standard approach*, Invent. Math. **76** (1984), 77–91.

[6] H. Schoutens, *Bounds in cohomology*, Israel J. Math. **116** (2000), 125–169.

[7] ———, *Uniform bounds in algebraic geometry and commutative algebra*, Connections between Model Theory and Algebraic and Analytic Geometry (A. Macintyre, ed.), Quaderni di Mathematica, vol. 6, 2000, pp. 43–93.

[8] ———, *Closure operations and pure subrings of regular rings*, preprint on `http://www.math.ohio-state.edu/~schoutens`, 2001.

[9] ———, *Lefschetz principle applied to symbolic powers*, preprint on `http://www.math.ohio-state.edu/~schoutens`, 2001.

[10] ———, *Non-standard tight closure*, preprint on `http://www.math.ohio-state.edu/~schoutens`, 2001.

[11] L. van den Dries, *Algorithms and bounds for polynomial rings*, Logic Colloquium, 1979, pp. 147–157.