Invent. math. 110, 207–235 (1992)

Inventiones mathematicae

Direct methods for primary decomposition*

David Eisenbud[1], **Craig Huneke**[2], **and Wolmer Vasconcelos**[3]

[1] Department of Mathematics, Brandeis University, Waltham MA 02254, USA
[2] Department of Mathematics, Purdue University, West Lafayette IN 47907, USA
[3] Rutgers University, New Brunswick NJ 08903, USA

Oblatum 10-I-1991 & 26-III-1992

Table of contents

Summary. Let I be an ideal in a polynomial ring over a perfect field. We give new methods for computing the equidimensional parts and radical of I, for localizing I with respect to another ideal, and thus for finding the primary decomposition of I. Our methods rest on modern ideas from commutative algebra, and are direct in the sense that they avoid the generic projections used by Hermann (1926) and all others until now.

Some of our methods are practical for certain classes of interesting problems, and have been implemented in the computer algebra system Macaulay of Bayer and Stillman (1982–1992).

Introduction

Among the most basic questions one could ask about an ideal I in a polynomial ring $S = k[x_1, \ldots, x_n]$ over a field k are the following:

A. What are the equidimensional parts of I?
B. What is the radical

$$\operatorname{rad} I = \{s \in S \mid s^m \in I \text{ for } m \gg 0\},$$

of I?

* The authors are grateful to the NSF for partial support during this work

C. What is the localization of I at an ideal J (that is, the intersection of the primary components of I which are contained in J or, if J is not prime, in primes containing J and having the same dimension as J)?
D. What are the associated primes of I?
E. What is a primary decomposition of I?

(Throughout this introduction, we will deal only with ideals, though in the body of the paper we will work systematically with modules.)

From an existential point of view these questions, all of which are essentially subsumed in E, were made easy by a fundamentally nonconstructive insight of Emmy Noether: the existence of primary decompositions depends only on the ascending chain condition. Algorithms for solving the problems computationally have also been known for a long time. Grete Hermann, a student of Noether's, showed (1926) (see also Seidenberg 1984, the literature cited there, and the more computational papers cited below) that answers can be effectively computed given methods for solving problems 1–3, below. But in terms of practical computation, problems A–E remain quite hard to this day.

The problems into which Hermann's methods translate problems A–E are the following:

1) Factor a polynomial in S into irreducible factors (FACTOR).

2) Find the polynomial solutions to linear equations with polynomial coefficients (SYZYGY).

3) Find the intersection of $I \subset k[x_1, \ldots, x_n]$ with a subring $k[y_1, \ldots, y_m]$ where the y_i are linear forms in the x_j (PROJECTION; the name comes from the geometric interpretation of this operation as finding the closure of the image of an affine variety in k^n under a linear projection of k^n to a subspace).

It is clear that FACTOR is a special case of the primary decomposition problem. The relevance of SYZYGY may be seen from a special case: If f and g are polynomials then the vectors of polynomials (a, b) which are solutions to the equation

$$fa + gb = 0$$

are precisely the multiples of the vector

$$(g/\mathrm{GCD}(f, g),\ -f/\mathrm{GCD}(f, g)).$$

Thus solving the equation is tantamount to finding a greatest common divisor. On the other hand, PROJECTION is not intrinsically related to the primary decomposition process, but was used by Hermann, and all others who have considered the problem till now, to reduce to the case of an ideal generated by one polynomial.

Hermann proposed using Hilbert's method (1890) for SYZYGY. This method is so slow that it cannot be used effectively even with the aid of modern computers! Fortunately, algorithms involving Gröbner bases are far more efficient, and several computer algebra packages have incorporated them. The methods for FACTOR, now mostly based on ideas of Berlekamp (see for example Knuth 1971, Sect. 4.6.2) have also become quite good. In Hermann's time PROJECTION was done using resultants, but it is now done more efficiently by using Gröbner bases (see for example Cox et al. 1992 for an introduction).

The increasing availability of symbolic algebra systems on computers and of efficient methods for 1)–3) has led to a renewed interest in the question of computing primary decompositions, as one sees from the work of Lazard (1982 and 1985), Gianni et al. (1988) (see also the references there), Bayer et al. (1992), and Krick and Logar (1991). However these authors make use of the same basic strategy as Hermann, using PROJECTION to reduce to the one-polynomial case as before. In this paper we introduce new methods, based on ideas of modern commutative algebra, which are "direct methods" in the sense that they do not require this reduction.

Why should one want to avoid the reduction? To answer questions A–E by the methods using projections one needs "sufficiently generic" projections. In practice, this currently means that one takes the y_i in 3) above to be random linear forms in the x_j, checking afterwards that the choice was "random enough". Unfortunately this randomness destroys whatever sparseness and symmetry the original problem may have had, and leads to computations which are often extremely slow. Although it seems one can often get away with special projections (choosing the y_j to be much sparser linear forms in the x_i), which usually makes computation much faster, a systematic understanding of how to do this is lacking. Such a lack becomes particularly significant if the methods are to be incorporated in a larger system.

The methods we propose here for answering the questions A, B and C, use only SYZYGY. We are able to avoid projection essentially because we introduce techniques which extend to arbitrary ideals operations which were previously possible to do directly only for principal ideals.

Because we avoid projections, our methods for solving problems A–C are practical, using the current system Macaulay, for handling some problems of genuine interest, and we have implemented them; they are now distributed with Macaulay as scripts. Our methods lead to methods for settling question D and E using only SYZYGY and FACTOR.

We do as much as possible without FACTOR, for reasons which we will now explain. SYZYGY and FACTOR, and the things that one can derive from them, differ in a fundamental way:

Neither the results nor the methods for performing SYZYGY (or, in general, for finding Gröbner bases) depend on the nature of the underlying field k. This is because the methods require only the solution of *linear* equations over k. One consequence is that the results are stable under the extension of the base field (to an algebraic closure, say).

By contrast, any method for solving FACTOR must be highly sensitive to the arithmetic of k. Indeed, one might say that ALL the arithmetic of k is already present in the problem of factoring polynomials of 1 variable.

For this reason it is natural and efficient to try to find methods avoiding FACTOR and rely only on SYZYGY and on Gröbner basis computations whenever possible. In the algorithms explained below, we use FACTOR only in the simplest case, the factorization of polynomials in 1 variable. Actually, our use of FACTOR appears only in the sub-problem of finding a maximal ideal of an artinian ring (that is, a not-necessarily rational point of a finite variety). There may well be more efficient ways to handle even this problem, such as the ones developed by Lazard (1992).

We now indicate in more detail the contents of this paper.

Our methods for answering question A, that is, finding the equidimensional parts of an ideal or submodule, are given in Sect. 1. For example, if S is a regular

ring and $I \subset S$ is an ideal of codimension c, then we show that the equidimensional part of I, that is, the intersection of all the primary components of I whose codimension is exactly c, is equal to the annihilator of the module

$$\mathrm{Ext}_S^c(S/I, S) .$$

This and related formulas for modules follow from the Auslander–Buchsbaum formula and a few exact sequences. They were known to the authors independently for some time, and probably to many other people, though their usefulness for practical computation seems to be a new observation.

Section 2, the heart of the paper, contains methods for finding the radical of an ideal. We introduce two methods which involve the use of the Jacobian matrix (Theorems 2.1 and 2.7). These methods should be viewed as generalizing to arbitrary ideals in many variables the ancient formula for polynomials F in one variable which says that the derivative F' is divisible by the $(n-1)^{\text{rst}}$ power of any irreducible polynomial whose n^{th} power divides F, so that the ideal generated by the square-free part of F – that is, the radical of (F) – may be computed as the "ideal quotient"

$$\mathrm{rad}(F) = ((F):(F')) := \{G \mid GF' \in (F)\} .$$

First of all, we prove that if the ideal I is generated by a regular sequence, that is, if I is a 'complete intersection', then the ideal generated by the maximal minors of the Jacobian matrix of I can be used in place of (F') in the formula above (with I playing the role of (F)), generalizing the formula above directly. The proof is based on a special case provided by a theorem of Scheja and Storch (related to the theory of residues): if an ideal I generated by a regular sequence is primary to the maximal ideal $\mathfrak{M}$ in a polynomial ring S, then the Jacobian determinant J generates the socle of S/I, so that $(I:J) = \mathfrak{M}$, which is indeed the radical. The same method works for ideals which are generically complete intersections.

The case where the ideal I is not (generically) a complete intersection can be reduced to the case where it is, if one knows a maximal regular sequence contained in I, by computing two more ideal quotients. However, finding a "simple" maximal regular sequence inside a given ideal can be quite hard, and if something like the right number of random linear combinations of the generators of the ideal is used, then the method becomes slow. Thus this method is most useful in practice when one knows a good regular sequence in advance.

To avoid these problems, we give a second Jacobian method, which computes the radical directly, not passing by way of a regular sequence. To do this, we systematically exploit the lower order minors of the Jacobian matrix. This is probably the most novel idea in the paper. The effect is to reduce to the case of a generically complete intersection. This is often the best method in practice when one does not known in advance a simple regular sequence contained in the ideal.

It is quite important from the point of view of practical computation to the able to work in characteristic p, over finite fields, even if one's ultimate interest is in characteristic 0 results. This is because of the familiar "coefficient explosion" in the Buchberger algorithm for Gröbner bases. In characteristic 0, one must use infinite precision arithmetic, which is slow, but there is no problem over a field small enough that its elements can all be represented in one computer word. Since the ultimate answers are typically far less sensitive to characteristic than the methods,

one can use characteristic p computations to get results which reliably reflect the characteristic 0 situation in a wide range of problems.

However, Jacobian methods are intrinsically sensitive to the characteristic. This is already obvious in the case of one polynomial in one variable above: if $F(x) = x^p$, and characteristic $k = p$, then of course $F'(x) \equiv 0$, so $((F):(F')) = S$, and the formula for rad (F) above is wrong! Of course there will be no problem if the degree of F is less than p. We are able to prove that our techniques are valid in a similar range in the general case (Lemma 2.6). The main result that we need generalizes a result of Grothendieck from the case of characteristic 0. It is interesting that our second Jacobian method is valid in a somewhat larger range of cases than the first, even when the ideal in question is itself a complete intersection.

Putting these techniques together, we give in Sect. 3 a theorem which leads to a method for computing the "localization of an ideal I at an ideal J". For example when J is a prime of S, we define the localization of I at J to be the ideal

$$I_J \cap S ,$$

where I_J is the usual localization of I at J, which is an ideal of the local ring S_J. In general we define the localization of I at J to be intersection of those primary components of I which are contained in primes containing J and having the same dimension as J. We then show how to use the formula

$$(I \text{ localized at } J) = \bigcap_n \text{hull}(I + J^n)$$

(where the "hull" of an ideal is the intersection of its primary components of maximal dimension) to effectively compute the localization, essentially by giving bounds of the power n to which one must go to separate the generators of I from forms of the same degree. Again this extends to general ideals a method that was previously understood and exploited only for principal ideals.

Using this notion of localization, we describe in Sect. 4 a new approach to computing primary decomposition.

Throughout the paper, we have described explicit algorithms for computation. We have isolated these algorithms, rather than letting the reader dig them out of the theorems, because they represent our belief about which parts of the theorems are most nearly practical. We have not, however, included any analyses of complexity. The most expensive step is almost always the Buchberger algorithm, and in contrast to its well-known worst-case behavior, the complexity of this algorithm in the cases of real interest in Algebraic Geometry is poorly understood.

The fundamental operations we use are the computation of a Gröbner basis of a submodule of a free module (with respect to some multiplicative order), and the corresponding computation of its syzygies. For convenience, however, we describe our algorithms in terms of some higher level procedures derived from these. These will be treated in detail in the forthcoming paper Eisenbud and Stillman (1992); most are in any case part of the folklore of this subject. They are all implemented as Macaulay scripts which are distributed with the current release of Macaulay.

We now describe some of the computations we will require as components in our algorithms. All modules will be modules over the polynomial ring S. To "give" a module means to give a presentation matrix (generators and relations) for it.

1) The codimension of a module (the dimension of S minus the dimension of the module) could be computed from the form of the free resolution, following Hilbert. Much more efficiently, it can be computed directly from a standard basis

for the relations on the module. Bayer and Stillman (1992) have developed a particularly good way to do this.

2) Given two ideals I, J one can compute $I \cap J$ from the syzygies of a certain module.

3) a. If $A \subset B$ are modules and J is an ideal, we can compute the quotients

$$(A:J) := \{b \in B \mid Jb \subset A\} \subset B$$

and

$$(A:B) := \{s \in S \mid sB \subset A\} \subset S\,.$$

In particular, we can compute the annihilator of a module A as

$$\operatorname{ann} A = (0:A) \subset S\,.$$

These computations are all easy given the ability to compute syzygies.

b. If $A \subset B$ are modules, and J is an ideal of S, then one may compute the *saturation of A with respect to J*

$$(A:J^\infty) := \bigcup_n (A:J^n) \subset B$$

in one standard basis operation. This operation was described by Bayer and Stillman (1987) in the case where J is a principal ideal generated by one of the variables. To reduce to this case, one may first replace J by a suitably generic linear combination of its generators; for example, if $J = (j_0, \ldots, j_m)$, we may use

$$f := t^m j_0 + t^{m-1} j_1 + \ldots + t j_{m-1} + j_m\,,$$

where t is a new variable, and then adjoin another new variable s and the relation $s - f$. One then saturates with respect to s. Alternately (and this is often faster when J is large) one may simply compute

$$(\ldots((A:J):J)\ldots)$$

until this stabilizes.

4) Given a module M and an integer i one can compute

$$\operatorname{Ext}^i(M, S)$$

from a free resolution of M, by dualizing the $(i+1)$st map in the resolution, computing its kernel, and then factoring out the image of the dual of the ith map map of the resolution. (Similar but slightly more complex considerations allow the computation of any $\operatorname{Ext}^i(M, N)$; we will not need this, however.)

5) Given a ring $R = S/I$ and a prime ideal $P \subset R$ we can compute the multiplicity of R at P, (that is, the multiplicity of the local ring R_p) by forming the associated graded ring (or *normal cone*)

$$T := R/P \oplus P/P^2 \oplus \ldots$$

and computing a "Gröbner basis for the generic fiber" of the inclusion $R/P \subset T$ in the manner described in Bayer et al. (1992). Actually a much simpler computation suffices for nearly all the uses made of this here: if S is the graded polynomial ring and P is the irrelevant ideal, then the multiplicity, which is the degree of the projective variety corresponding to I, is $(\dim I)!$ times the leading coefficient of the Hilbert polynomial of R.

Open problems

There are many interesting problems remaining in the area of effective computation in commutative algebra and algebraic geometry. Here are a few of our current favorites:

1) What is a good method of finding a "simple" maximal regular sequence in an ideal $I \subset S = k[x_1, \ldots, x_n]$? One can start with an element of least degree and adjoin generators one at a time to the ideal, adding a general linear combination of the generators already taken to the regular sequence whenever the codimension of the ideal increases. Unfortunately, this leads to highly non-sparse regular sequences, especially if the generators are homogeneous of different degrees, and one wants to maintain homogeneity. One can of course break up the generators of the ideal into subsets, and thus write $I = I_1 + \ldots + I_m$ where the I_j form a "regular sequence of ideals" in the sense that the codimension $I_1 + \ldots + I_j = j$. Given such a decomposition one could hope to choose a regular sequence whose jth element is a linear combination of the generators of I_j. However, in the "regular sequence" of ideals

$$I_1 = (x_1x_3 - x_2x_4), \quad I_2 = (x_1^2, x_2^2), \quad I_3 = (x_3^2), \quad I_4 = (x_4^2),$$

no sequence of the form

$$x_1x_3 - x_2x_4, \ \alpha x_1^2 + \beta x_2^2, \ x_3^2, \ x_4^2$$

is a regular sequence.

A less direct approach is to solve the problem first for ideals generated by monomials, apply this solution to the ideal generated by the leading forms of a Gröbner basis for the ideal, and then take the corresponding linear combinations of the Gröbner basis elements themselves. This reduces the question to the special case of monomial ideals. A solution to the problem in this form has been obtained by Eisenbud and Sturmfels (1992), but more remains to be done.

2) What is a good method of finding a "simple" Noether normalization of a ring S/I (that is, a simple sequence of elements $y_1, \ldots, y_d$ of $S = k[x_1, \ldots, x_n]$ with $d = \dim S/I$ such that S/I is a finite module over $k[y_1, \ldots, y_d]$. This is the first of a sequence of such problems that one must solve to make an efficient computation of primary decomposition by the method of projections, and would have other applications as well.

3) Are there direct methods for finding the radical which do not use Jacobians, or at any rate which work for arbitrary characteristics? For example, if $f_1, \ldots f_n$ generate a homogeneous ideal of codimension n in $S = k[x_1, \ldots, x_n]$, and if (a_{ij}) is an $n \times n$ matrix such that

$$f_i = \textstyle\sum_j a_{ij}x_j \,,$$

then $\operatorname{rad}(f_1, \ldots, f_n) = (x_1, \ldots, x_n) = (f_1, \ldots, f_n) : \det(a_{ij})$ (see Scheja and Storch 1975, Sect 1). One possible choice for the a_{ij} when the characteristic is not too low is, by Euler's formula, the Jacobian matrix with its rows divided by the degrees of the f_i. This fact leads to the computation for the radical given in Theorem 2.1. Can one exploit the existence of such matrices (a_{ij}) in general to get a computation for

the radical without restrictions on the characteristic? A good test case, suggested by David Jaffe, is the ideal

$$(z^7 - xyu^5, y^4 - x^3u)$$

in characteristic 7, whose radical is the ideal

$$(z^3 - yu^2, yz - xu, y^3 - x^2z, xz^2 - y^2u)$$

defining the rational quartic space curve parametrized by

$$(s, t) \mapsto (x, y, z, u) = (s^4, s^3t, st^3, t^4).$$

4) Regularity bounds: We say that a graded module over a polynomial ring S has regularity r if for each n its nth syzygy is generated in degrees $\leqq r + n$. It has been conjectured by the first author that the regularity of a factor ring S/I for any homogeneous prime ideal of degree d and codimension c is $\leqq d - c + 1$. (This is easy for 1 − dimensional primes. It was proved for 2-dimensional primes representing smooth curves by Castelnuovo, and for arbitrary 2-dimensional primes by Gruson et al. (1983). Various weaker results are known for higher dimensional primes; see for example Lazarsfeld (1987).)

Here is another problem of this type. A good answer might aid considerably in the computation of localizations given below:

Given a reduced equidimensional ideal $I \subset S = k[x_1, \ldots, x_n]$ generated by forms of degree $\leqq d$, and an ideal $J \supset I$ which is the intersection of a subset of the components of I, what is a bound on the degrees of elements necessary to generate J (perhaps just up to radical)? If J represents a single component of I which happens to be smooth, and if the characteristic of k is 0, then a recent theorem of Bertram, Ein, and Lazarsfeld implies that in fact the regularity of J is $\leqq cd - c$. Does this hold for arbitrary J as in the problem?

5) Given homogeneous radical ideals $I, J \subset S = k[x_1, \ldots, x_n]$, determine the least number r such that

$$\text{hull}\,(I + J^{rm}) \subset (x_1, \ldots, x_n)^m .$$

See Theorem 3.3 and the remarks following it for more information.

This paper owes much to Dave Bayer and Mike Stillman, who have generously shared with us their evolving ideas about the computation of primary decomposition. Their computer algebra system Macaulay (1982–1992) has helped us to many ideas in commutative algebra and algebraic geometry, as well as inspiring our interest in the results below.

1 The equidimensional hull of a submodule

In the following, *we will assume that all modules are finitely generated.* We define the *equidimensional hull* of 0 in a module M to be the submodule N consisting of all elements whose annihilators have dimension < the dimension of M; equivalently, N is the intersection of all the primary components of 0 in M having maximal dimension. If $M' \subset M$ is a submodule, we define the equidimensional hull of M' to be the preimage in M of the equidimensional hull of 0 in M/M'. If I is an ideal in

ring S, then the equidimensional hull of I will mean the equidimensional hull of I in S. We write

$$\text{hull}(N, M)$$

or, when there is no danger of confusion, simply

$$\text{hull}\, N,$$

for the equidimensional hull.

The following result connects the equidimensional hull and some other aspects of primary decomposition to the behaviour of Ext:

Theorem 1.1 *Let M be a module over a regular domain S, and set $I_e = \operatorname{ann} \operatorname{Ext}_S^e(M, S)$:*

1) *I_e has codimension $\geqq e$ and $M/(0:_M I_e)$ has no associated primes of codimension e. In particular, a prime ideal $P \subset S$ of codimension e is associated to M iff P contains the annihilator of $\operatorname{Ext}_S^e(M, S)$.*

2) *The equidimensional hull of 0 in M is the kernel of the natural map $\pi : M \to \operatorname{Ext}_S^c(\operatorname{Ext}_S^c(M, S), S)$ where c is the codimension of M.*

3) *If $I = \operatorname{ann}_S M$, then $\operatorname{hull} I = I_c$. In particular, for any ideal I, $\operatorname{hull} I = \operatorname{ann}_S \operatorname{Ext}_S^c(S/I, S)$.*

Remark. It would be nice to find some homological way of producing ideals that are simpler than I and intersect in I. If $M = S/I$ then $I \subseteq I_e$ for every e so one might at first hope that one could take the annihilators of suitable Ext's as a sort of "equidimensional decomposition" of an ideal. This is not the case: one may have

$$\bigcap_e \operatorname{ann} \operatorname{Ext}_S^e(S/I, S) \supsetneqq I.$$

as for example in the case $S = k[x, y]$, $I = (x^2, xy)$. It may be interesting to note that Eisenbud and Evans have shown that $\prod_e \operatorname{ann} \operatorname{Ext}_S^e(S/I, S)$ is contained in I.

Proof. 1) It is enough to prove the assertions after localizing at a prime of codimension e, so we may assume that S, P is regular local of dimension e. Let $M' \subset M$ be the largest submodule of finite length. From the short exact sequence $0 \to M' \to M \to M'' \to 0$ we get a long exact sequence ending with

$$\ldots \to \operatorname{Ext}_S^e(M'', S) \to \operatorname{Ext}_S^e(M, S) \to \operatorname{Ext}_S^e(M', S) \to 0$$

By the Auslander–Buchsbaum formula (see for example Matsumura 1986, Theorem 19.1),

$$\operatorname{Ext}_S^e(M'', S) = 0,$$

so

$$\operatorname{Ext}_S^e(M, S) \cong \operatorname{Ext}_S^e(M', S)\,.$$

Because $\operatorname{Ext}_S(-, S)$ is a functor, I_e, which is also the annihilator of $\operatorname{Ext}_S^c(M', S)$, contains the annihilator of M'. In particular, $\operatorname{codim} I_e \geqq e$. But since M' has finite length and S is regular, we have $M' = \operatorname{Ext}_S^e(\operatorname{Ext}_S^e(M', S), S)$. This follows immediately from the fact that the dual of an S-free resolution of M' is an S-free resolution of $\operatorname{Ext}_S^e(M', S)$. Applying the functoriality argument again, we see that I_e is actually equal to the annihilator of M'. Thus $(0:_M I_e) = M'$, proving the first statement. The second statement is a weaker form of the first.

2) and 3) Let c be the codimension of M (and thus of $I = \operatorname{ann} M$). For the proof of these parts, consider first the situation after we localize at a prime P of codimension c containing the annihilator of M. Since M_p has finite length and π is natural, the localized map

$$\pi_P : M_P \to \operatorname{Ext}^c_{S_P}(\operatorname{Ext}^c_{S_P}(M_P, S_P), S_P)$$

is an isomorphism and I_c is equal to the annihilator of M locally at P.

Next let $N \subset M$ be the equidimensional hull of 0, so that $\operatorname{codim} N$ ($= \operatorname{grade} N$) $> c$. Applying the long exact sequence in $\operatorname{Ext}_S(-, S)$, we see that the natural map

$$\operatorname{Ext}^c_S(M/N, S) \to \operatorname{Ext}^c_S(M, S)$$

is an isomorphism (see for example Matsumura 1986, Theorem 16.6 for the necessary vanishing theorem). Thus the right hand vertical map in the natural commutative diagram

$$\begin{array}{ccc} \pi : M & \to & \operatorname{Ext}^c_S(\operatorname{Ext}^c_S(M, S), S) \\ \downarrow & & \downarrow \\ \pi' : M/N & \to & \operatorname{Ext}^c_S(\operatorname{Ext}^c_S(M/N, S), S) \end{array}$$

is an isomorphism.

To prove 2) it now suffices to prove that the map labelled π' is a monomorphism. Since the associated primes of M/N are all of codimension c, it suffices to prove this after localizing at a prime P of codimension c. Since we know that $\pi'_P = \pi_P$ is an isomorphism, we are done.

We have already shown that I_c and ann M are equal locally at any c-codimensional prime. To complete the proof of 3) we must show that I_c has no associated primes of lower dimension. Since every associated prime of I_c is contained in an associated prime of $\operatorname{Ext}^c_S(M, S) = \operatorname{Ext}^c_S(M/N, S)$, it suffices to show that this latter module has no lower dimensional associated primes.

Let $x \in S$ be an element outside any of the c-codimensional associated primes of M. We must show that x is a nonzerodivisor on $\operatorname{Ext}^c_S(M/N, S)$. It follows from the definition of N that x is a nonzerodivisor on M/N. From the short exact sequence

$$0 \to M/N \xrightarrow{x} M/N \to M/(N + xM) \to 0$$

we derive the exact sequence

$$\ldots \to \operatorname{Ext}^c_S(M/(N + xM), S) \to \operatorname{Ext}^c_S(M/N, S) \xrightarrow{x} \operatorname{Ext}^c_S(M/N, S) \to \ldots .$$

But the codimension of $M/(N + xM)$ is $c + 1$, so the left hand term vanishes and we are done. □

Remark. 1) By the Auslander–Buchsbaum formula, $\operatorname{codim} \operatorname{Ext}^j_S(M, S) \geqq j$ for any module M.Thus a prime P as in the first part of the Theorem must be minimal over the annihilator of $\operatorname{Ext}^j_S(M, S)$.

2) Rather than use the annihilator of $\operatorname{Ext}^j_S(M, S)$ in part 1) of the Theorem, we could have used the ideal I_j which is generated by the $r_j \times r_j$ minors of the jth matrix, φ_j say, in a free resolution of M, where r_j is the rank of φ_j. The fact that this

works follows easily from the main result of Buchsbaum and Eisenbud (1973). This idea itself is probably not so practical, because the numbers r_j are often rather large. However, by the "first structure theorem" of Buchsbaum and Eisenbud (1974) one could also express this ideal as the ideal of minors of a submatrix of φ_j involving just r_j rows, divided by its greatest common divisor. This ideal can be computed as an annihilator without taking any determinants.

We may use Theorem 1.1 to find the equidimensional hull of an ideal, or to remove the components of dimension less than any given number. We express the result in the general case of modules:

Algorithm 1.2 (*Removing components of dimension* $< e$) Given a module M over $S = k[x_1, \ldots, x_n]$, and an integer e (normally taken $\geqq \dim M$) find a submodule N_e consisting of the intersection of the primary components of M of dimension $\geqq e$.

Set $f := \dim S$, and set $N := 0 \subset M$.

While $f > e$
{
Compute $\mathrm{Ext}^f(M, S)$;
If codim $\mathrm{Ext}^f(M, S) = f$, then set
$I_f := \text{annihilator } (\mathrm{Ext}^f(M, S))$;
$N := (N :_M I_f)$;
Decrement f;
(Optional: set $M := M/N$);
}
Return N.

The values of f in the While clause could in fact be done in any order, and the optional step could be performed some times but not others; this will strongly affect the efficiency in given cases. In practice (using Macaulay), it seems a good general rule to follow the order given, performing the optional step each time: Although not making the replacement allows one to use the originally computed resolution of M each time, the simplification in the resulting modules seems to repay the cost of computing more syzygies.

Algorithm 1.3 (*Equidimensional hull of an ideal*) Given $I \subset S = k[x_1, \ldots, x_n]$, find the ideal hull I consisting of the intersection of the primary components of I of maximal dimension.

$c := \text{codim } I$;
Return
$\text{ann } \mathrm{Ext}^c_S(S/I, S)$.

Of course we may compute the equidimensional hull of the support of any module M by replacing S/I by M in the second line above.

Algorithm 1.4 (*Equidimensional hull of 0 in a module*) Given a finitely generated module M over $S = k[x_1, \ldots, x_n]$, find the equidimensional kernel $N \subset M$.

$c := \text{codim } M$;
Return: $N = \text{kernel } M \to \mathrm{Ext}^c_S(\mathrm{Ext}^c_S(M, S), S)$, the kernel of the canonical map.

In practice the canonical map is computed by forming the comparison map between the dual of a free resolution of M and a free resolution of $\mathrm{Ext}_S^c(S/I, S)$. An alternative would be to construct a polynomial subring T of S such that $\dim T = \dim N$ and over which N is finitely generated (a Noether normalization for $S/\mathrm{ann}\, N$ will do) and then take the kernel of the natural map of N into its double dual over T. These two are actually extreme cases of a family of methods, one for each codimension . . . .

The following will be useful for purposes of localization:

Algorithm 1.5 (Associated primes of given codimension) Given a finitely generated module M over $S = k[x_1, \ldots, x_n]$, find an ideal whose associated primes are exactly the associated primes of S having codimension e.

$I_e :=$ ann $\mathrm{Ext}_S^e(M, S)$;
if codim $I_e > e$
  Return S;
else
  Return the equidimensional hull of I_e.

2 The radical of an ideal

In this section we present two methods for finding the radical of an ideal I in a polynomial ring S (the case of an ideal in a factor ring of S reduces immediately to this.) Actually we compute a little more: our formulas give the *equidimensional radical* which is the intersection of all the primes of maximal dimension containing I. Of course if I is equidimensional to begin with, then this is the same as the radical of I. In terms of the equidimensional radical and the ideas of Sect. 1 one can then compute for any module M the intersection of various sets of associated ideals of M, as outlined at the end of this section.

Our ideas revolve around the use of Jacobian ideals to replace the derivative in the usual formula for the square-free part of a univariate polynomial. As in the univariate case, extra care must be taken in characteristic p. We treat this case not for the sake of generality, but because the use of characteristic p is often necessary for efficient computation.

We begin by reviewing the definition of the Jacobian ideals:

Given any finitely generated k-algebra R (that is, an affine ring over k) there is a natural increasing sequence of ideals

$$0 \subset \mathscr{J}_0(R) \subset \mathscr{J}_1(R) \subset \ldots \subset R$$

which may be defined as follows: Choose a presentation

$$R = k[x_1, \ldots, x_n]/(f_1, \ldots, f_r)$$

or R as a k-algebra, and let $\mathscr{J}(f)$ be the *Jacobian matrix* of the sequence of relations $f = f_1, \ldots, f_r$; that is, $\mathscr{J}(f)$ is the $n \times r$ matrix having the partial derivative $\partial f_j/\partial x_i$ in the ith row and jth column. Write $\mathscr{J}_a(f)$ for the ideal of $(n-a) \times (n-a)$ minors (determinants of $(n-a) \times (n-a)$ submatrices) of $\mathscr{J}(f)$. Let I be the ideal generated by the f_i, and set $R = S/I$. Reducing $\mathscr{J}(f)$ modulo I, we

get a presentation matrix for the module of k-linear Kähler differentials $\Omega_{R/k}$ of R (Matsumura 1986, p. 192). Thus $\mathscr{J}_a(f)$ modulo I is the ath Fitting ideal of $\Omega_{R/k}$ as an R-module, an ideal of R which depends only on the isomorphism class of R, and not on the generators f chosen for I or the map from S (see for example the book of Kaplansky (1970) for a discussion of Fitting ideals.) We define

$$\mathscr{J}_a(R) = \mathscr{J}_a(f) \text{ modulo } I \ ,$$

and we set $\mathscr{J}_a(I) = \mathscr{J}_a(f) + I$, its preimage in S. Here $\mathscr{J}_n(R)$, the ideal of 0×0 minors, is the unit ideal, and we take $\mathscr{J}_a(R)$ to be the unit ideal for $a \geqq n$.

The formation of $\mathscr{J}_a(R)$ commutes with localization and change of base: that is, if R' is a localization of R then $\Omega_{R'/k} = R' \otimes_R \Omega_{R/k}$, so

$$\mathscr{J}_a(R') = \mathscr{J}_a(R)R' \ ,$$

while if k' is any k-algebra and $R' = k' \otimes_k R$ then $\Omega_{R'/k'} = R' \otimes_R \Omega_{R/k}$ so again

$$\mathscr{J}_a(R') = \mathscr{J}_a(R)R'$$

(see for example Matsumura 1986, exc. 25.4).

First, by way of notation, for any ideal K of a ring R, we write $\dim K$ for $\dim R/K$, and if $K = R$ is the unit ideal, we take $\dim K = -1$.

Our first method of finding the radical rests on the following result of Scheja and Storch (1975, Corollary 4.7) (see also the further references sketched in Eisenbud and Levine 1977, p. 34, and Kunz 1986, Example 3, p. 382): if S is a power series ring in c variables over a field k with maximal ideal P, and I is an ideal generated by a maximal regular sequence in P, then $\mathscr{J}_0(I)$, which is a principal ideal mod I, is $\dim_k S/I$ times the socle of S/I; that is,

$$(\dim_k S/I)(I : P) = \mathscr{J}_0(I) \ .$$

Suppose now that $(\dim_k S/I)$ is a unit in k, so that we may drop it from the formula above. By the definition of the socle,

$$(I : \mathscr{J}_0(I)) = P \ ,$$

that is,

$$(I : \mathscr{J}_0(I)) = \text{Radical}(I) \ .$$

The following Theorem generalizes this result to any ideal which is generically a complete intersection in an affine ring:

Theorem 2.1 *Let R be an equidimensional affine ring of dimension d over a field k with no embedded primes.*

If the characteristic of k is $p \neq 0$, suppose that R is (perhaps after a transcendental extension of the base field) a finitely generated module of rank $< p$ over a polynomial ring generated by sufficiently general linear forms.

If R is generically a complete intersection, then

$$\text{rad}(0) = (0 : \mathscr{J}_d(R)) \ .$$

Remarks. 1) If R is homogeneous, the main situation of interest, then the hypothesis given in characteristic $p > 0$ means that the degree of the corresponding projective variety is $< p$.

2) If $R = k[x_1, \ldots, x_{d+c}]/(f_1, \ldots, f_c)$ is a complete intersection, and $z_1, \ldots, z_d$ are linear forms in the x_i which are sufficiently general so that R is a finite module over $k[z_1, \ldots, z_d]$ (of rank $<$ char k if the characteristic is positive), then the argument below proves the following more precise result:

If

$$D := \det \partial(z_1, \ldots, z_d, f_1, \ldots f_c)/\partial(x_1, \ldots, x_{d+c})$$

then

$$\operatorname{rad}(f_1, \ldots, f_c) = ((f_1, \ldots, f_c) : D) .$$

One might call the element D thus constructed a *generic socle generator* for $(f_1, \ldots, f_c)$. There is at least one other expression for a generic socle generator: In the case of a complete intersection $J = (f_1, \ldots, f_n)$ of height n in $k[[x_1, \ldots, x_n]]$, if we write

$$f_i = \textstyle\sum_j a_{ij} x_j \quad \text{for } i = 1, \ldots, n ,$$

then $\det(a_{ij})$ is a socle generator (and thus a generic socle generator.) This is independent of characteristic, and in fact a suitable version works in any regular local ring (see for example Northcott 1963). But we do not know how to extend this formula beyond the artinian case. It would be interesting to know other formulas for generic socle generators.

Proof. By hypothesis, every associated prime of R is minimal. For any ideal J we have $\operatorname{rad}(0) = (0 : J)$ iff for every minimal prime P of R,

$$J_P \neq 0 ,$$

and

$$J_P P_P = 0 .$$

Thus to prove the theorem it suffices to show that

$$\operatorname{rad}(0) = (0 : J)$$

for any ideal J which is contained in $\mathcal{J}_d(R)$ and which contains a "sufficiently general" linear combination of the generators of $\mathcal{J}_d(R)$. Making a transcendental base field extension if necessary, we can even assume that k is infinite, and then it is enough for J to contain a general scalar linear combination of the generators of $\mathcal{J}_d(R)$.

Write $R = k[x_1, \ldots, x_n]/I$. By Noether normalization, R is a finite module over the polynomial ring $A := k[z_1, \ldots, z_d]$ for any sufficiently general linear forms z_i in the x_j. From the exact sequence of modules

$$R \otimes_A \Omega_{A/k} \to \Omega_{R/k} \to \Omega_{R/A} \to 0$$

we see that $J := F_0(\Omega_{R/A})$, the 0th Fitting ideal of $\Omega_{R/A}$, is contained in $\mathcal{J}_d(R)$ and contains a general linear combination of the generators of $\mathcal{J}_d(R)$. Thus it suffices to show that

$$(*) \qquad \operatorname{rad}(0) = (0 : F_0(\Omega_{R/A})) .$$

Since R is integral over A, the primes of R contracting to 0 in A are precisely the minimal primes. Thus every nonzero element of A is a nonzerodivisor on R and on $R/\mathrm{rad}(0)$, and, by Lemma 2.4 below, on $R/(0:F_0(\Omega_{R/A}))$. Since the definition of $F_0(\Omega_{R/A})$ commutes with localization, it suffices to prove (*) after inverting all nonzero elements of A, that is, after tensoring with the quotient field K of A. Writing $R' = K \otimes_A R$ we have $K \otimes_A \Omega_{R/A} = \Omega_{R'/K}$ and thus

$$\begin{aligned} K \otimes_A F_0(\Omega_{R/A}) &= F_0(K \otimes_A \Omega_{R/A}) \\ &= F_0(\Omega_{R'/K}) . \end{aligned}$$

It now suffices to show that in R',

$$\mathrm{rad}(0) = (0:F_0(\Omega_{R'/K})) .$$

As this is a local statement, we may (after inverting one element) assume R' is local, with maximal ideal P, say. Of course the old $F_0(\Omega_{R'/K})$ localizes to the 0th Fitting ideal of the new $\Omega_{R'/K}$.

It follows from our hypothesis that $\dim_K R' < \mathrm{char}\, K$ if $\mathrm{char}\, K$ is positive, so $K \subset R'/P$ is a separable field extension. By the Cohen Structure Theorem (see for example Matsumura 1986, Theorem 28.3) we may find a field of representatives $K' \subset R'$ which contains K and maps onto R'/P. From the exact sequence

$$R' \otimes_{K'} \Omega_{K'/K} \to \Omega_{R'/K} \to \Omega_{R'/K'} \to 0$$

and the fact that $\Omega_{K'/K} = 0$ it follows that

$$F_0(\Omega_{R'/K}) = F_0(\Omega_{R'/K'}) ,$$

so it will be enough to prove that in R',

$$\mathrm{rad}(0) = (0:F_0(\Omega_{R'/K'})) .$$

We may now write $R' = K'[[y_1, \ldots, y_m]]/J'$ for suitable generators y_i of P and some ideal J'. It follows by Avramov (1977, Proposition 3.8) that J' is a complete intersection, and thus $F_0(\Omega_{R'/K'})$ is a principal ideal, generated by the Jacobian determinant D of the m generators of J with respect to the y_i.

By Scheja and Storch (1975, 1.2 and 4.7)

$$(D) = (\dim_{K'} R')(0:(y_1, \ldots, y_m)) \text{ in } R' .$$

Under our assumption $\dim_{K'} R'$ is a unit, so

$$(D) = (0:(y_1, \ldots, y_m)) \text{ in } R' ,$$

whence

$$(0:D) = (y_1, \ldots, y_m) = \mathrm{rad}(0)$$

as required. □

Algorithm 2.2 (*Radical of a generically complete intersection*) Given an unmixed ideal $J = (f_1, \ldots, f_m) \subset k[x_1, \ldots, x_n]$ of pure codimension c which is known to be generically a complete intersection:

Set

J_{n-c}:= the ideal of $c \times c$ minors of the Jacobian matrix

$\partial(z_1, \ldots, z_d, f_1, \ldots, f_m)/\partial(x_1, \ldots, x_n)$, where $z_1, \ldots, z_d$ are general linear forms.

Return
rad $J := (J : J_{n-c})$.

Theorem 2.1 can be applied to find the radical of an ideal which is not generically a complete intersection because of the following result.

Proposition 2.3 *If $J \subset I \subset S = k[x_1, \ldots, x_n]$ are ideals of the same dimension, and J is equidimensional with radical J', then the equidimensional hull of the radical of I is given by the formula*

$$\text{equidimensional radical } I = (J' : (J' : I)) .$$

The proposition is proved by twice applying the last statement of the following easy but extremely useful lemma:

Lemma 2.4. *If J is an ideal in a noetherian ring R and M is a finitely generated R-module, then*

a) $(0 :_M J^\infty)$ *is the intersection of the primary components of* 0 *in M whose associated primes do not contain J.*

b) $\operatorname{Min} M \cap \operatorname{Supp} JM \subset \operatorname{Ass}(0 :_M J) \subset \operatorname{Ass} M \cap \operatorname{Supp} JM$,

where $\operatorname{Min} M$ *is the set of minimal associated primes of M. Further, given a primary decomposition of* 0 *in M, there is a primary decomposition of $(0 :_M J)$ for which each primary component contains the corresponding primary component of* 0.

c) *In particular, if I is a radical ideal, then $(I : J)$ is radical and*

$$(I : J) = \bigcap P_j ,$$

where P_j ranges over all primes containing I but not containing J.

Proof of 2.4. Let $0 = \bigcap Q_j$ be a primary decomposition of 0 in M, with Q_j a P_j-primary submodule of M. It is easy to see that

$$(0 :_M J) = \bigcap (Q_j :_M J) ,$$

and

$$(0 :_M J^\infty) = \bigcap (Q_j :_M J^\infty) .$$

It follows at once from the definitions that $(Q_j :_M J)$ and $(Q_j :_M J^\infty)$ are each P_j-primary submodules if they are proper. Thus in each case, we get a primary decomposition by throwing out unnecessary components.

To prove part a), note that

$$(Q_j : J) = (Q_j : J^\infty) = Q_j \quad \text{if } J \not\subset P_j$$

while

$$(Q_j : J^\infty) = R \text{ if } J \subset P_j .$$

To prove part b), suppose first that $P_j \in \operatorname{Min} M \cap \operatorname{Supp} JM$. We must have $P_j \in \operatorname{Supp} JM/Q_j$, since $JM_{P_j} = (JM/Q_j)_{P_j}$. Thus $(Q_j :_M J) \neq M$ so it is a P_j-primary submodule. By the minimality of P_j, $(Q_j :_M J)$ cannot be left out of the primary decomposition of $(0 :_M J)$. Thus P_j is associated to $(0 :_M J)$, proving the first inequality.

To prove the second inequality, note first that $\mathrm{Ass}(0:_M J) \subset \mathrm{Ass}\, M$ is obvious, and it suffices to show $\mathrm{Ass}(0:_M J) \subset \mathrm{Supp}\, JM$. Suppose that P_j is not in the support of JM. It follows that P_j is not in the support of JM/Q_j, so that $(Q_j:_M JM)$ is not proper. In this case $(Q_j:_M JM)$ may certainly be deleted from the decomposition, and P_j is not associated to $(0:_M JM)$. This completes the proof of b). Part c) follows at once from part b). □

Algorithm 2.5 (*Reduction of equidimensional radical to complete intersection case*) Given ideals $J \subset I \subset k[x_1, \ldots, x_n]$, where J is known to be a complete intersection and I and J both have the same codimension, compute the equidimensional hull of the radical of I:

Compute
  $J' := \mathrm{rad}\, J$
by Algorithm 2.2.
Return
  equidimensional radical $I := (J':(J':I))$.

To go further, we use the relation of Fitting ideals to smoothness. This is relevant to radicals because of the observation that a variety is generically reduced iff it is generically nonsingular; more precisely, Serre observed that an affine ring is reduced iff an ideal defining the singular locus (under favorable circumstances this may be taken to be a certain Jacobian ideal) contains a nonzerodivisor.

Suppose again that R is an affine ring over k, and let P be a prime of R. By the general properties of Fitting ideals (see for example Eisenbud 1989).

$$\mathscr{J}_{d-1}(R)_P = 0 \text{ while } \mathscr{J}_d(R) \not\subset P$$

iff

$$(\Omega_{R/k})_P \text{ is a free } R_P\text{-module of rank } d\,.$$

On the other hand, the local freeness of $\Omega_{R/k}$ characterizes the smoothness of R over k in most of the cases in which we are interested. If k is perfect, then the well-known Jacobian criterion (see for example Hartshorne 1977, Theorem II.8.8) says that R is smooth generically along P iff $(\Omega_{R/k})_P$ is free *of rank equal to the dimension of R along P* (here the dimension of R along P means the maximal dimension of a minimal prime contained in P). We need a version which operates without *the condition.* In characteristic 0 the appropriate result was proved by Grothendieck, but in positive characteristic it appears to be new:

Lemma 2.6 *If R is an affine ring over k, $P \subset R$ is a prime and $(\Omega_{R/k})_P$ is a free R_P – module of rank d, then R is smooth over k generically along P, necessarily of dimension d, if one of the following conditions holds*:

a) (Grothendieck 1967: EGA, Chap. 4, 17.15.7) $\mathrm{char}\, k = 0$.

b) *k is perpect of characteristic $p > 0$, and the nilpotent radical $\mathrm{rad}(0)$ of R is generated by elements whose index of nilpotency is $< p$.*

Proof of b). Replacing R by $R[g^{-1}]$ for a suitable element $g \notin P$ we may assume that $\Omega_{R/k}$ is free of rank d. We will show under this hypothesis that R is smooth. By the Jacobian criterion, we will be done as soon as we have shown that R is of dimension d.

Let Q be a minimal prime of R. Inverting another element if necessary, we may assume that Q is the only associated prime of R; this does not change the dimension of R/Q because R is affine. Set $S := R/Q$. We have

$$\Omega_{S/k} = \Omega_{R/k}/(\mathrm{d}(Q) + Q\Omega_{R/k}) .$$

Let $f \in Q$ be an element whose index of nilpotence is $n < p$. Differentiating $f^n = 0$ we get $nf^{n-1}\,df = 0$; since $n < p$, we get $f^{n-1}\,df = 0$ in $\Omega_{R/k}$. Since $\Omega_{R/k}$ is a free R-module, and Q is the only associated prime, we must have $df \in Q\Omega_{R/k}$. Under our hypotheses, Q will be generated by elements whose index of nilpotence is $< p$, so we have $d(Q) \subset Q\Omega_{R/k}$. It follows that

$$\Omega_{S/k} = \Omega_{R/k}/Q\Omega_{R/k} ,$$

and is thus free of rank d over S. As S is a domain, its dimension is the transcendence degree of its quotient field K over k. Since k is perfect, this transcendence degree is equal to $\dim_K \Omega_{K/k}$. As $\Omega_{R/k} = \Omega_{R/k} \otimes_R K$, the dimension is d as claimed. □

Our second method for computation of the radical is based on:

Theorem 2.7. *Let S be a polynomial ring over a perfect field k, and let $I \subset S$ be an ideal of dimension d. If the characteristic of k is not zero, suppose that the nil radical of S/I is generated by elements whose index of nilpotency is $<$ the characteristic of k. If for some integer $a \geqq d$ we have*

$$\dim \mathscr{J}_{a+1}(I) < d$$

then

$$I_1 := (I : \mathscr{J}_a(I))$$

has the same equidimensional radical as I. Further, if $a = d$ then I_1 is radical in dimension d; that is, the primary components of I_1 having dimension d are prime.

Remark. The condition on index of nilpotency is really required in characteristic p; for example, $R = k[x]/(x^p)$ has $\Omega_{R/k} = R$, and thus $\mathscr{J}_0(x^p) = 0$ while $\mathscr{J}_1(R) = R$, though the dimension of R is 0.

The theorem DOES NOT imply that under its hypothesis

$$(I : \mathscr{J}_a(I)^\infty) := (\ldots((I : \mathscr{J}_a(I)) : \mathscr{J}_a(I))\ldots)$$

has the same equidimensional radical as I, and indeed *this need not hold.* For example, consider the case $S = k[x, y] \supset I = (x, y)^2$, so that $d = 0$. Taking $a = 1$, we have $\mathscr{J}_2(I) = R$, but $\mathscr{J}_1(I) = (x, y)$, so that

$$(I : \mathscr{J}_1(I)^\infty) = R .$$

Instead, the theorem DOES imply that, with a as in the hypothesis of the Theorem, if we inductively define

$$K_1 = I ,$$

$$K_{n+1} = (K_n : \mathscr{J}_a(K_n)) ,$$

then all of the K_n have the same equidimensional radical. In the example above for instance, $K_2 = (x, y)$, $\mathcal{J}_1(K_2) = R$, so that

$$(x, y) = K_2 = K_3 = \ldots ,$$

and this is indeed the radical of I; that is,

$$(\ldots((I : \mathcal{J}_a(I)) : \mathcal{J}_a((I : \mathcal{J}_a(I)))) : \ldots)$$

has the same equidimensional radical as I.

The following is a formal consequence of Theorem 2.7 (or one can check that the same proof works):

Corollary 2.8 *Theorem* 2.7 *continues to hold if the ideals* $\mathcal{J}_a(I)$ *are replaced by any other ideals* $\mathcal{J}'_a(I)$ *such that*

$$\mathcal{J}_a(I) \subset \mathcal{J}'_a(I) \subset \text{radical } \mathcal{J}_a(I) . \quad \square$$

An interesting candidate for $\mathcal{J}'_a(I)$ may be provided as follows: If $f = (f_1, \ldots, f_g)$ is a set of generators for I, and $\mathcal{J}(f) : S^g \to S^n$ the corresponding matrix, then it is not hard to show (see for example Eisenbud and Buchsbaum 1977) that

$$\mathcal{J}_a(f) \subset \text{annihilator } \wedge^{a+1} \text{coker } \mathcal{J}(f) \subset \text{radical } \mathcal{J}_a(f) .$$

Thus the ideals $\mathcal{J}'_a(I) = I + \text{annihilator}(\wedge^{a+1} \text{coker } \mathcal{J}(f))$ may be used in Corollary 2.3. The potential advantage of this is that the annihilator of a module can be computed from a presentation matrix using standard basis techniques without taking any determinants; the presentation matrix for $\wedge^{a+1} \text{coker } \mathcal{J}(f)$ has entries that are linear forms in the entries of the matrix $\mathcal{J}(f)$, and is rather easy to write down.

Proof of Theorem 2.7. Suppose that $\dim \mathcal{J}_{a+1}(I) < d$. To check that I_1 has the same equidimensional radical as I, it is enough to check that for each prime $P \supset I$ of dimension d we have

$$(I : \mathcal{J}_a(I)) \subset P ,$$

or equivalently that $\mathcal{J}_a(I)_P \not\subset I_P$. In the contrary case, taking $R = S/I$, Lemma 2.6 yields $\dim R/P = a + 1 > d$, contradicting our hypothesis. This completes the proof of the first statement of the Theorem.

We must now show that if $a = d$ and $I_1 = I$, then I is radical in dimension d. Equivalently, if U is the open set of Spec S/I obtained by removing components of dimension $< d$, we must show that U is reduced.

The ideal $\mathcal{J}_d(I)$ defines the singular locus of U. Since

$$I_1 = (I : \mathcal{J}_d(I)) = I ,$$

$\mathcal{J}_d(I)$ contains a nonzerodivisor modulo I. Thus for any prime

$$Q \in \text{Sing } U ,$$

we have

$$\text{depth}(S/I)_Q \geqq 1 .$$

It follows that U satisfies Serre's conditions R_0 and S_1. By Serre's Criterion (Matsumura 1970, p. 125) U is reduced as required. $\square$

Here is the algorithm for finding the radical of an equidimensional ideal corresponding to Theorem 2.7:

Algorithm 2.9 (*Equidimensional Radical*) Given an equidimensional ideal $I \subset S = k[x_1, \ldots, x_n]$, find the equidimensional radical U of I, equal to the intersection of all primes containing I whose dimension is the same as the dimension of I.

$a := n - 1$.
$d := \dim I$

While $a > d$
{
While $\dim \mathscr{J}_a(I) = d$
$I := (I : \mathscr{J}_a(I))$;
decrement a;
}
$I := (I : \mathscr{J}_d(I))$;

Return I.

Here the order of the steps is crucial!

In terms of the algorithms above we can now compute the following fundamental invariants of any module:

Algorithm 2.10 (*Find the intersection of the primes associated to M having dimension e*)

$I_e := \operatorname{ann} \operatorname{Ext}_S^e(M, S)$.
If $\operatorname{codim} I_e = e$,
Return the radical of the equidimensional hull of I_e;
Else
Return S.

Alternately, with J_e as in Algorithm 1.2, the radical of the ideal $(J_e : J_{e+1})$ is by Lemma 2.4 the intersection of the primes of dimension d which are associated to I.

Algorithm 2.11 (*Find the intersection of the minimal primes of M having dimension e*)

Compute the ideals J_e and J_{e+1} using Algorithm 1.2.
Return $(\operatorname{rad} J_e : J_{e+1})$.

This gives the correct answer by Lemma 2.4.

Algorithm 2.12 (*Find the intersection of the embedded primes of M having dimension e*)

Let K_1 be the ideal output by Algorithm 2.10;
Let K_2 be the ideal output by Algorithm 2.11;
Return $(K_1 : K_2)$

Of course the support of M, that is the radical of $I := \operatorname{ann} M$, which is the intersection of all the primes containing I, may then be obtained by intersecting the ideals found in A) (or for that matter B) for various dimensions.

3 Localization

In this section we show how, given an affine ring S, an ideal $J \subset S$, and a finitely generated S-module and submodule $A \subset B$, to compute the *localization* $A_{[J]}$ defined by

$$A_{[J]} = \{b \in B \mid \dim(J + (A:b)) < \dim J\} ,$$

where we have written $(A:b)$ for the annihilator of b in B/A. If J is a prime ideal, we can even write this as $A_{[J]} = \{b \in B \mid (A:b) \not\subset J\}$. Note that this definition depends on B, although B does not appear in the notation.

In the case where J is a prime, $A_{[J]}$ is the preimage of the usual localization $A_J \subset B_J$ under the canonical map $B \to B_J$. The same goes for arbitrary J if we define B_J to be the semilocalization of B at the equidimensional radical of J.

Of course the localization at J is the same as the localization at the equidimensional radical of J. We have stated the definition in the case where J need not be prime, or even radical, for practical reasons: one often has an ideal J of which one knows only that it defines a locus at which one would like to localize. Our construction will work directly with a given ideal J, without the need to compute its equidimensional radical.

The leading special case of the localization problem is the case of an ideal I in S. We will handle this case separately, and reduce the case of arbitrary modules to it by using Algorithms 2.10–2.12.

It is of course easy to test whether a given element is in $A_{[J]}$:

Algorithm 3.1 (Test for membership in $A_{[J]}$) Given I, J ideals in $S = k[x_1, \ldots, x_n]$, and an element b test whether $b \in I_{[J]}$.

$c := \operatorname{codim} J$;
$c' := \operatorname{codim} J + (I:b)$;
if $c < c'$ then $f \in I_{[J]}$; else not.

Finding such elements is much harder. Our technique is based on the following, which expresses the localization in terms of equidimensional hulls:

Proposition 3.2 With notation as above,

$$A_{[J]} = \bigcap_{m=1}^{\infty} \operatorname{hull}(A + J^m B) .$$

Proof. Factoring out A if necessary, we may assume that $A = 0$; this will simplify the notation. Since the $\operatorname{rad} J$ acts nilpotently on $B/J^m B$, the primes of dimension equal to the dimension of J in the primary decomposition of $J^m B$ are all among the primes of that dimension containing J; thus $(J^m B)_{[J]} = \operatorname{hull} J^m B$, so

$$0_{[J]} \subset \bigcap_{m=1}^{\infty} \operatorname{hull} J^m B .$$

To prove the other inequality we must show that any element in $\bigcap_{m=1}^{\infty} \operatorname{hull} J^m B$ is mapped to 0 in the (semi-) localization B_J of B at the set of primes containing J and having the same dimension as J. As J is contained in the Jacobson radical of S_J,

and B_J is a finitely generated S_J-module, the Krull Intersection Theorem (see for example Matsumura 1986, Theorem 8.10) gives

$$0 = \bigcap_m J^m B_J ,$$

as required. □

The ungraded case of localization is easily reduced to the graded one by homogenizing, and the case where S is a factor ring of $k[x_1, \ldots, x_n]$ is easily reduced to the case $S = k[x_1, \ldots, x_n]$ so *we will henceforward assume that J is a homogeneous ideal of $S = k[x_1, \ldots, x_n]$, and that all modules and elements discussed are homogeneous.*

We will now take up the case where B is the ring S and A is an ideal, which we will rename I. By way of notation, we write $\deg I$ for the degree of the projective variety in $\mathbb{P}^{n-1}$ corresponding to I. In general, for any local ring R, we will write $e(R)$ for the multiplicity of R, so that $\deg I = e(S/I)_{(x_1, \ldots, x_n)}$.

To make computational use of Proposition 3.2 we need first to be able to say that if an element $b \in S$ is in the equidimensional part of some $I + J^m$, then under some extra hypothesis b is actually in $I_{[J]}$. It turns out in our homogeneous setting that it is enough to assume that the degree of b is not too big compared to m:

Theorem 3.3. *Suppose I is an equidimensional radical ideal. If*

$$b \in \operatorname{hull}(I + J^m)$$

and b has degree $< m/(\deg I)$, then

$$b \in I_{[J]} .$$

If J is prime, then it is enough to take the degree of b

$$< m\, e((S/I)_J)/(\deg I) .$$

Remarks. 1) It follows from the theorem that we could use any ideal $J_m \subset J^m$ whose radical is J in place of J^m. The ideal generated by the mth powers of a given set of generators of J is often a very convenient choice for computation.

2) Nagata (1962 p. 143) and Zariski (see Hironaka 1964, Theorem 1) provided Theorem 3.3 in the case where S/I is replaced by a regular local ring. The case of general domains is studied by Hochster (1971).

3) For an example where the given bound on the degree of b is sharp, consider $I = (x^{d-1}y - z^d) \subset k[x, y, z]$, an ideal of degree d, and let $J = (y, z)$. It is easy to see that $I \subset J$ and that $e((S/I)_J) = 1$ (so the two given bounds are the same). Further,

$$y \in \operatorname{hull}(I + J^d)$$

since x^{d-1} annihilates y modulo $I + J^d$. Thus

$$y^n \in \operatorname{hull}(I + J^{dn})$$

for every n.

4) Despite examples as in 3), the primes for which the given bound is sharp must be rather rare. It would be quite interesting to have a method for computing, given I and J, a better ratio than $e((S/I)_J)/(\deg I)$. We do not know of any finite computation of the minimal number r such that if

$$b \in \operatorname{hull}(I + J^m)$$

and b has degree $\leqq m/r$, then

$$b \in I_{[J]} .$$

Proof. Replacing J by a prime containing it and having the same dimension, we may assume that J is prime. Replacing S by the homogeneous affine ring $R := S/I_{[J]}$, we may assume $I_{[J]} = 0$. We will regard J as a prime of R. The ideal

$$(\text{hull}(I + J^m))/I_{[J]} \subset R$$

is then nothing but the mth symbolic power $J^{(m)}$ of J (that is, the J-primary component of J^m). Let $\mathfrak{M} = (x_1, \ldots, x_n)$ be the maximal ideal of R. The statement of the theorem will follow if we show that the nonzero homogeneous elements of $J^{(m)}$ have degree $\geqq me(R_J)/e(R_{\mathfrak{M}})$.

If $\dim J = \dim R$, then under our hypotheses J would be 0 and the result obvious, so writing $P_1, \ldots, P_t$ for the minimal primes, we may assume that J is not in any P_i. To prove that $J^{(m)} \subset \mathfrak{M}^s$, it then suffices to show that $J^{(m)} \subset \mathfrak{M}^s \cup P_1 \cup \ldots \cup P_t$; equivalently, it is enough to show that each homogeneous nonzerodivisor $b \in J^{(m)}$ has degree $\geqq me(R_J)/e(R_{\mathfrak{M}})$.

We will do this by computing multiplicities. If b has degree d, then since R is graded and b is a nonzerodivisor we have

$$de(R_{\mathfrak{M}}) = e(R_{\mathfrak{M}}/(b)) \geqq e(R_J/(b)),$$

the first equality by Bezout's Theorem (see for example Hartshorne 1977, Theorem 1.7.7). Note that we really need homogeneity here; the inequality that holds in the inhomogeneous case goes the wrong way!) and the second by the semicontinuity of multiplicity (Nagata 1962, 40.1).

On the other hand, by Lech's formula (see for example Matsumura 1986, Theorem 14.12), if $\dim R_J = u$ and $(y_1, \ldots, y_{u-1})$ is a minimal reduction of the maximal ideal $J_J \subset R_J/(b)$, then

$$e(R_J/(b)) = \lim_{i \to \infty} \{\text{length } R_J/(b, y_1^i, \ldots, y_{u-1}^i)\}/i^{u-1}$$

which by (Matsumura 1986, Theorem 14.9) is

$$\geqq e(R_J)mi^{u-1}/i^{u-1} = e(R_J)m ,$$

so $d \geqq m\ e(R_J)/e(R_{\mathfrak{M}})$ as claimed. □

Next, we would like a bound on the degrees of generators of $I_{[J]}$ in terms of computable information about I. In general the degrees involved will be too large for practical use. However, if I is radical and equidimensional of degree d then we will show that $I_{[J]}$ is generated "set theoretically" in degrees $\leqq d$, and, and using our ability to compute radicals and equidimensional parts by the techniques of the last sections, we can make do with this information.

First we show how to reduce to the case of equidimensional radical ideals. Note that the ideals I'_e which are used can be computed in our case by Algorithm 2.10:

Proposition 3.4 *Let $J \subset S$ be an ideal in a Noetherian ring, let $A \subset B$ be S-modules, and let I'_e be the intersection of all the associated primes of B/A having codimension exactly e. If we set*

$$K := \bigcap_e (I'_e : (I'_e)_J)$$

then

$$A_{[J]} = (A : K^{\infty}) .$$

Proof. By Lemma 2.4 part b) the ideal $K_e := (I'_e : (I'_e)_J)$ is the intersection of those associated primes of B/A having codimension e and not contained in a prime containing J and having the same dimension as J. Thus $K = \bigcap_e K_e$ is an ideal contained in all such associated primes of B/A, but not contained in any associated prime which is contained in a prime containing J and having the same dimension as J. By part c) of Lemma 2.4,

$$(A : K_e^{\infty})$$

is the result of removing all the corresponding primary components from A, and is thus equal to $A_{[J]}$. □

Next we give the degree bound necessary to handle the case of an equidimensional radical homogeneous ideal.

Proposition 3.5 *If k is a perfect field and $I \subset k[x_1, \ldots, x_n]$ is a homogeneous equidimensional radical ideal then I is generated up to radical by forms of degree $\leqq \deg I$.*

Remarks. This is in general best possible: if I is the ideal of the union X of d skew lines in $\mathbb{P}^n$, all meeting a common line $L \not\subset X$, then L is in every $(d-1)$-ic hypersurface containing X. However, if there are fewer than $d = \deg I$ components then a better result should hold. For example, it is a plausible conjecture, known for $\dim I = 2$, that if I is a prime, then I is generated (as an ideal) by forms of degree $\leqq \deg I - \operatorname{codim} I + 1$. This is sharp, even up to radical, as one sees from the example of a rational curve of degree d lying on a rational normal scroll of type $1, n-2$ in $\mathbb{P}^n$ and intersecting the directrix of the scroll $d-1$ times. This curve has degree $n+d-2$ and cannot be cut out set theoretically by $(d-1)$-ics for the same reason as above.

The result has been known for a long time; it is used (and proved) for example in Mumford (1969, Theorem 1); because that publication is somewhat hard to obtain, we give the proof:

Proof. Extending k if necessary, we may assume k algebraically closed; I remains equidimensional in such an extension and, since k is perfect, I remains radical. Let $X \subset \mathbb{P}^{n-1}$ be the corresponding variety. We must show that if $y \in \mathbb{P}^{n-1} - X$, then there is a hypersurface of degree $d := \deg X$ containing X but not y.

If X is a hypersurface of degree d, then the result is obvious. In the contrary case where X has codimension > 1, write m for the dimension of X. Let $\operatorname{join}(X, y)$ be the union of all the lines connecting y to points of X. Since $\dim \operatorname{join}(X, y) = m+1$, it is a proper subvariety of $\mathbb{P}^{n-1}$. Let z be a point of $\mathbb{P}^{n-1} - \operatorname{join}(X, y)$, and let

$$\pi_z : \mathbb{P}^{n-1} - \{z\} \to \mathbb{P}^{n-2}$$

be the projection map. By our choice of z,

$$\pi_z(y) \notin \pi_z(X) .$$

Further, $\deg \pi_z(X) \leqq \deg X$, so by induction on n there is a hypersurface H of degreee d in $\mathbb{P}^{n-2}$ containing $\pi_z(X)$ but not $\pi_z(y)$. The cone over H with vertex z is a hypersurface in $\mathbb{P}^{n-1}$ with the desired property. □

We can now give our algorithms for localization; their correctness follows from the results of this section:

Algorithm 3.6 (localization of a homogeneous equidimensional radical ideal) Given homogeneous ideals $I, J \subset k[x_1, \ldots, x_n]$, with I assumed radical and equidimensional, compute $I_{[J]}$.

$d := \deg I$
$I_1 := \text{hull}(I + J^{d(d+1)})$
$I_2 :=$ the ideal generated by the generators of I_1 with degree $\leqq d$
$I_3 := \text{hull}\, I_2$
Return $\text{rad}\, I_3$.

Remarks. 1) In practice, a much lower power of J than $J^{d(d+1)}$ will usually be sufficient. Thus one could begin with a lower power, say e, of order about d say, and choose some element b of degree d in

$$I_1 := \text{hull}(I + J^e) .$$

Using Algorithm 3.1 one would check to see whether $b \in I_{[J]}$. If so, adjoin it to I, replace (I, b) by its equidimensional radical, and start the whole process again. If not, one would proceed to the next power, J^{e+1}, and so forth. The advantage of this is that the degree of the new ideal (I, b) will be $< \deg I$. Unfortunately, we do not have an efficient way to tell when $I = I_{[J]}$ without going to high degree, so this method does nothing useful, for example, in the case where I happens to be equal to $I_{[J]}$ at the start.

2) To compute $\text{hull}(I + J^{d(d+1)})$ one could also compute $K := \text{hull}(I + J^{d+1})$, and then

$$\text{hull}(I + J^{d(d+1)}) = \text{hull}\, I + K^d .$$

One could further divide the work into more smaller steps. One might also use powers of the given generators of J instead of the powers of J. If J is known to be prime, then by the last statement of Theorem 3.3 we can use a smaller power than $d(d+1)$, as well. It would be useful to make an experimental comparison of these options.

3) At least when J is prime one can replace $d(d+1)$ in the algorithm above by $d(d-1)/e(k[x_1, \ldots, x_n]_J/I_J)$. The reason for the change from $d(d+1)$ to $d(d-1)$ is that if $I \neq I_{[J]}$ then $\deg I_{[J]} \leqq d - 1$. See Theorem 3.3 for the division by the multiplicity $e(k[x_1, \ldots, x_n]_J/I_J)$.

Algorithm 3.7 (localization of a submodule, graded case) Given a homogeneous ideal $J \subset S := k[x_1, \ldots, x_n]$, and finitely generated graded S-modules $A \subset B$, compute $A_{[J]}$.

Using Algorithm 2.10 to compute for each $e = \text{codim}\, B/A, \ldots, n$ the ideal I'_e which is the intersection of the associated primes of B/A having codimension e;

Using Algorithm 3.6, compute the ideals
  $I''_e := (I'_e)_{[J]}$
and the ideals
  $I'''_e := (I'_e : I''_e)$;
Set
  $K := \bigcap_e I'''_e$;
Return
  $A_{[J]} := (A :_M K^\infty)$.

Remark. In some cases it might be preferable to remove the unwanted components dimension by dimension. Letting I'''_e be as above, we would then do:

  $c :=$ codim A;
  $A_{n+1} := A$;
  For e from n down to c
    $A_e := (A_{e+1} : I'''^\infty_e)$;
  Return A_c.

Algorithm 3.8 (*localization of an arbitrary submodule*) Given an ideal $J \subset S := k[x_1, \ldots, x_n]$, and finitely generated S-modules $A \subset B$, compute $A_{[J]}$.

Homogenize
  J, A, and B
with respect to a new variable x_0 to get
  $\tilde{J}$, $\tilde{A}$, $\tilde{B}$;
Remove all extraneous components by the replacements
  $\tilde{J} := (\tilde{J} : x_0^\infty)$
  $\tilde{A} := (\tilde{A} : x_0^\infty)$;
  $\tilde{B} := (\tilde{B} : x_0^\infty)$;
Compute
  $\tilde{A}_{[\tilde{J}]}$;
Set x_0 to 1 in the generators of $\tilde{A}_{[\tilde{J}]}$ to get $A_{[J]}$.

4 Primary decomposition

It is of interest to know that the techniques introduced above, together with a technique for finding a maximal ideal containing a given ideal, suffice for finding primary decompositions. Since our method is not as yet very practical, we only sketch how this can be done. This discussion owes some ideas to conversations with Bayer and Stillman.

We may divide the process of finding a primary decomposition for an ideal I in a ring S into two parts: First, find the individual associated primes; second, given an associated prime, find a primary component for that associated prime.

The second part of this problem is rather easy, given the techniques developed above: A primary component for I with associated prime P may be taken as any ideal of the form

$$Q_m := \text{equidimensional part } (I + P^m)$$

for sufficiently large m (of course this is uniquely defined only when P is a minimal prime of I. Note that Q_m is in any case a P-primary ideal. Bounds for the m required can probably be given directly, but for practical computation it is almost certainly

better to guess and then check that m is in fact large enough, by the following criterion:

Let Q be a P-primary ideal containing I. Q is a primary component for I iff the natural map

$$(I_{[P]}: P^\infty)/I_{[P]} \to S/Q$$

is a monomorphism.

Thus it only remains to find the associated primes of I (and this is often the most interesting part of the information of primary decomposition anyway.) We may of course assume that S is a polynomial ring. Because we can already find the intersection of all the associated primes of a given dimension (computation A, at the beginning of Sect. 2) it is enough to find the individual components of an equidimensional radical ideal I. Using a reduction as in Algorithm 3.8, we may assume that I is a homogeneous ideal, as well. Of course finding the prime components of I is equivalent to finding the minimal primes of the ring $R := S/I$.

We begin by computing the integral closure R' of $R := S/I$,using for example the method of Vasconcelos (1991) (see also Brennan and Vasconcelos 1992). As presented, this is not a "direct" method in our sense; it uses a Noether normalization $T := k[z_1, \ldots, z_d] \subset R$ to compute the "S_2-ification"

$$R'' := \mathrm{Hom}_T(\mathrm{Hom}_T(R, T), T).$$

However, it follows from duality theory that there is also a direct method for finding this: it is given by

$$R'' = \mathrm{Ext}_S^c(\mathrm{Ext}_S^c(R, S)S),$$

where c is the codimension of I.

The minimal primes of R are the intersections of R with the minimal primes of R', so it suffices to find the minimal primes of a reduced integrally closed graded ring.

Any integrally closed ring is a product of integral domains (see Matsumura (1986, p. 64). Thus the minimal primes of R' are in one to one correspondence with the idempotents of R'. From the equation $e^2 = e$ we see that any idempotent must have degree 0; thus the idempotents lie in the finite dimensional algebra $A := R'_0$. The indecomposable idempotents generate the minimal ideals of A. These can be found directly, without computing the idempotents, as the intersections of all but one of the finitely may maximal ideals of A. Given a minimal ideal $\mathcal{N}$ of A, we may recover the corresponding prime of R' by choosing any nonzero element $g \in \mathcal{N}$ and computing

$$P := (0: g^\infty) \text{ in } R'.$$

To complete the methods needed for primary decomposition, it remains to give a method for finding the maximal ideals of a finite dimensional k-algebra $A = k[x_1, \ldots, x_r]/I$ – which is of course a special case of the original primary decomposition problem. A sophisticated recent approach to this is given by Lazard (1992). Here we mention a probabilistic method:

Since we can compute radicals, we may assume that A is reduced (so it is a product of fields).

Choose a random element $x \in A$, $x \notin k$, and test whether it is a zero-divisor (for example by computing a Gröbner basis for (I, x)). If x is a zerodivisor, we factor it

out and we are done by induction on the dimension of A. Assuming that x is a nonzerodivisor, compute $\dim_k A$ by finding a Gröbner basis for the ideal defining A. Let $m = m(x)$ be the smallest integer such that the powers

$$1, x, \ldots, x^m$$

are linearly dependent. If $m(x) = \dim_k A$, the dependence relation may be written $p(x) = 0$, where $p(t)$ is a polynomial in one variable t, so that $A = k[t]/(p)$. If p factors as a polynomial over k, say $p = q_1 q_2$, then $q_1(x)q_2(x) = 0$. Thus $q_1(x)$ is a zerodivisor, and we are done as before. If on the other hand p is irreducible, then A is a field and 0 is a maximal ideal.

Thus we have succeeded, inductively, as long as x is a zerodivisor or $m(x) = \dim_k A$. In the contrary case, we rechoose x and try again. To estimate the chance of success on a given try in one case of practical interest, suppose that k is a finite field of characteristic p, and that A has s maximal ideals, with residue class fields of orders p^{e_i}. The probability that x is a zerodivisor is then

$$1 - \prod_{i=1}^{s} (p^{e_i} - 1)/p^{e_i}$$

while the probability that $m(x) = \dim_k A$ is

$$\prod_{i=1}^{s} (p^{e_i} - p^{e_i - 1})/p^{e_i} = (p-1)^s/p^s.$$

If s is small compared to p, the second of these near 1; if s is large compared to p, and the e_i are not too big, then the first near 1.

References

1. Avramov, L.: Homology of local flat extensions and complete intersection defects. Math. Ann. **228**, 27–37 (1977)
2. Bayer, D.: The division algorithm and the Hilbert scheme. Thesis, Harvard University, 1982. Order number 82-22588, Univ. Microfilms Intl., Ann Arbor Michigan (1982)
3. Bayer, D., Galligo, A., Stillman, M.: Computing primary decompositions (in preparation)
4. Bayer, D., Stillman, M.: Macaulay: A system for computation in algebraic geometry and commutative algebra. Source and object code available for Unix and Macintosh computers. Contact the authors, or download from zariski. harvard. edu via anonymous ftp. (login: anonymous, password: any, cd Macaulay) (1982–1990)
5. Bayer, D., Stillman, M.: A criterion for detecting m-regularity. Invent. Math. **87**, 1–11 (1987)
6. Bayer, D., Stillman, M.: Computation of Hilbert functions. J. Symb. Comput. **14**, 31–50 (1992)
7. Bayer, D., Mumford, D.: What can be computed in algebraic geometry? In: Eisenbud, D., Robbiano, L. (eds.) Proceedings of the Cortona conference on computational algebraic geometry Cambridge: Cambridge University Press 1993
8. Bertram, A., Ein L., Lazarsfeld R.: Vanishing theorems, a theorem of Severi, and the equations defining projective varieties, (preprint)
9. Brennan, J.P., Vasconcelos, W.: Effective computation of the integral closure of a morphism. J. Pure Appl. Alg. (to appear)
10. Buchsbaum, D.A., Eisenbud, D.: What makes a complex exact? J. Algebra **25**, 259–268 (1973)
11. Buchsbaum, D.A., Eisenbud, D.: Some structure theorems for finite free resolutions. Adv. Math. **12**, 84–139 (1974)
12. Buchsbaum, D.A., Eisenbud, D.: What annihilates a module. J. Algebra **47**, 231–243 (1977)
13. Cox, D., Little, J., O'Shea, D.: Ideals, varieties and algorithms. Berlin Heidelberg New York: Springer 1992

14. Eisenbud, D.: Commutative algebra with a view toward algebraic geometry. (Brandeis Lect. Notes. 1989)
15. Eisenbud, D., Levine, H.: An algebraic formula for the degree of a C^∞ map germ. Ann. Math. **106**, 19–44 (1977)
16. Eisenbud, D., Stillman, M.: Methods in comp. algebraic geometry and commutative algebra (in preparation)
17. Eisenbud, D., Sturmfels, B.: Finding sparse systems of parameters. (in preparation)
18. Gianni, P., Trager, B., Zacharias, G.: Gröbner bases and primary decomposition of polynomials ideals. J. Symb. Comput **6**, 149–167 (1988)
19. Grothendieck, A., Dieudonné, J.: Éléments de géométrie algébrique IV. Publ. Math., Inst. Hautes Étud. Sci. **32** (1967)
20. Gruson, L., Lazarsfeld, R., Peskine, C.: On a theorem of Castelnuovo and the equations defining space curves. Invent Math. **72**, 491–506 (1983)
21. Hartshorne, R.: Algebraic geometry. Berlin Heidelberg New York: Springer 1977
22. Hermann, G.: Die Frage der endlich vielen Schritte in der Theorie der Polynomideale. Math. Ann. **95**, 736–788 (1926)
23. Hilbert, D.: Über die Theorie der algebraischer Formen. Math. Ann. **36**, 473–534 (1890)
24. Hironaka, H.: Resolution of singularities of an algebraic variety over a field of characteristic 0. Ann. Math. **79**, 205–326 (1964)
25. Hochster, M.: Symbolic powers in Noetherian domains. Ill. J. Math. **15**, 9–27 (1971)
26. Kaplansky, I.: Commutative Rings. Boston: Allyn and Bacon 1970
27. Knuth, D.: The art of computer programming vol. 2: Seminumerical algorithms. Reading: Addison-Wesley 1971
28. Krick, T., Logar, A.: An algorithm for the computation of the radical of an ideal in the ring of polynomials. In: Mattson, H.F. et al. (eds.) Proceedings 9th AAEEC. (Lect. Notes Comput. Sci., vol. 539, pp. 195–205) Berlin Heidelberg New York: Springer 1991
29. Kunz, E.: Kähler Differentials. Wiesbaden: Viehweg 1986
30. Lazard, D.: Ideal bases and primary decomposition: case of two variables. J. Symb. Comput. 261–270 (1985)
31. Lazard, D.: Commutative algebra and computer algebra. (Lect. Notes Comput. Sci., vol. 144, pp. 40–48) Berlin Heidelberg New York: Springer 1982
32. Lazard, D.: Solving zero-dimensional algebraic systems. J. Symb. Comput. (to appear)
33. Lazarsfeld, R.: A sharp Castelnuovo bound for smooth surfaces. Duke Math. J. **55**, 423–429 (1987)
34. Matsumura, H.: Commutative algebra. New York: Benjamin 1970
35. Matsumura, H: Commutative ring theory. Cambridge: Cambridge University Press 1986
36. Mumford, D.: Varieties defined by quadratic equations. In: Proceedings, of the conference at the Centro Int. Mat. Estivo (CIME). Varenna 1969. Rome: Cremonese 1970
37. Nagata, M.: Local rings. New York: Interscience 1962
38. Northcott, D.G.: A homological investigation of a certain residual ideal. Math. Ann. **150**, 99–110 (1963)
39. Peskine, C., Szpiro, L.: Liaison des variétés algébriques I. Invent. Math. **26**, 271–302 (1974)
40. Vasconcelos, W.: Computing the integral closure of an affine domain. Proc. Am. Math. Soc. **113**, 633–638 (1991)
41. Scheja, G., Storch, U.: Über Spurfunktionen bei vollständigen Durchschnitten, J. Reine Angew. Math. **278**, 157–170 (1975)
42. Seidenberg, A.: On the Lasker–Noether decomposition theorem. Am. J. Math. **106**, 611–638 (1984)