# FINDING NILPOTENTS WITH WOLMER VASCONCELOS

CRAIG HUNEKE

Abstract. This paper discusses the nilradical of ideals, especially concerning ideas surrounding the algorithm to compute the nilradical of ideals in polynomial rings which appears in the paper 'Direct Methods for Primary Decomposition', by David Eisenbud, Wolmer Vasconcelos and the current author. One new algorithm is given, which as far as we know has not been previously implemented.

## 1. Introduction

I first met Wolmer Vasconcelos at the important CBMS conference 'Analytic Methods in Commutative Algebra,' at George Mason University in 1979 (see [8]). But in a sense I had met him much earlier through studying several of his classic papers, and one of his books. As a graduate student at Yale University, I enjoyed prowling through the mathematics library in search of interesting books. Those books in commutative algebra particularly interested me. One I found early on was the book 'Divisor Theory in Module Categories', by Wolmer Vasconcelos [24]. This book was a far-seeing excursion into homological algebra and module theory. Many years later, when I told Wolmer about my early experience, he gave me a copy of the book –his last copy– he wrote on the flyleaf. I felt extremely honored. Vasconcelos had a great impact on the field of commutative algebra, because of the many fundamental theorems he proved, the field-expanding conjectures he stated, and his extremely generous and open nature. He welcomed everyone to do mathematics with him and shared his ideas without reservation.

In the 1980s, Vasconcelos's beautiful work with Juergen Herzog and Aron Simis, on approximation complexes and Koszul homology, dovetailed with my own work on d-sequences, Rees and symmetric algebras, and linkage. It was a time of many letters (real hand-written letters!) going back and forth between the two of us as we compared methods and results. In this way, Vasconcelos played a huge role in my own development. This entire body of work is summarized in Vasconcelos's book *Arithmetic of Blowup Algebras*, [26].

However, rather than write about these works, Aron Simis suggested that this paper be based on joint work of mine with Vasconcelos and David Eisenbud, *Direct Methods for Primary Decomposition* [10], whose main purpose was to derive computational methods to compute the nilradical of ideals. We sought methods that could actually be done in many examples without using so much computer memory that they would be impractical. Existing known methods at that time used generic projections, which in general were impractical. In fact, Aron was responsible for David and me joining forces with Vasconcelos on this topic.

*Date*: May 27, 2023.
2010 *Mathematics Subject Classification.* 13A02, 13F20, 13H15.
*Key words and phrases.* nilradical, Jacobian.

Vasconcelos had been working on this problem, independently from David and myself. When Aron told David about Vasconcelos's investigations, we began working together. Vasconcelos had a long and sustained interest in computational issues. His book *Computational Methods in Commutative Algebra and Algebraic Geometry* [25] is a testament to his interest and acuity in these matters.

## 2. The Nilradical

There are many closure operations used in commutative algebra, but probably the most basic, and the one learned almost immediately, is the nilradical of an ideal $I$ in a commutative ring $R$, denoted $\sqrt{I}$, namely the set of all elements $x \in R$ such that there is an integer $n$ with $x^n \in I$. One learns that $\sqrt{I} = \cap_{I \subset P} P$, the intersection of all prime ideals $P$ containing $I$. This is quite obviously *not* an effective way to compute this ideal. However, it does characterize the radical of an ideal $I$ as the elements $f \in R$ such that for every map $\phi : R \to K$, where $K$ is a field, $f \in IK$. This looks strange–after all, $IK$ is either 0 or $K$. If it is $K$, there is no condition; if $I$ goes to zero under the map $\phi$, then so must $f$. This reformulation can be seen by passing to the fraction fields of $R/P$ as $P$ ranges over all prime ideals of $R$. Our first example illustrates this principle.

**Example 2.1.** Let $A$ be a generic $n$ by $n$ matrix over a field $K$ of characteristic 0, and let $S$ be the polynomial ring over $K$ obtained by adjoining the variables of the entries of $A$. Consider the ideal $J$ generated by the entries of the matrix $A^n$. Clearly $V(J)$ defines the locus in which the matrix $A$ becomes nilpotent. What is $\sqrt{J}$?

To answer this question, let $f_1, f_2, ..., f_n$ be the coefficients of the Cayley-Hamilton equation of $A$, so that $f_1 = trace(A)$ and $f_n = det(A)$. Whenever $A$ is nilpotent and the entries are in a field, these coefficients must vanish. By the principle described in the first paragraph of this section, $f_1, ..., f_n \in \sqrt{J}$. Here are some thought questions for the reader: Is $\sqrt{J} = (f_1, ..., f_n)$? What is the height of $J$? What power of $f_1$ lies in $J$? For example, if $n = 3$, $J$ is defined by cubic equations and it turns out that $f_1^7 \in J$, but $f_1^6 \notin J$.

**Example 2.2.** For another nice use of the principle above, consider an $n$ by $(n+1)$ matrix $A$ whose first $n$ rows and columns $B$ are a symmetric matrix. We can then complete $A$ to an $(n+1)$ by $(n+1)$ symmetric matrix $C$ (in different ways). Prove that if $f = det(C), g = det(B)$, then $\sqrt{(f,g)} = \sqrt{I_n(A)}$, where $I_n(A)$ is the ideal generated by the $n$ by $n$ minors of $A$. (Think of rank conditions for such matrices over a field!)

Lest the reader think that the nilradical of ideal is well-understood, we give a couple of questions about radicals which are not easy. The first question, which was asked by Linda Rothschild to me in connection with her work with Salah Baouendi, is still unsolved to the best of my knowledge.

**Question 2.3.** Let $A = \mathbb{C}[[f_1, ..., f_n]] \subset B = \mathbb{C}[[x_1, ..., x_n]]$ be a module-finite extension of formal power series rings. Assume that $P$ is a prime ideal of $A$ with the property that $B/\sqrt{PB}$ is regular. Is $A/P$ regular?

For another thought exercise, consider the next question which falls into a theme in commutative algebra that suggests that basic ideal closures should never be contained in ideals generated by parameters. A good example of this phenomena is that the conductor of a one-dimensional local Noetherian domain is never inside a proper principal ideal. Can the conductor ever be in an ideal generated by a system of parameters in higher dimension? As far as I know, the answer to this question is not known. For another similar question:

**Question 2.4.** Let $R$ be a local Noetherian ring with nonzero nilradical $N$. Can $N$ ever be contained in an ideal generated by a system of parameters? (I do know the answer to this question!)

For example, consider the case in which $R/N$ is Cohen-Macaulay. Assume by way of contradiction that $N$ is contained in an ideal $I$ generated by a system of parameters $x_1, ..., x_d$, where $d$ is the dimension of $R$. Then $N \subset I \cap N = IN$, where the last property follows from the fact that $x_1, ..., x_d$ is a regular sequence modulo $N$. Nakayama's lemma shows that $N = 0$, a contradiction.

The most famous open question involving the nilradical is the question of whether affine curves are set-theoretic complete intersections. This was proved in positive characteristic by Cowsik and Nori [5], but remains open in characteristic 0. Even for something as simple as one of Moh's curves, the prime $P$ such that $K[[x, y, z]]/P \cong K[[t^6 + t^{31}, t^7, t^{10}]]$, where $K$ is a field of characteristic 0, it is not known whether or not there are two elements $f, g$ such that $\sqrt{(f, g)} = P$. One could hope that the algorithms presented here could lead one to 'reverse engineer' the problem to find such $f, g$ or to show no such elements exist, but as far as the author knows, this has never borne fruit.

**Remark 2.5.** An explicit use of Example 2.2 connected with the open problem above can be seen by using the Hilbert-Burch theorem. Let $S = K[[x, y, z]]$ (or a polynomial ring in 3-variables localized at a maximal ideal), and let $P$ be a height two prime ideal of $S$. Since $S/P$ is necessarily Cohen-Macaulay, the Hilbert-Burch theorem tells us that there is an $n$ by $(n+1)$ matrix $A$ with coefficients in the maximal ideal of $S$ such that $P = I_n(A)$, the ideal generated by the $n$ by $n$ minors of $A$. Suppose we can change $A$ by invertible row and column operations so that the first $n$ by $n$ submatrix $B$ of $A$ is symmetric. We can then complete $A$ to an $(n+1)$ by $(n+1)$ symmetric matrix $C$ (in different ways). By Example 2.2, if $f = det(C), g = det(B)$, then $\sqrt{(f, g)} = \sqrt{I_n(A)} = P$. This remark is attributed to Ferrand by Herzog and Ulrich in [15], who go on to discuss what this means in the case $P$ has three-generators.

As a related problem, one might expect that the radical of ideal is somehow simpler than the ideal one starts with, and might hope to prove this using the results described in this paper. However, there are several discouraging examples:

**Example 2.6.** One question which was answered in the negative a long time ago was the following: if $S/I$ is Cohen-Macaulay, is $S/\sqrt{I}$ also Cohen-Macaulay? The simplest counterexample is $K[[t^4, t^3s, ts^3, s^4]]$ in characteristic $p > 0$. This is known to be a set-theoretic complete intersection, so it is set-theorectically Cohen-Macaulay, but it is not itself Cohen-Macaulay. The nice paper [14] discusses positive examples of such transference of properties for monomial ideals.

**Example 2.7.** This is an interesting example from [4] which shows that the radical of an ideal may become worse than the ideal, at least in terms of regularity. Let $S = k[x, y, z, t]$. Set $I = (y^2z - x^2t, z^4 - xt^3, xy^2t^2 - x^2z^3)$. Then $\sqrt{I} = I + (x^4z^2 - xy^4t)$. They compute that the regularity of $I$ is 5, while the regularity of $\sqrt{I}$ is 6.

## 3. Computing the nilradical

Our basic question is very simple: given polynomials $f_1, ..., f_m \in K[x_1, .., x_n]$, where $K$ is a field, how does one compute the nilradical of the ideal $I$ generated by $f_1, ..., f_m$? This question is both a theoretical question–is there an algorithm to compute the nilradical?; and at same time practical–can one implement an algorithm that will compute the nilradical for many examples? For the last question one must be able to input the field, of course, into the one's program. As soon as one asks this question, the following subsidiary questions surely come to mind:

- Given an element $f \in R$, can we effectively test if $f \in \sqrt{I}$?
- How does one know (or test) if $I$ is self-radical, i.e., $I = \sqrt{I}$?
- What about the simplest case in which $R = K[x]$?
- If we know that $I \neq \sqrt{I}$, how can we find an element in $\sqrt{I}$ but not in $I$?

We will address these questions one by one. In general, one needs to know what one can compute. We will use all Gröbner basis calculations as our black box. Hence, we can compute resolutions, which also means we can test for ideal membership. Of course, it is well-known that in theory this could be doubly exponential in our input, but that is something we have to live with. (However, see [7] for the question of ideal membership–they prove it can be done in exponential time.)We still seek methods which are as efficient as possible. However this present paper is not so much about the computational effectiveness as much as understanding various theoretical issues which come up.

## 4. Can we effectively test if an element is in the nilradical of an ideal?

For the first question there seems to be an obvious answer. Of course given an ideal $I$ is a polynomial ring $R$ over a computable field $k$, and given an $f \in R$, we can simply take powers of $f$, and test whether or not that power of $f$ lies in $I$. But we need a bound for the stopping place of this algorithm, or else we might continue forever. Knowing this stopping time is sometimes called the 'effective' Nullstellensatz, first presented by Brownawell [1]. A more algebraic treatment which this author likes very much was given by Kollár, [17]. A simplified version of his theorem states the following:

**Theorem 4.1.** *Let $K$ be a field, and let $S = K[x_1, ..., x_n]$. Assume that $f_1, ..., f_k$ are homogeneous polynomials of degrees $d_1 \geq d_2 \geq ... \geq d_k > 2$. Let $I$ be the ideal generated by the $f_i$. Then, if $k \geq n$,*

$$(\sqrt{I})^{d_1 d_2 \cdots d_{n-1} d_k} \subset I.$$

*Otherwise, if $k < n$,*

$$(\sqrt{I})^{d_1 d_2 \cdots d_k} \subset I.$$

This theorem is sharp, at least for some examples:

**Example 4.2.** (See [17, 2.3]) Given any $n$ and $d$, consider the polynomials $x_1^d, x_1x_n^{d-1} - x_2^d, ..., x_{n-1}x_n^{d-1} - x_0^d$. Then clearly $x_0 \in \mathrm{rad}(x_1, ..., x_{n-1})$. However, $x_0^{d^{n-1}-1}$ is not in the ideal $I = (x_1, ..., x_{n-1})$. This claim can be seen by setting $x_n = 1$. Here the ideal is generated by $n-1$ forms of degree $d$. Kollar's theorem tells us that the $d^{n-1}$st power of the nilradical of $I$ lies inside $I$, and therefore shows his bound is sharp.

Before moving on, it is worthwhile to consider why it is reasonable that regardless of the number of defining equations of the ideal $I$, the worse-case scenario in Kollar's theorem uses at most $n$-equations. In part this is explained by theorems of Eisenbud and Evans [9]. They prove that any ideal $I$ in affine-space $K[x_1, ..., x_n]$ can be generated up to radical by $n$-equations. If they are homogeneous and represent a non-trivial projective variety, even $n-1$ suffice.

While Kollar's theorem (and its non-homogeneous version) do give an effective criteria to decide if a given $f \in S$ is in $\sqrt{I}$, it is certainly not the best computationally. In fact, a simple exercise provides an easier way: namely, an element $f \in S$ is in $\sqrt{I}$ if and only if $1 \in (1 - ft, IS[t])$, where $t$ is a new variable. The reason is that going modulo $(1 - ft)$ is the same as inverting $f$, and $I_f = S_f$ if and only if $f \in \sqrt{I}$. Using Gröbner bases, we can test ideal membership: is a given element in a given ideal, so that testing whether or not $1 \in (1-ft, IS[t])$ only requires basic Gröbner basis calculations of the type we wish to allow at the cost of adding one new variable.

Before leaving this section, there is one case where a good effective bound can be obtained, which I have always liked and wanted to understand better. It is given in Vasconcelos's book [26][Theorem 10.3.16], and he attributes it to Levin:

**Theorem 4.3.** *Let $R$ be a local ring, $I$ an ideal of $R$ of finite projective dimension $p$ such that $I$ is not generated by a regular sequence. Let $J$ be the ideal generated by the coefficients of relations on a minimal set of generators of $I$ (the so-called content of $I$). Then*

$$(I : J)^{p+1} \subset I.$$

## 5. Testing self-radical

We move on to the second question: *How does one know (or test) if $I$ is self-radical, i.e., $I = \sqrt{I}$?*

This turns out to be in some sense easy, but there are issues to consider. We use that a ring $R$ is *reduced* (i.e., has no nonzero nilpotent elements) if and only if it satisfies Serre's conditions $R_0$ and $S_1$. To put it more concretely, we use the following proposition:

**Proposition 5.1.** *Let $R$ be a Noetherian ring, and let $x \in R$ be a nonzero-divisor. If $R_x$, the localization of $R$ at the multiplicatively closed set of powers of $x$ is reduced then so is $R$. Conversely, if $R$ is reduced and has closed singular locus, then there exists a nonzero-divisor $x$ in $R$ such that $R_x$ is regular (and in particular is reduced).*

*Proof.* Since $x$ is assumed to be a nonzero-divisor, $R$ embeds in $R_x$. This proves the first statement. Conversely, choose a general element $x$ in the defining ideal of the singular locus. Since $R$ is reduced, $R_P$ is regular (in fact a field) for all minimal primes $P$ of $R$. Therefore the ideal defining the singular locus has height at least one, and the general element $x$ will avoid all minimal primes. Since the zerodivisors of $R$ are the union of these primes (as $R$ is reduced and in particular has no embedded associated primes), this means that $x$ is a nonzero-divisor on $R$. Clearly $R_x$ is regular and hence reduced. □

This Proposition gives an algorithm to decide if a quotient of a polynomial ring $S$ by an ideal $I$ is reduced, at least in the equidimensional case. Simply compute the relevant Jacobian ideal which defines the singular locus. We wish to know if that Jacobian ideal $J$ contains a nonzero-divisor, so we just need to compute the colon ideal into $I$, namely $I : J$. If $I : J = I$, then $I$ is self-radical. If not, it will not be self-radical. Of course we could have chosen a general element in that ideal, and then tested whether or not the element is a nonzero-divisor modulo the ideal $I$, which sounds simpler. However, this approachs brings up one of the main points of the paper under discussion. Whenever one has to choose a 'general' element (for example to avoid a finite set of prime ideals), the computational complexity of the problem seems to grow a great deal. One can take 'random' combinations of generators of a given ideal to make sense of the word 'general', but the number of generators is often very large, and taking random combinations gives elements with a very large number of terms. Moreover, one cannot be absolutely certain that the answer is correct. One could take generic generators by adjoining new variables, and using the new variables as coefficients, but this will almost always make actual computation impossible. Thus, our methods sought to **never** use random or generic combinations of generators of a given ideal. See the paper of Eisenbud and Sturmfels for work on finding sparse systems of parameters [11].

## 6. One variable

Let $R = K[x]$, where $K$ is a field, and let $f \in R$ be a nonzero element. How can one find $\sqrt{(f)}$? The seemingly obvious answer is that we know $R$ is a UFD, so we can factor $f$ into a product of powers of non-associate irreducibles:

$$f = f_1^{n_1} \cdots f_k^{n_k}.$$

In this case, we know that

$$\sqrt{(f)} = (f_1 \cdots f_k).$$

However, this process of factoring into irreducibles (which amounts to finding a primary decomposition of the ideal generated by $f$) is exactly the type of process we wish to avoid. To start with, it clearly depends upon the field. There is a much simpler way to proceed in characteristic 0 or large characteristic. Consider the derivative,

$$f'(x) = g f_1^{n_1-1} \cdots f_k^{n_k-1},$$

where $g = n_1 f_1' f_2 \cdots f_k + n_2 f_2' f_1 f_3 \cdots f_k + \ldots n_k f_k' f_1 \cdots f_{k-1}$.

Assume that $K$ has characteristic 0 or sufficiently large characteristic. In this case $f_i'$ and $f_i$ will be relatively prime since $f_i$ is a prime element, and $f_i'$ is smaller degree and nonzero. It follows that for every $i$, $f_i$ does not divide $g$. But then

$$(f) : f' = (f_1 \cdots f_k) : g = (f_1 \cdots f_k) = \sqrt{(f)}.$$

Thus one does not have to factor $f$ to compute the nilradical! This observation is the basis for the main algorithm of the paper.

## 7. Our Purpose

To understand the motivation for our work, it is worthwhile simply quoting a large passage from the introduction of our paper [10], since it explains the purpose extremely well:

"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 of $I$?

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 $I$?

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 [13] (see also Seidenberg [23], 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 $k[x_1, ..., x_n]$ with a subring $k[y_1, ..., y_m]$, where the $y_i$ are linear forms in the $x_j$ (PROJECTION)

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 $(g/GCD(fg), -f/GCD(fg))$. 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 [16] 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 [18], 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. [6] 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 ([20, 21]), Gianni et al. [12] (see also the references there), Bayer et al. [2], and Krick and Logar [19]. 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 $y_i$ to be much sparser linear forms in the $x_j$), 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 subproblem 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 [21]."

## 8. Regular Sequences

It is not difficult to envision how one might solve finding the nilradical of a regular sequence, $f_1, ..., f_n$. Namely, one needs a type of "generic" socle element, that is, an element $g$ such that for every minimal prime $P$ of the ideal $I = (f_1, ..., f_n)$, in the Artinian ring $S_P/I_P$, the image of $g$ is a non-zero socle element of this Artinian (and Gorenstein) ring. In this case, the colon ideal $I_P : g$ will locally be $PS_P$. Then the ideal $I : g$ will exactly be the intersection of the minimal primes of $I$, i.e.,

$$I : g = \sqrt{I}.$$

We are using that this ideal has no embedded components since $S/I$ is Cohen-Macaulay.

A good case to consider is when the regular sequence is a full system of parameters inside a regular local ring. Specifically, let $S = K[[x_1, ..., x_n]]$ be a complete regular local ring of dimension $n$ over a field $K$ of characteristic 0 with maximal ideal generated by $x_1, ..., x_n$, and let $f_1, .., f_n$ be a system of parameters, necessarily a regular sequence. We wish to find a generator for the socle of the quotient ring $S/(f_1, .., f_n)$. One well-known way is to use linkage theory [3][Cor. 2.3.10]: we write

$$f_i = \sum_j a_{ij} x_j.$$

Then the determinant of the $n$ by $n$ matrix of coefficients $(a_{ij})$ exactly generates $(f_1, ..., f_n) : (x_1, ..., x_n)$, i.e., generates the socle. However, one would like to have some canonical choice for the coefficients $a_{ij}$. If in addition the $f_i$ are homogeneous polynomials, then we can use Euler's formula to write

$$d_i f_i = \sum_j \frac{\partial f_i}{\partial x_j} x_j$$

where $d_i = deg(f_i)$. We can then take the $a_{ij}$ to be the partial derivatives of the $f_i$ up to constants, and a "generic" socle element will be given by the determinant of the Jacobian matrix,

$$\left( \frac{\partial f_i}{\partial x_j} \right).$$

It is a beautiful fact, proved by Scheja and Storch [22], that the determinant of the Jacobian matrix still works even in the case the $f_i$ are not homogeneous polynomials. Namely, if S is a power series ring in $n$ variables over a field $K$ of characteristic 0 (or characteristic $p > dim_K(S/I)$) with maximal ideal $M$, and $I$ is an ideal generated by a maximal regular sequence in $M$, then $\frac{I:M}{I}$ is generated by the determinant $\Delta$ of the Jacobian matrix of $I$. Thus, $I : \Delta = M$, and $\Delta$ is the 'generic' socle element we seek. This exactly generalizes what we saw in the one-variable case.

One of our first results generalizes this process even further to all unmixed rings which are generically complete intersections. We say that an ideal $I$ is *generically a complete intersection* if $I_P$ is generated by a regular sequence for every minimal prime $P$ containing $I$. Here, and throughout the rest of this paper, we denote the $(n-a)$ by $(n-a)$ minors of the Jacobian matrix of $I$ by $J_a(I)$ for an arbitrary ideal $I$ in $S$, a polynomial ring in $n$-variables.

**Theorem 8.1** ([10], Theorem 2.1)**.** *Let $R = K[x_1, ..., x_n]/I$ 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 strictly less than $p$ over a polynomial ring generated by sufficiently general linear forms. If $I$ is generically a complete intersection, then*

$$\sqrt{I} = (I : J_d(I)).$$

The content of this theorem is simply that the ideal $J_d(I)$ will always be inside the socle and have a nonzero socle element of $R_P$ for every minimal prime $P$ of $R$, in other words will generate the socle. This is very effective if one knows two things: first that $I$ is equidimensional and has no embedded primes, and secondly that $I$ is generically a complete intersection. We will show how to deal with the equidimensionality and embedded primes in the next section. As to determining whether or not $R$ is generically a complete intersection, we may use the following criteria: (see [25][Proposition 3.2.1].)

**Proposition 8.2.** *Let $S$ be a Cohen-Macaulay ring, and let $I$ be an unmixed ideal of codimension $c$ with a presentation*

$$S^m \xrightarrow{\phi} S^n \to I \to 0.$$

*Then $I$ is generically a complete intersection if and only if the height of $I_{n-c}(\phi) \geq c+1$.*

*Proof.* Here, $I_{n-c}(\phi)$ is the ideal of $(n-c)$-size minors of a matrix representing $\phi$. The closed set of $\mathrm{Spec}(S)$ defined by this ideal is exactly the set of primes $P$ such that the minimal number of generators of $I_P$ is at least $c+1$. Thus the condition on the height of this ideal stated in the proposition exactly says that $I_P$ is generated by $c$-elements at all primes $P$ of height $c$ which contain $I$. $\square$

If we can actually find, or are given, a maximal regular sequence inside an arbitrary ideal $I$, then the above theorem can be used to find the intersection of the minimal primes of maximal dimension, which we call the equidimensional hull of the radical of $I$. In general the equidimensional hull is the intersection of the primary components of $I$ of maximal dimension.

**Algorithm 8.3** ([10])**.** (Reduction of the equidimensional radical to the complete intersection case) Given ideals $J \subset I \subset K[x_1 \ldots x_n]$, where $J$ is known to be generated by a regular sequence, and $I$ and $J$ both have the same height, compute the equidimensional hull of the radical of $I$:
Compute $\sqrt{J}$
Return equidimensional radical $I := (\sqrt{J} : (\sqrt{J} : I))$.

Why does this work? First of all the theorem tells us how to compute $\sqrt{J}$. We take the colon ideal of $J$ with the appropriate size minors of its Jacobian. Write $\sqrt{I} = N \cap L$, where $N$ is the equidimensional radical—that is the intersection of minimal primes of smallest codimension, and $L$ is the intersection of all other minimal primes of $I$. Since $J \subset I$, and $J$ is a complete intersection, $\sqrt{J} = N \cap Q$, where $Q$ is the intersection of all minimal primes of $J$ which do not contain $I$. Hence,

$$(\sqrt{J} : I) = (N \cap Q : I) = (N : I) \cap (Q : I) = S \cap Q = Q.$$

Then

$$(\sqrt{J} : (\sqrt{J} : I)) = N \cap Q : Q = N,$$

which is what we want to compute.

Notice that this process will allow to finish our task by then replacing $I$ by $I : K^n$ for large n. We obtain that this colon ideal is the intersection of the primary components of $I$ whose associated primes do not contain $K$, i.e., $\sqrt{I : K^n} = L$, where as above $\sqrt{I} = K \cap L$. But there are two critical problems with this approach. First of all we need an effective bound for the $n$ we use. This can be done via Kollár's theorem, but is too large in practice. Secondly, to repeat the process, we would need to find a maximal regular sequence in $I : K^n$. As we discussed above, this becomes a problem. General combinations of generators will form a regular sequence (choosing up to the height of the ideal), but random combinations are not practical for computation. Notice that we cannot even begin the above algorithm unless we are given a maximal regular sequence inside $I$. Thus, we prefer to have other methods which will at least reduce to the case the ideal $I$ is unmixed, i.e., has no embedded components and has every minimal prime of the same height.

Before moving on, it is important to note that if $I$ is not generically a complete intersection, then the process of coloning the appropriate Fitting ideal of the Jacobian does not work. One might hope that even if it does not give the correct answer on the nose, that the colon might improve the situation. But exactly the opposite is true. Consider the following simple example:

**Example 8.4.** Let $I = (x, y)^2$ in $S = K[x, y]$. It is unmixed of height 2, and obviously the nilradical is $(x, y)$. The Jacobian matrix is

$$\begin{pmatrix} 2x & 0 \\ y & x \\ 0 & 2y \end{pmatrix}$$

Since $I$ has codimension 2, we would take the ideal $J$ to be 2 by 2 minors of this matrix which generate the ideal $(x, y)^2$ (in characteristic not equal to 2). But then $I : J = S$. We lose all information!

This is not an isolated example. The last section of the paper will deal with the case in which $I$ is not generically a complete intersection.

## 9. Reducing to Equidimensionality

Let $I$ be an ideal in a Cohen-Macaulay ring of height $c$. Write a primary decomposition of

$$I = \cap_{i=1}^{s} q_i \cap J,$$

where the $q_i$ are primary ideals of height $c$ with distinct associated primes $P_i$, and $J$ is the intersection of primary components of height strictly bigger than $c$. Our goal is to compute $q := \cap_{i=1}^{s} q_i$. The first proposition does this:

**Proposition 9.1.** *Let $I$ be an ideal in a Gorenstein ring of height $c$, and write $I = q \cap J$, where $q$ is the intersection of all primary components of $I$ of minimal height $c$, and $J$ is the intersection of all other primary components with respect to some primary decomposition of*

*$I$ (in fact $J$ is unique, but we don't need to know this). Choose a maximal regular sequence $x_1, ..., x_c$ in $I$, generating an ideal $K$. Then*

$$K : (K : I) = q.$$

*Proof.* As $K$ has no associated primes of height bigger than $c$ since $R$ is Cohen-Macaulay, the double colon ideal also has no associated primes of height bigger than $c$. Since $I$ is clearly in $(K : (K : I)$ any $P$ of height $c$ containing the double colon contains $I$. In this case we have that $I_P = q_P$. Therefore at all such primes $P$,

$$(K : (K : I))_P = K_P : (K : q)_P = q_P.$$

The proposition follows. □

This proposition allows us to identify the equidimensional hull of an arbitrary ideal in a Gorenstein ring, which is what we wish to do. However, you might reasonably object that it seems to depend on a choice of a maximal regular sequence inside the ideal, something which we have repeatedly said we do not wish to choose: hypocrisy! But we in fact do not have to choose the regular sequence as the next algorithm proves:

**Algorithm 9.2** ([10])**.** (Equidimensional hull of an ideal) Given $I \subset S = k[x_1, \ldots x_n]$, find the equidimensional hull of $I$ consisting of the intersection of the primary components of $I$ of maximal dimension.

$$c := codim I;$$

Return

$$ann_S Ext^c(S/I, S).$$

This algorithm works because for every maximal regular sequence in $I$ generating an ideal $K \subset I$,

$$Ext^c(S/I, S) \cong Hom_S(S/I, S/K) \cong (K : I)/K.$$

Hence the annihilator of the Ext module is exactly $K : (K : I)$, which by the above proposition is exactly the equidimensional hull of $I$.

In fact we can generalize the idea of this algorithm to do even more:

**Algorithm 9.3** ([10])**.** (Associated primes of given codimension) Given a finitely generated module $M$ over $S = k[x_1, ..., x_n]$, find an ideal whose associated primes are exactly the associated primes of $M$ having codimension e.

$$I_e := ann_S Ext^e_S(M, S);$$

if codim $I_e > e$
Return S; else
Return the equidimensional hull of $I_e$.

## 10. General Case

We now come to the general case in which we can assume our ideal $I$ is unmixed (using the results of the last section), but do not assume that the ideal is generically a complete intersection. As explained in that section, we cannot simply colon the ideal with the codimension-size minors of the Jacobian matrix and hope to improve the ideal. There are two related, but different approaches we will present, one of which is in the paper [10], and the other closely related to remarks in the same paper. Before presenting these methods, it is worthwhile to consider the problem from another perspective.

We have already shown how to reduce to the case in which the ideal $I$ is unmixed, i.e., equidimensional and without embedded components. Furthermore, if $I$ is generically a complete intersection, the colon $I : J = \sqrt{I}$ for $J$ the ideal generated by appropriate size minors of the Jacobian matrix. Such a $J$ represents a 'generic' socle. In general, there is some $J$ such that $I : J = \sqrt{I}$, but finding it is the problem. However, what if we simply try any $J$? The ideal $I : J$ is still unmixed, and every associated prime of $I : J$ is an associated prime of $I$. If $I$ is strictly contained in $I : J$, we have improved the situation and can repeat the process. The problem with this idea is twofold. First of all, simply choosing a 'random' $J$ cannot work, since if $J$ is not contained in any associated prime of $I$, $I = I : J$, and we have not improved anything. Secondly, if $J$ happens to be chosen inside a primary component $q$ of $I$ with associated prime $P = \sqrt{q}$, then $I : J \nsubseteq P$, and we have lost $P$. It turns out that there are natural good choices for such $J$, coming from the Jacobian matrix, and the presenting matrix of $I$, but one must be careful to do things in the right order. In the case of the Jacobian ideal, we start with the 1 by 1 minors of the Jacobian matrix, and then continue. Specifically, here is our main result:

**Theorem 10.1** ([10], Theorem 2.7)**.** *Let $S$ be a polynomial ring over a perfect field $K$ and let $I \subset S$ be an ideal with $dim(S/I) = d$. If the characteristic of $K$ is not zero, suppose that the nilradical of $S/I$ is generated by elements whose index of nilpotency is strictly less than the characteristic of $K$. If for some integer $a > d$ we have that*

$$dim(S/J_{a+1}(I)) < d,$$

*then*

$$I_1 := (I : J_a(I))$$

*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.*

This theorem leads to the main algorithm:

**Algorithm 10.2** ([10] Algorithm 2.9)**.** (Equidimensional Radical) Given an equidimensional ideal $I \subset S = K[x_1, ..., x_n]$, find $\sqrt{I}$.
$a := n - 1$. $d := dim(S/I)$.
While $a > d$
{
While dim $S/J_a(I) = d$
$I := (I : J_a(I))$;
decrement $a$;

}
$I := (I : J_d(I));$
Return $I$.

There is another approach to which the theorem of Levin, Theorem 4.3, is related. Recall that we can test whether or not an ideal is generically a complete intersection uses Fitting ideals of a presentation by 8.2: Let $S$ be a Cohen-Macaulay ring, and let $I$ be an unmixed ideal of codimension $c$ with a presentation

$$S^m \xrightarrow{\phi} S^n \to I \to 0.$$

Then $I$ is generically a complete intersection if and only if the height of $I_{n-c}(\phi) \geq c+1$. This suggests a new strategy which invovles taking colons of $I$ with respect of appropriate Fitting ideals of its presentation.

**Theorem 10.3.** *Let $S = K[x_1, ..., x_n]$, and let $I$ be an unmixed ideal of $S$ of codimension $c$, i.e., $I$ is equidimensional of height $c$ and has no embedded primes. Let*

$$S^m \xrightarrow{\phi} S^n \to I \to 0$$

*be a presentation for $I$, and set $J_m$ equal to the ideal $I_m(\phi)$, the ideal of $m$ by $m$ minors of $\phi$. Assume that $I$ is not generically a complete intersection. Then $J_{n-c}$ has height at most $c$. Choose $k$ maximal such that the height of $J_{n-k}$ has height $c$, and set $I_1 = I : J_{n-k}$. Then $I \subset I_1 \subset \sqrt{I}$. Moreover, $I \neq I_1$.*

*Proof.* Note that in general, $J_{n-k} \nsubseteq P$ if and only if $\mu(I_P) \leq k$. Here $\mu$ is the minimal number of generators. By the choice of $k$, $J_{n-k-1}$ is not contained in any minimal prime of $I$, since its codimension is at least $c+1$. Thus, $\mu(I_P) \leq k+1$. To prove the second statement, we have that assuming $\mu(I_P) \leq k$ implies that $J_{n-k} \nsubseteq P$. Therefore $(I_1)_P = I_P : (J_{n-k})_P = I_P$. By the choice of $k$, there is some minimal prime $P$ containing $I$ which contains $J_{n-k}$, and then $\mu(I_P) \geq k+1$ for that prime. But it cannot have more than $k+1$ generators by the first item. If we choose a minimal presentation for $I_P$, we obtain an exact sequence

$$S_P^l \xrightarrow{\phi_P} S_P^{k+1} \to I_P \to 0,$$

and furthermore $I_1(\phi_P) = I_{n-k}(\phi)_P$. Note that the same equality holds for every minimal prime $P$ of $I$ that contains $J_{n-k}$.

Theorem 4.3 of Levin tells us that $(I_P : I_1(\phi_P)) \subset \sqrt{I_P} = P_P$. In fact, it gives an explicit bound for the index of nilpotency, but we do not need this to prove the theorem. Since $I_1(\phi_P) = I_{n-k}(\phi)_P$, we conclude that $I_P \subset (I_P : I_1(\phi_P)) = (I_1)_P \subset \sqrt{I_P} = P_P$.

We have shown that if $P$ is a minimal prime of $I$, then one of two things occur: if $P$ does not contain $J_{n-k}$, then $(I_1)_P = I_P$, while if $P$ does contain $J_{n-k}$, $I_P$ is strictly contained in $(I_1)_P \subset P_P$. This proves the theorem.

□

The theorem gives us another algorithm for computing the nilradical of an unmixed ideal $I$: simply compute the largest $k$ with $J_{n-k}$ having height $c$. If $k = c$, then $I$ is generically a complete intersection, and we compute the nilradical of $I$ by using the generic socle. If $k > c$, we replace $I$ by $I_1 = I : J_{n-k}$. Notice that it is very important to not use the colon with respect to one of the Fitting ideals of the presentation of $I$ if $I$ is generically a complete intersection, since then at every minimal prime $P$, the content of $I_P$ is just $I_P$, since the Koszul complex is then a resolution of $I_P$.

Although as far as this author knows it is not implemented in Macaulay2, it seems to this author that a combination of the algorithm involving the minors of the Jacobian matrix and the algorithm described in Theorem 10.3 above might be the best. The size of the Jacobian matrix is $n$ by $m$, where $m$ is the number of generators of the ideal $I$, and $n$ is number of variables. On the other hand, the presentation matrix of $I$ is $m$ by $b$, where again $m$ is the number of generators of $I$, and $b$ is the second Betti number of $S/I$. If $b$ is smaller than $n$, then one will be using smaller size minors in the algorithm; otherwise it is likely the minors of the Jacobian matrix will be better. But then one needs to check at every repetition which one to use, by checking the minimal number of generators of the new ideal created in the algorithm. It would be interesting to run simulations where each algorithm is used, and a combination is used. The method using the presentation matrix of the ideal does not seem to be as sensitive to the characteristic of the field as the Jacobian method, which might be useful in some circumstances.

**Remark 10.4.** We are not using the explicit nilpotencey degree of $I : J$, where $J$ is the content of $I$, which is given in Levin's theorem. We only use the fact that if $I$ is finite projective dimension and primary to the maximal ideal of a local ring $R$, then the content of $I$ cannot be contained in $I$ unless $I$ is generated by a regular sequence. This follows from a famous theorem of Vasconcelos [27], which states that if $I/I^2$ is a free $R/I$-module, and $I$ has finite projective dimension, then $I$ is generated by a regular sequence. This follows since the statement that the content is in $I$ forces $Tor_1^R(R/I, R/I)$ to be free, and this Tor is isomorphic to $I/I^2$.

## References


[1] W. D. Brownawell, *Bounds for the degrees in Nullstellensatz*, Ann. of Math **126** 577- 592, (1987).

[2] D. Bayer, A. Galligo, and M. Stillman, *Computing primary decompositions*, unpublished.

[3] W. Bruns and J. Herzog, *Cohen-Macaulay Rings.* Cambridge Studies in Advanced Mathematics **39** (1993), Cambridge University Press, Cambridge, United Kingdom.

[4] M. Chardin and C. D'Cruz, *Castelnuovo-Mumford regularity: examples of curves and surfaces*, J. Algebra **270** 347–360, (2003).

[5] R.C. Cowsik and M. Nori, *Affine curves in characteristic p are set theoretic complete intersections*, Inventiones Math. **45**, 111–114 (1978).

[6] D. Cox, J. Little, and J. O'Shea, *Ideals, varieties and algorithms* Berlin-Heidelberg New York: Springer (1992).

[7] A. Dickenstein, N. Fitchas, M. Giusti, C. Sessa, *The membership problem for unmixed polynomial ideals is solvable in single exponential time* Mathematics, Computer Science Discret. Appl. Math. (1991)

[8] Richard N. Draper, editor, *Commutative Algebra, Analytic Methods* Lecture Notes in Pure and Applied Mathematics, **68**, Marcel Dekker, New York and Basel.

[9] D. Eisenbud and E.G.Evans, *Every algebraic set in n-space is the intersection of n-hypersurfaces*, Inventiones Math. **19**, 107–112, (1973).

[10] D. Eisenbud, C. Huneke, and W. Vasconcelos, *Direct Methods for Primary Decomposition*, Inventiones Math. **110**, 207-235, 1992.

[11] D. Eisenbud and B. Sturmfels, *Finding sparse systems of parameters*, J. Pure Appl. Math. , (1993).

[12] P. Gianni, B. Trager, and G. Zacharias, *Gröbner bases and primary decomposition of polynomial ideals*, J. Symb. Comput. **6** 19–167, (1981).

[13] G. Hermann, *Die Frage der endlich vielen Schritte in der Theorie der Polynomideale*, Math. Ann. **95** 736–788, (1926).

[14] J. Herzog, Y. Takayama, and N. Terai, *On the radical of a monomial ideal*, Archiv der Math. **85**, 397–408 (2005).

[15] J. Herzog and B. Ulrich, *Self-linked curve singularities*, Nagoya Math. J. **120** 129–153, (1990).

[16] D. Hilbert, *Über die Theorie der algebraishcer Formen*, Math. Ann. **36** 473–534 (1897).

[17] J. Kollár, *Sharp Effective Nullstellensatz.* J. Amer. Math. Soc., **1**, (1988), 963-975.

[18] D. Knuth, *The art of computer programming vol. 2. Seminumerical algorithms* Reading: Addison-Wesley (1971).

[19] T. Krick and A. Logar, *An algorithm for the computation of the radical of an ideal in the ring of polynomials.* In Mattson et al (eds), Proc. 9th AAEEC. (Lect. Notes Comput. Sci. **539**, 195–205) Berlin Heidelberg New York: Springer (1991).

[20] D. Lazard, *Ideal bases and primary decomposition: case of two variables*, J. Symb. Comput., **1**, 261–270 (1985).

[21] D. Lazard, *Solving zero-dimensional algebraic systems*, J. Symb. Comput., **13**, 117-131- (1992).

[22] G. Scheja and U. Storch, *Über Spurfunktionen bei vollständigen Durchschnitten*, J. Reine Angew. Math. **278**, (1975), 157–170.

[23] A. Seidenberg, *On the Lasker-Noether decomposition theorem*, Amer. J. Math, **106**, 611–638, (1984).

[24] W. V. Vasconcelos, *Divisor Theory in Module Categories*, North-Holland Mathematics Studies, **14**, (1974).

[25] W. V. Vasconcelos, *Computational Methods in Commutative Algebra and Algebraic Geometry*, Springer-Verlag, 1998.

[26] W. V. Vasconcelos, *Arithmetic of Blowup Algebras*, London Math. Soc. Lecture Note Series, **195**, Cambridge Univ. Press, 1994.

[27] W.V. Vasconcelos, *Ideals generated by R-sequences*, J. Algebra **6**, 309–316 (1967).

Department of Mathematics, University of Virginia, Charlottesville, VA 22903
*Email address*: huneke@virginia.edu