Segre-driven radicality testing

Martin Helmer, Elias Tsigaridas

Segre-Driven Radicality Testing

Martin Helmer* Elias Tsigaridas†

September 28, 2023

This article is part of the volume titled "Computational Algebra and Geometry: A special issue in memory and honor of Agnes Szanto".

Dedication:
Agnes was a prominent member of the community in the area of symbolic-numeric computation and an excellent person who had a positive impact to all of us that we were lucky enough to meet and hang out with her. Agnes left us far too soon but her dedication to the community and her spirit of kindness and generosity will never be forgotten. She will be greatly missed. We dedicate this article to her memory.

Abstract

We present a probabilistic algorithm to test if a homogeneous polynomial ideal I defining a scheme X in $\mathbb{P}^n$ is radical using Segre classes and other geometric notions from intersection theory which is applicable for certain classes of ideals. If all isolated primary components of the scheme X are reduced and it has no embedded components outside of the singular locus of $X_{\mathrm{red}} = \mathbb{V}(\sqrt{I})$, then the algorithm is not applicable and will return that it is unable to decide radically; in all the other cases it will terminate successfully and in either case its complexity is singly exponential in n. The realm of the ideals for which our radical testing procedure is applicable and for which it requires only single exponential time includes examples which are often considered pathological, such as the ones drawn from the famous Mayr-Meyer set of ideals which exhibit doubly exponential complexity for the ideal membership problem.

1 Introduction

We consider the problem of testing if an ideal is radical, or in other words if the associated scheme is reduced. More precisely, for a homogeneous ideal $I = \langle f_1, \ldots, f_s \rangle$ in $\mathbb{C}[x_0, x_1, \ldots, x_n]$ with d being the maximum degree of the polynomials f_i, we present a (probabilistic) algorithm to test if the scheme $X \subset \mathbb{P}^n$ defined by I is reduced, i.e., to test if I is radical (up to saturation by the irrelevant ideal). When all of the isolated primary components of X are reduced and when, in addition, X has no embedded components outside of the singular locus of $X_{\mathrm{red}} = \mathbb{V}(\sqrt{I})$, then the algorithm is unable to decide if the input is radical; in cases of failure the worst case complexity is singly exponential in n, however to resolve the question in these cases classical doubly exponential methods would need to be employed. In all the other cases the radical is not explicitly computed and the worst case complexity is singly exponential in n. To understand what types of embedded components we can deal with, while maintaining the singly exponential complexity bound, consider the following example.

*Corresponding Author
Room 4122, SAS Hall North Carolina State University, Raleigh, North Carolina 27695, USA.
Email: mhelmer@ncsu.edu
†Inria Paris, Institut de Mathématiques de Jussieu - Paris Rive Gauche, Sorbonne Université and Paris Université, France.
Email: elias.tsigaridas@inria.fr

Example 1 (Embedded components outside the singular locus of the radical)**.** *We work in* $\mathbb{P}^2$ *with coordinates* x, y, z *and we consider the scheme* X *defined by the ideal*

$$I = \left\langle -x^2y^2 + y^3z, -x^4 + x^2y\,z \right\rangle = \langle x^2 - yz\rangle \cap \langle y^2, x^4 - x^2yz\rangle.$$

In this case the only isolated primary component of X *is the reduced component* $X_{\mathrm{red}} = \mathbb{V}(x^2 - yz)$*; also* X_{red} *is a smooth curve in* $\mathbb{P}^2$ *and so its singular locus is empty. However,* X *has an embedded component, corresponding to the second ideal in the primary decomposition above, supported on the point* $[0:0:1]$*. The presence of this embedded component would be detected by our algorithm using methods which have singly exponential worst case complexity in the number of variables.*

A more interesting example of an ideal $I = \langle f_1, \ldots, f_s\rangle$, defining a scheme X with embedded components outside the singular locus of X_{red}, is furnished by the homogeneous version of the Mayr-Meyer ideals [34] introduced by Bayer and Stillman [4]. The Mayr-Meyer family of ideals is generated by polynomials of degree $\mathcal{O}(d)$ in $\mathcal{O}(n)$ variables. Ideals in this family have the property that for some polynomial $f \in I$ the polynomials r_i which solve the ideal membership problem via the expression $f = \sum_i r_i f_i$ are such that $\deg(r_i)$ is doubly exponential in n, i.e., $\mathcal{O}(d^{2^n})$. In [4, §2] a family of Mayr-Meyer ideals J_n is described in a ring with $10n$ variables and these generators are homogenized to give a homogeneous ideal J_n' in $10n+1$ variables. Consider the $n = 2$ case; in this case the homogeneous ideals J_2' are ideals in a ring with the 21 variables, i.e., $S_0, S_1, F_0, F_1, a_0, a_1, b_0, b_1, c_0, c_1, d_0, d_1, e_0, e_1, f_0, f_1, g_0, g_1, h_0, h_1, z$. One of these ideals is as follows (additional examples may be generated using the Macaulay2 [16] function `mayr` in [17]):

$$\begin{aligned} I = \langle & S_0h_0 - F_1z, S_0g_0 - F_0h_0, S_0f_0 - F_0h_0, F_0e_0 - F_0h_0, S_0e_0 - S_1z, F_0d_0h_0 - F_1z^2, F_0a_0h_0 - S_1z^2, \\ & F_0c_0g_0 - F_0h_0z, F_0b_0f_0 - F_0h_0z, F_0a_0f_0 - F_0d_0g_0, F_0c_0d_1f_0h_1 - F_0d_0g_0h_1z, \\ & F_0c_0c_1f_0g_1 - F_0d_0g_0g_1z, F_0b_1c_0f_0f_1 - F_0d_0f_1g_0z, F_0a_1c_0e_1f_0 - F_0d_0e_1g_0z\rangle. \end{aligned} \quad (1)$$

The ideal I defines a scheme $X \subset \mathbb{P}^{20}$ of codimension three. The irreducible component $\mathbb{V}(F_0, S_0, z)$ contains the embedded components $\mathbb{V}(z, g_0, f_0, F_0, S_0, F_1e_0 - S_1h_0)$ and $\mathbb{V}(z, f_0 - g_0, e_0 - h_0, d_0, c_0, b_0, a_0, F_0, S_1 - F_1, S_0)$; neither of these components is contained in the singular locus of $X_{\mathrm{red}} = \mathbb{V}(\sqrt{I})$.

While it seems to us interesting that many pathological examples, such as the Mayr-Meyer examples, with potentially numerous and complicated embedded components, can be considered by our algorithm in time at most singly exponential in the number of variables, it is worth noticing that many desirable (and perhaps more mundane seeming) examples, such as all ideals which are radical, are not covered by our approach. The latter case of course includes an ideal generated by generic polynomials, which is expected to be radical, so this is in that sense the "most common" case. Nevertheless, if we have the information that the ideal is "generic", then we can combine our approach with other algorithms that have single exponential complexity bounds in this case, e.g., [27, 2].

We now give a brief conceptual overview of our approach. For a homogeneous ideal I in $\mathbb{C}[x_0, \ldots, x_n]$ we consider the scheme $X = \mathbb{V}(I) \subset \mathbb{P}^n$ associated to it. We first sample (at least one) generic point p_i in each isolated primary component W_i of X and compute the multiplicity of p_i in W_i via a calculation which requires only the computation of the degree of an ideal (we do this in singly exponential time). If a generic point has multiplicity greater than one, then the associated component is not reduced and I is not radical. If all isolated primary components are reduced, then we compute the singularity subscheme of X, $\mathbb{Sing}(X) = \mathbb{V}(J)$ which is defined by an ideal J whose generators consist of the $\mathrm{codim}(X) \times \mathrm{codim}(X)$ minors of the Jacobian matrix of a generating set of I (along with the generators of I). This scheme $\mathbb{Sing}(X)$ has primary components whose support is either an embedded component of X not contained in the singular locus of X_{red} or else are supported on the singular locus of X_{red}. We use a multiplicity based test to identify the presence of embedded components of the first type. If no non-reduced structures in X have been identified at this stage of the algorithm we are unable to decide and it would be required that $\sqrt{I}$ be computed with standard methods.

We should also mention that we present a method to compute the multiplicity of an irreducible variety contained in some lower dimensional isolated primary component of a scheme (which is new); see Sections 3.2

and 3.3 and also (12). This method requires only the computation of dimension and the degree of a polynomial ideal and makes no assumptions on their structure. We can compute the dimension and the degree of an algebraic variety in single exponential time, e.g., [25].

Remark 2. *We note that all methods presented in this note are probabilistic in the sense that they require the, in practice random, choice of general constants to define various coefficients used in computation of the Hilbert-Samuel multiplicity and Segre class. A careful analysis of the probabilistic aspects of such methods can be found in [20, 21] and will not be repeated here.*

Historically, many different algorithms to test if an ideal I is radical have been presented in the literature; in most of the cases they test for radicality in the process of computing the radical or the primary decomposition. Roughly speaking, these algorithms tend to consist of a step which computes the radical $\sqrt{I}$, a step which computes a reduced Gröbner basis for both the ideal and its radical (in the same term order), and a step which checks if I and $\sqrt{I}$ have the same reduced Gröbner basis. For the step which computes the radical of I, the best known algorithms have (worst case) bounds *doubly exponential* in the number of variables or in the dimension of the ideal I, e.g., the algorithm of [30] has complexity $(rd)^{2^{\mathcal{O}(n^2)}}$ and that of [26] has complexity doubly exponential in the dimension of I; other algorithms have similar or worse bounds in the general case.

In particular, the algorithm by Krick and Logar [26] is based on Gröbner basis computations (extension-contraction of ideals). Even though the algorithm has double exponential worst case complexity, if these intermediate computations, for specially structured ideals, could be performed faster, then the complexity of the algorithm could be improved as well. Also, the algorithm involves the saturation of an ideal, which, as in our case, seems to be the (complexity) bottleneck of the analysis. Along the same lines, Laplagne's algorithm [30] performs iterative saturations with respect to one polynomial. It also relies on (a notion of) maximal independent sets, that allows us to perform a reduction of the problem to the 0-dimensional case, and contraction of ideals. For special polynomial systems, that is when we can perform these operations fast(er), then we can claim that the complexity of the algorithm is single exponential, instead of double exponential.

Let us also mention, that in certain special cases, such as when I is unmixed [26, Proposition 4.1], I is a complete intersection [2], or I has dimension zero or one [27], the dedicated algorithms have single exponential complexity bounds (in the number of variables n). The complexity of computing the Gröbner basis for the second step of testing if I is radical is analogous to radical computation, though in practice the computation of $\sqrt{I}$ is often much more difficult than computing a reduced Gröbner basis for I. Another approach of testing if an ideal is radical is to use the algorithm [11] that computes the primary decomposition, see also [14, 39, 7]. This approach also has doubly exponential worst case complexity in the number of variables.

On other previous work

Regarding other related work on polynomial system solving, primary and equidimensional decomposition, and radical computation, let us mention the work of Durvye and Lecerf [9] that present a stand-alone proof of Kronecker solver for solving polynomial systems, that is based on representing the polynomials as black boxes that allows us to evaluate them. It can also output a symbolic representation of the roots. Probably, the most recent addition to the complexity results in polynomial systems solving is the work of van der Hoeven and Lecerf [41] that achieves nearly quadratic, with respect to the Bézout number, arithmetic complexity bound, for sufficiently generic systems. It is a Las Vegas algorithm and it is based on the Kronecker solver, see [9], and some recent advances on multipoint evaluation.

Durvye [8] introduces an algorithm for computing the local algebras of the roots of a 0-dim polynomial system. One of its main characteristics is that its complexity depends on the cost of evaluating the input polynomials at a point (and on the Bézout number). Lecerf [32] presents a probabilistic algorithm that computes the equidimensional decomposition of the Zariski closure of the solution set of a system of polynomials equations and inequalities. One of the main novelties is the representation of the components by the means of generic fibers. The complexity is (essentially) cubic with respect to the degree of the (intermediate) systems

that it solves during its process, also called geometric degree, while it operates with polynomials represented as straight line programs. Also Lecerf [31], along the same lines, introduced an algorithm to perform an equidimensional decomposition of an algebraic variety, based on the Kronecker solver, see also [9]. For a predecessor of this algorithm, we refer to Giusti and Heintz [15] that they introduced algorithms for primary and irreducible decomposition of an algebraic variety

To obtain the equidimensional decomposition, we might also use the closely related algorithm(s) for computing efficiently the Chow form of a variety. For the state-of-the-art for this problem in the arithmetic complexity model we refer to Jeronimo et al [22].

Terminology and Notation

Since our algorithm arises from geometric ideas in intersection theory we will frequently find it useful to employ more geometric terminology (as we have in the introduction); we now make this terminology precise. We will, for the most part, work over an algebraically closed field of chacterisitic zero which we will denote k; usually this will be the complex numbers $\mathbb{C}$ or the algebraic closure of the rationals, $\overline{\mathbb{Q}}$. In particular, given a polynomial ideal I in $k[x_0, \ldots, x_n]$ we will think of it as defining a subscheme X of either $\mathbb{P}^n$ if I is homogeneous, or k^{n+1} if not; in both cases we will write $\mathbb{V}(I)$ for this *scheme* X defined by I. A variety will be a reduced scheme (we do not assume that a variety is irreducible). When the ideal I has primary decomposition $I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_r$, then we will refer to the schemes $\mathbb{V}(\mathfrak{q}_i)$ as *primary components* of X. Similarly we will refer to the scheme $\mathbb{V}(\mathfrak{q}_i)$ as an *isolated primary component*, if $\mathfrak{p}_i = \sqrt{\mathfrak{q}_i}$ is a minimal prime. The irreducible varieties $\mathbb{V}(\mathfrak{p}_i)$ for minimal primes $\mathfrak{p}_i$ will be called *irreducible components*, while the irreducible varieties $\mathbb{V}(\mathfrak{p}_j)$ for embedded primes $\mathfrak{p}_j = \sqrt{\mathfrak{q}_j}$ will be called *embedded components*. We write X_{red} for the reduced subscheme associated to the scheme X, i.e., X_{red} denotes the variety defined by $\sqrt{I}$.

Outline of the paper. In the next section we present the necessary background for Segre class computations and summarize symbolic methods for sampling at least one point in each irreducible component of a subscheme of affine space. Section 3 contains a collection of various results needed by our algorithm. In particular we show how to compute the degree of the isolated primary components of a scheme, and how to compute the multiplicities. Finally, in Section 4 we present our algorithm along with a proof of its correctness and a complexity analysis.

2 Background

We briefly review several important concepts and results which will be used extensively in later sections. In particular we review the notion of Segre classes and their association to the so called *algebraic* or *Hilbert-Samuel multiplicity*. We will also review how we can sample and represent symbolically points on a variety using the *Rational Univariant Representation (RUR)*.

2.1 Segre Classes and Algebraic Multiplicity

The algorithm that we present in Section 4 makes extensive use of ideas from (computational) intersection theory [13], and in particular of Segre classes. Below we give a brief overview of the relevant objects.

In general the Segre class $s(X, Y)$ is defined for pairs of schemes $X \subset Y$ and is an element of the *Chow group* $A_*(X)$of X (see [13, §4] for details); when X is smooth we will employ convention of writing $A^*(X)$ for a Chow ring graded by codimension. We will restrict our discussion to the case where X and Y are subschemes of a projective space $\mathbb{P}^n$ and will instead (via pushforward) consider the Segre class $s(X, Y)$ as an element of the *Chow ring* of the ambient projective space $\mathbb{P}^n$, $A^*(\mathbb{P}^n)$. More explicitly, if H is the rational equivalence class of a hyperplane in $\mathbb{P}^n$, then we will represent elements in the Chow ring $A^*(\mathbb{P}^n)$ as polynomials in H with integer coefficients via the isomorphism $A^*(\mathbb{P}^n) \cong \mathbb{Z}[H]/(H^{n+1})$; in this representation the rational

equivalence class of an irreducible variety V of codimension c is $[V] = \deg(V) \cdot H^c \in A^*(\mathbb{P}^n)$, where $\deg(V)$ denotes the *degree* of the variety V. Hence, in our setting the Segre class $s(X, Y)$ will be represented as a polynomial of degree at most n in H with integer coefficients.

Consider subschemes $X \subset Y$ of $\mathbb{P}^n$ and let $\mathrm{Bl}_X Y$ denote the blowup of Y along X. This comes equipped with a map $\pi : \mathrm{Bl}_X Y \to Y$ and an exceptional divisor $E = \pi^{-1}(X)$. In the case where Y is an irreducible variety and $I_X = (f_0, \ldots, f_r)$ is the ideal defining the scheme X we have that $\mathrm{Bl}_X Y$ is isomorphic to the graph Γ of $f_0, \ldots, f_r$. More specifically, the graph is

$$\Gamma = \overline{\{(y, z) \mid y \in Y, \;\; z = (f_0(y) : \cdots : f_r(y))\}} \subset \mathbb{P}^n \times \mathbb{P}^r,$$

and $\Gamma \cong \mathrm{Bl}_X Y$. In this setting π is the projection map $\Gamma \to Y$ from the graph onto Y and the exceptional divisor E is the inverse image of X under this projection map. The blowup (and hence the graph) captures information about how X sits inside Y and in particular quantifies how singular the embedding of X in Y is.

Informally speaking, the Segre class attempts to extract key parts of this information by considering how $E = \pi^{-1}(X)$ intersects with a similar scheme which is perturbed to be in general position inside of Γ. How 'general' of a position we can put a version of $\pi^{-1}(X)$ into within Γ is significantly determined by how closely X and Y are related. We now give a formal definition of the Segre class $s(X, Y)$.

Definition 3. *Let $X \subset Y$ be subschemes of $\mathbb{P}^n$. We have a blowup diagram*

$$\begin{array}{ccc} E & \longrightarrow & \mathrm{Bl}_X Y \\ \downarrow{\scriptstyle \eta} & \square & \downarrow{\scriptstyle \pi} \\ X & \longrightarrow & Y\,, \end{array}$$

where E is the exceptional divisor. The Segre class *of X in Y is*

$$s(X, Y) = \eta_*((1 - E + E^2 - \ldots) \cdot [E]) \in A_*(X).$$

We will abuse notation and also write $s(X, Y)$ for the pushforward to $A^*(\mathbb{P}^n)$.

We now briefly review results of [18] which give an explicit and computable expression for the Segre class. Using the notation above, consider the rational map $pr_X : Y \to \mathbb{P}^r$ which is defined by $pr_X : p \mapsto (f_0(p) : \cdots : f_r(p))$. We then have the following diagram:

$$\begin{array}{ccccc} & & \mathrm{Bl}_X Y & \subset & \mathbb{P}^n \times \mathbb{P}^r \\ & \swarrow^{\pi} & & \searrow^{\rho} & \\ Y & & \xrightarrow{\quad pr_X \quad} & & \mathbb{P}^r \end{array} \tag{2}$$

Computationally, rather than trying to understand the self intersections of $\pi^{-1}(X)$ we will instead seek to understand $pr_X^{-1}(\mathbb{P}^{r-\dim(Y)-i}) - X$ for $i = 0, \ldots, \dim(Y)$. In particular we will study the *projective degrees*, $\mathfrak{d}_i(X, Y)$, which are the coefficients appearing in the class

$$G(X, Y) = \sum_{i=0}^{\dim(Y)} [pr_X^{-1}(\mathbb{P}^{r-\dim(Y)-i}) - X] = \sum_{i=0}^{\dim(Y)} \mathfrak{d}_i(X, Y) H^{n-i}.$$

We now give explicit expressions for these objects in terms of polynomial ideals in $k[\boldsymbol{x}] = k[x_0, \ldots, x_n]$, the homogenous coordinate ring of $\mathbb{P}^n$. As above, k is an algebraically closed field of characteristic zero.

Definition 4 (Projective Degrees)**.** *Consider the subschemes $X \subset Y \subset \mathbb{P}^n$. Let X be defined by the homogeneous ideal $I_X = (f_0, \ldots, f_r)$ and let d be the maximum degree of the defining polynomials of X. We*

can, without loss of generality, assume that $\deg(f_i) = d$ *for all* $0 \leq i \leq r$. *Define the projection of* Y *along* X *as the rational map*

$$\begin{array}{rccc} \pi_X : & Y & \dashrightarrow & \mathbb{P}^r \\ & \boldsymbol{p} & \mapsto & (f_0(\boldsymbol{p}) : \cdots : f_r(\boldsymbol{p})). \end{array} \tag{3}$$

The projective degrees of π_X *are the sequence of integers* $(\mathfrak{d}_0(X,Y), \ldots, \mathfrak{d}_{\dim(Y)}(X,Y))$, *where*

$$\mathfrak{d}_i(X,Y) = \deg\left(\pi_X^{-1}\left(\mathbb{P}^{r-(\dim(Y)-i)}\right) - X\right). \tag{4}$$

Equivalently (via [18, Proposition 3.3]), we can define the projective degrees of π_X *as*

$$\mathfrak{d}_i(X,Y) = \deg(Y \cap L^{(i)} \cap \mathcal{U} - X), \tag{5}$$

where $\mathcal{U} = \mathbb{V}(P_1, \ldots, P_{\dim(Y)-i})$ *with* $P_j = \sum_{\nu=0}^{r} \lambda_\nu f_\nu$ *for generic* $\lambda_\nu \in k$ *and* $L^{(i)} \subset \mathbb{P}^n$ *is a generic linear space of codimension* i.

Using the latter characterization of projective degrees, we can express them with respect to the ideals corresponding to the subschemes $X \subset Y \subset \mathbb{P}^n$, that is $I_X = \langle f_0, \ldots, f_r \rangle$ and I_Y. Let t be a new variable; then, for $0 \leq i \leq r$, we define the family of ideals

$$\mathcal{I}_i = I_Y + \left\langle \sum_{j=0}^{r} \lambda_{1,j} f_j, \ldots, \sum_{j=0}^{r} \lambda_{\dim(Y)-i,j} f_j, \ell_1(\boldsymbol{x}), \ldots, \ell_i(\boldsymbol{x}), \ell_0(\boldsymbol{x}) - 1, 1 - t \sum_{j=0}^{r} \lambda_{0,j} f_j \right\rangle \subset k[\boldsymbol{x}][t], \tag{6}$$

where $\ell_\nu(\boldsymbol{x}) = \sum_{j=0}^{n} \theta_{\nu,j} x_j$ for generic $\theta_{l,j} \in k$, and generic $\lambda_{l,j} \in k$. We also write $\mathcal{I}_i(X,Y)$ to denote the dependency on the subschemes X and Y. By [18, Theorem 3.5] the projective degree of dimension i can be computed as

$$\mathfrak{d}_i(X,Y) = \dim_k\left(k[\boldsymbol{x},t]/\mathcal{I}_i\right). \tag{7}$$

In [18, §3] an explicit formula for the Segre class $s(X,Y)$ is given which depends only on the numbers $\mathfrak{d}_i(X,Y)$ obtained via the computation in (7) and the degree d of the generators of I_X (though the final Segre class does not depend on d). The projective degrees can also be used to compute the *algebraic multiplicity* of a variety inside a scheme.

Let $X \subset \mathbb{P}^n$ be an irreducible (and reduced) subvariety and let $Y \subset \mathbb{P}^n$ be a pure dimensional subscheme with $X \subset Y$ and with corresponding ideals $I_X = \langle f_0, \ldots, f_r \rangle$ and I_Y in $k[\boldsymbol{x}] = k[x_0, \ldots, x_n]$. The *algebraic or Hilbert-Samuel multiplicity* of X on Y, denoted $e_X Y$, is the integer coefficient of $[X]$ in the Segre class $s(X,Y)$. This multiplicity is more classically defined via the Hilbert-Samuel polynomial of the local ring $(k[x_0, \ldots, x_n]/I_Y)_{I_X}$, where the subscript denotes localization at the prime ideal I_X, see, e.g., [13, Example 4.3.1, Example 4.3.4] or [10, Chapter 12]. In practice we will compute this multiplicity as follows. Let d be the maximum degree among a set of generators of I_X. By [18, Theorem 5.2] we have that

$$e_X Y = \frac{\deg(Y) d^{\dim(Y)-\dim(X)} - \mathfrak{d}_{\dim(X)}(X,Y)}{\deg(X)}, \tag{8}$$

where $\mathfrak{d}_{\dim(X)}(X,Y)$ is the dimension X projective degree of X in Y, see (7), (5), or Definition 4.

By [13, Ex. 12.4.5(b)] (originally proved in a commutative algebra setting by Samuel [38]) we have that $e_X Y = 1$ if and only a generic point in X is not contained in the singularity subscheme of Y. We state this as a proposition below.

Proposition 5 (Example 12.4.5(b) of [13])**.** *Let* $X \subset \mathbb{P}^n$ *be an irreducible subvariety and let* $Y \subset \mathbb{P}^n$ *be a pure dimensional subscheme. Then* $e_X Y = 1$ *if and only if a generic point in* Y *is reduced and* X *is not contained in the singular locus of the reduced subscheme of* Y, Y_{red}.

This fact along with a formula derived in §3.2 will be adapted to furnish a test which tells us when an isolated primary component of a scheme is generically reduced.

In the final section we will additionally need to work with varieties X which are not irreducible, hence it is simpler to express our criterion in terms of the $\dim(X)$ part of the Segre class. Let Y be a pure dimensional subscheme of $\mathbb{P}^n$ and let X be a closed subscheme of Y. Let d be the maximum degree of the equations defining X. With the notations above the result of [18, Corollary 3.14] gives the following expression for the part of the Segre class $s(X, Y)$ in dimension equal to $\dim(X)$:

$$\{s(X,Y)\}_{\dim(X)} = d^{\dim(Y)-\dim(X)} \deg(Y) - \mathfrak{d}_{\dim(X)}(X,Y). \tag{9}$$

2.2 Rational Univariate Representation and Computing One Point in Each Irreducible Component

An important part of the main algorithm presented in Section 4 is the ability to sample points from each irreducible component of a scheme $X \subset \mathbb{C}^n$. Approximate point samples could be furnished using methods such as homotopy continuation from numeric algebraic geometry [40], we however opt for symbolic methods, e.g., [36], in our presentation as these methods have well understood worst case complexities. We note that our algorithm certainly could be implemented using numerical methods instead, see also Remark 12. In the symbolic setting, it is important for the sampling algorithms we employ to have an efficient and exact representation of the sampled points. For this we exploit the *rational univariate representation (RUR)* [37], see also [1, 33].

Briefly, given a zero dimensional ideal in $\mathbb{Q}[x_1, \ldots, x_n]$, RUR represents the coordinates of the associated points as a univariate rational function evaluated at the roots of univariate polynomial. It is of the form $R(t), x_1 = \frac{R_1(t)}{R_0(t)}, \ldots, x_n = \frac{R_n(t)}{R_0(t)}$ where $R, R_0, R_1, \ldots, R_n \in \mathbb{Q}[t]$ and t is a new variable. The following theorem provides a brief presentation of RUR and summarizes some of its important properties.

We note in the Theorem statement below we consider the (reduced) zero set associated to a polynomial system (or polynomial ideal). These methods do not require that the input polynomials define a radical ideal but will only furnish information about the zero set of the input polynomials, i.e., about the associated reduced subscheme.

Theorem 6. *Consider the solution set $W = \{x \in \mathbb{C}^n \mid f_1(x) = \cdots = f_n(x) = 0\}$, where the polynomials $f_i \in \mathbb{Z}[x_1, \ldots, x_n]$ are dense of degree d and maximum coefficient bitsize τ. Then, there is an algorithm that computes univariate polynomials of $R, R_1, \ldots, R_n \in \mathbb{Z}[t]$ such that:*

1. *The degrees of $R, R_1, \ldots, R_n$ are all bounded by d^n and their bitsize by $\mathcal{O}(d^n + nd^{n-1}\tau)$.*
2. *For any root ξ of $R(t) = 0$, the tuple $r(\xi) := \left(\frac{R_1(\xi)}{R'(\xi)}, \ldots, \frac{R_n(\xi)}{R'(\xi)}\right) \in (\mathbb{C}^*)^n$ is a point in W; R' is the derivative of R with respect to t. We call this representation the Rational Univariate Representation (RUR) [37].*
3. *The set of points $\{r(\xi) \in \mathbb{C}^n \mid R(\xi) = 0\}$ contains all the 0-dimensional irreducible components of W in $\mathbb{C}^n$.*
4. *We compute the RUR by performing $d^{\mathcal{O}(n)}$ arithmetic operations.*

Proof. For the bounds on the bitsize of the coefficients and a generalization to the sparse case and how we compute the RUR using resultants we refer the reader to [33, Theorem 4.3]. For item 3 we refer the reader to [36]. In the case where the system is 0-dimensional, then the multiplicities of the roots are preserved and we can recover them from the multiplicities of the roots of $R(t)$ [37].

To compute the RUR in the case where the system is not 0-dimensional we use Canny's generalized characteristic polynomial [6], or the toric variant by Rojas [36, 35, Main Theorem 2.4], that rely on Macaulay

and sparse resultant matrices, respectively, see [33]. If the system is not 0-dimensional, then the idea is to perform a symbolic perturbation, using a new variable s, of the input polynomials; for example we perturb all the diagonal entries of the Macaulay matrix in the dense case [6] or all the monomials in the toric case [36, Main Theorem 2.3 and 2.4], to ensure that the determinant of the corresponding resultant matrix is not zero. Then, we extract the resultant as the first non-vanishing coefficient of the resultant of the perturbed system, which is a univariate polynomial in s. We refer the reader to [36, 33] for the specific details.

The complexity bound follows from [5]. Let us mention that we compute the various resultants as determinants, or quotient of determinants, of matrices the elements of which are multivariate polynomials. □

We remark that the above result is presented in the case of a square system, however if the system is not square, then one may simply take a general linear combination of the generators to get a square system and verify which sampled points satisfy the original system. To get samples from all irreducible components of higher dimensions we may then add a generic linear polynomial to the defining ideal (i.e., intersect the scheme with a generic hyperplane) and repeat this procedure. Such considerations are discussed in more detail in the references.

The algorithms (and the corresponding mathematical results) that support Theorem 6 allow us to sample at least one (generic) point from each irreducible component of an arbitrary subscheme of $\mathbb{C}^n$. The symbolic algorithms that support these computations rely on resultant or Gröbner basis computations and careful analysis of the bitsize of the involved polynomial computations. We refer the interested reader to [12] for an approach based on Bézoutian matrices, to [33, 36] for an approach based on resultant matrices and to [24] for an implementation. This leads us to the following corollary.

Corollary 7. *Let I be a polynomial ideal generated by polynomials of degree at most d in $\mathbb{Q}[x_1, \ldots, x_n]$ defining a scheme $X \subset \mathbb{C}^n$. Then, we can obtain a collection of RUR of points containing at least one generic point in each irreducible component of X in at most $d^{\mathcal{O}(n)}$ arithmetic operations.*

3 A Collection of Results Which Enable Our Algorithm

In this section we gather together several results which will be employed by our main algorithm which is presented in Section 4. First in §3.1, we show how the degree of isolated primary components of any dimension can be computed in worst case singly exponential time with respect to the number of variables. Finally, in §3.2 and §3.3, we look at multiplicity and (partial) Segre class computations relative to isolated primary components of any dimension and how these computations can be done in a generic affine patch of projective space.

3.1 The Degree of Isolated Primary Components of a Scheme in Singly Exponential Time

In this subsection we describe how we can use methods to compute a geometric equidimensional decomposition such as [23], along with zero dimensional Gröbner basis computation, to obtain the sum of the degrees of all isolated primary components of a scheme of a given dimension. Given an ideal $I = \langle f_1, \ldots, f_r \rangle$ in the polynomial ring $\mathbb{Z}[x_1, \ldots, x_n]$ where $\deg(f_i) + 1 \leq d$ for all i which defines a scheme $X = \mathbb{V}(I) \subseteq \mathbb{C}^n$, we will show in Proposition 9, that this degree computation has worst case complexity bounded by $d^{\mathcal{O}(n^3)}$. We note that this computation takes as input only the generators of the ideal I.

The algorithm of [23] takes as input the ideal I and outputs (a straight-line program) defining (distinct) polynomial ideals $K_{i_1}, \ldots, K_{i_m}$ where these ideals give an equidimensional decomposition of the variety $X_{\text{red}} = \mathbb{V}(\sqrt{I})$, i.e.,

$$X_{\text{red}} = (\mathbb{V}(K_{i_1}))_{\text{red}} \cup \cdots \cup (\mathbb{V}(K_{i_m}))_{\text{red}},$$

where $(\mathbb{V}(K_{i_j}))_{\text{red}}$ is the union of all irreducible components of X_{red} of dimension i_j.

Without loss of generality we may assume that $i_1 > \cdots > i_m$. For each j let L_j be a general linear form in $\mathbb{C}[x_1, \ldots, x_n]$. Suppose that $K_{i_j} = \langle g_1, \ldots, g_r \rangle$ and define the polynomial $P(K_{i_j}, T)$ in $\mathbb{C}[x_1, \ldots, x_n, T]$ as

$$P(K_{i_j}, T) := 1 - T \cdot \sum_{\nu=1}^{r} \lambda_\nu g_\nu \tag{10}$$

for general constants $\lambda_\nu \in \mathbb{C}$. Fix a desired dimension μ and let $i_\nu > \mu \geq 0$ where i_ν is the smallest dimension which appears in the decomposition for which this inequality is true, note we require a strict inequality here as we seek to remove all components of dimension strictly larger than μ. To avoid trivialities we assume $i_1 > \mu \geq 0$. Define the *(isolated) degree in dimension* μ of I as

$$\deg_\mu(I) := \dim_{\mathbb{C}} \mathbb{C}[x_1, \ldots, x_n, T_1, \ldots, T_\nu]/\mathfrak{J}(\mu), \tag{11}$$

where

$$\mathfrak{J}(\mu) := I + \langle L_1, \ldots, L_\mu \rangle + \langle P(K_{i_1}, T_1), \ldots, P(K_{i_\nu}, T_\nu) \rangle.$$

If X is the subscheme of $\mathbb{C}^n$ defined by I we will define

$$\deg_\mu(X) := \deg_\mu(I).$$

Note that if there are no components of dimension μ for a chosen μ the system $\mathfrak{J}(\mu)$ has no solutions and hence the degree is zero.

Proposition 8. *Let I be a polynomial ideal in $\mathbb{Q}[x_1, \ldots, x_n]$. Suppose that the ideal $\mathfrak{I}_\mu$ is the intersection of all μ-dimensional isolated primary components of I. Then, with $\deg_\mu(I)$ as in (11), we have*

$$\deg_\mu(I) = \deg(\mathfrak{I}_\mu).$$

Proof. Note that this result is essentially an application of the standard Rabinowitsch trick. Let X be the scheme defined by I in $\mathbb{C}^{n+\nu}$. By construction all primary components of X which had dimension greater than $\mu + \nu$ in $\mathbb{C}^{n+\nu}$ (corresponding to components of $\mathbb{V}(I) \subset \mathbb{C}^n$ having dimension greater than μ in $\mathbb{C}^n$) have an empty intersection with the scheme defined by $\langle P(K_{i_1}, T_1), \ldots, P(K_{i_\nu}, T_\nu) \rangle$, note this also applies to any embedded components of X of any dimension which is contained in an isolated primary component of X of dimension greater than $\mu + \nu$ in $\mathbb{C}^{n+\nu}$. Note for points $(x_1, \ldots, x_n)$ not in $(\mathbb{V}(K_{i_l}))_{\text{red}}$ the polynomial $P(K_{i_l}, T)$ has a single solution of multiplicity one, hence intersection with these hypersurfaces can be thought of a intersection with hyperplanes for isolated primary components of X of dimension less than or equal to μ. Since the linear forms L_j are general and there are μ of them the conclusion follows since the only points which remain in the zero dimensional scheme defined by $\mathfrak{J}(\mu)$ came from those in the scheme defined by $\mathfrak{I}_\mu$. □

Finally we note that the expression in (11) can be computed in singly exponential time in the number of variables. More specifically we have the following result.

Proposition 9. *Consider a polynomial ideal $I = \langle f_1, \ldots, f_r \rangle$ in the polynomial ring $\mathbb{Z}[x_1, \ldots, x_n]$ where $\deg(f_i) + 1 \leq d$. For any $\mu \leq \dim(I)$, the worst case complexity of computing the expression $\deg_\mu(I)$ is bounded in $d^{\mathcal{O}(n^2)}$.*

Proof. From results [23, Theorem 9] we know the degree of the polynomials g_ν appearing in (10) is bounded by d^n. The output of [23] consists of polynomials in straight-line programs representation. However, using evaluation/interpolation we can convert them to a dense representation, using the bound on their degree.

Note that $\nu < n$ and we work in $n + \nu$ variables, hence we can bound the number of variables by $n + (n - 1) = 2n - 1$ Since the ideal $\mathfrak{J}(\mu)$ has dimension zero by construction, using standard bounds on the computation of Gröbner basis in dimension zero [19, 29] (or for other methods to compute the degree of a zero dimensional ideal) gives $(d^n)^{2n-1}$, since we have equations of degree at most d^n in $2n - 1$ variables, giving $d^{\mathcal{O}(n^2)}$. □

3.2 Multiplicity of a Subvariety in Isolated Primary Components

Using the dimension sensitive degree function from §3.1 and the multiplicity formula (8) we obtain a method to compute the multiplicity of an irreducible variety contained in the union of all ν-dimensional isolated primary components of a scheme $Y \subset \mathbb{P}^n$ with multiple components of different dimensions.

Let $Y \subset \mathbb{P}^n$ be an arbitrary subscheme. Let W be the union of all isolated primary components of Y of dimension ν and let $X = \mathbb{V}(f_0, \ldots, f_r) \subset \mathbb{P}^n$ be an irreducible subvariety of W with the generators chosen such that $\deg(f_i) = d$. Define the ideal

$$\mathcal{I}_\nu(X) = \mathcal{I}(X, W) = I_Y + \left\langle \sum_{j=0}^{r} \lambda_{1,j} f_j, \ldots, \sum_{j=0}^{r} \lambda_{\nu-\dim(X),j} f_j, \ell_0(\boldsymbol{x}) - 1, 1 - t \sum_{j=0}^{r} \lambda_{0,j} f_j \right\rangle \subset k[\boldsymbol{x}][t].$$

Since Y has isolated primary components of dimension ν the scheme $\mathbb{V}(\mathcal{I}_\nu(X))$ has isolated primary components of dimension equal to $\dim(X)$. Then, since $X \subset W$ we have

$$e_X W = \frac{\deg_\nu(Y) d^{\nu-\dim(X)} - \deg_{\dim(X)}(\mathcal{I}_\nu(X))}{\deg(X)}. \tag{12}$$

We note that this formula follows immediately from (8) since the functions $\deg_\nu$ and $\deg_{\dim(X)}$, respectively, will capture the degrees of the ν and $\dim(X)$ dimensional isolated primary components only, respectively. Hence, since X is contained in the pure ν-dimensional scheme W, the primary components of other dimensions play no role and we immediately obtain $e_X W$. Note that the only required inputs here are the equations for X and Y, which are used to construct the ideal $\mathcal{I}_\nu(X)$, the dimension sensitive degree function from §3.1 will require only the equations for $\mathcal{I}_\nu(X)$. For identical reasons we obtain an analogous version of (9) which we state below:

$$\{s(X, W)\}_{\dim(X)} = d^{\nu-\dim(X)} \deg_\nu(Y) - \deg_{\dim(X)}(\mathcal{I}_\nu(X)). \tag{13}$$

We note that these computations take as input only the equations defining the schemes X and Y and that their complexity is determined by that of the degree function of §3.1, see Proposition 9. We can also extend this to the case where X is an arbitrary variety not contained in W, but contained in Y, using [13, Example 4.3.4], or the similar result for Segre classes, [13, Lemma 4.2], however this extension will not be needed for our purposes here. It is worth noting, however, that in particular the result of [13, Lemma 4.2] implies that if $X \cap W$ is empty then $s(X, W) = 0$ and that if $\dim(X \cap W) < \dim(X)$ then $\{s(X, W)\}_{\dim(X)} = 0$, and further it follows from results in [18] that all these properties hold for the formula given above, e.g. (9) and (13).

3.3 Computing Multiplicity via Degree in Affine Patches

Let $X \subset W \subset \mathbb{P}^n$ with X a variety and W the union of all dimension ν isolated primary components of $Y \subset \mathbb{P}^n$. Suppose that $I_X = \langle f_0, \ldots, f_r \rangle$ and without loss of generality assume $d := \deg(f_i)$ for all i. Take $\ell_0(x) \in \mathbb{C}[x_0, \ldots, x_n]$ to be a general linear form and set $\hat{I}_X = I_X + \langle \ell_0 - 1 \rangle$ and $\hat{I}_Y = I_Y + \langle \ell_0 - 1 \rangle$. Finally, let $\hat{Y} \subset \mathbb{C}^{n+1}$ be the scheme defined by the ideal $I_Y + \langle \ell_0 - 1 \rangle$, let $\hat{W}$ be the pure ν-dimensional subscheme of $\hat{Y}$ arising from W and let $\hat{X} = \mathbb{V}(\hat{I}_X) \subset \mathbb{C}^{n+1}$. Note that $\hat{X}$ is a subvariety of $\hat{W}$ and that the degrees and dimensions are unchanged, i.e., $\deg(X) = \deg(\hat{X})$, $\deg_\mu(Y) = \deg_\mu(\hat{Y})$ for all μ such that Y has an isolated primary component of dimension μ, $\dim(X) = \dim(\hat{X})$, and $\dim(Y) = \dim(\hat{Y})$. We can think of this procedure of moving to the ideal $\hat{I}$ from I as a combination of dehomogenizing with respect to a general point at infinity and linearly embedding $\mathbb{C}^n$ into $\mathbb{C}^{n+1}$. Now let $\phi_i = f_i$ for $i = 1, \ldots, r$ and $\phi_{r+1} = \ell_0 - 1$, set

$$\hat{\mathcal{I}}_\nu(X) = \hat{I}_Y + \left\langle \sum_{j=0}^{r} \lambda_{1,j} \phi_j, \ldots, \sum_{j=0}^{r} \lambda_{\nu-\dim(X),j} \phi_j, \ell_0(\boldsymbol{x}) - 1, 1 - t \sum_{j=0}^{r} \lambda_{0,j} \phi_j \right\rangle \subset k[\boldsymbol{x}][t],$$

and as in the previous subsection

$$\mathcal{I}_\nu(X) = I_Y + \left\langle \sum_{j=0}^{r} \lambda_{1,j} f_j, \ldots, \sum_{j=0}^{r} \lambda_{\nu-\dim(X),j} f_j, \ell_0(\boldsymbol{x}) - 1, 1 - t \sum_{j=0}^{r} \lambda_{0,j} f_j \right\rangle \subset k[\boldsymbol{x}][t].$$

Observe that $\dim(\mathcal{I}_i) = \dim(\hat{\mathcal{I}}_i)$ and that $\deg_\nu(\mathcal{I}_i) = \deg_\nu(\hat{\mathcal{I}}_i)$. Hence if we define

$$e_{\hat{X}}\hat{W} := \frac{\deg_\nu(\hat{Y}) d^{\nu-\dim(\hat{X})} - \deg_{\dim(X)}(\hat{I}_\nu(X))}{\deg(\hat{X})}, \tag{14}$$

then using (12) we immediately obtain that $e_{\hat{X}}\hat{W} = e_X W$. This equivalence will be used extensively in the sequel to allow us to freely switch between projective and affine formulations. Applying this discussion to (9) also immediately gives the following formula for the dimension $\dim(X)$ part of the Segre class of X in W:

$$\{s(X,W)\}_{\dim(X)} = \deg_\nu(\hat{Y}) d^{\nu-\dim(\hat{X})} - \deg_{\dim(X)}(\hat{I}_\nu(X)), \tag{15}$$

Note that, since (9) holds for general subschemes X we no longer need to assume that X is irreducible or reduced, we only require X is a subscheme of W. In Algorithm 1 we will abuse notation and write $\{s(\hat{X},\hat{W})\}_{\dim(X)}$ to mean the expression $\{s(X,W)\}_{\dim(X)}$ computed via the affine formula (15) above.

4 Testing if an Ideal is Radical

In this section we present our main algorithm, Algorithm 1, for testing if a scheme Y in $\mathbb{P}^n$ is reduced or, equivalently, if the defining ideal is radical up to saturation by the irrelevant ideal. First, in §4.1, we give the idealized version (i.e., we assume that we can work over $\mathbb{C}$) and that for a point sampled from an irreducible component we obtain the associated maximal ideal in $\mathbb{C}[x_0,\ldots,x_n]$. Next, in §4.2, we explain how we would adapt Algorithm 1 to perform computations with (groups of) sampled points represented in the Rational Univariate Representation (RUR), as it is required for a realistic symbolic implementation.

4.1 Algorithm

Here we present our main algorithm, Algorithm 1, to test if a homogeneous ideal fails to be radical, up to saturation by the irrelevant ideal. We begin with a proof of correctness. We note that Algorithm 1 is probabilistic in the sense that the algorithm to compute Segre classes on which it depends is probabilistic, see Remark 2.

Theorem 10. *Given a homogeneous ideal I in $k[x_0,\ldots,x_n]$ Algorithm 1 correctly tests if $I : \langle x_0,\ldots,x_n\rangle^\infty$ is not radical or else returns that it is unable to decide and terminates in finite time. In particular, any cases where I has non-radical isolated components or embedded components outside the singular locus are successfully detected.*

Proof. The fact that Line 7 detects all isolated primary components which are non-reduced follows from Proposition 5, combined with (14) and (15), and the fact that we work with a single reduced point in the first factor of the Segre class. Now we consider the case where Line 16 detects embedded components which are not contained in the singular locus of Y_{red}. First, note that if q is a reduced point in the singular subscheme of Y, then either q is contained in an embedded component which is embedded outside of the singular locus of Y_{red} or q is inside the singular locus of Y_{red}. Note the loop in Line 14 starts in top dimension. Suppose that ν is the largest value such that q is contained in W_ν (in the notation of the algorithm). If q is inside the singular locus of Y_{red} then its multiplicity will always be greater than one in W_ν and $s(q,W_\rho) = 0$ for $\rho > \nu$ since q cannot be contained in these. If q is not inside the singular locus of Y_{red} then it must be inside some embedded component of Y. In this case q will also be contained in some higher dimensional isolated primary component,

but then since we know all the isolated primary components are reduced, and since multiplicity is computed relative to the top dimensional component, we will obtain that the multiplicity of q is one inside this highest dimensional component in which it is contained by Proposition 5. Hence we will have correctly identified the existence of any embedded components outside of the singular locus of Y_{red}. The algorithm terminates since there are finitely many components. □

Algorithm 1: DETECTABLEY_NON_RADICAL

Input: A homogeneous ideal $I = \langle f_0, \ldots, f_r \rangle \subset \mathbb{C}[x_0, \ldots, x_n]$ defining a subscheme Y of $\mathbb{P}^n$.

Output: TRUE if our tests are able to detect that Y is non-reduced, i.e. true if Y has non-reduced isolated components or if Y has embedded components outside the singular locus. Otherwise return FALSE as we are unable to decide.

1 Set $\ell_0(x)$ to be a generic (random) homogeneous linear form in $\mathbb{C}[x_0, \ldots, x_n]$;
2 Set $\hat{I} = I + \langle \ell_0 - 1 \rangle$; Set $\hat{Y}$ to be the subscheme of $\mathbb{C}^{n+1}$ associated to $\hat{I}$;
3 **for** $\nu = \dim(\hat{Y}), \ldots, 0$ **do**
4 Compute (at least) one generic point in each dim. ν irreducible component of $\hat{Y}$ via the method summarized in Corollary 7. Call the resulting collection of points $\{p_1, \ldots, p_m\} \subset \mathbb{C}^{n+1}$;
5 **for** $p \in \{p_1, \ldots, p_m\}$ **do**
6 Let $W(p)$ denote the isolated primary component of $\hat{Y}$ containing p;
7 Compute $\{s(p, W(p))\}_0$ using (15);
8 **if** $\{s(p, W(p))\}_0 \neq 1$ **then**
9 RETURN TRUE [*we have detected that the input fails to be radical; there is a non-reduced isolated component*];
10 Set $c = \operatorname{codim}(Y, \mathbb{P}^n)$;
11 Set $J = I + \mathfrak{Jac}_c(I)$ where $\mathfrak{Jac}_c(I)$ is the ideal generated by the $c \times c$ minors of the Jacobian matrix of $f_0, \ldots, f_r$; Set $\hat{J} = J + \langle \ell_0 - 1 \rangle$;
12 Using the method of Corollary 7 compute (at least) one generic point in each irreducible component of the singular subscheme $\mathbb{V}(\hat{J})$ of $\hat{Y}$, call this collection of points $\{q_1, \ldots, q_s\} \subset \mathbb{C}^{n+1}$;
13 **for** $q \in \{q_1, \ldots, q_s\}$ **do**
14 **for** *W_ν the union of isolated primary comp. of $\hat{Y}$ of dim. ν, starting from top dim.* $\nu = \dim(Y)$ **do**
15 Compute $\{s(q, W_\nu)\}_0$ using (15) ;
16 **if** $\{s(q, W_\nu)\}_0 = 1$ **then**
17 q is contained in an embedded component of Y but not in the singular locus of Y_{red};
18 RETURN TRUE [*we have detected that the input fails to be radical; there is an embedded component outside the singular locus*];
19 **if** $\{s(q, W_\nu)\}_0 > 0$ **then**
20 BREAK to line 13 and select the subsequent point q in the list;
21 RETURN FALSE [*we are unable to determine if the input is radical using our tests*].

Remark 11 (Using Algorithm 1 to Determine if an Ideal is Radical)**.** *Consider a homogeneous ideal I defining a scheme Y in $\mathbb{P}^n$. To use Algorithm 1 to test if Y is reduced, or equivalently to test if $I : \langle x_0, \ldots, x_n \rangle^\infty$ is radical, we first run Algorithm 1 with input I, then we proceed as follows:*

- *If Algorithm 1 returns* TRUE *then we may immediately conclude that Y is* **not** *reduced, i.e. we may conclude that $I : \langle x_0, \ldots, x_n \rangle^\infty$ is* **not** *radical.*
- *If Algorithm 1 returns* FALSE *then we know that all isolated components of Y are reduced and that Y has no embedded components outside the singular locus, but we cannot determine if Y is reduced from*

Algorithm 1 alone. Hence if Algorithm 1 returns FALSE*, then to decide if Y is reduced we must compute $\sqrt{I}$ and compare the result to I using other methods.*

We note again that Algorithm 1 as presented above assumes points in $\mathbb{C}^n$ can be represented exactly, in §4.2 we see how this could be done in practice using a rational univariate representation, below we briefly remark on some of the considerations for developing an approximate numeric version of Algorithm 1.

Remark 12 (Numerical Version of Algorithm 1)**.** *One could implement a version of Algorithm 1 using methods from numerical algebraic geometry [40] for point sampling and Segre class computations (via (15)). For both tasks, implementations such as Bertini [3], PHCPack [42], or the* `NumericalAlgebraicGeometry` *Macaulay2 [16] package could be employed. The only step which could not be implemented, at least straightforwardly, numerically is Line 21. However, we do not focus on this case here. We instead focus on the case where points are represented symbolically since our primary aim is to give complexity bounds and these are well understood for the symbolic methods such as [36] which we employ (via the adaptations discussed in §4.2 below, see Remark 17 specifically). To furnish a reliable numerical implementation would require us to establish bounds on the precision needed in the points sampled in Lines 4 and 12. The bound on the precision ensures that the numeric versions of the degree computations in (15) would produce the correct results using the approximate points (since (15) uses the defining equations of the point, which would in the numeric case be approximate).*

We now prove a worst case complexity bound for the operations preformed in Algorithm 1 above.

Theorem 13. *Let $I = \langle f_0, \ldots, f_r \rangle$ be a homogeneous ideal in $k[x_0, \ldots, x_n]$ with $\deg(f_i) \leq d$ defining a scheme Y in $\mathbb{P}^n$. Algorithm 1 has worst case complexity bounded in $d^{\mathcal{O}(n^4)}$, that is singly exponential in n.*

Proof. The complexity of Algorithm 1 is that of the $\deg_\nu$ function applied to an ideal generated by polynomials of degree no more than d^n, as this is the upper bound on the degree of the generators of the ideal J defined in line 11 of Algorithm 1. The conclusion then follows by Proposition 9. □

Remark 14 (The minors of the Jacobian)**.** *We should note that Algorithm 1 also computes, Line 11, all the $c \times c$ minors of the Jacobian. Each minor requires a determinant computation; this costs $\mathcal{O}(c^{\omega+1})$, where ω is the exponent of the complexity of matrix multiplication [28], [43]. There, are $\binom{r+1}{c} \cdot \binom{n+1}{c} \leq (16rn)^c$ minors; since $c \leq n$, this number is bounded by $(16rn)^n$. As r, the number of polynomials, is part of the input this bound is still singly exponential in n, if we ignore the (poly)logarithmic factors in the exponent. Even more, it is reasonable to assume that for all practical cases $r = \mathcal{O}(d^n)$.*

4.2 Using Points Represented in the Rational Univariate Representation

In the previous subsection we assumed that we can represent all the points exactly as maximal ideals in our ambient coordinate ring. In practice, that is working on a computer, we will in fact work in the ring $\mathbb{Q}[x_1, \ldots, x_m]$ and so we need a (computationaly efficient) way to represent each point which may appear in our algorithm in this ring. We will use the *rational univariate representation (RUR)*, see Theorem 6.

Consider the zero dimensional ideals defining sets of points in $\mathbb{C}^m$; usually for our purposes in what follows $m = n + 2$. We now consider the representation of points in RUR and how this interacts with multiplicity computation (14) and (partial) Segre class computation (15). To setup the context and the notation for a 0-dimensional ideal $\mathcal{I} \subset \mathbb{Q}[x_1, \ldots, x_m]$ the RUR of $(\mathbb{V}(\mathcal{I}))_{\text{red}}$ corresponds to the ideal

$$J = \left\langle R(\theta), x_1 - \frac{A_1(\theta)}{R'(\theta)}, \ldots, x_m - \frac{A_m(\theta)}{R'(\theta)} \right\rangle \subset \mathbb{Q}(\theta)[x_1, \ldots, x_m],$$

where $R, A_1, \ldots, A_m \in \mathbb{Q}[\theta]$ are square-free polynomials. Equivalently, we will consider the RUR of $(\mathbb{V}(\mathcal{I}))_{\text{red}}$ as the ideal

$$\mathcal{J} = \left\langle R(\theta), 1 - T \cdot R'(\theta), x_1 R'(\theta) - A_1(\theta), \ldots, x_m R'(\theta) - A_m(\theta) \right\rangle \subset \mathbb{Q}[x_1, \ldots, x_m, \theta, T].$$

Further, there is a $\mathbb{Q}$-algebra isomorphism between $\mathbb{Q}[x_1,\ldots,x_m]/\sqrt{\mathcal{I}}$ and $\mathbb{Q}(\theta)[x_1,\ldots,x_m]/J$, and between $\mathbb{Q}[x_1,\ldots,x_m]/\sqrt{\mathcal{I}}$ and $\mathbb{Q}[x_1,\ldots,x_m,\theta,T]/\mathcal{J}$, and the variety $(\mathbb{V}(\mathcal{I}))_{\text{red}}$ consists of $\deg(R(\theta))$ reduced points [37].

The following result let us compute the zero dimensional part of the Segre class of a set of points inside a scheme when the set of points is represented using a RUR.

Theorem 15. *Let $I = \langle f_1,\ldots,f_r\rangle$ be a homogeneous ideal in $\mathbb{Q}[x_0,\ldots,x_n]$ defining a scheme Y in $\mathbb{P}^n$ and let X be a zero dimensional variety (i.e., a union of reduced points) contained in Y. Fix a (general) dehomogenization of I via the linear form $\ell_0(x)$ corresponding to a generic affine patch of $\mathbb{P}^n$; this gives the scheme $\hat{Y}$ in $\mathbb{C}^{n+1}$ defined by the ideal $\hat{I} = \langle f_1,\ldots,f_r,\ell_0-1\rangle$ and a zero dimensional variety $\hat{X}\subset\hat{Y}\subset\mathbb{C}^{n+1}$ arising from X. Let $\mathcal{J} = \langle R(\theta), 1-T\cdot R'(\theta), x_0R'(\theta)-A_0(\theta),\ldots,x_nR'(\theta)-A_n(\theta)\rangle$ be a polynomial ideal in $\mathbb{Q}[x_0,\ldots,x_n,\theta,T]$ giving a RUR of $\hat{X}$ and set*

$$\mathcal{J}_{\text{cord}} = \langle g_0,g_1,\ldots,g_n\rangle := \left\langle x_0R'(\theta)-A_0(\theta),\ldots,x_nR'(\theta)-A_n(\theta)\right\rangle.$$

Finally consider the polynomial ring $\mathbb{Q}[x_0,\ldots,x_n,\theta,t,T]$ and define the ideal

$$\mathcal{I} = \hat{I} + \langle P_1,\ldots,P_{\dim(Y)},1-tP_0\rangle + \langle R(\theta),1-T\cdot R'(\theta)\rangle \subset \mathbb{Q}[x_0,\ldots,x_n,\theta,t,T],$$

where $P_j = \sum_{i=0}^n \lambda_i^{(j)} g_i$ for general $\lambda_i^{(j)}\in\mathbb{Q}$. Then

$$\{s(X,Y)\}_0 = \deg(Y)\cdot\deg(R(\theta))^{\dim(Y)} - \dim_{\mathbb{Q}}\left(\mathbb{Q}[x_0,\ldots,x_n,\theta,t,T]/\mathcal{I}\right).$$

Proof. In what follows, we will work in the affine patch specified by $\ell_0 = 1$. First note that X is a finite set of (reduced) points and hence we have that $\deg(X) = \#X = \deg(R(\theta))$; set $D = \#X$. Consider $\mathcal{I}$ as an ideal in $\mathbb{C}[x_0,\ldots,x_n,\theta,t,T]$, i.e., work over the complex numbers. By the fundamental theorem of algebra $R(\theta) = (\theta-a_1)\cdots(\theta-a_D)$, where $a_1,\ldots,a_D$ are the complex roots of $R(\theta)$; here we assume wlog that R is monic. Then in this ring we have

$$\mathcal{I} = \hat{I} + \bigcap_{i=1}^{D}\langle P_1(\theta,x),\ldots,P_{\dim(Y)}(\theta,x),1-tP_0(\theta,x),\theta-a_i,1-T\cdot R'(\theta)\rangle.$$

Since each ideal making up this intersection is prime (by construction since the $\lambda_i^{(j)}$ are general) then its degree is exactly the cardinality of the variety $V(\mathcal{I})$. Clearly, since the terms $\theta-a_i$ appearing in each factor of the ideal intersection are linear and since, given a fixed θ^*, the polynomial $1-TR'(\theta^*)$ is linear in T (and of course cannot have solutions where $R'(\theta^*)$ vanishes. It follows that the points in $V(\mathcal{I})\subset\mathbb{C}^{n+4}$ are in one to one correspondence with the points in $V(\mathcal{I}')\subset\mathbb{C}^{n+2}$ where

$$\mathcal{I}' = \hat{I} + \bigcap_{i=1}^{D}\langle P_1(a_i,x)/R'(a_i),\ldots,P_{\dim(Y)}(a_i,x)/R'(a_i),(1-tP_0(a_i,x))/R'(a_i)\rangle \text{ in } \mathbb{C}[x_0,\ldots,x_n,t].$$

Now note that $P_i(a_i,x)/R'(a_i)$ is exactly $\sum_{k=0}^n\lambda_k(x_k-b_k)$ where $\langle x_0-b_0,\ldots,x_n-b_n\rangle$ is the unique maximal ideal of the i^{th} point in X. Let $I_X = \langle w_0,\ldots,w_s\rangle$ in the ring $\mathbb{C}[x_0,\ldots,x_n]$ be the radical ideal which defines X and is given by the intersection of the maximal ideals of the D points in X; we have $\deg(w_i) = \#X = \deg(R(\theta))$. Note that if we compute the ideal intersection defining $\mathcal{I}'$ it is exactly the ideal

$$\mathfrak{V} = \hat{I} + \left\langle \sum_{i=1}^s \rho_i^{(1)}w_i,\ldots,\sum_{i=1}^s\rho_i^{(\dim(Y))}w_i, 1-t\left(\sum_{i=1}^s\rho_i^{(0)}w_i\right)\right\rangle \subset \mathbb{Q}[x_0,\ldots,x_n,t],$$

where the $\rho_i^{(j)}$ are constants determined by products and sums of the $\lambda_i^{(j)}$ defining the P_i; these constants remain general since the $\lambda_i^{(j)}$ are general. Since $D = \deg(w_i) = \deg(R(\theta))$ then by (6), (7), and (9) along with the discussion above, we have that

$$\begin{aligned}\{s(X,Y)\}_0 &= \deg(Y)\cdot D^{\dim(Y)} - \dim_{\mathbb{Q}}\left(\mathbb{Q}[x_0,\ldots,x_n,t]/\mathfrak{V}\right)\\ &= \deg(Y)\cdot \deg(R(\theta))^{\dim(Y)} - \dim_{\mathbb{Q}}\left(\mathbb{Q}[x_0,\ldots,x_n,\theta,t,T]/\mathcal{I}\right).\end{aligned}$$

□

This result in conjunction with Proposition 16 below, which can be used in Lines 8 and 16 of Algorithm 1 via the RUR of a zero dimensional variety $\hat{X}$. As noted in the proof this criterion is in effect testing all the multiplicities of dimension zero components at once.

Proposition 16. *Let Y be a scheme in $\mathbb{P}^n$, let W be the union of all ν-dimensional primary components of Y and let X a dimension zero variety fully contained in W and such that no point in X is in the singular locus of W_{red}. Then $\{s(X,W)\}_0 > \deg(X)$ if and only if W is not reduced.*

Proof. By [13, Example 4.3.4] we know that $\{s(X,W)\}_0$, the coefficient of the dimension 0 part of the Segre class, is the sum of the multiplicities of W along each point in X. For W to be reduced we require that it is reduced at a generic point (i.e., one outside the singular locus of W_{red}), in light of Proposition 5 we see that in particular we need $e_pW = 1$ for each $p \in X$ (since $\dim(X) = 0$), hence taken together, for W to be reduced we require the integer $\{s(X,W)\}_0$ to be equal the number of points in X. Conversely if W is reduced and all points in X are smooth in W_{red} (again via Proposition 5) $e_pW = 1$, for all $p \in X$; it follows that in this case we necessarily have $\{s(X,W)\}_0 = \deg(X)$. □

Remark 17 (Using the RUR in Algorithm 1)**.** *To use the RUR of sampled points in Algorithm 1 we make the following alterations:*

- *p in Line 6 and q in Line 13 are now both zero-dimensional varieties equal to the union of some set of reduced points represented as a RUR;*
- *in Line 7 we use Theorem 15 in conjunction with (15) to obtain the needed part of the Segre class and the criterion in Line 8 becomes $\{s(p,W(p))\}_0 > \deg(p)$ by Proposition 16;*
- *in Line 15 we use Theorem 15 in conjunction with (15) to obtain the needed part of the Segre class and the criterion in Line 16 becomes $\{s(q,W_\nu)\}_0 = \deg(q)$ by Proposition 16.*

The rest of the algorithm remains as it appears in Algorithm 1.

Acknowledgements The authors are grateful to Peter Bürgisser for various discussions and suggestions on the problems of computing the radical and testing for radicality. Elias Tsigaridas is partially supported by ANR JCJC GALOP (ANR-17-CE40-0009) and the PHC GRAPE. Martin Helmer is partially supported by the Air Force Office of Scientific Research (AFOSR) under grant: FA9550-22-1-0462.

References

[1] M.-E. Alonso, E. Becker, M.-F. Roy, and T. Wörmann. Zeros, multiplicities, and idempotents for zero-dimensional systems. In *Algorithms in algebraic geometry and applications*, volume 143 of *Progress in Mathematics*, pages 1–15. Springer, 1996.

[2] I. Armendáriz and P. Solernó. On the computation of the radical of polynomial complete intersection ideals. In *International Symposium on Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes*, pages 106–119. Springer, 1995.

[3] D. J. Bates, J. D. Hauenstein, A. J. Sommese, and C. W. Wampler. Bertini: Software for numerical algebraic geometry. Available at bertini.nd.edu with permanent doi: dx.doi.org/10.7274/R0H41PB5.

[4] D. Bayer and M. Stillman. On the complexity of computing syzygies. *Journal of Symbolic Computation*, 6(2-3):135–147, 1988.

[5] J. Canny. Some algebraic and geometric computations in PSPACE. In *Proc. 20th annual ACM Symposium on Theory Of Computing (STOC)*, pages 460–467, 1988.

[6] J. Canny. Generalised characteristic polynomials. *Journal of Symbolic Computation*, 9(3):241–250, 1990.

[7] W. Decker, G.-M. Greuel, and G. Pfister. Primary decomposition: algorithms and comparisons. In *Algorithmic algebra and number theory*, pages 187–220. Springer, 1999.

[8] C. Durvye. Evaluation techniques for zero-dimensional primary decomposition. *Journal of Symbolic Computation*, 44(9):1089–1113, 2009.

[9] C. Durvye and G. Lecerf. A concise proof of the Kronecker polynomial system solver from scratch. *Expositiones Mathematicae*, 26(2):101–139, 2008.

[10] D. Eisenbud. *Commutative Algebra: with a view toward algebraic geometry*, volume 150. Springer Science & Business Media, 2013.

[11] D. Eisenbud, C. Huneke, and W. Vasconcelos. Direct methods for primary decomposition. *Inventiones mathematicae*, 110(1):207–235, 1992.

[12] M. Elkadi and B. Mourrain. A new algorithm for the geometric decomposition of a variety. In *Proc. International Symposium on Symbolic and Algebraic Computation (ISSAC)*, pages 9–16. ACM, 1999.

[13] W. Fulton. *Intersection theory*, volume 2. Springer Science & Business Media, 2013.

[14] P. Gianni, B. Trager, and G. Zacharias. Gröbner bases and primary decomposition of polynomial ideals. *Journal of Symbolic Computation*, 6(2-3):149–167, 1988.

[15] M. Giusti and J. Heintz. Algorithmes–disons rapides–pour la décomposition d'une variété algébrique en composantes irréductibles et équidimensionnelles. In *Effective Methods in Algebraic Geometry*, pages 169–194. Springer, 1991.

[16] D. R. Grayson and M. E. Stillman. Macaulay2, a software system for research in algebraic geometry. Available at http://www.math.uiuc.edu/Macaulay2.

[17] D. R. Grayson and M. E. Stillman. Macaulay2 Example Ideals Package. Available at https://github.com/Macaulay2/M2/blob/f0ce581750dfd94336883695d3552671410f32f5/M2/Macaulay2/packages/undistributed-packages/ExampleIdeals/mayr-meyer.m2.

[18] C. Harris and M. Helmer. Segre class computation and practical applications. *Mathematics of Computation*, 2019.

[19] A. Hashemi and D. Lazard. Complexity of Zero-dimensional Gröbner Bases. Research Report RR-5660, INRIA, 2005.

[20] J. D. Hauenstein and M. Helmer. Probabilistic saturations and alt's problem. *Experimental Mathematics*, 31(3):975–987, 2022.

[21] M. Helmer. A direct algorithm to compute the topological Euler characteristic and Chern-Schwartz-MacPherson class of projective complete intersection varieties. *Theoretical Computer Science*, 681:54–74, 2017.

[22] G. Jeronimo, T. Krick, J. Sabia, and M. Sombra. The computational complexity of the chow form. *Foundations of Computational Mathematics*, 4:41–117, 2004.

[23] G. Jeronimo and J. Sabia. Effective equidimensional decomposition of affine varieties. *Journal of Pure and Applied Algebra*, 169(2-3):229–248, 2002.

[24] J. Keyser, K. Ouchi, and J. M. Rojas. The exact rational univariate representation for detecting degeneracies. *DIMACS Series in Discrete Mathematics and Theoretical Computer Science*, 67:299, 2005.

[25] P. Koiran. Randomized and deterministic algorithms for the dimension of algebraic varieties. In *Proc. 38th Annual Symposium on Foundations of Computer Science (FOCS)*. IEEE Comput. Soc, 1997.

[26] T. Krick and A. Logar. An algorithm for the computation of the radical of an ideal in the ring of polynomials. In *International Symposium on Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes*, pages 195–205. Springer, 1991.

[27] T. Krick and A. Logar. Membership problem, representation problem and the computation of the radical for one-dimensional ideals. In *Effective Methods in Algebraic Geometry*, pages 203–216. Springer, 1991.

[28] G. Labahn, V. Neiger, and W. Zhou. Fast, deterministic computation of the Hermite normal form and determinant of a polynomial matrix. *Journal of Complexity*, 42:44–71, Oct. 2017.

[29] Y. N. Lakshman. A single exponential bound on the complexity of computing Gröbner bases of zero dimensional ideals. In *Effective Methods in Algebraic Geometry*, pages 227–234. Birkhäuser Boston, 1991.

[30] S. Laplagne. An algorithm for the computation of the radical of an ideal. In *Proc. ACM International Symposium on Symbolic and Algebraic Computation (ISSAC)*, pages 191–195. ACM, 2006.

[31] G. Lecerf. Computing an equidimensional decomposition of an algebraic variety by means of geometric resolutions. In *Proceedings of the 2000 international symposium on Symbolic and algebraic computation*, pages 209–216. ACM, 2000.

[32] G. Lecerf. Computing the equidimensional decomposition of an algebraic closed set by means of lifting fibers. *Journal of Complexity*, 19(4):564–596, 2003.

[33] A. Mantzaflaris, E. Schost, and E. Tsigaridas. Sparse rational univariate representation. In *Proc. ACM on Int'l Symposium on Symbolic and Algebraic Computation (ISSAC)*, pages 301–308. ACM, 2017.

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

[35] J. M. Rojas. Toric generalized characteristic polynomials. *Arxiv preprint math/9702222*, 1997.

[36] J. M. Rojas. Solving degenerate sparse polynomial systems faster. *Journal of Symbolic Computation*, 28(1-2):155–186, 1999.

[37] F. Rouillier. Solving zero-dimensional systems through the rational univariate representation. *J. of Appl. Algebra in Engin., Comm. and Computing*, 9(5):433–461, 1999.

[38] P. Samuel. *Méthodes d'algèbre abstraite en géométrie algébrique*, volume 428. Springer, Berlin, 1955.

[39] T. Shimoyama and K. Yokoyama. Localization and primary decomposition of polynomial ideals. *Journal of Symbolic Computation*, 22(3):247–277, 1996.

[40] A. J. Sommese, C. W. Wampler, et al. *The Numerical solution of systems of polynomials arising in engineering and science*. World Scientific, 2005.

[41] J. van Der Hoeven and G. Lecerf. On the complexity exponent of polynomial system solving. *Foundations of Computational Mathematics*, 21:1–57, 2021.

[42] J. Verschelde. Algorithm 795: PHCpack: A general-purpose solver for polynomial systems by homotopy continuation. *ACM Trans. Math. Softw.*, 25(2):251–276, 1999.

[43] J. Von Zur Gathen and J. Gerhard. *Modern computer algebra*. Cambridge university press, 2013.