Complexity of the Wu-Ritt decomposition*

Ágnes Szántó

Cornell University

Abstract

Given a polynomial ideal $\mathcal{I}$ by a generating set of polynomials, we present an efficient parallel algorithm to express the radical of $\mathcal{I}$ as an intersection of unmixed ideals, each represented by a triangular set of polynomials. This triangular structure is convenient for many purposes, e.g. for conducting symbolic computation on the common roots of the polynomials in the ideal, or for computing the union, the intersection or the quotient of radicals. The sequential (parallel) complexity of our algorithm is subexponential (subpolynomial).

1 Introduction

The notion of a *characteristic set* of an ideal was first introduced by J.F. Ritt in 1950 [16] in the context of differential geometry. In 1984 Wu Wen-Tsün [22] realized the power of characteristic sets in commutative algebra and in automated geometric theorem proving. In the subsequent years, numerous results appeared about different applications, and characteristic sets became one of the most fundamental computational tools in commutative algebra. The "triangular" structure of characteristic sets, i.e. that each variable is introduced by one polynomial, is convenient for example when computing the common complex roots of polynomials or when conducting symbolic computation on the common roots without explicitly computing them. Although we might lose information about the original ideal when we consider only characteristic sets, the roots of the polynomials in the characteristic set and the roots of the polynomials in the ideal are related: only the degenerate cases, when leading coefficients of the characteristic set vanish, give superflous roots.

Our objective is to give an efficient method for finding a generalization of the Wu-Ritt characteristic sets in which the computational convenience of characteristic sets is preserved, but no information is lost about the roots of the polynomials in the ideal. It turns out that characteristic sets and decomposition of algebraic varieties are closely related: the Wu-Ritt prime decomposition algorithm, which expresses radicals as an intersection of ideals generated (or represented) by irreducible characteristic sets, were already proposed by Ritt in 1950 then by Wu in 1984 [16, 22], and modified by Kalkbrener and Wang in 1993 [13, 20]. In spite of their elegance and simplicity, these algorithms often compute superflous components embedded in other components, and no complexity analysis has been given for the worst case running time. As Kalkbrener notes it: "The complexity of computing characteristic sets has been analyzed by Gallo and Mishra (1990) [6]. But we do not know the complexity of the prime decomposition algorithm of Ritt and Wu or the complexity of the method presented in this paper [13]. We think that a complexity analysis of algorithms of this type and a comparison with the results in Chistov and Grigor'ev (1983) [3, 8] and Giusti and Heintz (1990) [7] are challenging problems for future research" [13].

In this paper we present a Wu-Ritt type decomposition algorithm. Similarly as in [12] we express the radical of an ideal given by a generating set as the intersection of "unmixed" ideals (defined later) represented by characteristic sets. To overcome the problem of computing superflous components, and to give a complexity analysis for the algorithm we need to modify Kalkbrener's algorithm using a similar approach as in [3, 8], and to add some extra work. We give an algorithm which is efficiently parallelizable, and the sequential [parallel] complexity is $(d^{n^2})^{O(1)}$ $[(n\log(d))^{O(1)}]$, where n is the number of variables and d is the maximal degree of the polynomials in the generating set (same bounds as in [7, 3, 8]). Note that the above bound is optimal in the sense that there are ideals in n variables such that the generating sets of the ideals have maximal degree d but the maximal degree in the characteristic sets is d^n, thus the size of the output is d^{n^2} in the dense representation (see the example in [6]). On the other hand, there are indications [17] that the algorithms in the present paper can be modified to preserve sparseness. The complexity analysis in the sparse representation is a problem for future research.

Furthermore, given a set of "unmixed" varieties represented by characteristic sets, we give an algorithm for finding the same representation for the intersection and difference of the varieties in the given set. Also, our method

*This research was supported by NSF grant CCR-9317320

gives a "lazy decomposition" procedure (see [4, 5]), which is an efficient algorithm for conducting symbolic arithmetic on algebraic numbers without explicitly computing them. In the zero-dimensional subcase both of these algorithms are in the complexity class NC (using arithmetic circuits over $\mathbb{Q}$). These results have applications for instance in mechanical geometric theorem proving [21], in resolving singularities of plane curves ([14, 18]) and of higher dimensional varieties, which is the subject of ongoing research.

2 Basics

2.1 Wu-Ritt Characteristic sets

Before defining Wu-Ritt characteristic sets, first we give some definitions following the approach in [2].

We consider polynomials in the polynomial ring $\mathbb{Q}[x_1, \ldots, x_n]$. Assume that the variables are linearly ordered by their subscript: $x_1 < x_2 < \cdots < x_n$. Then *class(p)* denotes the highest indeterminate appearing in a polynomial p, and $\mathrm{lc}(p)$ denote the leading coefficient of p regarded as a univariate polynomial in class(p). So, if class(p) $= x_k$ then $\mathrm{lc}(p) \in \mathbb{Q}[x_1, \ldots, x_{k-1}]$.

We call a set of polynomials $G = \{g_1, \ldots, g_k\}$ an *ascending set* if class(g_i) < class(g_j) for all $i < j$. E.g. $G = \{x_1x_2,\ x_1^3x_3^2 - x_1x_2^4,\ x_4^2,\ x_1x_2 + x_5\}$ is an ascending set because $\mathrm{class}(x_1x_2) = x_2 < \mathrm{class}(x_1^3x_3^2 - x_1x_2^4) = x_3 < \mathrm{class}(x_4^2) = x_4 < \mathrm{class}(x_1x_2 + x_5) = x_5$.

The procedure *pseudo division* generalizes the method of division with remainder for univariate polynomials to multivariate polynomials. Let $f, g \in \mathbb{Q}[x_1, \ldots, x_n]$ be polynomials with class(g) $= x_j$. Then there exist polynomials q and r and a number $\alpha \in \mathrm{N}$ such that

$$\mathrm{lc}(g)^{\alpha} f = qg + r$$

where $\deg_{x_j}(r) < \deg_{x_j}(g)$ and $\alpha \leq \deg_{x_j}(f) - \deg_{x_j}(g) + 1$. We denote by $r = \mathrm{prem}(f, g)$ the *pseudo remainder* of f by g, and by $q = \mathrm{pquo}(f, g)$ the *pseudo quotient* of f by g. If α is minimal, then q and r are uniquely determined.

In order to generalize the pseudo remainder concept for ascending sets, consider an ascending set $G = \{g_1, \ldots, g_k\} \subset \mathbb{Q}[x_1, \ldots, x_n]$ and a polynomial $f \in \mathbb{Q}[x_1, \ldots, x_n]$. There exists a sequence of polynomials $f_k = f, \ldots, f_0$ such that for each $k \geq s \geq 1$, f_{s-1} is the pseudo remainder obtained when dividing f_s by g_s. Combining these pseudo divisions for $k \geq s \geq 1$ we get that

$$\mathrm{lc}(g_r)^{\alpha_r} \cdots \mathrm{lc}(g_1)^{\alpha_1} f = \sum_{s=1}^{k} q_s g_s + f_0$$

and we denote by $f_0 = \mathrm{prem}(f, G)$ the pseudo remainder of f by G. Note that $\deg_{x_{i_s}}(f_0) < \deg_{x_{i_s}}(g_s)$ if class(g_s) $= x_{i_s}$ ($s = 1, \ldots k$). We say that f is *reduced* modulo the ascending set G if $f = \mathrm{prem}(f, G)$.

We give two definitions (and characterizations) of Wu-Ritt characteristic sets [2, 6]:

1. [6] If $G \subset \mathcal{I}$ is an ascending set, then it is a characteristic set of the ideal $\mathcal{I}$ if and only if for every element $f \in \mathcal{I}$, $\mathrm{prem}(f, G) = 0$.
Thus, if G is a characteristic set of the ideal $\mathcal{I}$, then

$$\langle G \rangle \subseteq \mathcal{I} \subseteq \{h \in \mathbb{Q}[x_1, \ldots, x_n] \mid \mathrm{prem}(h, G) = 0\}.$$

The above inclusions are usually proper.
Example: If $\mathcal{I} = \langle x^2y^2 - x^2 - y^2 + 1,\ xy\rangle$ and $x < y$, then $G = \{x^3 - x, xy\}$ is a characteristic set, but $\langle x^3 - x, xy\rangle \neq \langle x^2y^2 - x^2 - y^2 + 1,\ xy\rangle$ because the dimensions of the corresponding varieties are not equal. Also, $\langle x^2y^2 - x^2 - y^2 + 1,\ xy\rangle \neq \mathcal{J} = \{h \mid \mathrm{prem}(h, G) = 0\}$; for instance y is in $\mathcal{J}$ but not in $\mathcal{I}$.

2. In the words of [2]: Informally, if F is a finite set of polynomials, then G is a characteristic set of the ideal $\langle F\rangle$ if G is ascending and F and G have "almost" the same zeros. More formally, if F is a finite set of polynomials, then G is a characteristic set of the ideal $\langle F\rangle$ if:
   - G is ascending set
   - any zero of F is a zero of G
   - any zero of G that is not a zero of any of G's leading coefficients is a zero of F.

As we mentioned earlier, our objective is to find a generalization of the notion of Wu-Ritt characteristic sets, where the computational convenience of ascending sets is preserved, but no information is lost about the roots of the polynomials in the ideal. Below we define unmixed ascending sets, which are ascending sets representing algebraic varieties such that all the irreducible components have the same dimension. We show that every algebraic variety can be expressed as the union of varieties represented by unmixed ascending sets, and we give an algorithm which finds this unmixed representation. In the next subsection we discuss the connection between characteristic sets and decomposition of algebraic varieties. This will lead us to our main subject, the unmixed representation of radical ideals.

2.2 Decomposition of algebraic varieties

We start this section with an example:

Example 1 In the example of the previous subsection, $V(x^2y^2 - x^2 - y^2 + 1,\ xy) \subset \mathrm{A}^2$ consist of the four points $\{(1,0), (-1,0), (0,1), (0,-1)\}$, while $V(x^3 - x, xy)$ contains the points $\{(1,0), (-1,0)\}$ together with the whole y axis. We saw in the previous subsection that all the superflous zeros of the characteristic set comes from "degenerate" cases, when leading coefficients vanish. A possible solution to avoid superflous roots would be to find the subvarieties of $V(x^3 - x) \subset \mathrm{A}^1$, at which leading coefficients of the polynomials in $\{x^2y^2 - x^2 - y^2 + 1,\ xy\}$ vanish. These leading coefficients are x and $x^2 - 1$, thus we can factor $V(x^3 - x) = V(x) \cup V(x^2 - 1)$. After reducing the polynomials modulo $x^2 - 1$ and x, we get that

$$V(x^2y^2 - x^2 - y^2 + 1,\ xy) = V(x^2 - 1,\ y) \cup V(x, y^2 - 1).$$

Note that $\{x^2 - 1,\ y\}$ and $\{x, y^2 - 1\}$ are ascending sets and all the leading coefficients are 1. In the above example, we were able to express $\mathcal{I}$ as an intersection of two ideals which were generated by ascending sets, even though we could not find a generating characteristic set for $\mathcal{I}$.

More generally, suppose we are given an ideal $\mathcal{I} \subset \mathbf{Q}[x_1, \ldots, x_n]$. The example above suggests that if we could express the radical $\sqrt{\mathcal{I}}$ as

$$\sqrt{\mathcal{I}} = \mathcal{I}_1 \cap \ldots \cap \mathcal{I}_r$$

such that each $\mathcal{I}_i$ is generated by an ascending set, then this decomposition would preserve the computational convenience of ascending sets and give all the information about the roots of the polynomials in $\mathcal{I}$.

2.2.1 Zero dimensional ideals

In the case when the ideal $\mathcal{I}$ is zero dimensional, i.e. the polynomials in the ideal have only finitely many common zeros in $\mathbf{C}^n$, the prime decomposition of the radical will give the desired representation of the radical as intersection of ideals generated by ascending sets, as asserted by the following:

Proposition 2 *Let $\mathcal{P} \subset \mathbf{Q}[x_1, \ldots, x_n]$ be a zero-dimensional prime ideal. Then there exists an ascending set $G = \{g_1, \ldots, g_n\}$ such that G generates $\mathcal{P}$, $\mathrm{class}(g_i) = x_i$, $\mathrm{lc}(g_i) = 1$, and the image of g_i in $(\mathbf{Q}[x_1, \ldots, x_{i-1}]/\langle g_1, \ldots, g_{i-1}\rangle)[x_i]$ is irreducible.* ■

As a consequence, for a zero-dimensional prime ideal $\mathcal{P}$ we can find a characteristic set G such that

$$\langle G\rangle = \mathcal{P} = \{h \mid \mathrm{prem}(h, G) = 0\}.$$

Thus for zero-dimensional ideals, it is enough to find the prime decomposition of the radical, then find an ascending generating set for each prime ideal. The primary decomposition of zero-dimensional ideals has been studied and analyzed by D. Lazard in [15]. Also, D. Ierardi [11] gives a method for solving algebraic systems using generalized resultant methods. In fact, in both approaches, the prime decomposition of radicals is reduced to the problem of factoring multivariate polynomials. Unfortunately, there is no efficient parallel algorithm known for factoring polynomials over $\mathbf{Q}$.

As the example at the beginning of this subsection suggests, we do not necessarily need to find the complete prime decomposition of the ideal. The ideals $\langle x^2 - 1, y\rangle$ and $\langle x, y^2 - 1\rangle$ are not prime ideals, but they are generated by ascending sets of monic polynomials. To compute this decomposition, we did not need to factor polynomials completely, but only split a polynomial when there was a leading coefficient such that they have nontrivial gcd. Teitelbaum [18] proposes an algorithm for such "lazy factorization" of zero-dimensional ideals. He reduces the problem to the univariate case by applying rational coordinate transformations and by finding primitive elements.

Applied to zero-dimensional ideals $\mathcal{I} = \langle F\rangle$, the algorithms in the present paper will *decompose* the radical of a zero-dimensional ideal $\mathcal{I}$ into

$$\sqrt{\mathcal{I}} = \langle G_1\rangle \cap \cdots \cap \langle G_r\rangle$$

where G_i are ascending sets of monic polynomials. The sequential complexity of the algorithm is $(d^{n^2})^{O(1)}$, and the parallel arithmetic complexity is $(n \log(d))^{O(1)}$, where d is the maximal degree of the polynomials in F and n is the number of variables in F.

Moreover, given an ascending set G of monic polynomials, which generates a zero-dimensional radical, and also given a polynomial f, we give an algorithm which split $\langle G\rangle$ into

$$\langle G\rangle = (\bigcap_{i=1}^{r}\langle G'_i\rangle) \cap (\bigcap_{j=1}^{s}\langle G''_j\rangle)$$

where G'_i and G''_j are ascending sets of monic polynomials and

1. f is zero modulo $\langle G'_i\rangle$.
2. f has an inverse modulo $\langle G''_j\rangle$.

for each $1 \leq i \leq r$ and $1 \leq j \leq s$. This algorithm will enable us to conduct symbolic computation on the complex roots of the polynomials in a zero-dimensional ideal generated by an ascending set without computing the roots explicitly. Also, we give an algorithm which computes the union, the intersection and the quotient of zero-dimensional ideals generated by ascending sets of monic polynomials. These two algorithms are in the complexity class NC, i.e. they can be computed by an arithmetic circuit of polynomial size and depth polylogarithmic in the input size, which is in this case d^n, where d is the maximal degree of the input and n is the number of variables in the input. We use the dense representation of polynomials.

2.2.2 Higher dimensional ideals

In higher dimensions it is not true that every prime ideal is generated by an ascending set, or even by a *regular sequence*, i.e. a set of polynomials having cardinality equal to the codimension. Consider the following example:

Example 3 Consider the affine curve $\mathcal{C} = \{(x, y, z) \in \mathbf{A}^3 \mid x = t^3, y = t^4, z = t^5, t \in \mathbf{C}\}$. The corresponding ideal $\mathcal{I} \subset \mathbf{Q}[x, y, z]$ is generated by the polynomials $\{y^3 - x^4, z^2 - yx^2, xz - y^2\}$. It can be proved that $\mathcal{I}$ is a prime ideal in $\mathbf{Q}[x, y, z]$ (also in $\mathbf{C}[x, y, z]$), the codimension of $\mathcal{I}$ is 2 in $\mathbf{A}^3$, and $\mathcal{I}$ cannot be generated by fewer than 3 polynomials.

Ideals which are generated by a set of polynomials with cardinality equal to the codimension are called *complete intersections*. A more detailed treatment of the subject can be found e.g. in [9].

The above example suggests that if $\mathcal{P}$ is a prime ideal and G is any ascending set from $\mathcal{P}$, then in

$$\langle G\rangle \subseteq \mathcal{P} \subseteq \{h \mid \mathrm{prem}(h, G) = 0\}$$

the first inclusion must be proper if $\mathcal{P}$ is not a complete intersection. Our objective is to find an ascending set for which the second inclusion is an equation. It turns out that such an ascending set always exists [13].

Kalkbrener [13] gives a representation (described below) of a prime ideal $\mathcal{P}$ by an ascending set G such that the second inclusion above is an equality, i.e.

$$\mathcal{P} = \{h \mid \mathrm{prem}(h, G) = 0\}.$$

Therefore, ideal membership can be algorithmically decided, given this ascending set. Furthermore, certain non-prime ideals are also representable by ascending sets in the same manner. This will lead to the notion of unmixed sets and unmixed representations and will enable us to avoid prime factorization. Kalkbrener's approach is based on the following result:

Proposition 4 (Kalkbrener) *Let R be a Noetherian commutative ring and $\mathcal{I}$ be an ideal in $R[x]$. Denote by $\mathbf{K}(\mathcal{P})$ the quotient field of the integral domain $R/\mathcal{P}$ where $\mathcal{P}$ is a prime ideal in R. Then the following are equivalent:*

- *(a) $\mathcal{I}$ is a prime ideal in $R[x]$*
- *(b) $\mathcal{I} \cap R$ is prime in R, $\mathcal{J}$ is prime in $\mathbf{K}(\mathcal{I} \cap R)[x]$ and $\mathcal{I}(R/\mathcal{I} \cap R)[x] = \mathcal{J} \cap (R/\mathcal{I} \cap R)[x]$, where $\mathcal{J}$ is the ideal $\mathcal{I}\mathbf{K}(\mathcal{I} \cap R)[x]$.*
- *(c) $\mathcal{I} \cap R$ is prime in R and there exists a polynomial $q \in R[x]$ such that the image of q in $\mathbf{K}(\mathcal{I} \cap R)[x]$ is either irreducible over $\mathbf{K}(\mathcal{I} \cap R)$ or zero and*

  for every $f \in R[x]$: $f \in \mathcal{I} \iff f^{\mathcal{I}\cap R} \in \langle q \rangle_{\mathbf{K}}$

  where $\langle q \rangle_{\mathbf{K}}$ denotes the ideal in $\mathbf{K}(\mathcal{I} \cap R)[x]$ generated by q and $f^{\mathcal{I}\cap R}$ denotes the image of f in $(R/\mathcal{I} \cap R)[x]$. ■

We use the above proposition inductively for $R = \mathbb{Q}[x_1, \dots, x_{n-1}]$ with the trivial base case when $R = \mathbb{Q}$. If $\mathcal{P}$ is a prime ideal, then there exist polynomials $q_1, \dots, q_n$ such that each q_i is in $\mathbb{Q}[x_1, \dots, x_i]$ and q_i is either zero or irreducible over $\mathbf{K}(\mathcal{I} \cap \mathbb{Q}[x_1, \dots, x_{i-1}])$. Moreover, for every $f \in \mathbb{Q}[x_1, \dots, x_n]$,

$$f \in \mathcal{P} \iff f = \sum_{i=1}^{n} p_i q_i$$

for some $p_i \in \mathbf{K}(I \cap \mathbb{Q}[x_1, \dots, x_{i-1}])[x_i]$, $1 \leq i \leq n$. It is easy to see that the latter condition is equivalent to the following: if $G = \{q_i \mid q_i \neq 0,\ 1 \leq i \leq n\}$ then G is an ascending set and

$$\mathcal{P} = \{h \in \mathbb{Q}[x_1, \dots, x_n] \mid \mathrm{prem}(h, G) = 0\}.$$

Example 5 As in the previous example, let $\mathcal{I} = \langle y^3 - x^4,\ z^2 - yx^2,\ xz - y^2 \rangle \subset \mathbb{Q}[x, y, z]$ be the prime ideal defining the curve $C \in A^3$. For each $1 \leq i \leq 3$ we compute the polynomials q_i as follows:

1. For $i = 1$, $\mathcal{I} \cap \mathbb{Q}[x] = \{0\}$, so let $q_1 = 0$ and $\mathcal{P}_1 = \{0\}$. Then $\mathbf{K}(\mathcal{P}_1) = \mathbb{Q}(x)$.
2. For $i = 2$, $\mathcal{I} \cap \mathbb{Q}[x, y] = \langle y^3 - x^4 \rangle$ so let $q_2 = y^3 - x^4$. Then $\langle q_2 \rangle_{\mathbf{K}} \subset \mathbf{K}(\mathcal{P}_1)[y]$ obviously generates $\mathcal{I} \cap \mathbb{Q}[x, y]$. It is also clear that $\langle q_2 \rangle_{\mathbf{K}} \cap \mathbb{Q}[x, y] = \langle y^3 - x^4 \rangle$. Define $\mathcal{P}_2 = \langle y^3 - x^4 \rangle$; then $\mathbf{K}(\mathcal{P}_2) = \mathbb{Q}(x)[y]/\langle y^3 - x^4 \rangle$.
3. Since $\mathbf{K}(\mathcal{P}_2)[z]$ is a principal ideal domain, $\mathcal{I}\mathbf{K}(\mathcal{P}_2)[z] = \langle z^2 - yx^2,\ xz - y^2 \rangle_{\mathbf{K}}$ is generated by the gcd of the images of the polynomials $(z^2 - yx^2)$ and $(xz - y^2)$ in $\mathbf{K}(\mathcal{P}_2)[z]$. Since

$$\begin{aligned} (z^2 - yx^2) &= (xz - y^2)\left(\frac{z}{x} + \frac{y^2}{x^2}\right) + \left(\frac{y^4}{x^2} - yx^2\right) \\ \frac{y^4}{x^2} - yx^2 &= \frac{y}{x^2}(y^3 - x^4) \end{aligned}$$

we have that $\gcd(z^2 - yx^2, xz - y^2) = xz - y^2$ over $\mathbf{K}(\mathcal{P}_2)$. Note that after multiplying by the denominators in the above calculation we get the pseudo division of $(z^2 - yx^2)$ by the ascending set $\{y^3 - x^4,\ xz - y^2\}$. Let $q_3 = xz - y^2$.
Claim: $\langle q_3 \rangle_{\mathbf{K}} \cap \mathbb{Q}[x, y, z] = \mathcal{I}$.
Proof: First observe that

$$\langle q_3 \rangle_{\mathbf{K}} \cap \mathbb{Q}[x, y, z] = \{h \in \mathbb{Q}[x, y, z] \mid \mathrm{prem}(h, G) = 0\}$$

where $G = \{q_2, q_3\}$ is an ascending set. We saw in section 2.1 that $\mathrm{prem}(h, G) = 0$ iff there are numbers α, β such that $\mathrm{lc}(q_2)^\alpha \mathrm{lc}(q_3)^\beta h \in \mathcal{I}$. Here $\mathrm{lc}(q_2) = 1$ and $\mathrm{lc}(q_3) = x$. Thus $\mathrm{prem}(h, G) = 0$ iff $x^\beta h \in \mathcal{I}$ iff $h \in \mathcal{I}$ using that $x \notin \mathcal{I}$ and $\mathcal{I}$ is prime ideal. ■

To summarize the above results, let $\mathcal{P} \subset \mathbb{Q}[x_1, \dots, x_n]$ be a prime ideal. Then there exists an ascending set $G = \{g_1, \dots, g_m\}$ such that

$$\mathcal{P} = \{h \in \mathbb{Q}[x_1, \dots, x_n] \mid \mathrm{prem}(h, G) = 0\},$$

and if $\mathrm{class}(g_i) = x_j$ then g_i is irreducible in $\mathbf{K}(\mathcal{P} \cap \mathbb{Q}[x_1, \dots, x_{j-1}])[x_j]$. An ascending set with the latter condition is called an *irreducible ascending set.* We say that G *represents* the ideal $\mathcal{P}$ if $\mathcal{P} = \{h \in \mathbb{Q}[x_1, \dots, x_n] \mid \mathrm{prem}(h, G) = 0\}$, denoted by $\mathrm{Rep}(G)$. Thus using the prime decomposition of the radical of an ideal $\mathcal{I}$, we can express

$$\sqrt{\mathcal{I}} = \mathcal{I}_1 \cap \ldots \cap \mathcal{I}_r$$

where each $\mathcal{I}_i$ is represented by an irreducible ascending set.

Similarly to the zero-dimensional case, a "lazy" approach – using only gcd computations on polynomials – is sufficient to express radicals as

$$\sqrt{\mathcal{I}} = \mathcal{I}_1 \cap \ldots \cap \mathcal{I}_r$$

where $\mathcal{I}_i$ is represented by an ascending set G_i for each $1 \leq i \leq r$. We follow an approach similar to [12]. Again, an ascending set $G \subset \mathbb{Q}[x_1, \dots, x_n]$ represents the ideal $\mathcal{I}$ if

$$\mathcal{I} = \mathrm{Rep}(G) = \{h \in \mathbb{Q}[x_1, \dots, x_n] \mid \mathrm{prem}(h, G) = 0\}.$$

In the case of prime decomposition, we require the ascending set to be an irreducible ascending set in order to represent a prime ideal. In the "lazy" version we weaken this condition, and we only require the ideal represented by the ascending set to be radical and a proper subset of $\mathbb{Q}[x_1, \dots, x_n]$. The following result gives a sufficient condition for this:

Proposition 6 *Let $G = \{g_1, \dots, g_m\}$ be an ascending set and $\mathcal{I} = \mathrm{Rep}(G)$. For each $0 \leq i \leq m - 1$, let $G^{(i)} = \{g_1, \dots, g_i\}$ and $\{\mathcal{P}_{i,j}\}_{j=1}^{r_i}$ be the prime ideals in the irredundant prime decomposition of the radical of $\mathrm{Rep}(G^{(i)})$. Suppose that the following conditions are satisfied for each $0 \leq i \leq m - 1$:*

- *(a) $\mathrm{lc}(g_{i+1}) \notin \mathcal{P}_{i,j}$ for each $1 \leq j \leq r_i$.*
- *(b) g_{i+1} is squarefree over $\mathbf{K}(\mathcal{P}_{i,j})$ for each $1 \leq j \leq r_i$.*

Then $\mathcal{I}$ is radical and $\mathcal{I} \neq \mathbb{Q}[x_1, \dots, x_n]$. Furthermore, all the prime ideals in the irredundant prime decomposition of $\mathcal{I}$ have the same codimension. ■

A radical ideal and the corresponding variety are called *unmixed* if all the associated prime ideals have the same codimension. We will call an ascending set an *unmixed ascending set*, or simply unmixed set, if conditions (a) and (b) of Proposition 6 are satisfied. The *unmixed representation* of an ideal is a set of unmixed ascending sets such that the intersection of the radicals represented by these unmixed sets is the radical of the ideal.

2.3 Notation

In the following sections we will use the following notation:

Let R denote a Noetherian ring with identity and let F be a subset of R. The ideal generated by F is denoted by $\langle F\rangle$, the radical of $\langle F\rangle$ by $\sqrt{F}$. For $f \in R[x]$, $f^{\mathcal{I}}$ denotes the image of f in $(R/\mathcal{I})[x]$.

If $\mathcal{I} = \mathcal{Q}_1 \cap \ldots \cap \mathcal{Q}_r$ is the irredundant primary decomposition of $\mathcal{I}$, then $\mathcal{P}_1 = \sqrt{\mathcal{Q}_1}, \ldots, \mathcal{P}_r = \sqrt{\mathcal{Q}_r}$ are the associated primes of $\mathcal{I}$, and we denote the set $\{\mathcal{P}_1, \ldots, \mathcal{P}_r\}$ by $\mathrm{Ap}(I)$. For a prime ideal $\mathcal{P} \subset R$ the quotient field of the integral domain $R/\mathcal{P}$ is denoted by $\mathbf{K}(\mathcal{P})$.

The *codimension* (height) of a prime ideal $\mathcal{P} \neq R$ is said to be m if there exists at least one chain $\mathcal{P}_0 \subset \mathcal{P}_1 \subset \ldots \subset \mathcal{P}_m = \mathcal{P}$, where $\mathcal{P}_i$ are prime ideals, and there is no chain with more then $m+1$ elements. The codimension of an arbitrary ideal $\mathcal{I} \neq R$ is the minimum of the codimensions of the prime ideals containing $\mathcal{I}$. Note that the codimension of an ideal represented by an unmixed ascending set C is equal to the number of polynomials in C.

3 Outline of the algorithm

We will construct a modified version of the Wu-Ritt unmixed decomposition algorithm of Kalkbrener. In [12] $\mathbf{decompose}_{\mathbf{R}[\mathbf{x}]}$ has a finite set of polynomials F as input and it computes the unmixed representation of the corresponding radical $\sqrt{\langle F\rangle}$ by creating branches of the computation and recursively calling $\mathbf{decompose}_{\mathbf{R}[\mathbf{x}]}$. Unfortunately, it often computes superflous components embedded in other components computed in different branches. Below we present an algorithm $\mathbf{decompose}_{\mathbf{n}}^{\mathbf{m}}$ which restricts the output to unmixed sets of codimension m such that the union for $m = 1, \ldots, n$ gives an unmixed representation of $\sqrt{\langle F\rangle}$. By this restriction we are able to avoid the computation of superflous components because

- we ensure that the computed unmixed components of codimension m have no intersection of codimension m
- none of the components of codimension m computed are embedded in a component V' of $V(F)$ of codimension $m' < m$.

After finding an unmixed representation of a radical, we use the algorithm $\mathbf{split}_{\mathbf{n}}^{\mathbf{m}}$ to factor further the unmixed components (represented by unmixed ascending sets), depending on whether a given polynomial vanishes or not over the component. The algorithm $\mathbf{split}_{\mathbf{n}}^{\mathbf{m}}$ can be applied to conduct symbolic computation on algebraic numbers which are given as roots of polynomials in unmixed ascending sets. Also, $\mathbf{split}_{\mathbf{n}}^{\mathbf{m}}$ is a subroutine in $\mathbf{decompose}_{\mathbf{n}}^{\mathbf{m}}$. The algorithm is a generalization of the resultant method for finding the gcd of several univariate polynomials described in [10, chapter 15.2].

We also present an algorithm $\mathbf{simplify}_{\mathbf{n}}^{\mathbf{m}}$ which might have separate applications besides being a subroutine of the decomposition algorithm. Given a set of ideals represented by unmixed ascending sets, $\mathbf{simplify}_{\mathbf{n}}^{\mathbf{m}}$ computes the unmixed representation of the unions, the intersections and the quotients of the ideals in the given set. The algorithm is a generalization of the simple refinement method described in [1].

In the algorithms below we assume that every polynomial in the computation is reduced by the unmixed ascending set given in the input or previously computed. Therefore, in each step we must find the pseudo remainder of the polynomial computed by the unmixed ascending set. We omit the technical details of the algorithm $\mathbf{prem}_{\mathbf{n}}^{\mathbf{m}}$ but we give an outline of the complexity analysis in section 3.5.

3.1 The decompose algorithm

We will give an informal description of the algorithms using geometric notions instead of algebraic. In this section R will denote the polynomial ring $\mathbb{Q}[x_1, \ldots, x_{n-1}]$, so $R[x_n] = \mathbb{Q}[x_1, \ldots, x_n]$. Let $F = \{f_0, \ldots, f_k\} \subset R[x_n]$ be a set of polynomials, $\mathcal{I} = \langle f_0, \ldots, f_k\rangle$, $V = V(\mathcal{I}) \subset \mathbf{A}^n$. Abusing notation, for an unmixed ascending set C, $V(C)$ and $\mathrm{Ap}(C)$ denotes respectively the variety and the associated primes corresponding to the radical $\mathrm{Rep}(C)$ and not to $\langle C\rangle$.

3.1.1 Induction for codimension m

The algorithm described below is inductive on the codimension m of the components computed. The induction hypothesis for codimension m is the following:

- We have computed the set $\Gamma_m(F) = \{C_1, \ldots, C_{r_m}\}$ of unmixed ascending sets with the following properties:

  H.1 $V \subseteq \bigcup_{C_i \in \Gamma_m(F)} V(C_i)$

  H.2 $\mathrm{codim}(V(C_i)) \leq m$ for all $C_i \in \Gamma_m(F)$.

  H.3 Each $C_i \in \Gamma_m(F)$ is one of the following two types:

  (a) *first type*: $V(C_i) \subseteq V$.

  (b) *second type*: No irreducible components of $V(C_i)$ contained by V, but for every irreducible component of $V(C_i)$ there exists a component V' of V of codimension $\geq m+1$ such that V' is contained in the irreducible component.

  H.4 If $\mathrm{codim}(V(C_i)) < m$ then C_i is first type, i.e. $V(C_i) \subseteq V$.

  H.5 If $\mathrm{codim}(C_i) \leq \mathrm{codim}(C_j)$ then no component of $V(C_j)$ is completely contained in a component of $V(C_i)$.

  H.6 $\Gamma_m(F)$ is *simple*: $V(C_i)$ and $V(C_j)$ do not contain any common irreducible components, $i \neq j$.

We terminate the algorithm if all the components $C_1, \ldots, C_{r_m}$ are of the first type, thus the set $\Gamma_m(F) = \{C_1, \ldots, C_{r_m}\}$ gives the desired unmixed representation of the radical of $\mathcal{I}$. This occurs when m reaches the maximal codimension of the irreducible components in V. If not all the components are of the first type, we call the variety $\bigcup_{C \in \Gamma_m(F)} V(C)$ a *hull* of V of codimension m.

3.1.2 Case $m + 1$

In this step, we distribute the computation creating a new branch for each $C \in \Gamma_m(F)$ of second type. On each branch, the algorithm $\mathbf{decompose}_{\mathbf{n}}^{\mathbf{m+1}}(C, F)$ computes an unmixed representation of a hull of $V(C) \cap V(F)$ of codimension $m+1$.

Let $\Gamma_m^{(1)}$ and $\Gamma_m^{(2)}$ be the first and second type components of $\Gamma_m(F)$, resp. Also let $\Delta_{m+1}(C, F)$ be the output of $\mathbf{decompose}_{\mathbf{n}}^{\mathbf{m+1}}(C, F)$. To see how the induction hypothesis is maintained, define

$$\Gamma'_{m+1}(F) = \Gamma_m^{(1)} \cup \Big(\bigcup_{C \in \Gamma_m^{(2)}} \Delta_{m+1}(C, F) \Big).$$

$\Gamma'_{m+1}(F)$ will satisfy H.1-H.4 of the induction hypothesis (for $m = m + 1$) if we adequately specify the output Δ_{m+1} of $\mathbf{decompose}_{\mathbf{n}}^{\mathbf{m+1}}$, described in the next subsection. H.5 is satisfied because we only decompose unmixed sets of second type. As for the sixth property H.6, a component of $V(F)$ with codimension $\geq m + 1$ might be contained in more than one component from $\Gamma_m(F)$, so it might be computed on more than one branch. Thus $\Gamma'_{m+1}(F)$ is not necessary simple, so care must be taken. We will describe how to compute the *simple refinement* $\Gamma_{m+1}(F)$ of $\Gamma'_{m+1}(F)$ in section 3.3.

3.1.3 The input and output

We define $\mathbf{decompose}_{\mathbf{n}}^{\mathbf{m+1}}$ to be slightly more general than the description above implies. We will have an extra optional argument T, which will be used in the iterative calls. This change is not essential, but it does simplify the presentation.

The input of $\mathbf{decompose}_{\mathbf{n}}^{\mathbf{m+1}}$ consists of

I.1 an unmixed set $C = \{g_1, \ldots, g_m\} \subset R[x_n]$ of codimension m,

I.2 a set of polynomials $F = \{f_0, \ldots, f_k\} \subset R[x_n]$

I.3 an optional argument $T = \{q_1, \cdots, q_c\} \subset R[x_n, x_{n+1}, \ldots, x_l]$ for some $l \geq n$.

The output of $\mathbf{decompose}_{\mathbf{n}}^{\mathbf{m+1}}(C, F, T)$ consists of the unmixed sets

$$\Delta_{m+1}(C, F, T) = \{C_1, \ldots, C_r\}$$

in $R[x_n]$ such that for all $1 \leq i \leq r$

O.1 $\mathrm{codim}(C_i) = m + 1 = \mathrm{codim}(C) + 1$

O.2 $V(C_i) \subset V(C)$

O.3 $\bigcup_{i=1}^r V(C_i) \supseteq (V(C) \cap V(F))_{\geq m+1}$ where $(V(C) \cap V(F))_{\geq m+1}$ denotes the union of the irreducible components of $V(C) \cap V(F)$ of codimension $\geq m + 1$.

O.4 $\Delta_{m+1}(C, F, T)$ is simple.

O.5 $q_k \not\equiv 0$ modulo $\mathcal{P}$ for all $\mathcal{P} \in \mathrm{Ap}(C_i)$ and for all $q_k \in T$.

O.6 each $V(C_i)$ is either first or second type.

3.1.4 Description of the algorithm

First we show how to compute $\mathbf{decompose}_{\mathbf{n}}^{\mathbf{m+1}}(C, \{h\}, \emptyset)$, where $h \in R[x_n]$ is a polynomial and all the components of $V(C) \cap V(h)$ have codimension $m + 1$. Then we show how to reduce the computation of $\mathbf{decompose}_{\mathbf{n}}^{\mathbf{m+1}}(C, F, T)$ to the computation of $\mathbf{decompose}_{\mathbf{n}}^{\mathbf{m+1}}(C, \{h\}, \emptyset)$.

Let $C = \{g_1, \ldots, g_m\} \subset R[x_n]$ be an unmixed ascending set of codimension m and h be a polynomial in $R[x_n]$ such that $V(C) \cap V(h)$ is an unmixed variety of codimension $m + 1$. Define $C' = C \cap R$, $g \in C - R$ ($g = 0$ if $C \subset R$). Note that C' is an unmixed set in R of codimension m or $m - 1$ depending on whether $C = C'$. We will compute $\mathbf{decompose}_{\mathbf{n}}^{\mathbf{m+1}}(C, \{h\}, \emptyset)$ by reducing the problem to the $n - 1$ variable case.

Consider the subvariety $V' \subset V(C') \subseteq \mathbf{A}^{n-1}$ such that $g(\vec{\alpha}, x_n)$ and $h(\vec{\alpha}, x_n)$ have common roots in $\mathbf{C}$ for all $\vec{\alpha} \in V'$. Since $V(C) \cap V(h)$ has codimension $m + 1$, V' has codimension m, but V' is not necessary unmixed. In order to find the unmixed representation of V', the main idea is to express

$$V' = \bigcup_{r,s,t} V'_{rst}$$

where $0 \leq r \leq \deg_{x_n}(g)$, $0 \leq s \leq \deg_{x_n}(h)$, $0 \leq t = t(r, s) \leq \min(r, s)$, V'_{rst} is either empty or unmixed, and for "almost all" $\vec{\alpha} \in V'_{rst}$ the following are satisfied:

- r is the largest exponent such that the coefficient of x_n^r in $g(\vec{\alpha}, x_n)$ is not zero, i.e. $g(\vec{\alpha}, x_n)$ has degree $r \geq 1$.
- s is the largest exponent such that the coefficient of x_n^s in $h(\vec{\alpha}, x_n)$ is not zero, i.e. $h(\vec{\alpha}, x_n)$ has degree $s \geq 1$.
- t is the smallest index such that the t^{th} subresultant φ_t of $g(\vec{\alpha}, x_n)$ and $h(\vec{\alpha}, x_n)$ is not zero, i.e. $\gcd(g(\vec{\alpha}, x_n),\ h(\vec{\alpha}, x_n))$ has degree $t \geq 1$.

Here "almost all" means that the points form an open dense subset of the variety. In the cases when $r = 0$ or $s = 0$, we need to be more careful, but the definition is similar.

It is easy to see that the unmixed representation of V'_{rst} is of the form

$$\Delta'_{rst} = \mathbf{decompose}_{\mathbf{n-1}}^{\mathbf{m}}(C', G_r \cup H_s \cup \Phi_t, \{g_r, h_r, \varphi_t\})$$

where G_r, H_s, Φ_t, $\{g_r, h_r, \varphi_t\} \subset R$ describe the above properties with polynomial equations and inequations. (The above is true only if C' has codimension $m - 1$. If C' has codimension m, we succeed similarly by calling the subroutine $\mathbf{split}_{\mathbf{n-1}}^{\mathbf{m}}$ described below. We omit the technical details here.)

Let $g_{rst} \in R[x_n]$ be the gcd of g and h over $\mathbf{K}(\mathcal{P})$ for all $\mathcal{P} \in \mathrm{Ap}(C'_{rst})$ where $C'_{rst} \in \Delta'_{rst}$. In fact, for $r, s, t \geq 1$, g_{rst} is computed by simply solving the linear system corresponding to the t^{th} subresultant φ_t of the degree r and s slices of g and h, resp. [19]. We use Cramer's rule without the division by the determinant φ_t, thus the leading coefficient of g_{rst} is φ_t.

Since C'_{rst} satisfies the above properties, we have $\mathrm{lc}(g_{rst}) \notin \mathcal{P}$ for all $\mathcal{P} \in \mathrm{Ap}(C'_{rst})$. We can also assume that g_{rst} is squarefree, otherwise we can squarefree factor with an algorithm similar to $\mathbf{split}^{\mathbf{m}}_{\mathbf{n}}$ described below. Thus $C'_{rst} \cup \{g_{rst}\}$ is an unmixed ascending set. For all $\Delta'_{rst} \neq \emptyset$, define

$$\Delta_{rst} = \{C'_{rst} \cup \{g_{rst}\} \mid C'_{rst} \in \Delta'_{rst}\}$$

and

$$\Delta_{m+1}(C, h) = \bigcup_{r,s,t} \Delta_{rst}.$$

It can be proved that $\Delta_{m+1}(C, h)$ is simple and is an unmixed representation of $V(C) \cap V(h)$.

Now we describe how to reduce $\mathbf{decompose}^{\mathbf{m+1}}_{\mathbf{n}}(C, F, T)$ to the computation of $\mathbf{decompose}^{\mathbf{m+1}}_{\mathbf{n}}(C, \{h\}, \emptyset)$.

Let $C = \{g_1, \ldots, g_m\} \subset R[x_n]$ be an unmixed ascending set of codimension m, $F = \{f_0, \ldots, f_k\} \subset R[x_n]$ and $T = \{q_1, \ldots, q_c\} \subset R[x_n, x_{n+1}, \ldots, x_l]$ for some $l \geq n$.

1. We need to compute a polynomial $h \in R[x_n]$ such that $(V(C) \cap V(h))$ is a hull of $(V(C) \cap V(F))$ of codimension $m+1$. We can assume that $(V(C) \cap V(F))$ has codimension $m+1$, otherwise we can factor out the components of codimension m. Then there exists a linear combination h of the polynomials in F which is in "general position", i.e. $(V(C) \cap V(h))$ has codimension $m+1$. We compute the polynomial h by calling $\mathbf{general}^{\mathbf{m+1}}_{\mathbf{n}}$ described in section 3.2.

2. We need to find an unmixed representation of the Zariski closure of $(V(C) \cap V(h)) - V(T)$. Suppose we have computed the unmixed representation of $(V(C) \cap V(h))$ as above. We use $\mathbf{split}^{\mathbf{m+1}}_{\mathbf{n}}$ (described in 3.4) to find those components where none of the polynomials $q_1, \ldots, q_c \in T$ vanish identically. We call $\mathbf{split}^{\mathbf{m+1}}_{\mathbf{n}}$ for the polynomial $q = \prod_{i=1}^{c} q_i$. Note that the number c never exeeds 3 in the recursive calls of $\mathbf{decompose}^{\mathbf{m+1}}_{\mathbf{n}}(C, \{h\}, \emptyset)$ above.

3. Last, we need to separate the first and second type components of the hull of $(V(C) \cap V(F)) - V(T)$. We define the polynomial

$$f(x_1, \ldots, x_{n+1}) = f_k x_{n+1}^k + \ldots + f_0$$

in $n+1$ variables, and by calling $\mathbf{split}^{\mathbf{m+1}}_{\mathbf{n}}$ for f (described in section 3.4), we find those components where all $f_0, \ldots, f_k$ vanish (first type), and those where at least one of them does not (second type).

3.2 The algorithm $\mathbf{general}^{\mathbf{m+1}}_{\mathbf{n}}$

Let $C = \{g_1, \ldots, g_m\} \subset R[x_n]$ be an unmixed set of codimension m and $F = \{f_0, \ldots, f_k\} \subset R[x_n]$ a finite set. Suppose that $V(C) \cap V(F)$ has codimension $\geq m+1$. Then there exists a polynomial $h \in R[x_n]$ such that

$$h = \sum_{j=0}^{k} a^j f_j$$

for some $a \in \mathbf{Q}$ and h is in *general position*, i.e. $V(\mathcal{P}) \cap V(h)$ has codimension $m+1$ for all $\mathcal{P} \in \mathrm{Ap}(C)$. We compute the polynomial h using the algorithm $\mathbf{general}^{\mathbf{m+1}}_{\mathbf{n}}(C, F)$ as follows:

If $m = 0$, then $h = f_0 \in F$ will satisfy the desired properties. If $m > 0$, then define

$$\Psi_{m+1}(\vec{x}, y) := f_k y^k + f_{k-1} y^{k-1} + \ldots + f_0 \in \mathbf{Q}[x_1, \ldots, x_n, y]$$

where y is a new variable. The algorithm is based on the equivalence of the following statements:

- $V(\mathcal{P}) \cap V(F)$ has codimension $\geq m+1$ for all $\mathcal{P} \in \mathrm{Ap}(C)$.
- The gcd of the polynomials $\{g_m, f_0, \ldots f_k\}$ is 1 over $K(\mathcal{P})$ for all $\mathcal{P} \in \mathrm{Ap}(C')$ where $C' = \{g_1, \ldots, g_{m-1}\}$.
- For $s = m, \ldots, 0$ define inductively $\Psi_s := \mathrm{RES}_{x_{i_s}}(\Psi'_{s+1}, g_s)$ the resultant in the variable $x_{i_s} = \mathrm{class}(g_s)$. Here Ψ'_{s+1} is the pseudoremainder of Ψ_{s+1} modulo g_s. Then $\Psi_0 \in \mathbf{Q}[\bar{x}, y]$, where $\bar{x} = \{x_i \mid i \neq i_s,\ 0 < s \leq m\}$ and Ψ_0 is not identically zero.
- Let Ψ_0 be as above. There exists $a \in \mathbf{Q}$ such that $\Psi_0(\bar{x}, a)$ is not identically zero.
- Let a be as above. Then $h := \Psi_{m+1}(\vec{x}, a)$ is in general position.

Moreover,

$$\begin{aligned} \deg_y(\Psi_0) &= (\deg_y(\Psi_1)) \cdot (\deg_{x_{i_1}}(g_1)) \\ &= (\deg_y(\Psi_{m+1})) \prod_{s=1}^{m} \deg_{x_{i_s}}(g_s) \\ &= k \prod_{s=1}^{m} \deg_{x_{i_s}}(g_s). \end{aligned}$$

Thus, if $S \subset \mathbf{Q}$ and $|S| = k(\prod_{s=1}^{m} \deg_{x_{i_s}}(g_s)) + 1$, then there must be $a \in S$ such that $\Psi_0(\bar{x}, a)$ is not identically zero. If $x_j \neq \mathrm{class}(g_s)$ for any $s = 1 \ldots m$ then let k_j be the maximum degree of the input in the variable x_j. The above bounds are also valid with any variable x_j in place of y and k_j in place of k. Thus the dense size of $\Psi_0(\bar{x}, a)$ is $(k' \prod_{s=1}^{m} \deg_{x_{i_s}}(g_s))^n$, where $k' = \max\{k, k_j \mid j \neq i_s\}$. ■

3.3 Simple refinement

Recall that a set of unmixed ascending sets Γ is *simple* if for all $C \neq C' \in \Gamma$, $V(C)$ and $V(C')$ do not contain common component, i.e. $\mathrm{Ap}(C) \cap \mathrm{Ap}(C') = \emptyset$. Note that if Γ contains unmixed components of a hull of V and Γ is simple, then $|\Gamma| \leq \deg(V)$.

Below we describe how to find a *simple refinement* of a given set of unmixed sets Γ, i.e. a new set Δ of unmixed sets which is simple and $\bigcup_{C \in \Gamma} \mathrm{Ap}(C) = \bigcup_{C \in \Delta} \mathrm{Ap}(C)$. The algorithm $\mathbf{simplify}^{\mathbf{m}}_{\mathbf{n}}$ is a generalization of the method in [1, section 2.1]. Besides being a subroutine of the decomposition algorithm, **simplify** has sepatate applications as a method to compute the union, quotient and intersection of ideals represented by unmixed sets.

First we show how to compute a simple refinement of the set $\{C, C'\}$ consisting of two unmixed sets. Let $C =$

$\{g_1, \ldots, g_m\}$ and $C' = \{g'_1, \ldots, g'_{m'}\}$ be unmixed ascending sets. We can assume that C and C' have the same type, i.e. $m = m'$ and $\mathrm{class}(g_s) = \mathrm{class}(g'_s)$ for all $s = 1, \ldots, m$, otherwise $\mathrm{Ap}(C) \cap \mathrm{Ap}(C') = \emptyset$. Let $d_s = \deg_{x_{i_s}}(g_s)$, where $x_{i_s} = \mathrm{class}(g_s)$, and let $T = \{(t_2, \ldots, t_m) \in \mathbf{N}^{m-1} \mid 0 \leq t_s \leq d_s,\ 2 \leq s \leq m\}$. We define inductively for $s = m, \ldots, 1$ the following polynomials for each $\vec{t} = (t_2, \ldots, t_m) \in T$:

- $\varphi_m^{(j)} = \mathrm{RES}_{x_{i_m}}^{(j)}(g_m, g'_m)$, the j^{th} subresultant in the variable $x_{i_m} = \mathrm{class}(g_m)$ for all $0 \leq j \leq d_m$.
- For $s \leq m - 1$ let $g_s^* = g'_s + y_s\varphi_{s+1}^{(0)} + \ldots + y_s^{t_{s+1}+1}\varphi_{s+1}^{(t_{s+1})}$, the combination of g'_s and the first t_{s+1} subresultants of g_{s+1} and g_{s+1}^*. Note that g_s^* contains variables $\{\vec{x}, y_m, \ldots, y_s\} - \{x_{i_{s'}} \mid x_{i_{s'}} = \mathrm{class}(g_{s'}),\ s' > s\}$.
- For $s \leq m - 1$ let $\varphi_s^{(j)} = \mathrm{RES}_{x_{i_s}}^{(j)}(g_s, g_s^*)$, the j^{th} subresultant in the variable $x_{i_s} = \mathrm{class}(g_s)$ for all $0 \leq j \leq d_s$. Note that $\varphi_s^{(j)}$ contains the variables $\{\vec{x}, y_m, \ldots, y_s\} - \{x_{i_{s'}} \mid x_{i_{s'}} = \mathrm{class}(g_{s'}),\ s' \geq s\}$.

For a given $\vec{t} \in T$, denote the polynomial g_1^* defined above by $g_1^{(\vec{t})}$. Informally, for a given $(t_2, \ldots t_m) \in T$ the gcd of $(g_1, g'_1, g_1^{(\vec{t})})$ is a univariate polynomial with roots $\alpha \in \mathbf{C}$ such that the gcd of $g_i|_{x_1=\alpha}$ and $g'_i|_{x_1=\alpha}$ has degree at least t_i for all $2 \leq i \leq m$. After computing the simple refinement of the set of univariate polynomials $\{\gcd(g_1, g'_1, g_1^{(\vec{t})})\}_{\vec{t}\in T}$ using the method in [1, section 2.1], each polynomial d_1 in the simple refinement corresponds to a vector $\vec{t} \in T$ such that $d_1(\alpha) = 0$ implies that the degree of $\gcd(g_i|_{x_1=\alpha}, g'_i|_{x_1=\alpha})$ is equal to t_i for all $2 \leq i \leq m$. Then it is easy to see how to compute the unmixed ascending sets $D^{(\vec{t})} = \{d_1^{(\vec{t})}, d_2^{(\vec{t})}, \ldots, d_m^{(\vec{t})}\}$ by solving linear equation systems, where $d_i^{(\vec{t})}$ is the unique gcd of degree t_i of g_i and g'_i modulo $\mathrm{Rep}(d_1^{(\vec{t})}, \ldots, d_{i-1}^{(\vec{t})})$. It can be shown that

$$\mathrm{Ap}(C) \cap \mathrm{Ap}(C') = \bigcup_{\vec{t}\in T} \mathrm{Ap}(D^{(\vec{t})}).$$

Also, using pseudo division we can find the unmixed sets $D_i^{(\vec{t})} = \{d_1^{(\vec{t})}, \ldots, g_i/d_i^{(\vec{t})}, g_{i+1}, \ldots, g_m\}$ for each $i = 1, \ldots, m$. It can be shown that

$$\mathrm{Ap}(C) - \mathrm{Ap}(C') = \bigcup_{\vec{t}\in T} \bigcup_{i=1}^{m} \mathrm{Ap}(D_i^{(\vec{t})}).$$

Using the same method for $\mathrm{Ap}(C') - \mathrm{Ap}(C)$, we get a simple refinement of the set $\{C, C'\}$.

Now let $\Gamma = \{C_1, \ldots, C_r\}$ and $\Gamma' = \{C'_1, \ldots, C'_t\}$ be two simple sets of unmixed sets. Again, we can assume that the unmixed sets in $\Gamma \cup \Gamma'$ all have the same type. We can express $\bigcup_{i=1}^r \mathrm{Ap}(C_i) \cup \bigcup_{j=1}^t \mathrm{Ap}(C'_j)$ as

$$\left[\mathrm{Ap}(C_i) - (\textstyle\bigcup_{C'_j\in\Gamma'} \mathrm{Ap}(C'_j))\right] \cup \left[\mathrm{Ap}(C'_j) - (\textstyle\bigcup_{C_i\in\Gamma} \mathrm{Ap}(C_i))\right] \cup \left(\textstyle\bigcup_{i,j=1}^{r,t}[\mathrm{Ap}(C'_j) \cap \mathrm{Ap}(C_i)]\right)$$

a disjoint union. An unmixed representation of the ideal corresponding to $\mathrm{Ap}(C_i) \cap \mathrm{Ap}(C'_j)$ can be found as in the previous paragraph.

To find $[\mathrm{Ap}(C_i) - (\bigcup_{C'_j\in\Gamma'} \mathrm{Ap}(C'_j))]$, let $g'_s = \prod_{j=1}^t g_s^{(j)}$ where $g_s^{(j)}$ is the s^{th} element in $C'_j \in \Gamma'$ $(s = 1, .., m)$. We can use the method of the previous paragraph with $C = C_i$ and $C' = \{g'_1, \ldots, g'_m\}$. Note that the fact that C' is not an unmixed set is not relevant here, as we only want to compute the ideal corresponding to $\mathrm{Ap}(C) - \mathrm{Ap}(C')$.

Now a straightforward divide-and-conquer yields the algorithm

$$\mathbf{simplify}_{\mathbf{n}}^{\mathbf{m}}(\Gamma_1, \ldots, \Gamma_r)$$

computing the simple refinement of the set $\{\Gamma_1, \ldots, \Gamma_r\}$, where each Γ_i is simple and all the unmixed sets in $\bigcup \Gamma_i$ have the same type.

3.4 The splitting algorithm

Let $C = \{g_1, \ldots, g_m\} \subset R[x_n]$ be an unmixed ascending set of codimension m and $f \in R[x_n, x_{n+1}, \ldots, x_l]$ for some $l \geq n$. The algorithm $\mathbf{split}_{\mathbf{n}}^{\mathbf{m}}(C, f)$ computes the unmixed decomposition

$$(\Gamma, \Delta) = (\{B_1, \ldots, B_s\}, \{D_1, \ldots, D_t\})$$

of C such that

- $\bigcup_i \mathrm{Ap}(B_i) = \{\mathcal{P} \in \mathrm{Ap}(C) \mid f^{\mathcal{P}} \not\equiv 0\}$
- $\bigcup_i \mathrm{Ap}(D_i) = \{\mathcal{P} \in \mathrm{Ap}(C) \mid f^{\mathcal{P}} \equiv 0\}$

where $f^{\mathcal{P}}$ denotes the image of f in $(R[x_n]/\mathcal{P})[x_{n+1}, \ldots, x_l]$. We also require the set $\Gamma \cup \Delta$ to be simple.

Note, that C, $B_1, \ldots, B_s$ and $D_1, \ldots, D_t$ all have the same type, i.e. if $C = \{g_1, \ldots, g_m\}$ and B_j or $D_j = \{g'_1, \ldots, g'_{m'}\}$, then $m = m'$ and $\mathrm{class}(g_i) = \mathrm{class}(g'_i)$ for all $i = 1, \ldots, m$.

Also, note that $f^{\mathcal{P}} \equiv 0$ if and only if all the coefficients of f are in $\mathcal{P}$ when f is considered as a multivariate polynomial in $x_{n+1}, \ldots, x_{n+l}$. On the other hand, given an unmixed ascending set C and a set of polynomials $F = \{f_0, \ldots, f_k\} \subset R[x_n]$, we can define the polynomial

$$f(x_1, \ldots, x_{n+1}) = f_k x_{n+1}^k + \ldots + f_0.$$

Then it is easy to see that the output of $\mathbf{split}_{\mathbf{n}}^{\mathbf{m}}(C, f)$ will separate the first and second type components of C corresponding to F [10].

3.4.1 Description of the algorithm

Again, let $C = \{g_1, \ldots, g_m\} \subset R[x_n]$ be an unmixed ascending set and $f \in R[x_n, x_{n+1}, \ldots, x_l]$ for some $l \geq n$. We show how to reduce the computation of $\mathbf{split}_{\mathbf{n}}^{\mathbf{m}}(C, f)$ to the computation of $\mathbf{split}_{\mathbf{n-1}}$ in one less variable. The main idea of the algorithm is similar to the one of **decompose**, only here we have fewer degenerate cases, since we do not need to eliminate variables.

Without loss of generality we can assume that $g_m \in R[x_n] - R$, otherwise we call $\mathbf{split}_{\mathbf{n-1}}^{\mathbf{m}}(C, f)$. Let $C' = \{g_1, \ldots, g_{m-1}\}$ the first $m - 1$ element of C, which is an unmixed ascending set in R of codimension $m - 1$.

Write f as a univariate polynomial in x_n, so the coefficients of f are in $R[x_{n+1}, \dots, x_l]$.

We split $V(C')$ into

$$V(C') = \bigcup_{s,t} V'_{st}$$

where $0 \leq s \leq \deg_{x_n}(f)$, $0 \leq t = t(s) \leq s$, V'_{st} is an unmixed component of $V(C')$ with codimension $m-1$, and for all irreducible components $V(\mathcal{P}') \subseteq V'_{rst}$ the following are satisfied:

- s is the largest index such that the coefficient of x_n^s in f does not vanish identically over $V(\mathcal{P}')$, i.e. $f^{\mathcal{P}'}$ has degree s in x_n.
- t is the smallest index such that the t^{th} subresultant $\varphi_t = \mathrm{RES}^t_{x_n}(f^{\mathcal{P}'}, g_m) \in R[x_{n+1}, \dots, x_l]$ is not identically zero over $V(\mathcal{P}')$, i.e. $\gcd(f, g_m) \in R[x_n]$ has degree t.

It is easy to see that we can define polynomials F_s and Φ_t in l variables such that the unmixed representation of V'_{st} can be found by first computing

$$(\Gamma'_{st}, \Delta'_{st}) = \mathbf{split}^{\mathbf{m}-1}_{\mathbf{n}-1}(C', F_s + \Phi_t)$$

and then finding the simple refinement of $\{\Delta'_{st}\}_{s,t}$ using the algorithm $\mathbf{simplify}^{\mathbf{m}-1}_{\mathbf{n}-1}$. We omit the technical details. Denote the unmixed representation of V'_{st} again by Δ'_{st}. Note that we used that the leading coefficient of g_m does not vanish over any component of $V(C')$.

Let $p_{st} \in R[x_n]$ be the gcd of g_m and f, and let q_{st} be the quotient of g_m and p_{st} over $\mathbf{K}(\mathcal{P}')$ for all $\mathcal{P}' \in \mathrm{Ap}(C'_{st})$, where $C'_{st} \in \Delta'_{st}$. The polynomial p_{st} is computed by simply solving the linear system corresponding to the t^{th} subresultant of g_m and the slice of f of degree s. The polynomial q_{st} is computed by a simple pseudodivision algorithm.

Since g_m is squarefree, we have that p_{st} and q_{st} are squarefree and relatively prime. Also, since C'_{st} satisfies the above properties, we have that $\mathrm{lc}(p_{st}), \mathrm{lc}(q_{st}) \notin \mathcal{P}'$ for all $\mathcal{P}' \in \mathrm{Ap}(C'_{st})$. Thus $C'_{st} \cup \{p_{st}\}$ and $C'_{st} \cup \{q_{st}\}$ are unmixed ascending sets. Define

$$(\Gamma, \Delta) = (\bigcup_{s,t} \Gamma_{st}, \bigcup_{s,t} \Delta_{st}).$$

where $\Gamma_{st} = \{C'_{st} \cup \{q_{st}\} \mid C'_{st} \in \Delta'_{st}\}$ and $\Delta_{st} = \{C'_{st} \cup \{p_{st}\} \mid C'_{st} \in \Delta'_{st}\}$. It can be proved that $\Gamma \cup \Delta$ is simple, it is an unmixed decomposition of $\mathrm{Rep}(C)$, and f identically vanish over the components in Δ but does not vanish identically ofer the components in Γ.

3.5 Complexity

The complexity bounds below are for arithmetic circuits over $\mathbb{Q}$. Let n be the number of variables. It can be shown that the sizes of the circuits in the first five cases below are polynomials in the bounds for the sizes of the polynomials occuring in the computation. Thus, if the degree bound for the polynomials occuring in the computation is D, then the size in the dense representation is D^n, and the size of the arithmetic circuit is $(D^n)^{O(1)}$. Below we give the degree bounds and the circuit depth for the algorithms described in the paper.

1. $\mathbf{prem}^{\mathbf{m}}_{\mathbf{n}}(f, C)$, where $C = \{g_1, \dots, g_m\} \subset \mathbb{Q}[x_1, \dots, x_n]$ unmixed set, $f \in \mathbb{Q}[x_1, \dots, x_l]$ for some $l \geq n$, and **prem** computes the pseudoremainder of f modulo C. Denote by d the maximum degree of the polynomials in the input. Also, if $x_{i_s} = \mathrm{class}(g_s)$ then d_s denotes the maximum of $\deg_{x_{i_s}}(f)$ and $\deg_{x_{i_s}}(g_s)$ $(s = 1, \dots, m)$, and if $x_j \neq \mathrm{class}(g_s)$ for any s then k_j denotes the maximal degree of the input in the variable x_j.

   Degree bounds Any polynomial p in the computation have $\deg_{x_{i_s}}(p) \leq 2d_s$ $(s = 1, \dots, m)$ and $\deg_{x_j}(p) \leq k_j \prod_{s=1}^m d_s$ if $j \neq i_s$. Note that the first bound holds for all variables in the zero-dimensional case $(n = m)$.

   Circuit depth For the pseudodivision we use similar method as in [19] solving linear equation systems. Thus using the definition in section 2.1, we have that

   $$\mathrm{Depth}(\mathbf{prem}^{\mathbf{m}}_{\mathbf{n}}(C, f)) \leq c_1 (n \log(d))^2$$

   for some constant c_1.

2. $\mathbf{simplify}^{\mathbf{m}}_{\mathbf{n}}(\Gamma_1, \dots, \Gamma_r)$, where $\Gamma_1, \dots, \Gamma_r$ are simple sets of unmixed ascending sets, and all unmixed set in $\bigcup \Gamma_i$ have the same type.

   Degree bounds If $x_{i_s} = \mathrm{class}(g_s)$ for some g_s in the input, then all the computed polynomials can be reduced by $g'_s \in \bigcup \Gamma_i$, the maximum degree polynomial in the variable x_{i_s}. Thus any polynomial p in the computation has $\deg_{x_{i_s}}(p) \leq 2\deg_{x_{i_s}}(g'_s) = 2d_s$. If $x_j \neq \mathrm{class}(g_s)$ for any polynomial g_s in the input, and k_j denotes the maximum degree of the input in the variable x_j, then any polynomial p in the computation has $\deg_{x_j}(p) \leq r k_j \prod_{s=1}^m d_s$.

   Circuit depth The depth of $\mathbf{simplify}^{\mathbf{m}}_{\mathbf{n}}(\Gamma_1, \dots, \Gamma_r)$ is $\log(r)$ times the depth of $\mathbf{simplify}^{\mathbf{m}}_{\mathbf{n}}(C, C')$. The latter algorithm has depth $c_2 mn \log^2(d')\mathrm{Depth}(\mathbf{prem})$, where $d' = rd$ is the maximum degree in C' and d is the maximum degree of the polynomials in $\bigcup \Gamma_i$. Thus

   $$\mathrm{Depth}(\mathbf{simplify}^{\mathbf{m}}_{\mathbf{n}}(\Gamma_1, \dots, \Gamma_r)) \leq c_2 (n \log(r) \log(d))^4$$

   for some constant c_2.

3. $\mathbf{split}^{\mathbf{m}}_{\mathbf{n}}(C, f)$, where $C = \{g_1, \dots, g_m\}$ and $f \in \mathbb{Q}[x_1, \dots, x_l]$ for some $l \geq n$, and d, d_s and k_j denotes the same as in 1. above.

   Degree bounds As above, any polynomial p in the computation has $\deg_{x_{i_s}}(p) \leq 2d_s$ $(s = 1, \dots, m)$ and $\deg_{x_j}(p) \leq k_j \prod_{s=1}^m d_s$ $(j \neq i_s)$.

Circuit depth $\mathbf{split}_{\mathbf{n}}^{\mathbf{m}}$ recursively calls $\mathbf{split}_{\mathbf{n-1}}^{\mathbf{m-1}}$, $\mathbf{simplify}_{\mathbf{n-1}}^{\mathbf{m-1}}$, and conducts determinant computations. An easy computation gives that

$$\text{Depth}(\mathbf{split}_{\mathbf{n}}^{\mathbf{m}}(C,f)) \leq c_3(n\log(d))^6$$

for some constant c_3.

4. $\mathbf{general}_{\mathbf{n}}^{\mathbf{m}}(C,F)$, where $C = \{g_1,\ldots,g_m\}$ and $F \subset \mathbb{Q}[x_1,\ldots,x_n]$ and the maximal degree of the polynomials in the input is d.

   Degree bounds Using the bounds in section 3.2 we get that any polynomial p in the computation has $\deg_{x_i}(p) \leq d^n$ for $i = 1,\ldots,n$.

   Circuit depth An easy computation gives that

   $$\text{Depth}(\mathbf{general}_{\mathbf{n}}^{\mathbf{m}}(C,F)) \leq c_4(n\log(d))^4$$

   for some constant c_4.

5. $\mathbf{decompose}_{\mathbf{n}}^{\mathbf{m}}(C,F,T)$, where $C = \{g_1,\ldots,g_m\}$, $F \subset \mathbb{Q}[x_1,\ldots,x_n]$, $T \subset \mathbb{Q}[x_1,\ldots,x_l]$ for some $l \geq n$. Here $|T| = c$ and the maximum degree of the polynomials in the input is d.

   Degree bounds As above, we get that any polynomial f in the computation has $\deg_{x_i}(f) \leq d^n$ for $i = 1,\ldots,n$.

   Circuit depth $\mathbf{decompose}_{\mathbf{n}}^{\mathbf{m}}$ calls the subroutine $\mathbf{general}_{\mathbf{n}}^{\mathbf{m}}$, and the subroutine $\mathbf{split}_{\mathbf{n}}^{\mathbf{m}}$ $c+2$ times, and iteratively calls $\mathbf{decompose}_{\mathbf{n-1}}^{\mathbf{m-1}}$. Using the above bounds we get that

   $$\text{Depth}(\mathbf{decompose}_{\mathbf{n}}^{\mathbf{m}}(C,F,T)) \leq c_5c(n\log(d))^8$$

   for some constant c_5.

6. Last, we note that in the computation of the unmixed representetion of $\sqrt{\langle F\rangle}$, the number of branches created at each codimension m (corresponding to the components) never exceeds the square of the number of irreducible components in the variety of $\langle F\rangle$ (using the simple refinement algorithm). If the maximal degree of the polynomials in F is d then the number of irreducible components is $\leq d^n$, so the number of branches is always $\leq d^{2n}$.

Acknowledgements

I would like to thank Dexter Kozen for many helpful conversations and suggestions.

References

[1] Ben-Or, M., Kozen, D., and Reif, J. The complexity of elementary algebra and geometry. *J. Comput. Syst. Sci. 32* (1985), 251–264.

[2] Buchberger, B., Collins, G. E., and Kutzler, B. Algebraic methods for geometric reasoning. *Ann. Rev. Comput. Sci. 3* (1988), 85–119.

[3] Chistov, A. L. An algorithm of polynomial complexity for factoring polynomials, and determination of the components of a variety in a subexponential time. *Zap. Nauchn. Se,. Leningrad. Otdel. Inst. Steklov (LOMI) 137* (1984), 124–188. Russian, English summary.

[4] Dicrescenzo, C., and Duval, D. *Computations on curves*, vol. 174 of *Lecture Notes in Computer Science*. Springer, 1984, pp. 100–107.

[5] Dicrescenzo, C., and Duval, D. Algebraic computations on algebraic numbers. In *Informatique et Calcul*. Wiley-Masson, 1985, pp. 54–61.

[6] Gallo, G., and Mishra, B. Wu-Ritt characteristic sets and their complexity. *DIMACS Series in Discrete Mathematics and Theoretical Computer Science 6* (1991), 111–136.

[7] Giusti, M., and Heintz, J. Algorithmes - disons rapides - pour la décomposition d'une variété algébrique en composantes irréductibles et équidimensionnelles. In *Effective Methods in Algebraic Geometry*, T. Mora and C. Traverso, Eds. Birkhäuser, 1991, pp. 169–194.

[8] Grigorév, D. Y. Factoring polynomials over a finite field and solving systems of algebraic equations. *Zap. Nauchn. Se,. Leningrad. Otdel. Inst. Steklov (LOMI) 137* (1984), 20–79. Russian, English summary.

[9] Hartshorne, R. *Algebraic Geometry*. Springer-Verlag, 1977.

[10] Ierardi, D., and Kozen, D. Parallel resultant computation. In *Synthesis of Parallel Algorithms*, J. Reif, Ed. Morgan Kauffman, 1993, pp. 679–720.

[11] Ierardi, D. J. *The complexity of quantifier elimination in the theory of an algebraically closed field.* PhD thesis, Cornell University, 1989.

[12] Kalkbrener, M. Algorithmic properties of polynomial rings. Habilitationsschrift.

[13] Kalkbrener, M. Prime decomposition of radicals in polynomial rings. *J. Symbolic Computation 18* (1994), 365–372.

[14] Kozen, D. Efficient resolution of singularities of plane curves. Tech. rep., Cornell University, Mathematical Science Institute, 1994.

[15] Lazard, D. Resolution des systemes d'equations algebriques. *Theoret. Comp. Sci. 15*, 1 (1981). French, English summary.

[16] Ritt, J. F. *Differential algebra*. American Mathematical Society, 1950.

[17] Sturmfels, B. Sparse elimination theory. In *Computational algebraic geometry and commutative algebra*, D. Eisenbud and L. Robbiano, Eds. Cambridge, 1991, pp. 264–298.

[18] Teitelbaum, J. The computational complexity of the resolution of plane curve singularities. *Math. Comp. 54* (1990), 797–837.

[19] von zur Gathen, J. Parallel algorithms for algebraic problems. *SIAM J. Comput. 13*, 4 (1984), 802–824.

[20] Wang, D. Irreducible decomposition of algebraic varieties via characteristic sets and Gröbner bases. *Computer Aided Geometric Design 9* (1992), 471–484.

[21] WANG, D. Elimination method for mechanical theorem proving in geometries. *Annals of Math. and Artificial Intelligence 13* (1995), 1–24.

[22] WU, W.-T. Basic principles of mechanical theorem proving in elementary geometries. *J. Syst. Sci. Math. Sci. 4* (1984), 207–235.