IJMMS 2003:70, 4421–4434
PII. S0161171203205378
http://ijmms.hindawi.com
© Hindawi Publishing Corp.

ON THE RESOLVENT OF AN IDEAL AND SOME APPLICATIONS

DRISS BOUZIANE and ABDELILAH KANDRI RODY

Received 5 May 2002

We give an algorithm to compute a resolvent of an algebraic variety without computing its irreducible components; we decompose the radical of an ideal into prime ideals and we test the primality of a regular ideal.

2000 Mathematics Subject Classification: 68W30.

1. Introduction. A fundamental construction in algebraic geometry is the decomposition of a variety into irreducible components; this is connected from commutative algebra viewpoint with the primary decomposition of ideals. The purpose of this paper is to study the structure of an affine variety V defined by a zero-set of a finite set of the polynomial ring $K[x_1,\dots,x_n]$. We characterize the associated irreducible varieties of V by a resolvent.

The concept of resolvent was introduced by Ritt [14] in his work on differential algebra. He showed that generic zeros of a prime differential ideal are birationally equivalent to general zeros of one differential polynomial.

Based on Ritt-Wu's algorithm to decompose a variety into irreducible varieties, Gao and Chou [8] extended Ritt's concept of resolvent to an ideal, not necessarily prime, with respect to a parametric set. They use a factorization over a tower of algebraic extensions of the field of coefficients. In the ordinary differential case, Cluzeau and Hubert [6] extended also Ritt's concept of resolvent to regular differential ideals. We exploit the interplay between both results to compute a resolvent of an ideal $\mathcal{I}$ with respect to a parametric set. We use a decomposition of $\sqrt{\mathcal{I}}$ as an intersection of regular ideals, we compute a basis of $\sqrt{\mathcal{I}}$, and then we deduce the resolvent of the ideal $\sqrt{\mathcal{I}}$. The approach taken in this paper is interesting. Avoiding factorization, we compute irreducible varieties associated to a given affine variety and we check whether a regular ideal is prime.

We begin the paper with some basic definitions and properties on irreducible, regular, and characterizable ideals and we recall the link between Gröbner bases and characteristic sets. In Section 4, we prove the Ritt's theorem and some related properties of the resolvent. Section 5 describes an algorithm which computes a resolvent of an ideal. In Section 6, we illustrate some applications of resolvents.

2. Preliminaries and notation

2.1. Definitions and notation. Let $K[x] = K[x_1,\dots,x_n]$ be the ring of algebraic polynomials in n indeterminates with coefficients in a field K of characteristic zero. We fix an order on the indeterminates such that $x_1 \prec \cdots \prec x_n$. Let f be a polynomial not in K. The leading variable of f is the highest indeterminate x_i appearing in f; it is denoted by $\mathrm{lv}(f)$. The *initial* of f, $\mathrm{init}(f)$, is the coefficient of the highest power of $\mathrm{lv}(f)$ in f. The *rank* of f, $\mathrm{rank}(f)$, is the monomial $\mathrm{lv}(f)^d$, where d is the degree of f in $\mathrm{ld}(f)$. The *tail* of f, $\mathrm{tail}(f)$, is the polynomial $f - \mathrm{init}(f)\cdot\mathrm{lv}(f)^d$. The *separant* of f, $\mathrm{sep}(f)$, is equal to $\partial f/\partial v$ with $v = \mathrm{lv}(f)$. We also define h_f to be the product of the *initial* and the *separant* of f.

Let Σ be a subset of $K[x]$. We denote, respectively, by (Σ) and $\sqrt{(\Sigma)}$ the ideal and the radical ideal generated by Σ. An ideal $\mathcal{I}$ is said to be radical if $\sqrt{\mathcal{I}} = \mathcal{I}$.

A polynomial g is said to be *reduced* with respect to f if the degree of g in $\mathrm{lv}(f)$ is strictly less than the degree of f in $\mathrm{lv}(f)$.

Let f and g be two elements of $K[x]$. With a finite number of pseudodivisions, we can compute a polynomial $\mathrm{rem}(g;f)$ reduced with respect to f such that there exists $\alpha \in \mathbb{N}$ satisfying

$$\mathrm{init}(f)^{\alpha}\cdot g \equiv \mathrm{rem}(g;f)\,\mathrm{mod}(f). \tag{2.1}$$

Any order $\prec$ on x can be extended to a partial order on $K[x]$ as follows: for f and g in $K[x]$, we say that f is less than g, and we write $f \prec g$ if either

(i) $f \in K$ and $g \notin K$;

(ii) $\mathrm{lv}(f) \prec \mathrm{lv}(g)$; or

(iii) $\mathrm{lv}(f) = \mathrm{lv}(g) = v$ and $\mathrm{degree}(f,v) < \mathrm{degree}(g,v)$.

If neither $f \prec g$ nor $g \prec f$, we say that f and g are equivalent, we write $f \equiv g$.

2.2. Autoreduced sets. A subset $\mathcal{A}$ of $K[x]$ is called an *autoreduced set* if every element of $\mathcal{A}$ is reduced with respect to the others. An autoreduced set is finite (see [13, page 77]). An autoreduced set $\mathcal{A} = \{A_1,\dots,A_p\}$ is denoted by $A_1,\dots,A_p$ if $A_1 \prec \cdots \prec A_p$. If $\mathcal{A} = A_1,\dots,A_p$ and $\mathcal{B} = B_1,\dots,B_q$ are two autoreduced sets, we say that $\mathcal{A}$ is less than $\mathcal{B}$ and we write $\mathcal{A} \prec \mathcal{B}$ if either

(i) there exists $k \le \min(p,q)$ such that $A_i \equiv B_i$ for $i < k$ and $A_k \prec B_k$; or

(ii) $p > q$ and $A_i \equiv B_i$ for $1 \le i \le q$.

If neither $\mathcal{A} \prec \mathcal{B}$ nor $\mathcal{B} \prec \mathcal{A}$, we say that $\mathcal{A}$ and $\mathcal{B}$ are equivalent, we write $\mathcal{A} \equiv \mathcal{B}$.

Remark 2.1. The order on the set of autoreduced sets is Artinian (well ordering) (see [14, page 4] and [13, page 81]).

Let F be a nonempty subset of $K[x]$, then the set of all autoreduced sets of F has a minimal element; it is called a *characteristic set* of F. There is no nonzero element of F reduced with respect to its characteristic set. Two characteristic sets of F are equivalent.

Proposition 2.2. *Let $\mathcal{A} = A_1, \dots, A_p$ be an autoreduced set. Then for any polynomial f, there exist nonnegative integer α and a polynomial g reduced with respect to $\mathcal{A}$ such that $I_{\mathcal{A}}^{\alpha} \cdot f \equiv g \operatorname{mod}(\mathcal{A})$, where $I_{\mathcal{A}}$ is the product of the initials of elements in $\mathcal{A}$.*

Let S be a nonempty subset of $K[x]$ and let $\mathcal{I}$ be an ideal of $K[x]$. We define the saturation of $\mathcal{I}$ by S as $\mathcal{I} : S^{\infty} = \{f \in K[x] : h \cdot f \in \mathcal{I}$ for h a product of elements of $S\}$. It is also an ideal of $K[x]$. When S is finite, $\mathcal{I} : S^{\infty}$ is in fact equal to $\{f \in K[x] \mid \exists \alpha \in \mathbb{N},\ s^{\alpha} \cdot f \in \mathcal{I}\}$ that is usually denoted by $\mathcal{I} : s^{\infty}$, where s is the product of elements of S.

Proposition 2.3. *Let Σ be a nonempty subset of $K[x]$. Let $f_1, \dots, f_r \in K[x]$ and let S be a finite subset of $K[x]$. Then the following properties hold true:*

(i) $\sqrt{(\Sigma, \prod_{i=1}^{r} f_i)} = \bigcap_{i=1}^{r} \sqrt{(\Sigma, f_i)}$;

(ii) $\sqrt{(\Sigma) : S^{\infty}} = \sqrt{(\Sigma)} : s$, *where s is the product of elements of S.*

Proof. See [1, 9]. □

2.3. Regular and characterizable ideal. Let $\mathcal{A}$ be an autoreduced set with respect to some given order on x. Let $H_{\mathcal{A}} = I_{\mathcal{A}} S_{\mathcal{A}}$, where $I_{\mathcal{A}}$ and $S_{\mathcal{A}}$ are, respectively, the product of initials and the product of separants of elements in $\mathcal{A}$. The autoreduced set $\mathcal{A}$ is said to be consistent if $1 \notin (\mathcal{A}) : H_{\mathcal{A}}^{\infty}$.

Definition 2.4. Let $\mathcal{I}$ be an ideal of $K[x]$.

(i) The ideal $\mathcal{I}$ is said to be a *regular* ideal with respect to some order $\prec$ on the variables x if it is of the form $(\mathcal{A}) : H_{\mathcal{A}}^{\infty}$, where $\mathcal{A}$ is an autoreduced set with respect to the same order $\prec$.

(ii) The ideal $\mathcal{I}$ is said to be a *characterizable* ideal with respect to some order $\prec$ on x if there is an autoreduced set $\mathcal{A}$ with respect to the same order $\prec$ such that $\mathcal{A}$ is a characteristic set of $\mathcal{I}$ and $\mathcal{I} = (\mathcal{A}) : H_{\mathcal{A}}^{\infty}$. In this case we say that $\mathcal{A}$ is a characteristic set.

Remark 2.5. (1) Every characterizable ideal is regular. The converse is false (see [10, Example 2.5]).

(2) Every prime ideal is characterizable for any order on the variables. But a characterizable ideal is not necessarily prime.

(3) There exists some ideal that is characterizable with respect to some order on x but not with respect to another order (see [10, Example 3.6]).

(4) There is an algorithm to decompose a radical of an ideal as intersection of characterizable ideals (see [5, 10]).

(5) There is an algorithm to decompose a radical of an ideal as intersection of regular ideals (see [3]).

In the following theorem we recall some properties of a regular ideal.

Theorem 2.6 (Lazard's lemma). *Let $\mathcal{A}$ be an autoreduced set of $K[x]$. Then $(\mathcal{A}) : H_{\mathcal{A}}^{\infty}$ is a radical ideal. Furthermore, the characteristic set of a minimal prime component of $(\mathcal{A}) : H_{\mathcal{A}}^{\infty}$ has the same set of leaders as $\mathcal{A}$.*

Proof. See [4, 10]. □

The following theorem gives a necessary and sufficient condition for a regular ideal to be characterizable.

Theorem 2.7. *Let $\mathcal{A} = A_1,\dots,A_p$ be an autoreduced set of $K[x]$. The autoreduced set $\mathcal{A}$ is a characteristic set if and only if*

(i) $\operatorname{init}(A_i)$ *is not a zero divisor modulo* $(\mathcal{A}_{i-1}):I^{\infty}_{\mathcal{A}_{i-1}}$;

(ii) $\operatorname{sep}(A_i)$ *is not a zero divisor modulo* $(\mathcal{A}_i):I^{\infty}_{\mathcal{A}_i}$,

where $\mathcal{A}_i = A_1,\dots,A_i$.

Proof. See [1, 5]. □

2.4. Irreducible autoreduced set. Let $\mathcal{A} = A_1,\dots,A_p$ be an autoreduced set of $K[x]$ and $y = y_1,\dots,y_p$ are the leading variables of elements in $\mathcal{A}$, and let $u = u_1,\dots,u_q$ be the other indeterminates that are present in the elements of $\mathcal{A}$. The autoreduced set $\mathcal{A}$ becomes an autoreduced set in the ring $K[u,y]$.

Definition 2.8. An autoreduced set $\mathcal{A}$ is said to be irreducible if either

(i) $p = 1$ and A_1 is irreducible in $K(u)[y_1]$; or

(ii) $A_1,\dots,A_{p-1}$ is *irreducible* and A_p is irreducible as a polynomial in y_p with coefficients considered in the quotient field of $K(u)[y_1,\dots,y_{p-1}]/\mathcal{I}_{p-1}$, where $\mathcal{I}_{p-1} = (\mathcal{A}_{p-1}):H^{\infty}_{\mathcal{A}_{p-1}}$ and $\mathcal{A}_{p-1} = A_1,\dots,A_{p-1}$.

Proposition 2.9. *Let $\mathcal{A} = A_1,\dots,A_p$ be an autoreduced set in $K[x]$ such that A_1 is irreducible in $K(u)[y_1]$ and for all $i = 2,\dots,p$, A_i has degree one in its leading variable. Then $\mathcal{A}$ is an irreducible autoreduced set.*

Proposition 2.10. *An irreducible autoreduced set $\mathcal{A}$ is a characteristic set of a prime ideal. This ideal is exactly the regular one associated to $\mathcal{A}$, that is, $(\mathcal{A}):H^{\infty}_{\mathcal{A}}$.*

2.5. The link between Gröbner basis and characteristic set. In this section, we recall an interesting result cited in [11, 12], which says that we can extract a characteristic set from a lexicographical Gröbner basis.

Lemma 2.11. *Let $\mathcal{A}$ be an autoreduced set in $K[x]$ and let $\mathcal{I}$ be an ideal containing $\mathcal{A}$. Then $\mathcal{A}$ is a characteristic set of $\mathcal{I}$ if and only if for all nonzero polynomial f in $\mathcal{I}$, f is not reduced with respect to $\mathcal{A}$.*

Proof. See [14, page 5]. □

Let $\mathcal{B} = B_1 \prec \cdots \prec B_r$ be the reduced Gröbner basis (see [2] for more details about this notion) of $\mathcal{I}$ an ideal in $K[x]$ with respect to the lexicographical term order such that $x_1 \prec \cdots \prec x_n$.

Let $C_1 = B_1$, $C_2 = \operatorname{rem}(B_{i_1};C_1)$ with B_{i_1} the first polynomial that contains a new variable not appearing in B_1.

Let $C_2 = \operatorname{rem}(B_{i_2};C_1,C_2)$ with B_{i_2} the first polynomial that contains a new variable not appearing in B_{i_1}.

We continue this finite processes; we obtain a family of polynomials $\mathcal{C} = C_1,\dots,C_s$ which is an autoreduced set with respect to the order $x_1 \prec \cdots \prec x_n$.

Proposition 2.12. *With the same notation as above, $\mathcal{C}$ is a characteristic set of $\mathcal{I}$ with respect to the order $x_1 \prec \cdots \prec x_n$ and is called the extracted characteristic set from $\mathcal{B}$.*

Proof. Let $f \in \mathcal{I}$ and $f \neq 0$; by Lemma 2.11 it is sufficient to show that f is not reduced with respect to $\mathcal{C}$. Since $\mathcal{B}$ is a Gröbner basis of $\mathcal{I}$, then there is B_i in $\mathcal{B}$ such that the leading lexicographical monomial of B_i divides some monomial in f. So there exists C_j in $\mathcal{C}$ such that $\deg(f,\mathrm{lv}(C_j)) \geq \deg(C_j,\mathrm{lv}(C_j))$. Hence, f is not reduced with respect to $\mathcal{C}$. □

In what follows, autoreduced sets are supposed to be consistent.

3. Resolvent of an ideal. Gao and Chou have introduced in [8] the notion of resolvent for an arbitrary ideal with respect to a parametric set as a generalization of the one introduced by Ritt for a prime ideal; they have given an algorithm to compute a resolvent using the decomposition of a radical ideal into prime ideals. In this section, we recall some definitions and properties about this notion. Then we give an algorithm to compute a resolvent of an ideal $\mathcal{I}$ using a decomposition of $\sqrt{\mathcal{I}}$ into regular ideals without using factorization over a tower of algebraic extensions.

Definition 3.1. Let $\mathcal{I}$ be an ideal of $K[x]$. A subset $u = u_1,\dots,u_q$ of $\{x_1,\dots,x_n\}$ is said to be a parametric set of $\mathcal{I}$ if $K[u] \cap \mathcal{I} = (0)$ and for every $y \in \{x_1,\dots,x_n\} \setminus \{u_1,\dots,u_q\}$, $K[u,y] \cap \mathcal{I} \neq (0)$.

The set of nonleading variables of elements in an autoreduced set $\mathcal{A}$ is called the parametric set of $\mathcal{A}$.

Remark 3.2. Let $\mathcal{A}$ be an irreducible autoreduced set with the parametric set u. Then u is a parametric set of the prime ideal $(\mathcal{A}) : H_{\mathcal{A}}^{\infty}$.

Lemma 3.3. *Let $\mathcal{P}$ be a prime ideal with a parametric set u and let $f \notin \mathcal{P}$. Then $(\mathcal{P}, f) \cap K[u] \neq (0)$.*

Proof. See [14]. □

Lemma 3.4. *Let $\mathcal{A}$ be an autoreduced set in $K[x]$ with u the parametric set of $\mathcal{A}$. Then u is a parametric set of $(\mathcal{A}) : H_{\mathcal{A}}^{\infty}$.*

Proof. By Lazard's lemma, each minimal prime component of $(\mathcal{A}) : H_{\mathcal{A}}^{\infty}$ has u as a parametric set. Then $(\mathcal{A}) : H_{\mathcal{A}}^{\infty}$ is a decomposition of prime ideals such that each one has u as a parametric set. So u is a parametric set of $(\mathcal{A}) : H_{\mathcal{A}}^{\infty}$. □

Lemma 3.5. *Let $\mathcal{I}$ be an ideal of $K[x] = K[u,y]$ having $u = u_1,\dots,u_q$ as a parametric set with $y = x \setminus u = y_1,\dots,y_p$. Let $\mathcal{I}'$ be the ideal obtained from $\mathcal{I}$*

by replacing each y_i by a new variable z_i. Consider $\mathcal{J}$ the ideal generated by $\mathcal{I}$ and $\mathcal{I}'$ in $K[u,y,z]$. Then $\mathcal{J}$ has u as a parametric set.

Proof. Let $h \in \mathcal{J} \cap K[u]$, since h is independent of y and z, then if we replace z_i's by the y_i's, we obtain that h is in $\mathcal{I}$, hence $\mathcal{J} \cap K[u] = (0)$. Since $\mathcal{I} \subseteq \mathcal{J}$, then for all $i = 1,\dots,p$, we have $\mathcal{J} \cap K[u,y_i] \neq (0)$ and $\mathcal{J} \cap K[u,z_i] \neq (0)$. □

In the following theorem proved in [7] for a prime ideal, we extend the same result for an arbitrary ideal.

Theorem 3.6 (Ritt's theorem). *Let $\mathcal{I}$ be an ideal of $K[u,y]$ with $u = u_1,\dots, u_q$ as a parametric set. Then there exist $G \in K[u] \setminus \{0\}$ and integers $M_1,\dots,M_p$ such that two distinct zeros of $\mathcal{I}$ with the u taking the same values for which G does not vanish give different values for $Q = M_1 y_1 + \cdots + M_p y_p$.*

Proof. Let $\mathcal{J} = (\mathcal{I},\mathcal{I}')$ be the ideal defined in Lemma 3.5.

(a) Let $\sqrt{\mathcal{J}} = \mathcal{J}_1 \cap \cdots \cap \mathcal{J}_t$ be the decomposition of $\sqrt{\mathcal{J}}$ into prime ideals.

(A) If, for some $j \in \{1,\dots,t\}$, u is not a parametric set of $\mathcal{J}_j$, then there is $h_j(u) \in \mathcal{J}_j \cap K[u]$ and $h_j \neq 0$.

(B) If, for some j, the ideal $(y_1 - z_1,\dots,y_p - z_p) \subseteq \mathcal{J}_j$ and u is a parametric set of $\mathcal{J}_j$, then we put $h'_j = 1$.

(C) If, for some j, the ideal $(y_1 - z_1,\dots,y_p - z_p)$ is not a subset of $\mathcal{J}_j$ and u is a parametric set of $\mathcal{J}_j$. Then there exists $k \in \{1,\dots,p\}$ such that $y_k - z_k \notin \mathcal{J}_j$. Since $\mathcal{J}_j$ is a prime ideal and u is a parametric set of $\mathcal{J}_j$, then by Lemma 3.3, $(\mathcal{J}_j, y_k - z_k) \cap K[u] \neq (0)$, hence there exists $h'_j(u) \in (\mathcal{J}_j, y_k - z_k) \cap K[u]$, $h'_j(u) \neq 0$.

The cases (A), (B), and (C) exhaust all possibilities.

(b) Let $j_1,\dots,j_s$ be such that u is a parametric set of $\mathcal{J}_j$ and $(y_1 - z_1,\dots,y_p - z_p)$ is not a subset of $\mathcal{J}_j$ for all $j \in \{j_1,\dots,j_s\}$. Then there exist integers $M_1,\dots,M_p$ such that $\bar{c} = M_1(y_1 - z_1) + \cdots + M_p(y_p - z_p) \notin \mathcal{J}_j$ for all $j \in \{j_1,\dots,j_s\}$. Consequently, by Lemma 3.3, $(\mathcal{J}_j, \bar{c}) \cap K[u] \neq (0)$. We put $h'' = h''_1 \cdots h''_s$ with $h''_j \in (\mathcal{J}_j,\bar{c}) \cap K[u]$, $h''_j \neq 0$.

(c) Let G be the product of h_j (case (A)), of h'_j (cases (B) and (C)), and of h''. Let $(\bar{u}, y')$ and $(\bar{u}, y'')$ be two distinct zeros of $\mathcal{I}$, then $(\bar{u}, y', y'')$ is a zero of $\mathcal{J}$.

We assume that $\sum_{i=1}^{p} M_i(y'_i - y''_i) = 0$; there are three cases to be distinguished:

(i) $(\bar{u}, y', y'')$ is a zero of some $\mathcal{J}_j$ satisfying case (A), then $h_j(\bar{u}) = 0$, and hence $G(\bar{u}) = 0$;

(ii) $(\bar{u}, y', y'')$ is a zero of some $\mathcal{J}_j$ satisfying case (B), then $y' = y''$ and hence $(\bar{u}, y') = (\bar{u}, y'')$. This case is impossible;

(iii) $(\bar{u}, y', y'')$ is a zero of some $\mathcal{J}_j$ satisfying case (C).

If there exists $k \in \{1,\dots,p\}$ such that $y'_k = y''_k$, then $(\bar{u}, y', y'')$ will be a zero of $(\mathcal{J}_j, y_k - z_k)$, and we will have $h'_j(\bar{u}) = 0$; this implies that $G(\bar{u}) = 0$. If $y'_k \neq y''_k$

for all $k \in \{1,\dots,p\}$, then $(\bar{u},y',y'')$ will be a zero of $(\mathcal{J}_j,\bar{c})$, hence $h''(\bar{u}) = 0$, and then $G(\bar{u}) = 0$. □

Lemma 3.7. *Let $\mathcal{I}_1$ and $\mathcal{I}_2$ be two ideals in $K[x]$, ω a new variable, and $Q = \sum_{i=1}^{p} M_i y_i$, where the M_i's are integers. Then $(\mathcal{I}_1 \cap \mathcal{I}_2, \omega - Q) = (\mathcal{I}_1, \omega - Q) \cap (\mathcal{I}_2, \omega - Q)$.*

Proof. It is sufficient to prove the indirect inclusion.

Let f be in $(\mathcal{I}_1, \omega - Q) \cap (\mathcal{I}_2, \omega - Q)$, then $f = \sum_{i=1}^{s} \lambda_i f_i + h_1(\omega - Q) = \sum_{j=1}^{t} \mu_j g_j + h_2(\omega - Q)$, where h_1, h_2, λ_i, μ_j are in $K[x,\omega]$ and $f_i \in \mathcal{I}_1$ and $g_j \in \mathcal{I}_2$ for $i = 1,\dots,s$ and $j = 1,\dots,t$.

We can consider the λ_i's and the μ_j's as free from ω because otherwise we reduce these polynomials with respect to $\omega - Q$, then $\sum_{i=1}^{s} \lambda_i f_i - \sum_{j=1}^{t} \mu_j g_j = (h_2 - h_1)(\omega - Q)$.

Since the left-hand side is free of ω, then $\sum_{i=1}^{s} \lambda_i f_i = \sum_{j=1}^{t} \mu_j g_j$, and f is in $(\mathcal{I}_1 \cap \mathcal{I}_2, \omega - Q)$. □

Lemma 3.8. *Let $\mathcal{I}$ be a prime ideal in $K[u,y]$ such that u is a parametric set, ω a new variable, and $Q = \sum_{i=1}^{p} M_i y_i$, where the M_i's integers. Then the ideal $(\mathcal{I}, w - Q)$ is prime and has u as a parametric set.*

Proof. See [14, page 40]. □

Lemma 3.9. *Let $\mathcal{I}$ be an ideal of $K[u,y]$ having u as a parametric set. Let ω be a new variable and $Q = \sum_{i=1}^{p} M_i y_i$ with the M_i's integers. Then $\sqrt{(\mathcal{I}, w - Q)} = (\sqrt{\mathcal{I}}, w - Q)$ and u is a parametric set of the ideal $\mathcal{J} = (\mathcal{I}, w - Q)$ in $K[x,\omega]$.*

Proof. For the first point, let $f \in \sqrt{(\mathcal{I}, w - Q)}$, then there exists $\alpha \in \mathbb{N}$ such that $f^\alpha \in (\mathcal{I}, \omega - Q)$, hence $f^\alpha = g + h(\omega - Q)$, where $g \in (\mathcal{I})$ in $K[x,\omega]$ and $h \in K[x,\omega]$. We reduce f and g with respect to $\omega - Q$, then we obtain $f = f_1 + f_2(\omega - Q)$ and $g = g_1 + g_2(\omega - Q)$ with $f_1 \in K[x]$, $g_1 \in \mathcal{I}$, and $f_2, g_2 \in K[x,\omega]$. Consequently, $f^\alpha = f_1^\alpha + F(\omega - Q) = g_1 + g_2(\omega - Q)$ for some $F \in K[x,\omega]$, then $f_1^\alpha = g_1 \in \mathcal{I}$; this implies that $f \in (\sqrt{\mathcal{I}}, \omega - Q)$.

For the second property, we show that $\mathcal{J} \cap K[u] = (0)$ and $\mathcal{J} \cap K[u,\omega] \neq (0)$. Firstly, we assume that $\mathcal{J} \cap K[u] \neq (0)$, then there exist a nonzero polynomial $P(u)$ in $\mathcal{J} \cap K[u]$; this implies that there exist $f, f_1,\dots,f_r \in K[x,\omega]$ and $g_1,\dots,g_r \in \mathcal{I}$ such that $P(u) = \sum_{i=1}^{r} f_i g_i + f(w - Q)$; for $\omega = Q$, we will have $P(u) \in K[u] \cap \mathcal{I}$, but this is impossible because u is a parametric set of $\mathcal{I}$. Secondly, we decompose $\sqrt{\mathcal{I}}$ into prime ideals such that $\sqrt{\mathcal{I}} = (\bigcap_{i=1}^{s} m_i) \cap (\bigcap_{j=1}^{t} p_j)$, where the m_i's are the prime components having u as a parametric set and the p_j's are those satisfying $p_j \cap K[u] \neq (0)$. By Lemma 3.8, we have $(m_i, \omega - Q) \cap K[u,\omega] \neq (0)$, then by the first property and Lemma 3.7, we deduce that u is a parametric set of $\mathcal{J}$. □

Theorem 3.10. *Let $\mathcal{I}$ be an ideal of $K[u,y]$ with u a parametric set. Let w be a new variable, $M_1,\dots,M_p$ integers satisfying the Ritt's theorem, and $Q = \sum_{i=1}^{p} M_i y_i$. Let $\mathcal{J} = (\mathcal{I}, w - Q)$. Then $\sqrt{\mathcal{J}}$ has a characteristic set of the form*

$R(u,w), R_1(u,w,y_1),\dots,R_p(u,w,y_p)$ with respect to the order $u_1 < \cdots < u_q < w < y_1 < \cdots < y_p$ such that $\deg(R_j,y_j) = 1$ *for* $j = 1,\dots,p$.

Proof. See [8, page 7]. □

Corollary 3.11. *Let $\mathcal{I}$ be an ideal of $K[u,y]$ with u a parametric set. Let $w,\lambda_1,\dots,\lambda_p$ be indeterminates and $Q = \sum_{i=1}^{p}\lambda_i y_i$. Then $\mathcal{J} = (\mathcal{I}, w - Q)$ has u as parametric set and $\sqrt{\mathcal{J}}$ has a characteristic set of the form $R(\lambda,u,w)$, $R_1(\lambda,u,w,y_1),\dots,R_p(\lambda,u,w,y_p)$ with respect to the order $\lambda_1 \prec \cdots \prec \lambda_p \prec u_1 < \cdots < u_q < w < y_1 < \cdots < y_p$ such that* $\deg(R_j,y_j) = 1$ *for* $j = 1,\dots,p$.

Proof. For showing that u is a parametric set of $\mathcal{J}$, we use the same proof as the one given for Lemma 3.9.

It is clear that $\lambda_1,\dots,\lambda_p$ satisfy the Ritt's theorem for the ideal $\mathcal{I}$, then by Theorem 3.10 the R_i's are linear in their leading variables. □

Definition 3.12. The polynomial R defined in Theorem 3.10 is said to be a resolvent of $\mathcal{I}$ with respect to the parametric set u.

4. Computation of the resolvent

4.1. Computation of a basis of the radical of an ideal

Lemma 4.1. *Let $\mathcal{A}$ be an autoreduced set in $K[x]$ and z a new indeterminate. Then $(\mathcal{A}) : H_{\mathcal{A}}^{\infty} = (\mathcal{A}, zH_{\mathcal{A}} - 1) \cap K[x]$.*

Proof. For the direct inclusion, let $f \in (\mathcal{A}) : H_{\mathcal{A}}^{\infty}$, then there exists $\alpha \in \mathbb{N}$ such that $H_{\mathcal{A}}^{\alpha} f \in (\mathcal{A})$, hence $(zH_{\mathcal{A}})^{\alpha} f \in (\mathcal{A})$ in $K[x,z]$ since $f = f + f(zH_{\mathcal{A}})^{\alpha} - f(zH_{\mathcal{A}})^{\alpha}$, therefore $f \in (\mathcal{A}, zH_{\mathcal{A}} - 1) \cap K[x]$. For the other inclusion, we take $f \in (\mathcal{A}, zH_{\mathcal{A}} - 1) \cap K[x]$, then f will be a linear combination of elements in $\mathcal{A}$ and the polynomial $zH_{\mathcal{A}} - 1$ with coefficients in $K[x,z]$ since f is independent of z, so if we replace z by $1/H_{\mathcal{A}}$, we will obtain that $f \in (\mathcal{A}) : H_{\mathcal{A}}^{\infty}$. □

Remark 4.2. By Lemma 4.1, one can compute a basis of the ideal $(\mathcal{A}) : H_{\mathcal{A}}^{\infty}$ using Gröbner basis.

Lemma 4.3. *Let $\mathcal{I}$ be an ideal in $K[x]$. Then there is an effective method to compute a basis of $\sqrt{\mathcal{I}}$.*

Proof. We decompose $\sqrt{\mathcal{I}}$ into regular ideals as $\sqrt{\mathcal{I}} = \bigcap_{i=1}^{s}((\mathcal{A}_i) : H_{\mathcal{A}_i}^{\infty})$ (see Remark 2.5). By Lemma 4.1, we can determine a basis of each $(\mathcal{A}_i) : H_{\mathcal{A}_i}^{\infty}$. So, by the use of Gröbner-basis computation, we deduce a basis of $\sqrt{\mathcal{I}}$. □

4.2. Computation of the resolvent of a regular ideal. In [6], Cluzeau and Hubert have given an algorithm to compute a resolvent of a regular differential ideal in ordinary differential case. In this subsection, we give a deterministic method to compute a resolvent of a regular ideal using zero-dimensional Gröbner-basis computation.

Lemma 4.4. *Let $\mathscr{A}$ be an autoreduced set in $K[x]$, u the parametric set of $\mathscr{A}$, ω a new variable, $M_1,\dots,M_p$ integers satisfying Ritt's theorem, and $Q = \sum_{i=1}^{p}$. Then the ideal $(\mathscr{A}, \omega - Q) : H_{\mathscr{A}}^{\infty}$ is a characterizable ideal with respect to $u \prec \omega \prec y$.*

Proof. See [6]. □

Lemma 4.5. *Let $\mathscr{A}$ be an autoreduced set with u the parametric set and y the other variables. Then $\mathscr{A}$ is a characteristic set in $K[u,y]$ if and only if $\mathscr{A}$ is a characteristic set in $K(u)[y]$.*

Proof. See [10]. □

Theorem 4.6. *Let $\mathscr{A}$ be an autoreduced set in $K[u,y]$ with u the parametric set. Then there is an algorithm to compute a resolvent of $(\mathscr{A}) : H_{\mathscr{A}}^{\infty}$.*

Proof. Let $\lambda_1,\dots,\lambda_p$ be new variables. The λ_i's satisfy the Ritt's theorem for $(\mathscr{A}) : H_{\mathscr{A}}^{\infty}$, then, by Lemma 4.4, $(\mathscr{A}, w - \sum_{i=1}^{p} \lambda_i y_i) : H_{\mathscr{A}}^{\infty}$ is characterizable with respect to $\lambda \prec u \prec w \prec y$ and has a characteristic set of the form $R, R_1, \dots, R_p$ such that $\deg(R_i, y_i) = 1$ (by Corollary 3.11). Let $D = II_1 \cdots I_p$ with $I, I_1, \dots, I_p$, respectively, the initials of $R, R_1, \dots, R_p$. Let $M_1, \dots, M_p$ be integers such that $D(M,u,w) \neq 0$. After substituting the M_i's in λ_i's, we obtain $R', R'_1, \dots, R'_p$ which will be a characteristic set of $((\mathscr{A}) : H_{\mathscr{A}}^{\infty}, \omega - \sum_{i=1}^{p} M_i y_i)$ verifying $\deg(R'_i, y_i) = 1$.

The polynomial R' is a resolvent of $(\mathscr{A}) : H_{\mathscr{A}}^{\infty}$ with respect to the parametric set u. □

Algorithm 4.7. Let $\mathscr{A}$ be an autoreduced set in $K[u,y]$, where u is the parametric set.

Step 1. Let $\lambda_1,\dots,\lambda_p$ and z be new variables. We compute $\mathscr{B}$, the Gröbner basis in $K(\lambda,u)[w,y,z]$, of the zero-dimensional ideal $(\mathscr{A}, zH_{\mathscr{A}} - 1, w - \sum_{i=1}^{p} \lambda_i y_i)$ with respect to a lexicographical order such that $w \prec y \prec z$.

Step 2. Let $\mathscr{C} := C, C_1, \dots, C_p$ be the extracted characteristic set from $\mathscr{B} \cap K(\lambda,u)[w,y]$.

Step 3. Let $\mathscr{T} := T, T_1, \dots, T_p$ be obtained from $\mathscr{C}$ by clearing out the denominators.

Step 4. Let $\mathscr{R} := R, R_1, \dots, R_p$ be obtained from $\mathscr{T}$ by replacing the λ_i's by M_i's such that $D(M,u,y) \neq 0$, where $D = II_1 \cdots I_p$ with $I, I_1, \dots, I_p$, respectively, the initials of $T, T_1, \dots, T_p$.

The polynomial R is a resolvent of $(\mathscr{A}) : H_{\mathscr{A}}^{\infty}$ with respect to the parametric set u.

Correctness 4.8. It is a consequence of Lemmas 4.4, 4.5 and Theorem 4.6.

4.3. Computation of the resolvent of an ideal

Algorithm 4.9. Let $\mathscr{I}$ be an ideal of $K[x]$.

Step 1 (the computation of a parametric set of $\mathcal{I}$). We decompose $\sqrt{\mathcal{I}}$ into regular ideals $\bigcap_{i=1}^{s}(\mathcal{A}_i):H_{\mathcal{A}_i}^{\infty}$. The parametric set of $\mathcal{A}_i$ such that $|\mathcal{A}_i|$ is minimal is a parametric set of $\mathcal{A}$.

Step 2. We compute a basis G of $\sqrt{\mathcal{I}}$.

Step 3. Let $\omega,\lambda_1,\dots,\lambda_p$ be new variables.

We compute the Gröbner basis $\mathcal{B}$ of the ideal $(\sqrt{\mathcal{I}},\omega-\sum_{i=1}^{p}\lambda_i y_i)=(G,\omega-\sum_{i=1}^{p}\lambda_i y_i)$ with respect to the lexicographical order term satisfying $\lambda \prec u \prec \omega \prec y$.

Let $\mathcal{C}$ be the extracted characteristic set from $\mathcal{B}$.

The autoreduced set $\mathcal{C}$ has the form $R,R_1,\dots,R_p$ such that $\deg(R_i,y_i)=1$.

Step 4. Let $D=II_1\cdots I_p$ with $I,I_1,\dots,I_p$, respectively, the initials of $R,R_1,\dots,R_p$.

Let $M_1,\dots,M_p$ be integers such that $D(M,u,w)\neq 0$.

Let $R',R'_1,\dots,R'_p$ be obtained from $R,R_1,\dots,R_p$ after substituting the M_i's in λ_i's.

The autoreduced set $R',R'_1,\dots,R'_p$ is a characteristic set of $(\sqrt{\mathcal{I}},\omega-\sum_{i=1}^{p}M_i y_i)$ verifying $\deg(R'_i,y_i)=1$.

The polynomial R' is a resolvent of $\mathcal{I}$ with respect to the parametric set u.

Correctness 4.10. It is a consequence of Proposition 2.12, Corollary 3.11, and Lemma 4.3.

5. Applications.

The resolvent has a wide range of applications, namely it transforms a set of polynomial equations to a single polynomial equation such that their varieties are birationally equivalent, it permits to compute a primitive element for a finitely generated algebraic extension over a field of characteristic zero, and obviously it has other areas of applications.

In this section, we show how the resolvent can be used to decompose a variety into irreducible varieties and how to test that a variety associated to a regular ideal is irreducible.

5.1. Decomposition of a variety into irreducible varieties.

Let $\mathcal{A}=A_1,\dots,A_p$ be an autoreduced set, $M_1,\dots,M_p$ integers satisfying Ritt's theorem for the regular ideal $(\mathcal{A}):H_{\mathcal{A}}^{\infty}$, and w a new indeterminate. Put $\mathcal{J}=(\mathcal{A},w-Q):H_{\mathcal{A}}^{\infty}$, where $Q=M_1y_1+\cdots+M_py_p$. We know that $\mathcal{J}$ is characterizable and has a characteristic set of the form $\mathcal{R}=R,R_1,\dots,R_p$, where each R_i is linear in y_i. We can assume R square free because $\mathcal{J}$ is radical.

Lemma 5.1. *With the same notations as above, the following properties hold:*

(1) $\mathcal{J}=(\mathcal{B}):H_{\mathcal{B}}^{\infty}$;

(2) $\mathcal{J}\cap K[u,y]=(\mathcal{A}):H_{\mathcal{A}}^{\infty}$.

Proof. (1) It is a corollary of Lemma 4.4.

(2) It is sufficient to prove the direct inclusion; for this, let f be in $\mathcal{J}\cap K[u,y]$, then there exists $g\in((\mathcal{A}):H_{\mathcal{A}}^{\infty})$ (considered in the ring $K[u,y,w]$) and there

exists $h \in (w - Q)$ such that $f^r = g + h$ for $r \in \mathbb{N}$. Let $\bar{g} = \operatorname{rem}(g; w - Q)$; we obtain $f^r = \bar{g} + \bar{h}$ for $\bar{h} \in (w - Q)$. Since f^r is free of w, then $f^r = \bar{g}$, hence $f^r \in (\mathcal{A}) : H_{\mathcal{A}}^{\infty}$, therefore $f \in (\mathcal{A}) : H_{\mathcal{A}}^{\infty}$ because $(\mathcal{A}) : H_{\mathcal{A}}^{\infty}$ is perfect by Lazard's lemma. □

Theorem 5.2. *With the same notations as in Lemma 5.1. Let $R = B_1 \cdots B_s$ be the factorization of R into irreducible polynomials in $K[u][\omega]$ and $\mathcal{B}_i = B_i, R_1, \ldots, R_p$ for $i = 1, \ldots, s$. Then, $(\mathcal{A}, \omega - Q) : H_{\mathcal{A}}^{\infty} = \bigcap_{i=1}^{s} (\mathcal{B}_i) : H_{\mathcal{B}_i}^{\infty}$ and each $(\mathcal{B}_i) : H_{\mathcal{B}_i}^{\infty}$ is a prime ideal with $\mathcal{B}_i$ a characteristic set.*

Proof. Since the M_i's satisfy The Ritt's theorem, then, by Lemma 4.4, $(\mathcal{A}, \omega - Q) : H_{\mathcal{A}}^{\infty}$ is a characterizable ideal with respect to $u \prec \omega \prec y$ and by Lazard's lemma the ideal $(\mathcal{A}, \omega - Q) : H_{\mathcal{A}}^{\infty}$ is radical and is equal to $(\mathcal{R}\mathcal{S}) : H_{\mathcal{R}\mathcal{S}}^{\infty}$ with $\mathcal{R}\mathcal{S} = R, R_1, \ldots, R_p$, then $(\mathcal{A}, \omega - Q) : H_{\mathcal{A}}^{\infty} = (\mathcal{R}\mathcal{S}) : H_{\mathcal{R}\mathcal{S}}^{\infty} = \sqrt{((\mathcal{R}\mathcal{S}) : H_{\mathcal{R}\mathcal{S}}^{\infty})} = \sqrt{(\mathcal{R}\mathcal{S})} : H_{\mathcal{R}\mathcal{S}} = \bigcap_{i=1}^{s} \sqrt{(B_i, R_1, \ldots, R_p)} : H_{\mathcal{R}\mathcal{S}}^{\infty}$ (by Proposition 2.3). To finish the proof, it is sufficient to show that $\sqrt{(B_i, R_1, \ldots, R_p)} : H_{\mathcal{R}\mathcal{S}} = \sqrt{(\mathcal{B}_i)} : H_{\mathcal{B}_i}$.

For this let $f \in \sqrt{(B_i, R_1, \ldots, R_p)} : H_{\mathcal{R}\mathcal{S}}$, then

$$f \cdot H_{\mathcal{R}\mathcal{S}} \in \sqrt{(B_i, R_1, \ldots, R_p)}. \tag{5.1}$$

We have $H_{\mathcal{R}\mathcal{S}} = h_R \cdot H_{\mathcal{R}\mathcal{S}'} = I \cdot S \cdot H_{\mathcal{R}\mathcal{S}'}$, where $\mathcal{R}\mathcal{S}' = R_1, \ldots, R_p$, $I = \operatorname{init}(R)$ and $S = \operatorname{sep}(R)$. We have $\operatorname{sep}(R) = \partial R / \partial \omega = \partial (B_1 \cdots B_s) / \partial \omega = \sum_{k=1}^{s} (S_k \cdot \prod_{j \neq k} B_j)$, where $S_k = \operatorname{sep}(B_k)$. Furthermore, $\operatorname{init}(R) = \prod_{k=1}^{s} I_k$, where $I_k = \operatorname{init}(B_k)$. Since all terms in $\sum_{k=1}^{s} (S_k \cdot \prod_{j \neq k} B_j)$, except $S_i \cdot \prod_{j \neq i} B_j$, are in $\sqrt{(B_i, R_1, \ldots, R_p)}$, then

$$\begin{aligned}
f \cdot H_{\mathcal{R}\mathcal{S}} \in \sqrt{(B_i, R_1, \ldots, R_p)} &\Longrightarrow f \cdot \operatorname{init}(R) \cdot S_i \cdot \prod_{j \neq i} B_j \cdot H_{\mathcal{R}\mathcal{S}'} \in \sqrt{(B_i, R_1, \ldots, R_p)} \\
&\Longrightarrow f \cdot \prod_{j \neq i} (I_j B_j) \in \sqrt{(B_i, R_1, \ldots, R_p)} : H_{\mathcal{B}_i} \\
&\qquad \left(\text{since } \operatorname{init}(R) = \prod_{k=1}^{s} I_k,\ H_{\mathcal{B}_i} = I_i S_i H_{\mathcal{R}\mathcal{S}'} \right) \\
&\Longrightarrow f \cdot \prod_{j \neq i} (I_j B_j) \in (B_i, R_1, \ldots, R_p) : H_{\mathcal{B}_i}^{\infty}
\end{aligned} \tag{5.2}$$

(the last implication follows by Proposition 2.3 and Lazard's lemma).

The autoreduced set $\mathcal{B}_i$ is irreducible, then it is a characteristic set of the prime ideal $(\mathcal{B}_i) : H_{\mathcal{B}_i}^{\infty}$. For $j \neq i$, $B_j \notin (\mathcal{B}_i) : H_{\mathcal{B}_i}^{\infty}$ because otherwise B_i will be equal to B_j. So $f \in (\mathcal{B}_i) : H_{\mathcal{B}_i}^{\infty}$. □

In the following, we will illustrate how one obtains the decomposition of $(\mathcal{A}) : H_{\mathcal{A}}^{\infty}$ into prime ideals from the decomposition of the characterizable ideal $\mathcal{J} = (\mathcal{A}, w - Q) : H_{\mathcal{A}}^{\infty}$. For $j = 1, \ldots, s$, let $\bar{\mathcal{D}}_j = D_1, \ldots, D_p$, $\bar{D}_j$ be a characteristic set of $(\mathcal{B}_j) : H_{\mathcal{B}_j}^{\infty}$ with respect to the order $u \prec y \prec w$.

Lemma 5.3. *With the same notations as above, the ideal $(\mathcal{B}_j):H^{\infty}_{\mathcal{B}_j}\cap K[u,y]$ has $\tilde{\mathcal{D}}_j = D_1,\dots,D_p$ as a characteristic set with respect to $u \prec y$ and it is equal to $(\tilde{\mathcal{D}}_j):H^{\infty}_{\tilde{\mathcal{D}}_j}$ for $j = 1,\dots,s$.*

Proof. We have that $\mathcal{B}_j$ is irreducible by Proposition 2.9, then $(\mathcal{B}_j):H^{\infty}_{\mathcal{B}_j}$ is a prime ideal and also $(\mathcal{B}_j):H^{\infty}_{\mathcal{B}_j}\cap K[u,y]$.

Let f be in $(\mathcal{B}_j):H^{\infty}_{\mathcal{B}_j}\cap K[u,y]$ and $\bar{f} = \operatorname{rem}(f;\tilde{\mathcal{D}}_j)$. Since f is in $K[u,y]$, then $\operatorname{rem}(f;\tilde{\mathcal{D}}_j) = \operatorname{rem}(f;\bar{\mathcal{D}}_j) = 0$ because $\bar{\mathcal{D}}_j$ is a characteristic set of $(\mathcal{B}_j):H^{\infty}_{\mathcal{B}_j}$. It follows that $(\mathcal{B}_j):H^{\infty}_{\mathcal{B}_j}\cap K[u,y] = (\tilde{\mathcal{D}}_j):H^{\infty}_{\tilde{\mathcal{D}}_j}$ because it is a prime ideal and $\tilde{\mathcal{D}}_j$ is its characteristic set. □

The following proposition is the aim result; it gives the decomposition of $(\mathcal{A}):H^{\infty}_{\mathcal{A}}$ into prime ideals that each one is given by its characteristic set $\tilde{\mathcal{D}}_j$.

Proposition 5.4. *With the same notations as above,*

$$(\mathcal{A}):H^{\infty}_{\mathcal{A}} = \bigcap_{j=1}^{s}(\tilde{\mathcal{D}}_j):H^{\infty}_{\tilde{\mathcal{D}}_j}. \tag{5.3}$$

Proof. This result is a corollary of Lemma 5.1 and Theorem 5.2. □

Remark 5.5. For the radical of an ideal $\mathcal{I} = (\Sigma)$, we firstly decompose $\sqrt{\mathcal{I}}$ into regular ideals (see [3, 4, 5, 9]), and afterwards, using the techniques above, decompose each regular ideal into prime ideals.

5.2. Test of the primality of a regular ideal

Proposition 5.6. *Let $\mathcal{I} = (\mathcal{A}):H^{\infty}_{\mathcal{A}}$ with $\mathcal{A}$ an autoreduced set having u as the parametric set and R a resolvent of $\mathcal{I}$ with respect to u. Then R is irreducible over $K(u)$ if and only if $\sqrt{\mathcal{I}}$ is a prime ideal.*

Proof. Let $M_1,\dots,M_p$ be integers satisfying the Ritt's theorem for the ideal $\mathcal{I}$ with respect to the parametric set u, then there exist $R_1,\dots,R_p$ linear in their leading variables such that $R,R_1,\dots,R_p$ is a characteristic set of $\sqrt{(\mathcal{I},w-Q)}$, where $Q = M_1y_1+\cdots+M_py_p$, hence, by Lemma 4.4, $\sqrt{(\mathcal{I},w-Q)} = (\mathcal{R}):H^{\infty}_{\mathcal{R}}$, where $\mathcal{R} = R,R_1,\dots,R_p$. This implies, by Proposition 2.9 and Lemma 5.1, that R is irreducible over $K(u)$ if and only if $\mathcal{I}$ is prime. □

6. Examples

Example 6.1. Let $\mathcal{I}$ be the ideal, in the ring $K[x,y,z]$, generated by the following polynomials:

$$\begin{aligned} f_1 &:= y^6-2x^5y^3+x^{10},\\ f_2 &:= x^2y^3z-x^7z-y^5+x^5y^2,\\ f_3 &:= y^4z-x^5yz-x^3y^3+x^8,\\ f_4 &:= x^4z^2-2x^2y^2z+y^4. \end{aligned} \tag{6.1}$$

Firstly, we compute the decomposition of $\sqrt{\mathcal{I}}$ into regular ideals; we obtain

$$\sqrt{\mathcal{I}} := \mathcal{I}_1 \cap \mathcal{I}_2, \quad \mathcal{I}_1 := (x^2z - y^2, y^3 - x^5) : (x,y)^\infty,\ \mathcal{I}_2 := (x,y). \tag{6.2}$$

We remark that x is a parametric set of $\mathcal{I}$.

We verify that $M_1 = 1$, $M_2 = 1$ are integers satisfying Ritt's theorem for the ideal $\mathcal{I}_1$ with respect to the parametric set x (that is two distinct zeros of $\mathcal{I}_1$, with the x taking the same value, give different values for $Q = M_1 y + M_2 z = y + z$), and so we obtain a characteristic set R, R_1, R_2 of $(\mathcal{I}_1, w - y - z)$, satisfying the definition of the resolvent, that is, $\deg(R_1, y) = \deg(R_2, z) = 1$, where $R := -3x^3w + w^3 - x^5 - x^4$, $R_1 := (-x + x^2)y + w^2 - x^2w - 2x^3$, and $R_2 := (-x + x^2)z + xw - w^2 + 2x^3$. Since R is irreducible, then $\sqrt{\mathcal{I}} := \mathcal{I}_1 \cap \mathcal{I}_2$ is the decomposition into prime ideals. The polynomial xR is a resolvent of $\mathcal{I}$ with respect to the parametric set x.

Example 6.2. Let $\mathcal{A} := A_1, A_2$ be an autoreduced set in $K[x,y,z]$ with $A_1 := y^2 - (1+x)y + x$ and $A_2 := z^2 - (3+x)z + 3x$.

The autoreduced set R, R_1, R_2 is a characteristic set of $((\mathcal{A}) : H_{\mathcal{A}}^\infty, w - y - z)$ with respect to $x \prec w \prec y \prec z$, where $R := 24x + w^4 + 5w^2x^2 - 4w^3x + 32x^2 - 2x^3w + 8x^3 - 8w^3 + 19w^2 - 54xw - 28x^2w - 12w + 28xw^2$, $R_1 := (-4 + 2x)y - 8x^2 + 15xw - 6w^2 - 14x + 9w + w^3 - 3xw^2 + 2x^2w$, $R_2 := (-4 + 2x)z + 3xw^2 - 2x^2w - w^3 + 6w^2 + 14x + 8x^2 - 17xw - 5w$, R is a resolvent of $(\mathcal{A}) : H_{\mathcal{A}}^\infty$ with respect to the parametric set x, and $R := (w-4)(w-2x)(w-x-3)(w-x-1)$ is the factorization of R over $K[u]$.

We put $B_1 := w - 4$, $B := w - 2x$, $B_3 := w - x - 3$, and $B_4 := w - x - 1$. Then $((\mathcal{A}) : H_{\mathcal{A}}^\infty, w - y - z) := \bigcap_{i=1}^4 \mathcal{B}_i$, where $\mathcal{B}_i := ((B_i, R_1, R_2) : H^\infty)$ and $H := \operatorname{init}(R_1)\operatorname{init}(R_2) := (4 - 2x)^2$.

Changing of the order on the variables, we obtain

$$(\mathcal{A}) : H_{\mathcal{A}}^\infty := (z-3, y-1) \cap (z-x, y-x) \cap (z-x, y-1) \cap (z-3, y-x). \tag{6.3}$$

7. Conclusion. We have developed an algorithm to compute a resolvent of an algebraic variety. No factorization is needed. Some of the main problems in polynomial ideal theory can be solved by means of the resolvent. We compute the irreducible varieties associated to a given affine variety, we test the primality of a regular ideal.

The algebraic complexity of the resolvent and the computational complexity of the associated algorithms have been explicitly explored by Gallo and Mishra [7].

The generalization of the resolvent and its complexity to differential equations is a future investigation.

References

[1] F. Aubry, *Ensembles triangulaires de polynomes et résolution de systèmes algèbriques. Implantation en Axiom*, Ph.D. thesis, Université Paris VI, Paris, 1999.

[2] T. Becker and V. Weispfenning, *Gröbner Bases. A Computational Approach to Commutative Algebra*, Graduate Texts in Mathematics, vol. 141, Springer-Verlag, New York, 1993.

[3] F. Boulier, D. Lazard, F. Ollivier, and M. Petitot, *Representation for the radical of a finitely generated differential ideal*, Proceedings of the International Symposium on Symbolic and Algebraic Computation (Montreal, Canada) (A. H. M. Levelt, ed.), ACM Press, New York, 1995.

[4] ______, *Computing representations for radicals of finitely generated differential ideal*, Tech. Report IT-306, LIFL, Villeneuve d'Ascq, 1997.

[5] D. Bouziane, A. Kandri Rody, and H. Maârouf, *Unmixed-dimensional decomposition of a finitely generated perfect differential ideal*, J. Symbolic Comput. **31** (2001), no. 6, 631–649.

[6] T. Cluzeau and E. Hubert, *Resolvent representation for regular differential ideals*, Appl. Algebra Engrg. Comm. Comput. **13** (2003), no. 5, 395–425.

[7] G. Gallo and B. Mishra, *The complexity of resolvent resolved*, Proceedings of the 5th Annual ACM-SIAM Symposium on Discrete Algorithms (Arlington, Va), ACM Press, New York, 1994, pp. 280–289.

[8] X. Gao and S.-C. Chou, *On the theory of resolvents and its applications*, Systems Sci. Math. Sci. **12** (1999), 17–30.

[9] E. Hubert, *Quelques algorithmes pour l'Étude des Solutions des Équations Différentielles Algèbriques*, Ph.D. thesis, Institut National Polytechnique de Grenoble, Grenoble, 1997.

[10] ______, *Factorization-free decomposition algorithms in differential algebra*, J. Symbolic Comput. **29** (2000), no. 4-5, 641–662.

[11] A. Kandri Rody, *Effective methods in the theory of polynomial ideals*, Ph.D. thesis, Rensselaer Polytechnic Institute, New York, 1984.

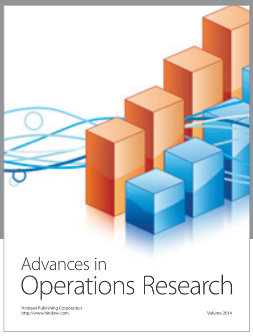
[12] A. Kandri Rody and B. D. Saunders, *Primality of ideals in polynomial rings*, Proceedings of the 3rd MACSYMA Users Conference, General Electric Schenectady, New York, 1984, pp. 459–471.

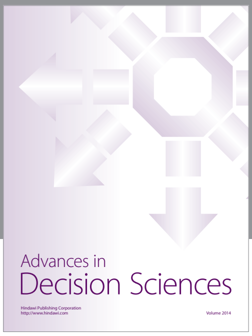
[13] E. R. Kolchin, *Differential Algebra and Algebraic Groups*, Pure Appl. Math, vol. 54, Academic Press, New York, 1973.

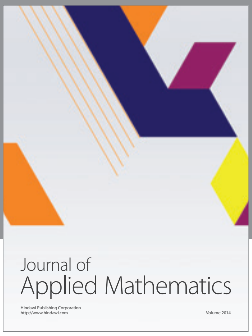
[14] J. F. Ritt, *Differential Algebra*, Dover Publications, New York, 1966.

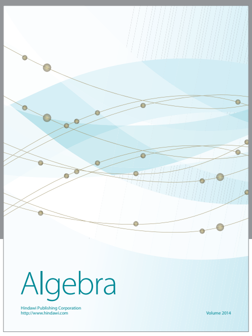
Driss Bouziane: Département de Mathématiques, Faculté des Sciences Semlalia, Université Cadi Ayyad, BP 2390, Marrakech, Morocco
E-mail address: mbouziane@ucam.ac.ma

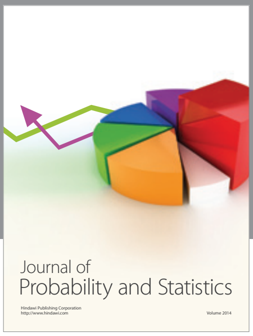
Abdelilah Kandri Rody: Département de Mathématiques, Faculté des Sciences Semlalia, Université Cadi Ayyad, BP 2390, Marrakech, Morocco
E-mail address: kandri@ucam.ac.ma


Advances in
Operations Research

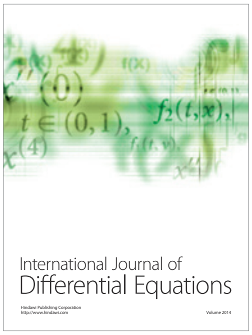

Advances in
Decision Sciences

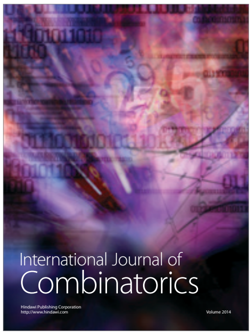

Journal of
Applied Mathematics

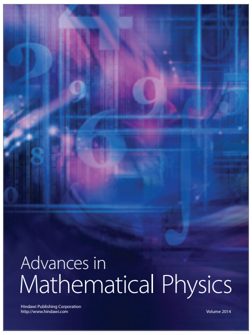

Algebra

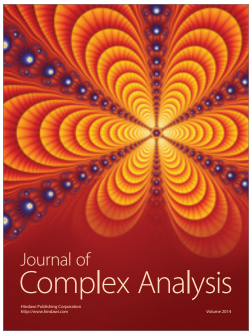

Journal of
Probability and Statistics

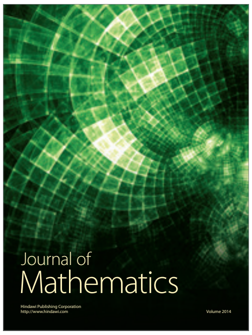
The Scientific
World Journal

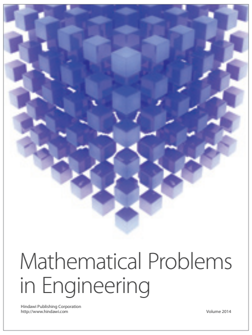

International Journal of
Differential Equations

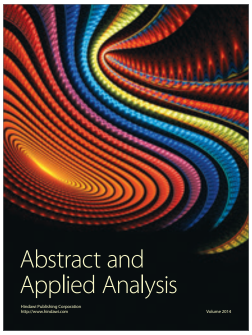

International Journal of
Combinatorics

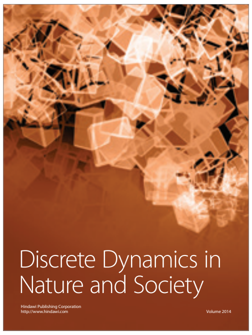

Advances in
Mathematical Physics

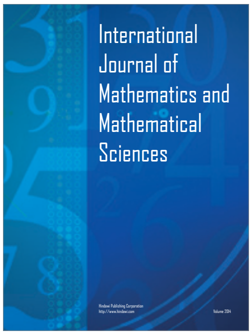

Journal of
Complex Analysis


Journal of
Mathematics


Mathematical Problems
in Engineering

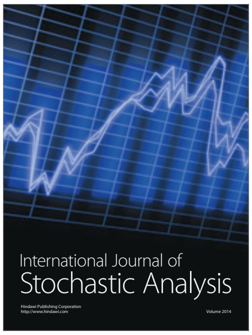

Abstract and
Applied Analysis


Discrete Dynamics in
Nature and Society


International
Journal of
Mathematics and
Mathematical
Sciences

Journal of
Discrete Mathematics

Journal of
Function Spaces


International Journal of
Stochastic Analysis

Journal of
Optimization