Birational properties of the gap subresultant varieties

M’hammed El Kahoui

Department of Mathematics, Faculty of Sciences Semlalia, Cadi Ayyad University, P.O. Box 2390, Marrakech, Morocco

Received 30 March 2003; accepted 10 September 2004

Abstract

In this paper we address the problem of understanding the gaps that may occur in the subresultant sequence of two polynomials. We define the gap subresultant varieties and prove that they are rational and have the expected dimension. We also give explicitly their corresponding prime ideals.

© 2004 Elsevier Ltd. All rights reserved.
MSC: 12Y05; 68W30; 13P10
Keywords: Subresultant sequence; Local coordinate system; Gap subresultant varieties

1. Introduction

Subresultants theory, which dates back to the 19th century (see e.g. Sylvester (1853)), is nowadays one of the main tools of elimination in polynomial rings. The most known applications of such tools are gcd computation for parameter dependent univariate polynomials, the real root counting problem (see e.g. Collins (1967), Brown and Traub (1971), González-Vega et al. (1989, 1999)) and quantifier elimination over real closed fields (see e.g. González-Vega (1998)). There are also many other applications of subresultants, such as the detection of “symmetries” in the complex roots of real coefficients univariate polynomials (Guckenheimer et al., 1997; El Kahoui and Weber, 2000). Recently, a connection between subresultants and locally nilpotent derivations

E-mail address: elkahoui@ucam.ac.ma.
is established in El Kahoui (2004). This gives new formulas for the expression of subresultants, and hopefully could help in understanding algebraic actions on affine spaces.

There are actually two main approaches to study subresultants. The first one exploits the connection established in Collins (1967) between subresultant sequences and Euclidean remainder sequences (see also Loos (1982)). A typical instance of this way of reasoning is given in Hong (1997) where the behavior of subresultants under composition is studied. The second approach, systematically studied in Hong (1999) and Diaz-Toca and González-Vega (in press), is based on an explicit expression of subresultants in terms of the roots of the input polynomials, which generalizes the well-known formula of the resultant. One feature of this approach is the possibility of geometric reasoning it offers. Notice also that an elementary approach to subresultants is given in El Kahoui (2003). By elementary it is meant that the main properties of subresultants are deduced from algebraic identities that the coefficients of the subresultants fulfill.

One of the main results of subresultants theory is the so-called gap structure theorem established in Lickteig and Roy (1996) (see also Lickteig and Roy (2001), Lombardi et al. (2000), El Kahoui (2003)), which is a refinement of Habicht theorem (Habicht, 1948). It gives a precise understanding of the structure of the subresultant sequence in the singular cases where a polynomial, or even several ones in this sequence drop down in degree. Such a result lies at the tip of the most efficient algorithms for computing the subresultant sequence of two polynomials (Lombardi et al., 2000; Ducos, 2000; Lickteig and Roy, 2001).

In this paper we address the problem of understanding the gaps that may occur in the subresultant sequence of two polynomials. It seems that the geometric aspect of this problem has been poorly studied before. In this work we investigate its birational aspect. More precisely, we study some birational properties of the algebraic sets consisting of polynomials of given degree and whose subresultant sequence has prescribed gaps. The paper is structured as follows: In Section 2 we give a review of subresultants and their properties that will be needed for our purpose. In Section 3 we study a special class of local coordinate systems in polynomial rings. This will be the basic tool we use to study the eventual gaps in subresultant sequences. Section 4 is devoted to a birational study of the gap subresultant varieties. Our main result in this paper is that such varieties are rational and have the expected dimension.

2. Review of subresultants

In this section we recall how subresultants are defined and give some of their properties that will be needed for our purpose. For more details on subresultants theory we refer to González-Vega et al. (1990), Hong (1999), Collins (1967), Lombardi et al. (2000), Loos (1982), Brown and Traub (1971), Lickteig and Roy (2001), Habicht (1948), El Kahoui (2003), Cheng (2001), Ho and Yap (1996), Gathen and Luking (2000), Hong (1997), Chardin (1991), but the list is nowhere near exhaustive.

Throughout this paper all considered rings are commutative with unit. Given two positive integers \( m \) and \( n \) we denote by \( \mathcal{M}_{m,n}(\mathcal{A}) \) the \( \mathcal{A} \)-module of \( m \times n \) matrices with coefficients in \( \mathcal{A} \). Consider the free \( \mathcal{A} \)-module \( \mathcal{P}_n \) of polynomials with coefficients in \( \mathcal{A} \).
of degree at most \( n - 1 \) equipped with the basis \( \mathcal{B}_n = [y^{n-1}, \ldots, y, 1] \). A sequence of polynomials \( \{P_1, \ldots, P_m\} \) in \( \mathcal{P}_n \) will be identified to the \( m \times n \) matrix whose row’s coefficients are the coordinates of the \( P_i \)'s in the basis \( \mathcal{B}_n \). Given positive integers \( p, q \) we let \( \delta(p, q) = q - 1 \) if \( p = q \), and \( \delta(p, q) = \min(p, q) \) if \( p \neq q \).

The following definition, introduced in González-Vega et al. (1989), is a slight modification of the usual one. It allows to get some control on the formal degrees of the polynomials in the subresultant sequence.

**Definition 2.1.** Let \( \mathcal{A} \) be a ring and \( p, q \) be positive integers. Let \( P, Q \in \mathcal{A}[y] \) be two polynomials with \( \deg(P) \leq p \) and \( \deg(Q) \leq q \) respectively. For any \( i \leq \delta(p, q) \) we define the \( i \)-th subresultant polynomial associated to \( (P, p) \) and \( (Q, q) \) as follows:

\[
Sr_i(P, p, Q, q) = \sum_{j=0}^{i} sr_{i, j}(P, p, Q, q)y^j,
\]

where \( sr_{i, j}(P, p, Q, q) \) is the determinant of the matrix built with the columns 1, 2, \ldots, \( p + q - 2i - 1 \) and \( p + q - i - j \) in the matrix

\[
\text{Sylv}_i(P, p, Q, q) = [y^{q-i-1}P, \ldots, P, y^{p-i-1}Q, \ldots, Q].
\]

The determinant \( sr_{i, i}(P, p, Q, q) \) is called the \( i \)-th principal subresultant coefficient of \( P \) and \( Q \) and is denoted by \( sr_i(P, p, Q, q) \).

When \( \deg(P) = p \) and \( \deg(Q) = q \) we write \( Sr_i(P, Q) \) and \( sr_{i, j}(P, Q) \) for short instead of \( Sr_i(P, p, Q, q) \) and \( sr_{i, j}(P, p, Q, q) \). If no risk of confusion arises, we also use the abbreviations \( Sr_i \) and \( sr_{i, j} \).

In the sequel we give some fundamental properties of subresultants. The first one answers the well known problem of finding algebraic conditions on the coefficients of \( P \) and \( Q \) in order that they have a \ gcd of given degree.

**Theorem 2.1.** Let \( \mathcal{A} \) be a domain and \( P, Q \in \mathcal{A}[y] \) be two polynomials with \( \deg(P) = p \) and \( \deg(Q) = q \). Then the \ gcd of \( P \) and \( Q \) over the fractions field \( K \) of \( \mathcal{A} \) is of degree \( k \) if and only if

\[
Sr_i = 0, \quad i = 0, 1, \ldots, k - 1,
\]

\[
Sr_k \neq 0.
\]

In this case, \( Sr_k \) is a \ gcd of \( P \) and \( Q \) in \( K[y] \).

Another fundamental property subresultants satisfy is the so-called specialization property. A complete study of this property can be found in González-Vega et al. (1990).

**Theorem 2.2.** Let \( \mathcal{A} \) and \( \mathcal{B} \) be two rings, \( \phi : \mathcal{A} \rightarrow \mathcal{B} \) be a ring homomorphism and \( P, Q \in \mathcal{A}[y] \) be two polynomials with \( \deg(P) \leq p \) and \( \deg(Q) \leq q \). Then the following hold:

(i) for any \( i = 0, \ldots, \delta(p, q) \)

\[
Sr_i(\phi(P), p, \phi(Q), q) = \phi(Sr_i(P, p, Q, q)).
\]
Theorem 2.3. Let \( A \) be a domain and \( p \ge q \) be positive integers and \( P, Q \) be two polynomials in \( A[y] \) such that \( \deg(P) = p \) and \( \deg(Q) = q \). Then for any \( j < i \le q - 1 \) we have:

\[
Sr_i(P, p, Q, q) = Sr_j(Sr_{i+1}, i + 1, Sr_i, i).
\]

In particular, if \( \deg(Sr_{i+1}) = i + 1 \) and \( \deg(Sr_i) = i \) then

\[
Sr_{i+1}^2Sr_{i-1} = \text{prem}(Sr_{i+1}, Sr_i),
\]

where \( \mu_i = (q - i)(p - p_1) \).

Now we turn to give some algebraic identities that the subresultants fulfill. Before doing this we need to fix some conventions. From now on we assume that \( p \ge q \), and in case \( p = q \) we let \( Sr_q(P, p, Q, q) = Q \). The following result is a slight modification of Habicht theorem (Habicht, 1948).

**Theorem 2.3.** Let \( A \) be a domain and \( p \ge q \) be positive integers and \( P, Q \) be two polynomials in \( A[y] \) such that \( \deg(P) = p \) and \( \deg(Q) = q \). Then for any \( j < i \le q - 1 \) we have:

\[
Sr_i(P, p, Q, q) = a_p^{q - q_1}Sr_i(P, p, Q_1),
\]

where \( \mu_i = (q - i)(p - p_1) \).

3. Local coordinate systems

Let \( A \) be a domain and \( A[x_1, \ldots, x_n] = A[x] \) be the ring of polynomials in the indeterminates \( x_1, \ldots, x_n \) with coefficients in \( A \). The most commonly used idea to investigate the properties of an ideal \( \mathcal{I} \) of \( A[x] \) is to find a suitable generating system from which one can easily read the properties of \( \mathcal{I} \). Gröbner bases theory gives a systematic and algorithmic way for this. An alternative, but less systematic, way to study ideals of \( A[x] \) is to operate changes on the coordinate system \( x \) in such a way to make easier the reading of the properties of an ideal from its given generating system. In this section we will proceed according to this last point of view.

If \( s_1, \ldots, s_t \) are nonzero elements in \( A \) we let \( \{s_1, \ldots, s_t\} \) be the multiplicative subset of \( A \) generated by the \( s_i \)'s. Given a multiplicative subset \( S \) of \( A \), we denote by \( A_S \) the localization ring of \( A \) at \( S \). When \( S \) is finitely generated, say \( S = \{s_1, \ldots, s_t\} \), the localization ring \( A_S \) can canonically be identified to \( A[z]/\mathcal{I}(s_1 \ldots s_t z - 1) \).

We will need the following classical fact of commutative algebra.

**Lemma 3.1.** Let \( A \) be a domain, \( \mathcal{I} \) be an ideal of \( A \) and \( \pi : A \rightarrow A/\mathcal{I} \) be the canonical projection. Let \( S \) be a multiplicative subset of \( A \) such that \( \mathcal{I} \cap S = \emptyset \). Then \( \pi(S) \) is a multiplicative subset of \( A/\mathcal{I} \), and \( A_S/\mathcal{I}_S \) and \( (A/\mathcal{I})_{\pi(S)} \) are isomorphic.
In the sequel we will make use of the above lemma without explicit reference. We will also write by abuse of notation \( (A/I) \cap S \) instead of \( (A/I)_{\cap S} \).

Let \( f = f_1, \ldots, f_n \) be a list of polynomials in \( A[x] \) and \( T \) be a subset of \( \{1, \ldots, n\} \). We let \( J_{f,T} \) be the ideal of \( A[x] \) generated by \( \{f_i : i \in T\} \).

If \( V \) is a subset of \( \{1, \ldots, n\} \) and \( S \) is the multiplicative subset of \( A[x] \) generated by \( \{f_i : i \in V\} \) then the localization ring \( A[f]_S \) is well defined and is a subring of \( A[x]_S \).

**Definition 3.1.** Let \( A \) be a domain and \( S \) be a multiplicative subset of \( A[x] \). A list \( f_1, \ldots, f_n \) of polynomials in \( A[x] \) will be called an \( S \)-local coordinate system if the following conditions hold:

(i) there exists a subset \( V \) of \( \{1, \ldots, n\} \) such that \( S = \{f_i : i \in V\} \),
(ii) \( A[f]_S = A[x]_S \).

Notice that the condition (ii) in the definition is equivalent to \( A[x] \subseteq A[f]_S \). It is also straightforward to see that any \( S \)-local coordinate system is algebraically independent over the ground ring \( A \). The following theorem gathers some important geometric properties of local coordinates systems.

**Theorem 3.1.** Let \( A \) be a domain, \( f = f_1, \ldots, f_n \) be an \( S \)-local coordinate system in \( A[x] \) with \( S = \langle f_{r+1}, \ldots, f_n \rangle \), and let \( s = f_{r+1} \cdots f_n \). If \( S_0 = \langle x_{r+1}, \ldots, x_n \rangle \) then the \( A \)-algebra endomorphism \( \phi(x_i) = f_i \) induces an \( A \)-isomorphism from \( A[x]_{S_0} \) onto \( A[x]_S \). As by product, for any algebraically closed field \( F \) containing \( A \), any subset \( T \) of \( \{1, \ldots, r\} \) the following hold:

(i) the ideal \( J_{f,T} : s^\infty \) is prime of dimension \( n - |T| \) in \( F[x] \),
(ii) the variety \( V_{f,T} \) defined over \( F \) by the ideal \( I(f_i : i \in T) : s^\infty \) is rational,
(iii) any point \( \alpha \) of \( V_{f,T} \) satisfying the condition \( s(\alpha) \neq 0 \) is nonsingular.

**Proof.** Since the \( f_i \)'s are algebraically independent over \( A \) the map \( \phi \) is injective, and so it induces an injective \( A \)-homomorphism from \( A[x]_{S_0} \) into \( A[x]_S \). For the sake of simplicity we also denote it \( \phi \). Clearly, \( \phi \) maps \( A[x]_{S_0} \) onto \( A[f]_S \), and so it is surjective according to the fact that \( A[f]_S = A[x]_S \).

Let \( T \subseteq \{1, \ldots, r\} \). The \( A \)-isomorphism \( \phi \) maps \( J_{f,T} A[x]_{S_0} \) onto \( J_{f,T} A[x]_S \), and this induces an \( A \)-isomorphism

\[
\overline{\phi} : A[x]_{S_0}/J_{f,T} A[x]_{S_0} \longrightarrow A[x]_S/J_{f,T} A[x]_S .
\]

Clearly, \( A[x]_{S_0}/J_{f,T} A[x]_{S_0} \) is canonically \( A \)-isomorphic to \( A[x_i : i \notin T]_{S_0} \). On the other hand, it is easy to see that \( J_{f,T} A[x]_S \cap A[x] = J_{f,T} : s^\infty \), and so the ideal \( J_{f,T} : s^\infty \) is prime. Moreover, by Lemma 3.1 the algebra \( (A[x]/J_{f,T} : s^\infty)_S \) is \( A \)-isomorphic to \( A[x]_S/J_{f,T} A[x]_S \). This proves that \( (A[x]/J_{f,T} : s^\infty)_S \) is \( A \)-isomorphic to \( A[x_i : i \notin T]_{S_0} \).

If we replace \( A \) by the algebraically closed field \( F \) we obtain the same isomorphism. In particular, the quotient field of \( F[x]/J_{f,T} : s^\infty \) is \( A \)-isomorphic to \( F(x_i : i \notin T) \). As by product, \( J_{f,T} : s^\infty \) is of dimension \( n - |T| \) according to the fact that in the case of affine rings dimension equals transcendence degree.
Since the algebraic variety underlying the affine ring $\mathcal{F}[x_i \mid i \notin \mathcal{T}]_{S_0}$ satisfies the properties (ii) and (iii) these same properties hold for $V_{f,T}^{\mathcal{F}}$. □

In all the rest of this paper we let $P$ and $Q$ be two polynomials with indeterminate coefficients over a domain $A$, we assume that $\deg(p) = p \geq \deg(Q) = q \geq 1$ and write

\[ P = a_p y_p + a_{p-1} y_{p-1} + \cdots + a_0, \]
\[ Q = b_q y_q + b_{q-1} y_{q-1} + \cdots + b_0. \]

The ring generated by the coefficients of $P$ and $Q$ is denoted by $A[a,b]$. We let $s_j = s_{j_1} \cdots s_{j_q}$ and $S_j$ be the multiplicative subset $(s_{j_1}, \ldots, s_{j_q})$ of $A[a,b]$.

**Theorem 3.2.** Let $A$ be a domain and $p \geq q$ be positive integers. Let $P$, $Q$ be two polynomials with indeterminate coefficients over $A$ such that $\deg(P) = p$ and $\deg(Q) = q$. We let

\[ L_{q-1} = s_{q-1}, \ldots, s_{q-1,0}, b_{q}, \ldots, b_{0}, a_{p}, \ldots, a_{q}, \]
\[ L_j = s_{j_1} \cdots s_{j_q}, s_{j+1,0}, \ldots, s_{j+1,0,0}, s_{j+2,0,1}, \ldots, s_{j+2,0,1,0}, s_{j+2,0,1,0,0}, \ldots, s_{q}, s_{q-1}, \]
\[ a_{p}, \ldots, a_{q}, \]

for $j \leq q - 2$. Then, for any $j \leq q - 1$ the list of polynomials $L_j$ is an $S_{j+1}$-local coordinate system of $A[a,b]$.

**Proof.** Without loss of generality we may restrict to the case $A = \mathbb{Z}$. To prove the claimed result we use induction on $j$ starting from $q - 1$. Using pseudo-division we may write

\[ (-b_q)^{p-q+1} P = Q_{q-1} Q + S_{q-1} \]

where $Q_{q-1}$ is of degree $p - q$ and its coefficients are polynomials in terms of $a_p, \ldots, a_q$ and the coefficients of $Q$. This proves in particular that for any $k \leq q - 1$ the monomial $b_q^{p-q+1} a_k$ is polynomial in terms of $a_p, \ldots, a_q$, the coefficients of $Q$ and those of $S_{q-1}$.

Thus $b_q^{p-q+1} a_k \in \mathbb{Z}[L_{q-1}]$ and so $a_k \in \mathbb{Z}[L_{q-1}]_{S_{q-1}} = \mathbb{Z}[L_{q-1}]_{S_{q-1}}$, according to the fact that $s_{q-1} = b_q^{p-q}$. This proves that $\mathbb{Z}[a,b] \subseteq \mathbb{Z}[L_{q-1}]_{S_{q-1}}$ and establishes the result for $j = q - 1$.

Assume by induction that $\mathbb{Z}[a,b] \subseteq \mathbb{Z}[L_{j+1}]_{S_{j+2}}$ and let us prove that $\mathbb{Z}[a,b] \subseteq \mathbb{Z}[L_{j}]_{S_{j+2}}$. By Habicht theorem we have

\[ s_{j+2}^2 S_j = S_j (S_{j+2}, S_{j+1}) = \text{rem}(S_{j+2}, S_{j+1}). \]

Writing down this last equation we get

\[ s_{j+1}^2 S_{j+2} = (s_{j+1} S_{j+2} + (s_{j+1} S_{j+2} + 1 - s_{j+2} S_{j+1,j})) S_{j+1} + s_{j+2}^2 S_j. \]

This proves that for any $k \leq j$ the quantity $s_{j+1}^2 s_{j+2}^2$ is polynomial in terms of $s_{j_1} \cdots s_{j_1,0}, s_{j+1,0}, \ldots, s_{j+1,0,0}, s_{j+2,0,1}, \ldots, s_{j+2,0,1,0}, s_{j+2,0,1,0,0}, \ldots, s_{q}, s_{q-1}, s_{q-1,0}, b_{q}, \ldots, b_{0}, a_{p}, \ldots, a_{q}$. As by product, we get the inclusion $\mathbb{Z}[L_{j+1}] \subseteq \mathbb{Z}[L_{j}]_{S_{j+2}}$, and therefore $\mathbb{Z}[L_{j+1}]_{S_{j+2}} \subseteq (\mathbb{Z}[L_{j}]_{S_{j+1}})_{S_{j+2}} = \mathbb{Z}[L_{j}]_{S_{j+1}}$. By induction hypothesis we have $\mathbb{Z}[a,b] \subseteq \mathbb{Z}[L_{j+1}]_{S_{j+2}}$ and so $\mathbb{Z}[a,b] \subseteq \mathbb{Z}[L_{j}]_{S_{j+1}}$. □
4. The gap subresultant varieties

In this section we state the main result of this paper concerning some birational properties of the gap subresultant varieties.

Let \( q \) be a positive integer. A gap sequence between 0 and \( q \) is a sequence \( g = (j_1, i_1), \ldots, (j_r, i_r) \) such that \( q \geq j_1 > i_1 > j_2 > i_2 > \cdots > j_r > i_r \geq 0 \). The length of \( g \) is defined as \( l(g) = \sum (j_k - i_k) \), and its number of gaps is \( r(g) = r \). The support of the sequence \( g \) is \( \text{supp}(g) = \{ j : \exists k (1 \leq k \leq r, i_k \leq j \leq j_k - 1) \} \). We also define the separant of \( g \) as

\[
\text{sp}_g = p \prod_{k=j_1}^q \prod_{t=1}^{r-1} \text{sr}_{i_t-1} \cdots \text{sr}_{j_t+1}.
\]

Notice that in case \( p = q \) we have not defined the subresultant \( \text{Sr}_q \). In this case we replace \( \text{sr}_q \) by \( b_q \) in the definition of the separant.

**Definition 4.1.** Let \( p \geq q \) be positive integers and \( g \) be a gap sequence between 0 and \( q \). We define the \( g \)-gap subresultant ideal of \( p \) and \( q \), and denote it by \( \mathcal{I}_g(p, q) \), to be the ideal

\[
\mathcal{I}(\text{sr}_{j_1-1}, \ldots, \text{sr}_{j_1-i_1}, \text{sr}_{j_2-1}, \ldots, \text{sr}_{j_2-i_2}, \ldots, \text{sr}_{j_r-1}, \ldots, \text{sr}_{j_r-i_r}) : \text{sp}_g^\infty
\]

of \( \mathbb{Z}[a, b] \). Given any algebraically closed field \( F \), we let \( \mathcal{V}^F_g(p, q) \) be the algebraic set of \( F^{p+q+2} \) defined by \( \mathcal{I}_g(p, q) \). This algebraic set will be called the \( g \)-gap subresultant variety over \( F \) of \( p \) and \( q \).

There is an ambiguity in the definition of the algebraic set \( \mathcal{V}^F_g(p, q) \) that we should make clear. Given any algebraically closed field \( F \) we let \( \phi_F \) be the canonical homomorphism from \( \mathbb{Z} \) into \( F \). The algebraic set \( \mathcal{V}^F_g(p, q) \) is then defined by the ideal generated by \( \phi_F(\mathcal{I}_g(p, q)) \) in \( F[a, b] \).

Generically, the points of \( \mathcal{V}^F_g(p, q) \) represent the polynomials \( \gamma_1, \gamma_2 \in F[y] \), with \( \text{deg}(\gamma_1) = p \) and \( \text{deg}(\gamma_2) = q \), such that:

- for any \( k = 1, \ldots, r \) the subresultant polynomial \( \text{Sr}_{j_k-1} \) is of degree \( i_k - 1 \) (or \( \text{Sr}_{j_k-1} = 0 \) in case \( i_k = 0 \)),

- for any \( j \geq i_r \) with \( j \notin \text{supp}(g) \) the subresultant polynomial \( \text{Sr}_j \) has the expected degree, namely \( j \).

**Example 4.1.** Let \( g = (j, 0) \) with \( j \geq 1 \), and let \( F \) be an algebraically closed field. By Theorem 2.1 the points of \( \mathcal{V}^F_g(p, q) \) are generically the pairs of polynomials \( (\gamma_1, \gamma_2) \) of degree \( (p, q) \) having a gcd of degree \( j \). We may write these pairs in the form \( (\delta_1, \delta_2, \delta_3) \), with \( \text{deg}(\delta) = j, \text{deg}(\delta_1) = p - j, \text{deg}(\delta_2) = q - j \) and the leading coefficient of \( \delta \) is 1. We can therefore parameterize \( \mathcal{V}^F_g(p, q) \) in a rational way using \( p + q + 2 - j \) parameters, and this proves that it is rational of dimension \( p + q + 2 - j \).

We will see later that this way of reasoning can be extended to the other gap sequences, by fixing the degree of the gcd and those of the quotient. But it should be noticed here that we did not prove that the ideal \( \mathcal{I}_g(p, q) \) is prime.

We have now enough material to state the main result of this paper.
Theorem 4.1. Let \( A \) be a domain, \( p \geq q \) be positive integers and \( g \) be a gap sequence between 0 and \( q \). Then the \( A \)-algebra \( \left( A[a, b]/I_g(p, q) \right)_{sp_g} \) is \( A \)-isomorphic to an algebra of the type \( A[x]_\alpha \), where \( x \) is a list of \( p + q + 2 - l(g) \) indeterminates and \( z \in A[x] \) is the product of elements among the \( x_i \)'s. As by product, for any algebraically closed field \( F \) containing \( A \) the following hold:

(i) the ideal \( I_g(p, q) \) is prime of dimension \( p + q + 2 - l(g) \) in \( F[x] \).

(ii) the variety \( \gamma^F_g(p, q) \) is rational.

(iii) any point \( \alpha \) of \( \gamma^F_g(p, q) \) satisfying the condition \( sp_g(\alpha) \neq 0 \) is nonsingular.

Proof. To prove that \( \left( A[a, b]/I_g(p, q) \right)_{sp_g} \) is \( A \)-isomorphic to \( A[x]_\alpha \) we use induction on the number of gaps \( r \). Let \( g = (j, i) \) be a gap sequence with \( r(g) = 1 \), and notice that in this case \( sp_g = s_j \).

By Theorem 3.2 we can make a local change of coordinates so that \( A[a, b]_{s_j} = A[L_{j-1}]_{s_j} \). This proves that \( A[a, b]_{sp_g}/I_g(p, q)_{sp_g} = \left( A[a, b]/I_g(p, q) \right)_{sp_g} \) is the same as \( A[L_{j-1}]/I_g(p, q)_{sp_g} \). Taking into account the fact that

\[
L_{j-1} = sr_{j-1}, \ldots, sr_{j-1,0}, sr_j, \ldots, sr_{j,0}, (sr_k, sr_{k-1})_{k=j+1,a_p,\ldots,a_q}
\]

we deduce that \( A[L_{j-1}]/I_g(p, q)_{sp_g} \) is \( A \)-isomorphic to the algebra

\[
A[ sr_{j-1,i-1}, \ldots, sr_{j-1,0}, sr_j, \ldots, sr_{j,0}, sr_j, sr_{j+1,i}, \ldots, sr_q, sr_{q-1}, a_p, \ldots, a_q ]_{s_j}.
\]

This proves the claimed result for the case \( r(g) = 1 \). Assume now that the result holds for any domain \( A \) and any gap sequence \( g \) with \( r(g) = 1 \), and let us prove this for gap sequences \( g \) such that \( r(g) = r \).

Let \( g = (j_1, i_1), \ldots, (j_r, i_r) \) be such a sequence, and to simplify the rest of the proof we let \( g = (j_1, i_1), g' \) and \( sp_g = s_{j_1} s_{g'} \).

By Theorem 3.2 we can make a local change of coordinates in such a way that \( A[a, b]_{s_{j_1}} = A[L_{j_1-1}]_{s_{j_1}} \). This local change of coordinates is interesting in so far as it displays a subset of \( L_{j_1-1} \), namely \( sr_{j_1-1}, \ldots, sr_{j_1-1,i_1} \), which belongs to the ideal \( I_g(p, q) \), and so allows a first simplification of \( \left( A[a, b]/I_g(p, q) \right)_{sp_g} \). Indeed, by using basic properties of localization we can identify this last algebra to \( \left( (A[a, b]/I_g(p, q))_{s_{j_1}^{g'}} \right)_{s_{g'}} \). For a moment, let us forget about \( s_{g'} \) and focus on

\[
(A[a, b]/I_g(p, q))_{s_{j_1}^{g'}}.
\]

Clearly, this algebra is isomorphic to \( A[L']_{s_{j_1}/J'} \), with

\[
L' = sr_{j_1-1,i_1-1}, \ldots, sr_{j_1-1,0}, sr_{j_1,0}, sr_j, sr_{j,1-i_1-1}, \ldots, sr_{q, q-1}, a_q, \ldots, a_p,
\]

\[
J = (I(sr_{j_2-1}, \ldots, sr_{j_2-1,i_2}, \ldots, sr_{j_r-1,i_r}, \ldots, sr_{j_r-1,0}) : sp_{\infty}^g A[L']_{s_{j_1}}).
\]

Using once again basic properties of polynomial rings and localization we can write

\[
A[L']_{s_{j_1}} = \left( A[L']_{s_{j_1}} \right)_{s_{j_1}} = A[L'']_{s_{j_1}},
\]

with

\[
B = A[ sr_{j_1}, sr_{j_1,1}, \ldots, sr_{q, q-1}, a_q, \ldots, a_p ]_{s_{j_1+1}},
\]

\[
L'' = sr_{j_1-1,i_1-1}, \ldots, sr_{j_1-1,0}, sr_j, \ldots, sr_{j_1,0}.
\]
Notice that the polynomials $S_{r_j}$ and $S_{r_{j-1}}$ are of degrees respectively $j_1$ and $i_1 - 1$ in $B[L''[y]],$ and that $B[L'']$ is nothing but the ring generated over $B$ by the coefficients of $S_{r_j}$ and $S_{r_{j-1}}.$ Moreover, $L''$ is algebraically independent over $B$ according to Theorem 3.2.

On the other hand, by Habicht theorem we have for any $j < j_1 - 1,$

$$2(j_1 - j - 1)S_{r_j} = S_{r_j}(S_{r_{j_1}}, j_1, S_{r_{j-1}}, j_1 - 1).$$  

(1)

By Theorem 2.2, and taking into account the fact that $\deg(S_{r_j}) = j_1$ and $\deg(S_{r_{j-1}}) = i_1 - 1,$ this last equation writes as

$$2(j_1 - j - 1)S_{r_j} = s_{r_j}^{j_1 - i_1}S_{r_j}(S_{r_{j_1}}, S_{r_{j-1}}).$$  

(2)

To simplify the rest of the proof we write $S_{r_j}^*$ and $s_{r_j}^{*, k}$ for short instead of $S_{r_j}(S_{r_{j_1}}, S_{r_{j-1}})$ and $s_{r_j, k}(S_{r_{j_1}}, S_{r_{j-1}}).$ Since $s_{r_{j_1}}$ is a unit in $B[L'']_{S_{r_{j_1}}}$ we have by (2) the equality

$$J = I(s_{r_{j_1}}^*, \ldots, s_{r_{j_1-1}}^*, \ldots, s_{r_{j_1-1, i_1 - 1}}^*, \ldots, s_{r_{j_1-1}}, \ldots) : sp_{g'}^{* \infty} = I_{g'}(j_1, i_1 - 1)_{S_{r_{j_1}}}$$

where $sp_{g'}^*$ stands for the separant of $g'.$ By induction hypothesis we deduce that the algebra $(B[L'']/I_{g'}(j_1, i_1 - 1))_{sp_{g'}}$ is $B$-isomorphic to $B[x,]$ where $x$ is a list of $j_1 + (i_1 - 1) + 2 - l(g')$ indeterminates. On the other hand, by localizing at $s_{r_{j_1}}$ we deduce that

$$\left(\left(B[L'']/I_{g'}(j_1, i_1 - 1)\right)_{sp_{g'}}\right)_{s_{r_{j_1}}} = \left(B[L'']_{S_{r_{j_1}}}/J\right)_{sp_{g'}}$$

is $B$-isomorphic to $B[x,]$ with $z' \in B[x].$ Since the algebras $\left(B[L'']_{S_{r_{j_1}}}/J\right)_{sp_{g'}}$ and $\left(A[a, b]/I_{g'}(p, q)\right)_{sp_{g'}}$ are $A$-isomorphic we have the claimed result. $\square$

It is possible, but quite involved, to extract from the proof of Theorem 4.1 a parameterization of $V_{g'}^{F}(p, q).$ We will not give it here because there is another, and much simpler, way to get a parameterization of such variety. Indeed, the close relation between the subresultant sequence of two polynomials and their Euclidean remainder sequence implies that these two sequences have the same gaps. On the other hand, fixing a gap sequence in the Euclidean remainder sequence of two polynomials $P$ and $Q$ reduces to fix the degree of their gcd and those of their successive quotients.

Once these degrees are fixed, and by going back up the division process one easily recovers the coefficients of $P$ and $Q$ as rational functions in terms of the coefficients of the quotients together with those of the gcd. This of course gives a parameterization of $V_{g'}^{F}(p, q),$ but also proves the property (iii) of Theorem 4.1. However, the question of finding a system of algebraic equations defining $V_{g'}^{F}(p, q),$ and showing that $I_{g'}(p, q)$ is prime become more complicated if one uses Euclidean remainders instead of subresultants.

So the moral of the tale is that the use of Euclidean remainders is more suited for the manipulation of $V_{g'}^{F}(p, q)$ in parametric form, while the method presented in this paper is more appropriate for the manipulation of $V_{g'}^{F}(p, q)$ in implicit form.
5. Conclusion

There are many situations in which the subresultant sequence of two polynomials presents some gaps. For example, given an algebraically closed field \( K \) of characteristic zero and \( (\gamma_1, \gamma_2) \) an algebraic embedding of \( K \) in \( K^2 \), the subresultant sequence of \( \gamma_1 \) and \( \gamma_2 \) always presents a special sequence of gaps. This fact is due to the famous Abhyankar–Moh theorem (see Abhyankar and Moh (1975)) which states that either \( \deg(\gamma_1) \mid \deg(\gamma_2) \) or \( \deg(\gamma_2) \mid \deg(\gamma_1) \).

An interesting question is to study the algebraic set of embeddings of given degree (see e.g. Furter (1997)). Clearly, this algebraic set can be split into algebraic subsets, each one gathering the embeddings which present a fixed gap sequence in their subresultant sequence. The question that arises is whether such algebraic sets are irreducible, and if so whether they are rational. Such questions will be the subject of a future work.

The results of this paper also highlight another aspect of subresultants, namely that they give explicit examples of local coordinate systems. This could be used in the study of coordinates in polynomial rings, which is a central topic in the study of affine spaces, see e.g. Kraft (1994–1995).

Acknowledgments

I would like to thank the anonymous referees for their very constructive comments and their great help in improving the results and the quality of this paper.

References


