Available online at www.sciencedirect.com

SCIENCE DIRECT®

Journal of Symbolic Computation 39 (2005) 61–71

Journal of Symbolic Computation

www.elsevier.com/locate/jsc

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.

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.

0747-7171/$ - see front matter
doi:10.1016/j.jsc.2004.09.005

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 polynomials 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 $\mathcal{A}$