Dense Resultant of Composed Polynomials

Mixed - Mixed Case

Manfred Minimair

Department of Mathematics and Computer Science
Seton Hall University
400 South Orange Avenue
South Orange, NJ 07079, USA

Abstract

The main question of this paper is: *What is the dense (Macaulay) resultant of composed polynomials?* By a composed polynomial $f \circ (g_1, \ldots, g_n)$, we mean the polynomial obtained from a polynomial f in the variables $y_1, \ldots, y_n$ by replacing y_j by by some polynomial g_j. Cheng, McKay and Wang and Jouanolou have provided answers for two particular subcases. The main contribution of this paper is to complete these works by providing a uniform answer for all subcases. In short, it states that the dense resultant is the product of certain powers of the dense resultants of the component polynomials and of some of their leading forms. It is expected that these results can be applied to compute dense resultants of composed polynomials with improved efficiency. We also state a lemma of independent interest about the dense resultant under vanishing of leading forms.

Key words: Resultant, Composition, Factorization

1 Introduction

Resultants are of fundamental importance for solving systems of polynomial equations and therefore have been extensively studied (cf. Dixon [1908], Macaulay [1916], Cayley [1848], Canny et al. [1989], Chardin [1990], Gonzáles-Vega [1991], Manocha and Canny [1993], Nakos and Williams [1997], Lewis and Stiller [1999]). Recent research is focused on utilizing structure, naturally occurring in real life problems, of polynomials, for example, sparsity (cf. Pedersen

Email address: manfred@minimair.org (Manfred Minimair).
URL: http://minimair.org (Manfred Minimair).

Preprint submitted to Elsevier Science *16 May 2003*

and Sturmfels [1993], Gelfand et al. [1994], Emiris and Pan [1997], Cox et al. [1998], Cattani et al. [1998], Rojas [1999], Canny and Emiris [2000]) and composition (cf. Jouanolou [1991], Cheng et al. [1995], Kapur and Saxena [1996], Hong and Minimair [2002]).

We ask: *What is the dense (Macaulay) resultant of composed polynomials?* By a composed polynomial $f \circ (g_1, \ldots, g_n)$, we mean the polynomial obtained from a polynomial f in the variables $y_1, \ldots, y_n$ by replacing y_j by by some polynomial g_j. Cheng, McKay and Wang (cf. Cheng et al. [1995]) and Jouanolou (cf. Jouanolou [1991]) have provided answers for two particular subcases, namely, for n homogeneous polynomials composed with n homogeneous polynomials in n variables of same total degrees and for n inhomogeneous polynomials composed with $n-1$ inhomogeneous polynomials in $n-1$ variables of same total degrees. The main contribution of this paper is to complete these works by providing a uniform answer for all subcases, namely, for all cases of n homogeneous or n inhomogeneous polynomials composed with n or $n-1$ homogeneous or inhomogenenous polynomials in n or $n-1$ variables. In short, they state that the dense resultant is the product of certain powers of the dense resultants of the component polynomials and of some of their leading forms (cf. Theorem 1 and Remark 4). We also state a lemma (cf. Lemma 9) of independent interest about dense resultant under vanishing of leading forms.

Applying this result is expected to allow computations dramatically more efficient than computing without taking advantage of the composition structure. That is, in order to compute the dense resultant of composed polynomials we need only compute the dense resultants of the component polynomials and some of their leading forms. This is expected to be much more efficient than computing the dense resultant of expanded composed polynomials which are of higher degrees and much larger.

The reader might wonder whether one can use composition structures for other fundamental operations. In fact, this has already been done for some operations. For examples, Gröbner bases, subresultants, and Galois groups of certain differential operators have been studied in Hong [1997], Hong [1998] and Berman and Singer [1999], resp., using various mathematical techniques. However, it seems that those techniques cannot be applied to the study of dense resultants of polynomials composed with mixed polynomials. Therefore in this paper we use mathematical methods that are essentially different from those.

2 Main result

Before we state the main theorem we fix some notations. We let the symbol $\mathrm{Res}_{d_1,\ldots,d_n}(f_1,\ldots,f_n)$ stand for the dense (Macaulay) resultant of the homogeneous polynomials f_i of total degree d_i (cf. Cox et al. [1998]) with respect to the total degrees $d_1,\ldots,d_n$. That is, this symbol stands for the irreducible polynomial in the coefficients of the f_i's which vanishes iff the f_i's have a common non-trivial zero and which is normalized such that $\mathrm{Res}_{d_1,\ldots,d_n}(x_1^{d_1},\ldots,x_n^{d_n}) = 1$.

Now we are ready to state the main theorem.

Theorem 1 (Main theorem) *Let $f_1,\ldots,f_n$ be homogeneous polynomials in n variables of total degrees $d_1,\ldots,d_n$ and suppose that d_i is either positive or f_i is zero. Let $g_1,\ldots,g_n$ be polynomials (not necessarily homogeneous) in $n-1$ variables of total degrees $e_1,\ldots,e_n$ and suppose that either the maximum of the e_j's is positive or all the g_j's are zero. Further, let $\overline{e}$ and $\underline{e}$, resp., stand for the maximum and minimum, resp., of the e_j's. Then*

$$\mathrm{Res}_{d_1\overline{e},\ldots,d_n\overline{e}}\left(f_1\circ(g_1,\ldots,g_n),\ldots,f_n\circ(g_1,\ldots,g_n)\right) = \mathrm{Res}_{d_1,\ldots,d_n}\left(f_1,\ldots,f_n\right)^{\overline{e}^{n-1}} \ \mathrm{Res}_{\overline{e},\ldots,\overline{e}}\left(g_1,\ldots,g_n\right)^{d_1\cdots d_n}$$

and the second factor can be factorized further, that is,

$$\begin{aligned}\mathrm{Res}_{\overline{e},\ldots,\overline{e}}\left(g_1,\ldots,g_n\right)^{d_1\cdots d_n} = \\ &\mathrm{Res}_{\overline{e},\ldots,\overline{e},\underline{e},\overline{e},\ldots,\overline{e}}\left(g_1,\ldots,g_{k-1},g_k,g_{k+1},\ldots,g_n\right)^{d_1\cdots d_n} \\ &\mathrm{Res}_{\overline{e},\ldots,\overline{e}}\left({g_1}^{[\overline{e}]},\ldots,{g_{k-1}}^{[\overline{e}]},{g_{k+1}}^{[\overline{e}]},\ldots,{g_n}^{[\overline{e}]}\right)^{d_1\cdots d_n\cdot(\overline{e}-\underline{e})},\end{aligned}$$

where ${g_j}^{[\overline{e}]}$ stands for the homogeneous part of g_j of total degree $\overline{e}$.

This factorization is irreducible if the f_i's and g_j's have distinct symbolic coefficients.

Example 2 We illustrate the main theorem. Let

$$\begin{aligned}f_1 &:= 3\,y_1 - 5\,y_2 + 8\,y_3,\\ f_2 &:= 2\,y_1^2 + 11\,y_1\,y_2 - 7\,y_1\,y_3 + 5\,y_2^2 + 18\,y_2\,y_3 - 6\,y_3^2,\\ f_3 &:= 23\,y_1 + 3\,y_2 - 9\,y_3,\end{aligned}$$

and let

$$\begin{aligned}
g_1 &:= 2\,x_1 \,+\, 12\,x_2 \,+\, 14, \\
g_2 &:= 8\,x_1^3 \,+\, 3\,x_1^2\,x_2 \,+\, 7\,x_1\,x_2^2 \,-\, 5\,x_2^3 \\
&\quad + 19\,x_1^2 + 17\,x_1\,x_2 - 14\,x_2^2 + 12\,x_1 - 11\,x_2 + 3, \\
g_3 &:= 6\,x_1^3 \,+\, 7\,x_1^2\,x_2 \,-\, 19\,x_1\,x_2^2 \,-\, 4\,x_2^3 \\
&\quad + 4\,x_1^2 - 5\,x_1\,x_2 + 33\,x_2^2 + 11\,x_1 + 9\,x_2 + 10.
\end{aligned}$$

Observe that $n = 3,\ d_1 = 1,\ d_2 = 2,\ d_3 = 1,\ e_1 = \underline{e} = 1 \ <\ e_2 = e_3 = \overline{e} = 3$, $k = 1$ and that

$$\begin{aligned}
{g_2}^{[3]} &= 8\,x_1^3 \,+\, 3\,x_1^2\,x_2 \,+\, 7\,x_1\,x_2^2 \,-\, 5\,x_2^3 \\
{g_3}^{[3]} &= 6\,x_1^3 \,+\, 7\,x_1^2\,x_2 \,-\, 19\,x_1\,x_2^2 \,-\, 4\,x_2^3.
\end{aligned}$$

Therefore

$$\begin{aligned}
&\mathrm{Res}_{3,6,3}\left(f_1 \circ (g_1, g_2, g_3)\,,\, f_2 \circ (g_1, g_2, g_3)\,,\, f_3 \circ (g_1, g_2, g_3)\right) \\
&\qquad = \ \mathrm{Res}_{1,2,1}\left(f_1, f_2, f_3\right)^{3^2}\ \mathrm{Res}_{3,3,3}\left(g_1, g_2, g_3\right)^{1\cdot 2\cdot 1}
\end{aligned}$$

and the second factor can be factorized further as

$$\mathrm{Res}_{3,3,3}\left(g_1, g_2, g_3\right)^{1\cdot 2\cdot 1} \ = \ \mathrm{Res}_{1,3,3}\left(g_1, g_2, g_3\right)^{1\cdot 2\cdot 1}\ \mathrm{Res}_{3,3}\left({g_2}^{[3]}, {g_3}^{[3]}\right)^{1\cdot 2\cdot 1\cdot (3-1)}.$$

Remark 3 The reader might wonder why in the main theorem we consider the case of dense resultant of homogeneous polynomials composed with not necessarily homogeneous polynomials. It turns out that the other cases can be trivially transformed into the case of the main theorem. The following two trivial rules allow us to transform all the other cases into the case of the main theorem.

(1) Suppose that the g_j's are homogeneous in n variables of same total degrees. Then

$$\begin{aligned}
&\mathrm{Res}_{d_1\overline{e},\ldots,d_n\overline{e}}\left(f_1 \circ (g_1, \ldots, g_n), \ldots, f_n \circ (g_1, \ldots, g_n)\right) \ = \\
&\qquad\qquad \mathrm{Res}_{d_1\overline{e},\ldots,d_n\overline{e}}\left(f_1 \circ \left(g_1^{\mathrm{d}}, \ldots, g_n^{\mathrm{d}}\right), \ldots, f_n \circ \left(g_1^{\mathrm{d}}, \ldots, g_n^{\mathrm{d}}\right)\right),
\end{aligned}$$

where g^{d} stands for the dehomogenization of g, that is, g^{d} is formed by replacing the variable x_n by 1.

(2) Suppose that the g_j's are not necessarily homogeneous and the f_i's are not necessarily homogeneous in $n-1$ variables. Then

$$\begin{aligned}
&\mathrm{Res}_{d_1\overline{e},\ldots,d_n\overline{e}}\left(f_1 \circ (g_1, \ldots, g_{n-1}), \ldots, f_n \circ (g_1, \ldots, g_{n-1})\right) \ = \\
&\qquad\qquad \mathrm{Res}_{d_1\overline{e},\ldots,d_n\overline{e}}\left(f_1^{\mathrm{h}} \circ (g_1, \ldots, g_{n-1}, 1), \ldots, f_n^{\mathrm{h}} \circ (g_1, \ldots, g_{n-1}, 1)\right),
\end{aligned}$$

where ${f_i}^{\mathrm{h}}$ stands for the homogenization of f_i to the total degree d_i.

Remark 4 It is important to point out that in a particular degenerate case the definition of the dense resultant in the main theorem is slightly different from the usual one. For degenerate cases with $d_k = 0$, we define

$$\mathrm{Res}_{d_1,\ldots,d_{k-1},0,d_{k+1},\ldots,d_n}(f_1,\ldots,f_{k-1},f_k,f_{k+1},\ldots,f_n) \;:=\; f_k^{d_1\cdots d_{k-1}\cdot d_{k+1}\cdots d_n},$$

whereas usually one defines

$$\mathrm{Res}_{d_1,\ldots,d_{k-1},0,d_{k+1},\ldots,d_n}(f_1,\ldots,f_{k-1},f_k,f_{k+1},\ldots,f_n) \;:=\; f_k.$$

The first definition allows us to give a uniform formula for all subcases of dense resultant of composed polynomials, whereas the second definition seems not to allow this.

Remark 5 We consider the dense resultant of the composed polynomials $f_i \circ (g_1,\ldots,g_n)$ with respect to the total degrees "$d_i\overline{e}$". This is natural because almost always the total degree of $f_i \circ (g_1,\ldots,g_n)$ is $d_i\overline{e}$.

Remark 6 From the main theorem we can see immediately that if at least two of the e_j's are smaller than $\overline{e}$ then

$$\mathrm{Res}_{d_1\overline{e},\ldots,d_n\overline{e}}(f_1\circ(g_1,\ldots,g_n),\ldots,f_n\circ(g_1,\ldots,g_n)) \;=\; 0.$$

In the proof (cf. Section 3) we will see why this happens. In short, the dense resultant vanishes because the $f_i \circ (g_1,\ldots,g_n)$'s have naturally generated common zeros at infinity.

Remark 7 The main theorem covers the cases of dense resultant of composed polynomials considered by Cheng et al. [1995] and Jouanolou [1991]. [1] As an example, we show how one can recover from the main theorem the formula of Cheng et al. [1995] for dense resultant of inhomogeneous polynomials composed with inhomogeneous polynomials of same total degrees. Let the f_i's be inhomogeneous in $n-1$ variables of positive total degrees and let the g_j's be inhomogeneous in $n-1$ variables of same positive total degree. By the main

[1] Note that Jouanolou gives, in Proposition 5.11.2 of Jouanolou [1991], an interesting formula for dense resultant of certain *sparse* linear polynomials composed with homogeneous polynomials. This formula is not among the cases of this paper because the linear polynomials are sparse. We suggest that one classifies formulas involving sparse composed polynomials within the theory of sparse resultants (cf. Cox et al. [1998]). Some work in this direction has already been done, for example in Hong and Minimair [2002].

theorem,

$$
\begin{aligned}
&\operatorname{Res}_{d_1\overline{e},\ldots,d_n\overline{e}}\left(f_1\circ(g_1,\ldots,g_{n-1}),\ldots,f_n\circ(g_1,\ldots,g_{n-1})\right)\\
&\qquad=\operatorname{Res}_{d_1\overline{e},\ldots,d_n\overline{e}}\left(f_1^{\mathrm{h}}\circ(g_1,\ldots,g_{n-1},1),\ldots,f_n^{\mathrm{h}}\circ(g_1,\ldots,g_{n-1},1)\right)\\
&\qquad=\operatorname{Res}_{d_1,\ldots,d_n}\left(f_1^{\mathrm{h}},\ldots,f_n^{\mathrm{h}}\right)^{\overline{e}^{n-1}}\ \operatorname{Res}_{\overline{e},\ldots,\overline{e}}\left(g_1,\ldots,g_{n-1},1\right)^{d_1\cdots d_n}\\
&\qquad=\operatorname{Res}_{d_1,\ldots,d_n}\left(f_1,\ldots,f_n\right)^{\overline{e}^{n-1}}\\
&\qquad\qquad\operatorname{Res}_{\overline{e},\ldots,\overline{e},0}\left(g_1,\ldots,g_{n-1},1\right)^{d_1\cdots d_n}\ \operatorname{Res}_{\overline{e},\ldots,\overline{e}}\left({g_1}^{[\overline{e}]},\ldots,{g_{n-1}}^{[\overline{e}]}\right)^{d_1\cdots d_n\cdot(\overline{e}-0)}\\
&\qquad=\operatorname{Res}_{d_1,\ldots,d_n}\left(f_1,\ldots,f_n\right)^{\overline{e}^{n-1}}\operatorname{Res}_{\overline{e},\ldots,\overline{e}}\left({g_1}^{[\overline{e}]},\ldots,{g_{n-1}}^{[\overline{e}]}\right)^{d_1\cdots d_n\cdot\overline{e}},
\end{aligned}
$$

which is the expression given by Cheng et al. [1995].

Remark 8 Applying the main theorem when computing the dense resultant of composed polynomials can be expected to yield a dramatic improvement in efficiency (compare Hong and Minimair [2002]). In order to compute the dense resultant of composed polynomials, we only have to compute the dense resultants of the component polynomials and some of their leading forms, which is expected to be much more efficient than computing the dense resultant of the expanded composed polynomials because the components and the leading forms are much smaller and have a lower degree than the expanded composed polynomials.

3 Proof

Before we prove the main theorem, we state a lemma that is of independent interest. We want to know what happens to the dense resultant when some leading forms of the input polynomials vanish or, equivalently, if some input polynomials have a total degree that is lower than the total degree with respect to which the dense resultant is computed.

In the lemma we allow the g_j's also to be non zero constants.

Lemma 9 *We have*

$$
\begin{aligned}
&\operatorname{Res}_{\overline{e},\ldots,\overline{e}}\left(g_1,\ldots,g_n\right)\\
&\qquad=\ \operatorname{Res}_{\overline{e},\ldots,\overline{e},\,e_k,\,\overline{e},\ldots,\overline{e}}\left(g_1,\ldots,g_{k-1},\ g_k,\ g_{k+1},\ldots,g_n\right)\\
&\qquad\qquad\operatorname{Res}_{\overline{e},\ldots,\overline{e}}\left({g_1}^{[\overline{e}]},\ldots,{g_{k-1}}^{[\overline{e}]},\ {g_{k+1}}^{[\overline{e}]},\ldots,{g_n}^{[\overline{e}]}\right)^{\overline{e}-\underline{e}},
\end{aligned}
$$

where ${g_j}^{[\overline{e}]}$ *stands for the homogeneous part of* g_j *of total degree* $\overline{e}$*.*

This factorization is irreducible, if the g_j*'s have distinct symbolic coefficients.*

Example 10 (continuing Example 2) We illustrate the lemma. Observe that $e_1 = 1 \; < \; e_2 = e_3 = \overline{e} = 3$ and $k = 1$. Therefore

$$\mathrm{Res}_{3,3,3}\,(g_1, g_2, g_3) \;=\; \mathrm{Res}_{1,3,3}\,(g_1, g_2, g_3)\; \mathrm{Res}_{3,3}\left(w_2{}^{[3]}, w_3{}^{[3]}\right)^2 .$$

Proof (of Lemma 9):

Firstly, we suppose that the g_j's have positive total degrees, distinct symbolic coefficients and there is exactly one k such that $e_k = \underline{e}$ and $e_j = \overline{e}$, for $j \neq k$. Since the lemma is invariant under reordering of the g_j's, we assume without loss of generality that $k = 1$. Let $\widehat{g}$ denote a polynomial in the variables $x_1, \ldots, x_{n-1}$ of total degree $\overline{e}$ with distinct symbolic coefficients, let K denote the algebraic closure of the field generated by the complex numbers and the symbolic coefficients of $\widehat{g}$ and $g_2, \ldots, g_n$ and let $m_{\widehat{g}}$ denote the linear operator $p \mapsto p \cdot \widehat{g}$, defined on the K-vector space $K\,[x_1, \ldots, x_{n-1}] \,/_{\langle g_2, \ldots, g_n \rangle}$, where $\langle g_2, \ldots, g_n \rangle$ denotes the ideal generated by $g_2, \ldots, g_n$ in $K\,[x_1, \ldots, x_{n-1}]$. By the Poisson formula (cf. Jouanolou [1991] and Cox et al. [1998]), we have

$$\mathrm{Res}_{\overline{e},\ldots,\overline{e}}\,(\widehat{g}, g_2, \ldots, g_n) \;=\; \det\left(m_{\widehat{g}}\right)\; \mathrm{Res}_{\overline{e},\ldots,\overline{e}}\left(g_2{}^{[\overline{e}]}, \ldots, g_n{}^{[\overline{e}]}\right)^{\overline{e}} .$$

Further, by the techniques of Pedersen et al. [1993], we have

$$\mathrm{Res}_{\overline{e},\overline{e},\ldots,\overline{e}}\,(\widehat{g}, g_2, \ldots, g_n) \;=\; \prod_{\xi \,\in\, \widehat{V}} \widehat{g}\,(\xi_1, \ldots, \xi_{n-1})\; \mathrm{Res}_{\overline{e},\ldots,\overline{e}}\left(g_2{}^{[\overline{e}]}, \ldots, g_n{}^{[\overline{e}]}\right)^{\overline{e}} ,$$

where $\xi \;=\; (\xi_1, \ldots, \xi_{n-1})$ and $\widehat{V}$ is the common solution set of $g_2, \ldots, g_n$ in K^n. Since the symbolic coefficients of $\widehat{g}$ are algebraically independent from the symbolic coefficients of $g_2, \ldots, g_n$, the previous formula is stable under specialization of the coefficients of $\widehat{g}$. By specializing $\widehat{g}$ to g_1, we get

$$\mathrm{Res}_{\overline{e},\ldots,\overline{e}}\,(g_1, \ldots, g_n) \;=\; \prod_{\xi \,\in\, V} g_1\,(\xi_1, \ldots, \xi_{n-1})\; \mathrm{Res}_{\overline{e},\ldots,\overline{e}}\left(g_2{}^{[\overline{e}]}, \ldots, g_n{}^{[\overline{e}]}\right)^{\overline{e}} ,$$

where V is the common solution set of $g_2, \ldots, g_n$ over the algebraic closure of the field generated by the complex numbers and the coefficients of $g_2, \ldots, g_n$. Now, observe that, by the Poisson formula and by Pedersen et al. [1993],

$$\mathrm{Res}_{e_1,\overline{e},\ldots,\overline{e}}\,(g_1, g_2, \ldots, g_n) \;=\; \prod_{\xi \,\in\, V} g_1\,(\xi_1, \ldots, \xi_{n-1})\; \mathrm{Res}_{\overline{e},\ldots,\overline{e}}\left(g_2{}^{[\overline{e}]}, \ldots, g_n{}^{[\overline{e}]}\right)^{e_1} .$$

Therefore

$$\begin{aligned}
\mathrm{Res}_{\overline{e},\ldots,\overline{e}}\,(g_1, \ldots, g_n) \;&=\; \prod_{\xi \,\in\, V} g_1\,(\xi_1, \ldots, \xi_{n-1})\; \mathrm{Res}_{\overline{e},\ldots,\overline{e}}\left(g_2{}^{[\overline{e}]}, \ldots, g_n{}^{[\overline{e}]}\right)^{\overline{e}} \\
&= \prod_{\xi \,\in\, V} g_1\,(\xi_1, \ldots, \xi_{n-1})\; \mathrm{Res}_{\overline{e},\ldots,\overline{e}}\left(g_2{}^{[\overline{e}]}, \ldots, g_n{}^{[\overline{e}]}\right)^{e_1}\; \mathrm{Res}_{\overline{e},\ldots,\overline{e}}\left(g_2{}^{[\overline{e}]}, \ldots, g_n{}^{[\overline{e}]}\right)^{\overline{e}-e_1} \\
&= \mathrm{Res}_{g_1,\overline{e},\ldots,\overline{e}}\,(g_1, \ldots, g_n)\; \mathrm{Res}_{\overline{e},\ldots,\overline{e}}\left(g_2{}^{[\overline{e}]}, \ldots, g_n{}^{[\overline{e}]}\right)^{\overline{e}-e_1} .
\end{aligned}$$

Secondly, we suppose that the g_j's have distinct symbolic coefficients with positive total degrees and at least two of the e_j's are smaller than $\overline{e}$. Since the lemma is invariant under reordering of the g_j's, we assume without loss of generality that $e_1, e_2 < \overline{e}$. We regard $g_2, \ldots, g_n$ as specialized polynomials of total degree $\overline{e}$, whose forms of degrees $e_j + 1, \ldots, \overline{e}$ vanish. Obviously, the formula, which we have already shown, of the first part of the lemma, holds for such specialized polynomials as well.

Thirdly, we suppose that the g_j's have distinct symbolic coefficients and at least one of the e_j's is zero. Since the lemma is invariant under reordering of the g_j's, we assume without loss of generality that $e_1 = 0$. We have, if $e_j = \overline{e}$ for $j \geq 2$, by the multihomogeneity of the dense resultant (cf. Cox et al. [1998]) and by the Poisson formula (cf. Jouanolou [1991]),

$$\begin{aligned} \mathrm{Res}_{\overline{e},\overline{e},\ldots,\overline{e}}\,(g_1, g_2, \ldots, g_n) &= g_1^{\overline{e}^{n-1}}\ \mathrm{Res}_{\overline{e},\overline{e},\ldots,\overline{e}}\,(1, g_2, \ldots, g_n) \\ &= g_1^{\overline{e}^{n-1}}\ \mathrm{Res}_{\overline{e},\ldots,\overline{e}}\left(g_2{}^{[\overline{e}]}, \ldots, g_n{}^{[\overline{e}]}\right)^{\overline{e}} \end{aligned}$$

and, by definition (cf. Remark 4),

$$\mathrm{Res}_{\,0,\overline{e},\ldots,\overline{e}}\,(g_1, g_2, \ldots, g_n) \;=\; g_1^{\overline{e}^{n-1}}$$

and thus, by specialization, the formula of the lemma also holds in this case.

Therefore we have shown the formula of the lemma for g_j's with distinct symbolic coefficients and it remains to relax the formula to g_j's which do not have symbolic coefficients. This is easy because the formula, involving only polynomials in the symbolic coefficients of the g_j's, is stable under specialization.

Now we prove that the factorization given by the formula of the lemma is irreducible if the g_j's have distinct symbolic coefficients. This is obvious if at most one e_j is smaller than $\overline{e}$. Suppose that at least two of the e_j's are smaller than $\overline{e}$. Since the lemma is invariant under reordering of the g_j's, we assume without loss of generality that $e_1, e_2 < \overline{e}$. We show that

$$\mathrm{Res}_{\overline{e},\ldots,\overline{e}}\,(g_1, \ldots, g_n) \;=\; 0.$$

The forms of $g_1, \ldots, g_n$ of total degree $\overline{e}$ are $0, 0, g_3{}^{[\overline{e}]}, \ldots, g_n{}^{[\overline{e}]}$. By Bezout's theorem (cf. Danilov and Shokurov [1998] and Cox et al. [1998]) the $n-2$ homogeneous polynomials $g_3{}^{[\overline{e}]}, \ldots, g_n{}^{[\overline{e}]}$ in the variables $x_1, \ldots, x_{n-1}$ have a non trivial common zero in the algebraic closure of the field generated by the complex numbers and the symbolic coefficients of $g_3, \ldots, g_n$. Therefore

$$\mathrm{Res}_{\overline{e},\ldots,\overline{e}}\,(g_1, \ldots, g_n) \;=\; 0.$$

Thus we have shown the lemma.

□

Now we are ready to prove the main theorem. We are aware of several different proofs. The most elegant one is the proof given here. The proof is elegant because we base the proof on Lemma 9 and on the formula of Cheng et al. [1995] and Jouanolou [1991] for dense resultant of homogeneous polynomials composed with homogeneous polynomials of same total degrees.

Proof of Theorem 1 (Main theorem):

It is easy to see that the homogenization of $f_i \circ (g_1, \ldots, g_n)$ to the total degree $d_i\,\overline{e}$ is $f_i \circ \left({g_1}^{\mathrm{h}}, \ldots, {g_n}^{\mathrm{h}}\right)$, where ${g_j}^{\mathrm{h}}$ is the homogenization of g_j to the total degree $\overline{e}$. By Cheng et al. [1995] and Jouanolou [1991], we get

$$\begin{aligned} &\mathrm{Res}_{d_1\overline{e},\ldots,d_n\overline{e}}\,(f_1 \circ (g_1, \ldots, g_n), \ldots, f_n \circ (g_1, \ldots, g_n)) \\ &\quad = \mathrm{Res}_{d_1\overline{e},\ldots,d_n\overline{e}}\left(f_1 \circ \left({g_1}^{\mathrm{h}}, \ldots, {g_n}^{\mathrm{h}}\right), \ldots, f_n \circ \left({g_1}^{\mathrm{h}}, \ldots, {g_n}^{\mathrm{h}}\right)\right) \\ &\quad = \mathrm{Res}_{d_1,\ldots,d_n}\,(f_1, \ldots, f_n)^{\overline{e}^{n-1}}\ \mathrm{Res}_{\overline{e},\ldots,\overline{e}}\left({g_1}^{\mathrm{h}}, \ldots, {g_n}^{\mathrm{h}}\right)^{d_1\cdots d_n} \\ &\quad = \mathrm{Res}_{d_1,\ldots,d_n}\,(f_1, \ldots, f_n)^{\overline{e}^{n-1}}\ \mathrm{Res}_{\overline{e},\ldots,\overline{e}}\,(g_1, \ldots, g_n)^{d_1\cdots d_n}\,. \end{aligned}$$

By Lemma 9, we have that

$$\begin{aligned} &\mathrm{Res}_{d_1\overline{e},\ldots,d_n\overline{e}}\,(f_1 \circ (g_1, \ldots, g_n), \ldots, f_n \circ (g_1, \ldots, g_n)) \\ &= \mathrm{Res}_{d_1,\ldots,d_n}\,(f_1, \ldots, f_n)^{\overline{e}^{n-1}}\ \mathrm{Res}_{\overline{e},\ldots,\overline{e},e_k,\overline{e},\ldots,\overline{e}}\,(g_1, \ldots, g_{k-1}, g_k, g_{k+1}, \ldots, g_n)^{d_1\cdots d_n} \\ &\qquad \mathrm{Res}_{\overline{e},\ldots,\overline{e}}\left({g_1}^{[\overline{e}]}, \ldots, {g_{k-1}}^{[\overline{e}]}, {g_{m+1}}^{[\overline{e}]}, \ldots, {g_n}^{[\overline{e}]}\right)^{d_1\cdots d_n\cdot(\overline{e}-e_m)}\,. \end{aligned}$$

It remains to show that this factorization is irreducible if the f_i's and g_j's have distinct symbolic coefficients. This follows from Lemma 9 and we could stop. However, we show the irreducibility without using Lemma 9 because the proof gives some interesting insight. If at most one e_j is smaller than $\overline{e}$ it is easy to see that the factorization is irreducible. Assume that at least two of the e_j's are smaller than $\overline{e}$. We show that

$$\mathrm{Res}_{d_1\overline{e},\ldots,d_n\overline{e}}\,(f_1 \circ (g_1, \ldots, g_n), \ldots, f_n \circ (g_1, \ldots, g_n)) \;=\; 0.$$

The dense (Macaulay) resultant vanishes because the composed polynomials $f_i \circ (g_1, \ldots, g_n)$ have some common zeros at infinity. It is interesting to know what these common zeros at infinity are. We show that they are the common zeros of certain leading forms of the g_j's.

Since we can rename the variables of the f_i's and the g_j's such that $e_1, \ldots, e_k = \overline{e}$ and $e_{k+1}, \ldots, e_n < \overline{e}$ without changing the composed polynomials $f_i \circ (g_1, \ldots, g_n)$. We assume that, for $k \le n-2$, $e_1, \ldots, e_k = \overline{e}$ and $e_{k+1}, \ldots, e_n < \overline{e}$. We start with computing the leading form of $f_i \circ (g_1, \ldots, g_n)$. Note that $f_i = f_i^+ + f_i^-$, where each monomial in f_i^+ is only divisible by variables among $x_1, \ldots, x_k$, and where each monomial in f_i^- is divisible by at least one x_j, for $j > k$, and thus

$$f_i \circ (g_1, \ldots, g_n) = f_i^+ \circ (g_1, \ldots, g_k) + f_i^- \circ (g_1, \ldots, g_n)\,.$$

Since the total degree of $f_i^+ \circ (g_1, \ldots, g_k)$ is $d_i\,\overline{e}$ and the total degree of $f_i^- \circ (g_1, \ldots,\ g_n)$ is smaller than $d_i\,\overline{e}$, the leading form of $f_i \circ (g_1, \ldots, g_n)$ equals the leading form of $f_i^+ \circ (g_1, \ldots, g_k)$. Now we intend to apply Lemma 10 of Hong and Minimair [2002] to $f_i^+ \circ (g_1, \ldots,\ g_k)$. Note that this lemma is stated for homogeneous polynomials composed with n *homogeneous* (Laurent) polynomials of same total degrees. It is easy to see that this lemma also holds for homogeneous polynomials composed with k *not necessarily homogeneous* polynomials of same total degrees. Following the notation of the lemma, we denote the leading form of $f_i^+ \circ (g_1, \ldots, g_k)$ by $\left(f_i^+ \circ (g_1, \ldots, g_k)\right)_{\mathcal{E}}^{\omega}$, where $\omega = (1, \ldots, 1)$ and $\mathcal{E}$ is the set of all monomials contained in $f_i^+ \circ (g_1, \ldots, g_n)$. Then, by the adapted Lemma 10 of Hong and Minimair [2002],

$$\left(f_i^+ \circ (g_1, \ldots, g_k)\right)_{\mathcal{E}}^{\omega} \;=\; f_i^+ \circ ({g_1}_{\mathcal{B}}^{\omega}, \ldots, {g_k}_{\mathcal{B}}^{\omega})\,,$$

where B is the set of all monomials contained in $g_1, \ldots, g_k$. Note that ${g_j}_{\mathcal{B}}^{\omega} = {g_j}^{[\overline{e}]}$. Therefore the leading form of $f_i \circ (g_1, \ldots, g_n)$ is $f_i^+ \circ \left({g_1}^{[\overline{e}]}, \ldots, {g_k}^{[\overline{e}]}\right)$. Now, by Bezout's theorem (cf. Danilov and Shokurov [1998] and Cox et al. [1998]) the k homogeneous polynomials ${g_1}^{[\overline{e}]}, \ldots, {g_k}^{[\overline{e}]}$ in the variables $x_1, \ldots, x_{n-1}$ have a non trivial common zero over the algebraic closure of the field generated by the complex numbers and the symbolic coefficients of ${g_1}^{[\overline{e}]}, \ldots, {g_k}^{[\overline{e}]}$. Since there is at least one e_j that equals $\overline{e}$, the sequence $g_1, \ldots, g_k$ is not empty and such a non trivial common zero ξ exists. Take any such non trivial common zero ξ. Then ξ is a non trivial common zero of the $f_i^+ \circ \left({g_1}^{[\overline{e}]}, \ldots, {g_k}^{[\overline{e}]}\right)$'s and thus ξ is a common zero at infinity of the $f_i \circ (g_1, \ldots, g_n)$'s.

Thus we have shown the main theorem. □

4 Conclusion

In this paper we studied the dense (Macaulay) resultant of composed polynomials. Cheng, McKay and Wang and Jouanolou have studied two particular subcases. The main contribution of this paper was to complete these works by providing a uniform answer for all subcases. In short, it states that the dense resultant of composed polynomials is the product of certain powers of the dense resultants of the component polynomials and of some of their leading forms.

Acknowledgment

I thank my colleague Jack Perry for computing some dense resultants. Further, I thank my PhD adviser Prof. Hoon Hong for guidance and support. This research was partially supported by NSF project "Computing with composed functions", NSF CCR-9972527.

References

P. H. Berman and M. F. Singer. Calculating the Galois group of $L_1(L_2(y)) = 0$, L_1, L_2 completely reducible operators. *J. Pure Appl. Algebra*, 139(1-3):3–23, 1999. Effective methods in algebraic geometry (Saint-Malo, 1998).

J. Canny and I. Emiris. A subdivision-based algorithm for the sparse resultant. *J. ACM*, 47(3):417–451, May 2000.

J. Canny, E. Kaltofen, and Lakshman Y. Solving systems of non-linear polynomial equations faster. In *Proc. ACM-SIGSAM 1989 Internat. Symp. Symbolic Algebraic Comput. ISSAC'89*, pages 121–128. ACM, 1989.

E. Cattani, A. Dickenstein, and B. Sturmfels. Residues and resultants. *J. Math. Sci. Univ. Tokyo*, 5(1):119–148, 1998.

A. Cayley. On the theory of elimination. *Cambridge and Dublin Math. J.*, 3: 116–120, 1848.

M. Chardin. *Contributions à l'algèbre commutative effective et à la théorie de l'élimination*. PhD thesis, Université Paris VI, 1990.

C. C. Cheng, J. H. McKay, and S. S. Wang. A chain rule for multivariable resultants. *Proceedings of the American Mathematical Society*, 123(4):1037–1047, April 1995.

D. Cox, J. Little, and D. O'Shea. *Using Algebraic Geometry*. Springer Verlag, New York, Berlin, Heidelberg, 1998.

V. I. Danilov and V. V. Shokurov. *Algebraic Curves, Algebraic Manifolds and Schemes*. Springer-Verlag, Berlin Heidelberg New York, 2nd edition, 1998.

A.-L. Dixon. The eliminant of three quantics in two independent variables. *Proc. London Math. Soc.*, 7:49–69, 473–492, November 1908.

I. Emiris and V. Pan. The structure of sparse resultant matrices. In *Proc. Int. Symp. on Symbolic and Algebraic Computation (ISSAC)*. ACM Press, 1997.

I. M. Gelfand, M. M. Kapranov, and A. V. Zelevinsky. *Discriminants, Resultants and Multidimensional Determinants*. Birkhäuser, Boston, 1994.

L. Gonzáles-Vega. Une théorie des sous-résultants pour les polynômes en plusieurs variables. *C. R. Acad. Sci. Paris Sér. I Math.*, 313/13:905–908, 1991.

H. Hong. Subresultants under composition. *J. Symbolic Computation*, 23(4): 355–365, 1997.

H. Hong. Groebner basis under composition. I. *J. Symbolic Computation*, 25 (5):643–663, 1998.

H. Hong and M. Minimair. Sparse resultant of composed polynomials I. *J. Symbolic Computation*, 33:447–465, 2002.

J. P. Jouanolou. Le formalisme du résultant. *Adv. Math.*, 90(2):117–263, 1991.

D. Kapur and T. Saxena. Sparsity considerations in Dixon resultants. In *Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing (Philadelphia, PA, 1996)*, pages 184–191, New York, 1996. ACM.

R. Lewis and P. Stiller. Solving the recognition problem for six lines using the Dixon resultant. *Math. Comput. Simulation*, 49(3):205–219, 1999.

F. S. Macaulay. *The algebraic theory of modular systems*. Cambridge Mathematical Library, 1916.

D. Manocha and J. Canny. Multipolynomial resultant algorithms. *J. Symbolic Computation*, 15(2):99–122, 1993.

G. Nakos and R. M. Williams. Eliminiation with the Dixon resultant. *Mathematica for Education and Research*, 6/3:11–21, 1997.

P. Pedersen, M.-F. Roy, and A. Szpirglas. Counting real zeros in the multivariate case. In *Computational Algebraic Geometry (Nice, 1992)*, volume 109 of *Progr. Math*, pages 203–224, Boston, MA, 1993. Birkhäuser.

P. Pedersen and B. Sturmfels. Product formulas for resultants and Chow forms. *Mathematische Zeitschrift*, 214:377–396, 1993.

J. M. Rojas. Solving degenerate sparse polynomial systems faster. *J. Symbolic Computation*, 28(1 and 2):155–186, July/August 1999. Special Issue Polynomial Elimination – Algorithms and Applications.