Article Submitted to a journal

Sparse Resultant of Composed Polynomials I*

Mixed - Unmixed Case

HOON HONG†1 AND MANFRED MINIMAIR†2

[1] *hong@math.ncsu.edu*
http://www.math.ncsu.edu/~ hong
Department of Mathematics
North Carolina State University
Box 8205, Raleigh, NC 27695, USA

[2] *manfred@minimair.org*
http://minimair.org

Old mailing address:
Department of Mathematics
North Carolina State University
Box 8205, Raleigh, NC 27695, USA

New mailing address:
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 happens to sparse resultants under composition?* More precisely, let $f_1, \ldots, f_n$ be homogeneous sparse polynomials in the variables $y_1, \ldots, y_n$ and $g_1, \ldots, g_n$ be homogeneous sparse polynomials in the variables $x_1, \ldots, x_n$. Let $f_i \circ (g_1, \ldots, g_n)$ be the sparse homogeneous polynomial obtained from f_i by replacing y_j by g_j. Naturally a question arises: Is the sparse resultant of $f_1 \circ (g_1, \ldots, g_n)$, $\ldots, f_n \circ (g_1, \ldots, g_n)$ in any way related to the (sparse) resultants of $f_1, \ldots, f_n$ and $g_1, \ldots, g_n$? The main contribution of this paper is to provide an answer for the case when $g_1, \ldots, g_n$ are unmixed, namely,

$$\begin{aligned}&\operatorname{Res}_{\mathcal{C}_1,\ldots,\mathcal{C}_n}\left(f_1 \circ (g_1,\ldots,g_n), \ldots, f_n \circ (g_1,\ldots,g_n)\right)\\ &\qquad\qquad = \operatorname{Res}_{d_1,\ldots,d_n}\left(f_1,\ldots,f_n\right)^{\operatorname{Vol}(Q)} \operatorname{Res}_{\mathcal{B}}\left(g_1,\ldots,g_n\right)^{d_1\cdots d_n},\end{aligned}$$

where $\operatorname{Res}_{d_1,\ldots,d_n}$ stands for dense (Macaulay) resultant with respect to the total degrees d_i of the f_i's, $\operatorname{Res}_{\mathcal{B}}$ stands for unmixed sparse resultant

---

*Originally titled "A Chain Rule for Sparse Resultants".

†Partially supported by NSF project "Computing with composed functions", NSF CCR-9972527

with respect to the support $\mathcal{B}$ of the g_j's, $\mathrm{Res}_{\mathcal{C}_1,\ldots,\mathcal{C}_n}$ stands for mixed sparse resultant with respect to the naturally induced supports $\mathcal{C}_i$ of the $f_i \circ (g_1, \ldots, g_n)$'s, and $\mathrm{Vol}\,(Q)$ for the normalized volume of the Newton polytope of the g_j. The above expression can be applied to compute sparse resultants of composed polynomials with improved efficiency.

1. Introduction

Resultants are fundamental in solving systems of polynomial equations and thus have been extensively studied (cf. [Dix08], [Mac16], [Cay48], [CKY89], [Cha90], [CMW95], [GV91], [Jou91], [MC93], [KS96], [NW97], [LS99], [DD00], [BEM00]). Recently the research is focused on utilizing the sparsity structure of polynomials which are prevalent in almost all real life problems, yielding a generalized resultant, named the sparse resultant (cf. [PS93], [EC95], [GKZ94], [CLO98], [CDS98], [Roj99a]).

It turns out that in real life problems another structure occurs naturally, namely "composition". More precisely, the polynomials occurring in real life are often formed by composing many sparse polynomials iteratively. This is because large scale engineering systems are almost always designed by composing modular components hierarchically, naturally resulting in mathematical models involving composed polynomials. Thus we think that it is important to investigate how to utilize the inherent composition structure as well. In this regard a fundamental question is: *What happens to sparse resultants under composition?* That is, is the sparse resultant of composed polynomials in any way related to the (sparse) resultants of the component polynomials?

We give an answer for the case of homogeneous polynomials composed with *unmixed homogeneous*[‡] polynomials. In short, it states that the sparse resultant of composed polynomials is the product of certain powers of the (sparse) resultants of the component polynomials. This result can be viewed as a generalization of the work of Cheng, McKay and Wang (cf. [CMW95]) where they answered the same question but for dense polynomials. This result can also be viewed as a generalization of the work of Gelfand, Kapranov and Zelevinsky (cf. Corollary 2.2 in Chapter 8 of [GKZ94]) where they answered the same question but for linear polynomials composed with sparse polynomials.

Applying this result yields dramatic improvement in efficiency both in space and in time over computing without taking advantage of the composition structure (cf. Theorem 1).

The reader might wonder whether one can utilize 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

---

[‡] One of the authors, Manfred Minimair, has investigated, as part of his PhD work, the same question but for a more general class of inputs, namely allowing *mixed non homogeneous* polynomials.

differential operators have been studied in [Hon97], [Hon98] and [BS99], resp., using various mathematical techniques. However, it seems that those techniques cannot be applied to the study of sparse resultants. Therefore in this paper we use mathematical methods that are essentially different from those.

We assume that the reader is familiar with the notions of dense (Macaulay) resultant of homogeneous polynomials, sparse resultant of inhomogeneous Laurent polynomials, mixed volume, normalized volume of Newton polytope. For their definitions see, for example, [CLO98], [PS93]. There are different definitions of normalized volume in the literature. We follow the definition given in [PS93]. Further, we assume that the reader is familiar with the notions of arithmetic time and space complexity and Newton matrix. For their definitions see, for example, [vAHU83] and [EC95]. We also assume that the reader is familiar with the algorithms that are described in [EC95] and in [EP97], for computing Newton matrices and sparse resultants.

2. Main result

Let $f_1, \ldots, f_n$ be homogeneous[§] sparse polynomials in the variables $y_1, \ldots, y_n$ with distinct symbolic coefficients of positive total degrees $d_1, \ldots, d_n$ and let $g_1, \ldots, g_n$ be homogeneous sparse Laurent polynomials in the variables $x_1, \ldots, x_n$ with distinct symbolic coefficients distinct from the coefficients of the f_i's.[¶] Let $d_{\max}$ stand for the maximum of the d_i's.

We assume that the g_j's are *unmixed*, that is, all the g_j's have the same set $\mathcal{B}$ of supporting Laurent monomials. Let V_Q stand for the volume of the Newton polytope Q of the g_j's and let $\mathrm{Vol}\,(Q)$ stand for the normalized volume of the Newton polytope Q, that is, $\mathrm{Vol}\,(Q) = V_Q \cdot (n-1)!$.

Further we assume that the dimension of the Newton polytope Q of the g_j's is $n-1$ and that the exponents of the Laurent monomials of the g_j's affinely

[§] In the literature sparse resultants and (normalized) volumes are defined for *inhomogeneous* (Laurent) polynomials. However, in this paper we will consider those for *homogeneous* (Laurent) polynomials, which are simply defined as those for (Laurent) polynomials dehomogenized with respect to some variable (compare Footnote †† in the proof of Lemma 16). It is easy to show that it does not matter with respect to which variable we dehomogenize. Hence they are well defined. We consider homogeneous (Laurent) polynomials because they allow us to formulate the main theorem in a very succinct way. With a little effort one can also derive a version of the main theorem for inhomogeneous (Laurent) polynomials. But the resulting expression is less elegant.

[¶] In allowing the g_j's to be *Laurent* polynomials instead of polynomials (thus allowing negative exponents) we follow common practice. The purpose of this relaxation is mainly notational and does not essentially contribute to the problem.

We restrict the f_i's to be polynomials. This restrictions ensures that the $f_i \circ (g_1, \ldots, g_n)$'s are again Laurent polynomials.

For the sake of a simple presentation we also assume that all the (Laurent) polynomials have distinct symbolic coefficients. Obviously, the main result can be specialized to numeric coefficients after fixing appropriate sets of supporting monomials for all the (Laurent) polynomials involved.

span over $\mathbb{Z}$ the lattice of integer points of the hyperplane containing the Newton polytope Q. This is nothing but the homogenized version of the standard restrictions on sparse resultants (cf. [CLO98]).

Let $f_i \circ (g_1, \ldots, g_n)$ be the sparse homogeneous Laurent polynomial obtained from f_i by replacing y_j with g_j and let $\mathcal{C}_i$ denote its naturally induced support. Let $\operatorname{Res}_{d_1,\ldots,d_n}(.)$ stand for dense (Macaulay) resultant, $\operatorname{Res}_{\mathcal{B}}(.)$ stand for unmixed sparse resultant and $\operatorname{Res}_{\mathcal{C}_1,\ldots,\mathcal{C}_n}(.)$ stand for mixed sparse resultant. Now we are ready to state the main theorem.

Theorem 1 (Main theorem): *We have*

$$\begin{aligned}
&\operatorname{Res}_{\mathcal{C}_1,\ldots,\mathcal{C}_n}(f_1 \circ (g_1, \ldots, g_n), \ldots, f_n \circ (g_1, \ldots, g_n)) \\
&\qquad\qquad = \operatorname{Res}_{d_1,\ldots,d_n}(f_1, \ldots, f_n)^{\operatorname{Vol}(Q)} \operatorname{Res}_{\mathcal{B}}(g_1, \ldots, g_n)^{d_1 \cdots d_n} .
\end{aligned}$$

Further, Table 1 shows by which factors the arithmetic complexities of the main tasks of sparse resultant computation (for details see Remark 2) are lower for the f_i's and for the g_j's than for the expanded composed Laurent polynomials $f_i \circ (g_1, \ldots, g_n)$.

Table 1: *Factors by which the arithmetic complexities of main tasks of sparse resultant computation are lower for the f_i's and for the g_j's than for the $f_i \circ (g_1, \ldots, g_n)$'s*

Newton matrix extraction:

	time	*space*
f_i's	$V_Q^2 \frac{\log^3\left(d_{\max}^{2n-2} \cdot n^3 \cdot (n-1)^{2n-2} \cdot V_Q^2\right)}{\log^3\left(d_{\max}^{2n-2} \cdot n^3 \cdot (n-1)^{2n-2}\right)}$	$V_Q \frac{\log^2\left(d_{\max}^{n-1} \cdot n^2 \cdot (n-1)^{n-1} \cdot V_Q\right)}{\log^2\left(d_{\max}^{n-1} \cdot n^2 \cdot (n-1)^{n-1}\right)}$
g_j's	$d_{\max}^{2n-2} \frac{\log^3\left(d_{\max}^{2n-2} \cdot n^3 \cdot (n-1)^{2n-2} \cdot V_Q^2\right)}{\log^3\left(n^3 \cdot (n-1)^{2n-2} \cdot V_Q^2\right)}$	$d_{\max}^{n-1} \frac{\log^2\left(d_{\max}^{n-1} \cdot n^2 \cdot (n-1)^{n-1} \cdot V_Q\right)}{\log^2\left(n^2 \cdot (n-1)^{n-1} \cdot V_Q\right)}$

versus $f_i \circ (g_1, \ldots, g_n)$'s

Sparse resultant extraction:

	time	*space*
f_i's	$V_Q^3 \ (n-1)! \frac{\log^2\left(d_{\max}^{3n-3} \cdot n^5 \cdot (n-1)^{2n-2} \cdot V_Q^3 \cdot (n-1)!\right)}{\log^2\left(d_{\max}^{3n-3} \cdot n^5 \cdot (n-1)^{2n-2}\right)}$	$V_Q \frac{\log^2\left(d_{\max}^{n-1} \cdot n^2 \cdot (n-1)^{n-1} \cdot V_Q\right)}{\log^2\left(d_{\max}^{n-1} \cdot n^2 \cdot (n-1)^{n-1}\right)}$
g_j's	$d_{\max}^{3n-3} \frac{\log^2\left(d_{\max}^{3n-3} \cdot n^5 \cdot (n-1)^{2n-2} \cdot V_Q^3 \cdot (n-1)!\right)}{\log^2\left(n^5 \cdot (n-1)^{2n-2} \cdot V_Q^3 \cdot (n-1)!\right)}$	$d_{\max}^{n-1} \frac{\log^2\left(d_{\max}^{n-1} \cdot n^2 \cdot (n-1)^{n-1} \cdot V_Q\right)}{\log^2\left(n^2 \cdot (n-1)^{n-1} \cdot V_Q\right)}$

versus $f_i \circ (g_1, \ldots, g_n)$'s

Remark 2: In Table 1 we compare the *arithmetic* complexities of the main tasks, that is, "Newton matrix computation" and "sparse resultant extraction", for sparse resultant computation, as in [EP97] and [EP01], for the f_i's, g_j's and the expanded composed Laurent polynomials $f_i \circ (g_1, \ldots, g_n)$. We chose the algorithms of [EP97] and [EP01] because they are efficient and their arithmetic complexities have been analyzed thoroughly.

Next, we give brief descriptions of the algorithms of [EP97] and [EP01] and of certain assumptions used in the complexity analysis of Newton matrix computation.

We start with Newton matrix computation. The algorithm for Newton matrix computation is a numeric algorithm. It has a subalgorithm that tests, up to a precision ϵ specified by the user, if certain matrices are invertible. Further, Emiris and Pan restrict the complexity analysis to certain families of systems of Laurent polynomials. In essence, they assume that the absolute value of the lowest and highest degree in each variable of these systems is dominated by the square of the number of columns of the Newton matrices generated by the algorithm. (It would be interesting to find out if the set of systems of equations can be partitioned into a finite number of families such that the systems in each family uniformly fulfill this assumption.) Obviously, we can add three systems of f_i's, g_j's and $f_i \circ (g_1, \ldots, g_n)$'s to any such family without violating this assumption. Further, Emiris and Pan conjecture in [EP97] and [EP01] that the number of rows of any Newton matrix generated by the algorithm is bounded by some constant multiple of the total degree of the corresponding sparse resultant. This assumption is used only in the analysis of the time complexity.

Next we consider sparse resultant extraction. The algorithm, a variant of the so-called division method, extracts the sparse resultant from a suitable (cf. [EP97] and [EP01]) list of maximal minors of Newton matrices. It is a numeric Las Vegas algorithm (for details see [EP97] and [EP01]).

Example 3: We illustrate the notations and the main theorem. Let

$$\begin{aligned}
f_1 &:= a_{1600}\, y_1^6 \;+\; a_{1411}\, y_1^4\, y_2\, y_3 \;+\; a_{1222}\, y_1^2\, y_2^2\, y_3^2 \;+\; a_{1105}\, y_1\, y_3^5 \;+\; a_{1006}\, y_3^6,\\
f_2 &:= a_{2700}\, y_1^7 \;+\; a_{2331}\, y_1^3\, y_2^3\, y_3 \;+\; a_{2142}\, y_1\, y_2^4\, y_3^2 \;+\; a_{2025}\, y_2^2\, y_3^5 \;+\; a_{2070}\, y_2^7,\\
f_3 &:= a_{3900}\, y_1^9 \;-\; a_{3621}\, y_1^6\, y_2^2\, y_3 \;+\; a_{3432}\, y_1^4\, y_2^3\, y_3^2 \;+\; a_{3063}\, y_2^6\, y_3^3 \;+\; a_{3009}\, y_3^9,\\
g_1 &:= b_{1221}\, x_1^2\, x_2^2\, x_3 \;+\; b_{1230}\, x_1^2\, x_2^3 \;+\; b_{1\,-1\,42}\, x_1^{-1}\, x_2^4\, x_3^2 \;+\; b_{1014}\, x_2\, x_3^4,\\
g_2 &:= b_{2221}\, x_1^2\, x_2^2\, x_3 \;+\; b_{2230}\, x_1^2\, x_2^3 \;+\; b_{2\,-1\,42}\, x_1^{-1}\, x_2^4\, x_3^2 \;+\; b_{2014}\, x_2\, x_3^4,\\
g_3 &:= b_{3221}\, x_1^2\, x_2^2\, x_3 \;+\; b_{3230}\, x_1^2\, x_2^3 \;+\; b_{3\,-1\,42}\, x_1^{-1}\, x_2^4\, x_3^2 \;+\; b_{3014}\, x_2\, x_3^4.
\end{aligned}$$

Observe that $n = 3$, $d_1 = 6, d_2 = 7$, $d_3 = 9$, $d_{\max} = 9$, and thus $d_1 \cdot d_2 \cdot d_3 = 378$. Observe that $\mathcal{B} = \left\{x_1^2\, x_2^2\, x_3,\; x_1^2\, x_2^3,\; x_1^{-1}\, x_2^4\, x_3^2,\; x_2\, x_3^4\right\}$ and that $\mathcal{C}_1$ is the set of monomials occurring in $f_1 \circ (g_1, g_2, g_3)$, namely,

$$\begin{gathered}
x_2^{16}x_3^{15}x_1^{-1},\, x_1^5x_2^{14}x_3^{11},\, x_1^6x_2^{19}x_3^5,\, x_1^7x_2^{16}x_3^7,\, x_1^8x_2^{13}x_3^9,\, x_1^6x_2^{11}x_3^{13},\, x_1^{10}x_2^{15}x_3^5,\, x_1^3x_2^{20}x_3^7,\, x_1^4x_2^{17}x_3^9,\, x_1^7x_2^{13}x_3^{10},\\
x_1^8x_2^{10}x_3^{12},\, x_1^3x_2^{18}x_3^9,\, x_1^4x_2^{15}x_3^{11},\, x_2^{13}x_3^{17},\, x_1^{12}x_2^{14}x_3^4,\, x_1^{10}x_2^{12}x_3^8,\, x_1^6x_2^{16}x_3^8,\, x_1\,x_2^{10}x_3^{19},\, x_2^{22}x_3^{11}x_1^{-3},\, x_2^{19}x_3^{13}x_1^{-2},\\
x_1^9x_2^{15}x_3^6,\, x_1^8x_2^{11}x_3^{11},\, x_1^{12}x_2^{12}x_3^6,\, x_1^{12}x_2^{13}x_3^5,\, x_1^9x_2^{14}x_3^7,\, x_1^{10}x_2^{11}x_3^9,\, x_1^6x_2^9x_3^{15},\, x_1^7x_2^{14}x_3^9,\, x_1^{12}x_2^{17}x_3,\, x_1^2x_2^7x_3^{21},\, x_1^6x_2^{17}x_3^7,\\
x_1^{12}x_2^{18},\, x_2^6x_3^{24},\, x_2^{12}x_3^{20}x_1^{-2},\, x_2^{21}x_3^{14}x_1^{-5},\, x_2^{18}x_3^{16}x_1^{-4},\, x_2^{15}x_3^{18}x_1^{-3},\, x_2^{24}x_3^{12}x_1^{-6},\, x_2^9x_3^{22}x_1,\, x_1^4x_2^{10}x_3^{16},\, x_1^3x_2^{13}x_3^{14},\\
x_2^{22}x_3^8,\, x_1\,x_2^{19}x_3^{10},\, x_1^2x_2^{16}x_3^{12},\, x_1^9x_2^{19}x_3^2,\, x_2^{14}x_3^{16},\, x_1^6x_2^{20}x_3^4,\, x_1^7x_2^{17}x_3^6,\, x_1^8x_2^{14}x_3^8,\, x_1^6x_2^{12}x_3^{12},\, x_1^{10}x_2^{16}x_3^4,\, x_1^3x_2^{21}x_3^6,\\
x_1^4x_2^{18}x_3^8,\, x_1^5x_2^{15}x_3^{10},\, x_1\,x_2^{11}x_3^{18},\, x_2^{23}x_3^{10}x_1^{-3},\, x_2^{20}x_3^{12}x_1^{-2},\, x_2^{17}x_3^{14}x_1^{-1},\, x_1^6x_2^{18}x_3^6,\, x_1^8x_2^{12}x_3^{10},\, x_1^6x_2^{10}x_3^{14},\, x_1^{10}x_2^{14}x_3^6,\\
x_1^3x_2^{19}x_3^8,\, x_1^4x_2^{16}x_3^{10},\, x_1^5x_2^{13}x_3^{12},\, x_1^2x_2^8x_3^{20},\, x_1^7x_2^{15}x_3^8,\, x_1^5x_2^{12}x_3^{13},\, x_1^{12}x_2^{15}x_3^3,\, x_1^9x_2^{16}x_3^5,\, x_1^{10}x_2^{13}x_3^7,\, x_1^{12}x_2^{16}x_3^2,\, x_1^4x_2^9x_3^{17},\\
x_1^3x_2^{12}x_3^{15},\, x_2^{21}x_3^9,\, x_1\,x_2^{18}x_3^{11},\, x_1^2x_2^{15}x_3^{13},\, x_1^9x_2^{18}x_3^3,\, x_1^4x_2^8x_3^{18},\, x_1^3x_2^{11}x_3^{16},\, x_2^{20}x_3^{10},\, x_1\,x_2^{17}x_3^{12},\, x_1^2x_2^{14}x_3^{14},\, x_1^9x_2^{17}x_3^4.
\end{gathered}$$

and similarly for $\mathcal{C}_2$ and $\mathcal{C}_3$. The Newton polytope Q of the g_j's is shown in

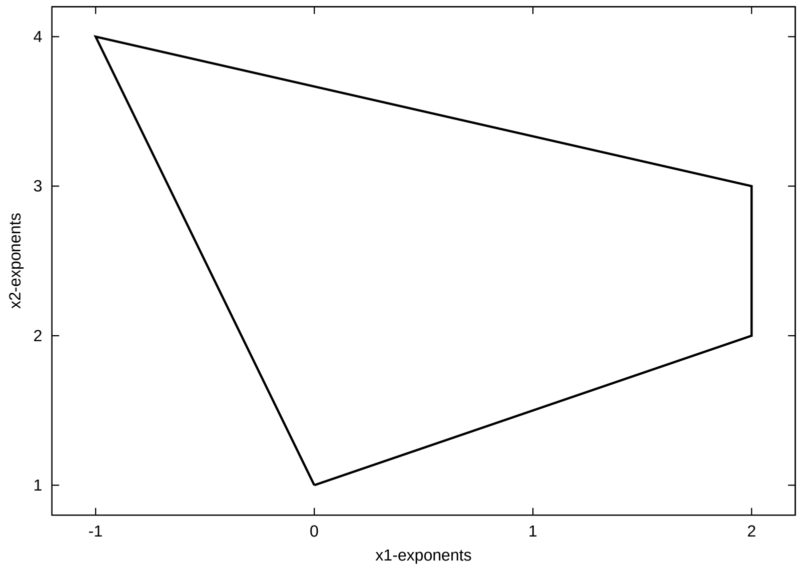

Figure 1: Newton polytope Q of g_1, g_2 and g_3 after orthogonal projection onto (x_1, x_2)-exponent plane

Figure 1. From the figure we see that $\mathrm{Vol}\,(Q) = 10$ and $V_Q = 5$. Thus the main theorem states that

$$\begin{aligned}\mathrm{Res}_{\mathcal{C}_1,\mathcal{C}_2,\mathcal{C}_3}\left(f_1 \circ (g_1, g_2, g_3), f_2 \circ (g_1, g_2, g_3), f_3 \circ (g_1, g_2, g_3)\right) &= \\ &\mathrm{Res}_{6,7,9}\left(f_1, f_2, f_3\right)^{10}\, \mathrm{Res}_{\mathcal{B}}\left(g_1, g_2, g_3\right)^{378}.\end{aligned}$$

Further, the main theorem states the factors of Table 2 for the improved complexities of the main tasks of sparse resultant computation.

Table 2: Approximate factors by which the arithmetic complexities of main tasks of sparse resultant computation are lower for the f_i's and for the g_j's than for the $f_i \circ (g_1, \ldots, g_n)$'s in Example 3

Newton matrix computation:

	time	*space*
f_i's	$5^2 \cdot 1.21 \approx 30$	$5 \cdot 1.20 \approx 6$
g_j's	$9^4 \cdot 1.94 \approx 12770$	$9^2 \cdot 1.84 \approx 150$

versus $f_i \circ (g_1, \ldots, g_n)$'s

Sparse resultant extraction:

	time	*space*
f_i's	$5^3 \cdot 2! \cdot 1.25 \approx 314$	$5 \cdot 1.20 \approx 6$
g_j's	$9^6 \cdot 1.95 \approx 1039609$	$9^2 \cdot 1.84 \approx 150$

versus $f_i \circ (g_1, \ldots, g_n)$'s

Even this simple example illustrates that the use of the main theorem provides a dramatic improvement of efficiency (see Table 2). If one tries to compute the sparse resultant of the composed Laurent polynomials without using the main theorem, then one will first have to expand the composed Laurent polynomials into distributive representation and then compute their sparse resultant. It is expected that computing the sparse resultant of the expanded Laurent polynomials takes a very long time. Moreover the output is expected to be enormous in size (see the huge exponents) and therefore it is expected that using the output in further computations will be difficult. However, using the main theorem we do not have to expand the composed input. We only need to compute the (sparse) resultants of the smaller component polynomials, which can be done much more efficiently (cf. Table 1), calculate the exponents and keep the final output in the compact factored form. Note that we do not have to compute the exponent $\mathrm{Vol}\,(Q)$ separately because current algorithms for sparse resultant computation would calculate the mixed volume of $n-1$ copies of Q, i.e. $\mathrm{Vol}\,(Q)$, along the way, i.e. we get $\mathrm{Vol}\,(Q)$ as a byproduct of the computation without additional effort. Further, note that Table 1 contains ratios of *arithmetic* complexities, which do not consider the coefficient blow up of computations in exact arithmetic. It is expected that, under consideration of the coefficient blow up, the decrease of complexity will be of much higher order than the decrease stated in Table 1.

Remark 4: At first sight it may be surprising that the formula of Theorem 1 contains the *dense* resultant $\mathrm{Res}_{d_1,\ldots,d_n}(f_1,\ldots,f_n)$ of the f_i's instead of their *sparse* resultant. The reader will find the detailed explanation for this phenomenon in the proof of Theorem 1. In short: The composed polynomial $f_i \circ (g_1,\ldots,g_n)$ has the same support as $F_i \circ (g_1,\ldots,g_n)$, where F_i is a dense homogeneous polynomial of the same total degree as f_i. Thus the f_i's must be viewed as dense which introduces the dense resultant in Theorem 1.

3. Proof of the main theorem

Before going into the details of the proof we describe its main structure. In the first four lemmas we will derive a “skeleton” of the main theorem, involving some unknown coefficients and exponents, when the f_i's are restricted to be *dense*. In the following three lemmas we will determine the unknown coefficients and exponents. Finally, we will allow the f_i's to be sparse, proving the main theorem. The dependency of all these lemmas is shown in Figure 2.

Before listing the lemmas, we fix some notations.

Notation 5: Let h be a (sparse) homogeneous (Laurent) polynomial with distinct symbolic coefficients. Then H is the *dense completion* of h, that is, the *dense* homogeneous polynomial with the same total degree as h with distinct symbolic coefficients.

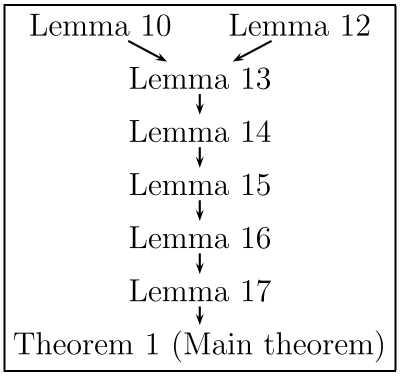

Figure 2: Dependency of the lemmas

Example 6: Consider $h = a\,x_1^2 + b\,x_1\,x_2$. Then we have $H = a\,x_1^2 + b\,x_1\,x_2 + c\,x_2^2$.

Now, we fix how to denote certain leading forms of (Laurent) polynomials.

Notation 7: Let p be any (Laurent) polynomial in the variables $x_1, \ldots, x_n$ with numeric or symbolic coefficients, let ω be a vector in $\mathbb{Z}^n$ and let $\mathcal{E}$ be a set of monomials in $x_1, \ldots, x_n$. The *leading form* of p with respect to ω and $\mathcal{E}$, written as $p_{\mathcal{E}}^{\omega}$, is the maximal part of p whose Newton polytope lies in the face, with ω being an inner normal vector, of the Newton polytope naturally generated by the exponents in $\mathcal{E}$.

Example 8: Let

$$\begin{aligned} p &:= 8\,x_1 + 3\,x_2 + d, \\ \omega &:= (-1, 0)\,, \\ \mathcal{E} &:= \left\{x_1^2 x_2,\, x_1^2,\, x_2,\, 1\right\}. \end{aligned}$$

Figure 3 shows a triangle, the Newton polytope of p, inscribed into a rectangle, the Newton polytope generated by the exponents in $\mathcal{E}$. Observe that the leading form of p with respect to ω and the support of p is $8\,x_1$. However the leading form of p with respect to ω and $\mathcal{E}$, written as $p_{\mathcal{E}}^{\omega}$, is 0.

Finally, we fix a notation for the support sets of the dense homogeneous polynomial F_i, the dense completion of the sparse homogeneous polynomial f_i, composed with the sparse homogeneous polynomials g_j.

Notation 9: Let $\mathcal{D}_i$ be the set of naturally induced supporting Laurent monomials of $F_i \circ (g_1, \ldots, g_n)$.

Now we are ready to state and prove lemmas. In essence the next lemma is the so-called "vanishing theorem for resultants" stated by Rojas in [Roj99a]

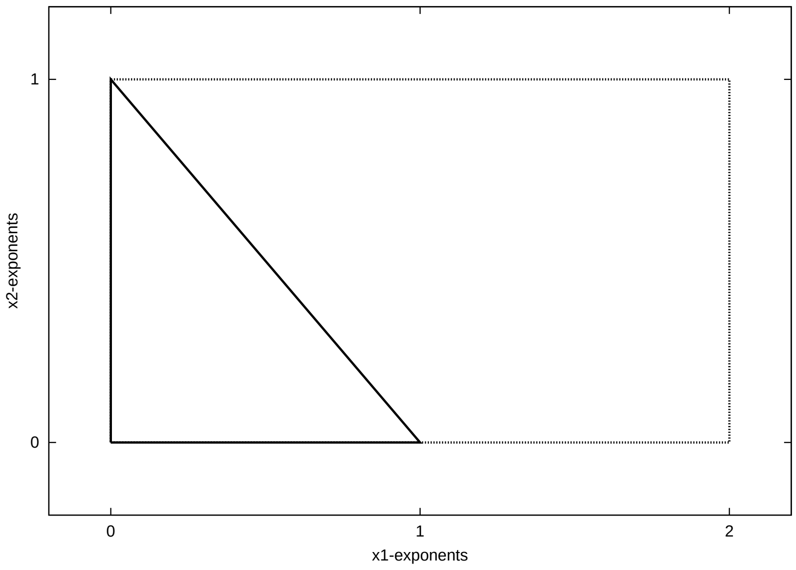

Figure 3: A triangle, the Newton polytope of p, inscribed into a rectangle, the Newton polytope generated by exponents in $\mathcal{E}$

in different language. The vanishing theorem tells us when exactly the mixed sparse resultant vanishes (cf. also [CLO98] for unmixed sparse resultants). Rojas presents the theorem using the language of toric varieties (cf. [CLO98]) and divisors (cf. [Ful98]). However, for this paper a different presentation is more suitable. Thus we give a lemma expressed in a different formalism.

Let $h_1, \ldots, h_n$ be homogeneous Laurent polynomials in the variables $x_1, \ldots, x_n$ with supports $\mathcal{E}_1, \ldots, \mathcal{E}_n$ and with distinct symbolic coefficients. Again we make the usual assumption ([CLO98]) that the dimension of the Newton polytopes of the h_i's is $n-1$.

Lemma 10: *For all specializations, with complex numbers, of the coefficients of the h_j's, we have* $\operatorname{Res}_{\mathcal{E}_1,\ldots,\mathcal{E}_n}(h_1, \ldots, h_n) = 0$ *iff there is a vector ω such that the leading forms $h^{\omega}_{\mathcal{E}_1}, \ldots, h^{\omega}_{\mathcal{E}_n}$ of $h_1, \ldots, h_n$ have a common zero in $(\mathbb{C}\setminus\{0\})^n$.*

Proof: We assume that the reader is familiar with the notions of cycle (cf. [Ful98]), glueing, scheme, spectrum and coordinate ring (cf. [Sha94a], [Sha94b]) and toric varieties (cf. [Ful93], [GKZ94], [CLO98]).

Let $h^{\mathrm{d}}_1, \ldots, h^{\mathrm{d}}_n$ denote dehomogenizations of the *unspecialized* $h_1, \ldots, h_n$, without loss of generality, with respect to x_n with supports $\mathcal{E}^{\mathrm{d}}_1, \ldots, \mathcal{E}^{\mathrm{d}}_n$. For the rest of the proof we *specialize the coefficients* of the h_j's with some arbitrary but fixed complex numbers. Note that for the proof it is crucial that we have fixed some specializations of the coefficients. The "vanishing theorem for resultants" ([Roj99a]) tells us that

$$\operatorname{Res}_{\mathcal{E}_1,\ldots,\mathcal{E}_n}(h_1, \ldots, h_n) = 0$$

iff

$$\mathcal{D}_{R_1+\cdots+R_n}\left(\left(h_1^{\mathrm{d}},\ldots,h_n^{\mathrm{d}}\right),\left(R_1,\ldots,R_n\right)\right) \neq \emptyset,$$

where $\mathcal{D}_{R_1+\cdots+R_n}\left(\left(h_1^{\mathrm{d}},\ldots,h_n^{\mathrm{d}}\right),\left(R_1,\ldots,R_n\right)\right)$ stands for the underlying scheme of a certain cycle (cf. [Roj99a]) and R_j stands for the Newton polytope naturally generated by $\mathcal{E}_j^{\mathrm{d}}$. For a precise definition of the operator $\mathcal{D}$ see [Roj99a] and [Roj99b]. Rojas represents the scheme

$$\mathcal{D}_{R_1+\cdots+R_n}((h_1^{\mathrm{d}},\ldots,h_n^{\mathrm{d}}),(R_1,\ldots,R_n))$$

(cf. [Roj99a], Lemma 5.1, and [Roj99b], Lemma 3) by the standard glueing of certain affine schemes lying in the usual affine pieces (cf. [Ful93]) that cover the toric variety constructed from the polytope $R_1+\cdots+R_n$.[‖] Following Rojas and Fulton using slightly simplified notation, these affine pieces and affine schemes can be constructed as follows. Let $v_1,\ldots,v_l$ be the vertices of the polytope $R_1+\cdots+R_n$ and let $\sigma_i^\vee$ be $\sigma_i'-v_i$, where σ_i' denotes the inner cone of the polytope $R_1+\cdots+R_n$ formed by the supporting hyperplanes of $R_1+\cdots+R_n$ that pass through v_i. Then an affine piece U_i of the toric variety is given as the points of the spectrum of the ring $\mathbb{C}\left[\sigma_i^\vee\cap\mathbb{Z}^{n-1}\right]$ (cf. [Ful93]). It can be shown (cf. [Ful93]) that the toric variety constructed from the polytope $R_1+\cdots+R_n$ is isomorphic to an appropriate glueing of $U_1,\ldots,U_l$. Further, let $w_j^{(i)}$ denote the vertex of R_j with the same inner normal vector as v_i. Such vertices exist because the Minkowski sum $R_1+\cdots+R_n$ is compatible with each R_j (cf. [Roj99a]). Then, according to [Roj99a], Lemma 5.1, and [Roj99b], Lemma 3, on U_i the scheme $\mathcal{D}_{R_1+\cdots+R_n}((h_1^{\mathrm{d}},\ldots,h_n^{\mathrm{d}}),(R_1,\ldots,R_n))$ is represented by the ideal generated by $x^{-w_1^{(i)}}h_1^{\mathrm{d}},\ldots,x^{-w_n^{(i)}}h_n^{\mathrm{d}}$ in $\mathbb{C}\left[\sigma_i^\vee\cap\mathbb{Z}^{n-1}\right]$. Therefore

$$\mathrm{Res}_{\mathcal{E}_1,\ldots,\mathcal{E}_n}\left(h_1,\ldots,h_n\right) = 0$$

iff there is a U_i such that $x^{-w_1^{(i)}}h_1^{\mathrm{d}},\ldots,x^{-w_n^{(i)}}h_n^{\mathrm{d}}$, viewed as functions on U_i in the coordinate ring $\mathbb{C}\left[\sigma_i^\vee\cap\mathbb{Z}^{n-1}\right]$, have a common zero in U_i.

Now fix U_i and let $p\in U_i$ be a point such that $x^{-w_1^{(i)}}h_1^{\mathrm{d}},\ldots,x^{-w_n^{(i)}}h_n^{\mathrm{d}}$ vanish on p. Then the coordinates of p and their power products (cf. [Ful93], the proposition on p. 54) are $x^e=\xi^e$, for $e\in\left(\tau_i^\vee\cap\mathbb{Z}^{n-1}\right)\setminus\{0\}$ and for some $\xi\in\left(\mathbb{C}\setminus\{0\}\right)^{n-1}$ and $x^e=0$, for $e\notin\left(\tau_i^\vee\cap\mathbb{Z}^{n-1}\right)\setminus\{0\}$, where $\tau_i^\vee$ is a face of the cone $\sigma_i^\vee$ with inner normal vector ω. Let j be arbitrary but fixed. It follows that $x^{-w_j^{(i)}}h_j^{\mathrm{d}}$ vanishes on p iff the leading form $h^{\mathrm{d}\,\omega}_{j\,\mathcal{E}_j^{\mathrm{d}}}$ vanishes when $x_1,\ldots,x_{n-1}$ is replaced by $\xi_1,\ldots,\xi_{n-1}$. Therefore and vice versa, the leading forms $h^{\mathrm{d}\,\omega}_{1\,\mathcal{E}_1^{\mathrm{d}}},\ldots,h^{\mathrm{d}\,\omega}_{n\,\mathcal{E}_n^{\mathrm{d}}}$ have a common zero in $\left(\mathbb{C}\setminus\{0\}\right)^{n-1}$. It is easy to see that these leading forms can be obtained by dehomogenizing, with respect to x_n, certain leading forms, with respect to the same vector, of $h_1,\ldots,h_n$. Thus and vice versa, these appropriate leading forms of $h_1,\ldots,h_n$ have a common zero in $\left(\mathbb{C}\setminus\{0\}\right)^n$. □

[‖] Rojas also shows how to canonically represent this scheme on the intersection of these affine pieces, but this is not needed in the proof.

Next we would like to understand how the leading forms of composed Laurent polynomials are related to the leading forms of the component (Laurent) polynomials. At first it seems that there is no meaningful relationship at all. In fact, it is well known that the shapes of Newton polytopes are very unstable under elementary operations like unions, Minkowski sums, etc. However it turns out that there is some relationship – a very natural one. Let's have a look at an example.

Example 11: Let $p := y_1^2 + y_2y_3$ and

$$q_j \;:=\; \begin{array}{ccc} x_1^{-1}x_2^3x_3^3 & + & x_1^2x_2^3 \\ + & & + \\ x_1^{-1}x_3^6 & + & x_1^2x_3^3, \end{array}$$

for $j = 1, 2, 3$. The Newton polytope of the q_j's is a rhombus. Instead of drawing this rhombus we have arranged the monomials of the q_j's in a square which is supposed to represent the rhombus. The exponents of the edges and vertices of this square lie in the corresponding edges and vertices of the rhombus. The Newton polytope of $p \circ (q_1, q_2, q_3)$ is also a rhombus. We represent $p \circ (q_1, q_2, q_3)$ in the same manner as the q_j's, namely,

$$p \circ (q_1, q_2, q_3) \;=\; \begin{array}{ccccc} 2x_1^{-2}x_2^6x_3^6 & + & 4x_1^{-2}x_2^3x_3^9 & + & 2x_1^{-2}x_2^6x_3^6 \\ + & & + & & + \\ 4x_1x_2^6x_3^3 & + & 8x_1x_2^3x_3^6 & + & 4x_1x_3^9 \\ + & & + & & + \\ 2x_1^4x_2^6 & + & 4x_1^4x_2^3x_3^3 & + & 2x_1^4x_3^6. \end{array}$$

For example, the leading form of $p \circ (q_1, q_2, q_3)$, with respect to $\omega = (1, -2, 1)$ and the naturally induced Laurent monomials of $p \circ (q_1, q_2, q_3)$, is the first row of $p \circ (q_1, q_2, q_3)$. It can be decomposed as

$$p \circ \left(x_1^{-1}x_2^3x_3^3 + x_1^2x_2^3,\;\; x_1^{-1}x_2^3x_3^3 + x_1^2x_2^3,\;\; x_1^{-1}x_2^3x_3^3 + x_1^2x_2^3\right),$$

where $x_1^{-1}x_2^3x_3^2 + x_1^2x_2^3x_3$ is the first row of the q_j's, that is, the leading form of the q_j's with respect to ω and the Laurent monomials of the q_j's. In fact, similar statements are true for any other leading form of $p \circ (q_1, q_2, q_3)$.

In order to state generally what we have observed in the above example, let F be a dense homogeneous polynomial in the variables $y_1, \ldots, y_n$ with distinct symbolic coefficients distinct from the symbolic coefficients of any other Laurent polynomial in this paper. We state the lemma only for (Laurent) polynomials with distinct *symbolic* coefficients because, for fixed support sets, it is trivial to specialize the lemma.

Lemma 12: *We have*[**]

$$(F \circ (g_1, \ldots, g_n))_{\mathcal{E}}^{\omega} \;=\; F \circ (g_{1\mathcal{B}}^{\;\omega}, \ldots, g_{n\mathcal{B}}^{\;\omega}),$$

[**] We formulate the lemma for dense F's because we only need it for such polynomials. It is easy to see that the lemma is also true for sparse polynomials.

where $\mathcal{E}$ is the set of Laurent monomials contained in $F \circ (g_1, \ldots, g_n)$.

Proof: Since $F \circ (g_1, \ldots, g_n) = \sum_{\alpha_1+\cdots+\alpha_n=d} a_\alpha g_1^{\alpha_1} \cdots g_n^{\alpha_n}$, for some symbolic coefficients a_α and some d, we have

$$(F \circ (g_1, \ldots, g_n))_{\mathcal{E}}^{\omega} = \sum_{\alpha_1+\cdots+\alpha_n=d} a_\alpha (g_1^{\alpha_1} \cdots g_n^{\alpha_n})_{\mathcal{E}}^{\omega}.$$

We show that

$$(g_1^{\alpha_1} \cdots g_n^{\alpha_n})_{\mathcal{E}}^{\omega} = ({g_1}_{\mathcal{B}}^{\omega})^{\alpha_1} \cdots ({g_n}_{\mathcal{B}}^{\omega})^{\alpha_n} .$$

Note that

$$\begin{aligned} g_1^{\alpha_1} \cdots g_n^{\alpha_n} &= ({g_1}_{\mathcal{B}}^{\omega} + h_1)^{\alpha_1} \cdots ({g_n}_{\mathcal{B}}^{\omega} + h_n)^{\alpha_n} \\ &= ({g_1}_{\mathcal{B}}^{\omega})^{\alpha_1} \cdots ({g_n}_{\mathcal{B}}^{\omega})^{\alpha_n} + \sum_{0 \neq (\beta_1,\ldots,\beta_n) \leq (\alpha_1,\ldots,\alpha_n)} ({g_1}_{\mathcal{B}}^{\omega})^{\alpha_1-\beta_1} h_1^{\beta_1} \cdots ({g_1}_{\mathcal{B}}^{\omega})^{\alpha_1-\beta_n} h_n^{\beta_n}, \end{aligned}$$

for some fixed $h_1, \ldots, h_n$ whose Laurent monomials have exponents different from those in ${g_1}_{\mathcal{B}}^{\omega}, \ldots, {g_n}_{\mathcal{B}}^{\omega}$. Let $(l, .)$ be a linear form defined on $\mathbb{Z}^n$ such that the Newton polytope of the g_j's is contained in the halfspace $\{e \mid (l, e) \leq r\}$, for some $r \in \mathbb{Z}$, and such that the hyperplane $\{e \mid (l, e) = r\}$ contains the exponents of the ${g_j}_{\mathcal{B}}^{\omega}$'s. By well known properties of the Newton polytope (cf. [CLO98], Exercise 3, p. 318) and the Minkowski sum (cf. [CLO98], Exercise 12, p. 325) we know that the supporting hyperplane of the exponents of the Laurent monomials that are contained in the leading form $(g_1^{\alpha_1} \cdots g_n^{\alpha_n})_{\mathcal{E}}^{\omega}$ is $\{e \mid (d \cdot l, e) = d \cdot r\}$ and the exponents of the Laurent monomials that are contained in $({g_1}_{\mathcal{B}}^{\omega})^{\alpha_1} \cdots ({g_n}_{\mathcal{B}}^{\omega})^{\alpha_n}$ lie in this hyperplane as well. Therefore the Laurent monomials, together with their coefficients, of $({g_1}_{\mathcal{B}}^{\omega})^{\alpha_1} \cdots ({g_n}_{\mathcal{B}}^{\omega})^{\alpha_n}$ are contained in the leading form $(g_1^{\alpha_1} \cdots g_n^{\alpha_n})^{\omega}$. Now, fix a tuple $(\beta_1, \ldots, \beta_n) \neq 0$. The exponents of the Laurent monomials in the h_j's are contained in the set $\{e \mid (l, e) < r\}$ and thus the exponents of the Laurent monomials in $(g_1^{\omega})^{\alpha_1-\beta_1} h_1^{\beta_1} \cdots (g_1^{\omega})^{\alpha_1-\beta_n} h_n^{\beta_n}$ are contained in the set $\{e \mid (d \cdot l, e) < d \cdot r\}$. Therefore the Laurent monomials in $({g_1}_{\mathcal{B}}^{\omega})^{\alpha_1-\beta_1} h_1^{\beta_1} \cdots ({g_1}_{\mathcal{B}}^{\omega})^{\alpha_1-\beta_n} h_n^{\beta_n}$ are not contained in the leading form $(F \circ (g_1, \ldots, g_n))_{\mathcal{E}}^{\omega}$.

Now, since composition commutes with addition, it follows

$$\begin{aligned} (F \circ (g_1, \ldots, g_n))_{\mathcal{E}}^{\omega} &= \sum_{\alpha_1+\cdots+\alpha_n=d} a_\alpha \, ({g_1}_{\mathcal{B}}^{\omega})^{\alpha_1} \cdots ({g_n}_{\mathcal{B}}^{\omega})^{\alpha_n} \\ &= F \circ ({g_1}_{\mathcal{B}}^{\omega}, \ldots, {g_n}_{\mathcal{B}}^{\omega}) . \end{aligned}$$

□

Next we make the connection between the vanishing of the sparse resultant of composed Laurent polynomials and the vanishing of the (sparse) resultants of the components.

LEMMA 13: *For all specializations, with complex numbers, of the coefficients of the* F_i*'s and of the* g_j*'s,*

$$\begin{array}{c}\operatorname{Res}_{\mathcal{D}_1,\ldots,\mathcal{D}_n}\left(F_1\circ(g_1,\ldots,g_n),\ldots,F_n\circ(g_1,\ldots,g_n)\right) \;=\; 0 \\ \textit{implies} \\ \operatorname{Res}_{\mathcal{B}}(g_1,\ldots,g_n) \;=\; 0 \quad \textit{or} \quad \operatorname{Res}_{d_1,\ldots,d_n}(F_1,\ldots,F_n) \;=\; 0.\end{array}$$

Proof: We would like to apply Lemma 10 to the sparse resultant of specializations of the $F_i\circ(g_1,\ldots,g_n)$'s, but first we have to show that the dimension of the Newton polytope of $F_i\circ(g_1,\ldots,g_n)$, i.e. the Newton polytope naturally generated by $\mathcal{D}_i$, is $n-1$, which we will do now. Note that for this paragraph it is crucial that the F_i's and g_j's have distinct symbolic coefficients. We observe that $F_i\circ(g_1,\ldots,g_n)$ contains only summands of the form $g_1^{\alpha_1}\cdots g_n^{\alpha_n}$ with some distinct symbolic coefficient, where $\alpha_1+\cdots+\alpha_n = d_i$. From the distributivity of multiplication and addition it follows immediately that all summands of this form contain the same Laurent monomials with, in general, different coefficients. Therefore the Newton polytope of $F_i\circ(g_1,\ldots,g_n)$ is the same as the Newton polytope of any $g_1^{\alpha_i}\cdots g_n^{\alpha^n}$, where $\alpha_1+\cdots+\alpha_n = d_i$. By well known properties of multiplication of polynomials and the Minkowski sum (cf. [CLO98]), the Newton polytope of $g_1^{\alpha_i}\cdot\cdots\cdot g_n^{\alpha^n}$ is $d_i\cdot Q$. Thus we have shown that the dimension of the Newton polytope of $F_i\circ(g_1,\ldots,g_n)$ is $n-1$.

Now, suppose

$$\operatorname{Res}_{\mathcal{D}_1,\ldots,\mathcal{D}_n}\left(F_1\circ(g_1,\ldots,g_n),\ldots,F_n\circ(g_1,\ldots,g_n)\right) \;=\; 0,$$

for arbitrary but fixed *specializations*, with complex numbers, of the coefficients of the F_i's and of the g_j's. Note that for the rest of the proof it is crucial that we have fixed some specializations of the coefficients. Then by Lemma 10 and by Lemma 12, which can be trivially specialized, there are appropriate leading forms

$$\left(F_i\circ(g_1,\ldots,g_n)\right)^{\omega}_{\mathcal{D}_i} \;=\; F_i\circ\left({g_1}^{\omega}_{\mathcal{B}},\ldots,{g_n}^{\omega}_{\mathcal{B}}\right)$$

of $F_1\circ(g_1,\ldots,g_n),\ldots,F_n\circ(g_1,\ldots,g_n)$ that have a common zero $(\xi_1,\ldots,\xi_n)\in(\mathbb{C}\setminus\{0\})^n$. This implies that either

$${g_1}^{\omega}_{\mathcal{B}}(\xi_1,\ldots,\xi_n)=0,\ldots,{g_n}^{\omega}_{\mathcal{B}}(\xi_1,\ldots,\xi_n)=0$$

or

$$F_1(\upsilon_1,\ldots,\upsilon_n)=0,\ldots,F_n(\upsilon_1,\ldots,\upsilon_n)=0,$$

where $0\neq(\upsilon_1,\ldots,\upsilon_n) := \left({g_1}^{\omega}_{\mathcal{B}}(\xi_1,\ldots,\xi_n),\ldots,{g_n}^{\omega}_{\mathcal{B}}(\xi_1,\ldots,\xi_n)\right)$. Therefore

$$\operatorname{Res}_{\mathcal{B}}(g_1,\ldots,g_n) \;=\; 0 \quad \text{or} \quad \operatorname{Res}_{d_1,\ldots,d_n}(F_1,\ldots,F_n) \;=\; 0.$$

□

Now we show that the sparse resultant of composed Laurent polynomials is the product of some powers of the (sparse) resultants of the component (Laurent) polynomials. We show this only for *dense* outer polynomials.

LEMMA 14:

$$\begin{aligned}\mathrm{Res}_{\mathcal{D}_1,\ldots,\mathcal{D}_n}(F_1\circ(g_1,\ldots,g_n),\ldots,F_n\circ(g_1,\ldots,g_n))\\ = \lambda\ \mathrm{Res}_{d_1,\ldots,d_n}(F_1,\ldots,F_n)^{\mu}\ \mathrm{Res}_{\mathcal{B}}(g_1,\ldots,g_n)^{\nu},\end{aligned}$$

where $\lambda\in\mathbb{C}$ *and* μ *and* ν *are non negative integers.*

Proof: Hilbert's Nullstellensatz is the key. By Lemma 13, for all specializations, with complex numbers, of the coefficients of the F_i's and of the g_j's,

$$\mathrm{Res}_{\mathcal{B}}(F_1\circ(g_1,\ldots,g_n),\ldots,F_n\circ(g_1,\ldots,g_n)) = 0$$

implies that

$$(\mathrm{Res}_{d_1,\ldots,d_n}(F_1,\ldots,F_n)\cdot\mathrm{Res}_{\mathcal{B}}(g_1,\ldots,g_n)) = 0.$$

Note that for this proof it is crucial that the F_i's and g_j's have distinct symbolic coefficients. Further, note that the (sparse) resultants

$$\begin{gathered}\mathrm{Res}_{\mathcal{D}_1,\ldots,\mathcal{D}_n}(F_1\circ(g_1,\ldots,g_n),\ldots,F_n\circ(g_1,\ldots,g_n)),\\ \mathrm{Res}_{d_1,\ldots,d_n}(F_1,\ldots,F_n)\quad\text{and}\quad\mathrm{Res}_{\mathcal{B}}(g_1,\ldots,g_n)\end{gathered}$$

are polynomials in the symbolic coefficients of the F_i's and g_j's. Thus, by Hilbert's Nullstellensatz, we have that

$$(\mathrm{Res}_{d_1,\ldots,d_n}(F_1,\ldots,F_n)\cdot\mathrm{Res}_{\mathcal{B}}(g_1,\ldots,g_n))$$

is in the radical of $\mathrm{Res}_{\mathcal{D}_1,\ldots,\mathcal{D}_n}(F_1\circ(g_1,\ldots,g_n),\ldots,F_n\circ(g_1,\ldots,g_n))$. Therefore

$$\begin{aligned}p\cdot\mathrm{Res}_{\mathcal{D}_1,\ldots,\mathcal{D}_n}(F_1\circ(g_1,\ldots,g_n),\ldots,F_n\circ(g_1,\ldots,g_n))\\ = (\mathrm{Res}_{d_1,\ldots,d_n}(F_1,\ldots,F_n)\ \mathrm{Res}_{\mathcal{B}}(g_1,\ldots,g_n))^{\delta},\end{aligned}$$

where $p\neq 0$ is a polynomial in the symbolic coefficients of the F_i's and g_j's and δ is a positive integer. Since $\mathrm{Res}_{d_1,\ldots,d_n}(F_1,\ldots,F_n)$ and $\mathrm{Res}_{\mathcal{B}}(g_1,\ldots,g_n)$ are irreducible polynomials, the polynomial $\mathrm{Res}_{\mathcal{D}_1,\ldots,\mathcal{D}_n}(F_1\circ(g_1,\ldots,g_n),\ldots,F_n\circ(g_1,\ldots,g_n))$ must be, up to a constant factor, a product of certain non negative powers of $\mathrm{Res}_{d_1,\ldots,d_n}(F_1,\ldots,F_n)$ and $\mathrm{Res}_{\mathcal{B}}(g_1,\ldots,g_n)$ and thus we have shown the lemma. □

Now we determine the unknown coefficient λ in the previous lemma.

Lemma 15: *We have*

$$\begin{aligned}\operatorname{Res}_{\mathcal{D}_1,\ldots,\mathcal{D}_n}(F_1\circ(g_1,\ldots,g_n),\ldots,F_n\circ(g_1,\ldots,g_n))\\ = \operatorname{Res}_{d_1,\ldots,d_n}(F_1,\ldots,F_n)^{\mu}\operatorname{Res}_{\mathcal{B}}(g_1,\ldots,g_n)^{\nu},\end{aligned}$$

i.e. $\lambda = 1$.

Proof: In the equality of the previous lemma we specialize the F_i to $y_i^{d_i}$ and we get

$$\operatorname{Res}_{\mathcal{D}_1,\ldots,\mathcal{D}_n}\left(g_1^{d_1},\ldots,g_n^{d_n}\right) = \lambda \operatorname{Res}_{d_1,\ldots,d_n}\left(y_1^{d_1},\ldots,y_n^{d_n}\right)^{\mu}\operatorname{Res}_{\mathcal{B}}(g_1,\ldots,g_n)^{\nu}.$$

Note that the set of Laurent monomials contained in the $F_i\circ(g_1,\ldots,g_n)$ is $\prod_{k=1}^{d_i}\mathcal{B}$; in detail: in the proof of Lemma 13 we saw that $g_1^{\alpha_1}\cdots g_n^{\alpha_n}$ contains the same Laurent monomials as $F_i\circ(g_1,\ldots,g_n)$ and thus its set of supporting Laurent monomials is $\prod_{k=1}^{d_i}\mathcal{B}$. This observation allows us to apply the product formula presented in [PS93] to $\operatorname{Res}_{\mathcal{D}_1,\ldots,\mathcal{D}_n}\left(g_1^{d_1},\ldots,g_n^{d_n}\right)$. We get

$$\operatorname{Res}_{\mathcal{B}}(g_1,\ldots,g_n)^{\kappa} = \lambda \operatorname{Res}_{d_1,\ldots,d_n}\left(y_1^{d_1},\ldots,y_n^{d_n}\right)^{\mu}\operatorname{Res}_{\mathcal{B}}(g_1,\ldots,g_n)^{\nu},$$

for some $\kappa > 0$. On the right hand side of this equality we have, by definition of dense (Macaulay) resultant,

$$\operatorname{Res}_{d_1,\ldots,d_n}\left(y_1^{d_1},\ldots,y_n^{d_n}\right) = 1.$$

The other factors in the equality are not zero. Therefore

$$\operatorname{Res}_{\mathcal{B}}(g_1,\ldots,g_n)^{\kappa-\nu} = \lambda \in \mathbb{C}.$$

The sparse resultant $\operatorname{Res}_{\mathcal{B}}(g_1,\ldots,g_n)$ is a non constant polynomial in the symbolic coefficients of $g_1,\ldots,g_n$. Therefore $\kappa-\nu=0$ and thus $\lambda=1$. □

In order to determine the remaining unknowns μ and ν, we use the multihomogeneity of the (sparse) resultant (cf. [CLO98], p. 343). First we derive the exponent μ.

Lemma 16: *We have*

$$\begin{aligned}\operatorname{Res}_{\mathcal{D}_1,\ldots,\mathcal{D}_n}(F_1\circ(g_1,\ldots,g_n),\ldots,F_n\circ(g_1,\ldots,g_n))\\ = \operatorname{Res}_{d_1,\ldots,d_n}(F_1,\ldots,F_n)^{\operatorname{Vol}(Q)}\operatorname{Res}_{\mathcal{B}}(g_1,\ldots,g_n)^{\nu},\end{aligned}$$

i.e. $\mu = \operatorname{Vol}(Q)$.

Proof: In the equality of the previous lemma, we specialize F_1 to $c \cdot F_1$, for some new constant c distinct from any other symbolic constant used until now, and get

$$\begin{aligned} &\mathrm{Res}_{\mathcal{D}_1,\ldots,\mathcal{D}_n}\left(c \cdot F_1 \circ (g_1,\ldots,g_n), F_2 \circ (g_1,\ldots,g_n),\ldots,F_n \circ (g_1,\ldots,g_n)\right) \\ &\qquad = \mathrm{Res}_{d_1,\ldots,d_n}\left(c \cdot F_1, F_2,\ldots,F_n\right)^{\mu}\, \mathrm{Res}_{\mathcal{B}}\left(g_1,\ldots,g_n\right)^{\nu}. \end{aligned}$$

By the multi-homogeneity of the dense (Macaulay) resultant we know that

$$\begin{aligned} \mathrm{Res}_{\mathcal{B}}\left(c \cdot F_1, F_2,\ldots,F_n\right) &= c^{\mathrm{MV}(d_2 \cdot S,\ldots,d_n \cdot S)} \cdot \mathrm{Res}_{d_1,\ldots,d_n}\left(F_1,\ldots,F_n\right) \\ &= c^{d_2 \cdots d_n\, \mathrm{MV}(S,\ldots,S)} \cdot \mathrm{Res}_{d_1,\ldots,d_n}\left(F_1,\ldots,F_n\right) \\ &= c^{d_2 \cdots d_n} \cdot \mathrm{Res}_{d_1,\ldots,d_n}\left(F_1,\ldots,F_n\right), \end{aligned}$$

where S denotes the $(n-1)$-dimensional standard simplex and $\mathrm{MV}(.)$ denotes the usual $(n-1)$-dimensional real mixed volume.

Similarly, by the multi-homogeneity of the sparse resultant, we have

$$\begin{aligned} &\mathrm{Res}_{\mathcal{D}_1,\ldots,\mathcal{D}_n}\left(c \cdot F_1 \circ (g_1,\ldots,g_n), F_2 \circ (g_1,\ldots,g_n),\ldots,F_n \circ (g_1,\ldots,g_n)\right) \\ &= c^{d_2 \cdots d_n\, \mathrm{MV}\left(Q^{\mathrm{d}},\ldots,Q^{\mathrm{d}}\right)} \\ &\qquad \mathrm{Res}_{\mathcal{D}_1,\ldots,\mathcal{D}_n}\left(F_1 \circ (g_1,\ldots,g_n), F_2 \circ (g_1,\ldots,g_n),\ldots,F_n \circ (g_1,\ldots,g_n)\right), \end{aligned}$$

Q^{d} denotes the Newton polytope of $g_1,\ldots,g_n$ dehomogenized w.r.t. any fixed variable x_k.[††]

By comparing powers in the specialized equality

$$\mu = \mathrm{MV}\left(Q^{\mathrm{d}},\ldots,Q^{\mathrm{d}}\right) = \mathrm{Vol}(Q).$$

□

Finally we derive the exponent ν and obtain the formula of Theorem 1 restricted to sparse resultants of dense homogeneous polynomials composed with sparse homogeneous Laurent polynomials.

[††] It does not matter which variable x_k we choose because $\mathrm{MV}\left(Q^{\mathrm{d}},\ldots,Q^{\mathrm{d}}\right)$, which equals $(n-1)!$ times the $(n-1)$-dimensional volume of Q^{d}, is invariant under the choice of dehomogenizing variable x_k. This can be seen easily: Let Q^{d_1} and Q^{d_2}, resp., be the Newton polytopes of the g_j's dehomogenized, without loss of generality, with respect to x_1 and x_2, resp. Equivalently, $Q^{d_1} = P_1(Q)$, where P_1 is the projection mapping $(v_1,v_2,v_3,\ldots,v_n) \mapsto (0,v_2,v_3,\ldots,v_n)$, and $Q^{d_2} = P_2(Q)$, where P_2 is the projection mapping $(v_1,v_2,v_3,\ldots,v_n) \mapsto (v_1,0,v_3,\ldots,v_n)$. We want to show that the $(n-1)$-dimensional volumes of Q^{d_1} and Q^{d_2} are equal. Equivalently, we show that the $(n-1)$-dimensional volumes of $R_1 := Q^{d_1} - \frac{e}{n}(0,1,1,\ldots,1)$ and $R_2 := Q^{d_2} - \frac{e}{n}(1,0,1,\ldots,1)$ are equal, where e is the total degree of the g_j's. Equivalently, we show that the $(n-1)$-dimensional volumes of R_1 and $T(R_2)$ are equal, where $T : (v_1,v_2,v_3,\ldots,v_n) \mapsto (v_2,v_1,v_3,\ldots,v_n)$. It is easy to see that $T(R_2) = S(R_1)$, where $S : (v_1,v_2,v_3,\ldots,v_n) \mapsto (v_1,-v_2-\cdots-v_n,v_3,\ldots,v_n)$. Note that R_1 and $S(R_1)$ are contained in the same $(n-1)$-dimensional subspace defined by the equation $v_1 = 0$. Obviously S restricted to this subspace is an automorphism whose determinant is -1. Therefore the $(n-1)$-dimensional volumes of R_1 and $S(R_1)$ are equal. Thus we have shown that the $(n-1)$-dimensional volumes of Q^{d_1} and Q^{d_2} are equal.

Lemma 17: *We have*

$$\operatorname{Res}_{\mathcal{D}_1,\ldots,\mathcal{D}_n}(F_1\circ(g_1,\ldots,g_n),\ldots,F_n\circ(g_1,\ldots,g_n)) \\ = \operatorname{Res}_{d_1,\ldots,d_n}(F_1,\ldots,F_n)^{\operatorname{Vol}(Q)}\operatorname{Res}_{\mathcal{B}}(g_1,\ldots,g_n)^{d_1\cdots d_n},$$

i.e. $\nu = d_1\cdots d_n$.

Proof: In the equality of the previous lemma, we specialize g_j to $c\cdot g_j$, for $j = 1,\ldots,n$, for some new constant c distinct from any other symbolic constant used until now, and get

$$\operatorname{Res}_{\mathcal{D}_1,\ldots,\mathcal{D}_n}(F_1\circ(c\cdot g_1,\ldots,c\cdot g_n),\ldots,F_n\circ(c\cdot g_1,\ldots,c\cdot g_n)) \\ = \operatorname{Res}_{d_1,\ldots,d_n}(F_1,\ldots,F_n)^{\operatorname{Vol}(Q)}\operatorname{Res}_{\mathcal{B}}(c\cdot g_1,\ldots,c\cdot g_n)^{\nu}.$$

By the multi-homogeneity of the sparse resultant, we have

$$\operatorname{Res}_{\mathcal{B}}(c\cdot g_1,\ldots,c\cdot g_n) = c^{n\operatorname{Vol}(Q)}\cdot\operatorname{Res}_{\mathcal{B}}(g_1,\ldots,g_n).$$

Further, since F_i is homogeneous of total degree d_i, we have $F_i\circ(c\cdot g_1,\ldots,c\cdot g_n) = c^{d_i}\cdot F_i\circ(g_1,\ldots,g_n)$. Therefore, by the multi-homogeneity of the sparse resultant,

$$\operatorname{Res}_{\mathcal{D}_1,\ldots,\mathcal{D}_n}(F_1\circ(c\cdot g_1,\ldots,c\cdot g_n),\ldots,F_n\circ(c\cdot g_1,\ldots,c\cdot g_n)) \\ = c^{n\,d_1\cdots d_n\operatorname{Vol}(Q)}\cdot\operatorname{Res}_{\mathcal{D}_1,\ldots,\mathcal{D}_n}(F_1\circ(g_1,\ldots,g_n),\ldots,F_n\circ(g_1,\ldots,g_n)).$$

By comparing powers in the specialized equality, $\nu = d_1\cdots d_n$. □

Proof of theorem 1 (Main theorem):

Now we are ready to prove the main theorem, that is, we show the formula and we prove the complexities.

Formula: We generalize the previous lemma in order to allow dense outer polynomials. We specialize the formula of Lemma 17 to

$$\operatorname{Res}_{\mathcal{C}_1,\ldots,\mathcal{C}_n}(f_1\circ(g_1,\ldots,g_n),\ldots,f_n\circ(g_1,\ldots,g_n)) \\ = \operatorname{Res}_{d_1,\ldots,d_n}(f_1,\ldots,f_n)^{\operatorname{Vol}(Q)}\operatorname{Res}_{\mathcal{B}}(g_1,\ldots,g_n)^{d_1\cdots d_n}.$$

It is clear that we can specialize $\operatorname{Res}_{d_1,\ldots,d_n}(F_1,\ldots,F_n)^{\operatorname{Vol}(Q)}\operatorname{Res}_{\mathcal{B}}(g_1,\ldots,g_n)^{d_1\cdots d_n}$ to $\operatorname{Res}_{d_1,\ldots,d_n}(f_1,\ldots,f_n)^{\operatorname{Vol}(Q)}\operatorname{Res}_{\mathcal{B}}(g_1,\ldots,g_n)^{d_1\cdots d_n}$. But can we specialize

$$\operatorname{Res}_{\mathcal{D}_1,\ldots,\mathcal{D}_n}(F_1\circ(g_1,\ldots,g_n),\ldots,F_n\circ(g_1,\ldots,g_n))$$

to

$$\operatorname{Res}_{\mathcal{C}_1,\ldots,\mathcal{C}_n}(f_1\circ(g_1,\ldots,g_n),\ldots,f_n\circ(g_1,\ldots,g_n))?$$

In other words, is the set $\mathcal{D}_i$ of Laurent monomials of $F_i \circ (g_1, \ldots, g_n)$ stable under a specialization of F_i to f_i, that is, $\mathcal{D}_i = \mathcal{C}_i$? The answer is yes and we will show it. We know that $F_i \circ (g_1, \ldots, g_n)$ consists of a positive number of summands of the form $g_1^{\alpha_1} \cdot \ldots \cdot g_n^{\alpha_n}$ with distinct symbolic coefficients, where $\alpha_1 + \cdots + \alpha_n = d_i$. Likewise $f_i \circ (g_1, \ldots, g_n)$ consists of a positive number of summands of the very same form. In the proof of Lemma 13 we have already seen that all such summands contain the same Laurent monomials. Therefore $\mathcal{D}_i = \mathcal{C}_i$.

Complexities: The complexity analysis is based on the algorithms in [EP97] and [EP01]. Let Q^{d} denote the Newton polytope of the *unspecialized* dehomogenizations, w.l.o.g. with respect to x_n, of the Laurent polynomials g_j. From now on, we assume that all the (Laurent) polynomials f_i and g_j are *specialized.* We will compute orders of the arithmetic time and space complexities of Newton matrix computation as well as sparse resultant extraction for the f_i's, g_j's and $f_i \circ (g_1, \ldots, g_n)$'s in terms of n, $d_{\max}$ and V_Q. Then we will compare the ratios of these complexities. For this complexity analysis, we apply the general *sparse* resultant algorithms even to the *dense* polynomials f_i. However, in practice, for the dense polynomials f_i, one might prefer to use more efficient algorithms that are designed only for dense (Macaulay) resultant computation.

Next we introduce some notation and make an important remark about the presentation of the results of [EP97] and [EP01]. Most of the complexities in [EP97] and [EP01] are given in terms of $\mathrm{O}^*(\chi)$, standing for $\mathrm{O}(\chi \log^v \chi)$, for some fixed constant v independent from χ. We have computed the relevant exponents v because we want to compare the complexities as explicitly as possible. Computing the relevant exponents v is easy and can be done by analyzing the proofs in [EP01]. Further, we want to follow [EP97] and [EP01] as closely as possible in presenting the complexities. Therefore we introduce a notation that is similar to [EP97] and [EP01] and that allows us to precisely specify the value of v as well. That is, we let $\mathrm{O}_v^*(\chi)$ stand for $\mathrm{O}(\chi \log^v \chi)$. Further, we point out that we mean "$\mathrm{O}(.)$" when writing "of order".

We start with Newton matrix computation. Under the assumptions of Theorem 6.2 and Corollary 6.4 of [EP97] (cf. also Remark 2 of the present paper) the arithmetic time and space complexities of an efficient algorithm for Newton matrix computation of some specialized Laurent polynomials $h_1, \ldots, h_n$ are $\mathrm{O}_3^*(c^2 n)$ and $\mathrm{O}_2^*(cn)$, resp., where c is the number of columns of the Newton matrix that is generated by the algorithm.[‡‡] As described in [EC95], the number of columns are bounded, from above, by the sum, over k, of the number of integer points in the Minkowski sum of the Newton polytopes of $h_1, \ldots, h_{k-1}, h_{k+1}, \ldots, h_n$. First, we compute an order of this bound for the f_i's. Let S_{d_i} denote the standard

---

[‡‡] In [EP97], Emiris and Pan give another algorithm with arithmetic time complexity $\mathrm{O}^*(acn)$, where a is the number of rows of the Newton matrix. We don't use this algorithm because currently there seems to be no formula, in terms of the sparsity parameters, like mixed volumes of Newton polytopes, etc., for a tight bound of a available.

simplex of dimension $n-1$ with edge length d_i. The number of columns is bounded, from above, by the sum, over k, of the number of integer points in $\sum_{i\neq k} S_{d_i} \subseteq (n-1)\, S_{d_{\max}}$. Thus the number of columns is less than or equal to n times the number of integer points in $(n-1)\, S_{d_{\max}}$. Now, by Theorem 5.1 and Corollary 5.2 of [Erh67], n times the number of integer points in $(n-1)\, S_{d_{\max}}$ is of order $d_{\max}^{n-1} \cdot n \cdot (n-1)^{n-1} \cdot \frac{\mathrm{Vol}(S_1)}{(n-1)!} = d_{\max}^{n-1} \cdot n \cdot (n-1)^{n-1}$. Second, we compute an order of the number of columns for the g_j's. The number of columns is bounded, from above, by the sum, over k, of the number of integer points in $\sum_{i\neq k} Q^{\mathrm{d}} = (n-1)\, Q^{\mathrm{d}}$. Thus the number of columns is less than or equal to n times the number of integer points in $(n-1)\, Q^{\mathrm{d}}$. Similar to above, the number of integer points is of order $n \cdot (n-1)^{n-1} \cdot V_Q$. Third, we consider the number of columns for the $f_i \circ (g_1, \ldots, g_n)$'s. In the proof of Lemma 13 we have seen that the Newton polytope of $f_i \circ (g_1, \ldots, g_n)$ is $d_i\, Q$. Similar to the f_i's, the number of columns of the Newton matrix is less than or equal to a bound of order $d_{\max}^{n-1} \cdot n \cdot (n-1)^{n-1} \cdot V_Q$. Therefore the arithmetic time and space complexities of Newton matrix computation are as shown in Table 3. Thus the ratios of the arithmetic time and space complexities of Newton matrix computation for the $f_i \circ (g_1, \ldots, g_n)$'s and the f_i's are $V_Q^2 \frac{\log^3\left(d_{\max}^{2n-2} \cdot n^3 \cdot (n-1)^{2n-2} \cdot V_Q^2\right)}{\log^3\left(d_{\max}^{2n-2} \cdot n^3 \cdot (n-1)^{2n-2}\right)}$ and $V_Q \frac{\log^2\left(d_{\max}^{n-1} \cdot n^2 \cdot (n-1)^{n-1} \cdot V_Q\right)}{\log^2\left(d_{\max}^{n-1} \cdot n^2 \cdot (n-1)^{n-1}\right)}$, resp., the ratios for the $f_i \circ (g_1, \ldots, g_n)$'s and the g_j's are $d_{\max}^{2n-2} \frac{\log^3\left(d_{\max}^{2n-2} \cdot n^3 \cdot (n-1)^{2n-2} \cdot V_Q^2\right)}{\log^3\left(n^3 \cdot (n-1)^{2n-2} \cdot V_Q^2\right)}$ and $d_{\max}^{n-1} \frac{\log^2\left(d_{\max}^{n-1} \cdot n^2 \cdot (n-1)^{n-1} \cdot V_Q\right)}{\log^2\left(n^2 \cdot (n-1)^{n-1} \cdot V_Q\right)}$, resp.

Table 3: Arithmetic complexities of Newton matrix computation

	argument χ for	
	arithmetic time complexity $\mathrm{O}_3^*(\chi)$	arithmetic space complexity $\mathrm{O}_2^*(\chi)$
f_i's	$d_{\max}^{2n-2} \cdot n^3 \cdot (n-1)^{2n-2}$	$d_{\max}^{n-1} \cdot n^2 \cdot (n-1)^{n-1}$
g_j's	$n^3 \cdot (n-1)^{2n-2} \cdot V_Q^2$	$n^2 \cdot (n-1)^{n-1} \cdot V_Q$
$f_i \circ (g_1, \ldots, g_n)$'s	$d_{\max}^{2n-2} \cdot n^3 \cdot (n-1)^{2n-2} \cdot V_Q^2$	$d_{\max}^{n-1} \cdot n^2 \cdot (n-1)^{n-1} \cdot V_Q$

Now we turn to sparse resultant extraction. Under the assumptions of Theorem 7.1 of [EP97] (cf. also Remark 2 of the present paper) the arithmetic time and space complexities of the division method for sparse resultant extraction of some specialized Laurent polynomials $h_1, \ldots, h_n$ are $\mathrm{O}_2^*(c^2 n^2 \deg R)$ and $\mathrm{O}_2^*(cn)$, resp., where c is the number of columns of the Newton matrix and $\deg R$ is the total degree of the sparse resultant of $h_1, \ldots, h_n$ in the coefficients of the h_i's. Note that we utilize the division method and not the GCD method because the GCD method has a more restricted set of input Laurent polynomials (cf. [EP97] and [CE93]) and we want to make a comparison of the complexities under as few restrictions as possible. For the order $\mathrm{O}_2^*(cn)$ of the space complexity, we have already computed the ratios for the composed Laurent polynomials and their components. It remains to compute an order of the total degree $\deg R$ and the ratios of the arithmetic time complexities $\mathrm{O}_2^*\left(c^2 n^2 \deg R\right)$. First, we consider $f_1, \ldots, f_n$. Since the dense (Macaulay) resultant is multihomogeneous in the coefficients of f_k of degree $\mathrm{MV}\left(S_{d_1}, \ldots, S_{d_{k-1}}, S_{d_{k+1}}, \ldots, S_{d_n}\right)$, the total degree of the dense (Macaulay) resultant of the f_i's is

$$\begin{aligned}\sum_{k=1}^{n} \mathrm{MV}\left(S_{d_1}, \ldots, S_{d_{k-1}}, S_{d_{k+1}}, \ldots, S_{d_n}\right) & \\ = \sum_{k=1}^{n} d_1 \cdots d_{k-1} \cdot d_{k+1} \cdots d_n \ \mathrm{MV}\left(S_1, \ldots, S_1\right) & \\ \leq\ n \cdot d_{\max}^{n-1}. &\end{aligned}$$

Similarly, the total degrees of the sparse resultants of the g_j's and the $f_i \circ (g_1, \ldots, g_n)$'s are less than or equal to $n \cdot (n-1)!\, V_Q$ and $n \cdot d_{\max}^{n-1} \cdot (n-1)!\, V_Q$, resp. Therefore the arithmetic time and space complexities of sparse resultant extraction by the division method are as shown in Table 4. Thus the ratios of the arithmetic time and space complexities of sparse resultant extraction by the division method for the $f_i \circ (g_1, \ldots, g_n)$'s and the f_i's are $V_Q^3 \cdot (n-1)! \frac{\log^2\left(d_{\max}^{3n-3} \cdot n^5 \cdot (n-1)^{2n-2} \cdot V_Q^3 \cdot (n-1)!\right)}{\log^2\left(d_{\max}^{3n-3} \cdot n^5 \cdot (n-1)^{2n-2}\right)}$ and $V_Q \frac{\log^2\left(d_{\max}^{n-1} \cdot n^2 \cdot (n-1)^{n-1} \cdot V_Q\right)}{\log^2\left(d_{\max}^{n-1} \cdot n^2 \cdot (n-1)^{n-1}\right)}$, resp., the ratios for the $f_i \circ (g_1, \ldots, g_n)$'s and the g_j's are $d_{\max}^{3n-3} \frac{\log^2\left(d_{\max}^{3n-3} \cdot n^5 \cdot (n-1)^{2n-2} \cdot V_Q^3 \cdot (n-1)!\right)}{\log^2\left(n^5 \cdot (n-1)^{2n-2} \cdot V_Q^3 \cdot (n-1)!\right)}$ and $d_{\max}^{n-1} \frac{\log^2\left(d_{\max}^{n-1} \cdot n^2 \cdot (n-1)^{n-1} \cdot V_Q\right)}{\log^2\left(n^2 \cdot (n-1)^{n-1} \cdot V_Q\right)}$, resp.

Table 4: Arithmetic complexities of sparse resultant extraction by division method

	argument χ for	
	arithmetic time complexity $\mathrm{O}_2^*(\chi)$	arithmetic space complexity $\mathrm{O}_2^*(\chi)$
f_i's	$d_{\max}^{3n-3} \cdot n^5 \cdot (n-1)^{2n-2}$	$d_{\max}^{n-1} \cdot n^2 \cdot (n-1)^{n-1}$
g_j's	$n^5 \cdot (n-1)^{2n-2} \cdot V_Q^3 \cdot (n-1)!$	$n^2 \cdot (n-1)^{n-1} \cdot V_Q$
$f_i \circ (g_1, \ldots, g_n)$'s	$d_{\max}^{3n-3} \cdot n^5 \cdot (n-1)^{2n-2} \cdot V_Q^3 \cdot (n-1)!$	$d_{\max}^{n-1} \cdot n^2 \cdot (n-1)^{n-1} \cdot V_Q$

Thus we have shown the main theorem. $\square$

4. Conclusion

In this paper we studied sparse resultants of composed polynomials

$$f_1 \circ (g_1, \ldots, g_n), \ldots, f_n \circ (g_1, \ldots, g_n),$$

where the g_j's are unmixed. We have essentially shown that the sparse resultant of the composed polynomials is the product of certain powers of the (sparse) resultants of the f_i's and of the g_j's. Applying this theorem in computing sparse resultants of composed polynomials is dramatically more efficient than computing the sparse resultant of the expanded polynomials without utilizing the composition structure.

Acknowledgment

We thank the anonymous referees for suggestions on improving the paper.

References

[BEM00] L. Busé, M. Elkadi, and B. Mourrain. Generalized resultants over unirational algebraic varieties. *J. Symbolic Computation*, 29(4-5):515–526, 2000.

[BS99] 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).

[Cay48] A. Cayley. On the theory of elimination. *Cambridge and Dublin Math. J.*, 3:116–120, 1848.

[CDS98] E. Cattani, A. Dickenstein, and B. Sturmfels. Residues and resultants. *J. Math. Sci. Univ. Tokyo*, 5(1):119–148, 1998.

[CE93] J. Canny and I. Emiris. An efficient algorithm for the sparse mixed resultant. In G. Cohen, T. Mora, and O. Moreno, editors, *Proc. Intern. Symp. on Applied Algebra, Algebraic Algor. and Error-Corr. Codes*, number 263 in Lect. Notes in Comp. Science, pages 89–104. Springer-Verlag, 1993.

[Cha90] M. Chardin. *Contributions à l'algèbre commutative effective et à la théorie de l'élimination.* PhD thesis, Université Paris VI, 1990.

[CKY89] J. Canny, E. Kaltofen, and Lakshman Y. Solving systems of nonlinear polynomial equations faster. In *Proc. ACM-SIGSAM 1989 Internat. Symp. Symbolic Algebraic Comput. ISSAC'89*, pages 121–128. ACM, 1989.

[CLO98] D. Cox, J. Little, and D. O'Shea. *Using Algebraic Geometry.* Springer Verlag, New York, Berlin, Heidelberg, 1998.

[CMW95] 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.

[DD00] C. D'Andrea and A. Dickenstein. Explicit formulas for the multivariate resultant. In *Proc. Mega 2000*, 2000. To appear.

[Dix08] A. L. Dixon. The eliminant of three quantics in two independent variables. *Proc. Lond. Math. Soc.*, 7:49–69, 1908.

[EC95] I. Emiris and J. Canny. Efficient incremental algorithms for the sparse resultant and mixed volume. *J. Symbolic Computation*, 20(2):117–149, 1995.

[EP97] I. Emiris and V. Pan. The structure of sparse resultant matrices. In *Proc. Int. Symp. on Symbolic and Algebraic Computation (ISSAC)*. ACM Press, 1997.

[EP01] I. Emiris and V. Pan. Symbolic and numeric methods for exploiting structure in constructing resultant matrices. Preprint, June 2001.

[Erh67] E. Erhart. Sur un problème de géométrie diophantienne linéaire. I. *J. Reine Angew. Math.*, 226:1–29, 1967.

[Ful93] W. Fulton. *Introduction to Toric Varieties.* Number 131 in Annals of Mathematics Studies. Princeton University Press, Princeton, New Jersey, 1993.

[Ful98] W. Fulton. *Intersection Theory.* Springer-Verlag, Berlin Heidelberg New York, 2 edition, 1998.

[GKZ94] I. M. Gelfand, M. M. Kapranov, and A. V. Zelevinsky. *Discriminants, Resultants and Multidimensional Determinants.* Birkhäuser, Boston, 1994.

[GV91] 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.

[Hon97] H. Hong. Subresultants under composition. *J. Symbolic Computation*, 23(4):355–365, 1997.

[Hon98] H. Hong. Groebner basis under composition. I. *J. Symbolic Computation*, 25(5):643–663, 1998.

[Jou91] J. P. Jouanolou. Le formalisme du résultant. *Adv. Math.*, 90, 1991.

[KS96] 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.

[LS99] R. Lewis and P. Stiller. Solving the recognition problem for six lines using the Dixon resultant. *Math. Comput. Simulation*, 49(3):205–219, 1999.

[Mac16] F. S. Macaulay. *The algebraic theory of modular systems.* Cambridge Mathematical Library, 1916.

[MC93] D. Manocha and J. Canny. Multipolynomial resultant algorithms. *J. Symbolic Computation*, 15(2):99–122, 1993.

[NW97] G. Nakos and R. M. Williams. Eliminiation with the Dixon resultant. *Mathematica for Education and Research*, 6/3:11–21, 1997.

[PS93] P. Pedersen and B. Sturmfels. Product formulas for resultants and Chow forms. *Mathematische Zeitschrift*, 214:377–396, 1993.

[Roj99a] 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.

[Roj99b] J. M. Rojas. Toric intersection theory for affine root counting. *J. Pure and Applied Algebra*, 136(1):67–100, March 1999.

[Sha94a] I. R. Shafarevich. *Basic Algebraic Geometry*, volume 1. Springer-Verlag, Berlin Heidelberg New York, 2nd edition, 1994.

[Sha94b] I. R. Shafarevich. *Basic Algebraic Geometry*, volume 2. Springer-Verlag, Berlin Heidelberg New York, 2nd edition, 1994.

[vAHU83] A. von Aho, J. E. Hopcroft, and J. D. Ullman. *Data Structures and Algorithms.* Addison-Wesley, 1983.