RESULTANTS OF COMPOSED POLYNOMIALS

By

MANFRED MINIMAIR

A dissertation submitted to the graduate faculty of
North Carolina State University
in partial fullfilment of the
requirements for the Degree of
Doctor of Philosophy

APPLIED MATHEMATICS /
CONCENTRATION IN COMPUTATIONAL MATHEMATICS

Raleigh, North Carolina
February 2000

APPROVED BY:

Hoon Hong
Chair of advisory committee

Erich Kaltofen

Dinesh Manocha

Michael Singer

Abstract

MINIMAIR, MANFRED. Resultants of Composed Polynomials. (Under the direction of Hoon Hong.)

The objective of this research has been to develop methods for computing resultants of composed polynomials, efficiently, by utilizing their composition structure. By the resultant of several polynomials in several variables (one fewer variables than polynomials) we mean an irreducible polynomial in the coefficients of the polynomials that vanishes if they have a common zero. By a composed polynomial we mean the polynomial obtained from a given polynomial by replacing each variable by a polynomial.

The main motivation for this research comes from the following observations: Resultants of polynomials are frequently computed in many areas of science and in applications because they are fundamentally utilized in solving systems of polynomial equations. Further, polynomials arising in science and applications are often composed because humans tend to structure knowledge modularly and hierarchically. Thus, it is important to have theories and software libraries for

efficiently computing resultants of composed polynomials.

However, most existing mathematical theories do not adequately support composed polynomials and most algorithms as well as software libraries ignore the composition structure, thus suffering from enormous blow up in space and time. Thus, it is important to develop theories and software libraries for efficiently computing resultants of composed polynomials.

The main finding of this research is that resultants of composed polynomials can be nicely factorized, namely, they can be factorized into products of powers of the resultants of the component polynomials and of some of their parts. These factorizations can be utilized to compute resultants of composed polynomials with dramatically improved efficiency.

Dedication

I dedicate this work to my parents, Alfred and Doris, and my brothers Gerald and Hannes.

Biography

Manfred Minimair was born in Wels, Austria. He received his M.S. degree in Applied Mathematics & Mathematical Computer Science from Johannes Kepler University, Linz, Austria, and Research Institute for Symbolic Computation, Hagenberg, Austria, in 1997. He received his Ph.D. in Applied Mathematics / Concentration in Computational Mathematics from North Carolina State University, Raleigh, North Carolina, USA, in 2001.

Acknowledgements

I thank my advisor Prof. Hoon Hong for his guidance and for the many hours he has spent teaching me research and many practical aspects, such as writing research proposals, writing scientific papers, preparing talks, etc. I also thank Prof. Erich Kaltofen, Prof. Dinesh Manocha and Prof. Micheal Singer, members of my Ph.D. committee, for their support. Moreover, I thank Prof. Erich Kaltofen for spending time with us students during our weekly lunches. Through our discussions during these lunches I learnt a lot about mathematical research and life in USA, which made my transition from Austria much easiser.

This research was partially supported by NSF project "Computing with composed functions", NSF CCR-9972527. I greatly appreciate the Department of Mathematics as a whole and the Symbolic Solutions Group for the supportive environment they have provided. I thank April Jackson, the graduate secretary, for dilligently answering all my questions about the administrative matters of Ph.D. study. Further, I thank Jack Perry, with whom I have shared my office, for computing some huge Macaulay resultants for me.

Further, I thank Prof. Chris Brown, Prof. Mark Giesbrecht, Prof. Serkan Hosten, Prof. George Nakos, Prof. Greg Reid, Prof. David Saunders, Prof. Bernd Sturmfels and Prof. Chee Yap for discussions on matters related to my Ph.D. research.

I thank my dad Alfred, my mom Doris, my brothers Gerald and Hannes and all other members of my family for all their support. Moreover, I thank them for making possible the visit to Yellowstone Park, which helped refreshing my mind and recharging my energy after my first year in the strenuous Ph.D. program. I thank my dad for saving me much time by ironing my clothes and by going shopping for me, when he visited me. I thank my mom for making my work much more enjoyable by sending, via e-mail, recipes, because if I don't eat good food I can't work well, and for saving me much time by cleaning up my appartment when she visited me. I thank Gerald for sending me the book "Komm Süßer Tod" by Wolf Haas. This book covers a very special aspect of Austria, namely the emergency medical services of Austria (which are organized very differently from the American services), in which I have enjoyed participating and which I have been missing. Reading the book made me happy and thus helped me to stay focused on my work. I thank Hannes for answering many questions about the maintainance of my computer, which saved me much time. I thank my aunt Erni Minimair and my uncle Franz Minimair for the money they gave to me and which has been very useful for me. I thank my aunt Lilo Stugger for finding relatives in USA. Knowing that I am not completely remote from my family made me happy and helped me to stay focused on my work. I thank my uncle Günter Stugger and my aunt Lilo for the nice graphic calculator which has served me very well. Further, let me tell you that my cousin Erik Stugger is an expert in fitness. I thank him for being such a good example for me. We all know that the struggle for intellectual achievements is easier when being fit physically.

Further, I thank my friends for all their support. I greatly appreciate Pauline Hong, my advisor's wife, for inviting me to stay at her home for the first few weeks and for repeatedly inviting me for lunch and dinner throughout my Ph.D. program and for introducing me to many friendly North Carolinnians. All this was very important because it made my transition to USA much easier and therefore I could better concentrate on my work. Morover, I thank John and Susan Haws for making my transition to USA much easier, inspiring my thoughts and refreshing my mind by sharing with me delicious American dinners. Moreover, I thank Axelle Person for passing on, when leaving USA, to me a very nice appartment, in which living and working is pleasant. Moreover, I very much appreciate Lucy Traunmüller, Roland Traunmüller, Karl Laukenberger, Gustav Gurtbichel and Patrick for maintaining contact and sending many e-mails from Austria. I thank Lucy for vivid stories about Spanish life and culture. Reading the stories made me feel like being at home in Europe even though I was miles away. All this made me happy which helped me to better concentrate on my work. I thank Gustav for providing me with translations of excellent Hungarian poems which I enjoyed in my spare free time and which helped me to recharge my energy and refresh my mind in between tough days of discovering and proving theorems. Further, I don't thank Roland Traunmüller for coping with his spectacular car crash surprisingly well. However, I point out that I am really happy about it. I would not have enjoyed finishing the thesis if he had been injured severely. Moreover, I thank Patrick for discussions, which were very refreshing and inspiring and thus helped my work very much.

Contents

List of Tables

List of Figures

Chapter 1

Overview

1.1 Motivation

Resultants are fundamental in solving systems of polynomial equations (cf. [Buc70], [WBLR85], [Cav86], [AS88], [Mis93], [VVC94], [Win96], [Vas98], [Pfa99], [Tay00], [Yap00]) and inequations (cf. [HLS95], [Bro00], [Dor00]) and thus have been extensively studied (cf. [Dix08], [Mac16], [Cay48], [Col71], [CKY89], [Cha90], [GVLRR90], [GV91], [MC93], [KS96], [NW97], [ZCG98], [LS99], [DD00], [BEM00]). Recently the research is focused on utilizing the sparsity structure (cf. also [LS95]) of polynomials which are prevelant in almost all real life problems, yielding a generalized resultant, named the sparse resultant (cf. Definition 1.1, [PS93], [GKZ94], [EP97], [CLO98], [CDS98], [Roj99a], [CE00]). Since Chapters 3, 4 and 5 of this thesis deal with sparse resultants and Chapter 2 deals with dense (Macaulay) resultants, which can be viewd as special sparse resultants, we give, for the convenience of the reader, a definition of sparse resultant.

Definition 1.1 ([PS93],[GKZ94]) Let $\mathcal{C}_i := \{\gamma_{i1}, \ldots, \gamma_{ik_i}\}$, where $\gamma_{ij} \in \mathbb{Z}^{n-1}$, be a set of integer tuples and let $h_i := c_{i1}\, x^{\gamma_{i1}} + \cdots + c_{ik_i}\, x^{\gamma_{ik_i}}$, where $c_{ij} \in \mathbb{C}$ and $x = (x_1, \ldots, x_{n-1})$, be a Laurent polynomial in variables[1] x_j with support $\mathcal{C}_i$, for $i = 1, \ldots, n$. Further, let $Z \subseteq \mathbb{C}^{k_1} \times \cdots \times \mathbb{C}^{k_n}$ be the algebraic closure ot the set of all tuples (c_{ij}) for which $h_1, \ldots, h_n$ have a common zero in the algebraic torus $(\mathbb{C}^*)^{n-1}$ and note that, if Z is a hypersurface, then Z is the set of zeros of an irreducible polynomial with integer coefficients (cf. [PS93]).

If Z is a hypersurface then the sparse resultant $\mathrm{Res}_{\mathcal{C}_1,\ldots,\mathcal{C}_n}$ is defined, up to sign, to be the primitive irreducible polynomial whose set of zeros is Z. Otherwise, the sparse resultant $\mathrm{Res}_{\mathcal{C}_1,\ldots,\mathcal{C}_n}$ is defined to be the constant 1. Further, $\mathrm{Res}_{\mathcal{C}_1,\ldots,\mathcal{C}_n}(h_1, \ldots, h_n) \in \mathbb{C}$ is defined to be the complex number obtained by evaluating the sparse resultant polynomial $\mathrm{Res}_{\mathcal{C}_1,\ldots,\mathcal{C}_n}$ at the coefficients of the Laurent polynomials $h_1, \ldots, h_n$.

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 dense or sparse polynomials iteratively. This is because large scale engineering systems are almost always designed by composing modular components hierarchically, naturally resulting in mathematical models

[1]One can also define sparse resultant for certain Laurent polynomials in k variables, where $k \neq n-1$. These Laurent polynomials can be transformed into Laurent polynomials in $n-1$ varibles by a suitable variable transformation (cf. [PS93], [GKZ94]).

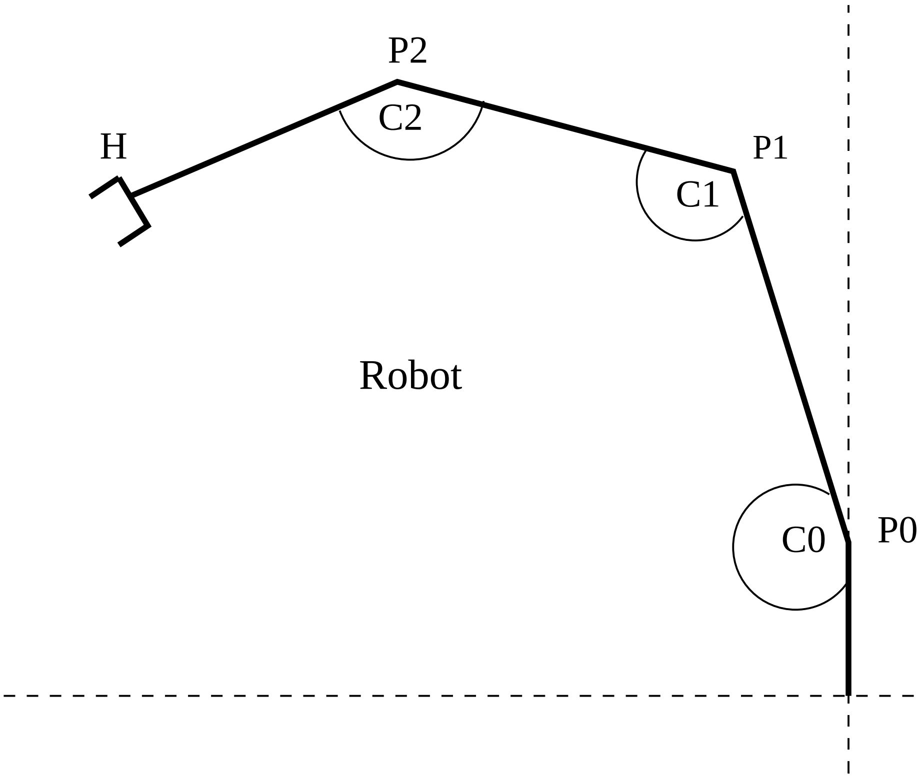

Figure 1.1: Composition in robotics

involving composed polynomials. Because of this, the inherent composition structure is already known or may be recovered (cf. [vW95], [vzGGR99], [KLZ96]). Thus we think that it is important to investigate how to utilize the inherent composition structure as well (cf. also [Jou91], [CMW95], [Hon96], [KS96], [KS97], [Hon97], [Hon98], [GM98], and [BS99]).

Example 1.2 We give an example from robotics showing how composition can arise.

Figure 1.1 shows the simplified diagram of an industrial robot. The dashed lines in Figure 1.1 represent Cartesian coordinate axes. The industrial robot consists of four segements in between three joints, that are labelled by P0, P1 and P2, and the hand H of the industrial robot. The joints are flexible vertically, that is, the segments can be moved up and down. The angles between the segments are specified by some parameters C0, C1 and C2.

In order to determine how different assignments for the parameters C0, C1 and C2 for the angles affect the position of the hand H, one wants to compute the position of the hand in terms of the parameters. Usually one proceeds stepwise. Firstly, one computes the position of the joint P1 in terms of the position of the joint P0 and the parameter C0, that is, $\mathrm{P1} = f_1(\mathrm{P0}, \mathrm{C0})$, for some function f_1. Secondly, one computes the position of the joint P2 in terms of the position of the joint P1 and the parameter C1, that is, $\mathrm{P2} = f_2(\mathrm{P1}, \mathrm{C1})$, for some function f_2. Subsituting the formula for P1, one obtains $\mathrm{P2} = f_2(f_1(\mathrm{P0}, \mathrm{C0}), \mathrm{C1})$. Similarly, one computes the position of the hand H in terms of the position of the joint P2 and the parameter C2. By subsituting for P2, one obtains $\mathrm{H} = f_3(f_2(f_1(\mathrm{P0}, \mathrm{C0}), \mathrm{C1}), \mathrm{C2})$, for some function f_3. Obviously, H is given by a nesting of the functions f_3, f_2 and f_1, which can also be viewed as a certain composition structure.

Table 1.1: Cases of composed polynomials

	$\boldsymbol{f_i}$**'s**	$\boldsymbol{g_j}$**'s**
Case 1	dense	dense
	Chapter 2, Dense Resultant of Composed Polynomials	
Case 2	sparse	sparse same supports
	Chapter 3, Sparse Resultant of Composed Polynomials I	
Case 3	sparse same supports	sparse
	Chapter 4, Sparse Resultant of Composed Polynomials II	
Case 4	*sparse*	*sparse*
	???	

In this regard a fundamental question is: *What happens to resultants under composition?* That is, is the resultant of composed polynomials in any way related to the resultants of the component polynomials?

We consider certain cases of composed polynomials $f_i \circ (g_1, \ldots, g_n)$. These cases are shown in Table 1.1. The most general case of composed polynomials, Case 4 in Table 1.1, is not subject of this thesis. It would be very interesting to study this case.

In the following sections we give an overview over the main results of the thesis. For the following sections we assume that the reader is familiar with the notions of dense (Macaulay) resultant, sparse resultant, support of sparse

Laurent polynomials, mixed volume, integer lattice and normalized volume of Newton polytope (cf. [CLO98], [GKZ94], [PS93]). There are different definitions of normalized volume in the literature. We follow the definition given in [PS93]. Algorithms for volume computation can be found in [Min97].

1.2 Dense Resultant of Composed Polynomials

The main question of Chapter 2 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 chapter 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.

1.3 Sparse Resultant of Composed Polynomials I

The main question of Chapter 3 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 chapter is to provide an answer for the case when $g_1, \ldots, g_n$ are unmixed, namely,

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

where $\mathrm{Res}_{d_1,\ldots,d_n}$ stands for dense (Macaulay) resultant with respect to the total degrees d_i of the f_i's, $\mathrm{Res}_{\mathcal{B}}$ stands for unmixed sparse resultant 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 viewed as a chain rule for sparse resultants. It can be applied to compute sparse resultants of composed polynomials with improved efficiency.

1.4 Sparse Resultant of Composed Polynomials II

Chapter4 is the second chapter on sparse resultants of composed polynomials. In the first chapter, Chapter 3, "Sparse Resultant of Composed Polynomials I", the author and Hoon Hong considered the sparse resultant of polynomials having arbitrary (mixed) supports composed with polynomials having the same (unmixed) supports. Here, we consider the sparse resultant of polynomials having the same (unmixed) supports composed with polynomials having arbitrary (mixed) supports. The main contribution of this chapter is to show that the sparse resultant of these composed polynomials is the product of certain powers of the (sparse) resultants of the component polynomials. The resulting formula looks similar to the formula of the first chapter, which is good because it suggests that there is some common underlying structure for sparse resultants of composed polynomials. However, the formulae differ substantially in details. It also seems that it is not possible to apply the techniques used to show the main result of the first chapter in order to show the formula of the present chapter. It is expected that this result can be applied to compute sparse resultants of composed polynomials with improved efficiency.

1.5 Sparse Resultant under Vanishing Coefficients

The main question of Chapter 5 is: *What happens to the sparse resultant under vanishing coefficients?* More precisely, let $f_1, \ldots, f_n$ be sparse Laurent polynomials with supports $\mathcal{A}_1, \ldots, \mathcal{A}_n$ and let $\widetilde{\mathcal{A}}_1 \supset \mathcal{A}_1$. Naturally a question arises: Is the sparse resultant of $f_1, f_2, \ldots, f_n$ with respect to the supports $\widetilde{\mathcal{A}}_1, \mathcal{A}_2, \ldots, \mathcal{A}_n$ in any way related to the sparse resultant of $f_1, f_2, \ldots, f_n$ with respect to the supports $\mathcal{A}_1, \mathcal{A}_2, \ldots, \mathcal{A}_n$? The main contribution of this chapter is to provide an answer. The answer is important for applications with perturbed data where very small coefficients arise as well as when one computes resultants with respect to some fixed supports, not necessarily the supports of the f_i's, in order to speed up compuations. Further, we were motivated to work on sparse resultant under vanishing coefficients because we want to give an irreducible factorization of the chain rule formula of Chapter 3. This can be achieved by applying Theorem 5.1, the main result of Chapter 5. This work extends some work by Sturmfels on sparse resultant under vanishing coefficients. We also state a corollary about sparse resultant under powering of variables which is a generalization of a theorem for Dixon resultant by Kapur and Saxena. We also state a lemma of independent interest generalizing Pedersen's and Sturmfels' Poisson-type product formula.

Now we are ready to elaborate in detail on the main results.

Chapter 2

Dense Resultant of Composed Polynomials

2.1 Introduction

The main question of this chapter 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 (cf. [CMW95]) and Jouanolou (cf. [Jou91]) 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 chapter 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 2.1 and Remark 2.4). We also state a lemma (cf. Lemma 2.9) 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 which 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 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 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 dense resultants of polynomials composed with mixed polynomials. Therefore in this chapter we use mathematical methods that are essentially different from those.

This chapter has been submitted to a journal (cf. [Min00a]).

2.2 Main result

We assume that the reader is familiar with the notion of dense (Macaulay) resultant (cf. [CLO98]) and we let $\mathrm{Res}_{d_1,\ldots,d_n}$ stand for the dense resultant with respect to the total degrees $d_1,\ldots,d_n$. 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.

Now we are ready to state the main theorem.

Theorem 2.1 (Main theorem)

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

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 2.2 We illustrate the main theorem. Let

$$f_1 := 3\,y_1 \,-\, 5\,y_2 \,+\, 8\,y_3,$$

$$f_2 := 2\,y_1^2 \,+\, 11\,y_1\,y_2 \,-\, 7\,y_1\,y_3 \,+\, 5\,y_2^2 \,+\, 18\,y_2\,y_3 \,-\, 6\,y_3^2,$$

$$f_3 := 23\,y_1 \,+\, 3\,y_2 \,-\, 9\,y_3,$$

and let

$$g_1 := 2\,x_1 \,+\, 12\,x_2 \,+\, 14,$$

$$\begin{aligned} g_2 := {} & 8\,x_1^3 \,+\, 3\,x_1^2\,x_2 \,+\, 7\,x_1\,x_2^2 \,-\, 5\,x_2^3 \\ & +\, 19\,x_1^2 \,+\, 17\,x_1\,x_2 \,-\, 14\,x_2^2 \,+\, 12\,x_1 \,-\, 11\,x_2 \,+\, 3, \end{aligned}$$

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

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

$$g_2{}^{[3]} = 8\,x_1^3 \;+\; 3\,x_1^2\,x_2 \;+\; 7\,x_1\,x_2^2 \;-\; 5\,x_2^3$$

$$g_3{}^{[3]} = 6\,x_1^3 \;+\; 7\,x_1^2\,x_2 \;-\; 19\,x_1\,x_2^2 \;-\; 4\,x_2^3.$$

Therefore

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

and the second factor can be factorized further as

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

Remark 2.3 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

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

where ${g_j}^{\mathrm{d}}$ stands for the dehomogenization of g_j.

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

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

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

Remark 2.4 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

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

whereas usually one defines

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

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 2.5 We consider the dense resultant of the composed polynomials $f_i \circ$

$(g_1, \ldots, g_n)$ with respect to the total degrees "$d_i\bar{e}$". This is natural because almost always the total degree of $f_i \circ (g_1, \ldots, g_n)$ is $d_i\bar{e}$.

Remark 2.6 From the main theorem we can see immediately that if at least two of the e_j's are smaller than $\bar{e}$ then

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

In the proof (cf. Section 2.3) 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 2.7 The main theorem covers the cases of dense resultant of composed polynomials considered by [CMW95] and [Jou91].[1] As an example, we show how one can recover from the main theorem the formula of [CMW95] for dense resultant of inhomogenous 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

[1] Note that Jouanolou gives, in Proposition 5.11.2 of [Jou91], an interesting formula for dense resultant of certain *sparse* linear polynomials composed with homogeneous polynomials. This formula is not among the cases of this chapter because the linear polynomials are sparse. We suggest that one classifies formulae involving sparse composed polynomials within the theory of sparse resultants (cf. [CLO98]).

total degree. By the main theorem,

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

which is the expression given by [CMW95].

Remark 2.8 Applying the main theorem when computing the dense resultant of composed polynomials is expected to yield a dramatic improvement in efficiency. 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.

2.3 Proof of the main theorem

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 degee 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 2.9 *We have*

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

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 2.10 (continuing Example 2.2) 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 2.9 Firstly, we suppose that the g_j's have distinct symbolic coefficients with positive total degrees 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. [Jou91] and [CLO98]), we have

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

Further, by the techniques of [PRS93], 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 numbes and the coefficients of $g_2, \ldots, g_n$. Now, observe that, by the poisson formula and by [PRS93],

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

Therefore

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

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

$$= \mathrm{Res}_{g_1,\overline{e},\ldots,\overline{e}}(g_1, \ldots, g_n) \ \mathrm{Res}_{\overline{e},\ldots,\overline{e}}\left(g_2{}^{[\overline{e}]}, \ldots, g_n{}^{[\overline{e}]}\right)^{\overline{e}-e_1}.$$

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. [CLO98]) and by the

Poisson formula (cf. [Jou91]),

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

and, by definition (cf. Remark 2.4),

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

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

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

The forms of $g_1,\dots,g_n$ of total degree $\overline{e}$ are $0, 0, {g_3}^{[\overline{e}]},\dots,{g_n}^{[\overline{e}]}$. By Bezout's theorem (cf. [DS98] and [CLO98]) the $n-2$ homogeneous polynomials ${g_3}^{[\overline{e}]},\dots,{g_n}^{[\overline{e}]}$

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.

$\square$

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 2.9 and on the formula of [CMW95] and [Jou91] for dense resultant of homogeneous polynomials composed with homogeneous polynomials of same total degrees.

Proof of Theorem 2.1 (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 [CMW95] and [Jou91], we get

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

By Lemma 2.9, we have that

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

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 2.9 and we could stop. However, we show the irreducibility without using Lemma 2.9 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

$$\operatorname{Res}_{d_1\overline{e},\dots,d_n\overline{e}}\left(f_1\circ(g_1,\dots,g_n),\dots,f_n\circ(g_1,\dots,g_n)\right)\ =\ 0.$$

The dense (Macaulay) resultant vanishes because the composed polynomials $f_i\circ(g_1,\dots,g_n)$ 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 $e_1,\dots,e_k = \overline{e}$ and $e_{k+1},\dots,e_n < \overline{e}$ without changing the composed polynomials $f_i\circ(g_1,\dots,g_n)$. We assume that, for $k\le n-2$, $e_1,\dots,e_k=\overline{e}$ and $e_{k+1},\dots,e_n<\overline{e}$. We start with computing the leading form of $f_i\circ(g_1,\dots,g_n)$. 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 3.10, which has been shown independent from the theorems and lemmas preceding it. 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 3.10,

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

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. [DS98] and [CLO98]) 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. □

2.4 Conclusion

In this chapter 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 chapter 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. These results can be applied to compute dense resultants of composed polynomials with improved efficiency. We also determined the common zeros naturally generated by composition in some cases when the dense resultant vanishes and we stated a lemma of independent interest about dense resultant under vanishing of leading forms.

Chapter 3

Sparse Resultant of Composed Polynomials I

3.1 Introduction

The main question of this chapter 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*[1] 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 is a work joint between Hoon Hong and the author, Manfred Minimair. 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

[1] The author, Manfred Minimair, is currently investigating, the same question but for a more general class of inputs, namely allowing *mixed non homogeneous* polynomials.

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 3.1).

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 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 chapter 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 [CE95]. We also assume that the reader is familiar with the algorithms that are described in [CE95] and in [EP97], for computing Newton matrices and sparse resultans.

This chapter has been submitted to a journal (cf. [HM00]).

3.2 Main result

Let $f_1, \ldots, f_n$ be homogeneous[2] sparse polynomials in the variables $y_1, \ldots, y_n$ with distinct symbolic coefficients of 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.[3] 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

[2] In the literature sparse resultants and (normalized) volumes are defined for *inhomogeneous* (Laurent) polynomials. However, in this chapter we will consider those for *homogeneous* (Laurent) polynomials, which are simply defined as those for (Laurent) polynomials dehomogenized with respect to some variable. 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.

[3] In allowing the g_j's to be *Laurent* polynomials instead of polynomials we follow common practice. The purpose of this relaxation is only notational convenience 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.

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 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 $\mathrm{Res}_{d_1,\ldots,d_n}(.)$ stand for dense (Macaulay) resultant, $\mathrm{Res}_{\mathcal{B}}(.)$ stand for unmixed sparse resultant and $\mathrm{Res}_{\mathcal{C}_1,\ldots,\mathcal{C}_n}(.)$ stand for mixed sparse resultant. Now we are ready to state the main theorem, namely a "chain rule" for sparse resultants.

Theorem 3.1 (Main theorem) *We have*

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

Further, Table 3.1 shows by which factors the arithmetic complexities of the main tasks of sparse resultant computation (see [EP97]) 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 3.1: 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 $f_i \circ (g_1, \dots, g_n)$'s

Newton matrix computation of:

	time	*space*
f_i's	V_Q^2	V_Q
g_j's	$d_{\max}^{2n-2}$	$d_{\max}^{n-1}$

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

Sparse resultant extraction of:

	time	*space*
f_i's	$(V_Q)^3 \cdot (n-1)!$	V_Q
g_j's	$d_{\max}^{3n-3}$	$d_{\max}^{n-1}$

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

Example 3.2 We illustrate the notations and the main theorem. Let

$$f_1 := a_{1600}\, y_1^6 \;+\; a_{1411}\, y_1^4\, y_2\, y_3 \;+\; a_{1222}\, y_1^2\, y_2^2\, y_3^2 \;+\; a_{1105}\, y_1\, y_3^5 \;+\; a_{1006}\, y_3^6,$$

$$f_2 := a_{2700}\, y_1^7 \;+\; a_{2331}\, y_1^3\, y_2^3\, y_3 \;+\; a_{2142}\, y_1\, y_2^4\, y_3^2 \;+\; a_{2025}\, y_2^2\, y_3^5 \;+\; a_{2070}\, y_2^7,$$

$$f_3 := a_{3900}\, y_1^9 \;-\; a_{3621}\, y_1^6\, y_2^2\, y_3 \;+\; a_{3432}\, y_1^4\, y_2^3\, y_3^2 \;+\; a_{3063}\, y_2^6\, y_3^3 \;+\; a_{3009}\, y_3^9,$$

$$g_1 := b_{1221}\, x_1^2\, x_2^2\, x_3 \;+\; b_{1230}\, x_1^2\, x_2^3 \;+\; b_{1\,-1\,42}\, x_1^{-1}\, x_2^4\, x_3^2 \;+\; b_{1014}\, x_2\, x_3^4,$$

$$g_2 := b_{2221}\, x_1^2\, x_2^2\, x_3 \;+\; b_{2230}\, x_1^2\, x_2^3 \;+\; b_{2\,-1\,42}\, x_1^{-1}\, x_2^4\, x_3^2 \;+\; b_{2014}\, x_2\, x_3^4,$$

$$g_3 := b_{3221}\, x_1^2\, x_2^2\, x_3 \;+\; b_{3230}\, x_1^2\, x_2^3 \;+\; b_{3\,-1\,42}\, x_1^{-1}\, x_2^4\, x_3^2 \;+\; b_{3014}\, x_2\, x_3^4.$$

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

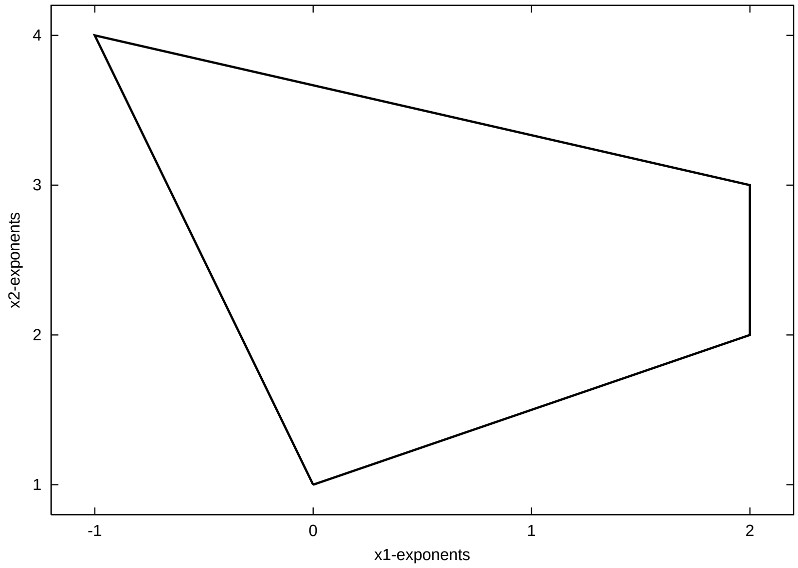

Figure 3.1: Newton polytope Q of g_1, g_2 and g_3 after orthogonal projection onto (x_1, x_2)-exponent plane

monomials occuring in $f_1 \circ (g_1, g_2, g_3)$, namely,

$$
\begin{gathered}
x_2^{16} x_3^{15} x_1^{-1},\ x_1^5 x_2^{14} x_3^{11},\ x_1^6 x_2^{19} x_3^5,\ x_1^7 x_2^{16} x_3^7,\ x_1^8 x_2^{13} x_3^9,\ x_1^6 x_2^{11} x_3^{13},\ x_1^{10} x_2^{15} x_3^5,\ x_1^3 x_2^{20} x_3^7,\ x_1^4 x_2^{17} x_3^9,\ x_1^7 x_2^{13} x_3^{10}, \\
x_1^8 x_2^{10} x_3^{12},\ x_1^3 x_2^{18} x_3^9,\ x_1^4 x_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_1^6 x_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_1^9 x_2^{15} x_3^6,\ x_1^8 x_2^{11} x_3^{11},\ x_1^{12} x_2^{12} x_3^6,\ x_1^{12} x_2^{13} x_3^5,\ x_1^9 x_2^{14} x_3^7,\ x_1^{10} x_2^{11} x_3^9,\ x_1^6 x_2^9 x_3^{15},\ x_1^7 x_2^{14} x_3^9,\ x_1^{12} x_2^{17} x_3,\ x_1^2 x_2^7 x_3^{21},\ x_1^6 x_2^{17} x_3^7, \\
x_1^{12} x_2^{18},\ x_2^6 x_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_2^9 x_3^{22} x_1,\ x_1^4 x_2^{10} x_3^{16},\ x_1^3 x_2^{13} x_3^{14}, \\
x_2^{22} x_3^8,\ x_1 x_2^{19} x_3^{10},\ x_1^2 x_2^{16} x_3^{12},\ x_1^9 x_2^{19} x_3^2,\ x_2^{14} x_3^{16},\ x_1^6 x_2^{20} x_3^4,\ x_1^7 x_2^{17} x_3^6,\ x_1^8 x_2^{14} x_3^8,\ x_1^6 x_2^{12} x_3^{12},\ x_1^{10} x_2^{16} x_3^4,\ x_1^3 x_2^{21} x_3^6, \\
x_1^4 x_2^{18} x_3^8,\ x_1^5 x_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_1^6 x_2^{18} x_3^6,\ x_1^8 x_2^{12} x_3^{10},\ x_1^6 x_2^{10} x_3^{14},\ x_1^{10} x_2^{14} x_3^6, \\
x_1^3 x_2^{19} x_3^8,\ x_1^4 x_2^{16} x_3^{10},\ x_1^5 x_2^{13} x_3^{12},\ x_1^2 x_2^8 x_3^{20},\ x_1^7 x_2^{15} x_3^8,\ x_1^5 x_2^{12} x_3^{13},\ x_1^{12} x_2^{15} x_3^3,\ x_1^9 x_2^{16} x_3^5,\ x_1^{10} x_2^{13} x_3^7,\ x_1^{12} x_2^{16} x_3^2,\ x_1^4 x_2^9 x_3^{17}, \\
x_1^3 x_2^{12} x_3^{15},\ x_2^{21} x_3^9,\ x_1 x_2^{18} x_3^{11},\ x_1^2 x_2^{15} x_3^{13},\ x_1^9 x_2^{18} x_3^3,\ x_1^4 x_2^8 x_3^{18},\ x_1^3 x_2^{11} x_3^{16},\ x_2^{20} x_3^{10},\ x_1 x_2^{17} x_3^{12},\ x_1^2 x_2^{14} x_3^{14},\ x_1^9 x_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 3.1. From the figure we see that $\operatorname{Vol}(Q) = 10$ and $V_Q = 5$. Thus the main theorem states that

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

Table 3.2: 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 3.2

Newton matrix computation of:

	time	*space*
f_i's	$5^2 = 25$	5
g_j's	$9^4 = 6561$	$9^2 = 81$

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

Sparse resultant extraction of:

	time	*space*
f_i's	$5^3 \cdot 2! = 250$	5
g_j's	$9^6 = 531441$	$9^2 = 81$

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

Further, the main theorem states the factors of Table 3.2 for the improved complexities of the main tasks of sparse resultant computation.

Even this simple example illustrates that the use of the main theorem provides a dramatic improvement of efficiency (see Table 3.2). 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 3.1), calculate the exponents and keep the final output in the compact factored form. Note that we do not have to compute the exponent $\mathrm{Vol}\,(Q)$ seperately because current algorithms for sparse resultant computation require that the mixed volume of $n-1$ copies of Q, i.e. $\mathrm{Vol}\,(Q)$, is computed in a subroutine and therefore we get $\mathrm{Vol}\,(Q)$ as a byproduct of the computation without additional effort. Further, note that Table 3.1 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 higer order than the decrease stated in Table 3.1.

3.3 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 3.2.

$$
\begin{tikzcd}[column sep=small]
\text{Lemma 3.8} \arrow[dr] & & \text{Lemma 3.10} \arrow[dl] \\
& \text{Lemma 3.11} \arrow[d] & \\
& \text{Lemma 3.12} \arrow[d] & \\
& \text{Lemma 3.13} \arrow[d] & \\
& \text{Lemma 3.14} \arrow[d] & \\
& \text{Lemma 3.15} \arrow[d] & \\
& \text{Theorem 3.1 (Main theorem)} &
\end{tikzcd}
$$

Figure 3.2: Dependency of the lemmas

Before listing the lemmas, we fix some notations.

Notation 3.3 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.

Example 3.4 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 3.5 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 3.6 Let

$$p := 8\,x_1 \,+\, 3\,x_2 + d,$$

$$\omega := (-1, 0)\,,$$

$$\mathcal{E} := \left\{x_1^2 x_2,\, x_1^2,\, x_2,\, 1\right\}.$$

Figure 3.3 shows a triangle, the Newton polytope of p, inscribed into a rectangle,

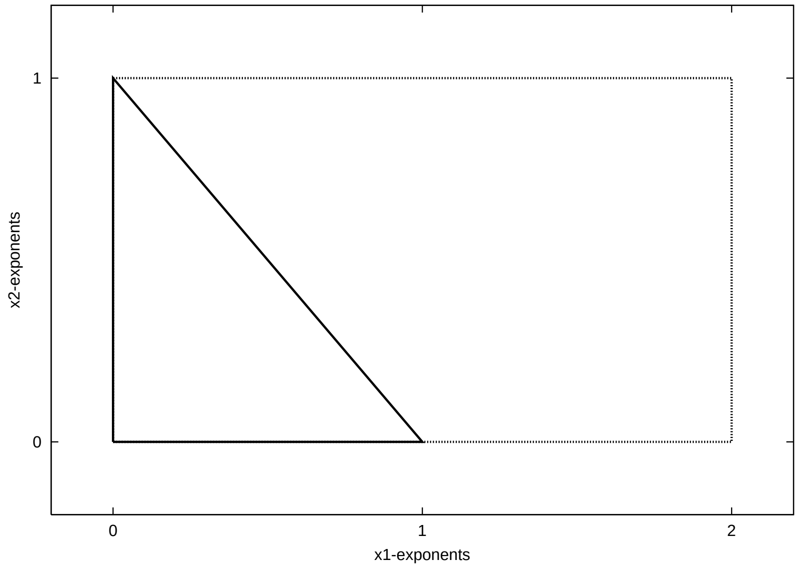

Figure 3.3: A triangle, the Newton polytope of p, inscribed into a rectangle, the Newton polytope generated by exponents in $\mathcal{E}$

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 leanding form of p with respect to ω and $\mathcal{E}$, written as $p^{\omega}_{\mathcal{E}}$, 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 3.7 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] 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 chapter 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 3.8 *For all specializations, with complex numbers, of the coefficients of the h_j's, we have* $\mathrm{Res}_{\mathcal{E}_1,\ldots,\mathcal{E}_n}(h_1,\ldots,h_n) = 0$ *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

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

iff

$$\mathcal{D}_{R_1+\cdots+R_n}\left(\left(h^{\mathrm{d}}_1,\ldots,h^{\mathrm{d}}_n\right),(R_1,\ldots,R_n)\right) \neq \emptyset,$$

where $\mathcal{D}_{R_1+\cdots+R_n}\left(\left(h^{\mathrm{d}}_1,\ldots,h^{\mathrm{d}}_n\right),(R_1,\ldots,R_n)\right)$ 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 $R_1+\cdots+R_n$.[4] 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 innter 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 $\mathbb{C}[\sigma_i^\vee\cap\mathbb{Z}^{n-1}]$ (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

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

$x^{-w_1^{(i)}}h_1^{\mathrm{d}}, \ldots, x^{-w_n^{(i)}}h_n^{\mathrm{d}}$ in $\mathbb{C}[\sigma_i^\vee \cap \mathbb{Z}^{n-1}]$. Therefore

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

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 $\mathbb{C}[\sigma_i^\vee \cap \mathbb{Z}^{n-1}]$, 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 $e \in (\tau_i^\vee \cap \mathbb{Z}^{n-1}) \setminus \{0\}$ and for some $\xi \in (\mathbb{C}\setminus\{0\})^{n-1}$ and $x^e = 0$, for $e \notin (\tau_i^\vee \cap \mathbb{Z}^{n-1}) \setminus \{0\}$, 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 $h_{j\,\mathcal{E}_j^{\mathrm{d}}}^{\mathrm{d}\,\omega}$ vanishes when $x_1, \ldots, x_{n-1}$ is replaced by $\xi_1, \ldots, \xi_{n-1}$. Therefore and vice versa, the leading forms $h_{1\mathcal{E}_1^{\mathrm{d}}}^{\mathrm{d}\omega}, \ldots, h_{n\mathcal{E}_n^{\mathrm{d}}}^{\mathrm{d}\,\omega}$ have a common zero in $(\mathbb{C}\setminus\{0\})^{n-1}$. 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 $(\mathbb{C}\setminus\{0\})^n$.

$\square$

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 3.9 Let $p := y_1^2 + y_2 y_3$ 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 symolic coefficients of any other Laurent polynomial in this chapter. 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 3.10 *We have*[5]

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

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

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

[5] 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.

We show that

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

Note that

$$g_1^{\alpha_1} \cdots g_n^{\alpha_n} \;=\; ({g_1}^{\omega}_{\mathcal{B}} + h_1)^{\alpha_1} \cdots ({g_n}^{\omega}_{\mathcal{B}} + h_n)^{\alpha_n}$$

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

for some fixed $h_1, \dots, h_n$ whose Laurent monomials have exponents different from those in ${g_1}^{\omega}_{\mathcal{B}}, \dots, {g_n}^{\omega}_{\mathcal{B}}$. 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 ${g_j}^{\omega}_{\mathcal{B}}$'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 $(g_1^{\alpha_1} \cdots g_n^{\alpha_n})^{\omega}_{\mathcal{E}}$ is $\{e \mid (d \cdot l, e) = d \cdot r\}$ and the exponents of the Laurent monomials that are contained in $({g_1}^{\omega}_{\mathcal{B}})^{\alpha_1} \cdots ({g_n}^{\omega}_{\mathcal{B}})^{\alpha_n}$ lie in this hyperplane as well. Therefore the Laurent monomials, together with their coefficients, of $({g_1}^{\omega}_{\mathcal{B}})^{\alpha_1} \cdots ({g_n}^{\omega}_{\mathcal{B}})^{\alpha_n}$ are contained in the leading form $(g_1^{\alpha_1} \cdots g_n^{\alpha_n})^{\omega}$. Now, fix a tuple $(\beta_1, \dots, \beta_n) \neq 0$. The exponents of the Laurent monomials in the h_j's are contained in the set $\{e \mid (l, e) < r\}$ und 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 3.11 *For all specializations, with complex numbers, of the coefficients of the F_i's and of the g_j's,*

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

implies

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

Proof:

We would like to apply Lemma 3.8 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

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

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 3.8 and by Lemma 3.10, which can be trivially specialized, there are appropriate leading forms

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

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

$$g_{1\mathcal{B}}^{\omega}(\xi_1, \ldots, \xi_n) = 0, \ldots, g_{n\mathcal{B}}^{\omega}(\xi_1, \ldots, \xi_n) = 0$$

or

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

where $0 \neq (\upsilon_1, \ldots, \upsilon_n) := (g_{1\mathcal{B}}^{\omega}(\xi_1, \ldots, \xi_n), \ldots, g_{n\mathcal{B}}^{\omega}(\xi_1, \ldots, \xi_n))$. Therefore

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

□

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 3.12

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

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

Proof:

Hilbert's Nullstellensatz is the key. By Lemma 3.11, for all specializations, with complex numbers, of the coefficients of the F_i's and of the g_j's,

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

implies that

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

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

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

$$\mathrm{Res}_{d_1,\ldots,d_n}\left(F_1, \ldots, F_n\right) \quad \text{and} \quad \mathrm{Res}_{\mathcal{B}}\left(g_1, \ldots, g_n\right)$$

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

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

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

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

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 $\mathrm{Res}_{d_1,\ldots,d_n}\left(F_1, \ldots, F_n\right)$ and $\mathrm{Res}_{\mathcal{B}}\left(g_1, \ldots, g_n\right)$ are irreducible polynomials, the polynomial

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

must be, up to a constant factor, a product of certain non negative powers of $\operatorname{Res}_{d_1,\ldots,d_n}(F_1,\ldots,F_n)$ and $\operatorname{Res}_{\mathcal{B}}(g_1,\ldots,g_n)$ and thus we have shown the lemma.

□

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

Lemma 3.13 *We have*

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

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 3.11 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 $\mathrm{Res}_{\mathcal{D}_1,\ldots,\mathcal{D}_n}\left(g_1^{d_1},\ldots,g_n^{d_n}\right)$. We get

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

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

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

The other factors in the equality are not zero. Therefore

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

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

$\square$

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 3.14 *We have*

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

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

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

$$\begin{aligned}
&\mathrm{Res}_{\mathcal{D}_1,\ldots,\mathcal{D}_n}\left(c \cdot F_1 \circ (g_1, \ldots, g_n), F_2 \circ (g_1, \ldots, g_n), \ldots, F_n \circ (g_1, \ldots, g_n)\right) \\
&\qquad = c^{d_2 \cdots d_n \, \mathrm{MV}\left(Q^{\mathrm{d}}, \ldots, Q^{\mathrm{d}}\right)} \cdot \mathrm{Res}_{d_1,\ldots,d_n}\left(F_1, \ldots, F_n\right),
\end{aligned}$$

where Q^{d} is the Newton polytope of $g_1, \ldots, g_n$ dehomogenized w.r.t. any fixed variable x_k.[6] By comparing powers in the specialized equality

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

[6]It is easy to see that it does not matter which variable x_k we choose.

$\square$

Finally we derive the exponent ν and obtain the chain rule for sparse resultants of dense homogeneous polynomials composed with sparse homogeneous Laurent polynomials.

Lemma 3.15 *We have*

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

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 $j = 1,\dots,n$, for some new constant c distinct from any other symbolic constant used until now, and get

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

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

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

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,

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

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

$\square$

Proof of theorem 3.1 (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 3.15 to

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

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

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

to

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

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 3.11 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]. 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 desined only for dense (Macaulay) resultant computation. As in [EP97], we will compare some of the complexities in terms of $\mathrm{O}^*(\chi)$, standing for $\mathrm{O}(\chi \log^v \chi)$, for any fixed constant v independent from χ. However, when we write "of order" we mean "$\mathrm{O}(.)$".

We start with Newton matrix computation. Under the assumptions of Theorem 6.2 and Corollary 6.4 of [EP97] 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 $\mathrm{O}^*(c^2 n)$ and $\mathrm{O}^*(cn)$, resp., where c is the number of columns of the Newton matrix that is generated by the algorithm.[7] As described in [CE95], 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 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

[7]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.

Table 3.3: Arithmetic complexities of Newton matrix computation

	arithmetic time complexity	arithmetic space complexity
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	$d_{\max}^{2n-2} \cdot n^3 \cdot (n-1)^{2n-2} \cdot V_Q^2$	$d_{\max}^{n-1} \cdot n^2 \cdot (n-1)^{n-1} \cdot V_Q$

is less or equal 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 or equal 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 3.11 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 or equal 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 3.3. 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 and V_Q, resp., the ratios for the

$f_i \circ (g_1, \ldots, g_n)$'s and the g_j's are $d_{\max}^{2n-2}$ and $d_{\max}^{n-1}$, resp.

Now we turn to sparse resultant extraction. Under the assumptions of Theorem 7.1 of [EP97] 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 $\mathrm{O}^*\left(c^2 n^2 \deg R\right)$ and $\mathrm{O}^*\left(cn\right)$, 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 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 $\mathrm{O}^*\left(c^2 n^2 \deg R\right)$. 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)

Table 3.4: Arithmetic complexities of sparse resultant extraction by division method

	arithmetic time complexity	arithmetic space complexity
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	$d_{\max}^{3n-3} \cdot n^5 \cdot (n-1)^{2n-2} \cdot V_Q^3 \cdot (n-1)!$	$d_{\max}^{n-1} \cdot n^2 \cdot (n-1)^{n-1} \cdot V_Q$

resultant of the f_i's is

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

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 or equal $n \cdot (n-1)!\, V_Q$ 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 3.4. 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 $V_Q^3 \cdot (n-1)!$ and V_Q, resp., the ratios for the $f_i \circ (g_1, \ldots, g_n)$'s and the g_j's are $d_{\max}^{3n-3}$ and $d_{\max}^{n-1}$, resp.

Thus we have shown the main theorem. □

3.4 Conclusion

In this chapter we gave a chain rule for 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. This rule essentially states 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.

Chapter 4

Sparse Resultant of Composed Polynomials II

4.1 Introduction

This chapter is the second one on sparse resultants of composed polynomials. In the first chapter, "Sparse Resultant of Composed Polynomials I", the author and Hoon Hong considered the sparse resultant of polynomials having arbitrary (mixed) supports composed with polynomials having the same (unmixed) supports. Here, the author considers the sparse resultant of polynomials having the same (unmixed) supports composed with polynomials having arbitrary (mixed) supports. The main contribution of this chapter is to show that the sparse resultant of these composed polynomials is the product of certain powers of the (sparse) resultants of the component polynomials. The resulting formula looks similar to the formula of the first chapter, which is good because it suggests that there is some common underlying structure for sparse resultants of composed polynomials. However, the formulae differ substantially in details. It also seems that it is not possible to apply the techniques used to show the main result of the first chapter in order to show the formula of the present chapter.

It is expected that this result can be applied to compute sparse resultants of composed polynomials with improved efficiency.

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, dense (Macaulay) resultant, Gröbner bases, subresultants and Galois groups of certain differential operators have been studied in Chapter 2, [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 chapter we use mathematical methods that are essentially different from those.

We assume that the reader is familiar with the notions of dense (Macaulay) resultant, sparse resultant, support of sparse Laurent polynomials, mixed volume, integer lattice and normalized volume of Newton polytope (cf. [CLO98], [GKZ94], [PS93]). There are different definitions of normalized volume in the literature. We follow the definition given in [PS93].

This chapter has been submitted to a journal (cf. [Min00b]).

4.2 Main result

Let $f_1, \dots, f_n$ be homogeneous sparse polynomials, having the same Newton polytopes, in the variables $y_1, \dots, y_n$ with distinct symbolic coefficients of positive total degree d.[1] Further, let $g_1, \dots, g_n$ be sparse Laurent polynomials, whose Newton polytopes have dimension $n-1$, in the variables $x_1, \dots, x_{n-1}$ with distinct symbolic coefficients distinct from the coefficients of the f_i's.[2]

We assume that the supports of the g_j's affinely generate over $\mathbb{Z}$ the integer lattice $\mathbb{Z}^{n-1}$. This is nothing but the standard restriction on sparse resultants (cf. [CLO98]).

Let $f_i \circ (g_1, \dots, g_n)$ be the sparse Laurent polynomial obtained from f_i by replacing y_j with g_j and let $\mathcal{C}_i$ denote its naturally induced support. Further, let $\mathrm{Res}_d\,(.)$ stand for dense (Macaulay) resultant with respect to unmixed total degrees, let $\mathrm{Res}_{\mathcal{B}}\,(.)$ stand for unmixed sparse resultant and let $\mathrm{Res}_{\mathcal{C}_1,\dots,\mathcal{C}_n}\,(.)$ stand for mixed sparse resultant.

Now we are ready to state the main theorem.

[1]Since there is no essential difference between proving the main theorem for f_i's having the same supports and for f_i's having the same Newton polytopes, we assume that the f_i's have the same Newton polytopes which is slightly more general.

[2]In allowing the g_j's to be *Laurent* polynomials instead of polynomials we follow common practice. The purpose of this relaxation is only notational convenience and does not essentially contribute to the problem.

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

Theorem 4.1 (Main theorem) *We have*

$$\operatorname{Res}_{\mathcal{C}_1,\ldots,\mathcal{C}_n}\left(f_1\circ(g_1,\ldots,g_n),\ldots,f_n\circ(g_1,\ldots,g_n)\right) = \operatorname{Res}_d\left(f_1,\ldots,f_n\right)^{\operatorname{Vol}(Q)}\operatorname{Res}_{\mathcal{B}}\left(g_1,\ldots,g_n\right)^{d^n},$$

where $\mathcal{B}$ is the union of the supports of the g_j's and $\operatorname{Vol}(Q)$ is the normalized volume of the Newton polytope Q generated by $\mathcal{B}$.

Example 4.2 We illustrate the notations and the main theorem. Let

$$f_1 := a_{1600}\,y_1^6 + a_{1411}\,y_1^4\,y_2\,y_3 + a_{1060}\,y_2^6 + a_{1105}\,y_1\,y_3^5 + a_{1006}\,y_3^6,$$

$$f_2 := a_{2600}\,y_1^6 + a_{2222}\,y_1^2\,y_2^2\,y_3^2 + a_{2060}\,y_2^6 + a_{2015}\,y_2\,y_3^5 + a_{2006}\,y_3^6,$$

$$f_3 := a_{3600}\,y_1^6 + a_{3321}\,y_1^3\,y_2^2\,y_3 + a_{1060}\,y_2^6 + a_{1501}\,y_1^5\,y_3 + a_{1006}\,y_3^6,$$

$$g_1 := b_{110}\,x_1 + b_{120}\,x_1^2 + b_{121}\,x_1^2\,x_2,$$

$$g_2 := b_{210}\,x_1 + b_{221}\,x_1^2\,x_2 + b_{2\,-1\,2,}\,x_1^{-1}\,x_2^2,$$

$$g_3 := b_{310}\,x_1 + b_{3\,-1\,2,}\,x_1^{-1}\,x_2^2 + b_{3\,-2\,0}\,x_1^{-2}.$$

Observe that $n = 3$, $d = 6$, and thus $d^3 = 216$. Further, observe that the dimension of the Newton polytopes of the g_j's is 2,

$$\mathcal{B} = \left\{x_1,\; x_1^2\,x_2,\; x_1^{-1}\,x_2^2,\; x_1^{-2}\right\}$$

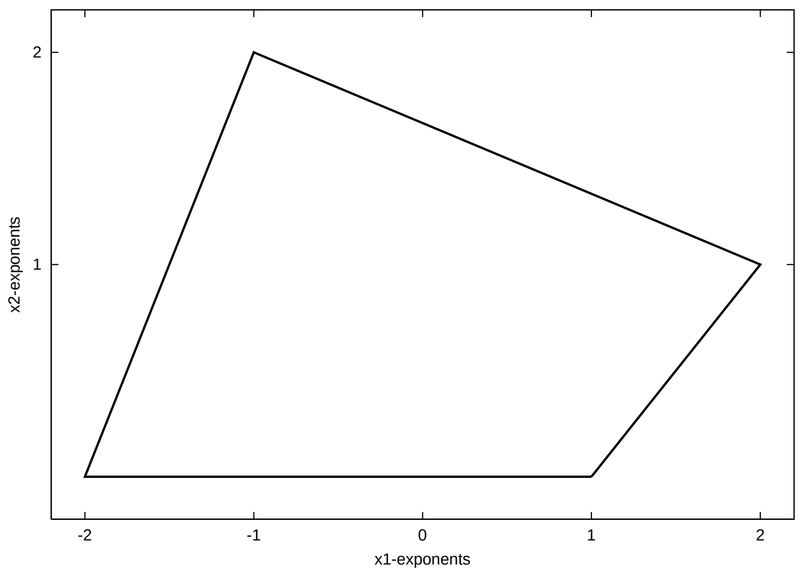

Figure 4.1: Newton polytope Q generated by the union $\mathcal{B}$ of the supports of g_1, g_2 and g_3

and that $\mathcal{C}_1$ is the set of monomials occuring in $f_1 \circ (g_1, g_2, g_3)$, namely,

$$\begin{gathered}
\{1, x1, x1^{-2}, x1^{6}, x1^{7}, x1^{8}, x1^{9}, x1^{10}, x1^{11}, x1^{12}, x2^{6}, x2^{4}, x2^{5}, x1^{3}, x1^{5}, \\
x1^{4}, x1^{-6}, x2^{10}, x1^{-9}, x1^{-8}, x1^{-3}, x1^{-12}, x1^{-5}, x2^{6}x1^{12}, x2\, x1^{7}, x2^{2}x1^{8}, x2^{3}x1^{9}, \\
x2^{4}x1^{10}, x2^{5}x1^{11}, x2\, x1^{11}, x2^{2}x1^{11}, x2^{3}x1^{11}, x2^{4}x1^{11}, x2\, x1^{10}, x2^{2}x1^{10}, x2^{3}x1^{10}, x2\, x1^{8}, \\
x2\, x1^{9}, x2^{2}x1^{9}, x2\, x1^{12}, x2^{2}x1^{12}, x2^{3}x1^{12}, x2^{4}x1^{12}, x2^{5}x1^{12}, x2^{2}x1^{5}, x2^{2}x1^{6}, x2^{2}x1^{7}, x2^{6}x1^{8}, \\
x2^{4}x1^{7}, x2^{7}x1^{9}, x2^{5}x1^{8}, x2^{8}x1^{6}, x2^{6}x1^{5}, x2^{3}x1^{5}, x2\, x1^{4}, x2^{2}x1^{4}, x2^{4}x1^{2}, x2^{2}x1, x2^{4}x1^{6}, x2^{5}x1^{3}, \\
x2^{3}x1^{2}, x2^{5}x1^{7}, x2^{3}x1^{6}, x2^{6}x1^{4}, x2^{4}x1^{3}, x2^{7}x1^{5}, x2^{5}x1^{4}, x2^{3}x1^{8}, x2^{4}x1^{9}, x2^{5}x1^{6}, x2^{4}x1^{8}, \\
x2^{5}x1^{9}, x2^{6}x1^{6}, x2^{4}x1^{5}, x2^{3}x1^{7}, x2^{6}x1^{9}, x2^{7}x1^{6}, x2^{5}x1^{5}, x2\, x1^{5}, x2^{2}x1^{2}, x2\, x1^{6}, x2^{4}x1^{4}, \\
x2^{2}x1^{3}, x2^{3}x1^{3}, x2^{3}x1^{4}, x2^{12}x1^{-6}, x2^{8}x1^{-2}, x2^{10}x1^{-4}, x2^{8}x1^{2}, x2^{9}x1^{-1}, x2^{7}x1, x2^{9}x1^{3}, \\
x2^{11}x1^{-3}, x2^{10}x1^{-3}, x2\, x1^{-8}, x2^{8}x1^{-5}, x2^{6}x1^{-6}, x2^{4}x1^{-7}, x2^{2}x1^{-8}, x2^{6}x1^{-3}, x2^{4}x1^{-4}, x2^{2}x1^{-5}, \\
x2^{4}x1^{-1}, x2^{2}x1^{-2}, x2^{6}x1, x2^{8}x1^{-1}, x2^{8}x1^{-4}, x2^{6}x1^{-5}, x2^{4}x1^{-6}, x2^{2}x1^{-7}, x2^{6}x1^{-2}, x2^{4}x1^{-3}, \\
x2^{2}x1^{-4}, x2^{2}x1^{-1}, x2^{9}x1^{-4}, x2^{7}x1^{-5}, x2^{5}x1^{-6}, x2^{3}x1^{-7}, x2\, x1, x2\, x1^{-2}, x2\, x1^{-5}, x2^{7}x1^{-2}, \\
x2^{5}x1^{-3}, x2^{3}x1^{-4}, x2^{3}x1^{-1}, x2^{2}x1^{-11}, x2^{10}x1^{-7}, x2^{8}x1^{-8}, x2^{6}x1^{-9}, x2^{4}x1^{-10}\}
\end{gathered}$$

and similarly for $\mathcal{C}_2$ and $\mathcal{C}_3$. The Newton polytope Q generated by the union of the supports of the g_j's is shown in Figure 4.1. From the figure we see that

$\mathrm{Vol}\,(Q) = 11$. Thus the main theorem states that

$$\mathrm{Res}_{\mathcal{C}_1,\mathcal{C}_2,\mathcal{C}_3}\left(f_1 \circ (g_1, g_2, g_3)\,, f_2 \circ (g_1, g_2, g_3)\,, f_3 \circ (g_1, g_2, g_3)\right) = \mathrm{Res}_6\left(f_1, f_2, f_3\right)^{11}\ \mathrm{Res}_{\mathcal{B}}\left(g_1, g_2, g_3\right)^{216}.$$

Remark 4.3 From the proof of Theorem 4.1 we see that

$$\mathrm{Res}_{\mathcal{C}_1,\ldots,\mathcal{C}_n}\left(f_1 \circ (g_1, \ldots, g_n), \ldots, f_n \circ (g_1, \ldots, g_n)\right) = 0$$

if the polynomials f_i do not contain all the monomials $y_1^d, \ldots, y_n^d$.

Remark 4.4 The factorization given in Theorem 4.1 is not irreducible for most composed Laurent polynomials. One can use Theorem 5.1, which has been shown independently from the theorems and lemmas preceding it, in order to further factorize, into irreducible factors, the right hand side of the equality of Theorem 4.1.

Remark 4.5 One can adjust the proof of Lemma 4.11 of Section 4.3, Proof of the main theorem, if the f_i's do not necessarily have the same total degrees d_i and contain the monomials $y_1^{d_i}, \ldots, y_n^{d_i}$, the dimension of the Newton polytope of g_j is not necessarily $n-1$ and the the dimension of the Newton polytope generated by $\mathcal{B}$ is $n-1$, and show an accordingly modified version of Lemma 4.11, that is,

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

where $\operatorname{Res}_{d_1,\ldots,d_n}(.)$ stands for dense (Macaulay) resultant. Obviously, this modified Lemma 4.11 generalizes the first part of Theorem 5.1.

Remark 4.6 Applying the main theorem when computing the sparse resultant of the composed Laurent polynomials is expected to yield a dramatic improvement in efficiency. In order to compute the sparse resultant of the composed Laurent polynomials, we only have to compute the dense (Macaulay) resultant and sparse resultant, resp., of the component polynomials, which is expected to be much more efficient than computing the sparse resultant of the expanded composed polynomials because the components are much smaller and have lower total degrees than the expanded composed polynomials. Note that we do not have to compute the exponent $\operatorname{Vol}(Q)$ seperately because current algorithms for sparse resultant computation require that the mixed volume of $n-1$ copies of Q, i.e. $\operatorname{Vol}(Q)$, is computed in a subroutine and therefore we get $\operatorname{Vol}(Q)$ as a byproduct of the computation without additional effort.

4.3 Proof of the main theorem

Before going into the details of the proof we describe its main structure. The proof is based on the main results of Chapter 3 and Chapter 5. First we show, in Lemma 4.11, using the main theorems of Chapter 3 and Chapter 5 and Lemma 4.9 and Lemma 4.10, a formula for the sparse resultant of the composed Laurent polynomials $f_i \circ (g_1, \dots, g_n)$, where the supports of the f_i's have some particular structure. Then we relax the assumption on the supports of the f_i's, proving the main theorem, Theorem 4.1. The dependency of the lemmas is shown in

$$\boxed{\begin{tikzcd}
\text{Lemma 4.8} \arrow[d] & & \\
\text{Lemma 4.9} \arrow[dr] & & \text{Lemma 4.10} \arrow[dl] \\
& \text{Lemma 4.11} \arrow[d] & \\
& \text{Theorem 4.1 (Main theorem)} &
\end{tikzcd}}$$

Figure 4.2: Dependency of the lemmas

Figure 4.2.

Before we state the lemmas, we fix some notations.

Notation 4.7 Let

1. f be a sparse homogeneous polynomial in the variables $y_1, \dots, y_n$ with distict symbolic coefficients containing the monomials $y_1^d, \dots, y_n^d$.

2. G_j be a Laurent polynomial with distinct symbolic coefficients whose support is $\mathcal{B}$, the union of the supports of the g_j's.

3. $\langle v, w \rangle$ be the Euclidean inner product of two vectors $v, w \in \mathbb{R}^{n-1}$.

Now we are ready to state lemmas.

First we give a lemma describing the convex hull of the union of some polytopes.

Lemma 4.8 *Let $P_1, \ldots, P_n$ be polytopes.*

There exists a finite set $W \subseteq \mathbb{R}^{n-1}$ such that

$$P_j \;=\; \bigcap_{w \in W} \left\{ p \in \mathbb{R}^{n-1} \mid \langle w,\, p \rangle \;\leq\; r_w^{(j)} \right\}$$

and such that the convex hull of $\bigcup_{j=1}^{n} P_j$ is

$$\bigcap_{w \in W} \left\{ p \in \mathbb{R}^{n-1} \mid \langle w,\, p \rangle \;\leq\; \max_{j=1}^{n} \left(r_w^{(j)} \right) \right\},$$

where the $r_w^{(j)}$'s are some real numbers.

Proof:

Let R stand for the convex hull of $\bigcup_{j=1}^{n} P_j$. By [Zie94], we can represent P_j and R as follows.

$$P_j = \bigcap_{w \in V^{(j)}} \left\{ p \in \mathbb{R}^{n-1} \mid \langle w,\, p \rangle \;\leq\; \max_{p \in P_j} \left(\langle w,\, p \rangle \right) \right\},$$
$$R = \bigcap_{w \in V} \left\{ p \in \mathbb{R}^{n-1} \mid \langle w,\, p \rangle \;\leq\; \max_{p \in R} \left(\langle w,\, p \rangle \right) \right\}.$$

Now, let $W := V^{(1)} \cup \cdots \cup V^{(n)} \cup V$ and

$$r_w^{(j)} := \max_{p \in P_j} \left(\langle w,\, p \rangle \right),$$

$$t_w := \max_{p \in R} \left(\langle w,\, p \rangle \right).$$

Then

$$P_j = \bigcap_{w \in W} \left\{ p \in \mathbb{R}^{n-1} \mid \langle w,\, p \rangle \;\le\; r_w^{(j)} \right\},$$
$$R = \bigcap_{w \in W} \left\{ p \in \mathbb{R}^{n-1} \mid \langle w,\, p \rangle \;\le\; t_w \right\}.$$

Firstly, we show that $t_w \le \max_{j=1}^{n}(r_w^{(j)})$. Take $q \in R$. Then $q = \tau_1 p_1 + \cdots + \tau_n p_n$, where $p_j \in P_j$, $0 \le \tau_j$ and $\sum_{j=1}^{n} \tau_j = 1$. We have

$$< w, q > = \tau_1 < w, p_1 > + \cdots + \tau_n < w, p_n >$$

$$\le \tau_1 r_w^{(1)} + \cdots + \tau_n r_w^{(n)}$$

$$\le \max_{j=1}^{n}(r_w^{(j)})$$

and thus $t_w \le \max_{j=1}^{n}(r_w^{(j)})$.

Now, we show that $t_w = \max_{j=1}^{n}(r_w^{(j)})$. Suppose that, for some $w \in W$, we have $t_w < \max_{j=1}^{n}(r_w^{(j)})$, that is, for all $p \in R$, we have $\langle w,\, p \rangle < \max_{j=1}^{n}(r_w^{(j)})$. Without loss of generality let $\max_{j=1}^{n}(r_w^{(j)}) = r_w^{(1)}$. By construction of $r_w^{(1)}$, there exists $p \in P_1 \subseteq R$ such that $\langle w,\, p \rangle = r_w^{(1)}$. Contradiction!

Thus we have shown the lemma.

□

Next we study the Newton polytope of certain composed Laurent polynomials.

Lemma 4.9 *The Newton polytope of $f \circ (g_1, \ldots, g_n)$ equals the Newton polytope of $f \circ (G_1, \ldots, G_n)$.*

Proof:

In the proof we let $\mathrm{NP}\,(h)$ stand for the Newton polytope of a Laurent polynomial h.

We start with showing that $\mathrm{NP}\,(f \circ (g_1, \ldots, g_n)) = \mathrm{NP}\left(g_1^d + \cdots + g_n^d\right)$. Firstly, it is obvious that $\mathrm{NP}\left(g_1^d + \cdots + g_n^d\right) \subseteq \mathrm{NP}\,(f \circ (g_1, \ldots, g_n))$ because the monomials of $g_1^d + \cdots + g_n^d$, multiplied by some symbolic coefficients, are contained in $f \circ (g_1, \ldots, g_n)$. Secondly, we show that $\mathrm{NP}\left(g_1^d + \cdots + g_n^d\right) \supseteq \mathrm{NP}\,(f \circ (g_1, \ldots, g_n))$. Let $f = \sum_{k=1}^m a_{\alpha_k}\, y^{\alpha_k}$, where $|\alpha_k| = d$. Note that $\mathrm{NP}\,(f \circ (g_1, \ldots, g_n))$ is the convex hull of $\bigcup_{k=1}^m \mathrm{NP}\,(g_1^{\alpha_{1k}} \cdots g_n^{\alpha_{nk}})$, where $(\alpha_{1k}, \ldots, \alpha_{nk}) = \alpha_k$. Therefore it is sufficient to show that $p \in \mathrm{NP}\left(g_1^d + \cdots + g_n^d\right)$, for arbitrary but fixed $p \in \mathrm{NP}\left(g_{i_1}^{\alpha_{i_1}} \ldots g_{i_\mu}^{\alpha_{i_\mu}}\right)$ and $\alpha_{i_1}, \ldots, \alpha_{i_\mu}$ with $\alpha_{i_1} + \cdots + \alpha_{i_\mu} = d$, $\alpha_{i_l} > 0$ and $\mu \le n$. Since $\mathrm{NP}\left(g_1^d + \cdots + g_n^d\right)$ is the convex hull of $\bigcup_{j=1}^n \mathrm{NP}\left(g_j^d\right)$, by Lemma 4.8, we see that there is some finite set $W \subseteq \mathbb{R}^{n-1}$ and real numbers $s_w^{(j)}$ such that

$$\mathrm{NP}\left(g_j^d\right) = \bigcap_{w \in W} \left\{p \in \mathbb{R}^{n-1} \,|\, \langle w,\, p\rangle \,\le\, s_w^{(j)}\right\}$$
$$\mathrm{NP}\left(g_1^d + \cdots + g_n^d\right) = \bigcap_{w \in W} \left\{p \in \mathbb{R}^{n-1} \,|\, \langle w,\, p\rangle \,\le\, s_w\right\},$$

where $s_w = \max_{j=1}^{n}\{s_w^{(j)}\}$. Thus it is sufficient to show that $\langle w, p\rangle \leq s_w$. Note that

$$\begin{aligned} p &= q_{i_1} + \cdots + q_{i_\mu} \\ &= \frac{\alpha_{i_1}}{d} q'_{i_1} + \cdots + \frac{\alpha_{i_\mu}}{d} q'_{i_\mu}, \end{aligned}$$

where $q_{i_l} \in \mathrm{NP}(g_{i_l}^{\alpha_{i_l}}) = \alpha_{i_l}\,\mathrm{NP}\,(g_{i_l})$ and $q'_{i_l} = \frac{d}{\alpha_{i_l}} q_{i_l} \in d\,\mathrm{NP}\,(g_{i_l}) = \mathrm{NP}\left(g_{i_l}^d\right)$. Now, we have

$$\begin{aligned} < w, p > &= \frac{\alpha_{i_1}}{d} < w, q'_{i_1} > + \cdots + \frac{\alpha_{i_\mu}}{d} < w, q'_{i_\mu} > \\ &\leq \frac{\alpha_{i_1}}{d} s_w^{(1)} + \cdots + \frac{\alpha_{i_\mu}}{d} s_w^{(n)} \\ &\leq \left(\frac{\alpha_{i_1}}{d} + \cdots + \frac{\alpha_{i_\mu}}{d}\right) s_w \\ &= s_w. \end{aligned}$$

Next we show that $\mathrm{NP}\left(g_1^d + \cdots + g_n^d\right) = \mathrm{NP}\left(G_1^d + \cdots + G_n^d\right)$. Obviously the support of $g_1^d + \cdots + g_n^d$ is a subset of the support of $G_1^d + \cdots + G_n^d$ and thus $\mathrm{NP}\left(g_1^d + \cdots + g_n^d\right) \subseteq \mathrm{NP}\left(G_1^d + \cdots + G_n^d\right)$. The other inclusion, namely, $\mathrm{NP}\left(G_1^d + \cdots + G_n^d\right) \subseteq \mathrm{NP}\left(g_1^d + \cdots + g_n^d\right)$, can be seen in the following way. Take an arbitrary but fixed element p of the support of $G_1^d + \cdots + G_n^d$. Then $p = q_1 + \cdots + q_d$, where q_i is in the support of some g_j. Now, we rewrite this sum. Since some of the q_i's may be equal, we have $p = (\beta_{k_1} r_{k_1} + \cdots + \beta_{k_2-1} r_{k_2-1}) + \cdots + (\beta_{k_n} r_{k_n} + \cdots + \beta_{k_{n+1}-1} r_{k_{n+1}-1})$, where $k_1 = 1$, $k_{n+1} = d+1$, $\sum_{i=1}^{d} \beta_i = d$, $\beta_i \geq 0$ and r_i is in the support of g_j, for $k_j \leq i \leq k_{j+1} - 1$. Now, let $f := \sum_{|\alpha|=d} a_\alpha\, y^\alpha$.

By the previous formula, we see that p is in the support of $f \circ (g_1, \dots, g_n)$. Thus $\mathrm{NP}\left(G_1^d + \cdots + G_n^d\right) \subseteq \mathrm{NP}\left(f \circ (g_1, \dots, g_n)\right)$ and, by the previous paragraph, $\mathrm{NP}\left(G_1^d + \cdots + G_n^d\right) \subseteq \mathrm{NP}\left(f \circ (g_1, \dots, g_n)\right) \subseteq \mathrm{NP}\left(g_1^d + \cdots + g_n^d\right)$.

Therefore we have shown that the $\mathrm{NP}\left(f \circ (g_1, \dots, g_n)\right) = \mathrm{NP}\left(G_1^d + \cdots + G_n^d\right)$. By replacing g_j by G_j, we see that $\mathrm{NP}\left(f \circ (G_1, \dots, G_n)\right) = \mathrm{NP}\left(G_1^d + \cdots + G_n^d\right)$.

Thus we have shown the lemma.

□

Next we study the integer lattice affinely generated by the support of certain composed Laurent polynomials.

Lemma 4.10 *The integer lattice affinely generated by the support of $f \circ (g_1, \dots, g_n)$ is $\mathbb{Z}^{n-1}$.*

Proof:

Since the integer lattice L affinely generated by the supports of $g_1, \dots, g_n$ is $\mathbb{Z}^{n-1}$, it is sufficient to show that L is contained in the integer lattice K affinely generated by the support of $f \circ (g_1, \dots, g_n)$. Recall that L is the coarsest sublattice of $\mathbb{Z}^{n-1}$, for all j, containing all pairwise differences of elements of the support of g_j. Thus we show that the difference $v - w$ for any v, w that are contained in the support of g_j, for arbitrary but fixed g_j, is contained in K.

Since f contains y_j^d, there is some $\alpha \in \mathbb{Z}^{n-1}$ and some polynomial p, a polynomial in the symbolic coefficients of f and of the g_j's, such that $p\,x^\alpha\,g_j$ is a part of $f \circ (g_1, \ldots, g_n)$. Thus the composed Laurent polynomial $f \circ (g_1, \ldots, g_n)$ contains the monomials $x^{\alpha+v}$ and $x^{\alpha+w}$. Since K is the coarsest sublattice of $\mathbb{Z}^{n-1}$ containing all pairwise differences of elements of the support of the composed Laurent polynomial $f \circ (g_1, \ldots, g_n)$, the difference $v - w$ is contained in K.

Thus we have shown the lemma.

$\square$

Now we show a restricted version of the formula of the main theorem.

Lemma 4.11 *If f_i contains for all i the monomials $y_1^d, \ldots, y_n^d$, then we have*

$$\operatorname{Res}_{\mathcal{C}_1,\ldots,\mathcal{C}_n}\left(f_1 \circ (g_1, \ldots, g_n), \ldots, f_n \circ (g_1, \ldots, g_n)\right) = \operatorname{Res}_d\left(f_1, \ldots, f_n\right)^{\operatorname{Vol}(Q)} \operatorname{Res}_{\mathcal{B}}\left(g_1, \ldots, g_n\right)^{d^n},$$

where $\mathcal{B}$ is the union of the supports of the g_j's and $\operatorname{Vol}(Q)$ is the normalized volume of the Newton polytope Q generated by $\mathcal{B}$.

Proof:

Since by Lemma 4.9 the Newton polytope of $f_i \circ (g_1, \ldots, g_n)$ equals the Newton polytope of $f_i \circ (G_1, \ldots, G_n)$, we have, by Theorem 5.1, which has been shown independently from the theorems and lemmas preceding it, similarly to the first paragraph of the proof of Corollary 5.4, that

$$\operatorname{Res}_{\mathcal{D}_1,\ldots,\mathcal{D}_n}\left(f_1\circ(g_1,\ldots,g_n),\ldots,f_n\circ(g_1,\ldots,g_n)\right) = \operatorname{Res}_{\mathcal{C}_1,\ldots,\mathcal{C}_n}\left(f_1\circ(g_1,\ldots,g_n),\ldots,f_n\circ(g_1,\ldots,g_n)\right)^I,$$

where $\mathcal{D}_i$ is the support of $f_i\circ(G_1,\ldots,G_n)$ and I is the quotient of the fundamental simplices of the lattice affinely generated by $\mathcal{C}_1,\ldots,\mathcal{C}_n$ and by $\mathcal{D}_1,\ldots,\mathcal{D}_n$. Since by Lemma 4.10, the lattice affinely generated by $\mathcal{C}_1,\ldots,\mathcal{C}_n$ is $\mathbb{Z}^{n-1}$ and again by Lemma 4.10, by replacing g_j by G_j, the lattice affinely generated by $\mathcal{D}_1,\ldots,\mathcal{D}_n$ is $\mathbb{Z}^{n-1}$, we have that $I=1$.

Now, by Theorem 3.1 with $d_1=\cdots=d_n=d$ and by viewing g_j as specialized Laurent polynomial with support $\mathcal{B}$, we have

$$\begin{aligned}\operatorname{Res}_{\mathcal{C}_1,\ldots,\mathcal{C}_n}\left(f_1\circ(g_1,\ldots,g_n),\ldots,f_n\circ(g_1,\ldots,g_n)\right) &= \\ \operatorname{Res}_{\mathcal{D}_1,\ldots,\mathcal{D}_n}\left(f_1\circ(g_1,\ldots,g_n),\ldots,f_n\circ(g_1,\ldots,g_n)\right) &= \\ \operatorname{Res}_d\left(f_1,\ldots,f_n\right)^{\mathrm{Vol}(Q)}\operatorname{Res}_{\mathcal{B}}\left(g_1,\ldots,g_n\right)^{d^n}.\end{aligned}$$

□

Now we are ready to prove the main theorem.

Proof:

Theorem 4.1 If f_i contains for all i the monomials $y_1^d, \ldots, y_n^d$, then Theorem 4.1 holds by Lemma 4.11.

Suppose there is one f_i that does not contain all monomials $y_1^d, \ldots, y_n^d$, say, does not contain y_j^d. Since the f_i's have the same Newton polytope and the f_i's are polynomials (not *Laurent* polynomials), either all f_i's contain y_j^d or none of the f_i's contains y_j^d. Thus suppose that y_j^d is not contained in any f_i and, without loss of generality, suppose that $y_j = y_1$. We will show that in this case the right hand side as well as the left hand side of the equality of Theorem 4.1 is zero.

We start with the right hand side of the equality of Theorem 4.1. Since f_i does not contain y_1^d, we have $f_i(y_1, 0, \ldots, 0) = 0$ and thus

$$\mathrm{Res}_d(f_1, \ldots, f_n) \;=\; 0.$$

Since, by assumption, the dimension of the Newton polytope of g_j is positive[3] and thus the dimension of Q is positive, we have $\mathrm{Vol}(Q) > 0$. Therefore

$$\mathrm{Res}_d(f_1, \ldots, f_n)^{\mathrm{Vol}(Q)} \;=\; 0$$

and thus the right hand side of the equality of Theorem 4.1 vanishes.

Now we consider the left hand side of the equality of Theorem 4.1. Since the dimension of the Newton polytope of g_j is $n-1$, there exists, by Bernshtein's theorem (cf. [CLO98], [GKZ94]), a common zero, in $(K \setminus \{0\})^{n-1}$, of $g_2, \ldots, g_n$,

[3]The case $n = 1$ is covered by the first paragraph.

where K is the algebraic closure of the field generated by the complex numbers and the symbolic coefficients of the g_j's. Thus, as in the previous paragraph, there exists a common zero, in $(K\setminus\{0\})^{n-1}$, of the $f_i \circ (g_1, \ldots, g_n)$'s and therefore

$$\mathrm{Res}_{\mathcal{C}_1,\ldots,\mathcal{C}_n}\,(f_1 \circ (g_1, \ldots, g_n), \ldots, f_n \circ (g_1, \ldots, g_n)) \;=\; 0$$

and therefore the left hand side of the equality of Theorem 4.1 vanishes.

Thus we have shown the main theorem.

$\square$

4.4 Conclusion

This chapter was the second one in a series of chapters on sparse resultants of composed polynomials. In the first chapter, "Sparse Resultant of Composed Polynomials I", the author and Hoon Hong considered the sparse resultant of polynomials having arbitrary (mixed) supports composed with polynomials having the same (unmixed) supports. Here, we considered the sparse resultant of polynomials having the same (unmixed) supports composed with polynomials having arbitrary (mixed) supports. The main contribution of this chapter was to show that the sparse resultant of these composed polynomials is the product of certain powers of the (sparse) resultants of the component polynomials. The resulting formula looks similar to the formula of the first chapter, which is good because it suggests that there is some common underlying structure for sparse resultants of composed polynomials. However, the formulae differ substantially in details. It also seems that it is not possible to apply the techniques used to show the main result of the first chapter in order to show the formula of the present chapter. This result can be applied to compute sparse resultants of composed polynomials with improved efficiency.

Chapter 5

Sparse Resultant under Vanishing Coefficients

5.1 Introduction

We ask: *What happens to the sparse resultant under vanishing coefficients?* More precisely, let $f_1, \ldots, f_n$ be sparse Laurent polynomials with the supports $\mathcal{A}_1, \ldots, \mathcal{A}_n$ and let $\widetilde{\mathcal{A}}_1 \supset \mathcal{A}_1$. Naturally a question arises: Is the sparse resultant of $f_1, f_2, \ldots, f_n$ with respect to the supports $\widetilde{\mathcal{A}}_1, \mathcal{A}_2, \ldots, \mathcal{A}_n$ in any way related to the sparse resultant of $f_1, f_2, \ldots, f_n$ with respect to the supports $\mathcal{A}_1, \mathcal{A}_2, \ldots, \mathcal{A}_n$? The main contribution of this chapter is to provide an answer: The sparse resultant of $f_1, f_2, \ldots, f_n$ with respect to the supports $\widetilde{\mathcal{A}}_1, \mathcal{A}_2, \ldots, \mathcal{A}_n$ is some power of the sparse resultant of $f_1, f_2, \ldots, f_n$ with respect to the supports $\mathcal{A}_1, \mathcal{A}_2, \ldots, \mathcal{A}_n$ times a product of powers of sparse resultants of some parts of the f_i's. We also state a corollary (cf. Corollary 5.4) about sparse resultant under powering of variables which is a generalization of a theorem for Dixon resultant shown by

Kapur and Saxena using different techniques (cf. [KS97]). We also state a lemma (cf. Lemma 5.12) of independent interest generalizing Pedersen's and Sturmfels' Poisson-type product formula.

This result is important for applications where perturbed data with very small coefficients arise as well as when one computes resultants with respect to some fixed supports, not necessarily the supports of the f_i's, in order to speed up compuations. Further, we were motivated to work on sparse resultant under vanishing coefficients because we want to give an irreducible factorization of the chain rule formula of Chapter 3. This can be achieved by applying the main theorem, Theorem 5.1, of the present chapter.

This result, Theorem 5.1, extends a corollary by Sturmfels (cf. Corollary 4.2 of [Stu94]) which essentially states that the sparse resultant of the Laurent polynomials $f_1, \dots, f_n$ with respect to their precise supports divides the sparse resultant of $f_1, \dots, f_n$ with respect to larger supports. This result, Theorem 5.1, also generalizes a Lemma2.9, for Macaulay resultant of dense polynomials under vanishing of leading forms.

We assume that the reader is familiar with the notions of sparse resultant, essential and essential subset of supports, integer lattice, fundamental simplex of an integer lattice, Newton polytope, primitive inner normal vector, mixed volume (cf. [CLO98], [GKZ94], [Stu94], [PS93]). We let $\mathrm{Res}_{\mathcal{A}_1,\dots,\mathcal{A}_n}(.)$ stand for sparse resultant with respect to the supports $\mathcal{A}_1, \ldots, \mathcal{A}_n \subseteq \mathbb{Z}^{n-1}$, we let $\mathcal{L}(\mathcal{A}_1, \ldots, \mathcal{A}_n)$ stand for the integer sublattice of $\mathbb{Z}^{n-1}$ affinely generated by $\mathcal{A}_1, \ldots, \mathcal{A}_n$, we let $[L_1 : L_2]$ stand for the quotient of the volumes of the fundamental simplices of the integer lattice L_2 and L_1 and we let $\mathcal{A}^\omega \subseteq \mathcal{A}$ stand for the set of vectors that lie in the face, with primitive inner normal vector ω, of the Newton polytope generated by the bounded set $\mathcal{A}$.

This chapter has been submitted to a journal (cf. [Min00c]).

5.2 Main result

Let $f_1, \ldots, f_n$ be sparse Laurent polynomials in the variables $x_1, \ldots, x_{n-1}$ with supports $\mathcal{A}_1, \ldots, \mathcal{A}_n$ and, for the sake of a simple presentation, with distinct symbolic coefficients.

Let $\widetilde{\mathcal{A}}_1$ be a finite set with $\mathcal{A}_1 \subseteq \widetilde{\mathcal{A}}_1 \subset \mathbb{Z}^{n-1}$ and let $\{\widetilde{\mathcal{A}}_1, \mathcal{A}_2, \ldots, \mathcal{A}_n\}$ have a unique essential subset, not necessarily equal $\{\widetilde{\mathcal{A}}_1, \mathcal{A}_2, \ldots, \mathcal{A}_n\}$, containing $\widetilde{\mathcal{A}}_1$ (cf. Remark 5.2).

Let $f^{\mathcal{A}}$ stand for the part, whose support is contained in the set $\mathcal{A}$, of the Laurent polynomial f and let $a_{\mathcal{A}}(\omega)$ stand for $-\min_v(\langle\omega, v\rangle)$, where $\langle\omega, v\rangle$ denotes the usual Euclidean inner product and v ranges over the Newton polytope generated by $\mathcal{A}$. Further let H^ω stand for the lattice of all integer points contained in the hyperplane, passing through the origin, with normal vector ω.

Now we are ready to state the main theorem.

Theorem 5.1 (Main theorem) *We have*

$$\operatorname{Res}_{\widetilde{\mathcal{A}}_1,\mathcal{A}_2,\dots,\mathcal{A}_n}(f_1,f_2,\dots,f_n) \;=\; \operatorname{Res}_{\mathcal{A}_1,\mathcal{A}_2,\dots,\mathcal{A}_n}(f_1,f_2,\dots,f_n)^{[\mathcal{L}(\widetilde{\mathcal{A}}_1,\mathcal{A}_2,\dots,\mathcal{A}_n):\mathcal{L}(\mathcal{A}_1,\dots,\mathcal{A}_n)]} \prod_{\omega} \operatorname{Res}_{\mathcal{A}_2^\omega,\dots,\mathcal{A}_n^\omega}\left({f_2}^{\mathcal{A}_2^\omega},\dots,{f_n}^{\mathcal{A}_n^\omega}\right)^{(\mathrm{a}_{\widetilde{\mathcal{A}}_1}(\omega)-\mathrm{a}_{\mathcal{A}_1}(\omega))\,\frac{[\mathrm{H}^\omega:\mathcal{L}(\mathcal{A}_2^\omega,\dots,\mathcal{A}_n^\omega)]}{[\mathbb{Z}^{n-1}:\mathcal{L}(\widetilde{\mathcal{A}}_1,\mathcal{A}_2,\dots,\mathcal{A}_n)]}},$$

where ω ranges over the primitive inner normal vectors of the facets of the Newton polytope generated by $\mathcal{A}_2+\cdots+\mathcal{A}_n$.

This factorization is irreducible.

Remark 5.2 It is important to point out that in a particular degenerate case the definition of the sparse resultant in the main theorem is slightly different from the usual one. For degenerate cases where a strict subset $\{\mathcal{A}_{i_1},\dots,\mathcal{A}_{i_m}\}$ of $\{\mathcal{A}_1,\dots,\mathcal{A}_n\}$ is uniquely essential, we define

$$\operatorname{Res}_{\mathcal{A}_1,\dots,\mathcal{A}_n}(f_1,\dots,f_n) \;:=\; \operatorname{Res}_{\mathcal{A}_{i_1},\dots,\mathcal{A}_{i_m}}(f_{i_1},\dots,f_{i_m})^{\mathrm{e}_{\mathcal{A}_1,\dots,\mathcal{A}_n}},$$

where the exponent $\mathrm{e}_{\mathcal{A}_1,\dots,\mathcal{A}_n}$ is defined in the following paragraph, whereas usually one defines

$$\operatorname{Res}_{\mathcal{A}_1,\dots,\mathcal{A}_n}(f_1,\dots,f_n) \;:=\; \operatorname{Res}_{\mathcal{A}_{i_1},\dots,\mathcal{A}_{i_m}}(f_{i_1},\dots,f_{i_m})\,.$$

The first definition allows us to handle the degenerate cases in a uniform and elegant way, whereas the second definition seems not to allow this.

In the following, we define the exponent $\mathrm{e}_{\mathcal{A}_1,\ldots,\mathcal{A}_n}$, where $\{\mathcal{A}_1, \ldots, \mathcal{A}_n\}$ has a unique essential (not necessarily strict) subset $\{\mathcal{A}_{i_1}, \ldots, \mathcal{A}_{i_m}\}$. Let L be an integer lattice such that the integer lattice affinely generated by $\mathcal{A}_1, \ldots, \mathcal{A}_n$ is the direct sum, as $\mathbb{Z}$-modules, of L and the integer lattice affinely generated by $\mathcal{A}_{i_1}, \ldots, \mathcal{A}_{i_m}$. Let π denote the projection onto L, which we naturally extend to the Laurent polynomials f_i. Then $\mathrm{e}_{\mathcal{A}_1,\ldots,\mathcal{A}_n}$ is defined to be the quotient of the mixed volume of the Newton polytopes of $\pi\left(f_{i_{m+1}}\right), \ldots, \pi\left(f_{i_n}\right)$ and the volume ot the fundamental parallelotope of L. It is easy to see that $\mathrm{e}_{\mathcal{A}_1,\ldots,\mathcal{A}_n}$ is well defined.

Note that this remark generalizes Remark 2.4.

Example 5.3 We illustrate Therorem 5.1 and Remark 5.2. Let

$$
\begin{aligned}
f_1 &:= a_{100} + a_{120}\, x_1^2, \\
f_2 &:= a_{200} + a_{220}\, x_1^2 + a_{201}\, x_2 + a_{221}\, x_1^2\, x_2, \\
f_3 &:= a_{300} + a_{340}\, x_1^4 + a_{321}\, x_1^2\, x_2 + a_{302}\, x_2^2
\end{aligned}
$$

and let

$$\widetilde{\mathcal{A}}_1 := \{(0,0),\, (2,0),\, (5,0)\}\,.$$

Observe that $n = 3$,

$$\mathcal{A}_1 = \{(0,0),\ (2,0)\},$$

$$\mathcal{A}_2 = \{(0,0),\ (2,0),\ (0,1),\ (2,1)\},$$

$$\mathcal{A}_3 = \{(0,0),\ (4,0),\ (2,1),\ (0,2)\},$$

$$\left[\mathcal{L}\left(\widetilde{\mathcal{A}}_1, \mathcal{A}_2, \mathcal{A}_3\right) : \mathcal{L}\left(\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3\right)\right] \; = \; 2,$$

$$\mathrm{e}_{\mathcal{A}_1,\mathcal{A}_2,\mathcal{A}_3} \; = \; 1$$

and

$$\begin{aligned}\mathcal{A}_2 + \mathcal{A}_3 = \{&(0,0),\ (4,0),\ (2,1),\ (0,2),\\ &(2,0),\ (6,0),\ (4,1),\ (2,2),\\ &(0,1),\ (4,1),\ (2,2),\ (0,3),\\ &(2,1),\ (6,1),\ (4,2),\ (2,3)\}.\end{aligned}$$

The Newton polytope (polygon) generated by $\mathcal{A}_2 + \mathcal{A}_3$ is shown in Figure 5.1. It has four facets (edges) with primitive inner normal vectors

$$\omega_1 = (0,-1),$$

$$\omega_2 = (1,0),$$

$$\omega_3 = (-1,0),$$

$$\omega_4 = (-1,-2).$$

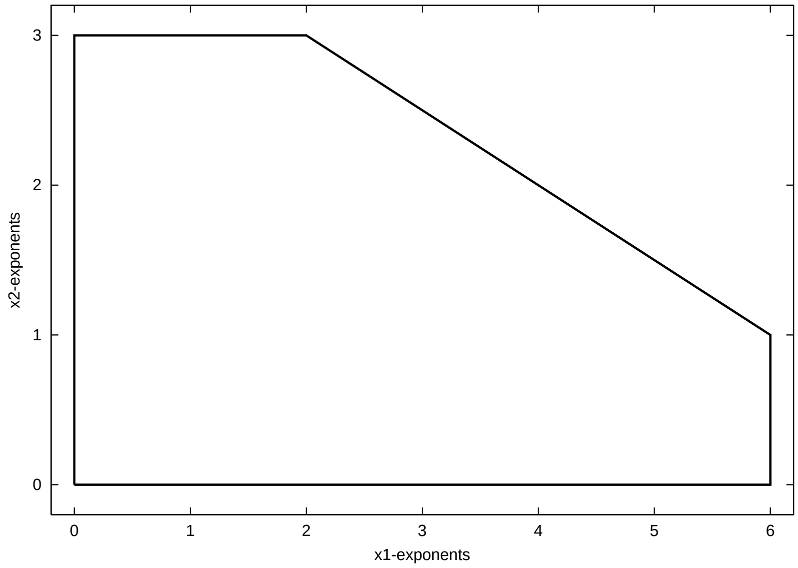

Figure 5.1: Newton polytope generated by $\mathcal{A}_2 + \mathcal{A}_3$

Observe that

$$
\begin{aligned}
&\mathrm{a}_{\widetilde{\mathcal{A}}_1}(\omega_1) = 0, && \mathrm{a}_{\mathcal{A}_1}(\omega_1) = 0,\\
&\mathrm{a}_{\widetilde{\mathcal{A}}_1}(\omega_2) = 0, && \mathrm{a}_{\mathcal{A}_1}(\omega_2) = 0,\\
&\mathrm{a}_{\widetilde{\mathcal{A}}_1}(\omega_3) = 5, && \mathrm{a}_{\mathcal{A}_1}(\omega_3) = 2,\\
&\mathrm{a}_{\widetilde{\mathcal{A}}_1}(\omega_4) = 5, && \mathrm{a}_{\mathcal{A}_1}(\omega_4) = 2,
\end{aligned}
$$

$$
\begin{aligned}
&\mathcal{A}_2^{\omega_3} = \{(2,0),\,(2,1)\}, && \\
&\mathcal{A}_3^{\omega_3} = \{(4,0)\}, && \mathrm{e}_{\mathcal{A}_2^{\omega_3},\mathcal{A}_3^{\omega_3}} = 1,\\
&\mathcal{A}_2^{\omega_4} = \{(2,1)\}, && \\
&\mathcal{A}_3^{\omega_4} = \{(4,0),\,(2,1),\,(0,2)\}, && \mathrm{e}_{\mathcal{A}_2^{\omega_4},\mathcal{A}_3^{\omega_4}} = 2,
\end{aligned}
$$

$$[\mathrm{H}^{\omega_3} : \mathcal{L}(\mathcal{A}_2^{\omega_3}, \mathcal{A}_3^{\omega_3})] = 1,$$

$$[\mathrm{H}^{\omega_4} : \mathcal{L}(\mathcal{A}_2^{\omega_4}, \mathcal{A}_3^{\omega_4})] = 1$$

and

$$\left[\mathcal{L}\left(\mathbb{Z}^2\right) : \mathcal{L}(\widetilde{\mathcal{A}}_1, \mathcal{A}_2, \mathcal{A}_3)\right] \;=\; 1.$$

Thus

$$\begin{aligned}\mathrm{Res}_{\widetilde{\mathcal{A}}_1,\mathcal{A}_2,\mathcal{A}_3}(f_1, f_2, f_3) = \mathrm{Res}_{\mathcal{A}_1,\mathcal{A}_2,\mathcal{A}_3}(f_2, f_2, f_3)^2 \\ \mathrm{Res}_{\mathcal{A}_2^{\omega_3},\mathcal{A}_3^{\omega_3}}(f_2^{\omega_3}, f_3^{\omega_3})^{(5-2)\cdot 1} \\ \mathrm{Res}_{\mathcal{A}_2^{\omega_4},\mathcal{A}_3^{\omega_4}}(f_2^{\omega_4}, f_3^{\omega_4})^{(5-2)\cdot 1}.\end{aligned}$$

In the following corollary we prove a formula for sparse resultant under powering of variables. This corollary generalizes a theorem for Dixon resultant, shown by Kapur and Saxena (cf. [KS97]) using different techniques.

Corollary 5.4 *Let $\widetilde{f}_i$ be obtained from f_i by replacing the variable x_j by $x_j^{d_j}$, for $j = 1, \ldots, n-1$, and let $\widetilde{\mathcal{A}}_i$ be the set of all integer points contained in the Newton polytope generated by $\widetilde{f}_i$. Then*

$$\mathrm{Res}_{\widetilde{\mathcal{A}}_1,\ldots,\widetilde{\mathcal{A}}_n}\left(\widetilde{f}_1, \ldots, \widetilde{f}_n\right) \;=\; \mathrm{Res}_{\mathcal{A}_1,\ldots,\mathcal{A}_n}(f_1, \ldots, f_n)^{|d_1 \cdots d_{n-1}|\,[\mathcal{L}(\widetilde{\mathcal{A}}_1,\ldots,\widetilde{\mathcal{A}}_n):\mathcal{L}(\mathcal{A}_1,\ldots,\mathcal{A}_n)]}.$$

Example 5.5 *Let*

$$f_1 := a_{100} \; + \; a_{124}\, x_1^2\, x_2^4,$$

$$f_2 := a_{200} \; + \; a_{266}\, x_1^6\, x_2^6,$$

$$f_3 := a_{300} \; + \; a_{342}\, x_1^4\, x_2^2$$

and $\widetilde{f_i}$ *be obtained from* f_i *by replacing* x_1 *by* x_1^2 *and* x_2 *by* x_2^3*.*

Observe that $d_1 = 2$, $d_2 = 3$ *and*

$$\widetilde{f_1} = a_{100} \; + \; a_{124}\, x_1^4\, x_2^{12},$$

$$\widetilde{f_2} = a_{200} \; + \; a_{266}\, x_1^{12}\, x_2^{18},$$

$$\widetilde{f_3} = a_{300} \; + \; a_{342}\, x_1^8\, x_2^6.$$

Further observe that

$$\mathcal{A}_1 = \{(0,0),(2,4)\}\,,$$

$$\mathcal{A}_2 = \{(0,0),(6,6)\}\,,$$

$$\mathcal{A}_3 = \{(0,0),(4,2)\}\,,$$

$$\widetilde{\mathcal{A}}_1 = \{(0,0),\,(1,3),\,(2,6),\,(4,12)\}\,,$$

$$\widetilde{\mathcal{A}}_2 = \{(0,0),\,(2,3),\,(4,6),\,(6,9),\,(8,12),\,(10,15),\,(12,18)\}\,,$$

$$\widetilde{\mathcal{A}}_3 = \{(0,0),\,(4,3),\,(8,6)\}\,,$$

$\mathcal{L}(\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3)$ is spanned by $\{(2,4), (4,2)\}$ and that $\mathcal{L}(\widetilde{\mathcal{A}}_1, \widetilde{\mathcal{A}}_2, \widetilde{\mathcal{A}}_3)$ is spanned by $\{(1,3), (2,3)\}$. Thus the fundamental simplex of $\mathcal{L}(\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3)$ has volume (area) 6 and the fundamental simplex of $\mathcal{L}(\widetilde{\mathcal{A}}_1, \widetilde{\mathcal{A}}_2, \widetilde{\mathcal{A}}_3)$ has volume (area) $\frac{3}{2}$ and therefore

$$[\mathcal{L}(\widetilde{\mathcal{A}}_1, \widetilde{\mathcal{A}}_2, \widetilde{\mathcal{A}}_3) : \mathcal{L}(\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3)] \;=\; 4.$$

Thus

$$\operatorname{Res}_{\widetilde{\mathcal{A}}_1, \widetilde{\mathcal{A}}_2, \widetilde{\mathcal{A}}_3}\left(\widetilde{f}_1, \widetilde{f}_2, \widetilde{f}_3\right) \;=\; \operatorname{Res}_{\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3}(f_1, f_2, f_3)^{2\cdot 3\cdot 4}.$$

Proof:

Corollary 5.4 Let $\mathcal{B}_i$ be the support of $\widetilde{f}_i$. Since the Newton polytope generated by $\mathcal{B}_i$ equals the Newton polytope generated by $\widetilde{\mathcal{A}}_i$, we have by Theorem 5.1

$$\operatorname{Res}_{\widetilde{\mathcal{A}}_1, \ldots, \widetilde{\mathcal{A}}_n}\left(\widetilde{f}_1, \ldots, \widetilde{f}_n\right) \;=\; \operatorname{Res}_{\mathcal{B}_1, \ldots, \mathcal{B}_n}\left(\widetilde{f}_1, \ldots, \widetilde{f}_n\right)^P,$$

where P is

$$\begin{aligned}
&[\mathcal{L}(\widetilde{\mathcal{A}}_1, \widetilde{\mathcal{A}}_2, \ldots, \widetilde{\mathcal{A}}_n) : \mathcal{L}(\mathcal{B}_1, \widetilde{\mathcal{A}}_2, \ldots, \widetilde{\mathcal{A}}_n)] \\
&\qquad [\mathcal{L}(\mathcal{B}_1, \widetilde{\mathcal{A}}_2, \ldots, \widetilde{\mathcal{A}}_n) : \mathcal{L}(\mathcal{B}_1, \mathcal{B}_2, \widetilde{\mathcal{A}}_3, \ldots, \widetilde{\mathcal{A}}_n)] \\
&\qquad\qquad \cdots \\
&\qquad\qquad\qquad [\mathcal{L}(\mathcal{B}_1, \ldots, \mathcal{B}_{n-1}, \widetilde{\mathcal{A}}_n) : \mathcal{L}(\mathcal{B}_1, \ldots, \mathcal{B}_{n-1}, \mathcal{B}_n)].
\end{aligned}$$

Thus

$$P \;=\; [\mathcal{L}(\widetilde{\mathcal{A}}_1, \ldots, \widetilde{\mathcal{A}}_n) : \mathcal{L}(\mathcal{B}_1, \ldots, \mathcal{B}_n)].$$

By the construction of $\widetilde{f}_i$, we have $\mathcal{B}_i = D\mathcal{A}_i$, where D is a diagonal matrix with diagonal entries $d_1, \ldots, d_{n-1}$. Therefore $w = |d_1 \cdots d_n|\ v$, where w and v, resp., is the volume of the fundamental simplex of $\mathcal{L}(\mathcal{B}_1, \ldots, \mathcal{B}_n)$ and $\mathcal{L}(\mathcal{A}_1, \ldots, \mathcal{A}_n)$, resp. Let $\widetilde{v}$ be the volume of the fundamental simplex of $\mathcal{L}(\widetilde{\mathcal{A}}_1, \ldots, \widetilde{\mathcal{A}}_n)$. Then

$$\begin{aligned} P = \frac{w}{\widetilde{v}} &= \frac{|d_1 \cdots d_n|\ v}{\widetilde{v}} \\ &= |d_1 \cdots d_n|\ [\mathcal{L}(\widetilde{\mathcal{A}}_1, \ldots, \widetilde{\mathcal{A}}_n) : \mathcal{L}(\mathcal{A}_1, \ldots, \mathcal{A}_n)]. \end{aligned}$$

Finally, note that

$$\mathrm{Res}_{\mathcal{B}_1, \ldots, \mathcal{B}_n}\left(\widetilde{f}_1, \ldots, \widetilde{f}_n\right) = \mathrm{Res}_{\mathcal{A}_1, \ldots, \mathcal{A}_n}(f_1, \ldots, f_n).$$

Thus we have shown the corollary.

□

5.3 Proof of the main theorem

Before going into the details of the proof we describe its main structure. The proof is based on some generalization of Pedersen's and Sturmfels' Poisson-type product formula (cf. [PS93]). For the convenience of the reader we state this product formula first (cf. Theorem 5.7 and Remark 5.8). In the following lemmas we generalize this product formula and then we prove the main theorem. The dependency of the lemmas and of Pedersen's and Sturmfels' Poisson-type product formula is shown in Figure 5.2.

$$\begin{tikzcd}[column sep=tiny]
\text{Theorem 5.7 ([PS93])} \arrow[dr] & & \text{Lemma 5.9} \arrow[dl] & & \\
& \text{Lemma 5.10} \arrow[dr] & & \text{Lemma 5.11} \arrow[dl] & \\
& & \text{Lemma 5.12} \arrow[dr] & & \text{Lemma 5.13} \arrow[dl] \\
& & & \text{Theorem 5.1 (Main theorem)} &
\end{tikzcd}$$

Figure 5.2: Dependency of the lemmas

Before listing the lemmas, we fix some notations.

Notation 5.6 We let

1. $\operatorname{sign}(r)$ stand for the sign of a real number r.
2. $\operatorname{NP}(\mathcal{A}) \subset \mathbb{R}^{n-1}$ stand for the convex hull of a bounded set $\mathcal{A} \subset \mathbb{Z}^{n-1}$, mostly a **N**ewton **p**olytope.
3. $\operatorname{Vol}(P)$ stand for the volume of some polytope P.
4. $\operatorname{Vol}_L(P)$ stand for the normalized volume of some polytope P (not necessarily an L-lattice polytope), that is, the quotient between the volume of P and the volume of the fundamental simplex of the integer lattice L.
5. $\prod_\gamma f(\gamma)$, as in [PS93], stand for the product, over the common roots γ with respect to some lattice of certain Laurent polynomials, of f evaluated at γ.

We state Pedersen's and Sturmfels' Poisson-type product formula.

Theorem 5.7 ([PS93]) *If $\{\mathcal{A}_1, \ldots, \mathcal{A}_n\}$ is essential and $\mathcal{L}(\mathcal{A}_1, \ldots, \mathcal{A}_n) = \mathbb{Z}^{n-1}$, then*

$$\operatorname{Res}_{\mathcal{A}_1,\ldots,\mathcal{A}_n}(f_1, \ldots, f_n) = \prod_{\gamma} f_1(\gamma) \prod_{\omega} \operatorname{Res}_{\mathcal{A}_2^\omega,\ldots,\mathcal{A}_n^\omega}(f_2^\omega, \ldots, f_n^\omega)^{\rho_{\mathcal{A}_1,\ldots,\mathcal{A}_n}(\omega)}$$

where

$$\rho_{\mathcal{A}_1,\ldots,\mathcal{A}_n}(\omega) := -\operatorname{sign}(\mathrm{a}_{\mathcal{A}_1}(\omega)) \frac{\operatorname{Vol}_{\mathbb{Z}^{n-1}}(\mathrm{NP}(\mathcal{A}_1^\omega \cup \{0\}))}{\operatorname{Vol}_{\mathcal{L}((\mathcal{A}_2+\cdots+\mathcal{A}_n)^\omega)}(\mathrm{NP}(\mathcal{A}_1)^\omega)},$$

γ ranges over the common zeros in $(K\setminus\{0\})^{n-1}$, with respect to $\mathcal{L}(\mathcal{A}_1, \ldots, \mathcal{A}_n)$, of $f_2, \ldots, f_n$, where K is the algebraic closure of the field generated by the complex numbers and the symbolic coefficients of the f_i's, and ω ranges over the primitive inner normal vectors of the facets of the Newton polytope generated by $\mathcal{A}_2 + \cdots + \mathcal{A}_n$.

Remark 5.8 Firstly, note that in [PS93] Pedersen's and Sturmfels' Poisson-type product formula was not considered for degenerate cases where a strict subset of $\{\mathcal{A}_2^\omega, \ldots, \mathcal{A}_n^\omega\}$ is essential. However, it can be seen easily that Pedersen's and Sturmfels' Poisson-type product formula also holds for these degenerate cases if we utilize the alternative definition of the sparse resultant given in Remark 5.2. One can adjust the proof of Theorem 1.1 of [PS93] in order to handle these cases. That is, one can easily show, similarly to the proof of Line (5.4), a version of

Proposition 7.1 of [PS93] for the alternatively defined sparse resultant. The rest of the proof of Theorem 1.1 of [PS93] remains unchanged and the version, given in Theorem 5.7, of Pedersen's and Sturmfels' Poisson-type product formula follows.

Secondly, note that the presentation of the exponent $\rho_{\mathcal{A}_1,\dots,\mathcal{A}_n}(\omega)$ in Theorem 5.7 is slightly different from the presentation in [PS93]. From the proof of Lemma 2.2 of [PS93] one can easily see that both presentations are equivalent. We chose this alternative presentation because it is more suitable for this chapter.

Now we are ready to state lemmas.

In the following lemma we study a generalized version $\delta_{\mathcal{A}_1,\dots,\mathcal{A}_n}(\omega)$ of the exponent $\rho_{\mathcal{A}_1,\dots,\mathcal{A}_n}(\omega)$ of Pedersen's and Sturmfels' Theorem 5.7.

Lemma 5.9 *Let $\mathcal{B}_1,\dots,\mathcal{B}_n \subset \mathbb{Z}^{n-1}$ be finite sets and let the map M, from $\mathcal{L}(\mathcal{A}_1,\dots,\mathcal{A}_n)$ to $\mathcal{L}(\mathcal{B}_1,\dots,\mathcal{B}_n)$, be a $\mathbb{Z}$-lattice isomorphism such that $\mathcal{B}_i = M(\mathcal{A}_i)$. Then*

$$\delta_{\mathcal{A}_1,\dots,\mathcal{A}_n}(\omega) \;=\; \delta_{\mathcal{B}_1,\dots,\mathcal{B}_n}(\nu)\,,$$

where ω is a positive multiple of $M^{\mathrm{T}}(\nu)$, where M^{T} is the transpose of M, viewed as a $\mathbb{Q}$-linear map, and

$$\delta_{\mathcal{A}_1,\dots,\mathcal{A}_n}(\omega) \;:=\; -\,\mathrm{sign}\left(\mathrm{a}_{\mathcal{A}_1}(\omega)\right)\,\frac{\mathrm{Vol}_{\mathcal{L}(\mathcal{A}_1,\dots,\mathcal{A}_n)}\left(\mathrm{NP}\left(\mathcal{A}_1^{\omega}\cup\{0\}\right)\right)}{\mathrm{Vol}_{\mathcal{L}((\mathcal{A}_2+\cdots+\mathcal{A}_n)^{\omega})}\left(\mathrm{NP}\left(\mathcal{A}_1\right)^{\omega}\right)}.$$

Proof:

For $n = 1$, the lemma is trivial. Assume $n \geq 2$.

We show that $M^{-1}\left(\mathrm{NP}\left(\mathcal{B}_1\right)^{\nu}\right)$ is a face of $\mathrm{NP}\left(\mathcal{A}_1\right)$ with primitive inner normal vector ω that is a positive multiple of $M^{\mathrm{T}}(\nu)$. Firstly "$\subseteq$": Let $\langle \nu, y\rangle \geq \mathrm{a}_{\mathcal{B}_1}(\nu)$ be an inequality defining a halfspace, with primitive inner normal vector $\nu \neq 0$, that supports the Newton polytope generated by $\mathcal{B}_1$. The inequality $\left\langle M^{\mathrm{T}}(\nu), x\right\rangle \geq \mathrm{a}_{\mathcal{B}_1}(\nu)$ defines a halfspace with normal vector $M^{\mathrm{T}}(\nu) \neq 0$. By definition $M^{\mathrm{T}}(\nu)$ is an *inner* normal vector of this half space and the primitive inner normal vector ω is a positive multiple of $M^{\mathrm{T}}(\nu)$. Since $\langle \nu, y\rangle = \left\langle M^{\mathrm{T}}(\nu), M^{-1}(y)\right\rangle$ and $\mathrm{NP}\left(\mathcal{A}_1\right) = \mathrm{NP}\left(M^{-1}\left(\mathcal{B}_1\right)\right) = M^{-1}\left(\mathrm{NP}\left(\mathcal{B}_1\right)\right)$, this halfspace contains $\mathrm{NP}\left(\mathcal{A}_1\right)$ and, since the points $M^{-1}\left(\mathrm{NP}\left(\mathcal{B}_1\right)^{\nu}\right) \subseteq \mathrm{NP}\left(\mathcal{A}_1\right)$ satisfy the equality, this halfspace supports $\mathrm{NP}\left(\mathcal{A}_1\right)$. Secondly "$\supseteq$": Take $x \in \mathrm{NP}\left(\mathcal{A}_1\right)$ such that $\left\langle M^{\mathrm{T}}(\nu), x\right\rangle = \mathrm{a}_{\mathcal{B}_1}(\nu)$ and $M(x) \notin \mathrm{NP}\left(\mathcal{B}_1\right)^{\nu}$. Then $M(x)$ is contained in $M\left(\mathrm{NP}\left(\mathcal{A}_1\right)\right) = \mathrm{NP}\left(M\left(\mathcal{A}_1\right)\right) = \mathrm{NP}\left(\mathcal{B}_1\right)$ and $\langle \nu, M(x)\rangle = \mathrm{a}_{\mathcal{B}_1}(\nu)$. Contradiction!

Next observe that the second paragraph implies that

$$\operatorname{sign}\left(\mathrm{a}_{\mathcal{B}_1}(\nu)\right) = \operatorname{sign}\left(\mathrm{a}_{\mathcal{A}_1}(\omega)\right)$$

because $\mathrm{a}_{\mathcal{A}_1}(\omega)$ is a certain positive multiple of $\mathrm{a}_{\mathcal{B}_1}(\nu)$.

Next we show that

$$\mathrm{Vol}_{\mathcal{L}(\mathcal{B}_1,\ldots,\mathcal{B}_n)}\left(\mathrm{NP}\left(\mathcal{B}_1^{\nu} \cup \{0\}\right)\right) \;=\; \mathrm{Vol}_{\mathcal{L}(\mathcal{A}_1,\ldots,\mathcal{A}_n)}\left(\mathrm{NP}\left(\mathcal{A}_1^{\omega} \cup \{0\}\right)\right).$$

Let B be a basis for the lattice $\mathcal{L}(\mathcal{A}_1, \ldots, \mathcal{A}_n)$. Since the map M, from the lattice $\mathcal{L}(\mathcal{A}_1, \ldots, \mathcal{A}_n)$ to the lattice $\mathcal{L}(\mathcal{B}_1, \ldots, \mathcal{B}_n)$, is a lattice isomorphism, $M(B)$ is a basis for $\mathcal{L}(\mathcal{B}_1, \ldots, \mathcal{B}_n)$. Further, let $\Delta_{\mathcal{L}(\mathcal{A}_1,\ldots,\mathcal{A}_n)}$ and $\Delta_{\mathcal{L}(\mathcal{B}_1,\ldots,\mathcal{B}_n)}$, resp., denote the fundamental lattice simplex spanned by B and $M(B)$, resp. Then we have

$$\Delta_{\mathcal{L}(\mathcal{B}_1,\ldots,\mathcal{B}_n)} = M\left(\Delta_{\mathcal{L}(\mathcal{A}_1,\ldots,\mathcal{A}_n)}\right)$$

and thus

$$\begin{aligned}
\mathrm{Vol}_{\mathcal{L}(\mathcal{B}_1,\ldots,\mathcal{B}_n)}\left(\mathrm{NP}\left(\mathcal{B}_1^{\nu} \cup \{0\}\right)\right) &= \frac{\mathrm{Vol}\left(\mathrm{NP}\left(\mathcal{B}_1^{\nu} \cup \{0\}\right)\right)}{\mathrm{Vol}\left(\Delta_{\mathcal{L}(\mathcal{B}_1,\ldots,\mathcal{B}_n)}\right)} \\
&= \frac{\mathrm{Vol}\left(\mathrm{NP}\left(M\left(\mathcal{A}_1\right)^{\nu} \cup \{0\}\right)\right)}{\mathrm{Vol}\left(M\left(\Delta_{\mathcal{L}(\mathcal{A}_1,\ldots,\mathcal{A}_n)}\right)\right)}.
\end{aligned}$$

Since

$$\mathrm{NP}\left(M\left(\mathcal{A}_1^{\omega}\right) \cup \{0\}\right) = M\left(\mathrm{NP}\left(\mathcal{A}_1^{\omega} \cup \{0\}\right)\right),$$

for some ω, we have by the substitution rule of integration

$$\mathrm{Vol}_{\mathcal{L}(\mathcal{B}_1,\ldots,\mathcal{B}_n)}\left(\mathrm{NP}\left(\mathcal{B}_1^{\nu} \cup \{0\}\right)\right) \;=\; \frac{\mathrm{Vol}\left(\mathrm{NP}\left(\mathcal{A}_1^{\omega} \cup \{0\}\right)\right)}{\mathrm{Vol}\left(\Delta_{\mathcal{L}(\mathcal{A}_1,\ldots,\mathcal{A}_n)}\right)}.$$

Finally we show that

$$\mathrm{Vol}_{\mathcal{L}((\mathcal{B}_2+\cdots+\mathcal{B}_n)^{\nu})}\left(\mathrm{NP}\left(\mathcal{B}_1\right)^{\nu}\right) \;=\; \mathrm{Vol}_{\mathcal{L}((\mathcal{A}_2+\cdots+\mathcal{A}_n)^{\omega})}\left(\mathrm{NP}\left(\mathcal{A}_1\right)^{\omega}\right).$$

We have already seen that $\mathrm{NP}(\mathcal{B}_1)^{\nu} = M(\mathrm{NP}(\mathcal{A}_1)^{\omega})$. Further, we view the lattice $\mathcal{L}((\mathcal{A}_2 + \cdots + \mathcal{A}_n)^{\omega})$ and $\mathcal{L}((\mathcal{B}_2 + \cdots + \mathcal{B}_n)^{\nu})$, resp., as affine sublattice of $\mathcal{L}(\mathcal{A}_1, \ldots, \mathcal{A}_n)$ and $\mathcal{L}(\mathcal{B}_1, \ldots, \mathcal{B}_n)$, resp. Then

$$M : \mathcal{L}\left(\left(\mathcal{A}_2 + \cdots + \mathcal{A}_n\right)^{\omega}\right) \to \mathcal{L}\left(\left(\mathcal{B}_2 + \cdots + \mathcal{B}_n\right)^{\nu}\right)$$

is an affine lattice isomorphism and thus

$$\Delta_{\mathcal{L}((\mathcal{B}_2+\cdots+\mathcal{B}_n)^\nu)} \; = \; M\left(\Delta_{\mathcal{L}((\mathcal{A}_2+\cdots+\mathcal{A}_n)^\omega)}\right),$$

where $\Delta_{\mathcal{L}((\mathcal{B}_2+\cdots+\mathcal{B}_n)^\nu)}$ and $\Delta_{\mathcal{L}((\mathcal{A}_2+\cdots+\mathcal{A}_n)^\omega)}$, are the fundamental lattice simplices spanned by appropriate, similar to above, bases of the lattices $\mathcal{L}\left((\mathcal{B}_2+\cdots+\mathcal{B}_n)^\nu\right)$ and $\mathcal{L}\left((\mathcal{A}_2+\cdots+\mathcal{A}_n)^\omega\right)$. Since the map M restricted to the hyperplane with normal vector ω containing $\mathcal{L}\left((\mathcal{A}_2+\cdots+\mathcal{A}_n)^\omega\right)$ is obviously injective, we have by the substitution rule of integration

$$\begin{aligned}
\mathrm{Vol}_{\mathcal{L}((\mathcal{B}_2+\cdots+\mathcal{B}_n)^\nu)}\left(\mathrm{NP}\left(\mathcal{B}_1\right)^\nu\right) &= \frac{\mathrm{Vol}\left(\mathrm{NP}\left(\mathcal{B}_1\right)^\nu\right)}{\mathrm{Vol}\left(\Delta_{\mathcal{L}((\mathcal{B}_2+\cdots+\mathcal{B}_n)^\nu)}\right)} \\
&= \frac{\mathrm{Vol}\left(M\left(\mathrm{NP}\left(\mathcal{A}_1\right)^\omega\right)\right)}{\mathrm{Vol}\left(M\left(\Delta_{\mathcal{L}((\mathcal{A}_2+\cdots+\mathcal{A}_n)^\omega)}\right)\right)} \\
&= \frac{\mathrm{Vol}\left(\mathrm{NP}\left(\mathcal{A}_1\right)^\omega\right)}{\mathrm{Vol}\left(\Delta_{\mathcal{L}((\mathcal{A}_2+\cdots+\mathcal{A}_n)^\omega)}\right)}.
\end{aligned}$$

Thus we have shown the lemma.

□

Essentially, the following lemma contains the Poisson-type product formula for sparse resultant shown by Pedersen and Sturmfels. In [PS93] they show a formula assuming that the lattice generated by the supports of $f_1, \ldots, f_n$ is $\mathbb{Z}^{n-1}$. We remove this assumption.

Lemma 5.10 *If* $\{\mathcal{A}_1, \ldots, \mathcal{A}_n\}$ *is essential, then*

$$\operatorname{Res}_{\mathcal{A}_1,\ldots,\mathcal{A}_n}(f_1, \ldots, f_n) = \prod_\gamma f_1(\gamma) \prod_\omega \operatorname{Res}_{\mathcal{A}_2^\omega,\ldots,\mathcal{A}_n^\omega}(f_2^\omega, \ldots, f_n^\omega)^{\delta_{\mathcal{A}_1,\ldots,\mathcal{A}_n}(\omega)}$$

where γ *ranges over the common zeros in* $(K\setminus\{0\})^{n-1}$*, with respect to the lattice* $\mathcal{L}(\mathcal{A}_1, \ldots, \mathcal{A}_n)$*, of* $f_2, \ldots, f_n$*, where* K *is the algebraic closure of the field generated by the complex numbers and the symbolic coefficients of the* f_i*'s,* $\delta_{\ldots}(\omega)$ *is as defined in Lemma 5.9 and* ω *ranges over the primitive inner normal vectors of the facets of the Newton polytope generated by* $\mathcal{A}_2 + \cdots + \mathcal{A}_n$*.*

Proof:

Note that, since $\{\mathcal{A}_1, \ldots, \mathcal{A}_n\}$ is essential, $\mathcal{L}(\mathcal{A}_1, \ldots, \mathcal{A}_n)$ is a sublattice of $\mathbb{Z}^{n-1}$ of rank $n-1$. By mapping a basis of $\mathcal{L}(\mathcal{A}_1, \ldots, \mathcal{A}_n)$ onto the canoncial basis of $\mathbb{Z}^{n-1}$ we construct a lattice isomorphism M from $\mathcal{L}(\mathcal{A}_1, \ldots, \mathcal{A}_n)$ to $\mathcal{L}(\mathcal{B}_1, \ldots, \mathcal{B}_n)$, where $\mathcal{B}_i := M(\mathcal{A}_i)$. Further we canonically extend M to Laurent polynomials with support in $\mathcal{L}(\mathcal{A}_1, \ldots, \mathcal{A}_n)$ and let g_i stand for the image of f_i under M.

Note that $\operatorname{Res}_{\mathcal{A}_1,\ldots,\mathcal{A}_n}(f_1, \ldots, f_n) = \operatorname{Res}_{\mathcal{B}_1,\ldots,\mathcal{B}_n}(g_1, \ldots, g_n)$.

Further, by the Poisson-type product formula of [PS93] (cf. Theorem 5.7), we have

$$\operatorname{Res}_{\mathcal{B}_1,\ldots,\mathcal{B}_n}(g_1,\ldots,g_n) = \prod_{\beta} g_1(\beta) \prod_{\nu} \operatorname{Res}_{\mathcal{B}_2^{\nu},\ldots,\mathcal{B}_n^{\nu}}(g_2^{\nu},\ldots,g_n^{\nu})^{\delta_{\mathcal{B}_1,\ldots,\mathcal{B}_n}(\nu)},$$

where β ranges over the common zeros in $(K\setminus\{0\})^{n-1}$ of $g_2,\ldots,g_n$ with respect to $\mathcal{L}(\mathcal{B}_1,\ldots,\mathcal{B}_n)$, where K is the algebraic closure of the field generated by the complex numbers and the symbolic coefficients of the g_i's and ν ranges over the primitive inner normal vectors of the facets of the Newton polytope generated by $\mathcal{B}_2+\cdots+\mathcal{B}_n$. Since M is invertible and by Lemma 5.9, we have

$$\operatorname{Res}_{\mathcal{B}_1,\ldots,\mathcal{B}_n}(g_1,\ldots,g_n) = \prod_{\beta} g_1(\beta) \prod_{\omega} \operatorname{Res}_{\mathcal{A}_2^{\omega},\ldots,\mathcal{A}_n^{\omega}}(f_2^{\omega},\ldots,f_n^{\omega})^{\delta_{\mathcal{A}_1,\ldots,\mathcal{A}_n}(\omega)},$$

where ω ranges over the primitive inner normal vectors of the facets of the Newton polytope generated by $\mathcal{A}_2+\cdots+\mathcal{A}_n$. Now, observe that by the construction (cf. [PS93]) of $\prod_{\beta} g_1(\beta)$, we have

$$\prod_{\beta} g_1(\beta) = \prod_{\gamma} f_1(\gamma),$$

where γ ranges over the common zeros in $(K\setminus\{0\})^{n-1}$ of $f_2,\ldots,f_n$ with respect to $\mathcal{L}(\mathcal{A}_1,\ldots,\mathcal{A}_n)$.

Thus we have shown the lemma.

□

Next we rewrite the exponent $\delta_{\mathcal{A}_1,\dots,\mathcal{A}_n}(\omega)$.

Lemma 5.11

$$\delta_{\mathcal{A}_1,\dots,\mathcal{A}_n}(\omega) \;=\; -\frac{\mathrm{a}_{\mathcal{A}_1}(\omega)\;[\mathrm{H}^\omega : \mathcal{L}(\mathcal{A}_2^\omega,\dots,\mathcal{A}_n^\omega)]}{[\mathbb{Z}^{n-1} : \mathcal{L}(\mathcal{A}_1,\dots,\mathcal{A}_n)]},$$

where $\delta_{\mathcal{A}_1,\dots,\mathcal{A}_n}(\omega)$ *is defined in Lemma 5.9.*

Proof:

Note that

$$\delta_{\mathcal{A}_1,\dots,\mathcal{A}_n}(\omega) \;=\; -\operatorname{sign}(\mathrm{a}_{\mathcal{A}_1}(\omega))\;\frac{\frac{\mathrm{Vol}(\mathrm{NP}(\mathrm{NP}(\mathcal{A}_1)^\omega)\cup\{0\})}{v}}{\frac{\mathrm{Vol}(\mathrm{NP}(\mathcal{A}_1)^\omega)}{v^\omega}},$$

where v and v^ω, resp., is the volume of the fundamental simplex of the lattice generated by $\mathcal{A}_1,\dots,\mathcal{A}_n$ and $(\mathcal{A}_2+\cdots+\mathcal{A}_n)^\omega$, resp. Note that

$$\mathrm{Vol}(\mathrm{NP}(\mathrm{NP}(\mathcal{A}_1)^\omega\cup\{0\})) \;=\; \frac{\mathrm{Vol}(\mathrm{NP}(\mathcal{A}_1)^\omega)\;d^\omega}{n-1},$$

where d^ω is the distance of the origin from the hyperplane supporting $\mathrm{NP}(\mathcal{A}_1)^\omega$. Thus

$$\begin{aligned}
\delta_{\mathcal{A}_1,\dots,\mathcal{A}_n}(\omega) &= -\operatorname{sign}(\mathrm{a}_{\mathcal{A}_1}(\omega))\;d^\omega\;v^\omega\;\frac{1}{(n-1)\,v}\\
&= -\operatorname{sign}(\mathrm{a}_{\mathcal{A}_1}(\omega))\;d^\omega\;(n-2)!\,h^\omega\;\frac{v^\omega}{h^\omega}\;\frac{1}{(n-1)!\,v}\\
&= \frac{-\operatorname{sign}(\mathrm{a}_{\mathcal{A}_1}(\omega))\;d^\omega\;(n-2)!\,h^\omega}{[\mathbb{Z}^{n-1} : \mathcal{L}(\mathcal{A}_1,\dots,\mathcal{A}_n)]}\;\frac{v^\omega}{h^\omega},
\end{aligned}$$

where h^ω is the volume of the fundamental simplex of the lattice of all integer points contained in the hyperplane, passing through the origin, with normal vector ω.

Now, by [CLO98], page 319, we have $\|\omega\| = (n-2)!\, h^\omega$, where $\|\omega\|$ stands for the Euclidean norm of ω. Further, it is easy to see that we have

$$\operatorname{sign}\left(\mathrm{a}_{\mathcal{A}_1}(\omega)\right)\; d^\omega \;\; \|\omega\| \;=\; \mathrm{a}_{\mathcal{A}_1}(\omega)$$

and thus we have shown the lemma.

$\square$

Now we further generalize the Poisson-type product formula of Lemma 5.10. In the following lemma the set $\{\mathcal{A}_1, \ldots, \mathcal{A}_n\}$ is not necessarily the unique essential subset of $\{\mathcal{A}_1, \ldots, \mathcal{A}_n\}$.

Lemma 5.12 *If $\mathcal{A}_1$ is contained in the unique essential subset of the set $\{\mathcal{A}_1, \ldots, \mathcal{A}_n\}$, then*

$$\operatorname{Res}_{\mathcal{A}_1,\ldots,\mathcal{A}_n}(f_1, \ldots, f_n) \;=\; \prod_{\gamma} f_1(\gamma) \;\prod_{\omega} \operatorname{Res}_{\mathcal{A}_2^\omega,\ldots,\mathcal{A}_n^\omega}\left(f_2^\omega, \ldots, f_n^\omega\right)^{\delta_{\mathcal{A}_1,\ldots,\mathcal{A}_n}(\omega)}$$

where γ ranges over the common zeros in $(K\setminus\{0\})^{n-1}$, with respect to the lattice $\mathcal{L}(\mathcal{A}_1, \ldots, \mathcal{A}_n)$, of $f_2, \ldots, f_n$, where K is the algebraic closure of the field generated by the complex numbers and the symbolic coefficients of the f_i's, $\delta_{\ldots}(\omega)$ is *as defined in Lemma 5.9 and ω ranges over the primitive inner normal vectors of the facets of the Newton polytope generated by $\mathcal{A}_2 + \cdots + \mathcal{A}_n$.*

Proof:

If $\{\mathcal{A}_1, \ldots, \mathcal{A}_n\}$ is the unique essential subset of $\{\mathcal{A}_1, \ldots, \mathcal{A}_n\}$ then the formula holds by Lemma 5.10.

Suppose, without loss of generality, $\{\mathcal{A}_1, \ldots, \mathcal{A}_k\}$ is the uniqe essential subset of $\{\mathcal{A}_1, \ldots, \mathcal{A}_n\}$. Further let $\mathcal{B}$ be the set of vertices of the standard simplex of $\mathbb{R}^{n-1}$ and g be a polynomial with distinct symbolic coefficients with support $\mathcal{B}$. The overall strategy of the proof is as follows. We factorize

$$\mathrm{Res}_{\mathcal{A}_1+\mathcal{B}, \mathcal{A}_2, \ldots, \mathcal{A}_n}(f_1\, g, f_2, \ldots, f_n)$$

in two different ways. One factorization is the right hand side of the lemma raised by some power times some factor and the second factorization is the left hand side of the lemma raised by the same power times the same factor. Thus the lemma follows up to some factor that is a certain root of unity. Then we show that this root of unity is one.

Now we carry out this startegy. Note that $f_1\, g$ has support $\mathcal{A}_1 + \mathcal{B}$. Further note that the Newton polytope of $f_1\, g$ is $(n-1)$-dimensional and therefore

$\{\mathcal{A}_1 + \mathcal{B}, \mathcal{A}_2, \ldots, \mathcal{A}_n\}$ is essential. By Lemma 5.10 we have

$$\operatorname{Res}_{\mathcal{A}_1+\mathcal{B},\mathcal{A}_2,\ldots,\mathcal{A}_n}(f_1\, g, f_2, \ldots, f_n) = \prod_{\beta} f_1(\beta)\; g(\beta) \prod_{\omega} \operatorname{Res}_{\mathcal{A}_2^{\omega},\ldots,\mathcal{A}_n^{\omega}}(f_2^{\omega}, \ldots, f_n^{\omega})^{\delta_{\mathcal{A}_1+\mathcal{B},\mathcal{A}_2,\ldots,\mathcal{A}_n}(\omega)}$$

where β ranges over the common zeros in $(K\setminus\{0\})^{n-1}$, with respect to the lattice $\mathcal{L}(\mathcal{A}_1 + \mathcal{B}, \mathcal{A}_2, \ldots, \mathcal{A}_n)$, of $f_2, \ldots, f_n$, where K is the algebraic closure of the field generated by the complex numbers and the symbolic coefficients of g and the f_i's, $\delta_{\ldots}(\omega)$ is as defined in Lemma 5.9 and ω ranges over the primitive inner normal vectors of the facets of the Newton polytope generated by $\mathcal{A}_2 + \cdots + \mathcal{A}_n$. Note that by Exercise 3, page 318, of [CLO98] the Newton polytope of $f_1\, g$ equals $\mathrm{NP}(\mathcal{A}_1) + \mathrm{NP}(\mathcal{B})$ and thus by Exercise 12, page 325, of [CLO98], we have $\mathrm{a}_{\mathcal{A}_1+\mathcal{B}}(\omega) = \mathrm{a}_{\mathcal{A}_1}(\omega) + \mathrm{a}_{\mathcal{B}}(\omega)$ and therefore, by Lemma 5.11,

$$\begin{aligned}
&\delta_{\mathcal{A}_1+\mathcal{B},\mathcal{A}_2,\ldots,\mathcal{A}_n}(\omega) \\
&= \frac{\mathrm{a}_{\mathcal{A}_1+\mathcal{B}}(\omega)\;[\mathrm{H}^{\omega} : \mathcal{L}(\mathcal{A}_2^{\omega}, \ldots, \mathcal{A}_n^{\omega})]}{[\mathbb{Z}^{n-1} : \mathcal{L}(\mathcal{A}_1 + \mathcal{B}, \mathcal{A}_2, \ldots, \mathcal{A}_n)]} \\
&= \frac{\mathrm{a}_{\mathcal{A}_1}(\omega)\;[\mathrm{H}^{\omega} : \mathcal{L}(\mathcal{A}_2^{\omega}, \ldots, \mathcal{A}_n^{\omega})]}{[\mathbb{Z}^{n-1} : \mathcal{L}(\mathcal{A}_1 + \mathcal{B}, \mathcal{A}_2, \ldots, \mathcal{A}_n)]} + \frac{\mathrm{a}_{\mathcal{B}}(\omega)\;[\mathrm{H}^{\omega} : \mathcal{L}(\mathcal{A}_2^{\omega}, \ldots, \mathcal{A}_n^{\omega})]}{[\mathbb{Z}^{n-1} : \mathcal{L}(\mathcal{A}_1 + \mathcal{B}, \mathcal{A}_2, \ldots, \mathcal{A}_n)]}.
\end{aligned}$$

Further

$$\begin{aligned}
&\delta_{\mathcal{A}_1+\mathcal{B},\mathcal{A}_2,\ldots,\mathcal{A}_n}(\omega) = \\
&\quad \delta_{\mathcal{A}_1,\ldots,\mathcal{A}_n}(\omega)\,[\mathcal{L}(\mathcal{A}_1 + \mathcal{B}, \mathcal{A}_2, \ldots, \mathcal{A}_n) : \mathcal{L}(\mathcal{A}_1, \ldots, \mathcal{A}_n)] \\
&\quad + \delta_{\mathcal{B},\mathcal{A}_2,\ldots,\mathcal{A}_n}(\omega)\,[\mathcal{L}(\mathcal{A}_1 + \mathcal{B}, \mathcal{A}_2, \ldots, \mathcal{A}_n) : \mathcal{L}(\mathcal{B}, \mathcal{A}_2, \ldots, \mathcal{A}_n)],
\end{aligned}$$

because

$$\begin{aligned}
&\left[\mathbb{Z}^{n-1} : \mathcal{L}\left(\mathcal{A}_1 + \mathcal{B}, \mathcal{A}_2, \ldots, \mathcal{A}_n\right)\right] \\
&= \frac{\left[\mathbb{Z}^{n-1} : \mathcal{L}\left(\mathcal{A}_1, \ldots, \mathcal{A}_n\right)\right]}{\left[\mathcal{L}\left(\mathcal{A}_1 + \mathcal{B}, \mathcal{A}_2, \ldots, \mathcal{A}_n\right) : \mathcal{L}\left(\mathcal{A}_1, \ldots, \mathcal{A}_n\right)\right]} \\
&= \frac{\left[\mathbb{Z}^{n-1} : \mathcal{L}\left(\mathcal{B}, \mathcal{A}_2, \ldots, \mathcal{A}_n\right)\right]}{\left[\mathcal{L}\left(\mathcal{A}_1 + \mathcal{B}, \mathcal{A}_2, \ldots, \mathcal{A}_n\right) : \mathcal{L}\left(\mathcal{B}, \mathcal{A}_2, \ldots, \mathcal{A}_n\right)\right]}.
\end{aligned}$$

Thus, by Lemma 5.10 and by the construction of $\prod_\beta f_1(\beta)\, g(\beta)$ (cf. [PS93]),

$$\begin{aligned}
&\operatorname{Res}_{\mathcal{A}_1+\mathcal{B},\mathcal{A}_2,\ldots,\mathcal{A}_n}\left(f_1\, g, f_2, \ldots, f_n\right) \\
&= \prod_\beta f_1(\beta) \prod_\omega \operatorname{Res}_{\mathcal{A}_2^\omega,\ldots,\mathcal{A}_n^\omega}\left(f_2^\omega, \ldots, f_n^\omega\right)^{\delta_{\mathcal{A}_1,\ldots,\mathcal{A}_n}(\omega)\, I_1} \\
&\quad \prod_\beta g(\beta) \prod_\omega \operatorname{Res}_{\mathcal{A}_2^\omega,\ldots,\mathcal{A}_n^\omega}\left(f_2^\omega, \ldots, f_n^\omega\right)^{\delta_{\mathcal{B},\mathcal{A}_2,\ldots,\mathcal{A}_n}(\omega)\, I_2} \\
&= \prod_\beta f_1(\beta) \prod_\omega \operatorname{Res}_{\mathcal{A}_2^\omega,\ldots,\mathcal{A}_n^\omega}\left(f_2^\omega, \ldots, f_n^\omega\right)^{\delta_{\mathcal{A}_1,\ldots,\mathcal{A}_n}(\omega)\, I_1} \\
&\quad \left(\prod_{\beta''} g(\beta'') \prod_\omega \operatorname{Res}_{\mathcal{A}_2^\omega,\ldots,\mathcal{A}_n^\omega}\left(f_2^\omega, \ldots, f_n^\omega\right)^{\delta_{\mathcal{B},\mathcal{A}_2,\ldots,\mathcal{A}_n}(\omega)}\right)^{I_2} \\
&= \prod_\beta f_1(\beta) \prod_\omega \operatorname{Res}_{\mathcal{A}_2^\omega,\ldots,\mathcal{A}_n^\omega}\left(f_2^\omega, \ldots, f_n^\omega\right)^{\delta_{\mathcal{A}_1,\ldots,\mathcal{A}_n}(\omega)\, I_1} \\
&\quad \operatorname{Res}_{\mathcal{B},\mathcal{A}_2,\ldots,\mathcal{A}_n}\left(g, f_2, \ldots, f_n\right)^{I_2}, \qquad (5.1)
\end{aligned}$$

where β'' ranges over the common zeros in $(L\setminus\{0\})^{n-1}$, with respect to the lattice $\mathcal{L}(\mathcal{B}, \mathcal{A}_2, \ldots, \mathcal{A}_n)$, of $f_2, \ldots, f_n$, where L is the algebraic closure of the field generated by the complex numbers and the symbolic coefficients of g and $f_2, \ldots, f_n$ and where

$$I_1 = \left[\mathcal{L}\left(\mathcal{A}_1 + \mathcal{B}, \mathcal{A}_2, \ldots, \mathcal{A}_n\right) : \mathcal{L}\left(\mathcal{A}_1, \ldots, \mathcal{A}_n\right)\right]$$

$$I_2 = \left[\mathcal{L}\left(\mathcal{A}_1 + \mathcal{B}, \mathcal{A}_2, \ldots, \mathcal{A}_n\right) : \mathcal{L}\left(\mathcal{B}, \mathcal{A}_2, \ldots, \mathcal{A}_n\right)\right].$$

Now we rewrite Line (5.1) further. Note that

$$\prod_{\beta} f_1(\beta) = \left(\prod_{\beta'} f_1(\beta')\right)^{[\mathcal{L}(\mathcal{A}_1+\mathcal{B},\mathcal{A}_2,\dots,\mathcal{A}_n):\mathcal{L}(\mathcal{A}_1,\dots,\mathcal{A}_n)]\ \mathrm{e}_{\mathcal{A}_1,\dots,\mathcal{A}_n}}, \tag{5.2}$$

where β' ranges over the common zeros in $(K' \setminus \{0\})^{n-1}$, with respect to the lattice $\mathcal{L}(\mathcal{A}_1, \dots, \mathcal{A}_k)$, of $f_2, \dots, f_k$, where K' is the algebraic closure of the field generated by the complex numbers and the symbolic coefficients of $f_1, \dots, f_k$. Therefore we conclude by Lemma 5.12 that

$$\begin{aligned} &\mathrm{Res}_{\mathcal{A}_1+\mathcal{B},\mathcal{A}_2,\dots,\mathcal{A}_n}(f_1\, g, f_2, \dots, f_n) \\ &= \mathrm{Res}_{\mathcal{A}_1,\dots,\mathcal{A}_n}(f_1, \dots, f_n)^{[\mathcal{L}(\mathcal{A}_1+\mathcal{B},\mathcal{A}_2,\dots,\mathcal{A}_n):\mathcal{L}(\mathcal{A}_1,\dots,\mathcal{A}_n)]} \\ &\quad\ \mathrm{Res}_{\mathcal{B},\mathcal{A}_2,\dots,\mathcal{A}_n}(g, f_2, \dots, f_n)^{[\mathcal{L}(\mathcal{A}_1+\mathcal{B},\mathcal{A}_2,\dots,\mathcal{A}_n):\mathcal{L}(\mathcal{B},\mathcal{A}_2,\dots,\mathcal{A}_n)]} \\ &\quad\ Q, \end{aligned}$$

where Q is a rational function depending only on the coefficients of the Laurent polynomials $f_2, \dots, f_n$. Now we show that Q is 1. First we observe that Q is a polynomial: Obviously $Q = \frac{R}{S}$, where R and S are relatively prime polynomials. Since the left hand side of the previous equality is a polynomial, the denominator S divides either

$$\mathrm{Res}_{\mathcal{A}_1,\dots,\mathcal{A}_n}(f_1, \dots, f_n)$$

or

$$\mathrm{Res}_{\mathcal{B},\mathcal{A}_2,\dots,\mathcal{A}_n}(g, f_2, \dots, f_n).$$

Since these two resultants are irreducible and depend on either f_1 or g, the denominator S, which does not depend on f_1 or g, is a constant. Next we show that the total degree of Q in the coefficients of $f_2, \ldots, f_{n-1}$ and f_n, resp., is zero. That is, we show that, for $i \geq 2$,

$$\frac{\mathrm{MV}\left(\mathrm{NP}\left(\mathcal{A}_1+\mathcal{B}\right), \mathrm{NP}\left(\mathcal{A}_2\right), \ldots, \mathrm{NP}\left(\mathcal{A}_{i-1}\right), \mathrm{NP}\left(\mathcal{A}_{i+1}\right), \ldots, \mathrm{NP}\left(\mathcal{A}_n\right)\right)}{\left[\mathbb{Z}^{n-1}: \mathcal{L}\left(\mathcal{A}_1+\mathcal{B}, \mathcal{A}_2, \ldots, \mathcal{A}_n\right)\right]} =$$
$$\frac{\mathrm{MV}\left(\mathrm{NP}\left(\mathcal{M}_1\right), \ldots, \mathrm{NP}\left(\mathcal{M}_{i-1}\right), \mathrm{NP}\left(\mathcal{M}_{i+1}\right), \ldots, \mathrm{NP}\left(\mathcal{M}_k\right)\right)\ E_1}{\left[\mathbb{Z}^{k-1}: \mathcal{L}\left(\mathcal{M}_1, \ldots, \mathcal{M}_k\right)\right]}$$
$$+\ \frac{\mathrm{MV}\left(\mathrm{NP}\left(\mathcal{B}\right), \mathrm{NP}\left(\mathcal{A}_2\right), \ldots, \mathrm{NP}\left(\mathcal{A}_{i-1}\right), \mathrm{NP}\left(\mathcal{A}_{i+1}\right), \ldots, \mathrm{NP}\left(\mathcal{A}_n\right)\right)\ E_2}{\left[\mathbb{Z}^{n-1}: \mathcal{L}\left(\mathcal{B}, \mathcal{A}_2, \ldots, \mathcal{A}_n\right)\right]}, \quad (5.3)$$

where

$$E_1 = \mathrm{e}_{\mathcal{A}_1, \ldots, \mathcal{A}_n}\ \left[\mathcal{L}\left(\mathcal{A}_1+\mathcal{B}, \mathcal{A}_2, \ldots, \mathcal{A}_n\right): \mathcal{L}\left(\mathcal{A}_1, \ldots, \mathcal{A}_n\right)\right],$$

$$E_2 = \left[\mathcal{L}\left(\mathcal{A}_1+\mathcal{B}, \mathcal{A}_2, \ldots, \mathcal{A}_n\right): \mathcal{L}\left(\mathcal{B}, \mathcal{A}_2, \ldots, \mathcal{A}_n\right)\right],$$

$M: \mathcal{L}\left(\mathcal{A}_1, \ldots, \mathcal{A}_k\right) \rightarrow \mathbb{Z}^{k-1}$ is a lattice embedding, $\mathcal{M}_i$ stands for $M\left(\mathcal{A}_i\right)$ and $\mathrm{MV}(.)$ stands for the mixed volume (cf. [CLO98]). Now, equality (5.3) can be proven as follows: By Exercise 3, page 318, and by Exercise 12, page 325, of [CLO98] and by the multilinearity of the mixed volume

$$\frac{\mathrm{MV}\left(\mathrm{NP}\left(\mathcal{A}_1+\mathcal{B}\right), \mathrm{NP}\left(\mathcal{A}_2\right), \ldots, \mathrm{NP}\left(\mathcal{A}_{i-1}\right), \mathrm{NP}\left(\mathcal{A}_{i+1}\right), \ldots, \mathrm{NP}\left(\mathcal{A}_n\right)\right)}{\left[\mathbb{Z}^{n-1}: \mathcal{L}\left(\mathcal{A}_1+\mathcal{B}, \mathcal{A}_2, \ldots, \mathcal{A}_n\right)\right]} =$$
$$\frac{\mathrm{MV}\left(\mathrm{NP}\left(\mathcal{A}_1\right), \mathrm{NP}\left(\mathcal{A}_2\right), \ldots, \mathrm{NP}\left(\mathcal{A}_{i-1}\right), \mathrm{NP}\left(\mathcal{A}_{i+1}\right), \ldots, \mathrm{NP}\left(\mathcal{A}_n\right)\right)}{\left[\mathbb{Z}^{n-1}: \mathcal{L}\left(\mathcal{A}_1+\mathcal{B}, \mathcal{A}_2, \ldots, \mathcal{A}_n\right)\right]} +$$
$$\frac{\mathrm{MV}\left(\mathrm{NP}\left(\mathcal{B}\right), \mathrm{NP}\left(\mathcal{A}_2\right), \ldots, \mathrm{NP}\left(\mathcal{A}_{i-1}\right), \mathrm{NP}\left(\mathcal{A}_{i+1}\right), \ldots, \mathrm{NP}\left(\mathcal{A}_n\right)\right)}{\left[\mathbb{Z}^{n-1}: \mathcal{L}\left(\mathcal{A}_1+\mathcal{B}, \mathcal{A}_2, \ldots, \mathcal{A}_n\right)\right]}.$$

In order to further rewrite this equality we apply Bernshtein's theorem (cf.

[CLO98], [GKZ94]):

$$\frac{\mathrm{MV}\left(\mathrm{NP}\left(\mathcal{A}_1\right), \mathrm{NP}\left(\mathcal{A}_2\right), \ldots, \mathrm{NP}\left(\mathcal{A}_{i-1}\right), \mathrm{NP}\left(\mathcal{A}_{i+1}\right), \ldots, \mathrm{NP}\left(\mathcal{A}_n\right)\right)}{\left[\mathbb{Z}^{n-1} : \mathcal{L}\left(\mathcal{A}_1, \mathcal{A}_2, \ldots, \mathcal{A}_n\right)\right]}$$

is the number of roots with respect to the lattice $\mathcal{L}\left(\mathcal{A}_1, \ldots, \mathcal{A}_n\right)$ of a system of Laurent polynomial equations with symbolic coefficients with supports $\mathcal{A}_1, \mathcal{A}_2, \ldots, \mathcal{A}_{i-1}, \mathcal{A}_{i+1}, \ldots, \mathcal{A}_n$, where obviously the roots are defined over the algebraic closure of the field generated by the complex numbers and the symbolic coefficients of the Laurent polynomials. Similarly one can interpret the first summand in the right hand side of Line (5.3). Thus we see by the definition of e... that

$$\frac{\mathrm{MV}\left(\mathrm{NP}\left(\mathcal{A}_1\right), \mathrm{NP}\left(\mathcal{A}_2\right), \ldots, \mathrm{NP}\left(\mathcal{A}_{i-1}\right), \mathrm{NP}\left(\mathcal{A}_{i+1}\right), \ldots, \mathrm{NP}\left(\mathcal{A}_n\right)\right)}{\left[\mathbb{Z}^{n-1} : \mathcal{L}\left(\mathcal{A}_1 + \mathcal{B}, \mathcal{A}_2, \ldots, \mathcal{A}_n\right)\right]} = \frac{\mathrm{MV}\left(\mathrm{NP}\left(\mathcal{M}_1\right), \ldots, \mathrm{NP}\left(\mathcal{M}_{i-1}\right), \mathrm{NP}\left(\mathcal{M}_{i+1}\right), \ldots, \mathrm{NP}\left(\mathcal{M}_k\right)\right) \ E_1}{\left[\mathbb{Z}^{k-1} : \mathcal{L}\left(\mathcal{M}_1, \ldots, \mathcal{M}_k\right)\right]}$$

and we also see easily that

$$\frac{\mathrm{MV}\left(\mathrm{NP}\left(\mathcal{B}\right), \mathrm{NP}\left(\mathcal{A}_2\right), \ldots, \mathrm{NP}\left(\mathcal{A}_{i-1}\right), \mathrm{NP}\left(\mathcal{A}_{i+1}\right), \ldots, \mathrm{NP}\left(\mathcal{A}_n\right)\right)}{\left[\mathbb{Z}^{n-1} : \mathcal{L}\left(\mathcal{A}_1 + \mathcal{B}, \mathcal{A}_2, \ldots, \mathcal{A}_n\right)\right]} = \frac{\mathrm{MV}\left(\mathrm{NP}\left(\mathcal{B}\right), \mathrm{NP}\left(\mathcal{A}_2\right), \ldots, \mathrm{NP}\left(\mathcal{A}_{i-1}\right), \mathrm{NP}\left(\mathcal{A}_{i+1}\right), \ldots, \mathrm{NP}\left(\mathcal{A}_n\right)\right) \ E_2}{\left[\mathbb{Z}^{n-1} : \mathcal{L}\left(\mathcal{B}, \mathcal{A}_2, \ldots, \mathcal{A}_n\right)\right]}.$$

Thus we have shown equality (5.3) and therefore Q is a constant. Now, by the construction of Q, we have that Q is of the form $Q_1^{\alpha_1} \cdots Q_m^{\alpha_m}$ and, since Q is a constant, we have $\alpha_j = 0$ and $Q = 1$. Thus we have shown that

$$\begin{aligned}
&\operatorname{Res}_{\mathcal{A}_1+\mathcal{B},\mathcal{A}_1,\dots,\mathcal{A}_n}(f_1\, g, f_2, \dots, f_n) \\
&= \operatorname{Res}_{\mathcal{A}_1,\dots,\mathcal{A}_n}(f_1, \dots, f_n)^{[\mathcal{L}(\mathcal{A}_1+\mathcal{B},\mathcal{A}_2,\dots,\mathcal{A}_n):\mathcal{L}(\mathcal{A}_1,\dots,\mathcal{A}_n)]} \\
&\qquad \operatorname{Res}_{\mathcal{B},\mathcal{A}_1,\dots,\mathcal{A}_n}(g, f_2, \dots, f_n)^{[\mathcal{L}(\mathcal{A}_1+\mathcal{B},\mathcal{A}_2,\dots,\mathcal{A}_n):\mathcal{L}(\mathcal{B},\mathcal{A}_2,\dots,\mathcal{A}_n)]}. \qquad (5.4)
\end{aligned}$$

Since the right hand side of Line (5.1) equals the right hand side of Line (5.4), by taking into account Line (5.2) and the equality

$$\prod_{\gamma} f_1(\gamma) = \left(\prod_{\beta'} f_1(\beta')\right)^{\mathrm{e}_{\mathcal{A}_1,\dots,\mathcal{A}_n}}, \qquad (5.5)$$

the formula of the lemma holds up to a certain constant factor σ, namely an $[\mathcal{L}(\mathcal{A}_1 + \mathcal{B}, \mathcal{A}_2, \dots, \mathcal{A}_n) : \mathcal{L}(\mathcal{A}_1, \dots, \mathcal{A}_n)]$-th root of unity.

Now, we show that $\sigma = 1$. By Lemma 5.10 and Remark 5.2, we have

$$\begin{aligned}
\operatorname{Res}_{\mathcal{A}_1,\dots,\mathcal{A}_n}(f_1, \dots, f_n) = \Bigg(&\prod_{\beta'} f_1(\beta') \\
&\prod_{\nu} \operatorname{Res}_{M(\mathcal{A}_2)^\nu,\dots,M(\mathcal{A}_k)^\nu}\left(M(f_2)^\nu, \dots, M(f_k)^\nu\right)^{\delta_{M(\mathcal{A}_1),\dots,M(\mathcal{A}_k)}(\nu)}\Bigg)^{E},
\end{aligned}$$

where $E := \mathrm{e}_{\mathcal{A}_1,\dots,\mathcal{A}_n}$, the vector ν ranges over the primitive inner normal vectors of the facets of the Newton polytope generated by $M(\mathcal{A}_2) + \cdots + M(\mathcal{A}_k)$, where $M : \mathcal{L}(\mathcal{A}_1, \dots, \mathcal{A}_k) \to \mathbb{Z}^{k-1}$ is some lattice isomorphism which we naturally extend to the f_i's. Since this factorization of $\operatorname{Res}_{\mathcal{A}_1,\dots,\mathcal{A}_n}(f_1, \dots, f_n)$ equals the factorization, we have derived previously and because of Line 5.5, we have $\sigma = 1$.

Thus we have shown the lemma.

$\square$

Lemma 5.13 *The set* $\{\mathcal{A}_1, \ldots, \mathcal{A}_n\}$ *has a unique essential subset containing* $\mathcal{A}_1$.

Proof:

If $\mathcal{A}_1$ consists only of one point then obviously $\{\mathcal{A}_1\}$ is the unique essential subset of $\{\mathcal{A}_1, \ldots, \mathcal{A}_n\}$.

Suppose $\dim(\mathcal{L}(\mathcal{A}_1)) \geq 1$, where $\dim(L)$ denotes the rank of an integer lattice L. Since $\dim(\mathcal{L}(\mathcal{A}_1, \ldots, \mathcal{A}_n)) \leq n-1$, the set $\{\mathcal{A}_1, \ldots, \mathcal{A}_n\}$ has an essential subset: otherwise, for $i = 1, \ldots, n$, $\dim(\mathcal{L}(\mathcal{A}_1, \ldots, \mathcal{A}_i)) \geq i$, which contradicts $\dim(\mathcal{L}(\mathcal{A}_1, \ldots, \mathcal{A}_n)) \leq n-1$.

The support $\mathcal{A}_1$ is contained in any essential subset of $\{\mathcal{A}_1, \ldots, \mathcal{A}_n\}$; otherwise $\{\widetilde{\mathcal{A}}_1, \mathcal{A}_2, \ldots, \mathcal{A}_n\}$ has a subset being essential but not containing $\widetilde{\mathcal{A}}_1$. Take two essential subsets I and J, resp., of $\{\mathcal{A}_1, \ldots, \mathcal{A}_n\}$ which contain $\mathcal{A}_1$, whose elements affinely span integer lattices of rank d_1 and d_2, resp., and thus whose cardinality is $d_1 + 1$ and $d_2 + 1$, resp. Further let $K := I \cap J$, whose cardinality is $k \geq 1$. Then the cardinality of $(I \cup J) \setminus \{\mathcal{A}_1\}$ is $d_1 + d_2 + 1 - k$. We show that $\dim \mathcal{L}((I \cup J) \setminus \{\mathcal{A}_1\}) \leq d_1 + d_2 - k$, where $\mathcal{L}(S)$ denotes the integer lattice affinely generated by the elments of some set S of supports. Note that, since I and J are essential, $\dim \mathcal{L}(I \setminus \{\mathcal{A}_1\}) = \dim \mathcal{L}(I) = d_1$ and $\dim \mathcal{L}(J \setminus \{\mathcal{A}_1\}) = \dim \mathcal{L}(J) = d_2$. Therefore $\dim \mathcal{L}((I \cup J) \setminus \{\mathcal{A}_1\}) = \dim \mathcal{L}(I \cup J)$ which is at most $\dim \mathcal{L}(I) + \dim \mathcal{L}(J) - \dim \mathcal{L}(K)$. Since $\dim \mathcal{L}(K) \geq k$, we have

$$\dim \mathcal{L}\left((I \cup J) \setminus \{\mathcal{A}_1\}\right) \leq d_1 + d_2 - k.$$

Therefore, similar to above, $(I \cup J) \setminus \mathcal{A}_1$ contains an essential subset, that is, an essential subset, not containing $\widetilde{\mathcal{A}}_1$, of $\{\widetilde{\mathcal{A}}_1, \mathcal{A}_2, \ldots, \mathcal{A}_n\}$. Contradiction!

□

Now we are ready to prove the main theorem.

Proof:

Theorem 5.1 Let $\widetilde{f}_1$ be a Laurent polynomial with distinct symbolic coefficients with support $\widetilde{\mathcal{A}}_1$. By Lemma 5.12 we have

$$\begin{aligned}\operatorname{Res}_{\widetilde{\mathcal{A}}_1,\mathcal{A}_2,\ldots,\mathcal{A}_n}\left(\widetilde{f}_1, f_2, \ldots, f_n\right) &= \\ &\prod_{\gamma} \widetilde{f}_1(\gamma) \prod_{\omega} \operatorname{Res}_{\mathcal{A}_2^{\omega},\ldots,\mathcal{A}_n^{\omega}}\left(f_2^{\omega}, \ldots, f_n^{\omega}\right)^{\delta_{\widetilde{\mathcal{A}}_1,\mathcal{A}_2,\ldots,\mathcal{A}_n}(\omega)},\end{aligned}$$

where γ ranges over the common zeros in $\left(\widetilde{K} \setminus \{0\}\right)^{n-1}$, with respect to the lattice $\mathcal{L}(\widetilde{\mathcal{A}}_1, \mathcal{A}_2, \ldots, \mathcal{A}_n)$, of $f_2, \ldots, f_n$, where $\widetilde{K}$ is the algebraic closure of the field generated by the complex numbers and the symbolic coefficients of $\widetilde{f}_1$ and the f_i's, and ω ranges over the primitive inner normal vectors of the facets of the Newton polytope generated by $\mathcal{A}_2 + \cdots + \mathcal{A}_n$. Since the symbolic coefficients of $\widetilde{f}_1$ are algebraically independent from the symbolic coefficients of $f_2, \ldots, f_n$, Lemma 5.12 is stable under specialization of $\widetilde{f}_1$ and we have

$$\operatorname{Res}_{\widetilde{\mathcal{A}}_1,\mathcal{A}_2,\ldots,\mathcal{A}_n}(f_1,\ldots,f_n) = \prod_\gamma f_1(\gamma) \prod_\omega \operatorname{Res}_{\mathcal{A}_2^\omega,\ldots,\mathcal{A}_n^\omega}(f_2^\omega,\ldots,f_n^\omega)^{\delta_{\widetilde{\mathcal{A}}_1,\mathcal{A}_2,\ldots,\mathcal{A}_n}(\omega)},$$

where γ ranges over the common zeros in $(K\setminus\{0\})^{n-1}$, where K is the algebraic closure of the field generated by the complex numbers and the symbolic coefficients of f_1 and the remaining f_i's and ω is as before.

Further, as in [PS93] by the construction of $\prod_\gamma f_1(\gamma)$, we have

$$\prod_\gamma f_1(\gamma) = \prod_{\gamma'} f_1(\gamma')^{\left[\mathcal{L}\left(\widetilde{\mathcal{A}}_1,\mathcal{A}_2,\ldots,\mathcal{A}_n\right):\mathcal{L}(\mathcal{A}_1,\ldots,\mathcal{A}_n)\right]}, \tag{5.6}$$

where γ' ranges over the common zeros in $(K\setminus\{0\})^{n-1}$ of $f_2,\ldots,f_n$ with respect to $\mathcal{L}(\mathcal{A}_1,\ldots,\mathcal{A}_n)$.

By Lemma 5.13 and Lemma 5.12, we have

$$\prod_{\gamma'} f_1(\gamma') = \operatorname{Res}_{\mathcal{A}_1,\ldots,\mathcal{A}_n}(f_1,\ldots,f_n) \prod_\omega \operatorname{Res}_{\mathcal{A}_2^\omega,\ldots,\mathcal{A}_n^\omega}(f_2^\omega,\ldots,f_n^\omega)^{-\delta_{\mathcal{A}_1,\ldots,\mathcal{A}_n}(\omega)}$$

and thus

$$\prod_\gamma f_1(\gamma) = \operatorname{Res}_{\mathcal{A}_1,\ldots,\mathcal{A}_n}(f_1,\ldots,f_n)^{\left[\mathcal{L}\left(\widetilde{\mathcal{A}}_1,\mathcal{A}_2,\ldots,\mathcal{A}_n\right):\mathcal{L}(\mathcal{A}_1,\ldots,\mathcal{A}_n)\right]} \prod_\omega \operatorname{Res}_{\mathcal{A}_2^\omega,\ldots,\mathcal{A}_n^\omega}(f_2^\omega,\ldots,f_n^\omega)^{-\delta_{\mathcal{A}_1,\ldots,\mathcal{A}_n}(\omega)\left[\mathcal{L}\left(\widetilde{\mathcal{A}}_1,\mathcal{A}_2,\ldots,\mathcal{A}_n\right):\mathcal{L}(\mathcal{A}_1,\ldots,\mathcal{A}_n)\right]}.$$

Therefore

$$\begin{aligned}
&\operatorname{Res}_{\widetilde{\mathcal{A}}_1,\mathcal{A}_2,\dots,\mathcal{A}_n}\left(\widetilde{f}_1, f_2, \dots, f_n\right) \;= \\
&\operatorname{Res}_{\mathcal{A}_1,\dots,\mathcal{A}_n}(f_1,\dots,f_n)^{\left[\mathcal{L}\left(\widetilde{\mathcal{A}}_1,\mathcal{A}_2,\dots,\mathcal{A}_n\right):\mathcal{L}(\mathcal{A}_1,\dots,\mathcal{A}_n)\right]} \qquad (5.7)\\
&\prod_{\omega}\operatorname{Res}_{\mathcal{A}_2^{\omega},\dots,\mathcal{A}_n^{\omega}}(f_2^{\omega},\dots,f_n^{\omega})^{\delta_{\widetilde{\mathcal{A}}_1,\mathcal{A}_2,\dots,\mathcal{A}_n}(\omega)\,-\,\delta_{\mathcal{A}_1,\dots,\mathcal{A}_n}(\omega)\,I},
\end{aligned}$$

where $I := \left[\mathcal{L}\left(\widetilde{\mathcal{A}}_1, \mathcal{A}_2, \dots, \mathcal{A}_n\right) : \mathcal{L}(\mathcal{A}_1, \dots, \mathcal{A}_n)\right]$. Note that

$$\frac{[\mathcal{L}(\widetilde{\mathcal{A}}_1, \mathcal{A}_2, \dots, \mathcal{A}_n) : \mathcal{L}(\mathcal{A}_1, \dots, \mathcal{A}_n)]}{[\mathbb{Z}^{n-1} : \mathcal{L}(\mathcal{A}_1, \dots, \mathcal{A}_n)]} \;=\; \frac{1}{[\mathbb{Z}^{n-1} : \mathcal{L}(\widetilde{\mathcal{A}}_1, \mathcal{A}_2, \dots, \mathcal{A}_n)]}$$

and therefore by Lemma 5.11

$$\begin{aligned}
&\delta_{\widetilde{\mathcal{A}}_1,\mathcal{A}_2,\dots,\mathcal{A}_n}(\omega) - \delta_{\mathcal{A}_1,\dots,\mathcal{A}_n}(\omega) \;= \\
&\qquad\qquad \frac{\left(\mathrm{a}_{\widetilde{\mathcal{A}}_1}(\omega) - \mathrm{a}_{\mathcal{A}_1}(\omega)\right)\,[\mathrm{H}^{\omega} : \mathcal{L}(\mathcal{A}_2^{\omega}, \dots, \mathcal{A}_n^{\omega})]}{[\mathbb{Z}^{n-1} : \mathcal{L}(\widetilde{\mathcal{A}}_1, \mathcal{A}_2, \dots, \mathcal{A}_n)]}.
\end{aligned}$$

Therefore we have shown the equality of the main theorem.

Since the Laurent polynomials in the main theorem have symbolic coefficients and the sparse resultants on the right hand side of the equality are defined with respect to the precise supports of these Laurent polynomials, the factorization on the right hand side is irreducible.

Thus we have shown the main theorem.

□

5.4 Conclusion

In this chapter we studied sparse resultant under vanishing of coefficients. The sparse resultant of some Laurent polynomials f_i with respect to any supports is some power of the sparse resultant of the f_i's with respect to their precise supports times a product of powers of sparse resultants of some parts of the f_i's. This result is important for applications where perturbed data with very small coefficients arise as well as when one computes resultants with respect to some fixed supports, not necessarily the supports of the f_i's, in order to speed up compuations. This work extended some work by Sturmfels on sparse resultant under vanishing coefficients (cf. Corollary 4.2 of [Stu94]). We also stated a corollary about sparse resultant under powering of variables which is a generalization of a theorem by Kapur and Saxena for Dixon resultant. We also stated a lemma of independent interest generalizing Pedersen's and Sturmfels' Poisson-type product formula.

Chapter 6

Conclusion

The objective of this research has been to develop methods for computing resultants of composed polynomials, efficiently, by utilizing their composition structure. By the resultant of several polynomials in several variables (one fewer variables than polynomials) we mean an irreducible polynomial in the coefficients of the polynomials that vanishes if they have a common zero. By a composed polynomial we mean the polynomial obtained from a given polynomial by replacing each variable by a polynomial.

The main motivation for this research came from the following observations: Resultants of polynomials are frequently computed in many areas of science and in applications because they are fundamentally utilized in solving systems of polynomial equations. Further, polynomials arising in science and applications are often composed because humans tend to structure knowledge modularly and hierarchically. Thus, it is important to have theories and software libraries for efficiently computing resultants of composed polynomials.

However, most existing mathematical theories have not adequately supported composed polynomials and most algorithms as well as software libraries have ignored the composition structure, thus suffering from enormous blow up in space and time. Thus, it has been important to develop theories and software libraries for efficiently computing resultants of composed polynomials.

The main finding of this research has been that resultants of composed polynomials can be nicely factorized, namely, they can be factorized into products of powers of the resultants of the component polynomials and of some of their parts. These factorizations can be utilized to compute resultants of composed polynomials with dramatically improved efficiency.

We point out some future directions for the research: It would be interesting to study resultants of arbitrary sparse polynomials composed with arbitrary sparse polynomials (cf. Case 4 of Table 1.1). Finding a compact product formula seems to be very challenging. Further, it would be interesting to study resultants of polynomials composed with k polynomials in $n-1$ variables, where n and k are different. Such composed polynomials occur frequently in practice. Finally, it would be interesting to study how to efficiently compute other fundamental operations, besides resultants, for composed objects. This has already been done for some operations, such as subresultants (cf. [Hon97]), Gröbner bases (cf. [Hon98],

[GM98]) and Galois groups of certain differential operators (cf. [BS99]).

This concludes the main part of the thesis.

Bibliography

[AS88] W. Auzinger and H. Stetter. An elimination algorithm for the computation of all zeros of a system of multivariate polynomial equations. In *Proc. International Conference on Numerical Mathematics*, volume 86, pages 12–30, Basel, 1988. Birkhäuser.

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

[Bro00] C. W. Brown. Simple CAD construction and its applications. *J. Symbolic Computation*, May 2000. Accepted for publication.

[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).

[Buc70] B. Buchberger. Ein algorithmisches Kriterium für die Lösbarkeit eines algebraischen Gleichungssystems. *Aequationes Math.*, 4:374–383, 1970.

[Cav86] B. F. Caviness. Computer algebra: past and future. *J. Symbolic Computation*, 2(3):217–236, 1986.

[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.

[CE95] J. Canny and I. Emiris. Efficient incremental algorithms for the sparse resultant and mixed volume. *J. Symbolic Computation*, 20(2):117–149, 1995.

[CE00] J. Canny and I. Emiris. A subdivision-based algorithm for the sparse resultant. *J. ACM*, 47(3):417–451, May 2000.

[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 non-linear 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.

[Col71] G. Collins. The calculation of multivariate polynomial resultants. *J. Assoc. Comput. Mach.*, 18:515–532, 1971.

[Dan78] V. I. Danilov. The geometry of toric varieties. *Russian Math. Surveys*, 33:97–154, 1978.

[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.

[Dor00] P. Dorato. Quantified multivariate polynomial inequalities. *IEEE Control Systems Magazine*, 2000.

[DS98] V. I. Danilov and V. V. Shokurov. *Algebraic Curves, Algebraic Manifolds and Schemes.* Springer-Verlag, Berlin Heidelberg New York, 2nd edition, 1998.

[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.

[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.

[GM98] J. Gutierrez and R. Rubio San Miguel. Reduced Gröbner bases under composition. *J. Symbolic Computtation*, 26(4):433–444, 1998.

[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.

[GVLRR90] L. Gonzáles-Vega, H. Lombardi, T. Recio, and M.-F. Roy. Spécialisation de la suite de sturm et sous-résultants. *RAIRO Inform. Théor. Appl.*, 24(6):561–588, 1990.

[HLS95] H. Hong, R. Liska, and S. Steinberg. Testing stability by quantifier elimination. *J. Symbolic Computation*, 24(2):161–187, 1995.

[HM00] H. Hong and M. Minimair. Sparse resultant of composed polynomials I. submitted to a journal, available at http://www.math.ncsu.edu/˜mminima/HM2000.ps, May 2000.

[Hon96] H. Hong. Groebner basis under composition II. In *Proceedings of ISSAC 96 (International Symposium on Symbolic and Algebraic Computation)*, pages 79–85. ACM, 1996.

[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.

[KKMSD73] G. Kempf, F. Knudsen, D. Mumford, and B. Saint-Donat. *Toroidal Embeddings I*, volume 339 of *Springer Lecture Notes*. Springer-Verlag, Berlin Heidelberg New York, 1973.

[KLZ96] D. Kozen, S. Landau, and R. Zippel. Decomposition of algebraic functions. *J. Symbolic Computation*, 22(3):235–246, 1996.

[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.

[KS97] D. Kapur and T. Saxena. Extraneous factors in the Dixon resultant formulation. In *ISSAC '97*. ACM, 1997.

[LS95] Y. Lakshman and D. Saunders. Sparse polynomial interpolation in nonstandard bases. *SIAM J. Comput*, 24(2):387–397, 1995.

[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.

[Min97] M. Minimair. Volume of Parametrized Polyhedra. Technical Report 97-03, RISC - Linz, Johannes Kepler University Linz, A-4040 Linz, Austria, January 1997. M.S. thesis.

[Min00a] M. Minimair. Dense resultant of composed polynomials. submitted to a journal, available at http://www.math.ncsu.edu/~mminima/M2000.ps, August 2000.

[Min00b] M. Minimair. Sparse resultant of composed polynomials II. Submitted to a journal, available at http://www.math.ncsu.edu/~mminima/M2000c.ps, October 2000.

[Min00c] M. Minimair. Sparse resultant under vanishing coefficients. Submitted to a journal, available at http://www.math.ncsu.edu/~mminima/M2000b.ps, October 2000.

[Mis93] B. Mishra. *Algorithmic Algebra.* Texts and Monographs in Computer Science. Springer-Verlag, New York, 1993.

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

[Oda88] T. Oda. *Convex Bodies and Algebraic Geometry.* Springer-Verlag, Berlin Heidelberg New York, 1988.

[Pfa99] J. Pfalzgraf. On finding zeros of complex polynomials: an experimental case study. Research report, University of Salzburg, 1999.

[PRS93] 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.

[PS93] P. Pedersen and B. Sturmfels. Product formulas for resultants and Chow forms. *Mathematische Zeitschrift*, 214(3):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.

[Stu94] Bernd Sturmfels. On the Newton polytope of the resultant. *Journal of Algebraic Combinatorics*, 3:207–236, 1994.

[Tay00] A. Taylor. *On Initial Ideals of Prime Ideals and The Inverse Problem in Gröbner Basis Theory.* PhD thesis, University of Kansas, Lawrence, KS, 2000.

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

[Vas98] W. Vasconcelos. *Computational methods in commutative algebra and algebraic geometry.* Algorithms and computations in mathematics. Springer-Verlag, Berlin, New York, 1998. With chapters by David Eisenbud, et al.

[VVC94] J. Verschelde, P. Verlinden, and R. Cools. Homotopies exploiting Newton polytopes for solving sparse polynomial systems. *SIMA J. Numer. Anal.*, 31:915–930, 1994.

[vW95] J. von zur Gathen and J. Weiss. Homogeneous bivatiate decompositions. *J. Symbolic Computation*, 19(5):409–434, 1995.

[vzGGR99] J. von zur Gathen, J. Gutierrez, and R. Rubio. On multivatiate polynomial decompostion. In *Computer algebra in scientific computing – CASC'99 (Munich)*, pages 463–478, Berlin, 1999. Springer.

[WBLR85] F. Winkler, B. Buchberger, F. Lichtenberger, and H. Rolletschek. Algorithm 628. An algorithm for constructing canonical bases for an ideal. *ACM Trans. Math. Software*, 11(1):66–78, 1985.

[Win96] F. Winkler. *Polynomial algorithms in computer algebra.* Texts and monographs in symbolic computation. Springer-Verlag, Vienna, 1996.

[Yap00] C. Yap. *Fundamental Problems in Algorithmic Algebra.* Oxford University Press, New York, 2000.

[ZCG98] M. Zhang, E. Chionh, and R. N. Goldman. Hybrid Dixon resultants. In *The mathematics of surfaces, VIII (Birmingham, 1998)*, pages 193–212, Winchester, 1998. Info. Geom.

[Zie94] Günter M. Ziegler. *Lectures on Polytopes.* Springer-Verlag, Berlin Heidelberg New York, 1994.

Appendix

Chapter 7

Appendix: Tutorial on Toric Varieties

7.1 Introduction

Toric varieties play a fundamental role in the theory of resultants (cf. [CLO98], [GKZ94]).

We give a brief intuitive introduction into the theory of toric varieties. We illustrate toric varieties and explain, by examples, how they can be constructed. It is easy to generalize these examples to arbitrary toric varieties. We do not cover toric varieties in complete generality. More general and comprehensive treatises can be found in [GKZ94], [Ful93], [Oda88], [Dan78] and [KKMSD73].

7.2 Intuitive definition of toric varieties

Toric varieties naturally arise from the study of solution sets of multivariate polynomial equations, like the equation

$$11\,x\,y^3 \;-\; 2\,x^2\,y \;+\; 7\,x\,y^2 \;-\; 3\,x\,y \;+\; 8\,y^2 \;+\; 5\,y \;+\; 9 \;=\; 0, \tag{7.1}$$

which we will consider throughout the appendix.

In the following, we will only consider solutions in $(\mathbb{C}\setminus\{0\})^2$ of Equation (7.1), which will naturally lead to constructing a certain toric variety. Obviously, Equation (7.1) also has solutions with

$$x = 0 \quad \text{and} \quad 8\,y^2 \;+\; 5\,y \;+\; 9 \;=\; 0, \quad \text{where } \; y \in \mathbb{C}. \tag{7.2}$$

The equation, univariate in y, of Line (7.2), similarly leads to constructing another toric variety.

Now we describe how a certain toric variety arises from the study of solutions in $(\mathbb{C}\setminus\{0\})^2$ of Equation (7.1). We proceed in three steps.

Firstly, we rewrite Equation (7.1) into an equivalent linear one. This equivalent linear equation is

$$11\,z_{03} \;-\; 2\,z_{21} \;+\; 7\,z_{12} \;-\; 3\,z_{11} \;+\; 8\,z_{02} \;+\; 5\,z_{01} \;+\; 9 \;=\; 0,$$

where

$$(z_{03}, z_{21}, z_{12}, z_{11}, z_{02}, z_{01}) \ \in \ S,$$

$$S \ := \ \left\{ \left(x\, y^3, x^2\, y, x\, y^2, x\, y, y^2, y\right) \mid (x, y) \in (\mathbb{C} \setminus \{0\})^2 \right\}.$$

It turns out that studying, through techniques of commutative algebra and algebraic geometry, solutions in the set S is difficult because the set S is not an algebraic set. Therefore we extend S a bit in order to be, in a sense which is described below, algebraically closed. This closure is formed in the remaining two steps.

Secondly, we homogenize the linear equation. Note that

$$11\, z_{03} \ - \ 2\, z_{21} \ + \ 7\, z_{12} \ - \ 3\, z_{11} \ + \ 8\, z_{02} \ + \ 5\, z_{01} \ + \ 9 \ = \ 0$$

iff

$$11\, Z_{03} \ - \ 2\, Z_{21} \ + \ 7\, Z_{12} \ - \ 3\, Z_{11} \ + \ 8\, Z_{02} \ + \ 5\, Z_{01} \ + \ 9\, Z_{00} \ = \ 0,$$

where $Z_{ij} = z_{ij}\, Z_{00}$ for any $Z_{00} \neq 0$. We denote the solution set of the homogenized equation by T, namely

$$T \ := \ \left\{ \left(Z_{00} \cdot x\, y^3,\ Z_{00} \cdot x^2\, y,\ Z_{00} \cdot x\, y^2,\ Z_{00} \cdot x\, y,\ Z_{00} \cdot y^2,\ Z_{00} \cdot y,\ Z_{00}\right) \mid \right.$$
$$\left. (x, y) \in (\mathbb{C} \setminus \{0\})^2 \ \text{ and } \ Z_{00} \in \mathbb{C} \setminus \{0\} \right\}.$$

Thirdly, we form the projective closure V of T. That is, V is the solution set of all homogeneous sevenvariate polynomials vanishing on T. Note that V is a projective set. Thus we can view V as algebraic subset of six dimensional projective space by considering the Z_{ij}'s as homogeneous coordinates. The algebraic set V is called *toric variety*.

Summarizing, in order to construct a toric variety as a solution space of an equation, we have applied well known techniques. We have linearized the equation, homogenized the equation and extended the solution space appropriately.

7.3 Motivation for the name "toric variety" and basic properties

We give a motivation for the name "toric variety", point out some technical issue associated with the adjective "toric" and state some basic properties of toric varieties.

The name "toric variety" has the following motivation. Firstly, the set V from Section 7.2 is called a "variety" because one can show that the set V is irreducible. Secondly, the variety V is called "toric" because a certain torus can be embedded into V: One can show that the set $(\mathbb{C}\setminus\{0\})^2$, which can be considered as an abstract torus, is *injectively* mapped onto the set S. Thus the torus $(\mathbb{C}\setminus\{0\})^2$ is embedded into the algebraic set V.

It is important to point out the following technical issue associated with the adjective "toric": Not all varieties that are constructed like V have a torus embedding. It is easy to state a neccessary and sufficient condition for the torus being embedded into the toric variety. We illustrate this condition on the example toric variety V. We require that the exponents of the monomials in the polynomial $f := 11\,x\,y^3 - 2\,x^2\,y + 7\,x\,y^2 - 3\,x\,y + 8\,y^2 + 5\,y + 9$ affinely span $\mathbb{Z}^2$ over $\mathbb{Z}$, which is in fact true: For each integer point in the Newton polygon

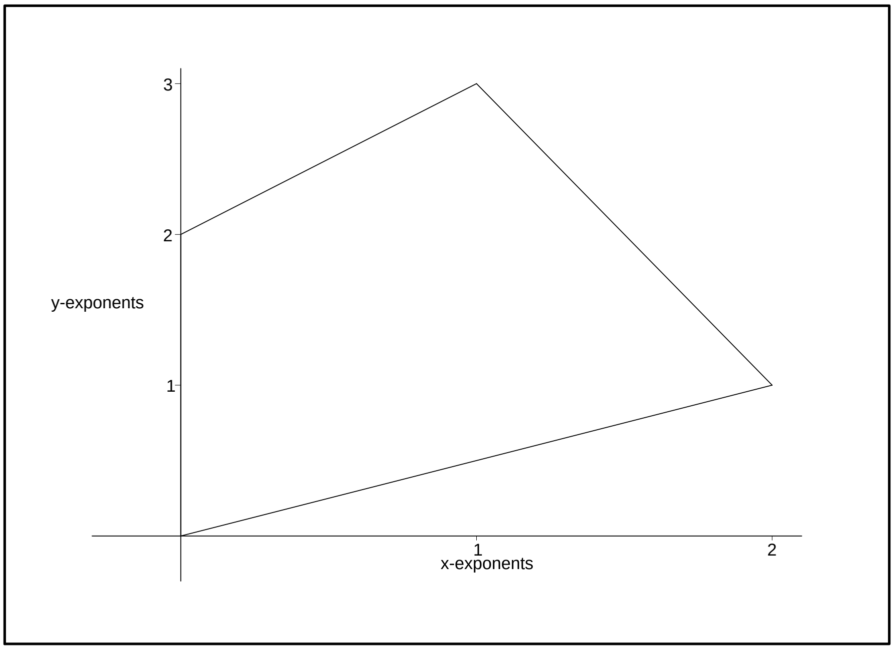

Figure 7.1: Newton polygon of f

of f, shown in Figure 7.1, we can find a monomial in f having this integer point as exponent. Since the dimension of the Newton polygon is 2, the integer points affinely span $\mathbb{Z}^2$ over $\mathbb{Z}$.

Note that we will focus for the rest of this appendix on toric varieties with torus embedding.

Toric varieties with torus embeddings have certain useful properties of which we state two: Firstly, their set of singularities is of codimension of at least 2. Secondly, a toric variety with torus embedding is a normalization of a toric variety without torus embedding.

7.4 Points in the projective closure

In Section 7.2, we have obtained the algebraically closed projective set V by expanding the set T. The main question of thie section is: What points have we added to T in order to obtain V?

One can show that

$$V \;=\; T \cup W_1 \cup W_2 \cup W_3 \cup W_4,$$

where W_1, W_2, W_3 and W_4 are certain lower dimensional toric varieties. In detail: Let

$$\begin{aligned}
f_1 &:= -2\,x^2\,y \;+\; 9,\\
f_2 &:= 11\,x\,y^3 \;-\; 2\,x^2\,y,\\
f_3 &:= 11\,x\,y^3 \;+\; 8\,y^2,\\
f_4 &:= 8\,y^2 \;+\; 5\,y \;+\; 9
\end{aligned}$$

be the maximal parts of f whose exponents lie in the edges of the Newton polygon of f. As before we can form toric varieties V_1, V_2, V_3 and V_4 from f_1, f_2, f_3 and

f_4. For example V_1 is the projective closure of the set

$$\left\{ \left(Z_{00}\, x^2\, y,\ Z_{00} \right) \,|\, x, y, Z_{00} \in \mathbb{C} \setminus \{0\} \right\}.$$

Then we define

$$\begin{aligned} W_1 \;:=\; \{ & (Z_{03},\, Z_{21},\, Z_{12},\, Z_{11},\, Z_{02},\, Z_{01},\, Z_{00}) \mid \\ & (Z_{21}, Z_{00}) \in V_1,\ Z_{03},\, Z_{12},\, Z_{11},\, Z_{02},\, Z_{01} \;=\; 0 \}. \end{aligned}$$

Obviously W_1 is isomorphic to V_1. The sets W_2, W_3 and W_4 are constructed likewise.

7.5 Alternative definition of toric varieties

Now we describe an alternative, equivalent definition of the toric variety V of Section 7.2. Sometimes this alternative definition is more useful than the definition of Section 7.2.

Recall that V is a projective variety. Very often projective varieties are defined as the glueing of certain affine varieties. We describe how V can be represented by a glueing of affine varieties.

Firstly, we define some affine sets that cover V. Let

$$U_{00} := \{Z \in V \mid Z_{00} \neq 0\},$$

$$U_{21} := \{Z \in V \mid Z_{21} \neq 0\},$$

$$U_{13} := \{Z \in V \mid Z_{13} \neq 0\},$$

$$U_{02} := \{Z \in V \mid Z_{02} \neq 0\}$$

be these affine sets. Note that U_{ij} is defined exactly for i, j such that (i, j) is a vertex of the Newton polygon in figure 7.1. It is almost trivial to see that $V = U_{00} \cup U_{21} \cup U_{13} \cup U_{20}$.

Secondly, we describe how the affine sets are glued together, i.e. in which way certain points are identified among the different affine sets. If we keep the same homogeneous coordinates for each affine set then the glueing is trivial. For example, U_{00} and U_{21} overlap in $U_{00} \cap U_{21}$. The points in $U_{00} \cap U_{21} \subseteq U_{00}$ are trivially identified with the identical ones in $U_{00} \cap U_{21} \subseteq U_{21}$.

The glueing that is described in the previous paragraph is trivial because the affine sets U_{ij} are defined as subsets of the toric variety V having the same homogenous coordinates. Usually the affine sets U_{ij} are not defined in this way, but directly from the given polynomial without first constructing V. If the affine sets U_{ij} are defined without referring to V, then each affine set U_{ij} has a distinct set of affine coordinates. Then the glueing is described in terms of these distinct affine coordinates. We describe this process in the following paragraphs.

Firstly, we define the affine sets. Consider the cone with vertex in $(0,0)$ that contains and touches the Newton polygon of f (cf. figure 7.2). We call this cone the cone of U_{00}. The integer points in this cone are spanned by

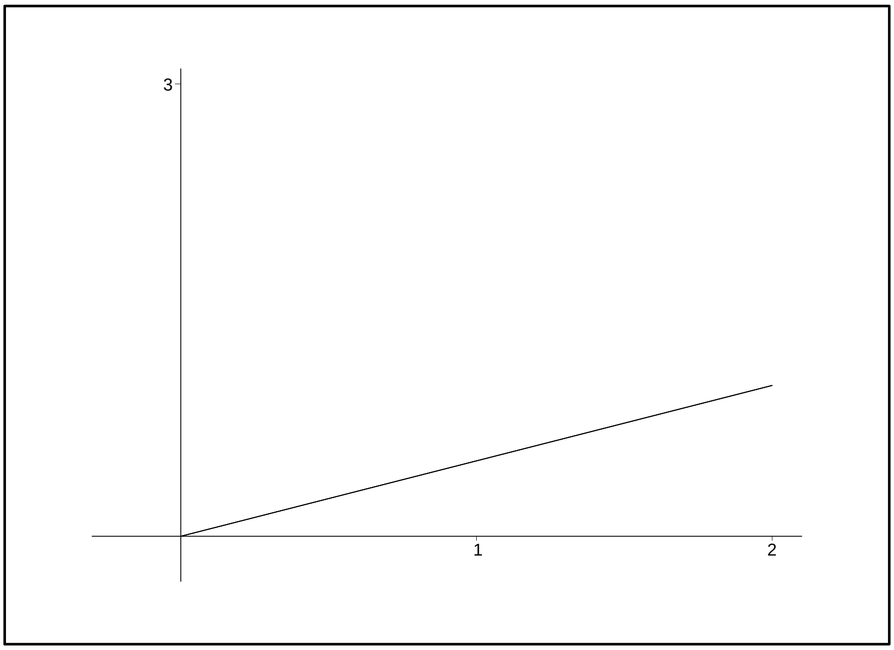

Figure 7.2: Cone of vertex $(0,0)$

$\{(0,1),(1,1),(2,1)\}$ over $\mathbb{N}_0$. The points $(0,1),(1,1),(2,1)$ are linearly dependent over, that is, they are related by the equality $2\cdot(1,1)=(0,1)+(2,1)$. We use this equality in order to define U'_{00}, namely,

$$U'_{00} \;:=\; \left\{(u_{01},u_{11},u_{21})\in\mathbb{C}^3 \mid u_{11}^2=u_{01}\cdot u_{21}\right\}.$$

It is obvious that U'_{00} is isomorphic to U_{00}. We can retrieve the affine coordinates in U'_{00} from the projective coordinates in U_{00} by dividing the projective coordinates by Z_{00} and by discarding redundant coordinates. In formulae, we have

$u_{01} = \frac{Z_{01}}{Z_{00}}$, $u_{11} = \frac{Z_{11}}{Z_{00}}$ and $u_{21} = \frac{Z_{21}}{Z_{00}}$. Now, consider the analog cone with vertex in $(2,1)$. We call this cone the cone of U_{21}. Further we move the cone of U_{21} by $(-2,-1)$ such that the vertex lies in the origin (cf. figure 7.3). The integer points

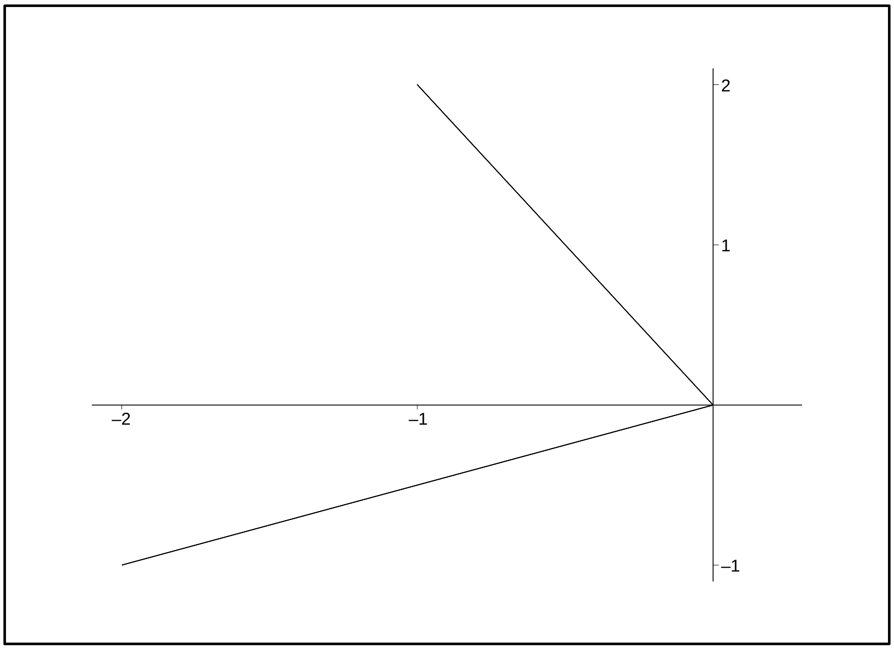

Figure 7.3: Cone of vertex $(2,1)$

in this cone are spanned by $\{(-2,-1),(-1,0),(-1,1),(-1,2)\}$ over $\mathbb{N}_0$. Note that $3\cdot(-1,0) = (-2,-1)+(-1,0)$ and $2\cdot(-1,1) = (-1,0)+(-1,2)$ and thus, similarly to above, we define

$$\begin{aligned} U'_{2,1} := \Big\{ & (v_{-2\,-1}, v_{-1\,0}, v_{-1\,1}, v_{-1\,2}) \in \mathbb{C}^4 \mid \\ & \qquad v_{-1\,0}^3 = v_{-2\,-1}\cdot v_{-1\,0},\;\; v_{-1\,1}^2 = v_{-1\,0}\cdot v_{-1\,2} \Big\}. \end{aligned}$$

It is obvious that U'_{21} is isomorphic to U_{21}. We can retrieve the affine coordinates in U'_{21} from the projective coordinates in U_{21} by dividing the projective coordinates by Z_{21} and by discarding redundant coordinates. In formulae, we have $v_{-2\,-1} = \frac{Z_{00}}{Z_{21}}$, $v_{-1\,0} = \frac{Z_{11}}{Z_{21}}$, $v_{-1\,1} = \frac{Z_{12}}{Z_{21}}$ and $v_{-1\,2} = \frac{Z_{13}}{Z_{21}}$. Likewise, we can define affine sets U'_{13} and U'_{02}.

Secondly, we describe the glueing. We describe how U'_{00} and U'_{21} are glued together in terms of the affine coordinates. We identify the points in U'_{00} with $u_{21} \neq 0$ with the points in U'_{21} with $v_{-2\,-1} \neq 0$. We choose $u_{21} \neq 0$ because $(2,1)$ is contained in the cone of U_{00} and is the vertex of the cone of U_{21}. Further, we choose $v_{-2\,-1} \neq 0$ because, undoing the translation by $(-2,-1)$, $(0,0) = (-2,-1) - (-2,-1)$ is contained in the cone of U_{21} and is the vertex of the cone of U_{00}. One can see easily how the u_{ij}'s and the v_{ij}'s are related by considering the relations on the u_{ij}'s and on the v_{ij}'s and by writing the u_{ij}'s and v_{ij}'s as fractions of homogeneous coordinates. That is, onc can see that $u_{01} = \frac{v_{-1\,0}^2}{v_{-2\,-1}}$, $u_{11} = \frac{v_{-1\,0}}{v_{-2\,-1}}$ and $u_{21} = \frac{1}{v_{-2\,-1}}$. Similarly, one can describe the glueings between the other affine sets.

Summarizing, there is a natural way to represent toric varieties as the glueing of affine varieties. For each vertex of a given Newton polytope we construct an affine set. The glueing mapping between the distinct affine coordinates is defined as products of certain powers of the affine coordinates.

We conclude the tutorial on toric varieties and the thesis.