Technical Report (1996)

Multivariate Resultants Under Composition

Hoon Hong

Research Institute for Symbolic Computation

Johannes Kepler University

A-4040 Linz, Austria

e-mail: hhong@risc.uni-linz.ac.at

Composition is an operation of replacing variables in a polynomial with other polynomials. The main question of this paper is: *What happens to multivariate resultants under composition?* We prove that the multivariate resultant of composed polynomial is a product of certain powers of the multivariate resultants of the original polynomials and the composition polynomials. This generalizes the well known fact for the linear case to the non-linear case.

1. Introduction

The main question of this paper is: *What happens to multivariate resultants under composition?*

More precisely, let $F = (f_1, \ldots, f_n)$ be a list of homogeneous polynomials in the variables $x_1, \ldots, x_n$, and let R be its resultant. Let $\Theta = (\theta_1, \ldots, \theta_n)$ be a list of homogeneous polynomials in the variables $x_1, \ldots, x_n$ of same degrees.† Let F^* be the list obtained from F by replacing x_i by θ_i, and let R^* be its resultant. Naturally one asks the question: Is R^* in any way related to R? In other words, *What happens to multivariate resultants under composition?*

The main contribution of this paper is to show that the resultant of the composed polynomials F^* is a product of certain powers of the multivariate resultants of the original polynomials F and the composition polynomials Θ. Precisely, we prove that

$$\mathrm{Res}(F^*) = \mathrm{Res}(F)^{\ell^{n-1}} \mathrm{Res}(\Theta)^{d_1 \cdots d_n}$$

where d_i is the degree of f_i and ℓ is the degree of every θ_i.

This generalizes the following well known fact for the linear case. Let θ_i be linear. Then, it is well known that

$$\mathrm{Res}(F^*) = \mathrm{Res}(F) \det(\Theta)^{d_1 \cdots d_n}$$

where $\det(\Theta)$ stands for the determinant of the matrix of the coefficients of Θ. Recalling another well known fact that $\det(\Theta)$ is $\mathrm{Res}(\Theta)$, one sees immediately that this is a special case of the theorem proved in this paper.

† This restriction is need to ensure that F^* is homogeneous.

Obviously, this has an application in the computation of resultants of composed polynomials. In order to compute the resultant of F^*, we compute the resultants of F and Θ, power them, and multiply them.[‡] This should be more efficient (in time/space) than computing the resultant of F^* directly (ignoring the structural information).

Composed objects (polynomials) occur often in real-life problem solving because the underlying mathematical models are usually hierarchically structured. For instance, numerous physical quantities (such as work, torque, etc) are defined in terms of other more basic quantifies (such as length, time, etc). Thus, we often need to deal with a set of polynomials where the variables in them are defined in terms of other variables.

The reader might be interested in two related papers (Hong 1995b, Hong 1995a) where we study how two other fundamental operations, namely univariate subresultants and Groebner basis computation, behave under composition.

The structure of the paper is as follows. In Section 2, we recall the definition and some properties of multivariate resultants. In Section 3, we give a precise statement of the main theorem of this paper. In Sections 4, we give a proof of the main theorem.

2. Review of Multivariate Resultants

In this section, we review the definition and some elementary properties of multivariate resultants. For details, see (Macaulay 1916, Cayley 1865, Dixon 1908, White 1909, der Waerden 1966). For various modern methods for computing resultants, see (Kaltofen and Lakshman 1988, Zippel 1990, Chardin 1991, Sturmfels 1991, Canny and Imiris 1993, Manocha 1993, Kapur and Saxena 1995). Also the recent survey (Kapur and Lakshman 1992) gives highly readable descriptions of both classical and modern methods. We begin by fixing some notations that will be used throughout this paper.

Notations 2.1.

D	*an integral domain.*
K	*an algebraic closure of the quotient field of D.*
X	*a list $(x_1, \ldots, x_n)$ of variables, $n > 0$.*
F	*a list $(f_1, \ldots, f_n)$ of homogeneous polynomials in $D[X]$. Each f_i is either 0 or of positive degree.*

Remark: Note that F is *not* allowed to contain non-zero constant polynomials (that is, of degree 0). Thus, when we define the resultant of F below, it is important to remember that the resultant is defined only when F does not contain non-zero constants. It is possible to generalize the definition of resultants in order to allow non-zero constants. But then, the definition will have to be modified technically to take care of several special cases. I decided that it is not worthwhile since we do not gain much generality, but lose simplicity.

Now we give a definition of resultants. In the literature, there are several different versions. We find the following most useful and elegant among them. It consists of four

‡ In fact, in most situations, it is better to keep the factored form, and thus it is not necessary to carry out the powering and the multiplication.

properties that are to be satisfied by resultants. In the following sections, we will refer to the properties by their labels such as **(P1)**, **(P2)**, etc.

DEFINITION 2.1. (RESULTANT) *The resultant of F, written as* $\mathrm{Res}(F)$, *is the unique element of D such that*

(P1) $\mathrm{Res}(F) = 0$ *iff there exists a non-trivial common solution in K^n of F. Precisely, we have*

$$\forall F\ [\ \mathrm{Res}(F) = 0 \iff \exists \bar{X} \in K^n\ [F(\bar{X}) = 0 \wedge \bar{X} \neq 0\ ]\ ].$$

(P2) *Resultants commutes with coefficient homomorphisms. Precisely, let D' be an integral domain. Let $\phi : D \longrightarrow D'$ be a homomorphism and let $\Phi : D[x] \longrightarrow D'[x]$ be the induced homomorphism. Then we have*

$$\mathrm{Res}(\Phi(F)) = \phi(\mathrm{Res}(F)).$$

(P3) *The resultant of a generic list of polynomials* † *is irreducible.*

(P4) $\mathrm{Res}(x_1^{e_1}, \ldots, x_n^{e_n}) = 1.$ □

We list two more properties of resultants that will be used in the following sections.

LEMMA 2.1. *Let*

$$\begin{aligned} F &= (f_1, \ldots, f_{i-1}, gh, f_{i+1}, \ldots, f_n) \\ G &= (f_1, \ldots, f_{i-1}, g, f_{i+1}, \ldots, f_n) \\ H &= (f_1, \ldots, f_{i-1}, h, f_{i+1}, \ldots, f_n). \end{aligned}$$

Then we have

$$\mathrm{Res}(F) = \mathrm{Res}(G)\mathrm{Res}(H). \ \square$$

LEMMA 2.2. *Let c be an indeterminate. Then we have*

$$\mathrm{Res}(cx_1, x_2, \ldots, x_n) = c. \ \square$$

3. Main Result

In this section, we make a precise statement of the main theorem of this paper.

DEFINITION 3.1. (COMPOSITION) *Let $\Theta = (\theta_1, \ldots, \theta_n)$ be a list of n homogeneous polynomials. Then the* composition *of F by Θ, written as $F \circ \Theta$, is the list of polynomial obtained from F by replacing each x_i in it with θ_i.* □

Now we are ready to state the main result of this paper.

† A list $(f_1, \ldots, f_n)$ is called generic if $f_i = \sum_{e_1 + \cdots + e_n = d_i} a_{i,e_1,\ldots,e_n} x_1^{e_1} \cdots x_n^{e_n}$ and each coefficient $a_{i,e_1,\ldots,e_n}$ is a distinct indeterminate. In that case, the coefficient domain D can be chosen as $\mathbf{Z}[A]$ where $\mathbf{Z}$ is the ring of integers and A is the list of all those indeterminates.

THEOREM 3.1. (MAIN THEOREM) *Let F be a list of n homogeneous polynomials of degrees $d_1, \ldots, d_n > 0$. Let Θ be a list of n homogeneous polynomials of degree $\ell > 0$. Then we have*

$$\mathrm{Res}(F \circ \Theta) = \mathrm{Res}(F)^{\ell^{n-1}} \mathrm{Res}(\Theta)^{d_1 \cdots d_n}. \quad \square$$

Remark: Note that we require the polynomials in Θ to have the same degree ℓ. It is to ensure that the polynomials in $F \circ \Theta$ are homogeneous.

Remark: Note also that we require that the polynomials in F and Θ are of positive degrees (non constants). We could have allowed constants, in particular 0, but then the statement of the theorem must be modified technically, losing its elegance. I decided against it, because such degenerate cases are not important enough to cover in the expense of the elegance of the above formula.

Remark: Note that $f_i \circ \Theta$ is "usually" of degree $d_i \ell$. But sometimes it could be 0. For instance, let $f_i = x_1 - x_2$ and $\Theta = (x_1, x_1)$. Then $f_i \circ \Theta = x_1 - x_1 = 0$. However, fortunately, $f_i \circ \Theta$ can never be non-zero constant. Thus, $\mathrm{Res}(F \circ \Theta)$ is defined.

4. Proof

In this section, we give a proof of the main theorem. The proof is divided into several lemmas which are interesting on their own. First, we fix some notations that will be used throughout the section.

NOTATIONS 4.1.

G	*a list $(g_1, \ldots, g_n)$ of* **generic** *homogeneous polynomials in $K[A][X]$ of degrees $d_1, \ldots, d_n > 0$, where A is a list of all the indeterminate coefficients.*
Ψ	*a list $(\psi_1, \ldots, \psi_n)$ of* **generic** *homogeneous polynomials in $K[B][X]$ of degrees $\ell > 0$, where B is a list of all the indeterminate coefficients. Assume that B is disjoint from A.*
C	*a list $(c_1, \ldots, c_\lambda)$ of all the indeterminates in A and B. Obviously $K[A][X]$ and $K[B][X]$ can be embedded into $K[C][X]$.*
$\bar{C}$	*a list $(\bar{c}_1, \ldots, \bar{c}_\lambda)$ of elements of K.*
$P \bullet \bar{C}$	*the object obtained from the object P by replacing c_i in P with $\bar{c}_i$.*
$P \circ Q$	*the object obtained from the object P by replacing x_i in P with q_i where $Q = (q_1, \ldots, q_n)$.* $\square$

Remark: The symbols $\bullet$ and $\circ$ are "over-loaded", that is, the same symbols will be used for different domains/co-domains (different types). The reason is obvious: *notational economy.* It will not cause confusion since their types will be always clear from the context where they appear.

Remark: Obviously " $\bullet \bar{C}$ " is a coefficient homomorphism.

Remark: In order to avoid writing numerous parentheses, we will assume that the operations $\bullet$ and $\circ$ are *left-associative*, that is, for instance,

$$P \circ Q \bullet R \circ S \qquad \text{stands for} \qquad ((P \circ Q) \bullet R) \circ S.$$

We will also assume that those operations have higher precedence over the multiplication, that is, for instance,

$$P \circ Q R \bullet S \qquad \text{stands for} \qquad (P \circ Q)(R \bullet S).$$

We list some elementary facts about the operations $\circ$ and $\bullet$. These will be used frequently, but *without* explicit reference to them.

PROPOSITION 4.1.

(a) $(PQ) \circ R = P \circ R \; Q \circ R$

(b) $(PQ) \bullet R = P \bullet R \; Q \bullet R$

(c) $P \circ Q \circ R = P \circ (Q \circ R)$

(d) $P \circ Q \bullet R = (P \bullet R) \circ (Q \bullet R)$. □

PROOF. Immediate from their definitions. □

LEMMA 4.1. $\mathrm{Res}(G \circ \Psi) \bullet \bar{C} = 0 \quad \Longrightarrow \quad \mathrm{Res}(G) \bullet \bar{C} \; \mathrm{Res}(\Psi) \bullet \bar{C} = 0$. □

PROOF. We prove the contrapositive of this. Thus, assume that

$$\mathrm{Res}(G) \bullet \bar{C} \; \mathrm{Res}(\Psi) \bullet \bar{C} \neq 0.$$

Then obviously $\mathrm{Res}(G) \bullet \bar{C} \neq 0$ and $\mathrm{Res}(\Psi) \bullet \bar{C} \neq 0$. We will show that $\mathrm{Res}(G \circ \Psi) \bullet \bar{C} \neq 0$. Let $\bar{X} \in K^n$ be an arbitrary solution of $G \circ \Psi \bullet \bar{C}$, that is,

$$G \circ \Psi \bullet \bar{C} \circ \bar{X} = 0.$$

Claim: $\bar{X}$ is trivial. In order to prove this, first note

$$0 = G \circ \Psi \bullet \bar{C} \circ \bar{X} = (G \bullet \bar{C}) \circ (\Psi \bullet \bar{C}) \circ \bar{X} = (G \bullet \bar{C}) \circ (\Psi \bullet \bar{C} \circ \bar{X}).$$

Thus, $\Psi \bullet \bar{C} \circ \bar{X}$ is a solution of $G \bullet \bar{C}$. By **(P2)** and the assumption that $\mathrm{Res}(G) \bullet \bar{C} \neq 0$, we have $\mathrm{Res}(G \bullet \bar{C}) \neq 0$. Thus, by **(P1)**, there is *no* non-trivial solution of $G \bullet \bar{C}$. Thus $\Psi \bullet \bar{C} \circ \bar{X}$ must be a trivial solution of $G \bullet \bar{C}$, that is,

$$\Psi \bullet \bar{C} \circ \bar{X} = 0.$$

Thus $\bar{X}$ is a solution of $\Psi \bullet \bar{C}$. By **(P2)** and the assumption that $\mathrm{Res}(\Psi) \bullet \bar{C} \neq 0$, we have $\mathrm{Res}(\Psi \bullet \bar{C}) \neq 0$. Thus, by **(P1)**, there is *no* non-trivial solution of $\Psi \bullet \bar{C}$. Thus $\bar{X}$ must be trivial. The claim has been proved.

From the claim and **(P1)**, we have $\mathrm{Res}(G \circ \Psi \bullet \bar{C}) \neq 0$. Then, by **(P2)**, we finally have $\mathrm{Res}(G \circ \Psi) \bullet \bar{C} \neq 0$. □

LEMMA 4.2. $\mathrm{Res}(G \circ \Psi) = w \; \mathrm{Res}(G)^{\mu} \; \mathrm{Res}(\Psi)^{\nu}$ *for some* $w \in K$ *and* $\mu, \nu \geq 0$. □

PROOF. By applying Hilbert's Nullstellensatz on Lemma 4.1, we have

$$\left(\mathrm{Res}(G)\mathrm{Res}(\Psi)\right)^{\delta} \quad \in \quad \mathrm{Ideal}(\mathrm{Res}(G \circ \Psi)).$$

for some $\delta > 0$. Thus, we have

$$\mathrm{Res}(G\circ\Psi) \quad | \quad (\mathrm{Res}(G)\mathrm{Res}(\Psi))^{\delta}.$$

Recall that G is generic with the indeterminate coefficients A and Ψ is also generic with the indeterminate coefficients B, and that A and B are disjoint. Thus, by **(P3)**, we see that $\mathrm{Res}(G)$ and $\mathrm{Res}(\Psi)$ are irreducible and that they are relatively prime. From this, the lemma follows immediately. □

Thus, we have obtained a "skeleton" of the main theorem for the generic case. In the following, we will fill in the flesh, that is, determine the values of w, μ, and ν. After that, we will relax it to non-generic cases.

LEMMA 4.3. $\mathrm{Res}(G\circ\Psi) = \mathrm{Res}(G)^{\mu}\,\mathrm{Res}(\Psi)^{\nu}$ *for some* $\mu, \nu \geq 0$. □

PROOF. Recalling Lemma 4.2, we need to show that $w = 1$. For this let $\bar{C}$ be such that

$$\begin{aligned} G\bullet\bar{C} &= (x_1^{d_1}, \ldots, x_n^{d_n}) \\ \Psi\bullet\bar{C} &= (x_1^{\ell}, \ldots, x_n^{\ell}). \end{aligned}$$

Such $\bar{C}$ exists since G and Ψ are generic. Now we have

$$\begin{aligned} \mathrm{Res}(G\circ\Psi\bullet\bar{C}) &= \mathrm{Res}((G\bullet\bar{C})\circ(\Psi\bullet\bar{C})) \\ &= \mathrm{Res}((x_1^{d_1}, \ldots, x_n^{d_n})\circ(x_1^{\ell}, \ldots, x_n^{\ell})) \\ &= \mathrm{Res}(x_1^{d_1\ell}, \ldots, x_n^{d_n\ell}) \\ &= 1 && \text{by } \mathbf{(P4)}. \end{aligned}$$

Next we will determine again the value of $\mathrm{Res}(G\circ\Psi\bullet\bar{C})$, but following a different "path" of reasoning.

$$\begin{aligned} \mathrm{Res}(G\circ\Psi\bullet\bar{C}) &= \mathrm{Res}(G\circ\Psi)\bullet\bar{C} && \text{by } \mathbf{(P2)} \\ &= (w\mathrm{Res}(G)^{\mu}\mathrm{Res}(\Psi)^{\nu})\bullet\bar{C} && \text{by Lemma 4.2} \\ &= w(\mathrm{Res}(G)\bullet\bar{C})^{\mu}(\mathrm{Res}(\Psi)\bullet\bar{C})^{\nu} \\ &= w\mathrm{Res}(G\bullet\bar{C})^{\mu}\mathrm{Res}(\Psi\bullet\bar{C})^{\nu} && \text{by } \mathbf{(P2)} \\ &= w\mathrm{Res}(x_1^{d_1}, \ldots, x_n^{d_n})^{\mu}\mathrm{Res}(x_1^{\ell}, \ldots, x_n^{\ell})^{\nu} \\ &= w && \text{by } \mathbf{(P4)}. \end{aligned}$$

Thus, we conclude that $w = 1$. □

Now we need to determine the exponents μ and ν. For this, the following lemma will be used frequently.

LEMMA 4.4. *Let c be an indeterminate and $e, e_1, \ldots, e_n > 0$. Then we have*

$$\mathrm{Res}(c^e x_1^{e_1}, x_2^{e_2}, \ldots, x_n^{e_n}) = c^{e e_2 \cdots e_n}. \ \Box$$

PROOF. When $e_1 = 1$, we obviously have,

$$\mathrm{Res}(c^e x_1^{e_1}, x_2^{e_2}, \ldots, x_n^{e_n}) = \mathrm{Res}(c^e x_1, x_2^{e_2}, \ldots, x_n^{e_n}).$$

When $e_1 > 1$, we have, by Lemma 2.1 and **(P4)**,

$$\begin{aligned}\mathrm{Res}(c^e x_1^{e_1}, x_2^{e_2}, \ldots, x_n^{e_n}) &= \mathrm{Res}(c^e x_1, x_2^{e_2}, \ldots, x_n^{e_n})\mathrm{Res}(x_1^{e_1-1}, x_2^{e_2}, \ldots, x_n^{e_n}) \\ &= \mathrm{Res}(c^e x_1, x_2^{e_2}, \ldots, x_n^{e_n}).\end{aligned}$$

Thus, we always have

$$\mathrm{Res}(c^e x_1^{e_1}, x_2^{e_2}, \ldots, x_n^{e_n}) = \mathrm{Res}(c^e x_1, x_2^{e_2}, \ldots, x_n^{e_n}).$$

By repeatedly applying Lemma 2.1, we have

$$\mathrm{Res}(c^e x_1, x_2^{e_2}, \ldots, x_n^{e_n}) = \mathrm{Res}(c^e x_1, x_2, \ldots, x_n)^{e_2\cdots e_n}.$$

By applying **(P2)** on Lemma 2.2, with $\phi(c) = c^e$, we obtain

$$\mathrm{Res}(c^e x_1, x_2, \ldots, x_n)^{e_2\cdots e_n} = (c^e)^{e_2\cdots e_n}.$$

Putting the last three equalities together we see immediately that

$$\mathrm{Res}(c^e x_1^{e_1}, x_2^{e_2}, \ldots, x_n^{e_n}) = c^{e e_2\cdots e_n}.$$

□

LEMMA 4.5. $\mathrm{Res}(G\circ\Psi) = \mathrm{Res}(G)^{\ell^{n-1}}\,\mathrm{Res}(\Psi)^{\nu}$ *for some* $\nu \geq 0$. □

PROOF. Recalling Lemma 4.3, we need to show that $\mu = \ell^{n-1}$. For this let $\bar{C}$ be such that

$$\begin{aligned}G\bullet\bar{C} &= (cx_1^{d_1}, x_2^{d_2}, \ldots, x_n^{d_n}) \\ \Psi\bullet\bar{C} &= (x_1^{\ell}, \ldots, x_n^{\ell})\end{aligned}$$

where c is an indeterminate. Such $\bar{C}$ exists since G and Ψ are generic. Now we have

$$\begin{aligned}\mathrm{Res}(G\circ\Psi\bullet\bar{C}) &= \mathrm{Res}((G\bullet\bar{C})\circ(\Psi\bullet\bar{C})) \\ &= \mathrm{Res}((cx_1^{d_1}, x_2^{d_2}, \ldots, x_n^{d_n})\circ(x_1^{\ell}, \ldots, x_n^{\ell})) \\ &= \mathrm{Res}(cx_1^{d_1\ell}, x_2^{d_2\ell}, \ldots, x_n^{d_n\ell}) \\ &= c^{d_2\cdots d_n\ell^{n-1}} && \text{by Lemma 4.4.}\end{aligned}$$

Next we will determine again the value of $\mathrm{Res}(G\circ\Psi\bullet\bar{C})$, but following a different path of reasoning.

$$\begin{aligned}\mathrm{Res}(G\circ\Psi\bullet\bar{C}) &= \mathrm{Res}(G\circ\Psi)\bullet\bar{C} && \text{by } \mathbf{(P2)} \\ &= (\mathrm{Res}(G)^{\mu}\mathrm{Res}(\Psi)^{\nu})\bullet\bar{C} && \text{by Lemma 4.3} \\ &= (\mathrm{Res}(G)\bullet\bar{C})^{\mu}(\mathrm{Res}(\Psi)\bullet\bar{C})^{\nu} \\ &= \mathrm{Res}(G\bullet\bar{C})^{\mu}\mathrm{Res}(\Psi\bullet\bar{C})^{\nu} && \text{by } \mathbf{(P2)} \\ &= \mathrm{Res}(cx_1^{d_1}, x_2^{d_2}, \ldots, x_n^{d_n})^{\mu}\mathrm{Res}(x_1^{\ell}, \ldots, x_n^{\ell})^{\nu} \\ &= \mathrm{Res}(cx_1^{d_1}, x_2^{d_2}, \ldots, x_n^{d_n})^{\mu} && \text{by } \mathbf{(P4)} \\ &= c^{d_2\cdots d_n\mu} && \text{by Lemma 4.4.}\end{aligned}$$

Combining the results of the two derivations, we have $c^{d_2\cdots d_n\ell^{n-1}} = c^{d_2\cdots d_n\mu}$. Since c is an indeterminate, we have $d_2\cdots d_n\ell^{n-1} = d_2\cdots d_n\mu$. Since $d_i > 0$ for every i, we conclude that $\mu = \ell^{n-1}$. □

LEMMA 4.6. $\mathrm{Res}(G\circ\Psi) = \mathrm{Res}(G)^{\ell^{n-1}}\,\mathrm{Res}(\Psi)^{d_1\cdots d_n}$. □

PROOF. Recalling Lemma 4.5, we need to show that $\nu = d_1 \cdots d_n$. We will use the same proof technique as in the proof of Lemma 4.5. Thus, the proofs will be almost the same in their structures. The only main difference will be that we put an indeterminate on Θ instead of on G.

Let $\bar{C}$ be such that

$$\begin{aligned} G\bullet\bar{C} &= (x_1^{d_1}, \ldots, x_n^{d_n}) \\ \Psi\bullet\bar{C} &= (cx_1^{\ell}, x_2^{\ell}, \ldots, x_n^{\ell}) \end{aligned}$$

where c is an indeterminate. Such $\bar{C}$ exists since G and Ψ are generic. Now we have

$$\begin{aligned} \mathrm{Res}(G\circ\Psi\bullet\bar{C}) &= \mathrm{Res}((G\bullet\bar{C})\circ(\Psi\bullet\bar{C})) \\ &= \mathrm{Res}((x_1^{d_1}, \ldots, x_n^{d_n})\circ(cx_1^{\ell}, x_2^{\ell}, \ldots, x_n^{\ell})) \\ &= \mathrm{Res}(c^{d_1} x_1^{d_1\ell}, x_2^{d_2\ell}, \ldots, x_n^{d_n\ell}) \\ &= c^{d_1\cdots d_n \ell^{n-1}} && \text{by Lemma 4.4.} \end{aligned}$$

Next we will determine again the value of $\mathrm{Res}(G\circ\Psi\bullet\bar{C})$, but following a different path of reasoning.

$$\begin{aligned} \mathrm{Res}(G\circ\Psi\bullet\bar{C}) &= \mathrm{Res}(G\circ\Psi)\bullet\bar{C} && \text{by } \mathbf{(P2)} \\ &= (\mathrm{Res}(G)^{\ell^{n-1}}\mathrm{Res}(\Psi)^{\nu})\bullet\bar{C} && \text{by Lemma 4.5} \\ &= (\mathrm{Res}(G)\bullet\bar{C})^{\ell^{n-1}}(\mathrm{Res}(\Psi)\bullet\bar{C})^{\nu} \\ &= \mathrm{Res}(G\bullet\bar{C})^{\ell^{n-1}}\mathrm{Res}(\Psi\bullet\bar{C})^{\nu} && \text{by } \mathbf{(P2)} \\ &= \mathrm{Res}(x_1^{d_1}, \ldots, x_n^{d_n})^{\ell^{n-1}}\mathrm{Res}(cx_1^{\ell}, x_2^{\ell}, \ldots, x_n^{\ell})^{\nu} \\ &= \mathrm{Res}(cx_1^{\ell}, x_2^{\ell}, \ldots, x_n^{\ell})^{\nu} && \text{by } \mathbf{(P4)} \\ &= c^{\nu\ell^{n-1}} && \text{by Lemma 4.4.} \end{aligned}$$

Combining the results of the two derivations, we have $c^{d_1\cdots d_n\ell^{n-1}} = c^{\nu\ell^{n-1}}$. Since c is an indeterminate, we have $d_1 \cdots d_n \ell^{n-1} = \nu\ell^{n-1}$. Since $\ell > 0$, we conclude that $\nu = d_1 \cdots d_n$.
□

Thus, we have proved the main theorem for the *generic* case. Now, we will relax it to (possibly) non-generic cases, finally proving the main theorem of this paper.

THEOREM 4.1. (MAIN THEOREM) *Let F be a list of n homogeneous polynomials of degrees $d_1, \ldots, d_n > 0$. Let Θ be a list of n homogeneous polynomials of degree $\ell > 0$. Then we have,*

$$\mathrm{Res}(F\circ\Theta) = \mathrm{Res}(F)^{\ell^{n-1}}\mathrm{Res}(\Theta)^{d_1\cdots d_n}. \ \square$$

PROOF. Obviously,

$$\begin{aligned} F &= G\bullet\bar{C} \\ \Theta &= \Psi\bullet\bar{C} \end{aligned}$$

for some $\bar{C}$. Now note

$$\begin{array}{rcll}
\mathrm{Res}(F\circ\Theta) & = & \mathrm{Res}((G\bullet\bar{C})\circ(\Psi\bullet\bar{C})) & \\
& = & \mathrm{Res}(G\circ\Psi\bullet\bar{C}) & \\
& = & \mathrm{Res}(G\circ\Psi)\bullet\bar{C} & \text{by } \mathbf{(P2)} \\
& = & (\mathrm{Res}(G)^{\ell^{n-1}}\mathrm{Res}(\Psi)^{d_1\cdots d_n})\bullet\bar{C} & \text{by Lemma 4.6} \\
& = & (\mathrm{Res}(G)\bullet\bar{C})^{\ell^{n-1}}(\mathrm{Res}(\Psi)\bullet\bar{C})^{d_1\cdots d_n} & \\
& = & \mathrm{Res}(G\bullet\bar{C})^{\ell^{n-1}}\mathrm{Res}(\Psi\bullet\bar{C})^{d_1\cdots d_n} & \text{by } \mathbf{(P2)} \\
& = & \mathrm{Res}(F)^{\ell^{n-1}}\mathrm{Res}(\Theta)^{d_1\cdots d_n}. &
\end{array}$$

□

Acknowledgment: This research was done in the framework of the European project ACCLAIM sponsored by Austrian Science Foundation.

References

Canny, J. F., Imiris, I. (1993). An efficient algorithm for the sparse mixed resultant. In *Proc. of AAECC*.

Cayley, A. (1865). On the theory of elimination. *Cambridge and Dublin Mathematical Journal*, III:210–270.

Chardin, M. (1991). Un algorithme pour le calcul des resultants. In *Proc. of Effective Methods in Algebraic Geometry*, pages 47–62. Birkhauser.

der Waerden, B. L. Van (1966). *Modern Algebra Vols. I and II.* Fredrick Ungar Publishing Co., New York.

Dixon, A. L. (1908). The eliminant of three quantics in two independent variables. *Proc. London Mathematical Society*, 6:468–478.

Hong, H. (1995). Groebner basis Under Composition. Technical Report 95-55, Research Institute for Symbolic Computation, Johannes Kepler University A-4040 Linz, Austria. Submitted for publication.

Hong, H. (1995). Subresultant Under Composition. Technical Report 95-47, Research Institute for Symbolic Computation, Johannes Kepler University A-4040 Linz, Austria. Submitted for publication.

Kaltofen, E., Lakshman, Y.N. (1988). Improved sparse multivariate polynomial interpolation algorithms. In *Lecture Notes in Computer Science*, volume 358, pages 467–474. Springer-Verlag.

Kapur, D., Lakshman, Y. N. (1992). Elimination methods: An introduction. In *Symbolic and Numerical Computation for Artificial Intelligence*, pages 45–89. Academic Press.

Kapur, Deepak, Saxena, Tushar (1995). Comparison of various multivariate resultant formulations. In *ISSAC95*. ACM Press.

Macaulay, F. S. (1916). *The Algebraic Theory of Modular Systems.* Cambridge University Press.

Manocha, D. (1993). Efficient algorithms for multipolynomial resultant. *The Computer Journal*, 36(5):485–496. In a special issue on *computational quantifier elimination*, edited by H. Hong.

Sturmfels, B. (1991). Sparse elimination theory. In Robbiano, L., Eisenbud, D., editors, *Proc. Cortona 1991.* Cambridge University Press.

White, H.S. (1909). Bezout's theory of resultants and its influence on geometry. *Bulletin of the American Mathematical Society*, 112:59–68.

Zippel, R. E. (1990). Interpolating polynomials from their values. *Journal of Symbolic Computation*, 9:375–403.