



**HAL**  
open science

# The Vandermonde determinant identity in higher dimension

Itaï Ben Yaacov

► **To cite this version:**

| Itaï Ben Yaacov. The Vandermonde determinant identity in higher dimension. 2017. hal-00983858v3

**HAL Id: hal-00983858**

**<https://hal.science/hal-00983858v3>**

Preprint submitted on 20 Mar 2017 (v3), last revised 12 Feb 2024 (v5)

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

# THE VANDERMONDE DETERMINANT IDENTITY IN HIGHER DIMENSION

ITAI BEN YAACOV

ABSTRACT. We generalise the Vandermonde determinant identity to one which tests whether a family of hypersurfaces in  $\mathbf{P}^n$  has an unexpected intersection point.

The intended application is an asymptotic estimate of the volume of certain spaces of homogeneous polynomials on an embedded projective variety.

## CONTENTS

Introduction	1
1. Appetiser: a linear Vandermonde identity	1
2. A brief and elementary introduction to Chow forms and resultants	3
2.1. General preliminaries	3
2.2. Splitting polynomials	4
2.3. Chow forms and resultants	5
3. An asymptotic Vandermonde determinant relation for hypersurfaces	9
References	15

## INTRODUCTION

The Vandermonde determinant identity tests by a single determinant whether a family of points on the line are distinct. We generalise this to dimension  $n$ , testing by a single determinant whether some  $n + 1$  hyperplanes among a large family intersect. This is further generalised for a family of hypersurfaces, up to an asymptotically negligible error.

### 1. APPETISER: A LINEAR VANDERMONDE IDENTITY

The classical Vandermonde determinant identity asserts that in any commutative unital ring  $A$ ,

$$\det \begin{pmatrix} 1 & a_0 & \dots & a_0^m \\ 1 & a_1 & \dots & a_1^m \\ \vdots & \vdots & & \vdots \\ 1 & a_m & \dots & a_m^m \end{pmatrix} = \prod_{i < j \leq m} (a_j - a_i). \quad (1)$$

This instance of the identity is in degree  $m$ , and since each row depends on a single unknown, it is in (affine) dimension one. Homogenising (and transposing) we get the projective dimension one version, namely

$$\det \begin{pmatrix} a_0^m & a_1^m & \dots & a_m^m \\ a_0^{m-1}b_0 & a_1^{m-1}b_1 & \dots & a_m^{m-1}b_m \\ \vdots & \vdots & & \vdots \\ b_0^m & b_1^m & \dots & b_m^m \end{pmatrix} = \prod_{i < j \leq m} (a_i b_j - a_j b_i) = \prod_{i < j \leq m} \det \begin{pmatrix} a_i & a_j \\ b_i & b_j \end{pmatrix}. \quad (2)$$

The matrix on the left hand side is obtained from the family of points  $(a_i, b_i)$  via the *Veronese map*, namely the map sending the coordinates of a point  $x$  to the family of values of monomials of degree  $m$  at  $x$ , which can be viewed as the coordinates of the evaluation functional at  $x$  on homogeneous polynomials of degree  $m$ .

2010 *Mathematics Subject Classification.* 15A15.

*Key words and phrases.* Vandermonde ; determinant.

Author supported by ANR projects GruPoLoCo (ANR-11-JS01-008) and ValCoMo (ANR-13-BS01-0006).

*Revision* 3435 of 20th March 2017.

**Notation 1.1.** Let  $A$  be a commutative ring,  $n, m, \ell \in \mathbf{N}$ . The set of multi-exponents of total degree  $m$  in  $n + 1$  unknowns will be denoted  $\varepsilon(n, m) = \{\alpha \in \mathbf{N}^{n+1} : \sum \alpha = m\}$ , which we equip with inverse lexicographic ordering (namely, the exponent of  $X_n$  is most significant), giving an ordering on the monomials. We define  $v_m: A^{n+1} \rightarrow A^N$ , where  $N = \binom{n+m}{n}$  is the number of monomials, as the corresponding Veronese embedding, that is,  $v_{m,i}(x)$  is the  $i$ th monomial applied to  $x$ . We extend  $v_m$  to a map  $M_{(n+1) \times \ell}(A) \rightarrow M_{N \times \ell}(A)$  by applying  $v_m$  to each column. Notice that  $n$  is determined by the argument so we shall use the same notation for different values of  $n$ .

In projective dimension  $n = 1$ , letting  $a_i = (a_{i,0}, a_{i,1})$  (viewed as a column vector), the Vandermonde identity (2) becomes:

$$\det(v_m(a_0, \dots, a_m)) = \prod_{i < j \leq m} \det(a_i, a_j). \quad (3)$$

The right hand side tests whether all points are distinct in a given family in  $\mathbf{P}^1$ . In higher dimension, we may ask whether a family of points  $\mathbf{P}^n$  is in general position, namely, no  $n + 1$  lie in a single hyperplane. Alternatively, since points in  $\mathbf{P}^1$  are also hyperplanes, we may also ask the dual question, whether a family of hyperplanes in  $\mathbf{P}^n$  is in general position, namely, no  $n + 1$  of them intersect.

The correct generalisation turns out to be the second one, and it suggests how the left hand side should be generalised as well. Indeed, the Veronese map acts on points, and if we consider the unknowns to represent a family of hyperplanes in  $\mathbf{P}^n$ , then in order to get points we still need to intersect sub-families of size  $n$ .

Algebraically, a hyperplane is given as a linear form. A family of hyperplanes is then given as a matrix  $\Lambda \in M_{(n+1) \times m}(A)$ , and intersections of sub-families are represented by minors of this matrix.

**Notation 1.2.** Let  $A$  be a commutative ring,  $n, m \in \mathbf{N}$ .

(i) We define  $\mu: M_{(n+1) \times m}(A) \rightarrow M_{(n+1) \times \binom{m}{n}}(A)$  by sending a matrix  $\Lambda$  to the matrix of minors of  $\Lambda$  of order  $n$ . Minors are ordered by lexicographic ordering on the sequences of rows/columns which are chosen.

(ii) We define  $\delta: M_{(n+1) \times m}(A) \rightarrow A$  by sending a matrix  $\Lambda$  to the product of minors of  $\Lambda$  of order  $n + 1$ .

Again,  $n$  and  $m$  are determined by the arguments.

In projective dimension one we have  $\mu\Lambda = \Lambda$  and (2) asserts that  $\det(v_m\Lambda) = \det(v_m\mu\Lambda) = \delta\Lambda$ . This generalises to higher projective dimension.

**Lemma 1.3.** Let  $A$  be a commutative ring,  $n \leq m \in \mathbf{N}$ , and let  $\Lambda \in M_{(n+1) \times m}(A)$ . Then

(i) Adding one row of  $\Lambda$ , times a scalar, to another, does not change either  $\det(v_{m-n}\mu\Lambda)$  or  $\delta\Lambda$ .

(ii) Multiplying a row of  $\Lambda$  by a scalar  $\alpha$  multiplies  $\det(v_{m-n}\mu\Lambda)$  by  $\alpha^{n \binom{m}{n+1}}$  and  $\delta\Lambda$  by  $\alpha^{\binom{m}{n+1}}$ .

(iii) Multiplying a column of  $\Lambda$  by a scalar  $\alpha$  multiplies  $\det(v_{m-n}\mu\Lambda)$  by  $\alpha^{n \binom{m-1}{n}}$  and  $\delta\Lambda$  by  $\alpha^{\binom{m-1}{n}}$ .

*Proof.* All three assertions are clear for  $\delta\Lambda$ , and we verify them for  $\det(v_{m-n}\mu\Lambda)$ .

For the first assertion, adding a multiple of a row in  $\Lambda$  to another amounts to a similar operation on  $\mu\Lambda$  and to a sequence of several such operations on  $v_{m-n}\mu\Lambda$ . For the second assertion, multiplying a row of  $\Lambda$  by  $\alpha$  amounts to multiplying  $n$  rows of  $\mu\Lambda$  by  $\alpha$ . The sum of total degrees of all monomials is  $(m-n)\binom{m}{n} = (n+1)\binom{m}{n+1}$ , so the sum of degrees in  $n$  out of  $n+1$  unknowns is  $n\binom{m}{n+1}$ . For the third assertion, multiplying a column of  $\Lambda$  by  $\alpha$  amounts to multiplying  $\binom{m-1}{n-1}$  columns of  $\mu\Lambda$  by  $\alpha$ , and the same columns of  $v_{m-n}\mu\Lambda$  by  $\alpha^{m-n}$ , for a total degree of  $(m-n)\binom{m-1}{n-1} = n\binom{m-1}{n}$  ■

**Theorem 1.4.** Let  $A$  be a commutative ring,  $n \leq m \in \mathbf{N}$ , and let  $\Lambda \in M_{(n+1) \times m}(A)$ . Then  $v_{m-n}\mu\Lambda$  is a square matrix of order  $\binom{m}{n}$ , and the Vandermonde identity of order  $m$  in dimension  $n$  holds:

$$\det(v_{m-n}\mu\Lambda) = (\delta\Lambda)^n. \quad (4)$$

*Proof.* We proceed by induction on  $(n, m-n)$ . When  $n = 0$  or  $n = m$ , both sides of (4) are equal to one. When  $n, m-n > 0$ , it will suffice to prove (4) in the case where  $A$  is a polynomial ring, and in particular, an integral domain.

If the first column of  $\Lambda$  vanishes then so do both sides of (4) and we are done. Otherwise, by Lemma 1.3 we may assume that the first column is of the form  $(1, 0, \dots, 0)$ . Let  $\Lambda_0$  be  $\Lambda$  without this column and let  $\Lambda_1$  be  $\Lambda$  with both first row and column dropped. Then  $\delta\Lambda = (\delta\Lambda_0)(\delta\Lambda_1)$ , and by the induction hypothesis for  $(n, m-n-1)$  and  $(n-1, m-n)$  we have

$$\det(v_{m-n-1}\mu\Lambda_0) = (\delta\Lambda_0)^n, \quad \det(v_{m-n}\mu\Lambda_1) = (\delta\Lambda_1)^{n-1}.$$

Now,

$$\mu\Lambda = \begin{pmatrix} \mu\Lambda_1 & \\ & \mu\Lambda_0 \end{pmatrix}, \quad \nu_{m-n}\mu\Lambda = \begin{pmatrix} \nu_{m-n}\mu\Lambda_1 & \\ & \nu_{m-n}\mu\Lambda_0 \end{pmatrix} = \begin{pmatrix} \nu_{m-n}\mu\Lambda_1 & ? \\ & C \end{pmatrix}.$$

The matrix  $\nu_{m-n}\mu\Lambda_1$  is square of order  $\binom{m-1}{n-1}$ , and  $C$  is the lower square part of  $\nu_{m-n}\mu\Lambda_0$ , of order  $\binom{m}{n} - \binom{m-1}{n-1} = \binom{m-1}{n}$ . The rows of  $C$  correspond to monomials in which the last unknown appears. Factoring this common unknown out, and letting  $(\dots, b_j, \dots)$  denote the last row of  $\mu\Lambda_0$ , we see that  $C$  is obtained by multiplying each column of  $\nu_{m-n-1}\mu\Lambda_0$  by the corresponding  $b_j$ . Notice that the  $b_j$  are simply the minors of order  $n$  of  $\Lambda_1$ , so

$$\det(\nu_{m-n}\mu\Lambda) = \det(\nu_{m-n}\mu\Lambda_1) \det(\nu_{m-n-1}\mu\Lambda_0) \prod b_j = (\delta\Lambda_1)^{n-1} (\delta\Lambda_0)^n (\delta\Lambda_1) = (\delta\Lambda)^n,$$

as desired.  $\blacksquare$

**Corollary 1.5.** *Let  $A$  be a commutative ring,  $n \leq m \in \mathbf{N}$ , and let  $\Lambda = (\lambda_{i,j}) \in M_{(n+1) \times m}(A)$ . Identify the  $j$ th column of  $\Lambda$  with a linear form  $\lambda_j = \sum_{i \leq n} \lambda_{i,j} X_i$ . For a subset  $\xi \subseteq m$  of size  $n$ , define  $\varphi_\xi$  as the product of  $\lambda_j$  for  $j \notin \xi$ , a homogeneous polynomial of degree  $m - n$ . Ordering monomials as earlier we may identify  $\varphi_\xi$  with the column vector of coefficients. Ordering the subsets  $\xi$  lexicographically we obtain a matrix denoted  $\pi\Lambda$ .*

*Then  $\pi\Lambda$  is a square matrix of order  $\binom{m}{n}$ , and the dual Vandermonde identity of order  $m$  in dimension  $n$  holds:*

$$\det(\pi\Lambda) = \pm \delta\Lambda. \quad (5)$$

*Proof.* Let  $\xi$  and  $\zeta$  denote subsets of  $m$  of size  $n$ . Let  $\mu'\Lambda$  be obtained by permuting rows of  $\mu\Lambda$  and multiplying some rows by  $-1$ . Then  $\nu_{m-n}\mu'\Lambda$  is also obtained from  $\nu_{m-n}\mu\Lambda$  by a permutation and sign changes to the rows. Let  $p_\zeta \in A^{n+1}$  be the column of  $\mu'\Lambda$  corresponding to  $\zeta$ : with an adequate choice of  $\mu'\Lambda$  (i.e., of permutation and signs), it is the intersection point of the kernels of  $(\lambda_i)_{i \in \xi}$  (we may assume that  $\Lambda$  consists of formal unknowns, so the kernels intersect at a single line, i.e., single projective point). By definition of the Veronese map, the dot product of the columns of  $\pi\Lambda$  and  $\nu_{m-n}\mu'\Lambda$  corresponding to  $\xi$  and  $\zeta$ , respectively, is  $\varphi_\xi(p_\zeta)$ , viewed as a polynomial evaluated at a point. If  $\xi \neq \zeta$ , then  $\varphi_\xi(p_\zeta) = 0$ , and  $\varphi_\xi(p_{\bar{\zeta}})$  is equal, up to sign, to the product of minors of order  $n + 1$  of  $\Lambda$  corresponding to the  $n$  columns in  $\xi$  plus one more. Thus each minor of order  $n + 1$  of  $\Lambda$  is a factor of  $n + 1$  expressions  $\varphi_\xi(p_{\bar{\zeta}})$ . We conclude that

$$\det(\pi\Lambda) \det(\nu_{m-n}\mu'\Lambda) = \prod_{\xi} \varphi_\xi(p_{\bar{\zeta}}) = \pm (\delta\Lambda)^{n+1}.$$

Since  $\det(\nu_{m-n}\mu'\Lambda) = \pm \det(\nu_{m-n}\mu\Lambda) = \pm (\delta\Lambda)^n$ , and since we may assume  $A$  is an integral domain, our assertion follows.  $\blacksquare$

Somewhat informally we may restate (5) as saying that for a family  $\Lambda$  of  $m$  linear forms in affine dimension  $n + 1$ :

$$\det\left(\prod \lambda : \lambda \in \binom{\Lambda}{m-n}\right) = \pm \prod_{\lambda \in \binom{\Lambda}{n+1}} \det(\lambda). \quad (6)$$

## 2. A BRIEF AND ELEMENTARY INTRODUCTION TO CHOW FORMS AND RESULTANTS

In dimension one, a hypersurface is a hyperplane is a point, but in higher dimension one may ask if the Vandermonde identity can be extended to intersections of hypersurfaces, rather than hyperplanes. Intersections of hypersurfaces are calculated, algebraically, by resultants, generalising intersections of hyperplanes via determinants. Given the manner in which we use resultants here and in some intended applications, we prefer to give a presentation which diverges slightly from what we found in the literature, e.g., [GKZ94].

**2.1. General preliminaries.** Before starting, let us give a few reminders regarding integral dependence in rings (see for example [AM69]). We recall that if  $A \subseteq B$  are rings, then  $b \in B$  is *integral* over  $A$  if it satisfies a monic polynomial over  $A$ . We are only going to consider integral domains, in which case we have a convenient characterisation.

**Fact 2.1.** *Let  $L$  be a field,  $A \subseteq L$  a sub-ring. Then  $b \in L$  is integral over  $A$  if and only if, for every valuation  $w$  of  $L$ , if  $\mathcal{O}_w \supseteq A$  then  $b \in \mathcal{O}_w$  as well.*

If  $A \subseteq B$  are rings, then the *integral closure* of  $A$  in  $B$  consists of all  $b \in B$  integral over  $A$ . When  $A$  is an integral domain and  $K = \text{Frac}(A)$ , the *integral closure*  $A$  is its integral closure in  $K$ , and its *absolute integral closure* is its integral closure in the algebraic closure  $K^a$ . The integral closure of  $A$  (in  $B$ ) is *integrally closed* (in  $B$ ), i.e., equal to its own integral closure.

Unique factorisation domains are integrally closed (in their fraction fields), and a polynomial ring over an integrally closed ring is integrally closed. Moreover, we have the following characterisation of the absolute integral closure of a unique factorisation domain, which will be used in [Section 3](#).

**Fact 2.2.** *Let  $A$  be a unique factorisation domain,  $K = \text{Frac}(A)$  and  $L = K^a$  the algebraic closure. Then a necessary and sufficient condition for  $a \in L$  to be integral over  $A$  is that for every prime  $p \in A$  and valuation  $w$  of  $L$  extending the  $p$ -adic valuation  $v_p$  we have  $w(a) \geq 0$ .*

XXX CHECK LITERATURE XXX. The condition is clearly necessary. Conversely, if it holds for  $a$  it also holds for all its conjugates over  $K$ , so the monic irreducible polynomial of  $a$  over  $K$  is in fact over  $A$ . ■

When  $K$  is a field, we define for any  $f = \sum \alpha_s X^s \in K[X]$ :

$$v(f) = \min_s v(\alpha_s).$$

This is multiplicative on  $K[X]$  and therefore defines a valuation on  $K(X)$ .

**2.2. Splitting polynomials.** Throughout,  $n$  is a fixed projective dimension. A point  $[x] \in \mathbf{P}^n$  will be called *geometric*, and a representative  $x$  will be called an *algebraic point*.

We fix unknowns  $X = (X_0, \dots, X_n)$ , and let  $A[X]_m$  denote the module of homogeneous polynomials of degree  $m$  over a ring  $A$ . The unknowns  $X$  form a basis for the module of linear forms  $E = A[X]_1$ , and we let  $X^* = (X_0^*, \dots, X_n^*) \subseteq E^*$  be the dual basis. We may identify  $E^*$  with the pre-dual of  $E$ , namely with the space of algebraic points, identifying  $\sum x_i X_i^* \in E^*$  with  $x = (x_0, \dots, x_n)$ . Alternatively, we may view  $X^*$  as a new system of “dual unknowns”, in which case  $E^* = A[X^*]_1$ , and  $A[X^*]$  is the ring of polynomial functions on the space  $E$  of linear forms.

**Convention 2.3.** Let  $A$  be an integral domain,  $D \in \mathbf{N}$ , and  $g \in A[X^*]_D$ . When we say that  $g$  *splits*, we mean that it splits over some field  $L \supseteq \text{Frac}(A)$  as  $\alpha \prod_{i < D} x_i$ , where  $\alpha \in L$  and each  $x_i$  is a non-zero linear form in  $X^*$ , namely, an algebraic point.

A non-zero splitting polynomial  $g = \alpha \prod_{i < D} x_i$  codes the finite multi-set (namely, set with multiplicities) of geometric points  $[g] = \{[x_i] : i < D\}$ . As a polynomial function,  $g$  vanishes at  $\lambda$  if and only if  $\lambda$  vanishes at some  $x_i$ . Several special cases deserve particular attention:

- (i) Since we want everything to commute well with specialisations, we must allow the zero polynomial  $0 \in A[X^*]_D$ . It always splits as  $0 \cdot \prod_{i < D} x_i$ , where  $x_i$  are arbitrary (and does not code any set).
- (ii) When  $D = 0$ , every  $\alpha \in A[X^*]_0 = A$  splits in a unique fashion, and (except when  $\alpha = 0$ ) codes the empty set.

Before turning to Chow forms and resultants, which are very special examples of such splitting polynomials, let us consider the general case.

**Lemma 2.4.** *Let  $A$  be an integral domain, and let  $f \in A[X_0, \dots, X_{D-1}]$  be homogeneous of degree  $d$  in each  $X_j = (X_{j,0}, \dots, X_{j,m})$ , and assume that  $g \in A[X^*]_D$  splits over some field  $L \supseteq \text{Frac}(A)$ , say as  $\alpha \prod_{i < D} x_i$ .*

- (i) *The field  $L$  can always be taken to be an algebraic extension of  $\text{Frac}(A)$ .*
- (ii) *If  $w$  is any valuation of  $L$  such that  $\mathcal{O}_w \supseteq A$ , then  $g$  splits in  $\mathcal{O}_w[X^*]$ .*
- (iii) *Any ring epimorphism  $\varphi: A \rightarrow \overline{A}$ , with  $\overline{A}$  an integral domain can be extended to  $\psi: B \rightarrow \overline{B} \supseteq \overline{A}$ , where  $A \subseteq B \subseteq L$  and  $g$  splits in  $B[X^*]$ . In other words, any specialisation of  $g$  can be extended to a specialisation of its linear factors.*
- (iv) *The value  $\beta = \alpha^d f(x_0, \dots, x_{D-1}) \in L$  depends only on the order of the geometric points  $[x_0], \dots, [x_{D-1}]$ , and is integral over  $A$ .*

*Proof.* Items (i) and (ii) are easy. Item (iii) is merely the fact that for any prime ideal  $P$  of  $A$  there exists a valuation  $w$  on  $L$  such that  $P = A \cap \mathfrak{m}_w$ , so take  $B = \mathcal{O}_w$  and  $\overline{B}$  the residue field. The first part of (iv) is easy. It follows that if  $w$  is any valuation on  $L$  such that  $\mathcal{O}_w \supseteq A$ , then  $\beta \in \mathcal{O}_w$ , so  $\beta$  is integral over  $A$ . ■

**Definition 2.5.** Let  $A$  be an integral domain. Let  $f \in A[X]_d$  and  $g \in A[X^*]_D$ , and assume that  $g$  splits as  $\alpha \prod_{i < D} x_i$ . Then we define

$$f \wedge g = \alpha^d \prod f(x_i),$$

following the convention that  $0^0 = 1$ .

In particular, if  $D = 0$  then  $f \wedge g = g^d$ , and if  $d = 0$  then  $f \wedge g = f^D$ . When  $d = D = 0$  we have  $f \wedge g = 1$ . With our convention that  $0^0 = 1$  this includes the case where  $f$  and/or  $g$  (of degree zero) vanish.

*Question 2.6.* Assume  $A$  is a unique factorisation domain and both  $f$  and  $g$  are irreducible in  $A[X]$  and in  $A[X^*]$ , respectively. Is  $f \wedge g$  irreducible in  $A$  (or at least a unit times a power of an irreducible)?

**Lemma 2.7.** *Let  $A$  be an integrally closed integral domain. Let  $f \in A[X]_d$  and  $g \in A[X^*]_D$  be as in [Definition 2.5](#). Then*

(i) *When defined, we have*

$$(f_1 f_2) \wedge g = (f_1 \wedge g)(f_2 \wedge g), \quad f \wedge (g_1 g_2) = (f \wedge g_1)(f \wedge g_2).$$

(ii) *If  $f$  and  $h$  are of the same degree,  $g$  splits as  $\alpha \prod x_i$ , and  $h(x_i) = 0$  for all  $i$ , then*

$$(f + h) \wedge g = f \wedge g.$$

(iii) *The value  $f \wedge g$  is well defined and belongs to  $A$ .*

(iv) *Assume that  $A = B[Y]$ , and that  $f$  and  $g$  are homogeneous in  $Y$ , say of degrees  $\ell$  and  $k$ , respectively. Then  $f \wedge g$  is homogeneous in  $Y$  of degree  $\ell D + k d$ .*

(v) *The wedge operation commutes with specialisation. In other words, if  $\bar{A}$  is another integral domain and  $\bar{\cdot}: A \rightarrow \bar{A}$  is a ring homomorphism, which extends in the obvious way to polynomial rings over  $A$ , then*

$$\bar{f} \wedge \bar{g} = \overline{f \wedge g} \in \bar{A}.$$

*Proof.* Items (i) and (ii) are clear. For (iii), let  $K = \text{Frac}(A)$  and  $L = K^a$ , so  $f \wedge g \in L$ .

Assume first (in positive characteristic) that  $A = K$  is separably closed. Applying an invertible linear transformation to  $X^*$  (and its inverse to  $X$ ), we may assume that the coefficient of  $(X_n^*)^D$  in  $g$  does not vanish. We may therefore assume that it is one, and in fact that the coefficient of  $X_n^*$  is one in each  $x_i$ . We may also assume that  $g$  is irreducible in  $K[X^*]$ . Let  $M = K(X_0^*, \dots, X_{n-1}^0)$ . Then  $g$  is also an irreducible unital polynomial in  $M[X_n^*]$ , with roots  $X_n^* - x_i$  in  $ML \subseteq M^a$ . Since  $L/K$  is purely inseparable algebraic extension, any  $\varphi \in \text{Aut}(M^a/M)$  must be the identity on  $ML$ . It follows that all the  $x_i$  are equal and  $g$  is of the form  $x^{p^f}$ , from which one calculates that  $f \wedge g \in K$ .

In the general case,  $f \wedge g$  is separable over  $K$  by the previous argument. Since  $f \wedge g$  is fixed by the Galois group, it belongs to  $K$ . Since  $f \wedge g$  is integral over  $A$  by [Lemma 2.4\(iv\)](#), it belongs to  $A$ .

Item (iv) is easy.

Item (v) follows directly from [Lemma 2.4\(iii\)](#). ■

**2.3. Chow forms and resultants.** Let us recall the notion of a Chow form, and more generally, of a resultant form. The fundamental notion is that of a resultant form for a projective variety (here a *variety* is always irreducible). While it is standard to extend the definition to the (unique) resultant form of a positive projective cycle, for our purposes it will be preferable to define a (non-unique) resultant form associated with an algebraic set. We even allow zero as a resultant form, associated with any algebraic set whose dimension is too big (this excludes zero as a resultant form in dimension  $n$ , since there are no sets of dimension  $n + 1$ , but this borderline case will not bother us).

**Notation 2.8.** Throughout we let  $\mathbf{D} = \mathbf{N} \setminus \{0\}$ .

**Definition 2.9.** Let  $\ell \leq n$  and  $d \in \mathbf{D}^{\ell+1}$ . For  $i \leq \ell$  let  $T_i^* = (T_{i,\alpha}^* : |\alpha| = d_i)$  be unknowns representing the coefficients of a homogeneous polynomial of degree  $d_i$ . Let  $K$  be an algebraically closed field.

(i) Let  $W \subseteq \mathbf{P}^n$  be a non-empty algebraic set defined over  $K$ . We say that a polynomial  $\mathfrak{R} \in K[T_0^*, \dots, T_\ell^*]$  is a *resultant form associated with  $W$*  in dimension  $\ell$  and degrees  $d$  if for every family of polynomials  $f \in K[X]^{\ell+1}$ , where  $f_i \in K[X]_{d_i}$ , we have

$$\mathfrak{R}(f) = 0 \quad \iff \quad W \cap V(f) \neq \emptyset. \tag{7}$$

Notice that this determines the family of prime factors of  $\mathfrak{R}$ , up to multiplicity.

(ii) Let  $W \subseteq \mathbf{P}^n$  be a variety of dimension  $\ell$ , defined over  $K$ . An irreducible resultant form in dimension  $\ell$  and degrees  $d$  associated with  $W$ , which is unique up to a scalar factor, is called *the resultant form of  $W$  in degrees  $d$* , denoted  $\mathfrak{R}_{W,d}$ .

(iii) When  $d = (1, 1, \dots, 1)$  we write  $\mathfrak{C}(X_0^*, \dots, X_\ell^*)$  instead of  $\mathfrak{R}(T_0^*, \dots, T_\ell^*)$ , calling the *Chow form* rather than resultant form.

**Fact 2.10.** *Let  $W \subseteq \mathbf{P}^n$  be an algebraic set of dimension  $\ell$ . Let  $p \in \mathbf{P}^n$ , and for  $i \leq \ell$  let  $f_i$  be homogeneous polynomials whose coefficients are generic modulo the constraint that  $p \in V(f)$ . Then  $W \cap V(f) \subseteq \{p\}$ .*

*Proof.* For  $i \leq \ell$  and irreducible component  $U$  of  $W_i = W \cap V(f_0, \dots, f_{i-1})$ , if  $U \neq \{p\}$ , then there exists a polynomial vanishing at  $p$  and not at a generic point of  $U$ . Therefore  $f_i$  is such. It follows by induction that  $\dim W_\ell = 0$  and so  $W_{\ell+1} \subseteq \{p\}$ .  $\blacksquare$

**Fact 2.11.** Let  $\ell \leq n$  and  $d \in \mathbf{D}^{\ell+1}$ .

- (i) The resultant form in degrees  $d$  exists for any variety  $W \subseteq \mathbf{P}^n$  of dimension  $\ell$ .
- (ii) More generally, let  $W \subseteq \mathbf{P}^n$  be an algebraic set defined over  $K$  and  $\mathfrak{R} \in K[T_0^*, \dots, T_\ell^*]$ . Then  $\mathfrak{R}$  is a resultant form in dimension  $\ell$  and degrees  $d$ , associated with  $W$ , if and only if
  - either  $\dim W > \ell$  and  $\mathfrak{R} = 0$ ,
  - or  $W$  is of pure dimension  $\ell$ , and

$$\mathfrak{R} = \prod_k \mathfrak{R}_{U_k, d}^{m_k}$$

where  $(U_k)$  are the irreducible components of  $W$  and  $m_k \geq 1$ . In this case  $\mathfrak{R}$  determines  $W$ .

(In the latter case, one may also say that  $\mathfrak{R}$  is the resultant form of the positive projective cycle  $\sum m_k U_k$ .)

- (iii) A resultant form  $\mathfrak{R}(T_0^*, \dots, T_\ell^*)$  is homogeneous in each  $T_i^*$ .
- (iv) If  $d_0 = d_1$  then  $\mathfrak{R}(T_0^*, T_1^*, \dots) = \pm \mathfrak{R}(T_1^*, T_0^*, \dots)$ , and similarly for any other pair of arguments with  $d_i = d_j$ . This is in particular true of the Chow form, where all degrees are equal.

*Proof.* For (i), say that  $W$  is defined over  $K$ . Let  $L \supseteq K$  be some very rich field, and let  $[\hat{x}] \in W(L)$  be a generic point of  $W$  with  $\hat{x}_i = 1$  for some  $i$ , so  $\text{trdeg}_K K(\hat{x}) = \ell$ . For  $i \leq \ell$  choose  $\hat{f}_i = \sum r_{i,\alpha} X^\alpha \in L[X]_{d_i}$  with coefficient which are generic over  $K(\hat{x})$  modulo the constraint that  $\hat{f}_i(\hat{x}) = 0$ . Let  $N = \sum_{i \leq \ell} \binom{d_i+n}{n}$  denote the total number of coefficients  $r_{i,\alpha}$ . By **Fact 2.10**,  $\hat{x}$  is algebraic over  $K(r)$ , so

$$\text{trdeg}_K K(r) = \text{trdeg}_K K(\hat{x}, r) = \text{trdeg}_K K(\hat{x}) + \text{trdeg}_{K(\hat{x})} K(\hat{x}, r) = \ell + \sum_{i \leq \ell} \left( \binom{d_i+n}{n} - 1 \right) = N - 1.$$

Therefore the  $r$  are related by a single irreducible polynomial  $\mathfrak{R}(T_0^*, \dots, T_\ell^*)$ .

Now let  $f$  be any polynomials of the appropriate degrees. Assume that  $\mathfrak{R}(f) = 0$ , so  $f$  is a specialisation over  $K$  of  $\hat{f}$ . Letting  $x$  be the corresponding specialisation of  $\hat{x}$  we have  $[x] \in W \cap V(f)$ . Conversely, assume that  $[x] \in W \cap V(f)$ , so  $x$  specialises  $\hat{x}$  over  $K$ . Then  $x, f$  specialises  $\hat{x}, g$  over  $K$  for some family  $g$  of polynomials, such that we still have  $\hat{x} \in V(g)$ . But then  $g$  is a specialisation of  $\hat{f}$  over  $K(\hat{x})$ . Composing,  $f$  specialises  $\hat{f}$  and so  $\mathfrak{R}(f) = 0$ . Therefore,  $\mathfrak{R}$  satisfies (7) and is the desired resultant form.

For (ii), right to left is evident. Assume therefore that  $\mathfrak{R}$  is a resultant form associated with  $W$ . If  $\mathfrak{R} = 0$  then  $\dim W > \ell$ , by **Fact 2.10**, so assume that  $\mathfrak{R} \neq 0$ . Let  $\mathfrak{R}'$  be a prime factor of  $\mathfrak{R}$  (over an algebraically closed field) and let  $f = (f_0, \dots, f_\ell)$  be a generic root of  $\mathfrak{R}'$ . This implies, first, that for any  $\ell' < \ell$  there exists a proper sub-family of  $f$  whose coefficients are entirely free over  $K$ , and second, that  $\mathfrak{R}(f) = 0$ , so  $U_k \cap V(f) \neq \emptyset$  for some  $k$ . If  $\dim U_k < \ell$  then every sub-family of  $f$  of size  $\dim U_k$  must satisfy the corresponding resultant form of  $U_k$ , contradicting the above. Therefore  $\dim U_k = \ell$ , and consequently  $\mathfrak{R}' = \mathfrak{R}_{U_k, d}$  (up to some scalar factor). We conclude that  $\mathfrak{R}$  has the stated form, where  $U_k$  varies over the irreducible components of dimension  $\ell$ . By **Fact 2.10**,  $W$  can have no additional irreducible components.

Homogeneity follows from (7).

For (iv) we may assume that  $\mathfrak{R} = \mathfrak{R}_{W, d}$  for some variety  $W$ . Exchanging any two arguments corresponding to the polynomials of the same degree yields another resultant form for  $W$ , so it multiplies  $\mathfrak{R}_{W, d}$  by some  $\alpha \neq 0$ . Doing this a second time we find  $\mathfrak{R}_{W, d}$  again, so  $\alpha = \pm 1$ .  $\blacksquare$

It follows that for a Chow form  $\mathfrak{C}$ , the degree  $\deg_{X_i^*} \mathfrak{C}$  does not depend on  $i$ , and will simply be denoted  $\deg \mathfrak{C}$ . If  $W \subseteq \mathbf{P}^n$  is a variety, then  $\deg W = \deg \mathfrak{C}_W$  is the degree of  $W$  as embedded in  $\mathbf{P}^n$ .

*Example 2.12.* The Chow form of  $\mathbf{P}^n$  is  $\det (X_{i,j}^*)_{i,j \leq n}$  (i.e., the volume form  $X_0^* \wedge \dots \wedge X_n^*$ ), and the Chow form of a single point  $[x]$  is  $x$  (both of degree 1). The resultant  $\mathfrak{R}_{\mathbf{P}^1}(f, g)$  of two polynomials in  $\mathbf{P}^1$  can be expressed in the familiar determinant form.

**Lemma 2.13.** Let  $\mathfrak{C} \in K[X_0^*, \dots, X_\ell^*]$  be a Chow form in dimension  $\ell$  associated with an algebraic set  $W$ , and let  $\lambda$  be a family of  $\ell$  linear forms over  $K$ . Then  $\mathfrak{C}(\lambda, X^*)$  is a Chow form in dimension 0, associated with  $W \cap V(\lambda)$ . In particular,  $\mathfrak{C}(\lambda, X^*)$  splits, and

- either  $\mathfrak{C}(\lambda, X^*)$  vanishes, and  $\dim(W \cap V(\lambda)) > 0$ ,
- or  $\mathfrak{C}(\lambda, X^*) = \prod_{k < D} x_k$ , and  $W \cap V(\lambda) = \{[x_k] : k < D\}$  (possibly with repetitions).

If  $L = K(X_0^*, \dots, X_{\ell-1}^*)$ , then  $\mathfrak{C} \in L[X_\ell^*]$  splits over  $L^a$ .

*Proof.* We know that  $\mathfrak{C}(\lambda, \mu) = 0$  if and only if  $W \cap V(\lambda, \mu) \neq \emptyset$ , which means exactly that  $\mathfrak{C}(\lambda, X^*)$  is a Chow form in dimension 0 associated with  $W \cap V(\lambda)$ . The dichotomy is the just a special case of [Fact 2.11\(ii\)](#).

In particular,  $\mathfrak{C} = \mathfrak{C}(\hat{\lambda}, X_\ell^*)$  where  $\hat{\lambda}_i = \sum X_{i,j}^* X_j$ , so  $\mathfrak{C}$  splits as a special case of the above.  $\blacksquare$

**Definition 2.14.** Let  $\mathfrak{C}(X_0^*, \dots, X_\ell^*)$  be a Chow form. As above, let  $L = K(X_0^*, \dots, X_{\ell-1}^*)$  and identify  $X_\ell^*$  with  $X^*$ , so  $\mathfrak{C} \in L[X^*]$  splits over  $L^a$ . Let also  $f \in K[X]_m$ , where  $m > 0$ . Then, in accordance with [Definition 2.5](#), we define

$$f \wedge \mathfrak{C} = \prod_{k < D} f(x_k), \quad \text{where} \quad \mathfrak{C} = \prod_{k < D} x_k.$$

In particular we have  $f \wedge 0 = 0 \wedge \mathfrak{C} = 0$ . As we shall see promptly,  $f \wedge \mathfrak{C} \in K[X_0^*, \dots, X_{\ell-1}^*]$  is again a Chow form (in dimension  $\ell - 1$ ), so we may iterate the operation and define, for  $f = (f_i : i < k)$ :

$$f \wedge \mathfrak{C} = f_0 \wedge (f_1 \wedge \dots (f_{k-1} \wedge \mathfrak{C}) \dots).$$

**Proposition 2.15.** Let  $A$  be an integrally closed integral domain. Let  $\mathfrak{C} \in A[X_0^*, \dots, X_\ell^*]$  be a Chow form in dimension  $\ell$ , associated with an algebraic set  $W$ .

- (i) Let also  $k \leq \ell + 1$  and  $f = (f_0, \dots, f_{k-1})$  be homogeneous polynomials over  $A$ . Then the iterated wedge operation  $f \wedge \mathfrak{C} \in A[X_0^*, \dots, X_{\ell-k}^*]$  is well defined (i.e., all intermediate steps yield Chow forms), and is a Chow form in dimension  $\ell - k$  associated with  $W \cap V(f)$ .
- (ii) Fix degrees  $d \in \mathbf{D}^k$  and for  $i < k$  let

$$\hat{f}_i = \sum T_{i,\alpha}^* X^\alpha$$

be a polynomial of degree  $d_i$  with formal unknown coefficients. Then

$$\hat{f} \wedge \mathfrak{C} \in A[X_0^*, \dots, X_{\ell-k}^*, T_0^*, \dots, T_{k-1}^*]$$

is a resultant form in dimension  $\ell$  associated with  $W$ , related with  $f \wedge \mathfrak{C}$  of the previous item by

$$(\hat{f} \wedge \mathfrak{C})(\lambda, f) = (f \wedge \mathfrak{C})(\lambda). \quad (8)$$

If  $\mathfrak{C} = \mathfrak{C}_W$  is the Chow form of a variety  $W$  of dimension  $\ell$ , then  $\hat{f} \wedge \mathfrak{C} = \mathfrak{R}_{W, (1, \dots, 1, d)}$  is the resultant form (in the appropriate degrees) of  $W$ .

- (iii) If  $g$  is a permutation of  $f$  then  $f \wedge \mathfrak{C} = \pm g \wedge \mathfrak{C}$ .

*Proof.* For (i) we only need to consider the case  $k = 1$ . Since  $A$  is integrally closed, so is  $A[X_0^*, \dots, X_{\ell-1}^*]$ , so  $f \wedge \mathfrak{C} \in A[X_0^*, \dots, X_{\ell-1}^*]$  by [Lemma 2.7](#). Let  $\lambda$  be a family of  $\ell$  linear forms. Both  $\mathfrak{C}$  and  $\mathfrak{C}(\lambda, X^*)$  are Chow forms (in dimensions  $\ell$  and 0, respectively), and since the wedge operation commutes with specialisation, we have  $(f \wedge \mathfrak{C})(\lambda) = f \wedge \mathfrak{C}(\lambda, X^*)$ . By [Lemma 2.13](#), we have  $f \wedge \mathfrak{C}(\lambda, X^*) = 0$  if and only if  $W \cap V(\lambda, f) \neq \emptyset$ . Thus  $f \wedge \mathfrak{C}$  is a Chow form associated with  $W \cap V(f)$ .

For (ii), observe first that (8) is merely the fact that wedge commutes with specialisation. This, together with (i), implies that  $\hat{f} \wedge \mathfrak{C}$  is indeed a resultant associated with  $W$ . Assume now that  $\mathfrak{C} = \mathfrak{C}_W$  for a variety  $W$ . By adding to  $\hat{f}$  formal linear forms  $\sum X_{i,j}^* X_j$  for  $i \leq \ell - k$ , we may assume that  $k = \ell$ . Thus  $\hat{f} \wedge \mathfrak{C}_W$  is a resultant form associated with  $W$ , so  $\hat{f} \wedge \mathfrak{C}_W = \mathfrak{R}_{W, d}^m$  for some  $m$ . Consider formal linear forms  $\lambda_{i,s} = \sum X_{i,s,j}^* X_j$  for  $i \leq \ell$  and  $s < d_i$ , and let  $g = \prod \lambda_{i,s}$ . On the one hand, we have

$$(\hat{f} \wedge \mathfrak{C}_W)(g) = g \wedge \mathfrak{C}_W = \prod \{\mathfrak{C}_W(\lambda_{0,s_0}, \dots, \lambda_{\ell,s_\ell}) : s_i < d_i\}.$$

On the other hand, for any choice of  $s_i$  we have

$$\mathfrak{C}_W(\lambda_{0,s_0}, \dots, \lambda_{\ell,s_\ell}) \mid \mathfrak{R}_{W, d}(g).$$

Thus necessarily  $m = 1$ .

For (iii) we may assume that  $\mathfrak{C} = \mathfrak{C}_W$  is the Chow form of some variety, and that  $f = \hat{f}$  are polynomials with formal unknown coefficients. Since the resultant form is unique up to a scalar factor, it follows from  $\hat{f} \wedge \mathfrak{C} = \mathfrak{R}_{W, d}$  that  $f \wedge \mathfrak{C} = \alpha \cdot g \wedge \mathfrak{C}$  for some  $\alpha \in K^\times$ . In order to obtain  $\alpha = \pm 1$ , specialise  $\hat{f}$  to appropriate powers of linear forms with formal unknown coefficients.  $\blacksquare$

Notice that [Proposition 2.15\(iii\)](#) remains valid if some of the polynomials in  $f$  are constant. Indeed, if  $d_i = 0$ , then  $f \wedge \mathfrak{C} = f_i^D$ , where  $D = \deg \mathfrak{C} \prod_{j \neq i} d_j$ , and this is invariant under permutations. In particular, if  $d_i = d_j = 0$  for  $i \neq j$  then  $f \wedge \mathfrak{C} = 1$ .



**Notation 2.16.** When  $\mathfrak{C} = \mathfrak{C}_{\mathbf{P}^n}$ , we allow ourselves to omit it from the notation:

$$f_0 \wedge \dots \wedge f_{k-1} = f_0 \wedge \dots \wedge f_{k-1} \wedge \mathfrak{C}_{\mathbf{P}^n}.$$

For a family of polynomials  $F = (f_i)_{i < k}$  we shall also write

$$F^\wedge = f_0 \wedge \dots \wedge f_{k-1}.$$

We observe that either  $\dim V(F) = n - k$  and  $F^\wedge$  is a Chow form for  $V(F)$ , or  $\dim V(F) > n - k$  and  $F^\wedge = 0$ . Also, any permutation of  $F$  can, at most, change the sign of  $F^\wedge$ . When all the  $f_i$  are linear, applying a permutation  $\sigma$  multiplies  $F^\wedge$  by  $\text{sgn}(\sigma)$ . So, considering the special case where each  $f_i$  is a product of linear forms, we conclude that applying a permutation  $\sigma$  to  $F$  multiplies  $F^\wedge$  by  $\text{sgn}(\sigma) \prod \deg f_i = \text{sgn} \deg F^\wedge$ .

**Proposition 2.17.** *Let  $K$  be algebraically closed,  $W \subseteq \mathbf{P}^n$  a variety of dimension  $\ell$ . Let  $d \in \mathbf{D}^\ell$  and  $D = \deg W \prod d_i$ . Finally, let  $\mathfrak{R}(T_0^*, \dots, T_{\ell-1}^*, X^*) = \mathfrak{R}(T^*, X^*)$  be the resultant of  $W$  in degrees  $(d, 1)$ , and let  $L = K(T^*)$ . Then  $\mathfrak{R} \in L[X^*]$  splits over  $L^a$  as  $\prod_{k < D} x_k$ , and the geometric points  $[x_k]$  are all distinct and conjugate over  $L$ . Moreover, none of the coordinates of  $x_k$  vanishes, and for any  $i < j \leq n$  the ratio  $x_{k,i}/x_{k,j}$  is distinct for the different  $x_k$ .*

*Proof.* Notice that we may assume that  $K$  is infinite, and that if we apply any linear change of coordinates with coefficients in  $K$  leaves us with the same situation (namely, a resultant applied to polynomials with algebraically independent coefficients), so  $(*)$  anything which would hold after some change of coordinates already holds.

It follows from **Proposition 2.15** that  $\mathfrak{R} = \hat{f} \wedge \mathfrak{C}_W$  (for  $\ell$  polynomials  $\hat{f}$  with unknown coefficients) splits, and  $\deg_{X^*} \mathfrak{R} = D$  by **Lemma 2.7(iv)**. By  $(*)$ , none of the coordinates of the points  $x_k$  can vanish. Let  $Y = X_n^*$ , so  $Y^D$  occurs in  $\mathfrak{R}$  with a non-zero coefficient  $\alpha \in L$ . Let  $M = L(X_0^*, \dots, X_{n-1}^*)$ , so  $\mathfrak{C} \in M[Y]$  can be written as  $\alpha Y^D + \dots = \alpha \prod_{k < D} (Y - \beta_k)$ , with  $\beta_k \in M^a$ . Then, up to a permutation, we have  $[x_k] = [Y - \beta_k]$ , i.e.,  $\beta_k = \sum_{i < n} \frac{-x_i}{x_n} X_i^*$ . Since  $\mathfrak{C}$  is irreducible over  $K$ , it is also irreducible over  $M$ , so all the  $\beta_k$  are conjugate over  $M$ , and therefore the geometric points  $[x_k]$  are conjugate over  $L$ .

In order to show that the points are distinct, assume first that  $d = (1, \dots, 1)$ , so  $\mathfrak{R} = \mathfrak{C}_W$ . If some  $[x_k]$  appears with multiplicity then necessarily  $K$  has positive characteristic  $p$  and, up to a permutation,  $\mathfrak{C}_W = \alpha \prod_{k < \frac{D}{p}} (Y - \beta_k)^p$ . It follows that  $X_0^*, \dots, X_n^*$  occur in  $\mathfrak{C}_W$  as powers of  $p$ , and therefore all the unknowns do, so  $\mathfrak{C}_W$  is reducible, a contradiction.

For the general case, for each  $j < \ell$  and  $m < d_j$  let  $\lambda_{j,m} = \sum_i X_{j,m,i}^* X_i$  be a linear form, and let  $\hat{g}_j = \prod_{m < d_j} \lambda_{j,m}$ . Then  $\mathfrak{R}(\hat{g}, X^*) = \hat{g} \wedge \mathfrak{R} = \prod_{m_0, \dots, m_{\ell-1}} \mathfrak{C}_W(X_{0,m_0}^*, \dots, X_{\ell-1, m_{\ell-1}}^*, X^*)$ , and each of the factors, viewed as a polynomial in  $X^*$ , splits as  $\deg W$  distinct points. Since the coefficients are generic, we obtain  $\deg W \cdot \prod d_j$  distinct points. Since this is a specialisation of  $\mathfrak{R}$ , it, too, must split as distinct points.

One last application of  $(*)$  shows that all the ratios must be distinct. ■

**Lemma 2.18.** *Let  $K$  be a field and  $W \subseteq \mathbf{P}^n$  a projective variety defined over  $K$ , of dimension  $\ell$ . Let  $d \in \mathbf{D}^{\ell+1}$ , and for  $i \leq \ell$ , let also  $f_i = \sum T_{i,\alpha}^* X^\alpha \in K(T^*)[X]_{d_i}$  be a formal homogeneous polynomial of degree  $d_i$ . Let  $\mathfrak{C} = \mathfrak{C}_W$  and  $\mathfrak{R} = \mathfrak{R}_{W,d} = f \wedge \mathfrak{C} \in K[T^*]$ . Let  $D = \prod d_i$  and let  $w$  be any extension of the  $\mathfrak{R}$ -adic valuation from  $K(T^*)$  to  $L = K(T^*)^a$ .*

*For  $i \leq n$  let  $D_i = D_i$ , let  $K_i = K(T_0^*, \dots, T_{i-1}^*, T_{i+1}^*, \dots, T_n^*)$  and let  $L_i = K_i^a$ , so  $(f_{\neq i}) \wedge \mathfrak{C} \in K_i[X^*]$  factors in  $L_i[X^*]$  as  $\alpha_i \prod_{k < D_i} x_{i,k}$ , with  $\alpha_i \in K_i$  and  $x_{i,k} = (\dots, 1)$ .*

(i) *We have  $L_i \subseteq \mathcal{O}_w$ , and there exists  $k_i \leq D_i$  such that*

$$w(f_i(x_{i,k})) = \begin{cases} 1 & k = k_i \\ 0 & k \neq k_i. \end{cases}$$

(ii) *We have  $w(x_{i,k_i} - x_{j,k_j}) \geq 1$  for all  $i, j \leq n$ .*

*Proof.* The restriction of  $w$  to  $K_i$ , and therefore to  $L_i$ , is trivial, so  $L_i \subseteq \mathcal{O}_w$ . The polynomial  $P = f_i(x_{i,0}) \in L_i[T_i^*]$  is irreducible, and the  $P$ -adic valuation on  $L_i(T_i^*)$  restricts to the  $\mathfrak{R}$ -adic valuation on  $K(T^*)$ . It follows that, up to an automorphism of  $L/K(T^*)$ , the valuation  $w$  extends the  $P$ -adic valuation on  $K_i(T_i^*)$ . The first assertion follows.

It follows that  $\overline{x_{0,k_0}} = \dots = \overline{x_{n,k_n}}$  is the unique common zero of the  $\overline{f_i}$ , where  $\overline{\cdot}$  is the residue map.

Let  $\delta = x_{0,k_0,0} - x_{1,k_1,0}$ , so  $w(\delta) > 0$ . Then  $\delta$  is algebraic over  $K_i(T_i^*)$ , and if  $\delta' \neq \delta$  is some conjugate, then it is of the form  $x_{0,k_0,0} - x_{1,k',0}$  for  $k' \neq k_1$ . By the moreover part of **Proposition 2.17** we have  $w(x_{1,k_1,0} - x_{1,k',0}) = 0$ , so  $w(\delta') = 0$  as well. If  $\Delta = \mathcal{N}(\delta/K_i(T_i^*))$ , then  $w(\Delta) = w(\delta) > 0$ , so necessarily  $w(\Delta) \geq 1$  (since we observed that the value group of  $w|_{K_i(T_i^*)}$  is  $\mathbf{Z}$ ). We conclude that  $w(\delta) \geq 1$ , and by the same reasoning,  $w(x_{i,k_i} - x_{j,k_j}) \geq 1$  for all  $i, j \leq n$ . ■

## 3. AN ASYMPTOTIC VANDERMONDE DETERMINANT RELATION FOR HYPERSURFACES

Our aim here is to extend [Theorem 1.4](#) (and [Corollary 1.5](#)) to intersections of hypersurfaces. Given a family of homogeneous polynomials  $F = (f_i : i < k)$ , there is little question as to the analogue of the right hand side, namely, some power of the product of all resultants  $G^\wedge$  where  $G \in \binom{F}{n+1}$ . The main obstacle is that we are missing points for a the large square matrix of the left hand side. More precisely, if  $m = \deg F = \sum \deg f_i$ , then the cardinal of the set up all intersection points  $\bigcup_{G \in \binom{F}{n}} [G^\wedge]$  will be smaller than  $\binom{m}{n}$  (unless all  $f_i$  are linear).

Our solution is to add new “parasitical” points in a *somewhat* canonical manner. We choose an algebraically generic direction for formal derivation (which is canonical), and use it to obtain the missing points. We then need to make some arbitrary choices, namely, partition these new points into  $n!$  smaller groups which can be used to complete the intersection points into good families of size  $\binom{m}{n}$ .

In order to see how to get all necessary points (intersection and parasitical), let us consider first how we would get them when all polynomials are linear, so let  $\Lambda = (\lambda_i : i < m)$  be a family of linear forms and  $f = \prod \Lambda = \prod_i \lambda_i$ . In characteristic zero,  $\zeta \in \mathbf{P}^n$  is an intersection point of  $k$  forms in the family if and only if  $f$  and all its derivatives (in some generic direction), up to order  $k - 1$ , vanish at  $\zeta$ . In positive characteristic, the usual notion of formal derivative can be a little problematic, and is better replaced with the following finer one.

**Definition 3.1.** Consider a polynomial in several unknowns  $f \in A[X]$ . Add a new set of unknowns (of the same number)  $dX$ , and decompose

$$f(X + dX) = \sum_k \partial_k f,$$

where  $\partial_k f$  is homogeneous in  $dX$  of degree  $k$ . We may specialise  $dX$  to any tuple in  $A$ , obtaining a family of operations  $\partial_k : A[X] \rightarrow A[X]$ , or, if we wish to keep  $dX$  generic,  $\partial_k : A[X, dX] \rightarrow A[X, dX]$ , which are called *formal Hasse derivatives*.

When  $A$  is a field of characteristic zero, we also have

$$\partial_k = \frac{d^k}{k!}.$$

The Hasse derivatives satisfy

$$\begin{aligned} \partial_k(f + g) &= \partial_k f + \partial_k g, & \partial_k(fg) &= \sum_{0 \leq \ell \leq k} (\partial_\ell f)(\partial_{k-\ell} g), & \partial_k \partial_\ell &= \binom{k+\ell}{k} \partial_{k+\ell}, \\ \partial_0 &= \text{id}, & \partial_1 X_i &= dX_i, & k > \deg f &\implies \partial_k f = 0, \end{aligned}$$

and are moreover determined by these axioms (the axiom for  $\partial_k \partial_\ell$  is superfluous in our context).

**Convention 3.2.** Throughout,  $A$  denotes some integrally closed integral domain, and  $dX$  a tuple of new unknowns, so the Hasse derivatives are operations  $A[X, dX] \rightarrow A[X, dX]$  (we notice that  $A[dX]$  is again an integrally closed integral domain).

We let  $K = \text{Frac}(A[dX])$  and  $L = K^a$  be the algebraic closure, so essentially everything will happen in  $L$ . We also let  $B$  denote the integral closure of  $A[dX]$  inside  $L$ , i.e., the absolute integral closure of  $A[dX]$ . We shall use the notation  $a \preceq b$  to denote divisibility in  $B$  (i.e., both  $a$  and  $b/a$  are integral over  $A[dX]$ ).

All polynomials are homogeneous.

**Notation 3.3.** For a single polynomial  $f$  and  $k \leq n + 1$  we define

$$f^{\partial k} = f \wedge \partial_1 f \wedge \dots \wedge \partial_{k-1} f.$$

In particular, for  $f \in A[X]_d$  with  $d \geq n$  we have  $f^{\partial n} \in A[dX, X^*]$  and  $f^{\partial n+1} \in A[dX]$ .

Notice that there can be no ambiguity of sign for  $f^{\partial k}$ : if  $k \leq 1$  then there is no question of order, and for  $k \geq 2$  the total degree is even.

*Remark 3.4.* Let  $f \in A[X]_d$ . If  $k = d + 1$  then  $f^{\partial k}$  is a scalar:

$$f^{\partial d+1} = f^{\partial d} \wedge \partial_d f = (\partial_d f)^{\deg f^{\partial d}} = (\partial_d f)^{d!}.$$

When  $k > d + 1$ , our definition of  $f^{\partial k}$  may seem nonsensical, since  $\partial_\ell f$  is “homogeneous of negative degree” for  $\ell > d$ . Still, one may still consider  $\partial_{d+1} f \wedge \dots \wedge \partial_{k-1} f$  to be of degree  $(-1)^{k-d-1} (k-d-1)!$ , so

$$f^{\partial k} = (\partial_d f)^{d!} \deg(\partial_{d+1} f \wedge \dots \wedge \partial_{k-1} f) = (\partial_d f)^{(-1)^{k-d-1} (k-d-1)! d!}.$$

**Lemma 3.5.** *If  $f^{\partial k} \neq 0$  for any  $2 \leq k \leq \min(n+1, \deg f)$  then  $f$  factors over any field extension as a product of distinct irreducible factors.*

*Proof.* If  $f = g^2h$  then  $g \mid \partial_1 f$  and so  $f^{\partial k} = 0$ . ■

**Lemma 3.6.** *For any two polynomials and  $k \leq n+1$ :*

$$(gh)^{\partial k} = \pm \prod_{0 \leq \ell \leq k} (g^{\partial \ell} \wedge h^{\partial k - \ell})^{\binom{k}{\ell}}.$$

*Proof.* For  $k=0$  there is nothing to prove ( $\mathfrak{C}_{\mathbb{P}^n} = \mathfrak{C}_{\mathbb{P}^n}$ ). We now proceed by induction:

$$\begin{aligned} (gh)^{\partial k+1} &= (gh)^{\partial k} \wedge \partial_k(gh) \\ &= \left( \pm \prod_{0 \leq \ell \leq k} (g^{\partial \ell} \wedge h^{\partial k - \ell})^{\binom{k}{\ell}} \right) \wedge \left( \sum_{0 \leq j \leq k} (\partial_j g)(\partial_{k-j} h) \right) \\ &= \pm \prod_{0 \leq \ell \leq k} \left( (g^{\partial \ell} \wedge h^{\partial k - \ell})^{\binom{k}{\ell}} \wedge \left( \sum_{0 \leq j \leq k} (\partial_j g)(\partial_{k-j} h) \right) \right) \\ &= \pm \prod_{0 \leq \ell \leq k} \left( (g^{\partial \ell} \wedge h^{\partial k - \ell})^{\binom{k}{\ell}} \wedge ((\partial_\ell g)(\partial_{k-\ell} h)) \right) \\ &= \pm \prod_{0 \leq \ell \leq k} \left( (g^{\partial \ell+1} \wedge h^{\partial k - \ell})^{\binom{k}{\ell}} (g^{\partial \ell} \wedge h^{\partial k+1-\ell})^{\binom{k}{\ell}} \right) \\ &= \pm \prod_{0 \leq \ell \leq k+1} (g^{\partial \ell} \wedge h^{\partial k+1-\ell})^{\binom{k+1}{\ell}}. \end{aligned}$$

Following **Remark 3.4**, this remains valid even for terms of the form  $g^{\partial \ell}$  where  $\ell > \deg g$ , or  $h^{\partial k - \ell}$  where  $k - \ell > \deg h$ . ■

*Question 3.7.* One cannot fail to notice the similarity between **Lemma 3.6** and the binomial formula. Can the former be made an instance of the latter, in a ring  $(\mathcal{R}, \oplus, \odot)$ , where  $\oplus$  is multiplication, and  $\odot$  is some operation based on  $\wedge$ ? In particular, we should only want to identify two polynomials  $f$  and  $g$  if  $f = \pm g$ , and for  $f$  with distinct irreducible factors, we should want its  $k$ th  $\odot$ -power to be  $f^{\partial k}$ .

**Notation 3.8.** It will be convenient to extend **Notation 3.3** (and other notations later on) to a family  $F = (f_i : i < m)$  of polynomials:

$$F^{\partial k} = \left( \prod_{i < m} f_i \right)^{\partial k}.$$

**Lemma 3.9.** *For a family  $F = (f_i : i < m)$  and  $\Omega = (\omega_i : i < m)$  such that  $\sum \Omega \leq n+1$ , we have*

$$F^{\partial k} = \pm \prod_{\sum \Omega = k} \left( \bigwedge_i f_i^{\partial \omega_i} \right)^{\binom{k}{\Omega}},$$

where

$$\binom{k}{\Omega} = \frac{k!}{\Omega!} = \frac{k!}{\prod \omega_i!}.$$

*Proof.* Follows directly from **Lemma 3.6**. Notice that following **Remark 3.4**, this remains valid even if  $k > \deg f_i$  for some  $i$ . Also, if  $\omega_i > \deg f_i$  for more than one  $i$ , then  $\bigwedge_i f_i^{\partial \omega_i} = 1$ . ■

**Definition 3.10.** Let  $f \in A[X]_m$ , where  $m > n$ , be such that  $f^{\partial n+1} \neq 0$ . We know that in this case  $f^{\partial n} \in A[dX, X^*]$  splits (as a polynomial in  $X^*$ ), coding a multi-set  $[f^{\partial n}]$  of cardinal  $\frac{m!}{(m-n)!} = n!N$ , where  $N = \binom{m}{n}$ .

For a subset  $\psi = \{x_i : i < N\} \subseteq [f^{\partial n}]$ , define

$$M_{f,\psi} = \left( \frac{v_{m-n}(x_i)}{\partial_n f(x_i)} : i < N \right),$$

namely the matrix whose  $i$ th column is  $\frac{v_{m-n}(x_i)}{\partial_n f(x_i)}$ . This is a square  $N \times N$  matrix which does not depend on the choice of representatives, and whose determinant only depends on the order of points for sign. We say that  $\psi$  is a *good* subset of  $[f^{\partial n}]$  if  $M_{f,\psi}$  is invertible, and in this case we define

$$\Phi_{f,\psi} = M_{f,\psi}^{-1}.$$

For  $\zeta \in \Psi$  we define  $\varphi_{f,\psi,\zeta} \in K[X]_{m-n}$  to be the unique polynomial such that for all  $[x] \in \psi$ :

$$\varphi_{f,\psi,\zeta}(x) = \begin{cases} \partial_n f(x) & [x] = \zeta, \\ 0 & [x] \neq \zeta. \end{cases}$$

In other words,  $\varphi_{f,\psi,\zeta}$  is the row of  $\Phi_{f,\psi}$  corresponding to  $\zeta$ .

By a *partition* of  $[f^{\partial n}]$  we mean a multi-set  $\Psi$  of subsets, such that each point belongs to as many  $\psi \in \Psi$  as its multiplicity in  $[f^{\partial n}]$ . A partition into  $n!$  good subsets will be called *good*. If  $\Psi$  is a good partition, we define (up to an undetermined sign) the “small” and the “large” associated determinants:

$$\mathfrak{d}_{f,\Psi} = \pm \prod_{\psi \in \Psi} \det \Phi_{f,\psi}, \quad \mathfrak{D}_{f,\Psi} = f^{\partial n+1} / \mathfrak{d}_{f,\Psi} = \pm f^{\partial n+1} \prod_{\psi \in \Psi} \det M_{f,\psi}.$$

We say that  $f$  of degree  $m > n$  is *good* if  $f^{\partial n+1} \neq 0$  and a good partition exists.

We extend the definition to the case  $m = n$ , with one caveat, namely, that even if  $f^{\partial n+1} = (\partial_n f)^{n!} \neq 0$ , it may still happen that  $f^{\partial n} = 0$ . Regardless of  $f^{\partial n}$ , we consider that there exists a unique good partition  $\Psi$  (this is indeed the case when  $f^{\partial n} \neq 0$ ), observing that in any case nothing depends on it:

$$M_{f,\psi} = (\partial_n f)^{-1}, \quad \mathfrak{d}_{f,\Psi} = (\partial_n f)^{-n!}, \quad \mathfrak{D}_{f,\Psi} = 1.$$

If  $F = (f_i : i < m)$  is a family of polynomials and  $f = \prod f_i$ , we have already agreed to use the notation  $F^{\partial k} = f^{\partial k}$ . Extending this convention, we shall say that  $F$  is good if  $f$  is good, write  $M_{F,\psi} = M_{f,\psi}$ ,  $\mathfrak{D}_{F,\Psi} = \mathfrak{D}_{f,\Psi}$ , and so on.

In particular,  $\mathfrak{D}_{f,\Psi} \mathfrak{d}_{f,\Psi} = f^{\partial n+1}$ .

**Lemma 3.11.** *Let  $f \in A[X]_m$ , with  $m \geq n$ .*

- (i) *If  $f$  splits and  $f^{\partial n+1} \neq 0$ , then  $f$  is good.*
- (ii) *If  $\Psi$  is a partition of  $[f^{\partial n}]$ , and one can specialise  $f, \Psi$  into  $\bar{f}, \bar{\Psi}$  which are good, then  $f$  and  $\Psi$  are good.*
- (iii) *If  $f$  specialises to a good polynomial  $\bar{f}$ , then  $f$  is good. Moreover, for any good partition  $\bar{\Psi}$  of  $[\bar{f}^{\partial n}]$ , there exists a good partition  $\Psi$  of  $[f^{\partial n}]$  such that  $f, \Psi$  specialise into  $\bar{f}, \bar{\Psi}$ .*

*Proof.* Assume that  $f = \prod_{i < m} \lambda_i$  and  $f^{\partial n+1} \neq 0$ . If  $m = n$ , then  $f$  is good, so we may assume that  $m > n$ . Then  $f^{\partial n} \neq 0$ , and  $[f^{\partial n}]$  consists of  $N$  distinct points  $(\zeta_j : j < N)$  (all possible intersections of  $n$  among the  $\lambda_i$ ), each repeated  $n!$  times. By [Theorem 1.4](#),  $\psi = (\zeta_j : j < N)$  is a good set, so  $\Psi = \{\psi, \psi, \dots\}$  ( $n!$  times) is a good partition.

The second item is clear.

For the third, again we may assume that  $m > n$ , and consider a specialisation  $\varphi: A \rightarrow \bar{A}$  such that  $\bar{f} = \varphi(f)$  is good, with good partition  $\bar{\Psi}$ . Extend  $\varphi$  to  $A[dX] \rightarrow \bar{A}[dX]$  as the identity on  $dX$ , and by [Lemma 2.4\(iii\)](#) we can extend it further to a specialisation  $C \rightarrow \bar{C}$  such that  $f^{\partial n}$  splits over  $C$ . Since factors of  $f^{\partial n}$  are sent to factors of  $\bar{f}^{\partial n}$ , there is a partition  $\Psi$  of  $[f^{\partial n}]$  which gets sent to  $\bar{\Psi}$ .  $\blacksquare$

**Convention 3.12.** When  $\Psi$  is a good partition we shall always enumerate  $\psi \in \Psi$  as  $\{\zeta_{\psi,i} : i < N\}$ . We may choose representatives  $x_{\psi,i}$  for  $\zeta_{\psi,i}$  as convenient.

**Lemma 3.13.** *Assume that  $\Psi$  is a good partition of  $[f^{\partial n}]$ . Then for every  $\Psi_0 \subseteq \Psi$  and choice of points  $\zeta_{\psi} \in \psi$  for  $\psi \in \Psi_0$ :*

$$\mathfrak{D}_{f,\Psi} \prod_{\psi \in \Psi_0} \varphi_{f,\psi,\zeta_{\psi}} \in B[X].$$

*In particular, we have*

$$\mathfrak{D}_{f,\Psi} \in B, \quad \mathfrak{D}_{f,\Psi} \prod_{\psi \in \Psi} \varphi_{f,\psi,\zeta_{\psi}} \in B[X].$$

*Proof.* Let us consider a valuation  $w$  of  $L$  such that  $\mathcal{O}_w \supseteq A[dX]$ . We choose representatives  $\xi_{\psi,i} = [x_{\psi,i}]$  such that  $f^{\partial n} = \prod_{\psi,i} x_{\psi,i}$  and  $w(x_{\psi,i}) \geq 0$  for all  $\psi, i$ . Therefore, all entries of the matrix  $M_\psi = (v_{m-n}(x_{\psi,i}) : i < N)$  are in  $\mathcal{O}_w$ , and the same holds for the co-factor matrix  $\det M_\psi \cdot M_\psi^{-1}$ . The  $i$ th row of the latter is  $\frac{\det M_\psi}{\partial_n f(x_{\psi,i})} \varphi_{f,\psi,\xi_{\psi,i}}$ . It follows, in particular, that  $\det M_\psi \varphi_{f,\psi,\xi_{\psi,i}} \in B[X]$ . Since  $\det M_\psi \in B$  as well, we have

$$\mathfrak{D}_{f,\Psi} \prod_{\psi \in \Psi_0} \varphi_{f,\psi,\xi_\psi} = \prod_{\psi \in \Psi \setminus \Psi_0} \det M_\psi \prod_{\psi \in \Psi_0} \left( \det M_\psi \varphi_{f,\psi,\xi_\psi} \right) \in B[X].$$

The rest consists of the two extreme cases  $\Psi_0 = \emptyset$  and  $\Psi_0 = \Psi$ . ■

**Lemma 3.14.** *Let  $f \in A[X]_d$  with  $d \geq n$  and  $g \in A[X]_{m-d}$ . Assume that  $fg$  is good, and let  $\Psi$  be a good partition. For  $\psi \in \Psi$  let  $\psi_f = \psi \cap [f^{\partial n}]$ , and let  $\Psi_f = \{\psi_f : \psi \in \Psi\}$  (again, a multi-set).*

- (i) *We have  $f^{\partial n} \mid (fg)^{\partial n}$ , and each point of  $(fg)^{\partial n}$  is either a point of  $f^{\partial n}$  or is a zero of  $g$  (but not both). Moreover,  $|\psi_f| = \binom{d}{n}$  for all  $\psi \in \Psi$ .*
- (ii) *The polynomial  $f$  is good, and  $\Psi_f$  is a good partition of  $[f^{\partial n}]$ .*
- (iii) *Recall that  $\preceq$  denotes divisibility in  $B$ ,  $B$ , the absolute integral closure of  $A[dX]$ . Then*

$$\mathfrak{D}_{f,\Psi_f} \preceq \mathfrak{D}_{fg,\Psi}.$$

- (iv) *For every  $\psi \in \Psi$  and  $\xi \in \psi_f$  we have*

$$\varphi_{fg,\psi,\xi} = g \varphi_{f,\psi_f,\xi}.$$

*Therefore, for every choice of points  $\xi_\psi \in \psi_f$ :*

$$\mathfrak{D}_{f,\Psi_f} \prod_{\psi \in \Psi} \varphi_{fg,\psi,\xi_\psi} \in B[X].$$

*Proof.* From **Lemma 3.6** we have  $f^{\partial n} \mid (fg)^{\partial n}$ . Recall that  $\partial_k(fg) = \sum_{\ell \leq k} \partial_\ell f \partial_{k-\ell} g$ , and let  $x \mid (fg)^{\partial n}$ . If  $g(x) = 0$  then, since  $\partial_n(fg)(x) \neq 0$ , we must have  $\partial_k f(x) \neq 0$  for some  $k < n$ , so  $[x] \notin [f^{\partial n}]$ . If, on the other hand,  $g(x) \neq 0$ , then by induction on  $k < n$ , one sees that  $\partial_k(fg)(x) = g(x) \partial_k f(x) = 0$ , so  $\partial_k f(x) = 0$ , and thus  $[x] \in [f^{\partial n}]$ . This proves the main assertion of (i). If  $g(x) = 0$  then  $v_{m-n}(x)$ , viewed as a linear function on  $K[X]_{m-n}$ , factors through  $\dim K[X]_{m-n}/(g)$ . Therefore  $|\psi| \cap V(g) \leq \dim K[X]_{m-n}/(g) = N - \binom{d}{n}$ , whence the moreover part.

Let  $w$  be a valuation of  $L$  such that  $\mathcal{O}_w \supseteq A[dX]$ . We may choose representatives  $[x_{\psi,i}] = \xi_{\psi,i}$  with

$$\begin{aligned} w(x_{\psi,i}) &\geq 0, \\ f^{\partial n} &= \prod_{\psi \in \Psi} \prod_{[x_{\psi,i}] \in \psi_f} x_{\psi,i}, \\ (fg)^{\partial n} / f^{\partial n} &= \prod_{\psi \in \Psi} \prod_{[x_{\psi,i}] \in \psi \cap V(g)} x_{\psi,i}. \end{aligned}$$

Writing  $g = \sum \alpha_s X^s$ , we let  $w(g) = \min_s w(\alpha_s)$ , and let  $s_0$  be lexicographically least such that  $w(\alpha_{s_0}) = w(g)$ . Order the monomials of order degree  $m-n$  such that the first  $\binom{d}{n}$  are those of the form  $X^{s+s_0}$ , where  $|s| = d-n$ . Order the points of  $\psi$  such that those of  $\psi_f$  come first. Let  $M$  be the matrix whose first  $\binom{d}{n}$  rows are the coefficient vectors of  $X^s g / \alpha_{s_0}$  for  $|s| = d-n$ , and the remaining rows are the same as in the identity matrix. Then  $w(\det M) = 0$ , and for  $\psi \in \Psi$ :

$$M(v_{m-n}(x_{\psi,i}) : i < N) = \left( \begin{array}{c|c} \left( g(x_{\psi,i}) v_{d-n}(x_{\psi,i}) / \alpha_{s_0} : i < \binom{d}{n} \right) & 0 \\ \hline ? & M_\psi \end{array} \right),$$

where  $M_\psi$  is polynomial in  $(x_{\psi,i} : i \geq \binom{d}{n})$ , so  $w(\det M_\psi) \geq 0$ . It follows that

$$\begin{aligned} w(\mathfrak{D}_{fg,\Psi}) &= \sum_{\psi} w(\det M(v_{m-n}(x_{\psi,i}) : i < N)) \\ &\geq \sum_{\psi} w\left(\det\left(g(x_{\psi,i})v_{m-n}(x_{\psi,i})/\alpha_{s_0} : i < \binom{d}{n}\right)\right) \\ &\geq \sum_{\psi} w\left(\det\left(v_{m-n}(x_{\psi,i}) : i < \binom{d}{n}\right)\right) \\ &= w(\mathfrak{D}_{f,\Psi_f}). \end{aligned}$$

This tells us first that  $\Psi_f$  is indeed a good partition, so  $f$  is good as well, whence (ii). Since  $w$  was arbitrary such that  $\mathcal{O}_w \supseteq A[dX]$ , this proves (iii).

For  $\zeta = [x] \in \psi_f \in \Psi_f$  we have  $f(x) = \dots = \partial_{n-1}f(x) = 0$ , so  $\partial_n(fg)(x) = g(x)\partial_n f(x)$ . Thus, for  $[y] \in \psi$  we have

$$g(y)\varphi_{f,\psi_f,\zeta}(y) = \begin{cases} g(y)\partial_n f(y) = \partial_n(fg)(y) & \zeta = [y], \\ g(y) \cdot 0 = 0 & \zeta \neq [y] \in \psi_f, \\ 0 \cdot \varphi_{f,\psi_f,\zeta}(y) = 0 & [y] \notin \psi_f. \end{cases}$$

This proves the first assertion of (iv), and the second follows from Lemma 3.13.  $\blacksquare$

In what follows, we shall consider a family of (non constant) polynomials  $F = (f_i : i < m)$ , such that  $m \geq n$ . We are going to associate to it two “error terms”, again a “small” and a “large” one.

$$\begin{aligned} \mathfrak{e}_{F,\Psi} &= \prod_{G \in \binom{F}{n}} \mathfrak{D}_{G,\Psi_G}^{(\deg G)}, \\ \mathfrak{E}_{F,\Psi} &= \prod_{G \in \binom{F}{n}} \left( \mathfrak{D}_{G,\Psi_G}^{(\deg G)} G^{\partial n+1} \right) = \mathfrak{e}_{F,\Psi} \prod_{G \in \binom{F}{n}} G^{\partial n+1}. \end{aligned}$$

We observe that in either one, the number of terms grows as  $m^n$ .

**Lemma 3.15.** *Let  $F = (f_i : i < m)$  be a family of polynomials in  $A[X]$ , where  $m \geq n$ , and let  $\Psi_F$  be a good partition for  $F$ . Then*

$$\mathfrak{e}_{F,\Psi_F} \mathfrak{D}_{F,\Psi_F} \in B.$$

If  $g \in A[X]$  is an additional polynomial, and  $\Psi$  is a good partition for the augmented family  $Fg$ , then

$$\mathfrak{e}_{F,\Psi_F} \mathfrak{D}_{F,\Psi_F} \preceq \mathfrak{e}_{Fg,\Psi} \mathfrak{D}_{Fg,\Psi}.$$

*Proof.* Let  $w$  be such that  $\mathcal{O}_w \supseteq A[dX]$ . Choose some enumeration  $\{G_i : i < N\} = \binom{F}{n}$ , and enumerate each  $\psi_F$  as  $\{[x_{\psi,j}] : j\}$ , first putting all points of  $\psi_{G_0}$ , then all those of  $\psi_{G_1} \setminus \psi_{G_0}$ , and so on, noting that this indeed exhausts  $\psi_F$ . Notice that  $\psi_G \cap \psi_{G'} = \psi_{G \cap G'}$  is of cardinal  $\binom{\deg G \cap G'}{n}$  (or empty if  $\deg G \cap G' < n$ ), and similarly for intersections of more than two  $G_i$ 's. In other words, for each  $j$  we have some  $i_j$  such that  $[x_{\psi,j}] \in \psi_{G_{i_j}}$  for all  $\psi$ . By Lemma 3.14(iv), for each  $j$ :

$$\sum_{\psi} w(\varphi_{F,\psi_F,[x_{\psi,j}]}) + w(\mathfrak{D}_{G_{i_j},\Psi_{G_{i_j}}}) \geq 0.$$

Finally, for each  $G_i$  there can be at most  $\binom{\deg G_i}{n}$  many values of  $j$  such that  $i = i_j$ . Therefore

$$w(\mathfrak{e}_{F,\Psi_F} \mathfrak{D}_{F,\Psi_F}) = \sum_{\psi} w(\det \Phi_{F,\psi_F}) + \sum_{G \in \binom{F}{n}} \binom{\deg G}{n} w(\mathfrak{D}_{G,\Psi_G}) \geq 0.$$

This proves our first assertion.

For the second, start in the same fashion, this time for the augmented family  $Fg$ , putting all  $G \in \binom{F}{n}$  before any  $G \in \binom{Fg}{n} \setminus \binom{F}{n}$ . In particular, the first  $\binom{\deg F}{n}$  points of any  $\psi$  are those of  $\psi_F$ . The matrix  $\Phi_{Fg,\psi}$  takes the form

$$\Phi_{Fg,\psi} = \begin{pmatrix} \Phi_{F,\psi_F} W \\ V \end{pmatrix} = \begin{pmatrix} \Phi_{F,\psi_F} & \\ & I \end{pmatrix} \begin{pmatrix} W \\ V \end{pmatrix},$$

where  $W$  is the matrix of the operation  $A[X]_{\deg F-n} \rightarrow A[X_{\deg F-g-n}]$  of multiplication by  $g$ , and the rows of  $V$  are of the form  $\varphi_{Fg,\psi,[x_{y,j}]}$  where  $G_{ij}$  can be written as  $G'_{ij}g$ , where  $G'_{ij} \in \binom{F}{n-1}$ . By the same reasoning as before:

$$\sum_{\psi} w(\det \Phi_{Fg,\psi}) + \sum_{G \in \binom{F}{n-1}} \binom{\deg Gg}{n} w(\mathfrak{D}_{Gg,\Psi_{Gg}}) \geq \sum_{\psi} w(\det \Phi_{F,\psi_F}),$$

i.e.,

$$\begin{aligned} w(\mathfrak{e}_{Fg,\Psi} \mathfrak{D}_{Fg,\Psi}) &= \sum_{\psi} w(\det \Phi_{Fg,\psi}) + \sum_{G \in \binom{Fg}{n}} \binom{\deg G}{n} w(\mathfrak{D}_{G,\Psi_G}) \\ &\geq \sum_{\psi} w(\det \Phi_{F,\psi_F}) + \sum_{G \in \binom{F}{n}} \binom{\deg G}{n} w(\mathfrak{D}_{G,\Psi_G}) \\ &= w(\mathfrak{e}_{F,\Psi_F} \mathfrak{D}_{F,\Psi_F}). \end{aligned}$$

This concludes the proof.  $\blacksquare$

By a *generic family of polynomials* we mean a family  $F = (f_i : i < m)$  of polynomials with formal unknown coefficients:  $f_i = \sum_s T_{i,s}^* X^s \in A[X]$ , where  $A = \mathbf{Z}[T^*]$ . By [Lemma 3.11](#), every generic family is good. For any  $H \in \binom{F}{n+1}$  we have  $H^\wedge \in \mathbf{Z}[T^*]$ . By [Proposition 2.15](#),  $H^\wedge$  is the resultant form for  $\mathbf{P}^n(\mathbf{Q}^a)$  in the appropriate degrees, so it is irreducible in  $\mathbf{Q}[T^*]$ . On the other hand, reducing modulo any prime  $p$  sends  $H^\wedge$  to the resultant form for  $\mathbf{P}^n(\mathbf{F}_p^a)$ . It follows that  $H^\wedge$  is irreducible in  $\mathbf{Z}[T^*]$ .

**Theorem 3.16.** *Let  $F = (f_i : i < k)$  be a family of polynomials in  $A[X]$ , where  $k \geq n$ , and let  $\Psi$  be a good partition for  $F$ . Then*

$$1 \preceq \mathfrak{D}_{F,\Psi} \prod_{H \in \binom{F}{n+1}} (H^\wedge)^{-n!n} \preceq \mathfrak{E}_{F,\Psi}, \quad (9)$$

$$1 \preceq \mathfrak{e}_{F,\Psi} \mathfrak{D}_{F,\Psi} \prod_{H \in \binom{F}{n+1}} (H^\wedge)^{-n!} \preceq \mathfrak{E}_{F,\Psi}. \quad (10)$$

*Proof.* We may assume that  $F$  is a generic family, and  $A = \mathbf{Z}[T^*]$  (since any family is a specialisation of a generic one). Let  $H \in \binom{F}{n+1}$ , and let  $w$  be any extension to  $L$  of the  $H^\wedge$ -adic valuation on  $A[dX]$ . Fix representatives such that  $w(x_{\psi,i}) \geq 0$  and  $F^{\partial n} = \prod_{\psi,i} x_{\psi,i}$ . For every  $G \in \binom{H}{n}$  we have  $(G^\wedge)^{n!} \mid f^{\partial n}$ , so  $\psi \in \Psi$  contains  $[G^\wedge]$ . By [Lemma 2.18](#):

$$w(\mathfrak{D}_{f,\Psi}) = \sum_{\psi} w(\det(v_{m-n}(x_{\psi,i}) : i < N)) \geq n!n.$$

With [Fact 2.2](#), this proves the first relation of (9).

Let  $(\alpha_i : i < \ell)$  be all  $K$ -conjugates of  $\mathfrak{D}_{F,\Psi}$ , so  $w(\alpha_i) \geq n!n$  for all  $i$ . If we had  $w(\alpha_j) > n!n$  for some  $j$ , then  $w(\prod \alpha_i) > \ell n!n$ , i.e.,  $(H^\wedge)^{\ell n!n+1} \mid \prod \alpha_i$ . We can specialise the whole situation to the case where all the polynomials are products of generic linear forms, in which case the latter divisibility relation is impossible. Therefore  $w(\alpha) = n!n$  for every conjugate of  $\mathfrak{D}_{F,\Psi}$ . On the other hand, we have  $\mathfrak{D}_{F,\Psi} \mathfrak{D}_{F,\Psi} = F^{\partial n+1}$ , and  $w(F^{\partial n+1}) = (n+1)!$ , so  $w(\mathfrak{D}_{F,\Psi}) = n!$ . For  $G \in \binom{F}{n}$ , the valuation  $w$  is trivial on  $\mathbf{Z}[G, dX]$  (the sub-ring of  $A[dX]$  generated by  $dX$  and the coefficients of  $G$ ), so  $w(\mathfrak{e}_{F,\Psi} \mathfrak{D}_{F,\Psi}) = n!$ . With [Lemma 3.15](#), the first relation of (10) follows.

Finally, by [Lemma 3.9](#) we have

$$\mathfrak{e}_{F,\Psi} \mathfrak{D}_{F,\Psi} \mathfrak{D}_{F,\Psi} = \mathfrak{e}_{F,\Psi} F^{\partial n+1} \preceq \mathfrak{E}_{F,\Psi} \prod_{H \in \binom{F}{n+1}} (H^\wedge)^{(n+1)!},$$

i.e.,

$$\left( \mathfrak{D}_{F,\Psi} \prod_{H \in \binom{F}{n+1}} (H^\wedge)^{-n!n} \right) \left( \mathfrak{e}_{F,\Psi} \mathfrak{D}_{F,\Psi} \prod_{H \in \binom{F}{n+1}} (H^\wedge)^{-n!} \right) \preceq \mathfrak{E}_{F,\Psi}.$$

The remaining relations follows.  $\blacksquare$

We consider [Theorem 3.16](#) to be the analogue for hypersurfaces of the Vandermonde identity [Theorem 1.4](#). Indeed, consider first the case where all the  $f_i$  are linear. Then  $\prod_{H \in \binom{F}{n+1}} (H^\wedge)^{n!n}$  is just the  $n!$  power of the right hand side of the Vandermonde identity [\(4\)](#), while  $\mathfrak{D}_{\Psi, f}$  is in fact in  $A[dX]$ , and is the  $n!$  power of the left hand side, multiplied by some power of the scalars  $\partial_1 f_i = f_i(dX)$ . In addition, the error terms  $\mathfrak{e}_{f, \Psi}$  and  $\mathfrak{E}_{f, \Psi}$  are scalars (again, powers of  $f_i(dX)$ ). Thus [Theorem 1.4](#) is a special case of [\(9\)](#). Similarly,  $\mathfrak{d}_{f, \Psi}$  is the  $n!$  power of the left hand side of the dual Vandermonde identity [\(5\)](#), so [Corollary 1.5](#) is a special case of [\(10\)](#).

In the general case,  $\prod_{H \in \binom{F}{n+1}} (H^\wedge)^{n!n}$  analogous to the right hand side of [\(4\)](#), telling us whether  $n+1$  polynomials of our family have a common zero, while  $\mathfrak{D}_{\Psi, f}$  is analogous to the determinant of the left hand side. Thus [\(9\)](#) tells us that they are *asymptotically* the same: one is a factor of the others, with the degree of the quotient having a strictly smaller rate of growth ( $m^n$ , compared with  $m^{n+1}$ ), and similarly for [\(10\)](#).

We obtain, using the same ideas, a version relative to a hypersurface defined by a polynomial  $g$ . The “right hand side”, telling us whether  $n$  polynomials have a common zero on the hypersurface, is  $\prod_{H \in \binom{F}{n}} (g \wedge H^\wedge)^{n!n}$ , and the theorem tells us that it divides the “relative determinant”  $\mathfrak{D}_{fg, \Psi} / \mathfrak{D}_{f, \Psi}$ , and asymptotically equal to it, again with the degree of the quotient having a strictly smaller rate of growth ( $m^{n-1}$ , compared with  $m^n$ ). Indeed, for the rather of growth of the error terms, observe that:

$$\frac{\mathfrak{e}_{Fg, \Psi}}{\mathfrak{e}_{F, \Psi_F}} = \prod_{G \in \binom{F}{n-1}} \mathfrak{D}_{Gg, \Psi_{Gg'}}^{\binom{\deg Gg}{n}} \quad \frac{\mathfrak{E}_{Fg, \Psi}}{\mathfrak{E}_{F, \Psi_F}} = \frac{\mathfrak{e}_{Fg, \Psi}}{\mathfrak{e}_{F, \Psi_F}} \prod_{G \in \binom{F}{n-1}} (Gg)^{\partial n+1}.$$

**Corollary 3.17.** *Let  $F = (f_i : i < k)$  be a family of polynomials in  $A[X]$ , where  $k \geq n-1$ , let  $g \in A[X]$  be one additional polynomial, and let  $\Psi$  be a good partition for  $Fg$ . Then*

$$1 \prec \frac{\mathfrak{D}_{Fg, \Psi}}{\mathfrak{D}_{F, \Psi_F}} \prod_{H \in \binom{F}{n}} (g \wedge H^\wedge)^{-n!n} \prec \frac{\mathfrak{E}_{Fg, \Psi}}{\mathfrak{E}_{F, \Psi_F}}, \quad (11)$$

$$1 \prec \frac{\mathfrak{e}_{Fg, \Psi} \mathfrak{D}_{Fg, \Psi}}{\mathfrak{e}_{F, \Psi_F} \mathfrak{D}_{F, \Psi_F}} \prod_{H \in \binom{F}{n}} (g \wedge H^\wedge)^{-n!} \prec \frac{\mathfrak{E}_{Fg, \Psi}}{\mathfrak{E}_{F, \Psi_F}}. \quad (12)$$

*Proof.* As in the proof of [Theorem 3.16](#), we may assume that  $Fg$  forms a generic family. We know from [Lemma 3.14\(iii\)](#) that  $\mathfrak{D}_{Fg, \Psi} / \mathfrak{D}_{F, \Psi_F} \in B$ . If  $H \in \binom{F}{n}$  and  $w$  extends the  $(g \wedge H^\wedge)$ -adic valuation, then  $w(\mathfrak{D}_{Fg, \Psi}) = n!n$  while  $w(\mathfrak{D}_{F, \Psi_F}) = 0$ . The first relation of [\(11\)](#) follows. The first relation of [\(12\)](#) follows by the same kind of reasoning, using [Lemma 3.15](#). As in the proof of [Theorem 3.16](#), the product of the two middle terms divides the common right term, concluding the proof. ■

## REFERENCES

- [AM69] M. F. ATIYAH and I. G. MACDONALD, *Introduction to commutative algebra*, Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969.  
 [GKZ94] I. M. GEL'FAND, M. M. KAPRANOV, and A. V. ZELEVINSKY, *Discriminants, resultants, and multidimensional determinants*, Mathematics: Theory & Applications, Birkhäuser Boston, Inc., Boston, MA, 1994.

ITAÏ BEN YAACOV, UNIVERSITÉ CLAUDE BERNARD – LYON 1, INSTITUT CAMILLE JORDAN, CNRS UMR 5208, 43 BOULEVARD DU 11 NOVEMBRE 1918, 69622 VILLEURBANNE CEDEX, FRANCE

URL: <http://math.univ-lyon1.fr/~begnac/>