THE VANDERMONDE DETERMINANT IDENTITY IN HIGHER DIMENSION

ITAÏ 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.

This is work in progress.

CONTENTS

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 (as the family increases).

1. THE LINEAR VANDERMONDE IDENTITY

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

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

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

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

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.

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 $n+1$ indeterminates 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 $\nu_m \colon A^{n+1} \to A^N$, where $N = \binom{n+m}{n}$ is the number of monomials, as the corresponding Veronese embedding,

2010 *Mathematics Subject Classification.* 15A15.
Key words and phrases. Vandermonde; determinant; hypersurface; intersection; resultant; Chow form.
Author supported by ANR project ValCoMo (ANR-13-BS01-0006) and ERC Grant no. 291111.
Revision 3693 *of* 11th January 2018.

that is, $\nu_{m,i}(x)$ is the ith monomial applied to x. We extend ν_m to a map $M_{(n+1)\times\ell}(A) \to M_{N\times\ell}(A)$ by applying ν_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:

$$\det\bigl(\nu_m(a_0, \ldots, a_m)\bigr) = \prod_{i<j\leq m} \det(a_i, a_j). \tag{3}$$

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. The equivalent dual question is whether a family of hyperplanes in $\mathbf{P}^n$ is in general position, namely, no $n+1$ of them intersect. As it turns out, the dual point of view will be more suitable. In particular, if we consider the indeterminates to represent a family of hyperplanes in $\mathbf{P}^n$, then in order to get points (on which the Veronese map can act) 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 $\mu\colon M_{(n+1)\times m}(A) \to M_{(n+1)\times\binom{m}{n}}(A)$ by sending a matrix Λ to the matrix of minors of Λ of order n. Minors are ordered by lexicographic ordering on the sequences of rows/columns which are chosen.

(ii) We define $\delta\colon M_{(n+1)\times m}(A) \to A$ by sending a matrix Λ to the product of minors of Λ 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 $\det(\nu_m\Lambda) = \det(\nu_m\mu\Lambda) = \delta\Lambda$. 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 Λ, times a scalar, to another, does not change either $\det(\nu_{m-n}\mu\Lambda)$ or $\delta\Lambda$.*

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

(iii) *Multiplying a column of Λ by a scalar α multiplies $\det(\nu_{m-n}\mu\Lambda)$ 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 $\det(\nu_{m-n}\mu\Lambda)$.

For the first assertion, adding a multiple of a row in Λ to another amounts to a similar operation on $\mu\Lambda$ and to a sequence of several such operations on $\nu_{m-n}\mu\Lambda$. For the second assertion, multiplying a row of Λ by α amounts to multiplying n rows of $\mu\Lambda$ by α. 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 $n+1$ indeterminates is $n\binom{m}{n+1}$. For the third assertion, multiplying a column of Λ by α amounts to multiplying $\binom{m-1}{n-1}$ columns of $\mu\Lambda$ by α, and the same columns of $\nu_{m-n}\mu\Lambda$ by α^{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 $\nu_{m-n}\mu\Lambda$ is a square matrix of order $\binom{m}{n}$, and the* Vandermonde identity of order m in dimension n *holds:*

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

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 Λ 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 $(1, 0, \ldots, 0)$. Let Λ_0 be Λ without this column and let Λ_1 be Λ with both first row and column dropped. Then $\delta\Lambda = (\delta\Lambda_0)(\delta\Lambda_1)$, and by the the induction hypothesis for $(n, m-n-1)$ and $(n-1, m-n)$ we have

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

Now,

$$\mu\Lambda = \begin{pmatrix} \mu\Lambda_1 & \\ & \mu\Lambda_0 \\ 0 & \end{pmatrix}, \qquad \nu_{m-n}\mu\Lambda = \begin{pmatrix} \nu_{m-n}\mu\Lambda_1 & \\ & \nu_{m-n}\mu\Lambda_0 \\ 0 & \end{pmatrix} = \begin{pmatrix} \nu_{m-n}\mu\Lambda_1 & * \\ 0 & C \end{pmatrix}.$$

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 indeterminate appears. Factoring this common indeterminate out, and letting $(\ldots, b_j, \ldots)$ 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 Λ_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. ■

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 jth column of Λ 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 φ_ξ as the product of λ_j for $j \notin \xi$, a homogeneous polynomial of degree $m-n$. Ordering monomials as earlier we may identify φ_ξ with the column vector of coefficients. Ordering the subsets ξ 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:*

$$\det(\pi\Lambda) = \pm\delta\Lambda. \tag{5}$$

Proof. Let ξ and ζ 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 ζ: with an adequate choice of $\mu'\Lambda$ (i.e., of permutation and signs), it is the intersection point of the kernels of $(\lambda_i)_{i\in\zeta}$ (we may assume that Λ consists of indeterminates, 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 ξ and ζ, 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 $\varphi_\xi(p_\xi)$ is equal, up to sign, to the product of minors of order $n+1$ of Λ corresponding to the n columns in ξ plus one more. Thus each minor of order $n+1$ of Λ is a factor of $n+1$ expressions $\varphi_\xi(p_\xi)$. We conclude that

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

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. ■

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

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

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].

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

We fix indeterminates $X = (X_0, \ldots, X_n)$, and let $A[X]_m$ denote the module of homogeneous polynomials of degree m over a ring A. The indeterminates X form a basis for the module of linear forms $E = A[X]_1$, and we let $X^* = (X_0^*, \ldots, X_n^*) \subseteq E^*$ 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 $x = (x_0, \ldots, x_n)$. Alternatively, we may view X^* as a new system of "dual indeterminates", in which case $E^* = A[X^*]_1$, and $A[X^*]$ is the ring of polynomial functions on the space E of linear forms.

Definition 2.1. Let $D \in \mathbf{N}$. Let $x_i = \sum_{j\leq n} X_{i,j}X_j^*$ be indeterminate algebraic points, and $g_0(X^*) = \prod_{i<D} x_i$. Let $T = (T_\alpha)$ be indeterminates representing the coefficients of a homogeneous polynomials in X^* of degree D, and let $I \leq \mathbf{Z}[T]$ be the (homogeneous) ideal satisfied by the coefficients of g_0. We say that a homogeneous polynomial of degree D in X^* (over any ring) *splits* if its coefficients satisfy I, i.e., if it is a specialisation of g_0.

If $g \in A[X^*]_D$ splits, as per Definition 2.1, then, for every algebraically closed field K and every homomorphism $A \to K$, the image of g in $K[X^*]$ is either zero, or splits into algebraic points. When A has no nilpotent elements, these two properties of g are equivalent. When A is an integral domain, this is equivalent to g splitting (or being zero) in $K[X]$ where $K = \operatorname{Frac}(A)^a$.

From now on let A be indeed an integral domain. A splitting polynomial $g \in A[X^*]_D$ can be written as $g = a\prod_{i<D} x_i$, where the x_i are algebraic points (the scalar coefficient $a \in A$ allows us to include the cases where $g = 0$ or $D = 0$).

(i) When $g \neq 0$, it codes the finite multi-set (namely, set with multiplicities) of geometric points $[g] = \{[x_i] : i < D\}$. As a polynomial function, g vanishes at a linear form λ if and only if λ vanishes at some x_i.
(ii) The zero polynomial always splits, but does not code any set.
(iii) When $D = 0$, every $a \in A[X^*]_0 = A$ splits, and (except when $a = 0$) codes the empty set.

Before turning to Chow forms, which are very special examples of such splitting polynomials, let us consider the general case. Recall (e.g., from [AM69]) 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 2.2. *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.*

Also, an integral domain A is *integrally closed* if every member of $\operatorname{Frac} A$ which is integral over A already belongs to A. Every unique factorisation domain is integrally closed, so, in particular, every polynomial ring over a field, or over $\mathbf{Z}$, is integrally closed (in fact, every polynomial ring over an integrally closed domain is integrally closed).

Lemma 2.3. *Let A be an integral domain, and let $f \in A[X_0, \ldots, X_{D-1}]$ be homogeneous of degree d in each $X_j = (X_{j,0}, \ldots, X_{j,n})$, and assume that $g \in A[X^*]_D$ splits over some field $L \supseteq \operatorname{Frac}(A)$, say as $a\prod_{i<D} x_i$.*

(i) *The field L can always be taken to be an algebraic extension of* $\operatorname{Frac}(A)$.
(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 $\varphi\colon A \twoheadrightarrow \overline{A}$, with $\overline{A}$ an integral domain can be extended to $\psi\colon B \twoheadrightarrow \overline{B} \supseteq \overline{A}$, 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 $b = a^d f(x_0, \ldots, x_{D-1}) \in L$ depends only on the order of the geometric points $[x_0], \ldots, [x_{D-1}]$, 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 $b \in \mathcal{O}_w$, so b is integral over A. ■

Definition 2.4. Let A be an integral domain. Let $f \in A[X]_d$ and $g \in A[X^*]_D$, and assume that g splits as $a\prod_{i<D} x_i$. Then we define

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

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.

Lemma 2.5. *Let A be an integrally closed integral domain. Let $f \in A[X]_d$ and $g \in A[X^*]_D$ be as in Definition 2.4. Then*

(i) *When defined, we have*

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

(ii) *If f and h are of the same degree, g splits as $a\prod x_i$, 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 ℓ and k, respectively. Then $f \wedge g$ is homogeneous in Y of degree $\ell D + kd$.*

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

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

Proof. Items (i) and (ii) are clear. For (iii), let $K = \mathrm{Frac}(A)$ 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 $M = K(X_0^*, \ldots, X_{n-1}^0)$. 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 $\varphi \in \mathrm{Aut}(M^a/M)$ must be the identity on ML. It follows that all the x_i are equal and g is of the form x^{p^t}, 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 2.3(iv), it belongs to A.

Item (iv) is easy.

Item (v) follows directly from Lemma 2.3(iii). ■

Let $\ell \leq n$, and for each $j \leq \ell$ let $X_j^* = (X_{j,i}^* : i \leq n)$ be a copy of X^*, so $A[X_0^*, \ldots, X_\ell^*]$ is the algebra of polynomials in $\ell + 1$ linear forms.

Lemma 2.6. *Let $K \subseteq L$ be fields, $\xi = [x] \in \mathbf{P}^n(L)$, and let $(\lambda_i : i < m)$ be linear forms which are generic over $K(\xi)$ modulo the constraint that they vanish at ξ.*

(i) *If $W \subseteq \mathbf{P}^n$ is defined over K and $\dim W < m$, then $V(\lambda) \cap W \subseteq \{\xi\}$.*
(ii) *If $\mathrm{trdeg}_K K(\xi) \geq m$ then $(\lambda_i : i < m)$ are generic over K.*

Proof. Let $W \subseteq \mathbf{P}^n$ have dimension $\leq m$. Then by induction on m, $\dim W \cap V(\lambda) = \dim W - m$. In particular, if $\dim W = m$ then $W \cap V(\lambda)$ is finite, whence (i). When W is the locus of ξ we obtain $\mathrm{trdeg}_{K(\lambda)} K(\lambda, \xi) \leq \mathrm{trdeg}_K K(\xi) - m$. Since $\mathrm{trdeg}_{K(\xi)} K(\lambda, \xi) = nm$ by hypothesis, we obtain $\mathrm{trdeg}_K K(\lambda) \geq (n+1)m$, whence (ii). ■

Definition 2.7. Say that a polynomial $\mathfrak{C} \in A[X_0^*, \ldots, X_\ell^*]$ is *anti-symmetric (of degree D)* if it is homogeneous (of degree D) in X_ℓ^* and $\mathfrak{C}(\ldots, X_j^*, \ldots) = \mathfrak{C}(\ldots, X_j^* + X_k^*, \ldots)$ for all $j \neq k$. In this case we write $D = \deg \mathfrak{C}$.

Letting $(Y_0, \ldots, Y_{\ell+1})$ be $\ell + 2$ new indeterminate, and $\mu_0, \ldots, \mu_{\ell+1} \in A[X]_1$, we also define

$$P_{\mathfrak{C},\mu}(Y) = \mathfrak{C}\left(\frac{\mu_j}{Y_j} - \frac{\mu_{\ell+1}}{Y_{\ell+1}} : j \leq \ell\right) \prod_{i \leq \ell+1} Y_j^D \qquad \text{and} \qquad Q_{\mathfrak{C},\mu}(X) = P_{\mathfrak{C},\mu}(\mu X).$$

Lemma 2.8. *Assume that $\mathfrak{C} \in A[X_0^*, \ldots, X_\ell^*]$ is a non-zero anti-symmetric polynomial of degree D.*

(i) *The polynomial $\mathfrak{C}$ is homogeneous of degree D in each X_j^*.*
(ii) *For every $\sigma \in \mathfrak{S}_{\ell+1}$ we have:*

$$\mathfrak{C}(X_{\sigma 0}^*, \ldots, X_{\sigma \ell}^*) = \mathrm{sgn}\, \sigma^D \mathfrak{C}.$$

(iii) *Assuming μ are over A, we have $P_{\mathfrak{C},\mu} \in A[Y]_D$ and $Q_{\mathfrak{C},\mu} \in A[X]_D$, and applying a permutation $\sigma \in \mathfrak{S}_{\ell+2}$ to Y multiplies $P_{\mathfrak{C},\mu}$ by $\mathrm{sgn}\, \sigma^D$.*
(iv) *When $\ell < n$, and μ are indeterminate forms (i.e., with indeterminate coefficients), we have $Q_{\mathfrak{C},\mu} \neq 0$. Moreover, working over a field, if $(\mu^k : k < n - \ell)$ are indeterminate families of linear forms, then $\dim V(Q_{\mathfrak{C},\mu^k} : k < n - \ell) = \ell$.*

Proof. Successive applications of the hypothesis yield $\mathfrak{C} = \mathfrak{C}(X_1^*, -X_0^*, X_2^*, \ldots, X_\ell^*)$, and similarly for any pair of indices, proving (i) and (ii).

We may rewrite $P_{\mathfrak{C},\mu}$ as

$$\mathfrak{C}\left(\mu_j - \frac{Y_j}{Y_{\ell+1}} \mu_{\ell+1} : j \leq \ell\right) Y_{\ell+1}^D.$$

In particular, it is a polynomial in $Y_0, \ldots, Y_\ell$. If $j \leq \ell$, then by subtracting $\mu_j/Y_j - \mu_{\ell+1}/Y_{\ell+1}$ from all other arguments of $\mathfrak{C}$ in the definition of $P_{\mathfrak{C},\ell}$, and multiplying the argument $\mu_j/Y_j - \mu_{\ell+1}/Y_{\ell+1}$ by -1, we effectively exchange the indices j and $\ell + 1$, with the effect of and multiplying $P_{\mathfrak{C},\mu}$ by $(-1)^D$, proving (iii).

For (iv) we may assume that $A = K$ is a field. Let L be a large field containing K, the indeterminate coefficients of μ, as well as another indeterminate tuple X', and let $Y' = \mu X'$. The forms $\lambda_j = \mu_j/Y'_j -$

$\mu_{\ell+1}/Y'_{\ell+1}$, for $j \leq \ell$, are generic over $K(X')$ modulo the constraint that they all vanish at $[X']$. By Lemma 2.6, the λ_j are generic over K, so $\mathfrak{C}(\lambda) \neq 0$ and therefore $Q_{\mathfrak{C},\mu}(X') \neq 0$. For the moreover part, the dimension is at least ℓ. If it is not equal to ℓ, then there exists $m < n - \ell$ such that

$$\dim V(Q_{\mathfrak{C},\mu^k} : k < m) = \dim V(Q_{\mathfrak{C},\mu^k} : k \leq m) = n - m > \ell.$$

Choose $\xi = [x] \in V(Q_{\mathfrak{C},\mu^k} : k \leq m)$ such that $\operatorname{trdeg}_K K(\xi) = n - m$. Then ξ is algebraically independent from μ^m over $K(\mu^k : k < m)$, i.e., μ^m is generic over $K(\xi)$. But then the linear forms $\lambda'_j = \mu^m_j - (\mu^m_{\ell+1}x/\mu^m_j x)\mu^m_{\ell+1}$, for $j \leq \ell$, are generic over $K(\xi)$ modulo their vanishing at ξ. By Lemma 2.6(ii), they are generic over K, so $\mathfrak{C}(\lambda') \neq 0$ and $\xi \notin V(Q_{\mathfrak{C},\mu^m})$ after all. ■

Let us finally define Chow forms. The fundamental notion is that of a Chow form for a projective variety (here a *variety* is always irreducible). While it is standard to extend the definition to the (unique, up to scalar factor) Chow form of a cycle, for our purposes it will be preferable to define a (non-unique) Chow form associated with an algebraic set.

Definition 2.9. Let $\ell \leq n$, and for $j \leq \ell$ let $X^*_j = (X^*_{j,i} : i \leq n)$ be a copy of X^*. We may think of each group of indeterminates X^*_j as representing (the coefficients of) a linear form. Let K be an algebraically closed field.

(i) A polynomial $\mathfrak{C} \in K[X^*_0, \ldots, X^*_\ell]$ is a *Chow form in dimension* ℓ if there exists a Zariski-closed set $W \subseteq \mathbf{P}^n$ defined over K such that for every family of linear forms $\lambda = (\lambda_0, \ldots, \lambda_\ell)$ we have
$$\mathfrak{C}(\lambda) = 0 \qquad \Longleftrightarrow \qquad W \cap V(\lambda) \neq \varnothing. \tag{7}$$
We then say that $\mathfrak{C}$ is *associated with* W. Notice that this determines the family of prime factors of $\mathfrak{C}$, up to multiplicity.

(ii) Let $W \subseteq \mathbf{P}^n$ be a variety of dimension ℓ, defined over K. An irreducible Chow form in dimension ℓ associated with W, which is unique up to a scalar factor, is called *the Chow form of* W, denoted $\mathfrak{C}_W$.

Notice that we allow zero as a Chow form, associated with any algebraic set whose dimension is too big (this excludes zero as a Chow form in dimension n, since there are no sets of dimension $n+1$, but this borderline case will not bother us), as well as a non-zero constant Chow form, associated with $W = \varnothing$. With this we may extend the definition to a "Chow form" in dimension -1: this is a constant $a \in K$ which is zero if and only if $W \neq \varnothing$.

Fact 2.10. *Let $\ell \leq n$.*

(i) *The Chow form exists for any variety $W \subseteq \mathbf{P}^n$ of dimension ℓ.*

(ii) *More generally, let $W \subseteq \mathbf{P}^n$ be an algebraic set defined over K and $\mathfrak{C} \in K[X^*_0, \ldots, X^*_\ell]$. Then $\mathfrak{C}$ is a Chow form in dimension ℓ, associated with W, if and only if*
- *either $\dim W > \ell$ and $\mathfrak{C} = 0$,*
- *or W is of pure dimension ℓ, and*
$$\mathfrak{C} = \prod_k \mathfrak{C}^{m_k}_{W_k},$$
where (W_k) are the irreducible components of W and $m_k \geq 1$. In this case $\mathfrak{C}$ determines W.

(In the latter case, one usually says that $\mathfrak{C}$ is the *Chow form of the projective cycle $\sum m_k W_k$.)*

(iii) *Let $\mathfrak{C} \in K[X^*_0, \ldots, X^*_\ell]$ be a Chow form in dimension ℓ associated with W, and let λ be a family of ℓ 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 $\dim\big(W \cap V(\lambda)\big) > 0$,*
- *or $\mathfrak{C}(\lambda, X^*) = \prod_{k<D} x_k$, and $W \cap V(\lambda) = \big\{[x_k] : k < D\big\}$ (possibly with repetitions).*

In particular, if $L = K(X^*_0, \ldots, X^*_{\ell-1})$, then $\mathfrak{C} \in L[X^*_\ell]$ splits over L^a.

(iv) *If K is algebraically closed and $\mathfrak{C}$ is irreducible, splitting as in the previous item, then all the geometric points $\xi_k = [x_k]$ are conjugate over L and distinct. Each of the extensions $L(\xi_k)/L$ is separable, and $L(\xi_k : k < D)/L$ is Galois.*

(v) *Let $\mathfrak{C} \in K[X^*_0, \ldots, X^*_\ell]$ be a non-zero Chow form in dimension ℓ, associated with W. Then it is an anti-symmetric polynomial, and a point $[x] \in \mathbf{P}^n$ belongs to W if and only if $Q_{\mathfrak{C},\mu}(x) = 0$, where $\mu_0, \ldots, \mu_{\ell+1}$ are indeterminate linear forms and $Q_{\mathfrak{C},\mu}$ is as per Definition 2.7.*

Proof. For (i), say that W is defined over K. Let $L \supseteq K$ be some very rich field, and let $\xi \in W(L)$ be a generic point of W over K, so $\operatorname{trdeg}_K K(\xi) = \ell$. Let $\lambda = (\lambda_0, \ldots, \lambda_\ell)$ be linear forms whose coefficients which are generic over $K(x)$ modulo the constraint that $\xi \in V(\lambda)$. By Lemma 2.6, ξ is algebraic over $K(\lambda)$, so

$$\operatorname{trdeg}_K K(\lambda) = \operatorname{trdeg}_K K(\xi, \lambda) = \operatorname{trdeg}_K K(\xi) + \operatorname{trdeg}_{K(\xi)} K(\xi, \lambda) = \ell + (\ell+1)n = (\ell+1)(n+1) - 1.$$

The coefficients of λ are therefore related by a single irreducible polynomial $\mathfrak{C}_W(X_0^*, \ldots, X_\ell^*)$, unique up to a scalar factor.

Now let λ' be any $\ell + 1$ linear forms. Assume that $\mathfrak{C}_W(\lambda') = 0$, so λ' is a specialisation over K of λ. We may choose a compatible specialisation ξ' of ξ, and then $\xi' \in W \cap V(\lambda')$. Conversely, assume that $\xi' \in W \cap V(\lambda')$, so ξ' specialises ξ over K. Then ξ', λ' specialises ξ, λ'' over K for some family λ'' of linear forms, such that $\xi \in V(\lambda'')$. But then λ'' is a specialisation of λ over $K(\xi)$. Composing, λ' specialises λ, so $\mathfrak{C}_W(\lambda') = 0$. Therefore, $\mathfrak{C}_W$ satisfies (7). It is clearly unique, up to a scalar factor.

For (ii), right to left is evident. Assume therefore that $\mathfrak{C}$ is a Chow form in dimension ℓ, associated with W. We have $\mathfrak{C} = 0$ if and only if every $\ell + 1$ linear forms have a common zero in W, if and only if $\dim W > \ell$. Let us assume therefore that $\mathfrak{C} \neq 0$ and $\dim W \leq \ell$. Let $\mathfrak{C}_0$ be a prime factor of $\mathfrak{C}$ and let $\lambda = (\lambda_0, \ldots, \lambda_\ell)$ be a generic root of $\mathfrak{C}_0$. Then $W' \cap V(\lambda) \neq \varnothing$ for some irreducible component $W' \subseteq W$, and may assume that the coefficients of $\lambda_0, \ldots, \lambda_{\ell-1}$ are algebraically independent over K. Since $\mathfrak{C}_{W'}(\lambda_0, \ldots, \lambda_{\dim W'}) = 0$, we have $\dim W' = \ell$ and $\mathfrak{C}_0 = \mathfrak{C}_{W'}$ up to a scalar factor. Conversely, if W' is an irreducible component and $(\lambda_0, \ldots, \lambda_\ell)$ are generic modulo their vanishing at a generic point $\xi \in W'$, then $W \cap V(\lambda) = \{\xi\}$ by Lemma 2.6(i). Therefore $\dim W' = \ell$ and $\mathfrak{C}_{W'}$ is a factor of $\mathfrak{C}$.

For (iii), we know that $\mathfrak{C}(\lambda, \mu) = 0$ if and only if $W \cap V(\lambda, \mu) \neq \varnothing$, 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 (ii). In particular, $\mathfrak{C} = \mathfrak{C}(\lambda, X_\ell^*)$ where $\lambda_j = \sum X_{j,i}^* X_i$, so $\mathfrak{C}$ splits as a special case of the above.

For (iv) we assume that K is algebraically closed and $\mathfrak{C}$ is irreducible. Let $Y = X_n^*$. Up to a linear change of coordinates with coefficients in K, Y^D occurs in $\mathfrak{C}$ with a non-zero coefficient $a \in L$, and we may assume that $\mathfrak{C} = a \prod x_k$ where $x_{k,n} = 1$ for all k. Let $M = L(X_i^* : i < n)$, so $\mathfrak{C} \in M[Y]$ can be written as $aY^D + \ldots = a \prod_{k<D}(Y - b_k)$, with $\beta_k \in M^a$. Up to a permutation, we have $x_k = Y - b_k$, i.e., $b_k = -\sum_{i<n} x_{k,i} X_i^*$. Since $\mathfrak{C}$ is irreducible over K, it is also irreducible over M, so all the b_k are conjugate over M, and therefore the geometric points $[x_k]$ are conjugate over L. If some $[x_k]$ appears with multiplicity then necessarily K has positive characteristic p and, up to a permutation, $\mathfrak{C} = a \prod_{k<\frac{D}{p}}(Y - b_k)^p$. It follows that $\mathfrak{C}$ is a pth power, contradicting irreducibility. Up to some linear change of coordinates, we may further assume that for each $i < n$, the values $\{x_{k,i} : k < D\}$ are distinct. In $\mathfrak{C}$, let us substitute $X_i^* = -1$ and $X_j^* = 0$ for $i \neq j < n$, to obtain a polynomial $a \prod_k (Y - x_{k,i}) \in L[Y]$. We conclude that each $x_{k,i}$ is separable over L, so $L(\xi_k)/L$ is separable, and $L(\xi_k : k < D)/L$ is Galois.

For (v), homogeneity in each X_j^* separately follows from (7). From the previous item it follows that, if $j \neq k$, then $\mathfrak{C}$ remains unchanged when substituting $X_j^* + X_k^*$ for X_j^* (consider first the case when $j = \ell$). Therefore $\mathfrak{C}$ satisfies the hypothesis of Lemma 2.8. Let $\xi = [x] \in \mathbf{P}^n$ and let $\mu_0, \ldots, \mu_{\ell+1}$ be indeterminate linear forms. For $j \leq \ell$ define $\lambda_j = \mu_j - (\mu_j x / \mu_{\ell+1} x)\mu_{\ell+1}$, so $\lambda_0, \ldots, \lambda_\ell$ vanish at ξ and are generic modulo this constraint. By Lemma 2.6(i), $W \cap V(\lambda) = \{\xi\}$. Then $Q_{\mathfrak{C},\mu}(x) = 0$ if and only if $\mathfrak{C}(\lambda) = 0$ if and only if $\xi \in W$. ■

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 2.11. The Chow form of $\mathbf{P}^n$ is $\det(X_{i,j}^*)_{i,j \leq n}$ (i.e., the volume form $X_0^* \wedge \ldots \wedge X_n^*$), and the Chow form of a single point $[x]$ is x (both of degree 1).

Definition 2.12. Let $\mathfrak{C}(X_0^*, \ldots, X_\ell^*)$ be a Chow form in dimension ℓ. As in Fact 2.10(iii), let $L = K(X_0^*, \ldots, X_{\ell-1}^*)$ and identify X_ℓ^* with X^*, so $\mathfrak{C} \in L[X^*]$ splits. Let also $f \in K[X]_m$. Then, in accordance with Definition 2.4, we define

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

In particular we have $f \wedge 0 = 0 \wedge \mathfrak{C} = 0$ (assuming that $\deg f > 0$ and $\deg \mathfrak{C} > 0$).

Lemma 2.13. *Let A be an integrally closed integral domain. Let $\mathfrak{C} \in A[X_0^*, \ldots, X_\ell^*]$ be a Chow form in dimension ℓ, associated with an algebraic set W.*

(i) *Let $f \in A[X]_d$. Then $f \wedge \mathfrak{C} \in A[X_0^*, \ldots, X_{\ell-1}^*]$ is a Chow form in dimension $\ell - 1$ and degree $d \deg \mathfrak{C}$, associated with $W \cap V(f)$. When $\ell = 0$, this means that $f \wedge \mathfrak{C} \in A$ vanishes if and only if $W \cap V(f) \neq \varnothing$.*

(ii) *Let $f = \sum T_\alpha^* X^\alpha$ be a polynomial of degree d with indeterminate coefficients (let us simply call this an indeterminate polynomial of degree d). If $\mathfrak{C}$ is irreducible over $K = \mathrm{Frac}(A)$, then so is $f \wedge \mathfrak{C} \in A[X_0^*, \ldots, X_{\ell-1}^*, T^*]$.*

(iii) *Let $f \in A[X]_d$, $g \in A[X]_D$, and assume that $\ell \geq 1$. Then*

$$f \wedge g \wedge \mathfrak{C} = (-1)^{dD \deg \mathfrak{C}} g \wedge f \wedge \mathfrak{C}.$$

Proof. For (i), $A[X_0^*, \ldots, X_{\ell-1}^*]$ is integrally closed, so $f \wedge \mathfrak{C} \in A[X_0^*, \ldots, X_{\ell-1}^*]$ by Lemma 2.5, of degree $d \deg \mathfrak{C}$ in each X_j^*. Let λ be a family of ℓ linear forms. By Fact 2.10(iii), both $\mathfrak{C}$ and $\mathfrak{C}(\lambda, X^*)$ are Chow forms (in dimensions ℓ and 0, respectively), and $f \wedge \mathfrak{C}(\lambda, X^*) = 0$ if and only $W \cap V(\lambda, f) \neq \varnothing$. Since the wedge operation commutes with specialisation, we have $(f \wedge \mathfrak{C})(\lambda) = f \wedge \mathfrak{C}(\lambda, X^*)$. Thus $f \wedge \mathfrak{C}$ is a Chow form associated with $W \cap V(f)$.

For (ii), let $\lambda_k = \sum Y_{k,i}^* X_i$ for $k < d$ be indeterminate linear forms, and $g = \prod_k \lambda_k$. Then $\lambda_k \wedge \mathfrak{C} = \mathfrak{C}(X_0^*, \ldots, X_{\ell-1}^*, Y_k^*)$ is irreducible, and

$$(f \wedge \mathfrak{C})(X_0^*, \ldots, X_{\ell-1}^*, g) = g \wedge \mathfrak{C} = \prod_k \lambda_k \wedge \mathfrak{C}.$$

Assume that $f \wedge \mathfrak{C}$ factors as $h_0 h_1$ over K. Without loss of generality, $\lambda_0 \wedge \mathfrak{C} \mid h_0(X_0^*, \ldots, X_{\ell-1}^*, g)$. Since there exists an automorphism sending λ_0 to any λ_k over $K(X_0^*, \ldots, X_{\ell-1}^*, g)$, we have $g \wedge \mathfrak{C} \mid h_0(X_0^*, \ldots, X_{\ell-1}^*, g)$. It follows that h_1 is constant.

For (iii), we may assume that $A = K$, $\mathfrak{C}$ is irreducible, and f and g are indeterminate polynomials. In particular, $\mathfrak{C} = \mathfrak{C}_W$, and W is a variety defined over K. By (ii), both $f \wedge g \wedge \mathfrak{C}$ and $g \wedge f \wedge \mathfrak{C}$ are irreducible over K, and therefore also over $L = K(f, g)$. Both are therefore Chow forms for $W \cap V(f, g)$, a variety defined over L, so $f \wedge g \wedge \mathfrak{C} = a \cdot g \wedge f \wedge \mathfrak{C}$ for some $a \in L$. Since both are irreducible over K, we must have $a \in K$. Let λ and μ be indeterminate linear forms. We already know that $\lambda \wedge \mu \wedge \mathfrak{C} = (-1)^{\deg \mathfrak{C}} \mu \wedge \lambda \wedge \mathfrak{C}$, so substituting λ^d for f and μ^D for g we obtain $a = (-1)^{dD \deg \mathfrak{C}}$. ■

Definition 2.14. Let $\mathfrak{C}(X_0^*, \ldots, X_\ell^*)$ be a Chow form in dimension ℓ, and $k \leq \ell + 1$. For a sequence $f = (f_j : j < k)$ of homogeneous polynomials, we can iterate the wedge operation:

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

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

(i) *Let $k \leq \ell + 1$ and $f = (f_j : j < k)$ be homogeneous polynomials over A. Then the iterated wedge operation $f \wedge \mathfrak{C} \in A[X_0^*, \ldots, X_{\ell-k}^*]$ is a Chow form in dimension $\ell - k$ associated with $W \cap V(f)$. When $k = \ell - 1$, this means that $f \wedge \mathfrak{C} \in A$ vanishes if and only if $W \cap V(f) \neq \varnothing$.*

(ii) *For $j \leq \ell$ let $f_j = \sum T_{j,\alpha}^* X^\alpha$ be an indeterminate polynomial of degree d_j, and let $\mathfrak{R} = f \wedge \mathfrak{C} \in A[T^*]$. We may think of $\mathfrak{R}$ as a polynomial function in (the coefficients of) $\ell + 1$ homogeneous polynomials of appropriate degrees. For such polynomials $g = (g_0, \ldots, g_\ell)$ we have $\mathfrak{R}(g) = g \wedge \mathfrak{C}$, and*

$$\mathfrak{R}(g) = 0 \qquad \Longleftrightarrow \qquad W \cap V(g) \neq \varnothing. \tag{8}$$

In other words, $\mathfrak{R}$ is a resultant form associated with W. *If $\mathfrak{C}$ is irreducible over* $\mathrm{Frac}(A)$, *then so is $\mathfrak{R}$.*

(iii) *If g is a permutation of f then $f \wedge \mathfrak{C} = \pm g \wedge \mathfrak{C}$. More precisely, if $\sigma \in \mathfrak{S}_{\ell+1}$, then $(\sigma f) \wedge \mathfrak{C} = \operatorname{sgn} \sigma^{\deg \mathfrak{C} \prod d_j} f \wedge \mathfrak{C}$.*

Proof. Immediate from Lemma 2.13. ■

Notice that, if $d_j = 0$, then $f \wedge \mathfrak{C} = f_j^D$, where $D = \deg \mathfrak{C} \prod_{k \neq j} d_k$. In particular, if $d_j = d_k = 0$ for $j \neq k$ then $f \wedge \mathfrak{C} = 1$ (even if some of the f vanish).

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

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

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

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

Remark 2.17. Let $\mathfrak{C} \in K[X_0^*, \ldots, X_\ell^*]$. The polynomial $\mathfrak{C}$ is a Chow form if and only if it anti-symmetric and divides $\mathfrak{D} = Q_{\mathfrak{C},\mu^1} \wedge \ldots \wedge Q_{\mathfrak{C},\mu^{n-\ell}}$, where $\mu^1, \ldots, \mu^{n-\ell}$ are indeterminate families of $\ell + 2$ linear forms each and $Q_{\mathfrak{C},\mu}$ is as per Definition 2.7.

Notice that this condition is expressible as the vanishing of certain homogeneous polynomials over $\mathbf{Z}$ in the coefficients of $\mathfrak{C}$ (whence the existence of the *Chow scheme* consisting of all Chow forms in a given dimension and degree).

Proof. Assume that $\mathfrak{C}$ is a Chow form. Since $Q_{\mathfrak{C}\mathfrak{C}',\mu} = Q_{\mathfrak{C},\mu} Q_{\mathfrak{C}',\mu}$, we may assume that $\mathfrak{C} = \mathfrak{C}_W$ for some variety W. Each $Q_{\mathfrak{C},\mu^k}$ vanishes on W, so $\mathfrak{D}$ is a Chow form in dimension ℓ associated with an algebraic set containing W, and $\mathfrak{C}_W \mid \mathfrak{D}$.

Conversely, if $\mathfrak{C}$ is anti-symmetric, $V(Q_{\mathfrak{C},\mu^1},\dots,Q_{\mathfrak{C},\mu^{n-\ell}})$ has dimension ℓ, so $\mathfrak{D} \neq 0$. Then $\mathfrak{C}$ is a non-zero Chow form in dimension ℓ, being a factor of one. ■

3. The Macaulay resultant

In this section we give an explicit formula (Theorem 3.1) for the resultant of $n+1$ polynomials in $\mathbf{P}^n$, also know as the *Macaulay resultant*. Our formula is fairly similar to the formula given by Macaulay [Mac02]. In contrast with Macaulay's formula (or variants thereof which appear in the literature), ours has the general form of an exclusion/inclusion product of determinants, and each row of the matrices may code multiplication by more than one polynomial. While this makes our formula "longer" and thus less useful for numeric calculations, it is more amenable to formal manipulation.

Let us fix, as usual, $X = (X_0,\dots,X_n)$, and let $F = (f_i : i \leq n)$ be a family of indeterminate polynomials, i.e., each $f_i = \sum_\alpha T^*_{i,\alpha} X^\alpha$ is homogeneous of degree d_i with indeterminate coefficients. Thus $f_i \in A[X]$ where $A = \mathbf{Z}[T^*]$. By Proposition 2.15, $F^\wedge \in \mathbf{Z}[T^*]$ is (absolutely) irreducible in $\mathbf{Q}[T^*]$. Substituting $X_i^{d_i}$ for f_i in $F^\wedge$ we obtain 1, so it is in fact irreducible in $\mathbf{Z}[T^*]$.

For $i \leq n$ and a monomial $\mathfrak{m}$, let us define

$$\tilde{f}_i = \frac{f_i}{X_i^{d_i}}, \qquad \rho(\mathfrak{m}) = \{i \leq n : X_i^{d_i} \mid \mathfrak{m}\}.$$

Macaulay's formula expresses the resultant $F^\wedge$ in terms of determinants of matrices which code multiplication of monomials $\mathfrak{m}$ by these $\tilde{f}_i$, with the restriction that $\mathfrak{m}\tilde{f}_i$ be a polynomial, i.e., that $i \in \rho(\mathfrak{m})$. We modify this a little by considering multiplication by more than one $\tilde{f}_i$ at a time.

For $\sigma \subseteq n+1$ let $d_\sigma = \sum_{i\in\sigma} \deg f_i$. Let also $\tilde{f}_\sigma = \prod_{i\in\sigma} \tilde{f}_i$. Let $\mathfrak{M}_\ell$ denote all monomials of degree ℓ in X, and more generally, let $\mathfrak{M}^\sigma_\ell = \{\mathfrak{m} \in \mathfrak{M}_\ell : \rho(\mathfrak{m}) \supseteq \sigma\}$ (naturally identified with $\mathfrak{M}_{\ell-d_\sigma}$) We shall mostly be interested in this for $\ell \geq \ell_0 = \deg F - n$ (where $\deg F = \sum \deg f_i$). We identify a polynomial involving monomials from $\mathfrak{M}^\sigma_\ell$ with a row vector indexed by $\mathfrak{M}^\sigma_\ell$, and define an $\mathfrak{M}^\sigma_\ell \times \mathfrak{M}^\sigma_\ell$ matrix with entries in $\mathbf{Z}[T^*]$ by

$$\mathfrak{m}\mathbf{A}^\sigma_{F,\ell} = \mathfrak{m}\tilde{f}_{\rho(\mathfrak{m})\smallsetminus\sigma}, \qquad \mathfrak{m} \in \mathfrak{M}^\sigma_\ell.$$

In other words, for $i \notin \sigma$, we multiply by $\tilde{f}_i$ whenever possible. The determinant of $\mathbf{A}^\sigma_{F,\ell}$ does not depend on the order we put on $\mathfrak{M}^\sigma_\ell$. In this section we prove:

Theorem 3.1. *For all $\ell \geq \ell_0 = \deg F - n$, the Macaulay resultant $F^\wedge$ is given by*

$$F^\wedge = \prod_{\sigma\subseteq n+1} (\det \mathbf{A}^\sigma_{F,\ell})^{(-1)^{|\sigma|}}. \tag{9}$$

Example 3.2. Let $n = 1$, $F = (f, g)$, and $\ell = \ell_0 = \deg f + \deg g - 1$. Then for each monomial $\mathfrak{m} \in \mathfrak{M}_\ell$ we have either $\rho(\mathfrak{m}) = \{0\}$ or $\rho(\mathfrak{m}) = \{1\}$. It follows that $\mathbf{A}^{\{0\}}_{f,g,\ell}$ and $\mathbf{A}^{\{1\}}_{f,g,\ell}$ are identity matrices (and $\mathbf{A}^{\{0,1\}}_{f,g,\ell}$ is empty), so $f \wedge g = \det \mathbf{A}^\varnothing_{f,g,\ell}$, which is the familiar determinant formula for the resultant of two polynomials.

For the proof, let $\mathbf{a}^\sigma_{F,\ell} = \det \mathbf{A}^\sigma_{F,\ell}$ and similarly for other matrices we introduce later on. If we specialise each f_i to $X_i^{d_i}$, then $\mathbf{A}^\sigma_{F,\ell}$ specialises to the identity matrix, so $\mathbf{a}^\sigma_{F,\ell} \neq 0$.

Convention 3.3. From this point onward, let us always assume that $\sigma \subseteq n$, i.e., $n \notin \sigma$, and let $\sigma n = \sigma \cup \{n\}$.

Lemma 3.4. *Assume that $n > 0$. Let $X' = (X_0,\dots,X_{n-1})$, and let $F' = \big(f_i(X', 0) : i < m\big)$ (in other words, we go down to projective dimension $n-1$ by dropping all monomials involving X_n). Then F' is a family of indeterminate polynomials in X', and*

$$\mathbf{a}^{\sigma n}_{F,\ell} = \prod_{k\leq \ell-d_n} \mathbf{a}^\sigma_{F',k}. \tag{10}$$

Proof. Grouping the monomials in $\mathfrak{M}^\sigma_\ell$ by the degree of X_n, the matrix $\mathbf{A}^{\sigma n}_{F,\ell}$ is block-triangular. The diagonal block corresponding to degree $\ell - k$ is $\mathbf{A}^\sigma_{F',k}$. Since all monomials in $\mathfrak{M}^{\sigma n}_\ell$ are divisible by $X_n^{d_n}$, such blocks exist for $k \leq \ell - d_n$, whence (10). ■

Let us define a slight modification of $\mathbf{A}^{\sigma}_{F,\ell}$, in which one does not always multiply by $\tilde{f}_n$, even when possible. For $T \subseteq \mathcal{P}(n)$ we define an $\mathfrak{M}^{\sigma}_{\ell} \times \mathfrak{M}^{\sigma}_{\ell}$ matrix $\mathbf{A}^{\sigma,T}_{F,\ell}$ by

$$\mathfrak{m}\mathbf{A}^{\sigma,T}_{F,\ell} = \begin{cases} \mathfrak{m}\tilde{f}_{\rho(\mathfrak{m})\smallsetminus\{n\}\smallsetminus\sigma} & \rho(\mathfrak{m}) \smallsetminus \{n\} \in T \\ \\ \mathfrak{m}\tilde{f}_{\rho(\mathfrak{m})\smallsetminus\sigma} & \text{otherwise.} \end{cases}$$

The distinction between cases is of interest only if $n \in \rho(\mathfrak{m})$. By the same argument as above, the determinant of any such matrix is a non-zero polynomial in $\mathbf{Z}[T^*]$.

When $T = \varnothing$, we have $\mathbf{A}^{\sigma,\varnothing}_{F,\ell} = \mathbf{A}^{\sigma}_{F,\ell}$. When $T = \mathcal{P}(n)$, we have $\mathbf{A}^{\sigma,\mathbf{P}(n)}_{F,\ell} = \mathbf{A}^{\sigma n}_{F,\ell+d_n}$ modulo the obvious identification between $\mathfrak{M}^{\sigma}_{\ell}$ and $\mathfrak{M}^{\sigma n}_{\ell+d_n}$ (namely, multiplication by $X_n^{d_n}$). We are going to consider two additional special cases:

$$\mathbf{B}^{\sigma}_{F,\ell} = \mathbf{A}^{\sigma,\{\varnothing\}}_{F,\ell}, \qquad \mathbf{C}_{F,\ell} = \mathbf{A}^{\varnothing,\mathcal{P}(n)\smallsetminus\{\varnothing\}}_{F,\ell}.$$

Lemma 3.5. *We have*

$$\frac{\mathbf{a}^{\sigma,T}_{F,\ell}}{\mathbf{a}^{\sigma}_{F,\ell}} = \prod_{\sigma\subseteq\tau\in T} \frac{\mathbf{b}^{\tau}_{F,\ell}}{\mathbf{a}^{\tau}_{F,\ell}}.$$

Proof. We may assume that every $\tau \in T$ contains σ. When $T = \varnothing$, both sides equal one. When $T \neq \varnothing$, let $\tau \in T$ be maximal and $T' = T \smallsetminus \{\tau\}$. Let $\mathbf{D}$ be the $\mathfrak{M}^{\sigma}_{\ell} \times \mathfrak{M}^{\sigma}_{\ell}$ matrix such that $\mathfrak{m}\mathbf{D} = \mathfrak{m}\tilde{f}_{\tau\smallsetminus\sigma}$ if $\mathfrak{m} \in \mathfrak{M}^{\tau}_{\ell}$, and $\mathbf{D}\mathfrak{m} = \mathfrak{m}$ otherwise.. As earlier, substituting $X_i^{d_i}$ for f_i we see that $\mathbf{D}$ is invertible. Considering $\mathfrak{M}^{\tau}_{\ell}$ as an initial segment of $\mathfrak{M}^{\sigma}_{\ell}$, we have

$$\mathbf{A}^{\sigma,T}_{F,\ell} = \begin{pmatrix} \mathbf{B}^{\tau}_{F,\ell} & 0 \\ ? & E \end{pmatrix} \mathbf{D}, \qquad \mathbf{A}^{\sigma,T'}_{F,\ell} = \begin{pmatrix} \mathbf{A}^{\tau}_{F,\ell} & 0 \\ ? & E' \end{pmatrix} \mathbf{D}.$$

On the other hand, the bottom parts (rows corresponding to $\mathfrak{m} \notin \mathfrak{M}^{\tau}_{\ell}$) of $\mathbf{A}^{\sigma,T}_{F,\ell}$ and $\mathbf{A}^{\sigma,T'}_{F,\ell}$ are identical, so $E = E'$. We conclude that $\mathbf{a}^{\sigma,T}_{F,\ell} / \mathbf{a}^{\sigma,T'}_{F,\ell} = \mathbf{b}^{\tau}_{F,\ell} / \mathbf{a}^{\tau}_{F,\ell}$, whence follows our assertion by induction. ■

In particular:

$$\frac{\mathbf{a}^{\sigma n}_{F,\ell+d_n}}{\mathbf{a}^{\sigma}_{F,\ell}} = \frac{\mathbf{a}^{\sigma,\mathcal{P}(n)}_{F,\ell}}{\mathbf{a}^{\sigma}_{F,\ell}} = \prod_{\sigma\subseteq\tau\subseteq n} \frac{\mathbf{b}^{\tau}_{F,\ell}}{\mathbf{a}^{\tau}_{F,\ell}}.$$

Applying inclusion/exclusion, we obtain

$$\frac{\mathbf{b}^{\sigma}_{F,\ell}}{\mathbf{a}^{\sigma}_{F,\ell}} = \prod_{\sigma\subseteq\tau\subseteq n} \left(\frac{\mathbf{a}^{\tau n}_{F,\ell+d_n}}{\mathbf{a}^{\tau}_{F,\ell}} \right)^{(-1)^{|\tau\smallsetminus\sigma|}}.$$

Applying Lemma 3.5 for $\mathbf{c}_{F,\ell}$, we get:

$$\frac{\mathbf{c}_{F,\ell}}{\mathbf{a}^{\varnothing}_{F,\ell}} = \frac{\mathbf{a}^{\varnothing}_{F,\ell}}{\mathbf{b}^{\varnothing}_{F,\ell}} \prod_{\sigma\subseteq n} \frac{\mathbf{b}^{\sigma}_{F,\ell}}{\mathbf{a}^{\sigma}_{F,\ell}} = \frac{\mathbf{a}^{\{n\}}_{F,\ell+d_n}}{\mathbf{a}^{\varnothing}_{F,\ell}} \prod_{\sigma\subseteq n} \left(\frac{\mathbf{a}^{\sigma}_{F,\ell}}{\mathbf{a}^{\sigma n}_{F,\ell+d_n}} \right)^{(-1)^{|\sigma|}},$$

i.e.,

$$\frac{\mathbf{c}_{F,\ell}}{\mathbf{a}^{\{n\}}_{F,\ell+d_n}} = \prod_{\sigma\subseteq n} \left(\frac{\mathbf{a}^{\sigma}_{F,\ell}}{\mathbf{a}^{\sigma n}_{F,\ell+d_n}} \right)^{(-1)^{|\sigma|}}. \tag{11}$$

Lemma 3.6. *Assume $\ell \geq \ell_0$ (where, we recall, $\ell_0 = \deg F - n$). Then*

$$\frac{\mathbf{c}_{F,\ell}}{\mathbf{a}^{\{n\}}_{F,\ell+d_n}} = \frac{\mathbf{c}_{F,\ell_0}}{\mathbf{a}^{\{n\}}_{F,\ell_0+d_n}}. \tag{12}$$

In addition, the Macaulay resultant $F^{\wedge}$ divides $\mathbf{c}_{F,\ell}$ in $\mathbf{Z}[T^*]$, and T_n^* does not appear in the quotient $\mathbf{c}_{F,\ell}/F^{\wedge}$.

Proof. Let $\mathfrak{m} \in \mathfrak{M}_\ell$. If $\mathbf{C}_{F,\ell+1} \cdot (\mathfrak{m}X_n) \neq (\mathbf{C}_{F,\ell} \cdot \mathfrak{m})X_n$ then necessarily $\mathbf{C}_{F,\ell+1} \cdot (\mathfrak{m}X_n)$ involves multiplication by f_n but $\mathbf{C}_{F,\ell} \cdot \mathfrak{m}$ does not, i.e., $\rho(\mathfrak{m}X_n) = \{n\}$ and $\rho(\mathfrak{m}) = \varnothing$. The latter is, however, impossible for $\ell \geq \ell_0$, so $\mathbf{C}_{F,\ell+1} \cdot (\mathfrak{m}X_n) = (\mathbf{C}_{F,\ell} \cdot \mathfrak{m})X_n$. On the other hand, if $\mathfrak{m} \in \mathfrak{M}_{\ell+1} \setminus \mathfrak{M}_\ell X_n$, i.e., if X_n does not appear in $\mathfrak{m}$, then $\mathbf{C}_{F,\ell+1} \cdot \mathfrak{m} = \mathbf{A}_{F',\ell+1} \cdot \mathfrak{m} + X_n \cdot ???$. It follows that

$$\mathbf{C}_{F,\ell+1} = \begin{pmatrix} \mathbf{C}_{F,\ell} & ? \\ 0 & \mathbf{A}^{\varnothing}_{F',\ell+1} \end{pmatrix}.$$

Therefore, using (10):

$$\frac{\mathbf{c}_{F,\ell+1}}{\mathbf{a}^{\{n\}}_{F,\ell+1+d_n}} = \frac{\mathbf{c}_{F,\ell}\mathbf{a}^{\varnothing}_{F',\ell+1}}{\mathbf{a}^{\{n\}}_{F,\ell+d_n}\mathbf{a}^{\varnothing}_{F',\ell+1}} = \frac{\mathbf{c}_{F,\ell}}{\mathbf{a}^{\{n\}}_{F,\ell+d_n}}.$$

From this (12) follows.

Let $B = \mathbf{Z}[T^*]/(F^\wedge)$ and $K = \mathrm{Frac}(B)^a$, and let us consider the natural map $\varphi\colon \mathbf{Z}[T^*] \to K$. Let $g_i = \varphi(f_i) \in K[X]$. Since the resultant of $(g_i : i \leq n)$ vanishes, they admit a common zero $x \in K^{n+1} \setminus \{0\}$. Let y be the Veronese image of degree ℓ of x, viewed as a vector indexed by $\mathfrak{M}_\ell$. Since $\ell \geq \ell_0$, we have $\rho(\mathfrak{m}) \neq \varnothing$ for all $\mathfrak{m}$, so each row of $\mathbf{C}_{F,\ell}$ involves multiplication by at least one polynomial f_i (either by f_n, if $\rho(\mathfrak{m}) = \{n\}$, or by at least one other polynomial). Then $y \neq 0$, and $\varphi(\mathbf{C}_{F,\ell}) \cdot y = 0$, so $\varphi(\mathbf{c}_{F,\ell}) = 0$. This proves that $F^\wedge \mid \mathbf{c}_{F,\ell}$.

By construction of $F^\wedge$, we know that $\deg_{T^*_n} F^\wedge = \prod_{i<n} d_i$. For $\mathbf{c}_{F,\ell}$, we count the number of rows in which f_n appears:

$$\begin{aligned}
\deg_{T^*_n} \mathbf{c}_{F,\ell} &= \left| \mathfrak{M}^{\{n\}}_\ell \setminus \bigcup_{\sigma \supsetneq \{n\}} \mathfrak{M}^\sigma_\ell \right| \\
&= \sum_{\sigma \subseteq n} (-1)^{|\sigma|} \, |\mathfrak{M}^{\sigma n}_\ell| \\
&= \sum_{\sigma \subseteq n} (-1)^{|\sigma|} \binom{\ell - d_{\sigma n} + n}{n} \\
&= \sum_{\sigma \subseteq n} (-1)^{|\sigma|} \binom{d_{n \setminus \sigma} + \ell - \ell_0}{n} = \prod_{i<n} d_i.
\end{aligned}$$

(For the last calculation: we have n bags, containing $d_0, \ldots, d_{n-1}$ balls, respectively, as well as a box containing $\ell - \ell_0$ balls, and we choose n balls. By excluding all choices in which balls are not taken from every bag, we obtain the number of possible choices of exactly one ball from each bag.) It follows that T^*_n cannot appear in $\mathbf{c}_{F,\ell}/F^\wedge$. ■

We can now conclude.

Proof of Theorem 3.1. By induction on n. When $n = 0$, our family consists of a single polynomial $f_0 = T^* X_0^{d_0}$, and for every $\ell \geq \ell_0 = d_0$ we have $\mathfrak{M}^{\varnothing}_\ell = \mathfrak{M}^{\{0\}}_\ell = \{X_0^\ell\}$. The matrices $\mathbf{A}^{\varnothing}_{F,\ell}$ and $\mathbf{A}^{\{0\}}_{F,\ell}$ are (T^*) and (1), respectively, so (9) evaluates to T^* which is indeed the Macaulay resultant.

Now let $n > 0$. By the induction hypothesis, whenever $\ell \geq \ell_0 - d_n + 1 = \deg F' - (n-1)$, we have

$$F'^\wedge = \prod_{\sigma \subseteq n} (\mathbf{a}^\sigma_{F',\ell})^{(-1)^{|\sigma|}}.$$

Then, for $\ell \geq \ell_0$:

$$\begin{aligned}
\prod_{\sigma \subseteq n+1} (\mathbf{a}^\sigma_{F,\ell})^{(-1)^{|\sigma|}} &= \prod_{\sigma \subseteq n} \left(\frac{\mathbf{a}^\sigma_{F,\ell}}{\mathbf{a}^{\sigma n}_{F,\ell}} \right)^{(-1)^{|\sigma|}} \\
&= \prod_{\sigma \subseteq n} \left(\frac{\mathbf{a}^\sigma_{F,\ell}}{\mathbf{a}^{\sigma n}_{F,\ell+d_n}} \right)^{(-1)^{|\sigma|}} \prod_{\sigma \subseteq n} \left(\frac{\mathbf{a}^{\sigma n}_{F,\ell+d_n}}{\mathbf{a}^{\sigma n}_{F,\ell}} \right)^{(-1)^{|\sigma|}} \\
&= \frac{\mathbf{c}_{F,\ell}}{\mathbf{a}^{\{n\}}_{F,\ell+d_n}} \prod_{\sigma \subseteq n} \prod_{\ell - d_n < k \leq \ell} \left(\mathbf{a}^\sigma_{F',k} \right)^{(-1)^{|\sigma|}} && \text{by (11) and (10)} \\
&= \frac{\mathbf{c}_{F,\ell_0}}{\mathbf{a}^{\{n\}}_{F,\ell_0+d_n}} (F'^\wedge)^{d_n} && \text{by (12).}
\end{aligned}$$

By the last part of Lemma 3.6, the quotient of $\prod_{\sigma\subseteq n+1}(\mathbf{a}^{\sigma}_{F,\ell})^{(-1)^{|\sigma|}}$ by $F^{\wedge}$ is a rational function in which T^*_n does not appear. By symmetry, no T^*_i can appear there, i.e., $\prod_{\sigma\subseteq n+1}(\mathbf{a}^{\sigma}_{F,\ell})^{(-1)^{|\sigma|}} = tF^{\wedge}$ for some $t \in \mathbf{Z}$. Specialising to $f_i = X_i^{d_i}$ we see that $t = 1$. ■

4. The Vandermonde determinant identity 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 may be missing points for 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 of 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 some "auxiliary" 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. More precisely, we get a multi-set (set with multiplicities) consisting of $n!\binom{m}{n}$ points, and there are some arbitrary choices involved in partitioning it into $n!$ appropriated sets of $\binom{m}{n}$ points each (intersection points plus auxiliary ones).

Let us first consider the case where 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, $\xi \in \mathbf{P}^n$ 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 ξ. In positive characteristic, the usual notion of formal derivative can be a little problematic, and is better replaced with the following finer one.

Definition 4.1. Consider a polynomial in several indeterminates $f \in A[X]$. Add a new set of indeterminates dX (of the same number), 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 $\partial_k \colon A[X] \to A[X]$, or, if we wish to keep dX generic, $\partial_k \colon A[X, dX] \to A[X, dX]$. These 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

$$\partial_k(f+g) = \partial_k f + \partial_k g, \qquad \partial_k(fg) = \sum_{0\leq\ell\leq k} (\partial_\ell f)(\partial_{k-\ell} g), \qquad \partial_k\partial_\ell = \binom{k+\ell}{k}\partial_{k+\ell},$$
$$\partial_0 = \mathrm{id}, \qquad \partial_1 X_i = dX_i, \qquad k > \deg f \Longrightarrow \partial_k f = 0,$$

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

Convention 4.2. Throughout, A denotes some integrally closed integral domain, and dX a tuple of new indeterminates, so the Hasse derivatives are operations $A[X, dX] \to A[X, dX]$ (we notice that $A[dX]$ is again an integrally closed integral domain).

We let $K = \mathrm{Frac}\big(A[dX]\big)$ and $L = K^a$ be the algebraic closure, so essentially everything will happen in L.

All polynomials are homogeneous.

Notation 4.3. For a single polynomial f and $k \leq n+1$ we define

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

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

Remark 4.4. Let $f \in A[X]_d$, and observe that $\partial_d f = f(dX)$. In particular, assuming that $f \neq 0$ (and that dX is a generic tuple), we have $\partial_d f \neq 0$. If $k = d+1$ then $f^{\partial k}$ is a scalar:

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

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 $\partial_{d+1} f \wedge \ldots \wedge \partial_{k-1} f$ to be of degree $(-1)^{k-d-1}(k-d-1)!$, so

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

Lemma 4.5. *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 ($\mathfrak{C}_{\mathbf{P}^n} = \mathfrak{C}_{\mathbf{P}^n}$). 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 4.4, this remains valid even for terms of the form $g^{\partial \ell}$ where $\ell > \deg g$, or $h^{\partial k-\ell}$ where $k - \ell > \deg h$. ∎

Notation 4.6. It will be convenient to extend Notation 4.3 (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 4.7. *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 4.5. Notice that following Remark 4.4, 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 $\bigwedge_i f^{\partial \omega_i} = 1$. ∎

Definition 4.8. 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 set of geometric points $\psi = \{[x_i] : i < N\} \subseteq [f^{\partial n}]$ we have $\partial_n f(x_i) \neq 0$ (since $f^{\partial n+1} \neq 0$), and we define the normalised Veronese matrix

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

namely the matrix whose ith column is the normalised Veronese image $\frac{v_{m-n}(x_i)}{\partial_n f(x_i)}$, which only depends on the geometric point $[x_i]$. This is a square $N \times N$ matrix, whose determinant only depends on the order of points for sign.

We say that ψ is a *bad* subset of $[f^{\partial n}]$ if $\det V_{f,\psi} = 0$. By a *partition* of $[f^{\partial n}]$ we mean a multi-set Ψ of subsets, such that each point belongs to as many $\psi \in \Psi$ as its multiplicity in $[f^{\partial n}]$. A partition into $n!$ subsets, none of which is bad, will be called *good*. We say that $\psi \subseteq [f^{\partial n}]$ is *good* if it is a part of good partition, and that f is *good* if $f^{\partial n+1} \neq 0$ and a good partition exists.

When $m \leq n$, we say that f is *good* if it is a factor of some good polynomial of degree $> n$ (this may not seems to be the most elegant definition, but is quite convenient). In this case, $f^{\partial n+1}$ is an integer (possibly negative) power of $f(dX)$, and $f^{\partial n} \neq 0$. If $m = n$, then $[f^{\partial n}]$ admits a unique good partition into $n!$ singletons, and if $m < n$, then $[f^{\partial n}] = \varnothing$, with a unique good partition into $n!$ empty sets.

By a *specialisation* of $f \in A[X]_m$ we mean a ring morphism $\varphi\colon A \to \overline{A}$. We extend it to $A[X] \to \overline{A}[X]$ in the obvious manner, and let $\overline{f} \in \overline{A}[X]$ denote the image. We extend similarly to other indeterminates such as dX or X^*. By Lemma 2.3, φ can be extended to a specialisation of the set $[f^{\partial n}]$, necessarily into the set $[\overline{f}^{\partial n}]$.

Lemma 4.9. *Let $f \in A[X]_m$, with $m > n$.*

(i) *If f splits and $f^{\partial n+1} \neq 0$, then f is good.*
(ii) *Assume that f specialises to a good polynomial $\overline{f}$, with good partition $\overline{\Psi}$. Then $[f^{\partial n}]$ admits a partition Ψ such that f, Ψ specialise into $\overline{f}, \overline{\Psi}$, and Ψ is necessarily good.*
(iii) *In particular, if f specialises to a good polynomial $\overline{f}$, then f is good, and if $\psi \subseteq [f^{\partial n}]$ specialises to a good subset $\overline{\psi} \subseteq [\overline{f}^{\partial n}]$, then ψ is good.*

Proof. Assume that $f = \prod_{i<m} \lambda_i$ and $f^{\partial n+1} \neq 0$. Then $f^{\partial n} \neq 0$, and $[f^{\partial n}]$ consists of N distinct points $(\xi_j : j < N)$ (all possible intersections of n among the λ_i), each repeated $n!$ times. By Theorem 1.4, $\psi = (\xi_j : j < N)$ is not bad, so $\Psi = \{\psi, \psi, \ldots\}$ ($n!$ times) is a good partition.

Consider now a specialisation $\varphi\colon A \to \overline{A}$ such that $\overline{f} = \varphi(f)$ is good, with good partition $\overline{\Psi}$. Extend φ to $A[dX] \to \overline{A}[dX]$ as the identity on dX, and by Lemma 2.3(iii) we can extend it further to a specialisation $C \to \overline{C}$ where $f^{\partial n}$ splits over C. Since factors of $f^{\partial n}$ are sent to factors of $\overline{f}^{\partial n}$, there is a partition Ψ of $[f^{\partial n}]$ which gets sent to $\overline{\Psi}$.

The last item follows. ■

Definition 4.10. Assume that f and $\psi \subseteq [f^{\partial n}]$ are good, with $\deg f = m > n$. We define a matrix $\Phi_{f,\psi}$ by

$$\Phi^t_{f,\psi} = V_{f,\psi}.$$

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

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

In other words, $\varphi_{f,\psi,\xi}$ is the row of $\Phi_{f,\psi}$ corresponding to ξ. If Ψ is a good partition, we define (up to an undetermined sign) the "small" and the "large" associated determinants:

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

If $m = n$, then the only definition consistent with the case $m > n$ is

$$\mathfrak{d}_{f,\psi} = \partial_n f = f(dX), \qquad \mathfrak{d}_{f,\Psi} = f(dX)^{n!} = f^{\partial n+1}, \qquad \mathfrak{D}_{f,\Psi} = 1.$$

If $m < n$, then $[f^{\partial n}] = \varnothing$ and

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

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 $V_{F,\psi} = V_{f,\psi}$, $\mathfrak{D}_{F,\Psi} = \mathfrak{D}_{f,\Psi}$, and so on.

Convention 4.11. When Ψ is a good partition we shall always enumerate $\psi \in \Psi$ as $\{\xi_{\psi,i} : i < N\}$. We may choose representatives $x_{\psi,i}$ for $\xi_{\psi,i}$ as convenient.

Lemma 4.12. *Let $f \in A[X]_d$ with $d \geq n$ and $g \in A[X]_{m-d}$. Assume that fg is good, and let Ψ 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).*
(ii) *For every $\psi \in \Psi$ (i.e., for every good ψ) we have $|\psi_f| = \binom{d}{n}$, and any $h \in K[X]_{m-n}$ which vanishes on $\psi \smallsetminus \psi_f$ is divisible by g.*
(iii) *The polynomial f is good, and Ψ_f is a good partition of $[f^{\partial n}]$. For every $\psi \in \Psi$ and $\xi \in \psi_f$ we have*

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

Proof. From Lemma 4.5 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 (i).

If $g(x) = 0$ then $\nu_{m-n}(x)$, viewed as a linear form on $K[X]_{m-n}$, factors through $K[X]_{m-n}/(g)$. Therefore $|\psi \smallsetminus \psi_f| \leq \dim K[X]_{m-n}/(g) = N - \binom{d}{n}$, i.e., $|\psi_f| \geq \binom{d}{n}$. On the other hand, Ψ_f is a partition of $[f^{\partial n}]$, so $|\psi_f| = \binom{d}{n}$. Then the set of $\nu_{m-n}(x)$, as x varies in $\psi \smallsetminus \psi_f$, is a dual basis for $K[X]_{m-n}/(g)$, whence (ii).

Let us fix ψ and let $[x] = \xi \in \psi_f$. It follows that $g \mid \varphi_{fg,\psi,\xi}$, say $\varphi_{fg,\psi,\xi} = gh_\xi$ Since $\partial_i f(x) = 0$ for $i < n$ we have $\partial_n(fg)(x) = g(x)\partial_n f(x)$. Therefore,

$$h_\xi(x) = \frac{\varphi_{fg,\psi,\xi}(x)}{g(x)} = \frac{\partial_n(fg)(x)}{g(x)} = \partial_n f(x),$$

and if $\xi \neq [y] \in \psi$, then by the same calculation $h_\xi(y) = 0$. It follows that the matrix whose rows are the polynomials h_ξ is the inverse of $V_{f,\psi}$, whence (iii). ■

Let $n < m$, and let $F = (f_i : i < m)$ be a generic family, with $d_i = \deg f_i$. In particular, by Lemma 4.9, it is a good family, so let ψ be a good set for F. Let $\ell = \deg F - n$.

Let us use the notation $\mathbf{A}^\sigma_{F,\ell}$ of Section 3 (ignoring f_i for $n < i < m$), and similarly $\mathfrak{M}^\sigma_\ell$. For $\xi \in \psi$ we define $\rho(\xi) = \{i \leq n : f_i(\xi) \neq 0\}$, observing that $\rho(\xi)$ can never be empty, since at most n polynomials from F can vanish at ξ.

For $\sigma \subseteq n+1$, let

$$F^\sigma = (f_i : i \in m \smallsetminus \sigma), \qquad f^\sigma = \prod F^\sigma,$$
$$\psi^\sigma = \psi_{F^\sigma} = \psi_{f^\sigma} = \{\xi \in \psi : \rho(\xi) \supseteq \sigma\} = \psi \smallsetminus V(f_\sigma).$$

Let us group coordinates in $\mathfrak{M}^\sigma_\ell$ and ψ^σ by ρ:

$$\widehat{\mathfrak{M}}^\sigma_\ell = \{\mathfrak{m} \in \mathfrak{M}_\ell : \rho(\mathfrak{m}) = \sigma\} = \mathfrak{M}^\sigma_\ell \smallsetminus \bigcup_{\sigma \subsetneq \tau \subseteq n+1} \mathfrak{M}^\tau_\ell,$$
$$\widehat{\psi}^\sigma = \{\xi \in \psi : \rho(\xi) = \sigma\} = \psi^\sigma \smallsetminus \bigcup_{\sigma \subsetneq \tau \subseteq n+1} \psi^\tau.$$

Since $|\mathfrak{M}^\sigma_\ell| = |\psi^\sigma|$, a quick inclusion/exclusion calculation yields that $|\widehat{\mathfrak{M}}^\sigma_\ell| = |\widehat{\psi}^\sigma|$. In particular, $\widehat{\mathfrak{M}}^\varnothing_\ell = \widehat{\psi}^\varnothing = \varnothing$ (neither $\rho(\xi)$ can be empty, as observed earlier, nor $\rho(\mathfrak{m})$, since the total degree ℓ is too large for that).

The matrix $\Phi_{F^\sigma,\psi^\sigma}$ is a square $\psi^\sigma \times \mathfrak{M}_{\ell-d_\sigma}$ matrix, which we identify with $\psi^\sigma \times \mathfrak{M}^\sigma_\ell$ via multiplication of monomials by $\prod_{i\in\sigma} X_i^{d_i}$. Given that F and ψ are fixed, we may denote it more conveniently as Φ^σ. It is invertible, and we define an $\mathfrak{M}^\sigma_\ell \times \psi^\sigma$ matrix B^σ by:

$$B^\sigma \Phi^\sigma = \mathbf{A}^\sigma_{F,\ell}.$$

We denote the $\widehat{\mathfrak{M}}^\sigma_\ell \times \widehat{\psi}^\sigma$ block of B^σ by $\widehat{B}^\sigma$.

Lemma 4.13. (i) *If $\sigma \subseteq \tau \subseteq n+1$ and $\mathfrak{m} \in \mathfrak{M}^\tau_\ell \subseteq \mathfrak{M}^\sigma_\ell$, then the $\mathfrak{m}$th row of B^σ is the extension by zeros of the $\mathfrak{m}$th row of B^τ.*

(ii) *If $\sigma \subseteq \tau \subseteq n+1$, then the $\widehat{\mathfrak{M}}^\tau_\ell \times \widehat{\psi}^\tau$ block of B^σ is $\widehat{B}^\tau$. If, on the other hand, $\sigma \subseteq \pi \subseteq n+1$ but $\tau \nsubseteq \pi$, then the $\widehat{\mathfrak{M}}^\tau_\ell \times \widehat{\psi}^\pi$ block of B^σ vanishes.*

(iii) *We have*

$$\det B^\sigma = \prod_{\sigma \subseteq \tau \subseteq n+1} \det \widehat{B}^\tau.$$

Proof. Let us denote the polynomial $\varphi_{F,\psi,\xi}$ by φ_ξ. By Lemma 4.12(iii), the row of Φ^σ corresponding to $\xi \in \psi^\sigma$, is $\frac{\varphi_\xi}{\tilde{f}_\sigma}$. If $(\beta_\xi : \xi \in \psi^\tau)$ is the $\mathfrak{m}$th row of B^τ, then:

$$\mathfrak{m}\tilde{f}_{\rho(\mathfrak{m})\smallsetminus\tau} = \sum_{\xi\in\psi^\tau} \beta_\xi \frac{\varphi_\xi}{\tilde{f}_\tau} \qquad \Longrightarrow \qquad \mathfrak{m}\tilde{f}_{\rho(\mathfrak{m})\smallsetminus\sigma} = \sum_{\xi\in\psi^\tau} \beta_\xi \frac{\varphi_\xi}{\tilde{f}_\sigma}.$$

This proves (i) and (ii). The latter tells us that B^σ is block-triangular, so its determinant is the product of the determinants of blocks along the diagonal, whence (iii). ■

Lemma 4.14. *With out hypotheses, we have*

$$\prod_{\sigma \subseteq n+1} (\det \Phi^\sigma)^{(-1)^{|\sigma|}} = f_0 \wedge \ldots \wedge f_n.$$

In particular, this alternating product of determinants does not depend on ψ.

Proof. We have

$$\prod_{\sigma \subseteq n+1} (\det \Phi^\sigma)^{(-1)^{|\sigma|}} = \prod_{\sigma \subseteq n+1} (\det \mathbf{A}^\sigma_{F,\ell})^{(-1)^{|\sigma|}},$$

since $\widehat{B}^\varnothing$ is the empty matrix, and all other determinants of $\widehat{B}^\sigma$ cancel each other. Now apply Theorem 3.1. ■

Given any function $\chi(F)$ applied to finite sets of polynomials, with non-zero values in a field (or in an integral domain, embedded in its field of fractions) define

$$\widehat{\chi}(F) = \prod_{G \subseteq F} \chi(G)^{(-1)^{|F \setminus G|}}, \qquad \text{so} \qquad \chi(F) = \prod_{G \subseteq F} \widehat{\chi}(G).$$

This inclusion/exclusion stratification applies of course for any maps from finite sets into an Ableian (in our case, multiplicative) group. We apply this notation in particular to

$$\widehat{F^{\partial k}} = \prod_{G \subseteq F} (G^{\partial k})^{(-1)^{|F \setminus G|}}, \qquad \widehat{\mathfrak{d}}_{F,\psi} = \prod_{G \subseteq F} (\mathfrak{d}_{G,\psi_G})^{(-1)^{|F \setminus G|}}, \qquad \widehat{\mathfrak{D}}_{F,\Psi} = \prod_{G \subseteq F} (\mathfrak{D}_{G,\Psi_G})^{(-1)^{|F \setminus G|}}.$$

Theorem 4.15 (Vandermonde identity and dual identity for hypersurfaces)**.** *Let F be a good family of polynomials, Ψ a good partition of $[F^{\partial n}]$, and ψ a good subset of $[F^{\partial n}]$. Then*

$$\mathfrak{D}_{F,\Psi} = \prod_{H \in \binom{F}{n+1}} (H^\wedge)^{n!n} \prod_{G \subseteq F,\ |G| \leq n} \widehat{\mathfrak{D}}_{G,\Psi}, \tag{13}$$

$$\mathfrak{d}_{F,\psi} = \prod_{H \in \binom{F}{n+1}} H^\wedge \prod_{G \subseteq F,\ |G| \leq n} \widehat{\mathfrak{d}}_{G,\psi}. \tag{14}$$

Proof. It will suffice to prove that, for a generic family F of size $m > n$:

$$\begin{aligned} m &= n+1 && \Longrightarrow && \widehat{F^{\partial n+1}} = (F^\wedge)^{(n+1)!}, && \widehat{\mathfrak{D}}_{F,\Psi} = (F^\wedge)^{n!n}, && \widehat{\mathfrak{d}}_{F,\psi} = F^\wedge, \\ m &> n+1 && \Longrightarrow && \widehat{F^{\partial n+1}} = 1, && \widehat{\mathfrak{D}}_{F,\Psi} = 1, && \widehat{\mathfrak{d}}_{F,\psi} = 1. \end{aligned}$$

For $\widehat{F^{\partial n+1}}$, this is an easy exclusion-inclusion calculation (using Lemma 4.7). For $\widehat{\mathfrak{d}}$, assume that $|F| = m \geq n+1$. Grouping the factors of the alternating product $\widehat{\mathfrak{d}}_{F,\psi}$ by the set $S = \{i > n : f_i \in G\}$, each group evaluates by Lemma 4.14 to $(f_0 \wedge \ldots \wedge f_n)^{(-1)^{m-n-1-|S|}}$, and both cases follow. The case of $\widehat{\mathfrak{D}}$ follows, since $F^{\partial n+1} = \mathfrak{D}_{F,\Psi} \prod_{\psi \in \Psi} \mathfrak{d}_{F,\psi}$. ■

Notice that if $F = (\lambda_i : i < m)$ is a family of linear forms, then the second factor in either (13) or (14) is a power of $\prod_i \lambda_i(dX)$. In particular, the second factor cannot vanish if no λ_i does. There exists a unique good set ψ, consisting of all $\binom{m}{n}$ intersection points, and a unique good partition $\Psi = \{\psi, \psi, \ldots\}$ of $[F^{\partial n}]$. If $x = G^\wedge$ for some $G \in \binom{F}{n}$, then $\varphi_{F,\psi,[x]} = \prod(F \setminus G) \prod G(dX)$. In other words, the matrix $\Phi_{F,\psi}$ is the same as in the left hand side of (5), up to multiplying by some $\lambda_i(dX)$, so (14) specialises to Corollary 1.5. We therefore consider (14) to be the dual Vandermonde identity for hypersurfaces. Similarly, one can check that (13) specialises in this case to the $n!$ power of Theorem 1.4, so, up to a root of unity, (13) is the (plain) Vandermonde identity for hypersurfaces.

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.

[Mac02] F. S. Macaulay, *Some Formulæ in Elimination*, Proceedings of the London Mathematical Society **S1-35** (1902), no. 1, 3–27, doi:10.1112/plms/s1-35.1.3.

Itaï Ben Yaacov, Université de Lyon, 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/