

Lecture Notes 4.

MA 722

1 Bézout's Theorem

We follow the approach of [BCSS98, Chapter 10].

Bézout's theorem is the n -dimensional generalization of the univariate Fundamental Theorem of Algebra (FTA). Before we state the theorem, we need to define projective spaces. First we give motivations by revisiting the univariate case.

1.1 Motivation: FTA Revisited

Let $f(z) = az^2 + bz + c$. Then f has two roots in \mathbb{C} , counted with multiplicity, which are

$$\xi_1 = \frac{-b + \sqrt{b^2 - 4ac}}{2a} \quad \text{and} \quad \xi_2 = \frac{-b - \sqrt{b^2 - 4ac}}{2a}.$$

What happens when $a \rightarrow 0$? It is easy to check that

$$\lim_{a \rightarrow 0} \xi_1 = -\frac{c}{b} \quad \text{and} \quad \lim_{a \rightarrow 0^\pm} \xi_2 = \pm\infty.$$

In other word, ξ_2 “escapes” to infinity. In order to make the roots continuous functions of the coefficients, we will “compactify” \mathbb{C} , by introducing the *projective space* denoted by $\mathbb{P}_{\mathbb{C}}^1$ or by $\mathbb{P}(\mathbb{C}^2)$. There are several ways to define $\mathbb{P}_{\mathbb{C}}^1$. For example,

$$\mathbb{P}_{\mathbb{C}}^1 := \{L \subset \mathbb{C}^2 \mid L \text{ is a line through the origin}\}$$

or by the factor set

$$\mathbb{P}_{\mathbb{C}}^1 := \frac{\mathbb{C}^2 - \{0\}}{\{(\zeta, \mu) - (\lambda\zeta, \lambda\mu) \mid \zeta, \mu, \lambda \in \mathbb{C}, (\zeta, \mu) \neq 0, \lambda \neq 0\}}.$$

Usually the points $L \in \mathbb{P}_{\mathbb{C}}^1$ are denoted by $(\zeta : \mu)$ where $(\zeta, \mu) \neq 0$ is any point on the line L . Then we can associate the points $(\zeta : 1)$ with \mathbb{C} and the

point $(1 : 0)$ with infinity. Informally, a sequence in \mathbb{C} converging to infinity will correspond to a sequence in $\mathbb{P}_{\mathbb{C}}^1$ with the limit $(1 : 0)$.

In order to make polynomials well defined on the projective space, we need to *homogenize* them. For $f = a_d z^d + \dots + a_0$ we define its homogenization

$$f^h(z, w) := a_d z^d + a_{d-1} z^{d-1} w + \dots + a_1 z w^{d-1} + a_0 w^d.$$

Then $f^h(\zeta, \mu) = 0$ if and only if $f^h(\lambda\zeta, \lambda\mu) = 0$ for all $\lambda \neq 0$, thus roots of homogeneous polynomials are points in $\mathbb{P}_{\mathbb{C}}^1$.

Roots of f and f^h are closely related. On one hand, if $f(\xi) = 0$ for some $\xi \in \mathbb{C}$ then $f^h(\xi, 1) = 0$. On the other hand, if $f^h(\zeta, \mu) = 0$, then we have two cases:

- (1) if $\mu \neq 0$ then $f(\frac{\zeta}{\mu}) = 0$.
- (2) if $\mu = 0$ then $a_d = 0$, and the root “escaped to infinity”.

In order to state a more sophisticated version of the FTA, we need to define multiplicity. The following simple definition only works in the univariate case, however we will define multiplicity more generally in Theorem 1.11.

Definition 1.1. We say that a root $(\zeta : \mu) \in \mathbb{P}_{\mathbb{C}}^1$ of f^h has *multiplicity* m if

$$f^h(z, w) = (\mu z - \zeta w)^m g^h(z, w)$$

and $g^h(\zeta, \mu) \neq 0$.

Theorem 1.2 (FTA version 2.). *Let $f^h(z, w)$ be a non-zero homogeneous polynomial of degree d . Then f^h has d roots in $\mathbb{P}_{\mathbb{C}}^1$, counted with multiplicity.*

1.2 n -Dimensional Projective Space

Definition 1.3. The n -dimensional projective space, denoted by $\mathbb{P}(\mathbb{C}^{n+1})$ or $\mathbb{P}_{\mathbb{C}}^n$, is the set of one dimensional subspaces of \mathbb{C}^{n+1} (i.e. lines through the origin). We denote the point $L \in \mathbb{P}(\mathbb{C}^{n+1})$ by $(x_0 : \dots : x_n)$, where $(x_0, \dots, x_n) \neq 0 \in \mathbb{C}^{n+1}$ is any point on the line L . Similarly, for any vector space W , we can define $\mathbb{P}(W)$ the projective space of dimension $\dim(W) - 1$.

First note that $\mathbb{P}(\mathbb{C}^{n+1})$ is not a vector space: addition of points is not well defined. We can study the structure of $\mathbb{P}(\mathbb{C}^{n+1})$ by looking at its tangent spaces and by defining metrics on it.

Just as in the univariate case, \mathbb{C}^n can be embedded into $\mathbb{P}(\mathbb{C}^{n+1})$ by the map

$$(\xi_1, \dots, \xi_n) \mapsto (1 : \xi_1 : \dots : \xi_n).$$

The set of points in $\mathbb{P}(\mathbb{C}^{n+1}) - \mathbb{C}^n = \{(0 : \xi_1 : \dots : \xi_n)\}$ are the “points at infinity”, and can be considered as $\mathbb{P}_{\mathbb{C}}^{n-1}$.

We can also define the map

$$Q : \mathbb{C}^{n+1} \rightarrow \mathbb{P}(\mathbb{C}^{n+1})$$

where $Q(w)$ is the point $L \in \mathbb{P}(\mathbb{C}^{n+1})$ such that w lies on the line $L \subset \mathbb{C}^{n+1}$. Note that $Q^{-1}(L)$ is the line $L \subset \mathbb{C}^{n+1}$.

Let

$$S_1 := \{w \in \mathbb{C}^{n+1} : \|w\| = 1\}$$

be the unit sphere. Here $\|w\|^2 = \sum_{i=0}^n w_i \bar{w}_i$. We define the restriction of Q to S_1 by

$$\rho : S_1 \rightarrow \mathbb{P}(\mathbb{C}^{n+1}), \quad w \mapsto L \text{ if } w \in L.$$

Here

$$\rho^{-1}(L) = S_1 \cap L = \{tw \mid t \in \mathbb{C}, |t| = 1\}$$

is a unit circle in \mathbb{C} – our intuition from \mathbb{R}^2 does not work here!

1.3 Homogeneous Systems

Define the vector space

$$\mathcal{H}_d := \{f \in \mathbb{C}[x_0, \dots, x_n] \mid f \text{ is homogeneous of degree } d\}.$$

If $f \in \mathcal{H}_d$ then $f(\xi_0, \dots, \xi_n) = 0$ if and only if $f(\lambda\xi_0, \dots, \lambda\xi_n) = 0$ for all $\lambda \neq 0$ in \mathbb{C} . Thus, the roots of polynomials in \mathcal{H}_d are elements of $\mathbb{P}(\mathbb{C}^{n+1})$.

Let $(d) := (d_1, \dots, d_k) \in \mathbb{N}^k$ and define the space of polynomial systems

$$\mathcal{H}_{(d)} := \mathcal{H}_{d_1} \times \dots \times \mathcal{H}_{d_k} = \{f = (f_1, \dots, f_k) \mid f_i \text{ is homogeneous of degree } d_i\}.$$

Definition 1.4. The *solution variety* is defined by

$$V := \{(f, x) \in (\mathcal{H}_{(d)} - \{0\}) \times \mathbb{P}(\mathbb{C}^{n+1}) \mid f(x) = 0\}.$$

Theorem 1.5. Let $(d) := (d_1, \dots, d_k) \in \mathbb{N}^k$. Then the solution variety V is a smooth and connected subvariety of $\mathcal{H}_{(d)} \times \mathbb{P}(\mathbb{C}^{n+1})$ of codimension k .

Proof. Here we give an outline of the proof for

$$V' := \{(f, x) \in (\mathcal{H}_{(d)} - \{0\}) \times (\mathbb{C}^{n+1} - \{0\}) \mid f(x) = 0\}$$

instead of V .

To prove that V' is smooth and has codimension k in $\mathcal{H}_{(d)} \times \mathbb{C}^{n+1}$ we first note that the tangent space of V' at $(f, x) \in V'$ is given by

$$T_{(f,x)} = \{(h, w) \in \mathcal{H}_{(d)} \times \mathbb{C}^{n+1} \mid h(x) + Df(x)w = 0\},$$

where $Df(x)$ is the Jacobian matrix of f . Then $\text{codim } T_{(f,x)} = k$, since the linear map

$$\phi : \mathcal{H}_{(d)} \times \mathbb{C}^{n+1} \rightarrow \mathbb{C}^k, \quad (h, w) \mapsto h(x) + Df(x)w$$

is surjective, and $T_{(f,x)} = \ker(\phi)$.

To prove that V' is connected, for any fixed $x \in \mathbb{C}^{n+1} - \{0\}$, we define the set

$$V'_x := \{(f, x) \in V'\}.$$

Since V'_x is a vector space, it is connected. Now let $x, x' \in \mathbb{C}^{n+1} - \{0\}$. We will connect V'_x and $V'_{x'}$ by a path. Fix $(f, x) \in V'_x$ and define the path in V' by

$$(f_t, x_t) := (f - f(p(t)), p(t)) \quad \text{for } 0 \leq t \leq 1$$

where $p(t) : [0, 1] \rightarrow \mathbb{C}^{n+1} - \{0\}$ is any path connecting x and x' in $\mathbb{C}^{n+1} - \{0\}$ with $p(0) = x$ and $p(1) = x'$. Thus, we get a path $P : [0, 1] \rightarrow V'$ with $P(t) = (f_t, x_t)$ such that $P(0) = (f_0, x_0) = (f, x) \in V'_x$ and $P(1) = (f_1, x_1) = (f', x') \in V'_{x'}$. \square

From now on we will assume that $k = n$, i.e. $\mathcal{H}_{(d)} = \mathcal{H}_{d_1} \times \cdots \times \mathcal{H}_{d_n}$ and $f = (f_1, \dots, f_n)$.

Definition 1.6. The *critical variety* $\Sigma' \subset V$ is defined

$$\Sigma' := \{(f, x) \mid f(x) = 0, \text{ and } \text{rank}(Df(x)) < n\}$$

where $Df(x)$ is the Jacobian matrix of f . Define the projection

$$\pi_1 : \mathcal{H}_{(d)} \times \mathbb{P}(\mathbb{C}^{n+1}) \rightarrow \mathcal{H}_{(d)}.$$

The *discriminant variety* is defined

$$\Sigma := \pi_1(\Sigma') \subset \mathcal{H}_{(d)}.$$

Lemma 1.7. Σ' and Σ are Zariski closed subvarieties of V and $\mathcal{H}_{(d)}$, respectively, i.e. they are defined by polynomial equations.

Proof. Σ' is Zariski closed, since it is defined by $f(x) = 0$ and $\det(M) = 0$ for all $n \times n$ submatrices M of $Df(x)$. These are algebraic equations in the coefficients of f and in the coordinates of x .

Σ is Zariski closed because of the *Projective Elimination Theorem*, which states that for any projection

$$\pi : \mathbb{C}^m \times \mathbb{P}(\mathbb{C}^{n+1}) \rightarrow \mathbb{C}^m$$

if $Z \subset \mathbb{C}^m \times \mathbb{P}(\mathbb{C}^{n+1})$ is Zariski closed then $\pi(Z)$ is also Zariski closed. (We will not prove this theorem, see the proof in [CLO98].) \square

Remark 1.8. Note that the previous lemma and the Main Theorem of Elimination Theory is not true if we change $\mathbb{P}(\mathbb{C}^{n+1})$ to \mathbb{C}^n . For example, consider $\pi_1 : \mathcal{H}_2 \times \mathbb{C} \rightarrow \mathcal{H}_2$, and

$$\Sigma' = \{(a_0, a_1, a_2, x) \mid a_2x^2 + a_1x + a_0 = 2a_2x + a_1 = 0\}.$$

Clearly, Σ' is Zariski closed, but

$$\pi_1(\Sigma') = \Sigma - \{a_2 = 0\}$$

is not Zariski closed. Here $\Sigma = \{(a_0, a_1, a_2) \mid a_1^2 - 4a_2a_0\}$ is the discriminant variety if we use $\mathbb{P}(\mathbb{C}^2)$.

Corollary 1.9. Let $B \subset \mathcal{H}_{(d)} - \{0\}$ be an open ball, i.e.

$$B = B(f, \delta) = \{h \in \mathcal{H}_{(d)} - \{0\} \mid \|h - f\| < \delta\}$$

for some $f \in \mathcal{H}_{(d)} - \{0\}$ and $\delta > 0$. Then $B - \Sigma$ is connected.

Proof. Note first that the corollary is counter intuitive, since it is not true in \mathbb{R}^2 .

We will prove the corollary for any ball $B \subset \mathbb{C}^m$ and for any Zariski closed subset $\Sigma \subset \mathbb{C}^m$. Let $L := \{tx \mid t \in \mathbb{C}\}$ be a line in \mathbb{C}^m for a fixed $x \in B$. Since $L \cong \mathbb{C}$, therefore $L \cap \Sigma$ is a finite set, thus $L \cap B \cap \Sigma$ is also a finite set. Thus $(L \cap B) - \Sigma$ is a disc in \mathbb{C} minus a finite set, which is connected. \square

Now we have all the ingredients to prove Bézout's theorem, which will be stated in the next subsection.

1.4 Bézout's Theorem

We give two versions of the theorem.

Theorem 1.10 (Bézout's Theorem). *Let $(d) = (d_1, \dots, d_n)$ and $f \in \mathcal{H}_{(d)} - \Sigma - \{0\}$. Define*

$$\mathcal{D} := \prod_{i=1}^n d_i,$$

the so called Bézout's number. Then f has \mathcal{D} zeroes in $\mathbb{P}(\mathbb{C}^{n+1})$.

Proof. Since $\mathcal{H}_{(d)} - \Sigma - \{0\}$ is connected by Corollary 1.9, the Inverse Function Theorem (IFT) implies that any two systems f and \tilde{f} in $\mathcal{H}_{(d)} - \Sigma - \{0\}$ have the same number of roots. More precisely, consider the projection $\pi : V - \Sigma' \rightarrow \mathcal{H}_{(d)} - \Sigma$. For any path $\{f_t : t \in [0, 1]\} \subset \mathcal{H}_{(d)} - \Sigma$ connecting f and \tilde{f} , by IFT there exist \mathcal{D} distinct paths $\{(f_t, \xi_{i,t}) : t \in [0, 1]\} \subset V - \Sigma'$ for $i = 1, \dots, \mathcal{D}$, such that $\xi_{1,0}, \dots, \xi_{\mathcal{D},0}$ are the distinct roots of f and $\xi_{1,1}, \dots, \xi_{\mathcal{D},1}$ are the roots of \tilde{f} . Moreover, the system

$$f^* := (x_1^{d_1} - x_0^{d_1}, x_2^{d_2} - x_0^{d_2}, \dots, x_n^{d_n} - x_0^{d_n})$$

is in $\mathcal{H}_{(d)} - \Sigma - \{0\}$ and has \mathcal{D} roots. □

The second version of Bézout's Theorem considers systems in Σ as well. Note that systems in Σ not only have roots with multiplicities, but may also have infinitely many roots as well. The theorem deals with this situation, and also defines a notion of *multiplicity* which works in the most general case.

Theorem 1.11 (Bézout's Theorem - Extended to Σ). *Let $f \in \mathcal{H}_{(d)} - \{0\}$, and \mathcal{D} as in Theorem 1.10. Let $Z_j := Z_j(f)$ for $j = 1, \dots, k$ be the connected components of the set of zeroes of f in $\mathbb{P}(\mathbb{C}^{n+1})$. Then we can assign a multiplicity $m(Z_j)$ to each Z_j which satisfies the following properties:*

- (a) $m(Z_j) \geq 1$;
- (b) $\sum_{j=1}^k m(Z_j) = \mathcal{D}$;
- (c) $m(Z_j) = 1$ if Z_j is a non-degenerate isolated zero, i.e. if $Z_j = \{x\}$ and $(f, x) \in V - \Sigma'$;

(d) There exist $U_j \subset \mathbb{P}(\mathbb{C}^{n+1})$ open neighborhood of Z_j for $j = 1, \dots, k$, and an open ball $B \subset \mathcal{H}_{(d)} - \{0\}$ around f such that for any $g \in B$, the set of roots $Z(g)$ of g satisfies $Z(g) \subset \bigcup_{i=1}^k U_j$, and for all $j = 1, \dots, k$

$$\sum_{Z_t(g) \subseteq U_j} m(Z_t(g)) = m(Z_j).$$

Proof. First we prove that $Z(f) \neq \emptyset$. Since $\mathcal{H}_{(d)} - \Sigma - \{0\}$ is everywhere dense, there exist a sequence $f^{(1)}, f^{(2)}, \dots$ in $\mathcal{H}_{(d)} - \Sigma - \{0\}$ such that $\lim_{i \rightarrow \infty} f^{(i)} = f$. By the Inverse Function Theorem and the compactness of $\mathbb{P}(\mathbb{C}^{n+1})$ we can define $(f^{(i)}, \xi^{(i)}) \in V - \Sigma'$ and a limit point $(f, \xi) \in V$. Thus, $\xi \in Z(f)$.

Next we define the multiplicity of the connected components Z_j . Let U_j be disjoint open neighborhoods of Z_j for $j = 1, \dots, k$. By the continuity of the roots in terms of the coefficients, there exists a ball B around f such that for any $g \in B$ $Z(g) \subset \bigcup_{j=1}^k U_j$. Fix $g \in B - \Sigma$ and define $m(Z_j)$ to be the number of zeroes of g in U_j . This definition is independent of the choice of $g \in B - \Sigma$, since $B - \Sigma$ is connected by Corollary 1.9. Also, the properties (b), (c) and (d) of the multiplicity follow directly from the definition.

To prove (a), we define

$$V_j := \{(g, z) \in V \mid g \in B, z \in U_j\}$$

for $j = 1, \dots, k$. Since $\{f\} \times Z_j \subset V_j$, V_j is a non-empty open subset of V . Therefore, $V_j \not\subseteq \Sigma'$, since Σ' is Zariski closed. Thus, there exists $(g_j, z) \in V_j - \Sigma'$ such that $g_j \in B - \Sigma$, $z \in U_j$ and $g_j(z) = 0$. Therefore $m(Z_j) \geq 1$. \square

2 Multipolynomial Resultants

We follow the approach of [CLO98, Chapter 3].

Given $n + 1$ homogeneous polynomials

$$f_0(x_0, \dots, x_n), \dots, f_n(x_0, \dots, x_n) \in \mathbb{C}[x_0, \dots, x_n]$$

in $n + 1$ variables of total degrees d_0, \dots, d_n . We are considering their common roots in $\mathbb{C}^{n+1} - \{0\}$, or equivalently in the projective space $\mathbb{P}_{\mathbb{C}}^n$. Since (f_0, \dots, f_n) forms an over-constrained system of equations over $\mathbb{P}_{\mathbb{C}}^n$, usually no solution exists. As we will see later, the set of systems which do have

common roots in $\mathbb{P}_{\mathbb{C}}^n$ form a co-dimension one hypersurface in the vector space

$$\mathcal{H}_{(d)} = \{(f_0, \dots, f_n) \in \mathbb{C}[x_0, \dots, x_n]^n : \deg(f_i) = d_i\}$$

where $(d) = (d_0, \dots, d_n)$.

Example 2.1. For $d_0 = \dots = d_n = 1$ we have the homogeneous linear system

$$\begin{aligned} f_0 &= c_{0,0}x_0 + \dots + c_{0,n}x_n \\ &\vdots \\ f_n &= c_{n,0}x_0 + \dots + c_{n,n}x_n. \end{aligned}$$

This system has a solution in $\mathbb{C}^{n+1} - \{0\}$ if and only if

$$\det(c_{i,j}) = 0.$$

This is clearly a one co-dimensional hypersurface in $\mathcal{H}_{(1,\dots,1)}$.

In the general case, in order to define the equation of the hypersurface defining the systems with common roots, we first have to introduce “universal polynomials” of given degree.

Definition 2.2. The polynomials

$$F_i = \sum_{|\alpha|=d_i} u_{i,\alpha} x^\alpha \quad i = 0, \dots, n,$$

with coefficients $u_{i,\alpha}$ which are parameters, are called *universal polynomials*. Here for $\alpha = (\alpha_0, \dots, \alpha_n) \in \mathbb{N}^{n+1}$ we denote

$$|\alpha| = \sum_{i=0}^n \alpha_i \quad \text{and} \quad x^\alpha = x_0^{\alpha_0} \dots x_n^{\alpha_n}.$$

Note that

$$F_i \in \mathbb{Z}[u_{i,\alpha} : |\alpha| = d_i][x_0, \dots, x_n].$$

For any substitution of the parameters $u_{i,\alpha}$ by complex numbers, the resulting homogeneous polynomials $\tilde{F}_0, \dots, \tilde{F}_n \in \mathcal{H}_{(d)}$ are called the *specialization* of the universal polynomials.

Theorem 2.3 (Existence of Resultant). *Fix $(d) = (d_0, \dots, d_n)$. Then there exists a unique polynomial*

$$\text{Res}_{(d)} \in \mathbb{Z}[u_{i,\alpha} : i = 0, \dots, n]$$

with the following properties:

- (i) *If $\tilde{F}_0, \dots, \tilde{F}_n \in \mathbb{C}[x_0, \dots, x_n]$ are specializations of the universal polynomials of degrees d_0, \dots, d_n , then they have a common root in $\mathbb{P}_{\mathbb{C}}^n$ if and only if*

$$\text{Res}_{(d)}(\tilde{F}_0, \dots, \tilde{F}_n) = 0.$$

- (ii) $\text{Res}_{(d)}(x_0^{d_0}, \dots, x_n^{d_n}) = 1$.

- (iii) $\text{Res}_{(d)}$ is irreducible in $\mathbb{C}[u_{i,\alpha}]$.

Outline of Proof. Let $V \subset \mathcal{H}_{(d)} \times \mathbb{P}_{\mathbb{C}}^n$ be the solution variety, i.e.

$$V = \{(\tilde{F}, x) : \tilde{F}(x) = 0\}.$$

Let $\pi : \mathcal{H}_{(d)} \times \mathbb{P}_{\mathbb{C}}^n \rightarrow \mathcal{H}_{(d)}$ be the projection, so that

$$\pi(V) = \{\tilde{F} = (\tilde{F}_0, \dots, \tilde{F}_n) : \exists x \in \mathbb{P}_{\mathbb{C}}^n, \tilde{F}(x) = 0\} \subset \mathcal{H}_{(d)}.$$

What we are going to prove is that $\pi(V)$ is defined by a single irreducible equation $\text{Res}_{(d)} = 0$. To prove this we need to show that $\pi(V)$ is Zariski closed (i.e. defined by polynomials), it has co-dimension one in $\mathcal{H}_{(d)}$, and it is irreducible.

To prove that $\pi(V)$ is Zariski closed, we use the *Projective Elimination Theorem* in [CLO98], which states that for a projection

$$\pi : \mathbb{C}^m \times \mathbb{P}_{\mathbb{C}}^n \rightarrow \mathbb{C}^m$$

if $Z \subset \mathbb{C}^m \times \mathbb{P}_{\mathbb{C}}^n$ is Zariski closed then $\pi(Z)$ is also Zariski closed. We will not prove this theorem.

To prove that $\pi(V)$ has codimension one in $\mathcal{H}_{(d)}$, denote by $M := \dim_{\mathbb{C}} \mathcal{H}_{(d)}$. Then $\dim_{\mathbb{C}} \mathcal{H}_{(d)} \times \mathbb{P}_{\mathbb{C}}^n = M + n$. Since V is defined by the $n + 1$ equation $F_0, \dots, F_n \in \mathbb{Z}[u_{i,\alpha}][x_0, \dots, x_n]$, and each equation drops the dimension by one, we have that

$$\dim_{\mathbb{C}} V = M + n - (n + 1) = M - 1.$$

Note that $\pi|_V$ is one-to-one almost everywhere on V , except a lower dimensional subvariety, since if $\tilde{F}_0, \dots, \tilde{F}_n$ do have a common root in $\mathbb{P}_{\mathbb{C}}^n$, it is “usually” unique. Therefore $\pi|_V$ has also dimension $M - 1$, i.e. it has co-dimension one.

To prove that $\pi(V)$ is irreducible, we first show that V is irreducible. This follows from the fact that using the second projection $\tilde{\pi} : \mathcal{H}_{(d)} \times \mathbb{P}_{\mathbb{C}}^n \rightarrow \mathbb{P}_{\mathbb{C}}^n$, the restriction $\tilde{\pi}|_V : V \rightarrow \mathbb{P}_{\mathbb{C}}^n$ is surjective and all inverse images of points are linear subspaces, so they are irreducible. This implies (without proof here) that V is an irreducible variety. Then a standard argument shows that $\pi(V)$ is also irreducible.

The uniqueness of $\text{Res}_{(d)}$ follows from properties (ii) and (iii). \square

Definition 2.4. $\text{Res}_{(d)}(F_0, \dots, F_n) \in \mathbb{Z}[u_{i,\alpha}]$ is called the *projective resultant* for degrees $(d) = (d_0, \dots, d_n)$.

We give two examples. The first one is the $n = 1$ case, and we give the well-known Sylvester matrix construction, and also the Bézout matrix construction for the resultant.

Example 2.5. Let

$$\begin{aligned} F_0 &:= u_{0,0}x_0^{d_0} + u_{0,1}x_0^{d_0-1}x_1 + \dots + u_{0,d_0}x_1^{d_0} \\ F_1 &:= u_{1,0}x_0^{d_1} + u_{1,1}x_0^{d_1-1}x_1 + \dots + u_{1,d_1}x_1^{d_1} \end{aligned}$$

be the universal polynomials for $n = 1$ of degrees $(d) = (d_0, d_1)$. To compute the projective resultant $\text{Res}_{(d_0, d_1)}$ we define a matrix called the *Sylvester matrix*, such that its determinant will be the resultant.

Denote by

$$\mathcal{H}_d := \{f \in \mathbb{C}[x_0, x_1] : f \text{ homogeneous, } \deg(f) = d\}$$

For a specialization \tilde{F}_0, \tilde{F}_1 , the Sylvester matrix $S(\tilde{F}_0, \tilde{F}_1)$ is the transpose of the matrix of the linear map

$$\begin{aligned} \text{syl}_{\tilde{F}_0, \tilde{F}_1} : \mathcal{H}_{d_1-1} \times \mathcal{H}_{d_0-1} &\rightarrow \mathcal{H}_{d_0+d_1-1} \\ (p, q) &\mapsto p\tilde{F}_0 + q\tilde{F}_1 \end{aligned}$$

written in the monomial basis $\{x_0^d, x_0^{d-1}x_1, \dots, x_1^d\}$ of \mathcal{H}_d . In other words, for the universal polynomials F_0, F_1 the Sylvester matrix $S(F_0, F_1)$ has rows corresponding to the coefficients of the polynomials

$$x_0^{d_1-1}F_0, x_0^{d_1-2}x_1F_0, \dots, x_1^{d_1-1}F_0, x_0^{d_0-1}F_1, x_0^{d_0-2}x_1F_1, \dots, x_1^{d_0-1}F_1$$

and in matrix form we get the following $(d_0 + d_1) \times (d_0 + d_1)$ matrix:

$$S(F_0, F_1) = \begin{vmatrix} u_{0,0} & \dots & u_{0,d_0} & & & \\ & & \ddots & & \ddots & \\ & & & u_{0,0} & \dots & u_{0,d_0} \\ u_{1,0} & \dots & u_{1,d_1} & & & \\ & & \ddots & & \ddots & \\ & & & u_{1,0} & \dots & u_{1,d_1} \end{vmatrix} \begin{matrix} d_1 \\ \\ \\ d_0 \\ \\ \end{matrix}$$

Clearly, if a specialization \tilde{F}_0, \tilde{F}_1 has a common roots $(\xi_0 : \xi_1) \in \mathbb{P}_{\mathbb{C}}^1$ then the vector

$$v := [\xi_0^{d_0+d_1-1}, \xi_0^{d_0+d_1-2}\xi_1, \dots, \xi_1^{d_0+d_1-1}]$$

satisfy $S(\tilde{F}_0, \tilde{F}_1)v^T = 0$, so the matrix $S(\tilde{F}_0, \tilde{F}_1)$ has a non-trivial kernel, thus its determinant is zero. This implies that $\text{Res}_{(d_0, d_1)}$ divides $\det(S(F_0, F_1))$. One can also prove the other direction, so that

$$\text{Res}_{(d_0, d_1)} = \det(S(F_0, F_1)).$$

Another matrix construction for the resultant $\text{Res}_{(d_0, d_1)}$ is the Bézout matrix. Consider the new variables y_0, y_1 and define the *Bezoutian* to be the polynomial in x_0, x_1, y_0, y_1

$$\text{Bez}(x_0, x_1, y_0, y_1) := \frac{F_0(x_0, x_1)F_1(y_0, y_1) - F_1(x_0, x_1)F_0(y_0, y_1)}{x_0y_1 - y_0x_1}.$$

Note that the Bezoutian is a polynomial, since the denominator divides the numerator. To see this we write $F_0(x_0, x_1)F_1(y_0, y_1) - F_1(x_0, x_1)F_0(y_0, y_1)$ in the form

$$\sum_{t=0}^{d_0} \sum_{s=0}^{d_1} u_{0,t}u_{1,s}(x_0^{d_0-t}x_1^t y_0^{d_1-s}y_1^s - y_0^{d_0-t}y_1^t x_0^{d_1-s}x_1^s).$$

If $s = t$ then the terms with coefficients $u_{0,t}u_{1,s}$ and $u_{0,s}u_{1,t}$ cancel each other. Similarly for $d_0 - t = d_1 - s$. Then assuming for example that $d_0 - t < d_1 - s$ and $t > s$ we have that

$$x_0^{d_0-t}x_1^t y_0^{d_1-s}y_1^s - y_0^{d_0-t}y_1^t x_0^{d_1-s}x_1^s = x_0^{d_0-t}x_1^s y_0^{d_0-t}y_1^s(x_1^{t-s}y_0^{d_1-s-d_0+t} - y_1^{t-s}x_0^{d_1-s-d_0+t}).$$

It is easy to see that if $a, b \geq 1$ then

$$x_1^a y_0^b - y_1^a x_0^b = (x_1 y_0 - y_1 x_0)(x_1^{a-1} y_0^{b-1} + x_1^{a-2} y_0^{b-2} y_1 x_0 + \dots + y_1^{a-1} x_0^{b-1}).$$

This implies that the Bezoutian is a polynomial which is homogeneous in both pairs of the variables (x_0, x_1) and (y_0, y_1) separately, and have degree $d := \max(d_0, d_1) - 1$ in both. Now write

$$\text{Bez}(x_0, x_1, y_0, y_1) = \sum_{a,b=0}^d b_{a,b} x_0^{d-a} x_1^a y_0^{d-b} y_1^b$$

where $b_{a,b} \in \mathbb{Z}[u_{i,j}]$. Then the Bezoutian matrix is the symmetric $(d+1) \times (d+1)$ matrix defined as

$$B(F_0, F_1) := [b_{a,b}]_{a,b=0}^d$$

For example, for $d_0 = d_1 = 3$ we have that $B(F_0, F_1)$ is equal to

$$\begin{bmatrix} u_{0,1}u_{1,0} - u_{1,1}u_{0,0} & u_{0,2}u_{1,0} - u_{1,2}u_{0,0} & u_{0,3}u_{1,0} - u_{1,3}u_{0,0} \\ u_{0,2}u_{1,0} - u_{1,2}u_{0,0} & -u_{1,3}u_{0,0} + u_{0,3}u_{1,0} + u_{0,2}u_{1,1} - u_{1,2}u_{0,1} & -u_{1,3}u_{0,1} + u_{0,3}u_{1,1} \\ u_{0,3}u_{1,0} - u_{1,3}u_{0,0} & -u_{1,3}u_{0,1} + u_{0,3}u_{1,1} & u_{0,3}u_{1,2} - u_{1,3}u_{0,2} \end{bmatrix}.$$

One can see that $\text{Bez}(x_0, x_1, y_0, y_1) \in \langle F_0(x_0, x_1), F_1(x_0, x_1) \rangle$, therefore each of its coefficients as a polynomial in y_0, y_1 is in $\langle F_0(x_0, x_1), F_1(x_0, x_1) \rangle$. This implies that if $(\xi_0 : \xi_1)$ is a common root of \tilde{F}_0, \tilde{F}_1 then the vector $w := (\xi_0^{d-1}, \xi_0^{d-2}\xi_1, \dots, \xi_1^{d-1})$ is in the nullspace of $B(\tilde{F}_0, \tilde{F}_1)$. Therefore $\det(B(\tilde{F}_0, \tilde{F}_1))$ divides the resultant. The other direction is also true, so we have

$$\det(B(F_0, F_1)) = \text{Res}_{(d_0, d_1)}.$$

Our second example is for the case $n = 2$ and $d_0 = d_1 = d_2 = 2$, i.e. for three quadratic forms.

Example 2.6. Let

$$\begin{aligned} F_0 &= u_{0,1}x^2 + u_{0,2}y^2 + u_{0,3}z^2 + u_{0,4}xy + u_{0,5}xz + u_{0,6}yz, \\ F_1 &= u_{1,1}x^2 + u_{1,2}y^2 + u_{1,3}z^2 + u_{1,4}xy + u_{1,5}xz + u_{1,6}yz, \\ F_2 &= u_{2,1}x^2 + u_{2,2}y^2 + u_{2,3}z^2 + u_{2,4}xy + u_{2,5}xz + u_{2,6}yz. \end{aligned}$$

Denote by J the Jacobian determinant

$$J := \det \begin{pmatrix} \frac{\partial F_0}{\partial x} & \frac{\partial F_0}{\partial y} & \frac{\partial F_0}{\partial z} \\ \frac{\partial F_1}{\partial x} & \frac{\partial F_1}{\partial y} & \frac{\partial F_1}{\partial z} \\ \frac{\partial F_2}{\partial x} & \frac{\partial F_2}{\partial y} & \frac{\partial F_2}{\partial z} \end{pmatrix},$$

which is a cubic homogeneous polynomial in x, y, z . This implies that the partial derivatives of J are homogeneous of degree two, and can be written as

$$\begin{aligned}\frac{\partial J}{\partial x} &= b_{0,1}x^2 + b_{0,2}y^2 + b_{0,3}z^2 + b_{0,4}xy + b_{0,5}xz + b_{0,6}yz, \\ \frac{\partial J}{\partial y} &= b_{1,1}x^2 + b_{1,2}y^2 + b_{1,3}z^2 + b_{1,4}xy + b_{1,5}xz + b_{1,6}yz, \\ \frac{\partial J}{\partial z} &= b_{2,1}x^2 + b_{2,2}y^2 + b_{2,3}z^2 + b_{2,4}xy + b_{2,5}xz + b_{2,6}yz.\end{aligned}$$

Now consider the determinant of the 6×6 matrix

$$M(F_0, F_1, F_2) := \begin{pmatrix} u_{0,1} & u_{0,2} & u_{0,3} & u_{0,4} & u_{0,5} & u_{0,6} \\ u_{1,1} & u_{1,2} & u_{1,3} & u_{1,4} & u_{1,5} & u_{1,6} \\ u_{2,1} & u_{2,2} & u_{2,3} & u_{2,4} & u_{2,5} & u_{2,6} \\ b_{0,1} & b_{0,2} & b_{0,3} & b_{0,4} & b_{0,5} & b_{0,6} \\ b_{1,1} & b_{1,2} & b_{1,3} & b_{1,4} & b_{1,5} & b_{1,6} \\ b_{2,1} & b_{2,2} & b_{2,3} & b_{2,4} & b_{2,5} & b_{2,6} \end{pmatrix}.$$

Note that by the Euler Identity we have that

$$x \cdot J = 2 \det \begin{pmatrix} F_0 & \frac{\partial F_0}{\partial y} & \frac{\partial F_0}{\partial z} \\ F_1 & \frac{\partial F_1}{\partial y} & \frac{\partial F_1}{\partial z} \\ F_2 & \frac{\partial F_2}{\partial y} & \frac{\partial F_2}{\partial z} \end{pmatrix},$$

and similarly one can prove that

$$xJ, yJ, zJ \in \langle F_0, F_1, F_2 \rangle.$$

Thus J vanishes at all nontrivial solutions of $F_1 = F_2 = F_3 = 0$. Also, it is easy to see that the partial derivatives of xJ, yJ, zJ by x, y, z vanish at all nontrivial solutions of $F_1 = F_2 = F_3 = 0$ (need to use the fact that the derivative of a determinant is the sum of the determinants of the matrices with the derivative of one of the columns). This also implies that the partial derivatives of J vanish at all nontrivial solutions of $F_1 = F_2 = F_3 = 0$. Thus, if $F_1 = F_2 = F_3 = 0$ has a solution (x_0, y_0, z_0) not all zero, then the vector

$$v := (x_0^2, y_0^2, z_0^2, x_0y_0, x_0z_0, y_0z_0)$$

is in the kernel of $M(F_0, F_1, F_2)$. Thus $\det(M(F_0, F_1, F_2)) = 0$. This implies that $\text{Res}_{(2,2,2)}$ divides $\det(M(F_0, F_1, F_2)) = 0$. In fact, it is possible to show that

$$\text{Res}_{(2,2,2)} = \frac{-1}{512} \det(M(F_0, F_1, F_2)).$$

The coefficient $-1/512$ comes from the value of $\det(M(x^2, y^2, z^2))$.

3 Properties of the Projective Resultant

Our first theorem gives the degree of the resultant as a polynomial in the coefficients of F_i . We will not give a proof here, just check the correctness for the examples discussed in the last section.

Theorem 3.1. *Let F_0, \dots, F_n be universal polynomials of degrees $(d) = (d_0, \dots, d_n)$, as defined in Definition 2.2. Fix $0 \leq j \leq n$. Then $\text{Res}_{(d)}$ is homogeneous in the variables $\{u_{j,\alpha} : |\alpha| = d_j\}$ and*

$$\deg_{u_{j,\alpha}}(\text{Res}_{(d)}) = d_0 \cdots d_{j-1} d_{j+1} \cdots d_n.$$

Example 3.2. For the univariate case it is easy to check the claim using the Sylvester matrix construction.

For the $n = 2$, $d_0 = d_1 = d_2 = 2$ case we use the matrix construction described in Example 2.6. To prove the theorem for $\text{Res}_{(2,2,2)}$ it is sufficient to prove that

$$\text{Res}_{(2,2,2)}(\lambda \cdot F_0, F_1, F_2) = \lambda^4 \cdot \text{Res}_{(2,2,2)}(F_0, F_1, F_2).$$

Consider the Jacobian determinant J_λ of the system $(\lambda \cdot F_0, F_1, F_2)$. Then

$$J_\lambda = \lambda \cdot J$$

since the first column of the Jacobian matrix is multiplied by λ . Similarly, the partial derivatives of J_λ are λ times the partial derivatives of J . Therefore, in the matrix $M(\lambda \cdot F_0, F_1, F_2)$ the first row and each of the last three rows are λ times the corresponding rows in $M(F_0, F_1, F_2)$. Therefore $\det(M(\lambda \cdot F_0, F_1, F_2)) = \lambda^4 \cdot \det(M(F_0, F_1, F_2))$ as claimed.

The next theorem gives a product formula for the resultant, and is called the Poisson Product Formula.

Theorem 3.3 (Poisson Product Formula). *Let $F_0, \dots, F_n \subset k[x_0, \dots, x_n]$ be homogeneous polynomials of degrees $(d) = (d_0, \dots, d_n)$. Define for $i = 0, \dots, n$*

$$\begin{aligned}\bar{F}_i(x_0, \dots, x_{n-1}) &:= F_i(x_0, \dots, x_{n-1}, 0), \\ f_i(x_0, \dots, x_{n-1}) &:= F_i(x_0, \dots, x_{n-1}, 1).\end{aligned}$$

Assume that

$$\text{Res}_{(d_0, \dots, d_{n-1})}(\bar{F}_0, \dots, \bar{F}_{n-1}) \neq 0.$$

(Note that \bar{F}_i is a homogeneous polynomial in x_0, \dots, x_{n-1} of degree d_i). Then the following statements are true:

(i) If we define $A := k[x_0, \dots, x_{n-1}]/\langle f_0, \dots, f_{n-1} \rangle$, then

$$\dim_k(A) = d_0 \cdots d_{n-1}.$$

(ii) If M_{f_n} denotes the matrix of the multiplication map

$$\mu_{f_n} : A \rightarrow A; \quad [q] \mapsto [f_n q]$$

then

$$\text{Res}_{(d)}(F_0, \dots, F_n) = \text{Res}_{(d_0, \dots, d_{n-1})}(\bar{F}_0, \dots, \bar{F}_{n-1})^{d_n} \det(M_{f_n}).$$

(iii) Let $V := V(f_0, \dots, f_{n-1}) \subset \bar{k}^n$ where \bar{k} is the algebraic closure of k . Then

$$\text{Res}_{(d)}(F_0, \dots, F_n) = \text{Res}_{(d_0, \dots, d_{n-1})}(\bar{F}_0, \dots, \bar{F}_{n-1})^{d_n} \prod_{\xi \in V} f_n(\xi)^{m(\xi)},$$

where $m(\xi)$ is the multiplicity of ξ in V .

Outline of Proof. To prove (i) we note that the condition that

$$\text{Res}_{(d_0, \dots, d_{n-1})}(\bar{F}_0, \dots, \bar{F}_{n-1}) \neq 0$$

implies that no common roots of F_0, \dots, F_{n-1} has $x_n = 0$, i.e. all roots of F_0, \dots, F_{n-1} are in the affine subset $\{x_n \neq 0\} \cong \bar{k}^n$ in \mathbb{P}_k^n . We use the following lemma, without proof:

Lemma 3.4. *If a projective variety $V \in \mathbb{P}_{\bar{k}}^n$ is contained in an affine subset $\bar{k}^n \subset \mathbb{P}_{\bar{k}}^n$ then V is finite.*

This lemma implies that F_0, \dots, F_{n-1} has finitely many roots and they correspond to roots of f_0, \dots, f_{n-1} . Thus by Bezout's Theorem we have that

$$|V| = d_0 \cdots d_{n-1}$$

counting multiplicities, which implies (i).

To prove (ii), first we claim that $\det(M_{f_n})$ satisfies the first property of the definition of the projective resultant in Theorem 2.3, i.e. it vanishes if and only if F_0, \dots, F_n has a common root, provided that $\text{Res}(\bar{F}_0, \dots, \bar{F}_{n-1}) \neq 0$. This is true since the eigenvalues of M_{f_n} are $f_n(\xi)$ for $\xi \in V$, and F_0, \dots, F_n have a common root if and only if one or more of the $f_n(\xi)$ are zero, using the argument in the proof of (i).

Since $\det(M_{f_n})$ is a rational function of the coefficients of the F_i 's over k , this implies that $\text{Res}_{(d)}(F_0, \dots, F_n)$ divided by a power of $\text{Res}(\bar{F}_0, \dots, \bar{F}_{n-1})$ must be equal to $\det(M_{f_n})$. The power d_n in the formula comes from comparing degrees in the coefficients of F_0, \dots, F_n .

To prove (iii) one needs to prove that the eigenvalue $f_n(\xi)$ of M_{f_n} has the same multiplicity as the multiplicity of ξ in V . We do not prove this. \square

4 Computation of the Projective Resultant

The main idea to compute the resultant is the following: we consider each monomial as a separate linear variable. Most often the $n + 1$ polynomials have many more monomials than $n + 1$, so the resulting linear system is under-constrained. In order to get a well-constrained linear system we generate more polynomials by taking multiples of them, or by constructing polynomials which vanish if the input polynomials do. This way we may increase the degree, so there will be even more monomials, but hopefully the number of new polynomials we gain is even larger. The construction of Macaulay described in this section is the simplest such demonstration that a well-constrained (square) linear system can be constructed this way.

Once we get a square linear system, we can argue that if this linear system has no non-trivial solution, our original polynomials cannot have non-trivial solutions either. This will imply that the determinant of the

coefficient matrix of the square linear system divides the resultant. We will investigate how to find the “extraneous factor” to get the resultant form this determinant.

Definition 4.1. Let F_0, \dots, F_n be universal polynomials over $\mathbb{Z}[u_{i,\alpha}]$ of degrees $(d) = (d_0, \dots, d_n)$. First define

$$D := \sum_{i=0}^n (d_i - 1) + 1.$$

Next define sets of monomials that we will use to multiply F_i to generate polynomials in the ideal $\langle F_0, \dots, F_n \rangle$ of degree D :

$$\begin{aligned} S_0 &:= \{x^\alpha : |\alpha| = D, x_0^{d_0} |x^\alpha\} \\ S_1 &:= \{x^\alpha : |\alpha| = D, x_1^{d_1} |x^\alpha, x_0^{d_0} \nmid x^\alpha\} \\ &\vdots \\ S_n &:= \{x^\alpha : |\alpha| = D, x_n^{d_n} |x^\alpha, x_0^{d_0}, \dots, x_{n-1}^{d_{n-1}} \nmid x^\alpha\} \end{aligned}$$

We will denote by \mathcal{S}_i the vector spaces over $\mathbb{Q}(u_{i,\alpha})$ with bases S_i . Also denote by \mathcal{M}_D the vector space generated by the set of all monomials of degree D . Consider the linear map over $\mathbb{Q}(u_{i,\alpha})$

$$\begin{aligned} \Phi : \mathcal{S}_0 \oplus \dots \oplus \mathcal{S}_n &\rightarrow \mathcal{M}_D \\ (q_0, \dots, q_n) &\mapsto \sum_{i=0}^n \frac{q_i}{x_i^{d_i}} F_i. \end{aligned}$$

Then the *Macaulay matrix* $M(F_0, \dots, F_n)$ is defined to be the transpose of the matrix of Φ in the monomial basis. In other words, the rows of $M(F_0, \dots, F_n)$ correspond to the coefficients of the polynomials $\frac{x^\alpha}{x_i^{d_i}} F_i$ for all $x^\alpha \in S_i$ and $i = 0, \dots, n$.

Example 4.2. For $(d) = (1, 1, 2)$ and

$$F_0 = a_1x + a_2y + a_3z, \quad F_1 = b_1x + b_2y + b_3z, \quad F_2 = c_1x^2 + c_2y^2 + c_3z^2 + c_4xy + c_5xz + c_6yz$$

we have $D = 2$ and

$$\begin{aligned} S_0 &= \{x^2, xy, xz\} \\ S_1 &:= \{y^2, yz\} \\ S_2 &:= \{z^2\}. \end{aligned}$$

Therefore, the rows of the Macaulay matrix correspond to the coefficients of the polynomials

$$xF_0, yF_0, zF_0, yF_1, zF_1, F_2.$$

Since the number of monomials of degree 2 equals 6, we get that

$$M(F_0, F_1, F_2) = \begin{array}{c|cccccc} & x^2 & y^2 & z^2 & xy & xz & yz \\ \hline a_1 & 0 & 0 & a_2 & a_3 & 0 & xF_0 \\ 0 & a_2 & 0 & a_1 & 0 & a_3 & yF_0 \\ 0 & 0 & a_3 & 0 & a_1 & a_2 & zF_0 \\ 0 & b_2 & 0 & b_1 & 0 & b_3 & yF_1 \\ 0 & 0 & b_3 & 0 & b_1 & b_2 & zF_1 \\ c_1 & c_2 & c_3 & c_4 & c_5 & c_6 & F_2 \end{array} . \quad (1)$$

Proposition 4.3. *The Macaulay matrix $M(F_0, \dots, F_n)$ is square.*

Proof. Let $N := \binom{D+n}{n}$ be the number of monomials in $n + 1$ variables of degree D . It suffices to prove that

$$|S_0| + |S_1| + \dots + |S_n| = N.$$

First of all $S_i \cap S_j = \emptyset$ if $i \neq j$ because if $i < j$ then $x_i^{d_i}$ divides the elements in S_i but it doesn't divide the elements of S_j . Secondly, $\bigcup_{i=0}^n S_i$ is all the monomials of degree D , since for every x^α of degree $D = \sum_{i=0}^n (d_i - 1) + 1$ there must exist i such that $\alpha_i > d_i$, and for the smallest such i we have $x^\alpha \in S_i$. \square

Proposition 4.4. *Denote by $R_n = R_n(F_0, \dots, F_n)$ the determinant of the Macaulay matrix $M(F_0, \dots, F_n)$. Then*

(i) R_n is a homogeneous polynomial in the set of coefficients of F_i and

$$\deg_{u_{i,\alpha}} R_n = |S_i|.$$

(ii) $\text{Res}_{(d)}$ divides R_n in $\mathbb{Z}[u_{i,\alpha}]$, i.e. there exists an extraneous factor $E_n \in \mathbb{Z}[u_{i,\alpha}]$ such that

$$R_n = E_n \cdot \text{Res}_{(d)}.$$

(iii) E_n does not depend on the coefficients of F_n .

Proof. Part (i) is clear from the Macaulay matrix construction.

To prove (ii), notice that the rows of $M(F_0, \dots, F_n)$ correspond to polynomials in the ideal $\langle F_0, \dots, F_n \rangle$. Therefore, for any specialized system $\tilde{F}_0, \dots, \tilde{F}_n$, if $\xi \in \mathbb{P}^n$ is a common root of $\tilde{F}_0, \dots, \tilde{F}_n$ then the vector $v := [\xi^\alpha]_{|\alpha|=D}$ is in the kernel of $M(\tilde{F}_0, \dots, \tilde{F}_n)$, thus $R_n(\tilde{F}_0, \dots, \tilde{F}_n) = 0$. Since the resultant is an irreducible polynomial, this implies that $\text{Res}_{(d)}$ divides R_n .

To prove (iii) we will prove that

$$\deg_{u_n, \alpha}(R_n) = \deg_{u_n, \alpha}(\text{Res}_{(d)}) = d_0 \cdots d_{n-1}.$$

The second equation is proved in Theorem 3.1. To prove the first equation, it suffices to prove that $|S_n| = d_0 \cdots d_{n-1}$. This is true because if $x^\alpha \in S_n$ for some $\alpha = (\alpha_0, \dots, \alpha_n)$, then $\alpha_0, \dots, \alpha_{n-1}$ can be chosen arbitrarily as long as $0 \leq \alpha_i \leq d_i - 1$, and since $\sum_{i=0}^{n-1} \alpha_i < D$, therefore α_n is uniquely determined to be $D - \sum_{i=0}^{n-1} \alpha_i$. \square

In the next corollary we give a method to compute the projective resultant as the GCD of determinants of certain Macaulay matrices. First we need a definition:

Definition 4.5. Since the Macaulay matrix construction depends on the order of the variables, for $i = 0, \dots, n$ we denote by R_i the determinant of the Macaulay matrix with an ordering of the variables such that x_i is the last variable.

Corollary 4.6.

$$\text{Res}_{(d)} = \pm \text{gcd}(R_0, \dots, R_n).$$

where the greatest common divisor is taken in the ring $\mathbb{Z}[u_{i,\alpha}]$.

Proof. On one hand the resultant divides the GCD. On the other hand, for any fixed i , by Proposition 4.4(iii), the degree of the GCD in $u_{i,\alpha}$ is at most $d_0 \cdots d_{i-1} d_{i+1} \cdots d_n$, which is the degree of the resultant, so their degrees must be equal. Therefore they are constant multiples of each other. This constant must be ± 1 since the GCD is only determined up to invertible elements, and the only invertible elements in $\mathbb{Z}[u_{i,\alpha}]$ are ± 1 . \square

Unfortunately computing the GCD of $n+1$ polynomials in many variables is usually not feasible. The next construction, due to Macaulay's original

work [Mac02], gives the resultant as the ratio of R_n and a smaller subdeterminant of the Macaulay matrix $M(F_0, \dots, F_n)$. To define this subdeterminant of $M(F_0, \dots, F_n)$ we need the following definition:

Definition 4.7. Define

$$\mathcal{E}_n = \{x^\alpha : |\alpha| = D, \exists i \neq j \ x_i^{d_i} | x^\alpha \text{ and } x_j^{d_j} | x^\alpha\},$$

i.e. all the monomials of degree D which are divisible by $x_i^{d_i}$ for more than one i . Let R'_n be the determinant of the submatrix of $M(F_0, \dots, F_n)$ with rows and columns corresponding to the monomials \mathcal{E}_n (note that the union of the elements in S_i is all the monomials of degree D).

Example 4.8. In the case of $(d) = (1, 1, 2)$ the only monomial in \mathcal{E}_2 is xy . The corresponding subdeterminant of $M(F_0, F_1, F_2)$ in (1) is the determinant of the 1×1 submatrix of the second row and the fourth column, which is $[a_1]$, so $R'_2 = a_1$.

Theorem 4.9. Let F_0, \dots, F_n be universal polynomials of degrees $(d) = (d_0, \dots, d_n)$. Then the resultant is given by

$$\text{Res}_{(d)} = \pm \frac{R_n}{R'_n}.$$

Proof Outline. We only give the main idea of the proof, which appeared originally in [Mac02]. First one can prove that R'_n divides R_n in $\mathbb{Z}[u_{i,\alpha}]$. Once this is proved, one can give an argument based on counting the degrees in $u_{i,\alpha}$ of both sides. The ± 1 multiple follows from the fact that

$$R_n(x_0^{d_0}, \dots, x_n^{d_n}) = R'_n(x_0^{d_0}, \dots, x_n^{d_n}) = \pm 1.$$

□

Example 4.10. In the $(d) = (1, 1, 2)$ case we have that

$$\text{Res}_{(1,1,2)} = \det(M(F_0, F_1, F_2))/a_1$$

which is equal to

$$\begin{aligned} & -a_1^2 b_2 b_3 c_6 - 2a_1 b_2 b_1 a_2 c_3 + a_3 a_1 b_2 b_1 c_6 + a_1 b_2 a_2 b_3 c_5 - 2a_3 b_2 a_2 b_3 c_1 \\ & + a_1^2 b_2^2 c_3 - a_3 a_1 b_2^2 c_5 + a_3^2 b_2^2 c_1 + b_1 a_2 a_1 b_3 c_6 - 2a_3 b_1 a_1 b_3 c_2 + b_1^2 a_2^2 c_3 \\ & - a_3 b_1^2 a_2 c_6 + a_3^2 b_1^2 c_2 - b_1 a_2^2 b_3 c_5 + a_3 b_1 a_2 b_2 c_5 + b_3^2 a_1^2 c_2 - c_4 a_2 a_1 b_3^2 \\ & + a_3 c_4 a_2 b_3 b_1 + a_3 c_4 a_1 b_2 b_3 - a_3^2 c_4 b_2 b_1 + a_2^2 b_3^2 c_1. \end{aligned}$$

References

- [BCSS98] Lenore Blum, Felipe Cucker, Michael Shub, and Steve Smale. *Complexity and real computation*. Springer-Verlag, New York, 1998. With a foreword by Richard M. Karp.
- [CLO98] David Cox, John Little, and Donal O'Shea. *Using Algebraic Geometry*. Graduate Texts in Mathematics, 185. Springer-Verlag, 1998.
- [Mac02] F. Macaulay. Some formulae in elimination. *Proc. London. Math. Soc.*, 33(1):3–27, 1902.