C7 _ Macaulay's resultant

1) Elimination theorem

We suppose given r homogeneous polynomials in variables $x_1, \dots, x_n$:

$$f_i(x_1, \dots, x_n) = \sum_{|\alpha| = d_i \geq 1} u_{i,\alpha} x^\alpha \qquad x^\alpha = x_1^{\alpha_1} \dots x_n^{\alpha_n}$$

$i = 1, \dots, r$.

We set
- $A := \mathbb{Z}[u_{i,\alpha} : i = 1, \dots, r, \ |\alpha| = d_i]$ universal ring of coeffs.
- $C := A[x_1, \dots, x_n]$, graded by $\begin{cases} \deg(x_i) = 1 \\ \deg(u_{i,\alpha}) = 0 \end{cases}$
- $f_i \in C_{d_i}$; $I = (f_1, \dots, f_r) \subset C$.
- $\mathfrak{m} = (x_1, \dots, x_n) \subset C$.

Question: Let k be a field and $\rho : \begin{matrix} A \to k \\ u_{i,\alpha} \to c_{i,\alpha} \end{matrix}$ a specialization map

We are looking for a necessary and sufficient condition on the $u_{i,\alpha}$ so that $\rho(f_1) = \dots = \rho(f_r) = 0$ (ρ is extended canonically to $A[\underline{x}] \to k[\underline{x}]$) have a non-trivial common root in $\bar{k}$ (alg. closure of k).

THM (elimination):
- There exist $P_1, \dots, P_p \in A$ such that $\rho(P_1) = \dots = \rho(P_p) = 0 \iff \rho(f_1) = \dots = \rho(f_r) = 0$ has a common root in $\mathbb{P}^{n-1}_{\bar{k}}$
- The resultant ideal $\mathfrak{a}(I) := (I : \mathfrak{m}^\infty) \cap A = \{a \in A : \forall i \ \exists m \ x_i^m a \in I\}$ satisfies

$$\rho(\mathfrak{a}(I)) = 0 \iff \rho(f_1) = \dots = \rho(f_r) = 0 \text{ has a common root in } \mathbb{P}^{n-1}_{\bar{k}}$$

Example: $r=n=2$: the Sylvester resultant.

$$f=\sum a_i x_1^i x_2^{d_1-i} \qquad g=\sum b_j x_1^j x_2^{d_2-j} \qquad Res(f,g)\in \mathbb{Z}[a_i,b_j]$$

$\rho(Res(f,g))=0 \iff \rho(f)=\rho(g)=0$ has a common root in $\mathbb{P}^1_{\bar{k}}$.

In this case, one can show that $\mathfrak{a}(I)=(Res(f,g))\subset A$.

2) Geometric interpretation

* For a proof of the elimination THM we refer to Cox-Little-O'Shea's book.

* For now, we provide a geometric interpretation of this theorem in the case where $r=n$ (resultant theory), over a field $k=\bar{k}$.

- Homogeneous polynomials of degree d form an affine space:

$$\sum_{|\alpha|=d} u_\alpha x^\alpha \longleftrightarrow (u_\alpha)_{|\alpha|=d}\in \mathbb{A}^{N(d)} \qquad N(d)=\binom{n+d-1}{n-1}$$

- Consider the incidence variety $W:=V(f_1,\dots,f_r)\subset \mathbb{P}^{n-1}\times\prod_{i=1}^n \mathbb{A}^{N(d_i)}$

$$\begin{tikzcd} \mathbb{P}^{n-1}\times\prod \mathbb{A}^{N(d_i)} \\ W \arrow[u, phantom, "\cup"] \arrow[r, "\pi_2"] \arrow[d, "\pi_1"] & \prod \mathbb{A}^{N(d_i)} \\ \mathbb{P}^{n-1} \end{tikzcd}$$

- π_1 is surjective and its fiber are linear spaces of codimension n

$\rightsquigarrow$ W is a fiber bundle : it is an irreducible variety of dimension $\left(\sum N(d_i)\right)-1$.

Let $\nabla:=\pi_2(W)$: this is an irreducible variety (elim. theorem)

As the general fiber is of dimension 0 (finitely many points) then $\dim(\nabla)=\dim(W)$ and hence ∇ is an irreducible hypersurface in $\prod \mathbb{A}^{N(d_i)}$ $\rightsquigarrow$ resultant theory. Next we turn to a more algebraic treatment of this elimination process.

3) Inertia forms

Take again the notation of 1). But now, let k be any commutative ring and $A := k[u_{j,\alpha}]$ the universal ring of coeffs over k.

Def: The ideal of inertia forms is the ideal $(I : m^\infty) \subset C$
An inertia form is an element in $(I : m^\infty)$.

Rk: $(I : m^\infty)$ is a graded ideal in $C = A[x_1, \dots, x_n]$.

We have $\mathfrak{e}(I) = (I : m^\infty)_0 = (I : m^\infty) \cap A$.

Proposition: $f \in (I : m^\infty) \Leftrightarrow \exists\, i, m$ such that $x_i^m f \in I$

Proof: Pick $i \in \{1, \dots, n\}$ and for any $j = 1, \dots, r$ set

$$f_j(x_1, \dots, x_n) = \varepsilon_{ij}\, x_i^{d_j} + \sum_{\substack{|\alpha| = d_j \\ u_{j,\alpha} \neq \varepsilon_{ij}}} u_{j,\alpha}\, x^\alpha$$

We have $f_j = x_i^{d_j} \Big[\varepsilon_{ij} + \sum_{\substack{|\alpha| = d_j \\ u_{j,\alpha} \neq \varepsilon_{ij}}} u_{j,\alpha} \frac{x^\alpha}{x_i^{d_j}} \Big]$ in $C[x_i^{-1}]$

Denoting $B := C/I$, we get an isomorphism of graded k-algebra:

$$\left(C/I\right)_{x_i} = B_{x_i} \xrightarrow{\sim} k[u_{j,\alpha} \mid u_{j,\alpha} \neq \varepsilon_{ij},\, j = 1..r][x_1, \dots, x_n][x_i^{-1}]$$

$$\varepsilon_{ij} \longrightarrow -\sum u_{j,\alpha} \frac{x^\alpha}{x_i^{d_j}}$$

(taking quotient with f_j amounts to say $\varepsilon_{ij} = -\sum u_{j,\alpha} x^\alpha / x_i^{d_j}$ (division))

As a consequence, x_j is not a zero divisor in B_{x_i} for any couple of integers (i, j).

So we have commutative diagrams

$$\begin{tikzcd} C \arrow[r] \arrow[d] \arrow[dr, phantom, "\circlearrowleft"] & B_{x_i} \arrow[d, hook] \\ B_{x_j} \arrow[r, hook] & B_{x_i x_j} \end{tikzcd}$$

If $x_i^M f \in I$, i.e. $f=0$ in B_{x_i} then $f=0$ in $B_{x_i x_j}$ and hence in B_{x_j}, i.e. $x_j^{m'} f \in I$. $\square$.

Corollary: If k is a domain then $(I : m^\infty)$ (and $\varepsilon(I)$) is a prime ideal.

Proof: We have just proved that

$$(I : m^\infty) = \ker\left(C = A[x_1, \dots, x_n] \to B_{x_n} \right)$$

and that B_{x_n} is a polynomial ring over k, hence a domain. It follows that $C/_{(I : m^\infty)}$ is a domain and hence $(I : m^\infty)$ is prime. Same conclusion follows for $\varepsilon(I) = i^{-1}(I : m^\infty)$ where $i : A \hookrightarrow A[x_1, \dots, x_n]$. $\square$.

Geometrically, $(I : m^\infty)$ defines the incidence variety (actually scheme) and $\varepsilon(I)$ its image via π_2. We have just proved that they are both irreducible geom. objects.

THM (HURWITZ): If $r < n$ then $(I : m^\infty) = I$.

This theorem implies that the projection π_2 of the incidence variety is surjective, as $\varepsilon(I) = I \cap A = 0$ as soon as $d_i \geq 1$ $\forall i$. This means that there always exists common roots.

The proof of HURWITZ's theorem requires the properties of regular sequences that are given in the exercises sheet.

Lemma: If $r \leq n$ then $\{f_1, \dots, f_r\}$ is a regular sequence in C.

Proof: set $f_i = \varepsilon_i x_i^{d_i} + \dots$ for all $i = 1, \dots, r$.

Build the sequence $S := \{ u_{1,\alpha} \text{ except } \varepsilon_1, u_{2,\alpha} \text{ except } \varepsilon_2, \dots, u_{r,\alpha} \text{ except } \varepsilon_r \}$.

In $C/(S)$ we have $\overline{f_i} = \varepsilon_i x_i^{d_i}$.

Now add to S the elements $\varepsilon_1 - x_1, \dots, \varepsilon_r - x_r$ so that $\overline{f_i} = x_i^{d_i+1}$
(obvious)

The sequence $x_1^{d_1+1}, \dots, x_r^{d_r+1}$ is regular, which implies that $S \cup \{f_1, \dots, f_r\}$ is regular. As the elements are homogeneous, we can permute the order and hence $\{f_1, \dots, f_r\} \cup S$ is regular, hence $\{f_1, \dots, f_r\}$ is regular. $\square$

Proof of HURWITZ's theorem:

- Let $f \in (I : x_n^\infty)$. We want to show that $f \in I$.
By assumption, $\exists s$ such that $x_n^s \cdot f \in I$. If $s=0$ we are done.
If not, it is enough to show that $x_n f \in I \Rightarrow f \in I$ because then one can iterate $(x_n^s f = x_n(x_n^{s-1} f))$.
- So, let f be such that

$$x_n f = h_1 f_1 + h_2 f_2 + \dots + h_r f_r \quad \text{in } C = A[x_1, \dots, x_n].$$

By specialization $x_n \to 0$ we get $\quad (P(x_n=0) =: \overline{P})$

$$0 = \overline{h_1}\,\overline{f_1} + \cdots + \overline{h_r}\,\overline{f_r} \quad \text{in } A[x_1, \ldots, x_{n-1}].$$

Since $r<n$, $\{\overline{f_1}, \ldots, \overline{f_r}\}$ is a regular sequence and hence there exists a skew-symmetric matrix $M = (d_{ij})$ such that

$$\begin{pmatrix} \overline{h_1} \\ \vdots \\ \overline{h_r} \end{pmatrix} = M \begin{pmatrix} \overline{f_1} \\ \vdots \\ \overline{f_r} \end{pmatrix} \qquad \begin{pmatrix} d_{ii}=0 \\ d_{ij}=-d_{ji} \end{pmatrix}$$

Set $\begin{pmatrix} g_1 \\ | \\ g_r \end{pmatrix} := M \begin{pmatrix} f_1 \\ | \\ f_r \end{pmatrix}$ i.e. $g_i = \sum_{j=1}^{r} d_{ij} f_j$.

One has $\sum_{i=1}^{r} g_i f_i = 0$ (M skew-sym.).

Moreover $\overline{g_i} = \overline{h_i}$ hence $-g_i + h_i = x_n l_i$ in $A[x_1, \ldots, x_n]$.

It follows that

$$x_n f = (g_1 + x_n l_1) f_1 + \cdots + (g_r + x_n l_r) f_r$$
$$= \sum g_i f_i + x_n \sum l_i f_i = x_n \sum l_i f_i.$$

Therefore $f = \sum l_i f_i \in I$ because x_n is not a zerodivisor in $A[x_1 \ldots x_n]$ $\square$

4) <u>The case $r=n$: Macaulay resultant</u>

We will prove the following result:

<u>THM</u> ($r=n$): If k is a UFD then $\mathfrak{a}(I) \subset A$ is a principal ideal and has a unique generator, denoted $\operatorname{Res}(f_1, \ldots, f_n)$ such that $\operatorname{Res}(x_1^{d_1}, \ldots, x_n^{d_n}) = 1$.

* A word on the notation "$\mathrm{Res}(f_1,\dots,f_n)$":

$\mathrm{Res}(f_1,\dots,f_n) \in k[u_{i,\alpha}]$ by definition.

Let $(g_1,\dots,g_n) \in S[x_1,\dots,x_n]$, S a commutative ring, $g_i = \sum c_{i,\alpha} x^\alpha$, $c_{i,\alpha} \in S$.

One has a ring morphism (specialization)

$$\begin{aligned} \vartheta : \mathbb{Z}[u_{i,\alpha}] &\to S \\ u_{i,\alpha} &\mapsto c_{i,\alpha} \\ 1 &\mapsto 1 \end{aligned}$$

The resultant of $g_1,\dots,g_n$ is defined by specialization:

$$\mathrm{Res}(g_1,\dots,g_n) := \vartheta(\mathrm{Res}(f_1,\dots,f_n)).$$

In this way, one has $\vartheta(\mathrm{Res}(f_1,\dots,f_n)) = \mathrm{Res}(\vartheta(f_1),\dots,\vartheta(f_n))$ (ϑ is extended canonically to polynomial rings).

Thus $\mathrm{Res}(-,\dots,-)$ is seen as an operator, similarly to determinant.

* First example of non trivial inertia forms.

The Jacobian determinant:

$$\mathrm{Jac}(f_1,\dots,f_n) = \det\begin{pmatrix} \frac{\partial f_1}{\partial x_1} & \cdots & \frac{\partial f_1}{\partial x_n} \\ \vdots & & \\ \frac{\partial f_n}{\partial x_1} & \cdots & \frac{\partial f_n}{\partial x_n} \end{pmatrix} \in (I : \mathfrak{m}^\infty).$$

It is easy to check that $x_i \,\mathrm{Jac}(f_1,\dots,f_n) \in I$ for all i.

* Macaulay determinants (examples of non-trivial inertia forms indep of the variables $x_1,\dots,x_n$).

These determinants have been historically introduced by Macaulay in 1902.

Set $\delta := \sum_{i=1}^{n} (d_i - 1)$ where $d_i := \deg(f_i)$ $i = 1, \dots, n$.

and $\mathrm{Mon}(n;t) := \{ x^\alpha \text{ such that } |\alpha| = t \} = \mathrm{Mon}(t)$

For all $t \geq \delta + 1$, any $x^\alpha \in \mathrm{Mon}(t)$ is divisible by $x_i^{d_i}$ for some i.
(because $x_1^{d_1 - 1} \cdots x_n^{d_n - 1}$ is of degree δ).

Def: Let $t \geq \delta + 1$. For all $x^\alpha \in \mathrm{Mon}(t)$ we define its index as

$$i(\alpha) := \min \{ i \text{ such that } \alpha_i \geq d_i \}.$$

Def: $\mathbb{M}(\underline{f}; t) = (m_{\alpha\beta})$ is the matrix defined as follows:

$$\mathrm{Mon}(n;t) \times \mathrm{Mon}(n;t) \longrightarrow A = k[u_{i,\alpha}]$$
$$(\alpha, \beta) \longrightarrow m_{\alpha\beta}$$

where $\dfrac{x^\beta}{x_{i(\beta)}^{d_{i(\beta)}}} f_{i(\beta)} = \sum_{|\alpha| = t} m_{\alpha\beta} x^\alpha$ with $x^\beta \in \mathrm{Mon}(n;t)$.

In other words,

$$\mathbb{M}(\underline{f}; t) = \begin{array}{c} \begin{array}{ccccc} x_1^t & \cdots & x^\beta & \cdots & x_n^t \end{array} \\ \left(\begin{array}{ccccc} & & & & \\ & & \dfrac{x^\beta}{x_{i(\beta)}^{d_{i(\beta)}}} f_{i(\beta)} & & \\ & & & & \end{array} \right) \end{array} \begin{array}{c} x_1^t \\ \vdots \\ x_n^t \end{array}$$

Exercise: If $r = n = 2$ show that the Sylvester matrix is obtained as above with $t = \delta + 1$.

Proposition: The determinant $D(t) := \det(\mathbb{M}(\underline{f}; t))$, $t \geq \delta+1$, belongs to $(I : m^\infty)$, hence to $\mathfrak{A}(I) = (I : m^\infty)_0$. Moreover, $D(t) \neq 0$ and is homogeneous with respect to the coeff. of each polynomial $f_i(x_1, \ldots, x_n)$.

Proof: – Multiply the first row by x_1^t (for instance) and then add combinations of the other rows to get multiples of f_i's in the first row ($L_1 \leftarrow L_1 + \sum x^\alpha m_{\alpha\beta}$).
It follows that $x_1^t \cdot D(t) \in I$, so $D(t) \in (I : m^\infty)$.
– Now, by specializing all f_i to $x_i^{d_i}$ respectively, one get that $\mathbb{M}(\underline{f}; t)$ specializes to the identity matrix, so we deduce that $D(t) \neq 0$.
– Finally the homogeneity property follows from the development of the determinant.

Proposition: $\deg_{f_n}(D(t)) = d_1 \cdots d_{n-1}$

Proof: $\deg_{f_i}(D(t)) = \#\{\alpha \text{ s.t. } |\alpha| = t \text{ and } i(\alpha) = i\}$
but $i(\alpha) = n \iff 0 \leq \alpha_i \leq d_i - 1 \quad i = 1 \ldots n-1$.

Corollary: For all $i = 1, \ldots, n$ $\exists\, D_i(t) \neq 0$ such that
$D_i(t) \in (I : m^\infty)_0$ and $\deg_{f_i} = \dfrac{d_1 \cdots d_n}{d_i}$

Proof: simply permute the f_i's in the previous construction. $\square$.

* Come back to the proof of the main THM.

Proposition. ~~Let~~ $f \in (I : \eta^\infty)$. Then, either $f \in I$ (in which case f is called a trivial inertia form) or either f depends on each coefficient of each polynomial f_i, $i = 1, \dots, n$.

Proof: This is a consequence of HURWITZ's THM.

Let $u := u_{i,\alpha}$ be one coeff. of the polynomial f_i, for some i.
Suppose there exists $f \in (I : \eta^\infty)$ but f does not depend on u.
We have $f_i = u x^\alpha + g_i = u_{i,\alpha} x^\alpha + \dots$ (notation).
By assumption $\exists N$ s.t.

$$x_n^N f = h_1 f_1 + \dots + h_n f_n \, , \quad h_i \in {}_k A[x_1, \dots, x_n]$$

Consider the k-algebra morphism

$$\begin{aligned} \varphi : A[x_1, \dots, x_n] &\longrightarrow A[x_1, \dots, x_n]_{x_1 x_2 \dots x_n} \\ u &\longmapsto - g_i / x^\alpha \\ u_{j,\beta} &\longmapsto u_{j,\beta} \quad (j,\beta) \neq (i,\alpha) \\ x_i &\longmapsto x_i \end{aligned}$$

Since f is indep of u, one has $\varphi(x_n^N f) = x_n^N f$, hence

$$x_n^N f = \varphi(x_n^N f) = H_1 \cdot f_1 + \dots + H_{i-1} f_{i-1} + H_{i+1} f_{i+1} + \dots + H_n f_n$$

since $\varphi(f_i) = 0$

but $x_1 \dots x_n$ is not a zero divisor in $A[x_1, \dots, x_n]$, so there exists x^β s.t.

$$x^\beta x_n^N f = l_1 f_1 + \dots + l_{i-1} f_{i-1} + l_{i+1} f_{i+1} + \dots + h f_n \text{ in } A[x_1 \dots x_n].$$

Therefore, $f \in (f_1, \dots, f_{i-1}, f_{i+1}, \dots, f_n : y^\alpha)$ and hence (HURWITZ) $f \in (f_1, \dots, \hat{f_i}, \dots, f_n)$]

Proof of the main THM.

Pick a coeff $u := u_{i,\alpha}$ and set $A = A'[u]$ (A' is also a UFD).

We know that:
- $\mathfrak{q}(I) \neq 0$, because of $D(+)$ determinants
- $\forall a \neq 0 \in \mathfrak{q}(I)$, $\deg_u(a) \geq 1$ (previous propositi).

We define $s := \inf_{\substack{a \in \mathfrak{q}(I) \\ a \neq 0}} (\deg_u(a)) \geq 1$

- We first show that there exists a prime element $R \in \mathfrak{q}(I)$ such that $\deg_u(R) = s$:

Let $a \neq 0 \in \mathfrak{q}(I)$ such that $\deg_u(a) = s$. On can decompose a as follows:

$a = q_1 \dots q_t$ where q_i are primes in $A'[u]$ (UFD).

But $\mathfrak{q}(I)$ is prime, so there exists i such that $q_i \in \mathfrak{q}(I)$.

Moreover, $1 \leq \deg_u(q_i) \leq \deg_u(a) = s$, so by definition of s, $\deg_u(q_i) = s$. We set $R := q_i$.

- Now, we show that R is a generator of $\mathfrak{e}(I)$:

For any $b \in \mathfrak{e}(I)$ we have ("division" by R in $A'[u]$)

$$d.b = q.R + v \quad \text{with } d \in A' \text{ and } \begin{cases} v = 0 \\ \text{or} \\ \deg_u(v) < s \end{cases}$$

Thus $v = db - q.R \in \mathfrak{e}(I)$.

If $v \neq 0$ then $\deg_u(v) \geq 1$ (previous property) and even better $\deg_u(v) \geq s$ by def of s: impossible.

It follows that $v = 0$ and hence $db = q.R$ in $A'[u]$.

R being irred., it must divides d or b. But d does not depend of u therefore $R \mid b$ and we conclude that $\mathfrak{e}(I) = (R)$.

- In conclusion, $\mathfrak{e}(I)$ is principal generated by R which is defined up to multiplication by an invertible element in A', hence in k. This invertible element is set by the condition $Rs(x_1^{d_1}, \dots, x_n^{d_n}) = 1$

$\square$.

Rq: • $Res(f_1, \dots, f_n)$ is called the resultant of $f_1, \dots, f_n$.

• $Res(f_1, f_2)$ is equal to the Sylvester resultant.

5) Properties of the resultant

- R a commutative ring and $l_1, \dots, l_n \in R[x_1, \dots, x_n]_1$ linear forms.

$$l_i = \sum_{j=1}^{n} u_{i,j}\, x_j \qquad i = 1 \dots n$$

Then $\operatorname{Res}(l_1, \dots, l_n) = \det(u_{i,j})$.

Proof: Assume we are in the generic setting over $\mathbb{Z}$.

$x_1 \det(u_{i,j}) \in (l_1, \dots, l_n) \Rightarrow \det(u_{i,j}) \in \mathcal{E}(I) = (\operatorname{Res}(l_1 \dots l_n))$.

It follows that $\operatorname{Res}(l_1 \dots l_n) \mid \det(u_{i,j})$

Moreover $\deg_{l_i} \det(u_{ij}) = 1$ and $\underset{\substack{\uparrow \\ \text{depends on} \\ \text{all coeff.}}}{1 \leq} \deg_{l_i} (\operatorname{Res}) \underset{\substack{\uparrow \\ \text{Macaulay matrices}}}{\leq}$

so $c \cdot \operatorname{Res}(l_1, \dots, l_n) = \det(u_{i,j})$ with $c \in \mathbb{Z}$.

By specialization $l_i \to x_i$ we get $1 = c \cdot 1$ □.

- Divisibility. R a commutative ring and $(f_1, \dots, f_n), (g_1, \dots, g_n)$ two sequences of hom. polynomials in $R[x_1, \dots, x_n]$ such that $g_i \in (f_1, \dots, f_n) \subset R[x_1, \dots, x_n]$ for all i then

$$\operatorname{Res}(f_1, \dots, f_n) \mid \operatorname{Res}(g_1, \dots, g_n) \quad \text{in } R.$$

Proof: $g_i = \sum_{j=1}^{n} h_{ij} f_j$ by assumption. By specialization, one can assume that both f_j's and h_{ij}'s have indeterminate coefficients over $\mathbb{Z}$.

Then $x_n^N \operatorname{Res}(g_1, \dots, g_n) \underset{\substack{\uparrow \\ \text{inertia form} \\ \text{and specialization}}}{\in} (g_1, \dots, g_n) \underset{\substack{\uparrow \\ \text{assumption}}}{\subset} (f_1, \dots, f_n)$

and hence $\operatorname{Res}(f_1, \dots, f_n) \mid \operatorname{Res}(g_1, \dots, g_n)$ (f_i's are generic). □.

- Multi-degree of the resultant

$Res(f_1, \dots, f_n) \in {}_k A[x_1, \dots, x_n] = k[u_{i,\alpha}][x_1, \dots, x_n]$ is homogeneous in the coeff $u_{i,\alpha}$ of f_i, for each i, of degree $\frac{d_1 \dots d_n}{d_i}$.

Proof: • The existence of the Macaulay determinants imply that $\deg_{f_i} Res(f_1 \dots f_n) \leq \frac{d_1 \dots d_n}{d_i}$ $\forall i$

• Now, specialize each f_i into a product of linear forms:

$$f_i \overset{\rho}{\mapsto} g_i := \prod_{j=1}^{d_i} l_{i,j} \qquad l_{i,j} \text{ generic}$$

By divisibility we have $Res(l_{1,j_1}, \dots, l_{n,j_n}) \mid Res(g_1, \dots, g_n)$ $\forall j_1, \dots, j_n$.

We deduce that

$$\prod_{\substack{1 \leq j_1 \leq d_1 \\ \vdots \\ 1 \leq j_n \leq d_n}} Res(l_{1,j_1}, \dots, l_{n,j_n}) \mid Res(g_1 \dots g_n) \quad (*)$$

Moreover, $\deg_{l_{i,j_k}} Res(l_{1,j_1}, \dots, l_{n,j_n}) = 1$ $\forall i, j_k$.

We have $d_1 \dots d_n$ terms in the product $(*)$. In addition the coeffs of f_i become of degree d_i in the coeff of l_{i,j_k} via ρ.

Therefore we conclude that $\deg_{f_i} Res(f_1 \dots f_n) \geq \frac{d_1 \dots d_n}{d_i}$ $\square$

- Multiplicativity If $f_i = f_i' f_i''$ then

$$Res(f_1, \dots, f_i, \dots, f_n) = Res(f_1, \dots, f_i', \dots, f_n)\, Res(f_1, \dots, f_i'', \dots, f_n).$$

(See Cox-Little-O'Shea).

- Invariance under elementary transformations

$$Res(f_1, \dots, f_i + \sum_{j \neq i} h_{ij} f_j, \dots, f_n) = Res(f_1, \dots, f_i, \dots, f_n).$$

(exercise).

- Macaulay formula

Recall that for all $t \geq \delta + 1$, $\delta = \sum_{i=1}^{n} (d_i - 1)$, we have built the Macaulay determinants

$$D_i(t) \in A = k[U_{i,\alpha}] \; ; \; \deg_{f_i} D_i(t) = \frac{d_1 \dots d_n}{d_i}.$$

They are inertia forms and are hence divisible by the resultant:

$$D_i(t) = Res(f_1, \dots, f_n) \cdot H_i(t) \quad i = 1, \dots, n.$$

By degree property, it is clear that $H_i(t)$ is indep of the coeff of f_i. This implies the following fact.

$$Res(f_1 \dots f_n) = \gcd(D_1(t), \dots, D_n(t)), \; k \text{ UFD}.$$

Nevertheless, $H_i(t)$ can be computed as follows:

For all $t \geq \delta + 1$ set

$$Dod(n; t) = \{ x^\alpha \text{ such that } \exists\, i \neq j : \alpha_i \geq d_i \text{ and } \alpha_j \geq d_j \}$$

and let $\Delta(\underline{f}; t)$ the submatrix of $\mathbb{M}(\underline{f}; t)$ indexed by $Dod(n; t)$.

THM (Macaulay): For all $t \geq \delta + 1$ we have

$$\det(\mathbb{M}(\underline{f}; t)) = Res(f_1, \dots, f_n) \det(\Delta(\underline{f}; t)).$$

(see e.g. Cox-Little-O'Shea). $\square$