Resultants modulo p

Laurent Busé, **Carlos D'Andrea**, Martín Sombra

SIAM Conference on Applied Algebraic Geometry
July 31 – August 4, 2017
Georgia Institute of Technology
Atlanta, Georgia, USA

ARCADES

Universitat de Barcelona

Disclaimer

Disclaimer

Last summer you may have heard:

$$\boxed{\mathrm{val}_p\left(\mathrm{Res}(f_1,\ldots,f_n)\right) \geq d(V_p)}$$

(**D**-Sombra 2016)

Disclaimer

Last summer you may have heard:

$$\boxed{\mathrm{val}_p\left(\mathrm{Res}(f_1,\dots,f_n)\right) \geq d(V_p)}$$

(**D**-Sombra 2016)

Today:

$$\boxed{\mathrm{val}_p\left(\mathrm{Res}(f_1,\dots,f_n)\right) \geq e(V_p)}$$

(Busé-**D**-Sombra 2017)

The setting

The setting

- $f_1, \ldots, f_n \in \mathbb{Z}[X_1, \ldots, X_n]$ homogeneous of degrees $d_1, \ldots, d_n$

The setting

- $f_1, \ldots, f_n \in \mathbb{Z}[X_1, \ldots, X_n]$ homogeneous of degrees $d_1, \ldots, d_n$
- $\mathrm{Res}_{d_1,\ldots,d_n}(f_1, \ldots, f_n) \in \mathbb{Z}$ the *Macaulay* or *dense resultant*

Resultants modulo p

Resultants modulo p

$$\mathrm{Res}_{d_1,\ldots,d_n}(f_1,\ldots,f_n) = p_1^{a_1}\ldots p_N^{a_N}$$

Resultants modulo p

$$\mathrm{Res}_{d_1,\ldots,d_n}(f_1,\ldots,f_n) = p_1^{a_1}\ldots p_N^{a_N}$$

The system $f_1 \bmod p = \ldots f_n \bmod p = 0$ has a solution in $\mathbb{P}^{n-1}_{\overline{\mathbb{F}_p}}$

Resultants modulo p

$$\mathrm{Res}_{d_1,\ldots,d_n}(f_1,\ldots,f_n) = p_1^{a_1}\ldots p_N^{a_N}$$

The system $f_1 \bmod p = \ldots f_n \bmod p = 0$ has a solution in $\mathbb{P}^{n-1}_{\overline{\mathbb{F}_p}}$

$$\iff p \neq p_i,\ i = 1,\ldots,N$$

But what is $p = p_i$?

But what is $p = p_i$?

Then we know that

$$\emptyset \neq V_{p_i}(f_1, \ldots, f_n) \subset \mathbb{P}^{n-1}_{\overline{\mathbb{F}_{p_i}}}$$

But what is $p = p_i$?

Then we know that

$$\emptyset \neq V_{p_i}(f_1, \ldots, f_n) \subset \mathbb{P}^{n-1}_{\overline{\mathbb{F}_{p_i}}}$$

Can we say something about a_i?

But what is $p = p_i$?

Then we know that

$$\emptyset \neq V_{p_i}(f_1, \ldots, f_n) \subset \mathbb{P}^{n-1}_{\overline{\mathbb{F}_{p_i}}}$$

Can we say something about a_i?

Is geometry related with arithmetics?

$n = 2$

$$\mathrm{Res}(f_1, f_2) = 0 \bmod p \iff \deg(\gcd(f_1 \bmod p, f_2 \bmod p)) > 0$$

$n = 2$

$$\mathrm{Res}(f_1, f_2) = 0 \bmod p \iff \deg(\gcd(f_1 \bmod p, f_2 \bmod p)) > 0$$

$$\boxed{p^{\deg(\gcd(f_1 \bmod p, f_2 \bmod p))} \mid \mathrm{Res}(f_1, f_2)}$$

(Gomez-Gutierrez-Ibeas-Sevilla 2009)

In General...

In General...

- A a factorial ring

In General...

- A a factorial ring
- $p \in A$ an irreducible element

In General...

- A a factorial ring
- $p \in A$ an irreducible element
- $f_1, \ldots, f_n \in A[X_1, \ldots, X_n]$ homogeneous of degrees $d_1, \ldots, d_n$

In General...

- A a factorial ring
- $p \in A$ an irreducible element
- $f_1, \ldots, f_n \in A[X_1, \ldots, X_n]$ homogeneous of degrees $d_1, \ldots, d_n$
- $\mathrm{Res}_{d_1,\ldots,d_n}(f_1, \ldots, f_n) \in A$ the *homogeneous* or *dense resultant*

Numerical invariants

Numerical invariants

For the ideal $I_p := \langle f_1, \ldots, f_n \rangle \subset R_p := (K(A)/p)\,[x_1, \ldots, x_n]$

Numerical invariants

For the ideal $I_p := \langle f_1, \ldots, f_n \rangle \subset R_p := (K(A)/p)\,[x_1, \ldots, x_n]$

- **degree** $d_p = \dim\left(R_p/I_p\right)_t$ for $t \gg 0$

Numerical invariants

For the ideal $I_p := \langle f_1, \ldots, f_n \rangle \subset R_p := (K(A)/p)[x_1, \ldots, x_n]$

- **degree** $d_p = \dim (R_p/I_p)_t$ for $t \gg 0$
- **Hilbert-Samuel multiplicity** $e_p := \min\{d_p(J_p),\ J_p \subset I_p\}, J_p$ generated by $n-1$ elements

Known

(Chardin, Teissier, Rémond,...)

If $\dim \left(V_p(f_1, \ldots, f_n) \right) \leq 0$

Known

(Chardin, Teissier, Rémond,...)

If $\dim \left(V_p(f_1, \ldots, f_n) \right) \leq 0$

$$\boxed{\mathrm{val}_p \left(\mathrm{Res}(f_1, \ldots, f_n) \right) \geq d_p}$$

Our result

(Busé-D-Sombra 2017)

If $\dim\left(V_p(f_1,\ldots,f_n)\right) \leq 0$

Our result

(Busé-D-Sombra 2017)

If $\dim\left(V_p(f_1,\ldots,f_n)\right)\leq 0$

$$\boxed{\mathrm{val}_p\left(\mathrm{Res}(f_1,\ldots,f_n)\right)\geq e_p}$$

Our result

(Busé-D-Sombra 2017)

If $\dim\left(V_p(f_1,\ldots,f_n)\right) \leq 0$

$$\boxed{\mathrm{val}_p\left(\mathrm{Res}(f_1,\ldots,f_n)\right) \geq e_p}$$

Equality holds if a polynomial of minimal degree f_i is replaced by a "generic" $f_i + pF_i$

Corollary

The factorization of the resultant actually bounds the (finite) zeroes modulo p

Corollary

The factorization of the resultant actually bounds the (finite) zeroes modulo p for all p!

$$\boxed{p^{e_p} | \mathrm{Res}(f_1, \dots, f_{n+1})}$$

The univariate Theorem revisited

$$\deg(\gcd(f_1 \bmod p, f_2 \bmod p))$$
$$=$$
$$e_p = d_p$$
$$=$$
$$\deg(V_p(f_1, f_2))$$

(Gomez-Gutierrez-Ibeas-Sevilla 2009)

Remarks

- The result works under the (generic) hypothesis of finiteness modulo p

Remarks

- The result works under the (generic) hypothesis of finiteness modulo p
- Bound is sharp but the “gap” may be be large

Remarks

- The result works under the (generic) hypothesis of finiteness modulo p
- Bound is sharp but the “gap” may be be large
- Not a clear “algorithm” for deciding if $\dim\left(V_p(f_1, \ldots, f_n)\right) > 0$

Idea of our proof

- "Remove" the zeroes from the infinite & get $f_1, \ldots, f_{n-1}$ general complete intersection

Idea of our proof

- "Remove" the zeroes from the infinite & get $f_1, \ldots, f_{n-1}$ general complete intersection (linear change of coordinates)

Idea of our proof

- "Remove" the zeroes from the infinite & get $f_1, \ldots, f_{n-1}$ general complete intersection (linear change of coordinates)
- $\mathrm{val}_p(\xi_j) \in \mathbb{Z}_{\geq 0} \forall \xi \in V(f_1, \ldots, f_{n-1})$

Idea of our proof

- "Remove" the zeroes from the infinite & get $f_1, \ldots, f_{n-1}$ general complete intersection (linear change of coordinates)
- $\text{val}_p(\xi_j) \in \mathbb{Z}_{\geq 0} \forall \xi \in V(f_1, ..., f_{n-1})$
- $\text{val}_p(f_n(\xi)) \geq 1 \forall \xi \in V_p(f_1, \ldots, f_n)$

Idea of our proof

- "Remove" the zeroes from the infinite & get $f_1, \ldots, f_{n-1}$ general complete intersection (linear change of coordinates)
- $\mathrm{val}_p(\xi_j) \in \mathbb{Z}_{\geq 0} \forall \xi \in V(f_1, ..., f_{n-1})$
- $\mathrm{val}_p(f_n(\xi)) \geq 1 \forall \xi \in V_p(f_1, \ldots, f_n)$
- Poisson formula

Applications 1

Applications 1

- GCP $\mathrm{Res}(f_1 + t x_1^{d_1}, \ldots, f_n + t x_n^{d_n})$

Applications 1

- GCP $\mathrm{Res}(f_1 + tx_1^{d_1}, \ldots, f_n + tx_n^{d_n}) = t^{e(f_1,\ldots,f_n)}\,\mathcal{O}(1)$

Applications 1

- GCP $\mathrm{Res}(f_1 + tx_1^{d_1}, \ldots, f_n + tx_n^{d_n}) = t^{e(f_1,\ldots,f_n)}\,\mathcal{O}(1)$
- The "Milnor Number" $e(J_f) = \mathrm{val}_t\,(\mathrm{Disc}(f + tF))$ (Pham-Teissier)

Applications 1

- GCP $\mathrm{Res}(f_1 + t x_1^{d_1}, \ldots, f_n + t x_n^{d_n}) = t^{e(f_1,\ldots,f_n)}\mathcal{O}(1)$
- The "Milnor Number" $e(J_f) = \mathrm{val}_t\,(\mathrm{Disc}(f + tF))$ (Pham-Teissier)
- Number of roots of tropical polynomials (Hong-Sendra)

Applications 2

- Polynomial Dynamical Systems modulo p (Shparlinski)

Applications 2

- Polynomial Dynamical Systems modulo p (Shparlinski)
- Removing the "extraneous factor" in the computation of the "Salmon Polynomial" (Busé-Chardin-**D**-Sombra-Weimann2017)

Generalizations?

- Everybody uses that $\mathrm{Res}(f_1, \ldots, f_n) \bmod p = \mathrm{Res}(f_1 \bmod p, \ldots, f_n \bmod p)$

Generalizations?

- Everybody uses that $\mathrm{Res}(f_1, \ldots, f_n) \bmod p = \mathrm{Res}(f_1 \bmod p, \ldots, f_n \bmod p)$
- We also use Poisson formula & linear change of coordinates

Generalizations?

- Everybody uses that $\mathrm{Res}(f_1, \ldots, f_n) \bmod p = \mathrm{Res}(f_1 \bmod p, \ldots, f_n \bmod p)$
- We also use Poisson formula & linear change of coordinates
- Makes hard to adapt to **sparse resultants** and **subresultants**


"That's all Folks!"