

Resultants modulo p

Carlos D'Andrea

July 28th 2016

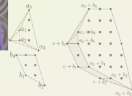
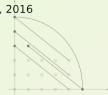


Computational Algebra, Algebraic Geometry and Applications

A conference in honor of

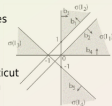
Alicia Dickenstein

Buenos Aires, Argentina, August 1-3, 2016



Invited Speakers:

- Carolina Araujo** - Rio de Janeiro
- Laurent Busé** - Nice
- Eduardo Cattani** - Amherst
- David Cox** - Amherst
- Fernando Cukierman** - Buenos Aires
- Sandra Di Rocco** - Stockholm
- Gabriela Jeronimo** - Buenos Aires
- Teresa Krick** - Buenos Aires
- Reinhard Laubenbacher** - Connecticut
- Laura Matusevich** - College Station
- Roberto Miatello** - Córdoba
- Bernard Mourrain** - Nice
- Marie-Françoise Roy** - Rennes
- Juan Sabia** - Buenos Aires
- Aron Simis** - Pernambuco
- Frank Sottile** - College Station
- Frank Sturmfels** - Berkeley



Organizing Committee:

- Nicolás Botbol
- Carlos D'Andrea
- Mercedes Pérez Millán

<http://mate.dm.uba.ar/~coalaga/>



Univariate Resultants

$$\begin{cases} f_1 = a_{10}x_0^{d_1} + a_{11}x_0^{d_1-1}x_1 + \dots + a_{1d_1}x_1^{d_1} \\ f_2 = a_{20}x_0^{d_2} + a_{21}x_0^{d_2-1}x_1 + \dots + a_{2d_2}x_1^{d_2} \end{cases}$$

Univariate Resultants

$$\begin{cases} f_1 = a_{10}x_0^{d_1} + a_{11}x_0^{d_1-1}x_1 + \dots + a_{1d_1}x_1^{d_1} \\ f_2 = a_{20}x_0^{d_2} + a_{21}x_0^{d_2-1}x_1 + \dots + a_{2d_2}x_1^{d_2} \end{cases}$$

$$\text{Res}(f_1, f_2) = \det \begin{pmatrix} a_{10} & a_{11} & \dots & a_{1d_1} & 0 & \dots & 0 \\ 0 & a_{10} & \dots & a_{1d_1-1} & a_{1d_1} & \dots & 0 \\ \vdots & \vdots & \ddots & \dots & \dots & \ddots & \vdots \\ 0 & 0 & \dots & a_{10} & \dots & \dots & a_{1d_1} \\ a_{20} & a_{21} & \dots & a_{2d_2} & 0 & \dots & 0 \\ 0 & a_{20} & \dots & a_{2d_2-1} & a_{2d_2} & \dots & 0 \\ \vdots & \vdots & \ddots & \dots & \dots & \ddots & \vdots \\ 0 & 0 & \dots & a_{20} & \dots & \dots & a_{2d_2} \end{pmatrix}$$

Resultants modulo p

$$f_1, f_2 \in \mathbb{Z}[x_1, x_2] \implies \text{Res}(f_1, f_2) \in \mathbb{Z}$$

Resultants modulo p

$$\begin{aligned} f_1, f_2 \in \mathbb{Z}[x_1, x_2] &\implies \text{Res}(f_1, f_2) \in \mathbb{Z} \\ \text{Res}(f_1, f_2) = 0 \pmod{p} &\iff \\ \deg(\gcd(f_1 \pmod{p}, f_2 \pmod{p})) &> 0 \end{aligned}$$

Resultants modulo p

$$f_1, f_2 \in \mathbb{Z}[x_1, x_2] \implies \text{Res}(f_1, f_2) \in \mathbb{Z}$$
$$\text{Res}(f_1, f_2) = 0 \pmod{p} \iff$$
$$\deg(\gcd(f_1 \pmod{p}, f_2 \pmod{p})) > 0$$

$$p^{\deg(\gcd(f_1 \pmod{p}, f_2 \pmod{p}))} \mid \text{Res}(f_1, f_2)$$

(Gomez-Gutierrez-Ibeas-Sevilla 2009)

This fact has been used!

(Chang-D-Ostafe-Shparlinski-Sombra 2016)

This fact has been used!

(Chang-D-Ostafe-Shparlinski-Sombra 2016)

bounding the cardinality of the
reduction mod p of lengths of orbits
of pairs of univariate dynamical
systems

Igor Shparlinski's Question

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

Igor Shparlinski's Question

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

How general is this?



Vanishing of Resultantes modulo p

(Busé-D-Sombra 2016)

$$\left\{ \begin{array}{l} f_1 = \sum_{\alpha_0 + \dots + \alpha_n = d_1} a_{1, \alpha_0, \dots, \alpha_n} X_0^{\alpha_0} \dots X_n^{\alpha_n} \\ f_2 = \sum_{\alpha_0 + \dots + \alpha_n = d_2} a_{2, \alpha_0, \dots, \alpha_n} X_0^{\alpha_0} \dots X_n^{\alpha_n} \\ \vdots \\ f_{n+1} = \sum_{\alpha_0 + \dots + \alpha_n = d_{n+1}} a_{n+1, \alpha_0, \dots, \alpha_n} X_0^{\alpha_0} \dots X_n^{\alpha_n} \end{array} \right.$$

Vanishing of Resultantes modulo p

(Busé-D-Sombra 2016)

$$\left\{ \begin{array}{l} f_1 = \sum_{\alpha_0 + \dots + \alpha_n = d_1} a_{1, \alpha_0, \dots, \alpha_n} x_0^{\alpha_0} \dots x_n^{\alpha_n} \\ f_2 = \sum_{\alpha_0 + \dots + \alpha_n = d_2} a_{2, \alpha_0, \dots, \alpha_n} x_0^{\alpha_0} \dots x_n^{\alpha_n} \\ \vdots \\ f_{n+1} = \sum_{\alpha_0 + \dots + \alpha_n = d_{n+1}} a_{n+1, \alpha_0, \dots, \alpha_n} x_0^{\alpha_0} \dots x_n^{\alpha_n} \end{array} \right.$$

$$f_1, \dots, f_{n+1} \in \mathbb{Z}[\underline{x}] \implies \text{Res}(f_1, \dots, f_{n+1}) \in \mathbb{Z}$$

Known case

If $d_1 = d_2 = \dots = d_{n+1} = 1$, then

$$\text{Res}(f_1, \dots, f_{n+1}) = \det (a_{ij})_{1 \leq i, j \leq n+1}$$

A non trivial example

$$f_0 = a_{00}x_0 + a_{01}x_1 + a_{02}x_2$$

$$f_1 = a_{10}x_0 + a_{11}x_1 + a_{12}x_2$$

$$f_2 = a_{20}x_0^2 + a_{21}x_0x_1 + a_{22}x_0x_2 + a_{23}x_1^2 + a_{24}x_1x_2 + a_{25}x_2^2$$

A non trivial example

$$f_0 = a_{00}x_0 + a_{01}x_1 + a_{02}x_2$$

$$f_1 = a_{10}x_0 + a_{11}x_1 + a_{12}x_2$$

$$f_2 = a_{20}x_0^2 + a_{21}x_0x_1 + a_{22}x_0x_2 + a_{23}x_1^2 + a_{24}x_1x_2 + a_{25}x_2^2$$

$$\begin{aligned} \text{Res}(f_0, f_1, f_2) = & a_{00}^2 a_{11}^2 a_{25} - a_{00}^2 a_{11} a_{12} a_{24} + a_{00}^2 a_{12}^2 a_{23} \\ & - 2a_{00} a_{01} a_{10} a_{11} a_{25} + a_{00} a_{01} a_{10} a_{12} a_{24} + a_{00} a_{01} a_{11} a_{12} a_{22} \\ & - a_{00} a_{01} a_{12}^2 a_{21} + a_{00} a_{02} a_{10} a_{11} a_{24} - 2a_{00} a_{02} a_{10} a_{12} a_{23} \\ & - a_{00} a_{02} a_{11}^2 a_{22} + a_{00} a_{02} a_{11} a_{12} a_{21} + a_{01}^2 a_{10}^2 a_{25} \\ & - a_{01}^2 a_{10} a_{12} a_{22} + a_{01}^2 a_{12}^2 a_{20} - a_{01} a_{02} a_{10}^2 a_{24} \\ & + a_{01} a_{02} a_{10} a_{11} a_{22} + a_{01} a_{02} a_{10} a_{12} a_{21} - 2a_{01} a_{02} a_{11} a_{12} a_{20} \\ & + a_{02}^2 a_{10}^2 a_{23} - a_{02}^2 a_{10} a_{11} a_{21} + a_{02}^2 a_{11}^2 a_{20} \end{aligned}$$

Properties of $\text{Res}(f_1, \dots, f_{n+1})$

- It is irreducible

Properties of $\text{Res}(f_1, \dots, f_{n+1})$

- It is irreducible
- It is homogeneous in each group of variables, of degree $\frac{d_1 \cdot d_2 \cdot \dots \cdot d_{n+1}}{d_i}$

Properties of $\text{Res}(f_1, \dots, f_{n+1})$

- It is irreducible
- It is homogeneous in each group of variables, of degree $\frac{d_1 \cdot d_2 \cdot \dots \cdot d_{n+1}}{d_i}$
- It is invariant under linear changes of coordinates

Geometric Properties

Geometric Properties

- $\text{Res}(f_1, \dots, f_{n+1}) = 0 \iff$
 $\exists \xi \in \mathbb{P}^n$ such that
 $f_1(\xi) = \dots = f_{n+1}(\xi) = 0$

Geometric Properties

- $\text{Res}(f_1, \dots, f_{n+1}) = 0 \iff$
 $\exists \xi \in \mathbb{P}^n$ such that
 $f_1(\xi) = \dots = f_{n+1}(\xi) = 0$

- Poisson Formula:

$$\begin{aligned} & \text{Res}(f_1, \dots, f_{n+1}) \\ & = \\ & \text{Res}(f_1^0, \dots, f_n^0)^{d_{n+1}} \prod_{\xi \in V(f_1^1, \dots, f_n^1)} f_{n+1}(\xi) \end{aligned}$$

Resolution of systems of polynomials

$$P(u_0, u_i) = \text{Res}(u_i x_0 - u_0 x_i, f_1, \dots, f_n)$$

Resolution of systems of polynomials

$$P(u_0, u_i) = \text{Res}(u_i x_0 - u_0 x_i, f_1, \dots, f_n)$$

can be used to compute the
coordinates of the (finite) roots of
the system

$$f_1 = 0, \dots, f_n = 0$$

Computation

$$\mathcal{R}(f_0, f_1, f_2) = \det \begin{bmatrix} -b_1 & -b_3 & 0 & a_1 & a_3 & 0 & 0 & 0 & 0 & 0 \\ -b_0 & -b_2 & 0 & a_0 & a_2 & 0 & 0 & 0 & 0 & 0 \\ 0 & -b_1 & -b_3 & 0 & a_1 & a_3 & 0 & 0 & 0 & 0 \\ 0 & -b_0 & -b_2 & 0 & a_0 & a_2 & 0 & 0 & 0 & 0 \\ -c_4 & -c_5 & -c_6 & 0 & 0 & 0 & a_1 & 0 & a_3 & 0 \\ -c_1 & -c_3 & -c_7 & 0 & 0 & 0 & a_0 & a_1 & a_2 & a_3 \\ -c_0 & -c_2 & -c_6 & 0 & 0 & 0 & 0 & a_0 & 0 & a_2 \\ 0 & 0 & 0 & -c_4 & -c_5 & -c_6 & b_1 & 0 & b_3 & 0 \\ 0 & 0 & 0 & -c_1 & -c_3 & -c_7 & b_0 & b_1 & b_2 & b_3 \\ 0 & 0 & 0 & -c_0 & -c_2 & -c_6 & 0 & b_0 & 0 & b_2 \end{bmatrix}$$

Resultants modulo p

(Busé-D-Sombra 2016)

If $\dim (V_p(f_1, \dots, f_{n+1})) \leq 0$

Resultants modulo p

(Busé-D-Sombra 2016)

If $\dim (V_p(f_1, \dots, f_{n+1})) \leq 0$
 $N_p := \deg (V_p(f_1, \dots, f_{n+1}))$

Resultants modulo p

(Busé-D-Sombra 2016)

If $\dim (V_p(f_1, \dots, f_{n+1})) \leq 0$
 $N_p := \deg (V_p(f_1, \dots, f_{n+1}))$

$$p^{N_p} \mid \text{Res}(f_1, \dots, f_{n+1})$$

Corollary

$$p^{N_p} \mid \text{Res}(f_1, \dots, f_{n+1})$$

Corollary

$$p^{N_p} \mid \text{Res}(f_1, \dots, f_{n+1})$$

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

Corollary

$$p^{N_p} \mid \text{Res}(f_1, \dots, f_{n+1})$$

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

The Cantabrian Theorem revisited

$$\begin{aligned} \deg(\gcd(f_1 \bmod p, f_2 \bmod p)) \\ &= \\ N_p \\ &= \\ \deg(V_p(f_1, f_2)) \end{aligned}$$

(Gomez-Gutierrez-Ibeas-Sevilla 2009)



Remarks

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

Remarks

- Still the result works under the (generic) hypothesis of finiteness modulo p
- the “gap” in the bound can be large

Remarks

- Still the result works under the (generic) hypothesis of finiteness modulo p
- the “gap” in the bound can be large
- Not a clear “algorithm” for $\dim (V_p(f_1, \dots, f_{n+1})) > 0$

Idea of our proof

- “Remove” all the zeroes from the infinite

Idea of our proof

- “Remove” all the zeroes from the infinite (linear change of coordinates)

Idea of our proof

- “Remove” all the zeroes from the infinite (linear change of coordinates)
- Apply Poisson formula

Idea of our proof

- “Remove” all the zeroes from the infinite (linear change of coordinates)
- Apply Poisson formula
- Get a “determinantal” version of Poisson modulo p

Idea of our proof

- “Remove” all the zeroes from the infinite (linear change of coordinates)
- Apply Poisson formula
- Get a “determinantal” version of Poisson modulo p
- Compute the dimension of the Nullspace of the determinantal matrix

Generalizations and Extensions

- One could get a refinement of the exponent by taking into account the valuation mod p of the roots (Smirnov's Theorem)

Generalizations and Extensions

- One could get a refinement of the exponent by taking into account the valuation mod p of the roots (Smirnov's Theorem)
- Slight generalization to *sparse resultants* under stronger hypothesis

Generalizations and Extensions

- One could get a refinement of the exponent by taking into account the valuation mod p of the roots (Smirnov's Theorem)
- Slight generalization to *sparse resultants* under stronger hypothesis
- The result holds for any domain, for instance polynomials with coefficients in $R[y_1, \dots, y_l]$

Applications

- Finding points in varieties modulo p
(Shparlinski)

Applications

- Finding points in varieties modulo p
(Shparlinski)
- The “Generalized Characteristic Polynomial”
revisited! (Mourrain)

Applications

- Finding points in varieties modulo p
(Shparlinski)
- The “Generalized Characteristic Polynomial”
revisited! (Mourrain)
- “Extraneous factors” in the Computation of the
“Salmon Polynomial”
(Busé-Chardin-D-Sombra-Weimann)

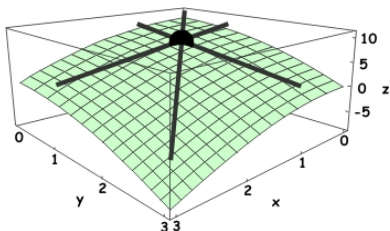
Computation of the Salmon Polynomial

(Busé-Chardin-D-Sombra-Weimann)

$$\mathbb{Z} \leftrightarrow \mathbb{C}[x, y, z, h] / \langle f(x, y, z, h) \rangle$$

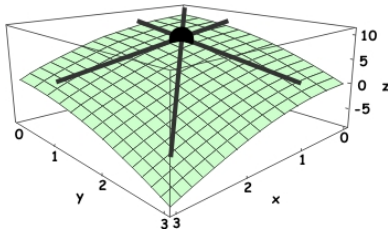
$$p \leftrightarrow h$$

Salmon's polynomial



A point b in a surface $S \subset \mathbb{C}^3$ is called *flex* (or *inflection*) of S

Salmon's polynomial



A point b in a surface $S \subset \mathbb{C}^3$ is called *flex* (or *inflection*) of S if there exists a line passing through b having contact order at least 3 with S

Theorem (Salmon, 1862)

If $S = V(f(x, y, z)) \subset \mathbb{C}^3$ of degree d , and not ruled, there is

$F_f(x, y, z) \in \mathbb{C}[x, y, z]$ of degree $\leq 11d - 24$ such that

$$\text{Flex}(S) = V(f(x, y, z), F_f(x, y, z))$$



Computing $F_f(x, y, z)$

$$f((x, y, z) + t(u, v, w)) =$$

Computing $F_f(x, y, z)$

$$\begin{aligned} f((x, y, z) + t(u, v, w)) = & \\ f(x, y, z) + t f_1(x, y, z; u, v, w) + & \\ t^2 f_2(x, y, z; u, v, w) + & \\ t^3 f_3(x, y, z; u, v, w) + \mathcal{O}(t^4) & \end{aligned}$$

Computing $F_f(x, y, z)$

The “candidate” for $F_f(x, y, z)$ should be the resultant in (u, v, w) of

- $f_1(x, y, z; u, v, w)$
- $f_2(x, y, z; u, v, w)$
- $f_3(x, y, z; u, v, w)$

Janos Kollár (Adv. Math. 2015)

“I get a polynomial of degree $11d - 18$. Salmon claims that in fact the degree should be $11d - 24$. I have not checked this”

Terence Tao (blog, 2014)

“The original proof of the Cayley-Salmon theorem, dating back to at least 1915, is not easily accessible and not written in modern language”

Our Result

(Busé-Chardin-D-Sombra-Weimann)

Modulo $f(x, y, z, h)$, if we set $h = 0$
we get a nontrivial solution of the
system of multiplicity 6

Our Result

(Busé-Chardin-D-Sombra-Weimann)

Modulo $f(x, y, z, h)$, if we set $h = 0$
we get a nontrivial solution of the
system of multiplicity 6

$$\begin{aligned} & \text{Res}(f_1, f_2, f_3) \\ & = \\ & h^6 \cdot F_f(x, y, z) \bmod f(x, y, z, h) \end{aligned}$$

FoCM 2017
Foundations of Computational Mathematics
Barcelona, July 10th-19th, 2017

<http://www.ub.edu/focm2017>

Workshops

- Approximation Theory
- Computational Algebraic Geometry
- Computational Dynamics
- Computational Harmonic Analysis and Compressive Sensing
- Computational Mathematical Biology with emphasis on the Genome
- Computational Number Theory
- Computational Geometry and Topology
- Continuous Optimization
- Foundations of Numerical PDEs
- Geometric Integration and Computational Mechanics
- Graph Theory and Combinatorics
- Information-based Complexity
- Learning Theory
- Mathematical Foundations of Data Acquisition and Inverse Problems
- Multiresolution and Adaptivity in Numerical PDEs
- Numerical Linear Algebra
- Random Matrices
- Fast Number Complexity
- Ring of Polynomials and Orthogonal Polynomials
- Symbolic Computation
- Symbolic Algebra

Microsoft
 Intel
 IBM
 Google
 Oracle
 SAP
 AWS

Plenary Speakers

- Karim Adigralsho
- Jean-David Benamou
- Alexei Borodin
- Mirielle Bousquet-Mélou
- Mark Braverman
- Claudio Canuto
- Martin Haier
- Pierre Lafitte
- Monique Laurent
- Melvin Look
- Gábor Lugosi
- Bruno Salvy
- Sylvia Serfaty
- Steve Smolm
- Andrew Stuart
- Roman Vershynin
- Shmuel Weinberger



FoCM 2017
Foundations of Computational Mathematics
Barcelona, July 10th-19th, 2017

<http://www.ub.edu/focm2017>

Workshops

- Approximation Theory
- Computational Algebraic Geometry
- Computational Dynamics
- Computational Harmonic Analysis and Compressive Sensing
- Computational Mathematical Biology with emphasis on the Genome
- Computational Number Theory
- Computational Geometry and Topology
- Continuous Optimization
- Foundations of Numerical PDEs
- Geometric Integration and Computational Mechanics
- Graph Theory and Combinatorics
- Information-based Complexity
- Learning Theory
- Mathematical Foundations of Data Acquisition and Inverse Problems
- Multiscale and Adaptive Numerical PDEs
- Numerical Linear Algebra
- Reverse Mode
- Fast Number Complexity
- Ring of Polynomials and Orthogonal Polynomials
- Symbolic Computation

Plenary Speakers

- Karim Adigralho
- Jean-David Benamou
- Alexei Borodin
- Mirella Bousquet-Mélou
- Mark Branner
- Claudio Canuto
- Martin Hairer
- Pierre Lafitte
- Monique Laurent
- Melvin Leok
- Gábor Lugosi
- Bruno Salvy
- Sylvia Serfaty
- Steve Smale
- Andrew Stuart
- Roman Vershynin
- Stefan Weinberger



Thanks!

