Elimination Theory in Positive Characteristic

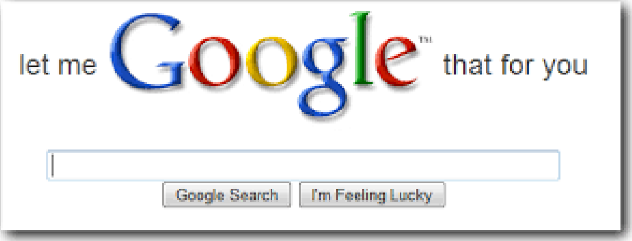
Carlos D'Andrea

June 23rd, 2016

UNIVERSITAT DE BARCELONA

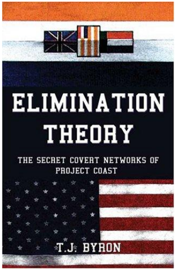
What is Elimination Theory?

What is Elimination Theory?

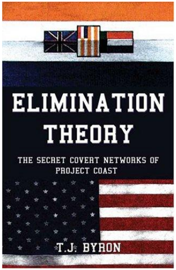


Elimination Theory

Elimination Theory

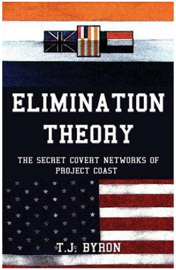


Elimination Theory



$$\operatorname{Res}(f(x),\ g(x)) = \begin{vmatrix} a_m & a_{m-1} & \cdots & a_1 & a_0 & 0 & \cdots & 0 \\ 0 & a_m & a_{m-1} & \cdots & a_1 & a_0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \cdots & 0 & a_m & a_{m-1} & \cdots & a_1 & a_0 \\ b_n & b_{n-1} & \cdots & b_1 & b_0 & 0 & \cdots & 0 \\ 0 & b_n & b_{n-1} & \cdots & b_1 & b_0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \cdots & 0 & b_n & b_{n-1} & \cdots & b_1 & b_0 \end{vmatrix}.$$

Elimination Theory



$$\mathrm{Res}(f(x),\ g(x)) = \begin{vmatrix} a_m & a_{m-1} & \cdots & a_1 & a_0 & 0 & \cdots & 0 \\ 0 & a_m & a_{m-1} & \cdots & a_1 & a_0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \cdots & 0 & a_m & a_{m-1} & \cdots & a_1 & a_0 \\ b_n & b_{n-1} & \cdots & b_1 & b_0 & 0 & \cdots & 0 \\ 0 & b_n & b_{n-1} & \cdots & b_1 & b_0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \cdots & 0 & b_n & b_{n-1} & \cdots & b_1 & b_0 \end{vmatrix}.$$

Important for both algorithmic and complexity aspects of polynomial system solving

The Example: Determinants

Find "the condition" on

$a_{10}, a_{11}, a_{20}, a_{21}$ so that the system

$$\begin{cases} a_{10}x_0 + a_{11}x_1 = 0 \\ a_{20}x_0 + a_{21}x_1 = 0 \end{cases}$$

has a solution different from $(0,0)$

Elimination Theory

$$a_{10}x_0 + a_{11}x_1, \; a_{20}x_0 + a_{21}x_1$$

$$\in \mathbb{K}[a_{10}, a_{11}, a_{20}, a_{21}, x_0, x_1]$$

Elimination Theory

$$a_{10}x_0 + a_{11}x_1,\ a_{20}x_0 + a_{21}x_1$$

$$\in \mathbb{K}[a_{10}, a_{11}, a_{20}, a_{21}, x_0, x_1]$$
$$\downarrow$$
$$a_{10}a_{21} - a_{20}a_{11} \in \mathbb{K}[a_{10}, a_{11}, a_{20}, a_{21}]$$

More general

Find "the condition" for the system

$$\begin{cases} a_{10}x_0 + a_{11}x_1 + \ldots + a_{1n}x_n & = & 0 \\ a_{20}x_0 + a_{21}x_1 + \ldots + a_{2n}x_n & = & 0 \\ \vdots & \vdots & \vdots \\ a_{(n+1)0}x_0 + a_{(n+1)1}x_1 + \ldots + a_{(n+1)n}x_n & = & 0 \end{cases}$$

More general

Find "the condition" for the system

$$\begin{cases} a_{10}x_0 + a_{11}x_1 + \ldots + a_{1n}x_n & = & 0 \\ a_{20}x_0 + a_{21}x_1 + \ldots + a_{2n}x_n & = & 0 \\ \vdots & \vdots & \vdots \\ a_{(n+1)0}x_0 + a_{(n+1)1}x_1 + \ldots + a_{(n+1)n}x_n & = & 0 \end{cases}$$

to have a solution different from

$$(0, 0, \ldots, 0)$$

Another more general

Let $d_1, d_2 \in \mathbb{N}$. Find "the condition" for the system of polynomials

$$\begin{cases} a_{10}{x_0}^{d_1} + a_{11}{x_0}^{d_1-1}x_1 + \ldots &= 0 \\ a_{20}{x_0}^{d_2} + a_{21}{x_0}^{d_2-1}x_1 + \ldots &= 0 \end{cases}$$

to have a solution different from $(0,0)$

More more more general...

Let $n \in \mathbb{N}$, and $d_1, \ldots, d_{n+1} \in \mathbb{N}$, find the condition for

$$\left\{\begin{array}{lcl} \sum_{\alpha_0+\ldots+\alpha_n=d_1} a_{1,\alpha_0,\ldots,\alpha_n} {x_0}^{\alpha_0} \ldots {x_n}^{\alpha_n} & = & 0 \\ \sum_{\alpha_0+\ldots+\alpha_n=d_2} a_{2,\alpha_0,\ldots,\alpha_n} {x_0}^{\alpha_0} \ldots {x_n}^{\alpha_n} & = & 0 \\ \vdots & \vdots & \vdots \\ \sum_{\alpha_0+\ldots+\alpha_n=d_{n+1}} a_{n+1,\alpha_0,\ldots,\alpha_n} {x_0}^{\alpha_0} \ldots {x_n}^{\alpha_n} & = & 0 \end{array}\right.$$

to have a solution different from $(0, 0, \ldots, 0)$

Elimination: The general problem

For $\mathbf{a} = (a_1, \ldots, a_N)$, $k, n \in \mathbb{N}$ let $f_1(\mathbf{a}, x_1, \ldots, x_n), \ldots, f_k(\mathbf{a}, x_1, \ldots, x_n) \in \mathbb{K}[\mathbf{a}, x_1, \ldots, x_n]$. Find conditions on $\mathbf{a}$ such that

$$\begin{cases} f_1(\mathbf{a}, x_1, \ldots, x_n) & = & 0 \\ f_2(\mathbf{a}, x_1, \ldots, x_n) & = & 0 \\ \vdots & \vdots & \vdots \\ f_k(\mathbf{a}, x_1, \ldots, x_n) & = & 0 \end{cases}$$

has a solution

Solution?

- Depends on the ground field

Solution?

- Depends on the ground field
- There is not necessarily a “closed” condition

Solution?

- Depends on the ground field
- There is not necessarily a "closed" condition
- The computation of the conditions may be out of control

Easy example

$$\begin{cases} a_{11}x_1 + \ldots + a_{1n}x_n & = & 0 \\ a_{21}x_1 + \ldots + a_{2n}x_n & = & 0 \\ \vdots & \vdots & \vdots \\ a_{kn}x_1 + \ldots + a_{kn}x_n & = & 0 \end{cases}$$

with $k \geq n$

Easy example

$$\left\{\begin{array}{rcl} a_{11}x_1 + \ldots + a_{1n}x_n & = & 0 \\ a_{21}x_1 + \ldots + a_{2n}x_n & = & 0 \\ \vdots & \vdots & \vdots \\ a_{kn}x_1 + \ldots + a_{kn}x_n & = & 0 \end{array}\right.$$

with $k \geq n$

Conditions: all maximal minors of $\left(a_{ij}\right)_{1\leq i\leq k,\, 1\leq j\leq n}$ equal to zero

Another "easy" example

$$k = n = 1,$$

$$a_0 + a_1 x_1 + a_2 {x_1}^2 + \ldots + a_d {x_1}^d = 0$$

Another "easy" example

$$k = n = 1,$$

$$a_0 + a_1 x_1 + a_2 {x_1}^2 + \ldots + a_d {x_1}^d = 0$$

Conditions?

Geometry

$$V = \{(\mathbf{a}, x_1, \ldots, x_n) : f_1(\mathbf{a}, x_1, \ldots, x_n) = 0, \ldots f_k(\mathbf{a}, x_1, \ldots, x_n) = 0\}$$

Geometry

$$V = \{(\mathbf{a}, x_1, \ldots, x_n) : f_1(\mathbf{a}, x_1, \ldots, x_n) = 0, \ldots f_k(\mathbf{a}, x_1, \ldots, x_n) = 0\}$$

$$\begin{array}{ccc} V & \subset & \mathbb{K}^N \times \mathbb{K}^n \\ \downarrow \pi_1 & & \downarrow \pi_1 \\ \pi_1(V) & \subset & \mathbb{K}^N \end{array}$$

Geometry

$$V = \{(\mathbf{a}, x_1, \ldots, x_n) : f_1(\mathbf{a}, x_1, \ldots, x_n) = 0, \ldots f_k(\mathbf{a}, x_1, \ldots, x_n) = 0\}$$

$$\begin{array}{ccc} V & \subset & \mathbb{K}^N \times \mathbb{K}^n \\ \downarrow \pi_1 & & \downarrow \pi_1 \\ \pi_1(V) & \subset & \mathbb{K}^N \end{array}$$

The set of conditions is $\pi_1(\mathbf{V})$, not necessarily described by zeroes of polynomials

Elimination Theorem

$$V = \{(a, x_0, x_1, \ldots, x_n) : f_1(a, x_0, x_1, \ldots, x_n) = 0, \ldots f_k(a, x_0, x_1, \ldots, x_n) = 0\}$$

Elimination Theorem

$$V=\{(\mathbf{a},x_0,x_1,\ldots,x_n):\ f_1(\mathbf{a},x_0,x_1,\ldots,x_n)=0,\ldots f_k(\mathbf{a},x_0,x_1,\ldots,x_n)=0\}$$

$$\begin{array}{ccc} V & \subset & \mathbb{K}^N\times\mathbb{P}^n \\ \downarrow\pi_1 & & \downarrow\pi_1 \\ \pi_1(V) & \subset & \mathbb{K}^N \end{array}$$

Elimination Theorem

$$V = \{(\mathbf{a}, x_0, x_1, \ldots, x_n) : f_1(\mathbf{a}, x_0, x_1, \ldots, x_n) = 0, \ldots f_k(\mathbf{a}, x_0, x_1, \ldots, x_n) = 0\}$$

$$\begin{array}{ccc} V & \subset & \mathbb{K}^N \times \mathbb{P}^n \\ \downarrow \pi_1 & & \downarrow \pi_1 \\ \pi_1(V) & \subset & \mathbb{K}^N \end{array}$$

$$\pi_1(V) = \{p_1(\mathbf{a}) = 0, \ldots, p_\ell(\mathbf{a}) = 0\}$$

“The” Condition

$$V = \{(\mathbf{a}, x_0, x_1, \ldots, x_n) : f_1(\mathbf{a}, x_0, x_1, \ldots, x_n) = 0, \ldots, f_{n+1}(\mathbf{a}, x_0, x_1, \ldots, x_n) = 0\}$$

"The" Condition

$$V = \{(\mathbf{a}, x_0, x_1, \ldots, x_n) : f_1(\mathbf{a}, x_0, x_1, \ldots, x_n) = 0, \ldots, f_{n+1}(\mathbf{a}, x_0, x_1, \ldots, x_n) = 0\}$$

$$\begin{array}{ccc} V & \subset & \mathbb{K}^N \times \mathbb{P}^n \\ \downarrow \pi_1 & & \downarrow \pi_1 \\ \pi_1(V) & \subset & \mathbb{K}^N \end{array}$$

“The” Condition

$$V = \{(\mathbf{a}, x_0, x_1, \ldots, x_n) : f_1(\mathbf{a}, x_0, x_1, \ldots, x_n) = 0, \ldots, f_{n+1}(\mathbf{a}, x_0, x_1, \ldots, x_n) = 0\}$$

$$\begin{array}{ccc} V & \subset & \mathbb{K}^N \times \mathbb{P}^n \\ \downarrow \pi_1 & & \downarrow \pi_1 \\ \pi_1(V) & \subset & \mathbb{K}^N \end{array}$$

$$\boxed{\pi_1(V) = \{p_1(\mathbf{a}) = 0\}}$$

Example 1

$$\begin{cases} a_{00}x_0 + a_{01}x_1 + \ldots + a_{0n}x_n & = & 0 \\ a_{10}x_0 + a_{11}x_1 + \ldots + a_{1n}x_n & = & 0 \\ \vdots & \vdots & \vdots \\ a_{n0}x_0 + a_{n1}x_1 + \ldots + a_{nn}x_n & = & 0 \end{cases}$$

Example 1

$$\begin{cases} a_{00}x_0 + a_{01}x_1 + \ldots + a_{0n}x_n &= 0 \\ a_{10}x_0 + a_{11}x_1 + \ldots + a_{1n}x_n &= 0 \\ \vdots & \vdots \quad \vdots \\ a_{n0}x_0 + a_{n1}x_1 + \ldots + a_{nn}x_n &= 0 \end{cases}$$

$$\boxed{p_1(a) = \det(a_{ij})}$$

Example 2

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

Example 2

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

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

Example 3

$$\begin{cases} f_1 = \sum_{\alpha_0+\ldots+\alpha_n=d_1} a_{1,\alpha_0,\ldots,\alpha_n} x_0{}^{\alpha_0} \ldots x_n{}^{\alpha_n} \\ f_2 = \sum_{\alpha_0+\ldots+\alpha_n=d_2} a_{2,\alpha_0,\ldots,\alpha_n} x_0{}^{\alpha_0} \ldots x_n{}^{\alpha_n} \\ \vdots \\ f_{n+1} = \sum_{\alpha_0+\ldots+\alpha_n=d_{n+1}} a_{n+1,\alpha_0,\ldots,\alpha_n} x_0{}^{\alpha_0} \ldots x_n{}^{\alpha_n} \end{cases}$$

Example 3

$$\begin{cases} f_1 = \sum_{\alpha_0+\ldots+\alpha_n=d_1} a_{1,\alpha_0,\ldots,\alpha_n} x_0{}^{\alpha_0} \ldots x_n{}^{\alpha_n} \\ f_2 = \sum_{\alpha_0+\ldots+\alpha_n=d_2} a_{2,\alpha_0,\ldots,\alpha_n} x_0{}^{\alpha_0} \ldots x_n{}^{\alpha_n} \\ \vdots \\ f_{n+1} = \sum_{\alpha_0+\ldots+\alpha_n=d_{n+1}} a_{n+1,\alpha_0,\ldots,\alpha_n} x_0{}^{\alpha_0} \ldots x_n{}^{\alpha_n} \end{cases}$$

$$\boxed{\mathrm{Res}(f_1, f_2, \ldots, f_{n+1})}$$

The "elimination" dictionary

Linear **Polynomial**

The “elimination” dictionary

Linear	**Polynomial**
Gauss elimination	Gröbner Bases

The "elimination" dictionary

Linear	**Polynomial**
Gauss elimination	Gröbner Bases
Triangulation	Triangular systems

The "elimination" dictionary

Linear	**Polynomial**
Gauss elimination	Gröbner Bases
Triangulation	Triangular systems
Determinants	Resultants

The "elimination" dictionary

Linear	**Polynomial**
Gauss elimination	Gröbner Bases
Triangulation	Triangular systems
Determinants	Resultants
Cramer's rule	u-resultants
...	...

Positive characteristic

- The elimination theorems work independently of the characteristic of $\mathbb{K}$

Positive characteristic

- The elimination theorems work independently of the characteristic of $\mathbb{K}$
- We want to consider this scenario: $\mathbb{Z} \to \mathbb{F}_p$ for different primes $p \in \mathbb{Z}$

Warming-up example

$f = 15x^3 + x^2 - 5x + 1 \in \mathbb{Z}[x]$ has

Warming-up example

$f = 15x^3 + x^2 - 5x + 1 \in \mathbb{Z}[x]$ has

- 1 triple root if $p = 2$

Warming-up example

$f = 15x^3 + x^2 - 5x + 1 \in \mathbb{Z}[x]$ has

- 1 triple root if $p = 2$
- 1 double root if $p = 3$

Warming-up example

$f = 15x^3 + x^2 - 5x + 1 \in \mathbb{Z}[x]$ has

- 1 triple root if $p = 2$
- 1 double root if $p = 3$
- 2 different roots if $p = 5$

Warming-up example

$f = 15x^3 + x^2 - 5x + 1 \in \mathbb{Z}[x]$ has

- 1 triple root if $p = 2$
- 1 double root if $p = 3$
- 2 different roots if $p = 5$
- 3 different roots if $p \notin \{2, 3, 5\}$

Warming-up example

$f = 15x^3 + x^2 - 5x + 1 \in \mathbb{Z}[x]$ has

- 1 triple root if $p = 2$
- 1 double root if $p = 3$
- 2 different roots if $p = 5$
- 3 different roots if $p \notin \{2, 3, 5\}$
- 3 different roots over $\overline{\mathbb{Q}}$

Why do we care?

- Local-Global principles

Why do we care?

- Local-Global principles
- Chinese Remainder like methods

Why do we care?

- Local-Global principles
- Chinese Remainder like methods
- Newton-like methods

Why do we care?

- Local-Global principles
- Chinese Remainder like methods
- Newton-like methods
- Dynamical systems modulo p

Why do we care?

- Local-Global principles
- Chinese Remainder like methods
- Newton-like methods
- Dynamical systems modulo p
- ...

Local-Global Elimination Challenge

Given $f_1, \ldots, f_k \in \mathbb{Z}[x_1, \ldots, x_n]$

Local-Global Elimination Challenge

Given $f_1, \ldots, f_k \in \mathbb{Z}[x_1, \ldots, x_n]$
describe $V_p(f_1, \ldots, f_k) \subset \overline{\mathbb{F}_p}^n$

Local-Global Elimination Challenge

Given $f_1, \ldots, f_k \in \mathbb{Z}[x_1, \ldots, x_n]$ describe $V_p(f_1, \ldots, f_k) \subset \overline{\mathbb{F}_p}^n$ (dimension, degree, height, irreducible components...)

- for a given prime $p \in \mathbb{Z}$

Local-Global Elimination Challenge

Given $f_1, \ldots, f_k \in \mathbb{Z}[x_1, \ldots, x_n]$ describe $V_p(f_1, \ldots, f_k) \subset \overline{\mathbb{F}_p}^n$ (dimension, degree, height, irreducible components...)

- for a given prime $p \in \mathbb{Z}$
- for **all** prime $p \in \mathbb{Z}$
- Compare with $V_{\overline{\mathbb{Q}}}(f_1, \ldots, f_k) \subset \overline{\mathbb{Q}}^n$

Interesting Analogy

Polynomial world

Systems over $\mathbb{Z}$

Interesting Analogy

Polynomial world

Systems over $\mathbb{Z}$

Linear world

Systems with parameters

$$\begin{bmatrix} -a & 1 & a \\ 1 & 0 & 0 \\ 0 & 1 & a \end{bmatrix}$$

Interesting-Nice fact

- There is a "generic" case

Interesting-Nice fact

- There is a "generic" case
- The generic case "is" the case over $\overline{\mathbb{Q}}$

Interesting-Nice fact

- There is a "generic" case
- The generic case "is" the case over $\overline{\mathbb{Q}}$
- We have size bounds for p to be generic

Example 1: Arithmetic Nullstellensatz

$$V_{\overline{\mathbb{Q}}}(f_1, \ldots, f_k) = \emptyset$$

$$\Longleftrightarrow$$

$$1 \in \langle f_1, \ldots, f_k \rangle_{\mathbb{Q}}$$

Example 1: Arithmetic Nullstellensatz

$$V_{\overline{\mathbb{Q}}}(f_1, \ldots, f_k) = \emptyset$$

$$\Longleftrightarrow$$

$$1 \in \langle f_1, \ldots, f_k \rangle_{\mathbb{Q}}$$

$$\Longleftrightarrow \ \exists a \in \mathbb{Z} : \ a \in \langle f_1, \ldots, f_k \rangle_{\mathbb{Z}}$$

Example 1: Arithmetic Nullstellensatz

$$V_{\overline{\mathbb{Q}}}(f_1, \ldots, f_k) = \emptyset$$

$$\Longleftrightarrow$$

$$1 \in \langle f_1, \ldots, f_k \rangle_{\mathbb{Q}}$$

$$\Longleftrightarrow \ \exists a \in \mathbb{Z} : \ a \in \langle f_1, \ldots, f_k \rangle_{\mathbb{Z}}$$

and we have bounds for a

(D-Krick-Sombra 2013)

Corollary

If $p \nmid a$ then $V_p(f_1, \ldots, f_k) = \emptyset$

Corollary

If $p \nmid a$ then $V_p(f_1, \ldots, f_k) = \emptyset$

Nullstellensatz $\leftrightarrow$ "empty" triangulation

$$
\begin{aligned}
a_{11}x_1 + a_{12}x_2 + a_{13}x_3 + \ldots + a_{1n}x_n &= b_1 && \ldots (1)\\
a'_{22}x_2 + a'_{23}x_3 + \ldots + a'_{2n}x_n &= b'_2 && \ldots (2)\\
a''_{33}x_3 + \ldots + a''_{3n}x_n &= b''_3 && \ldots (3)\\
\vdots \quad & \quad \vdots && \quad \vdots\\
a_{nn}^{(n-1)}x_n &= b_n^{(n-1)} && \ldots (n)
\end{aligned}
$$

Example 2: zero dimensional systems

If $V_{\overline{\mathbb{Q}}}(f_1, \ldots, f_k)$ is a set of T points, then

Example 2: zero dimensional systems

If $V_{\overline{\mathbb{Q}}}(f_1, \ldots, f_k)$ is a set of T points, then $V_p(f_1, \ldots, f_k)$ is also a set of T points

Example 2: zero dimensional systems

If $V_{\overline{\mathbb{Q}}}(f_1, \ldots, f_k)$ is a set of T points, then

$V_p(f_1, \ldots, f_k)$ is also a set of T points for $p \nmid a$ bounded

(D-Ostafe-Shparlinski-Sombra 2015)

What about the bad p's?

$$\begin{bmatrix} -a & 1 & a \\ 1 & 0 & 0 \\ 0 & 1 & a \end{bmatrix}$$

What about the bad p's?

$$\begin{bmatrix} -a & 1 & a \\ 1 & 0 & 0 \\ 0 & 1 & a \end{bmatrix}$$

Anything can happen:

What about the bad p's?

$$\begin{bmatrix} -a & 1 & a \\ 1 & 0 & 0 \\ 0 & 1 & a \end{bmatrix}$$

Anything can happen:

- Dimension change

What about the bad p's?

$$\begin{bmatrix} -a & 1 & a \\ 1 & 0 & 0 \\ 0 & 1 & a \end{bmatrix}$$

Anything can happen:

- Dimension change
- Degree change

What about the bad p's?

$$\begin{bmatrix} -a & 1 & a \\ 1 & 0 & 0 \\ 0 & 1 & a \end{bmatrix}$$

Anything can happen:

- Dimension change
- Degree change
- Ramifications

What about the bad p's?

$$\begin{bmatrix} -a & 1 & a \\ 1 & 0 & 0 \\ 0 & 1 & a \end{bmatrix}$$

Anything can happen:

- Dimension change
- Degree change
- Ramifications
- Embedded multiplicities . . .

One interesting result

One interesting result

Resultants modulo p

Resultants modulo p

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

Resultants modulo p

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

Resultants modulo p

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

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

(Gomez-Gutierrez-Ibeas-Sevilla 2009)

Questions

- What does this say about $V_p(f_1, f_2)$?

Questions

- What does this say about $V_p(f_1, f_2)$?
- Can you do it with more generality?

Vanishing of Resultantes modulo p

(D-Sombra 2016)

$$\begin{cases} f_1 = \sum_{\alpha_0+\ldots+\alpha_n=d_1} a_{1,\alpha_0,\ldots,\alpha_n} {x_0}^{\alpha_0} \ldots {x_n}^{\alpha_n} \\ f_2 = \sum_{\alpha_0+\ldots+\alpha_n=d_2} a_{2,\alpha_0,\ldots,\alpha_n} {x_0}^{\alpha_0} \ldots {x_n}^{\alpha_n} \\ \vdots \\ f_{n+1} = \sum_{\alpha_0+\ldots+\alpha_n=d_{n+1}} a_{n+1,\alpha_0,\ldots,\alpha_n} {x_0}^{\alpha_0} \ldots {x_n}^{\alpha_n} \end{cases}$$

Vanishing of Resultantes modulo p

(D-Sombra 2016)

$$\begin{cases} f_1 = \sum_{\alpha_0+\ldots+\alpha_n=d_1} a_{1,\alpha_0,\ldots,\alpha_n} x_0^{\alpha_0} \ldots x_n^{\alpha_n} \\ f_2 = \sum_{\alpha_0+\ldots+\alpha_n=d_2} a_{2,\alpha_0,\ldots,\alpha_n} x_0^{\alpha_0} \ldots x_n^{\alpha_n} \\ \vdots \\ f_{n+1} = \sum_{\alpha_0+\ldots+\alpha_n=d_{n+1}} a_{n+1,\alpha_0,\ldots,\alpha_n} x_0^{\alpha_0} \ldots x_n^{\alpha_n} \end{cases}$$

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

Known case

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

$$\mathrm{Res}(f_1, \ldots, f_{n+1}) = \det\left(a_{ij}\right)_{1 \leq i, j \leq n+1}$$

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

$$
\begin{aligned}
f_0 &= a_{00}x_0 + a_{01}x_1 + a_{02}x_2\\
f_1 &= a_{10}x_0 + a_{11}x_1 + a_{12}x_2\\
f_2 &= a_{20}{x_0}^2 + a_{21}x_0x_1 + a_{22}x_0x_2 + a_{23}{x_1}^2 + a_{24}x_1x_2 + a_{25}{x_2}^2
\end{aligned}
$$

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

Properties of $\mathrm{Res}(f_1, \ldots, f_{n+1})$

- It is irreducible

Properties of $\mathrm{Res}(f_1, \ldots, f_{n+1})$

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

Properties of $\mathrm{Res}(f_1, \ldots, f_{n+1})$

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

Geometric Properties

Geometric Properties

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

Geometric Properties

- $\mathrm{Res}(f_1, \ldots, f_{n+1}) = 0 \iff$ $\exists \xi \in \mathbb{P}^n$ such that $f_1(\xi) = \ldots = f_{n+1}(\xi) = 0$
- Poisson Formula:

$$\mathrm{Res}(f_1, \ldots, f_{n+1}) = \mathrm{Res}(f_1^0, \ldots, f_n^0)^{d_{n+1}} \prod_{\xi \in V(f_1^1, \ldots, f_n^1)} f_{n+1}(\xi)$$

Resolution of systems of polynomials

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

Resolution of systems of polynomials

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

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

$$f_1 = 0, \ldots, f_n = 0$$

Computation

$$\mathcal{R}(f_0\ ,f_1\ ,f_2\ ) = \det\begin{bmatrix} -b_1 & -b_3 & 0 & a_1 & a_3 & 0 & 0 & 0 & 0 & 0 \\ -b_0 & -b_2 & 0 & a_0 & a_2 & 0 & 0 & 0 & 0 & 0 \\ 0 & -b_1 & -b_3 & 0 & a_1 & a_3 & 0 & 0 & 0 & 0 \\ 0 & -b_0 & -b_2 & 0 & a_0 & a_2 & 0 & 0 & 0 & 0 \\ -c_4 & -c_5 & -c_8 & 0 & 0 & 0 & a_1 & 0 & a_3 & 0 \\ -c_1 & -c_3 & -c_7 & 0 & 0 & 0 & a_0 & a_1 & a_2 & a_3 \\ -c_0 & -c_2 & -c_6 & 0 & 0 & 0 & 0 & a_0 & 0 & a_2 \\ 0 & 0 & 0 & -c_4 & -c_5 & -c_8 & b_1 & 0 & b_3 & 0 \\ 0 & 0 & 0 & -c_1 & -c_3 & -c_7 & b_0 & b_1 & b_2 & b_3 \\ 0 & 0 & 0 & -c_0 & -c_2 & -c_6 & 0 & b_0 & 0 & b_2 \end{bmatrix}$$

Resultants modulo p

(D-Sombra 2016)

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

Resultants modulo p

(D-Sombra 2016)

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

$$N_p := \deg\big(V_p(f_1,\ldots,f_{n+1})\big)$$

Resultants modulo p

(D-Sombra 2016)

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

$$N_p := \deg\left(V_p(f_1,\ldots,f_{n+1})\right)$$

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

Corollary

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

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

The Cantabrian Theorem revisited

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

(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 deciding when $\dim\left(V_p(f_1,\ldots,f_{n+1})\right)>0$

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 modulo p of the roots (Smirnov's Theorem)

Generalizations and Extensions

- One could get a refinement of the exponent by taking into account the valuation modulo 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 modulo 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 $R[y_1, \ldots, y_l]$

Applications

- Finding points in varieties modulo p (Shparlinski)

Applications

- Finding points in varieties modulo p (Shparlinski)
- Removing some “extraneous factors” in the Computation of the “Salmon Polynomial” (Busé-Chardin-D-Sombra-Weimann)

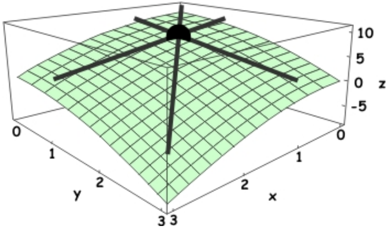
Computation of the Salmon Polynomial

(Busé-Chardin-D-Sombra-Weimann)

$$\mathbb{Z} \leftrightarrow \mathbb{C}[x, y, z]$$

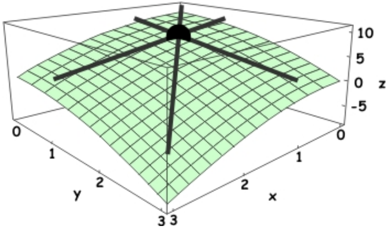
$$p \leftrightarrow f(x, y, z)$$

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

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

Computing $F_f(x, y, z)$

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

Computing $F_f(x, y, z)$

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

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 (arxiv: 2014)

"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)

Working modulo $f(x, y, z)$, the resultant has a spurious factor of degree 6

Our Result

(Busé-Chardin-D-Sombra-Weimann)

Working modulo $f(x,y,z)$, the resultant has a spurious factor of degree 6

$$11d - 18 - 6 = 11d - 24$$

Thanks!

UNIVERSITAT DE BARCELONA