

Subresultants and the Shape Lemma

David Cox & **Carlos D'Andrea**

Paris, June 16 2023





Download full issue



Journal of Symbolic Computation

Volume 43, Issue 1, January 2008, Pages 46-74



Solving over-determined systems by the subresultant method (with an appendix by Marc Chardin)

Agnes Szanto¹

Show more

Add to Mendeley Share Cite

<https://doi.org/10.1016/j.jsc.2007.09.001>

[Get rights and content](#)

Under an [Elsevier user license](#)

[open archive](#)

Abstract

A general *subresultant method* is introduced to compute elements of a given ideal with few terms and bounded coefficients. This subresultant method is applied to solve over-determined polynomial systems by either finding a triangular representation of the solution set or by reducing the problem to eigenvalue computation. One of the ingredients of the subresultant method is



Resultant matrices

$$f(\xi) = f_m \xi^m + \dots + f_1 \xi + f_0 = 0$$

$$g(\xi) = g_n \xi^n + \dots + g_1 \xi + g_0 = 0$$

Great Idea



■ Hilbert-Burch

Great Idea



- Hilbert-Burch
- Cramer's rule

Great Idea



- Hilbert-Burch
- Cramer's rule
- Minors of resultant matrices

Great Idea



- Hilbert-Burch
- Cramer's rule
- Minors of resultant matrices
- Subresultants

Great Idea



- Hilbert-Burch
- Cramer's rule
- Minors of resultant matrices
- Subresultants
- Overdetermined systems

Used in

- Busé, **D**: *Inversion of parameterized hypersurfaces by means of subresultants*. ISSAC 04
- **D**, Khetan: *Macaulay style formulas for toric residues*. Compos. Math. 05
- **D**, Jeronimo: *Subresultants and generic monomial bases*. J. Symbolic Comput. 05
- Buse, **D**: *A matrix-based approach to properness and inversion problems for rational surfaces*. AAEC 06
- **D**, Chipalkatti: *On the Jacobian ideal of the binary discriminant*. Collect. Math. 07
- **D** Sombra: *A Poisson formula for the sparse resultant*. Proc. Lond. Math. Soc. 15
- Buse, **D** ; Sombra, Weimann: *The geometry of the flex locus of a hypersurface*. Pacific J. Math. 20

And also in

Cox, **D**: *Subresultants and the Shape Lemma*. *Math. Comp.* 92 (2023),
no. 343, 2355–2379

And also in

Cox, **D**: *Subresultants and the Shape Lemma*. *Math. Comp.* 92 (2023),
no. 343, 2355–2379



Starting example

In $\mathbb{C}[x_1, x_2]$ set

$$f = x_1^2 - x_2 - 1, \quad g = x_1^2 + x_1x_2 - 2$$

Starting example

In $\mathbb{C}[x_1, x_2]$ set

$$f = x_1^2 - x_2 - 1, \quad g = x_1^2 + x_1x_2 - 2$$

A lex Gröbner basis of $\langle f, g \rangle$ with $x_2 \prec x_1$ is $\{x_2^3 + 2x_2 - 1, x_1 - x_2^2 + 1\}$

Shape Lemma

A zero-dimensional ideal $I \subset \mathbb{C}[x_1, x_2]$
has a **Shape Lemma** if

Shape Lemma

A zero-dimensional ideal $I \subset \mathbb{C}[x_1, x_2]$
has a **Shape Lemma** if

$$I = \langle p(x_2), x_1 - q(x_2) \rangle$$

Shape Lemma

A zero-dimensional ideal $I \subset \mathbb{C}[x_1, x_2]$
has a **Shape Lemma** if

$$I = \langle p(x_2), x_1 - q(x_2) \rangle$$

- A generator depending only on x_2

Shape Lemma

A zero-dimensional ideal $I \subset \mathbb{C}[x_1, x_2]$
has a **Shape Lemma** if

$$I = \langle p(x_2), x_1 - q(x_2) \rangle$$

- A generator depending only on x_2
- A monic generator linear in x_1

Resultants and Subresultants

Resultants and Subresultants

$$I = \langle f, g \rangle = \langle x_2^3 + 2x_2 - 1, x_1 - x_2^2 - 1 \rangle$$

Resultants and Subresultants

$$I = \langle f, g \rangle = \langle x_2^3 + 2x_2 - 1, x_1 - x_2^2 - 1 \rangle$$

$$x_2^3 + 2x_2 - 1$$

Resultants and Subresultants

$$I = \langle f, g \rangle = \langle x_2^3 + 2x_2 - 1, x_1 - x_2^2 - 1 \rangle$$

$$x_2^3 + 2x_2 - 1 = \boxed{\text{Res}(f, g, x_1)}$$

Resultants and Subresultants

$$I = \langle f, g \rangle = \langle x_2^3 + 2x_2 - 1, x_1 - x_2^2 - 1 \rangle$$

$$x_2^3 + 2x_2 - 1 = \boxed{\text{Res}(f, g, x_1)}$$

$$x_1 - x_2^2 - 1$$

Resultants and Subresultants

$$I = \langle f, g \rangle = \langle x_2^3 + 2x_2 - 1, x_1 - x_2^2 - 1 \rangle$$

$$x_2^3 + 2x_2 - 1 = \boxed{\text{Res}(f, g, x_1)}$$

$$x_1 - x_2^2 - 1 \stackrel{?}{=}$$

Resultants and Subresultants

$$I = \langle f, g \rangle = \langle x_2^3 + 2x_2 - 1, x_1 - x_2^2 - 1 \rangle$$

$$x_2^3 + 2x_2 - 1 = \boxed{\text{Res}(f, g, x_1)}$$

$$x_1 - x_2^2 - 1 \stackrel{?}{=} \boxed{\text{Sres}_1(f, g, x_1)}$$

Resultants

$$f(x_1) = f_m x_1^m + \dots + f_1 x_1 + f_0$$
$$g(x_1) = g_n x_1^n + \dots + g_1 x_1 + g_0$$

In our case...

In our case...

$$S_{\text{res}_1}(f, g, x_1) = x_2x_1 + x_2 - 1$$

In our case...

$$\text{Sres}_1(f, g, x_1) = x_2x_1 + x_2 - 1 \neq x_1 - x_2^2 - 1$$

In our case...

$$\text{Sres}_1(f, g, x_1) = x_2x_1 + x_2 - 1 \neq x_1 - x_2^2 - 1$$

But

$$\langle f, g \rangle = \langle \text{Res}(f, g, x_1), \text{Sres}_1(f, g, x_1) \rangle$$

Questions



Questions



Suppose $I = \langle f(x_1, x_2), g(x_1, x_2) \rangle$

Questions



Suppose $I = \langle f(x_1, x_2), g(x_1, x_2) \rangle$

- When has I a Shape Lemma?

Questions



Suppose $I = \langle f(x_1, x_2), g(x_1, x_2) \rangle$

- When has I a Shape Lemma?
- When $I \cap \mathbb{C}[x_2] = \langle \text{Res}(f, g, x_1) \rangle$?

Questions



Suppose $I = \langle f(x_1, x_2), g(x_1, x_2) \rangle$

- When has I a Shape Lemma?
- When $I \cap \mathbb{C}[x_2] = \langle \text{Res}(f, g, x_1) \rangle$?
 $I = \langle \text{Res}(f, g, x_1), \text{Sres}_1(f, g, x_1) \rangle$?

Warning!



Warning!



$$f = x_2x_1^2 + x_1 + x_2^2 + x_2, \quad g = x_2x_1 + 1$$

Warning!



$$f = x_2x_1^2 + x_1 + x_2^2 + x_2, \quad g = x_2x_1 + 1$$
$$\text{Res}(f, g, x_1) = x_2^3(x_2 + 1)$$

Warning!



$$f = x_2x_1^2 + x_1 + x_2^2 + x_2, \quad g = x_2x_1 + 1$$

$$\text{Res}(f, g, x_1) = x_2^3(x_2 + 1)$$

$$\text{Sres}_1(f, g, x_1) = x_2x_1 + 1$$

Warning!



$$f = x_2x_1^2 + x_1 + x_2^2 + x_2, \quad g = x_2x_1 + 1$$

$$\text{Res}(f, g, x_1) = x_2^3(x_2 + 1)$$

$$\text{Sres}_1(f, g, x_1) = x_2x_1 + 1$$

$$I = \langle x_2^3(x_2 + 1), x_2x_1 + 1 \rangle$$

Warning!



$$f = x_2x_1^2 + x_1 + x_2^2 + x_2, \quad g = x_2x_1 + 1$$

$$\text{Res}(f, g, x_1) = x_2^3(x_2 + 1)$$

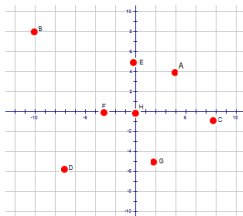
$$\text{Sres}_1(f, g, x_1) = x_2x_1 + 1$$

$$I = \langle x_2^3(x_2 + 1), x_2x_1 + 1 \rangle = \\ \langle x_2 + 1, x_1 - 1 \rangle$$

Geometry of the Shape Lemma

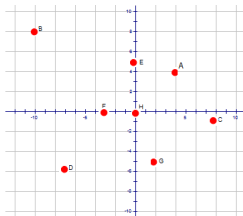
Geometry of the Shape Lemma

$$I = \langle p(x_2), x_1 - q(x_2) \rangle$$



Geometry of the Shape Lemma

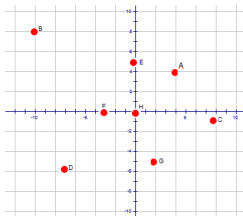
$$I = \langle p(x_2), x_1 - q(x_2) \rangle$$



- Projection onto the x_2 axis should be injective

Geometry of the Shape Lemma

$$I = \langle p(x_2), x_1 - q(x_2) \rangle$$



- Projection onto the x_2 axis should be injective
- How about multiplicities?

Equivalences

If $I \cap \mathbb{C}[x_2] = \langle r(x_2) \rangle$ and the projection $V(I) \rightarrow \mathbb{C}$ onto the x_2 -axis injective, TFAE:

Equivalences

If $I \cap \mathbb{C}[x_2] = \langle r(x_2) \rangle$ and the projection $V(I) \rightarrow \mathbb{C}$ onto the x_2 -axis injective, TFAE:

- I has a Shape Lemma

Equivalences

If $I \cap \mathbb{C}[x_2] = \langle r(x_2) \rangle$ and the projection $V(I) \rightarrow \mathbb{C}$ onto the x_2 -axis injective, TFAE:

- I has a Shape Lemma
- $\forall \underline{\xi} \in V(I), m_V(\underline{\xi}) = m_r(\xi_2)$

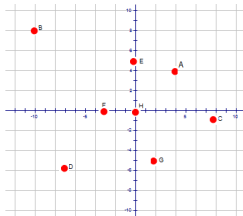
Equivalences

If $I \cap \mathbb{C}[x_2] = \langle r(x_2) \rangle$ and the projection $V(I) \rightarrow \mathbb{C}$ onto the x_2 -axis injective, TFAE:

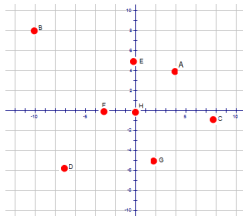
- I has a Shape Lemma
- $\forall \underline{\xi} \in V(I), m_V(\underline{\xi}) = m_r(\xi_2)$
- $\forall \underline{\xi} \in V(I), T_{\underline{\xi}}(V(I)) \xrightarrow{\sim} T_{\xi_2}(V(r))$

Geometry of Resultants

Geometry of Resultants

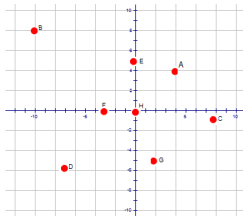


Geometry of Resultants



Poisson formula:

Geometry of Resultants



Poisson formula:

$$\text{Res}(f, g, x_1) = c^* \cdot \prod_{(\xi_1, \xi_2) \in V(I^h)} (x_2 - \xi_2)^{m_\xi}$$

Resultants and Shape Lemma

(Cox-D)

Resultants and Shape Lemma

(Cox-D)

If the projection $V(I) \rightarrow \mathbb{C}$ onto the x_2 -axis is injective,

Resultants and Shape Lemma

(Cox-D)

If the projection $V(I) \rightarrow \mathbb{C}$ onto the x_2 -axis is injective, any two of the following conditions imply the third:

Resultants and Shape Lemma

(Cox-D)

If the projection $V(I) \rightarrow \mathbb{C}$ onto the x_2 -axis is injective, any two of the following conditions imply the third:

- I has a Shape Lemma

Resultants and Shape Lemma

(Cox-D)

If the projection $V(I) \rightarrow \mathbb{C}$ onto the x_2 -axis is injective, any two of the following conditions imply the third:

- I has a Shape Lemma
- $I \cap \mathbb{C}[x_2] = \langle \text{Res}(f, g, x_1) \rangle$

Resultants and Shape Lemma

(Cox-D)

If the projection $V(I) \rightarrow \mathbb{C}$ onto the x_2 -axis is injective, any two of the following conditions imply the third:

- I has a Shape Lemma
- $I \cap \mathbb{C}[x_2] = \langle \text{Res}(f, g, x_1) \rangle$
- $\gcd(\text{lc}_{x_1}(f), \text{lc}_{x_1}(g)) = 1$

Example

Example

$$f = x_2x_1^2 + x_1 + x_2^2 + x_2, \quad g = x_2x_1 + 1$$

Example

$$f = x_2x_1^2 + x_1 + x_2^2 + x_2, \quad g = x_2x_1 + 1$$
$$\text{lc}_{x_1}(f) = \text{lc}_{x_1}(g) = x_2$$

Example

$$f = x_2x_1^2 + x_1 + x_2^2 + x_2, \quad g = x_2x_1 + 1$$

$$\text{lc}_{x_1}(f) = \text{lc}_{x_1}(g) = x_2$$

$$I = \langle f, g \rangle = \langle x_2 + 1, x_1 - 1 \rangle$$

Example

$$f = x_2x_1^2 + x_1 + x_2^2 + x_2, \quad g = x_2x_1 + 1$$

$$\text{lc}_{x_1}(f) = \text{lc}_{x_1}(g) = x_2$$

$$I = \langle f, g \rangle = \langle x_2 + 1, x_1 - 1 \rangle$$

$$\text{Res}(f, g, x_1) = x_2^3(x_2 + 1)$$

Subresultants and Shape Lemma

(Cox-D) TFAE:

Subresultants and Shape Lemma

(Cox-D) TFAE:

- f has a Shape Lemma and $\gcd(\text{lc}_{x_1}(f), \text{lc}_{x_1}(g)) = 1$

Subresultants and Shape Lemma

(Cox-D) TFAE:

- I has a Shape Lemma and $\gcd(\text{lc}_{x_1}(f), \text{lc}_{x_1}(g)) = 1$
- $I \cap \mathbb{C}[x_2] = \langle \text{Res}(f, g, x_1) \rangle$ and $\gcd(\text{Res}(f, g, x_1), \text{Sres}_1(f, g)) = 1$

Subresultants and Shape Lemma

(Cox-D) TFAE:

- I has a Shape Lemma and $\gcd(\text{lc}_{x_1}(f), \text{lc}_{x_1}(g)) = 1$
- $I \cap \mathbb{C}[x_2] = \langle \text{Res}(f, g, x_1) \rangle$ and $\gcd(\text{Res}(f, g, x_1), \text{Sres}_1(f, g)) = 1$
- $I = \langle \text{Res}(f, g, x_1), \text{Sres}_1(f, g, x_1) \rangle$ and $I \cap \mathbb{C}[x_2] = \langle \text{Res}(f, g, x_1) \rangle$

Where is the great idea?



Where is the great idea?



$S_{\text{res}_1}(f, g, x_1)$ gives the only
“solution” modulo $\text{Res}(f, g, x_1)$

Where is the great idea?



$Sres_1(f, g, x_1)$ gives the only
“solution” modulo $Res(f, g, x_1)$



Works in several variables!

Works in several variables!

Same results for zero-dim ideals

$$I = \langle f_1, \dots, f_n \rangle \subset \mathbb{K}[x_1, \dots, x_n]$$

Works in several variables!

Same results for zero-dim ideals

$$I = \langle f_1, \dots, f_n \rangle \subset \mathbb{K}[x_1, \dots, x_n]$$

using multivariate **resultants** and
subresultants

Multivariate Resultants

Multivariate Resultants

- A an integral domain

Multivariate Resultants

- A an integral domain
- g_1, \dots, g_n homogeneous polynomials in $A[x_0, \dots, x_{n-1}]$ of degrees d_1, \dots, d_n

Multivariate Resultants

- A an integral domain
- g_1, \dots, g_n homogeneous polynomials in $A[x_0, \dots, x_{n-1}]$ of degrees d_1, \dots, d_n
- $\text{Res}_{d_1, \dots, d_n}(g_1, \dots, g_n) \in A$ the multivariate resultant

Multivariate Resultants

Multivariate Resultants

- $f_1, \dots, f_n \in \mathbb{K}[x_n][x_1, \dots, x_{n-1}]$

Multivariate Resultants

- $f_1, \dots, f_n \in \mathbb{K}[x_n][x_1, \dots, x_{n-1}]$
- $f_1^h, \dots, f_n^h \in \mathbb{K}[x_n][x_0, \dots, x_{n-1}]$
their homogenizations

Multivariate Resultants

- $f_1, \dots, f_n \in \mathbb{K}[x_n][x_1, \dots, x_{n-1}]$
- $f_1^h, \dots, f_n^h \in \mathbb{K}[x_n][x_0, \dots, x_{n-1}]$
their homogenizations
- $d_i = \deg_{x_1, \dots, x_{n-1}}(f_i), i = 1, \dots, n$

$$\text{Res}_{d_1, \dots, d_n}^{x_n}(f_1, \dots, f_n) := \\ \text{Res}_{d_1, \dots, d_n}(f_1^h, \dots, f_n^h) \in \mathbb{K}[x_n]$$

Resultants and Shape Lemma

(Cox-D)

Resultants and Shape Lemma

(Cox-D)

Any two of the following three conditions imply the third:

Resultants and Shape Lemma

(Cox-D)

Any two of the following three conditions imply the third:

- 1 $\langle f_1, \dots, f_n \rangle$ has a Shape Lemma

Resultants and Shape Lemma

(Cox-D)

Any two of the following three conditions imply the third:

- 1 $\langle f_1, \dots, f_n \rangle$ has a Shape Lemma
- 2 f_1, \dots, f_n have no solutions at ∞

Resultants and Shape Lemma

(Cox-D)

Any two of the following three conditions imply the third:

- 1 $\langle f_1, \dots, f_n \rangle$ has a Shape Lemma
- 2 f_1, \dots, f_n have no solutions at ∞
- 3 $\langle f_1, \dots, f_n \rangle \cap \mathbb{K}[x_n] = \langle \text{Res}_{d_1, \dots, d_n}^{x_n}(f_1, \dots, f_n) \rangle$

“First Subresultant Polynomials”

“First Subresultant Polynomials”

$$p_i(x_i, x_n) = s_0(x_n)x_i - s_i(x_n) \in \langle f_1, \dots, f_n \rangle$$

“First Subresultant Polynomials”

$$p_i(x_i, x_n) = s_0(x_n)x_i - s_i(x_n) \in \langle f_1, \dots, f_n \rangle$$

Szanto, A. Multivariate subresultants using Jouanolou matrices. *J. Pure Appl. Algebra* 214 (2010), no. 8, 1347–1369

Subresultants and Shape Lemma

(Cox-D)

Subresultants and Shape Lemma

(Cox-D)

If $I = \langle f_1, \dots, f_n \rangle$ is zero-dimensional

Subresultants and Shape Lemma

(Cox-D)

If $I = \langle f_1, \dots, f_n \rangle$ is zero-dimensional TFAE:

- I has a Shape Lemma and no solutions at ∞

Subresultants and Shape Lemma

(Cox-D)

If $I = \langle f_1, \dots, f_n \rangle$ is zero-dimensional TFAE:

- I has a Shape Lemma and no solutions at ∞
- $I \cap \mathbb{K}[x_n] = \langle \text{Res}_{d_1, \dots, d_n}^{x_n}(f_1, \dots, f_n) \rangle$ and $\text{gcd}(\text{Res}_{d_1, \dots, d_n}^{x_n}(f_1, \dots, f_n), s_0(x_n)) = 1$

Subresultants and Shape Lemma

(Cox-D)

If $I = \langle f_1, \dots, f_n \rangle$ is zero-dimensional TFAE:

- I has a Shape Lemma and no solutions at ∞
- $I \cap \mathbb{K}[x_n] = \langle \text{Res}_{d_1, \dots, d_n}^{x_n}(f_1, \dots, f_n) \rangle$ and $\text{gcd}(\text{Res}_{d_1, \dots, d_n}^{x_n}(f_1, \dots, f_n), s_0(x_n)) = 1$
- $I = \langle \text{Res}_{d_1, \dots, d_n}^{x_n}(f_1, \dots, f_n), p_1(x_1, x_n), \dots, p_{n-1}(x_{n-1}, x_n) \rangle$ and $I \cap \mathbb{K}[x_n] = \langle \text{Res}_{d_1, \dots, d_n}^{x_n}(f_1, \dots, f_n) \rangle$

Subresultants and Shape Lemma

(Cox-D)

Subresultants and Shape Lemma

(Cox-D)

If $I = \langle f_1, \dots, f_n \rangle =$
 $\langle \text{Res}_{d_1, \dots, d_n}^{x_n}(f_1, \dots, f_n), p_1(x_1, x_n), \dots, p_{n-1}(x_{n-1}, x_n) \rangle$
is zero-dimensional, then:

Subresultants and Shape Lemma

(Cox-D)

If $I = \langle f_1, \dots, f_n \rangle =$
 $\langle \text{Res}_{d_1, \dots, d_n}^{x_n}(f_1, \dots, f_n), p_1(x_1, x_n), \dots, p_{n-1}(x_{n-1}, x_n) \rangle$
is zero-dimensional, then:

$$\gcd(\text{Res}_{d_1, \dots, d_n}^{x_n}(f_1, \dots, f_n), s_0(x_n), \dots, s_{n-1}(x_n)) = 1$$

Subresultants and Shape Lemma

(Cox-D)

If $I = \langle f_1, \dots, f_n \rangle =$
 $\langle \text{Res}_{d_1, \dots, d_n}^{x_n}(f_1, \dots, f_n), p_1(x_1, x_n), \dots, p_{n-1}(x_{n-1}, x_n) \rangle$
is zero-dimensional, then:

$$\gcd(\text{Res}_{d_1, \dots, d_n}^{x_n}(f_1, \dots, f_n), s_0(x_n), \dots, s_{n-1}(x_n)) = 1$$

and I has a Shape Lemma

FoCM 2017 – Barcelona



FoCM 2017 – Barcelona



Thanks!