Polynomial Systems:
Properties and Algorithms

Ioannis Z. Emiris

ATHENA Research Center, Greece
Dept. of Informatics & Telecoms, NKU Athens

IHP Paris, 10-11 October 2023
(with slides contributed by Carles Checa)

ATHENA Research & Innovation Information Technologies

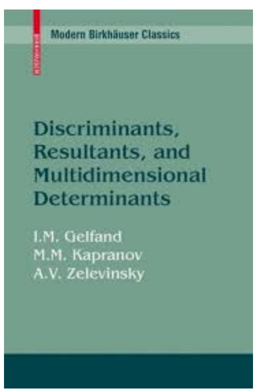
National and Kapodistrian UNIVERSITY OF ATHENS

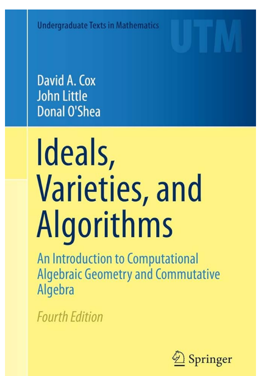
Some Questions in Computer Algebra

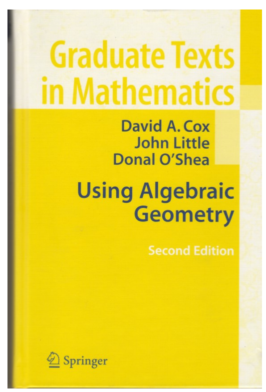
- How can we efficiently solve polynomial systems . . .
- . . . by leveraging the breakthroughs of linear algebra?
- . . . or by exploiting combinatorics?
- Are polynomials useful in modeling real-world problems?

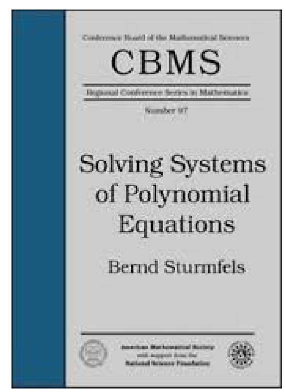
Some Big Ideas in Computer Algebra

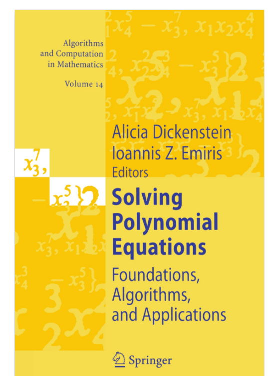
- algebra-geometry dictionary (Hilbert)
  [Cox,Litlle,O'Shea:Ideals,Varieties,Algorithms]
- polynomial system solving by linear algebra
  [Gelfand,Kapranov,Zelevinsky] [CLO:Using algebraic geometry,ch.3]
- polynomials $\sim$ polytopes (Gelfand)
  [Gelfand,Kapranov,Zelevinsky] [CLO2:ch.7] [Sturmfels:Solving. . .]
- polynomials model the real world [Sturmfels:Solving Systems of polynomial equations] [Dickenstein-E:Solving polynomial equations]











Outline

Introduction to polynomial systems

From one to many

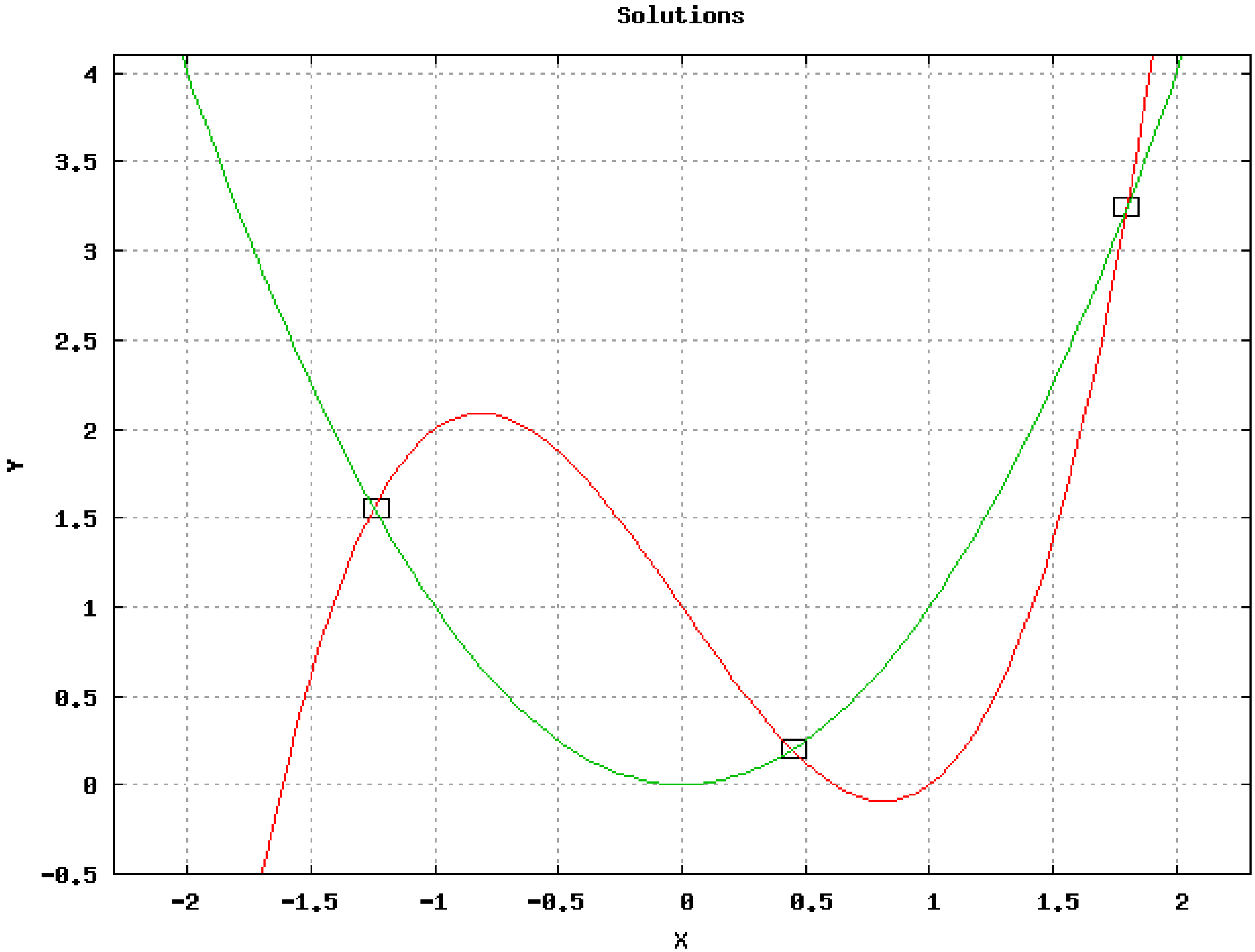
$$f(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_d x^d \ \in \ K[x].$$

- Fundamental theorem of algebra: There are d roots in $\overline{K}$.

E.g. $\overline{\mathbb{Q}} =$ Algebraic numbers.

- Fundamental problem of real algebra: How many roots are real?
- Fundamental problem of computational real algebra: Isolate all real roots of a given polynomial equation.
- Fundamental problem of computational algebraic geometry: Isolate/approximate all complex roots of a given polynomial system.
- Fundamental problem of computational real algebraic geometry: Isolate all real roots of a given polynomial system.

A Polynomial system



$f_1 = y - x^3 + 2x - 1$, $f_2 = y - x^2$:

3 common solutions: $(0.45, 0.20), (-1.25, 1.55), (1.80, 3.25)$

Varieties and ideals

$$f_1, \ldots, f_m \in \mathbb{Q}[x_1, \ldots, x_n].$$

Definition. The polynomial system's variety (or zero-set) is

$$V(f_1, \ldots, f_m) := \{x \in \mathbb{C}^n : f_1(x) = \cdots = f_m(x) = 0\}.$$

The variety is algebraic since it is defined by equations.

Given a polynomial ring $R = K[x_1, \ldots, x_n]$, a non-empty (algebraic) ideal $I \subset R$ is closed under addition and multiplication by any ring element: $a, b \in I, p \in R \Rightarrow a + b, ap \in I$.

Given a set of polynomials, all elements in the generated (algebraic) ideal vanish at the set's variety. The ideal is the largest set of polynomials vanishing precisely at this variety.

Fact. Given set $X \subset \mathbb{C}^n$, the polynomials $J(X) := \{f \in \mathbb{Q}[x] : f(x) = 0, \forall x \in X\}$ form an ideal.

Degree

Definition: (total) degree of polynomial $F(x_1, \ldots, x_n)$ is the maximum sum of exponents in any monomial (term).
E.g. $\deg(x^2 - xy^2 + z) = 3$.

We also talk of degree in some variable(s).
E.g.: $\deg_x(F) = 2$, $\deg_y(F) = 2$, $\deg_z(F) = 1$.

The polynomial is homogeneous (wrt to all n variables) if all monomials have the same degree.

E.g. $x^2w - xy^2 + zw^2$. Here $w \neq 0$ is the homogenizing variable.
For an affine root $(x, y, z) \in \mathbb{C}^3$ there is a projective root $(x : y : z : 1) \in \mathbb{P}^3$

Number of roots

Recall the complex projective space $\mathbb{P}^n_{\mathbb{C}}$ or $\mathbb{P}^n$ or $\mathbb{P}(\mathbb{C})^n$ as the set of equivalence classes:

$$\left\{(\alpha_0 : \cdots : \alpha_n) \in \mathbb{C}^{n+1} - \{0^{n+1}\} \mid \alpha \sim \lambda\alpha,\ \lambda \in \mathbb{C}^*\right\} =$$

$$= \{(1 : \beta) \mid \beta \in \mathbb{C}^n\} \cup \{(0 : \beta) \mid \beta \in \mathbb{C}^n - \{0^n\},\ \beta \sim \lambda\beta\}.$$

E.g. $n = 1$: $\mathbb{P}^1 \simeq \mathbb{C} \cup \{(0 : 1)\}$.

Theorem [Bézout,1790]. Given (homogeneous) $f_1, \ldots, f_n \in K[x_1, \ldots, x_n]$, the number of common isolated roots (counting multiplicities) in $\mathbb{P}(\overline{K})^n$ is bounded by

$$\prod_{i=1}^{n} \deg\ f_i,$$

where $\deg(\cdot)$ is the polynomial's total degree.
The bound is exact for generic coefficients.
More generally, it bounds the degree of the variety.

Example: intersecting circles

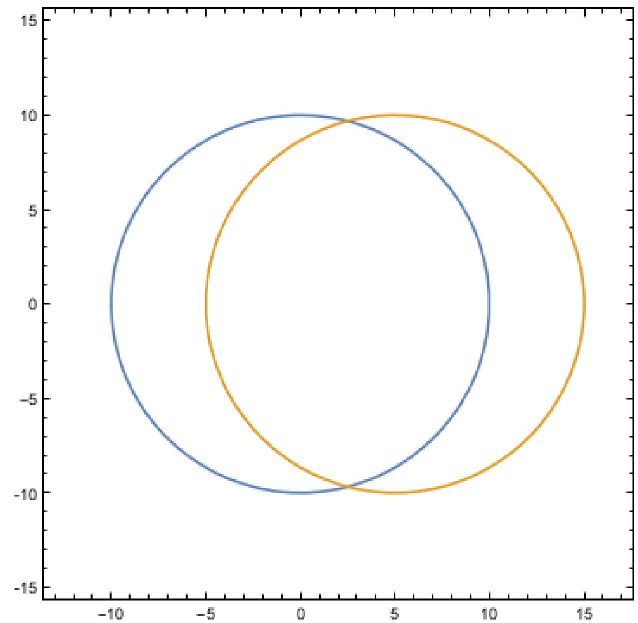
$x^2 + y^2 = 100$, and $(x-5)^2 + y^2 = 100$. Bézout bound $= 2 \cdot 2 = 4$.

Where are the solutions?

If $x, y \in \mathbb{R}$, the circles intersect in ≤ 2 points.

If $x, y \in \mathbb{C}$, they still intersect in 2 points...

...and 2 more intersections at infinity.



Polynomial system solving

A perspective. . .  on system solving

Input: n polynomial equations in n variables, coefficients in a ring (e.g. $\mathbb{Z}$, $\mathbb{R}$, $\mathbb{C}$).
Output: All n-vectors of values s.t. all polynomials evaluate to 0.

Type	Algebraic	Analytic
Approach	Combine constraints	Use values (or signs)
Computation	Exact (+ possibly numerical)	Numerical mostly
Methods	Matrix-based: resultant + continuity w.r.t. coefficients + exploit structure − high-dimensional components $O_b^*(d^n)$	Homotopy continuation + exploit structure + output sensitive − divergent paths
	Gröbner bases + complete information − discontinuity w.r.t. coefficients dimension=0: $O_b^*(d^{n^2})$, else $O_b^*(d^{2^n})$ Normal forms, boundary bases	Exclusion, interval, topological degree + focuses on given domain − costly for large n
	Characteristic sets Straight-line programs express evaluation	Newton-based optimization + simple, fast − local, needs initial point

Resultants

Resultant definition

Given $n+1$ polynomials $f_0, \ldots, f_n \in K[x_1, \ldots, x_n]$ with indeterminate coefficients $\vec{c}$, their projective *resultant* is the unique (up to sign) irreducible polynomial $R(\vec{c}) \in \mathbb{Z}[\vec{c}]$ such that

$$R(\vec{c}) = 0 \Leftrightarrow \exists\, \xi = (\xi_1, \ldots, \xi_n) \in X \,:\, f_0(\xi) = \cdots = f_n(\xi) = 0$$

where the variety X equals:

- the projective space $\mathbb{P}^n$ over the algebraic closure $\overline{K}$,

Generalizations

The projective resultant for $n+1$ *dense* polynomials reduces to:

- the determinant of the coefficient matrix of a *linear* system,
- the Sylvester or Bézout determinant of 2 *univariate* polynomials.

Resultant degree

The projective, resultant polynomial $R \in \mathbb{Z}[\vec{c}]$ is separately homogeneous in the coefficients of each f_i, with *degree* equal to $\prod_{j \neq i} \deg f_j$ (Bézout's number).

Poisson Formula

Given $f_0, \ldots, f_n \in K[x_1, \ldots, x_n]$, with coefficients $c = (c_0, \ldots, c_n)$ in K.

Poisson formula:

$$R \;=\; T \;\cdot \prod_{\alpha \in V(f_1,\ldots,f_n)} f_0(\alpha)$$

where V is (generically) a 0-dimensional variety $\subset \mathbb{C}^n$, and
T is a polynomial in $c_1, \ldots, c_n$ such that R is a polynomial in $\mathbb{Z}[c]$.

Corollary. By Bézout's bound:

$$\deg_{c_0} R = \prod_{i=1}^{n} \deg f_i.$$

Matrix formulae

- Resultant matrix s.t. the resultant divides the determinant.
- Rational, Macaulay-type formula: The resultant equals the ratio of two determinants.
- Determinantal formula: the resultant equals a determinant
- Polynomial formula: A power of the resultant equals the determinant, Pfaffian when $R = \sqrt{\det M}$.

- Matrix formulae allow system solving by: an eigenproblem, factoring the u-resultant, primitive/separating element (RUR).

Resultant matrices

- Sylvester 1840, Macaulay 1902, [Canny-E'93], greedy [Canny-Pedersen], generalized [Sturmfels'94], rational [D'Andrea'02, E-Konaxis'09, D'Andrea,Jeronimo,Sombra], [Checa-E'22].

- Bézout 1779, [Chtcherba-Kapur'00], [Kapur et.al], [Cardinal-Mourrain'95], [Elkadi-Mourrain], [Busé et al.].

- Hybrid: Morley, Dixon, [Jouanolou'97], [Checa-Busé'23], homogeneous [D'Andrea-Dickenstein'01], [CoxMatera08], with toric Jacobian [Cattani-Dickenstein-Sturmfels], [D'Andrea-E'01], Tate resolution [Khetan'02], complexes [Eisenbud-Schreyer'03].

- Multihomogeneous [Weyman-Zelevinsky'94] [Sturmfels-Zelevinsky'94] [Chionh-Goldman-Zhang'98], [Dickenstein-E'03, E-Mantzaflaris'09], [Awane-Chkiriba-Goze'05], [Bender et al'21].

Survey [E,Mourrain'99:Matrices in elimination theory]

Toy example

$$\begin{aligned} f_0 &= c_{01}x + c_{00} \\ f_1 &= c_{11}x + c_{10} \end{aligned}$$

$$R = \det \begin{bmatrix} c_{01} & c_{00} \\ c_{11} & c_{10} \end{bmatrix} = c_{01}c_{10} - c_{00}c_{11}$$

Solve f_0 yields $x_0 = -c_{00}/c_{01}$. Substitute, then

$$R \sim f_1(x_0) = c_{11}(-c_{00}/c_{01}) + c_{10}.$$

Compare to the Poisson formula.

Exercise. Find the defining polynomial of the sum of roots α, β of polynomials $f(x), g(x)$ respectively.

Linear system

$$
\begin{aligned}
f_0 &= c_{01}x + c_{02}y + c_{00} \\
f_1 &= c_{11}x + c_{12}y + c_{10} \\
f_2 &= c_{21}x + c_{22}y + c_{20}
\end{aligned}
$$

$$
R = \det \begin{array}{c c}
\begin{array}{ccc} x & y & 1 \end{array} & \\
\underbrace{\begin{bmatrix} c_{01} & c_{02} & c_{00} \\ c_{11} & c_{12} & c_{10} \\ c_{21} & c_{22} & c_{20} \end{bmatrix}}_{M} & \begin{array}{c} f_0 \\ f_1 \\ f_2 \end{array}
\end{array}
$$

For indeterminates c_{ij}: $R \neq 0$ iff there is no common solution.

$R = 0$ iff there is a (unique) solution of $f_i = 0 \Leftrightarrow \exists \vec{v} \neq \vec{0} : M\vec{v} = \vec{0}$.

Linear system (cont'd): linear algebra

Matrix-vector multiplication expresses evaluation of the row polynomials f_i at point (x_0, y_0):

$$M \begin{bmatrix} x_0 \\ y_0 \\ 1 \end{bmatrix} = \begin{bmatrix} f_0(x_0, y_0) \\ f_1(x_0, y_0) \\ f_2(x_0, y_0) \end{bmatrix}$$

where the vector is indexed by the column monomials, actually contains values at (x_0, y_0) of the column monomials.

So when $(x_0, y_0) \in \mathbb{C}^2$ is a root of $f_0 = f_1 = f_2 = 0$, then $M\vec{v} = \vec{0}$.

Linear system (cont'd)

Develop $\det M$ along, say, the f_0 row:

$$\det M = c_{01}\begin{vmatrix} c_{12} & c_{10} \\ c_{22} & c_{20} \end{vmatrix} + c_{02}\begin{vmatrix} c_{11} & c_{10} \\ c_{21} & c_{20} \end{vmatrix} + c_{00}\begin{vmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{vmatrix}$$

equals $f_0(x_0 : y_0 : 1)$, where $\alpha = (x_0, y_0) \in \mathbb{C}^2$ is the root of $f_1 = f_2 = 0$.

Poisson formula: $R = \begin{vmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{vmatrix} f_0(\alpha), \quad \alpha \in \mathbb{C}^2 : f_1(\alpha) = f_2(\alpha) = 0.$

Sylvester matrix

Overconstrained system

$$\begin{aligned} f_0 &= a_{d_0}x^{d_0} + \cdots + a_0, & a_{d_0} \neq 0, \\ f_1 &= b_{d_1}x^{d_1} + \cdots + b_0, & b_{d_1} \neq 0. \end{aligned}$$

Define S:

$$R = \det \begin{array}{c} \begin{array}{cccc} x^{d_0+d_1-1} & \cdots & x & 1 \end{array} \\ \begin{bmatrix} a_{d_0} & \cdots & a_0 & & 0 \\ & \ddots & & \ddots & \\ 0 & & a_{d_0} & \cdots & a_0 \\ b_{d_1} & \cdots & \cdots & b_0 & 0 \\ 0 & b_{d_1} & \cdots & \cdots & b_0 \end{bmatrix} \end{array} \begin{array}{cc} f_0 * & \begin{array}{c} x^{d_1-1} \\ \vdots \\ 1 \end{array} \\ f_1 * & \begin{array}{c} x^{d_0-1} \\ \vdots \\ 1 \end{array} \end{array} \begin{array}{l} \left.\begin{array}{c} \\ \\ \\ \end{array}\right\} B_0 \\ \left.\begin{array}{c} \\ \\ \\ \end{array}\right\} B_1 \end{array}$$

Lem. S is a square matrix, and $R = \det S$ (see below).

Poisson formula: $$R = T \prod_{\alpha : f_1(\alpha)=0} f_0(\alpha).$$

Sylvester matrix: properties

The two sets of rows correspond to the two polynomials: The d_1 **black rows** contain f_0 coefficients, corresponding to polynomials

$$f_0, xf_0, \ldots, x^{d_1-1}f_0.$$

The d_0 **blue rows** have f_1 coefficients, corresponding to polynomials

$$f_1, xf_1, \ldots, x^{d_0-1}f_1.$$

Lemma: S is a square matrix.
Proof. There are $d_0 + d_1$ rows. The f_0 multiples have powers 1 to $x^{d_0}x^{d_1-1}$, hence $d_0 + d_1$ columns. Analogously for the f_1 powers.

Exactness of Sylvester matrix

Lemma. If S is the Sylvester matrix of f_0, f_1, then

$$\det S = 0 \Leftrightarrow \deg \gcd(f_0, f_1) \geq 1.$$

Proof. [$\Leftarrow$] $\deg \gcd(f_0, f_1) \geq 1 \Rightarrow \exists\, r \in \mathbb{C}$: root of the (univariate) gcd, hence $f_0(r) = f_1(r) = 0$.
Define nonzero column vector $[r^{d_0+d_1-1}, \ldots, r^2, r, 1]$ that lies in the right kernel of S, hence $\det S = 0$.

[$\Rightarrow$] $\det S = 0 \Rightarrow \exists w \neq 0$ vector s.t. $wS = 0$. Consider w contains the coefficients of polynomials q_0, q_1 of degrees $d_1 - 1, d_0 - 1$, hence

$$f_0 q_0 + f_1 q_1 = 0 \Rightarrow f_0 q_0 = -f_1 q_1,$$

which has degree $< d_0 + d_1$, hence $\deg \operatorname{lcm}(f_0, f_1) < d_0 + d_1$. Then,

$$\gcd = \frac{f_0 f_1}{\operatorname{lcm}} \Rightarrow \deg \gcd(f_0, f_1) = d_0 + d_1 - \deg \operatorname{lcm}(f_0, f_1) \geq 1.$$

Corollary. $R = \det S$.

Example: Circle

The circle $\subset \mathbb{R}^2$ is the set of values (x, y) s.t.:

$$x = \cos\theta,\ y = \sin\theta, \qquad \theta \in [0, 2\pi),$$

$$x = \frac{\tan^2(\theta/2) - 1}{\tan^2(\theta/2) + 1} = \frac{t^2 - 1}{t^2 + 1}, \quad y = \frac{2\tan(\theta/2)}{\tan^2(\theta/2) + 1} = \frac{2t}{t^2 + 1},$$

for $t \in (-\infty, \infty)$.

Exercise: Use the resultant to obtain the equation $x^2 + y^2 - 1 = 0$.

System solving by linear algebra (I)

Matrix Algorithms

Dense matrices $n \times m$: add/subtract in $\Theta_A(nm)$
(as opposed to sparse or structured matrices)

Square matrices $n \times n$: Multiplication $= \Omega_A(n^2)$.
Question: Is this tight?

Algorithms: school $= O_A(n^3)$.
D+C [Strassen'69] $O_A(n^{\lg 7}) = O_A(n^{2.81})$ using 4×4 matrices
[Coppersmith-Winograd'90] $O_A(n^{2.376})$ used tensor square.
Slightly worse bound using Group theory [Cohn,Umans'03]

Improvement to $\omega < 2.373$ [Stothers'10] using 4th tensor power.
Using 8th power $\omega < 2.3729$ [Vassilevska-Williams'12],
using 32nd power $\omega < 2.37286$ [Le Gall'13],
laser method $\omega < 2.3728596$ [Alman,Vassilevska-Williams'21].

Matrix operations

Let $T(n)$ be the asymptotic arithmetic complexity of multiplication. Inversion, determinant, solving $Mx = b$, factoring $M = LU$, and factoring with permutation $M = LUP$ (Gaussian elimination), all lie in $\Theta(T(n))$.

Compute the kernel $\{x : Mx = 0\}$ and the rank: both in $O(T(n))$.
Compute the characteristic polynomial in $O(T(n) \log^2 n)$.
Numeric approximation of eigen-vectors/values in $25n^3$.

Integer determinant, for entries of bit size L.
Worst-case optimal $\det A$ size $= O^*(nL)$ [Hadamard]
Algorithm avoiding rationals [Bareiss'68] $O_B^*(n^4 L)$
Baby steps / giant steps: $O_B(n^{3.2} L)$ [Kaltofen,Villard'01]

Example I

Well-constrained system
$\subset (K[y])[x]$ by "hiding" y :

$$\begin{aligned} f_0 &= (2y)x + (y-3), \\ f_1 &= yx^2 + 4x + (-y+5). \end{aligned}$$

$$\begin{array}{cc} & \begin{array}{ccc} x^2 & x & 1 \end{array} \\ \begin{array}{c} xf_0 \\ f_0 \\ f_1 \end{array} & \begin{bmatrix} 2y & y-3 & 0 \\ 0 & 2y & y-3 \\ y & 4 & -y+5 \end{bmatrix} \end{array} \begin{bmatrix} x^2 \\ x \\ 1 \end{bmatrix} = \begin{bmatrix} xf_0(x,y) \\ f_0(x,y) \\ f_1(x,y) \end{bmatrix}$$

System solving reduced to an eigenproblem:

$$\left(\underbrace{\begin{bmatrix} 0 & -3 & 0 \\ 0 & 0 & -3 \\ 0 & 4 & 5 \end{bmatrix}}_{M_0} + \beta \underbrace{\begin{bmatrix} 2 & 1 & 0 \\ 0 & 2 & 1 \\ 1 & 0 & -1 \end{bmatrix}}_{M_1} \right) \underbrace{\begin{bmatrix} \alpha^2 \\ \alpha \\ 1 \end{bmatrix}}_{v} = \vec{0}$$

$\Rightarrow \exists v : (M - \beta I)\, v = 0$ for $|M_1| \neq 0,\ M := -M_1^{-1} M_0$.

Example I (cont'd)

Invertible M_1 with $\kappa(M_1) = 2.88$:

$$C = -\begin{bmatrix} 2 & 1 & 0 \\ 0 & 2 & 1 \\ 1 & 0 & -1 \end{bmatrix}^{-1} \begin{bmatrix} 0 & -3 & 0 \\ 0 & 0 & -3 \\ 0 & 4 & 5 \end{bmatrix} = \begin{bmatrix} 0 & 10/3 & 2/3 \\ 0 & -11/3 & -4/3 \\ 0 & 22/3 & 17/3 \end{bmatrix},$$

and the standard eigenproblem $(C - \beta I)v = 0$ yields:

$$v = [1.23, \frac{-7-3\sqrt{3}}{11} \simeq -1.11, 1], \quad \beta = 1 - 2\sqrt{3},$$

$$v = [0.0269, \frac{-7+3\sqrt{3}}{11} \simeq -0.164, 1], \quad \beta = 1 + 2\sqrt{3},$$

$$v = (1, 0, 0), \quad \beta = 0.$$

Invertible M_2

Assuming $d = 2$, $\det M_2 \not\simeq 0$, $m = \dim M_i$:

$$(M_0 + M_1 y + y^2 M_2)v = 0 \iff$$

$$\iff y^2 v = (-M_2^{-1} M_0 - y M_2^{-1} M_1)v \iff$$

$$\iff \begin{bmatrix} 0_m & I_m \\ -M_2^{-1} M_0 & -M_2^{-1} M_1 \end{bmatrix} \begin{bmatrix} v \\ yv \end{bmatrix} = y \begin{bmatrix} v \\ yv \end{bmatrix} \iff Cw = yw,$$

where companion matrix C is of dimension $2m$, $0_m, I_m$ of dimension m.

Proof. The last matrix equation is equivalent to

$$\begin{cases} I_m yv = yv, \\ -M_2^{-1} M_0 v - M_2^{-1} M_1 yv = y^2 v, \end{cases}$$

where the first equation ensures the structure of the eigenvector, and the second is the original equation.

Invertible M_d

If $\det M_d \not\approx 0$, define the companion matrix C, $\dim(C) = md$, $m = \dim M_i$:

$$C = \begin{bmatrix} 0_m & I_m & & 0_m \\ \vdots & & \ddots & \\ 0_m & 0_m & & I_m \\ -M_d^{-1}M_0 & -M_d^{-1}M_1 & \cdots & -M_d^{-1}M_{d-1} \end{bmatrix}, \text{ then}$$

$$M(y)v = 0 \iff -M_d(-M_d^{-1}M_0 - \cdots - y^{d-1}M_d^{-1}M_{d-1} - y^d I_m)v = 0 \iff$$

$$\iff (-M_d^{-1}M_0 - \cdots - y^{d-1}M_d^{-1}M_{d-1})v = y^d v \iff Cw = yw,$$

where $w = (v, yv, y^2v, \ldots, y^{d-1}v) \in \mathbb{C}^{md}$, $w \neq 0$.

Now $(C - yI)w = 0$ is a standard eigenproblem: each eigenvalue yields one root's y-coordinate, the corresponding eigenvector w contains the values $y^i v$ at this root, for the monomials v indexing M.

Overview of System Solving

Hiding variable y leads to a resultant matrix $M(y)$ with entries in y. If y with degree d, we solve for y and vector $v \neq 0$ in $M(y)v = 0$:

$$M(y) = M_d y^d + \cdots + M_1 y + M_0.$$

The solutions (y, v), s.t. the eigenvalue y is simple (multiplicity $= 1$), yield (a superset of) simple solutions (x, y) of $f_0 = f_1 = 0$.

For $d \geq 1$, md-dimensional matrices are defined, $m = \dim M(y)$. Reduce to a standard eigenproblem (on companion matrix if M_d invertible) or generalized eigenproblem $L_1 - \lambda L_0$.

Example II

Hide variable y :

$$\begin{aligned} f_0 &= (y-1)x + (y+1), \\ f_1 &= (y-1)x^2 + (2y+1)x + (y+1). \end{aligned}$$

$$\begin{array}{cc} & \begin{array}{ccc} x^2 & \quad x & \quad 1 \end{array} \\ \begin{array}{c} x f_0 \\ f_0 \\ f_1 \end{array} & \begin{bmatrix} y-1 & y+1 & 0 \\ 0 & y-1 & y+1 \\ y-1 & 2y+1 & y+1 \end{bmatrix} \begin{bmatrix} x^2 \\ x \\ 1 \end{bmatrix} = \begin{bmatrix} x f_0(x,y) \\ f_0(x,y) \\ f_1(x,y) \end{bmatrix} \end{array}$$

$\det M_1 = 0, \kappa(M_1) \to \infty$, so generalized eigenproblem $(L_0 - \lambda L_1)v = 0$

$$\left(\begin{bmatrix} -1 & 1 & 0 \\ 0 & -1 & 1 \\ -1 & 1 & 1 \end{bmatrix} - \lambda \begin{bmatrix} -1 & -1 & 0 \\ 0 & -1 & -1 \\ -1 & -2 & -1 \end{bmatrix} \right) \begin{bmatrix} x^2 \\ x \\ 1 \end{bmatrix} = 0.$$

Example II (cont'd)

The following generalized eigenproblem:

$$(\begin{bmatrix} -1 & 1 & 0 \\ 0 & -1 & 1 \\ -1 & 1 & 1 \end{bmatrix} - \lambda \begin{bmatrix} -1 & -1 & 0 \\ 0 & -1 & -1 \\ -1 & -2 & -1 \end{bmatrix}) \begin{bmatrix} x^2 \\ x \\ 1 \end{bmatrix} = 0$$

has solutions:

- $\lambda = y = -1, x = 0$ from eigenvector $[0, 0, 1]$ (after normalizing the last coordinate); this is the unique "relevant" solution in $\mathbb{C}$.
- $\lambda = y = 1, x$ impossible in the original polynomial system since the (generalized) eigenvector equals $[1, 0, 0]$.
- $\lambda \to \infty$ hence y not affine; note eigenvector $[1, -1, 1]$ yields $x = -1$

Singular M_3

Assuming $d = 3$, $\det M_3 \simeq 0$:

$$(M_0 + M_1 y + y^2 M_2 + y^3 M_3)v = 0 \iff (L_1 y + L_0)w = 0 \iff$$

$$\iff \left(\begin{bmatrix} I_m & 0_m & 0_m \\ 0_m & I_m & 0_m \\ 0_m & 0_m & M_3 \end{bmatrix} y + \begin{bmatrix} 0_m & -I_m & 0_m \\ 0_m & 0_m & -I_m \\ M_0 & M_1 & M_2 \end{bmatrix} \right) \begin{bmatrix} v \\ yv \\ y^2 v \end{bmatrix} = 0.$$

Proof. The last matrix equation is equivalent to

$$\begin{cases} I_m yv - yv = 0, \\ I_m y^2 v - I_m \cdot y^2 v = 0, \\ M_3 y^3 v + M_0 v + M_1 yv + M_2 y^2 v = 0. \end{cases}$$

The first two equations impose the structure of the eigenvector $w \neq 0$, and the last one is the original matrix equation.

Singular M_d

If M_d is singular or ill-conditioned, i.e. with high condition number κ, M_d^{-1} is "noisy" so we solve generalized eigenproblem $(L_1 y + L_0)w = 0$ for matrices L_i, vector w:

$$\left(\begin{bmatrix} I_m & 0_m & \dots & 0_m \\ & \ddots & & \\ & & I_m & 0_m \\ 0_m & \dots & 0_m & M_d \end{bmatrix} y + \begin{bmatrix} 0_m & -I_m & 0_m & \dots \\ \vdots & & \ddots & \\ 0_m & & & -I_m \\ M_0 & M_1 & \cdots & M_{d-1} \end{bmatrix} \right) \begin{bmatrix} v \\ yv \\ \vdots \\ y^{d-1}v \end{bmatrix} = 0.$$

– $0_m, I_m$ are zero / identity $m \times m$ matrices, $\dim M_i = m$.
– Each generalized eigenvalue gives the y-coordinates of one root,
– the corresponding eigenvector $w \neq 0$ yields the x-coordinate of this root by looking at v, whose entries equal the column monomials of the Sylvester matrix evaluated at this x-coordinate.

Numerics

Let A with $\sigma_{\mathrm{max}}(A)$, $\sigma_{\mathrm{min}}(A)$ its maximal and minimal singular values, its condition number is $\kappa(A) = \sigma_{\mathrm{max}}(A)/\sigma_{\mathrm{min}}(A) = \max_v \|Av\|_2/\|v\|_2$.

Decide whether $m \times m$ matrix A is numerically invertible:
– Compute singular values $\sigma_1 \leq \cdots \leq \sigma_m$.
– If $\kappa < 10^5$ or $< 10^7$ (depending on the input), then invert A. But if σ_1 is (nearly) zero, or κ very large, then A should not be inverted.
– Rank balancing may help $x \mapsto (r_1 y + r_2)/(r_3 t + r_4)$

Eigenvectors. The v that yield a solution to the original system have a specific coordinate equal to 1: pick c so that cv has this coordinate $= 1$. If this coordinate is zero, then v does not lead to a system's solution.

Multiplicity

Defn. Let A be $n \times n$ and $|A - xI_n| = (x-\lambda_1)^{n_1} \cdots (x-\lambda_k)^{n_k}$, $\lambda_i \in \mathbb{C}$.
1. The $n_1, \ldots, n_k$ are algebraic multiplicities of the λ_i, $n_1 + \cdots + n_k = n$
2. The geometric multiplicity of $\lambda_i = \#$linearly independent eigenvectors corresponding to $\lambda_i = \dim(\text{nullspace}(A - \lambda_i I_n))$.
3. Fact: geometric multiplicity of $\lambda \leq$ algebraic multiplicity of λ. Hence the union of all eigenspaces may be a proper subspace of $\mathbb{C}^n$.

Algorithm. If multiplicity of an eigenvalue is > 1, then hard to use the eigenvector: solve the system for the hidden variable at the eigenvalue.

Multivariate polynomials

Matrix construction

Beyond Sylvester: $n \geq 2$

Problem: contruct M, equivalently define the row monomials, s.t.:
– M is square
– $\det M \neq 0$ for generic coefficients
– $\det M = 0$ if $R = 0$ (ideally iff $R = 0$)
– Hopefully $\deg_{f_0} \det M = \deg_{f_0} R$.
– Sylvester-type: rows contain the coefficient vector of f_i

Algorithms for Sylvester-type matrices:
– Dialytic elimination, incremental heuristics
– Macaulay's for the projective resultant
– Canny-E for the toric/sparse resultant, D'Andrea et al.
– Special cases (Khetan, D'Andrea . . .), multihomogeneous

A u-resultant matrix

$$\begin{aligned}
f_0 &= & & u_1x_1 + & & u_2x_2 + u_0 = 0,\\
f_1 &= x_1^2 + x_1x_2 + & & 2x_1 \quad + & & x_2 - \quad 1 = 0,\\
f_2 &= x_1^2 \qquad\quad + & & 3x_1 - x_2^2 + & & 2x_2 - \quad 1 = 0.
\end{aligned}$$

$$\text{Macaulay's matrix} = \begin{array}{c}
\begin{array}{cccccccccc} x_1^3 & x_1^2x_2 & x_1^2 & x_1x_2^2 & x_1x_2 & x_1 & x_2^3 & x_2^2 & x_2 & 1 \end{array}\\
\begin{bmatrix}
1 & 1 & 2 & 0 & 1 & -1 & 0 & 0 & 0 & 0\\
0 & 1 & 0 & 1 & 2 & 0 & 0 & 1 & -1 & 0\\
0 & 0 & 1 & 0 & 1 & 2 & 0 & 0 & 1 & -1\\
1 & 0 & 3 & -1 & 2 & -1 & 0 & 0 & 0 & 0\\
0 & 1 & 0 & 0 & 3 & 0 & -1 & 2 & -1 & 0\\
0 & 0 & 1 & 0 & 0 & 3 & 0 & -1 & 2 & -1\\
0 & u_1 & 0 & u_2 & u_0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & u_1 & 0 & u_2 & u_0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & u_1 & 0 & 0 & u_2 & u_0 & 0\\
0 & 0 & 0 & 0 & 0 & u_1 & 0 & 0 & u_2 & u_0
\end{bmatrix}
\end{array}
\begin{array}{c} x_1f_1\\ x_2f_1\\ f_1\\ x_1f_2\\ x_2f_2\\ f_2\\ x_1x_2f_0\\ x_1f_0\\ x_2f_0\\ f_0 \end{array}$$

The u-resultant is $|M| = (u_1 - u_2 + u_0)(-3u_1 + u_2 + u_0)(u_2 + u_0)(u_1 - u_2)$
$\Rightarrow$ the roots are $(1, -1), (-3, 1), (0, 1), (0 : 1 : -1)$.

Question. Can you find a smaller resultant matrix?

Macaulay's construction [1902]

Let $f_0, \ldots, f_n \in K[x_1, \ldots, x_n]$ each given by its total degree $d_i > 0$.

Let T be the set of monomials $t \in K[x]$ of degree $\leq \nu = \sum_{i=0}^{n} d_i - n$.

$$B_n := \{t \in T \mid \deg_{x_n} t \geq d_n\}, \; B_{n-1} := \{t \in T - B_n \mid \deg_{x_{n-1}} t \geq d_{n-1}\}, \ldots$$

$$\text{Generally } B_i := \left\{t \in T - \bigcup_{j=i+1}^{n} B_j \mid \deg_{x_i} t \geq d_i\right\}, \; i = 1, \ldots, n,$$

$$\text{and } B_0 := T - \bigcup_{i=1}^{n} B_i.$$

Example: linear system

$$f_i = c_{i3} + c_{i1}x_1 + c_{i2}x_2, \ i = 0, \ldots, 2,$$

Therefore $n = 2, \nu = 3 - 2 = 1$,
$B_2 = \{x_2\}, B_1 = \{x_1\}, B_0 = \{1\}$.

$$M = \begin{array}{cc} & \begin{array}{ccc} x_1 & x_2 & 1 \end{array} \\ & \begin{bmatrix} c_{01} & c_{02} & c_{03} \\ c_{11} & c_{12} & c_{13} \\ c_{21} & c_{22} & c_{23} \end{bmatrix} \end{array} \quad \begin{array}{c} {\color{red} f_0} \\ {\color{green} f_1} \\ {\color{blue} f_2} \end{array}$$

Macaulay's construction (cont'd)

Lemma. The B_i's partition T, such that

$$|B_i| \geq \prod_{j \neq i} d_j,\ i = 1, \ldots, n \text{ and } |B_0| = \prod_{j \neq 0} d_j.$$

Proof.
$|T| = \binom{n+\nu}{n}$ lattice points in n-dim simplex of edge length ν.

B_0 contains no monomial of total degree $\geq \nu$.
The B_i, $i \geq 1$ cut out pieces from the ν-simplex, hence B_0 corresponds to a hyper-rectangle with x_i-edge length $= d_i$.

B_n contains points in an n-dim simplex of size $\nu - d_n = \sum_{i<n} d_i - n$.
So $|B_n| = \binom{\sum_{i<n} d_i}{n} \geq \prod_{i<n} d_i$ by a combinatorial argument.

Exercise: prove the lemma for $B_1, \ldots, B_{n-1}$.

Macaulay matrix

Define the Macaulay matrix with rows expressing,

$$t f_0, \text{ for } t \in B_0, \quad \frac{t}{x_i^{d_i}} f_i, \text{ for } t \in B_i, \, i = 1, \ldots, n.$$

Thm. [Macaulay'1902] The Macaulay matrix M is:
(a) square, (b) generically nonsingular, (c) $R \mid \det M$,
(d) $\exists$ submatrix M' : $R = \det M / \det M'$.
Pf. Next slide.

Cor. Let the above matrix be M_0 then

$$\deg_{f_0} R = \prod_{i=1}^{n} \deg f_i = \deg_{f_0} |M_0|.$$

Analogously can define $M_1, \ldots, M_n$. Then $R = \gcd(|M_0|, \ldots, |M_n|)$.

Proof of theorem (a-c)

Thm. The Macaulay matrix M is: (a) square, (b) generically nonsingular, (c) $R \mid \det M$.

Proof.
(a) Columns and rows can be indexed by T.

(b) Take any row of f_i:

$$f_i = \cdots + c_i x_i^{d_i} + \cdots \Rightarrow \text{ row contains } \frac{t}{x_i^{d_i}} f_i = \cdots + c_i t + \cdots,$$

hence c_i appears on the diagonal. For a specialization where all f_i coefficients $\to 0, c_i \to 1$, we have $f_i \to x_i^{d_i}, f_0 \to 1$, thus $M \to I$.

(c) We showed $\deg_{f_i} |M| \geq \deg_{f_i} R$. Now, $R = 0 \Rightarrow \exists v$: contains values of T at root; $v \neq 0$ because $1 \in T$, and $Mv = 0 \Rightarrow \det M = 0$ (holds for every Sylvester-type resultant matrix).

Proof of theorem (d)

Thm. For the Macaulay matrix M:
(d) Specify submatrix M' : $R = \det M / \det M'$.

Recall B_n contains monomials divisible by $x_n^{d_n}$, B_{n-1} contains among the rest, those divisible by $x_{n-1}^{d_{n-1}}$, and so on. No $t \in B_0$ is divisible by any $x_i^{d_i}$.

Proof. (d) Specify the reduced monomials in T:
(i) $t \in B_i$, $i \in \{1, \ldots, n\}$, not divisible by $x_j^{d_j}$, $j \neq i$, and $\deg t > \nu - d_0$ so as not divisible by $x_0^{d_0}$, for x_0 homogenizing variable;
(ii) all $t \in B_0$ since $\deg t \leq \nu - d_0$ so divisible by $x_0^{d_0}$ only.

M' has rows/columns indexed by the non-reduced monomials in T.

Properties:

- $\det M' \not\equiv 0$ by similar proof as for $\det M$.
- $\deg_{f_i} |M'| = \deg_{f_i} R - \deg_{f_i} |M|$.
- For specialization in (b) $\det M \mid \det M'$, so $\det M' = 0 \Rightarrow \det M = 0$.

The u-resultant matrix

$$\begin{aligned} f_0 &= & & u_1 x_1 + & & u_2 x_2 + u_0 = 0, \\ f_1 &= x_1^2 + x_1 x_2 + & & 2x_1 \quad + & & x_2 - 1 = 0, \\ f_2 &= x_1^2 \quad\quad + & & 3x_1 - x_2^2 + & & 2x_2 - 1 = 0. \end{aligned}$$

$$\text{Macaulay matrix} = \begin{array}{c} \begin{array}{cccccccccc} x_1^3 & x_1^2 x_2 & x_1^2 & x_1 x_2^2 & x_1 x_2 & x_1 & x_2^3 & x_2^2 & x_2 & 1 \end{array} \\ \left[\begin{array}{cccccccccc} 1 & 1 & 2 & 0 & 1 & -1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 2 & 0 & 0 & 1 & -1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 2 & 0 & 0 & 1 & -1 \\ 1 & 0 & 3 & -1 & 2 & -1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 3 & 0 & -1 & 2 & -1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 3 & 0 & -1 & 2 & -1 \\ 0 & u_1 & 0 & u_2 & u_0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & u_1 & 0 & u_2 & u_0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & u_1 & 0 & 0 & u_2 & u_0 & 0 \\ 0 & 0 & 0 & 0 & 0 & u_1 & 0 & 0 & u_2 & u_0 \end{array}\right] \end{array} \begin{array}{c} x_1 f_1 \\ x_2 f_1 \\ f_1 \\ x_1 f_2 \\ x_2 f_2 \\ f_2 \\ x_1 x_2 f_0 \\ x_1 f_0 \\ x_2 f_0 \\ f_0 \end{array}$$

The u-resultant is $|M| = (u_1 - u_2 + u_0)(-3u_1 + u_2 + u_0)(u_2 + u_0)(u_1 - u_2)$
$\Rightarrow$ the roots are $(1, -1), (-3, 1), (0, 1), (0 : 1 : -1)$.

$\nu = 3$, optimal #rows is $4, 2, 2$.
$B_2 = \{x_1 x_2^2, x_2^3, x_2^2\}$, non-reduced monomials x_2^2, x_1^2 (divisible by x_0).

Bézout matrices

Bézout matrix

Defn. The Bézout matrix of polynomials f, g of degree n is $B = (b_{i,j})$ s.t.

$$\frac{f(x)g(y) - f(y)g(x)}{x - y} = \sum_{i,j \geq 0} b_{i,j} x^i y^j, \quad i, j = 0, \ldots, n.$$

It satisfies $R(f, g) = \mathrm{det}(B)$.

Example: $f = f_0 + f_1 x + f_2 x^2$, $g = g_0 + g_1 x + g_2 x^2$:

$$\mathrm{Sylv}(f,g) = \begin{bmatrix} f_0 & f_1 & f_2 & 0 \\ 0 & f_0 & f_1 & f_2 \\ g_0 & g_1 & g_2 & 0 \\ 0 & g_0 & g_1 & g_2 \end{bmatrix}, \quad B = \begin{bmatrix} f_0 g_1 - f_1 g_0 & f_0 g_2 - f_2 g_0 \\ f_0 g_2 - f_2 g_0 & f_1 g_2 - f_2 g_1 \end{bmatrix}.$$

General properties in [Elkadi-Mourrain'98].

Bezoutian

Definition. For $f_0, \ldots, f_n \in K[x_1, \ldots, x_n]$, the Bezoutian polynomial is

$$\Theta_{f_i}(x,z) = \det \begin{bmatrix} f_0(x) & \theta_1(f_0)(x,z) & \cdots & \theta_n(f_0)(x,z) \\ \vdots & \vdots & \vdots & \vdots \\ f_n(x) & \theta_1(f_n)(x,z) & \cdots & \theta_n(f_n)(x,z) \end{bmatrix},$$

$$\theta_i(f_j)(x,z) = \frac{f_j(z_1, \ldots, z_{i-1}, x_i, \ldots, x_n) - f_j(z_1, \ldots, z_i, x_{i+1}, \ldots, x_n)}{x_i - z_i}.$$

Let $$\Theta_{f_0,\ldots,f_n}(x,z) = \sum_{a,b} \theta_{ab}\, x^a z^b, \ \theta_{a,b} \in K, \ a, b \in \mathbb{N}^n.$$

Then Bézout's matrix of $f_0, \ldots, f_n$ is the matrix $[\theta_{ab}]_{a,b}$.

Theorem. [Cardinal-Mourrain'96] The resultant divides all maximal nonzero minors of Bézout's matrix.
The dimension of the matrix is $O(e^n d^n)$, $d = \max\{\deg f_i\}$.

Examples

$n = 1$ [Béz1779]

$$\begin{aligned} f_0 &= x_0^2 + x_0x_1 + 2x_0 \qquad + \quad x_1 - 1, \\ f_1 &= x_0^2 \qquad\qquad + 3x_0 - x_1^2 + 2x_1 - 1. \end{aligned}$$

$R = -{x_0}^3 - 2\,{x_0}^2 + 3\,x_0 =$

$$\det \begin{bmatrix} x_0 + 1 & {x_0}^2 + 2\,x_0 - 1 \\ -{x_0}^2 - 4\,x_0 - 1 & -(x_0+1)\left(x_0^2 + 3x_0 - 1\right) \end{bmatrix}$$

$n = 2$: Hide t_3 in cyclohexane system:

$$\begin{aligned} f_i &= (13 + t_3^2) - 24t_jt_3 + (1 + t_3^2)t_j^2 = 0,\ \{i, j\} = \{1, 2\} \\ f_3 &= 13 + t_2^2 - 24t_1t_2 + t_1^2 + t_1^2t_2^2 = 0 \end{aligned}$$

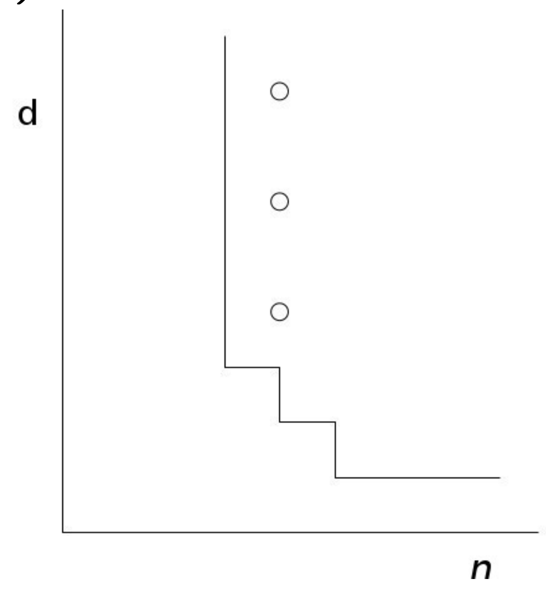
B is 8×8,

$|B| = 186624\ \left({t_3}^4 - 118\,{t_3}^2 + 13\right)\left({t_3}^4 - 22\,{t_3}^2 + 13\right)^3 \left({t_3}^2 + 1\right)^8.$

Homogeneous unmixed systems

State of the art. Given $n+1$ dense polynomials in n variables of total degree d, an optimal (Sylvester, Bézout or polynomial) formula is known for

- $d = 1$
- $n \leq 3$
- $n = 4$, $d \leq 3$, $d = 4, 6, 8$
- $n = 5$, $d = 2$



- [D'Andrea-Dickenstein'01] [Khetan'02]
- Koszul-Weyman complexes [GKZ'94]
- Chow complex [Eisenbud-Schreyer'03]

Gröbner bases

Gröbner bases

Fix a monomial order "$<$" in $K[x_1, \ldots, x_n]$.
- Lexicographical (LEX) order: $x^A > x^B \iff$ the first nonzero entry of $A - B$ is positive. E.g.: $x_1^2 < x_1x_2 < x_2^2 < x_1x_3 < x_2x_3 < x_3^2$.
- Degree (Graded) Reverse lexicographical (DRL): $x^A > x^B \iff \|A\|_1 > \|B\|_1$, or $\|A\|_1 = \|B\|_1$ & last nonzero entry of $A - B$ negative.

E.g. for $x_1 < x_2 < x_3$: $x_1^2 < x_1x_2 < x_1x_3 < x_2^2 < x_2x_3 < x_3^2$.

Definition. Let $in_<(f) =$ initial / leading monomial of f. For an ideal I, a family $G = \{g_i\}$ of generators of I, s.t. $\langle in(g_i)\rangle = in(I)$, is a Gröbner basis of I. Given an order and G, define NormalForm f mod $I = f$ mod G.

Algorithms

- [Buchberger] Given some generators G, for each pair of generators f_i, f_j, compute the S-polynomial:

$$S(i,j) = \frac{\text{lcm}(in(f_i), in(f_j))}{in(f_i)} f_i - \frac{\text{lcm}(in(f_i), in(f_j))}{in(f_j)} f_j.$$

Divide $S(i,j)$ by G, getting $S'(i,j)$. Update generators to $G \cup \{S'(i,j)\}$.

- F4 [Faugère'99] Build matrices at each step.
- F5 [Faugère'02] Optimality for regular sequences. The algorithms will end (Hilbert syzygy theorem), but at which degree?

Further bases: Border, SAGBI, Khovanski, Involutive . . .

Regularity and Gröbner bases

[Bayer-Stillman'87] After a generic change of coordinates and using DRL, computations will finish at reg(I) [Castelnuovo 1893], [Mumford'66].

Expect bad (double exponential in the degree) bounds for this regularity [Giusti'84], [Galligo'78].

Macaulay [Lazard'83]: For $n+1$ generic forms of degree $d_0, \ldots, d_n$,

$$\text{reg}(I) = \sum_{i=0}^{n} d_i - n.$$

and this is tight.

Multiplication maps

Let ideal $I := \langle f_1, \ldots, f_m \rangle \subset K[x_1, \ldots, x_n] = K[x]$. The quotient ring

$$K[x]/I = \{b \bmod I \, : \, b \in K[x]\}$$

is a K-vector-space if I is 0-dimensional.

Multiplication in $K[x]/I$ by polynomial $f \in K[x]$, is linear map:

$$M_f \; : \; K[x]/I \to K[x]/I \; : \; b \mapsto fb \bmod I.$$

For well-constrainted $f_1, \ldots, f_n$, multiplication map M_f obtained from Gröbner basis, of size $\deg I$, s.t. $f(r), r \in V(I)$ are the eigenvalues of M_f.

Resultant: Set overconstrained system with $f_0(u)$; build resultant matrix; Schur complement of dimension $\deg f_1 \cdots \deg f_n$ is M_{f_0}, indexed by B_0.

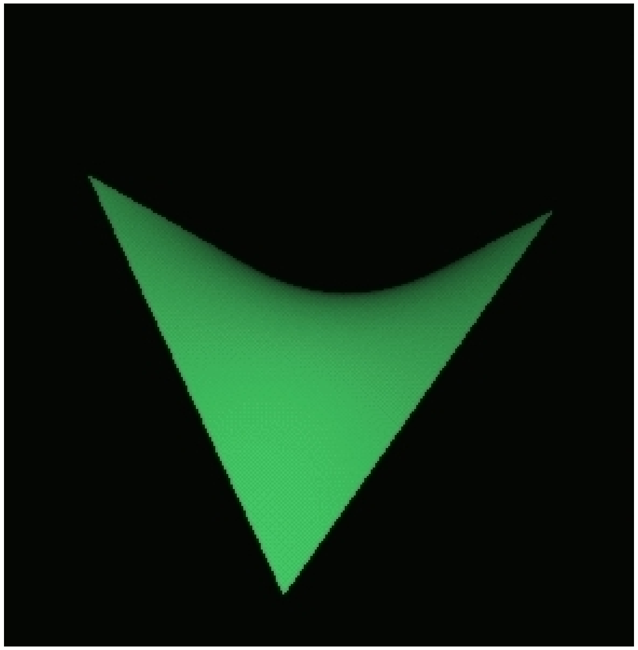
Beyond dense systems

Example: Bilinear surface

A bilinear surface $\subset \mathbb{R}^3$ is given as the set of values (x_1, x_2, x_3):

$$x_i = c_{i0} + c_{i1}s + c_{i2}t + c_{i3}st, \;\; i = 1,2,3, \quad \text{for } s,t \in [0,1],$$

or as the set of roots of a polynomial equation $H(x_1, x_2, x_3) = 0$.



Modeling/CAD use parametric *AND* implicit/algebraic representations
$\Rightarrow$ need to implicitize a curve/surface given a (rational) parameterization

Bilinear system: Resultant matrix

$$f_i = (c_{i0} - x_i) + c_{i1}s + c_{i2}t + c_{i3}st, \;\; i = 1, 2, 3.$$

The classical projective resultant vanishes identically.
The toric (sparse) resultant has $\deg R = 3 \cdot \deg_{f_i} R = 6$.

A determinantal Sylvester-type formula for the toric resultant is:

$$R = \det \begin{array}{cc} \begin{array}{cccccc} 1 & s & t & st & s^2 & s^2 t \end{array} & \\ \begin{bmatrix} c_{10} - x_1 & c_{11} & c_{12} & c_{13} & 0 & 0 \\ c_{20} - x_2 & c_{21} & c_{22} & c_{23} & 0 & 0 \\ c_{30} - x_3 & c_{31} & c_{32} & c_{33} & 0 & 0 \\ 0 & c_{10} - x_1 & 0 & c_{12} & c_{11} & c_{13} \\ 0 & c_{20} - x_2 & 0 & c_{22} & c_{21} & c_{23} \\ 0 & c_{30} - x_3 & 0 & c_{32} & c_{31} & c_{33} \end{bmatrix} & \begin{array}{c} f_1 \\ f_2 \\ f_3 \\ sf_1 \\ sf_2 \\ sf_3 \end{array} \end{array}$$

Sparse elimination theory

Newton polytopes

The support A_i of a polynomial $f_i \in K[x_1^{\pm 1}, \ldots, x_n^{\pm 1}]$, s.t.

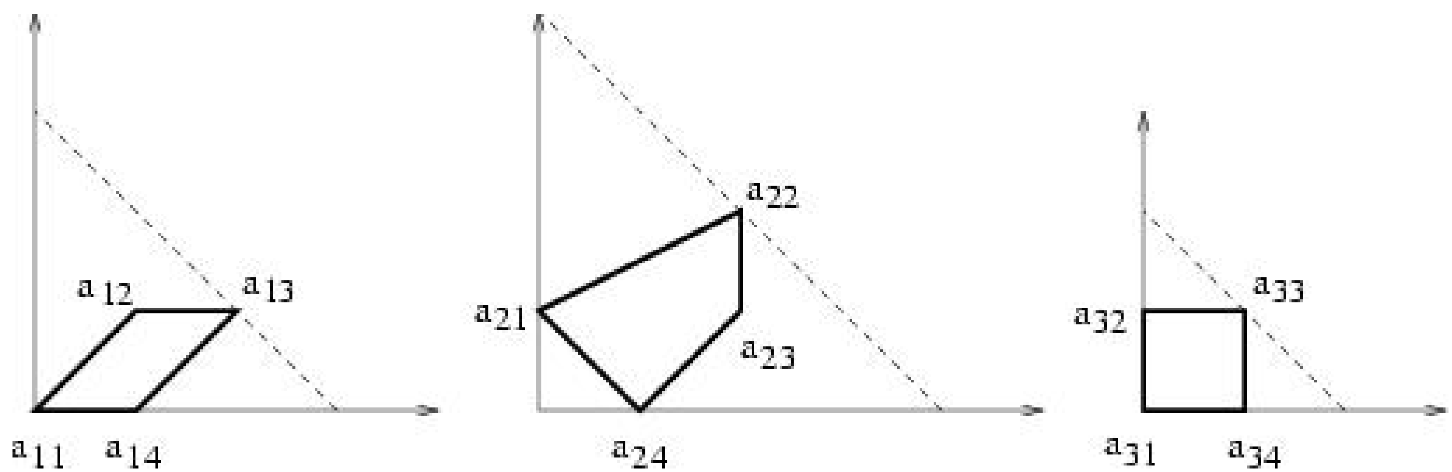
$$f_i = \sum_j c_{ij} x^{a_{ij}}, \qquad c_{ij} \neq 0,$$

is defined as the set $A_i := \{a_{ij} \in \mathbb{Z}^n : c_{ij} \neq 0\}$.

The Newton polytope $Q_i \subset \mathbb{R}^n$ of f_i is the Convex Hull of all $a_{ij} \in A_i$.

Example:

$$\begin{aligned} f_1 &= c_{11} + c_{12}xy + c_{13}x^2y + c_{14}x \\ f_2 &= c_{21}y + c_{22}x^2y^2 + c_{23}x^2y + c_{24}x + c_{25}xy \\ f_3 &= c_{31} + c_{32}y + c_{33}xy + c_{34}x \end{aligned}$$



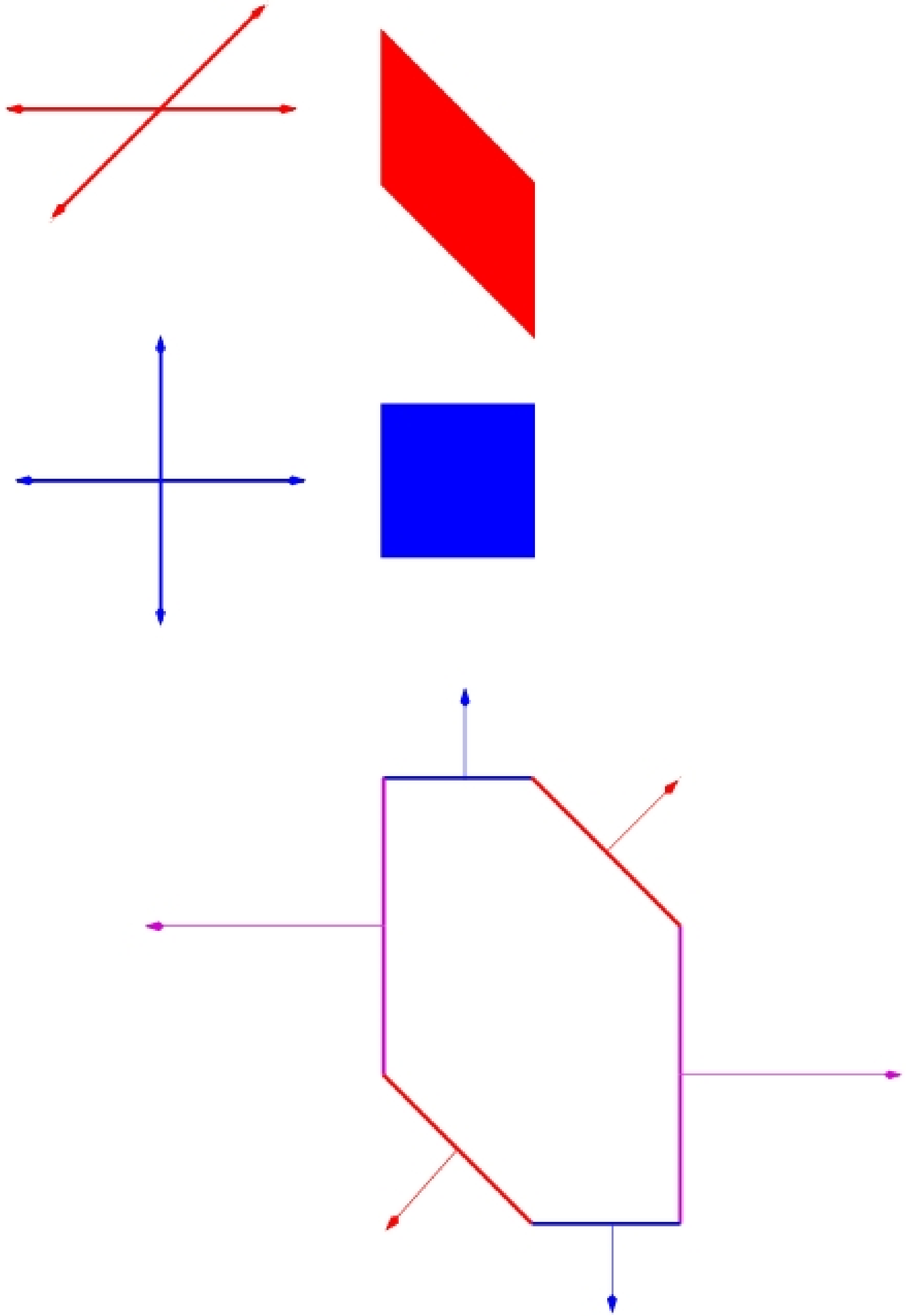
Minkowski addition

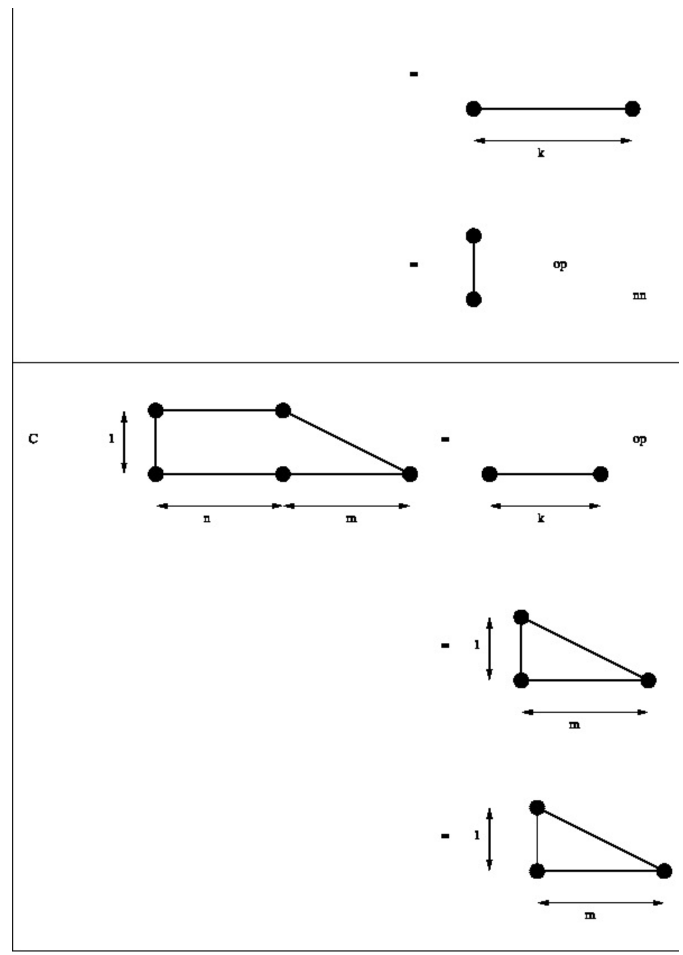
- The Minkowski sum of convex polytopes $P_1, P_2 \subset \mathbb{R}^n$ is convex polytope $P_1 + P_2 = \{p_1 + p_2 \mid p_i \in P_i\} \subset \mathbb{R}^n$.
If P_1, P_2 have integral vertices, then so does $P_1 + P_2$.

- Minkowski addition of polytopes $P_i \subset \mathbb{R}^n,\ i \in I$ is a many-to-one map

$$(P_i)_{i\in I} \to P := \sum_{i\in I} P_i \subset \mathbb{R}^n : (p_i \in P_i)_{i\in I} \mapsto \sum_{i\in I} p_i.$$

- Complexity in $\mathbb{R}^2$: Minkowski addition is linear, but Minkowski decomposition is NP-hard.





k
op
nn
C
1
n
m
k
op
1
m
1
m

Mixed volume

1. The mixed volume $\mathrm{MV}(P_1,\ldots,P_n) \in \mathbb{R}$ of convex polytopes $P_i \subset \mathbb{R}^n$

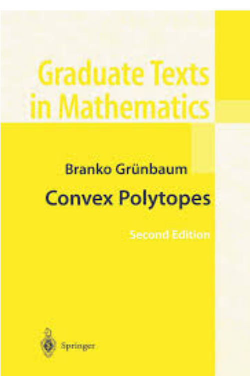
- is multilinear wrt Minkowski addition and scalar multiplication:

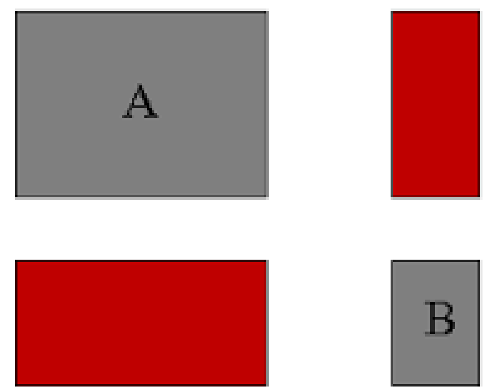
$$\mathrm{MV}(P_1,\ldots,\lambda P_i + \mu P_i',\ldots,P_n) =$$
$$= \lambda \mathrm{MV}(P_1,\ldots,P_i,\ldots,P_n) + \mu \mathrm{MV}(P_1,\ldots,P_i',\ldots,P_n), \qquad \lambda,\mu \in \mathbb{R},$$

- st. $\mathrm{MV}(P_1,\ldots,P_1) = n!\ \mathrm{vol}(P_1)$.

2. Equivalently, $\mathrm{vol}(\lambda_1 P_1 + \cdots + \lambda_n P_n)$ is a polynomial in scalar variables $\lambda_1,\ldots,\lambda_n$, with multilinear term $\mathrm{MV}(P_1,\ldots,P_n)\ \lambda_1 \cdots \lambda_n$.

3. Exclusion-Inclusion formula: $\displaystyle \mathrm{MV} := \sum_{I \subset \{1,\ldots,n\}} (-1)^{n-|I|}\ \mathrm{vol}\left(\sum_{i\in I} Q_i\right).$





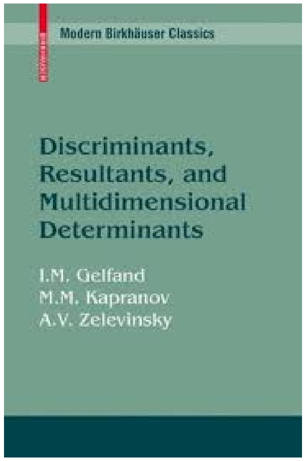
Mixed Volume characterization

Property	MV: $\text{vtx}(Q_i) \subset \mathbb{Z}^n$	Generic number of isolated solutions
$\in \mathbb{Z}_{\geq 0}$	$\text{MV}(\ldots, Q_i, \ldots)$	$\#\{x \in (\overline{K}^*)^n \mid \cdots = f_i(x) = \cdots = 0\}$
Invariance by permutation	$\text{MV}(\ldots, Q_j, \ldots, Q_i, \ldots) =$ $= \text{MV}(\ldots, Q_i, \ldots, Q_j, \ldots)$	$\#\{x \mid \cdots = f_j(x) = \cdots = f_i(x) = \cdots = 0\} =$ $= \#\{x \mid \cdots = f_i(x) = \cdots = f_j(x) = \cdots = 0\}$
Linearity wrt Minkowski addition	$\text{MV}(\ldots, Q_i + Q_i', \ldots) =$ $= \text{MV}(\ldots, Q_i, \ldots) +$ $+ \text{MV}(\ldots, Q_i', \ldots)$	$\#\{x \mid \cdots = (f_i f_i')(x) = \cdots = 0\} =$ $= \#\{x \mid \cdots = f_i(x) = \cdots = 0\} +$ $+ \#\{x \mid \cdots = f_i'(x) = \cdots = 0\}$
Linearity wrt scalar product	$\text{MV}(\ldots, \lambda Q_i, \ldots) =$ $= \lambda\ \text{MV}(\ldots, Q_i, \ldots)$	$\#\{x \mid \cdots = (f_i(x))^\lambda = \cdots = 0\} =$ $= \lambda\ \#\{x \mid \cdots = f_i(x) = \cdots = 0\}$
Monotone wrt volume	$\text{MV}(\ldots, Q_i \cup \{a\}, \ldots) \geq$ $\geq \text{MV}(\ldots, Q_i, \ldots)$	$\#\{x \mid \cdots = f_i(x) + cx^a = \cdots = 0\} \geq$ $\geq \#\{x \mid \cdots = f_i(x) = \cdots = 0\}$
[Kushnirenko]	$\text{MV}(Q_1, \ldots, Q_1) = n! V(Q_1)$	$\#\{x \mid f_1(x) = \cdots = f_n(x) = 0\} = n! V(Q_1)$

Bernstein (BKK) bound

Theorem [Bernstein'75,Kushnirenko'75,Khovanskii'78] [Danilov'78]:
Given polynomials $f_1, \ldots, f_n \in K[x_1^{\pm 1}, \ldots, x_n^{\pm 1}]$, for any field K, the number of common isolated zeros in $(\overline{K} - \{0\})^n$, counting multiplicities, is bounded by the mixed volume of the Newton polytopes MV$(Q_1, \ldots, Q_n)$ (irrespective of the variety's dimension).

Dense homogeneous: MV$(Q_1, \ldots, Q_n) = \prod_{i=1}^{n} d_i =$ Bézout's bound, where $d_i = \deg(f_i)$ and $Q_i = \text{simplex}\{0, (d_i, 0, \ldots, 0), \ldots, (0, \ldots, 0, d_i)\}$.



Exactness of BKK

Theorem 2 [Bernstein'75] BKK is exact if, $\forall\ v \in \mathbb{R}^n$, the face system $\partial_v f_1 = \cdots = \partial_v f_n = 0$ has no solution in $(\overline{K}^*)^n$.

[Canny,Rojas'91]: BKK is exact if the extremal coefficients are generic.

[Huber,Sturmfels'95]: BKK is exact if all facet systems $\partial_v f_1 = \ldots = \partial_v f_n = 0$, the sparse resultant equals a constant.

Extensions

Dense multi-homogeneous: $\mathsf{MV}(Q_1,\dots,Q_n) =$ m-Bézout's bound:

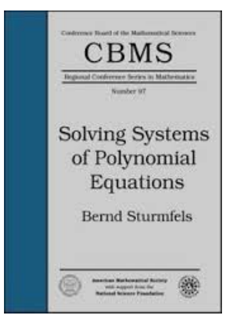
$$\text{the coefficient of } \prod_{j=1}^{r} y_j^{n_j} \text{ in } \prod_{i=1}^{n} (d_{i1}y_1 + \cdots + d_{ir}y_r),$$

where $\deg_{X_j} f_i = d_{ij}, j = 1,\dots,r$, and X_j contains n_j variables.

Affine [Huber,Sturmfels'95]: For indices I, let $\mathbb{C}_I = \{x \in \mathbb{C}^n : x_i = 0 \Rightarrow i \in I\}$. The number of isolated roots in $\mathbb{C}_I$, counting multiplicities, is bounded by the I-stable mixed volume of $A'_1,\dots,A'_n$, $A'_i = \mathrm{supp}(f_i) \cup \{0\}$:

$$\sum_{\sigma} \mathsf{MV}(F_1,\dots,F_n), \text{ over all } I\text{-stable cells } \sigma = \sum_i F_i.$$

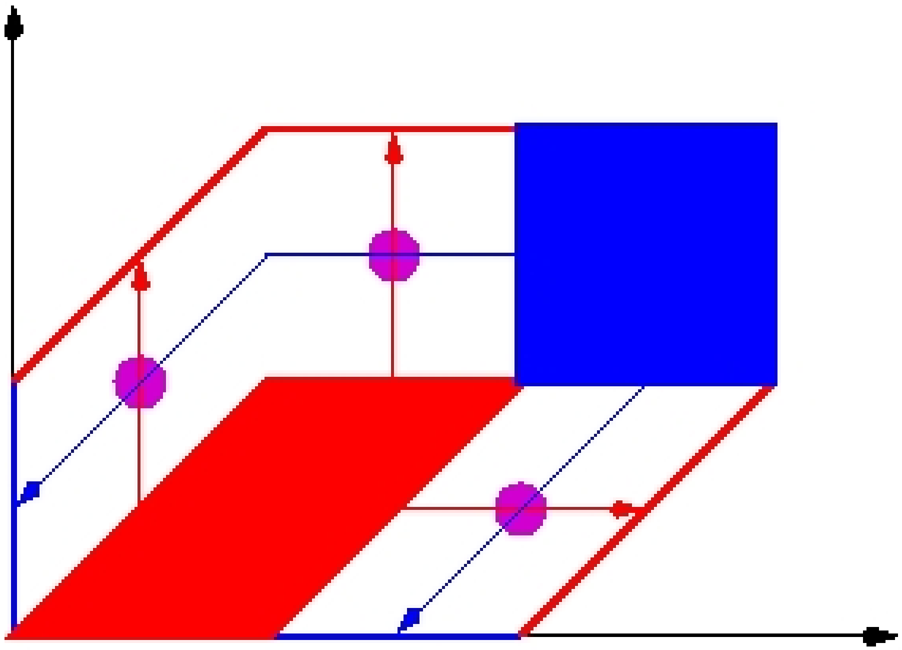
Equality holds for generic extremal coefficients.

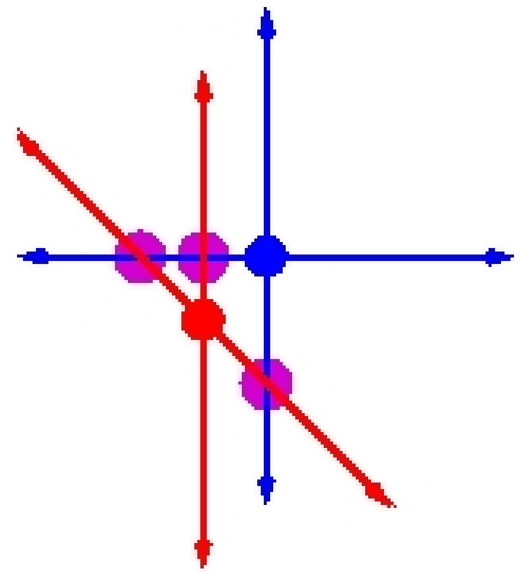


Cones in 2D

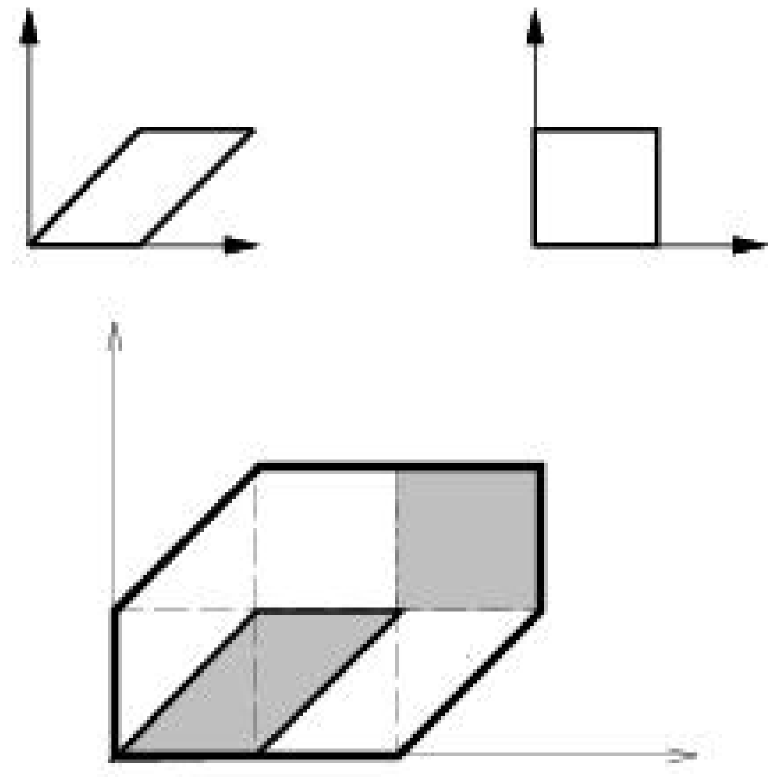
In the plane

- Given are 2 fans of cones whose origins are slightly perturbed.
- Red-blue crossings correspond to mixed cells.
- If $M = \#$mixed-cells, then algorithm in $O(n \log n + M)$ [Basch-Guibas].





Example: well-constrained system



1. Construct the Minkowski sum $Q = \sum_i Q_i$.
2. Place the Q_i's appropriately: no intersection of dimension ≥ 1.
3. Move edges to the boundary ∂Q: paths intersect at mixed cells.

Mixed subdivisions

Regular (induced) subdivisions

For $Q_i \subset \mathbb{R}^n$, $$(Q_i)_{i\in I} \to Q = \sum_{i\in I} Q_i \ : \ (q_i)_{i\in I} \mapsto \sum_{i\in I} q_i.$$

Consider (affine) lifting functions $l_i : \mathbb{R}^n \to \mathbb{R}$, which define

$$\widehat{Q}_i := \mathrm{CH}\{(p_i, l_i(p_i)) : p_i \in Q_i\} \subset \mathbb{R}^{n+1}.$$

Let $\widehat{Q}$ be the Minkowski sum $\sum_i \widehat{Q}_i$.

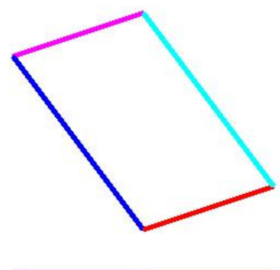
Lemma: If the l_i are sufficiently generic, then every face in the lower-hull of $\widehat{Q}$ is written uniquely as $\sum_i \widehat{F}_i$, for faces $\widehat{F}_i \subset \widehat{Q}_i$.

$\widehat{Q}$ projects onto Q, so its lower-hull faces induce a regular subdivision of Q, with faces (cells) $\sum_i F_i$, where $\widehat{F}_i$ is the lifted face $F_i \subset Q_i$.
Facets on the lower-hull project to maximal cells (dim$= n$).

Coherent subdivisions

A subdivision is coherent iff there is a continuous change of the unique expression of every cell as we move to its subcells and adjacent cells. Equivalently, the cells intersect properly as Minkowski sums.

All induced/regular subdivisions are coherent.



Eg: Not coherent subdivision of $Q_0 + Q_1,\ Q_i = [0,1]$.
Leftmost cell $=$ proj$(\widehat{0} + \widehat{Q}_1)$, so $\widehat{0} + \widehat{1} \mapsto 1 \in \mathbb{R}$.
Rightmost cell $=$ proj$(\widehat{1} + \widehat{Q}_1)$, so $\widehat{1} + \widehat{0} \mapsto 1$: different expression.

Tight coherent mixed subdivisions

In general: $\dim\left(\sum_i F_i\right) \leq \sum_i \dim F_i$.
Definition. A tight/exact/fine subdivision occurs when equality holds.
In particular, for a cell of maximum dimension, $n = \sum_i \dim F_i$.
Thus, the lower-hull of $\widehat{Q}$ corresponds bijectively to Q.

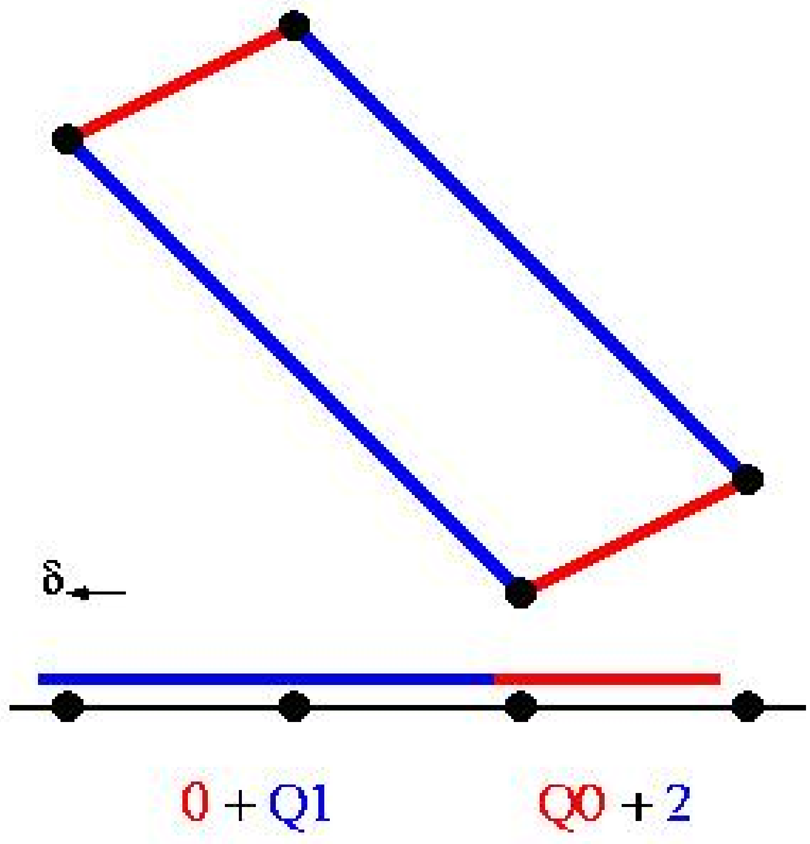
Eg: Not tight subdivision: 2 segments lifted in parallel:
$\dim(F_0 + F_1) = 1 < \dim F_0 + \dim F_1 = 1 + 1$.

Lemma. A regular subdivision by a generic lifting is tight and coherent. The latter captures continuity of the (unique) expressions of cells as Minkowski sums.

We call tight coherent mixed subdivisions simply mixed subdivisions.

Lifting in the Sylvester case

$$f_0 = c_{00} + c_{01}x, \; f_1 = c_{10} + c_{11}x + c_{12}x^2$$



Point $2 = 0 + 2$ from both maximal cells.

Example for the over-constrained problem

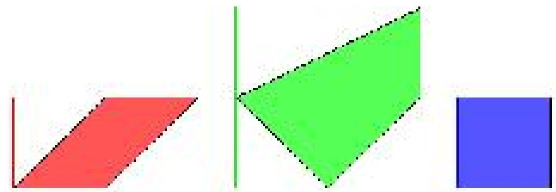


Figure 1: The given polytopes.

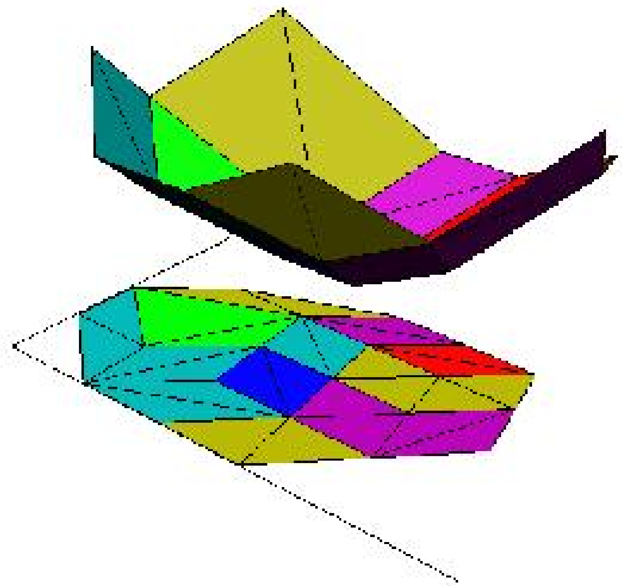


Figure 2: The lower hull of the lifted Minkowski Sum and its planar projection.

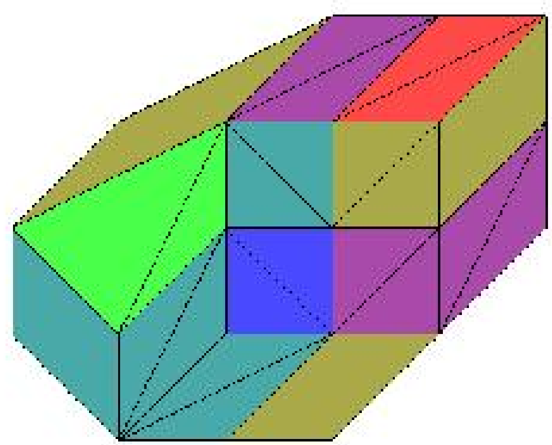


Figure 3: The mixed subdivision.

Cells in mixed subdivisions

Tightness of mixed subdivision implies for all maximal cells $\sigma = \sum_i F_i$:

$$\sum_i \dim F_i = n, \quad F_i \subset Q_i.$$

Corollary: when $n+1$ summands, $\exists\, i : F_i =$ vertex.

For linear/affine liftings, certain cells are copies of the original Q_i, and all other summands are vertices in the Q_j, for $j \neq i$.

Resultant case of $n+1$ polytopes: $Q = Q_0 + Q_1 + \cdots + Q_n$.
Every cell has at least one vertex summand.

Example of all possible summand dimensions (up to permutation):
$n = 2$, $Q_1 + Q_2$: 0,2 (Q_i) and 1,1 (mixed).
$n = 2$, $Q_0 + Q_1 + Q_2$: 0,0,2 (Q_i) and 0,1,1 (mixed).
$n = 3$, $Q_1 + \cdots + Q_3$: 0,0,3 (Q_i), 0,1,2 (unmixed), 1,1,1 (mixed).

Mixed cells

Defn. A maximal cell σ, in a mixed subdivision Δ, is mixed iff it has precisely n linear summands, i.e. n edge summands $F_i \; : \; \dim F_i = 1$.

- n polytopes: $Q = Q_1 + \cdots + Q_n$, mixed cells are sums of edges.

Thm: $\quad \text{MV}\ (Q_1, \ldots, Q_n) = \sum_\sigma \text{vol}(\sigma)$, over all mixed cells $\sigma \in \Delta$.

- $n+1$ polytopes: $Q = Q_0 + Q_1 + \cdots + Q_n$, i-mixed cells are sums of edges plus vertex $a_i \in Q_i$.

Thm:
$$\text{MV}(Q_0, \ldots, Q_{i-1}, Q_{i+1}, \ldots, Q_n) = \sum_\sigma \text{vol}(\sigma),$$

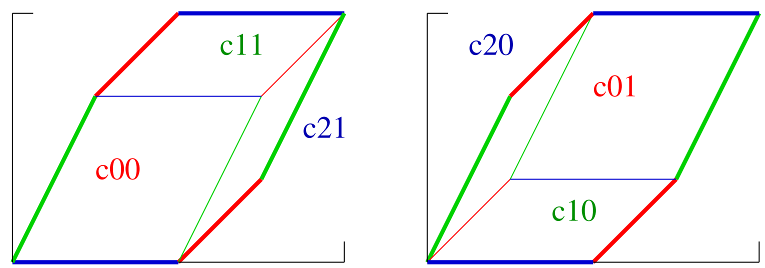
over all i-mixed cells $\sigma \in \Delta$.

Example: overconstrained system

The system

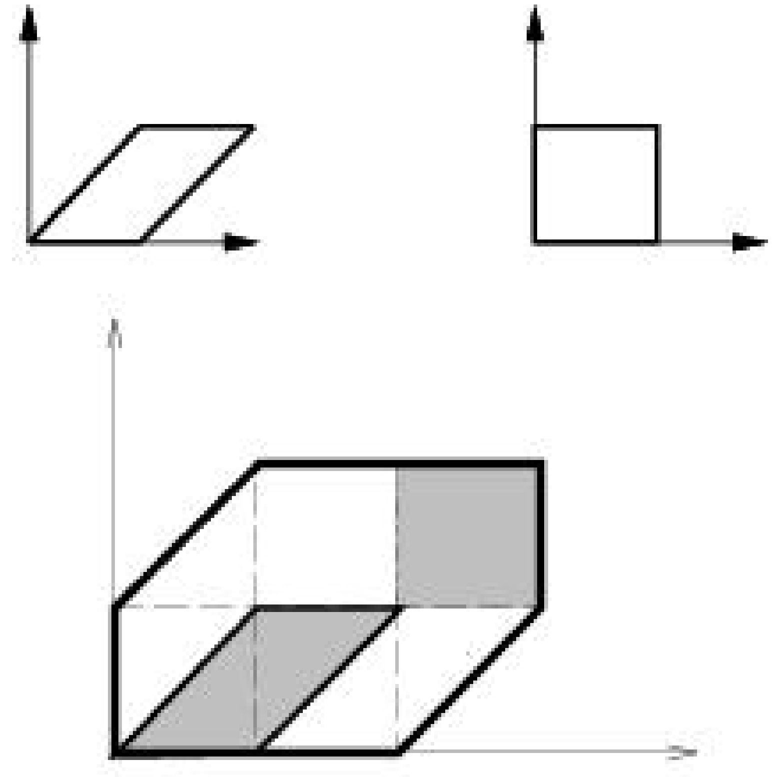
$$f_0 = c_{00} - c_{01}st, \; f_1 = c_{10} - c_{11}st^2, \; f_2 = c_{20} - c_{21}s^2,$$

has 2 possible mixed subdivisions, depending on the lifting:



Each subdivision contains exactly 3 maximal cells, all of which are mixed (vertex summands shown).

Example: well-constrained



Given $f_1 = c_{11} + c_{12}xy + c_{13}x^2y + c_{14}x$, $f_3 = c_{31} + c_{32}y + c_{33}xy + c_{34}x$,

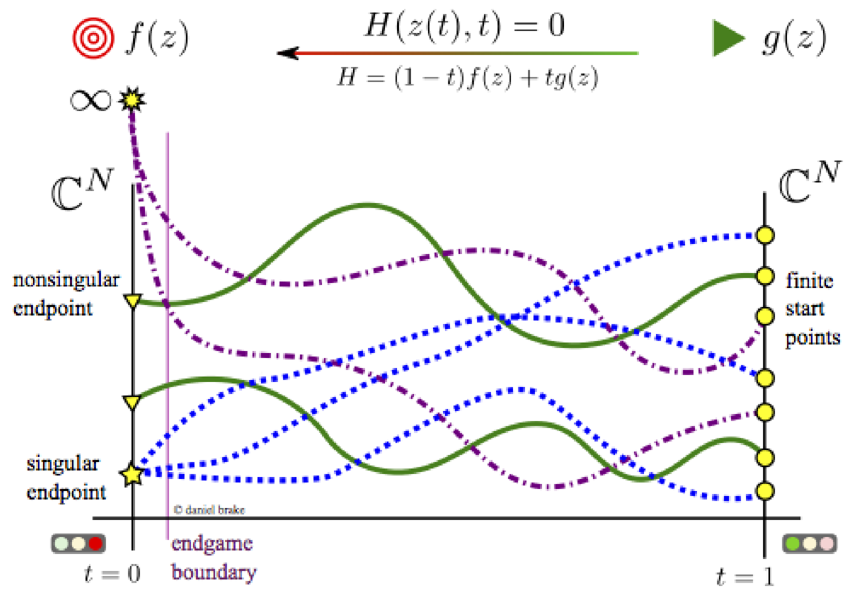
- construct their Newton polytopes in $\mathbb{R}^2$
- compute a mixed subdivision of the Minkowski Sum (3 mixed cells)
- compute the Mixed Volume using the formula MV$= \sum_\sigma V(\sigma)$, over all mixed cells σ of the mixed subdivision (here MV=3).

Homotopy continuation

Given system $f(z)$, pick simpler system $g(z)$ and define

$$F(z,t) = (1-t)f(z) + tg(z),\ t \in [0,1].$$

Starting at $t = 1$ ($F = g$ is easy), follow the roots while $t \to 0+$.



Sparse starting system given by mixed cells [Huber,Sturmfels'95]: correct cardinality, each equation is binomial.

Numerically follow the (real) roots: PHCpack [Verschelde et al.], Bertini [Hauenstein,Sommese,Wampler et al.] (figure)

Sparse resultant matrix

Sparse resultant definition

Given $n+1$ Laurent polynomials $f_0, \ldots, f_n \in K[x_1, \ldots, x_n, x_1^{-1}, \ldots, x_n^{-1}]$ with indeterminate coefficients $\vec{c}$, their projective, resp. toric / sparse, *resultant* is the unique (up to sign) irreducible polynomial $R(\vec{c}) \in \mathbb{Z}[\vec{c}]$ such that

$$R(\vec{c}) = 0 \Leftrightarrow \exists\, \xi = (\xi_1, \ldots, \xi_n) \in X \,:\, f_0(\xi) = \cdots = f_n(\xi) = 0$$

where the variety X equals:

- the projective space $\mathbb{P}^n$ over the algebraic closure $\overline{K}$,
- resp. the toric variety X, $(\overline{K}^*)^n \subset X \subset \mathbb{P}^N$.

[Gelfand-Kapranov-Zelevinsky, Cox-Little-O'Shea]

Resultant degree

The projective, resp. toric, resultant polynomial $R \in \mathbb{Z}[\vec{c}]$ is separately homogeneous in the coefficients of each f_i, with *degree* equal to $\prod_{j \neq i} \deg f_j$ (Bézout's number), resp. the n-fold mixed volume:

$$\mathrm{MV}_{-i} := \mathrm{MV}(f_0, \ldots, f_{i-1}, f_{i+1}, \ldots, f_n),$$

provided the supports of the f_i generate $\mathbb{Z}^n$.

Generalizations

The toric resultant reduces to:

- the determinant of the coefficient matrix of a *linear* system,
- the Sylvester or Bézout determinant of 2 *univariate* polynomials,
- the projective resultant for $n+1$ *dense* polynomials, where the toric variety equals $\mathbb{P}^n$ and $\mathrm{MV}_{-i} = \prod_{j \neq i} \deg f_j$.

Poisson Formula

Given $f_0, \dots, f_n \in K[x_1, \dots, x_n]$, with coefficients $c = (c_0, \dots, c_n)$ in K.

Poisson formula:

$$R \;=\; T \;\cdot \prod_{\alpha \in V(f_1,\dots,f_n)} f_0(\alpha)$$

where V is (generically) a 0-dimensional variety $\subset \mathbb{C}^n$, and
T is a polynomial in $c_1, \dots, c_n$ such that R is a polynomial in $\mathbb{Z}[c]$.

Corollary. By BKK bound:

$$\deg_{c_0} R = \mathrm{MV}(f_1, \dots, f_n).$$

Preview of Matrix construction

Consider Minkowski sum $Q = Q_0 + \cdots + Q_n \subset \mathbb{R}^n$,
and infinitesimal perturbation $\delta \in \mathbb{R}^n$ in generic direction.

For every point $p \in \mathcal{E} = (Q + \delta) \cap \mathbb{Z}^n$, $\exists$ unique cell $\sigma + \delta \ni p$,
s.t. $p - \delta \in \sigma = F_0 + \cdots + a_i + \cdots + F_n$ (max i).
Define RC(p) $:= (i, a_i)$: unique if σ is i-mixed, else pick max i.

Construct sparse resultant matrix M with rows/columns indexed by $\mathcal{E}$.
For $p, q \in \mathcal{E}$ the matrix row indexed by p contains

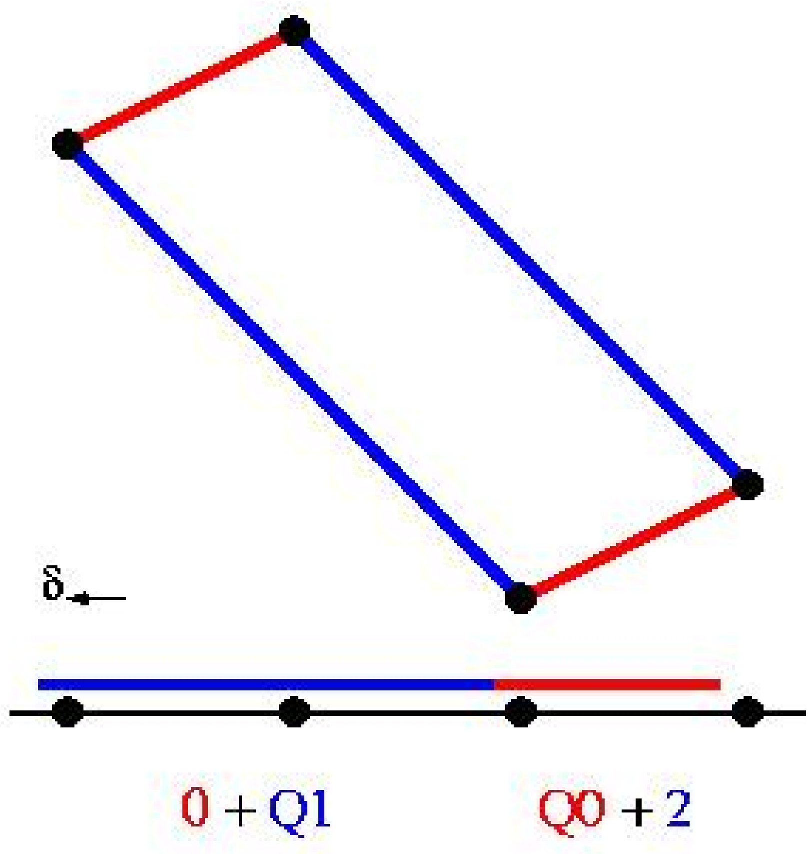
$$\text{polynomial } x^{p-a_i} f_i,$$

hence the matrix element (p, q) is

$$\text{the coefficient of } x^q \text{ in } x^{p-a_i} f_i.$$

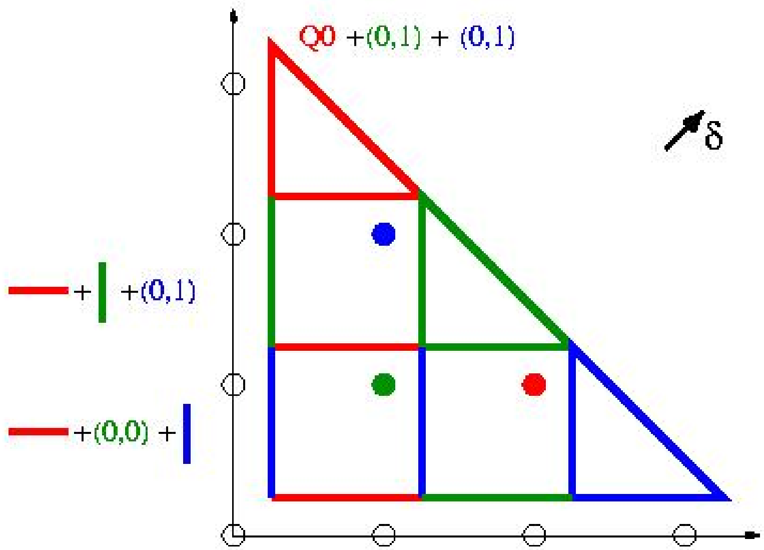
Lifting in the Sylvester case

$f_0 = c_{00} + c_{01}x$, $f_1 = c_{10} + c_{11}x + c_{12}x^2$



$\text{RC}(2) = (1;2)$ ie. $x^2 \mapsto x^{2-2}f_1$.

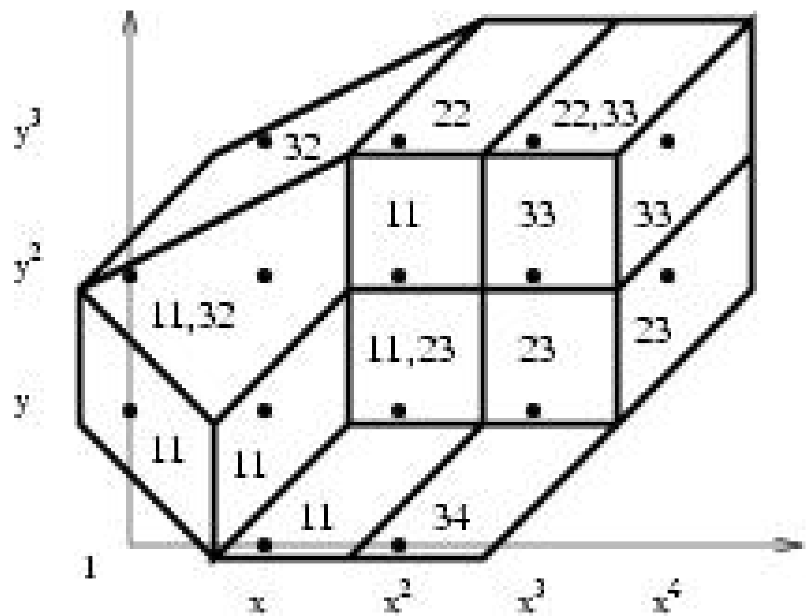
Mixed subdivision of a linear system



RC(1, 2) = [2, (0, 1)] ie. $x_1 x_2^2 \mapsto x^{(1,2)-(0,1)} f_2 = x^{(1,1)} f_2$
RC(1, 1) = [1, (0, 0)] ie. $x_1 x_2 \mapsto x^{(1,1)-(0,0)} f_1 = x^{(1,1)} f_1$
RC(2, 1) = [0, (1, 0)] ie. $x_1^2 x_2 \mapsto x^{(2,1)-(1,0)} f_0 = x^{(1,1)} f_0$

$$M = \begin{array}{c} \begin{array}{ccc} x_1^2 x_2 & x_1 x_2^2 & x_1 x_2 \end{array} \\ \begin{bmatrix} c_{01} & c_{02} & c_{03} \\ c_{11} & c_{12} & c_{13} \\ c_{21} & c_{22} & c_{23} \end{bmatrix} \end{array} \qquad \begin{array}{c} x_1 x_2 f_0 \\ x_1 x_2 f_1 \\ x_1 x_2 f_2 \end{array}$$

Example: mixed subdivision for the over-constrained problem



Eg: $x \mapsto (x, y)^{(1,0)-(0,0)} f_1$, $x^2 y \mapsto (x, y)^{(2,1)-(2,1)} f_2$.

Example: subdivision-based matrix

$$
\begin{aligned}
f_1 &= c_{11} + c_{12}xy + c_{13}x^2y + c_{14}x, \\
f_2 &= c_{21}y + c_{22}x^2y^2 + c_{23}x^2y + c_{24}x, \\
f_3 &= c_{31} + c_{32}y + c_{33}xy + c_{34}x.
\end{aligned}
$$

$$
\begin{array}{l|ccccccccccccccc}
 & 1,0 & 2,0 & 0,1 & 1,1 & 2,1 & 3,1 & 0,2 & 1,2 & 2,2 & 3,2 & 4,2 & 1,3 & 2,3 & 3,3 & 4 \\
\hline
1,0)x & c_{11} & c_{14} & 0 & 0 & c_{12} & c_{13} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
2,0)x & c_{31} & c_{34} & 0 & c_{32} & c_{33} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0,1)y & 0 & 0 & c_{11} & c_{14} & 0 & 0 & 0 & c_{12} & c_{13} & 0 & 0 & 0 & 0 & 0 & 0 \\
1,1)xy & 0 & 0 & 0 & c_{11} & c_{14} & 0 & 0 & 0 & c_{12} & c_{13} & 0 & 0 & 0 & 0 & 0 \\
2,1) & c_{24} & 0 & c_{21} & 0 & c_{23} & 0 & 0 & 0 & c_{22} & 0 & 0 & 0 & 0 & 0 & 0 \\
3,1)x & 0 & c_{24} & 0 & c_{21} & 0 & c_{23} & 0 & 0 & 0 & c_{22} & 0 & 0 & 0 & 0 & 0 \\
0,2)y & 0 & 0 & c_{31} & c_{34} & 0 & 0 & c_{32} & c_{33} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1,2)xy & 0 & 0 & 0 & c_{31} & c_{34} & 0 & 0 & c_{32} & c_{33} & 0 & 0 & 0 & 0 & 0 & 0 \\
2,2)x^2y^2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & c_{11} & c_{14} & 0 & 0 & 0 & c_{12} & c \\
3,2)x^2y & 0 & 0 & 0 & 0 & c_{31} & c_{34} & 0 & 0 & c_{32} & c_{33} & 0 & 0 & 0 & 0 & 0 \\
4,2)x^2y & 0 & 0 & 0 & 0 & 0 & c_{24} & 0 & 0 & c_{21} & 0 & c_{23} & 0 & 0 & 0 & c \\
1,3)xy^2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & c_{31} & c_{34} & 0 & 0 & c_{32} & c_{33} & 0 & 0 \\
2,3)y & 0 & 0 & 0 & c_{24} & 0 & 0 & c_{21} & 0 & c_{23} & 0 & 0 & 0 & c_{22} & 0 & 0 \\
3,3)x^2y^2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & c_{31} & c_{34} & 0 & 0 & c_{32} & c_{33} & 0 \\
4,3)x^3y^2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & c_{31} & c_{34} & 0 & 0 & c_{32} & c
\end{array}
$$

dim $M = 15$, greedy [Canny-Pedersen'93] 14, incremental [E-Canny] 12

MV $= 4, 3, 4 \Rightarrow \deg R_{tor} = 11$, $\deg(\text{classical } R) = 26$

Matrix construction

1. Pick (affine) liftings $\omega_i : \mathbb{Z}^n \to \mathbb{R} : \mathrm{supp}(f_i) \to \mathbb{Q}$.

2. Define (tight coherent polyhedral) mixed subdivision of the Minkowski sum $Q = Q_0 + \cdots + Q_n$ of the Newton polytopes.
Maximal cells are uniquely expressed as

$$\sigma = F_0 + \cdots + F_n, \qquad \text{with } \dim F_0 + \cdots + \dim F_n = n,$$

where F_i is a face of Q_i. σ is $i-$mixed $\iff \exists!\, i : \dim F_i = 0$.

3. For every point $p \in \mathcal{E} = (Q + \delta) \cap \mathbb{Z}^n$, $\exists$ unique $\sigma + \delta \ni p$.
Define function $\mathrm{RC}(p) = (i, F_i)$: unique if σ i-mixed, else pick max i.

4. Construct resultant matrix M with rows/columns indexed by $\mathcal{E}$:
for $p, q \in \mathcal{E}$, element (p, q) is the coefficient of x^q in $x^{p-a_i} f_i$:
$p - \delta \in \sigma = F_0 + \cdots + a_i + \cdots + F_n$ (max i), i.e. $\mathrm{RC}(p) = (i, a_i)$.

[Canny,E'93,00]

Correctness

Lemma. RC$(p) = (i, a_i) \Rightarrow$ support$(x^{p-a_i} f_i) \subset \mathcal{E}$.

Proof. $p \in \sigma + \delta \subset Q_0 + \cdots + Q_{i-1} + a_i + Q_{i+1} + \cdots + Q_n + \delta$ implies $p - a_i \in \sum_{i \neq j} Q_i + \delta$, hence $p - a_i + q \subset \mathcal{E}$ for all $q \in$ supp(f_i).

Corollary. The diagonal entry at the row indexed by p contains the f_i coefficient of x^{a_i}.

Proof. Consider the row indexed by p, s.t. RC$(p) = (i, a_i)$.
Then, the f_i coefficient of x^{a_i} is the coefficient of x^p in $x^{p-a_i} f_i$, hence it appears at the column indexed by p.

Newton polytope of the resultant

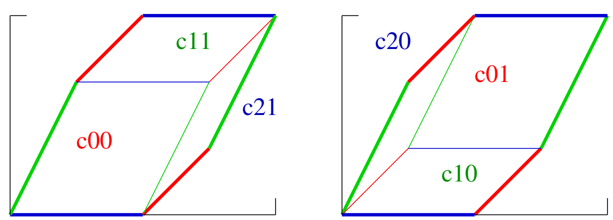
Given supports $A_0, \ldots, A_n$ s.t. $\dim(\sum_i A_i) = n$. If $k = \sum_i |A_i|$, sparse resultant R has Newton polytope in $\mathbb{R}^k$. Computed [E,Fisikopoulos et al'12].

Theorem [Sturmfels'94] For generic lifting $\omega \in \mathbb{R}^k$, the trailing monomial of R wrt ω, corresponding to vertex of supp(R) with inner normal ω, is

$$\prod_{i=0}^{n} \prod_{i-\text{mixed } \sigma} \text{coef}(f_i, a_i)^{\text{vol}(\sigma)},$$

where the i-mixed cells are $\sigma = F_0 + \cdots + a_i + \cdots + F_n : \dim a_i = 0$.

Example $f_0 = c_{00} - c_{01}st$, $f_1 = c_{10} - c_{11}st^2$, $f_2 = c_{20} - c_{21}s^2$



Extreme monomials $c_{00}^4 c_{11}^2 c_{21}$, $c_{01}^4 c_{10}^2 c_{20}$, $R = c_{00}^4 c_{11}^2 c_{21} - c_{01}^4 c_{10}^2 c_{20}$.

Rational formula

Proof using a single lifting [D'Andrea,Jernimo,Sombra'22].

Lemma. For lifting ω, pointset $\mathcal{E} \subset \mathbb{Z}^n$, matrix M satisfies

$$in_\omega(\det(M)) = \prod_{p \in \mathcal{E}} c_{i,a}, \quad \mathrm{RC}(p) = (i, a).$$

Theorem. Under some conditions on mixed subdivision $S(\omega)$,

$$R = \frac{\det(M)}{\det(M')}.$$

Idea of proof: As in the classical Macaulay formula, an induction using product formulas.

Example

Recursive lifting on n, using the subdivision algorithm [D'Andrea'01].

Bilinear: $f_i = a_i + b_i x_1 + c_i x_2 + d_i x_1 x_2$, $i = 0, 1, 2$.
Linear lift $(-\infty, \ldots), (0,1,1,2), (0,0,7,7)$, $\delta = (\frac{2}{3}, \frac{1}{2}) \Rightarrow \dim M = 16$ (numerator):

$$M = \begin{pmatrix}
a_1 & b_1 & 0 & c_1 & d_1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & a_0 & b_0 & 0 & c_0 & d_0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & a_1 & b_1 & 0 & c_1 & d_1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
a_2 & b_2 & 0 & c_2 & d_2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & a_2 & b_2 & 0 & c_2 & d_2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & a_0 & 0 & 0 & c_0 & d_0 & b_0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & a_2 & b_2 & 0 & c_2 & d_2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & a_2 & b_2 & 0 & c_2 & d_2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & a_1 & b_1 & 0 & c_1 & d_1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & a_1 & 0 & 0 & c_1 & d_1 & b_1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & a_2 & 0 & 0 & c_2 & d_2 & b_2 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & a_2 & 0 & 0 & c_2 & 0 & 0 & 0 & 0 & d_2 & b_2 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & a_2 & b_2 & 0 & 0 & 0 & 0 & c_2 & d_2 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & a_2 & b_2 & 0 & 0 & 0 & 0 & c_2 & d_2 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & a_2 & b_2 & 0 & 0 & 0 & 0 & c_2 & d_2 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & a_1 & b_1 & 0 & 0 & 0 & 0 & c_1 & d_1
\end{pmatrix}$$

Denominator

$$M' = \begin{pmatrix} a_1 & 0 & c_1 & d_1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & b_1 & 0 & c_1 & 0 & 0 & 0 & 0 & 0 & 0 \\ a_2 & 0 & c_2 & d_2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & b_2 & 0 & c_2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & a_2 & b_2 & c_2 & d_2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & a_2 & 0 & c_2 & d_2 & 0 & 0 & 0 \\ 0 & 0 & 0 & a_1 & 0 & c_1 & d_1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & c_2 & b_2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & a_2 & b_2 & 0 & c_2 & d_2 \\ 0 & 0 & 0 & 0 & 0 & 0 & a_2 & 0 & 0 & c_2 \end{pmatrix}$$

$\det(M) = \pm R \cdot \det(M')$: M' is a submatrix of M,

$|M'| = -c_2^3(-c_1a_2 + a_1c_2)b_2(c_1d_2 - d_1c_2)(-b_2c_1 + b_1c_2)$

Main step: lifting of some $b \in Q_0$ is very negative.

The mixed subdivision provides all info.

Single-lifting rational formula

$$M = \begin{array}{c} \begin{array}{ccccccccc} 00 & 10 & 01 & 11 & 21 & 12 & 20 & 02 & 22 \end{array} \\ \left[\begin{array}{ccccccccc}
c_{10} & c_{11} & c_{12} & c_{13} & 0 & 0 & 0 & 0 & 0 \\
c_{20} & c_{21} & c_{22} & c_{23} & 0 & 0 & 0 & 0 & 0 \\
c_{30} & c_{31} & c_{32} & c_{33} & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & c_{10} & c_{11} & c_{12} & 0 & 0 & c_{13} \\
0 & c_{20} & 0 & c_{22} & c_{23} & 0 & c_{21} & 0 & 0 \\
0 & 0 & c_{30} & c_{31} & 0 & c_{33} & 0 & c_{32} & 0 \\
0 & c_{30} & 0 & c_{32} & c_{33} & 0 & c_{31} & 0 & 0 \\
0 & 0 & c_{20} & c_{21} & 0 & c_{23} & 0 & c_{22} & 0 \\
0 & 0 & 0 & c_{20} & c_{21} & c_{22} & 0 & 0 & c_{23}
\end{array}\right] \end{array} \quad \begin{array}{c} \\ f_1 \\ f_2 \\ f_3 \\ x_1x_2f_1 \\ x_1f_2 \\ x_2f_3 \\ x_1f_3 \\ x_2f_2 \\ x_1x_2f_2 \end{array}$$

Same linear lifting $(-\infty, \ldots), (0,1,1,2), (0,0,7,7); \delta = (\frac{2}{3}, \frac{1}{2})$.

Denominator = submatrix of points in non-mixed cells:

$$M' = \begin{array}{c} \begin{array}{ccc} x_1 & x_2 & x_1x_2 \end{array} \\ \left[\begin{array}{ccc}
c_{21} & c_{22} & 0 \\
c_{31} & c_{32} & 0 \\
0 & 0 & c_{23}
\end{array}\right] \end{array} \quad \begin{array}{c} \\ f_2 \\ f_3 \\ x_1x_2f_2 \end{array} \qquad \Rightarrow R = \det M / \det M'.$$

Incremental algorithm

Limitation of subdivision-based algorithm

Bilinear system: $f_i = c_{i0} + c_{i1}x_1 + c_{i2}x_2 + c_{i3}x_1x_2, \; i = 1, 2, 3.$
The toric resultant has $\deg R = 3 \cdot \deg_{f_i} R = 6$.

$|\mathcal{E}| = 9 \Rightarrow$ the subdivision-based algorithm cannot yield an optimal matrix.
The greedy variant [Canny-Pedersen'93] *may* obtain an optimal matrix.
The incremental algorithm gets the following optimal matrix:

$$R = \det \begin{array}{cc} \begin{array}{cccccc} 1 & x_1 & x_2 & x_1x_2 & x_1^2 & x_1^2x_2 \end{array} & \\ \begin{bmatrix} c_{10} & c_{11} & c_{12} & c_{13} & 0 & 0 \\ c_{20} & c_{21} & c_{22} & c_{23} & 0 & 0 \\ c_{30} & c_{31} & c_{32} & c_{33} & 0 & 0 \\ 0 & c_{10} & 0 & c_{12} & c_{11} & c_{13} \\ 0 & c_{20} & 0 & c_{22} & c_{21} & c_{23} \\ 0 & c_{30} & 0 & c_{32} & c_{31} & c_{33} \end{bmatrix} & \begin{array}{c} f_1 \\ f_2 \\ f_3 \\ x_1f_1 \\ x_1f_2 \\ x_1f_3 \end{array} \end{array}$$

Sylvester-type matrices

Given: $f_0, \dots, f_m \in K[x^{\pm 1}]$, $x = (x_1, \dots, x_n), m \geq n$; $A_i = \mathrm{supp}(f_i)$. The supports $B_0, \dots, B_m \subset \mathbb{Z}^n$ define map M^T :

$$P(B_0) \times \cdots \times P(B_m) \to P\left(\bigcup_{i=0}^{m} A_i + B_i\right) : (g_0, \dots, g_m) \mapsto \sum_{i=0}^{m} f_i g_i,$$

s.t. $P(B) = \{g \in K[x^{\pm 1}] \colon \mathrm{supp}(g) \subset B\}$.

Example. $f_1 := c_0 + c_1 x + c_2 xy$, $B_1 := \{1, x\}$, $g_1 := s_0 + s_1 x$:

$$\begin{array}{c} \begin{array}{cccc} 1 & x & & \\ {[} & s_0 & s_1 & \cdots \;] \end{array} \end{array} \quad \begin{array}{c} \begin{array}{ccccc} 1 & x & xy & x^2 & x^2y \end{array} \\ \begin{bmatrix} c_0 & c_1 & c_2 & 0 & 0 \\ 0 & c_0 & 0 & c_1 & c_2 \\ & & \vdots & & \end{bmatrix} \end{array} \quad \begin{array}{c} f_1 \\ x f_1 \\ \vdots \end{array} \qquad =$$

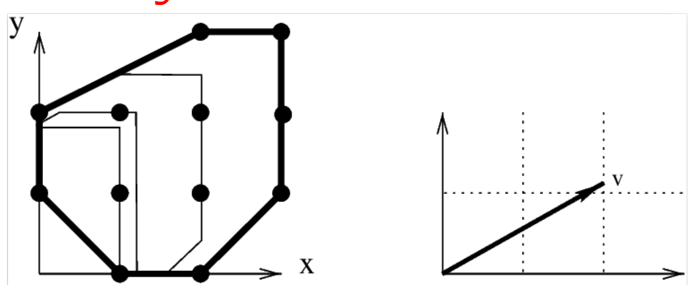
$$= \begin{array}{c} \begin{array}{ccccc} 1 & x & xy & x^2 & x^2y \end{array} \\ {[} \begin{array}{ccccc} s_0 a_0 & s_0 c_1 + s_1 c_0 & s_0 c_2 & s_1 c_1 & s_1 c_2 \end{array} {]} \end{array} + \cdots . \qquad \square$$

For coefficients c s.t. f_i have common root, $M^T(c)$ *shall be non surjective*.
Find B_i: $\sum_{i=0}^{m} |B_i| \geq \left| \bigcup_{i=0}^{m} A_i + B_i \right| = \mathrm{rank}(M)$ generically.

Incremental algorithm

Idea: Rows express $x^b f_i : b \in Q_{-i} \cap \mathbb{Z}^n$, where $Q_{-i} = Q_0 + \cdots + Q_{i-1} + Q_{i+1} + \cdots + Q_n$ so that column monomials $\subset \sum_i Q_i$ [E-Canny'95]

1. Sort $Q_{-i} \cap \mathbb{Z}^n$ on distance $\mathrm{dist}_v(\cdot)$ from ∂Q_{-i} along a vector $v \in \mathbb{Q}^n$.
2. Define rows of M by points $B_i = \{b : \mathrm{dist}_v(b) > \beta\}$, $\beta \in \mathbb{R}$. Columns indexed by $\cup_i \cup_{b \in B_i}$ supp$(x^b f_i)$.
3. Enlarge M by decreasing β until M (i) has at least as many rows as columns and (ii) is generically of full rank.



For multihomogeneous systems, deterministic v yields

- exact matrices if possible [Sturmfels-Zelevinsky'94],
- otherwise minimum matrices [Dickenstein-E'02].

Complexity in $\sim e^{2n}(\deg R)^2$ (by quasi-Toeplitz structure)

Related algorithm

Given f_i in polynomial ring S, consider graded map:

$$[\mathcal{M}_\lambda : \oplus_{i=0}^n S(-d_i) \to S]_\lambda \;:\; (g_0, \ldots, g_n) \to \sum_{i=0}^n f_i g_i.$$

Find λ so that $\mathcal{M}_\lambda$ satisfies:

- The corank of $\mathcal{M}_\lambda$ drops if there is a solution.
- If I is 0-dimensional, the corank is the number of solutions.

Macaulay's matrix is a minor of $\mathcal{M}_\lambda$

Incremental [Mourrain-Telen-Van Barel'19,Bender-Telen'21]

- Start at $\lambda = \max d_i$.
- Compute the cokernel of $\mathcal{M}_\lambda$.
- Use this cokernel to compute the one of $\mathcal{M}_{\lambda+1}$; $\lambda \leftarrow \lambda + 1$.
- Stopping criterion by elimination properties.

Matrices of Sylvester-type

Algorithms: subdivision-based, incremental, and greedy variants yield square matrix M, such that:

$$\det(M) \neq 0,$$
$$R \mid \det(M),$$
$$\deg_{f_0} \det(M) = \deg_{f_0} R,$$

where R is the sparse/toric resultant.

Similar properties as for the Macaulay matrix of the projective resultant: reduction to eigenproblem, u-resultant, multiplication map. . .

Rational form [D'Andrea'02,D'Andrea-Jeronimo-Sombra'22]: specify M' submatrix of M, generalizing Macaulay so that $R = \det(M)/\det(M')$.

Complexity [E'96] $O(e^n \deg R\, (\text{vtx}Q_i)^3)$, when n-fold Mixed Volumes > 0, and the Newton polytopes do not differ "too much" (bounded scaling).

Estimate $\mathrm{vol}\,(Q_1+\cdots+Q_n)\,/\,\mathrm{MV}\,(Q_1,\ldots,Q_n)$

The Aleksandrov-Fenchel inequality:
$\mathrm{MV}^2(Q_1,\ldots,Q_n) \ \geq \ \mathrm{MV}(Q_1,Q_1,Q_3,\ldots)\ \mathrm{MV}(Q_2,Q_2,Q_3,\ldots)$, implies:

$$\mathrm{MV}(Q_1,\ldots,Q_n) \geq n!\ \sqrt[n]{\prod_{i=1}^{n} \mathrm{vol}(Q_i)}.$$

If $\mathrm{vol}(Q_\mu)$ is minimal, the system's scaling factor is set to be the minimum real $s \geq 1$ s.t. $Q_i \subset sQ_\mu$, $\forall i$ (mod translations).
Thus, $s < \infty \Leftrightarrow$ all Q_i of the same dimension, $s = 1 \Leftrightarrow Q_1 = \cdots = Q_n$.

Corollary [E'94]. $$\frac{\mathrm{vol}\,(Q_1+\cdots+Q_n)}{\mathrm{MV}(Q_1,\ldots,Q_n)} < e^n s^n / \sqrt{2\pi n}.$$

Corollary [E'94]. For $\deg R = \sum_{i=0}^{n} \mathrm{MV}(Q_0,\ldots,Q_{i-1},Q_{i+1},\ldots,Q_n)$,

$$\mathrm{vol}\,(Q_0+\cdots+Q_n) = O\left(\frac{e^n s^n}{n^{3/2}}\ \deg R\right)$$

Mixed volume Approximation

- #P-complete: Hardness by reduction from permanent, or volume. m-Bézout: Optimal variable partition not APX [Malajovich,Meer'07]

- Poly-time deterministic, error in $n^{O(n)}$
  Poly-time randomized, simply exponential error [Gurvits'09]
  Permanent: Fully polytime randomized approx. scheme (FPRAS)

- FPRAS for H-polytope volume:
  [Kannan,Lovász,Simonovits'97;Lovász'99;Vempala et al'22].
  Software for d in 1000's, V-polytopes [E,Fisikopoulos,Chalkis]

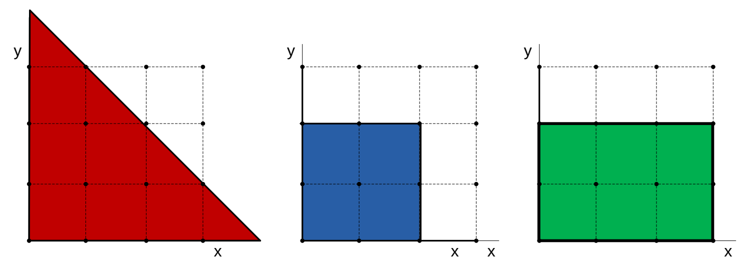
- Open: FPRAS for mixed volume of polytopes (or ellipsoids).
  Sample Minkowski sum? Easy to measure mixed cells but too many?

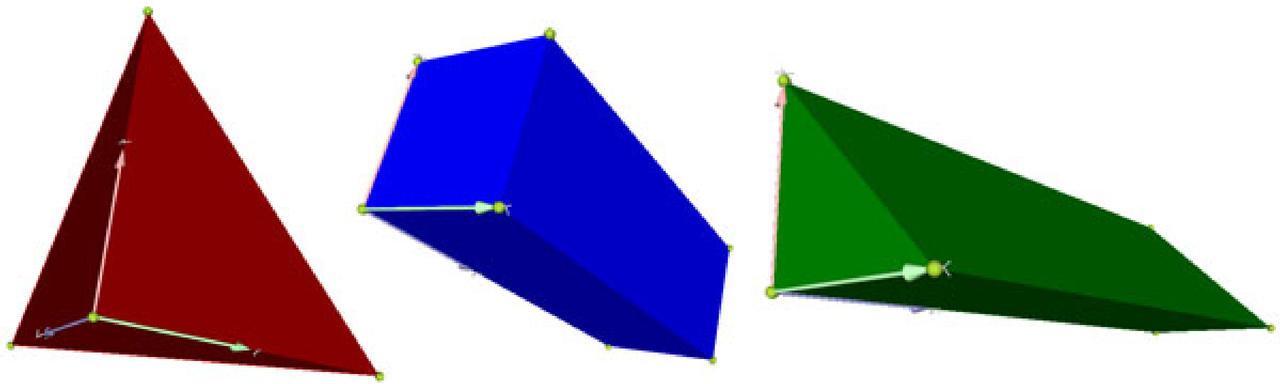
Multihomogeneous systems

Unmixed (multi)homogeneous systems

Partition variables into r subsets: every polynomial is homogeneous in each subset. The i-th subset has $l_i + 1$ homogeneous variables, of total degree d_i: type $(l_1, \dots, l_r; d_1, \dots, d_r)$.

Type $(2, 1; 2, 1)$, $(x_0 : x_1 : x_2, y_0 : y_1) \in \mathbb{P}^2 \times \mathbb{P}^1$: $c_0 + c_1x_1 + c_2x_2 + c_3x_1x_2 + c_4x_1^2 + c_5x_2^2 + c_6y_1 + c_7x_1y_1 + c_8x_2y_1 + c_9x_1x_2y_1 + c_{10}x_1^2y_1 + c_{11}x_2^2y_1$.

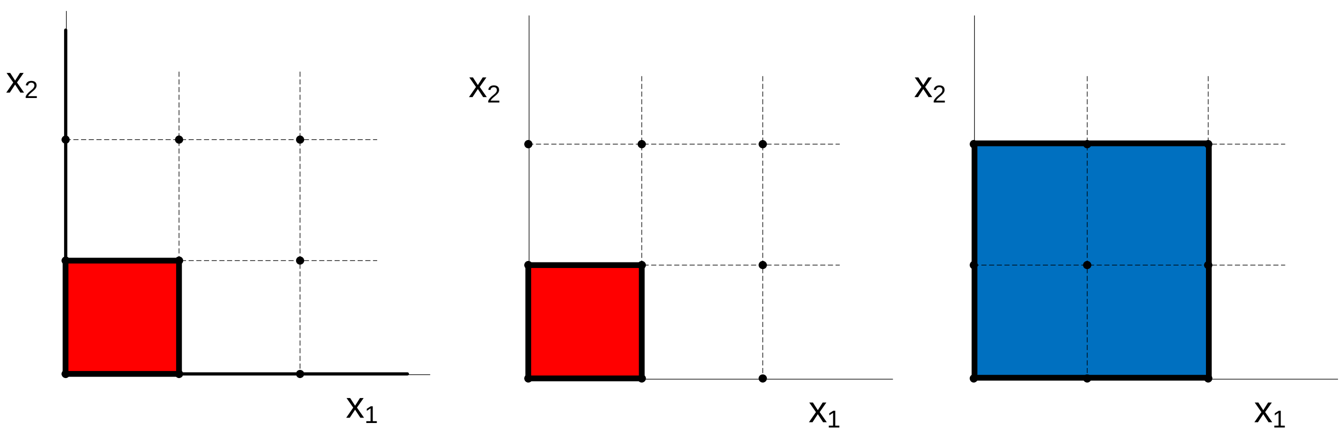




Scaled (multi)homogeneous systems

Scaled case: $\boxed{\deg f_i = s_i d \in \mathbb{N}^r}$

- Cardinalities $\ell = (\ell_1, \dots, \ell_r) \in \mathbb{N}^r$
- Base degrees $d = (d_1, \dots, d_r) \in \mathbb{N}^r$
- Scalars $s = (s_0, \dots, s_n) \in \mathbb{N}^{n+1}$



Running example: $\ell = (1,1)$, $d = (1,1)$, $s = (1,1,2)$:

$$f_0 = a_0 + a_1 x_1 + a_2 x_2 + a_3 x_1 x_2,$$
$$f_1 = b_0 + b_1 x_1 + b_2 x_2 + b_3 x_1 x_2,$$
$$f_2 = c_0 + c_1 x_1 + c_2 x_2 + c_3 x_1 x_2 + c_4 {x_1}^2 + c_5 {x_1}^2 x_2 + c_6 {x_2}^2 + \\ + c_7 x_1 x_2^2 + c_8 x_1^2 x_2^2$$

(Multihomogeneous) m-Bézout bound

Consider a system of n equations in n affine variables, partitioned into r subsets so that the j-th subset includes n_j variables: $n = n_1 + \cdots + n_r$. Let d_{ij} be the degree of the i-th equation in the j-th variable subset.

Theorem. The coefficient of $y_1^{n_1} \cdots y_r^{n_r}$ in

$$\prod_{i=1}^{n} (d_{i1} y_1 + \cdots + d_{ir} y_r)$$

bounds the number of isolated complex roots in

$$\mathbb{P}^{n_1} \times \mathbb{P}^{n_2} \times \cdots \times \mathbb{P}^{n_r}.$$

For generic coefficients this bound is tight.

For dense systems, it equals the mixed volume.

Multihomogeneous resultant

Consider systems of $n+1$ polynomials of same type $(l_1, \ldots, l_r; d_1, \ldots, d_r)$, $n = l_1 + \cdots + l_r$, possibly with scaling $(s_0, \ldots, s_n)$. Let projective variety $X := \mathbb{P}^{l_1} \times \ldots \times \mathbb{P}^{l_r}$ over a 0-characteristic algebraically-closed field.

Defn. The system's multihomogeneous (multigraded) resultant $R \in \mathbb{Z}[c]$ is irreducible, uniquely defined up to sign, and vanishes iff all polynomials have a common root in X. Its degree in coeff(f_i) is:

$$\deg_{f_i} R = \binom{n}{l_1, \ldots, l_r} d_1^{l_1} \cdots d_r^{l_r}\, s_0 \cdots s_{i-1} s_{i+1} \cdots s_n,$$

with $s_i = 1$ for unmixed systems.

Bilinear system: Sylvester-type matrix

$$\begin{aligned} f_0 &= a_0 + a_1x_1 + a_2x_2 + a_3x_1x_2, \\ f_1 &= b_0 + b_1x_1 + b_2x_2 + b_3x_1x_2, \\ f_2 &= c_0 + c_1x_1 + c_2x_2 + c_3x_1x_2, \end{aligned}$$

of type $(1,1;1,1)$, deg $R = 3 \cdot \deg_{f_i} R = 3\binom{2}{1,1} = 6$.

A determinantal pure Sylvester formula:

$$R = \det \begin{array}{c} \begin{array}{cccccc} 1 & x_1 & x_2 & x_1x_2 & x_1^2 & x_1^2x_2 \end{array} \\ \begin{bmatrix} a_0 & a_1 & a_2 & a_3 & 0 & 0 \\ b_0 & b_1 & b_2 & b_3 & 0 & 0 \\ c_0 & c_1 & c_2 & c_3 & 0 & 0 \\ 0 & a_0 & 0 & a_2 & a_1 & a_3 \\ 0 & b_0 & 0 & b_2 & b_1 & b_3 \\ 0 & c_0 & 0 & c_2 & c_1 & c_3 \end{bmatrix} \end{array} \quad \begin{array}{c} f_0 \\ f_1 \\ f_2 \\ x_1f_0 \\ x_1f_1 \\ x_1f_2 \end{array}$$

Bilinear system: Bézout-type matrix

The Bezoutian polynomial

$$B = \det \begin{bmatrix} f_0(x_1,x_2) & f_0(y_1,x_2) & f_0(y_1,y_2) \\ f_1(x_1,x_2) & f_1(y_1,x_2) & f_1(y_1,y_2) \\ f_2(x_1,x_2) & f_2(y_1,x_2) & f_2(y_1,y_2) \end{bmatrix} \;/\; (x_1-y_1)(x_2-y_2),$$

supported by $\{1,x_2\},\{1,y_1\}$, yields a determinantal pure Bézout formula:

$$R = \det \begin{bmatrix} [123] & [023] \\ -[103] & [012] \end{bmatrix} \quad : \qquad [ijk] = \begin{vmatrix} a_i & a_j & a_k \\ b_i & b_j & b_k \\ c_i & c_j & c_k \end{vmatrix}$$

Bilinear system: hybrid matrix

$$(l; d) = (1,1;1,1),\ \deg R = 6,\ \delta = (0,0).$$

$m = (1,1)$ defines $K_1 = H^0(0,0)^{\binom{3}{1}} \oplus H^2(-2,-2) \to K_0 = H^0(1,1)$,

which has a hybrid (transposed) matrix

$$\begin{array}{c} \begin{array}{cccc} 1 & x_1 & x_2 & x_1x_2 \end{array} \\ \begin{bmatrix} a_0 & a_1 & a_2 & a_3 \\ b_0 & b_1 & b_2 & b_3 \\ c_0 & c_1 & c_2 & c_3 \\ [012] & [013] & [032] & -[123] \end{bmatrix} \end{array}.$$

Determinantal formula

Theorem [Weyman,Zelevinsky'94, Sturmfels,Zelevinsky'94] A (hybrid) determinantal formula exists, for unmixed systems (scaling $s = 1$), iff all defects $\delta_k := l_k - \lceil l_k/d_k \rceil \leq 2$, $k = 1, \ldots, r$.

Theorem [Dickenstein-E] A determinantal formula of pure Sylvester type exists iff all defects vanish iff a determinantal formula of pure Bézout type exists.

Characterize determinantal formulae: $\forall$ permutation $\pi : [1, r] \to [1, r]$

$$m_k^\pi = \left(1 - \delta_k + \sum_{\pi(j) \geq \pi(k)} l_j \right) d_k - l_k \in \mathbb{Z}, \quad k = 1, \ldots, r.$$

- Includes all known determinantal Sylv.-matrices (Dixon, $n = 2$)
- m and its perturbations used in Incremental algo [E-Canny'95].

Generalize pure Sylvester-type complexes

Definition. For some $j : 0 \leq j \leq n$, the generalized complex is
$\cdots \to K_1(m) = H^j(X, m-d) \to K_0(m) = H^j(X, m) \to K_{-1}(m) = 0$

$$
\begin{array}{cc}
\begin{array}{cccccc} 1 & x_1 & x_2 & x_1x_2 & \dots & \end{array} & \\
\begin{bmatrix}
a_0 & a_1 & a_2 & a_3 & 0 & 0 \\
b_0 & b_1 & b_2 & b_3 & 0 & 0 \\
c_0 & c_1 & c_2 & c_3 & 0 & 0 \\
a_1 & 0 & a_3 & 0 & a_0 & a_2 \\
b_1 & 0 & b_3 & 0 & b_0 & b_2 \\
c_1 & 0 & c_3 & 0 & c_0 & c_2
\end{bmatrix}
&
\begin{array}{c} f_0 \\ f_1 \\ f_2 \\ x_1^{-1} f_0 \\ x_1^{-1} f_1 \\ x_1^{-1} f_2 \end{array}
\end{array}
$$

Theorem. If $\exists m \in \mathbb{Z}^r$ defining generalized pure-Sylvester complex
$\Rightarrow \exists\ m' \in \mathbb{Z}^r$ defining (standard) pure-Sylvester complex.

Hence we can focus on (standard) pure Sylvester-type complexes:
$\ldots \to K_1(m) = H^0(X, m-d) \to K_0(m) = H^0(X, m) \to K_{-1}(m) = 0$

Example: Hybrid determinantal formula

$$l = (3,2), d = (2,3)$$

then $\deg R = 6 \cdot \deg_{f_i} R = 6\binom{5}{3,2}2^3 3^2 = 4320.$

Found 30 determinantal m, $\min\{\dim M\} = 1320$, for $m = (6,3),(2,12)$.

For $m = (6,3)$ we get 3 pure Sylvester, 3 pure Bézout maps.

$$M: \quad \begin{array}{cc} & \begin{array}{ccc} 840 & 150 & 330 \end{array} \\ \begin{array}{c} 210 \\ 220 \\ 910 \end{array} & \left[\begin{array}{ccc} \phi_{00} & 0 & 0 \\ \phi_{20} & \phi_{22} & 0 \\ \phi_{50} & \phi_{52} & \phi_{55} \end{array}\right] \end{array} = \left[\begin{array}{ccc} S_{00} & 0 & 0 \\ B_{20}^{x_2} & \phi_{22} & 0 \\ B_{50} & B_{52}^{x_1} & S_{55}^T \end{array}\right]$$

Determinantal formula for scaled systems

Theorem A determinantal formula exists in the scaled case ($s \neq 1$):

- for scaled homogeneous systems ($r = 1$ blocks), iff $s_2 + \cdots + s_n - n < s_0 + s_1$ [D'Andrea-Dickenstein'01,Cox-Matera'08]
- for multi-homogeneous systems a determinantal pure-Sylvester formula exists iff $n = 1$ or $\ell = (1,1)$ [E-Mantzaflaris]

No pure-Bézout formula exists.

Characterize all formulae:

$$n = 1 \Rightarrow m = d \sum_0^n s_i - 1, \text{ or } m = -1 \quad \text{(both classic Sylvester).}$$

$$\ell = (1,1) \Rightarrow m = \left(-1,\ d_2 \sum_{i=0}^{2} s_i - 1 \right), \text{ or } m = \left(d_1 \sum_{i=0}^{2} s_i - 1, -1 \right).$$

Scaled determinantal Sylvester

$$\ell = (1,1),\quad d = (1,1),\quad s = (1,1,2)$$

$$f_0 = a_0 + a_1x_1 + a_2x_2 + a_3x_1x_2$$
$$f_1 = b_0 + b_1x_1 + b_2x_2 + b_3x_1x_2$$
$$f_2 = c_0 + c_1x_1 + c_2x_2 + c_3x_1x_2 + c_4{x_1}^2 + c_5{x_1}^2x_2 + \\ + c_6x_2^2 + c_7x_1x_2^2 + c_8x_1^2x_2^2$$

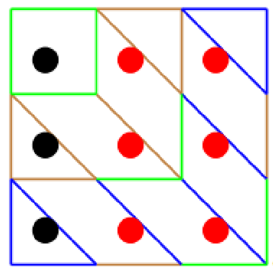
$\deg R = 4 + 4 + 2 = 10 \;\Rightarrow$ optimal matrix:

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

Lifting vs monomial order

Open: Relate liftings to monomial orders.

Open: Find a lifting yielding minimal matrices? (greedy or incremental)



It makes sense to think that this lifting is related to DRL:

$$x^A < x^B \iff \langle A, \omega \rangle < \langle B, \omega \rangle$$

Conjecture [Checa-E'23] For multihomogeneous systems, there is a (DRL) lifting providing "minimal" matrices.

Open: Is the rational form simplified ?

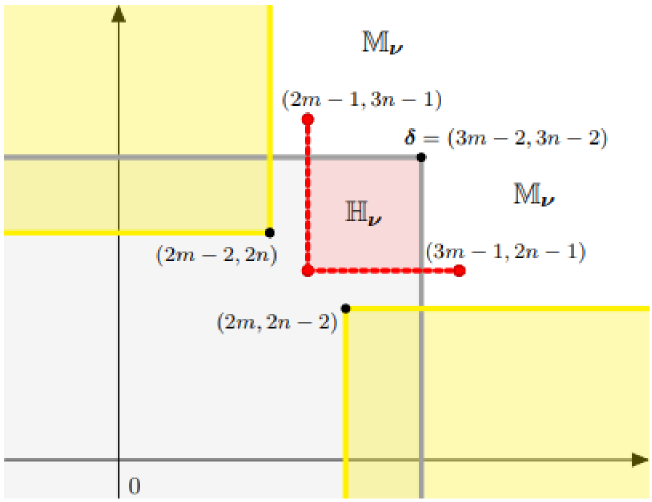
Towards Multigraded regularity

Complex relation between Gröbner base and reg(I): Heavy dependence on relative order of variables of different degrees in DRL.

Multihomogeneous "Macaulay" bound for generic forms of multidegrees $\mathbf{d}_i \in \mathbb{Z}^r$ with n_i variables per group:

$$\sum_{i=0}^{n} \mathbf{d}_i - (n_1 - 1, \ldots, n_r - 1)$$

is not tight. Example: bound $= (3m-1, 3n-1) \to (2,2)$ but Groebner computations end at $(1,2)$.



In sparse case, even a generic change of coordinates is not well defined

System solving by linear algebra

Polynomial System Solving I

Given $f_1, \ldots, f_n \in K[x_1^{\pm 1}, \ldots, x_n^{\pm 1}]$ defining a 0-dim radical ideal.
Add polynomial $f_0 = u + r_1 x_1 + \cdots + r_n x_n$, random r_i, symbolic u.

Build resultant matrix $M(u)$ of $f_0, f_1, \ldots, f_n$. At root α, $u = -\sum_i r_i \alpha_i$,

$$\begin{bmatrix} & \\ M_{11} & M_{12} \\ & \\ M_{21} & M_{22}(u) \\ & \end{bmatrix} \begin{bmatrix} \vdots \\ \alpha^p \\ \vdots \\ \alpha^q \\ \vdots \end{bmatrix} = \begin{bmatrix} \vdots \\ \alpha^a f_i(\alpha) \\ \vdots \\ \alpha^b f_0(u, \alpha) \\ \vdots \end{bmatrix} = \begin{bmatrix} \vdots \\ 0 \\ \vdots \\ 0 \\ \vdots \end{bmatrix}.$$

Maximal M_{11} s.t. $\det M_{11} \neq 0$, let $M'(u) = M_{22}(u) - M_{21} M_{11}^{-1} M_{12}$,

$$(M' + uI)v'_\alpha = 0, \qquad \dim M' = \mathrm{MV}(f_1, \ldots, f_n).$$

- Ratios of the entries of eigenvectors v'_α yield α, if the q span $\mathbb{Z}^n$.

- Otherwise, use some entries of $v_\alpha = -M_{11}^{-1} M_{12} v'_\alpha$, where $(v_\alpha, v'_\alpha)^T$ is the respective eigenvector of M.

Polynomial System Solving I (factoring)

For $f_0 = u_0 + u_1 x_1 + \cdots + u_n x_n$, with indeterminates u_i, the Poisson formula implies

$$R(u_0, \ldots, u_n) = C \prod_{\alpha \in V(f_1, \ldots, f_n)} (u_0 + \alpha_1 u_1 + \cdots + \alpha_n u_n)^{m_\alpha},$$

over all roots α with multiplicity m_α, where C depends on the coefficients of $f_1, \ldots, f_n$.

Setting $u_i = r_i$, $i = 1, \ldots, n$, for random r_i, we have

$$R(u_0) = C \prod_\alpha (u_0 + r_1 \alpha_1 + \cdots + r_n \alpha_n)^{m_\alpha}.$$

Solving $R(u_0)$ for u_0 yields $u_0 = -\sum_i r_i \alpha_i$ for all α.

$R(u_0)$ is used in the method of Rational Univariate Representation (primitive element) for isolating all (real) α.

Polynomial System Solving II

"Hide" a variable in the coefficient field: $f_0, f_1, \ldots, f_n \in (K[x_0])[x_1, x_1^{-1}, \ldots, x_n, x_n^{-1}]$

Hypothesis: x_0-coordinates of roots distinct, $|M(x_0)| \not\equiv 0$.

$$\det M(x_0) = \begin{vmatrix} M_{11} & M_{12}(x_0) \\ M_{21} & M_{22}(x_0) \end{vmatrix} = \begin{vmatrix} M_{11} & M_{12}(x_0) \\ 0 & M'(x_0) \end{vmatrix},$$

$|M'(x_0)| = |A_d x_0^d + \cdots + A_1 x_0 + A_0| = \det A_d \det(x_0^d + \cdots + A_d^{-1} A_1 x_0 + A_d^{-1} A_0)$.

- If $\det A_d \neq 0$, define companion matrix C:

$$C = \begin{bmatrix} 0 & I & & 0 \\ \vdots & & \ddots & \\ 0 & 0 & & I \\ -A_d^{-1}A_0 & -A_d^{-1}A_1 & \cdots & -A_d^{-1}A_{d-1} \end{bmatrix}$$

The eigenvalues of C are the x_0-coordinates of the solutions and its eigenvectors contain the values of the monomials indexing M' at the roots.

- Rank balancing improves the conditioning (of A_d) by $x \mapsto (t_1 y + t_2)/(t_3 y + t_4)$, $t_i \in_R \mathbb{Z}$.
- If A_d remains ill-conditioned, solve the generalized eigenproblem

$$\begin{bmatrix} I & & & \\ & \ddots & & \\ & & I & \\ & & & A_d \end{bmatrix} x + \begin{bmatrix} 0 & -I & & \\ & & \ddots & \\ & & & -I \\ A_0 & A_1 & \cdots & A_{d-1} \end{bmatrix}.$$

Change of variable

Consider the Sylvester matrix polynomial:

$$M(y) = M_d y^d + \cdots + M_1 y + M_0.$$

Rank balancing improves the conditioning of M_d by change of variable

$$y = (t_1 z + t_2)/(t_3 z + t_4), \text{ for random } t_i \in_R \mathbb{Z},$$

provided $t_3 z + t_4 \neq 0$. In practice, compute $M(z) = M'_d z^d + \cdots$ hoping $\kappa(M'_d) < \kappa(M_d)$. Repeat a few times; take the best vector $(t_1, \ldots, t_4)$.

Example. For $d = 1$, assuming $t_3 z + t_4 \neq 0$ (check *a posteriori*):

$$(M_1 y + M_0)v = 0 \iff (z(t_1 M_1 + t_3 M_0) + (t_2 M_1 + t_4 M_0))v = 0.$$

Matrix-based methods for system solving

Theorem. Let $\{z_k\}_k \subset \mathbb{C}^n$ be the isolated zeros of $f_1, \ldots, f_n \in \mathbb{Q}[x_1, \ldots, x_n]$. There exists matrix M_a expressing multiplication by a mod $\langle f_i \rangle$ s.t.

- the eigenvalues of M_a are $a(z_k)$, and
- the eigenvectors of M_a^t are, up to a scalar, $\mathbf{1}_{z_k} : p(x) \mapsto p(z_k)$.

Construct multiplication matrices by means of

- resultant matrices, e.g. Sylvester, Bézout, sparse, or
- normal forms, boundary bases (generalize Gröbner bases).

Stable with respect to input perturbations.

Handles multiplicities and zero sets at infinity.

Extends to over-constrained systems

Complexity: single exponential in n.

Open: Complete implementation, possible connections (LAPACK, SparseLU, GMP) [Emiris'12:General solver]

Multiplication maps

Let ideal $I := \langle f_1, \ldots, f_m \rangle \subset K[x_1, \ldots, x_n] = K[x]$. The quotient ring

$$K[x]/I = \{b \bmod I : b \in K[x]\}$$

is a K-vector-space if I is 0-dimensional.

Polynomial multiplication in $K[x]/I$ by $f \in K[x]$, is linear map:

$$M_f \ : \ K[x]/I \to K[x]/I \ : \ b \mapsto fb \bmod I.$$

For well-constrainted system $f_1, \ldots, f_n$, monomial basis = lattice points in mixed cells of mixed subdivision. Basis size $= MV(f_1, \ldots, f_n)$.

Map matrix: Set overconstrained system with $f_0(u)$; build resultant matrix; Schur complement of dimension $MV(f_1, \ldots, f_n)$ is M_{f_0} [E'94]. Values $f_0(r)$, $r \in V(I)$ are eigenvalues of M_{f_0}.

Matrix structure

Structured matrices

Defined by $O(n)$ elements, matrix-vector product is quasi-linear.

Two important examples:

- Vandermonde: matrix-vector multiply and solving in $O_A(n \log^2 n)$.
- Toeplitz iff $M(a+i, b+i) = M(a, b)$, $i > 0$, when defined: constant diagonals. Lower triangular * vector is polynomial multiplication $= O_A^*(n)$; same for vector * upper triangular.

∘ More: Hankel (constant anti-diagonals), Cauchy, Hilbert.

Theorem [Wiedemann (Lanszos)]. Determinant reduces to $O^*(n)$ matrix-vector products.

Toeplitz example

$$P_1(x) = x^4 - 2x^3 + 3x + 5,\ P_2(x) = 5x^3 + 2x - 11.$$

Upper triangular Toeplitz T has rows corresponding to P_2 multiples:

$$\begin{array}{cc} \begin{bmatrix} 5 & 0 & 2 & -11 & & & & \mathbf{0} \\ & 5 & 0 & 2 & -11 & & & \\ & & 5 & 0 & 2 & -11 & & \\ & & & 5 & 0 & 2 & -11 & \\ \mathbf{0} & & & & 5 & 0 & 2 & -11 \end{bmatrix} & \begin{array}{c} x^4 P_2 \\ x^3 P_2 \\ x^2 P_2 \\ x P_2 \\ P_2 \end{array} \end{array}$$

Row vector $v = [1, -2, 0, 3, 5]$ expresses P_1, then Vector-matrix multiplication vT is equivalent to polynomial multiplication

$$(P_1 P_2)(x) = 5x^7 - 10x^6 + 2x^5 + 47x^3 + 6x^2 - 23x - 55.$$

If multiplying polynomials of degree d costs $F(d)$, then multiplying $d \times d$ Toeplitz matrix by vector $= O(F(d))$.

Sparse polynomial multiplication

Input: Polynomials f, g: coefficients c_f, c_g, supports $A, B \subset [0, d]^n$.
Take set $S \supset A + B$, $s = |S|$.
Output: Coefficient vector c_{fg} wrt S.
Theorem. Time $= O^*(sn + n\sqrt{d})$, space $= O(sn)$.

Lemma. M is the Newton matrix of $f_0, \ldots, f_n$, v corresponds to $g_0, \ldots, g_n$.
Computing $v^T M$ is equivalent to computing $\sum_{i=0}^{n} f_i g_i$.

Theorem. M is $a \times c$ and the polynomials have degree $\leq d$ per variable.
Then, $v^T M$ computed in time / space complexity $O^*(cn + n\sqrt{d})$.
The same for Mv by Tellegen's theorem.

Quasi-Toeplitz structure

Theorem [E-Pan'02] Let M be $a \times c$, $d = O(c^2)$. Computing the rank numerically wrt $\epsilon > 0$ (or by an exact-arithmetic Las Vegas algorithm) takes time $= O^*(c^2 n)$, space $= O^*(cn)$.

Corollary. Having enumerated the column monomials, constructing M incrementally (and obtaining a $c \times c$ sparse resultant matrix) takes time $= O^*(c^2 nt)$, space $= O^*(cn)$, where $t =$ #rank-tests.
Experiments indicate $t = O(\log(cn))$, by binary search.

Block-Toeplitz example: Sylvester matrix

$$\begin{aligned} f_0 &= a_{d_0} x^{d_0} + \cdots + a_0, \\ f_1 &= b_{d_1} x^{d_1} + \cdots + b_0. \end{aligned}$$

$$R = \det \begin{array}{c} \begin{array}{ccccc} x^{d_0+d_1-1} & & \cdots & x & 1 \end{array} \\ \left[\begin{array}{ccccc} a_{d_0} & \cdots & a_0 & & 0 \\ & \ddots & & \ddots & \\ 0 & & a_{d_0} & \cdots & a_0 \\ b_{d_1} & \cdots & \cdots & b_0 & 0 \\ 0 & b_{d_1} & \cdots & \cdots & b_0 \end{array} \right] \end{array} \quad \begin{array}{cc} f_0 * & \left. \begin{array}{c} x^{d_1-1} \\ \vdots \\ 1 \end{array} \right\} B_0 \\ f_1 * & \left. \begin{array}{c} x^{d_0-1} \\ \vdots \\ 1 \end{array} \right\} B_1 \end{array}$$

Cyclohexane conformations

$f_i = c_{i1} + c_{i2} t_j + c_{i3} t_j^2 = 0$, $i, j \in \{1, 2\}$, $f_3 = c_{31} + c_{32} t_2^2 + c_{33} t_1 t_2 + c_{34} t_1^2 + c_{35} t_1^2 t_2^2 = 0$. $\vec{c}_i$: quadratic in hidden t_3; $\deg_c R = 12$; greedy/incremental 16×16 toric resultant matrix:

$$
\begin{array}{cccccccccccccccc}
1 & t_2 & t_2^2 & t_2^3 & t_1 & t_1t_2 & t_1t_2^2 & t_1t_2^3 & t_1^2 & t_1^2t_2 & t_1^2t_2^2 & t_1^2t_2^3 & t_1^3 & t_1^3t_2 & t_1^3t_2^2 & t_1^3t_2^3
\end{array}
$$

$$
\left[\begin{array}{cccccccccccccccc}
c_{11} & c_{12} & c_{13} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & c_{11} & c_{12} & c_{13} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & c_{11} & c_{12} & c_{13} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & c_{11} & c_{12} & c_{13} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\hline
c_{31} & 0 & c_{32} & 0 & 0 & c_{33} & 0 & 0 & c_{34} & 0 & c_{35} & 0 & 0 & 0 & 0 & 0 \\
0 & c_{31} & 0 & c_{32} & 0 & 0 & c_{33} & 0 & 0 & c_{34} & 0 & c_{35} & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & c_{31} & 0 & c_{32} & 0 & 0 & c_{33} & 0 & 0 & c_{34} & 0 & c_{35} & 0 \\
0 & 0 & 0 & 0 & 0 & c_{31} & 0 & c_{32} & 0 & 0 & c_{33} & 0 & 0 & c_{34} & 0 & c_{35} \\
\hline
c_{21} & 0 & 0 & 0 & c_{22} & 0 & 0 & 0 & c_{23} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & c_{21} & 0 & 0 & 0 & c_{22} & 0 & 0 & 0 & c_{23} & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & c_{21} & 0 & 0 & 0 & c_{22} & 0 & 0 & 0 & c_{23} & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & c_{21} & 0 & 0 & 0 & c_{22} & 0 & 0 & 0 & c_{23} & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & c_{21} & 0 & 0 & 0 & c_{22} & 0 & 0 & 0 & c_{23} & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & c_{21} & 0 & 0 & 0 & c_{22} & 0 & 0 & 0 & c_{23} & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & c_{21} & 0 & 0 & 0 & c_{22} & 0 & 0 & 0 & c_{23} & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & c_{21} & 0 & 0 & 0 & c_{22} & 0 & 0 & 0 & c_{23}
\end{array}\right]
$$

One specialization yields determinant of degree 24 (there are 16 roots):

$$\det M = -\frac{186624}{169} \left({t_3}^4 - 22\,{t_3}^2 + 13\right)^3 \left({t_3}^4 - 118\,{t_3}^2 + 13\right) \left({t_3}^2 + 1\right)^4$$

Polynomials model real problems

Recap: Resultant matrices

• Sylvester 1840, Macaulay 1902, [Canny-E'93], greedy [Canny-Pedersen], generalized [Sturmfels'94], rational [D'Andrea'02, E-Konaxis'09, D'Andrea,Jeronimo,Sombra], [Checa-E'22].

• Bézout 1779, [Chtcherba-Kapur'00], [Kapur et.al], [Cardinal-Mourrain'95], [Elkadi-Mourrain], [Busé et al.].

• Hybrid: Morley, Dixon, [Jouanolou'97], [Checa-Busé'23], homogeneous [D'Andrea-Dickenstein'01], [CoxMatera08], with toric Jacobian [Cattani-Dickenstein-Sturmfels], [D'Andrea-E'01], Tate resolution [Khetan'02], complexes [Eisenbud-Schreyer'03].

• Multihomogeneous [Weyman-Zelevinsky'94] [Sturmfels-Zelevinsky'94] [Chionh-Goldman-Zhang'98], [Dickenstein-E'03, E-Mantzaflaris'09], [Awane-Chkiriba-Goze'05], [Bender et al'21].

Survey [E,Mourrain'99:Matrices in elimination theory]

Voronoi diagrams

From Voronoi to Apollonius

Defn. Given n objects in $\mathbb{R}^2$, their Voronoi diagram is a subdivision into n cells, each comprising the points closer to one object.

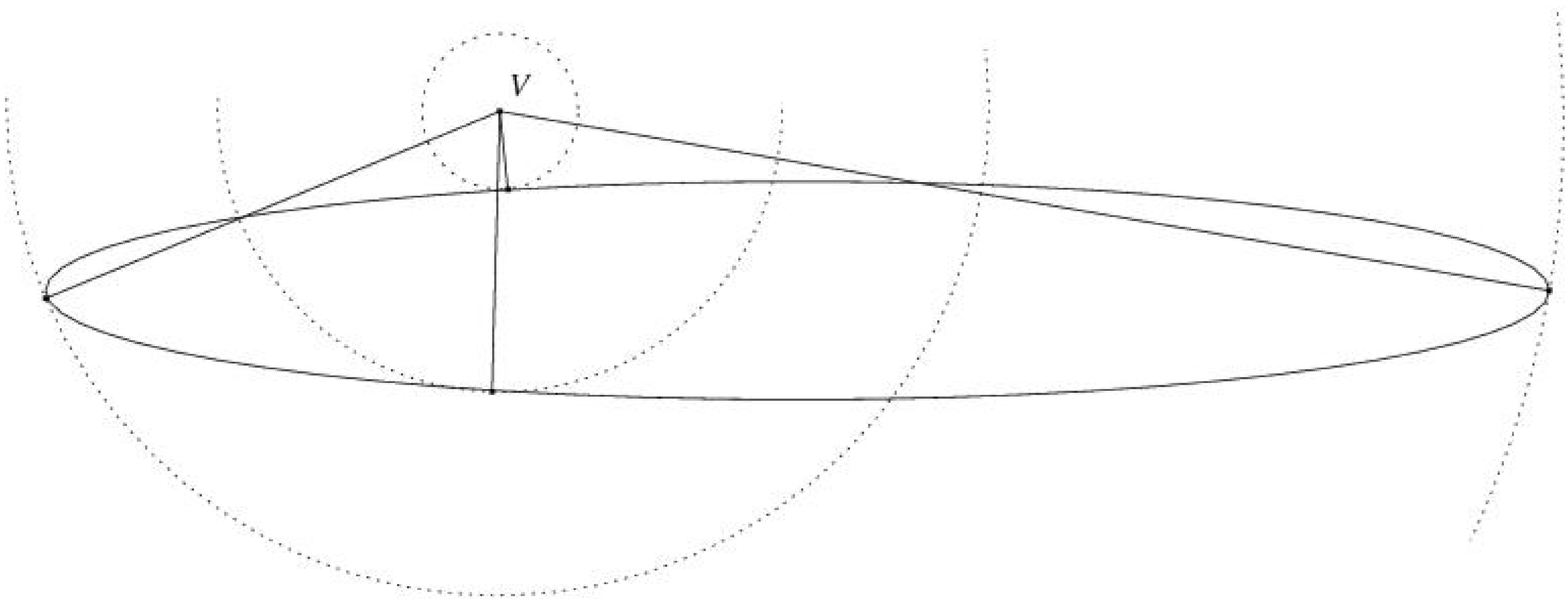
Apollonius diagram of ellipses:

- Problem: predicates, under Euclidean distance; n disjoint ellipses.

- Predicate 1. Given 2 ellipses and an external point, decide which ellipse is closer to the point.
- Main predicate: 3 ellipses define one Apollonius circle externally tritangent to all: decide relative position of 4th ellipse wrt circle.

Point-ellipse distance

For a point outside an ellipse, there are 2-4 normals onto the ellipse, depending on the point's position wrt the evolute curve.



Pencil of conics

General conic, M symmetric: $[x, y, 1]M[x, y, 1]^T = 0$.
Given ellipse, and circle centered at (v_1, v_2) with parametric radius:

$$E = \begin{pmatrix} a & b & d \\ b & c & e \\ d & e & f \end{pmatrix}, \qquad C(s) = \begin{pmatrix} 1 & 0 & -v_1 \\ 0 & 1 & -v_2 \\ -v_1 & -v_2 & v_1^2 + v_2^2 - s \end{pmatrix}$$

- define their pencil $\lambda E + C(s)$,
- with characteristic polynomial $\phi(s, \lambda) = |\lambda E + C(s)|$,
- and $\Delta(s)$ is ϕ's discriminant (wrt λ) [cf Sturmfels' afternoon talk]

Comparing point-ellipse distances

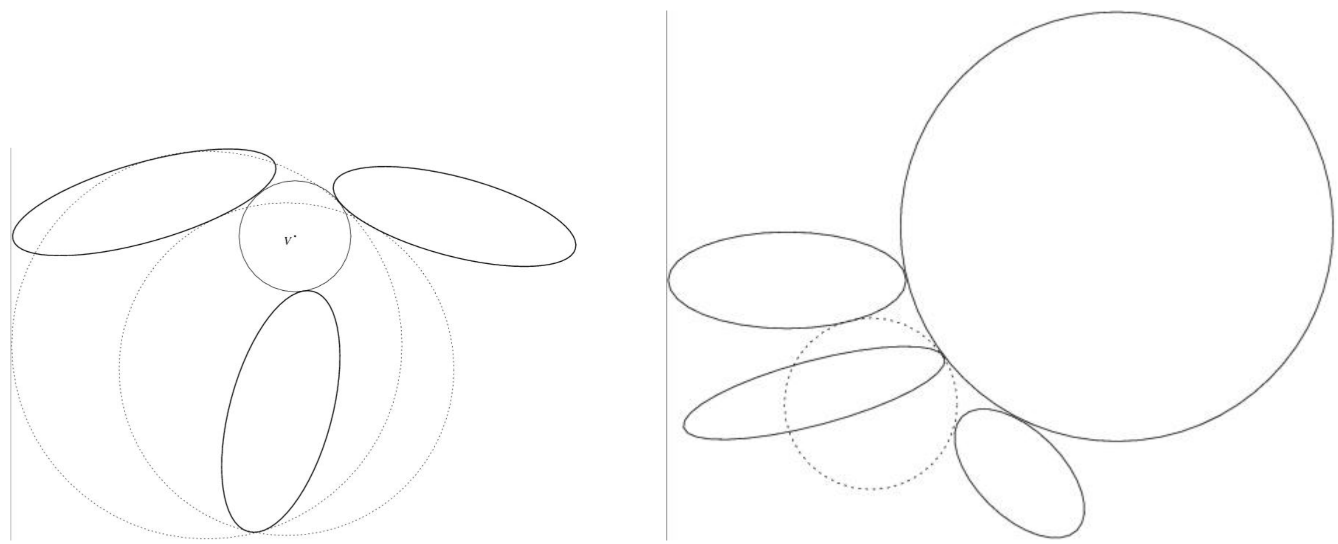
Thm. $\Delta(s) = 0 \Leftrightarrow E, C(s)$ have a multiple intersection (tangency)

Given ellipse E and point v outside E, their distance is the square-root of the smallest positive root of the discriminant $\Delta(s)$.

Deciding which ellipse is closest to an external point reduces to comparing two algebraic numbers of degree 4. This degree is optimal.

Apollonius circles

Given 3 ellipses, how many (real) tritangent circles are defined?



$$\text{MV}\ [\ \Delta_1(v_1,v_2,s), \Delta_2(v_1,v_2,s), \Delta_3(v_1,v_2,s)\ ] = 256.$$

$$q := v_1^2 + v_2^2 - s \quad \Rightarrow \quad C(s) = \begin{pmatrix} 1 & 0 & -v_1 \\ 0 & 1 & -v_2 \\ -v_1 & -v_2 & q \end{pmatrix} \quad \Rightarrow \quad \text{MV} \ = 184.$$

Upper bound seems tight but no match with lower bound on real roots

Unmixed bivariate systems

Given: unmixed system of 3 bivariate polynomials (identical supports).

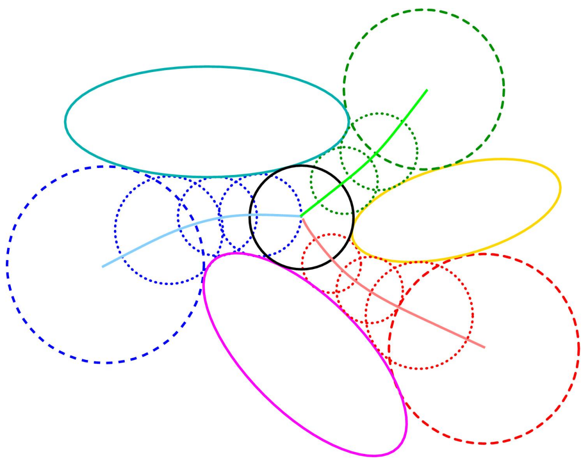
$\exists$ hybrid determinantal formula [Khetan'02]: $M = \begin{bmatrix} B & S \\ S^T & 0 \end{bmatrix}$

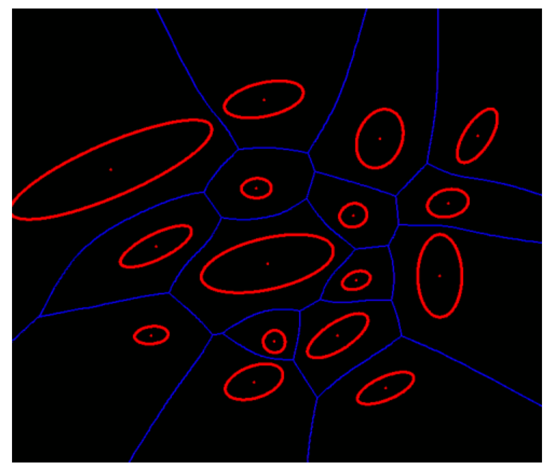
Eliminate $(v_1, v_2) \to 58 \times 58$ matrix with Sylvester and Bézout blocks: sparse resultant $= \det(M)$, of degree 184 in q.

Open: How many real tritangent circles, in general?
Random example yields 8 real roots.

Voronoi diagram of ellipses

- Sparse elimination, Mixed Volume: 184 complex tritangent circles
- Resultants, factoring: sparse, successive Sylvester
- Adapted Newton's: quadratic convergece, certified
- Real solving: Complexity and software
- Switch representation: implicit, parametric





- Geometric CGAL C++ software relying on algebra
- About 1sec per non-intersecting ellipse ["success story"]
- Faster than Voronoi of k-gons, $k \geq 15$ edges or $k \geq 200$ points.

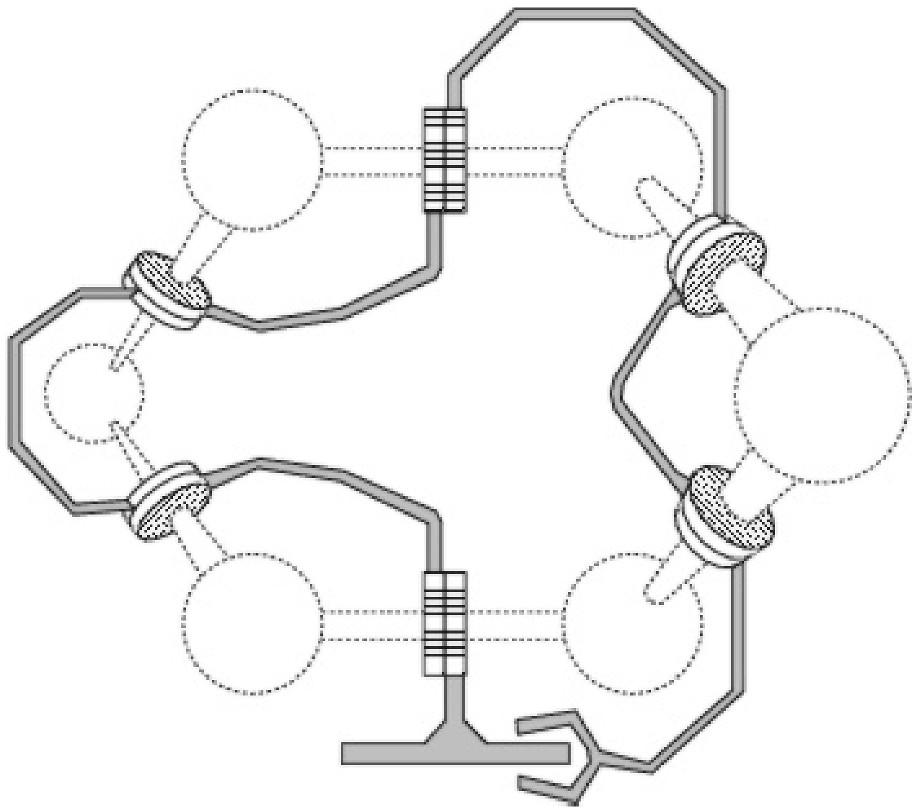
[E-Tsigaridas-Tzoumas,SoCG'06] [E-Tz,CAD'08] [E-Ts-Tz,ACM/SIAM-GPM'09]

Molecular conformations

Cyclohexane

Given some fixed geometric characteristics (angles, lengths) and the position of the end-effector (here a ring), compute all possible configurations defined by 6 consequent rotational DOFs.

Inverse kinematics of a 6R robot with consecutive axes intersecting.



Polynomial equations

Algebraic equations model geometry (rigidity and flexibility):

- Distance constraint: $\mathrm{dist}^2 = \|a - T\,b\|^2$, $a, b \in \mathbb{R}^3$.
- Convert trigs to polynomials by using half-angle:

$$\sin t = \frac{2x}{1+x^2}, \quad \cos t = \frac{1-x^2}{1+x^2}, \quad x = \tan\frac{t}{2}.$$

- DOF modeled by Euclidean/rigid transformations T_i:

Serial motions reduce to Matrix multiplication: $T_{all} = T_1 \cdot T_2 \cdots T_n$.

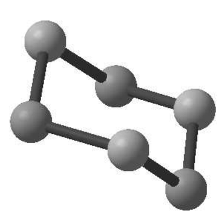
Parallel mechanisms: $T_1 = \cdots = T_n$, where T_i depends on parameters.

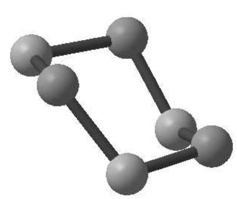
Example: Natural cyclohexane

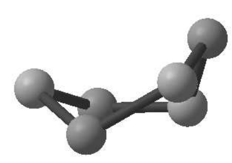
6 carbon atoms at almost equal distances with almost equal bond angles:

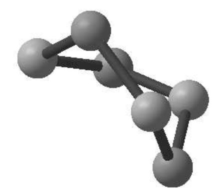
t_1	t_2	t_3
0.3684363946	0.3197251270	0.2969559367
- 0.3684363946	- 0.3197251270	- 0.2969559367
0.7126464332	- 0.01038413185	- 0.6234532743
- 0.7126464332	0.01038413185	0.6234532743

Solutions: 2 chair and 2 twisted boat (crown) backbone conformations:









Computing cyclohexane conformations

1. 8 roots $\pm(1,1,1), \pm(5,-1,-1), \pm(-1,5,-1), \pm(-1,-1,5)$. Add u-polynomial: sparse resultant degree $= 52$, $\dim M = 86$ (incremental), 30×30 u-matrix, generalized eigendecomposition.

2. Natural cyclohexane: 4 real solutions (2 chair, and 2 twisted-boat or crown):

Hide t_3: sparse resultant degree $= 12$, $\dim M = 16$ (incremental), $M = It_3^2 + B_1 t_3 + B_0$. 32×32 companion matrix, standard eigendecomposition.

3. 16 real solutions. Same approach, similar results and performance.

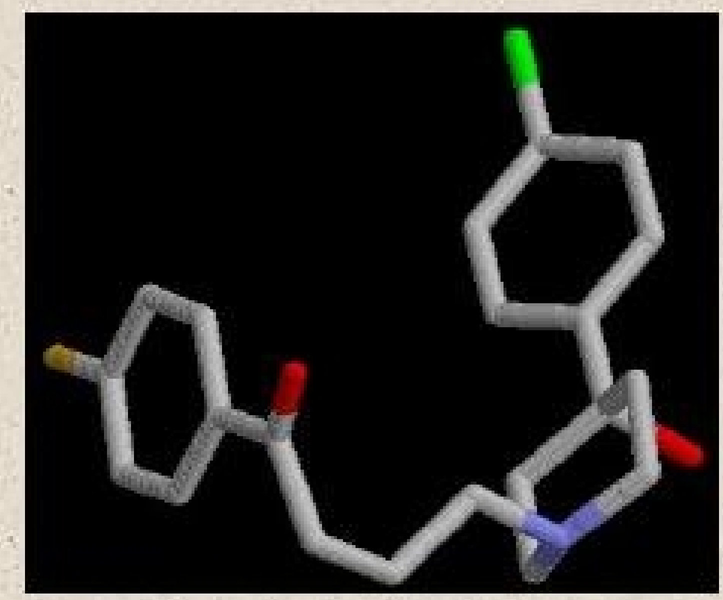
Families of Conformations

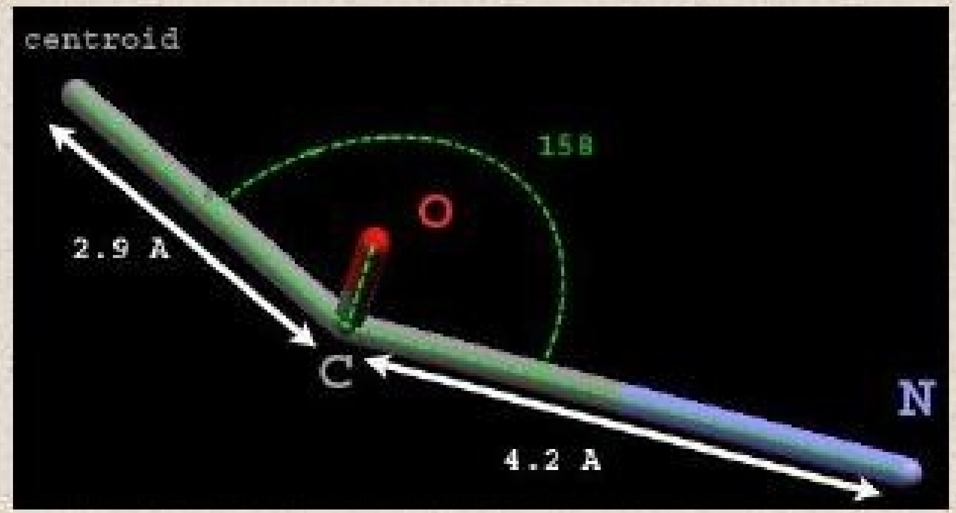
Input. Sequence, and certain number of distances.
Output. All possible tertiary structures.
An infinite number if fewer constraints than DOFs.
[E-Fritzilas'05]

Principle: Torsion/dihedral angles about simple bonds require lower energy than: angles about multiple bonds, or bond lengths/angles.

Goal: screening, pharmacophores, docking.

Dopamine inhibitor: setup



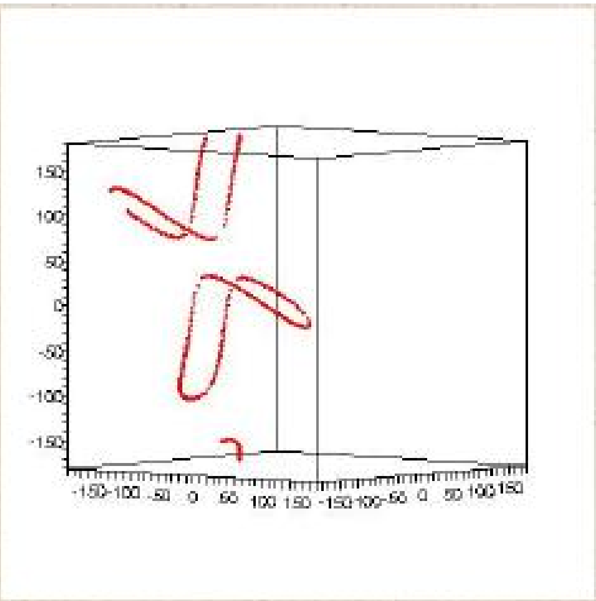


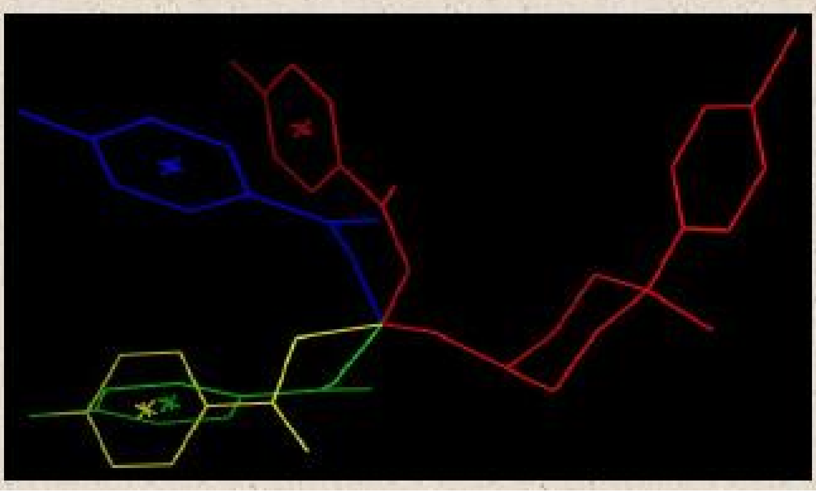
$$-1.89160046\, x_1^2 x_2^2 - 8.650398313\, x_1^2 x_2 - 7.881307764\, x_1 x_2^2 - 12.19454986\, x_1^2 - 10.83370506\, x_1 x_2 + 4.86126022\, x_2^2 + 2.089333272\, x_1 - 7.109323331\, x_2 + 1.42288800 = 0$$

$$-6.57607650\, x_1^2 x_2^2 x_3^2 + 3.548807050\, x_1^2 x_2^2 x_3 + 3.173505720\, x_1^2 x_2 x_3^2 - 3.996183430\, x_1 x_2^2 x_3^2 - 22.39131088\, x_1^2 x_2^2 + 4.572735762\, x_1^2 x_2 x_3 - 37.78781133\, x_1^2 x_3^2 + 7.783422078\, x_1 x_2^2 x_3 - 34.28219042\, x_1 x_2 x_3^2 + 3.98034964\, x_2^2 x_3^2 - 38.25194084\, x_1^2 x_2 - 22.60552493\, x_1^2 x_3 - 22.29539063\, x_1 x_2^2 - 28.82272082\, x_1 x_2 x_3 - 5.811791888\, x_1 x_3^2 - 22.84795777\, x_2^2 x_3 - 5.803007076\, x_2 x_3^2 - 30.57743509\, x_1^2 - 7.145038060\, x_1 x_2 + 4.086206002\, x_1 x_3 - 20.65136401\, x_2^2 - 3.838007950\, x_2 x_3 - 13.49781787\, x_3^2 + 17.74715011\, x_1 - 21.38247988\, x_2 - 37.95408683\, x_3 - 16.32125843 = 0$$

Dopamine inhibitor: conformations

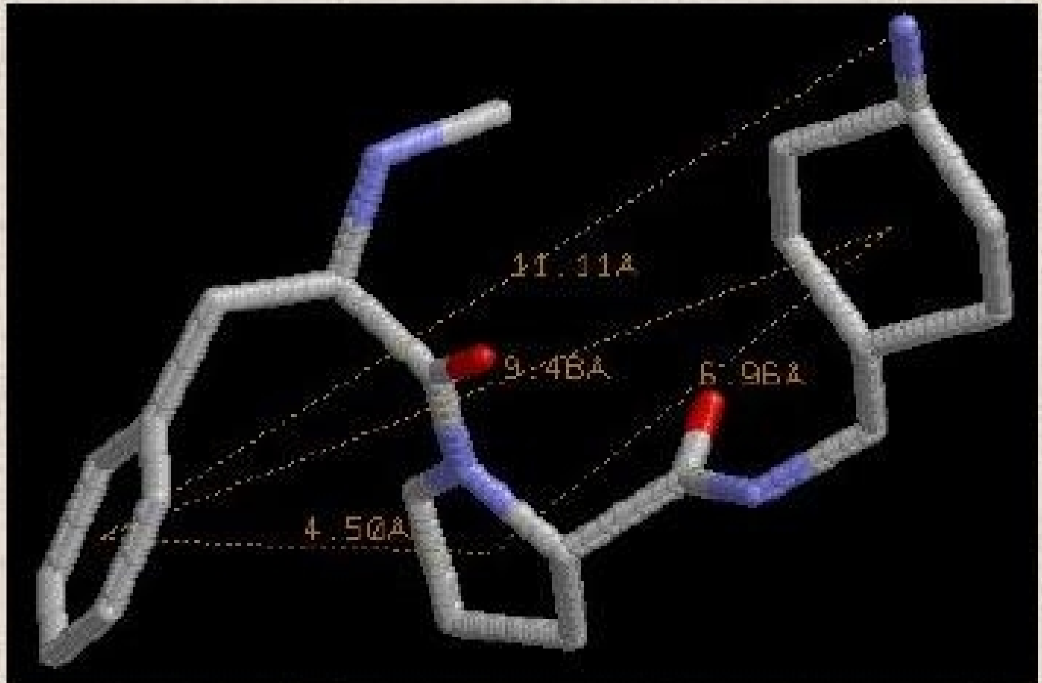
$[\theta_{17,18} = -177, \theta_{15,16} = 80, \theta_{16,17} = -164]$
$[\theta_{17,18} = -177, \theta_{15,16} = -111, \theta_{16,17} = 126]$
$[\theta_{17,18} = -177, \theta_{15,16} = 51, \theta_{16,17} = 175]$
$[\theta_{17,18} = -177, \theta_{15,16} = -83, \theta_{16,17} = 101]$
$[\theta_{17,18} = -175, \theta_{15,16} = -78, \theta_{16,17} = 97]$
$[\theta_{17,18} = -175, \theta_{15,16} = -113, \theta_{16,17} = 127]$
$[\theta_{17,18} = -175, \theta_{15,16} = 46, \theta_{16,17} = 170]$
$[\theta_{17,18} = -175, \theta_{15,16} = 81, \theta_{16,17} = -163]$
$[\theta_{17,18} = -173, \theta_{15,16} = -114, \theta_{16,17} = 128]$
$[\theta_{17,18} = -173, \theta_{15,16} = -73, \theta_{16,17} = 94]$
$[\theta_{17,18} = -173, \theta_{15,16} = 82, \theta_{16,17} = -162]$
$[\theta_{17,18} = -173, \theta_{15,16} = 42, \theta_{16,17} = 165]$
$[\theta_{17,18} = -171, \theta_{15,16} = 83, \theta_{16,17} = -162]$
$[\theta_{17,18} = -171, \theta_{15,16} = -114, \theta_{16,17} = 129]$
$[\theta_{17,18} = -171, \theta_{15,16} = 37, \theta_{16,17} = 161]$
$[\theta_{17,18} = -171, \theta_{15,16} = -69, \theta_{16,17} = 91]$



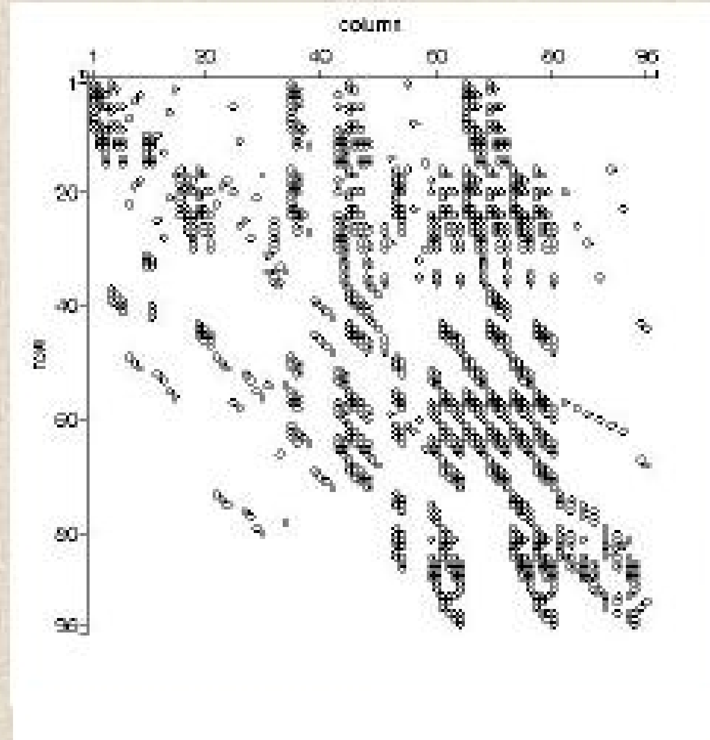


Sampling angles shows 2 families of conformations.

Thrombin ligand (1tom): resultant matrix



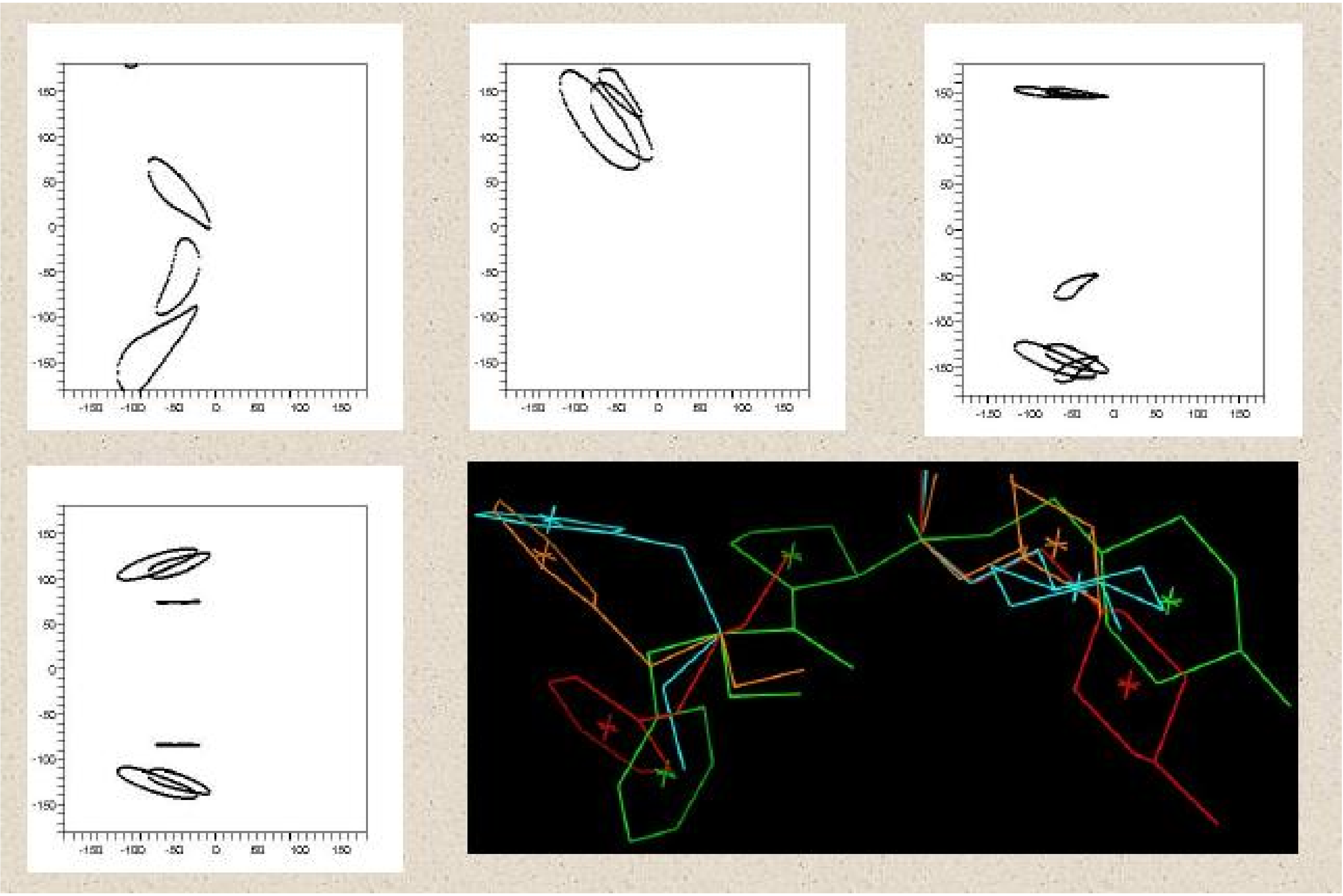
thrombin ligand
PDB code: 1TOM



$$p_1(x_1, x_2, x_3, x_4) = 0 \qquad p_3(x_1, x_2) = 0$$

$$p_2(x_1, x_2, x_3, x_4) = 0 \qquad p_4(x_3, x_4) = 0$$

Thrombin ligand: conformations



Game theory

Two player game

– The options (pure strategies) the players have; assume each player ℓ has m_ℓ strategies.
– The payoff for each player ℓ and for each combination of options, denoted $c_{ij}^{(\ell)}$ for $i \in \{1, \ldots, m_1\}$, $j \in \{1, \ldots, m_2\}$.
– The probability $p_k^{(\ell)}$ of player ℓ using option $k \in \{1, \ldots, m_\ell\}$.

Example: Paper-scissors-stone: $m_1 = m_2 = 3$,

$$C^{(1)} = \begin{bmatrix} 0 & 1 & -1 \\ -1 & 0 & 1 \\ 1 & -1 & 0 \end{bmatrix}, \quad C^{(2)} = \begin{bmatrix} 0 & -1 & 1 \\ 1 & 0 & -1 \\ -1 & 1 & 0 \end{bmatrix}.$$

Prisoner's dilemma (cont'd)

A player may play a mixed strategy, that is, choose to play some of his strategies with certain probabilities.

Payoff matrix of first player $C^{(1)} :=$

$$\begin{array}{r c} & \begin{array}{cc} \text{B admits} & \text{B not} \end{array} \\ \begin{array}{r} \text{A admits with prob. } p_1^{(1)} \\ \text{A not with prob. } p_2^{(1)} \end{array} & \left[\begin{array}{cc} -6 & 0 \\ -10 & -2 \end{array} \right] \end{array}$$

Player ℓ has 2 pure strategies chosen with probability $p_k^{(\ell)}$, $k = 1, 2$. Expected payoffs of 1st player choosing 1st and 2nd strategy are:

$$P_1 = -6p_1^{(2)}, \text{ and } P_2 = -10p_1^{(2)} - 2p_2^{(2)}.$$

Expected payoff of 2 players

Suppose the two players have $m_1 \times m_2$ payoff matrices A, B, and play their options with probabilities $(p_1, \ldots, p_{m_1}), (q_1, \ldots, q_{m_2})$, respectively.

Of course, $p_1 + \cdots + p_{m_1} = 1$, $q_1 + \cdots + q_{m_2} = 1$.

The expected payoffs of their pure strategies are:

$$P_i = q_1 a_{i1} + \cdots + q_{m_2} a_{im_2}, \qquad i = 1, \ldots, m_1,$$

$$Q_j = p_1 b_{1j} + \cdots + p_{m_1} b_{m_1 j}, \qquad j = 1, \ldots, m_2.$$

Typically the payoffs are known but the probabilities are not.

Nash equilibria

Definition. A Nash equilibrium is a combination of players' strategies where no player improves her payoff by unilaterally changing her strategy.

The payoff of a player does not depend on her strategy, as long as other players do not change their strategies.

Then, for each player, all payoffs for the chosen strategies are equal and not smaller than those of non-chosen strategies.

$$
\begin{array}{cc}
 & \begin{array}{cc} \text{B admits} & \text{B not} \end{array} \\
\begin{array}{c} \text{A admits} \\ \text{A not} \end{array} & \begin{bmatrix} \mathbf{-6,-6} & 0,-10 \\ -10,0 & \mathbf{-2,-2} \end{bmatrix}
\end{array}
$$

The Nash equilibrium is not the optimal.

Computation

A Nash equilibrium always exist. In zero-sum games, a Nash equilibrium is unique, and can be computed by a minimax routine. But generally, Nash equilibria are not easy to compute.

Enumerative question: How many Nash equilibria exist?
Known, for 2 players with $\lesssim 6$ strategies each. [von Steghel]
For different #strategies, known for up to 5 and 4: #equilibria ≤ 17 [Vidunas'14]. Little is known for ≥ 3 players.

A Totally mixed Nash equilibrium (TMNE) occurs when every player plays all strategies with positive probability.

Polynomials for TMNE

Consider a game of r players, where ℓ-th player has m_ℓ pure strategies, and the k-th strategy chosen with probability $p_k^{(\ell)}$.

Let $c^{(j)}_{k_1,\ldots,k_j,\ldots,k_r}$ be a $m_1 \times m_2 \times \cdots \times m_r$ table expressing the payoff of player j when player ℓ opts for pure strategy $k_\ell \in \{1,\ldots,m_\ell\}$.

The expexted payoff of player j choosing strategy k_j is

$$P^{(j)}_{k_j} = \sum_{k_1,\ldots,k_{j-1},k_{j+1},\ldots,k_r} c^{(j)}_{k_1,\ldots,k_j,\ldots,k_r} \cdot p^{(1)}_{k_1} \cdots p^{(j-1)}_{k_{j-1}} p^{(j+1)}_{k_{j+1}} \cdots p^{(r)}_{k_r}.$$

Well-constrained, multilinear system of $m_1 + \cdots + m_r - r$ equations with variables partitioned in r blocks, the ℓ-th block containing m_ℓ homogeneous variables $p^{(\ell)}_1, \ldots, p^{(\ell)}_{m_\ell}$, but miss variable set $p^{(j)}$.

m-Bézout bound for TMNE

Let $Y = y_1 + \cdots + y_r$.
The number of TMNE's equals the coefficient of $y_1^{n_1} \cdots y_r^{n_r}$ in

$$\prod_{i=1}^{r} (Y - y_i)^{m_i}.$$

Idea: write the equations, apply Bézout-type bound.
The m-Bézout bound yields upper (complex) bounds on the number of TMNE's. In the case of TMNE's, the m-Bézout bound yields tight bound [McLennan].

Conclusion

- Various open questions:

Unification, discriminant, tropical, approximate computing

- Develop good software:

Now just prototypes in C/C++, Maple, Singular, Macaulay.

- Machine Learning

(breakthroughs in linear algebra)

Thank you!