Computational Algebra: Big Ideas

Ioannis Z. Emiris

Dept. of Informatics & Telecoms

NKUA, 2016

Outline

05. Idea: coefficients $\equiv$ values (FFT)

17. Idea: matrices faster than Gauss

25. (Idea): real solving by remainders (Euclid)

41. intro to polynomial systems

48. Idea: algebra-geometry dictionary (Hilbert)

    52.Polynomial Degree

56. Idea: system solving by linear algebra

    68.Sylvester

    75.Macaulay

    80.Bilinear example

83: Idea: polynomials $\equiv$ polytopes (Gelfand)

    93.Mixed subdivisions

    107.Sylvester-type sparse-resultant matrices

    123.Polynomial system solving

133: (Applications): geometric modeling, robotics, game theory

Big Questions for 2016

- Can we efficiently solve (nonlinear) polynomial systems by linear algebra?
- Can combinatorics accelerate polynomial system solving?
- Do polynomials model effectively problems in 3D modeling?

Reading

coefficients $\equiv$ values

matrices faster than Gauss

real solving by remainders (Euclid)

[Yap: Fundamental Problems in Algorithmic algebra]

varieties vs ideals (Hilbert) [Cox-L-O:Ideals,Varieties,Algorithms]

system solving by linear algebra [CLO:Using algebraic geometry,ch.3]

polynomials $\equiv$ polytopes (Gelfand) [CLO:Using...,ch.7]

[Sturmfels: Solving Systems of polynomial equations]

[Dickenstein-E: Solving polynomial equations: Foundations, Algorithms...]

Arithmetic operations [Yap, ch.1]

Computational model

Real RAM (Random Access Machine):
provides $O(1)$ storage/access time/space for reals,
requires $O(1)$ time for arithmetic operations on reals, performed exactly.
Hence counts arithmetic complexity, notation $O_A(\cdot)$.

Boolean RAM (or Turing machine):
provides $O(1)$ storage/access time/space for bits,
requires $O(1)$ time for operations on bits, performed exactly.
Hence counts bit/Boolean complexity, notation $O_B(\cdot)$.

Integers

Integers with n bits:
sum/difference with $\leq n+1$ bits, in $\Theta_B(n)$.

Product with $\leq 2n$ bits, naive algorithm in $O_B(n^2)$.
Question: Is multiplication really harder? is it $O(n)$ additions?

Theorem. The asymptotic complexities of multiplication, division with remainder, inversion, and squaring are connected by constants.

Theorem [Karatsuba]

$$\text{Divide+Conquer yields } O_B(n^{\lg 3}) = O_B(n^{1.585\ldots}).$$

Pf. $a = a_0 + 2^{n/2}a_1$, $ab = a_0b_0 + 2^{n/2}(a_0b_1 + b_0a_1) + 2^n a_1b_1$,

$$(a_0b_1 + b_0a_1) = (a_0 + a_1)(b_0 + b_1) - a_0b_0 - a_1b_1.$$

$$M(n) = 3M(n/2) + 4A(n/2) + 2A(n) = 3M(n/2) + O(n) = O(n^{\lg 3}),$$

where complexities $M(n)$ of multiplication, $A(n)$ of addition.

Theorem. Fast Fourier Transform yields $O_B(n \log n \log\log n)$.

Univariate polynomials

$p_1(x), p_2(x) \in \mathbb{Z}[x]$, degrees d_1, d_2, and t_1, t_2 terms. Let $d = \max\{d_1, d_2\}$.

The sum has degree $\leq d$, $\leq t_1 + t_2$ terms, cost $\Theta(d)$.

Product of degree $d_1 + d_2$, $\leq t_1 t_2$ terms, cost depending on the algorithm:

$$O_A(d_1 d_2), O_A(d^{\lg 3}), O_A(d \log^2 d), O_A(d \log d),$$

by school, D+C, evaluate/interpolate, FFT (no carry needed) algorithms. In sparse representation: $O_A(t_1 t_2)$, $O_A(t^{\lg 3})$.

The arithmetic complexities of multiplication, squaring, division with remainder are connected with constants.

Integers to polynomials: Given binary integer $[c_{n-1}\ c_{n-2}\ \cdots\ c_0]$,
$\exists!$ polynomial $c_{n-1}x^{n-1} + c_{n-2}x^{n-2} + \cdots + c_0 \in \mathbb{Z}_2[x]$.

Evaluation

Horner's rule $p(a) = (\cdots(c_n a + c_{n-1})a + \cdots) + c_0$.
Requires n additions, n products, which is optimal.

Equivalent: $p(a) = p(x) \bmod (x - a)$,
since $p(x) = q(x)(x - a) + r(x), \deg(r(x)) = 0$.

General Problem: Given k points/values $x_0, \ldots, x_{k-1}$, and $n + 1$ coefficients of $p(x)$, i.e. $\deg(p) = n$, compute k values $p(x_0), \ldots, p(x_{k-1})$.

Horner yields $O_A(kn)$, we'll see a quasi-linear algorithm.

Quasi-linear multi-evaluation

[Note: this can be avoided if you go directly to FFT.]

Theorem. D+C algorithm $= O_A(n \lg^2 n)$, for $k = \Theta(n)$.

Lem. $a, b, c \geq 0 \Rightarrow (a \bmod (bc)) \bmod b = a \bmod b$.

Lem.

$$p(x) \bmod (x - x_i) = [p(x) \bmod \prod_{j \in J} (x - x_j)] \bmod (x - x_i), \qquad i \in J \subset \mathbb{N}.$$

Quasi-linear algorithm: fan-in

Assume we have $k = n$ points. We compute $\prod_j (x - x_j), j = 2^i - 1, \ldots, 2^{i+1}$, using fan-in, for appropriate i (see next page).

Leaves: Compute $n/2$ products of degree=2:

$$(x - x_{2i})(x - x_{2i+1}), i = 0, \ldots, \frac{n}{2} - 1.$$

Then $n/4$ products of degree 4, then $n/2^j$ products of degree 2^j in

$$O_A((n/2^j)M(2^{j-1})) = O_A(nj), \quad j = 1, \ldots, \lg n,$$

$M(t) = O(t \log t)$ corresponds to FFT multiplication.
Total $O(n(1 + \cdots + \lg n)) = O(n \lg^2 n)$.

Quasi-linear algorithm: Fan-out

Given $q(x) = p(x) \bmod \prod_{i=0}^{n-1}(x - x_i)$, compute

$$p(x) \bmod \prod_{i=0}^{n/2-1} (x - x_i) = q(x) \bmod \prod_{i=0}^{n/2-1} (x - x_i),$$

and $q(x) \bmod \prod_{i=n/2}^{n-1}(x - x_i)$, i.e. 2 polynomials of degree $n/2 - 1$, in $O(n \log n)$ by FFT. Then, 4 mod operations in $4(n-2)/2 \cdot O(\log n)$.

Stage k: compute 2^k remainders with divisor

$$\prod_i (x - x_i),\ i = \frac{mn}{2^k}, \ldots, \frac{(m+1)n}{2^k} - 1,\ m = 0, \ldots, 2^k - 1.$$

Divisor degree $= n/2^k$, remainder degree $= n/2^k - 1$, $k = 0, 1, \ldots, \lg n$.
Cost per level $= 2^k n/2^k \cdot O(\lg n)$.

Total $T(n) = 2T(n/2) + 2O(n \lg n) = 2nkO(\lg n) = O(n \lg^2 n)$.

Example

$$p(x) = 5x^3 + x^2 + 3x - 2, x_i = -1, 0, 3, 9.$$

$q_0(x) = p(x)$ mod $(x + 1)x = 7x - 2$,
$q_1(x) = p(x)$ mod $(x - 3)(x - 9) = 600x - 1649$.

$p(x)$ mod $(x + 1) = q_0(x)$ mod $(x + 1) = -9$,
$p(x)$ mod $x = q_0(x)$ mod $x = -2$,
$p(x)$ mod $(x - 3) = q_1(x)$ mod $(x - 3) = 151$,
$p(x)$ mod $(x - 9) = q_1(x)$ mod $(x - 9) = 3751$.

Interpolation

Def.: compute $n+1$ coefficients of $p(x)$ given $n+1$ values $r_i = p(x_i), i = 0, \ldots, n$ for distinct x_i's, assuming the degree n is known.

Lagrange: $L(x) := \prod_{i=0,\ldots,n}(x - x_i)$, $L'(x) = \sum_{i=0}^{n} \prod_{j \neq i}(x - x_j)$.
Then $L'(x_k) = \prod_{j \neq k}(x_k - x_j)$. Now define:

$$L_i(x) := \prod_{j=0,\ldots,n, j \neq i} \frac{x - x_j}{x_i - x_j}.$$

Hence the solution is:

$$p(x) = L(x) \sum_{i=0}^{n} \frac{r_i}{L'(x_i)(x - x_i)} = \sum_{i=0}^{n} \frac{r_i}{L_i'(x_i)} \prod_{j \neq i}(x - x_j) = \sum_{i=0}^{n} r_i L_i(x).$$

Clearly p satisfies the data; it is also unique with degree $\leq n$.

Fan-in computes $L(x)$, $L'(x)$, $L'(x_0), \ldots, L'(x_n)$, and $p(x)$ in $O_A(n \lg^2 n)$

FFT

Given polynomial

$$p(x) = c_{n-1}x^{n-1} + \cdots + c_0,$$

compute values at the complex n-th roots of unity:

$$\{1, \omega = e^{2\pi i/n}, \omega^2 = e^{4\pi i/n}, \ldots, \omega^{n-1} = e^{2\pi i(n-1)/n}\}.$$

Assume n is a power of 2:

$$p(x) = (c_0 + c_2x^2 + \cdots + c_{n-2}x^{n-2}) + x(c_1 + c_3x^2 + \cdots + c_{n-1}x^{n-2}) =$$

$$= q(x^2) + xs(x^2),$$

and set $y = x^2$, where $q(y), s(y)$ of degree $(n-2)/2$.

Property 1. $x = \omega^j$, $j = 0, \ldots, n-1$, then $y = \omega^{2j}$ takes only $n/2$ values.
Property 2. $\omega^j = -\omega^{j+n/2}$ reduces half of $q(y) + \ldots$ to $q(y) - \ldots$.

Complexity:

$$T(n) = 1.5n + 2T(\frac{n}{2}) = 1.5kn + 2^kT(\frac{n}{2^k}) = 1,5n \lg n + O(n) = O_A(n \lg n)$$

Inverse Fourier Transform

Def. Interpolate $(n-1)$-degree polynomial from values at n-th roots of 1

Let $n \times n$ Vandermonde matrix Ω with $\Omega_{ij} = [\omega^{ij}/\sqrt{n}]$, $0 \leq i, j < n$.
Fourier Transofrm computes

$$\sqrt{n}\,\Omega \begin{bmatrix} c_0 \\ \vdots \\ c_{n-1} \end{bmatrix} = \left[\omega^{ij}\right]_{i,j} \begin{bmatrix} c_0 \\ \vdots \\ c_{n-1} \end{bmatrix} = \begin{bmatrix} p(\omega^0) \\ \vdots \\ p(\omega^{n-1}) \end{bmatrix} =: p^T.$$

Inverse Transform: solve for c, given p: $c = \frac{1}{\sqrt{n}}\,\Omega^{-1}\,p^T$.

Lem. $\Omega^{-1} = [\omega^{-ij}/\sqrt{n}]$.
Pf. $\sum_k \omega^{-ik}\omega^{kj} = \sum_k \omega^{k(j-i)} = n$, if $i = j$; otherwise 0.
Cor. Since ω^{-1} is n–th root of 1, c is obtained by FFT.

Idea: Matrices faster than Gauss [Aho-Hopcroft-Ullman]

Matrices

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] $O_A(n^{\lg 7}) = O_A(n^{2.81})$.
[Coppersmith-Winograd'90] $O_A(n^{2.376})$.
Record bound still holds, also achieved (2010) by other approach.

New bounds achieved by tensor algebra, extending CW, see e.g. [Vassilevska-Williams].

Strassen's algorithm

Given 2×2 matrices $[a_{ij}], [b_{ij}]$, $i, j = 1, 2$, let the product be $[c_{ij}]$.

Set: $m_1 = (a_{12} - a_{22})(b_{21} + b_{22})$, $m_2 = (a_{11} + a_{22})(b_{11} + b_{22})$, $m_3 = (a_{11} + a_{12})b_{22}$, $m_4 = a_{22}(b_{21} - b_{11})$, $m_5 = a_{11}(b_{12} - b_{22})$, $m_6 = (a_{21} + a_{22})b_{11}$, $m_7 = (a_{11} - a_{21})(b_{11} + b_{12})$

$$\Rightarrow (c_{ij}) = \begin{bmatrix} m_1 + m_2 - m_3 + m_4 & m_3 + m_5 \\ m_4 + m_6 & m_2 + m_5 - m_6 - m_7 \end{bmatrix}$$

General dimension: replace a_{ij}, b_{ij}, c_{ij} by $\frac{n}{2} \times \frac{n}{2}$ submatrices A_{ij}, B_{ij}, C_{ij}. Then,

$$M(n) = 7M(\frac{n}{2}) + O(n^2) \leq \cdots \leq 7^k M(n/2^k) + kcn^2 = O(n^{\lg 7}).$$

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

Given is integer matrix $[a_{ij}]$, max entry length $L = \max_{ij}\{\lg |a_{ij}|\}$: Worst-case optimal bound on value [Hadamard]:

$$|\det A| \leq \prod_{i=1}^{n} \|a_i\|_2 \leq n^{n/2} \max\{|a_{ij}|\}^n.$$

1. Chinese remaindering avoids intermediate swell: $O^*(nL)$ evaluations modulo constant-length primes, each in $O^*(n^{2.38})$; Lagrange in $O^*_B(n^2L^2)$.

$$\text{Total: } O^*_B(n^{3.38}L).$$

2. Avoid rationals [Bareiss'68] in $\sum_{i=1}^{n} n^2 iL = O^*_B(n^4L)$.

Let $[12k] = |a_{ij} : i = 1,2,3, j = 1,2,k|$: Multiply by a_{11} rows $2\ldots,n$, eliminate:

$$\begin{bmatrix} a_{11} & a_{12} & \cdots \\ 0 & a_{11}a_{22} - a_{12}a_{21} & a_{11}a_{23} - a_{13}a_{21} \\ 0 & a_{11}a_{32} - a_{12}a_{31} & a_{11}a_{33} - a_{13}a_{31} \end{bmatrix} \to \begin{bmatrix} a_{11} & a_{12} & \cdots & \cdots \\ 0 & a_{11}a_{22} - a_{12}a_{21} & \cdots & \cdots \\ 0 & 0 & a_{11}[123] & a_{11}[124] \end{bmatrix}$$

3. Baby steps / giant steps $O_B(n^{3.2}L)$ [Kaltofen-Villard'01]

$n \times n$ **linear system**

rank(M) $= r \leq n$:

- $r = n \Rightarrow \exists!$ solution.
- $r < n \Rightarrow$ system defined by r equations.

remaining equations trivial (0=0) implies ∞ roots.

existence of incompatible equation (0=b) implies no roots.

rank(M) also defined for rectangular M.

Structured matrices

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

Two important examples:

- Vandermonde: matrix-vector multiply and solving in $O_A(n \log^2 n)$.
- Rectangular matrix is Toeplitz iff $M(a+i, b+i) = M(a,b)$, $i > 0$, when defined, i.e. constant diagonals. Lower triangular * vector is polynomial multiplication, hence in $O^*_A(n)$; same for vector * upper triangular.
- ◦ More types: Hankel (constant anti-diagonals), Cauchy, Hilbert.

Thm [Wiedemann (Lanszos)]. Matrix determinant reduced to $O^*(n)$ matrix-vector products.

Proof. Krylov sequence $M^i v$ computed as $M(M^{i-1}v)$,
charpoly $\chi(\lambda) = \det(M - \lambda I) = (-1)^{\pm 1}\lambda^n \pm \operatorname{tr}(M)\lambda^{n-1} + \cdots \pm \det M$.
Caley-Hamilton thm: $\chi(M) = 0$, so $\chi(M)v = 0$.
Berlekamp-Massey: finds k-recurrence from $2k$ (vector) elements.

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:

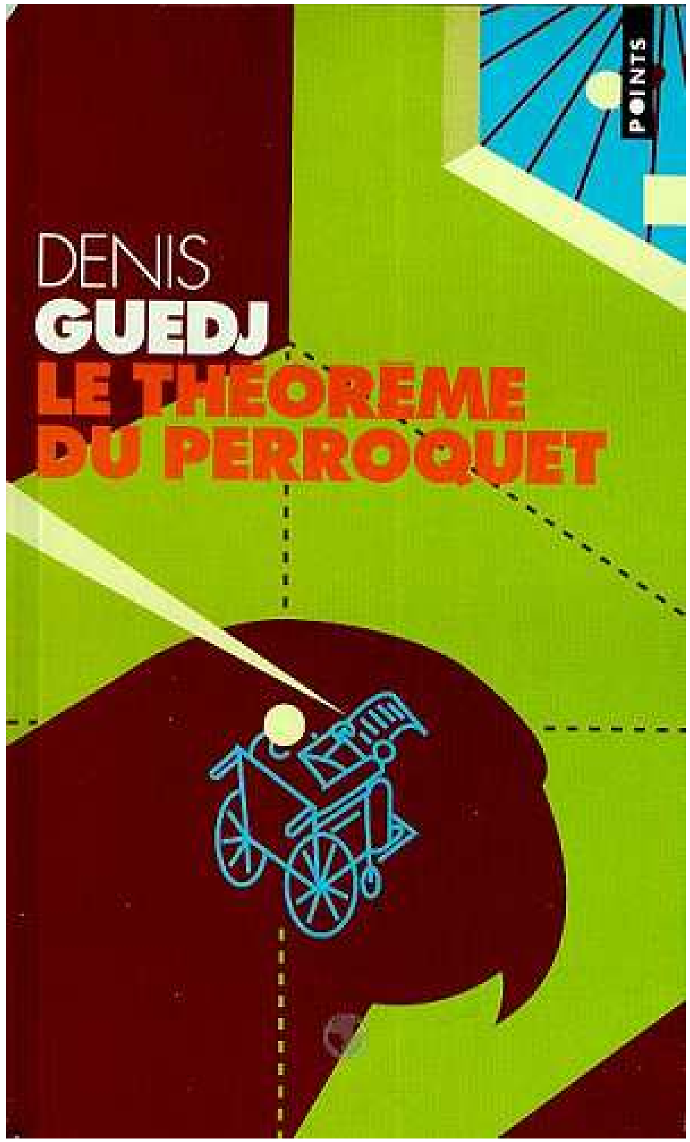
$$\begin{array}{cc} \begin{bmatrix} 5 & 0 & 2 & -11 & & & & \mathbf{0} \\ & 5 & 0 & 2 & -11 & & & \\ & & 5 & 0 & 2 & -11 & & \\ & & & 5 & 0 & 2 & -11 & \\ \mathbf{0} & & & & 5 & 0 & 2 & -11 \end{bmatrix} & \begin{array}{c} x^4P_2 \\ x^3P_2 \\ x^2P_2 \\ xP_2 \\ P_2 \end{array} \end{array}$$

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

$$(P_1P_2)(x) = 5x^7 - 10x^6 + 2x^5 + 47x^3 + 6x^2 - 23x - 55.$$

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

Real numbers



Univariate real solving

Univariate solving

- **Counting / Exclusion**
  - Interval arithmetic (cf. Matlab)
  - Descartes' rule, Bernstein basis (fast)
- Sturm sequences
  - Thom's encoding (good asymptotics)

- **Approximation**
  - Numeric solvers $O(d^3 L)$
  - Continued Fractions [E-Tsigaridas] (fast)

Polynomial in $\mathbb{Z}[x]$ of degree d and bitsize L.
Input size in $O(dL)$, output in $\Omega(dL)$.

Bit complexity of exact solvers

Cont.Frac.	Sturm	Descartes	Bernstein
$O^*(2^L)$ [Uspensky48] $O(d^5L^3)$ [Akritas'80]	$O^*(d^7L^3)$ [Heidel'71] $O^*(d^6L^3)$ [Davenport'88]	$O^*(d^6L^2)$ [Collins,Akritas'76] $O^*(d^5L^2)$ [Krandick'95] [Johnson'98]	[LaneReisenfeld81] $O^*(d^6L^3)$ [MourrainVrahatis] [-Yakoubson'04]
$O^*(d^8L^3)$ [Sharma07]	[DuSharmaYap05]	$O^*(d^4L^2)$ [EigenwilligSharmaYap06] + square-free + multiplicities [E,Mourrain,Tsigaridas'06]	[E,Mourrain,T'06]
$O^*(d^4L^2)$ [ET'06]	$O^*(r\,d^2L^2)$	$O^*(d^3L^2)$ [E,Tsigaridas]	

Polynomial in $\mathbb{Z}[x]$ of degree d and bitsize L.
Best numerical algorithm in $O(d^3L)$, input $= O(dL)$.
Worst-case vs. average-case complexities, $r =$ #real-roots.

Sturm theory

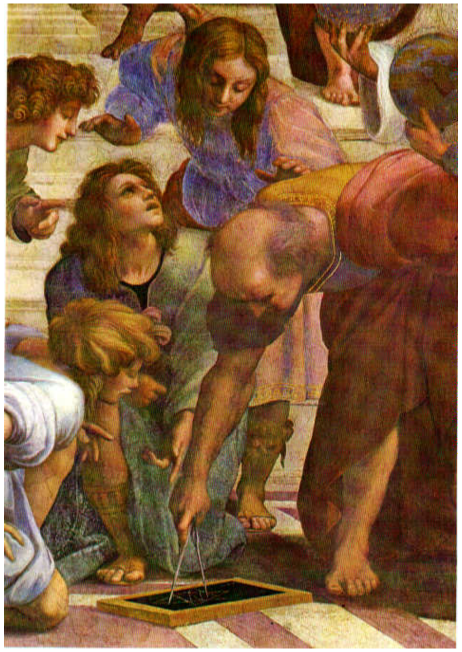
Sturm sequences

Definition. Given univariate polynomials $P_0, P_1 \in \mathbb{R}[x]$, their Sturm sequence is any (pseudo-remainder) sequence of polynomials $P_0, P_1, \ldots, P_n \in \mathbb{R}[x]$, $n \geq 1$ such that

$$\alpha_i P_{i-1} = Q P_i + \beta_i P_{i+1}, \quad i = 1, \ldots, n-1,$$

for some $Q \in \mathbb{R}[x]$, $\alpha_i, \beta_i \in \mathbb{R}$, and $\alpha_i \beta_i < 0$.

Remember $E\upsilon\kappa\lambda\epsilon\acute{\iota}\delta\eta s$



Example of Sturm sequence

Input: $f_i = \alpha_i x^2 - 2\beta_i x + \gamma_i$, $i = 1, 2$.
Hypothesis: the f_i are relatively prime, $\alpha_i, \Delta_i \neq 0$.

The Sturm sequence (P_i) of f_1, $f_1' f_2$:

$$
\begin{aligned}
P_0(x) &= f_1(x) \\
P_1(x) &= f_1'(x) f_2(x) \\
P_2(x) &= -f_1(x) \\
P_3(x) &= 2\alpha_1[-(\alpha_1 K + 2\alpha_2\Delta_1)x + (\gamma_1 J - \alpha_1 J')] \\
P_4(x) &= -\alpha_1\Delta_1(\alpha_1 K + 2\alpha_2\Delta_1)^2(G^2 - 4JJ') \\
&= -\alpha_1\Delta_1(\alpha_1 G - 2\beta_1 J)^2(G^2 - 4JJ')
\end{aligned}
$$

Root counting

Theorem [Tarski]. Suppose that

- $f_0, f_1 \in \mathbb{R}[x]$ are relatively prime,
- f_0 is square-free, and
- $p < q$ are not roots of f_0.

Then, for any Sturm sequence $P = (f_0, f_0' f_1, \ldots)$,

$$V_P(p) - V_P(q) = \sum_{f_0(\rho)=0, p<\rho<q} \mathrm{sign}(f_1(\rho)),$$

where $V_P(p) :=$ #sign variations in $P_0(p), \ldots, P_n(p)$.

The Sturm sequence here may be $(f_0, f_0' f_1, -f_0, \ldots)$.

More uses of Sturm sequences

Corollary. For $p < q$ non-roots of $f \in \mathbb{R}[x]$, the number of distinct real roots of f in (p, q) equals $V_{f,f'}(p) - V_{f,f'}(q)$.

Proof. Let $f_0 = f, f_1 = 1$ in Tarski's theorem.

Theorem [Schwartz-Sharir]. For square-free $f_0, f_1 \in \mathbb{R}[x]$ and $p < q$ non-roots of f_0,

$$V_{f_0,f_1}(p) - V_{f_0,f_1}(q) = \sum_{f_0(\rho)=0, p<\rho<q} \mathrm{sign}(f_0'(\rho) f_1(\rho)).$$

- Yields previous theorem by using $f_0, f_0' f_1$.

[Yap: Fundamental Problems of Algorithmic Algebra, 2000]

Generalizations of Sturm theory

Systems of univariate polynomials

Recall [Tarski]. For $f_0, f_1 \in \mathbb{R}[x]$ relatively prime, f_0 square-free and $p < q$ not roots of f_0, consider the Sturm sequence $(f_0, f_0' f_1, \ldots)$. Then

$$V(p) - V(q) = \sum_{f_0(\rho)=0, p<\rho<q} \mathrm{sign}(f_1(\rho)).$$

This equals

$$\#\{\rho \in (p,q) : f_0(\rho) = 0, f_1(\rho) > 0\} - \#\{\rho \in (p,q) : f_0(\rho) = 0, f_1(\rho) < 0\}.$$

Algorithm [Ben-Or,Kozen,Reif], [Canny]. Compute

$$\sum_{i=1}^{n} \# \ \{\rho \in (p,q) : P_0(\rho) = 0, P_i(\rho) \otimes_i 0\}, \quad \otimes_i \in \{<,>\}.$$

Generalized Sturm sequences

Definition. Given univariate polynomials $P_0, P_1 \in \mathbb{R}[x]$, where P_0 is square-free, their generalized Sturm sequence over an interval $[a,b] \subset \mathbb{R} \cup \{-\infty, +\infty\}$ is any sequence $P_0, P_1, \ldots, P_n \in \mathbb{R}[x], n \geq 1$ s.t.

1. $P_0(a)P_0(b) \neq 0$,
2. $\forall\ c \in [a,b],\ \ P_n(c) \neq 0$,
3. $\forall\ c \in [a,b],\ \ P_j(c) = 0 \Rightarrow P_{j-1}(c)P_{j+1}(c) < 0$,
4. $\forall c \in [a,b] : P_0(c) = 0 \Rightarrow\ \exists\ [c_1, c), (c, c_2]$ s.t. $u \in [c_1, c) \Rightarrow P_0(u)P_1(u) < 0$ and $u \in (c, c_2] \Rightarrow P_0(u)P_1(u) > 0$.

Corollary (Existance). For any $P_0, P_1 \in \mathbb{R}[x]$, the previously-defined Sturm sequence, using the pseudo-remainders and starting with $P_0/\gcd(P_0, P_0')$ and P_1 is "generalized" over an interval $[a,b]$ such that $P_0(a)P_0(b) \neq 0$.

Further generalization

Corollary. It is possible to omit [1. $P_0(a)P_0(b) \neq 0$] provided that, (4) is stated only in the appropriate subinterval of $[a, b]$, when $c = a$ or $c = b$.

Corollary. Relax (4) to require that the number of roots of $P_0(x)$ is odd between any two roots of $P_1(x)$.

Real Closed fields generalize $\mathbb{R}$

Definition. An ordered field K contains a positive subset $P \subset K$, ie. $a \in K - \{0\} \;\Rightarrow\; a \in P$ xor $-a \in P$.

Examples: $\mathbb{Q}, \mathbb{R}, \mathbb{Q}(\epsilon), \mathbb{R}(x), \mathbb{Q}(\sqrt[3]{2}) \equiv \mathbb{Q}[x]/\langle x^3 - 2\rangle$.
Counter-example: $\mathbb{C}$.

Definition. A real closed field K is

- ordered (hence contains positive $P \subset K$),
- $a \in P \;\Rightarrow\; \sqrt{a} \in P$ (ie. $x^2 = a$ has a root in P),
- equations of odd degree have a root in P.

Examples: $\mathbb{R}, \mathbb{R}(\epsilon), \mathbb{R}(\epsilon_1, \epsilon_2)$.
Counter-example: $\mathbb{Q}$, algebraic closure $\overline{\mathbb{Q}}$, $\mathbb{Q}(\sqrt[3]{2})$.

Sturm sequences are defined, and all stated properties hold, for polynomials over real closed fields.

Descartes' rule

Descartes' rule of sign

Theorem. The number of sign variations in the coefficients of a univariate polynomial exceeds the number of positive real roots by an even non-negative integer.

Proof by induction, using Sturm sequences.
Step: $V\left[(x-a)f\right] = V[f] +$ odd natural number.

Corollary. If all roots of the univariate polynomial are nonzero and real, then the number of sign variations in the coefficient sequence gives precisely the number of positive roots.

Proof by induction on the degree: the number of variations in the coefficients of $f(-x)$ bounds the number of negative roots.

Notions of Algebraic geometry

Introduction

Single polynomial

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

• 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.

Algebraic varieties

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

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

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

Examples.

- $V(x^2 + 1) = \{\pm\sqrt{-1}\}$,
- $V(\mathbb{Q}[x_1, \ldots, x_n]) = \emptyset$,
- $V(\emptyset) = \mathbb{C}^n$.

Properties.

- $S \subset T \Rightarrow V(T) \subset V(S)$

Dimension of a variety

Def. $\dim(V)$ = #degrees of freedom of V = #parameters for covering V

- $\dim(\text{point}) = 0$, $\dim(\text{line}) = 1$, $\dim(\text{surface}) = 2$.
- $\dim(V) = n \Leftrightarrow V = \mathbb{C}^n$.
- $\dim V(f_i) = n - 1$ generically.

Def. Dimension $\dim(V) := \max_C \{\dim(C) \ : \ \text{component } C \subset V\}$.

- $\dim(V) = 0 \Leftrightarrow V =$ point set (iff finite cardinality).
- $\dim(V) = 1 \Leftrightarrow V$ contains a curve (possibly straight line), may contain points, but no component of dim ≥ 2.
- $\dim(V) = 2 \Leftrightarrow V$ contains a surface (possibly planar), may contain 0-dim or 1-dim components, but no higher-dim component.

Algebraic varieties (cont'd)

System $f_1, \ldots, f_m \in K[x_1, \ldots, x_n]$.

- Well-constrained: $m = n$, generically 0-dim variety.
- Over-constrained: $m > n$, generically no roots (empty).
- Under-constrained: $m < n$, generically ∞ roots.

Lemma.

- $V(f_1, \ldots, f_m) = V(f_1) \cap \cdots \cap V(f_m) \subset \mathbb{C}^n$.
- $\dim(V \cap W) = \dim(V) -$ codim (W),

where $\operatorname{codim}(W) = n - \dim(W)$;
clearly, $\dim(V \cap W) = \dim(W) -$ codim (V).

E.g. $\mathbb{C}^2$: V, W =curves, $\dim(W \cap V) = 0$ (points).
E.g. $\mathbb{C}^3$: V, Wsurfaces, $\dim(W \cap V) = 1$ (curve).
E.g. $\mathbb{C}^3$: V =surface, W =curve, $\dim(W \cap V) = 0$.

$n \times n$ **linear system**

rank$(M) = r \leq n$:

- $r = n \Rightarrow \exists!$ solution.
- $r < n \Rightarrow$ system defined by r equations.

remaining equations trivial (0=0) implies ∞ roots.

existence of incompatible equation (0=b) implies no roots.

Hilbert's Nullstellensatz

Algebraic ideals

Given a polynomial ring $R = K[x_1, \ldots, x_n]$,

- a subring $S \subset R$ is closed under addition and multiplication: $a, b \in S \Rightarrow a + b, ab \in S$;
- an (algebraic) ideal $I \subset R$ is closed under addition and multiplication by any ring element: $a, b \in I, p \in R \Rightarrow a + b, ap \in I$.

E.g. $\langle x^2, x^5 \rangle = \langle x^2 \rangle$, $\langle x, x + y \rangle = \langle x, y \rangle$.

Fact. Given a set of polynomials, all elements in the generated (algebraic) ideal vanish at the set's variety.

Corollary. The ideal is the largest set of polynomials vanishing precisely at this variety.

Varieties vs Ideals

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

Properties.

- $J(\mathbb{C}^n) = \emptyset, J(\emptyset) = \mathbb{Q}[x]$,
- $X \subset Y \Rightarrow J(Y) \subset J(X)$,
- $X = V(J(X))$
- $S \subset J(V(S))$: when is it tight?
- Counter-example: $\langle x^2 \rangle \neq J(\{0\}) = \langle x \rangle$:

How do the roots of x and x^2 differ?

Hilbert's Nullstellensatz

Recall definition $J(X) := \{f \in \mathbb{Q}[x] \,:\, f(x) = 0, \forall x \in X \subset \mathbb{C}^n\}$.

Defn. Given an ideal I in a commutative ring R, its radical ideal is

$$\sqrt{I} := \{\, r \in R \,|\, r^n \in I,\ \exists\, n > 0\}.$$

Property. $I \subset \sqrt{I}$.

Intuition: taking the radical removes the multiplicities.

Eg. In ring $\mathbb{Z}$: $\sqrt{\langle 8 \rangle} = \langle 2 \rangle, \sqrt{\langle 12 \rangle} = \langle 6 \rangle,$

In a polynomial ring: $\sqrt{\langle x^3 \rangle} = \langle x \rangle, \sqrt{\langle x^2, x - 2y, y^3 \rangle} = \langle x, y \rangle.$

Hilbert's zeroes theorem. $\qquad J(V(I)) = \sqrt{I}.$

Specifies the algebra-geometry dictionary.

Polynomial Degree

Degree

Defn: (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. So, for every (affine) root $(x, y, z) \in \mathbb{C}^3$ there is now a (projective) root $(x : y : z : 1) \in \mathbb{P}^3$.

Intersection theory

Geometrically, $\deg f(x_1, \ldots, x_n)$ equals the number of intersection points of $f(x_1, \ldots, x_n) = 0$ with a generic line in $\mathbb{C}^n$.

Defn. The degree of a variety V is #points in the intersection of V with a generic linear subspace L of dimension = codim(V):

$$\deg V = \#(V \cap L) \ : \ \dim L = \mathrm{codim} V.$$

E.g. curve $V \subset \mathbb{C}^3$ defined by $f(x, y, z) = g(x, y, z)$. L is a generic plane.

Number of roots

Defn. The complex projective space $\mathbb{P}^n_{\mathbb{C}}$ or $\mathbb{P}^n$ or $\mathbb{P}(\mathbb{C})^n$ is the following 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 its common roots (counting multiplicities) in $\mathbb{P}(\overline{K})^n$ is bounded by

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

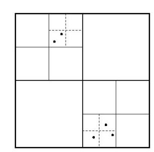
where $\deg(\cdot)$ is the polynomial's total degree.
The bound is exact for generic coefficients.
Note: The theorem considers dense polynomials.

Polynomial system solving

A perspective. . .  on La Boca

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 symbolic-numeric computation + exploit structure + continuity w.r.t. coefficients − high-dimensional components $O_b^*(d^n)$	Newton-like, optimization, discretization + simple, fast − local, may need initial point
	Gröbner bases + complete information − discontinuity w.r.t. coefficients dimension=0: $O_b^*(d^{n^2})$, else $O_b^*(d^{2^n})$ Characteristic sets dimension=0: $O_b^*(d^n)$, else $O_b^*(d^{n^2})$ Normal forms, boundary bases	Exclusion, interval, topological degree + simple, flexible, robust + focuses on given domain − costly for large n  $O_b^*(\log \frac{D}{\epsilon})$
	Straight-line programs express evaluation	Homotopy continuation + exploit structure − divergent paths

Resultants

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, $(\overline{K}^*)^n \subset X \subset \mathbb{P}^N$.

[van der Waerden, 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:

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

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 $\mathsf{MV}_{-i} = \prod_{j\neq i} \deg f_j$.

Matrix formulae

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

- Poisson formula.
- Determinantal from rational formula [Kaltofen-Koiran'08]

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

Resultant matrices

- $n = 1$: Bézout 1779, Sylvester 1840.

- Bézout: [Chtcherba-Kapur'00], [Kapur et.al], [Cardinal-Mourrain], [Busé et al.].

- Homogeneous: Macaulay, [GKZ'94], [Jouanolou'97], [D'Andrea-Dickenstein'01], [CoxMatera08], complexes [Eisenbud-Schreyer'03].

- Toric: [Canny-E'93], [E-Canny'93]*, generalized [Sturmfels'94], Jacobian [Cattani-Dickenstein-Sturmfels], [D'Andrea-E'01], complexes [Khetan'02], rational [D'Andrea'02], [E-Konaxis'09].

- m-homogeneous: Dixon, [GKZ], [Chionh-Goldman-Zhang98,ZG00], [Dickenstein-E'03, E-Mantzaflaris'09], [Awane-Chkiriba-Goze'05].

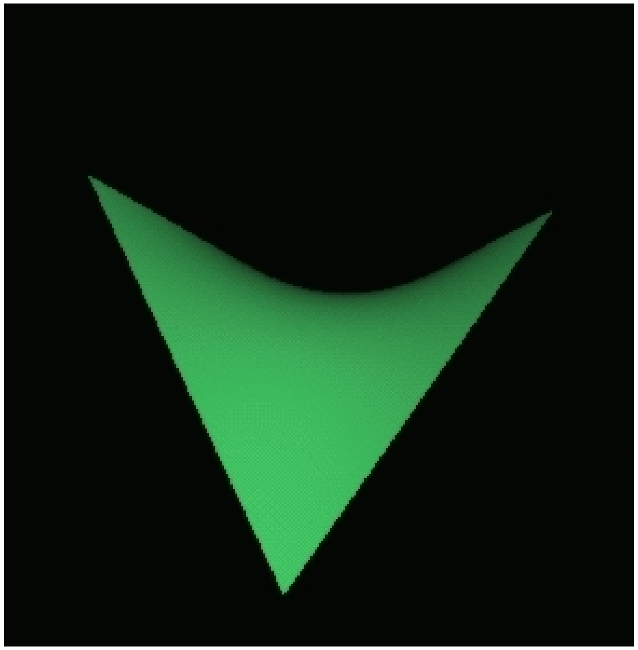
A bilinear example

Example: Bilinear surface

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

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

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



Modeling/CAD use parametric *AND* implicit/algebraic representations $\Rightarrow$ need to implicitize a (hyper)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:

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

Sparse elimination theory

Newton polytopes

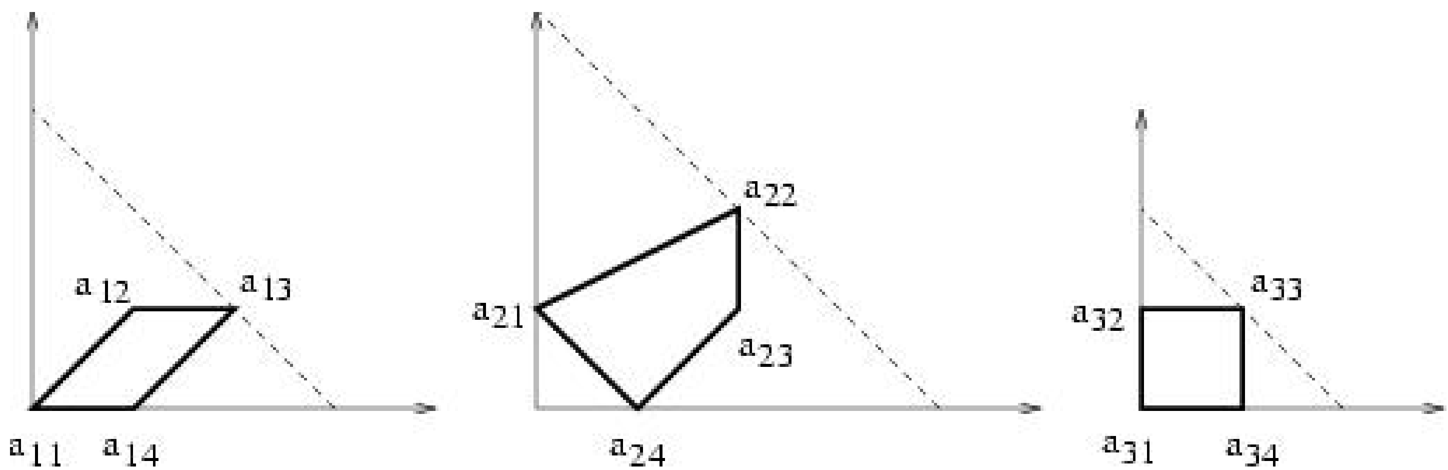
The support A_i of a polynomial $f_i \in K[x_1^{\pm 1}, \ldots, x_n^{\pm 1}]$, s.t.

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

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



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

Mixed Volume characterization

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

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 $\mathrm{MV}(Q_1, \ldots, Q_n)$ (irrespective of the variety's dimension).

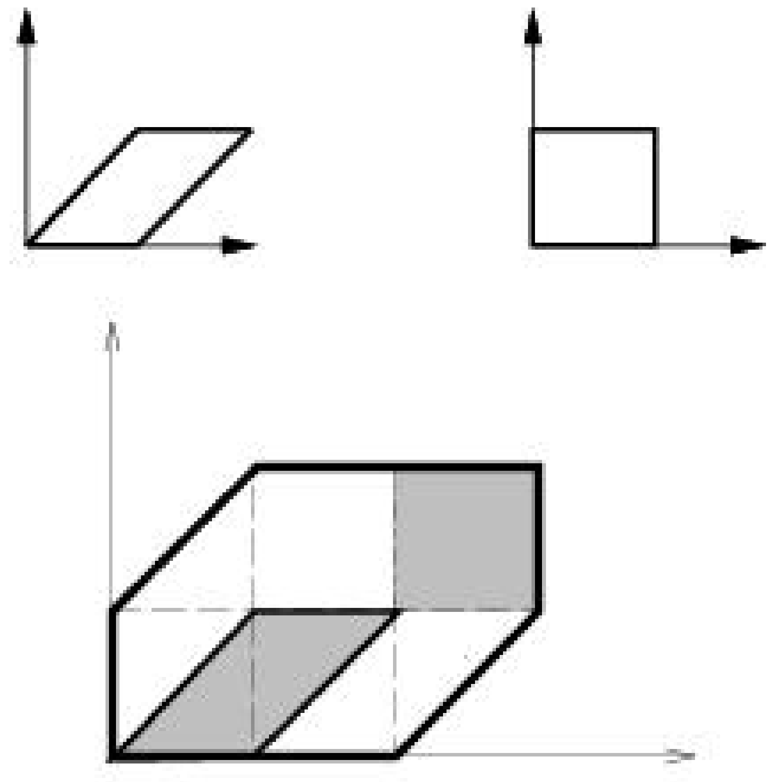
Dense homogeneous: $\mathrm{MV}(Q_1, \ldots, Q_n) = \prod_{i=1}^n d_i =$ Bézout's bound, where $d_i = \deg(f_i)$ and $Q_i = \text{simplex}\{0, (d_i, 0, \ldots, 0), \ldots, (0, \ldots, 0, d_i)\}$.

Dense multi-homogeneous: $\mathrm{MV}(Q_1, \ldots, Q_n) =$ 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 $\deg_{X_j} f_i = d_{ij}, j = 1, \ldots, r$, and X_j contains n_j variables.

Example: mixed subdivision for well-constrained problem



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).

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, $(\overline{K}^*)^n \subset X \subset \mathbb{P}^N$.

[van der Waerden, 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:

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

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

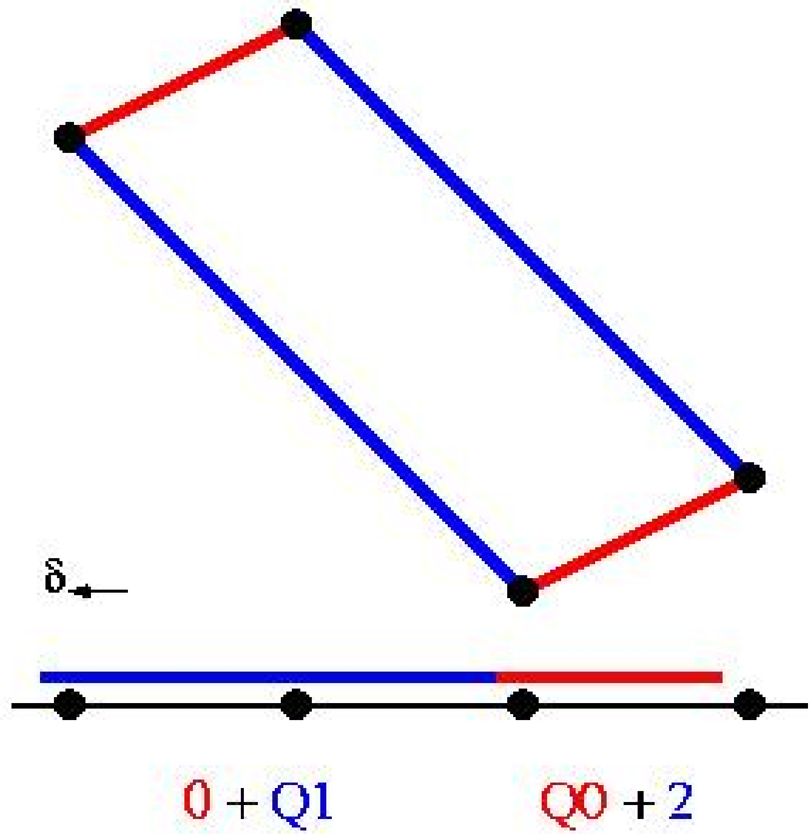
Generalizations

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 $\mathsf{MV}_{-i} = \prod_{j \neq i} \deg f_j$.

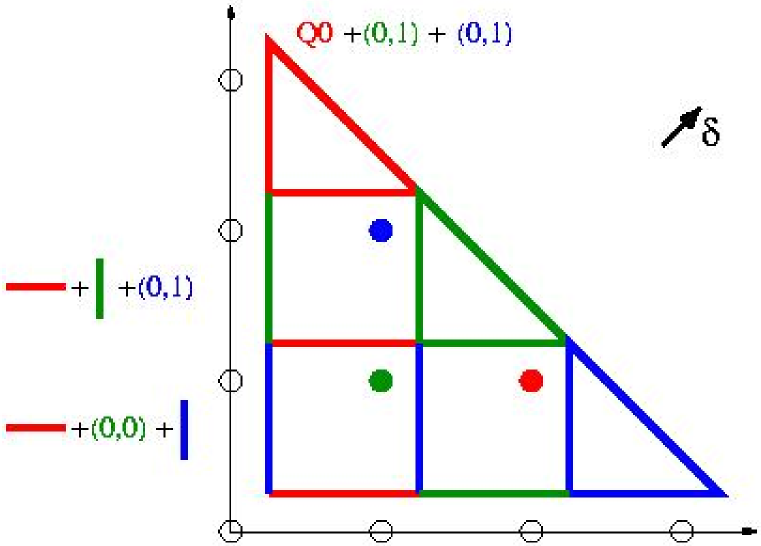
Lifting in the Sylvester case

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



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

Mixed subdivision of a linear system



$\mathrm{RC}(1,2) = [2,(0,1)]$ ie. $x_1x_2^2 \mapsto x^{(1,2)-(0,1)}f_2 = x^{(1,1)}f_2$
$\mathrm{RC}(1,1) = [1,(0,0)]$ ie. $x_1x_2 \mapsto x^{(1,1)-(0,0)}f_1 = x^{(1,1)}f_1$
$\mathrm{RC}(2,1) = [0,(1,0)]$ ie. $x_1^2x_2 \mapsto x^{(2,1)-(1,0)}f_0 = x^{(1,1)}f_0$

$$M = \begin{array}{c@{\quad}c} \begin{array}{ccc} x_1^2x_2 & x_1x_2^2 & x_1x_2 \end{array} & \\ \begin{bmatrix} c_{01} & c_{02} & c_{03} \\ c_{11} & c_{12} & c_{13} \\ c_{21} & c_{22} & c_{23} \end{bmatrix} & \begin{array}{c} x_1x_2f_0 \\ x_1x_2f_1 \\ x_1x_2f_2 \end{array} \end{array}$$

Example: subdivision-based matrix

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

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

$\dim M = 15$, greedy [Canny-Pedersen]: 14, incremental [E-Canny]: 12.

Mixed volumes $= 4, 3, 4 \Rightarrow \deg R_{tor} = 11$ while deg(classical resultant) $= 26$.

Polynomials of arbitrary support

Matrices of Sylvester-type

Algorithms: subdivision-based [Canny-E'93,'00], incremental [E-Canny'95] yield a square matrix M of the sparse/toric resultant, such that:

$$\det(M) \not\equiv 0,$$
$$R \mid \det(M),$$
$$\deg_{f_0} \det(M) = \deg_{f_0} R,$$

where R is the toric resultant.

Rational form [D'Andrea'02]: $R = \det(M)/\det(M')$,
where M' is a submatrix of M, generalizing Macaulay's construction.

Matrix construction [Canny,E'93,00]

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

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 $\text{RC}(p) = (i, F_i)$: 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. $\text{RC}(p) = (i, a_i)$.

Correctness

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

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 $q \in \mathrm{supp}(f_i)$.

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. $\mathrm{RC}(p) = (i, a_i)$.
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.

Incremental algorithm [E-Canny'95]

Idea: The 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 $\subset \sum_i Q_i$.

1. Sort $Q_{-i} \cap \mathbb{Z}^n$ on their distance $\text{dist}_v(\cdot)$ from the boundary of Q_{-i} along some vector $v \in \mathbb{Q}^n$.

2. Define the rows of M by points $B_i = \{b : \text{dist}_v(b) > \beta\}$, for bound $\beta \in \mathbb{R}$. The columns are indexed by $\cup_i \cup_{b \in B_i} \text{supp}(x^b f_i)$.

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 vector 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)

Unmixed multihomogeneous systems

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

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

A system is of type (l, d) iff all polynomials are of type (l, d).

[Sturmfels,Zelevinsky'94]. If $l_i = 1$ or $d_i = 1$, $\forall\, i$, then $\exists$ determinantal resultant formula i.e. $\det M = R$.
Type $(2, 1; 1, 1)$: $c_0 + c_1x_1 + c_2x_2 + c_3y_1 + c_4x_1y_1 + c_5x_2y_1$.

[Dickenstein,E'02] find minimum (non-optimal) Sylvester-type matrix; extended by [E-Mantzaflaris]
The incremental algorithm [E,Canny'95] constructs all these matrices.

Rational form

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):

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

Rational form: 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.

Open: $\exists$ single lifting yielding both numerator and denominator?
YES if $n = 2$, unmixed system, or sufficiently different Newton polytopes [E-Konaxis'11]

Bézout matrices

The 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 the Bezoutian 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 the Bezoutian matrix.
The dimension of the matrix is $O(e^n d^n)$, $d = \max\{\deg f_i\}$.

Polynomial system solving

Polynomial System Solving I

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

Construct resultant matrix $M(u)$ for $f_0, f_1, \ldots, f_n$. At root α, $u = -\sum r_i \alpha_i$,

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

If $\det M_{11} \neq 0$, 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) [Canny,Rouillier] 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

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

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 and 1-dimensional zero sets.

Complexity: single exponential in n.

Synaps/Mathemagix library: C++, fast univariate solvers (e.g. [E-Tsigaridas]), connections (GMP, MPFR, LAPACK, SparseLU etc).

Multiplication maps

Consider ideal $I := \langle p_1, \ldots, p_m \rangle \subset K[x_1, \ldots, x_n] = K[x]$,
and quotient ring $A_K := K[x]/I$.

Polynomial multiplication in A_K, ie. mod$I$, by some $a \in K[x]$, is a linear map:

$$M_a \ : \ K[x]/I \to K[x]/I \ : \ b \mapsto ab \ \text{ mod } I,$$

where ordered field $K \subset$ some real closed field.

Can compute M_a via Resultants, Gröbner bases, normal-form methods.

Software

Discrete geometry

- (Stable) Mixed Cells

Input: n polynomial supports in $\mathbb{Z}^n$ (well-constrained)

Output: Monomial basis of quotient,
generic number of roots in $(\overline{K}^*)^n, \overline{K}^n$,
starting system of sparse homotopy in $(\overline{K}^*)^n, \overline{K}^n$.

Code: Ansi-C.

Package: MMX (SYNAPS) and stand-alone.

Symbolic algebra

Input: $n+1$ polynomial supports in $\mathbb{Z}^n$ (over-constrained)
Output: Square toric resultant matrix, optimal size in specified polynomia

- Incremental algorithm

Features: Exact Sylvester-type matrix whenever possible
Code: Ansi-C.
Package: MMX (SYNAPS) or stand-alone.
Future work: Fast rank tests (quasi-Toeplitz matrices),
MMX (SYNAPS) sparse representations (superLU, Hewlett),
monomial set representation (+ arithmetic)

- Subdivision-based (greedy) algorithm

Features: Exact rational expression, allows linear perturbation.
Code: Maple.
Package: Multires or stand-alone.
Future work: Sparse / structured representations,
fast point-in-cell location (in implicit subdivision)

Numerical solving

- Polynomial system solving

Input: Polynomial supports and coefficients,
resultant matrix

Output: Superset of common roots

Features: Numerical linear algebra: LAPACK,
trade-off between speed and accuracy,
factors out constant submatrix: Schur factorization,
rank balancing of matrix polynomial,
regular or generalized eigenproblem.

Code: Ansi-C, some in Maple.

Package: Stand-alone.

Future work:

- MMX (SYNAPS) capabilities: Popov, quasi-Toeplitz structure, arithmetic.
- LAPACK capabilities: condition numbers, backward-error analysis.

Application: Geometric modeling

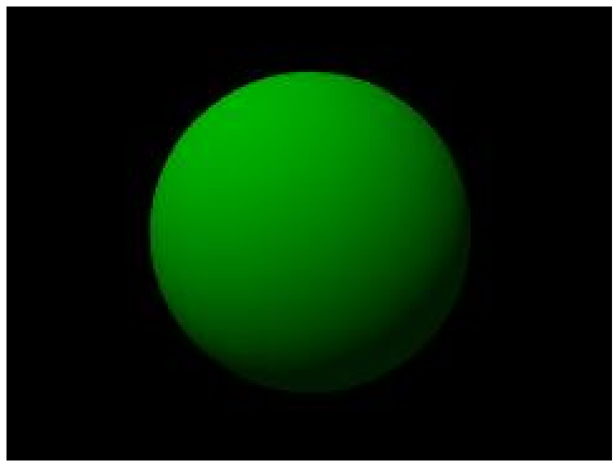
Implicitization of parametric surfaces

Example: sphere

The sphere in $\mathbb{R}^3$ is the set of values (x, y, z):

$$x = \frac{t_1^2 - t_2^2 - 1}{t_1^2 + t_2^2 + 1}, y = \frac{2t_1}{t_1^2 + t_2^2 + 1}, z = \frac{2t_1t_2}{t_1^2 + t_2^2 + 1}, \ t_1, t_2 \in [0, 1],$$

as well as the set of roots of $H(x, y, z) := x^2 + y^2 + z^2 - 1 = 0$.



Modeling/CAD use parametric *and* implicit/algebraic representations due to their complementary advantages. This is crucial in operations such as intersecting two surfaces. $\Rightarrow$ must implicitize a (hyper)surface given a (rational) parameterization

Implicitization of rational parametric surfaces

Given is a parametrization of a rational surface:

$$x_1 = \frac{p_1(t_1,t_2)}{p_0(t_1,t_2)},\ x_2 = \frac{p_2(t_1,t_2)}{p_0(t_1,t_2)},\ x_3 = \frac{p_3(t_1,t_2)}{p_0(t_1,t_2)}.$$

Homogenize the p_i $\theta : \mathbb{P}^2 \to \mathbb{P}^3 : (t_0 : t_1 : t_2) \mapsto (p_0 : p_1 : p_2 : p_3)$.

Problem: compute the smallest algebraic surface $H(x_1, x_2, x_3, x_0)$ containing $\overline{\mathrm{Im}(\theta)}$, including the case of base points $t \in \mathbb{P}^2 : p_i(t) = 0$.

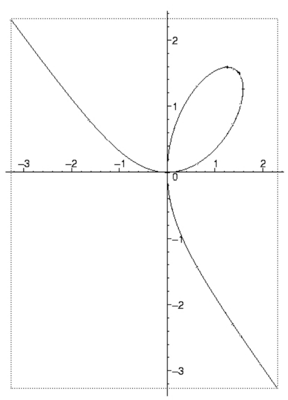
Methods: Gröbner bases, moving surfaces, resultant (perturbation, residual, Bezoutian), residue, Newton sums, numerical methods...

Implicitization examples

[Descartes' folium]

[1596-1650]

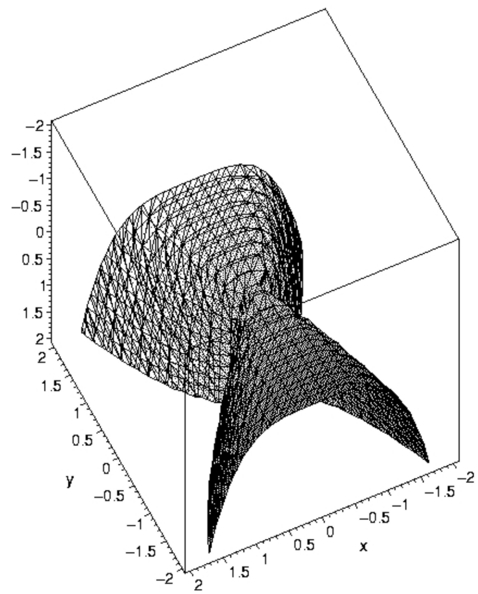
$$(x,y) = \left(\frac{3\ t^2}{t^3+1}, \frac{3\ t}{t^3+1}\right)$$



$$H = x^3 + y^3 - 3\ x\ y$$

[Buchberger'88]

$$(x,y,z) = (st, st^2, s^2)$$



$$H = x^4 - y^2 z$$

[Busé'01]

$$x = \frac{s^2}{s^3+t^3},$$

$$y = \frac{s^3}{s^3+t^3},$$

$$z = \frac{t^2}{s^3+t^3}$$

$$H = x^3 - 2x^3y + x^3y^2 - y^2z^3$$

Implicitization by linear algebra

$S =$ monomials forming (a superset of) the implicit support.
$C =$ unknown coefficients of implicit equation wrt S, $|C| = |S|$.

- $MC = \vec{0}$, where matrix M is $|S| \times |S|$, and contains values of S at points $(s_i, t_i), i = 1, \ldots, |S|$. Try roots of unity [Sturmfels-Tevelev-Yu'07].

- $(SS^T)C = \vec{0}$, substitute x, y, z by parametric expressions in $K[s,t]$, integrate over s, t; solve for C [Corless-Galligo-Kotsireas-Watt'01].
Example: supp$(H) \subset \{x^3y, x^3, x^3y^2, y^2z^3\}$, then

$$SS^T = \begin{bmatrix} x^6y^2 & x^6y & x^6y^3 & x^3y^3z^3 \\ x^6y & x^6 & x^6y^2 & x^3y^2z^3 \\ x^6y^3 & x^6y^2 & x^6y^4 & x^3y^4z^3 \\ x^3y^3z^3 & x^3y^2z^3 & x^3y^4z^3 & y^4z^6 \end{bmatrix} \Rightarrow C = \begin{bmatrix} -2 \\ 1 \\ 1 \\ -1 \end{bmatrix}.$$

- Approximate implicitization [Dokken].

Implicit Newton polytope

Consider parameterizations with fixed supports.

- Generic coefficients:

– Compute the resultant's Newton polytope, then specialize:
[E-Kotsireas'03] developed Maple code calling Topcom [Rambau];
[E-Konaxis-Palios'07] specify implicit Newton polygon for curves.
[E-Konaxis-Fysikopoulos-Penaranda'11] fast algorithm for projecting resultant polytope in high-dim.
– Tropical geometry for varieties of codim > 1.
For curves, specified implicit polygon [Sturmfels-Tevelev-Yu'07].

- Arbitrary coefficients:

– Implicit Newton polygon for curves:
[Dickenstein-Feichtner-Sturmfels'07] study tropical discriminants;
[D'Andrea-Sombra'07] use mixed fiber polytopes [Esterov-Khovanskii'07].

Voronoi / Apollonius diagrams

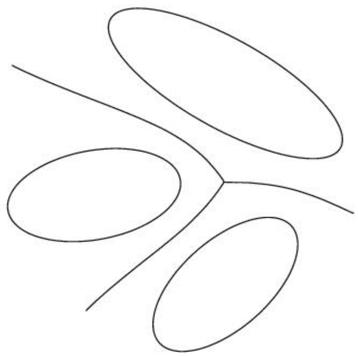
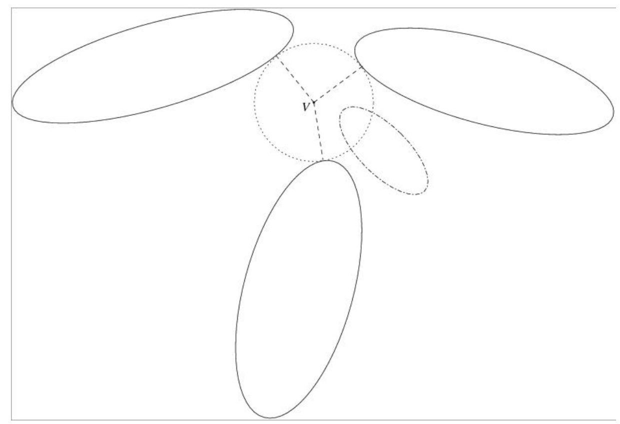
Apollonius diagrams

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

Nonlinear computational geometry considers circles, spheres, and ellipses. So, we refer to Apollonius diagrams.

Apollonius diagram of **green circles** [Karavelas-E'03], code in CGAL.

Apollonius diagram of ellipses

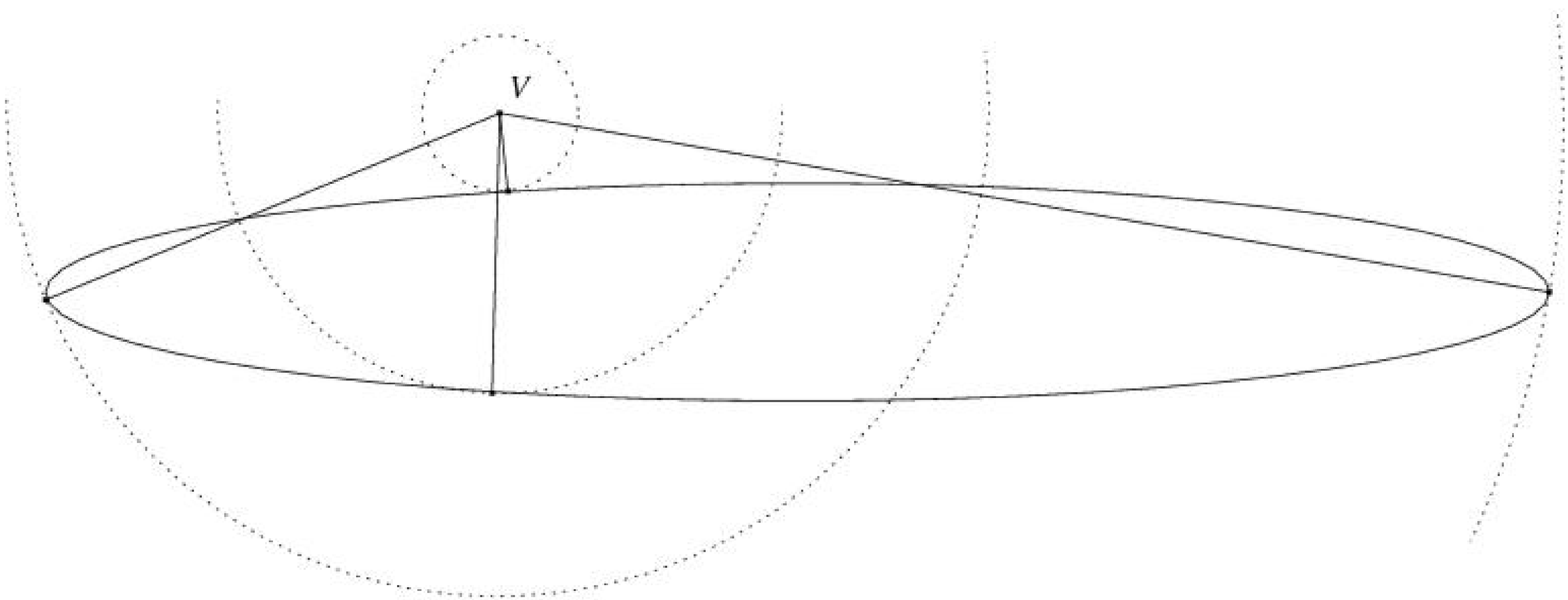



- Standard incremental algorithm.
- Problem: predicates, under Euclidean distance.
- For now: n disjoint ellipses.

- 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:

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

- Their pencil is $\lambda E + C(s)$,
- the characteristic polynomial is $\phi(s, \lambda) = |\lambda E + C(s)|$,
- and $\Delta(s)$ is ϕ's discriminant (wrt λ).

Comparing point-ellipse distances

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

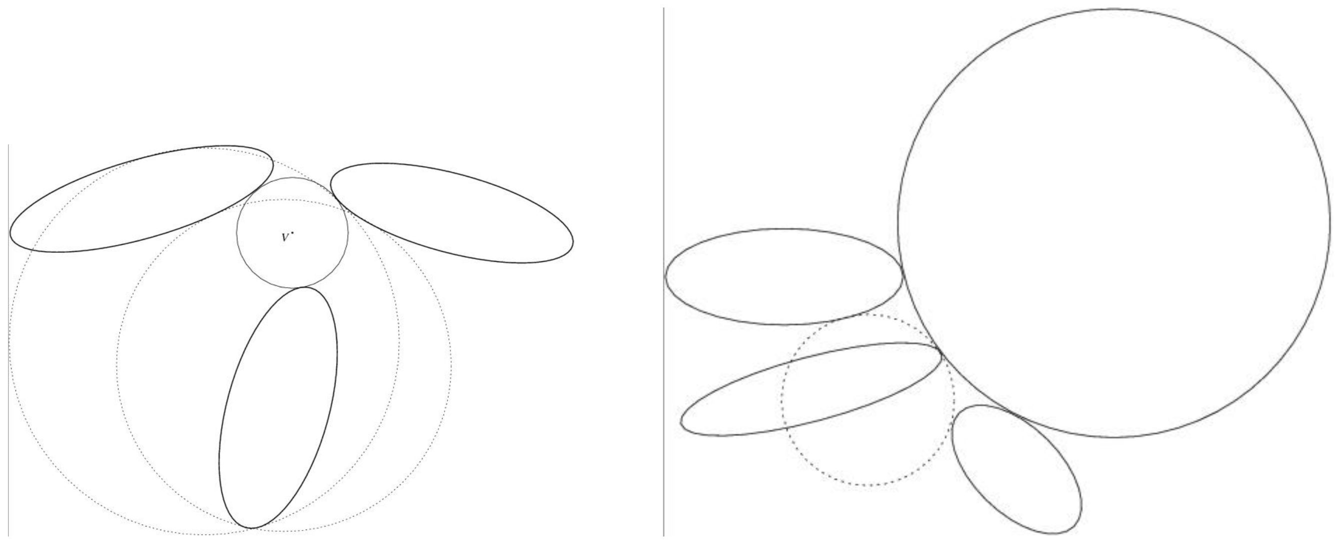
Given ellipse E and point v outside E, their distance is the square-root of the smallest positive root of the discriminant $\Delta(s)$.

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

Implemented in SYNAPS [E-Tsigaridas'04].

Apollonius circles

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



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

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

Arguments from real algebraic geometry yield same [Sottile].

Unmixed bivariate systems

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

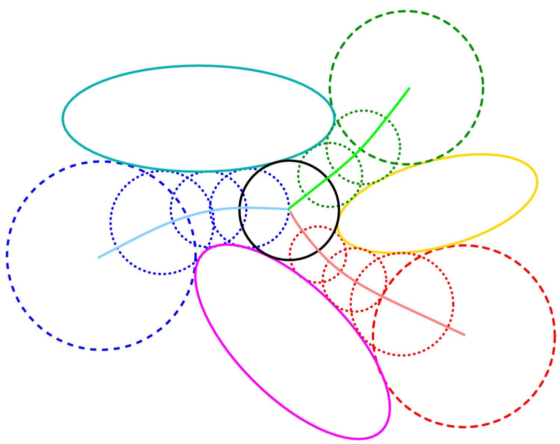
$\exists$ hybrid determinantal formula [Khetan'02]: $M = \begin{bmatrix} B & S \\ S^T & 0 \end{bmatrix}$

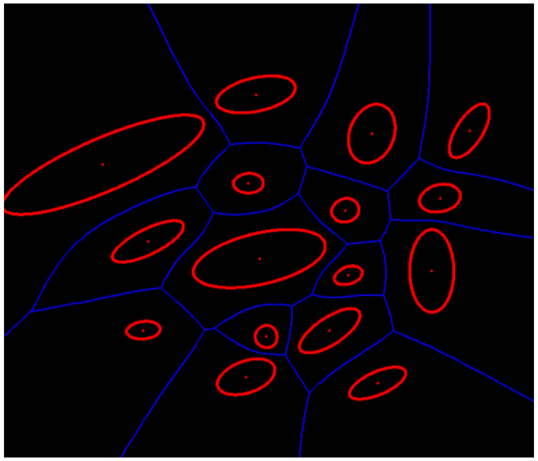
Eliminate $(v_1, v_2) \to 58 \times 58$ matrix with Sylvester and Bézout blocks:
sparse resultant $= \det(M)$, of degree 184 in q.

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 [E-Tsigaridas]
- Switch representation: implicit, parametric





- Geometric CGAL C++ software relying on algebra (Synaps, NTL).
- About 1sec per non-intersecting ellipse
- 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]

Parallel robots

Robot kinematics

Forward Kinematics: Compute all displacements for given configuration.
Easy/hard for serial/parallel robots respectively.

Inverse Kinematics: Compute all configurations that result to given translation – rotation (displacement).
Hard/easy for serial/parallel robots resp.

Parallel robots

Advantages: precision, rigidity, manipulation, force.
Examples: micro-surgery, flight simulation, heavy-duty objects etc.

Forward kinematics of Stewart platform: "The major outstanding problem in all of manipulator direct and inverse kinematics" [Roth93].
Configuration defined by the lengths of 6 articulations, system of 6 to 10 equations, ≤ 40 real solutions.

Stewart platform

Two rigid bodies connected with 6 sliding joints rotating freely at attachments: parallel mechanism.
Forward kinematics: Given joint lengths, compute pose of platform.

Rotation/translation/attachment quaternions $\dot{q}, \dot{t}, \dot{a}_i, \dot{a}'_i$

$$(-\dot{a}_i + \dot{t} + \dot{q}\dot{a}'_i\dot{q}^*)^T(-\dot{a}_i + \dot{t} + \dot{q}\dot{a}'_i\dot{q}^*) = L_i^2, \qquad i = 1, \ldots, 6.$$

Bézout bound $= 256$, $m-$Bézout $= 144$.
Exact bound $= 40$ [Ronga-Vust'92] [Mourrain'93] [Husty'94].
Can have 40 real solutions) [Dietmaier'98].

6×6 original system has MV$= 160$.
7×7 system with $\dot{x} = \dot{q}^* \dot{t}$ has MV$= 84$, deg $R_{tor} = 214$, dim $M = 405$.
10×10 system with $y_0 = \|\dot{q}\|^2, \dot{z} = \dot{q}^*\dot{t}\dot{q}$, has MV$= 54$.