Polyhedral Methods to find Common Factors of Algebraic Plane Curves

Jan Verschelde
in collaboration with Danko Adrovic

University of Illinois at Chicago
Department of Mathematics, Statistics, and Computer Science
http://www.math.uic.edu/~jan
jan@math.uic.edu

JMM AMS-MAA 2009 – AMS Special Session on Computational Algebraic and Analytic Geometry for Low-dimensional Varieties.
Washington DC, Tuesday 6 January 2009.

Problem Statement & Motivation

Input: two polynomials f and g in two variables x and y
with ***approximate*** complex coefficients.

Output: decide if f and g have a common factor, ***and***
provide certificates for the decision.

Why bother?

1. development of reliable blackbox polynomial system solver
computing isolated solutions and common factors
2. related to factorization in symbolic-numeric computing
computing a numerical greatest common divisor
3. tropical algebraic geometry as a source of inspiration
computing with polygons spanned by exponents (exact data)

Some Related Work

- T. Bogart, A.N. Jensen, D. Speyer, B. Sturmfels, and R.R. Thomas. **Computing tropical varieties.** *J. Symbolic Comput.* 42(1):54–73, 2007.
- G. Chèze and A. Galligo. **Four lectures on polynomial absolute factorization.** In *Solving Polynomial Equations. Foundations, Algorithms and Applications*, pages 339–394. Springer–Verlag, 2005.
- S. Gao and A.G.B. Lauder. **Decomposition of polytopes and polynomials.** *Discrete Comput. Geom.*, 26(1):89–104, 2001.
- A.N. Jensen, H. Markwig, and T. Markwig. **An algorithm for lifting points in a tropical variety.** *Collectanea Mathematica*, 59(2), 2008.
- E. Kaltofen, J.P. May, Z. Yang, and L. Zhi. **Approximate factorization of multivariate polynomials using singular value decomposition.** *J. Symbolic Comput*, 43(5):359–376, 2008.
- A. Poteaux and M. Rybowicz. **Towards a symbolic-numeric method to compute Puiseux series: the modular part.** `arXiv:0803.3027v1 [cs.SC] 20 Mar 2008`.

A Short Summary

When do two polynomials have a common factor?

- Key idea: if common factor, then common root at infinity.

  In the language of tropical algebraic geometry we can say

  tropisms give the germs to grow
  the tentacles of the common amoeba

- The cost of the preprocessing algorithm is cubic in the number of monomials in the worst case.

- Exploratory calculations with Maple:
  1. using `ConvexHull` for normal fan & tropisms,
  2. compute terms of Puiseux series using `subs`.

  SAGE components Singular and Gfan would work just as well.

Outline

1. Newton polygons and tropicalizations
   - tropical prevarieties and tropicalizations
   - tropisms and initial roots

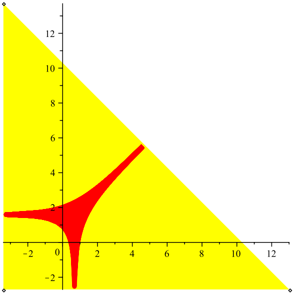
2. Puiseux series
   - a preprocessing algorithm
   - the second term in the Puiseux series

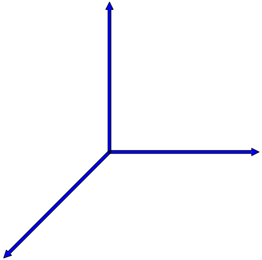
Amoebas and Normal Fans

an asymptotic view on algebraic varieties

Definition (Gel'fand, Kapranov, and Zelevinsky 1994)

The ***amoeba*** of a variety is its image under the map log:
$(\mathbb{C}^*)^2 \rightarrow \mathbb{R}^2 : (x, y) \mapsto (\log(|x|), \log(|y|))$, $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$.

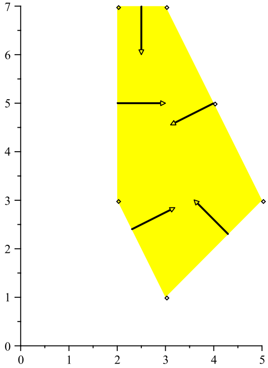


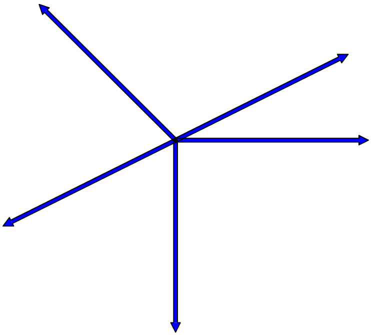


The tentacles of the amoeba are encoded in the inner normals,
i.e.: vectors perpendicular to the edges of the Newton polytope.

Inner Normals represent Tentacles

$$f := x^3y + x^2y^3 + x^5y^3 + x^4y^5 + x^2y^7 + x^3y^7$$



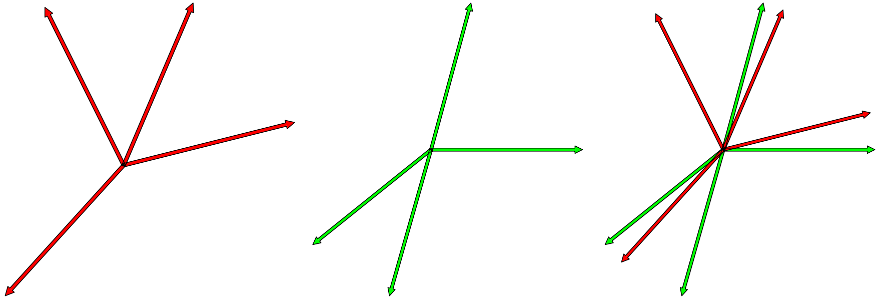


The collection of inner normals to the edges of the Newton polygon forms ***a tropicalization*** of f.

No Common Factor

implied by polygons in general position

Tropicalized two random polynomials of degree 15



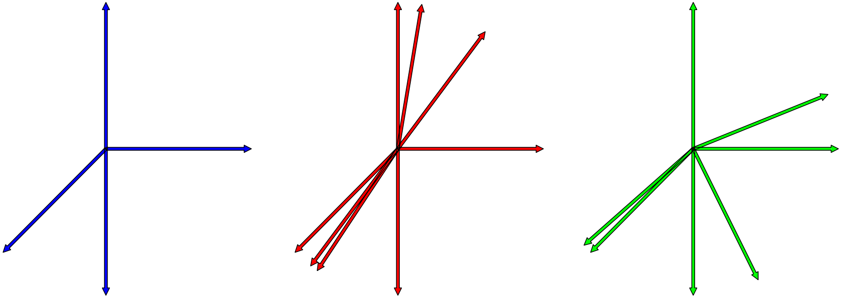
For nonzero coefficients, there can be no common factor.

Consequence of Bernshteĭn's second theorem (1975).

There is a Common Factor

Generated a factor of degree 5
and multiplied with two random polynomials of degree 10.

Tropicalization of the factor and the two polynomials:



Observe the common tentacles in the tropicalizations.

a Tropicalization of a Polynomial

Definition

Let P be the Newton polygon of f. Denote the inner product by $\langle \cdot, \cdot \rangle$.

The ***normal cone to a vertex*** p ***of*** P is $\{ \, v \neq 0 \mid \langle p, v \rangle = \min_{q \in P} \langle q, v \rangle \, \}$.

The ***normal cone to an edge spanned by*** p_1 ***and*** p_2 is

$$\{ \, v \neq 0 \mid \langle p_1, v \rangle = \langle p_2, v \rangle = \min_{q \in P} \langle q, v \rangle \, \}.$$

Normal cones to edges of P define ***a tropicalization of*** f***:*** $\mathrm{Trop}(f)$.

Proposition (first preprocessing step)

If $\mathrm{Trop}(f) \cap \mathrm{Trop}(g) = \emptyset$*, then* f *and* g *have no common factor.*

Consequence of Bernshteǐn's second theorem (1975).

Tropisms and Initial Forms

Definition (adapted from Joseph Maurer, 1980)

Let P and Q be Newton polygons of f and g respectively. A ***tropism*** is a vector perpendicular to one edge of P and one edge of Q.

The edges perpendicular to a tropism are Newton polytopes of *an initial form system* which may have roots in $(\mathbb{C}^*)^2$, $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$.

Definition

Consider $f = \sum_{(i,j) \in A} c_{i,j} x^i y^j$. Let (u, v) be a direction vector, and $m = \min\{ \langle (i,j), (u,v) \rangle \mid (i,j) \in A \}$.

The ***initial form of f in the direction (u, v)*** is

$$\mathrm{in}_{(u,v)}(f) = \sum_{\substack{(i,j) \in A \\ \langle (i,j),(u,v) \rangle = m}} c_{i,j} x^i y^j .$$

Initial Roots

An initial root is a solution of an initial form system.

Simplest case: Newton polytope of initial form system is an edge.

Proposition (second preprocessing step)

If for all $(u, v) \in \mathrm{Trop}(f) \cap \mathrm{Trop}(g)$*, the initial form system*

$$\left\{ \begin{array}{c} \mathrm{in}_{(u,v)}(f)(x,y) = 0 \\ \mathrm{in}_{(u,v)}(g)(x,y) = 0 \end{array} \right.$$

has no solution in $(\mathbb{C}^*)^2$*, then* f *and* g *have no common factor.*

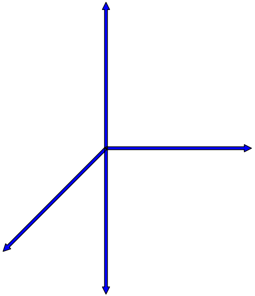
An initial root is where the common factor meets infinity.

For general factors, an initial root is the first coefficient of a Puiseux series expansion starting at infinity.

Where Tentacles meet Infinity

For example, the factor common to f and g is

$$r = 2xy + x^2y + 9xy^2 + 7x^3y + x^4y + 9x^3y^2.$$



Investigate 4 directions, take $(1,0)$:

$$\mathrm{in}_{(1,0)}(r) = 2xy + 9xy^2$$

Initial forms of f and g:

$$\mathrm{in}_{(1,0)}(f) = 55xy^6 + 10xy^5 + 45xy^7$$
$$\mathrm{in}_{(1,0)}(g) = 10xy^6 + 45xy^7$$

$\mathrm{in}_{(1,0)}(f) = 5xy^5(y+1)(2+9y)$ and $\mathrm{in}_{(1,0)}(g) = 5xy^5(2+9y)$
$\Rightarrow y = -2/9$ represents common root at (toric) infinity

Unimodular Transformations

Investigating the direction $(-1,-1)$:

$$\left\{ \begin{array}{rcl} \mathrm{in}_{(-1,-1)}(f)(x,y) & = & 54x^{13}y^2 + 6x^{14}y \\ \mathrm{in}_{(-1,-1)}(g)(x,y) & = & 72x^9y^{10} + 8x^{10}y^9 \end{array} \right.$$

Change coordinates using a unimodular matrix $\begin{bmatrix} -1 & -1 \\ 0 & -1 \end{bmatrix}$.

Substitute $x = X^{-1}$, $y = X^{-1}Y^{-1}$:

$$\left\{ \begin{array}{rcl} \mathrm{in}_{(-1,-1)}(f)(X,Y) & = & (54Y+6)/(X^{15}Y^2) \\ \mathrm{in}_{(-1,-1)}(g)(X,Y) & = & (72Y+8)/(X^{19}Y^{10}) \end{array} \right.$$

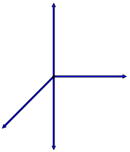
$\Rightarrow Y = -1/9$ represents common root at infinity, going back:

$$\left\{ \begin{array}{l} X = t \\ Y = -1/9 \end{array} \right. \quad \left(\begin{array}{l} x = X^{-1} \\ y = X^{-1}Y^{-1} \end{array} \right) \quad \Rightarrow \quad \left\{ \begin{array}{l} x = t^{-1} \\ y = -9t^{-1}. \end{array} \right.$$

Degrees of the Tentacles

$$r = 2xy + x^2y + 9xy^2 + 7x^3y + x^4y + 9x^3y^2$$

The amoeba for r has four tentacles. A tropicalization is



$$\{\, (1,0), (0,1), (-1,-1), (0,-1) \,\}.$$

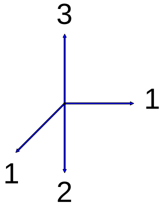
(u,v)	$\text{in}_{(u,v)}(r)$	degree
$(1,0)$	$2xy + 9xy^2$	1
$(0,1)$	$2xy + x^2y + 7x^3y + x^4y$	3
$(-1,-1)$	$x^4y + 9x^3y^2$	1
$(0,-1)$	$9xy^2 + 9x^3y^2$	2

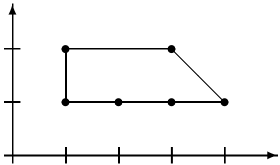
Count the number of nonzero solutions of the initial forms, after a proper unimodular coordinate transformation.

Orientation of the Normals

$$
\begin{aligned}
r &= 2xy + x^2y + 9xy^2 + 7x^3y + x^4y + 9x^3y^2 \\
&= xy(2 + x + 9y + 7x^2 + x^3 + 9x^2y)
\end{aligned}
$$

The factors $x = 0$ and $y = 0$ are trivial, r has degree 3.





The degree of r in x is 3, but r is linear in y.
Switch the normal form representation of the Puiseux series:

$$
\left\{
\begin{array}{l}
x = c_1 + c_2 t^w, \quad c_1, c_2 \in \mathbb{C}^*, w > 0 \\
y = t
\end{array}
\right.
\qquad as\ t \to 0.
$$

Only the normal (0,1) matters. Alternatively, $(-1,-1)$ and $(0,-1)$ contribute respectively 1 and 2 roots at infinity.

Computing a Series Expansion

finding a certificate for a regular common factor

tropicalization

compute tropisms

no tropism

$\Rightarrow$ no root at ∞

solve initial forms

no root at ∞

$\Rightarrow$ no series

compute 2nd term

no series

$\Rightarrow$ no curve

series

Four Steps in the Algorithm

Computations on **exact** and **approximate** data are interlaced:

1. **intersect normal fans**: $T = \mathrm{Trop}(f) \cap \mathrm{Trop}(g)$ (upper hulls)
   cost: $O(m_f \log(m_f)) + O(m_g \log(m_g))$, $m_h = \#\text{monomials}(h)$
2. for every tropism $(u, v) \in T$: **solve initial form system**
   transform $\mathrm{in}_{(u,v)}(f)$ and $\mathrm{in}_{(u,v)}(g)$ into univariate polynomials
   cost in worst case: $O((m_f + m_g)^3)$ via SVD on coefficients
3. **compute power of second term** in the Puiseux series
   impose pure lexicographic order on $\mathrm{in}_{(1,0)}(f)$, $\mathrm{in}_{(1,0)}(g)$
   and search for monomials with matching powers in x
   cost: $O(m_f \log(m_f)) + O(m_g \log(m_g))$, $m_h = \#\text{monomials}(h)$
4. **solve linear system** in c to find coefficient c of second term

the second term in the Puiseux series

After unimodular coordinate transformation:

$$\left\{ \begin{array}{l} x = t \\ y = c_0 + c_1 t^w \end{array} \right. \qquad \begin{array}{l} (1,0) \text{ is tropism} \\ c_0 \in \mathbb{C}^* \text{ is initial root} \end{array} \qquad \begin{array}{l} \text{unknown are } w \text{ and } c_2 \\ w \in \mathbb{N} \setminus \{0\}, c_1 \in \mathbb{C}^* \end{array}$$

We examine three examples:

$$\left\{ \begin{array}{l} f = r(1 + \alpha x^2 y^4) \\ g = r(1 + \beta x^4 y^2) \end{array} \right. \qquad \begin{array}{ll} (1) & r = 1 - y^7 + xy^3 \\ (2) & r = 1 - y + x^7 y^3 \\ (3) & r = 1 - y^7 + x^7 y^3 \end{array}$$

$$\alpha, \beta \in \mathbb{C}^*$$

The coefficients α and β are random numbers.

Because the tropism is $(1,0)$, the initial form is a polynomial in y.

first example: $r = 1 - y^7 + xy^3$

$$\begin{cases} x = t \\ y = 1 + c_1 t^w \end{cases}$$

$(1,0)$ is tropism
1 is initial root

unknown are w and c_2
$w \in \mathbb{N} \setminus \{0\}, c_1 \in \mathbb{C}^*$

Impose a pure lexicographic order on the monomials:

$$\begin{cases} f = 1 - y^7 + xy^3 + \alpha_{2,4}x^2y^4 + \alpha_{2,11}x^2y^{11} + \alpha_{3,4}x^3y^7 \\ g = 1 - y^7 + xy^3 + \beta_{4,2}x^4y^2 + \beta_{4,9}x^4y^9 + \beta_{5,2}x^5y^5 \end{cases}$$

Obviously xy^3 is the first match after the initial form, so try $w = 1$.

Substitute $(x = t, y = 1 + c_1 t)$ and select terms in t:

$$\begin{cases} -7c_1 + 1 = 0 \\ -7c_1 + 1 = 0 \end{cases} \quad \text{so: } c_1 = \frac{1}{7}.$$

Substitution of $(x = t, y = 1 + t/7)$ gives $O(t^3)$ as lowest order term.

second example: $r = 1 - y + x^7y^3$

$$\left\{\begin{array}{l} x = t \\ y = 1 + c_1 t^w \end{array}\right. \qquad \begin{array}{l} (1,0) \text{ is tropism} \\ 1 \text{ is initial root} \end{array} \qquad \begin{array}{l} \text{unknown are } w \text{ and } c_2 \\ w \in \mathbb{N} \setminus \{0\}, c_1 \in \mathbb{C}^* \end{array}$$

Impose a pure lexicographic order on the monomials:

$$\left\{\begin{array}{l} f = 1 - y + \alpha_{2,4}x^2y^4 + \alpha_{2,5}x^2y^5 + x^7y^3 + \alpha_{9,4}x^9y^7 \\ g = 1 - y + \beta_{4,2}x^4y^2 + \beta_{4,3}x^4y^3 + x^7y^3 + \beta_{11,2}x^{11}y^5 \end{array}\right.$$

The first term with matching exponent in x is x^7y^3, so try $w = 7$.

Substitute $(x = t, y = 1 + c_1t^7)$ and select terms in t^7:

$$\left\{\begin{array}{l} -c_1 + 1 = 0 \\ -c_1 + 1 = 0 \end{array}\right. \qquad \text{so: } c_1 = 1.$$

Substitution of $(x = t, y = 1 + t^7)$ gives $O(t^{14})$ as lowest order term.

third example: $r = 1 - y^7 + x^7y^3$

$$\left\{ \begin{array}{l} x = t \\ y = 1 + c_1 t^w \end{array} \right.$$

$(1,0)$ is tropism
1 is initial root

unknown are w and c_2
$w \in \mathbb{N} \setminus \{0\}, c_1 \in \mathbb{C}^*$

Impose a pure lexicographic order of the monomials:

$$\left\{ \begin{array}{l} f = 1 - y^7 + \alpha_{2,4}x^2y^4 + \alpha_{2,11}x^2y^{11} + x^7y^3 + \alpha_{9,4}x^9y^7 \\ g = 1 - y^7 + \beta_{4,2}x^4y^2 + \beta_{4,9}x^4y^9 + x^7y^3 + \beta_{11,2}x^{11}y^5 \end{array} \right.$$

The first term with matching exponent in x is x^7y^3, so try $w = 7$.

Substitute $(x = t, y = 1 + c_1t^7)$ and select terms in t^7:

$$\left\{ \begin{array}{l} -7c_1 + 1 = 0 \\ -7c_1 + 1 = 0 \end{array} \right. \qquad \text{so: } c_1 = 1/7.$$

Substitution of $(x = t, y = 1 + t^7/7)$ gives $O(t^{21})$ as lowest order term.

the exponent of the second term

Proposition (third preprocessing step)

Using the tropism (u,v) we can write f and g as (plex order)

$$\left\{ \begin{array}{l} f = \mathrm{in}_{(1,0)}(f) + O(x) = \alpha_{0,0} + \alpha_{0,a_1} y^{a_1} + \cdots + \alpha_{p_1,k} x^{p_1} y^k + \cdots \\ g = \mathrm{in}_{(1,0)}(g) + O(x) = \beta_{0,0} + \alpha_{0,b_1} y^{b_1} + \cdots + \beta_{q_1,l} x^{q_1} y^l + \cdots \end{array} \right.$$

If f and g have no monomial with $w = \frac{p_1}{a_1} = \frac{q_1}{b_1}$ then f and g have no common factor.

With the tropism $(1,0)$ the Puiseux series has the form

$$\left\{ \begin{array}{l} x = t \\ y = c_0 + t^w(c_1 + O(t)) \end{array} \right. \quad \text{with } c_0 \in \mathbb{C}^* : \quad \left\{ \begin{array}{l} \mathrm{in}_{(1,0)}(f)(c_0) = 0 \\ \mathrm{in}_{(1,0)}(g)(c_0) = 0. \end{array} \right.$$

Substituting $(x = t, y = c_0 + c_1 t^w)$ and looking for lowest powers of t: c_0 neutralizes powers of y in terms in $f - \mathrm{in}_{(1,0)}(f)$ and in $g - \mathrm{in}_{(1,0)}(g)$.

the coefficient of the second term

Proposition (fourth preprocessing step)

If for all $w = \frac{p_1}{a_1} = \frac{q_1}{b_1}$ *from*

$$\left\{ \begin{array}{l} f = \alpha_{0,0} + \alpha_{0,a_1} y^{a_1} + \cdots + x^{p_1}(\alpha_{p_1,k_1} y^{k_1} + \alpha_{p_1,k_2} y^{k_2} + \cdots) + O(x^{p_1+1}) \\ g = \beta_{0,0} + \alpha_{0,b_1} y^{b_1} + \cdots + x^{q_1}(\beta_{q_1,l_1} y^{l_1} + \beta_{q_1,l_2} y^{l_2} + \cdots) + O(x^{q_1+1}) \end{array} \right.$$

the linear system in c_1

$$\left\{ \begin{array}{r} a_1 \alpha_{0,a_1} c_1 + \alpha_{p_1,k_1} c_0^{k_1} + \alpha_{p_1,k_2} c_0^{k_2} + \cdots = 0 \\ b_1 \beta_{0,b_1} c_1 + \beta_{q_1,l_1} c_0^{l_1} + \beta_{q_1,l_2} c_0^{l_2} + \cdots = 0 \end{array} \right.$$

has no solution $c_1 \in \mathbb{C}^*$*, then* f *and* g *have no common factor.*

Substituting $(x = t, y = c_0 + c_1 t^w)$ into $\{f, g\}$ and selecting the terms with the lowest powers of t defines the linear system in c_1.

Concluding Remarks

We can detect common factors while gradually computing partial data:

- exact data: exponents of initial forms, second exponent in series,
- approximate data: initial roots, second coefficient in series,

via a preprocessing algorithm in four steps (prototype in Maple), with reductions to polynomials in one variable.

Still to do:

- an implementation which returns condition numbers
- use sparse interpolation to recover the factor
- apply deflation to deal with singular curves
- generalize to space curves defined by general systems