

CIMPA research school

Algebraic and Tropical Methods for Solving Differential Equations

Notes by The Students

please edit this document with your contributions!

June 28, 2023

Contents

Mathematica notebook and other resources	2
1 Tropical Geometry	3
1.1 Tropical Algebra	3
1.2 One variable polynomials	3
1.3 Two variables	6
1.4 Tropicalization	7
1.5 Enumerative Geometry	8
1.6 Matroids	8
1.7 Three examples (extra)	10
1.8 Benoit's talk on Real tropical geometry	12
1.9 An exercise on tropical geometry	13
1.10 Open problems	16
2 Computational commutative algebra	18
2.1 Univariate polynomials and resultants	18
2.1.1 Univariate polynomials	18
2.1.2 Solving bivariate polynomial systems	19
2.2 Ideals and varieties	20
2.2.1 Operations on ideals	22
2.2.2 Hilbert's Nullstellensatz	22
2.2.3 From geometry to algebra	22
2.2.4 Radical membership	23
2.3 Gröbner bases	24
2.3.1 Principal ideals	24
2.3.2 Monomial orderings	24

2.3.3	Polynomial division	25
2.3.4	Gröbner Bases	26
2.3.5	Applications of Gröbner Bases	27
2.4	Elimination theory	27
2.4.1	Saturation of ideals	28
2.5	Exercises	28
3	Differential Algebra	30
3.1	Differential polynomial rings and related notions	30
3.2	Rankings	30
3.3	Decomposition of Perfect Differential Ideals	31
3.4	Triangular sets and regular chains	32
3.5	Zero testing	32
3.6	Root separation bound	33
3.7	Counting solutions of differential equations	34
3.8	Respresentation of differential equations	35
3.9	Finding solutions	36
3.9.1	Rational solutions	36
3.9.2	Algebraic solutions	37
3.9.3	Local solutions	37
3.10	(Extra) Another view of Tropical Geometry	38
3.11	Problems on algebraic differential equations	39
3.12	Exercises	39
4	Tropical Differential Algebra	41
4.1	Tropical Differential Algebraic Geometry	42
4.2	Twisted evaluation actions	43
4.3	Combinatorics	43
4.4	An application of the lema	44
4.5	Exercises	45
5	Newton's Method	46
5.1	Excercises	49
6	References	52

Mathematica notebook and other resources

Here's a Mathematica notebook with the figures so far:

- Wolfram Cloud
- Google Drive (This may not be updated)

Did anyone work with other software?

If you are looking at a pdf, you may want to see and edit these notes **online**.

1 Tropical Geometry

Lucía López de Medrano.

For an introduction on these ideas, see [brugall2014bit].

1.1 Tropical Algebra

Let us define an operation for $a, b \in \mathbb{R}$:

$$a + b = \max\{a, b\}$$

So every element is idempotent, that is, $a + a = a$ for all a . Notice we cannot have a zero element, for there is no element e such that $a + e = a$ for all a . So we must work on the set $\mathbb{T} = \mathbb{R} \cup \{-\infty\}$.

And the product will be ordinary sum:

$$a \cdot b = a + b$$

We must also establish that $a \cdot -\infty = -\infty$ and $(-\infty) \cdot (-\infty) = -\infty$. This makes $(\mathbb{T}, +, \cdot)$ a semiring called the Tropical Semiring.

(Maybe see these related ideas in the differential algebra course)

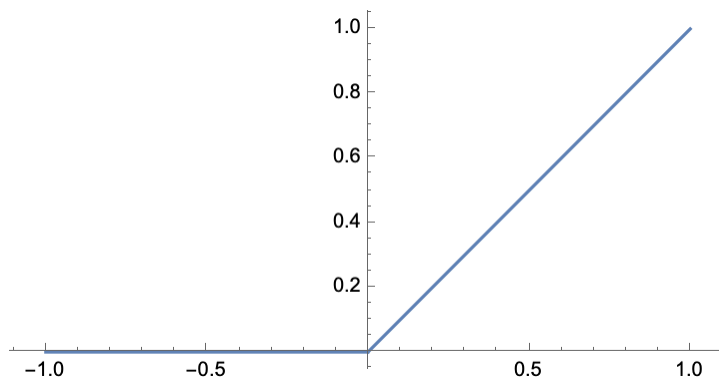
1.2 One variable polynomials

Notice these operations turn usual polynomials into linear equations:

$$\begin{aligned} "x^2" &= "xx" = 2x \\ "x^2 + y^3" &= "xyyy" = 2x + 3y \end{aligned}$$

We write with comas polynomials with usual operations.

Example 1. " $x + 0$ " = $\max\{x, 0\}$ is a piecewise linear function with a singularity at 0.



Example 1

Definition (Root). $r \in \mathbb{R}$ is a root of a polynomial f if we can write

$$f(x) = \sum_{i=0}^d c_i x^i = \max_{i=0}^d \{c_i + ix\}$$

and max is reached of at least two monomials. That is, $r \in \mathbb{R}$ is a root if the function defined by f is not lineal in a neighbourhood of r .

Which corresponds to the root 0 of the polynomial in our example.

Example 2. Take the polynomial

$$“0 + (-1)x + x^2”$$

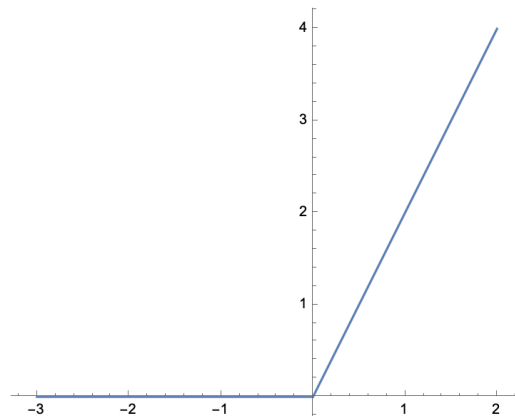


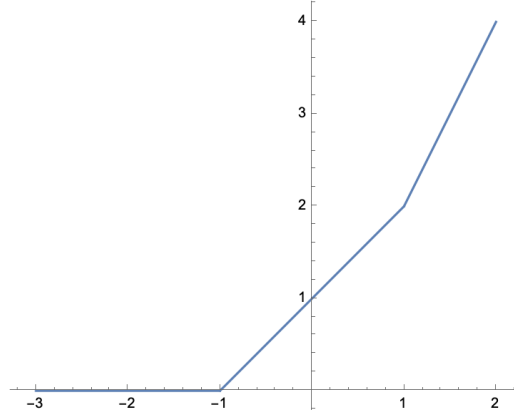
Figure 1

0 is a root of multiplicity 2, for 2 is the distance between the monomials that are not “ghosts” in the polynomial. Only -1 is a ghost coefficient, and the distance between 0 and 2 is 2.

Example 3. Take

$$“0x + 1 \cdot x + x^2” = \max\{0, x + 1, 2x\}$$

Now we have two singularities, which ammount to two roots, and now both have multiplicity 1.



Example 3

Definition. For $f(x) = \sum_{i=0}^d a_i x^i$ and $x_0 \in \mathbb{R}$, we define

$$\text{In}_{x_0} f(x) = \sum_{i \text{ s.t. } f(x_0) = a_i x_0^i} a_i x^i$$

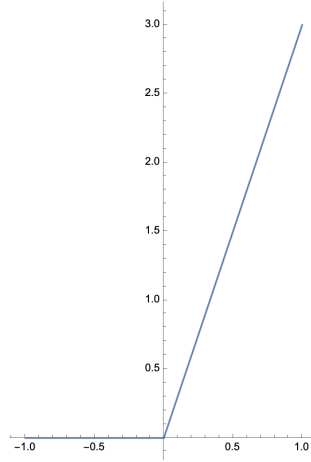
and

$$\text{mult}_f(x_0) = \ell(\text{conv} \{i : a_i x_0^i = f(x_0)\})$$

Example 4. Take

$$f(x) = 0 + x + x^2 + x^3$$

For $x_0 < 0$ we have $\text{In}_{x_0} f(x) = 0$ and $\text{mult}_f(x_0) = 0$. For $x_0 > 0$ we have $\text{In}_{x_0} f(x) = x^3$ and $\text{mult}_f(x_0) = 0$. And for $x_0 = 0$ we have $\text{In}_{x_0} f(x) = f(x)$ and $\text{mult}_f(x_0) = 3$.



Theorem (Fundamental Theorem of Tropical Algebra). For any polynomial of degree d ,

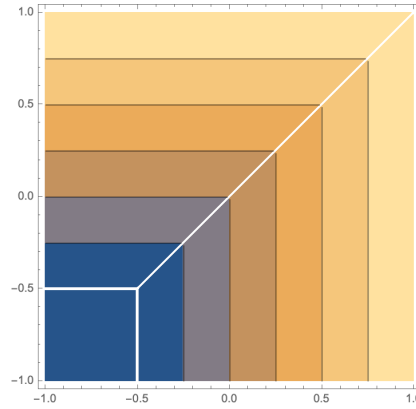
$$\sum_{r \text{ is a root of } f} \text{mult } r = d$$

Thus we now know what is the multiplicity of a root. We must agree that the multiplicity of $-\infty$ is the minimum exponent of the polynomial.

1.3 Two variables

Example 5.

$$f(x, y) = "0 + x + y" = \max\{0, x, y\}$$



Definition. For $f(x, y) = \sum a_{ij}x^i y^j$ define

$$\text{ex}_f = \{(i, j) : a_{ij} \neq 0\}$$

And then the Newton Polygon is

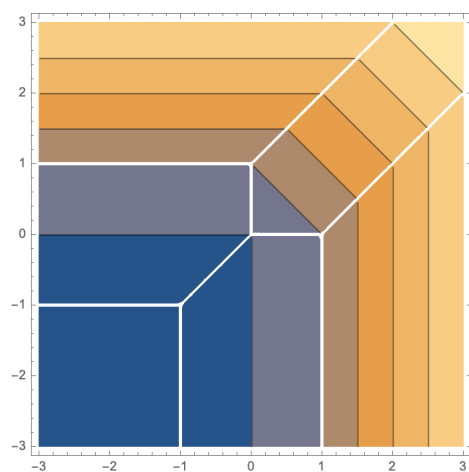
$$\text{conv } \{\text{ex}_f\}$$

So its a vertex for every monomial. And finally:

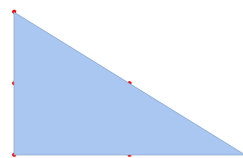
$$C_f := \{(x, y) : \text{In}_{(x,y)} f \text{ is not a monomial}\}$$

Example 6. Check this one out:

$$f(x, y) = "0 + x + y + xy + x^2 + y^2" = \max\{0, x + 1, y + 1, x + y + 1, 2x, 2y\}$$



Algebraic curve



Newton polygon

Although the Newton polygon is the dual geometric object of the graph, it cannot be superposed with it because they live in different geometric spaces.

Anyway let's define

Definition. A graph in \mathbb{R}^2 is tropical if

1. Edges to rational
2. Weights in the edges
3. Balanced

Definition. Tropical hypersurface defined by f :

$$H_f = \{p : \text{In}_p f \text{ is not a monomial}\}$$

And for an ideal I

$$N_I = \{p : \forall f \in I, \text{In}_p f \text{ is not a monomial}\}$$

1.4 Tropicalization

We will learn how to use tropical geometry to study classical geometry. How can we go from classical polynomial to tropical ones?

Let's take a classical polynomial in $\mathbb{C}[X]$ and induce a tropical polynomial:

$$F(X) = \sum_{i=0}^d A_i X^i \rightsquigarrow f(x) = \text{“} \sum_{i=0, A_i \neq 0}^d x^i \text{”}$$

It looks to me that you basically get rid of the coefficients and then take the tropical operations.

Now let's try making the coefficients functions of t :

$$F_t(X) = \sum_{i=0}^d A_i(t)X^i \rightsquigarrow f(x) = \sum_{i=0, A_i \neq 0}^d (-\gamma_i)x^i := F^{\text{trop}}$$

where $A_i(t) = \gamma_j t^j$.

So this time you only take the first coefficient. *Is there anything to correct here?*

Example 7.

$$3t^0 + 4t^0x + x^2 + x^3 + y + t^1xy + x^2y +$$

Theorem 1 (Kapranov).

$$\begin{array}{ccc} F_t & \xrightarrow{\text{zeroes}} & \text{Surface of genus } g \\ \text{tropicalization} \downarrow & & \downarrow \text{amoeba: } \text{Log}_t \text{ then } t \rightarrow 0 \\ f & \xrightarrow{\text{zeroes}} & \text{Tropical curve with } g \text{ bounded regions} \end{array}$$

And then we can calculate the Newton Polygon and do combinatorics.

1.5 Enumerative Geometry

$$N_{\mathbb{C}}(\delta, p) = N_{\mathbb{T}}(\delta, p)$$

1.6 Matroids

Definition (Matroid). $E \neq \emptyset$, B a set of bases that satisfies the Exchange property, that is, for $B_1, B_2 \in B$, there always exists $e_1 \in B_1$ and $e_2 \in B_2$ such that $B_1 \setminus e_1 \cup e_2 \in B$.

Example 8. Let $E = \{a, b, c, d, e\}$ and $B = \{\{a, b, c\}, \{a, b, d\}, \{a, b, e\}, \{a, c, d\}, \{a, c, e\}\}$. For every base let's produce a vector that has 1 if the base contains the element in the corresponding slot according to the order (a, b, c, d, e) . So for example the first base has vector $(1, 1, 1, 0, 0)$.

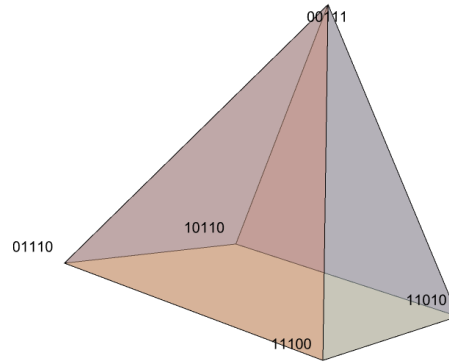
This produces five vectors in \mathbb{R}^5 whose convex hull is a polyhedron. Now it turns out that the independent set property lets us direct the edges in this polytope.

Definition. Δ is a matroidal polytope if all the edges of Δ are in direction $e_j - e_i$ for some i, j .

Actually there is a bijection between matroids and these directed polytopes.

Example 9 (Bergman fan, Ardila, Klivans). E of size 5, and a family in \mathbb{R}^4 . Let us associate:

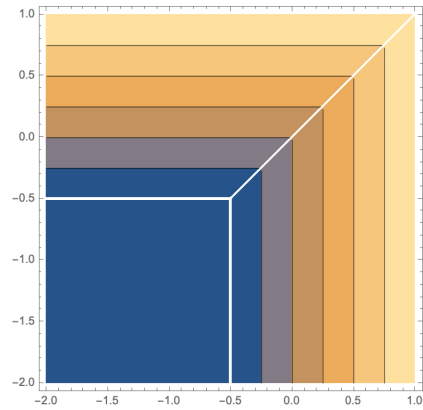
$$a \rightsquigarrow (-1, 0, 0, 0) \quad b \rightsquigarrow (0, -1, 0, 0) \quad c \rightsquigarrow (0, 0, -1, 0) \quad d \rightsquigarrow (0, 0, 0, -1) \quad e \rightsquigarrow (1, 1, 1, 1)$$



Example 10 (Balanced (Tropical) fan). E of size 3, say $E = \{0, 1, 2\}$ and $B = \{\{0\}, \{1\}, \{2\}\}$. Let us associate:

$$0 \rightsquigarrow (1, 1) \quad 1 \rightsquigarrow (-1, 0) \quad 2 \rightsquigarrow (0, -1)$$

And this produces

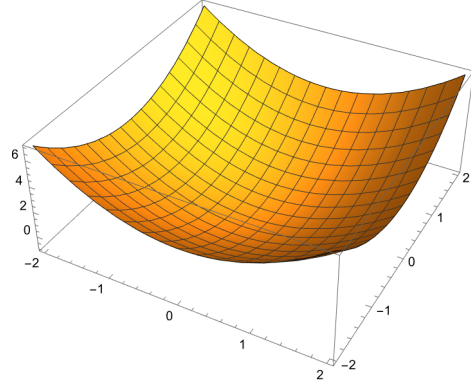
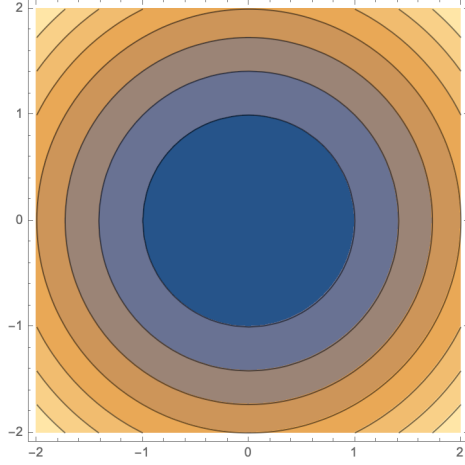


Where every line is a ray spanned by the three vectors we chose. This is the Tropical Fan.

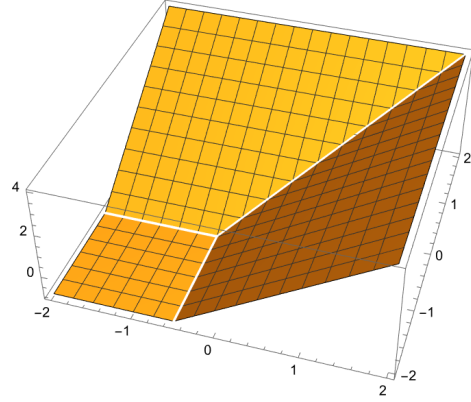
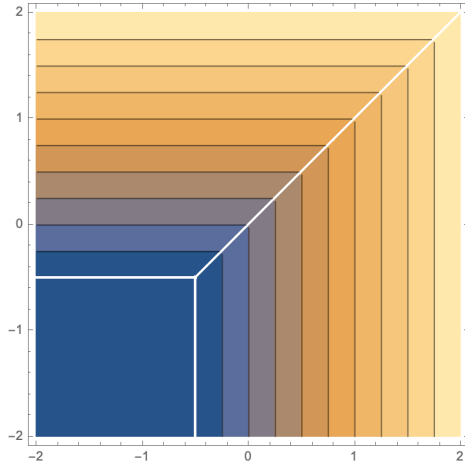
And it turns out matroids are the same as tropical fans of degree 1. And also there's the polytope idea so we have these three definitions. Another example of a tropical fan is the tropical curve in Example 6.

1.7 Three examples (extra)

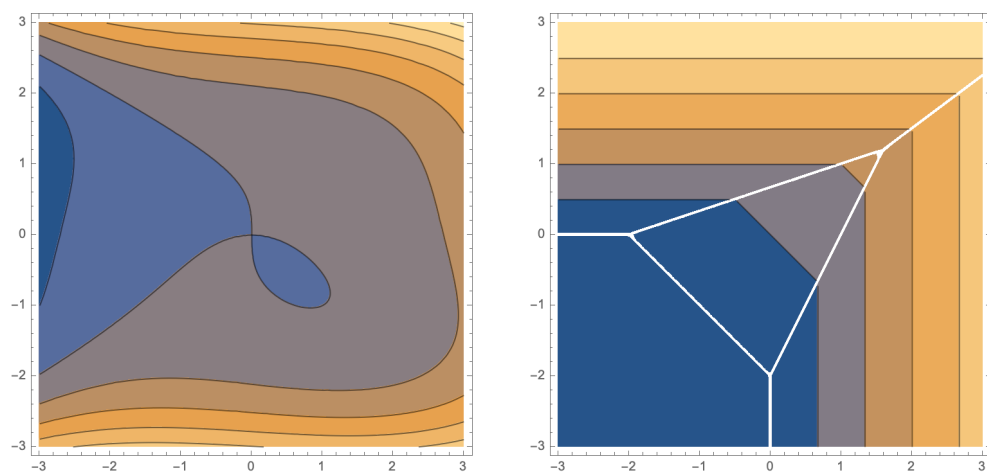
Example 11. Here are the roots of the classical polynomial $x^2 + y^2 - 1$ (with the usual operations in $\mathbb{R}[x, y]$) and its plot in \mathbb{R}^3 :



And now we do exactly the same but for the tropical polynomial “ $x^2 + y^2 - 1$ ” = $\max\{2x, 2y, 0\}$:



Example 12. Here are the roots of $x^3 + 2xy + y^4 \in \mathbb{R}[x, y]$ and a related tropical polynomial “ $x^3 + 2xy + y^4 + 0$ ” = $\max\{3x, 2 + x + y, 4y, 0\}$:



Notice we must include the 0 in the tropical polynomial, because without it we do not get the triangle in the plot.

1.8 Benoit's talk on Real tropical geometry

Let us define a family of polynomials of degree d parametrized by t :

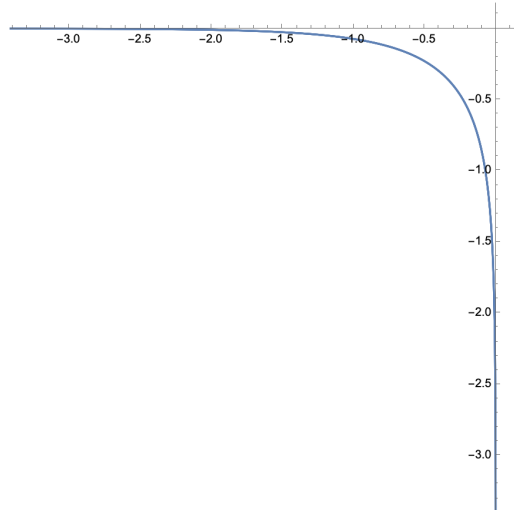
$$p_t(x, y) = \sum_{i+j \leq d} c_{i,j} t^{v_{i,j}} x^i y^j$$

Now consider the map

$$\begin{aligned} \text{Log}_t : (\mathbb{C}^\times)^2 &\rightarrow \mathbb{R}^2 \\ (x, y) &\mapsto \left(\frac{\log |x|}{\log t}, \frac{\log |y|}{\log t} \right) \end{aligned}$$

And then define for a curve $\mathcal{C} \subset (\mathbb{C}^\times)^2$ the amoeba of \mathcal{C} as $\text{Log}_t(\mathcal{C})$. Notice \mathcal{C} is a *complex* curve, which is a real surface. So the image of our function is a region in \mathbb{R}^2 .

Here's Dani's incomplete attempt of an amoeba:



And now define as in Lucía's talk:

$$\mathfrak{p} = \left\langle \sum_{i+j \leq d} c_{i,j} x^i y^j \right\rangle = \max_{i+j \leq d} \{c_{i,j} + ix + jy\}$$

Taking edges as perpendicular lines to edges in a tropical conic, and vertices as the centres of regions determined by the conic, we obtain a subdivision of the plane that looks like the dual tiling of the conic.

Remark. The genus of the curve equals the amount of bounded regions determined by the tropical curve.

Then he takes the amoebas of the real parts of curves and he obtains plane curves. He then 'unfolds' these curves by taking each part of the curve that is lying in each of the four quadrants of the plane, and then he pastes back each of these pieces.

And then take the limit as $t \rightarrow \infty$ and finally folding them back. This is some sort of combinatorial procedure. And it turns out that:

Theorem (Viro, 1976).

$$(\mathbb{R}^2, T_{\mathbb{R}}) \cong (\mathbb{R}^2, \mathcal{C}_{\mathbb{R}})$$

where \cong is homeomorphic. So they have the same Newton polygon and same degree.

Where $T_{\mathbb{R}}$ is the real part he's been working with in the last two paragraphs and $\mathcal{C}_{\mathbb{R}}$ looks like the whole complex curve (real surface).

Example 13 (Dani's attempt to use Benoit's Log function). Let us try to evaluate our Log_t function in a complex algebraic curve. We must remember that the zeroes of polynomials of the form $y^2 = \prod_{k=1}^{2g+1} (x - a_k)$ are called *hyperelliptic curves* when $g > 1$ and *elliptic curves* when $g = 1$ (According to [diez]).

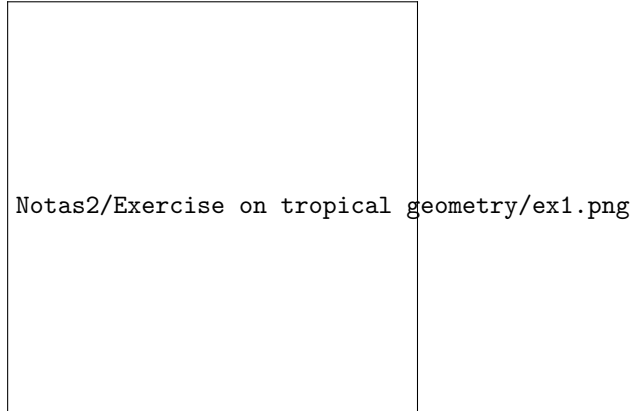
Taking $g = 1$, we have a curve of genus 1, that is, a torus. We hope that when we evaluate Log in this torus we get exactly one bounded region in the resulting drawing. The polynomial in this case is

$$y^2 = (x - a_1)(x - a_2)(x - a_3)$$

(Unfinished)

1.9 An exercise on tropical geometry

We are interested in the following figure:



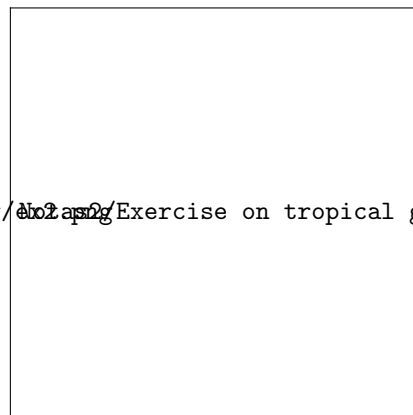
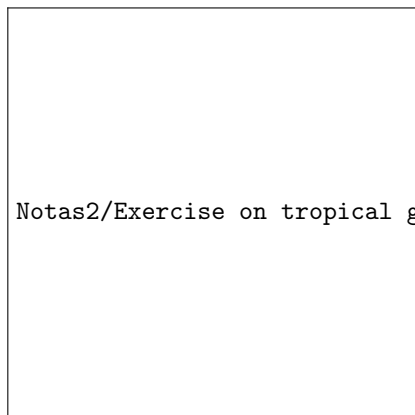
It represents the nullcline of some system of differential equations (See [curto2],[curto1]).

Also it is the zeroes of the classical (non-tropical) function

$$-y + \max\{1 - \frac{3}{4}, 0\} = 0$$


How can we make it into a tropical curve?

Benoit shows how it is contained in the zeroes of the tropical polynomial " $0-4x^3-4x^3y^4$ ", using its Newton Polygon:



Notas2/Exercise on tropical geometry/ex2.png


Here's how he did it:



Notas2/Exercise on tropical geometry/ex4.png

We next wonder, in the context of our nullcline original problem, what happens when we reflect the curve in the first figure with respect to the identity line? Is there a way to repeat the process? Can we reflect the second figure by the identity line and find the tropical polynomial whose zeroes is this curve?

Here's Benoit's unfinished attempt:



Notas2/Exercise on tropical geometry/ex5.png

Check Bezout Kouchnirenko, Tropical. Also Gelfand Kapranov Zelevinsky and Sturmfels, First steps in tropical geometry.

1.10 Open problems

1. Not every tropical object can be obtained using the Log_t and $t \rightarrow \infty$ method (limits of amoebas). Which tropical objects can?
2. Find correspondence theorems between classical and tropical geometry like Mikhalkin's ([mikhalkin2006tropical]?)
 - Number of curves passing through a number of points.

- Try finding a reference “Welschinger GW, Gromov Witten”

3. When can Viro Patchworking work? That is, find real algebraic objects with the same topology as algebraic varieties.

And what’s up with genus 2 cubics?

2 Computational commutative algebra

Matías Bender, matiasbender@inria.fr

2.1 Univariate polynomials and resultants

R a ring, like polynomials. It should be commutative and an integral domain ($a, b \in \mathbb{R} \setminus \{0\} \implies ab \neq 0$). Also take a field \mathbb{K} and its algebraic closure $\bar{\mathbb{K}}$.

2.1.1 Univariate polynomials

Take the polynomial ring $k[x]$ and $f \in k[x]$ with $f = \sum_{i=0}^d c_i x^i$ for $c_i \in k$ and $c_d \neq 0$. We say $\deg f = d$.

Now let $k \subseteq \mathbb{K}$ and $p \in \mathbb{K}$ we define $f(p) = \sum_i c_i p^i \in \mathbb{K}$ the evaluation of f . And we say a root of f is p such that $f(p) = 0$.

Question Given $f_1, \dots, f_r \in k[x]$, do they have a common root?

Definition. Given $f_1, \dots, f_r \in k[x]$ we define the ideal $\langle f_1, \dots, f_r \rangle = \{ \sum g_i f_i : (g_1, \dots, g_r) \in k[x]^r \}$

Prop. Let $p \in \mathbb{K}$. $\forall f \in \langle f_1, \dots, f_r \rangle$, $f(p) = 0 \iff f_i(p) = 0 \forall i$.

Remark. If $g \in \langle f \rangle$, then if $p \in \mathbb{K}$ is such that $f(p) = 0$ then $g(p) = 0$.

Prop. Given $f, g \in k[x]$, there are unique $(q, r) \in k[x]^2$ such that $f = q \cdot g + r$ and $r = 0$ or $\deg r < \deg g$.

We define $\text{rem}(f, g) = r$ and write $f|g$ if and only if $\text{rem}(f, g) = 0$.

Theorem 2. $k[x]$ is a principal ideal domain. That is, for every ideal $\langle f_1, \dots, f_r \rangle$ there exists one polynomial g such that $\langle f_1, \dots, f_r \rangle = \langle g \rangle$. g is called GCD of f_1, \dots, f_r .

I challenge to prove that

Prop. $\text{GCD}(f_1, \dots, f_r)$ is the smallest polynomial with degree such that if $(\forall i) h|f_i$, then $h|\text{GCD}(f_1, \dots, f_r)$.

Algorithm 1 Euclidean Algorithm

Input : $f, g \in k[x]$ with $\deg f \geq \deg g$

Output: $r \in k[x]$ such that $\langle f, g \rangle = \langle r \rangle$

if $r_{-1} = f, r_0 = g, i = 0$ **then**
 | $i = i + 1$ $r_i = \text{rem}(r_{i-2}, r_{i-1})$

end

return r_{i-1}

Theorem 3. Euclidean Algorithm terminates and is correct.

Proof. It terminates because $\forall i \geq 1) \deg(r_i) < \deg(r_{i-1})$. Hence $\exists i_*$ such that $r_{i_*} = 0$. Observe that for each i , $\exists q_i \in k[x]$ such that $r_{i-2} = r_{i-1}q_i + r_i$. Hence $\langle r_{i-2}, r_{i-1} \rangle =$

$\langle r_{i-1}, r_i \rangle$.

$$h_1 r_{i-2} + h_2 r_{i1} \iff (h_1 q_1 + h_2) r_{i-1} + h_i r_i.$$

Therefore, $\langle f, g \rangle = \langle r_{-1}, r_0 = \dots \rangle \langle r_{k-1}, r_{i*} \rangle$

□

HW Prove that $GCD(f_1, f_2, f_3) = GCD(GCD(f_1, f_2), f_3)$.

Conclusion If $GDC(f_1, \dots, f_r) = 1$, then there are no common solutions.

If $GCD(f_1, \dots, f_r) \neq 1$. Then f_1, \dots, f_r have ea common factor if $k = \bar{k}$ and $\exists p \in k$ such that $f_1(p) = \dots = f_r(p) = 0$.

Now consider a UFD ring R like $\mathbb{C}[y], \mathbb{C}[x, y]$.

Definition (Resultant). Given $f(x, y) = \sum_{i=1}^m f_i(y)x^i \in \mathbb{C}[x, y]$ that is, $f \in \mathbb{C}[y]$, and $g = \sum_{i=1}^m g_i(y)x^i$. We define Sylvester matrix $\text{Sylv}(f, g, x)$.

$$\begin{pmatrix} f_m & 0 & \dots & 0 & g_m & 0 & \dots & 0 \\ f_{m-1} & f_m & \dots & 0 & g_{m-1} & g_m & \dots & 0 \\ & & \dots & & & & \dots & \\ f_0 & f_1 & \dots & f_m & g_0 & g_1 & \dots & g_m \\ 0 & f_0 & \dots & f_{m-1} & 0 & g_0 & \dots & g_{m-1} \\ & & \dots & & & & \dots & \\ 0 & 0 & \dots & f_0 & 0 & 0 & \dots & g_0 \end{pmatrix}$$

The resultant $\text{Res}(f, g, x) = \det \text{Sylv}(f, g, x) \in \mathbb{C}$.

We may substitute \mathbb{C} with any ring R .

Remark. $\text{Sylv}(f, g, x)$ represents $\text{Sylv}_{f, g, x}^-(A, B) \mapsto Af + Bg = \sum c_i x^i$ with $c_i \in \mathbb{R}$. Where $\deg_x(A) < \deg_x(g)$ and $\deg_x(B) < \deg_x(f)$. So A and B are polynomials of the form $A = \sum_{i=0}^{m-1} A_i x^i$ and $B = \sum_{i=1}^{m-1} B_i x^i$. So with two polynomials I obtain another polynomial.

Prop. $\text{Res } f, g, x = \text{img } \text{Sylv}_{f, g, x}$ that is, $\exists A, B$ such that $\deg A < \deg g$, $\deg B < \deg A$ such that $Af + Bg = \text{Res}(f, g, x)$.

HW Prove it. Use adjugate matrix of $\text{Sylv}(f, g, x)$.

Prop. If $f, g \in k[x]$. The $\text{Res}(f, g, x) = 0 \iff GCD(f, g) \neq 1$.

2.1.2 Solving bivariate polynomial systems

Example 14.

$$\text{Sylv}(f, g) = \begin{pmatrix} y & 0 & 2y & 0 \\ y^2 + y & y & 0 & 2y \\ 1 & y^2 + y & -y^2 + 3 & 0 \\ 0 & 1 & 0 & y^2 + 3 \end{pmatrix}$$

Then $\text{Res}(f, g, x) = \underbrace{y^2}_{\text{does not lead to a solution}} \underbrace{(2y^2 - 3y - 1)(y + 1)^3}_{\text{lead to solutions!}}$

Theorem 4. If $(p_x, p_y) \in \mathbb{C}^2$ are such that $f(p_x, p_y) = g(p_x, p_y) = 0$ then $\text{Res}(f, g, x)|_{y=p_y} = 0$.

Proof. $\exists A, B$ such that $Af + Bg = \text{Res}(f, g, x) = 0 = \text{Res}(f, g, x)|_{y=p_y}$. \square

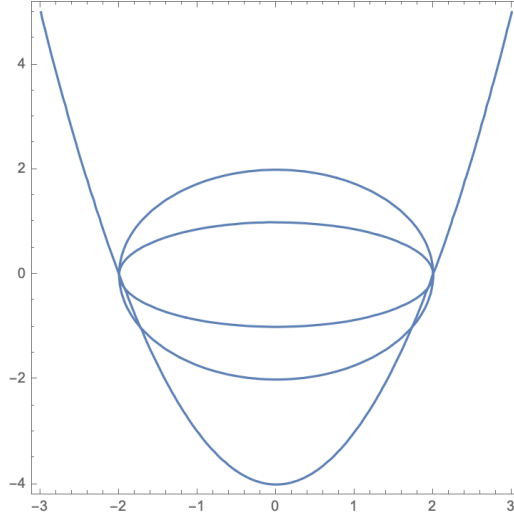
Theorem 5 (Extension theorem). Given $f, g \in \mathbb{C}[x, y]$ as before, let p_y be such that $\text{Res}(f, g, x)|_{y=p_y} = 0$. Then if $f_m(p_y) \neq 0$ or $g_m(p_y) \neq 0$, then $\exists p_x$ such that (p_x, p_y) is solution of $f(x, y) = g(x, y) = 0$.

2.2 Ideals and varieties

Example 15. Consider the polynomials

$$\begin{aligned} f_1 &= x^2 + 4y^2 - 4 \\ f_2 &= x^2 + y^2 - 4 \\ f_3 &= x^2 - y - 4 \end{aligned}$$

How can we verify that f_3 vanishes at common zeros of (f_1, f_2) ?



Let $R = \mathbb{C}[x_1, \dots, x_m]$, $f \in R$ with $f = \sum_{\alpha \in \mathbb{Z}_{\geq 0}^m} c_{\alpha} x^{\alpha}$ where $c_{\alpha} \in \mathbb{C}$ there finite α such that $c_{\alpha} \neq 0$, x^{α} is monomial, $x^{\alpha} = \prod_{i=1}^m x_i^{\alpha_i}$.

The degree is $\deg f = \max_{\alpha \in \mathbb{Z}_{\geq 0}^m} (\sum \alpha_i : c_{\alpha} \neq 0)$.

Ok now given $p \in \mathbb{C}^m$, we can evaluate f doing $f(p) = \sum c_{\alpha} p^{\alpha}$. And we say p is a zero if $f(p) = 0$.

Definition. Given $f_1, \dots, f_r \in \mathbb{R}$ we define the affine algebraic variety $V(f_1, \dots, f_r) = \{p \in \mathbb{C}^m : (\forall i) f_i(p) = 0\}$. And in general, if $I \subseteq R$ is an ideal, we define

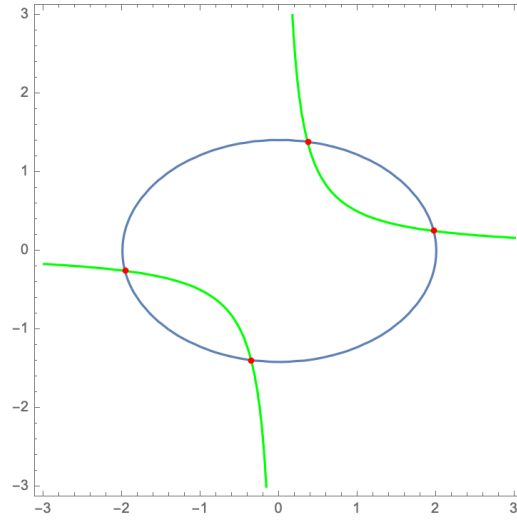
$$V(I) = \{p \in \mathbb{C}^m : (\forall i) f \in I = 0\}$$

.

Example 16. Take

$$f_1 = x^2 + 2y^2 - 4$$

$$f_2 = 2xy - 1$$



Definition. An ideal I is a subset of R such that $(\forall f, g \in I) f + g \in I$ and $(\forall f \in I)(\forall r \in \mathbb{R}) fr \in I$.

Prop. Given $f_1, \dots, f_r \in R$, we define the generated ideal as

$$\langle f_1, \dots, f_r \rangle = \left\{ \sum_{i=1}^r g_i f_i : g_1, \dots, g_r \in R \right\}$$

Prop. $V(\langle f_1, \dots, f_r \rangle) = V(f_1, \dots, f_r)$.

Definition. The ring R is Noetherian if when $I \subseteq R$ is an ideal then $\exists f_1, \dots, f_r$ such that $I = \langle f_1, \dots, f_r \rangle$.

2.2.1 Operations on ideals

Prop. Fix $I, J \subseteq R$ ideals. Then:

1. $I \subseteq J \implies V(J) \subseteq V(I)$
2. $I + J = \{f + g : f \in I, g \in J\}$ is an ideal.
3. $I \cap J$ is an ideal and $V(I \cap J) = V(I) \cup V(J)$.

2.2.2 Hilbert's Nullstellensatz

Definition. Let $W \subseteq \mathbb{C}^n$, we define the ideal

$$I(W) = \{f \in R : (\forall p \in W) f(p) = 0\}$$

Prop. Given $W \subseteq \mathbb{C}^n$, $V(W)$ is the smallest with inclusions of the affine algebraic varieties that contain W . If $W \subseteq Z$ and Z variety, then $V(I(W)) \subseteq Z$. Also $\bar{W} = V(I(W))$.

Theorem 6 (Hilbert's Nullstellensatz). Let $I \subseteq R$ be an ideal and $f \in R$. Then, $f \in I(V(I))$ if and only if $f^k \in I$ for some $k \in \mathbb{N}$.

Example 17. This is actually Example 5.

$$\begin{aligned} f_1 &= x^2 + 4y^2 - 4 \\ f_2 &= x^2 + y^2 - 4 \\ f_3 &= x^2 - y - 4 \end{aligned}$$

It turns out that $f_r \notin \langle f_1, f_2 \rangle$. But actually $f_3^2 = (x^2 + \frac{4}{3}y^2 + \frac{2}{3}y - \frac{11}{3})f_1 + (\frac{16}{3}y^2 + \frac{8}{3}y + \frac{1}{2})f_2$ is.

Definition. Given $I \subseteq R$ we define its radical ideal as

$$\sqrt{I} = \{f \in R : (\exists k \in \mathbb{N}) f^k \in I\}$$

Remark. By Hilbert's Nullstellensatz, $\sqrt{I} = I(V(I))$.

Remark. It is necessary that the field we are working on is algebraically closed for Hilbert's Nullstellensatz to be valid.

Corollary 1 (Weak version of Hilbert's Nullstellensatz). $V(I) = \emptyset \iff 1 \in I$

2.2.3 From geometry to algebra

Prop. Given $v, w \in \mathbb{C}^m$ varieties,

1. $I(V \cap W) = \sqrt{I(V) + I(W)}$
2. $I(V \cup W) = I(V) \cap I(W)$
3. Given ideals $I, J \subseteq R$, $\sqrt{I} \cap \sqrt{J} = \sqrt{I \cap J}$

2.2.4 Radical membership

Question Given I ideal and f polynomial, does $f \in \sqrt{I}$? Let us introduce a new variable t to define

$$R[t] = \mathbb{C}[x_1, \dots, x_n, t]$$

Theorem 7. Let $I = \langle f_1, \dots, f_r \rangle \subseteq R$. Consider $g \in R$. Then

$$g \in \sqrt{I} \iff 1 \in \langle f_1, \dots, f_r, gt - 1 \rangle \subseteq R[t]$$

Proof. By Hilbert's Nullstellensatz, $(\forall p \in V(I))g(p) = 0$. And by Weak Hilbert's Nullstellensatz, $V_{\mathbb{C}^{m+1}}(f_1, \dots, f_r, gt - 1) = \emptyset$. We will prove these two conditions are also equivalent.

We have:

$$(p_1, \dots, p_m, p_0) \in V_{\mathbb{C}^{m+1}}(f_1, \dots, f_r) \iff \begin{cases} f_1(p_1, \dots, p_m) = 0 \\ \dots \\ f_r(p_1, \dots, p_m) = 0 \\ g(p_1, \dots, p_m)p_0 - 1 = 0 \end{cases}$$

The first r equations are equivalent to $(p_1, \dots, p_m) \in V_{\mathbb{C}^m}(f_1, \dots, f_r)$. The last equation says $p_0 = \frac{1}{g(p_1, \dots, p_m)}$ and that $g(p_1, \dots, p_m) \neq 0$.

Anyway we get

$$V_{\mathbb{C}^{m+1}}(f_1, \dots, f_r, gt - 1) = \emptyset \iff (\forall p \in V_{\mathbb{C}^m}(I))g(p) = 0$$

□

Example 18 (The Rabinowitsch trick, 1929). Use Hilbert's Weak Nullstellensatz to prove Hilbert's Nullstellensatz.

Hint If $(\forall p \in V(I))g(p) = 0$, then $\exists h_1, \dots, h_r, h_0 \in R[t]$ such that $1 = \sum h_i f_i + h_0(gt - 1)$. Replace t by $\frac{1}{g(x_1, \dots, x_m)}$ symbolically and clean denominators.

Solution. Let $g \in I(V(I))$ for some ideal $I = \langle f_1, \dots, f_r \rangle$, that is, g vanishes whenever all the f_i vanish. Then the polynomials $f_1, \dots, f_r, gt - 1$ cannot vanish all at the same time, so that the zeroes of ideal generated by all of them is empty. By Hilbert's Weak Nullstellensatz, this ideal must be the unit ideal (1 is in there). All this is exactly the first phrase in the **Hint**: there must $\exists h_1, \dots, h_r, h_0 \in R[t]$ such that $1 = \sum h_i f_i + h_0(gt - 1)$.

When substituting t by $\frac{1}{g(x_1, \dots, x_m)}$ we obtain that

$$1 = \sum h_i \left(\frac{1}{g(x_1, \dots, x_m)}, x_1, \dots, x_n \right) f_i \left(\frac{1}{g(x_1, \dots, x_m)}, x_1, \dots, x_n \right)$$

Notice that the expression above is a sum that may have many coefficients of the form $\left(\frac{1}{g(x_1, \dots, x_m)}\right)^k$. Actually, any denominator on this sum must be of this kind. Thus we can write

$$1 = \frac{\sum h_i(x_1, \dots, x_n) f_i(x_1, \dots, x_n)}{g(x_1, \dots, x_n)^r}$$

for some r which makes $g(x_1, \dots, x_n)^r$ the common denominator. We have shown $g \in \sqrt{(V(I))}$ \square

2.3 Gröbner bases

How can we tell if $f \in I$?

2.3.1 Principal ideals

Remark If $f_1, \dots, f_r \in \mathbb{C}[x]$, $\exists f_*$ such that $\langle f_1, \dots, f_r \rangle = \langle f_* \rangle$. Then $g \in \langle f_1, \dots, f_r \rangle$ (implies?) $f_* | g$.

Remark We should be careful when dividing polynomials of more than one variable (we did a bad example to show this). So we make the following:

2.3.2 Monomial orderings

Definition. A monomial ordering $>$ is a total order for the monomials in R such that

1. $(\forall) x^\alpha \in R \setminus \{1\}, 1 < x^\alpha$.
2. $(\forall x^\alpha, x^\beta, x^\gamma) x^\alpha < x^\beta \implies x^\gamma x^\alpha < x^\gamma x^\beta$

Prop. If $x^\alpha x^\gamma = x^\beta$ and $x^\gamma \neq 1$, then $x^\alpha < x^\beta$ for any monomial ordering.

Proof. If $1 \neq x^\gamma$, by (1), $1 < x^\alpha$. By (2), $x^\alpha = 1x^\alpha < x^\gamma x^\alpha = x^\beta$. \square

Definition. The lexicographical monomial ordering $>_{\text{lex}}$ is an ordering such that

$$x^\alpha >_{\text{lex}} x^\beta \iff \exists k \leq m \text{ such that } \alpha_i = \beta_i \text{ for } i < k \text{ and } \alpha_k > \beta_k$$

Example 19.

$$x_1 x_2^2 x_3 >_{\text{lex}} x_1 x_2 x_3^{10}$$

Definition. The graded lexicographical monomial ordering $>_{\text{grlex}}$ is an ordering such that

$$x^\alpha >_{\text{grlex}} x^\beta \iff \sum \alpha_i > \sum \beta_i \text{ or } \sum \alpha_i = \sum \beta_i \text{ and } x^\alpha >_{\text{lex}} x^\beta$$

Example 20.

$$\begin{aligned} x_1^2 x_2^2 x_3^2 &>_{\text{grlex}} x_1^2 x_2^3 && \text{here we compute deg} \\ x_1^2 x_2^2 x_3^2 &>_{\text{grlex}} x_1^2 x_2^3 x_3 && \text{here we use } >_{\text{lex}} \end{aligned}$$

Definition. Given $>$ and $f = \sum_{\alpha \in \mathbb{Z}_{\geq 0}} c_{\alpha} x^{\alpha}$,

1. **Support.** $\text{supp}(f) = \{x^{\alpha} : c_{\alpha} \neq 0\}$
2. **Leading monomial.** $LM_{>}f = \max_{wrt >} \{x^{\alpha} \in \text{supp}(f)\}$
3. **Leading coefficient.** $LC_{>}(f) = c_{\alpha}$ where $x^{\alpha} = LM_{>}(f)$.
4. **Leading term.** $LT_{>}(f) = LC_{>}(f)LM_{>}(f)$

2.3.3 Polynomial division

Algorithm 2 Division Algorithm

Input : $f, g \in k[x]$

Output: $(q, r) \in \mathbb{C}[x_1, \dots, x_n]$ such that $g = qf + r$ and $\forall x \in \text{supp}(r) LM_{>}(f) \nmid x$

while $(h \neq 0)$ **do**

if $LM_{>}(f) \mid LM_{>}(h)$ **then**

$q = q + \frac{LT(h)}{LT(f)} \quad h = h - \frac{LT(h)}{LT(f)}LT(f)$

end

else

$r = r + LT(h) \quad h = h - LT(h)$

end

end

return (q, r)

HW With one variable, this is the same as the Euclidean algorithm.

Prop. Given $f, g \in R$, $LM_{>}(f, g) = LM_{>}(f)LM_{>}(g)$. In particular, if $g \in \langle f \rangle$, $LM_{>}(f)LM_{>}(g) > 0$?

Corollary 2. For some $f, g, g \in \langle f \rangle \iff \text{Rem}(g, f) = 0$

HW Prove this. You have to use the Prop many times.

And then make the division algorithm a little more general:

Theorem 8 (Another Division algorithm). Input: $g, [f_1, \dots, f_s] \in k[x]$ and monomial order $>$.

Output: $(q_1, \dots, q_s, r) \in \mathbb{C}[x_1, \dots, x_n]^{s+1}$ such that

1. $g = \sum q_i f_i + r$
2. $(\forall x^{\alpha} \in \text{supp}(r)) (\forall i \leq s) LM_{>}(f_i) \nmid x^{\alpha}$

$\text{Rem}(g, [f_1, \dots, f_s], >) = r$

Example 21. Using $>_{\text{lex}}$,

$$\begin{aligned} f_1 &= x^2 + y^2 + y \\ f_2 &= \underbrace{xy}_g + 1 \end{aligned}$$

Whops! Reminder is $r = 0$.

Prop. Given $f_1, \dots, f_s, g \in R$ and $>$, $g - \text{Rem}(g, [f_1, \dots, f_s], >) \in \langle f_1, \dots, f_s \rangle$. In particular, if $\text{Rem}(g, [f_1, \dots, f_s], >) = 0$, then $g \in \langle f_1, \dots, f_s \rangle$

Notice **the opposite does not hold**.

Remark. Given $\langle f_1, \dots, f_s \rangle$ we want $\bar{f}_1, \dots, \bar{f}_r$ such that $\langle f_1, \dots, f_r \rangle = \langle \bar{f}_1, \dots, \bar{f}_r \rangle$, $g \in \langle f_1, \dots, f_r \rangle \iff \text{Rem}(g, [\bar{f}_1, \dots, \bar{f}_r], >) = 0$

Example 22. If $f_1, \dots, f_s \in \mathbb{C}[x]$, then $\text{GCD}(f_1, \dots, f_r)$ satisfies the property in the Obs.

2.3.4 Gröbner Bases

Definition. Given an ideal I and a monomial ordering $>$, a Gröbner basis (GB) is a set $G \subseteq I$ such that $(\forall g \in I)(\exists f \in G) LM_{>}(f) LM_{>}(g)$.

Example 23 (Non-example). $G = [f - 1, \dots, f_2]$ is not a GB for $>_{\text{lex}}$ but $-x + y^3 + y = xf_1 - yf_2$, $LM(f_1)XX$ and $LM(f_2)XX$.

- If $I = \langle f \rangle$ then $[f]$ is a GB I for any monomial ordering.
- If $V(I) = \emptyset$, by Hilbert's Nullstellensatz then $1 \in I$. If G is a GB of I with respect to, $1 \in I$, so $\exists f \in G$ such that $LM(f) | 1$. Hence, $LM(f) = 1$ and then $1 \in G$.

Theorem 9. Every ideal has a finite GB basis with respect to any $>$.

Prop. If G is a finite GB of I with respect to $>$, then $\langle G \rangle = I$.

Proof. Let $g \in I$ and consider $g = \sum q_i f_i + r$ given by division algorithm. Hence, as $g \in I$, $r \in I$. Then another $r = 0$ or $\exists f \in G$. \square

Theorem 10. If $[f_1, \dots, f_s]$ is a GB of I with respect to $>$, $g \in I \iff \text{Rem}(g, [f_1, \dots, f_s], >) = 0$

Prop. Given $[f_1, \dots, f_s]$ and $[\bar{f}_1, \dots, \bar{f}_s]$ two GB of I with respect to $>$, then, for any $g \in \mathbb{C}[x_1, \dots, x_m]$,

$$\underbrace{\text{Rem}(g, [f_1, \dots, f_s])}_{r_1} = \underbrace{\text{Rem}(g, [\bar{f}_1, \dots, \bar{f}_s])}_{r_2}$$

Proof. 1. $r_1 - r_2 \in I$ because $g - r_1 \in I$

2. If $r_1 - r_2 \neq 0$, $LM_{>}(r_1, r_2) \in \text{supp}(r_1) \cup \text{supp}(r_2)$. Wlog, $LM_{>}(r_1 - r_2) \in \text{supp}(r_1)$. $\text{Rem}(r_1 - r_2, [f_1, \dots, f_s], >) = 0$ we get 0. This is a contradiction because $(\forall i \leq s) LM_{>}(f_i) \nmid LM_{>}(r_1 - r_2)$.

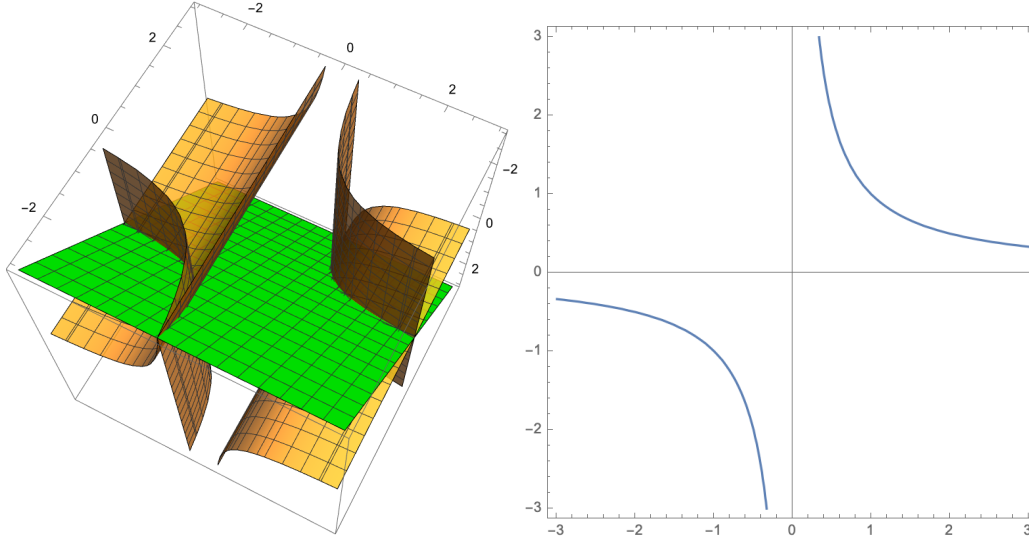
\square

2.3.5 Applications of Gröbner Bases

Example 24. Consider

$$f_1 = xy - 1 \quad \text{and} \quad f_2 = xz - 1$$

We must try to draw $V(f_1, f_2) \cap \mathbb{R}^3$ and $V(y - z) \cap \mathbb{R}^3$ so as to show the intersection in the green plane $y = z$.



Each polynomial is a surface

$V(f_1, f_2, y - z)$ is this curve

Project $\pi_1 : \mathbb{C}^3 \rightarrow \mathbb{C}^2$ with $(p_1, p_2, p_3) \mapsto (p_2, p_3)$ and show $\pi_1(V(f_1, f_2)) = V(y - z) \setminus \{(0, 0)\}$.

2.4 Elimination theory

There's something missing here

Theorem 11 (Extension theorem). $I = \langle f_1, \dots, f_s \rangle \subseteq \mathbb{C}[x_1, \dots, x_m]$. Let $I_1 = I \cap \mathbb{C}[x_1, \dots, x_m]$ we will write f_i as

$$f_i = c_i(x_1, \dots, x_m)x_1^{\alpha_i} + \text{forms of degree} < \alpha_i \text{ wrt } x_1$$

such that $c_i \in \mathbb{C}[x_1, \dots, x_m]$ is non zero.

If $(f_1, \dots, f_m) \in V_{\mathbb{C}^{m+1}}(I_1) \setminus V_{\mathbb{C}^{m+1}}(c_1, \dots, c_s)$ then $\exists p_1 \in \mathbb{C}$ such that $(p_1, \dots, p_m) \in C(I)$.

Theorem 12 (Closure theorem). $V_{\mathbb{C}^{m-\ell}}(I_\ell) = \overline{\Pi_\ell(V_{\mathbb{C}^m}(I))}$

Theorem 13 (Elimination theorem). Let G be a GB of I with respect to $>_{\text{lex}}$. Then, $G \cap \mathbb{C}[x_p, \dots, x_m]$ is a GB of I with respect to $>_{\text{lex}}$.

Lema. If $LM_{>\text{lex}}(f) \in \mathbb{C}[x_{\ell+1}, \dots, x_m]$, then $f \in \mathbb{C}[x_{\ell+1}, \dots, x_m]$

Proof. Any monomial x^α involving a variable in $\{x_1, \dots, x_\ell\}$ satisfies $x^\alpha >_{\text{lex}} x^\beta$ for $x^\beta \in \mathbb{C}[x_{\ell+1}, \dots, x_m]$. So, if $LM_{>\text{lex}}(f)$ does not involve $\{x_1, \dots, x_\ell\}$, no monomial in $\text{supp}(p)$ involves $\{x_1, \dots, x_{\ell-1}\}$.

Proof. Consider $f \in I_\ell$ as G is GB, $\exists g \in G$ such that $LM_{>\text{lex}}(g) | LM_{>\text{lex}}(f)$ then $LM_{>\text{lex}} <_{\text{lex}} LM_{>\text{lex}}(f)$, so by the lemma, $g \in \mathbb{C}[x_{\ell+1}, \dots, x_m] \cap G$. \square

2.4.1 Saturation of ideals

Definition. Given ideals I, J we define the saturation of I with respect to J as

$$(I : J^\infty) = \{f \in \mathbb{C}[x_1, \dots, x_m] \mid (\forall g \in J)(\exists k \in \mathbb{N}) g^k f \in I\}$$

Example 25. 1. $\langle x(x+1), y(x+1) \rangle : \langle x, y \rangle^\infty = \langle x+1 \rangle$

2. $\langle (x-y)xy, (x-y)^3x^4 \rangle : \langle x-y \rangle^\infty = \langle xy, x^3 \rangle$

Theorem 14. $V(I : J^\infty) = \overline{V(I)V(J)}$

Theorem 15. Let $I \subseteq \mathbb{C}[x_1, \dots, x_m]$ and $g \in \mathbb{C}[x_1, \dots, x_m]$. $I : \langle g \rangle^\infty = \langle I, 1-tg \rangle_{\mathbb{C}[x_1, \dots, x_m, t]} \cap \mathbb{C}[x_1, \dots, x_m]$

Remark. $g \in \sqrt{I} \iff 1 \in \langle I, 1-tg \rangle_{\mathbb{C}[x_1, \dots, x_m, t]} \iff (I : \langle g \rangle^\infty) \ni 1$

Prop. $(I : (J_1 + J_2)^\infty) = (I^\infty) \cap (I : J_2^\infty)$

Corollary 3. If $J = \langle g_1, \dots, g_s \rangle$, then $(I : J^\infty) = \bigcap_{i=1}^s (I : \langle g_i \rangle^\infty)$

2.5 Exercises

Exercise (1.2). Given a polynomial ring R like $\mathbb{C}[y]$, prove there are two polynomials $A, B \in R[x]$ such that $\text{Res}(f, g, x) = Ag + Bf$ such that $\deg_x(A) < \deg_x(g)$ and $\deg_x(B) < \deg_x(f)$. **Hint:** consider the adjugate matrix of the Sylvester matrix.

Solution. Recall our definition of the Sylvester matrix:

Definition (Resultant). Given $f(x, y) = \sum_{i=1}^m f_i(y)x^i \in \mathbb{C}[x, y]$ that is, $f \in \mathbb{C}[y]$, and $g = \sum_{i=1}^n g_i(y)x^i$. We define Sylvester matrix $\text{Sylv}(f, g, x)$.

$$\begin{pmatrix} f_m & 0 & \dots & 0 & g_m & 0 & \dots & 0 \\ f_{m-1} & f_m & \dots & 0 & g_{m-1} & g_m & \dots & 0 \\ & & \dots & & & & \dots & \\ f_0 & f_1 & \dots & f_m & g_0 & g_1 & \dots & g_m \\ 0 & f_0 & \dots & f_{m-1} & 0 & g_0 & \dots & g_{m-1} \\ & & \dots & & & & \dots & \\ 0 & 0 & \dots & f_0 & 0 & 0 & \dots & g_0 \end{pmatrix}$$

The resultant $\text{Res}(f, g, x) = \det \text{Sylv}(f, g, x) \in \mathbb{C}$.

Notice that for our excersie we need a more general definition: de degrees of f and g may be different. An attempt to write a general matrix is:

$$\begin{pmatrix} f_n & 0 & \dots & 0 & g_m & 0 & \dots & 0 \\ f_{n-1} & f_n & \dots & 0 & g_{m-1} & g_m & \dots & 0 \\ & & \dots & & & & \dots & \\ f_{n-m} & f_1 & \dots & f_m & g_? & g_1 & \dots & g_m \\ f_{n-(m-1)} & f_1 & \dots & f_{m-1} & g_? & g_1 & \dots & g_m \\ 0 & f_0 & \dots & f_? & 0 & g_0 & \dots & g_{m-1} \\ & & \dots & & & & \dots & \\ 0 & 0 & \dots & f_0 & 0 & 0 & \dots & g_0 \end{pmatrix}$$

So maybe we take $n = 2$, $m = 1$. Then $f = f_2x^2 + f_1x + f_0$ and $g = g_1x + g_0$, thus

$$\text{Sylv}(f, g, x) = \begin{pmatrix} f_2 & g_1 & 0 \\ f_1 & g_0 & g_1 \\ f_0 & 0 & g_0 \end{pmatrix}$$

Recall the formula

$$\det(A)Id = A^*A$$

donde A^* es la matriz adjunta. (unfinished)

□

3 Differential Algebra

We'll use the team's paper [falkensteiner2020fundamental], François' short notes (sent to us) and long notes [Francois], and Sebastian's notes [Sebastian]. Recall many ideas were first defined in [kolchin1973differential] and [ritt1950differential].

3.1 Differential polynomial rings and related notions

Definitions.

- An operator δ is called a **derivation operator** if $\delta(a + b) = \delta a + \delta b$ and $\delta(ab) = (\delta a)b + a\delta b$ for all elements a, b in a ring.
- A **partial differential ring** is a pair (R, D) consisting of a commutative ring with unity R and a set $D = \{\delta_1, \dots, \delta_n\}$ of $m > 1$ **derivations** which act on R and are pairwise commutative.
- We denote by Θ the free commutative monoid generated by D .
- Let (R, D) be a partial differential ring and x_1, \dots, x_n be n **differential indeterminates**. The monoid Θ acts on the differential indeterminates giving an infinite set of **derivatives**.
- We denote by $R\{x_1, \dots, x_n\}$ the ring of polynomials with coefficients in R and indeterminates which are the derivatives. So for example:

$$R\{x\} := R[x, \dot{x}, \ddot{x}, \dots]$$

are polynomials in the infinite set of derivative indeterminates. We may also denote this set by $R[\Theta X] = R\{x_1, \dots, x_n\}$ where X is the set of indeterminates.

- Then $(R\{x_1, \dots, x_n\}, D)$ is a **differential polynomial ring**.
- A differential polynomial induces an evaluation map from R^n to R . A **zero** or **solution** of $P \in R\{x_1, \dots, x_n\}$ is an n -tuple $\varphi \in R^n$ such that $P(\varphi) = 0$. For any $\Sigma \subseteq R\{x_1, \dots, x_n\}$ we denote $\text{Sol}\Sigma$ the set of solutions to every element of Σ .
- A **differential ideal** is an ideal in this ring that is stable under the action of Θ .
- A **perfect** differential ideal is an ideal that is equal to its radical.
- If $\Sigma \subseteq R\{x_1, \dots, x_n\}$ then $[\Sigma]$ is the ideal generated by Σ and $\{\Sigma\}$ is the perfect differential ideal generated by Σ , defined as the intersection of all perfect differential ideals containing Σ .

Prop. For any $\Sigma \subseteq R\{x_1, \dots, x_n\}$ there is a finite subset $\Phi \subset R^n$ such that $\text{Sol}\Sigma = \text{Sol}\Phi$.

3.2 Rankings

Definitions. Let $Y = \{y_1, \dots, y_n\}$ be a set of differential indeterminates.

- A **ranking** is a total ordering on ΘY such that for all derivative $u, v \in \Theta Y$ and all derivations $\theta \in \Theta$:

- $v \leq \theta v$
- $v < w \implies \theta v < \theta w$
- The **leading derivative** of $p \in \mathcal{F}\{y_1, \dots, y_n\}$ is the highest derivative $v \in \Theta Y$ such that the degree of p with respect to this derivative is positive, ie. $\deg(p, v) > 0$.
- Let $d = \deg(p, v)$ with v the leading derivative of p . Then v^d is the **rank** of p .
- **Thm.** Raking is a well-ordering (every finite strictly descending sequence of derivatives is finite).
- The **initial** of p is the leading coefficient in p seen as a univariate polynomial in v .
- The **separant** of p is the partial derivative of p with respect to its leading derivative.

So for example if $p = \dot{u}^2 + u^3$ its leading derivative is \dot{u} . So $\text{separant}(p) = \frac{\partial p}{\partial \dot{u}} = 2\dot{u}$ as u^3 is constant respect to \dot{u} .

3.3 Decomposition of Perfect Differential Ideals

First recall:

Definition.

- An ideal $\mathfrak{p} \subset R$ is **prime** if for all $a, b \in R$ we have $ab \in \mathfrak{p} \implies [a \in \mathfrak{p} \text{ or } b \in \mathfrak{p}]$.
- An ideal $\mathfrak{q} \subset R$ is **primary** if for all $a, b \in R$ we have $ab \in \mathfrak{q} \implies [a \in \mathfrak{p} \text{ or } \exists e \in \mathbb{N}, b^e \in \mathfrak{q}]$.

A representation of a perfect differential ideal \mathfrak{U}

$$\mathfrak{U} = \mathfrak{B}_1 \cup \dots \cup \mathfrak{B}_\varrho$$

is called **minimal** if for any different indices $1 \leq i, j \leq \varrho$ we have $\mathfrak{B}_i \not\subset \mathfrak{B}_j$.

Theorem 16 (From François's short notes). There exists a unique minimal representation of a perfect differential ideal \mathfrak{U} as a finite intersection of prime differential ideals.

Theorem 17 (From François's long notes. (Lasker-Noether Theorem)). For every ideal $\mathfrak{a} \subset R$ is a finite minimal intersection of of primary ideals

$$\mathfrak{a} = \mathfrak{q}_1 \cap \dots \cap \mathfrak{q}_r$$

Such a **minimal primary decomposition** is not necessarily unique but, if

$$\mathfrak{a} = \mathfrak{q}'_1 \cap \dots \cap \mathfrak{q}'_{r'}$$

is another minimal primary decomposition of \mathfrak{a} , then $r = r'$ and the 'set of the associated prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ of the two decompositions' is uniquely defined (that is, the \mathfrak{p}_i are the associated *prime* ideals of \mathfrak{a} , I think those from the last theorem).

3.4 Triangular sets and regular chains

(Here we pass from François's long notes [Francois] to Sebastian's notes [Sebastian].)

Let us say for now that a **triangular set** is a set of polynomials $A = \{p_1, \dots, p_r\}$ with some properties related to their leading variables (or leading derivatives, as defined earlier). Define $I_A = i_1 \dots i_r$ the product of the initial derivatives of the p_i .

Definition. The ideal generated by the triangular set A is denoted

$$\mathfrak{a} = (A) : I_A^\infty$$

And we shall also consider

$$(A) : S_A^\infty \quad \text{and} \quad (A) : H_A^\infty$$

where S_A^∞ is the product of the separants of A and H_A^∞ is the product of the initials and the separants of A .

Theorem 18. If A is a triangular set, then $(A) : S_A^\infty$ is radical.

Definition. Regular chain.

Theorem 19. For a given set of polynomials Σ there are finitely many regular differential chains A_1, \dots, A_ℓ such that

$$\{\Sigma\} = [A_1] : H_{A_1}^\infty \cap \dots \cap [A_\ell] : H_{A_\ell}^\infty$$

is a decomposition of the perfect differential ideal $\{\Sigma\}$ as an intersection of perfect differential ideals. We may “add H_i^∞ as inequalities to the regular differential chains A_i ”.

We shall call perfect differential ideals of the form $\mathfrak{U} = A : H_A^\infty$ given by single regular differential chains A **characterizable ideals**.

Using the “Thomas decomposition”, we find there is a decomposition of the solution space

$$\text{Sol}(\mathfrak{U}) = \bigcup_{1, \dots, \ell} \text{Sol}(A_i)$$

Theorem 20 (Nullstellensatz). If $\mathfrak{U} \subsetneq \mathcal{F}\{u_1, \dots, u_n\} := F\{\mathbf{u}\}$ is a radical differential ideal, then $\text{Sol}(\mathfrak{U}) \neq \emptyset$ and p is a polynomial that vanishes in $\text{Sol}(\mathfrak{U})$, then $p \in \mathfrak{U}$.

3.5 Zero testing

Definitions.

- Take a formal power series $u(x) \in \mathbb{C}[[x]] = \{\sum_{i=0}^\infty a_i x^i : a_i \in \mathbb{C}\}$. We call $u(x)$ **differentially algebraic** if there is $p \in \mathcal{F}\{u\} \setminus \mathcal{F}$ such that $p(u(x)) = 0$.
- In this case we say p is the **annihilator** of $u(x)$
- If p can be chosen to be in $\mathcal{F}[u] \setminus \mathcal{F}$, that is, if p doesn't involve any derivatives, we just say $u(x)$ is **algebraic**.

So what is this saying? Let p be just $p = \dot{u}$, then $p(u(x)) = \dot{u} = \sum_{i=1}^{\infty} a_i \cdot i \cdot x^{i-1}$. All there's to it really is a differential equation: if p annihilates $u(x)$, then we're just saying $\dot{u} = 0$. Thus every $p \in \mathcal{F}\{u\} \setminus \mathcal{F}$ is really a differential equation which can be evaluated in formal power series. (Notice formal power series are *not* the same as holomorphic functions in \mathbb{C}). So the roots of these polynomials are just the solutions of the differential equations. *That's the whole idea.*

Prop. The set of differentially algebraic functions is a ring which is closed under composition, differentiation and division (if they are defined).

The coefficients of a differentially algebraic function cannot be arbitrary:

Prop. A formal power series $u(x)$ is differentially algebraic over $\mathcal{F} \iff \mathcal{F}\{u(x)\}$ has finite transcendence degree over \mathcal{F} .

Example 26. $u(x) = 1 + \log(x)$ is differentially algebraic but not algebraic with annihilator $p = x\dot{u} - 1$. Now consider $q = \exp(u) - 1$. Then $q(u(x)) \neq 0$ but $q(0 + \log(x)) = 0$ Why?

Remark (Structural relation). $\text{prem}(q, A) = 0 \iff q \in \{A\} \iff \text{Sol}(A) \subseteq \text{Sol}(q)$

Example 27.

$$\begin{aligned} A &= \{p_1 = u^2 - x^3, p_2 = v^5 - x^3 u\} \\ q &= 8u'^3 - 27u \\ (u(x), v(x)) &= (x^{3/2}, x^{9/10}) \text{ is a zero of } A \text{ and } \text{prem}(q, A) \neq 0 \end{aligned}$$

And now make a slight change in p_2 :

$$\begin{aligned} A &= \{p_1 = u^2 - x^3, p_2 = v^{10} - x^9\} \\ q &= 8u'^3 - 27u \\ (u(x), v(x)) &= (x^{3/2}, x^{9/10}) \text{ is again a zero of } A \text{ and } \text{prem}(q, A) \neq 0 \end{aligned}$$

but in this second case we also have $q(u(x), v(x)) = 0$.

So if the remainder was zero then we would already have an answer for the zero testing. If not, we are showing what to do.

3.6 Root separation bound

Take $p \in \mathcal{F}\{u\}$ to be the annihilator of $u(x)$. Then $\rho \in \mathbb{N}$ called a **root separation bound** at $u(x)$ if it is the smallest number such that for every $v(x) \in \text{Sol}(p) \setminus \{u(x)\}$, $\text{ord}(u(x) - v(x)) > \rho$. This is like a smallest distance between all the solutions of p . (We are somehow trying to isolate roots so as to find solutions to differential equations.)

Algorithm 3 ZeroTest(q)

Input : $u(x) \in \mathbb{C}[[x]]$ with annihilator $p \in \mathcal{F}\{u\}$ and $q \in \mathcal{F}\{u\}$

Output: **true** if $q(u(x)) = 0$ and **false** otherwise

1. If $q \in \mathbb{C}[x]$, return $q = 0$
2. If ZeroTest(Iq) then return ZeroTest($\text{prem}(q, Iq)$)
3. If ZeroTest(Sq) then return ZeroTest($\text{prem}(q, Sq)$)
4. If $\text{prem}(q, p) \neq 0$ then return ZeroTest($\text{prem}(q, p)$)

return $\text{ord}_x(q(u(x))) > 2\rho_{q,u(x)}$

3.7 Counting solutions of differential equations

Let $p \in \mathcal{F}\{u\}$. Where $p(u(x)) = 0$ is of finite transcendence degree.

Definitions (And an example).

- (Chat GPT). Let L/K be a field extension, and let α be an element of L . The transcendence degree of α over K , denoted as $\text{trdeg}_K(\alpha)$, is the transcendence degree of the field extension $K(\alpha)/K$. It measures the number of algebraically independent elements in $K(\alpha)$ over K .
- Let \mathfrak{U} (for example, $\mathfrak{U} = (u^3, u, v) \subseteq \mathbb{Q}[u, v]$) be an algebraic prime ideal. Then $\dim \mathfrak{U}$ is defined as the transcendence degree of $\mathcal{F}(\mathbf{u})/\mathfrak{U}$. This is computed via Gröbner basis.
- The Hilbert Function is

$$\begin{aligned} \Omega_{\mathfrak{U}} : \mathbb{N} &\rightarrow \mathbb{N} \\ \ell &\mapsto \dim(\mathcal{F}(\mathbf{u}_{\ell})/\mathfrak{U}_{\ell}) \end{aligned}$$

So in our example we have $\Omega_{\mathfrak{U}}(0) = 1, \Omega_{\mathfrak{U}}(1) = 3, \Omega_{\mathfrak{U}}(\ell) = \ell + 3$ for $\ell \geq 2$, so this is a polynomial in ℓ .

Computed the generic solutions of the system of differential equations given by

$$u_i(\mathbf{x}) = u_i(x_1, \dots, x_m) = \sum c_{i,\theta} (x_1 - \xi_1)^{e_1} \dots (x_m - \xi_m)^{e_m}$$

then derived algebraic condicions on the $c_{i,\theta}$ for the differential dimension: number of unspecified coefficients, differential counting, number of possible chrees (?).

So let $\mathfrak{U} \subseteq \mathcal{F}\{\mathbf{u}\}$ be a differential ideal. Usually require that \mathfrak{U} is given via a regular differential chain, that is $\mathfrak{U} = [A]$. So now we have a **differential dimension function**

$$\begin{aligned} \Omega_{\mathfrak{U}} : \mathbb{N} &\rightarrow \mathbb{N} \\ \ell &\mapsto \dim(\mathcal{F}(\mathbf{u}_{\leq \ell})/\mathfrak{U}_{\leq \ell}) \end{aligned}$$

Where $\mathfrak{U}_{\leq \ell}$ are the elements in \mathfrak{U} of order less or equal to ℓ .

Prop. Is \mathfrak{U} is a characterizable differential ideal with corresponding regular differential chain A , and set of leading derivatives $\text{lead}(A)$, then for every $\ell \in \mathbb{N} \cup \{\infty\}$ we have

$$\Theta\{\mathbf{u}\}_{\leq \ell} \setminus \Theta \text{lead}(A)_{\leq \ell} = \dim(\{\mathbf{u}\}/\mathfrak{U}_{\leq \ell})$$

Example 28. The Burger's equation $p = u_{x_1, x_1} - u_{x_2} - 2uu_{x_1}$ defines a regular differential chain (w.r.t. any ranking). We shall obtain that $\omega_{\{p\}}(\ell) = 2\ell + 1$.

So whenever we have our assumption that $\mathfrak{U} = [A]$ then the counting function will be a polynomial in ℓ .

Theorem 21.

1. There exists a numerical polynomial $\omega_{\mathfrak{U}} \in \mathbb{Q}[\ell]$, called the **differential dimension** polynomial, with $\Omega_{\mathfrak{U}}(\ell) = \omega_{\mathfrak{U}}(\ell)$ for sufficiently large $\ell \in \mathbb{N}$.
2. This polynomial is of degree less or equal to n and can be written as $\omega_{\mathfrak{U}}(\ell) = \sum_{i=1}^m a_i \binom{\ell+i}{i}$ for some $a_i \in \mathbb{Z}$.
3. a_m is the **differential dimension**
4. If $\mathfrak{B} = [B]$ is another characterizable ideal of $\mathcal{F}\{\mathbf{u}\}$ with respect to the same ranking. It $\mathfrak{U} \subseteq \mathfrak{B}$, then $\omega_{\mathfrak{U}} \leq \omega_{\mathfrak{B}}$. Moreover, $\mathfrak{U} = \mathfrak{B}$ if and only if
 - $\omega_{\mathfrak{U}} = \omega_{\mathfrak{B}}$
 - The set of leaders of the corresponding regular chains are the same.
 - The equations have the same degree.

Let us make a super simple example

Example 29. Take $p = u_{x_1} = 0$ with $u(x_1, x_2) = \sum c_{ij} x_1^i x_2^j$. So

$$\frac{\partial}{\partial x_1}(u(x_1, x_2)) = \sum c_{ij} i x_1^{i-1} x_2^j = 0$$

and here $c_{ij} = 0 \forall i > 0, j \in \mathbb{N}$. Then c_{0j}, \dots are free coefficients for all $j \in \mathbb{N}$.

3.8 Representation of differential equations

Algebraic varieties are the zero sets of polynomials, that, as geometric objects, they can be sometimes represented with a parametrization. We attempt to do this for differential system with what we shall call **realizations**.

Algebraic case

- $\mathbb{V}(p)$ has a parametrization if and only iff genus is zero. For higher genus we might glue local parametrizations.
- For $p \in \mathbb{Q}[u_1, \dots, u_n]$ there exists an algorithm for deciding the existence of a rational parametrization of $\mathbb{V}(p)$ in the case of $n = 2, 3$, and it can compute it.

Differential case Now take $\{p_1, \dots, p_r\} \in \mathcal{F}\{u_1, \dots, u_n\}$. An **explicit representation** of these polynomials is a dynamical system

$$\begin{cases} \dot{\mathbf{t}} = \mathbf{f}(\mathbf{t}, \mathbf{y}) \\ \mathbf{u} = \mathbf{g}(\mathbf{t}, \mathbf{y}) \end{cases}$$

where everything is bold because they are vectors. So \mathbf{f}, \mathbf{g} are rational functions in \mathbf{t}, \mathbf{y} .
Let us now consider the problem of going from a realization to an implicit representation.

$$\begin{aligned} \dot{\mathbf{t}} \cdot \mathbf{Q} - \mathbf{F}, \quad \mathbf{u} \cdot \mathbf{Q} - \mathbf{G} \\ \frac{\mathbf{F}}{\mathbf{Q}} = f_i, \quad \frac{\mathbf{G}}{\mathbf{Q}} = g_i \\ \text{(unfinished)} \end{aligned}$$

Anyway, to go back to a realization, it is a necessary condition that $\mathbb{V}(p_1, \dots, p_r)$ is a rational variety.

So let us consider a polynomial $p \in \mathbb{Q}\{x, y\} = \mathbb{Q}[u, \dots, u^{(N)}, y, \dots, y^{(N)}]$ and $\mathbf{a}(t) \in \mathbb{Q}(y)(t) \times \mathbb{Q}(y, \dots, y^{(N)})(\mathbf{t})^N$ a rational parametrization of a hypersurface $\mathbb{V}(p)$. And eventually conclude that

$$\mathbb{V}(p) \text{ is rational} \iff p \text{ is realizable}$$

3.9 Finding solutions

3.9.1 Rational solutions

We look for solutions like

$$u(x) = \frac{c_0 + c_1 x + \dots + c_r}{d_0 + d_1 x + \dots + d_k x^k}$$

for $r, k \in \mathbb{N}$.

We may have $p_1, \dots, p_m \in \mathbb{Q}(\mathbf{x})\{\mathbf{u}\}$ and assume that $\mathbb{V}(p_1, \dots, p_m)$ is rational. Now we may take a rational parametrization \mathcal{P} of it, so there is a dynamical system such that

$$\begin{aligned} (1) \quad \sqrt{\mathbf{t}(\mathbf{x})} &= \mathbf{u}(x) \\ (2) \quad \mathbf{u}(\mathbf{x}) &\notin \text{img}(\mathcal{P}) \end{aligned}$$

for some $\mathbf{t}(\mathbf{x}) \in \mathbb{Q}(\mathbf{x})^N$. We develop necessary and sufficient conditions for finding solutions of rational first order differential equations:

Theorem 22. For $p \in \mathbb{Q}[u, u']$, the equation $p = 0$ has a rational solution, then $\mathbb{V}(p)$ is a rational algebraic variety.

If $\mathcal{P} = (p_1, p_2)$ is a rational parametrization of $\mathbb{V}(p)$, then $t = \frac{p_2}{p_1}$ has a rational solution if and only if $\exists a, b \in \mathbb{Q}$ such that $\frac{p_2}{p_1} = b(t - a)^2$. In this case, $u(s) = p_1(t(x + c))$ is a rational generic solution.

Example 30. Let $p = \dot{u}^3 + 4\dot{u}^2 + (27u^2 + 4)\dot{u} + 27u^4 + 4u^2$ and $\mathcal{P} = (216t^3 + 6t, -3888t^4 - 36t^2)$. So we have

$$\begin{aligned} p_2/p_1' &= -6t^2 = t' \\ t(x) &= \frac{1}{6(x + c)} \\ \implies u(x) &= p_1(t(x)) = \frac{(x + c)^2 + 1}{(x + 2)^2} \end{aligned}$$

3.9.2 Algebraic solutions

We now consider $u(x)$ as a zero of $q(x, u)$ for $p \in \mathbb{Q}[u, u']$. And we must

- Compute a local solution $u(x)$.
- Guess/check whether $u(x)$ is algebraic.

Theorem 23. If there exists an algebraic solution of $p = 0$, then all local solutions of $p = 0$ are algebraic. If $q(x, u)$ is the minimal polynomial associated, then

$$\deg_x(q) = \deg_{u'}(p), \quad \deg_u(q) \leq \deg_u(p) + \deg_{u'}(p)$$

Example 31. Take $p = u^4 + 3u'$ and $\mathcal{P} = (t, -t^4/3)$ so that $p_2/p_1' = \frac{-t^4/3}{t}$ and there's no rational solutions. Then, for the initial value $u(0) = 1$ and $u'(0) = -1/4$. Eventually we arrive to $q = xu^3 - 1$

3.9.3 Local solutions

Take $p \in \mathbb{Q}[u, u']$ so that $\mathbb{V}(p)$ always admits a local parametrization $\mathcal{P} \in \mathbb{Q}((t))^2 \setminus \mathbb{Q}^2$ which can be computed using the Puiseux expansion as was shown in Fuensanta's course.

Theorem 24. Take a local parametrization $o := \mathcal{P} = (p_1, p_2)$ of $\mathbb{V}(p)$. If $\text{ord}(p_1 - p_2(0) - \text{ord}(p_2)) > 0$ then there exist exactly o -many formal power solutions of p with initial value $u(0) = p_1(o)$, $u'(0) = p_2(o)$ and the corresponding branch (we must always choose a branch).

Example 32. $p = ((u' - 1)^2 + u^2)^3 - 4(u' - 1)^2 u^2 = 0$ and $(p_1, p_2) = (t^2, 1 + \sqrt{2} + \frac{3t^3}{4\sqrt{2}} + \dots)$

We shall obtain that $u(x) = x \pm \frac{2\sqrt{2}x^{3/2}}{3} + \dots$

Notas2/LastFig.png

3.10 (Extra) Another view of Tropical Geometry

Now that we've read some of [falkensteiner2020fundamental], let us define the following ideas that are related to the Tropical Geometry course:

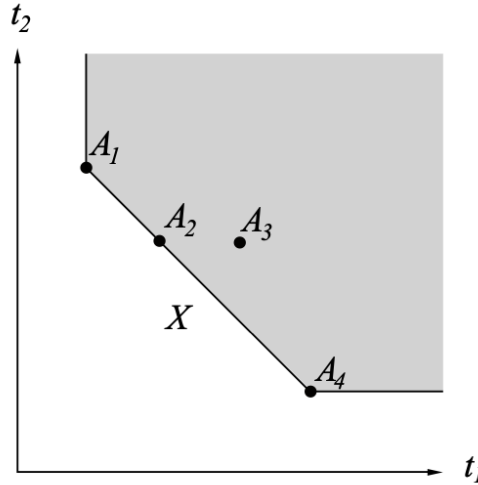
Definition.

- For $m \geq 1$ denote by $\mathcal{P}(\mathbb{Z}_{\geq 0}^m)$ the idempotent semiring whose elements are the subsets of $\mathbb{Z}_{\geq 0}^m$ equipped with the union $X \cup Y$ as sum and the Minkowsky sum $X + Y = \{x + y : x \in X, y \in Y\}$ as product. (Here nX denotes the sum of X n times). This structure is the **semiring of supports**.
- For an element $X \in \mathcal{P}(\mathbb{Z}_{\geq 0}^m)$, we define the **Newton polygon** $\mathcal{N}(X) \subseteq \mathbb{R}_{\geq 0}^m$ as the convex hull of $X + \mathbb{Z}_{\geq 0}^m$. It looks like this is all the right-up translates of the set X .
- Now we call $x \in X$ a vertex if it is in the left-down boundary of the Newton polygon, that is, is $x \notin X \setminus \{x\}$. And we denote $\text{Vert}X$ the set of vertices of X .

Lema. If two subsets $S, T \in \mathcal{P}(\mathbb{Z}_{\geq 0}^m)$ have the same Newton polygon, then their vertices sets are the same.

Lema. The Newton polygon of the vertex set of X is the same as the Newton polygon of X , that is, for any $X \in \mathcal{P}(\mathbb{Z}_{\geq 0}^m)$, $\mathcal{N}(X) = \mathcal{N}(\text{Vert}(X))$.

Corollary 4. For any $X, Y \in \mathcal{P}(\mathbb{Z}_{\geq 0}^m)$, we have $\text{Vert}(X) = \text{Vert}(Y) \iff \mathcal{N}(X) = \mathcal{N}(Y)$



Example of a Newton polygon

Definition.

- Define the map $\text{Vert} : \mathcal{P}(\mathbb{Z}_{\geq 0}^m) \rightarrow \mathcal{P}(\mathbb{Z}_{\geq 0}^m)$, which satisfies, by the Corollary, that $\text{Vert}^2 = \text{Vert}$.

- Denote by $\mathbb{T}[[t_1, \dots, t_m]]$ the image of the operator Vert , whose elements we call **vertex sets** or **tropical formal power series**. We define for $S, T \in \mathbb{T}[[t_1, \dots, t_m]]$,

$$S \oplus T = \text{Vert}(S \cup T) \quad \text{and} \quad S \odot T = \text{Vert}(S + T)$$

3.11 Problems on algebraic differential equations

1. Finding rational algebraic d finite solutions (solutions of algebraic equations with polynomial coefficients) of algebraic differential equations.

We know some things about the support (the zeroes) the functions involved in these equations. Use this knowledge to say something about possible solutions. This is known only for linear differential equations—we should be able to work on other types of differential equations.

2. Which eliminations and combinations could be used for simplifying differential systems? Maybe something from tropical algebraic geometry could help!
3. What we used for the computations of the solutions in 1. can also be used for computing simplifications of algebraic systems. Speed up computations.
4. Prove DL (Denef and Lipsitz) Thm 3.1.

3.12 Exercises

Exercise. Apply the Zero-Testing algorithm to $u(x) = \sqrt{1+x}$ and q for checking whether $q(u(x)) = 0$.

- a) $q = 2uu' - 1$
- b) $q = 2uu' - 1 + x^{10}/10^{10}$
- c) $q = (2uu' - 1)u'' - xu + 1$

Solution. Let us recall the Zero-Testing algorithm:

Algorithm 4 ZeroTest(q)

Input : $u(x) \in \mathbb{C}[[x]]$ with annihilator $p \in \mathcal{F}\{u\}$ and $q \in \mathcal{F}\{u\}$

Output: **true** if $q(u(x)) = 0$ and **false** otherwise

1. If $q \in \mathbb{C}[x]$, return $q = 0$
 2. If ZeroTest(I_q) then return ZeroTest($\text{prem}(q, I_q)$)
 3. If ZeroTest(Sq) then return ZeroTest($\text{prem}(q, Sq)$)
 4. If $\text{prem}(q, p) \neq 0$ then return ZeroTest($\text{prem}(q, p)$)
- return** $\text{ord}_x(q(u(x))) > 2\rho_{q,u(x)}$
-

- a) We have: $q \notin \mathbb{C}[x]$, so we find $I_q = 2u \notin \mathbb{C}[x]$. So then we go on to find $S_q = I_q = 2u \notin \mathbb{C}[x]$. Now we must find the annihilator: $p = u^2 - 1 - x$. Which has derivative $2uu' - 1 = q$, so that $\text{prem}(q, p) = 0$, and we go to the last line of the algorithm, which happens to be **true**. Of course: $q(u(x)) = 2\sqrt{1+x}(1/2)(1+x)^{-1/2} - 1 = 0$.

- b) Again $q \notin \mathbb{C}[x]$, $I_q = 2u \notin \mathbb{C}[x]$ and also $S_q = I_q = 2u \notin \mathbb{C}[x]$. We have the same annihilator $p = u^2 - 1 - x$ with has derivative $2uu' - 1 = q$. But how to calculate $\text{prem}(p, q)$?

□

4 Tropical Differential Algebra

Let us consider a system of differential equations in \mathbb{R}^4 :

$$\begin{cases} \frac{\partial y_1}{\partial t} &= \frac{1}{1200}y_1(t) + \frac{1}{500}y_2(t) + \frac{1}{500}y_3(t) \\ \frac{\partial y_2}{\partial t} &= \frac{1}{1500}y_1(t) - \frac{1}{1000}y_2(t) + \frac{1}{1000}y_3(t) + \frac{1}{1000}y_4(t) \\ \frac{\partial y_3}{\partial t} &= -\frac{1}{1000}y_1(t) - \frac{1}{500}y_2(t) + \frac{1}{500}y_3(t) + \frac{1}{1000}y_4(t) \\ \frac{\partial y_4}{\partial t} &= \frac{1}{1000}y_1(t) - \frac{1}{1000}y_3(t) \end{cases}$$

Where $y_i \in \mathcal{C}^1(\mathbb{R}^4)$. We can rewrite this as

$$\frac{d\mathbf{y}}{dt} = \mathbf{A}\mathbf{y}$$

That is,

$$\begin{pmatrix} \frac{\partial y_1}{\partial t} \\ \frac{\partial y_2}{\partial t} \\ \frac{\partial y_3}{\partial t} \\ \frac{\partial y_4}{\partial t} \end{pmatrix} = \begin{pmatrix} \frac{1}{1200} & \frac{1}{500} & \frac{1}{500} & 0 \\ \frac{1}{1500} & -\frac{1}{1000} & \frac{1}{1000} & \frac{1}{1000} \\ -\frac{1}{1000} & -\frac{1}{500} & \frac{1}{500} & \frac{1}{1000} \\ \frac{1}{1000} & 0 & -\frac{1}{1000} & 0 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \end{pmatrix}$$

It turns out \mathbf{A} is diagonalizable, and the system can be converted to

$$\begin{pmatrix} \frac{\partial x_1}{\partial t} \\ \frac{\partial x_2}{\partial t} \\ \frac{\partial x_3}{\partial t} \\ \frac{\partial x_4}{\partial t} \end{pmatrix} = \begin{pmatrix} 0.001 & 0 & 0 & 0 \\ 0 & -0.001 & 0 & 0 \\ 0 & 0 & 0.001 & 0 \\ 0 & 0 & 0 & -0.001 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix}$$

That is,

$$\begin{cases} \frac{\partial x_1}{\partial t} &= 0.001x_1(t) \\ \frac{\partial x_2}{\partial t} &= 0.001x_2(t) \\ \frac{\partial x_3}{\partial t} &= -0.001x_3(t) \\ \frac{\partial x_4}{\partial t} &= -0.001x_4(t) \end{cases}$$

And has solution

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} x_1(0)e^{0.001t} \\ x_2(0)e^{0.001t} \\ x_3(0)e^{-0.001t} \\ x_4(0)e^{-0.001t} \end{pmatrix}$$

Where the exponents here are the eigenvalues.

Now let us choose initial conditions $x_1(0) = x_2(0) = x_3(0) = x_4(0) = 1/2$.

So now we can change back to the original variables using the matrix made up of the eigenvectors:

$$\begin{pmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \end{pmatrix} = \begin{pmatrix} 1 & 1 & -1 & -1 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & -1 \\ 0 & 1 & 1 & 0 \end{pmatrix} \begin{pmatrix} \frac{1}{2}e^{0.001t} \\ \frac{1}{2}e^{0.001t} \\ \frac{1}{2}e^{-0.001t} \\ \frac{1}{2}e^{-0.001t} \end{pmatrix} = \begin{pmatrix} \frac{1}{2}e^{0.001t} + \frac{1}{2}e^{0.001t} - \frac{1}{2}e^{-0.001t} - \frac{1}{2}e^{-0.001t} \\ \frac{1}{2}e^{0.001t} + \frac{1}{2}e^{-0.001t} \\ \frac{1}{2}e^{0.001t} - \frac{1}{2}e^{-0.001t} \\ \frac{1}{2}e^{0.001t} + \frac{1}{2}e^{0.001t} + \frac{1}{2}e^{-0.001t} \end{pmatrix}$$

We now ask two questions:

Question 1.

Is it possible to tell apart between complex systems with feedbacks that create periodic solutions and the ones that do not have them through the classification of combinatoric objects in $\mathbb{B}[[t_1, t_2, \dots, t_n]]$? (Here \mathbb{B} is a Boolean field so coefficients are 0's and 1's).

So maybe there's a way to make a solution like

$$\begin{pmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \end{pmatrix} = \begin{pmatrix} \frac{1}{2}e^{0.001t} + \frac{1}{2}e^{0.001t} - \frac{1}{2}e^{-0.001t} - \frac{1}{2}e^{-0.001t} \\ \frac{1}{2}e^{0.001t} + \frac{1}{2}e^{-0.001t} \\ \frac{1}{2}e^{0.001t} - \frac{1}{2}e^{-0.001t} \\ \frac{1}{2}e^{0.001t} + \frac{1}{2}e^{0.001t} + \frac{1}{2}e^{-0.001t} \end{pmatrix}$$

Into a combinatorial object like

$$\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}$$

(number choices here are random). So its a matrix in \mathbb{B} .

Question 2. Are there subgroups of $\text{Aut}(\mathbb{D}^2)$ such that their combinatorial objects are generated by a non tropical vector?

Are there new properties on gradient flows over hyperbolic compact manifolds $\mathbb{D}^2/\text{Trop}(G)$?

So take a function $\omega : B_0^k \subseteq \mathbb{C} \rightarrow \mathbb{C}$ with $R = |z_0|$. And a nonlinear (but not complicated) differential equation

$$\begin{aligned} \frac{\partial \omega}{\partial z} &= \frac{\alpha}{c} \omega^2 \\ \omega(0) &= \beta + \frac{\alpha}{c} \frac{1}{z_0} \\ \omega(z) &= \beta + \frac{\alpha}{c} \frac{1}{z - z_0} = \beta + \frac{\alpha}{c} \sum_{i=0}^{\infty} \frac{1}{z_0^{(i)}} z^i \end{aligned}$$

and recall $\text{Aut}(\mathbb{D}^2) = \left\{ \frac{az+\bar{c}}{cz+\bar{u}} : |a|^2 - |c|^2 = 1 \right\}$

4.1 Tropical Differential Algebraic Geometry

Let k be a field of characteristic 0 and $m, n \in \mathbb{N}$. Define

$$k_{m,n} = k[[t_1, \dots, t_m]][x_i, J : 1 \leq i \leq n, J \in \mathbb{N}^m]$$

to be a ring inspired in $\mathcal{F}\{\mathbf{u}\}$ which had m variables u_1, \dots, u_m and infinite derivatives. Also define the monoid $\Theta \cong \mathbb{N}^m = \langle \frac{\partial}{\partial t_1}, \dots, \frac{\partial}{\partial t_m} \rangle$, and keep in mind the notation $\frac{\partial^{|\mathbf{J}|}}{\partial t_1^{j_1} \dots \partial t_m^{j_m}}$ for $J = (j_1, \dots, j_m) \in \mathbb{N}^m$.

Then Θ acts on $k_{m,n}$ by taking derivations of the functions. We shall work in the pair formed by our ring and this action, that is $(k_{m,n}, \Theta : \mathbb{N}^m \times k_{m,n} \rightarrow k_{m,n})$.

Define a differential equation E to be **algebraic** if there exists $p \in k_{m,n}$ such that $V(p) \cong \text{Sol}(E) = \{\varphi \in k[[t]] : p(\varphi) = 0\}$. Let us arrive to tropical geometry from here.

4.2 Twisted evaluation actions

This is a map $ev_{P,\Theta} : k[[t_1, \dots, t_m]]^n \rightarrow S[[t_1, \dots, t_m]]$ for $P \in S_{m,n}$.

Example 33. Take the system $P \in \mathbb{C}_{2,1}$ with

$$\begin{cases} P = tx_{(1,0)} + ux_{(0,1)} + (t^2 + u^3) \\ E = t \frac{\partial \varphi}{\partial t} + u \frac{\partial \varphi}{\partial u} + (t^2 + u^3) \end{cases}$$

so that by choosing

$$\begin{aligned} \varphi &= t^2 + t^1 u + u^3 \in \mathbb{B}[[t, u]] \\ \frac{\partial \varphi}{\partial t} &= t + u \\ \frac{\partial \varphi}{\partial u} &= t + u^2 \end{aligned}$$

we get

$$\begin{aligned} ev_{(P,\Theta)}(\varphi) &= t(t + u) + u(t + u^2) + (t^2 + u^3) \\ &= (t^2 + tu) + (tu + u^3) + t^2 + u^3 \\ &= t^2 + tu + u^3 \end{aligned}$$

with $\varphi \in \mathbb{C}[[t, u]]$.

Remark. Although we'd like to define $\varphi \in \mathbb{B}[[t, u]]$ to be a solution of $P \in \mathbb{B}_{2,1}$ is $P(\varphi) = 0$, this will not work. Why?

4.3 Combinatorics

Consider an operation $\mathbb{V} : \mathbb{B}[[t, u]] \rightarrow \mathbb{B}[[t, u]]$ that takes the Newton Polygon of a series and gives back the polynomial determined by the points in the boundary of the Newton Polygon. This is called the **vertex polynomial**. Now consider:

$$\begin{array}{ccc} \mathbb{B}[[t, u]] & \xrightarrow{\mathbb{V}} & \mathbb{B}[[t, u]] \\ & \searrow & \uparrow \\ & & (\mathbb{V}\mathbb{B}[[t, u]], \oplus, \odot) \end{array}$$

So it turns out we have a semiring $(\mathbb{V}\mathbb{B}[[t, u]], \oplus, \odot)$.

Definition. Let $a_1 \oplus \dots \oplus a_k = a$ be a sum in $\mathbb{V}\mathbb{B}[t, u]$. This sum **vanishes tropically** if $\forall (i, j) \in a$ there exist $\alpha \neq \beta$ such that $(i, j) \in a_\alpha, a_\beta$.

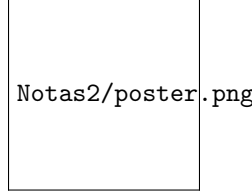
Example (30 Continued). It turns out this example vanishes tropically. This example wasn't easy to find.

Lema. If $\varphi \in \text{Sol}(p)$, then $\text{supp}(\varphi) \in \text{Sol}(\text{supp}(p))$.

Which is easy to prove. And then we have:

Theorem 25. For an ideal $[\Sigma] \subset K_{m,n}$ with $m, n \geq 1$, $\text{Sol}(p_1, \dots, p_s) = \bigcap_{p \in [\Sigma]} \text{Sol}(\text{supp}(p))$

Take a look at the school's poster:



So that combinatorial objects given by the supp map give us information on the solutions of differential equations.

Remark. Unlike notions of tropical convexity, tropical linear spaces are correctly defined using matroids. There is a relationship between matroids and tropical algebraic varieties that leads to visual figures.

4.4 An application of the lema

Let's go for a theorem.

Definition (Circuits). Take $E \neq \emptyset$ and $\mathcal{C} \subset \mathcal{P}(E)$ such that

- $\emptyset \notin \mathcal{C}$.
- $S, T \in \mathcal{C} \implies S \not\subset T$ and $T \not\subset S$

Definition (Scruls). It's a free semigroup on circuits. $\mathcal{S} = \{C_1 \cup C_2 \cup C_3 \cup \dots, \bigcup_{i \in I} C_i \neq \emptyset, C \in \mathcal{S} \text{ s.t. } C \text{ is maximal}\}$

Theorem 26 (A.L.S.G.). Let $W \subset K^E$ be a vector space with E infinite uncountable and $\dim W < \infty$. Then

$$\{\text{supp}(v) : v \in W\} \subset \mathcal{P}(E)$$

is a matroid of scruls.

So let $\Sigma \subset K_{m,n}$ be a h.s.l.d.e. such that $\dim \text{Sol}(\Sigma) < \infty \implies \text{supp}(\text{Sol}(\Sigma)) \subseteq \mathbb{B}[t_1, \dots, t_m]^n$. And we may consider the map

$$\mathbb{B}[t_1, \dots, t_m] \rightarrow \mathbb{B}[t_1, \dots, t_m, t_n, \dots, t_{nm}]$$

Remark (s).

- It would be nice to have a scheme theory on tropical fields so as to have better geometry.
- We are still looking for applications of this technology.
- *Don't we lose too much (qualitative) information when we booleanize differential equations?* Tropical geometry is “made to lose” information. How much of it can we recover?

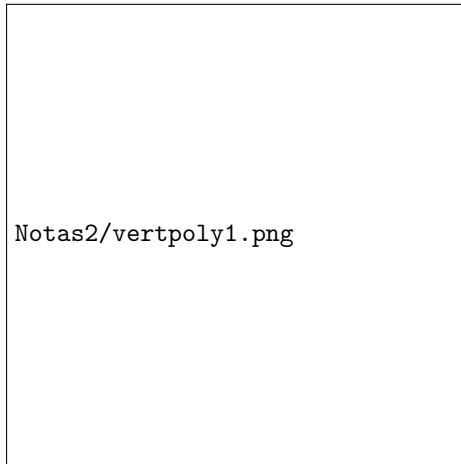
4.5 Exercises

Exercise (4.1 (b)). We attempt to show that the sum of two polynomials is not equal to the union of each vertex set. Recall a vertex polynomial is a set of points in convex position.

Exercise (4.2). Consider $a = t^2u^3 + t^3u + t^5 = \{(2, 3), (3, 1), (5, 0)\}$ and $b = u^4 + tu^3 + t^4u^2 = \{(0, 4), (1, 3), (4, 2)\}$ in $\mathbb{B}[[t, u]]$.

- (1) Show that a and b are vertex polynomials.
- (2) Compute $a \oplus b$ and $a \odot b$ and show that the inclusion $a \oplus b \subset V(a) + V(b)$ is proper.

Solution. (1)



a



b

- (2) We have $a \oplus b = V(a + b)$ and $a \odot b = V(ab)$ with the operations of $\mathbb{B}[[t, u]]$. So $a + b = t^2u^3 + t^3u + t^5 + u^4 + tu^3 + t^4u^2 = (\text{unfinished})$.

□

5 Newton's Method

(See [casas2019algebraic])

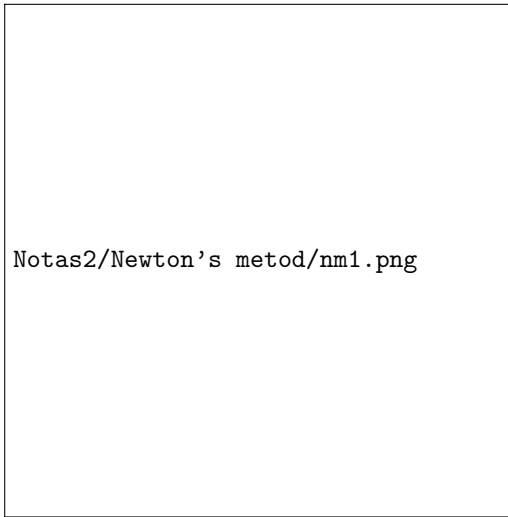
We will study Newton's method to parametrize algebraic curves, published in 1671. So let us start with a curve defined to be the zeroes of some function $f(x, y) = 0$. We wonder if it is possible to make y a function of x so as to parametrize the curve.

Let us agree that $f(0, 0) = 0$ translating if necessary. Using the Implicit Function Theorem, we know that if $\frac{\partial f}{\partial y}(0, 0) \neq 0$, then there exists an expression $y(x) = \sum_{i=1}^{\infty} c_i x^i$ such that $f(x, y(x)) = 0$.

We will say that if $\frac{\partial f}{\partial y}(0, 0) = 0 = \frac{\partial f}{\partial x}(0, 0)$ then $(0, 0)$ is a **singular point** of $f(x, y) = 0$.

Example 34. Take the curve

$$y^3 - x^2 = 0 \implies y(x) = x^{3/2}$$



In general, we have $f(x, y) = \sum_{(i,j) \in \mathbb{Z}_{\geq 0}^2} a_{ij} x^i y^j$ where the a_i are complex numbers, or elements in any algebraically closed field with characteristic 0.

Remark. Although there may not be a positive convergence ratio about $(0, 0)$, we can always evaluate our function in this exact point.

We are looking for an expression

$$y(x) = \sum_{i=0}^{\infty} c_{\mu_i} x^{\mu_i}, \quad \mu_i < \mu_j, \quad \mu_i \neq 0$$

Which of course is

$$y(x) = c_{\mu_0} x^{\mu_0} + \sum_{i>0}^{\infty} c_{\mu_i} x^{\mu_i} := c_{\mu_0} x^{\mu_0} + \bar{y}$$

and we might as well take the bar and the zero off and just write $c_\mu x^\mu + y$.

We require that

$$\begin{aligned}
0 &= f(x, y) \\
&= \sum_{(i,j) \in \mathbb{Z}_{\geq 0}^2} a_{ij} x^i y^j \\
&= \sum_{(i,j)} a_{ij} x^i (c_\mu x^\mu + y)^j \\
&= \sum_{(i,j)} a_{ij} x^i \sum_{k=0}^j \binom{j}{k} c_\mu^k x^{k\mu} + y^{j-k} \quad \text{binomio de Newton} \\
&= \sum_{(i,j)} \sum_{k=0}^j a_{ij} c_\mu^k x^{i+k\mu} + y^{j-k} \\
&= \sum_{(i,j)} a_{ij} c_\mu x^{i+j\mu} + \bar{y}
\end{aligned}$$

Now let $m = \min_{a_{ij} \neq 0} i + j\mu$ then

$$\sum_{i+j\mu=m} a_{ij} c_\mu^j x^m = 0 \iff \sum_{i+j\mu=m} a_{ij} c_\mu^j = 0$$

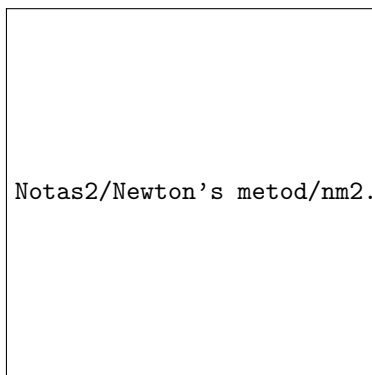
Definition. Given a formal power series $f \in \mathbb{C}[[x, y]]$, the **support** of f is $\text{supp}(f) = \{(i, j) : a_{ij} \neq 0\}$

Example 35.

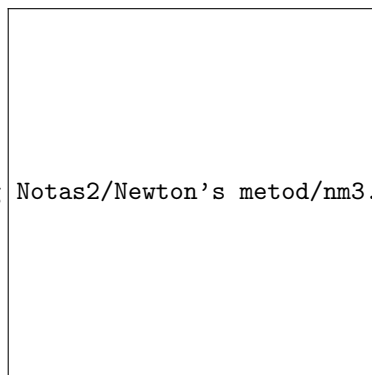
$$f(x, y) = x + y + x^3 y^4$$

has support

$$\text{supp}(f) = \{(1, 0), (0, 1), (3, 4)\}$$



Algebraic curve



Support polygon

But that's actually not the Newton Polygon!

Definition. The **Newton Polygon** of f is

$$\text{NP}(f) = \text{conv}(\text{supp}(f) + \mathbb{R}_{\geq 0}^2)$$

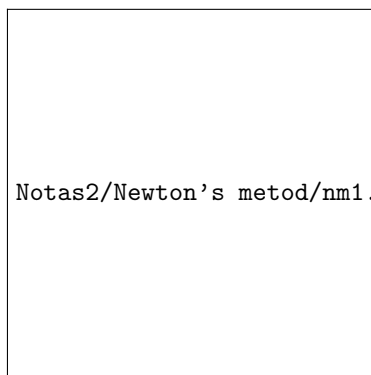
Theorem (Newton's lemma). If $f(x, y) = 0$ has a solution of order μ , then $(1, \mu)$ is orthogonal to a side of $\text{NP}(f)$. (So the slope of the side of the NP is $-\frac{1}{\mu}$).

Moreover, the first term is $c_\mu x^\mu$ where c_μ is a root of $f|_{L^\mu}(1, c_\mu)$ where

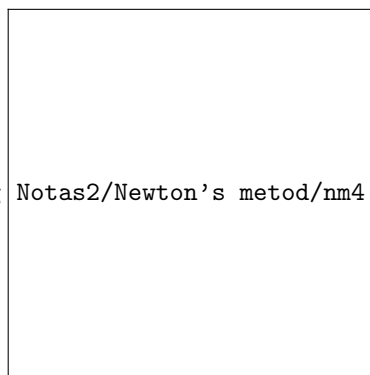
Definition. Let $S \subset (\mathbb{Z}_{\geq 0})^2$.

$$f|_S = \sum_{(i,j) \in S} a_{ij} x^i y^j$$

Example 36. So for our initial example we had the polynomial $y^2 - x^3$, so:



Algebraic curve

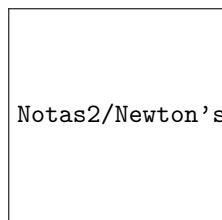


Newton Polygon

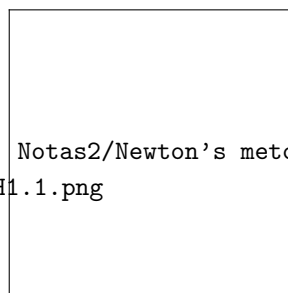
Example 37 (Homework). Give a parametric form for the curves

1. $y^2 + x + xy = 0$

Solution. We have $\text{supp}(f) = \{(1, 0), (1, 1), (0, 2)\}$ which amounts to



Support polygon



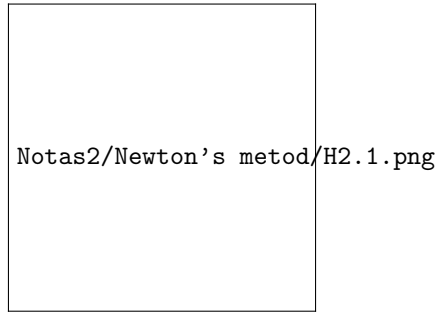
Newton Polygon

And we see that a side of the Newton Polygon is the line through $(0, 2)$ and $(1, 0)$, which has slope -2 . Using our theorem, $\mu = \frac{1}{2}$ and thus the first term of our function $y(x)$ is c_μ , a root of $f|_L$.

Now to find c_μ , we simply solve the equation $f(1, c_\mu) = 0$ on the side of the Newton Polygon, which amounts to ignoring the crossed term. So we get $0 = c_\mu^2 + 1 \iff c_\mu = \pm i$. More terms should be calculated. \square

2. $y^3 + xy + x^2 = 0$

Solution. Yikes! This time we'll have



Support polygon

So the Newton Polygon has two sides: which to choose? \square

We finally read [arocailardi], where Newton's Lemma is generalized to be applied not only to algebraic hypersurfaces like McDonald [grigoriev2015tropical] did but to algebraic varieties of arbitrary codimension. It was seen how to use Newton's Lema to solve linear and nonlinear partial differential equations as in [AROCA2001717] and [Aroca3].

5.1 Exercises

Exercise. Consider de Pfaffian equations given by

$$\omega_1 = 2ydx - 3xdy \tag{1}$$

$$\omega_2 = (y^3 - x^2y)dx + (x^3 - 2xy^2)dy \tag{2}$$

Show that there are infinite solutions of the form $y(x) = cx^{3/2} + \dots$, with $c \in \mathbb{C} \setminus \{0\}$.

Solution. 1. We wish to find $2y + 3xy'$. Suppose $y(x) = c_\mu x^\mu + \bar{y}$. Substituting,

$$0 = 2(c_\mu x^\mu + \bar{y}) - 3(c_\mu x^\mu + \bar{y})' = 2c_\mu x^\mu + 2\bar{y} - 3c_\mu \mu x^{\mu-1} - 3\bar{y}' = (2 - 3\mu)c_\mu x^\mu + 2\bar{y} - 3\bar{y}'$$

so that $\mu = 3/2$.

Now take $\delta y = xy'$, so that $2y - 3x\delta y/x = 2y - 3\delta y$.

For the Newton Polygon we must consider $(\underbrace{i}_x, \underbrace{j_1 + j_2}_{y \text{ and } \delta y})$. So in the first term of

our equation there is no x and $j_1 + j_2 = 1$. The same happens in the second term, so our Newton Polygon is degenerate: it is only the point $(0, 1)$. We understand in this case all solutions are of the form $(x, c_\mu x^{3/2})$, for any c_μ .

Now consider the following plots of the vector field and its curves of solutions:



(a) Vector field



(b) Solution curves

How can we relate this to what we have found?

- For the second equation we only include the diagrams:



(a) Vector field

(b) Solution curves



6 References