Polynomials over Power Series and their Applications to Limit Computations (lecture version)

Marc Moreno Maza

University of Western Ontario
IBM Center for Advanced Studie

September 17, 2018

Plan

Plan

Formal power series (1/4)

Notations

- $\mathbb{K}$ is a complete field, that is, every Cauchy sequence in $\mathbb{K}$ converges.
- $\mathbb{K}[[X_1, \ldots, X_n]]$ denotes the set of formal power series in $X_1, \ldots, X_n$ with coefficients in $\mathbb{K}$.
- These are expressions of the form $\Sigma_e \, a_e X^e$ where e is a multi-index with n coordinates $(e_1, \ldots, e_n)$, X^e stands for $X_1^{e_1} \cdots X_n^{e_n}$, $|e| = e_1 + \cdots + e_n$ and $a_e \in \mathbb{K}$ holds.
- For $f = \Sigma_e \, a_e X^e$ and $d \in \mathbb{N}$, we define
$$f_{(d)} = \sum_{|e|=d} a_e X^e \quad \text{and} \quad f^{(d)} = \sum_{k \leq d} f_{(k)},$$
which are the *homogeneous part* and *polynomial part* of f in degree d.

Addition and multiplication

For $f, g \in \mathbb{K}[[X_1, \ldots, X_n]]$, we define

$$f + g = \sum_{d \in \mathbb{N}} \left(f_{(d)} + g_{(d)}\right) \quad \text{and} \quad fg = \sum_{d \in \mathbb{N}} \left(\Sigma_{k+\ell=d} \left(f_{(k)} g_{(\ell)}\right)\right).$$

Formal power series (2/4)

Order of a formal power series

For $f \in \mathbb{K}[[X_1, \ldots, X_n]]$, we define its *order* as

$$\operatorname{ord}(f) = \begin{cases} \min\{d \mid f_{(d)} \neq 0\} & \text{if } f \neq 0, \\ \infty & \text{if } f = 0. \end{cases}$$

Remarks

For $f, g \in \mathbb{K}[[X_1, \ldots, X_n]]$, we have

$$\operatorname{ord}(f+g) \geq \min\{\operatorname{ord}(f), \operatorname{ord}(g)\} \quad \text{and} \quad \operatorname{ord}(fg) = \operatorname{ord}(f) + \operatorname{ord}(g).$$

Consequences

- $\mathbb{K}[[X_1, \ldots, X_n]]$ is an integral domain.
- $\mathcal{M} = \{f \in \mathbb{K}[[X_1, \ldots, X_n]] \mid \operatorname{ord}(f) \geq 1\}$ is the only maximal ideal of $\mathbb{K}[[X_1, \ldots, X_n]]$.
- We have $\mathcal{M}^k = \{f \in \mathbb{K}[[X_1, \ldots, X_n]] \mid \operatorname{ord}(f) \geq k\}$ for all $k \in \mathbb{N}$.

Krull Topology

Recall $\mathcal{M} = \{f \in \mathbb{K}[[X_1, \ldots, X_n]] \mid \mathrm{ord}(f) \geq 1\}$. Let $(f_n)_{n\in\mathbb{N}}$ be a sequence of elements of $\mathbb{K}[[\underline{X}]]$ and let $f \in \mathbb{K}[[\underline{X}]]$. We say that

- $(f_n)_{n\in\mathbb{N}}$ *converges* to f if for all $k \in \mathbb{N}$ there exists $N \in \mathbb{N}$ s.t. for all $n \in \mathbb{N}$ we have $n \geq N \quad \Rightarrow \quad f - f_n \in \mathcal{M}^k$,
- $(f_n)_{n\in\mathbb{N}}$ is a *Cauchy sequence* if for all $k \in \mathbb{N}$ there exists $N \in \mathbb{N}$ s.t. for all $n, m \in \mathbb{N}$ we have $n, m \geq N \quad \Rightarrow \quad f_m - f_n \in \mathcal{M}^k$.

Proposition 1

- We have $\bigcap_{k\in\mathbb{N}} \mathcal{M}^k \;=\; \langle 0 \rangle$,
- If every Cauchy sequence in $\mathbb{K}$ converges, then every Cauchy sequence of $\mathbb{K}[[\underline{X}]]$ converges too.

Formal power series (4/4)

Proposition 2

For all $f \in \mathbb{K}[[X_1, \ldots, X_n]]$, the following properties are equivalent:

(i) f is a unit,

(ii) $\mathrm{ord}(f) = 0$,

(iii) $f \notin \mathcal{M}$.

Sketch of proof

This follows from the classical observation that for $g \in \mathbb{K}[[X_1, \ldots, X_n]]$, with $\mathrm{ord}(g) > 0$, the following holds in $\mathbb{K}[[X_1, \ldots, X_n]]$

$$(1 - g)(1 + g + g^2 + \cdots) = 1$$

Since $(1 + g + g^2 + \cdots)$ is in fact a sequence of elements in $\mathbb{K}[[X_1, \ldots, X_n]]$, proving the above relation formally requires the use of Krull Topology.

Abel's Lemma (1/2)

Geometric series

From now on, the field $\mathbb{K}$ is equipped with an absolute value. The *geometric series* $\Sigma_e X^e$ is absolutely convergent provided that $|x_1| < 1, \ldots, |x_n| < 1$ all hold. Then we have

$$\Sigma_e \, x_1^{e_1} \cdots x_n^{e_n} = \frac{1}{(1-x_1)\cdots(1-x_n)}.$$

Abel's Lemma

Let $f = \Sigma_e \, a_e X^e \in \mathbb{K}[[\underline{X}]]$, let $x = (x_1, \ldots, x_n) \in \mathbb{K}^n$, let $M \in \mathbb{R}_{>0}$ and Let $\rho_1, \ldots, \rho_n$ be real numbers such that

(i) $|a_e x^e| \leq M$ holds for all $e \in \mathbb{N}^n$,
(ii) $0 < \rho_j < |x_j|$ holds for all $j = 1 \cdots n$.

Then f is uniformly and absolutely convergent in the polydisk

$$D = \{z \in \mathbb{K}^n \;\mid\; |z_j| < \rho_j\}.$$

In particular, the limit of the sum is independent of the summand order.

Abel's Lemma (2/2)

Corollary 1

Let $f = \Sigma_e \, a_e X^e \in \mathbb{K}[[\underline{X}]]$. Then, the following properties are equivalent:

(i) There exists $x = (x_1, \ldots, x_n) \in \mathbb{K}^n$, with $x_j \neq 0$ for all $j = 1 \cdots n$, s.t. $\Sigma_e \, a_e x^e$ converges.

(ii) There exists $\rho = (\rho_1, \ldots, \rho_n) \in {\mathbb{R}_{>0}}^n$ s.t. $\Sigma_e \, a_e \rho^e$ converges.

(iii) There exists $\sigma = (\sigma_1, \ldots, \sigma_n) \in {\mathbb{R}_{>0}}^n$ s.t. $\Sigma_e \, |a_e| \sigma^e$ converges.

Definition

A power series $f \in \mathbb{K}[[\underline{X}]]$ is said *convergent* if it satisfies one of the conditions of the above corollary. The set of the convergent power series of $\mathbb{K}[[\underline{X}]]$ is denoted by $\mathbb{K}\langle \underline{X} \rangle$.

Remark

It can be shown that, within its domain of convergence, a formal power series is a multivariate holomorphic function. Conversely, any multivariate holomorphic function can be expressed locally as the sum of a power series.

ρ-norm of a power series

Notation

Let $\rho = (\rho_1, \dots, \rho_n) \in {\mathbb{R}_{>0}}^n$. For all $f = \Sigma_e\, a_e X^e \in \mathbb{K}[[\underline{X}]]$, we define

$$\| f \|_\rho = \Sigma_e\, |a_e| \rho^e.$$

Proposition 3

For all $f, g \in \mathbb{K}[[\underline{X}]]$ and all $\lambda \in \mathbb{K}$, we have

- $\| f \|_\rho = 0 \quad \Longleftrightarrow \quad f = 0$,
- $\| \lambda f \|_\rho = |\lambda| \; \| f \|_\rho$,
- $\| f + g \|_\rho \leq \| f \|_\rho + \| g \|_\rho$,
- If $f = \Sigma_{k \leq d}\, f_{(d)}$ is the decomposition of f into homogeneous parts, then $\| f \|_\rho = \Sigma_{k \leq d} \| f_{(d)} \|_\rho$ holds.
- If f, g are polynomials, then $\| fg \|_\rho \leq \| f \|_\rho \| f \|_\rho$,
- $\lim_{\rho \to 0} \| f \|_\rho \; = \; |f(0)|$.

Convergent power series form a ring (1/5)

Notation

Let $\rho = (\rho_1, \ldots, \rho_n) \in {\mathbb{R}_{>0}}^n$. We define

$$B_\rho = \{f \in \mathbb{K}[[\underline{X}]] \;\mid\; \| f \|_\rho < \infty\}$$

Theorem

- The set B_ρ is a Banach algebra. Moreover, if $\rho \leq \rho'$ holds then we have $B_{\rho'} \subseteq B_\rho$.
- We define $\mathbb{K}\langle \underline{X} \rangle := \bigcup_\rho B_\rho$ $\mathbb{K}\langle \underline{X} \rangle$ is a subring of $\mathbb{K}[[\underline{X}]]$.

Cauchy's estimate

Observe that for all $f = \Sigma_e a_e X^e \in \mathbb{K}[[\underline{X}]]$, we have for all $e \in \mathbb{N}^e$

$$|a_e| \leq \frac{\|f\|_\rho}{\rho^e}.$$

Theorem 1

The set B_ρ is a Banach algebra. Moreover,

1. if $\rho \leq \rho'$ holds then we have $B_{\rho'} \subseteq B_\rho$,
2. we have $\bigcup_\rho B_\rho = \mathbb{K}\langle \underline{X} \rangle$.

Proof (1/3)

- From Proposition 3, we know that B_ρ is a normed vector space.
- Proving that $\parallel fg \parallel_\rho \leq \parallel f \parallel_\rho \parallel g \parallel_\rho$ holds for all $f, g \in \mathbb{K}[[\underline{X}]]$ is routine. Thus, B_ρ is a normed algebra.
- To prove (1), it remains to show that B_ρ is complete.
- Let $(f_j)_{j \in \mathbb{N}}$ be a Cauchy sequence in B_ρ. We write $f_j = \Sigma_e \, a_e^{(j)} X^e$.
- From Cauchy's estimate, for each $e \in \mathbb{N}^n$, for all $i, j \in \mathbb{N}$ we have $|a_e^{(j)} - a_e^{(i)}| \leq \dfrac{\parallel f_j - f_i \parallel_\rho}{\rho^e}$.

Proof (2/3)

- Since $\mathbb{K}$ is complete, for each $e \in \mathbb{N}^n$, the sequence $(a_e^{(j)})_{j\in\mathbb{N}}$ converges to an element $a_e \in \mathbb{K}$.
- We define $f = \Sigma_e\, a_e X^e$. It must be shown that
  - (i) $f \in B_\rho$ holds and
  - (ii) $\lim_{j\to\infty} f_j = f$ holds in the metric topology induced by the ρ-norm of the normed vector space B_ρ.
- Hence we must show that
  - (i) $\parallel f \parallel_\rho < \infty$ holds, and
  - (ii) for all $\varepsilon > 0$ there exists $j_0 \in \mathbb{N}$ s.t. for all $j \in \mathbb{N}$ we have $j \geq j_0 \ \Rightarrow \ \parallel f - f_j \parallel_\rho \leq \varepsilon$.
- Let $\varepsilon > 0$. Since $(f_j)_{j\in\mathbb{N}}$ is a Cauchy sequence in B_ρ, there exists $j_0 \in \mathbb{N}$ s.t. for all $j \geq j_0$ and all $i \geq 0$ we have
$$\sum_e |a_e^{(j+i)} - a_e^{(j)}|\rho^e \ = \ \parallel f_{j+i} - f_j \parallel_\rho \ < \ \frac{\varepsilon}{2}.$$

Convergent power series form a ring (4/5)

Proof (3/3)

- Let $s \in \mathbb{N}$ be fixed. Since for each $e \in \mathbb{N}^n$ the sequence $(a_e - a_e^{(i)})_{i \in \mathbb{N}}$ converges to 0 in $\mathbb{K}$, there exists $i_0 \in \mathbb{N}$ s.t. for all $j \geq j_0$ and all $i \geq i_0$ we have
$$\sum_{|e|=0}^{s} |a_e - a_e^{(j+i)}| \rho^e \ < \ \frac{\varepsilon}{2}.$$
- Therefore, for all $j \geq j_0$ and all $i \geq i_0$ we have
$$\sum_{|e|=0}^{s} |a_e - a_e^{(j)}| \rho^e \leq$$
$$\sum_{|e|=0}^{s} |a_e - a_e^{(j+i)}| \rho^e + \sum_e |a_e^{(j+i)} - a_e^{(i)}| \rho^e < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon.$$
- Since the above holds for all s, we deduce that for all $j \geq j_0$
$$\| f - f_j \|_\rho = \sum_e |a_e - a_e^{(j)}| \rho^e \leq \varepsilon,$$
- which proves (ii). Finally, (i) follows from
$$\| f \|_\rho \leq \ \| f - f_{j_0} \|_\rho + \ \| f_{j_0} \|_\rho \leq \varepsilon + \ \| f_{j_0} \|_\rho < \infty.$$

Convergent power series form a ring (5/5)

Corollary 2

$\mathbb{K}\langle \underline{X} \rangle$ is a subring of $\mathbb{K}[[\underline{X}]]$.

Proof

For $f, g \in \mathbb{K}\langle \underline{X} \rangle$, there exists $\rho \in {\mathbb{R}_{>o}}^n$ s.t. $f, g \in B_\rho$. While proving the previous theorem we proved $fg \in B_\rho$. Moreover, $f + g \in B_\rho$ clearly holds.

Corollary 3

Let $f \in \mathbb{K}\langle \underline{X} \rangle$. If f is a unit in $\mathbb{K}[[\underline{X}]]$, then f is also a unit in $\mathbb{K}\langle \underline{X} \rangle$.

Sketch of Proof

W.l.o.g. we can assume $f(0) = 1$ and we define $g = 1 - f$. We know that f^{-1} is the limit of the sequence $1 + g + g^2 + \cdots$ in Krull's topology. Since $g(0) = 0$, there exists $\rho \in {\mathbb{R}_{>o}}^n$ s.t. $\Theta := \parallel g \parallel_\rho < 1$. It follows that $\parallel f^{-1} \parallel_\rho \leq \sum_{k \in \mathbb{N}} \Theta^k = \frac{1}{1-\Theta}$ holds, thus we have $f^{-1} \in B_\rho$.

Substitution of power series (1/4)

Remark

If $g_1, \ldots, g_n \in \mathbb{K}[\underline{Y}]$ then $\Phi_g : \begin{array}{ccc} \mathbb{K}[\underline{X}] & \longrightarrow & \mathbb{K}[\underline{Y}] \\ f & \longmapsto & f(g_1(\underline{Y}), \ldots, g_n(\underline{Y})) \end{array}$ defines a homomorphism of $\mathbb{K}$-algebras. This is not always true of convergent power series, e.g. $\mathbb{K}[[\underline{X}]] \longrightarrow \mathbb{K}[[\underline{Y}]], X_1, \ldots, X_n \longmapsto 1$.

Theorem 2

For $g_1, \ldots, g_n \in \mathbb{K}[[\underline{Y}]]$, with $\operatorname{ord}(g_i) \geq 1$, there is a $\mathbb{K}$-algebra homomorphism

$$\overline{\Phi_g} : \begin{array}{ccc} \mathbb{K}[[\underline{X}]] & \longrightarrow & \mathbb{K}[[\underline{Y}]] \\ f & \longmapsto & f(g_1(\underline{Y}), \ldots, g_n(\underline{Y})) \end{array}$$

with the following properties

1. If $g_1, \ldots, g_n$ are polynomials, then $\overline{\Phi_g}$ is an extension of Φ_g
2. If $g_1, \ldots, g_n$ are convergent power series, then we have $\overline{\Phi_g}(\mathbb{K}\langle \underline{X} \rangle) \subseteq \mathbb{K}\langle \underline{Y} \rangle$.

Substitution of power series (2/4)

Proof (1/3)

- Let $f \in \mathbb{K}[[\underline{X}]]$. To define $\overline{\Phi_g}(f)$, we consider the polynomial part $f^{(k)}$ of f, for all $k \in \mathbb{N}$.
- Since $\mathbb{K}[[\underline{Y}]]$ is a ring, we observe that $f^{(k)}(g_1, \ldots, g_n) \in \mathbb{K}[[\underline{Y}]]$ holds.
- Let $k, \ell \in \mathbb{N}$ with $k < \ell$. Observe that we have $\mathrm{ord}(f^{(\ell)} - f^{(k)}) \geq k + 1$.
- Since $\mathrm{ord}(g_i) \geq 1$ holds, we deduce $\mathrm{ord}(f^{(\ell)}(g) - f^{(k)}(g)) \geq k + 1$.
- It follows that $(f^{(k)}(g))_{k \in \mathbb{N}}$ is a Cauchy sequence in Krull Topology and thus converges to an element $f(g) \in \mathbb{K}[[\underline{X}]]$. Therefore, $\overline{\Phi_g}(f)$ is well defined.
- Of the properties asserted for the map $\overline{\Phi_g}$ only the second one requires some care.

Substitution of power series (3/4)

Proof (2/3)

- Let $\rho = (\rho_1, \ldots, \rho_n) \in \mathbb{R}^n_{>0}$.
- It suffices to prove the following: there exists $\sigma = (\sigma_1, \ldots, \sigma_n) \in {\mathbb{R}_{>0}}^n$ such that we have
$$\overline{\Phi_g}(B_\rho) \subseteq B_\sigma.$$
- Since $g_j(0) = 0$ for all $j = 1 \cdots n$, there exists $\sigma_j \in {\mathbb{R}_{>0}}^n$ such that we have $\parallel g_j \parallel_{\sigma_j} \leq \rho_j$ for all $j = 1 \cdots n$.
- Taking the "component-wise min" of these $\sigma_j \in {\mathbb{R}_{>0}}^n$, we deduce the existence of a $\sigma \in {\mathbb{R}_{>0}}^n$ such that we have
$$\parallel g_j \parallel_\sigma \leq \rho_j$$
for all $j = 1 \cdots n$.
- It turns out that this σ has the desired property.

Substitution of power series (4/4)

Proof (3/3)

- Indeed, writing $f = \Sigma_e a_e X^e$, we have

$$\begin{array}{rcl} \| f^{(k)}(g) \|_\sigma & = & \| \sum_{d \le k} f_{(k)}(g) \|_\sigma \\ & \le & \sum_{d \le k} \| f_{(k)}(g) \|_\sigma \\ & \le & \sum_{d \le k} \sum_{|e|=k} |a_e| \| g_1 \|_\sigma{}^{e_1} \cdots \| g_n \|_\sigma{}^{e_n} \\ & \le & \sum_{d \le k} \sum_{|e|=k} |a_e| {\rho_1}^{e_1} \cdots {\rho_n}^{e_n} \\ & = & \| f^{(k)} \|_\rho. \end{array}$$

- Thus, we have

$$\begin{array}{rcl} \| f(g) \|_\sigma & = & \lim_{k \to \infty} \| f^{(k)}(g) \|_\sigma \\ & \le & \lim_{k \to \infty} \| f^{(k)} \|_\rho \\ & \le & \| f \|_\rho. \end{array}$$

- Finally, we have

$$f \in B_\rho \quad \Rightarrow \quad f(g) \in B_\sigma.$$

Plan

Plan

Weierstrass Polynomials (1/4)

Remark

Let $f \in \mathbb{K}[[X_1, \ldots, X_n]]$. We write $f = \sum_{j=0}^{\infty} f_j X_n^j$ with $f_j \in \mathbb{K}[[X_1, \ldots, X_{n-1}]]$ for $j \in \mathbb{N}$. Let $\rho = (\rho_1, \ldots, \rho_n) \in \mathbb{R}_{>0}^n$. We write $\rho' = (\rho_1, \ldots, \rho_{n-1})$. Then we have

$$\parallel f \parallel_\rho = \sum_{j=0}^{\infty} \parallel f_j \parallel_{\rho'} \rho_n^j.$$

Hence, if $f \in \mathbb{K}\langle X_1, \ldots, X_n \rangle$ holds, then so does $f_j \in \mathbb{K}\langle X_1, \ldots, X_{n-1} \rangle$ for all $j \in \mathbb{N}$.

Definition

Let $f \in \mathbb{K}[[X_1, \ldots, X_n]]$ with $f \neq 0$. We write $f(\underline{0}, X_n) = f(0, \ldots, 0, X_n)$. Let $k \in \mathbb{N}$. We say that f is

- *general* in X_n if $f(\underline{0}, X_n) \neq 0$ holds,
- *general* in X_n of order k if $\mathrm{ord}(f(\underline{0}, X_n)) = k$,

Clearly $\mathrm{ord}(f) \leq \mathrm{ord}(f(\underline{0}, X_n))$ holds. However, we have the following.

Lemma 1

Let $f \in \mathbb{K}[[X_1, \ldots, X_n]]$ with $f \neq 0$ and $k := \operatorname{ord}(f)$. Then there is a shear:

$$\begin{array}{ll} X_i = Y_i + c_i Y_n & i = 1, \ldots, n-1 \\ X_n = Y_n & \end{array}$$

such that $g(Y) = f(X(Y)) \in \mathbb{K}[[Y_1, \ldots, Y_n]]$ is general in Y_n of order k.

Proof (1/2)

- Let $d \in \mathbb{N}$. We write
$$f_{(d)} = \sum_{|e|=d} a_e X_1^{e_1} \cdots X_{n-1}^{e_{n-1}} X_n^{e_n}.$$
- Since the coordinate change is linear, we have
$$g_{(d)}(Y) = f_{(d)}(X(Y)).$$

Proof (2/2)

- For $d = k$ in particular, we have
$$\begin{array}{rcl} g_{(k)}(Y) & = & \sum_{|e|=k} a_e (Y_1 + c_1 Y_n)^{e_1} \cdots (Y_{n-1} + c_{n-1} Y_n)^{e_{n-1}} Y_n^{e_n} \\ & = & \left(\sum_{|e|=k} a_e c_1^{e_1} \cdots c_{n-1}^{e_{n-1}} Y_n^k \right) + h(Y) \end{array}$$
where $h(Y)$ necessarily satisfies $h(\underline{0}, Y_n) = 0$.
- Observe also that the coefficient of Y_n^k is a polynomial in $c_1, \ldots, c_{n-1}$, which is not identically zero.
- Indeed, if it would, then all its coefficients would be, that is, $f_{(k)} = 0$ would hold, in contradiction to our assumption $k := \mathrm{ord}(f)$.
- Since this polynomial in $c_1, \ldots, c_{n-1}$ is not zero, the variables $c_1, \ldots, c_{n-1}$ can be specialized to values that ensure that $g_{(k)}(Y)$ has degree k in Y_n. Quod erat demonstrandum!

Weierstrass Polynomials (4/4)

Remark

- Let $f \in \mathbb{K}[[X_1, \ldots, X_n]]$ such that $f \in \mathbb{K}\langle X_1, \ldots, X_{n-1}\rangle[X_n]$ holds and $k := \deg(f, X_n)$. Assume (just for this remark) that $\mathbb{K} = \mathbb{C}$.
- Hence, we write $f = \sum_{j=0}^{k} f_j X_n^j$ with $f_j \in \mathbb{K}\langle X_1, \ldots, X_{n-1}\rangle$ for all $j = 0 \cdots k$.
- In this case, the power series $f_0, \ldots, f_k$ have a common radius of convergence $\rho' \in \mathbb{R}_{>0}^{n-1}$ so that they are holomorphic in the polydisk $D' := \{x \in \mathbb{K}^{n-1} \ \mid \ |x_i| < \rho_i\}$.
- Consequently f is holomorphic in $D' \times \mathbb{K}$.

Definition

Let $k \in \mathbb{N}$. Let $f = \sum_{j=0}^{k} f_j X_n^j \in \mathbb{K}[[X_1, \ldots, X_{n-1}]][X_n]$ with $f_j \in \mathbb{K}\langle X_1, \ldots, X_{n-1}\rangle$ for $j = 0 \cdots k$ and with $f_k \neq 0$. We say that f is a *Weierstrass polynomial* if we have

$$f_0(\underline{0}) = \cdots = f_{k-1}(\underline{0}) = 0 \ \text{ and } \ f_k = 1.$$

Weierstrass preparation theorem

Theorem 3

Let $g \in \mathbb{K}\langle X_1, \ldots, X_n \rangle$ be general of order k. Then, there is a unique pair (α, p) with $\alpha \in \mathbb{K}\langle X_1, \ldots, X_n \rangle$ and $p \in \mathbb{K}\langle X_1, \ldots, X_{n-1} \rangle [X_n]$ such that

1. α is a unit,
2. p is a Weierstrass polynomial of degree k,
3. we have $g = \alpha\, p$.

Thus we have

$$g = \alpha(\underline{X}) \left(X_n^k + a_1(X_1, \ldots, X_{n-1}) X_n^{k-1} + \cdots + a_k(X_1, \ldots, X_{n-1}) \right),$$

with $a_1(\underline{0}) = \cdots = a_k(\underline{0}) = 0$. Moreover, if $g \in \mathbb{K}\langle X_1, \ldots, X_{n-1} \rangle [X_n]$ then $\alpha \in \mathbb{K}\langle X_1, \ldots, X_{n-1} \rangle [X_n]$ also holds.

Remark

The above theorem implies that in some neighborhood of the origin, the zeros of g are the same as those of the Weierstrass polynomial p.

Weierstrass division theorem

Theorem 4

Let $f, g \in \mathbb{K}\langle X_1, \ldots, X_n\rangle$ with g general in X_n of order k. Then, there exists a unique pair (q, r) with $q \in \mathbb{K}\langle X_1, \ldots, X_n\rangle$ and $r \in \mathbb{K}\langle X_1, \ldots, X_{n-1}\rangle[X_n]$ such that we have

1. $\deg(r, X_n) \leq k-1$,
2. $f = qg + r$.

Moreover, if $f, g \in \mathbb{K}\langle X_1, \ldots, X_{n-1}\rangle[X_n]$ with

$$g = g_0 + g_1 X_n + \cdots + g_k X_n^k \quad \text{and} \quad g_k(0) \neq 0,$$

then g_k is a unit in the ring $\mathbb{K}\langle X_1, \ldots, X_{n-1}\rangle$ and the classical division theorem (in polynomial rings) gives $q \in \mathbb{K}\langle X_1, \ldots, X_{n-1}\rangle[X_n]$.

Proof of the division theorem (1/7)

Proof of existence (1/5)

- We write $f = \sum_{j=0}^{\infty} f_j X_n^j$ with $f_j \in \mathbb{K}\langle X_1, \ldots X_{n-1}\rangle$ for $j \in \mathbb{N}$.
- We write $f = \hat{f} + \tilde{f} X_n^k$ with
$$\hat{f} = \sum_{j=0}^{k-1} f_j X_n^j \quad \text{and} \quad \tilde{f} = \sum_{j=k}^{\infty} f_j X_n^{j-k}.$$
- Let $\rho = (\rho_1, \ldots, \rho_n) \in \mathbb{R}_{>0}^n$. We have $\parallel f \parallel_\rho = \parallel \hat{f} \parallel_\rho + \parallel \tilde{f} \parallel_\rho \rho_n^k$. In particular
$$\parallel \tilde{f} \parallel_\rho \leq \rho_n^{-k} \parallel f \parallel_\rho. \tag{1}$$
- Similarly, we write $g = \hat{g} + \tilde{g} X_n^k$.
- Since g is general in X_n at order k, it follows that $\tilde{g}$ is a unit.
- Let ρ be chosen such that all of $f, g, \tilde{g}^{-1}$ are in B_ρ.
- We consider the auxiliary function h defined as
$$h \; = \; X_n^k - g\tilde{g}^{-1} \; = \; -\hat{g}\tilde{g}^{-1}.$$

Proof of the division theorem (2/7)

Proof of existence (2/5)

- We claim that for all $\nu \in \mathbb{R}$, with $0 < \nu < 1$, we can choose ρ such that we have
$$\parallel h \parallel_\rho \leq \nu \rho_n^k. \tag{2}$$
- Recall that we have $h = X_n^k - g\tilde{g}^{-1}$ and $\tilde{g}^{-1}(0_1, \ldots, 0_n) \neq 0$.
- More precisely, since $g = \hat{g} + \tilde{g}X_n^k$ holds, we have
$$h = X_n^k - g\tilde{g}^{-1} = X_n^k - \left(\hat{g} + \tilde{g}X_n^k\right)\tilde{g}^{-1} = -\tilde{g}^{-1}\left(\sum_{j=0}^{k-1} g_j X_n^j\right),$$
with $g_j \in \mathbb{K}\langle X_1, \ldots X_{n-1}\rangle$ and $g_j(0_1, \ldots, 0_{n-1}) = 0$ for $j = 0, \ldots, k-1$. Therefore $h(0_1, \ldots, 0_{n-1}, X_n)$ is identically zero.
- Writing $h = \hat{h} + \tilde{h}X_n^k$ with $\hat{h} = \sum_{j=0}^{k-1} h_j X_n^j$ and $h_j \in \mathbb{K}\langle X_1, \ldots X_{n-1}\rangle$, we deduce $\tilde{h}(0_1, \ldots, 0_n) = 0$.

Proof of the division theorem (3/7)

Proof of existence (3/5)

- Since $\tilde{h}(0_1, \ldots, 0_n) = 0$, we can decrease ρ such that we have

$$\parallel \tilde{h} \parallel_\rho \leq \frac{\nu}{2}, \text{ thus } \parallel \tilde{h} X_n^k \parallel_\rho \leq \frac{\nu}{2} \rho_n^k. \tag{3}$$

- With $\rho' = (\rho_1, \ldots, \rho_{n-1})$, and writing $\hat{h} = \sum_{j=0}^{k-1} h_j X_n^j$, we have
$$\parallel \hat{h} \parallel_\rho \leq \sum_{j=0}^{k-1} \parallel h_j \parallel_\rho \rho_n^j.$$
- Since $h_0(\underline{0}) = \cdots = h_{k-1}(\underline{0}) = 0$ holds, we can decrease ρ (actually ρ') while holding ρ_n fixed such that for $j = 0, \ldots, k-1$, we have

$$\parallel h_j \parallel_{\rho'} \leq \frac{\nu}{2} \rho_n^{k-j}, \text{ thus } \parallel \hat{h} \parallel_\rho \leq \frac{\nu}{2} \rho_n^k. \tag{4}$$

- Finally, the claim of (2) follows from (3) and (4).

Proof of the division theorem (4/7)

Proof of existence (4/5)

- The function h is used as follows. For every $\phi \in \mathbb{K}\langle X_1, \ldots, X_n \rangle$, we define $h(\phi) = h\tilde{\phi}$ where $\tilde{\phi}, \hat{\phi}$ are defined as $\tilde{f}, \hat{f}$.
- By combining (1) and (2), we deduce
$$\| h(\phi) \|_\rho \leq \ \| h \|_\rho \| \tilde{\phi} \|_\rho \leq \nu \rho_n^k \rho_n^{-k} \ \| \phi \|_\rho = \nu \ \| \phi \|_\rho.$$
- This lets us write an iteration process
$$\phi_0 := f, \ \phi_{i+1} := h(\phi_i) = h\tilde{\phi}_i.$$
- Observe that the series $\phi := \sum_{i=0}^{\infty} \phi_i$ converges for the metric topology of B_ρ since
$$\| \phi \|_\rho \leq \sum_{i=0}^{\infty} \ \| \phi_i \|_\rho \leq \sum_{i=0}^{\infty} \nu^i \ \| f \|_\rho = \ \| f \|_\rho \frac{\nu}{1-\nu}.$$
We define
$$q := \tilde{\phi}\tilde{g}^{-1} \ \text{ and } \ r := \hat{\phi}.$$
- Observe that $q \in B_\rho$ and $r \in B_{\rho'}[X_n]$ hold.

Proof of the division theorem (5/7)

Proof of existence (5/5)

- Clearly we have

$$\tilde{\phi} = \sum_{i=0}^{\infty} \tilde{\phi}_i \quad \text{and} \quad \hat{\phi} = \sum_{i=0}^{\infty} \hat{\phi}_i.$$

- Observe also that we have

$$\begin{array}{rcl} \phi_i - \phi_{i+1} & = & \phi_i - h\tilde{\phi}_i \\ & = & \hat{\phi}_i + X_n^k \tilde{\phi}_i - \left(X_n^k - g\tilde{g}^{-1}\right)\tilde{\phi}_i \\ & = & \hat{\phi}_i + g\tilde{g}^{-1}\tilde{\phi}_i. \end{array}$$

- Putting everything together

$$\begin{array}{rcl} f & = & \phi_0 \\ & = & \sum_{i=0}^{\infty} (\phi_i - \phi_{i+1}) \\ & = & \sum_{i=0}^{\infty} \hat{\phi}_i + g\tilde{g}^{-1} \sum_{i=0}^{\infty} \tilde{\phi}_i \\ & = & r + gq. \end{array}$$

- This proves existence.

Proof of the division theorem (6/7)

Proof of uniqueness (1/2)

- Proving the uniqueness is equivalent to prove that for all q, r satisfying $\deg(r, X_n) < k$ and $0 = qg + r$ we have $q = r = 0$.
- So let $q \in \mathbb{K}\langle \underline{X} \rangle$ and $r \in \mathbb{K}\langle X_1, \ldots, X_{n-1} \rangle [X_n]$ $\deg(r, X_n) < k$ and $0 = qg + r$.
- We have seen that there exists $\rho \in \mathbb{R}^n_{>0}$ such that $g, q, r, \tilde{g}^{-1} \in B_\rho$ holds.
- For $h = X_n^k - g\tilde{g}^{-1}$ as above, we have

$$q\tilde{g}h \; = \; q\tilde{g}X_n^k - q\tilde{g}g\tilde{g}^{-1} \; = \; q\tilde{g}X_n^k + r.$$

Proof of the division theorem (7/7)

Proof of uniqueness (2/2)

- We assume that ρ is chosen such that (2) holds, that is, $\| h \|_\rho \leq \nu \rho_n^k$. Defining $M = \| q\tilde{g} \|_\rho \rho_n^k$, and using $\deg(r, X_n) < k$, we have:

$$\begin{array}{rcl} M & = & \| q\tilde{g}X_n^k \|_\rho \\ & \leq & \| q\tilde{g}X_n^k + r \|_\rho \\ & = & \| q\tilde{g}h \|_\rho \\ & \leq & \| q\tilde{g} \|_\rho \| h \|_\rho \\ & \leq & \| q\tilde{g} \|_\rho \nu \rho_n^k \\ & = & \nu M. \end{array}$$

- Since $0 < \nu < 1$, we deduce $M = 0$.
- Since $\rho_n \neq 0$, we have $\| q\tilde{g} \|_\rho = 0$.
- Since $\tilde{g} \neq 0$, we finally have $q = 0$, and thus $r = 0$.

Proof of the first point of the preparation theorem

Proof of the existence

- We apply the division theorem and divide $f = X_n^k$ by g leading to
$$X_n^k \;=\; qg + \sum_{i=1}^k a_i X_n^{k-i} \;\text{ with }\; a_i \in \mathbb{K}\langle X_1, \ldots, X_{n-1}\rangle.$$
- That is,
$$qg \;=\; X_n^k - \sum_{i=1}^k a_i X_n^{k-i}.$$
- We substitute $X_1 = \cdots = X_{n-1} = 0$ leading to
$$q(\underline{0}, X_n)(cX_n^k + \cdots) \;=\; X_n^k - \sum_{i=1}^k a_i(\underline{0}) X_n^{k-i}.$$
with $c \in \mathbb{K}$ and $c \neq 0$.
- Comparing the coefficients of X_n^ℓ for all $\ell \in \mathbb{N}$ shows that $q(0,0) = \frac{1}{c} \neq 0$ and $a_1(0) = \cdots = a_k(0) = 0$
- Thus q is a unit and setting $\alpha = q^{-1}$ completes the proof of the existence statement.

Proof of the uniqueness

Follows immediately from the uniqueness of the division theorem.

Proof of the second point of the preparation theorem

Proving $g \in \mathbb{K}\langle X_1, \ldots, X_{n-1}\rangle[X_n] \quad \Rightarrow \alpha \in \mathbb{K}\langle X_1, \ldots, X_{n-1}\rangle[X_n]$

- Let (α, p) be given by the first point of the preparation theorem, thus, $g = \alpha\, p$ and p is a Weierstrass polynomial of degree k,
- We further assume $g \in \mathbb{K}\langle X_1, \ldots, X_{n-1}\rangle[X_n]$.
- Since p is a monic polynomial in X_n, we can divide g by p in $\mathbb{K}\langle X_1, \ldots, X_{n-1}\rangle[X_n]$ yielding $q, r \in \mathbb{K}\langle X_1, \ldots, X_{n-1}\rangle[X_n]$ such that
$$g = qp + r \quad \text{and} \quad \deg(r, X_n) < k.$$
- Applying the uniqueness of the Weierstrass preparation theorem, we deduce
$$\alpha = q \quad \text{and} \quad r = 0.$$

Quod erat demonstrandum!

Implicit Function Theorem (1/3)

Remark

An important special case of the Weierstrass preparation theorem is when the polynomial f has order $k = 1$ in X_n. In this case, we change the notations for convenience.

Notations and assumptions

- Let $f = \sum_{j=0}^{\infty} f_j Y^j$ with $f_j \in \mathbb{K}\langle X_1, \ldots, X_n \rangle$, $f(0) = 0$ and $\frac{\partial(f)}{\partial(Y)}(0) \neq 0$. Then f is general in Y of order 1.
- By the preparation theorem, there exists a unit $\alpha \in \mathbb{K}\langle X_1, \ldots, X_n, Y \rangle$ and $\phi \in \mathbb{K}\langle X_1, \ldots, X_n \rangle$ such that
$$f = \alpha(Y - \phi) \quad \text{and} \quad \phi(0) = 0.$$
- In this section on the *Implicit Function Theorem* we also assume that $\mathbb{K} = \mathbb{C}$ holds.

Observations

- We have
$$f(\underline{X}, \phi(\underline{X})) = \alpha(\underline{X}, \phi(\underline{X}))\,(\phi(\underline{X}) - \phi(\underline{X})) = 0.$$
- Now consider an arbitrary series $\psi(\underline{X}) \in \mathbb{K}\langle \underline{X} \rangle$ such that $\psi(0) = 0$ and $f(\underline{X}, \psi(\underline{X})) = 0$ hold.
- From $f(\underline{X}, \psi(\underline{X})) = 0$, we deduce
$$0 = f(\underline{X}, \psi(\underline{X})) = \alpha(\underline{X}, \psi(\underline{X}))\,(\psi(\underline{X}) - \phi(\underline{X})) = 0.$$
- Since $\psi(0) = 0$ and $\alpha(0, 0) \neq 0$, we have $\alpha(0, \psi(0)) \neq 0$.
- Since α and ψ are continuous, there exists a neighborhood of $\underline{0} \in \mathbb{K}^n$ in which $\alpha(x, \psi(x)) \neq 0$.
- It follows that $\psi(x) = \phi(x)$ holds in this neighborhood.
- Therefore, we have proved the following.

Implicit Function Theorem (3/3)

Theorem 5

Let $f \in \mathbb{C}\langle X_1, \ldots, X_n, Y\rangle$ such that

$$f(0) = 0 \text{ and } \frac{\partial(f)}{\partial(Y)}(0) \neq 0.$$

Then, there exists exactly one series $\psi \in \mathbb{C}\langle X_1, \ldots, X_n\rangle$ such that we have

$$\psi(0) = 0 \text{ and } f(X_1, \ldots, X_n, \psi(X_1, \ldots, X_n)) = 0.$$

Hensel Lemma (1/3)

Notations

- Let $f = a_0 Y^k + a_1 Y^{k-1} + \cdots + a_k$ with $a_k, \ldots, a_0 \in \mathbb{K}\langle X_1, \ldots, X_n \rangle$.
- We define $\overline{f} = f(0_1, \ldots, 0_n, Y) \in \mathbb{K}[Y]$.

Assumptions

1. f is monic in Y, that is, $a_0 = 1$.
2. $\mathbb{K}$ is algebraically closed. Thus, there exist positive integers $k_1, \ldots, k_r$ and pairwise distinct elements $c_1, \ldots, c_r \in \mathbb{K}$ such that we have
$$\overline{f} = (Y - c_1)^{k_1} (Y - c_2)^{k_2} \cdots (Y - c_r)^{k_r}.$$

Theorem 6

There exist $f_1, \ldots, f_r \in \mathbb{K}\langle X_1, \ldots, X_n \rangle[Y]$ all monic in Y s.t. we have

1. $f = f_1 \cdots f_r$,
2. $\deg(f_j, Y) = k_j$, for all $j = 1, \ldots, r$,
3. $\overline{f_j} = (Y - c_j)^{k_j}$, for all $j = 1, \ldots, r$.

Proof of Hensel Lemma (1/2)

- The proof is by induction on r.
- Assume first $r = 1$. Observe that $k = k_1$ necessarily holds. Now define $f_1 := f$. Clearly f_1 has all the required properties.
- Assume next $r > 1$. We apply a change of coordinates sending c_r to 0

$$\begin{array}{rcl} g(\underline{X}, Y) & = & f(\underline{X}, Y + c_r) \\ & = & (Y + c_r)^k + a_1 (Y + c_r)^{k-1} + \cdots + a_k \end{array}$$

- By definition of $\overline{f}$ and c_r, we deduce that $g(\underline{X}, Y)$ is general in Y of order k_r.
- By the preparation theorem, there exist $\alpha, p \in \mathbb{K}\langle X_1, \ldots, X_n \rangle [Y]$ such that α is a unit, p is a Weierstrass polynomial of degree k_r and we have $g = \alpha p$.

Hensel Lemma (3/3)

Proof of Hensel Lemma (1/2)

- Then, we set $f_r(Y) = p(Y - c_r)$ and $f^* = \alpha(Y - c_r)$.
- Thus f_r is monic in Y and we have $f = f^* f_r$.
- Moreover, we have
$$\overline{f^*} = (Y - c_1)^{k_1}(Y - c_2)^{k_2} \cdots (Y - c_{r-1})^{k_{r-1}}.$$
- The existence of $f_1, \ldots, f_{r-1}$ follows by applying the induction hypothesis on f^*.

Plan

Factorization Properties (1/9)

Notations

- Let $\mathcal{M}' = \langle X_1, \ldots, X_{n-1} \rangle$ be the maximal ideal of $\mathbb{K}\langle X_1, \ldots, X_{n-1} \rangle$.
- Let $p = X_n^k + a_1 X_n^{k-1} + \cdots + a_k \in \mathbb{K}\langle X_1, \ldots, X_{n-1} \rangle [X_n]$ be a Weierstrass polynomial of degree k. Thus $a_1, \ldots, a_k \in \mathcal{M}'$ holds.

Proposition 4

The following properties are equivalent

(i) $k = 0$,

(ii) p is a unit in $\mathbb{K}\langle X_1, \ldots, X_{n-1} \rangle [X_n]$,

(iii) p is a unit in $\mathbb{K}\langle X_1, \ldots, X_{n-1}, X_n \rangle$.

Proof

- The equivalence $(i) \iff (iii)$ is trivial.
- The equivalence $(i) \iff (ii)$ follows from $k = \deg(p, X_n)$, $1 = \mathrm{lc}(p, X_n)$ and the fact that $\mathbb{K}\langle X_1, \ldots, X_{n-1} \rangle$ is integral.

Proposition 5

Let $f, g, h \in \mathbb{K}\langle X_1, \ldots, X_{n-1}\rangle[X_n]$ be polynomials s. t. $f = gh$. Then

(i) if g, h are Weierstrass polynomials then so is f,

(ii) if f is a Weierstrass polynomial, then there exist units $\lambda, \mu \in \langle X_1, \ldots, X_{n-1}\rangle$ s. t. λg and μh are Weierstrass polynomials.

Proof

- Claim (i) is clear.
- To prove (ii), we write $g = b_0 X_n^\ell + \cdots + b_\ell$ and $h = c_0 X_n^m + \cdots + c_m$. We observe that $c_0 b_0 = 1$ holds. So we choose $\lambda = c_0$ and $\mu = b_0$.
- W.l.o.g. we assume $c_0 = b_0 = 1$. Thus, each of the following power series belongs to $\mathcal{M}'$

$$b_\ell c_m, b_\ell c_{m-1} + b_{\ell-1} c_m, b_\ell c_{m-2} + b_{\ell-1} c_{m-1} + b_{\ell-2} c_m, \ldots$$

- Since $\mathcal{M}'$ is a prime ideal then each coefficient $b_1, b_2, \ldots, b_\ell, c_1, c_2, \cdots, c_m$ belong to $\mathcal{M}'$

Lemma 2

Let $\mathbb{A}$ be a commutative ring and let $f = \sum_{s=0}^{k} a_s X^s$, $g = \sum_{i=0}^{\ell} b_i X^i$ and $h = \sum_{j=0}^{m} c_j X^j$ be polynomials s.t. a_0, b_0, c_0 units of $\mathbb{A}$ and $f = g\, h$ holds. Let $\mathcal{P}$ be a prime ideal s.t. $a_1, \ldots, a_k \in \mathcal{P}$ Then, we have $b_1, \ldots, b_\ell, c_1, \ldots, c_m \in \mathcal{P}$.

Proof (1/2)

- Consider a rectangular grid G where the points are indexed by the Cartesian Product $\{0, \ldots, \ell\} \times \{0, \ldots, m\}$.
- The point of G of coordinates (i, j) is mapped to $b_i c_j$ such that the sum of all points along a line $i + j = q$ equal a_q.
- There exists at least one such "line" consisting of a unique point. $b_i c_j$.

Proof (2/2)

- If there is only one such point then, this is $(0, 0)$ and G reduces to that point and we are done.
- If there are two such points, then for one of them, either $i > 0$ or $j > 0$ holds. Consider a point of that latter type. Since $\mathcal{P}$ is prime, either $b_i \in \mathcal{P}$ (provided $i > 0$) or $c_j \in \mathcal{P}$ (provided $j > 0$) holds. W.l.o.g., assume $b_i \in \mathcal{P}$ and erase from G all points of the form b_i-*something*.
- If G is not empty, we go back two steps above.
- It is not hard to see that this procedure will erase all rows $b_1, b_2, \ldots, b_\ell$ and all columns $c_1, c_2, \ldots, c_m$, which proves the lemma.

Lemma 3

For the Weierstrass polynomial
$p = X_n^k + a_1 X_n^{k-1} + \cdots + a_k \in \mathbb{K}\langle X_1, \ldots, X_{n-1}\rangle[X_n]$ the following properties are equivalent

(i) p is irreducible in $\mathbb{K}\langle X_1, \ldots, X_{n-1}\rangle[X_n]$,

(ii) p irreducible in $\mathbb{K}\langle X_1, \ldots, X_{n-1}, X_n\rangle$.

Proof of $(i) \Rightarrow (ii)$ (1/2)

- We proceed by contradiction. Assume that p reducible in $\mathbb{K}\langle X_1, \ldots, X_{n-1}, X_n\rangle$.
- So let $f_1, f_2 \in \mathbb{K}\langle X_1, \ldots, X_{n-1}, X_n\rangle$ be non-units s. t. $p = f_1 f_2$.
- Since p is general in X_n (that is, $p \not\equiv 0 \mod \mathcal{M}'$) we can assume that both f_1, f_2 are general in X_n.
- Applying the preparation theorem, we have $f_1 = \alpha_1 q_1$ and $f_2 = \alpha_2 q_2$, where α_1, α_2 are units and q_1, q_2 are Weierstrass polynomials.

Factorization Properties (6/9)

Proof of $(i) \Rightarrow (ii)$ (2/2)

- Thus, $p = \alpha_1 \alpha_2 q_1 q_2$. Observe that $q_1 q_2$ is a Weierstrass polynomial.
- Uniqueness from the preparation theorem implies $\alpha_1 \alpha_2 = 1$ and $p = q_1 q_2$, which is a factorization of p in $\mathbb{K}\langle X_1, \ldots, X_{n-1}\rangle[X_n]$.
- Recall that we assume that p irreducible in $\mathbb{K}\langle X_1, \ldots, X_{n-1}\rangle[X_n]$ and that we aim at contradicting p reducible in $\mathbb{K}\langle X_1, \ldots, X_{n-1}, X_n\rangle$.
- So, one of the polynomials q_i must be a unit in $\mathbb{K}\langle X_1, \ldots, X_{n-1}\rangle[X_n]$ This would imply $q_i = 1$, that is, $f_i = \alpha_i$. A contradiction.

Proof of $(ii) \Rightarrow (i)$

- We assume that p irreducible in $\mathbb{K}\langle X_1, \ldots, X_{n-1}, X_n\rangle$ and proceeding by contradiction, we assume p reducible in $\mathbb{K}\langle X_1, \ldots, X_{n-1}\rangle[X_n]$. Thus let $p_1, p_2 \in \mathbb{K}\langle X_1, \ldots, X_{n-1}\rangle[X_n]$ such that $p = p_1 p_2$ holds.
- We know that p_1, p_2 are Weierstrass polynomials of positive degree. Thus p is reducible in $\mathbb{K}\langle X_1, \ldots, X_{n-1}, X_n\rangle$, a contradiction.

Factorization Properties (7/9)

Theorem 7

The ring $\mathbb{K}\langle X_1, \ldots, X_{n-1}, X_n\rangle$ is a unique factorization domain (UFD).

Proof of the Theorem (1/3)

- The proof is by induction on n.
- For $n = 0$, this is clear since any field is a UFD.
- By induction hypothesis, we assume that $\mathbb{K}\langle X_1, \ldots, X_{n-1}\rangle$ is a UFD.
- It follows from Gauss Theorem that $\mathbb{K}\langle X_1, \ldots, X_{n-1}\rangle[X_n]$ is a UFD as well.
- Next, we show that every $f \in \mathbb{K}\langle X_1, \ldots, X_{n-1}, X_n\rangle$ has a factorization into irreducibles, unique up to order and units.
- We may assume that f is general in X_n. By the preparation theorem, we have $f = \alpha p$ with α a unit and $p \in \mathbb{K}\langle X_1, \ldots, X_{n-1}\rangle[X_n]$ a Weierstrass polynomial.

Proof of the Theorem (2/3)

- Since $\mathbb{K}\langle X_1, \ldots, X_{n-1}\rangle[X_n]$ is a UFD, there is a factorization
$$p = p_1 \cdots p_r$$
into irreducible elements, which is unique up to order, after $p_1, \ldots, p_r$ have been normalized to be Weierstrass polynomials.
- By the previous lemma,
$$f = \alpha p_1 \cdots p_r$$
is a factorization into irreducibles of $\mathbb{K}\langle X_1, \ldots, X_{n-1}, X_n\rangle$.
- Let $f = f_1 \cdots f_s$ be another such factorization into irreducibles of $\mathbb{K}\langle X_1, \ldots, X_{n-1}, X_n\rangle$.
- We apply the preparation theorem to $f_1, \ldots, f_s$, leading to $f_1 = \alpha_i q_1$, $\ldots$, $f_s = \alpha_s q_s$, where $\alpha_1, \ldots, \alpha_s$ are units and $q_1, \ldots, q_s$ are Weierstrass polynomials of positive degrees.

Factorization Properties (9/9)

Proof of the Theorem (3/3)

- By uniqueness in the preparation theorem, we have
$$p_1 \cdots p_r = q_1 \cdots q_s.$$
- Finally, since $\mathbb{K}\langle X_1, \ldots, X_{n-1}\rangle[X_n]$ is a UFD, we deduce $r = s$ and $\{p_1, \ldots, p_r\} = \{q_1, \ldots, q_s\}$.

Remarks

- Following the techniques of the above proof and using the preparation theorem, one can prove that $\mathbb{K}\langle X_1, \ldots, X_n\rangle$ is a Noetherian ring.
- One can prove the preparation theorem in $\mathbb{K}[[X_1, \ldots, X_n]]$ (instead of $\mathbb{K}\langle X_1, \ldots, X_n\rangle$).
- As a result, the results of this section can also be established in $\mathbb{K}[[X_1, \ldots, X_n]]$ (instead of $\mathbb{K}\langle X_1, \ldots, X_n\rangle$).
- In particular, one can prove that $\mathbb{K}[[X_1, \ldots, X_n]]$ is a UFD.

Weierstrass preparation theorem for formal power series (1/8)

Lemma 4

Assume $n \geq 2$. Let $f, g, h \in \mathbb{K}[[X_1, \ldots, X_{n-1}]]$ such that $f = gh$ holds. Let $\mathcal{M}$ be the maximal ideal of $\mathbb{K}[[X_1, \ldots, X_{n-1}]]$. We write $f = \sum_{i=0}^{\infty} f_i$, $g = \sum_{i=0}^{\infty} g_i$ and $h = \sum_{i=0}^{\infty} h_i$, where $f_i, g_i, h_i \in \mathcal{M}^i \setminus \mathcal{M}^{i+1}$ holds for all $i > 0$, with $f_0, g_0, h_0 \in \mathbb{K}$. We note that these decompositions are uniquely defined. Let $r \in \mathbb{N}$. We assume that $f_0 = 0$ and $h_0 \neq 0$ both hold. Then the term g_r is uniquely determined by $f_1, \ldots, f_r, h_0, \ldots, h_{r-1}$.

Proof (1/2)

- Since $g_0 h_0 = f_0 = 0$ and $h_0 \neq 0$ both hold, the claim is true for $r = 0$.
- Now, let $r > 0$. By induction hypothesis, we can assume that $g_0, \ldots, g_{r-1}$ are uniquely determined by $f_1, \ldots, f_{r-1}, h_0, \ldots, h_{r-2}$.
- Observe that for determining g_r, it suffices to expand $f = gh$ modulo $\mathcal{M}^{r+1}$.

Proof (2/2)

- Modulo $\mathcal{M}^{r+1}$, we have
$$\begin{array}{rcl} f_1 + f_2 + \cdots + f_r & = & (g_1 + g_2 + \cdots + g_r)(h_0 + h_1 + \cdots + h_r) \\ & = & g_1 h_0 + \\ & & g_2 h_0 + g_1 h_1 + \\ & & \vdots \\ & & g_r h_0 + g_{r-1} h_1 + \cdots + g_1 h_{r-1} \end{array}$$
- The conclusion follows.

Weierstrass preparation theorem for formal power series (3/8)

Notations

- Assume $n \geq 1$. Denote by $\mathbb{A}$ the ring $\mathbb{K}[[X_1, \ldots, X_{n-1}]]$ and by $\mathcal{M}$ be the maximal ideal of $\mathbb{A}$.
- Note that $n = 1$ implies $\mathcal{M} = \langle 0 \rangle$.
- Let $f \in \mathbb{A}[[X_n]]$, written as $f = \sum_{i=0}^{\infty} a_i X_n^i$ with $a_i \in \mathbb{A}$ for all $i \in \mathbb{N}$.

Theorem 8

We assume $f \not\equiv 0 \mod \mathcal{M}[[X_n]]$. Then, there exists a unit $\alpha \in \mathbb{A}[[X_n]]$, an integer $d \geq 0$ and a monic polynomial $p \in \mathbb{A}[X_n]$ of degree d such that we have

1. $p = X_n^d + b_{d-1} X^{d-1} + \cdots + b_1 X_1 + b_0$, for some $b_{d-1}, \ldots, b_1, b_0 \in \mathcal{M}$,
2. $f = \alpha p$.

Further, this expression for f is unique.

Proof (1/5)

- Let $d \geq 0$ be the smallest integer such that $a_d \notin \mathcal{M}$. Clearly d exists since we assume that $f \not\equiv 0 \mod \mathcal{M}[[X_n]]$ holds.
- If $n = 1$, then writing $f = \alpha X_n^d$ with $\alpha = \sum_{i=0}^{\infty} a_{i+d} X_n^i$ proves the existence of the claimed decomposition.
- From now on, we assume $n \geq 2$.
- Let us write $\alpha = \sum_{i=0}^{\infty} c_i X_n^i$ with $c_i \in \mathbb{A}$ for all $i \in \mathbb{N}$.
- Since we require α to be a unit, we have $c_0 \notin \mathcal{M}$. Note that c_0 is also a unit modulo $\mathcal{M}$.

Proof (2/5)

We must solve for $b_{d-1}, \ldots, b_1, b_0, c_0, c_1, \ldots, c_d, \ldots$ s. t. for all $m \geq 0$ we have

$$\begin{array}{rcl}
a_0 & = & b_0 c_0 \\
a_1 & = & b_0 c_1 + b_1 c_0 \\
a_2 & = & b_0 c_2 + b_1 c_1 + b_2 c_0 \\
& \vdots & \\
a_{d-1} & = & b_0 c_{d-1} + b_1 c_{d-2} + \cdots + \cdots + b_{d-2} c_1 + b_{d-1} c_0 \\
a_d & = & b_0 c_d + b_1 c_{d-1} + \cdots + \cdots + b_{d-1} c_1 + c_0 \\
a_{d+1} & = & b_0 c_{d+1} + b_1 c_d + \cdots + \cdots + b_{d-1} c_2 + c_1 \\
& \vdots & \\
a_{d+m} & = & b_0 c_{d+m} + b_1 c_{d+m-1} + \cdots + \cdots + b_{d-1} c_{m+1} + c_m \\
& \vdots &
\end{array}$$

Proof (3/5)

- We will compute each of $b_{d-1}, \ldots, b_1, b_0, c_0, c_1, \ldots, c_d, \ldots$ modulo each of the successive powers of $\mathcal{M}$, that is, $\mathcal{M}, \mathcal{M}^2, \ldots, \mathcal{M}^r, \ldots$.
- We start by solving for each of $b_{d-1}, \ldots, b_1, b_0, c_0, c_1, \ldots, c_d, \ldots$ modulo $\mathcal{M}$.
- By definition of d, the left hand sides of the first d equations above are all $\equiv 0 \mod \mathcal{M}$.
- Since c_0 is a unit modulo $\mathcal{M}$, these first d equations taken modulo $\mathcal{M}$ imply that each of $b_0, b_1, \ldots, b_{d-1}$ is $\equiv 0 \mod \mathcal{M}$.
- Plugging this into the remaining equations we obtain $c_m \equiv a_{d+m} \mod \mathcal{M}$, for all $m \geq 0$.
- Therefore, we have solved for each of $b_{d-1}, \ldots, b_1, b_0, c_0, c_1, \ldots, c_d, \ldots$ modulo $\mathcal{M}$.

Weierstrass preparation theorem for formal power series (7/8)

Proof (4/5)

- Let $r > 0$ be an integer. We assume that we have inductively determined each of $b_{d-1}, \ldots, b_1, b_0, c_0, c_1, \ldots, c_d, \ldots$ modulo each of $\mathcal{M}, \ldots, \mathcal{M}^r$. We wish to determine them modulo $\mathcal{M}^{r+1}$.
- Consider the first equation, namely $a_0 = b_0 c_0$, with $a_0, b_0, c_0 \in \mathbb{A}$. Recall that $a_0 \in \mathcal{M}$ and $c_0 \notin \mathcal{M}$ both hold. By assumption, b_0 and c_0 are known modulo each of $\mathcal{M}, \ldots, \mathcal{M}^r$. In addition, a_0 is known modulo each of $\mathcal{M}, \ldots, \mathcal{M}^r, \mathcal{M}^{r+1}$. Therefore, the previous lemma applies and we can compute b_0 modulo $\mathcal{M}^{r+1}$.
- Consider the second equation, that we re-write $a_1 - b_0 c_1 = b_1 c_0$. A similar reasoning applies and we can compute b_1 modulo $\mathcal{M}^{r+1}$.
- Continuing in this manner, we can compute each of $b_0, b_1, \ldots, b_{d-1}$ modulo $\mathcal{M}^{r+1}$ using the first d equations.
- Finally, using the remaining equations determine $c_m \mod \mathcal{M}^r$, for all $m \geq 0$.

Weierstrass preparation theorem for formal power series (8/8)

Proof (5/5)

- The induction is complete, and the existence of a factorization of f as claimed is proved.
- The uniqueness is obvious, because d is uniquely determined by f, and the unit α is uniquely determined as **the** coefficient of X_n^d in any two such factorizations.
- Finally, equating the coefficients of $X_n^{d-1}, \ldots, X_n, X_n^0$ in any two such factorizations determine p uniquely.

Remark

- The assumption of the theorem, namely $f \not\equiv 0 \mod \mathcal{M}[[X_n]]$, can always be assumed. Indeed, one can reduce to this case by a suitable linear change of coordinates.
- From this Weierstrass preparation theorem for formal power series, one can show that $\mathbb{K}[[X_1, \ldots, X_{n-1}]]$ is a UFD and a Noetherian ring.

Definition

Let $D := \{x = (x_1, \ldots, x_n) \in \mathbb{K}^n \ \mid \ |x_i| < \rho_i\}$ be a polydisk and let $M \subseteq D$. We say that M is a *principal analytic set* if there exists $f \in \mathbb{K}\langle X_1, \ldots, X_n \rangle$ that converges throughout D and satisfies

$$M = V_D(f) \ \text{ where } \ V_D(f) := \{x \in D \ \mid \ f(x) = 0\}.$$

Given f, the set $V_D(f)$ may be empty or not, depending on D.

Definition

Let D_1 and D_2 be two polydisks of $\mathbb{K}^n$. Let $M_1 \subseteq D_1$ and $M_2 \subseteq D_2$ be two principal analytic sets. We say that M_1 and M_2 are *equivalent* if there exists a polydisk $D \subseteq D_1 \cap D_2$ such that we have

$$M_1 \cap D \ = \ M_2 \cap D.$$

An equivalence class of principal analytic sets is called a *germ of a principal analytic set*, or, when $n = 2$, a germ of a curve.

Notation for a germ

Given two equivalent principal analytic sets $M_1 = V_{D_1}(f_1)$ and $M_2 = V_{D_1}(f_2)$ there exists a polydisk D such that we have

$$\{x \in D_1 \mid f_1(x) = 0\} \cap D = \{x \in D_2 \mid f_2(x) = 0\} \cap D.$$

Therefore $f_1 = f_2$ holds and we simply write $V(f)$ for the equivalent class of M_1 and M_2. Indeed, if the set of zeros of an analytic function f has an accumulation point inside the domain of f, then f is zero everywhere on the connected component containing the accumulation point.

The empty germ

It follows that $V(f) = \emptyset$ means that $0 \notin V_D(f)$ for any representative $V_D(f) \in V(f)$. This implies $f(0) \neq 0$, that is, f is a unit in $\mathbb{K}\langle X_1, \ldots, X_n\rangle$. The converse is clearly true, so we have

$$V(f) = \emptyset \iff f \not\equiv 0 \mod \mathcal{M}.$$

Binary operations on germs

An inclusion $V(f_1) \subseteq V(f_2)$ between two germs means that there exist representatives $V_{D_1}(f_1) \in V(f_1)$ and $V_{D_2}(f_2) \in V(f_2)$ together with a polydisk $D \subseteq D_1 \cap D_2$ such that we have

$$V_{D_1}(f_1) \cap D \ \subseteq \ V_{D_2}(f_2) \cap D.$$

We define $V(f_1) \cap V(f_2)$ and $V(f_1) \cup V(f_2)$ similarly.

Proposition 6

- For all $f, g \in \mathbb{K}\langle X_1, \ldots, X_n \rangle$ s.t f divides g, we have $V(f) \subseteq V(g)$.
- For all $f, f_1, \ldots, f_r \in \mathbb{K}\langle X_1, \ldots, X_n \rangle$ s.t. $f = f_1 \cdots f_r$ holds we have $V(f) = V(f_1) \cup \cdots \cup V(f_r)$.

Lemma (Study's Lemma)

Let $f, g \in \mathbb{K}\langle X_1, \ldots, X_n \rangle$ with f irreducible. If the germs $V(f), V(g)$ satisfy $V(f) \subseteq V(g)$ then f divides g in $\mathbb{K}\langle X_1, \ldots, X_n \rangle$.

Proof of Study's Lemma (1/3)

- We proceed by induction on n.
- The case $n = 0$ is trivial.
- Next, by induction hypothesis, we assume that the lemma holds in $\mathbb{K}\langle X_1, \ldots, X_{n-1} \rangle$.
- By definition of $V(f) \subseteq V(g)$ and thanks to the preparation theorem, we can assume that f, g are Weierstrass polynomials in $\mathbb{K}\langle X_1, \ldots, X_{n-1} \rangle[X_n]$. Thus we have

  $$f = X_n^k + a_1 X_n^{k-1} + \cdots + a_k, \quad g = X_n^\ell + b_1 X_n^{\ell-1} + \cdots + b_\ell,$$

  where $k, \ell \geq 1$ and each of $a_1, \ldots, a_k, b_1, \ldots, b_\ell$ is zero modulo $\mathcal{M}'$, where (as usual) $\mathcal{M}'$ is the maximal ideal of $\mathbb{K}\langle X_1, \ldots, X_{n-1} \rangle$.

Proof of Study's Lemma (2/3)

- Since $\mathbb{K}\langle X_1, \ldots, X_{n-1}\rangle$ is a UFD, it follows from resultant theory that f and g have a common divisor of positive degree ii and only if the resultant $\mathrm{res}(f, g)$ is not zero.
- Since f is also irreducible in $\mathbb{K}\langle X_1, \ldots, X_{n-1}\rangle[X_n]$, proving $\mathrm{res}(f, g) \neq 0$ would do what we need.
- Let $D = \{x = (x_1, \ldots, x_n) \in \mathbb{K}^n \mid |x_i| < \rho_\}$ be a polydisk throughout which f and g are convergent.
- Define $D' = \{x = (x_1, \ldots, x_{n-1}) \in \mathbb{K}^{n-1} \mid |x_i| < \rho_i\}$.
- For each $x' \in D'$, we denote by $f_{x'}$ and $g_{x'}$ the univariate polynomials of $\mathbb{K}[X_n]$ obtained by specializing $X_1, \ldots, X_{n-1}$ to x' into f, g.
- In particular, we have $f_0 = X_n^k$ and $g = X_n^\ell$, so $V(f_0) = V(g_0) = \{0\}$.

Proof of Study's Lemma (3/3)

- Since the roots of $f_{x'}$ and $g_{x'}$ depends continuously on x', one can choose the polydisk $D = \{x = (x_1, \ldots, x_n) \in \mathbb{K}^n \mid |x_i| < \rho_i\}$ (and thus D') such that for all $x' \in D'$ each root x_n of $f_{x'}$ and $g_{x'}$ satisfies $|x_n| < \rho_n$.
- For the same continuity argument, and since $V(f) \subseteq V(g)$ holds, the polydisk D can be further refined such that $V(f_{x'}) \subseteq V(g_{x'})$ holds for all $x' \in D'$.
- Hence, for all $x' \in D'$, the univariate polynomials $f_{x'}$ and $g_{x'}$ have a common prime factor, that is, $\mathrm{res}(f_{x'}, g_{x'}) = 0$.
- Finally, using the specialization property of the resultant, we conclude that $\mathrm{res}(f, g)(x') = 0$ holds for all $x' \in D'$.

Definition

A germ of a principal analytic set $V(f)$ is called *reducible* if there exist two germs of a principal analytic set $V(f_1)$ and $V(f_2)$ such that we have $V(f) = V(f_1) \cup V(f_2)$, $V(f_1) \neq \emptyset$, $V(f_2) \neq \emptyset$ and $V(f_1) \neq V(f_2)$. Otherwise, $V(f)$ is called irreducible.

Lemma 5

A germ of a principal analytic set $V(f)$ is irreducible if and only if there exists $g \in \mathbb{K}\langle X_1, \ldots, X_n \rangle$ and $k \in \mathbb{N}^*$ such that $f = g^k$ holds.

Theorem 9

Let $V(f)$ be a germ of a principal analytic set. Then, $V(f)$ admits a decomposition

$$V(f) = V(f_1) \cup \cdots \cup V(f_r).$$

where $V(f_1), \ldots, V(f_r)$ are irreducible. This decomposition is unique up to the order in which the components appear.

Germs of curves (8/8)

Definition

We call a series $f \in \mathbb{K}\langle X_1, \ldots, X_n\rangle$ *minimal* if every prime factor f_i of f occurs only once, that is, $f = f_1 \cdots f_r$.

- Then, for a curve (that is $n = 2$) the sets $V(f_1), \ldots, V(f_r)$ are called the branch of the curve at the origin.
- This notion can be translated at any point of the curve by an appropriate change of coordinates.
- If f is minimal, we call

  $$\mathrm{Ord}(V(f)) \; = \; \mathrm{ord}(f)$$

  the order of the germ.

Plan

Plan

Implicit function theorem and local parametrization

Definition

Let $f \in \mathbb{K}\langle X, Y\rangle$ be minimal, with $f(0,0) = 0$. The branch $V(f)$ is called smooth if we have

$$\operatorname{grad} f := \left(\frac{\partial f}{\partial X}(0), \frac{\partial f}{\partial Y}(0)\right) \neq (0,0).$$

Remark

If $\partial f/\partial Y \neq 0$, the implicit function theorem gives us a local parametrization $x \mapsto \Phi(x) = (x, \varphi(x))$ of $V(f)$. That is, there exists a convergent power series $\varphi \in \mathbb{K}\langle X\rangle$ such that $f(x, \varphi(x)) = 0$ holds in a neighborhood of the origin.

Motivating the notion of Puiseux series

Example

Let $f := X^3 - Y^2$. The implicit function theorem does not apply to f. However, there is a parametrization:

$$t \mapsto \Phi(t) = (t^2, \varphi(t)), \text{ where } \varphi(t) = t^3.$$

Setting $t = x^{1/2}$, we obtain a parametrization of the cuspidal cubic with fractional exponents

$$x \mapsto \left(x, x^{\frac{3}{2}}\right).$$

Remark

We will show that locally any branch of a curve has a parametrization of the form

$$t \mapsto (t^n, \varphi(t)) \text{ or } x \mapsto \left(x, \varphi(x^{\frac{1}{n}})\right),$$

for some power series $\varphi \in \mathbb{C}\langle T\rangle$. Such φ are called Puiseux Series.

Theorem on Puiseux Series

Definition

Let $f(X,Y) \in \mathbb{C}[[X,Y]]$ be with $f(0,0) = 0$. A pair (φ_1, φ_2) of series in $\mathbb{C}[[T]]$ is called a formal parametrization of f if we have:

1. $(\varphi_1, \varphi_2) \neq (0,0)$,
2. $\varphi_1(0) = \varphi_2(0) = 0$ and
3. $f(\varphi_1(T), \varphi_2(T)) = 0$ holds in $\mathbb{C}[[T]]$.

Here, the substitution is the sense of Theorem 2.

Puiseux's Theorem (algebraic version)

Let the series $f \in \mathbb{C}[[X,Y]]$ be general in Y of order $k \geq 1$. Then there exists a natural number $n \geq 1$ and $\varphi \in \mathbb{C}[[T]]$ such that $\varphi(0) = 0$ and $f(T^n, \varphi(T)) = 0$ hold in $\mathbb{C}[[T]]$. Moreover, if f is convergent, then so is φ.

The proof will be done throughout this section. In the first claim, the field $\mathbb{C}$ could be any algebraically closed field. In the second (convergence) methods from analysis are used, so $\mathbb{C}$ stand for the complex numbers.

Plan

Remark

- In the special case of the implicit function theorem, the convergence of φ can be derived easily from convergence of f, see Appendix 3.
- The general case is more complicated.

Remark

The proof (to be presented hereafter) combines

- methods from complex analysis and topology to prove the existence of sufficiently many "convergent solutions", and
- an algebraic trick to show that the formally constructed series is equal to one of the convergent solutions.

Thus φ must be convergent.

Discriminant (recall)

Notation

Let A be a commutative ring and $f \in \mathbb{A}[Y]$ a non-constant polynomial. We denote by D_f the discriminant of f.

Proposition

Let $U \subset \mathbb{C}$ be a domain, let $A := \mathcal{O}(U)$ be the ring of holomorphic functions in U. For $f \in A[Y]$ monic and $x \in U$, we write

$$f_x := Y^k + a_1(x)Y^{k-1} + \cdots + a_k(x) \in \mathbb{C}[Y].$$

Then f_x has a multiple root in $\mathbb{C}$ if and only if $D_f(x) = 0$ holds.

Proof

- By the specialization property of resultants, we have $D_f(x) = D_{f_x}$.
- Then, the assertion follows from definition of discriminants of D_{f_x}.

Puiseux's Theorem (geometric version)

Let $f(X,Y) = Y^k + a_1(X)Y^{k-1} + \cdots + a_k(X) \in \mathbb{C}\langle X\rangle[Y], k \geq 1$ be an irreducible Weierstrass polynomial. (Note that f could have irreducible factors that are not Weierstrass polynomials.) Let $\rho > 0$ be chosen such that

a) $a_1, \ldots, a_k$ converge in $U := \{x \in \mathbb{C} \mid |x| < \rho\}$,

b) $D_f(x) \neq 0$ in $U^* := U \setminus \{0\}$.

Furthermore, let

$$\begin{aligned} V &:= \{t \in \mathbb{C} \mid |t| < \rho^{\frac{1}{k}}\}, \\ \mathcal{C} &:= \{(x,y) \in U \times \mathbb{C} : f(x,y) = 0\}. \end{aligned}$$

Then, there exists a series $\varphi \in \mathbb{C}\langle T\rangle$ that converges in V and has the following properties:

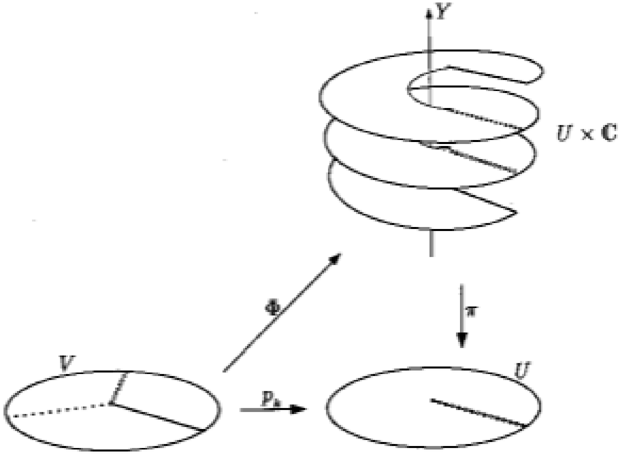
i) we have $f(t^k, \varphi(t)) = 0$ for all $t \in V$;

ii) the map $\Phi : V \to \mathcal{C},\ t \mapsto (t^k, \varphi(t))$, is bijective.

Illustration of the geometric version Puiseux's Theorem

The situation for $k = 3$ and $\rho = 1$ is illustrated in the following sketch. Only the real component of the Y-direction is drawn.

- $p_k : V \to U$ is given by $t \mapsto t^k$,
- $\pi : U \times \mathbb{C} \to U$, $(x, y) \mapsto x$, is projection.



Plan

Factoring Weierstrass polynomials (1/3)

Notations and hypotheses (recall)

- Let $f = Y^k + a_1(X)Y^{n-1} + \cdots + a_k(X) \in \mathbb{C}\langle X\rangle[Y]$ be an irreducible Weierstrass polynomial, with degree $k \geq 1$.
- Let $\rho > 0$ be chosen such that the series $a_1, \ldots, a_k$ converge in the open set $U := \{x \in \mathbb{C} \mid |x| < \rho\}$.
- The discriminant $\operatorname{discrim}(f, Y)(x)$ is not zero for all $x \in U \setminus \{0\}$.
- Let $V := \{t \in \mathbb{C} \mid |t| < \rho^{\frac{1}{k}}\}$.
- Let $\mathcal{C} := \{(x, y) \in U \times \mathbb{C} \mid f(x, y) = 0\}$.
- From the geometric version of Puiseux's theorem, there exists a power series $\phi \in \mathbb{C}\langle T\rangle$ that converges in V and has the following properties:
  1. for all $t \in V$, we have $f(t^k, \phi(t)) = 0$,
  2. $\Psi : V \to \mathcal{C},\ t \longmapsto (t^k, \phi(t))$ is bijective.

Factoring Weierstrass polynomials (2/3)

Proposition

Let $\zeta = \exp(2\pi\imath/k)$ be a k-th primitive root of unity. For all $i = 1, \ldots, k$, we define

$$\varphi_i = \varphi(\zeta^i t) \quad \text{and} \quad \Phi_i := (t^k, \varphi_i(t))$$

Then, $\Phi_1, \ldots, \Phi_k$ are distinct parametrizations of $\mathcal{C}$, that is, the series $\varphi_1, \ldots, \varphi_k$ are distinct.

Proof

- The maps $V \to V,\ t \longmapsto \zeta^i t$ are bijective. Thus, for $i = 1, \ldots, k$, they are distinct.
- Hence, the bijective maps $\Phi_1, \ldots, \Phi_k$ are distinct.

Remark

From a geometric point of view, the maps $\Phi_1, \ldots, \Phi_k$ differ from each other by permutations of the sheets of the covering map $\pi^* : \mathcal{C}^* \to U^*$. Thus, the roots of unity act as "covering transformations".

Factoring Weierstrass polynomials (3/3)

Remark

The parametrizations $\varphi_1, \ldots, \varphi_k$ can be used to extend each factorization

$$f_x(Y) = (Y - c_1) \cdots (Y - c_n), \quad \text{where} \quad c_i \in \mathbb{C}$$

for $x \in U \setminus \{0\}$, to the entire U.

Corollary

Let $(T^k, \varphi(T))$ be a parametrization given by the geometric version of Puiseux's theorem. Let $\zeta, \varphi_1, \ldots, \varphi_k$ be as in the previous proposition. Then, the following holds in $\mathbb{C}\langle T\rangle[Y]$

$$f(T^k, Y) \ = \ (Y - \varphi_1(T)) \cdots (Y - \varphi_k(T)).$$

Proof

Each of $\varphi_1, \ldots, \varphi_k$ is a distinct root in $\mathbb{C}\langle T\rangle$ of the polynomial $f(T^k, Y) \in \mathbb{C}\langle T\rangle[Y]$.

Complement on the algebraic version Puiseux's theorem (1/3)

Notations

- Let $f \in \mathbb{C}\langle X, Y\rangle$ be general in Y.
- Let $n \in \mathbb{N}$ and $\varphi(S) \in \mathbb{C}[[S]]$ be defining a solution to the algebraic version Puiseux's theorem, that is, $f(S^n, \varphi(S)) = 0$ holds in $\mathbb{C}[[S]]$.
- By the preparation theorem, there exist a unit $\alpha \in \langle X, Y\rangle$ and irreducible Weierstrass polynomials $p_1, \ldots, p_r \in \mathbb{C}\langle X\rangle[Y]$

Observations

- Since $\alpha(S^n, \varphi(S)) \neq 0$, there exists $j \in \{1, \ldots, r\}$ such that $p_j(S^n, \varphi(S)) = 0$ holds.
- Therefore, w.l.o.g. one can assume that f is an irreducible Weierstrass polynomial of $\mathbb{C}\langle X\rangle[Y]$ of degree k and of which ϕ is a formal solution in the sense of the algebraic version Puiseux's theorem.

Complement on the algebraic version Puiseux's theorem (2/3)

Observations

- From the previous corollary, there exist $\varphi_1, \ldots, \varphi_k \in \mathbb{C}\langle T \rangle$ such that we have in $\mathbb{C}\langle T \rangle[Y]$
$$f(T^k, Y) \;=\; (Y - \varphi_1(T)) \cdots (Y - \varphi_k(T)).$$
- In the algebraic of version Puiseux's theorem, the *denominator* n can be as large as desired. Thus we can assume $n = \ell k$, for some ℓ.
- Therefore, we have in $\mathbb{C}[[S]][Y]$
$$f(S^n, Y) \;=\; (Y - \varphi_1(S^\ell)) \cdots (Y - \varphi_k(S^\ell)).$$
- Since $\varphi \in \mathbb{C}[[S]]$ is also a zero of $f(S^n, Y)$ and since $\mathbb{C}[[S]][Y]$ is an integral domain, we have $\varphi_i = \phi$, for some i. Hence φ is convergent.

Corollary

If $f \in \mathbb{C}\langle X, Y \rangle$ is an irreducible power series, general in Y of order k, then there exists a convergent power series $\phi \in \mathbb{C}\langle T \rangle$ such that $f(T^k, \phi(T)) = 0$ holds in $\mathbb{C}\langle T \rangle$.

Corollary

If $f \in \mathbb{C}\langle X, Y\rangle$ is irreducible in $\mathbb{C}\langle X, Y\rangle$, then it is also irreducible in $\mathbb{C}[[X, Y]]$. (Thus, for power series, there is no change in the divisibility theory in passing from convergent to formal power series.)

Proof of the corollary

- We may assume that f is a Weierstrass polynomial of degree k.
- Since it is irreducible in $\mathbb{C}\langle X, Y\rangle$, the geometric version of Puiseux's theorem applies. Thus, there exist convergent power series $\varphi_1, \dots, \varphi_k$ such that we have
$$f(T^k, Y) \;=\; (Y - \varphi_1(T)) \cdots (Y - \varphi_k(T)).$$
- Since each factor on the right hand side of the above equality belongs to $\mathbb{C}\langle X, Y\rangle$ and since $\mathbb{C}[[X, Y]]$ is a unique factorization domain, it follows that all possible formal factor of f are necessarily convergent power series. This yields the conclusion.

Definition

- For $m \geq 1$, there is an injective homomorphism
$$\mathbb{C}[[X]] \to \mathbb{C}[[T]],\ X \mapsto T^m.$$
- We regard this as a ring extension
$$\mathbb{C}[[X]] \subseteq \mathbb{C}[[T]] \equiv \mathbb{C}[[X^{\frac{1}{m}}]]$$
- If $m = kn$, there are injections
$$\begin{aligned}&\mathbb{C}[[X]] \to \mathbb{C}[[T]] \to \mathbb{C}[[S]],\\ &X \mapsto T^n.\ T \mapsto S^k,\\ &X \mapsto (S^k)^n = S^m.\end{aligned}$$
which can be regarded as inclusions
$$\mathbb{C}[[X]] \subseteq \mathbb{C}[[X^{\frac{1}{n}}]] \subseteq \mathbb{C}[[X^{\frac{1}{m}}]].$$
- Continuing in this way, we define
$$\mathbb{C}[[X^*]] \ = \ \bigcup_{n=1}^{\infty} \mathbb{C}[[X^{\frac{1}{n}}]].$$
- This is an integral domain that contains all *formal Puiseux series*.

The ring of Puiseux series (2/9)

Definition

For a fixed $\varphi \in \mathbb{C}[[X^*]]$, there is an $n \in \mathbb{N}$ such that $\varphi \in \mathbb{C}[[X^{\frac{1}{n}}]]$. Hence

$$\varphi = \sum_{m=0}^{\infty} a_m X^{\frac{m}{n}}, \quad \text{where} \quad a_m \in \mathbb{C}.$$

and we call *order of* φ the rational number defined by

$$\mathrm{ord}(\varphi) \;=\; \min\{\tfrac{m}{n} \;\mid\; a_m \neq 0\} \geq 0.$$

Lemma

Every monic polynomial of $\mathbb{C}\langle X\rangle[Y]$ splits into linear factors in $\mathbb{C}[[X^*]][Y]$.

Proof of the lemma (1/3)

- Let $f \in \mathbb{C}\langle X\rangle[Y]$ be monic and $k := \deg(f)$. There exist $k_1, \ldots, k_r \in \mathbb{N}_{>0}$ and pairwise distinct $c_1, \ldots, c_r \in \mathbb{C}$ s, t. we have
$$f(0, Y) = (Y - c_1)^{k_1} \cdots (Y - c_r)^{k_r}.$$

Proof of the lemma (2/3)

- By Hensel's Lemma, there exist monic polynomials $f_1, \ldots, f_r \in \mathbb{C}\langle X \rangle[Y]$ such that $f_i(0, Y) = (Y - c_i)^{k_i}$ and
$$f = f_1 \cdots f_r.$$
- If some i, we have $c_i = 0$, then the Weierstrass preparation theorem can be applied to f_i, so $f_i = \alpha_i p_i$ where p_i is a Weierstrass polynomial of degree k_i and α_i is a unit.
- If q is an irreducible factor of p_i, say of degree ℓ, then q is itself a Weierstrass polynomial. Moreover, the geometric version of Puiseux's theorem implies the existence of Puiseux series $\phi_1, \ldots, \phi_\ell \in \mathbb{C}[[X^*]]$ of positive order such that we have
$$q(X, Y) \ = \ (Y - \phi_1(X)) \cdots (Y - \phi_\ell(X)).$$
- Thus, there exist Puiseux series $\varphi_{i,1}, \ldots, \varphi_{i,k_i} \in \mathbb{C}[[X^*]]$ s. t. we have
$$p_i \ = \ (Y - \varphi_{i,1}(X)) \cdots (Y - \varphi_{i,k_i}(X)).$$
and $\mathrm{ord}(\varphi_{i,j}) > 0$ for all $1 \leq j \leq k_i$.

Proof of the lemma (2/3)

- For each i, such that $c_i \neq 0$ holds, we apply the change of coordinates $\widetilde{Y} = Y + c_i$ and set $\widetilde{f_i}(Y) = f_i(\widetilde{Y})$. After returning to the original coordinate system, this gives a factorization of p_i similar to the one in the previous case (that is, the case $c_i = 0$) up to the fact that $\varphi_{i,j} = c_i + \cdots$, that is, $\mathrm{ord}(\varphi_{i,j}) = 0$ for all $1 \leq j \leq k_i$.
- Putting things together, we define $p := p_1 \cdots p_r$ and we have

$$p \;=\; \prod_{\substack{1 \leq i \leq r \\ 1 \leq j \leq k_i}} (Y - \varphi_{i,k_i}(X).$$

- Since f and p have the same roots (counted with multiplicities) in $\mathbb{C}[[X^*]]$ and are both normalized, we conclude $f = p$.

Notation

We denote by $\mathbb{C}((X^*))$ the quotient field of $\mathbb{C}[[X^*]]$.

Remark

In the previous lemma, the hypothesis f monic is essential. Consider $f = XY^2 + Y + 1$. We write $f = Xg(1/X, Y)$ with $g(T, Y) = Y^2 + TY + T$. The previous lemma applies to g which yields a factorization of f into linear factors of $\mathbb{C}((X^*))[Y]$.

Definition

Let $\varphi \in \mathbb{C}[[X^*]]$ and $n \in \mathbb{N}$ minimum with the property that $\varphi \in \mathbb{C}[[X^{\frac{1}{n}}]]$ holds. We say that the Puiseux series φ is *convergent* if we have $\varphi \in \mathbb{C}\langle X \rangle$. Convergent Puiseux series form an integral domain denoted by $\mathbb{C}\langle X^* \rangle$ and whose quotient field is denoted by $\mathbb{C}(\langle X^* \rangle)$.

Proposition

For every element $\varphi \in ((X^*))$, there exist $n \in \mathbb{Z}$, $r \in \mathbb{N}_{>0}$ and a sequence of complex numbers $a_n, a_{n+1}, a_{n+2}, \ldots$ such that

$$\varphi \; = \; \sum_{m=n}^{\infty} a_m X^{\frac{m}{r}} \quad \text{and} \quad a_n \neq 0.$$

and we define $\operatorname{ord}(\varphi) = \frac{n}{r}$. The proof, easy, uses power series inversion.

Remark

Formal Puiseux series can be defined over an arbitrary field $\mathbb{K}$. One essential property of Puiseux series is expressed by the following theorem, attributed to Puiseux for $\mathbb{K} = \mathbb{C}$ but which was implicit in Newton's use of the Newton polygon as early as 1671 and therefore known either as Puiseux's theorem or as the Newton–Puiseux theorem. In its modern version, this theorem requires only $\mathbb{K}$ to be algebraically closed and of characteristic zero. See corollary 13.15 in D. Eisenbud's *Commutative Algebra with a View Toward Algebraic Geometry*.

Theorem

If $\mathbb{K}$ is an algebraically closed field of characteristic zero, then the field $\mathbb{K}((X^*))$ of formal Puiseux series over $\mathbb{K}$ is the algebraic closure of the field of formal Laurent series over $\mathbb{K}$. Moreover, if $\mathbb{K} = \mathbb{C}$, then the field $\mathbb{C}(\langle X^* \rangle)$ of convergent Puiseux series over $\mathbb{C}$ is algebraically closed as well.

Proof of the Theorem (1/3)

- We restrict the proof to the case $\mathbb{K} = \mathbb{C}$. Hence, we prove that $\mathbb{C}((X^*))$ and $\mathbb{C}(\langle X^* \rangle)$ are algebraically closed. We follow the elegant and short proof of K. J. Nowak which relies only on Hensel's lemma.
- It suffices to prove that any monic polynomial $f \in \mathbb{C}((X^*))[Y]$ (resp. $f \in \mathbb{C}(\langle X^* \rangle)[Y]$)

$$f(X, Y) = Y^n + a_1(X)Y^{n-1} + \cdots + a_n(X)$$

of degree $n > 1$ is reducible.

Proof of the Theorem (2/3)

- Making use of the Tschirnhausen transformation of variables $\widetilde{Y} = Y + \frac{1}{n} a_1(X)$, we can assume that the coefficient $a_1(X)$ is identically zero. W.l.o.g., we assume $a_n(X)$ not identically zero.
- For each $k = 1, \ldots, n$, define $r_k = \mathrm{ord}(a_k(X)) \in \mathbb{Q}$, unless a_k is identically zero.
- Define $r := \min\{r_k/k\}$. Obviously, we have $r_k/k - r \geq 0$, with equality for at least one k.
- Take a positive integer q so large that all Puiseux series $a_k(X)$ are of the form $f_k(X^{1/q})$ for $f_k \in \mathbb{C}[[Z]]$ (resp. $f_k \in \mathbb{C}\langle Z \rangle$). Let $r := p/q$ for an appropriate $p \in \mathbb{Z}$.
- After the transformation of variables $X = w^q,\ Y = U \cdot w^p$, we get
$$f(X, Y) = w^{np} \cdot Q(w, U), \quad \text{where}$$
$$Q(w, U) = U^n + b_2(w) U^{n-2} + \cdots + b_n(w) \ \text{ and } \ b_k(w) = a_k(w^q) w^{-kp}.$$

Proof of the Theorem (3/3)

- Observe that $\mathrm{ord}(b_k(w)) \in \mathbb{Z}$ and satisfies in fact
$$\mathrm{ord}(b_k(w)) = q \cdot r_k - k \cdot p = q \cdot k(r_k \cdot k - r) \geq 0.$$
- Therefore $Q(w, U)$ is a polynomial in $\mathbb{C}[[w]][U]$ (resp. $\mathbb{C}\langle w\rangle[U]$).
- Furthermore we have $\mathrm{ord}(b_k(w)) = 0$ for at least one k. Thus, for every such k, we have $b_k(0) \neq 0$.
- Therefore, the complex polynomial
$$Q(0, U) = U^n + b_2(0)U^{n-2} + \cdots + b_n(0) \not\equiv (U - c)^n$$
for any $c \in \mathbb{C}$.
- Hence, $Q(0, U)$ is the product of two coprime polynomials in $\mathbb{C}[U]$.
- By Hensel's lemma, $Q(w, U)$ is the product of two polynomials $Q_1(w, U)$ and $Q_2(w, U)$ in $\mathbb{C}[[w]][U]$ (resp. $\mathbb{C}\langle w\rangle[U]$).
- Finally, we have
$$f(X, Y) = X^{nr} \cdot Q_1(X^{1/q}, X^{-r}Y) \cdot Q_2(X^{1/q}, X^{-r}Y).$$

Plan

The extended Hensel construction (EHC)

Goal

- Factorize $F(X,Y) \in \mathbb{C}[X,Y]$ into linear factors in X over $\mathbb{C}(\langle Y^* \rangle)$:
$$F(X,Y) = (X - \chi_1(Y))(X - \chi_2(Y)) \cdots (X - \chi_d(Y))$$
where each $\chi_i(Y)$ is a *Puiseux series*.
- Thus offers an alternative algorithm to that of Newton-Puiseux.

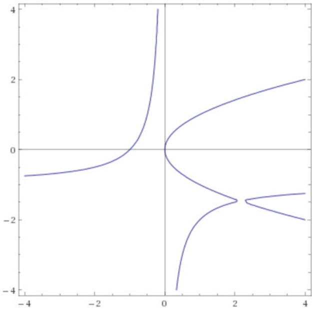
Remarks

- The EHC generalizes to factorize polynomials over multivariate power series rings
- Hence, the EHC has similar goal to Abhyankar-Jung theorem
- However, it is a weaker form:
  - less demanding hypotheses, and
  - weaker output format, making it easier to compute.

An example with the `PowerSeries` library

```
> P := PowerSeries([y]):
> U := UnivariatePolynomialOverPowerSeries([y], x):
> poly := y^2 *x + y^2 - y*x^3 - y*x^2 + y -x^2;
                                3      2         2    2    2
                 poly := -x   y - x   y + x y   - x   + y   + y

U:-ExtendedHenselConstruction(poly,[0],3);
                       -T - 1          2         2          2        2
          [[y = T, x = ------], [y = T , x = -T ], [y = T , x = T ]]
                         T
```



Another example

```
> P := PowerSeries([y, z]) :
  U := UnivariatePolynomialOverPowerSeries([y, z], x) :
  poly := y·x^3 + (−2 · y + z + 1)·x + y :
  U:−ExtendedHenselConstruction(poly, [0, 0], 3);
```

$$\left[\left[x = \frac{-\mathit{RootOf}(\_Z^2+y) + \mathit{RootOf}(\_Z^2+y)\, y - \frac{1}{2}\mathit{RootOf}(\_Z^2+y)\, z + \frac{1}{2} y^2}{y}\right],\right.$$

$$\left[x = \frac{\mathit{RootOf}(\_Z^2+y) - \mathit{RootOf}(\_Z^2+y)\, y + \frac{1}{2}\mathit{RootOf}(\_Z^2+y)\, z + \frac{1}{2} y^2}{y}\right],$$

$$\left.[x = -y]\right]$$

Related works (1/2)

1. Extended Hensel Construction (EHC):
   - Introduction: F. Kako and T. Sasaki, 1999
   - Extensions:
     - M. Iwami, 2003,
     - D. Inaba, 2005,
     - D. Inaba and T. Sasaki 2007,
     - D. Inaba and T. Sasaki 2016.
2. Newton-Puiseux:
   - H. T. Kung and J. F. Traub, 1978,
   - D. V. Chudnovsky and G. V. Chudnovsky, 1986
   - A. Poteaux and M. Rybowicz, 2015.

Related works (2/2)

- The Extended Hensel Construction (EHC) compute all branches concurrently
- while approaches based on Newton-Puiseux computes one branch after another.

For $F(X, Y) := -X^3 + Y\,X + Y$:

1. the EHC produces
   1. $\chi_1(Y) := Y^{\frac{1}{3}} + \frac{1}{3}\,Y^{\frac{2}{3}} + O(Y)$,
   2. $\chi_2(Y) := \frac{-1+\sqrt{-3}}{2}\,Y^{\frac{1}{3}} + \frac{1}{3}\,(\frac{-1-\sqrt{-3}}{2})\,Y^{\frac{2}{3}} + O(Y)$,
   3. $\chi_3(Y) := (\frac{-1-\sqrt{-3}}{2})\,Y^{\frac{1}{3}} + \frac{1}{3}\,(\frac{-1+\sqrt{-3}}{2})\,Y^{\frac{2}{3}} + O(Y)$.
2. Whereas Kung-Traub's method (based on Newton-Puiseux) computes
   1. $\chi_1(Y) := Y^{\frac{1}{3}} + \frac{1}{3}\,Y^{\frac{2}{3}} + O(Y)$,
   2. $\chi_2(Y) := \theta\,Y^{\frac{1}{3}} + \frac{\theta^2}{3}\,Y^{\frac{2}{3}} + O(Y)$,
   3. $\chi_3(Y) := \theta^2\,Y^{\frac{1}{3}} + \frac{\theta}{3}\,Y^{\frac{2}{3}} + O(Y)$,

   for $\theta \in \mathbb{C}$ such that $\theta^3 = 1, \theta^2 \neq 1, \theta \neq 1$, since $F(X, Y)$ is a Weierstrass polynomial.

Related works (2/2)

- The Extended Hensel Construction (EHC) compute all branches concurrently
- while approaches based on Newton-Puiseux computes one branch after another.

For $F(X,Y) := -X^3 + Y\,X + Y$:

1. the EHC produces
   1. $\chi_1(Y) := Y^{\frac{1}{3}} + \frac{1}{3}\,Y^{\frac{2}{3}} + O(Y)$,
   2. $\chi_2(Y) := \frac{-1+\sqrt{-3}}{2}\,Y^{\frac{1}{3}} + \frac{1}{3}\,(\frac{-1-\sqrt{-3}}{2})\,Y^{\frac{2}{3}} + O(Y)$,
   3. $\chi_3(Y) := (\frac{-1-\sqrt{-3}}{2})\,Y^{\frac{1}{3}} + \frac{1}{3}\,(\frac{-1+\sqrt{-3}}{2})\,Y^{\frac{2}{3}} + O(Y)$.
2. Whereas Kung-Traub's method (based on Newton-Puiseux) computes
   1. $\chi_1(Y) := Y^{\frac{1}{3}} + \frac{1}{3}\,Y^{\frac{2}{3}} + O(Y)$,
   2. $\chi_2(Y) := \theta\,Y^{\frac{1}{3}} + \frac{\theta^2}{3}\,Y^{\frac{2}{3}} + O(Y)$,
   3. $\chi_3(Y) := \theta^2\,Y^{\frac{1}{3}} + \frac{\theta}{3}\,Y^{\frac{2}{3}} + O(Y)$,

   for $\theta \in \mathbb{C}$ such that $\theta^3 = 1, \theta^2 \neq 1, \theta \neq 1$, since $F(X,Y)$ is a Weierstrass polynomial.

Related works (2/2)

- The Extended Hensel Construction (EHC) compute all branches concurrently
- while approaches based on Newton-Puiseux computes one branch after another.

For $F(X,Y) := -X^3 + Y\,X + Y$:

1. the EHC produces
   1. $\chi_1(Y) := Y^{\frac{1}{3}} + \frac{1}{3}\,Y^{\frac{2}{3}} + O(Y)$,
   2. $\chi_2(Y) := \frac{-1+\sqrt{-3}}{2}\,Y^{\frac{1}{3}} + \frac{1}{3}\,(\frac{-1-\sqrt{-3}}{2})\,Y^{\frac{2}{3}} + O(Y)$,
   3. $\chi_3(Y) := (\frac{-1-\sqrt{-3}}{2})\,Y^{\frac{1}{3}} + \frac{1}{3}\,(\frac{-1+\sqrt{-3}}{2})\,Y^{\frac{2}{3}} + O(Y)$.
2. Whereas Kung-Traub's method (based on Newton-Puiseux) computes

   1. $\chi_1(Y) := Y^{\frac{1}{3}} + \frac{1}{3}\,Y^{\frac{2}{3}} + O(Y)$,
   2. $\chi_2(Y) := \theta\,Y^{\frac{1}{3}} + \frac{\theta^2}{3}\,Y^{\frac{2}{3}} + O(Y)$,
   3. $\chi_3(Y) := \theta^2\,Y^{\frac{1}{3}} + \frac{\theta}{3}\,Y^{\frac{2}{3}} + O(Y)$,

   for $\theta \in \mathbb{C}$ such that $\theta^3 = 1, \theta^2 \neq 1, \theta \neq 1$, since $F(X,Y)$ is a Weierstrass polynomial.

Overview

Notations

- Let $F(x, y) \in \mathbb{C}[x, y]$ be square-free, monic in x and let $d := \deg_x(F)$.
- Note that assuming $F(x, y)$ is general in x of order $d = \deg_x(F)$ (thus meaning $F(x, 0) = x^d$ and $F(x, y)$ is a Weierstrass polynomial) is a stronger condition, which is not required here.
- On can easily reduce to the case where F is monic in x as long as the leading coefficient of F in x can be seen an invertible power series in $\mathbb{C}\langle y \rangle$.

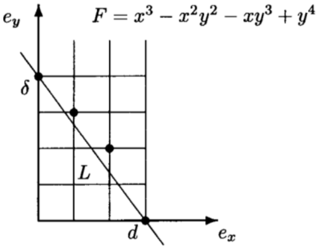
Objectives

- The final goal is to to factorize F over the field $\mathbb{C}(\langle y^* \rangle)$ of convergent Puiseux series over $\mathbb{C}$.
- This follows the ideas of Hensel lemma: lifting the factors of an intial factorization.
- If the initial factorization has no multile roots, then we are able to generate the homomogeneous parts (one degree after another) of the coefficients of the factors predicted by Puiseux's theorem.

Newton line (1/2)

Definition

- We consider a 2D grid G where the Cartesian coordinates (e_x, e_y) of a point are integers.
- Each nonzero term $c\, x^{e_x} y^{e_y}$ of $F(x, y)$, with $c \in \mathbb{C}$ is mapped to the point of coordinates (e_x, e_y) on the grid.
- Let L be the straight line passing through the point $(d, 0)$ as well as another point of the plot of F such that no points in the plot of F lye below L; The line L is called the *Newton line* of F.



Newton line (2/2)

```
> F := x^3  - x^2 * y^2  -x*y^3 + y^4;
                                   2  2       3    4    3
                            F := -x  y  - x y  + y  + x
> U := UnivariatePolynomialOverPowerSeries([y], x):
> U:-ExtendedHenselConstruction(F,[0],2);
                                       5       6
       3        4            5        T       T
[[y = T , x = T  %1 - 1/3 T  %1 + ---- + ----],
                                      3       3

          3         4         5         6
    [y = T , x = -T  - 1/3 T  + 1/3 T ],
                                                6
          3         4        4         5       T
    [y = T , x = -T  %1 + T  + 1/3 T  %1 + ----]]
                                               3

                2
%1 := RootOf(_Z  - _Z + 1)
```

Newton polynomial

Definition

The sum of all the terms of $F(x, y)$, which are plotted on the Newton line of F is called the *Newton polynomial* of F and is denoted by $F^{(0)}(x, y)$.

Remarks

- The Newton polynomial is uniquely determined and has at least two terms.
- Let $\delta \in \mathbb{Q}$ such that the equaton of the Newton line is $e_x/d + e_y/\delta = 1$.
- Observe that $F^{(0)}(x, y)$ is homogeneous in $(x, y^{\delta/d})$ of degree d.
- That is, $F^{(0)}(x, y)$ consists of monomials included in the set $\{x^d, x^{d-1}y^{\delta/d}, x^{d-2}y^{2\delta/d}, \ldots, y^{d\delta/d}\}$.

Factorizing Newton polynomial (1/2)

Notations

Let $r \geq 1$ be an integer, let $\zeta_1, \ldots, \zeta_r \in \mathbb{C}$, with $\zeta_i \neq \zeta_j$ for any $i \neq j$ and let $m_1, \ldots, m_r \in \mathbb{N}$ be positive such that we have

$$F^{(0)}(x, 1) = (x - \zeta_1)^{m_1} \cdots (x - \zeta_r)^{m_r}.$$

Recall that $F^{(0)}(x, y)$ is homogeneous in $(x, y^{\delta/d})$ of degree d.

Lemma

We have:

$$F^{(0)}(x, y) = (x - \zeta_1 y^{\delta/d})^{m_1} \cdots (x - \zeta_r y^{\delta/d})^{m_r}.$$

Proof of the lemma

- It is enough to show that $(\zeta_i y^{\delta/d}, y)$ vanishes $F^{(0)}(x, y)$ for all y.
- Define $\hat{y} = y^{\delta/d}$ such that $F^{(0)}(x, \hat{y})$ is homogeneous of degree d in $(x, \hat{y})$.
- Since each monomial of $F^{(0)}(x, \hat{y})$ is of the form $x^{e_x} y^{e_y}$ where $e_x + e_y = d$, we have
$$F^{(0)}(\zeta_i \hat{y}, \hat{y}) = \hat{y}^d \underbrace{(\cdots)}_{\text{some constant terms}} = 0.$$
- The last equality is valid since $F^{(0)}(\zeta_i, 1) = 0$ clearly holds.

Factorizing Newton polynomial (2/2)

```
> F := x^3  - x^2 * y^2  -x*y^3 + y^4;
                                    2  2      3    4    3
                             F := -x  y  - x y  + y  + x

>  L := x^3 - y^4;
                                            4    3
                                    L := -y  + x

> PolynomialTools:-Split(eval(L,[y=1]), x);
                         2                               2
  (x - 1) (x - RootOf(_Z  + _Z + 1)) (x + 1 + RootOf(_Z  + _Z + 1))

> U:-ExtendedHenselConstruction(F,[0],1);
                                        5      6
       3       4            5          T      T
[[y = T , x = T  %1 - 1/3 T  %1 + ---- + ----],
                                       3      3
          3        4        5        6
    [y = T , x = -T  - 1/3 T  + 1/3 T ],
                                                    6
          3        4       4        5              T
    [y = T , x = -T  %1 + T  + 1/3 T  %1 + ----]]
                                                    3
                 2
%1 := RootOf(_Z  - _Z + 1)
```

The moduli of the Hensel-Sasaki constuction (1/2)

Notations

Let $\hat{\delta}, \hat{d} \in \mathbb{Z}^{>0}$ such that:

$$\hat{\delta}/\hat{d} = \delta/d, \quad \gcd \hat{\delta}, \hat{d} = 1$$

Choosing such integers $\hat{\delta}, \hat{d}$ is possible since $\delta \in \mathbb{Q}$ and $d \in \mathbb{N}^{>0}$.

Lemma

Each non-constant monomial of $F(x, y)$ is contained in the set

$$\{x^d y^{(k+0)/\hat{d}}, x^{d-1} y^{(k+\hat{\delta})/\hat{d}}, x^{d-2} y^{(k+2\hat{\delta})/\hat{d}}, \ldots, x^0 y^{(k+d\hat{\delta})/\hat{d}} \mid k = 0, 1, 2, \ldots\}.$$

Proof of the lemma

- It is enough to show that for each exponent vector (e_x, e_y) which is not below the Newton's line, there exists i, k such that we have $x^{e_x} y^{e_y} = x^{d-i} y^{(k+i\hat{\delta})/\hat{d}}$.
- Given such an exponent vector (e_x, e_y), let us choose $i = d - e_x$ and $k = e_y \hat{d} - i\hat{\delta}$.
- One should check, of course, that $k \geq 0$ holds, which follows easily from $e_x/d + e_y/\delta \geq 1$.

The moduli of the Hensel-Sasaki constuction (2/2)

Notations

The previous lemma leads us to define the following monomial ideals

$$\begin{array}{rcl} S_k & = & <x, y^{\hat{\delta}/\hat{d}}>^d \times <y^{1/\hat{d}}>^k \\ & = & <x^d, x^{d-1}y^{\hat{\delta}/\hat{d}}, x^{d-2}y^{2\hat{\delta}/\hat{d}}, \ldots, x^0 y^{d\hat{\delta}/\hat{d}}> \times <y^{1/\hat{d}}>^k \\ & = & <x^d y^{(k+0)/\hat{d}}, x^{d-1}y^{(k+\hat{\delta})/\hat{d}}, x^{d-2}y^{(k+2\hat{\delta})/\hat{d}}, \ldots, x^0 y^{(k+d\hat{\delta})/\hat{d}}> \end{array}$$

Remark

- The generators of $<x, y^{\hat{\delta}/\hat{d}}>^d$ are homogeneous monomials in $(x, y^{\hat{\delta}/\hat{d}})$ of degree d.
- We can view S_k as a polynomial ideal in the variables x and $y^{1/\hat{d}}$; note that the monomials generating S_k regarded in this way do not all have the same total degree.
- We shall use the ideals S_k, for $k = 1, 2, \ldots$, as moduli of the Hensel-Sasaki construction to be described hereafter.
- We have $F(x,y) \equiv F^{(0)}(x,y) \mod S^{(1)}$.

A weak but algrithmic version of Puiseux theorem (1/2)

As before, for $F \in \mathbb{C}[x, y]$ (and in fact, even for $F(x, y) \in \mathbb{C}\langle y \rangle[x]$) our ultimate goal is to factorize $F(x, y)$ as

$$F(x, y) = G_1(x, y) \cdots G_r(x, y)$$

where

1. this factorization holds in $\mathbb{C}((y^*))$, and
2. $\deg_x (G_i) = 1$ holds for all $i = 1, \ldots, r$.

In our first step, we will allow $\deg_x (G_i) \geq 1$ for all $i = 1, \ldots, r$. Moreover, in practice,

1. we compute a truncated factorization, that is, $G_1(x, y), \ldots, G_r(x, y)$ are polynomials in $\mathbb{C}]x, y]$ (in fact homomogeneous polynomials) and,
2. the relation $F(x, y) = G_1(x, y) \cdots G_r(x, y)$ holds modulo an ideal S_k.

A weak but algrithmic version of Puiseux theorem (2/2)

Hypothesis

We assume that $F^{(0)}(x,y)$ has been factorized as

$$F^{(0)}(x,y) = G_1^{(0)}(x,y) \cdots G_r^{(0)}(x,y)$$

where the polynomials $G_i^{(0)}(x,y)$ are homomogeneous and coprime w.r.t. x (that is, once y is specialized to 1). Of course, a special case is

$$G_i^{(0)}(x,y) = (x - \zeta_i y^{\delta/d})^{m_i}$$

For simplicity, we write $\hat{y} = y^{\hat{\delta}/\hat{d}}$.

Lagrange's Interpolation polynomials (1/4)

Lemma

Let $\hat{G}_i(x,\hat{y}) \in \mathbb{C}[x,\hat{y}]$, for $i = 1,\ldots,r$, be homogeneous polynomials in $(x,\hat{y})$, that we regard in $\mathbb{C}\langle\hat{y}\rangle[x]$, such that

- $r \geq 2$ and $d = \deg_x\left(\hat{G}_1 \cdots \hat{G}_r\right)$,
- $\deg_x \hat{G}_i = m_i$ for $i = 1,\ldots,r$, and
- $\gcd_x(\hat{G}_i,\hat{G}_j) = 1$ for any $i \neq j$.

Then, for each $\ell \in \{0,\ldots,d-1\}$, there exists only one set of polynomials $\{W_i^{(\ell)}(x,\hat{y}) \in \mathbb{C}\langle\hat{y}\rangle[x] \mid i = 1,\ldots,r\}$ satisfying

1. $W_1^{(\ell)}\left(\left(\hat{G}_1\cdots\hat{G}_r\right)/\hat{G}_1\right) + \cdots + W_r^{(\ell)}\left(\left(\hat{G}_1\cdots\hat{G}_r\right)/\hat{G}_r\right) = x^\ell\hat{y}^{d-\ell}$,
2. $\deg_x\left(W_i^{(\ell)}(x,\hat{y})\right) < \deg_x\left(\hat{G}_i(x,\hat{y})\right)$, for $i = 1,\ldots,r$.

Moreover, the polynomials $W_i^{(0)},\ldots,W_i^{(d-1)}$, for $i = 1,\ldots,r$ are homogeneous in $(x,\hat{y})$ of degree m_i. We call them the *Lagrange's interpolation polynomials*.

Proof of the lemma (1/3)

- We shall first prove that there exists only one set of polynomials
$$\{W_i^{(\ell)}(x,1) \mid i = 1, \ldots, r\}$$
satisfying (1) and (2) in the above lemma statement, when $\hat{y} = 1$.
- Using the extended Euclidean algorithm, one can compute $A_1, \ldots, A_s \in \mathbb{C}[x]$ such that
$$A_1 \frac{\hat{G}_1 \cdots \hat{G}_s}{\hat{G}_1} + \cdots + A_s \frac{\hat{G}_1 \cdots \hat{G}_s}{\hat{G}_s} = 1.$$
- If we multiply both sides of the above equality by x^ℓ, then we have $A_1 x^\ell \frac{\hat{G}_1 \cdots \hat{G}_s}{\hat{G}_1} + \cdots + A_s x^\ell \frac{\hat{G}_1 \cdots \hat{G}_s}{\hat{G}_s} = x^\ell \quad (\bigstar)$.

Proof of the lemma (2/3)

- For each $i = 1, \ldots, r-1$, let $Q_i, R_i \in \mathbb{C}[x]$ such that
  - $A_i x^\ell = Q_i \hat{G}_i + R_i$ and
  - $\deg_x(R_i) < \deg_x(\hat{G}_i)$
- Thus the equality ($\bigstar$) can be re-written as:

$$R_1 \frac{\hat{G}_1 \cdots \hat{G}_r}{\hat{G}_1} + \cdots + R_{r-1} \frac{\hat{G}_1 \cdots \hat{G}_r}{\hat{G}_{r-1}} + (A_r x^\ell + \sum_{i=1}^{r-1} Q_i \hat{G}_r) \frac{\hat{G}_1 \cdots \hat{G}_r}{\hat{G}_r} = x^\ell.$$

- Observe that we have
  - $\deg_x(R_i \frac{\hat{G}_1 \cdots \hat{G}_r}{\hat{G}_i}) < d$ for $i = 1, \ldots, r-1$,
  - $\deg_x(\frac{\hat{G}_1 \cdots \hat{G}_r}{\hat{G}_r}) = d - m_r$, and also
  - $\ell < d$.
- Combined with relation ($\bigstar$), we obtain

$$\deg_x(A_r x^\ell + \sum_{i=1}^{r-1} Q_i \hat{G}_r) < m_r = \deg_x(\hat{G}_r).$$

Proof of the lemma (3/3)

- Hence, we set
  - $W_i^{(\ell)}(x, 1) = R_i,$ for $i = 1, \ldots, r-1$
  - $W_r^{(\ell)}(x, 1) = A_r x^\ell + \sum_{i=1}^{r-1} Q_i \hat{G}_r$
- The proof of the unicity will be added later ...
- Note that we have $\deg(x^\ell \hat{y}^{d-\ell}) = d$.
- Since $\deg_x \left(W_i^{(\ell)}(x, 1) \left(\hat{G}_1 \cdots \hat{G}_r \right) / \hat{G}_i \right) < d$, we can homogenize in degree d both $W_i^{(\ell)}(x, 1)$ and $\hat{G}_i(x, 1)$, for $i = 1, \ldots, r$, using $\hat{y}$ as homogeization variable.
- This homogeization process defines each $W_i^{(\ell)}(x, \hat{y})$ uniquely.
- Moreover we have,

$$\deg_x(W_i^{(\ell)}(x, \hat{y})) < \deg_x(\hat{G}_i),$$

since the homogenization has no effect on degrees in x.

Hensel-Sasaki construction: bivariate case

Theorem

Let $F(x, y) \in \mathbb{C}\langle y\rangle[x]$ be a square-free polynomial, monic in x of degree $d > 0$. Let $F^{(0)}(x, y)$ be the Newton polynomial of $F(x, y)$. Let $G_1^{(0)}(x, y), \ldots, G_r^{(0)}(x, y) \in \mathbb{C}[x, y]$ be homogeneous polynomials in $(x, \hat{y})$, pairwise coprime when $\hat{y} = 1$, such that we have:

$$F^{(0)}(x, y) = G_1^{(0)}(x, y) \cdots G_r^{(0)}(x, y).$$

Recall $S_k = <x^d y^{(k+0)/\hat{d}}, x^{d-1} y^{(k+\hat{\delta})/\hat{d}}, x^{d-2} y^{(k+2\hat{\delta})/\hat{d}}, \ldots, x^0 y^{(k+d\hat{\delta})/\hat{d}}>$ for $k = 1, 2, \ldots$. Then, for any positive integer k, we can construct $G_i^{(k)}(x, y) \in \mathbb{C}\langle y^{1/\hat{d}}\rangle[x]$, for $i = 1, \ldots, r$, satisfying

1. $F(x, y) = G_1^{(k)}(x, y) \cdots G_r^{(k)}(x, y) \mod S_{k+1}$,
2. $G_i^{(k)}(x, y) = G_i^{(0)}(x, y) \mod S_1, \quad i = 1, \ldots, r.$

The proof is by induction on k and constructive.

Proof (1/5)

- **base case:** Since $F(x,y) \equiv F^{(0)}(x,y) \mod S_1$, the theorem is valid for $k = 0$.
- **inductive step:** Let the theorem be valid up to the $(k-1)$-st construction. We write

$$G_i^{(k-1)} = G_i^{(0)}(x,y) + \Delta G_i^{(1)}(x,y) + \cdots + \Delta G_i^{(k-1)}(x,y),$$

  such that
  - $G_i^{(k')}(x,y) \in S_{k'}$ for $k' = 1, \ldots, k-1$,
  - $\deg_x(\Delta G_i^{(k')}(x,y)) < \deg_x(G_i^{(0)}(x,y)) = m_i, \quad k' = 1, \ldots, k-1.$

  These latter properties are part of the induction hypothesis.
  Note: Each $\Delta G_i^{(k')}(x,y)$ is being computed in the k'-th Hensel construction step. So the degree in x does not increase contrary to the degree in y, because of the definition of S_k.

Proof (2/5)

We define:

$$\Delta F^{(k)}(x,y) := F(x,y) - G_1^{(k-1)} \cdots G_r^{(k-1)} \mod S_{k+1}.$$

According to the format of monomials of $F(x,y)$ (Lemma in page 8) and also induction assumptions, we have

$$\begin{aligned}
&\Delta F^{(k)}(x,y) = f_{d-1}^{(k)} x^{d-1} y^{\hat{\delta}/\hat{d}} + \cdots + f_0^{(k)} x^0 y^{d\hat{\delta}/\hat{d}} \\
&f_\ell^{(k)} = c_\ell^{(k)} y^{k/\hat{d}},\ c_\ell^{(k)} \in \mathbb{C} \quad \text{for } \ell = 0, \ldots, d-1
\end{aligned}$$

We construct $G_i^{(k)}(x,y)$ by observing that we have:

$$G_i^{(k)}(x,y) = G_i^{(k-1)}(x,y) + \Delta G_i^{(k)}(x,y), \quad \Delta G_i^{(k)}(x,y) \equiv 0 \mod S_k$$

Then we have:

$$\begin{aligned}
F(x,y) &\equiv \left(G_1^{(k-1)} + \Delta G_1^{(k)}\right) \cdots \left(G_r^{(k-1)} + \Delta G_r^{(k)}\right) \mod S_{k+1} \\
&\equiv G_1^{(k-1)} \cdots G_r^{(k-1)} + \Delta G_1^{(k)} \left(G_2 \cdots G_r\right) + \cdots + \Delta G_r^{(k)} \left(G_1 \cdots G_{r-1}\right) + \\
&\qquad \underbrace{\text{other terms}}_{\text{containg } \Delta G_i^{(k)}(x,y) \text{ and } \Delta G_j^{(k)}(x,y)} \mod S_{k+1} \\
&\equiv G_1^{(k-1)} \cdots G_r^{(k-1)} + \Delta G_1^{(k)} \left(G_2 \cdots G_r\right) + \cdots + \Delta G_r^{(k)} \left(G_1 \cdots G_{r-1}\right) \mod S_{k+1} \\
&\equiv G_1^{(k-1)} \cdots G_r^{(k-1)} + \Delta G_1^{(k)} \left(G_2^{(0)} \cdots G_r^{(0)}\right) + \cdots + \Delta G_r^{(k)} \left(G_1^{(0)} \cdots G_{r-1}^{(0)}\right) \mod S_{k+1}
\end{aligned}$$

Proof (4/5)

The last two equivalence relations are valid, since

$$\Delta G_i^{(k)}(x,y)\Delta G_j^{(k')}(x,y) \equiv 0 \mod S_{k+1} \quad \text{for } k' = 1, \ldots, k.$$

It actually follows from the fact that by assumption,

- $\Delta G_j^{(k)} \equiv 0 \mod S_k$
- $\Delta G_j^{(k')} \equiv 0 \mod S_{k'}$ for $k' = 1, \ldots, k$

Thus,

$$\Delta G_j^{(k)} \Delta G_j^{(k')} \equiv 0 \mod S_k S_{k'}$$

Since, $S_k S_{k'} = S_{k+k'}$ then

$$\Delta G_j^{(k)} \Delta G_j^{(k')} \equiv 0 \mod S_{k+k'} \quad \text{for } k' = 1, \ldots, k$$

Furthermore, since $k' \geq 1$, then

$$\Delta G_j^{(k)} \Delta G_j^{(k')} \equiv 0 \mod S_{k+1} \quad \text{for } k' = 1, \ldots, k$$

Proof (5/5)

Therefore,

$$\Delta F^{(k)} \equiv \Delta G_1^{(k)}\left(G_2^{(0)}\cdots G_r^{(0)}\right)+\cdots+\Delta G_r^{(k)}\left(G_1^{(0)}\cdots G_{r-1}^{(0)}\right) \mod S_{k+1}$$

If in the lemma of Lagrange Interpolation polynomial we let $\hat{G}_i(x,\hat{y}) = G_i^{(0)}(x,\hat{y})$, using the other representation of $\Delta F^{(k)}(x,y)$, it allows us to solve the last equation (the equation above) as

$$\begin{aligned}
\textstyle\sum_{i=1}^{r} \Delta G_i^{(k)}(x,y)\frac{\left(G_1^{(0)}\cdots G_r^{(0)}\right)}{G_i^{(0)}} &= \textstyle\sum_{\ell=0}^{d-1} f_\ell^{(k)} x^\ell \hat{y}^{d-\ell} \\
&= \textstyle\sum_{\ell=0}^{d-1} f_\ell^{(k)}\left(\sum_{i=1}^{r} W_i^{(\ell)}\frac{\left(G_1^{(0)}\cdots G_r^{(0)}\right)}{G_i^{(0)}}\right) \\
&= \textstyle\sum_{i=1}^{r}\left(\sum_{\ell=0}^{d-1} f_\ell^{(k)} W_i^{(\ell)}\right)\frac{\left(G_1^{(0)}\cdots G_r^{(0)}\right)}{G_i^{(0)}}
\end{aligned}$$

Since $\deg_x(f_\ell^{(k)} W_i^{(\ell)}) < \deg_x(G_i^{(0)})$ and $\deg_x(\Delta G_i^{(k)}(x,y)) < \deg_x(G_i^{(0)})$ for $i = 1,\ldots,r$, then we have

$$\Delta G_i^{(k)}(x,y) = \textstyle\sum_{\ell=0}^{d-1} W_i^{(\ell)}(x,y) f_\ell^{(k)}(y) \quad i = 1,\ldots,r$$

About the theorem

Remarks

- The proof of the theorem constructs the $G_i^{(k)}(x,y)$ uniquely.
- The theorem holds in particular for the case where the case where $G_i^{(0)}(x,y) = (x - \zeta_i y^{\hat{\delta}/\hat{d}})^{m_i}$ holds for each $i = 1, \ldots, r$.
- However, the theorem is more generral and only requires that the $G_i^{(0)}(x,y)$ are homogeneous polynomials in $(x, \hat{y})$, pairwise coprime when $\hat{y} = 1$.
- And, in fact each factor $G_i^{(0)}(x,y)$ of the Newton polynomial are necessarily a product of some of the $(x - \zeta_i y^{\hat{\delta}/\hat{d}})$ and thus each factor $G_i^{(0)}(x,y)$ is homogeneous in $(x, \hat{y})$.

Proposition

If the initial factors $G_i^{(0)}(x,y)$ are in fact polynomials in $\mathbb{C}[x,y]$, then, after the k-th lifting step, the computed factors $G_i^{(k)}(x,y)$ are themselves polynomials in $\mathbb{C}[x,y]$.

The proof of this proposition follows by tracking the calculations of the lemma and the theorem.

Plan

Limit points of (the quasi-component of) a regular chain

- Let $R := \{t_2(x_1, x_2), \ldots, t_n(x_1, \ldots, x_n)\}$ where t_i has its coefficients in $\mathbb{C}$.
- We regard t_i as a univariate polynomial w.r.t. x_i, for $i = 2, \ldots, n$:
- We denote by h_i the leading coefficient (also called initial) of t_i w.r.t. x_i, and assume that h_i depends on x_1 only; hence we have

$$t_i \ = \ h_i(x_1) x_i^{d_i} + c_{d_i-1}(x_1, \ldots, x_{i-1}) x_i^{d_i-1} + \cdots + c_0(x_1, \ldots, x_{i-1})$$

- Consider the system

$$W(R) := \begin{cases} t_n(x_1, \ldots, x_n) = 0 \\ \vdots \\ t_2(x_1, x_2) = 0 \\ (h_2 \cdots h_n)(x_1) \neq 0 \end{cases}$$

- We want to compute the non-trivial limit points of $W(R)$, that is

$$\lim(W(R)) \ := \ \overline{W(R)}^{Z} \setminus W(R).$$

Puiseux expansions of a regular chain (1/2)

Notation

- Let R be as before. Assume R is strongly normalized, that is, every initial is a univariate polynomial in x_1
- Let $\mathbb{K} = \mathbb{C}(\langle x_1^* \rangle)$.
- Then R generates a zero-dimensional ideal in $\mathbb{C}[x_2, \ldots, x_n]$.
- Let $V^*(R)$ be the zero set of R in $\mathbb{K}^{n-1}$.

Definition

We call *Puiseux expansions* of R the elements of $V^*(R)$.

Puiseux expansions of a regular chain (1/2)

A regular chain R

$$R := \begin{cases} X_1X_3^2 + X_2 \\ X_1X_2^2 + X_2 + X_1 \end{cases}$$

Puiseux expansions of R

$$\begin{cases} X_3 &=& 1 + O(X_1^2) \\ X_2 &=& -X_1 + O(X_1^2) \end{cases} \quad \begin{cases} X_3 &=& -1 + O(X_1^2) \\ X_2 &=& -X_1 + O(X_1^2) \end{cases}$$

$$\begin{cases} X_3 &=& {X_1}^{-1} - \frac{1}{2}X_1 + O(X_1^2) \\ X_2 &=& -{X_1}^{-1} + X_1 + O(X_1^2) \end{cases} \quad \begin{cases} X_3 &=& -{X_1}^{-1} + \frac{1}{2}X_1 + O(X_1^2) \\ X_2 &=& -{X_1}^{-1} + X_1 + O(X_1^2) \end{cases}$$

Relation between $\lim_0(W(R))$ and Puiseux expansions of R

Theorem

For $W \subseteq \mathbb{C}^s$, denote

$$\lim_0(W) := \{x = (x_1, \ldots, x_s) \in \mathbb{C}^s \mid x \in \lim(W) \text{ and } x_1 = 0\},$$

and define

$$V^*_{\geq 0}(R) := \{\Phi = (\Phi^1, \ldots, \Phi^{s-1}) \in V^*(R) \mid \mathrm{ord}(\Phi^j) \geq 0, j = 1, \ldots, s-1\}.$$

Then we have

$$\lim_0(W(R)) = \cup_{\Phi \in V^*_{\geq 0}(R)} \{(X_1 = 0, \Phi(X_1 = 0))\}.$$

$$V^*_{\geq 0}(R) := \left\{ \begin{array}{lcl} X_3 & = & 1 + O(X_1^2) \\ X_2 & = & -X_1 + O(X_1^2) \end{array} \right. \cup \left\{ \begin{array}{lcl} X_3 & = & -1 + O(X_1^2) \\ X_2 & = & -X_1 + O(X_1^2) \end{array} \right.$$

Thus the limit ponts are $\lim_0(W(R)) = \{(0, 0, 1), (0, 0, -1)\}$.

Limit points: this example again

```
> R := PolynomialRing([x, y, z]):
  rc := Chain([y^(3)-2*y^(3)+y^(2)+z^(5), z^(4)*x+y^(3)-y^(2)], Empty(R), R): Display(rc, R);
  br := RegularChainBranches(rc, R, [z], coefficient = complex);
```

$$\begin{cases} z^4 x + y^3 - y^2 = 0 \\ -y^3 + y^2 + z^5 = 0 \\ z^4 \neq 0 \end{cases}$$

$$br := \left[\left[z = T^2, y = \frac{1}{2} T^5 \left(-T^5 + 2\, RootOf(\_Z^2+1)\right), x = -\frac{1}{8} T^2 \left(-T^{20} + 6\, T^{15}\, RootOf(\_Z^2+1) + 10\, T^{10} + 8\right)\right], \left[z = T^2, y = -\frac{1}{2} T^5 \left(T^5 + 2\, RootOf(\_Z^2+1)\right), x = \frac{1}{8} T^2 \left(T^{20} + 6\, T^{15}\, RootOf(\_Z^2+1) - 10\, T^{10} - 8\right)\right], \left[z = T, y = T^5 + 1, x = -T\left(T^{10} + 2\, T^5 + 1\right)\right]\right]$$

```
> br := RegularChainBranches(rc, R, [z], coefficient = real);
```

$$br := \left[\left[z = T, y = T^5 + 1, x = -T\left(T^{10} + 2\, T^5 + 1\right)\right]\right]$$

Figure: The command RegularChainBranches computes a parametrization for the complex and real paths of the quasi-component defined by rc. When coefficient argument is set as real, then the command RegularChainBranches computes the real branches.

Plan

Plan

Quotients of bivariate real analytic functions (1/3)

Notations

- Let $a, b \in \mathbb{R}$ and f, g be real analytic functions.
- Hence, f, g are given by power series which are absolutely convergent in an open disk centered at (a, b).

The problem

- Determining whether $\lim_{(x,y)\to(a,b)} \frac{f(x,y)}{g(x,y)}$ exists, and
- if it does then compute it.

Quotients of bivariate real analytic functions (2/3)

Weierstrass preparation theorem (recalled in $\mathbb{K}\langle X, Y\rangle$)

Let $h \in \mathbb{K}\langle X, Y\rangle$ be general in Y of order $d \in \mathbb{N}$. Then there exists a unique pair (α, p) such that

1. α is a unitt of $\mathbb{K}\langle X, Y\rangle$,
2. p is a Weierstrass polynomial in Y of degree k, that is, p writes $Y^d + a_1 Y^{d-1} + \cdots + a_d$ where $a_1, \ldots, a_d$ belong to the ideal generated by X in $\mathbb{K}\langle X\rangle$,
3. $h = \alpha p$.

The above theorem implies that in some neighborhood of the origin, the zeros of h are the same as those of the Weierstrass polynomial p.

Quotients of bivariate real analytic functions (3/3)

Reduction from analytic to polynomial functions

- Weierstrass preparation theorem allows us to reduce the paused problem to computing the limit of a quotient of rational function.
- Indeed, the hypothesis "general in Y of a finite order" always holds after a suitable change of coordinates of the form. Indeed, we have the following.

Proposition

For $h_1, \ldots, h_n \in \mathbb{K}\langle X, Y\rangle$, all non-zero, there exists a positive integer ν such that each power series ${h_i}'(X', Y') = h_i(X + Y^\nu, Y)$ is of finite order in the variable Y'.

Limits of multivariate real rational functions

Notations

Let $q \in \mathbb{Q}(X_1, \ldots, X_n)$ be a multivariate rational function.

The problem

We want to decide whether

$$\lim_{(x_1,\ldots,x_n)\to(0,\ldots,0)} q(x_1, \ldots, x_n)$$

exists, and if it does, whether it is finite.

Limits of rational functions: previous works (1/3)

Univariate functions (including transcendental ones)

D. Gruntz (1993, 1996), B. Salvy and J. Shackell (1999)

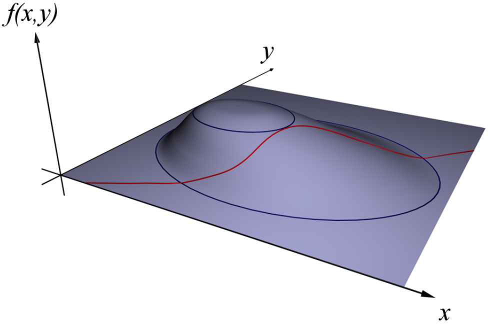
- Corresponding algorithms are available in popular computer algebra systems

Multivariate rational functions

S.J. Xiao and G.X. Zeng (2014)

- Given $q \in \mathbb{Q}(X_1, \ldots, X_n)$, they proposed an algorithm deciding whether or not: $\lim_{(x_1,\ldots,x_n)\to(0,\ldots,0)} q$ *exists and is zero*.
- No assumptions on the input multivariate rational function
- Techniques used:
  - triangular decomposition of algebraic systems,
  - rational univariate representation,
  - adjoining infinitesimal elements to the base field.

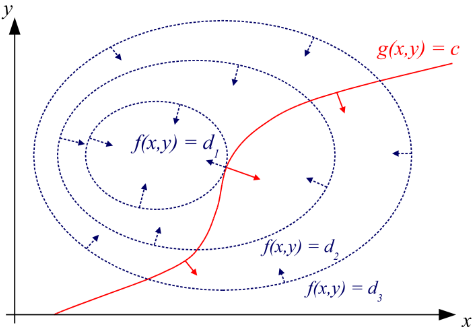
Interlude: the method of Lagrange multipliers (1/3)



- Let f and g be functions from $\mathbb{R}^n$ to $\mathbb{R}$ with continuous first partial derivatives.
- Consider the ooptimization problem

$$\max_{\text{subject to } g(x_1,\ldots,x_n)=0} f(x_1,\ldots,x_n)$$

Interlude: the method of Lagrange multipliers (2/3)



We are looking at points $(x_1, \ldots, x_n)$ where $f(x_1, \ldots, x_n)$ does not change much as we walk along $g(x_1, \ldots, x_n) = 0$. This can happen in two ways:

- either such a point is a optimizer (maximizer or minimizer),
- or we are following a level of f, that is, $f(x_1, \ldots, x_n) = d$ for some d.

Both cases are captured by imposing that the gradient vectors $\nabla_{x_1,\ldots,x_n} f$ and $\nabla_{x_1,\ldots,x_n} g$ are parallel.

Interlude: the method of Lagrange multipliers (3/3)

The previous observation translates into a system of equations that, in particular, maximizers and minimizers must satisfy.

$$\begin{aligned} g\left(x_1, x_2, \ldots, x_n\right) &= 0 \\ \frac{\partial f}{\partial x_1}\left(x_1, x_2, \ldots, x_n\right) - \lambda \frac{\partial g}{\partial x_1}\left(x_1, x_2, \ldots, x_n\right) &= 0 \\ \frac{\partial f}{\partial x_2}\left(x_1, x_2, \ldots, x_n\right) - \lambda \frac{\partial g}{\partial x_2}\left(x_1, x_2, \ldots, x_n\right) &= 0 \\ &\vdots \\ \frac{\partial f}{\partial x_n}\left(x_1, x_2, \ldots x_n\right) - \lambda \frac{\partial g}{\partial x_n}\left(x_1, x_2, \ldots, x_n\right) &= 0. \end{aligned}$$

where λ is an additional variable, called the Lagrange multiplier of the corresponding optimization problem.

Limits of rational functions: previous works (2/3)

C. Cadavid, S. Molina, and J. D. Vélez (2013):

- Assumes that the origin is an isolated zero of the denominator
- Maple built-in command `limit/multi`

Discriminant variety

$\chi(q) \; = \; \{(x, y) \in \mathbb{R}^2 \;\mid\; y\frac{\partial q}{\partial x} - x\frac{\partial q}{\partial y} = 0\}.$

Key observation

For determining the existence and possible value of

$$\lim_{(x,y)\to(0,0)} q(x, y),$$

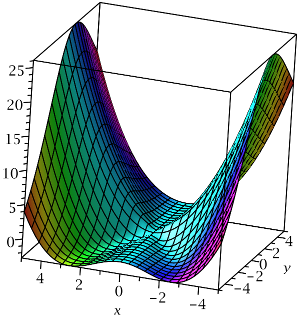
it is sufficient to compute

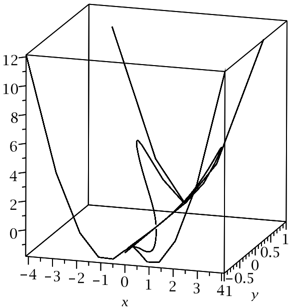
$$\lim_{\substack{(x,y) \to (0,0) \\ (x,y) \in \chi(q)}} q(x, y).$$

Example

Let $q \in \mathbb{Q}(x, y)$ be a rational function defined by $q(x, y) = \frac{x^4+3x^2y-x^2-y^2}{x^2+y^2}$.

$$\chi(q) = \left\{ \begin{array}{rcl} x^4 + 2x^2y^2 + 3y^3 & = & 0 \\ y & < & 0 \end{array} \right. \cup \left\{ \begin{array}{rcl} x & = & 0 \end{array} \right.$$





Limits of rational functions: previous works (3/3)

J.D. Vélez, J.P. Hernández, and C.A Cadavid (2015).

- Assumes that the origin is an isolated zero of the denominator
- Ad-hoc method reducing to the case of bivariate rational functions

Similar key observation

For determining the existence and possible value of

$$\lim_{(x,y,z)\to(0,0,0)} q(x,y,z),$$

it is sufficient to compute

$$\lim_{\substack{(x,y,z)\to(0,0,0)\\(x,y,z)\in\chi(q)}} q(x,y,z).$$

Techniques used

- Computation of singular loci
- Variety decomposition into irreducible components

The discriminant variety of Cadavid, Molina, Vélez (1/2)

Notations

- Let $q : \mathbb{R}^n \longrightarrow \mathbb{R}$ be a function with continuous first partial derivatives.
- For a postive real number ρ, let D^*_ρ be the punctured ball
$$D^*_\rho \ = \ \{(x_1, \ldots, x_n) \in \mathbb{R}^n \ \mid \ 0 < \sqrt{x_1^2 + \cdots + x_n^2} < \rho\}.$$
- Let $\chi(q)$ be the subset of $\mathbb{R}^n$ where the vectors $\nabla_{x_1,\ldots,x_n} q$ and $(x_1, \ldots, x_n)$ are parallel.
- For $n = 2$, we have
$$\chi(q) \ = \ \{(x, y) \in \mathbb{R}^2 \ \mid \ y\frac{\partial q}{\partial x} - x\frac{\partial q}{\partial y} = 0\}.$$

Theorem (Cadavid, Molina, Vélez)

For all $L \in \mathbb{R}$ the following assertions re equivalent:

1. $\lim_{(x_1,\ldots,x_n)\to(0,\ldots,0)} q(x_1, \ldots, x_n)$ exists and equals L,
2. for all $\varepsilon > 0$, there exists $0 < \delta < \rho$ such that for all $(x_1, \ldots, x_n) \in \chi(q) \cap D^*_\rho$ the inequality $|q(x_1, \ldots, x_n) - L| < \varepsilon$ holds.

The discriminant variety of Cadavid, Molina, Vélez (2/2)

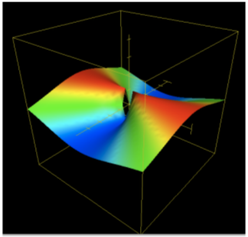
Proof

- Clearly the first assertion implies the second one.
- Next, we assume that the second one holds and we prove the first one.
- Hence, we assume that for all $\varepsilon > 0$, there exists $0 < \delta < \rho$ such that for all $(x_1, \ldots, x_n) \in \chi(q) \cap D_\rho^*$ the inequality $|q(x_1, \ldots, x_n) - L| < \varepsilon$ holds.
- We fix $\varepsilon > 0$. For every $r > 0$, we define
$$C_r = \{(x_1, \ldots, x_n) \in \mathbb{R}^n \ | \ \sqrt{x_1^2 + \cdots + x_n^2} = r\}.$$
- For all $r > 0$, we choose $t_1(r)$ (resp. $t_2(r)$) minimzing (resp. maximizing) q on C_r. Hence, for all $r > 0$, we have $t_1(r), t_2(r) \in \chi(q)$.
- For all $(x_1, \ldots, x_n) \in \mathbb{R}^n$, we have
$$q(t_1(r)) - L \ \leq \ q(x_1, \ldots, x_n) - L \ \leq \ q(t_2(r)) - L,$$
where $r = \sqrt{x_1^2 + \cdots | x_n^2}$.
- From the assumption and the definitions of $t_1(r), t_2(r)$, there exists $0 < \delta < \rho$ such that for all $r < \rho$ we have
$$-\varepsilon < q(t_1(r)) - L \ \text{ and } \ q(t_2(r)) - L < \varepsilon.$$
- Therefore, there exists $0 < \delta < \rho$ such that for all $(x_1, \ldots, x_n) \in D_\rho^*$ the inequality $|q(x_1, \ldots, x_n) - L| < \varepsilon$ holds.

The method of Cadavid, Molina, Vélez (1/2)

- Their approach transforms the initial limit computation in $n = 2$ variables to one or more limit computations in $n - 1 = 1$ variable.
- One non-trivial part of the method is to find the *real branches* of the variety $\chi(q)$ around the origin.
- This requires tools like Newton-Puiseux theorem in order to *parametrize* $\chi(q)$ around the origin.

The method of Cadavid, Molina, Vélez (2/2)



- Consider $q(x,y) = \frac{f(x,y)}{g(x,y)}$ with $f(x,y) = x^2 - y^2$ and $g(x,y) = x^2 + y^2$.
- We have $\chi(q) = \{(x,y) \in \mathbb{R}^2 \;\mid\; xy\left(x^2+y^2\right) = 0\}$
- Hence, $\chi(q)$ consists of the planes $x = 0$ and $y = 0$.
- Thus, for computing $\lim_{(x,y)\to(0,0)} q(x,y)$, it is enough to consider $\lim_{x\to 0} q(x,0)$ and $\lim_{y\to 0} q(0,y)$ which are equal to 1 and -1 respectively.
- Therefore, $\lim_{(x,y)\to(0,0)} q(x,y)$ does not exist.

Plan

Regular semi-algebraic system

Notation

- Let $T \subset \mathbb{Q}[X_1 < \ldots < X_n]$ be a regular chain with $\mathbf{y} := \{\mathrm{mvar}(t) \mid t \in T\}$ and $\mathbf{u} := \mathbf{x} \setminus \mathbf{y} = U_1, \ldots, U_d$.
- Let P be a finite set of polynomials, s.t. every $f \in P$ is regular modulo $\mathrm{sat}(T)$.
- Let $\mathcal{Q}$ be a quantifier-free formula of $\mathbb{Q}[\mathbf{u}]$.

Definition

We say that $R := [\mathcal{Q}, T, P_>]$ is a regular semi-algebraic system if:

(i) $\mathcal{Q}$ defines a non-empty open semi-algebraic set $\mathcal{O}$ in $\mathbb{R}^d$,

(ii) the regular system $[T, P]$ specializes well at every point u of $\mathcal{O}$

(iii) at each point u of $\mathcal{O}$, the specialized system $[T(u), P(u)_>]$ has at least one real solution.

Define

$$Z_{\mathbb{R}}(R) = \{(u, y) \mid \mathcal{Q}(u), t(u, y) = 0, p(u, y) > 0, \forall (t, p) \in T \times P\}.$$

Regular semi-algebraic system

Notation

- Let $T \subset \mathbb{Q}[X_1 < \ldots < X_n]$ be a regular chain with $\mathbf{y} := \{\mathrm{mvar}(t) \mid t \in T\}$ and $\mathbf{u} := \mathbf{x} \setminus \mathbf{y} = U_1, \ldots, U_d$.
- Let P be a finite set of polynomials, s.t. every $f \in P$ is regular modulo $\mathrm{sat}(T)$.
- Let $\mathcal{Q}$ be a quantifier-free formula of $\mathbb{Q}[\mathbf{u}]$.

Definition

We say that $R := [\mathcal{Q}, T, P_>]$ is a regular semi-algebraic system if:

(i) $\mathcal{Q}$ defines a non-empty open semi-algebraic set $\mathcal{O}$ in $\mathbb{R}^d$,

(ii) the regular system $[T, P]$ specializes well at every point u of $\mathcal{O}$

(iii) at each point u of $\mathcal{O}$, the specialized system $[T(u), P(u)_>]$ has at least one real solution.

Define

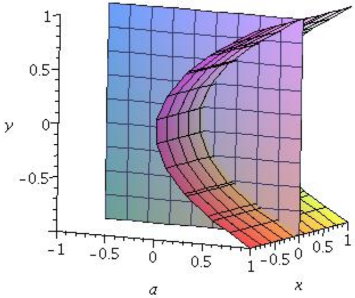
$$Z_{\mathbb{R}}(R) = \{(u, y) \mid \mathcal{Q}(u), t(u, y) = 0, p(u, y) > 0, \forall (t, p) \in T \times P\}.$$

Example

The system $[\mathcal{Q}, T, P_>]$, where

$$\mathcal{Q} := a > 0,\ T := \begin{cases} y^2 - a = 0 \\ x = 0 \end{cases},\ P_> := \{y > 0\}$$

is a regular semi-algebraic system.



Regular semi-algebraic system

Notations

Let $R := [\mathcal{Q}, T, P_>]$ be a regular semi-algebraic system. Recall that $\mathcal{Q}$ defines a non-empty open semi-algebraic set $\mathcal{O}$ in $\mathbb{R}^d$ and

$$Z_{\mathbb{R}}(R) = \{(u, y) \mid \mathcal{Q}(u), t(u, y) = 0, p(u, y) > 0, \forall(t, p) \in T \times P\}.$$

Properties

- Each connected component C of $\mathcal{O}$ in $\mathbb{R}^d$ is a real analytic manifold, thus locally homeomorphic to the hyper-cube $(0, 1)^d$
- Above each C, the set $Z_{\mathbb{R}}(R)$ consists of disjoint graphs of semi-algebraic functions forming a real analytic covering of C.
- There is at least one such graph.

Consequences

- R can be understood as a parameterization of $Z_{\mathbb{R}}(R)$
- The Jacobian matrix $\left[\ \nabla t, t \in T\ \right]$ is full rank.

Triangular decomposition of semi-algebraic sets

Proposition

Let $S := [F_{=}, N_{\geq}, P_{>}, H_{\neq}]$ be a semi-algebraic system. Then, there exists a finite family of regular semi-algebraic systems $R_1, \ldots, R_e$ such that

$$Z_{\mathbb{R}}(S) = \cup_{i=1}^{e} Z_{\mathbb{R}}(R_i).$$

Triangular decomposition

- In the above decomposition, $R_1, \ldots, R_e$ is called a triangular decomposition of S and we denote by `RealTriangularize` an algorithm computing such a decomposition.
- Moreover, such a decomposition can be computed in an incremental manner with a function `RealIntersect`
  - taking as input a regular semi-algebraic system R and a semi-algebraic constraint $f = 0$ (resp. $f > 0$) for $f \in \mathbb{Q}[X_1, \ldots, X_n]$
  - returning regular semi-algebraic system $R_1, \ldots, R_e$ such that

$$Z_{\mathbb{R}}(f = 0) \cap Z_{\mathbb{R}}(R) \quad = \quad \cup_{i=1}^{e} Z_{\mathbb{R}}(R_i).$$

Limit along a semi-algebraic set (1/2)

Notation

- Let S be a semi-algebraic set of dimension at least 1 and such that the origin of $\mathbb{R}^n$ belongs to the closure $\overline{Z_{\mathbb{R}}(S)}$ of $Z_{\mathbb{R}}(S)$ in the Euclidean topology.
- Let $L \in \mathbb{R}$.

Definition

We say that, when $(x_1, \ldots, x_n) \in \mathbb{R}^n$ approaches the origin along S, the limit of the rational function $q(x_1, \ldots, x_n)$ exists and equals L, whenever for all $\varepsilon > 0$, there exists $0 < \delta$ such that for all $(x_1, \ldots, x_n) \in S \cap D_\delta^*$ the inequality $|q(x_1, \ldots, x_n) - L| < \varepsilon$ holds. When this holds, we write

$$\lim_{\substack{(x_1, \ldots, x_n) \to (0, \ldots, 0) \\ (x_1, \ldots, x_n) \in S}} q(x_1, \ldots, x_n) = L$$

Limit along a semi-algebraic set (2/2)

Lemma

Let $R_1, \ldots, R_e$ be regular semi-algebraic systems forming a triangular decomposition of $\chi(q)$.

Then, for all $L \in \mathbb{R}$ the following two assertions are equivalent:

(i) $\lim_{\substack{(x_1, \ldots, x_n) \to (0, \ldots, 0) \\ (x_1, \ldots, x_n) \in \chi(q)}} q(x_1, \ldots, x_n)$ exists and equals L.

(ii) for all $i \in \{1, \ldots, e\}$ such that $Z_{\mathbb{R}}(R_i)$ has dimension at least 1 and the origin belongs to $\overline{Z_{\mathbb{R}}(R_i)}$, we have $\lim_{\substack{(x_1, \ldots, x_n) \to (0, \ldots, 0) \\ (x_1, \ldots, x_n) \in Z_{\mathbb{R}}(R_i)}} q(x_1, \ldots, x_n)$ exists and equals L.

Plan

Overview of main algorithms

Top-level algorithm

1. computes the discriminant variety $\chi(q)$ of q
2. applies the previous lemma and reduces the whole process to computing limits of q along finitely many pathes (i.e. space curves)
3. as soon as either one path produces an infinite limit or two pathes produce two different finite limits, the procedure stops and returns `no_finite_limit`.

Core algorithm

- reduces computations of limits of q along branches of $\chi(q)$ to computing limits of q along pathes.

Base-case algorithm

- handles the computation of q along space curves by means of Puiseux series expansions

The algorithm `RationalFunctionLimit`

Input: a rational function $q \in \mathbb{Q}(X_1, \ldots, X_n)$ such that origin is an isolated zero of the denominator.

Output: $\lim_{(x_1,\ldots,x_n)\to(0,\ldots,0)} q(x_1, \ldots, x_n)$

1. Apply `RealTriangularize` on $\chi(q)$, obtaining rsas $R_1, \ldots, R_e$
2. Discard R_i if either $\dim(R_i) = 0$ or $\underline{o} \notin \overline{Z_{\mathbb{R}}(R_i)}$
   - QuantifierElimination checks whether $\underline{o} \in \overline{Z_{\mathbb{R}}(R_i)}$ or not.
3. Apply LimitInner(R) on each regular semi algebraic system of dimension higher than one.
   - main task: solving constrained optimization problems
4. Apply `LimitAlongCurve` on each one-dimensional regular semi algebraic system resulting from Step 3
   - main task: Puiseux series expansions

Principles of LimitInner

Input: a rational function q and a regular semi algebraic system $R := [Q, T, P_>]$ with $\dim(Z_{\mathbb{R}}(R)) \geq 1$ and $\underline{o} \in \overline{Z_{\mathbb{R}}(R)}$

Output: limit of q at the origin along $Z_{\mathbb{R}}(R)$

1. if $\dim(Z_{\mathbb{R}}(R)) = 1$ then return LimitAlongCurve(q, R)
2. otherwise build $\mathcal{M} := \begin{bmatrix} X_1 & \cdots & X_n \\ \multicolumn{3}{c}{\nabla t, t \in T} \end{bmatrix}$
3. For all $m \in$ Minors$(\mathcal{M})$ such that $Z_{\mathbb{R}}(R) \not\subseteq Z_{\mathbb{R}}(m)$ build
$$\mathcal{M}' := \begin{bmatrix} \frac{\partial E_r}{\partial X_1} & \cdots & \frac{\partial E_r}{\partial X_n} \\ X_1 & \cdots & X_n \\ \multicolumn{3}{c}{\nabla t, t \in T} \end{bmatrix} \text{ with } E_r := \sum_{i=1}^{n} A_i X_i^2 - r^2$$
4. For all $m' \in$ Minors$(\mathcal{M}')$ $\mathcal{C} :=$ `RealIntersect`$(R, m' = 0, m \neq 0)$
5. For all $C \in \mathcal{C}$ such that $\dim(Z_{\mathbb{R}}(C)) > 0$ and $\underline{o} \in \overline{Z_{\mathbb{R}}(C)}$
   1. compute $L :=$ LimitInner(q, C);
   2. if L is `no_finite_limit` or L is finite but different from a previously found finite L then return `no_finite_limit`
6. If the search completes then a unique finite was found and is returned.

Principles of LimitAlongCurve

Input: a rational function q and a curve C given by $[Q, T, P_{>}]$

Output: limit of q at the origin along C

1. Let f, g be the numerator and denominator of q
2. Let $T' := \{gX_{n+1} - f\} \cup T$ with X_{n+1} a new variable
3. Compute the real branches of $W_{\mathbb{R}}(T') := Z_{\mathbb{R}}(T') \setminus Z_{\mathbb{R}}(h_{T'})$ in $\mathbb{R}^n$ about the origin via Puiseux series expansions
4. If no branches escape to infinity and if $W_{\mathbb{R}}(T')$ has only one limit point $(x_1, \ldots, x_n, x_{n+1})$ with $x_1 = \cdots = x_n = 0$, then x_{n+1} is the desired limit of q
5. Otherwise return `no_finite_limit`

Example

Let $q(x, y, z, w) = \frac{z\,w + x^2 + y^2}{x^2 + y^2 + z^2 + w^2}$.
`RealTriangularize` $(\chi(q))$:

$$Z_{\mathbb{R}}(\chi(q)) = Z_{\mathbb{R}}(R_1) \cup Z_{\mathbb{R}}(R_2) \cup Z_{\mathbb{R}}(R_3) \cup Z_{\mathbb{R}}(R_4),$$

where

$$R_1 := \begin{cases} x = 0 \\ y = 0 \\ z = 0 \\ w = 0 \end{cases}, R_2 := \begin{cases} x = 0 \\ y = 0 \\ z + w = 0 \end{cases},$$

$$R_3 := \begin{cases} x = 0 \\ y = 0 \\ z - w = 0 \end{cases}, R_4 := \begin{cases} z = 0 \\ w = 0 \end{cases}.$$

Example

- $\dim(Z_{\mathbb{R}}(R_1)) = 0$
- $\dim(Z_{\mathbb{R}}(R_2)) = 1 \Longrightarrow$ LimitAlongCurve $(q, R_2) = \frac{-1}{2}$
- $\dim(Z_{\mathbb{R}}(R_3)) = 1 \Longrightarrow$ LimitAlongCurve $(q, R_3) = \frac{1}{2}$
- $\dim(Z_{\mathbb{R}}(R_4)) = 2 \Longrightarrow$ LimitInner (q, R_4)
  -
$$R_5 := \begin{cases} z = 0 \\ w = 0 \\ x = 0 \\ y \neq 0 \end{cases}, R_6 := \begin{cases} z = 0 \\ w = 0 \\ y = 0 \\ x \neq 0 \end{cases}$$

  - $\dim(Z_{\mathbb{R}}(R_5)) = 1 \Longrightarrow$ LimitAlongCurve $(q, R_5) = 1$
  - $\dim(Z_{\mathbb{R}}(R_6)) = 1 \Longrightarrow$ LimitAlongCurve $(q, R_6) = 1$

$\Longrightarrow$ the limit does not exists.

Plan

The main result

Notation

- Assume that $n \geq 3$ holds.
- Let $S = [\mathcal{Q}, T, P_>]$ be a regular semi-algebraic system of $\mathbb{Q}[X_1, \ldots, X_n]$ such that $Z_{\mathbb{R}}(S)$ has dimension d, with $n > d \geq 2$, and the closure $\overline{Z_{\mathbb{R}}(S)}$ contains the origin.
- W.l.o.g. we can assume that the polynomials $t_{d+1}, \ldots, t_n$ forming the regular chain T have main variables $X_{d+1}, \ldots, X_n$.
- Let $\mathcal{M}$ be the $(n-d+1) \times n$ matrix whose first row is the vector $(X_1, \ldots, X_n)$ and, for $j = d+1, \ldots, n$, whose $(j-d+1)$-th row is the gradient vector

$$\nabla t_j = \begin{pmatrix} \frac{\partial t_j}{\partial X_1} & \cdots & \frac{\partial t_j}{\partial X_n} \end{pmatrix}$$

  where t_j is the polynomial of T with $\mathrm{mvar}(t_j) = X_j$.

Theorem

Then, there exists a non-empty set $\mathcal{O} \subset D_\rho^* \cap Z_{\mathbb{R}}(S)$, which is open relatively to $Z_{\mathbb{R}}(S)$ and which satisfies $\emptyset \in \overline{\mathcal{O}}$ (that is, the origin is in the closure of $\mathcal{O}$) such that $\mathcal{M}$ is full rank at any point of $\mathcal{O}$.

The main result in codimension 1

Notation

- Assume $n \geq 3$.
- Let $S = [\mathcal{Q}, \{t_n\}, P_>]$ be a regular semi-algebraic system of $\mathbb{Q}[X_1, \ldots, X_n]$ such that $Z_{\mathbb{R}}(S)$ has dimension $d := n - 1$, and the closure $\overline{Z_{\mathbb{R}}(S)}$ contains the origin.
- W.l.o.g. we assume that $\mathrm{mvar}(t_n) = X_n$ holds.
- Let $\mathcal{M}$ be the $2 \times n$ matrix with the vector $(X_1, \ldots, X_n)$ as first row and the gradient vector $\nabla t_n = \begin{pmatrix} \frac{\partial t_n}{\partial X_1} & \cdots & \frac{\partial t_n}{\partial X_n} \end{pmatrix}$ as second row.

Theorem

Then, there exists a non-empty set $\mathcal{O} \subset D_\rho^* \cap Z_{\mathbb{R}}(S)$, which is open relatively to $Z_{\mathbb{R}}(S)$, such that $\mathcal{M}$ is full rank at any point of $\mathcal{O}$, and the origin is in the closure of $\mathcal{O}$.

A simple topological argument

Notation

- Assume $n \geq 3$.
- Let $S = [\mathcal{Q}, T, P_>]$ be a regular semi-algebraic system of $\mathbb{Q}[X_1, \ldots, X_n]$ such that $Z_{\mathbb{R}}(S)$ has dimension d with $n > d \geq 1$.

Lemma

Then, the number of d-dimensional semi-algebraic sets which are the intersection of $Z_{\mathbb{R}}(S)$ and a sphere (or an ellipsoid) centred at the origin is finite.

The key PDE argument: simple version

Notation

- Let $h \in \mathbb{R}[X_1, \ldots, X_n]$ be of positive degree in X_n.
- Assume that there exists a real number λ such that $\nabla h(p) = \lambda p$ holds for all p in a neighbourhood V_0 of the origin in $\mathbb{R}^n$.
- Let also $U_0 \subset \mathbb{R}^{n-1}$ be a neighbourhood of the origin in $\mathbb{R}^{n-1}$ such that the standard projection of V_0 onto $(X_1, \ldots, X_{n-1})$ contains U_0.
- Assume the leading coefficient c of h in X_n and the discriminant Δ of h in X_n vanish nowhere on U_0.

Lemma

Then, there exists a smooth function $u : U_0 \longrightarrow \mathbb{R}$ for which

$$h(x_1, \ldots, x_{n-1}, u(x_1, \ldots, x_{n-1})) = 0 \tag{5}$$

holds, for all $(x_1, \ldots, x_{n-1}) \in U_0$. Moreover, the graph of every smooth function $u : U_0 \longrightarrow \mathbb{R}$ satisfying Relation (5) is contained in a sphere centred at the origin.

The key PDE argument: proof (1/6)

- We view h as a parametric polynomial in X_n with $X_1, \ldots, X_{n-1}$ as parameters.
- Recall that the leading coefficient c of h in X_n and the discriminant Δ of h in X_n vanish nowhere on U_0.
- It follows from the theory of parametric polynomial systems that the intersection of U_0 and the discriminant variety of h is empty.
- Therefore, there exists a smooth analytic function $u : U_0 \longrightarrow \mathbb{R}$ such that Equation (5) holds for all $(x_1, \ldots, x_{n-1}) \in U_0$.
- Let u be such a function and define

$$W = \{(x_1, \ldots, x_{n-1}, x_n) \mid x_1, \ldots, x_{n-1} \in U_0 \text{ and } x_n = u(x_1, \ldots, x_{n-1}$$

The key PDE argument: proof (2/6)

- Thus, the set W is the graph of u. For any $t \in W$, the normal vector of W at t is given by

$$n(t) = \frac{(-\partial u/\partial X_1, \ldots, -\partial u/\partial X_{n-1}, 1)}{\sqrt{(\partial u/\partial X_1)^2 + \cdots + (\partial u/\partial X_{n-1})^2 + 1}}.$$

- Using Equation (5) and the hypothesis on ∇h, elementary calculations yield

$$n(t) = \frac{(x_1, \ldots, x_{n-1}, u(x_1, \ldots, x_{n-1}))}{\sqrt{x_1^2 + \cdots + x_{n-1}^2 + u^2(x_1, \ldots, x_{n-1})}}$$

which results in the following equalities, for $i = 1, \ldots, n-1$:

$$\begin{cases} \frac{X_i}{\sqrt{X_1^2+\cdots+X_{n-1}^2+u^2(X_1,\ldots,X_{n-1})}} = -\frac{\partial u/\partial X_i}{\sqrt{(\partial u/\partial X_1)^2+\cdots+(\partial u/\partial X_{n-1})^2+1}} \\ \frac{u(X_1,\ldots,X_{n-1})}{\sqrt{X_1^2+\cdots+X_{n-1}^2+u^2(X_1,\ldots,X_{n-1})}} = \frac{1}{\sqrt{(\partial u/\partial X_1)^2+\cdots+(\partial u/\partial X_{n-1})^2+1}} \end{cases} \tag{6}$$

The key PDE argument: proof (3/6)

- The last equality in Relation (6) implies that we have:

$$u(X_1, \ldots, X_{n-1}) = \frac{\sqrt{X_1^2 + \cdots + X_{n-1}^2 + u^2(X_1, \ldots, X_{n-1})}}{\sqrt{(\partial u/\partial X_1)^2 + \cdots + (\partial u/\partial X_{n-1})^2 + 1}}.$$

- Consequently, we obtain the following system of PDEs:

$$\left\{ \; u(X_1, \ldots, X_{n-1})\, \partial u/\partial X_i = -X_i \quad , \text{ for } \; i = 1, \ldots, n-1. \right. \tag{7}$$

The key PDE argument: proof (4/6)

- Recalll

$$\left\{ \; u(X_1, \ldots, X_{n-1}) \, \partial u / \partial X_i = -X_i \quad , \text{ for } \; i = 1, \ldots, n-1. \right.$$

- Now for $i = 1$, we integrate both sides of Equation (7) with respect to X_1. There exists a differentiable function $F_2(X_2, \ldots, X_{n-1})$ such that we have:

$$\frac{u^2(X_1, \ldots, X_{n-1})}{2} = \frac{-X_1^2}{2} + F_2(X_2, \ldots, X_{n-1}). \tag{8}$$

- Now by taking the derivative of both sides of Equation (8) with respect to X_2, we have

$$u \, \partial u / \partial X_2 = \partial F_2 / \partial X_2.$$

The key PDE argument: proof (5/6)

- After substitution of the latter equality in the equation $u\,\partial u/\partial X_2 = -X_2$, there exists a differentiable function $F_3(X_3, \ldots, X_{n-1})$ such that we have:

$$\frac{-X_2^2}{2} = F_2(X_2, \ldots, X_{n-1}) + F_3(X_3, \ldots, X_{n-1}).$$

- By continuing in the same manner, we have

$$\frac{-X_{i-1}^2}{2} = F_{i-1}(X_{i-1}, \ldots, X_{n-1}) + F_i(X_i, \ldots, X_{n-1}),$$

  for $i = 2, 3, \ldots, n-2$.
- But for $i = n-1$, we have $u\,\partial u/\partial X_{n-1} = \partial F_{n-1}/\partial X_{n-1}$.
- After substitution of the latter equality in $u\,\partial u/\partial X_{n-1} = -X_{n-1}$, there exists a constant C such that we have:

$$\frac{-X_{n-1}^2}{2} = F_{n-1}(X_{n-1}) + C.$$

The key PDE argument: proof (6/6)

- Therefore. we have

$$\frac{u^2(X_1,\ldots,X_{n-1})}{2} = -\frac{X_1^2}{2} - \cdots - \frac{X_{n-1}^2}{2} + C.$$

- Let $\alpha = (\alpha_1,\ldots,\alpha_{n-1},\alpha_n)$ be a point of W.
- Since $u(\alpha_1,\ldots,\alpha_{n-1}) = \alpha_n$ holds, we have $C = 1/2(\alpha_1^2 + \cdots + \alpha_n^2)$. We deduce:

$$u(X_1,\ldots,X_{n-1}) = \sqrt{r^2 - X_1^2 - \cdots - X_{n-1}^2},$$

  where we define $r^2 := \alpha_1^2 + \cdots + \alpha_n^2$.
- Finally, we conclude that W is a neighbourhood of $p \in D_\rho^*$ contained in a sphere centred at the origin.

The main result in codimension 1 (recall)

Notation

- Assume $n \geq 3$.
- Let $S = [\mathcal{Q}, \{t_n\}, P_>]$ be a regular semi-algebraic system of $\mathbb{Q}[X_1, \ldots, X_n]$ such that $Z_{\mathbb{R}}(S)$ has dimension $d := n - 1$, and the closure $\overline{Z_{\mathbb{R}}(S)}$ contains the origin.
- W.l.o.g. we assume that $\mathrm{mvar}(t_n) = X_n$ holds.
- Let $\mathcal{M}$ be the $2 \times n$ matrix with the vector $(X_1, \ldots, X_n)$ as first row and the gradient vector $\nabla t_n = \left(\frac{\partial t_n}{\partial X_1} \ \cdots \ \frac{\partial t_n}{\partial X_n} \right)$ as second row.

Theorem

Then, there exists a non-empty set $\mathcal{O} \subset D_\rho^* \cap Z_{\mathbb{R}}(S)$, which is open relatively to $Z_{\mathbb{R}}(S)$, such that $\mathcal{M}$ is full rank at any point of $\mathcal{O}$, and the origin is in the closure of $\mathcal{O}$.

The main result in codimension 1: proof (1/2)

We shall first prove the following claim.

Claim

- Assume that there exists r such that $0 < r < \rho$ holds and $\mathcal{M}$ is not full rank at any point of $D_r^* \cap Z_{\mathbb{R}}(S)$.
- Then, there exists r' such that $0 < r' < r$ holds and $S_{r'}$, the r'-radius sphere centred at the origin, intercepts $Z_{\mathbb{R}}(S)$ on a semi-algebraic set of dimension $n - 1$.

Proof of the Claim

- Since the origin is in the closure of $Z_{\mathbb{R}}(S)$, we know that $D_r^* \cap Z_{\mathbb{R}}(S)$ is not empty.
- W.l.o.g. we can assume that $Z_{\mathbb{R}}(S) \subseteq D_r^*$ holds.
- Indeed, if this was not the case, we could decompose $D_r^* \cap Z_{\mathbb{R}}(S)$ into finitely many regular semi-algebraic systems and reason with each of those which has the origin of $\mathbb{R}^n$ in the topological closure (w.r.t. Euclidean topology) of its zero set.
- We apply the "key PDE argument" with $h := t_n$ and $V_0 := Z_{\mathbb{R}}(S)$. The conclusion of the claim follows.

The main result in codimension 1: proof (2/2)

Reduction step

- W.l.o.g. we can assume that $Z_{\mathbb{R}}(S)$ does not intercept a sphere centred at the origin on semi-algebraic sets W_i of dimension $n-1$ for $i = 1, 2, \ldots, m$ for some $m \geq 0$.
- Indeed, if this was the case, we could remove all such W_i from $Z_{\mathbb{R}}(S)$ (since such W_i doesn't have the origin of $\mathbb{R}^n$ in its topological closure) and keep reasoning with each component of $Z_{\mathbb{R}}(S) \setminus \cup_{i=1}^{m} W_i$ which contains the origin of $\mathbb{R}^n$ in its topological closure.

Using the claim

- As a consequence of the above claims, for every r such that $0 < r < \rho$ holds, there exists a point p of $D_r^* \cap Z_{\mathbb{R}}(S)$ at which $\mathcal{M}$ is full rank.
- Therefore, for all $r > 0$ small enough, the set $D_r^* \cap Z_{\mathbb{R}}(S)$ contains a point p_r, as well as a neighbourhood N_r of p_r (due to the full rank characterization in terms of minors) such that N_r is open relatively to $Z_{\mathbb{R}}(S)$ and $\mathcal{M}$ is full rank at any point of N_r.
- Taking the union of those neighbourhoods N_r finally yields the conclusion of the lemma.

The main result (recall

Notation

- Assume that $n \geq 3$ holds.
- Let $S = [\mathcal{Q}, T, P_>]$ be a regular semi-algebraic system of $\mathbb{Q}[X_1, \ldots, X_n]$ such that $Z_{\mathbb{R}}(S)$ has dimension d, with $n > d \geq 2$, and the closure $\overline{Z_{\mathbb{R}}(S)}$ contains the origin.
- W.l.o.g. we can assume that the polynomials $t_{d+1}, \ldots, t_n$ forming the regular chain T have main variables $X_{d+1}, \ldots, X_n$.
- Let $\mathcal{M}$ be the $(n-d+1) \times n$ matrix whose first row is the vector $(X_1, \ldots, X_n)$ and, for $j = d+1, \ldots, n$, whose $(j-d+1)$-th row is the gradient vector

$$\nabla t_j = \left(\frac{\partial t_j}{\partial X_1} \ \cdots \ \frac{\partial t_j}{\partial X_n} \right)$$

  where t_j is the polynomial of T with $\mathrm{mvar}(t_j) = X_j$.

Theorem

Then, there exists a non-empty set $\mathcal{O} \subset D_\rho^* \cap Z_{\mathbb{R}}(S)$, which is open relatively to $Z_{\mathbb{R}}(S)$ and which satisfies $\emptyset \in \overline{\mathcal{O}}$ (that is, the origin is in the closure of $\mathcal{O}$) such that $\mathcal{M}$ is full rank at any point of $\mathcal{O}$.

The main result - Proof (1/8)

Proof

The proof consists again of two main steps: a PDE argument and a topological argument.

Let $\mathcal{O}$ an open set in $Z_{\mathbb{R}}(S)$ with $\emptyset \in \overline{\mathcal{O}}$. With proper choice of open sets V_i for $i = n-d+1, \ldots, n$, there exist smooth analytic functions

$$\begin{cases} u_{n-d+1}(X_1, \ldots, X_{n-d+1}) : V_{n-d+1} \to \mathbb{R}, \\ \vdots \\ u_n(X_1, \ldots, X_{n-1}) : V_n \to \mathbb{R} \end{cases}$$

such that

$$\begin{cases} t_n(X_1, \ldots, X_{n-d}, u_{n-d+1}, \ldots, u_n) = 0 \\ \vdots \\ t_{n-d+1}(X_1, \ldots, X_{n-d}, u_{n-d+1}) = 0. \end{cases}$$

The main result - Proof (2/8)

For $i = 1, \cdots, n-d$, define:

$$m_i = det \begin{bmatrix} X_i & X_{n-d+1} & X_{n-d+2} & \dots & X_n \\ (u_n)_{X_i} & (u_n)_{X_{n-d+1}} & (u_n)_{X_{n-d+2}} & \dots & -1 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ (u_{n-d+1})_{X_i} & -1 & 0 & \dots & 0 \end{bmatrix}$$

$$m_{i1} = det \begin{bmatrix} X_{n-d+1} & X_{n-d+2} & X_{n-d+3} & \dots & X_n \\ (u_n)_{X_{n-d+1}} & (u_n)_{X_{n-d+2}} & (u_n)_{X_{n-d+3}} & \dots & -1 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ (u_{n-d+1})_{X_{n-d+1}} & -1 & 0 & \dots & 0 \end{bmatrix}$$

$$m_{i2} = det \begin{bmatrix} X_i & X_{n-d+2} & X_{n-d+3} & \dots & X_n \\ (u_n)_{X_i} & (u_n)_{X_{n-d+2}} & (u_n)_{X_{n-d+3}} & \dots & -1 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ (u_{n-d+1})_{X_i} & -1 & 0 & \dots & 0 \end{bmatrix}$$

The main result - Proof (3/8)

Assume the matrix M is not full rank at any point of $\mathcal{O}$. This implies we have the following system of partial differential equations:

$$\begin{cases} m_{11}\frac{\partial}{\partial X_1}u_{n-d+1} + m_{12} = 0 \\ m_{21}\frac{\partial}{\partial X_2}u_{n-d+1} + m_{22} = 0 \\ \qquad\vdots \\ m_{(n-d)1}\frac{\partial}{\partial X_{n-d}}u_{n-d+1} + m_{(n-d)2} = 0 \end{cases} \tag{9}$$

Claim:

$X_n u_n + X_{n-1}u_{n-1} + \ldots + X_{n-d+1}u_{n-d+1} + \frac{X_{n-d}^2}{2} + \frac{X_{n-d-1}^2}{2} + \ldots + \frac{X_1^2}{2} + c = 0$ is implied by System 9.

The main result - Proof (4/8)

Proof of the claim: We can expand the i-th differential equation, for $i = 1, \ldots, n-d$, in System 9 as:

$$\left(m_{i11}\frac{\partial u_{n-d+2}}{\partial X_{n-d+1}} + m_{i12}\right)\frac{\partial u_{n-d+1}}{\partial X_i} + m_{i21}\frac{\partial u_{n-d+2}}{\partial X_i} + m_{i22} = 0 \tag{10}$$

where

$$m_{i11} = det\begin{bmatrix} X_{n-d+2} & X_{n-d+3} & X_{n-d+4} & \ldots & X_n \\ (u_n)_{X_{n-d+2}} & (u_n)_{X_{n-d+3}} & (u_n)_{X_{n-d+4}} & \ldots & -1 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ (u_{n-d+3})_{X_{n-d+2}} & -1 & 0 & \ldots & 0 \end{bmatrix}$$

$$m_{i12} = det\begin{bmatrix} X_{n-d+1} & X_{n-d+3} & X_{n-d+4} & \ldots & X_n \\ (u_n)_{X_{n-d+1}} & (u_n)_{X_{n-d+3}} & (u_n)_{X_{n-d+4}} & \ldots & -1 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ (u_{n-d+3})_{X_{n-d+1}} & -1 & 0 & \ldots & 0 \end{bmatrix}$$

The main result - Proof (5/8)

$$m_{i21} = det \begin{bmatrix} X_{n-d+2} & X_{n-d+3} & X_{n-d+4} & \dots & X_n \\ (u_n)_{X_{n-d+2}} & (u_n)_{X_{n-d+3}} & (u_n)_{X_{n-d+4}} & \dots & -1 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ (u_{n-d+3})_{X_{n-d+2}} & -1 & 0 & \dots & 0 \end{bmatrix}$$

$$m_{i22} = det \begin{bmatrix} X_i & X_{n-d+3} & X_{n-d+4} & \dots & X_n \\ (u_n)_{X_i} & (u_n)_{X_{n-d+3}} & (u_n)_{X_{n-d+4}} & \dots & -1 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ (u_{n-d+3})_{X_i} & -1 & 0 & \dots & 0 \end{bmatrix}.$$

Observe $m_{i11} = m_{i21}$. So we can rewrite Equation 10 as

$$m_{i11}\frac{\partial u_{n-d+2}}{\partial X_{n-d+1}}\frac{\partial u_{n-d+1}}{\partial X_i} + m_{i12}\frac{\partial u_{n-d+1}}{\partial X_i} + m_{i11}\frac{\partial u_{n-d+2}}{\partial X_i} + m_{i22} = 0 \quad (11)$$

The main result - Proof (6/8)

Continuing the same approach on Equation 11, one can observe that the coefficient of X_k, for $k = n-d+1, \ldots, n$, is U_{ik} a function of partial derivatives of u_j, for $j = n-d+1, \ldots, n$, such that an anti-derivative of U_{ik} with respect to X_i is the function u_k.

Therefore, Equation 11 can be rewritten as

$$X_n U_{in} + X_{n-1} U_{i(n-1)} + \ldots + X_{n-d+1} U_{i(n-d+1)} + X_i = 0. \tag{12}$$

The main result - Proof (7/8)

For $i = 1$, there exists a differentiable function $F_1(X_2, \ldots, X_{n-d})$ such that we have:

$$X_n u_n + X_{n-1} u_{n-1} + \ldots + X_{n-d+1} u_{n-d+1} + \frac{X_1^2}{2} + F_1(X_2, \ldots, X_{n-d}) = 0.$$

Take derivative w.r.t. X_2 and substitute into Equation 12 for $i = 2$, we have $F_1(X_2, \ldots, X_{n-d}) = X_2$. Then there exists a differentiable function $F_2(X_3, \ldots, X_{n-d})$ such that $F_1 = \frac{X_2^2}{2} + F_2$. Therefore

$$X_n u_n + X_{n-1} u_{n-1} + \ldots + X_{n-d+1} u_{n-d+1} + \frac{X_1^2}{2} + \frac{X_2^2}{2} + F_2(X_3, \ldots, X_{n-d}) = 0.$$

The claim is proved by continuing the same approach. So $\exists c$ constant s.t.

$$X_n u_n + X_{n-1} u_{n-1} + \ldots + X_{n-d+1} u_{n-d+1} + \frac{X_1^2}{2} + \frac{X_2^2}{2} + \ldots + \frac{X_{n-d}^2}{2} + c = 0. \tag{13}$$

The main result - Proof (8/8)

The previous PDE argument helps us to prove the following claim: Assume that there exists r such that $0 < r < \rho$ holds and $\mathcal{M}$ is not full rank at any point of $D_r^* \cap Z_{\mathbb{R}}(S)$. Then, there exists r' such that $0 < r' < r$ holds and $E_{r'}$, the ellipsoid as in Equation 13 for $c = -r'^2$ (centred at the origin), intercepts $Z_{\mathbb{R}}(S)$ on a semi-algebraic set of dimension d.

Then, the *reduction step* and the *use-of-the-claim step* are similar to codimension 1.

Plan

Plan

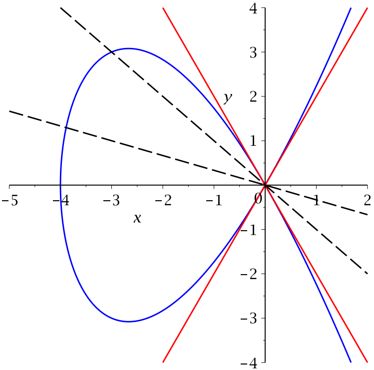
Previous Works

1. An algorithm to compute the equations of tangent cones (Mora 1982):
   - Based on Groebner basis (in fact Standard basis) computations

Our Contribution

1. A Standard Basis Free Algorithm for Computing the Tangent Cones of a Space Curve (P. Alvandi, M. Moreno Maza, É. Schost, P. Vrbik CASC 2015)
   - Based on computation of limit of secant lines

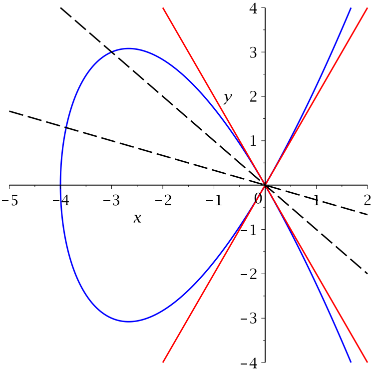
Tangent cones of space curves



Answer

The command `LimitPoints` for computing limit points corresponding to regular chains can be used to compute the limit of secant lines, as well.

Tangent cones of space curves



Answer

The command `LimitPoints` for computing limit points corresponding to regular chains can be used to compute the limit of secant lines, as well.

Tangent cones of space curves: example

- $\mathcal{C} = W(R)$ a curve with $R := \{2x_3^2 + x_1 - 1, 2x_2^2 + 2x_1^2 - x_1 - 1\}$
- Let $p = (x_1, x_2, x_3)$ be a singular point on C, e.g. $(1, 0, 0)$.

Compute the tangent cone of $\mathcal{C}$ at p

1. Let $q = (y_1, y_2, y_3)$ be a point on a secant line through p
2. When q is close enough to p, one of $x_1 - y_1$, $x_2 - y_2$ or $x_3 - y_3$ does not vanish, say $x_1 - y_1$
3. Hence, when q is close enough to p, $\vec{v} = (s_1, s_2, s_3)$ leads (pq) with
$$s_1 := 1, s_2 := \frac{x_2 - y_2}{x_1 - y_1}, s_3 := \frac{x_3 - y_3}{x_1 - y_1}$$
4. Viewing s_2, s_3 as new variables, consider $T := R \cup R'$ with
$$R' = \{(x_i - y_1)s_2 - (x_2 - y_2), (x_i - y_1)s_3 - (x_3 - y_3)\}$$
5. T is a regular chain for $s_2 > s_3 > x_3 > x_2 > x_1$
6. Computing the limit points of $W(T)$ around $x_1 - y_1 = 0$ yields the limits of the slopes s_2 and s_3, and thus the tangent cone.

Tangent cones of space curves: example

```
> R := PolynomialRing([x_3, x_2, x_1]) :
  Curve := [x_3^2 + x_2^2 + x_1^2 - 1, x_3^2 - x_2^2 - x_1*(x_1 - 1)] :
  rc := Chain([x_1 - 1, x_2, x_3], Empty(R), R) :
  tc := TangentCone(rc, Curve, R, equations); Display(tc[1][2], R);
```

$$tc := \{[[\_x\_1 - 1, -\_x\_2^2 + 3\ \_x\_3^2], regular\_chain]\}$$

$$\begin{cases} x\_3 = 0 \\ x\_2 = 0 \\ x\_1 - 1 = 0 \end{cases}$$

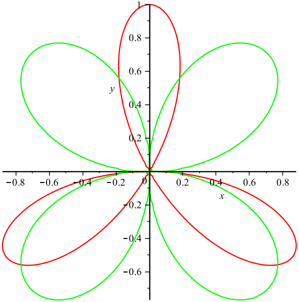
```
> tc := TangentCone(rc, Curve, R, slopes);
```

$$tc := \{[[\%x\_1, \%x\_2 - 1, 3\ \%x\_3^2 - 1], regular\_chain], [[\%x\_1, \%x\_2^2 - 3, \%x\_3 - 1], regular\_chain]\}$$

Plan

$> F := \left[(x^2+y^2)^2+3x^2y-y^3, (x^2+y^2)^3-4x^2y^2\right] :$

$> \text{plots[implicitplot]}(Fs, x=-2..2, y=-2..2) :$



$> R := \text{PolynomialRing}([x, y], 101) :$

$> \text{TriangularizeWithMultiplicity}(F, R);$

$$\left[\left[1, \left\{\begin{array}{c} x-1=0 \\ y+14=0 \end{array}\right.\right]\right], \left[\left[1, \left\{\begin{array}{c} x+1=0 \\ y+14=0 \end{array}\right.\right]\right], \left[\left[1, \left\{\begin{array}{c} x-47=0 \\ y-14=0 \end{array}\right.\right]\right], \left[\left[1, \left\{\begin{array}{c} x+47=0 \\ y-14=0 \end{array}\right.\right]\right], \left[\left[14, \left\{\begin{array}{c} x=0 \\ y=0 \end{array}\right.\right]\right] \tag{14}$$

The command RegularChains:-TriangularizeWithMultiplicity computes the

`TriangularizeWithMultiplicity`

We specify `TriangularizeWithMultiplicity`:

Input $f_1, \ldots, f_n \in \mathbb{C}[x_1, \ldots, x_n]$ such that $V(f_1, \ldots, f_n)$ is zero-dimensional.

Output Finitely many pairs $[(T_1, m_1), \ldots, (T_\ell, m_\ell)]$ where $T_1, \ldots, T_\ell$ are regular chains of $\mathbb{C}[x_1, \ldots, x_n]$ such that for all $p \in V(T_i)$

$$\mathcal{I}(p; f_1, \ldots, f_n) = m_i \text{ and } V(f_1, \ldots, f_n) = V(T_1) \uplus \cdots \uplus V(T_\ell)$$

`TriangularizeWithMultiplicity` works as follows

1. Apply `Triangularize` on $f_1, \ldots, f_n$,
2. Apply $\mathsf{IM}_n(T; f_1, \ldots, f_n)$ on each regular chain T.

$\mathsf{IM}_n(T; f_1, \ldots, f_n)$ works as follows

1. if $n = 2$ apply Fulton's algorithm extended for working at a regular chains instead of a point (S. Marcus, M., P. Vrbik; CASC 2013),
2. if $n > 2$ attempt a reduction from dimension n to $n - 1$ (P. Alvandi, M., É. Schost, P. Vrbik; CASC 2015),

Fulton's Properties

The intersection multiplicity of two plane curves at a point *satisfies and is uniquely determined by* the following.

(2-1) $I(p; f, g)$ is a non-negative integer for any C, D, and p such that C and D have no common component at p. We set $I(p; f, g) = \infty$ if C and D have a common component at p.

(2-2) $I(p; f, g) = 0$ if and only if $p \notin C \cap D$.

(2-3) $I(p; f, g)$ is invariant under affine change of coordinates on $\mathring{A}^2$.

(2-4) $I(p; f, g) = I(p; g, f)$

(2-5) $I(p; f, g)$ is greater or equal to the product of the multiplicity of p in f and g, with equality occurring if and only if C and D have no tangent lines in common at p.

(2-6) $I(p; f, gh) = I(p; f, g) + I(p; f, h)$ for all $h \in k[x, y]$.

(2-7) $I(p; f, g) = I(p; f, g + hf)$ for all $h \in k[x, y]$.

Fulton's Algorithm

Algorithm 1: $\mathsf{IM}_2(p; f, g)$

Input: $p = (\alpha, \beta) \in \mathring{\mathbb{A}}^2(\mathbb{C})$ and $f, g \in \mathbb{C}[y \succ x]$ such that $\gcd(f, g) \in \mathbb{C}$

Output: $I(p; f, g) \in \mathbb{N}$ satisfying (2-1)–(2-7)

if $f(p) \neq 0$ *or* $g(p) \neq 0$ **then**

  return 0;

$r, s = \deg\left(f(x, \beta)\right), \deg\left(g(x, \beta)\right)$; assume $s \geq r$.

if $r = 0$ **then**

  write $f = (y - \beta) \cdot h$ and $g(x, \beta) = (x - \alpha)^m \left(a_0 + a_1(x - \alpha) + \cdots\right)$;

  return $m + \mathsf{IM}_2(p; h, g)$;

  $\mathsf{IM}_2(p; (y - \beta) \cdot h, g) = \mathsf{IM}_2(p; (y - \beta), g) + \mathsf{IM}_2(p; h, g)$

  $\mathsf{IM}_2(p; (y - \beta), g) = \mathsf{IM}_2(p; (y - \beta), g(x, \beta)) = \mathsf{IM}_2(p; (y - \beta), (x - \alpha)^m) = m$

if $r > 0$ **then**

  $h \leftarrow \mathsf{monic}\,(g) - (x - \alpha)^{s-r}\mathsf{monic}\,(f)$;

  return $\mathsf{IM}_2(p; f, h)$;

Reducing from dim n to dim $n-1$: using transversality

The theorem again:

Theorem

Assume that $h_n = V(f_n)$ is non-singular at p. Let v_n be its tangent hyperplane at p. Assume that h_n meets each component (through p) of the curve $\mathcal{C} = V(f_1, \ldots, f_{n-1})$ transversely (that is, the tangent cone $TC_p(\mathcal{C})$ intersects v_n only at the point p). Let $h \in k[x_1, \ldots, x_n]$ be the degree 1 polynomial defining v_n. Then, we have

$$I(p; f_1, \ldots, f_n) = I(p; f_1, \ldots, f_{n-1}, h).$$

How to use this theorem in practise?

Assume that the coefficient of x_n in h is non-zero, thus $h = x_n - h'$, where $h' \in k[x_1, \ldots, x_{n-1}]$. Hence, we can rewrite the ideal $\langle f_1, \ldots, f_{n-1}, h \rangle$ as $\langle g_1, \ldots, g_{n-1}, h \rangle$ where g_i is obtained from f_i by substituting x_n with h'. Then, we have

$$I(p; f_1, \ldots, f_n) = I(p|_{x_1,\ldots,x_{n-1}}; g_1, \ldots, g_{n-1}).$$

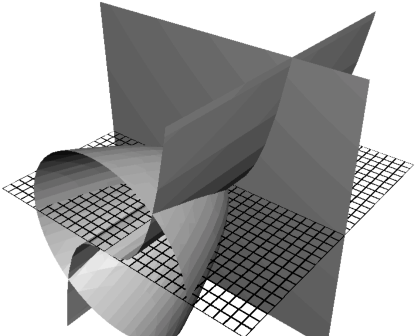
Reducing from dim n to dim $n-1$: a simple case (1/3)

Example

Consider the system

$$f_1 = x, \quad f_2 = x + y^2 - z^2, \quad f_3 := y - z^3$$

near the origin $o := (0,0,0) \in V(f_1, f_2, f_3)$



Reducing from dim n to dim $n-1$: a simple case (2/3)

Example

Recall the system

$$f_1 = x, \quad f_2 = x + y^2 - z^2, \quad f_3 := y - z^3$$

near the origin $o := (0,0,0) \in V(f_1, f_2, f_3)$.

Computing the IM using the definition

Let us compute a basis for $\mathcal{O}_{\mathring{A}^3,o}/ <f_1, f_2, f_3>$ as a vector space over $\overline{k}$.

Setting $x = 0$ and $y = z^3$, we must have $z^2(z^4+1) = 0$ in $\mathcal{O}_{\mathring{A}^3,o} = \overline{k}[x,y,z]_{(z,y,z)}$.

Since $z^4 + 1$ is a unit in this local ring, we see that

$$\mathcal{O}_{\mathring{A}^3,o}/ <f_1, f_2, f_3> = <1, z>$$

as a vector space, so $I(o; f_1, f_2, f_3) = 2$.

Reducing from dim n to dim $n-1$: a simple case (3/3)

Example

Recall the system again

$$f_1 = x, \quad f_2 = x + y^2 - z^2, \quad f_3 := y - z^3$$

near the origin $o := (0,0,0) \in V(f_1, f_2, f_3)$.

Computing the IM using the reduction

We have

$$\mathcal{C} := V(x, x + y^2 - z^2) = V(x, (y-z)(y+z)) = TC_o(\mathcal{C})$$

and we have

$$h = y.$$

Thus $\mathcal{C}$ and $V(f_3)$ intersect transversally at the origin. Therefore, we have

$$I_3(p; f_1, f_2, f_3) = I_2((0,0); x, x - z^2) = 2.$$