Validity proof of Lazard's method for C.A.D. construction

joint work with Scott McCallum (Macquarie University,, Sydney) and Laurentiu Paunescu (Sydney Uni)

Adam Parusiński

Université Nice Sophia Antipolis

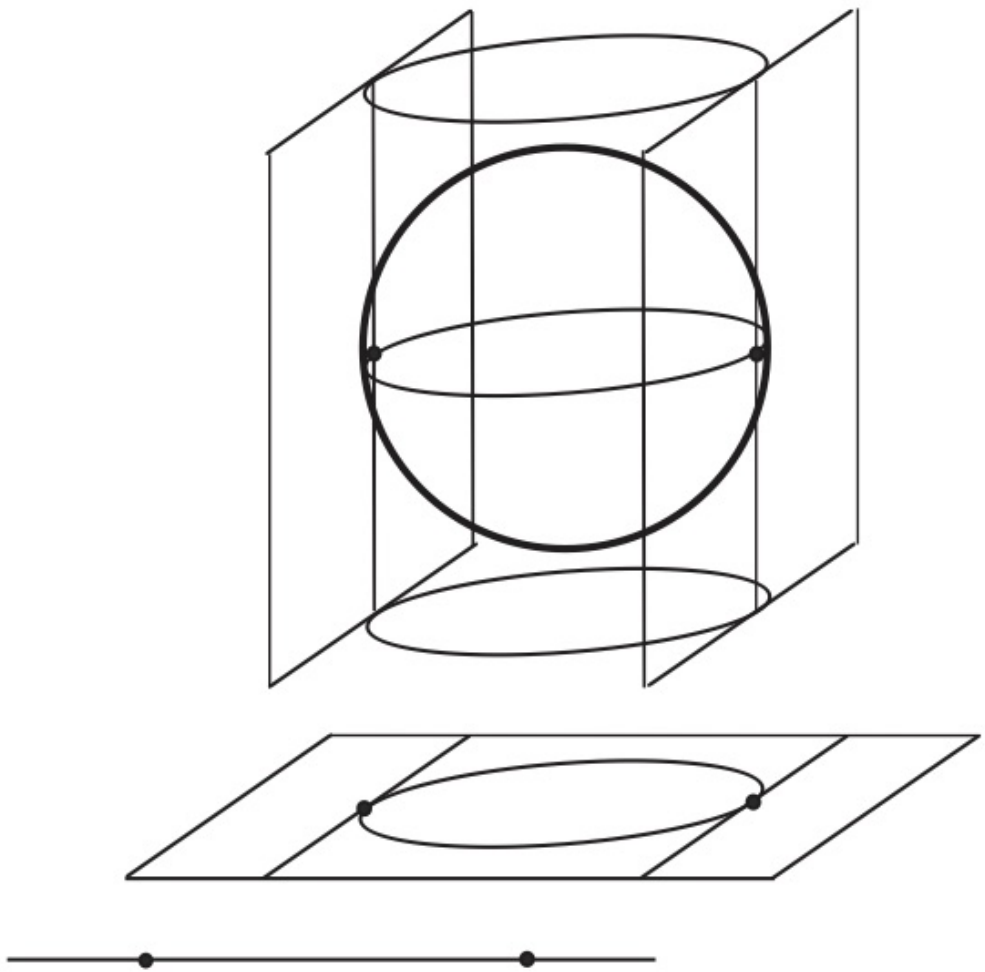


Figure 2.1: A c.a.d. adapted to the sphere

Cylindrical Algebraic Decomposition (C.A.D.)

C.A.D. was introduced by G. E. Collins (1975).

Cylindrical Algebraic Decomposition (C.A.D.)

C.A.D. was introduced by G. E. Collins (1975).

A **cylindrical algebraic decomposition** of $\mathbb{R}^n$ is a sequence $\mathcal{C}_1, ..., \mathcal{C}_n$, where each $\mathcal{C}_k$ is a finite partition of $\mathbb{R}^k$ into semialgebraic subsets (cells) s.t.

Cylindrical Algebraic Decomposition (C.A.D.)

C.A.D. was introduced by G. E. Collins (1975).

A **cylindrical algebraic decomposition** of $\mathbb{R}^n$ is a sequence $\mathcal{C}_1, ..., \mathcal{C}_n$, where each $\mathcal{C}_k$ is a finite partition of $\mathbb{R}^k$ into semialgebraic subsets (cells) s.t.

- each cell is homeomorphic to $(0,1)^s$;
- for every $k < n$ and for every $C \in \mathcal{C}_k$, there are continuous functions

$$\xi_1 < \cdots < \xi_{l_C} : C \to \mathbb{R}$$

dividing the cylinder $C \times \mathbb{R}$ in **sections** and **sectors** that belong to $\mathcal{C}_{k+1}$.

Input: A finite list of polynomials in $\mathcal{A} \subset \mathbb{Z}[X_1, ..., X_n]$.

Output: A C.A.D.: $\mathcal{C}_1, \ldots, \mathcal{C}_n$
s. t. $\forall C \in \mathcal{C}_n$, $\mathcal{A}$ **is** C **invariant** ($\forall P \in \mathcal{A}$, P has constant sign on C)

Input: A finite list of polynomials in $\mathcal{A} \subset \mathbb{Z}[X_1, ..., X_n]$.

Output: A C.A.D.: $\mathcal{C}_1, \ldots, \mathcal{C}_n$
s. t. $\forall C \in \mathcal{C}_n$, $\mathcal{A}$ **is** C **invariant** ($\forall P \in \mathcal{A}$, P has constant sign on C)

Phase I. Projection: $\mathcal{A} \to Proj(\mathcal{A})$
where $Proj(\mathcal{A}) \subset \mathbb{Z}[X_1, ..., X_{n-1}]$ is finite, and an associated C.A.D., $\mathcal{C}_1, ..., \mathcal{C}_{n-1}$ s.t.
for every $C \in \mathcal{C}_{n-1}$ every $P \in \mathcal{A}$ either vanishes identically on C or is **delineable** over C, with any two sections either identical or disjoint.

Input: A finite list of polynomials in $\mathcal{A} \subset \mathbb{Z}[X_1, ..., X_n]$.

Output: A C.A.D.: $\mathcal{C}_1, \ldots, \mathcal{C}_n$
s. t. $\forall C \in \mathcal{C}_n$, $\mathcal{A}$ **is** C **invariant** ($\forall P \in \mathcal{A}$, P has constant sign on C)

Phase I. Projection: $\mathcal{A} \to Proj(\mathcal{A})$
where $Proj(\mathcal{A}) \subset \mathbb{Z}[X_1, ..., X_{n-1}]$ is finite, and an associated C.A.D., $\mathcal{C}_1, ..., \mathcal{C}_{n-1}$ s.t.
for every $C \in \mathcal{C}_{n-1}$ every $P \in \mathcal{A}$ either vanishes identically on C or is **delineable** over C, with any two sections either identical or disjoint.

Definition

$P \in \mathbb{R}[X_1, ..., X_n]$ is **delineable over** $S \subset \mathbb{R}^{n-1}$ if there are continuous functions

$$\xi_1 < \cdots < \xi_{l_S} : S \to \mathbb{R},$$

precisely the real roots of $P(p', X_n)$ for $p' \in S$,
s.t. the **multiplicities** of these roots are constant for $p' \in S$.

Input: A finite list of polynomials in $\mathcal{A} \subset \mathbb{Z}[X_1, ..., X_n]$.

Output: A CAD: $\mathcal{C}_1, \ldots, \mathcal{C}_n$
s. t. $\forall C \in \mathcal{C}_n$, $\mathcal{A}$ **is** C **invariant** ($\forall P \in \mathcal{A}$, P has constant sign on C)

Phase I. Projection: $\mathcal{A} \to Proj(\mathcal{A})$
where $Proj(\mathcal{A}) \subset \mathbb{Z}[X_1, ..., X_{n-1}]$ is finite, and an associated C.A.D., $\mathcal{C}_1, ..., \mathcal{C}_{n-1}$

Input: A finite list of polynomials in $\mathcal{A} \subset \mathbb{Z}[X_1, ..., X_n]$.

Output: A CAD: $\mathcal{C}_1, \ldots, \mathcal{C}_n$
s. t. $\forall C \in \mathcal{C}_n$, $\mathcal{A}$ **is** C **invariant** ($\forall P \in \mathcal{A}$, P has constant sign on C)

Phase I. Projection: $\mathcal{A} \to Proj(\mathcal{A})$
where $Proj(\mathcal{A}) \subset \mathbb{Z}[X_1, ..., X_{n-1}]$ is finite, and an associated C.A.D., $\mathcal{C}_1, ..., \mathcal{C}_{n-1}$

Phase II. Lifting: Construction of $\mathcal{C}_n$
$\mathcal{C}_n$ is given by section and sectors of $\mathcal{A}$ over the cells of $\mathcal{C}_{n-1}$.

The CAD algorithm can be used to

- decide whether or not a given semialgebraic set is empty, finite, open, closed, connected, or bounded;
- decide whether or not a given semialgebraic set is contained in another one;
- determine a sample point of a given nonempty semialgebraic set;
- determine the connected components of a given semialgebraic set;
- determine the projection of a given semialgebraic set in $\mathbb{R}^n$ to a coordinate subspace $\mathbb{R}^k$;
- etc.

The CAD algorithm has been used in practice in several areas including

- control system design (Dorato et al., 1997; Jirstrand, 1997),
- stability analysis (Hong et al., 1997),
- multidimensional integration and graphical representation of semialgebraic sets (Strzeboński, 2000a),
- global optimization and assumption propagation in a computer algebra system (Strzeboński, 2000b).

The CAD algorithm has been used in practice in several areas including

- control system design (Dorato et al., 1997; Jirstrand, 1997),
- stability analysis (Hong et al., 1997),
- multidimensional integration and graphical representation of semialgebraic sets (Strzeboński, 2000a),
- global optimization and assumption propagation in a computer algebra system (Strzeboński, 2000b).

Remark: There have been several improvements made reducing the size of the original Collins projection : McCallum (1988, 1998), with an improvement by Brown (2001), Hong (1990), Collins (1998).

McCallum-Brown projection.

Given $\mathcal{A} \subset \mathbb{Z}[X_1, ..., X_n]$ finite.

$$Proj_M(\mathcal{A}) = cont(\mathcal{A}) \cup P_M(\mathcal{B})$$

McCallum-Brown projection.

Given $\mathcal{A} \subset \mathbb{Z}[X_1, ..., X_n]$ finite.

$$Proj_M(\mathcal{A}) = cont(\mathcal{A}) \cup P_M(\mathcal{B})$$

$cont(\mathcal{A}) =$ the set of non-zero non-unit contents of the elements of $\mathcal{A}$.

McCallum-Brown projection.

Given $\mathcal{A} \subset \mathbb{Z}[X_1, ..., X_n]$ finite.

$$Proj_M(\mathcal{A}) = cont(\mathcal{A}) \cup P_M(\mathcal{B})$$

$cont(\mathcal{A}) =$ the set of non-zero non-unit contents of the elements of $\mathcal{A}$.
$\mathcal{B} =$ irreducible factors of $prim(\mathcal{A})$.
$P_M(\mathcal{B}) =$ union of
all **leading** coefficients of the elements of $\mathcal{B}$, and
all **discriminants** of elements of $\mathcal{B}$ and
all **resultants** of pairs of distinct elements of $\mathcal{B}$.

McCallum-Brown projection.

Given $\mathcal{A} \subset \mathbb{Z}[X_1, ..., X_n]$ finite.

$$Proj_M(\mathcal{A}) = cont(\mathcal{A}) \cup P_M(\mathcal{B})$$

$cont(\mathcal{A}) =$ the set of non-zero non-unit contents of the elements of $\mathcal{A}$.
$\mathcal{B} =$ irreducible factors of $prim(\mathcal{A})$.
$P_M(\mathcal{B}) =$ union of
all **leading** coefficients of the elements of $\mathcal{B}$, and
all **discriminants** of elements of $\mathcal{B}$ and
all **resultants** of pairs of distinct elements of $\mathcal{B}$.

Important restriction
McCallum-Brown algorithm works well for the **well-oriented systems**

McCallum-Brown projection.

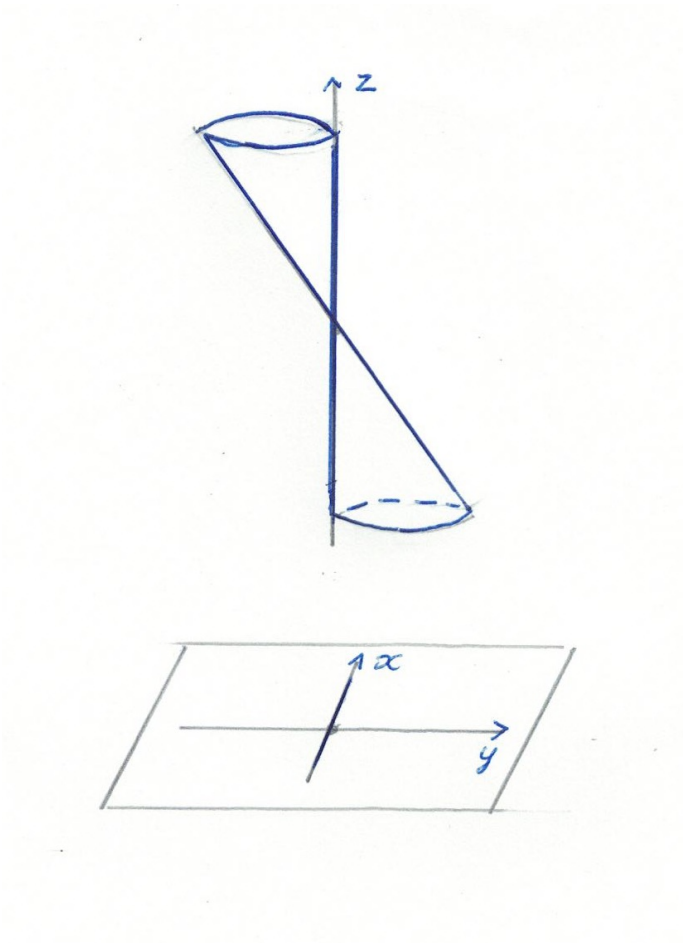
Given $\mathcal{A} \subset \mathbb{Z}[X_1, ..., X_n]$ finite.

$$Proj_M(\mathcal{A}) = cont(\mathcal{A}) \cup P_M(\mathcal{B})$$

$cont(\mathcal{A}) =$ the set of non-zero non-unit contents of the elements of $\mathcal{A}$.
$\mathcal{B} =$ irreducible factors of $prim(\mathcal{A})$.
$P_M(\mathcal{B}) =$ union of
all **leading** coefficients of the elements of $\mathcal{B}$, and
all **discriminants** of elements of $\mathcal{B}$ and
all **resultants** of pairs of distinct elements of $\mathcal{B}$.

Important restriction
McCallum-Brown algorithm works well for the **well-oriented systems**
i.e. if no element of $\mathcal{B}$ vanishes identically on any cell of positive dimension, and the same condition holds recursively for the subsequent projections.

C.A.D. adapted to $P(x, y, z) = (z + y)^2 + x^2 - z^2 = 2zy + x^2 + y^2$



On $f = 0$ we have $z = -\frac{x^2+y^2}{2y}$.

Lazard projection.

$$Proj_L(\mathcal{A}) = cont(\mathcal{A}) \cup P_L(\mathcal{B}),$$

$P_L(\mathcal{B}) =$
all **leading** coefficients of $\mathcal{B}$, and
all non-zero **trailing** coefficients of the elements of $\mathcal{B}$, and
all **discriminants** of elements of $\mathcal{B}$, and
all **resultants** of pairs of distinct elements of $\mathcal{B}$.

Lazard projection.

$$Proj_L(\mathcal{A}) = cont(\mathcal{A}) \cup P_L(\mathcal{B}),$$

$P_L(\mathcal{B}) =$
all **leading** coefficients of $\mathcal{B}$, and
all non-zero **trailing** coefficients of the elements of $\mathcal{B}$, and
all **discriminants** of elements of $\mathcal{B}$, and
all **resultants** of pairs of distinct elements of $\mathcal{B}$.

Important: Lazard's algorithm works without any assumption on the system of polynomials $\mathcal{A} \subset \mathbb{R}[X_1, ..., X_n]$.

Lazard valuation.

$$\mathbb{N}^n \ni \mathbf{v}_p(P) \leftarrow (p, P) \in \mathbb{R}^n \times \mathbb{R}[X_1, \ldots, X_n]$$

$\mathbf{v}_p(P) = (v_1, \ldots, v_n)$ is the smallest (w. r. t. $\leq_{lex}$) s.t. $\frac{\partial^{v_1+\cdots+v_n} P}{\partial x_1^{v_1} \cdots \partial x_n^{v_n}}(p) \neq 0$.

Examples.
1) $P(X_1, X_2) = X_1^2 X_2^3 + X_1^3 X_2^2$ Then $\mathbf{v}_{(0,0)}(P) = (2, 3)$,

Lazard valuation.

$$\mathbb{N}^n \ni \mathbf{v}_p(P) \leftarrow (p, P) \in \mathbb{R}^n \times \mathbb{R}[X_1, \ldots, X_n]$$

$\mathbf{v}_p(P) = (v_1, \ldots, v_n)$ is the smallest (w. r. t. $\leq_{lex}$) s.t. $\frac{\partial^{v_1+\cdots+v_n} P}{\partial x_1^{v_1} \cdots \partial x_n^{v_n}}(p) \neq 0$.

Examples.

1) $P(X_1, X_2) = X_1^2 X_2^3 + X_1^3 X_2^2$ Then $\mathbf{v}_{(0,0)}(P) = (2, 3)$,

2) If $P = X_n^d + a_1(X')X_n^{d-1} + \cdots a_d(X')$ and $p = (p', p_n)$ then

$$\mathbf{v}_p(P) = (0, ..., 0, m),$$

where m is the multiplicity p_n as a root of $P(p', X_n)$.

Lazard evaluation.

$$\mathbb{R}[X_n] \ni EP_{p'}(X_n) \leftarrow (p', P) \in \mathbb{R}^{n-1} \times \mathbb{R}[X_1, \ldots, X_n]$$

Lazard evaluation.

$$\mathbb{R}[X_n] \ni EP_{p'}(X_n) \leftarrow (p', P) \in \mathbb{R}^{n-1} \times \mathbb{R}[X_1, \ldots, X_n]$$

Lazard evaluation of P at p' equals, up to a non-zero scalar,

$$EP_{p'} = const \cdot \frac{\partial^{v_1+\cdots+v_{n-1}} P}{\partial x_1^{v_1} \cdots \partial x_{n-1}^{v_{n-1}}}.$$

Examples.
1) $P(X_1, X_2) = X_1^2 X_2^3 + X_1^3 X_2^2$. Then $EP_0 = X_2^3$,

Lazard evaluation.

$$\mathbb{R}[X_n] \ni EP_{p'}(X_n) \leftarrow (p', P) \in \mathbb{R}^{n-1} \times \mathbb{R}[X_1, \ldots, X_n]$$

Lazard evaluation of P at p' equals, up to a non-zero scalar,

$$EP_{p'} = const \cdot \frac{\partial^{v_1+\cdots+v_{n-1}} P}{\partial x_1^{v_1} \cdots \partial x_{n-1}^{v_{n-1}}}.$$

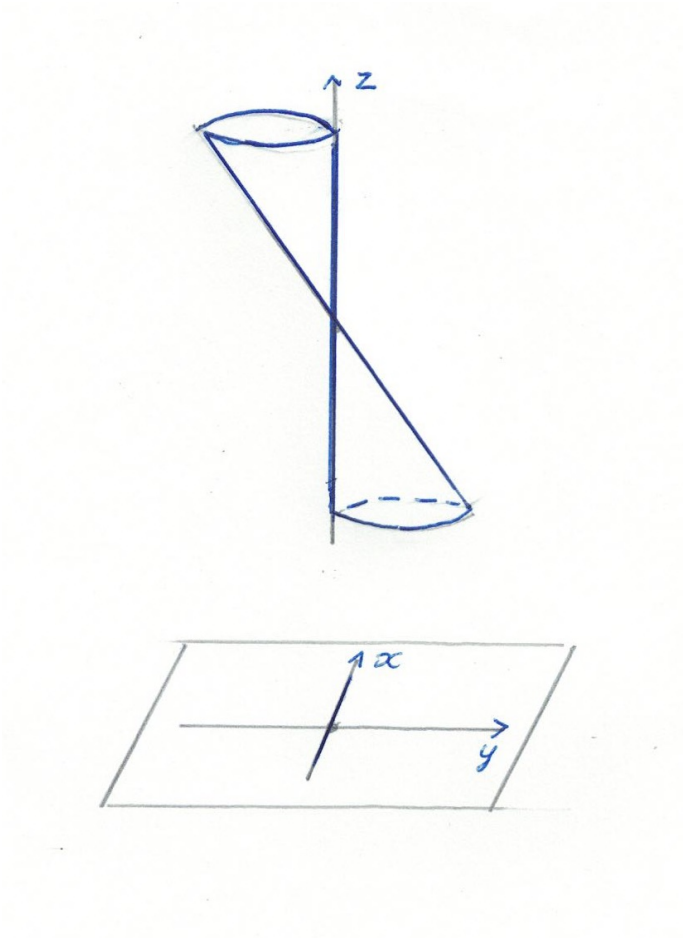
Examples.

1) $P(X_1, X_2) = X_1^2 X_2^3 + X_1^3 X_2^2$. Then $EP_0 = X_2^3$,

2) For $P = X_n^d + a_1(X')X_n^{d-1} + \cdots a_d(X')$

$$EP_{p'} = X_n^d + a_1(p')X_n^{d-1} + \cdots a_d(p')$$

C.A.D. adapted to $P(x, y, z) = 2zy + x^2 + y^2$



Lazard evaluation of P at the origin is $EP_0 = 2z$.

Lazard delineability.

Definition

Let $S \subset \mathbb{R}^{n-1}$ be semialgebraic and connected. A nonzero polynomial $P \in \mathbb{R}[X_1, ..., X_n]$ is **Lazard delineable over** S if

- the first $n-1$ components of $\mathbf{v}_p(P)$ are independent of $p \in S \times \mathbb{R}$.
- the real roots of $EP_{p'}$ for $p' \in S$ are continuous functions

$$\xi_1 < \cdots < \xi_{l_S} : S \to \mathbb{R},$$

- the multiplicities of these roots are independent of $p' \in S$.

Lazard delineability.

Definition

Let $S \subset \mathbb{R}^{n-1}$ be semialgebraic and connected. A nonzero polynomial $P \in \mathbb{R}[X_1, ..., X_n]$ is **Lazard delineable over** S if

- the first $n-1$ components of $\mathbf{v}_p(P)$ are independent of $p \in S \times \mathbb{R}$.
- the real roots of $EP_{p'}$ for $p' \in S$ are continuous functions

$$\xi_1 < \cdots < \xi_{l_S} : S \to \mathbb{R},$$

- the multiplicities of these roots are independent of $p' \in S$.

Easy: If P is Lazard-delineable on S then P is Lazard valuation-invariant in every Lazard section and sector over S.

The proof of Lazard (1994) of the validity of his algorithm was incomplete. Its validity follows from the following result.

Theorem (McCallum, –, Paunescu, arXiv:1607.00264)

Let $P \in \mathbb{R}[X_1, ..., X_n]$ have positive degree d in X_n.
Suppose that the discriminant Δ, the leading coefficients l and the trailing coefficient t of P are nonzero. Let $S \subset \mathbb{R}^{n-1}$ be a connected semialgebraic subset in which Δ, l and t are all Lazard valuation-invariant.

***Then** P **is Lazard delineable on** S and is Lazard valuation-invariant in every Lazard section and Lazard sector of P over S.*

Test curves for Lazard valuation.

For a polynomial g we transform the Lazard valuation $\mathbf{v}_p(g)$ into the order of g along a monomial curve of the form $\mathbb{R} \ni t \to p + (t^{c_1}, \ldots, t^{c_n})$:

Test curves for Lazard valuation.

For a polynomial g we transform the Lazard valuation $\mathbf{v}_p(g)$ into the order of g along a monomial curve of the form $\mathbb{R} \ni t \to p + (t^{c_1}, \ldots, t^{c_n})$:

Write $g(x) = \sum_{\mathbf{v} \in \mathbb{N}^n} a_{\mathbf{v}} (x - p)^{\mathbf{v}}$. Then

$$g(p + (t^{c_1}, \ldots, t^{c_n})) = a_{\mathbf{v}_p(g)} t^{\langle \mathbf{c}, \mathbf{v}_p(g) \rangle} + o(t^{\langle \mathbf{c}, \mathbf{v}_p(g) \rangle}),$$

where $c = (c_1, ..., c_n)$, provided $c_1 \gg c_2 \gg \cdots \gg c_n$.

Test curves for Lazard valuation.

For a polynomial g we transform the Lazard valuation $\mathbf{v}_p(g)$ into the order of g along a monomial curve of the form $\mathbb{R} \ni t \to p + (t^{c_1}, \ldots, t^{c_n})$:

Write $g(x) = \sum_{\mathbf{v} \in \mathbb{N}^n} a_{\mathbf{v}} (x - p)^{\mathbf{v}}$. Then

$$g(p + (t^{c_1}, \ldots, t^{c_n})) = a_{\mathbf{v}_p(g)} t^{\langle \mathbf{c}, \mathbf{v}_p(g) \rangle} + o(t^{\langle \mathbf{c}, \mathbf{v}_p(g) \rangle}),$$

where $c = (c_1, ..., c_n)$, provided $c_1 \gg c_2 \gg \cdots \gg c_n$.

Apply it to our construction

$$P(p' + (t^{c_1}, \ldots, t^{c_{n-1}}), X_n) = t^{\langle c', \mathbf{v}' \rangle} (EP_{p'}(X_n) + tR(t, X_n)),$$

where $(\mathbf{v}', v_n) = \mathbf{v}_p(P)$ for $p = (p', p_n)$, $c' = (c_1, ..., c_{n-1})$.

Theorem (Puiseux with parameter, Jung, Zariski)

Consider

$$F(x,t,Z) = Z^d + a_1(x,t)Z^{d-1} + \cdots + a_d(x,t),$$

where $x \in \mathbb{C}^k$, $t \in \mathbb{C}$, $a_j \in \mathbb{C}\{x,t\}$,

Theorem (Puiseux with parameter, Jung, Zariski)

Consider

$$F(x,t,Z) = Z^d + a_1(x,t)Z^{d-1} + \cdots + a_d(x,t),$$

where $x \in \mathbb{C}^k$, $t \in \mathbb{C}$, $a_j \in \mathbb{C}\{x,t\}$, *with the discriminant of* F *of the form*

$$\Delta_F(x,t) = t^M unit(x,t).$$

Then there are m *and* $\xi_j(x,s) \in \mathbb{C}\{x,s\}$ *s.t.*

$$F(x,s^m,Z) = \prod_{j=1}^{d}(Z - \xi_j(x,s)).$$

Theorem (Puiseux with parameter, Jung, Zariski)

Consider

$$F(x,t,Z) = Z^d + a_1(x,t)Z^{d-1} + \cdots + a_d(x,t),$$

where $x \in \mathbb{C}^k$, $t \in \mathbb{C}$, $a_j \in \mathbb{C}\{x,t\}$, *with the discriminant of* F *of the form*

$$\Delta_F(x,t) = t^M unit(x,t).$$

Then there are m *and* $\xi_j(x,s) \in \mathbb{C}\{x,s\}$ *s.t.*

$$F(x,s^m,Z) = \prod_{j=1}^{d}(Z - \xi_j(x,s)).$$

There is a version for $F(x,t,Z) = a_0(x,t)Z^d + a_1(x,t)Z^{d-1} + \cdots + a_d(x,t)$. Then we need that, moreover, a_0 and a_d are of the form: the power of t times a unit.

Final arguments.

1. Define

$$P_\psi(p', t, X_n) := P(\psi(p', t), X_n),$$

where $\psi : S \times \mathbb{R} \to \mathbb{R}^{n-1}$, $\psi(p', t) = p' + (s^{c_1}, \ldots, s^{c_{n-1}})$.

Final arguments.

1. Define
$$P_\psi(p', t, X_n) := P(\psi(p', t), X_n),$$
where $\psi : S \times \mathbb{R} \to \mathbb{R}^{n-1}$, $\psi(p', t) = p' + (s^{c_1}, \ldots, s^{c_{n-1}})$.

2. Use the assumptions (Δ, I and t are all Lazard valuation-invariant on S) and the property of the test curves to show that
$$t^{-\langle c', v' \rangle} P_\psi(p', t, X_n) = EP_{p'}(X_n) + tR(t, X_n)$$
satisfies the assumptions of Puiseux with parameter.

Final arguments.

1. Define
$$P_\psi(p', t, X_n) := P(\psi(p', t), X_n),$$
where $\psi : S \times \mathbb{R} \to \mathbb{R}^{n-1}$, $\psi(p', t) = p' + (s^{c_1}, \ldots, s^{c_{n-1}})$.

2. Use the assumptions (Δ, I and t are all Lazard valuation-invariant on S) and the property of the test curves to show that
$$t^{-\langle c', v' \rangle} P_\psi(p', t, X_n) = EP_{p'}(X_n) + tR(t, X_n)$$
satisfies the assumptions of Puiseux with parameter.

3. Conclure the delineablity of $EP_{p'}$ on S by setting $t = 0$.