Generalized Taylor formulae, computations in real closed valued fields and quantifier elimination

Mari-Emi Alonso [*] Henri Lombardi [†]

2002

Abstract

We use generalized Taylor formulae in order to give some simple constructions in the real closure of an ordered valued field. We deduce a new, simple quantifier elimination algorithm for real closed valued fields and some theorems about constructible subsets of real valuative affine space.

Key words: Valued fields, Real closed fields, Generalized Taylor formulae, Quantifier elimination, Constructive mathematics

MSC 2000: 14P10, 12J10, 12L05, 12Y05, 03F65, 03C10

Introduction

In this work, we consider the real closure of an ordered valued field and search for simple computations giving a constructive content to this real closure. We don't try to give sophisticated algorithms which would allow better complexity.

We consider an ordered valued field $(\mathbf{K}, \mathbf{V}, \mathbf{P})$ with $\mathbf{V}$ its valuation ring and $\mathbf{P}$ its positive cone. Recall that this means that the following properties hold

$$\begin{array}{lll} \mathbf{V}+\mathbf{V}\subseteq\mathbf{V}, & \mathbf{V}\times\mathbf{V}\subseteq\mathbf{V}, & \exists x\in\mathbf{K}\setminus\mathbf{V}, \\ & & \forall x,y\in\mathbf{K}\ (xy=1\ \Rightarrow\ x\in\mathbf{V}\vee y\in\mathbf{V}), \\ \mathbf{P}\times\mathbf{P}\subseteq\mathbf{P}, & \mathbf{P}+\mathbf{P}\subseteq\mathbf{P}, & \exists x\in\mathbf{K}\setminus\mathbf{P}, \\ & & \forall x,y\in\mathbf{K}\ (x+y=0\ \Rightarrow\ x\in\mathbf{P}\vee y\in\mathbf{P}), \end{array}$$

$$\forall x,y\in\mathbf{K}\ [(x+y\in\mathbf{V}, x\in\mathbf{P}, y\in\mathbf{P})\ \Rightarrow\ x\in\mathbf{V}].$$

For a, b in $\mathbf{K}$, we write $a\leq b$ if and only if $b-a$ is in $\mathbf{P}$. We shall use freely in the sequel some well known features of ordered valued fields: $\mathbb{Q}\subseteq\mathbf{V}$, elements of $\mathbf{V}$ bounded from below by some positive rational are units in $\mathbf{V}$, and the non-units in $\mathbf{V}$ are the infinitesimal elements of $\mathbf{K}$.

[*] Universitad Complutense, Madrid, España. Partially supported by: PB95/0563-A. M_Alonso@Mat.UCM.Es

[†] Laboratoire de Mathématiques, UMR CNRS 6623. Univ. de Franche-Comté, France. henri.lombardi@univ-fcomte.fr

Let $\mathbf{S}$ be a subring of $\mathbf{V}$ such that $\mathbf{K}$ is the fraction field of $\mathbf{S}$. We assume that $\mathbf{S}$ is an explicit ordered ring and that divisibility inside $\mathbf{V}$ is testable for two arbitrary elements of $\mathbf{S}$. These are our minimal assumptions of computability. If we want more assumptions in certain cases we shall make them explicit.

We denote the real closure of $(\mathbf{K}, \mathbf{P})$ by $(\mathbf{K}^{\mathrm{rc}}, \mathbf{P}^{\mathrm{rc}})$, and we write $\mathbf{V}^{\mathrm{rc}}$ for the convex hull of $\mathbf{V}$ inside $\mathbf{K}^{\mathrm{rc}}$; then $\mathbf{V}^{\mathrm{rc}}$ is the unique order-compatible valuation ring extending $\mathbf{V}$. We call $(\mathbf{K}^{\mathrm{rc}}, \mathbf{V}^{\mathrm{rc}}, \mathbf{P}^{\mathrm{rc}})$ the real closure of $(\mathbf{K}, \mathbf{V}, \mathbf{P})$.

In sections 1 and 2 our general purpose is to discuss computational problems in $(\mathbf{K}^{\mathrm{rc}}, \mathbf{V}^{\mathrm{rc}}, \mathbf{P}^{\mathrm{rc}})$ under our computability assumptions on $(\mathbf{K}, \mathbf{V}, \mathbf{P})$.

Each computational problem we shall consider has as *input* a finite family $(c_i)_{i=1,\dots,n}$ of *parameters* in the ring $\mathbf{S}$. We call them the *coefficients* of our computational problem. Our algorithms with the previous minimal computability assumptions work uniformly. This means that some computations are made that give polynomials in $\mathbb{Z}[C_1, \dots, C_n]$, and that all our tests are of the two following types:

$$\text{Is } P(c_1, \dots, c_n) \geq 0? \qquad \text{Does } \; Q(c_1, \dots, c_n) \; \text{ divide } \; P(c_1, \dots, c_n) \; \text{ in } \mathbf{V}?$$

We are not interested in how the answers to these tests are found. We may imagine these answers given either by some oracles or by some algorithms.

Let us state precisely some other notations. We shall denote the unit group of $\mathbf{V}$ by $\mathcal{U}_{\mathbf{V}}$, and $\mathcal{M}_{\mathbf{V}} = \mathbf{V} \setminus \mathcal{U}_{\mathbf{V}}$ will be the maximal ideal.

We shall denote the residue field $\mathbf{V}/\mathcal{M}_{\mathbf{V}}$ of $(\mathbf{K}, \mathbf{V})$ by $\overline{\mathbf{K}}$, and the value group, $\mathbf{K}^{\times}/\mathcal{U}_{\mathbf{V}}$, by $\Gamma_{\mathbf{K}}$. We use freely the value group's usual additive notation as well as its usual group-ordering (also denoted by $\leq$). Recall that $\Gamma_{\mathbf{K}^{\mathrm{rc}}}$ is the divisible hull $\Gamma_{\mathbf{K}}^{dh}$ of $\Gamma_{\mathbf{K}}$. For $x \in \mathbf{K}$ we write $v(x)$ or $v_{\mathbf{K}}(x)$ the valuation of x in $\Gamma_{\mathbf{K}} \cup \{+\infty\}$. So

$$v(0) = +\infty, \; v(xy) = v(x) + v(y), \; (x \geq 0, y \geq 0) \Rightarrow v(x+y) = \min(v(x), v(y)),$$

and

$$\forall x \in \mathbf{K} \;\; ((v(x) \geq 0 \;\Leftrightarrow\; x \in \mathbf{V}) \;\wedge\; (v(x) > 0 \;\Leftrightarrow\; x \in \mathcal{M}_{\mathbf{V}})).$$

We write $\mathbf{K}^{\mathrm{ac}} = \mathbf{K}^{\mathrm{rc}}[\sqrt{-1}]$ and we denote by $\mathbf{V}^{\mathrm{ac}}$ the natural valuation ring of $\mathbf{K}^{\mathrm{ac}}$ extending $\mathbf{V}^{\mathrm{rc}}$: for $a, b \in \mathbf{K}^{\mathrm{rc}}$, $v(a + b\sqrt{-1}) = (1/2)v(a^2 + b^2)$.

In fact elements of $\Gamma_{\mathbf{K}}^{dh} \cup \{+\infty\}$ are always defined through elements of $\mathbf{S}$ in the following form. We say that the valuation of some element x belonging to $\mathbf{K}^{\mathrm{ac}}$ is *well determined* if we know integers m and n, elements $c_1, ..., c_n$ in $\mathbf{S}$, and two elements F and G of $\mathbb{Z}[C_1, ..., C_n]$, such that, setting $f = F(c_1, \dots, c_n)$ $(f \neq 0)$ and $g = G(c_1, \dots, c_n)$, there exists a unit u in $\mathbf{V}^{\mathrm{ac}}$ with:

$$f x^m = u g$$

(in particular, $v(0)$ is well determined).

We read the previous formula as:

$$m\, v_{\mathbf{K}^{\mathrm{ac}}}(x) = v_{\mathbf{K}}(g) - v_{\mathbf{K}}(f),$$

or more simply as:

$$m\, v(x) = v(g) - v(f).$$

For $x, y \in \mathbf{K}^{\mathrm{ac}}$, we shall use the notation $x \preceq y$ for $v(x) \leq v(y)$ (i.e., $y = x = 0 \;\vee\; (x \neq 0 \wedge y/x \in \mathbf{V}^{\mathrm{ac}})$).

Example. Let us explain the computations that are necessary to compare $3v(x_1)+2v(x_2)$ to $7v(x_3)$ when the valuations are given by

$$f_1x_1^{m_1}=u_1g_1,\ f_2x_2^{m_2}=u_2g_2,\ f_3x_3^{m_3}=u_3g_3 \quad (g_1,g_2,g_3\neq 0).$$

We consider the LCM $m=m_1n_1=m_2n_2=m_3n_3$ of m_1,m_2,m_3. We have

$$f_1^{n_1}x_1^m=u_1^{n_1}g_1^{n_1},\ f_2^{n_2}x_2^m=u_2^{n_2}g_2^{n_2},\ f_3^{n_3}x_3^m=u_3^{n_3}g_3^{n_3}.$$

So $3v(x_1)+2v(x_2)\leq 7v(x_3)$ iff $g_1^{3n_1}g_2^{2n_2}f_3^{7n_3}\preceq f_1^{3n_1}f_2^{2n_2}g_3^{7n_3}$.

The reader can easily verify that computations we shall run in the value group are always meaningful under our computability assumptions on the ring **S**.

In the same way, elements of the residue field will in general be defined from elements of **V**. So computations inside the residue field are given by computations inside **S**.

We now give an outline of the paper.

In section 1 we give some basic tools used in the rest of the paper. First we recall the Newton Polygon Algorithm and the Generalized Tschirnhaus Transformation. Then we insist on Generalized Taylor formulae, which are formulae giving $P(x)$ on a Thom interval as a sum of terms all having the same sign. This feature allows us to give a good description for $v(P(x))$ with the crucial Theorem 1.3.6. This allows us to give a nice description for "constructible" subsets of the real line in the context of real closed valued fields (cf. Theorem 1.4.4).

In section 2 we settle three basic computational problems in the real closure of an ordered valued field. We solve the first problem by a simple trick (subsection 2.3). The consequence is that when we know how to compute in a given ordered valued field, we know how to compute in its real closure. This can be seen as a not too difficult extension of basic algorithms in real closed fields. Solving the second problem is possible by using our first algorithm, but we prefer to develop another algorithm, similar to the Cohen-Hörmander algorithm for ordered fields. We get in this way nice uniform results describing precisely some generalizations of the complete tableau of signs in the real closed case (Theorems 2.4.5 and 2.5.2).

In section 3 we give parametrized versions of previous algorithms (Theorems 3.1.1 and 3.1.3), and we apply these results to quantifier elimination in real closed valued fields. We consider the first order theory of real closed valued fields based on the language of ordered fields $(0,1,+,-,\times,=,\leq)$ to which we add the predicate $x\preceq y$. So, all constants and variables represent elements in **K** (this corresponds to our previously explained computability assumptions). We get the following theorem.

Theorem 3.2.1 *Let $\Phi(\underline{a},\underline{x})$ be a quantifier free formula in the first order theory of real closed valued fields. We view the a_i's as parameters and the x_j's as variables.*

Then one can give a quantifier free formula $\Psi(\underline{a})$ such that the two formulae $\exists\underline{x}\ \Phi(\underline{a},\underline{x})$ and $\Psi(\underline{a})$ are equivalent in the formal theory. (The terms appearing in the formulae Φ and Ψ are $\mathbb{Z}$–polynomials in the parameters, and, in the case of Φ, also in the variables.)

We think we have given here a rather simple proof of this fundamental, well known result (see e.g., [2]).

We also get the following abstract form of the previous theorem.

Theorem 3.3.2 *Let us denote the real-valuative spectrum of a commutative ring A by* Sperv$A$. *Then the canonical mapping from* Sperv$A[X]$ *to* Sperv$A$ *transforms any constructible subset into a constructible subset.*

In section 4 we apply the parametrized algorithms in order to study constructible subsets (in the meaning of real closed valued fields). First, we get the analogue of the Tarski-Seidenberg principle.

Theorem 4.1.1 *Let $(\mathbf{K},\mathbf{V},\mathbf{P})$ be an ordered valued subfield of a real closed valued field $(\mathbf{R},\mathbf{V_R},\mathbf{P_R})$. Let π be the canonical projection from $\mathbf{R}^{n+r}$ onto $\mathbf{R}^n$. Let $S\subseteq\mathbf{R}^{n+r}$ be any $(\leq,\preceq)$–constructible set defined over $(\mathbf{K},\mathbf{V},\mathbf{P})$. Assume that the sign test and the divisibility test are explicit inside the ring generated by the coefficients of the polynomials that appear in the definition of S. Then a description of the projection $\pi(S)\subseteq\mathbf{R}^n$ can be computed in a uniform way by an algorithm that uses only rational computations, sign tests and divisibility tests.*

In particular, the complexity of a description of $\pi(S)$ is explicitly bounded in terms of the complexity of a description of S.

Finally we construct a kind of stratification for $(\leq,\preceq)$–constructible sets, that we call stratification à la Cohen Hormander because it is a further development of the same notion for semialgebraic sets (cf. [1] chapter 9), and we finish the paper with the following cell-decomposition theorem (for a precise definition of $\mathbb{Q}$-semilinear functions see definition 2.4.4).

Theorem 4.2.5 (Cell decomposition theorem) *Let $(\mathbf{K},\mathbf{V},\mathbf{P})$ be an ordered valued subfield of a real closed valued field $(\mathbf{R},\mathbf{V_R},\mathbf{P_R})$. Let $g_1,\ldots,g_s$ be nonzero polynomials in $\mathbf{K}[x_1,\ldots,x_n]$. Consider a linear change of variables together with a family $(f_{i,j})_{i=1,\ldots,n;j=1,\ldots,\ell_i}$ that give a stratification for $(g_1,\ldots,g_s)$. Assume that this stratification is constructed à la Cohen-Hörmander. Consider any k-dimensional stratum C_ε corresponding to this stratification. Then there is a Nash isomorphism*

$$h:(\mathbf{R}^+)^k\longrightarrow C_\varepsilon,\quad (t_1,\ldots,t_k)\longmapsto h(t_1,\ldots,t_k)$$

with the following property.

If S is any $(\leq,\preceq)$–constructible subset described from $g_1,\ldots,g_s$, then $S\cap C_\varepsilon$ is a finite union of cells $h(L_i)$, where each L_i can be defined as

$$\left\{(t_1,\ldots,t_k)\in(\mathbf{R}^+)^k\ :\ \bigwedge_\ell a_\ell(\tau)=\alpha_\ell\ \wedge\ \bigwedge_m b_m(\tau)>\beta_m\right\},$$

where $\tau=(\tau_1,\ldots,\tau_k)=(v(t_1),\ldots,v(t_k))$, the a_ℓ's and b_m's are $\mathbb{Z}$-linear forms w.r.t. τ, and $\alpha_\ell,\ \beta_m\in\Gamma_{\mathbf{K}}^{dh}$.

Moreover, each τ_i is a $\mathbb{Q}$-semilinear function in some $v(F_j(x_1,\ldots,x_n))$'s (with F_j explicitly computable in $\mathbf{K}[x_1,\ldots,x_n]$).

1 Basic material

1.1 The Newton Polygon

Here we recall the well known Newton Polygon algorithm.

A *multiset* is a set with (nonnegative) multiplicities, or equivalently a list defined up to permutation. E.g., the roots of a polynomial $P(X)$ repeated according to multiplicities form a multiset in the algebraic closure of the base field. We shall use the notation $[x_1,\ldots,x_d]$ for the multiset corresponding to the list $(x_1,\ldots,x_d)$. The *cardinality* of a multiset is the length of a corresponding list, i.e., the sum of multiplicities occurring in the multiset.

The Newton polygon of a polynomial $P(X)=\sum_{i=0,\ldots,d}p_iX^i\in\mathbf{K}[X]$ (where $p_d\neq 0$) is obtained from the list of pairs in $\mathbb{N}\times(\Gamma_{\mathbf{K}}\cup\{+\infty\})$

$$((0,v(p_0)),(1,v(p_1)),\ldots,(d,v(p_d))).$$

The Newton polygon is "the bottom convex hull" of this list. It can be formally defined as the extracted list $((0,v(p_0)),\ldots,(d,v(p_d)))$ verifying: two pairs $(i,v(p_i))$ and $(j,v(p_j))$ are two consecutive vertices of the Newton polygon iff:

$$\begin{array}{rl} \text{if } 0 \le k < i & \text{then } (v(p_j) - v(p_i))/(j-i) > (v(p_i) - v(p_k)/(i-k)) \\ \text{if } i < k < j & \text{then } (v(p_k) - v(p_i))/(k-i) \ge (v(p_j) - v(p_i))/(j-i) \\ \text{if } j < k \le d & \text{then } (v(p_k) - v(p_j))/(k-j) > (v(p_j) - v(p_i))/(j-i) \end{array}$$

It is easily shown that if $(i, v(p_i))$ and $(j, v(p_j))$ are two consecutive vertices in the Newton polygon of the polynomial P, then the zeroes of P in $\mathbf{K}^{\mathrm{ac}}$ whose valuation in $\Gamma_{\mathbf{K}}^{dh}$ equals $(v(p_i) - v(p_j))/(j-i)$ form a multiset with cardinality $j-i$.

Computational problem 0 (Multiset of valuations of roots of polynomials)
Input: *Let $P \in \mathbf{K}[X]$ be a polynomial over a valued field $(\mathbf{K}, \mathbf{V})$.*
Output: *The multiset $[v(x_1), \ldots, v(x_n)]$ where $[x_1, \ldots, x_n]$ is the multiset of roots of P in $\mathbf{K}^{\mathrm{ac}}$.*

Newton Polygon algorithm
The number n_∞ of roots equal to 0 (i.e., with infinite valuation) is read on P. Let $P_0 := P/X^{n_\infty}$. Compute the Newton polygon of P_0, compute the slopes and output the answer. ∎

1.2 Generalized Tschirnhaus transformation

We recall here the well known (generalized) Tschirnhaus transformation, which we will use freely in our computations.

Let $\mathbf{K}$ be a field, $(P_j)_{j=1,\ldots,m}$ be a family of monic polynomials in $\mathbf{K}[X]$, and

$$P_j(X) = (X - x_{j,1}) \times \cdots \times (X - x_{j,d_j})$$

their decompositions in $\mathbf{K}^{\mathrm{ac}}$. Let $Q(Y_1, \ldots, Y_m)$ be a polynomial in $\mathbf{K}[Y_1, \ldots, Y_m]$. Then the polynomial

$$T_Q(Z) = (Z - Q(x_{1,1}, \ldots, x_{m,1})) \times \cdots \times (Z - Q(x_{1,d_1}, \ldots, x_{m,d_m}))$$

is the characteristic polynomial of A_Q where A_Q is the matrix of the multiplication by $Q(y_1, \ldots, y_m)$ inside the d-dimensional $\mathbf{K}$-algebra

$$\mathbf{K}[y_1, \ldots, y_m] := \mathbf{K}[Y_1, \ldots, Y_m] / \langle P_1(Y_1), \ldots, P_m(Y_m) \rangle$$

($d = d_1 \cdots d_m$, and y_i is the class of Y_i modulo $\langle P_1, \ldots, P_m \rangle$).

Now let $R \in \mathbf{K}[Y_1, \ldots, Y_m]$ with $R(\underline{x}) \neq 0$ for all m-tuples $\underline{x} = (x_{1,r_1}, \ldots, x_{m,r_m})$. So A_R is an invertible matrix. Let $F = Q/R$, then the polynomial

$$T_F(Z) = (Z - F(x_{1,1}, \ldots, x_{m,1})) \times \cdots \times (Z - F(x_{1,d_1}, \ldots, x_{m,d_m}))$$

is the characteristic polynomial of $A_Q(A_R)^{-1}$.

1.3 Generalized Taylor Formulas

Using the usual Taylor formula for computing valuations in $\Gamma_{\mathbf{K}}^{dh}$.

For $P \in \mathbf{K}[X]$ we denote $P^{[k]} = P^{(k)}/k!$, where $P^{(k)}$ is the k-th derivative of P. Let $t = x - a$, and assume $\deg(P) = d$, the usual Taylor formula at the point a is

$$P(x) = P(a) + P^{[1]}(a)t + P^{[2]}(a)t^2 + \cdots + P^{[d-1]}(a)t^{d-1} + P^{[d]}t^d.$$

Now assume that $P^{[d]} > 0$. Let a_0 be the greatest real root of the product $PP^{[1]} \cdots P^{[d-1]}$. If $a \ge a_0$ we see that all $P^{[k]}(a)$ are ≥ 0 and we get the following expression for the valuation $v(P(x))$ when $x > a$

$$v(P(x)) = \min(\nu_0, \nu_1 + \tau, \nu_2 + 2\tau, \ldots, \nu_d + d\tau)$$

where $\tau = v(t)$ and $\nu_j = v(P^{[j]}(a))$ (some ν_j's may be infinite). So, w.r.t. the variable τ the valuation of $P(x)$ in $\Gamma_{\mathbf{K}}^{dh}$ is piecewise linear and increasing. Note that τ decreases from $+\infty$ to $-\infty$ when t increases from 0 to $+\infty$.

In the following paragraphs, we see that generalized Taylor formulae allow us to give a similar description of the valuation $v(P(x))$ when x is inside a Thom interval.

What are generalized Taylor formulae?

A fundamental example of algebraic evidence for a sign is given by generalized Taylor formulae, which make explicit some consequences of Thom's lemma in terms of algebraic identities.

Thom's lemma implies that the set of points where a real polynomial and its successive derivatives have fixed signs is an interval. An easy proof, by induction on the degree of the polynomial, is based on the mean value theorem. We can translate this geometric fact under the form of algebraic identities called *Generalized Taylor Formulas* (GTF for short).

Let us see an example where $\deg(P) \leq 4$.

Example 1.3.1 *Consider the general polynomial of degree* 4

$$P(X) = c_0X^4 + c_1X^3 + c_2X^2 + c_3X + c_4,$$

consider the following system of sign conditions for the polynomial P and its successive derivatives with respect to the variable X:

$$H(X) : P(X) > 0,\ P^{[1]}(X) < 0,\ P^{[2]}(X) < 0,\ P^{[3]}(X) < 0,\ P^{[4]} > 0.$$

Consider also the system of sign conditions obtained by relaxing all the inequalities, except one of them, e.g., the last one:

$$H'(X) : P(X) \geq 0,\ P^{[1]}(X) \leq 0, P^{[2]}(X) \leq 0,\ P^{[3]}(X) \leq 0,\ P^{[4]} > 0.$$

Thom's lemma implies that:

$$[\,H'(a),\ H'(b),\ a < x < b\,] \implies H(x).$$

Put $e_1 = x - a$, $e_2 = b - x$. Consider the following algebraic identity in $\mathbb{Z}[c_0, \ldots, c_4, a, b, x]$

$$\begin{aligned} P(x) \;=\; & P(b) - e_2\, P^{[1]}(a) - (2e_1e_2 + {e_2}^2)\, P^{[2]}(a) \\ & -(3{e_1}^2e_2 + 3e_1{e_2}^2 + {e_2}^3)\, P^{[3]}(b) \\ & +(8{e_1}^3e_2 + 12{e_1}^2{e_2}^2 + 12e_1{e_2}^3 + 3{e_2}^4)\, P^{[4]}. \end{aligned}$$

This gives clearly an evidence that, when $P \in \mathbf{K}[X]$ where $\mathbf{K}$ is an ordered field,

$$[\,H'(a),\ H'(b),\ a < x < b\,] \implies P(x) > 0.$$

One can find more information about mixed and generalized Taylor formulae in [6, 10, 11]. The important thing is that for any fixed degree, and any combination of signs for P and its derivatives (which are assumed to be fixed on the interval), there exists a corresponding GTF. We state a general result giving the existence of GTF's.

Proposition 1.3.2 (see [10]) *Let P be a polynomial of degree d in $\mathbf{K}[X]$ and a, b, x three variables. Let $e_1 = x - a$, $e_2 = b - x$. Let $\varepsilon = (\epsilon_1, \ldots, \epsilon_d)$ be any sequence in $\{-1, +1\}$. Let $\epsilon_0 = 1$. Then there exists an algebraic identity*

$$P(x) = P(a_0) + \sum_{k=1}^{d-1} \epsilon_k H_{k,\varepsilon}(e_1, e_2) P^{[k]}(a_k) + \epsilon_d H_{d,\varepsilon}(e_1, e_2) P^{[d]}$$

where each polynomial $H_{k,\varepsilon}$ is homogeneous of degree k with nonnegative integer coefficients, $a_k = a$ if $\epsilon_k\epsilon_{k+1} = 1$, and $a_k = b$ if $\epsilon_k\epsilon_{k+1} = -1$.

Moreover, if $\epsilon_1 = 1$, then e_1 divides all the $H_{k,\varepsilon}$'s, and the coefficient of e_1^k in $H_{k,\varepsilon}$ is nonzero. In a similar way if $\epsilon_1 = -1$, then e_2 divides all the $H_{k,\varepsilon}$'s, and the coefficient of e_2^k in $H_{k,\varepsilon}$ is nonzero.

Remark 1.3.3 *Let P be a polynomial of degree d in $K[X]$ and let $a < b \in \mathbf{K}^{\mathrm{rc}}$ be such that $P^{[k]}(a)P^{[k]}(b) \geq 0$ for $k = 0, \ldots, d$. This gives a system of signs $(\sigma_0, \sigma_1, \ldots, \sigma_d)$ ($\sigma_i = \pm 1$) (σ_k is the sign of $P^{[k]}(x)$ on the open interval $]a, b[$). Let $\epsilon_i = \sigma_0\sigma_i$, $\varepsilon = (\epsilon_1, \ldots, \epsilon_d)$. Then the corresponding GTF gives an algebraic certificate for the fact that* $\mathrm{sign}(P(x)) = \sigma_0$ *when $a < x < b$.*

We now give four GTF's in degree 3, those beginning by $P(a) + e_1P^{[1]} \cdots$. Each formula is given also with e_1 in factor in the second part.

$$\begin{aligned}
P(x) = \;& P(a) + e_1P^{[1]}(a) + e_1^2P^{[2]}(a) + e_1^3P^{[3]} \\
=\; & P(a) + e_1\left(P^{[1]}(a) + e_1P^{[2]}(a) + e_1^2P^{[3]}\right) \\
\\
=\; & P(a) + e_1P^{[1]}(a) + e_1^2P^{[2]}(b) - \left(2e_1^3 + e_1^2e_2\right)P^{[3]} \\
=\; & P(a) + e_1\left(P^{[1]}(a) + e_1P^{[2]}(b) - \left(2e_1^2 + e_1e_2\right)P^{[3]}\right) \\
\\
=\; & P(a) + e_1P^{[1]}(b) - \left(e_1^2 + 2e_1e_2\right)P^{[2]}(a) - \left(2e_1^3 + 6e_1^2e_2 + 3e_1e_2^2\right)P^{[3]} \\
=\; & P(a) + e_1\left(P^{[1]}(b) - \left(e_1 + 2e_2\right)P^{[2]}(a) - \left(2e_1^2 + 6e_1e_2 + 3e_2^2\right)P^{[3]}\right) \\
\\
=\; & P(a) + e_1P^{[1]}(b) - \left(e_1^2 + 2e_1e_2\right)P^{[2]}(b) + \left(e_1^3 + 3e_1^2e_2 + 3e_1e_2^2\right)P^{[3]} \\
=\; & P(a) + e_1\left(P^{[1]}(b) - \left(e_1 + 2e_2\right)P^{[2]}(b) + \left(e_1^2 + 3e_1e_2 + 3e_2^2\right)P^{[3]}\right).
\end{aligned}$$

There are also four other GTF's beginning by $P(b) - e_2.P^{[1]} \cdots$. They can be obtained from the first ones by swapping a and b, and replacing e_1 and e_2 by $-e_2$ and $-e_1$

$$\begin{aligned}
P(x) = \;& P(b) - e_2P^{[1]}(b) + e_2^2P^{[2]}(b) - e_2^3P^{[3]} \\
=\; & P(b) - e_2\left(P^{[1]}(b) - e_2P^{[2]}(b) + e_2^2P^{[3]}\right) \\
\\
=\; & P(b) - e_2P^{[1]}(b) + e_2^2P^{[2]}(a) + \left(2e_2^3 + e_2^2e_1\right)P^{[3]} \\
=\; & P(b) - e_2\left(P^{[1]}(b) - e_2P^{[2]}(a) - \left(2e_2^2 + e_2e_1\right)P^{[3]}\right) \\
\\
=\; & P(b) - e_2P^{[1]}(a) - \left(e_2^2 + 2e_2e_1\right)P^{[2]}(b) + \left(2e_2^3 + 6e_2^2e_1 + 3e_2e_1^2\right)P^{[3]} \\
=\; & P(b) - e_2\left(P^{[1]}(a) + \left(e_2 + 2e_1\right)P^{[2]}(b) - \left(2e_2^2 + 6e_2e_1 + 3e_1^2\right)P^{[3]}\right) \\
\\
=\; & P(b) - e_2P^{[1]}(a) - \left(e_2^2 + 2e_2e_1\right)P^{[2]}(a) + \left(e_2^3 - 3e_2^2e_1 + 3e_2e_1^2\right)P^{[3]} \\
=\; & P(b) - e_2\left(P^{[1]}(a) + \left(e_2 + 2e_1\right)P^{[2]}(a) + \left(e_2^2 + 3e_2e_1 + 3e_1^2\right)P^{[3]}\right).
\end{aligned}$$

Using generalized Taylor formulae for computing the variations of the valuation $v(P(x))$.

Now let us see in the case of an ordered valued field how these formulae can be used in order to describe the variations of $v(P(x))$ when x is on the real line $\mathbf{K}^{\mathrm{rc}}$.

Example 1.3.4 *Let $a, b \in \mathbf{K}^{\mathrm{rc}}$ and assume that the signs of the derivatives of a polynomial P of degree 4 are the same in a and b, as in Example 1.3.1. If $x \in [a, b]$ let $x = a + t_1(b - a)$,*

$e = b - a$, $e_1 = t_1 e$, $e_2 = t_2 e$ (so $t_2 = 1 - t_1$), $\delta = v(e)$, $\tau_1 = v(t_1)$, $\tau_2 = v(t_2)$, $\nu_0 = v(P(b))$, $\nu_1 = v(P^{[1]}(a))$, $\nu_2 = v(P^{[2]}(a))$, $\nu_3 = v(P^{[3]}(b))$, $\nu_4 = v(P^{[4]})$. We rewrite the GTF as

$$\begin{aligned} P(x) \;=\; & P(b) - e\,t_2\,P^{[1]}(a) - e^2(2t_1t_2 + {t_2}^2)\,P^{[2]}(a) \\ & -e^3(3{t_1}^2t_2 + 3t_1{t_2}^2 + {t_2}^3)\,P^{[3]}(b) \\ & +e^4(8{t_1}^3t_2 + 12{t_1}^2{t_2}^2 + 12t_1{t_2}^3 + 3{t_2}^4)\,P^{[4]}. \end{aligned}$$

In the above GTF, since all terms of the sum are ≥ 0, the valuation of the sum is the minimum of valuations of the terms, so we get:

(1) *If t_1 and t_2 are units, then $\tau_1 = \tau_2 = 0$ and $v(P(x))$ is constant equal to*

$$v(P(x)) = \min(\nu_0,\, \nu_1 + \delta,\, \nu_2 + 2\delta,\, \nu_3 + 3\delta,\, \nu_4 + 4\delta).$$

(2) *If t_1 is infinitely close to 0, then $\tau_1 > 0$ (decreasing as t_1 increases), $\tau_2 = 0$, and $v(P(x))$ is a priori increasing "piecewise linearly w.r.t. τ_1", but in our case constant*

$$v(P(x)) = \min(\nu_0,\, \nu_1 + \delta,\, \nu_2 + 2\delta,\, \nu_3 + 3\delta,\, \nu_4 + 4\delta).$$

(3) *If t_1 is infinitely close to 1, then $\tau_1 = 0$, $\tau_2 > 0$ (increasing as t_1 increases), and $v(P(x))$ is increasing "piecewise linearly w.r.t. τ_2"*

$$v(P(x)) = \min(\nu_0,\, \nu_1 + \delta + \tau_2,\, \nu_2 + 2\delta + \tau_2,\, \nu_3 + 3\delta + \tau_2,\, \nu_4 + 4\delta + \tau_2).$$

In fact here we see that this formula is true in the three cases and that only two slopes (w.r.t. the variable τ_2) can appear since

$$v(P(x)) = \min(\nu_0,\, \min(\nu_1 + \delta,\, \nu_2 + 2\delta,\, \nu_3 + 3\delta,\, \nu_4 + 4\delta) + \tau_2).$$

Example 1.3.5 *In a similar way let us see what is given by the second GTF in degree 3*

$$P(x) = P(a) + e_1\,P^{[1]}(a) + e_1^2\,P^{[2]}(b) - \left(2e_1^3 + e_1^2e_2\right)\,P^{[3]}.$$

We assume $P(a) \geq 0$, $P^{[1]}(a) \geq 0$, $P^{[2]}(b) \geq 0$, $P^{[3]} < 0$, $x = a + t_1(b - a)$, $e = b - a$, $e_1 = t_1 e$, $e_2 = t_2 e$ ($t_2 = 1 - t_1$), $\delta = v(e)$, $\tau_1 = v(t_1)$, $\tau_2 = v(t_2)$, $\nu_0 = v(P(a))$, $\nu_1 = v(P^{[1]}(a))$, $\nu_2 = v(P^{[2]}(b))$, $\nu_3 = v(P^{[3]})$, and we get

$$P(x) = P(a) + e\,t_1\,P^{[1]}(a) + e^2t_1^2\,P^{[2]}(b) - e^3\left(t_1^3 + t_1^2t_2\right)\,P^{[3]}.$$

(1) *If t_1 and t_2 are units, then $\tau_1 = \tau_2 = 0$ and $v(P(x))$ is constant equal to*

$$v(P(x)) = \min(\nu_0,\, \nu_1 + \delta,\, \nu_2 + 2\delta,\, \nu_3 + 3\delta).$$

(2) *If t_1 is infinitely close to 1, then $\tau_1 = 0$, $\tau_2 > 0$ (increasing as t_1 increases), and $v(P(x))$ is increasing "piecewise linearly w.r.t. τ_2", but in our case constant*

$$v(P(x)) = \min(\nu_0,\, \nu_1 + \delta,\, \nu_2 + 2\delta,\, \nu_3 + 3\delta).$$

(3) *If t_1 is infinitely close to 0, then $\tau_1 > 0$ (decreasing as t_1 increases), $\tau_2 = 0$, and $v(P(x))$ is increasing "piecewise linearly w.r.t. τ_1",*

$$v(P(x)) = \min(\nu_0,\, \nu_1 + \delta + \tau_1,\, \nu_2 + 2\delta + 2\tau_1,\, \nu_3 + 3\delta + 2\tau_1).$$

In fact here we see that this formula is true in the three cases and that only three slopes (w.r.t. the variable τ_1) can appear since

$$v(P(x)) = \min(\nu_0,\, (\nu_1 + \delta) + \tau_1,\, \min(\nu_2 + 2\delta,\, \nu_3 + 3\delta) + 2\tau_1).$$

What we have seen on our two Examples 1.3.4 and 1.3.5 is a general result, that we immediately get as a corollary of Proposition 1.3.2.

Theorem 1.3.6 *Let P be a polynomial of degree d in $K[X]$ and $a < b \in \mathbf{K}^{\mathrm{rc}}$ such that $P^{[k]}(a)P^{[k]}(b) \geq 0$ for $k = 0, \ldots, d$. Let $(\sigma_0, \sigma_1, \ldots, \sigma_d)$ be the signs of $P, P^{[1]}, \ldots, P^{[d]}$ in the interval $]a, b[$ ($\sigma_i = \pm 1$). Let $\epsilon_i = \sigma_0\sigma_i$, $\varepsilon = (\epsilon_1, \ldots, \epsilon_d)$. Let us consider the corresponding GTF as in Proposition 1.3.2, and let us follow the notation there. Let $\nu_k = v(P^{[k]}(a_k))$ for $k = 0, \ldots, d$. Recall that $a_k = a$ if $\epsilon_k\epsilon_{k+1} = 1$, and $a_k = b$ if $\epsilon_k\epsilon_{k+1} = -1$. Note also that ν_k may be infinite if $k < d$. If $x \in [a, b]$ let $x = a + t_1(b - a)$, $e = b - a$, $t_2 = 1 - t_1$, $\delta = v(e)$, $\tau_1 = v(t_1)$, $\tau_2 = v(t_2)$.*

Then for $x \in [a, b]$ the valuation $v(P(x))$ is monotonic w.r.t. t_1 and more precisely can be described in the following way.

(a)
- *If $\epsilon_1 = 1$ we can extract from the GTF integers $k_2, \ldots, k_d$ such that $1 \leq k_j \leq j$ and*
$$v(P(x)) = \min(\nu_0,\ \nu_1 + \delta + \tau_1,\ \nu_2 + 2\delta + k_2\tau_1, \ldots, \nu_d + d\delta + k_d\tau_1).$$
- *If $\epsilon_1 = -1$ we can extract from the GTF integers $k_2, \ldots, k_d$ such that $1 \leq k_j \leq j$ and*
$$v(P(x)) = \min(\nu_0,\ \nu_1 + \delta + \tau_2,\ \nu_2 + 2\delta + k_2\tau_2, \ldots, \nu_d + d\delta + k_d\tau_2).$$

(b) *So in any case the valuation $v(P(x))$ is*
- *either constant (if $v(P(a)) = v(P(b))$),*
- *or increasing piecewise linearly w.r.t. $\tau_1 = v(\frac{x-a}{b-a})$ (if $v(P(a)) > v(P(b))$),*
- *or increasing piecewise linearly w.r.t. $\tau_2 = v(\frac{b-x}{b-a})$, (if $v(P(a)) < v(P(b))$).*

(c) *Introducing*
$$\tau = \tau_1 - \tau_2 = v\left(\frac{t_1}{1 - t_1}\right)$$
we also get: $\tau_1 = \max(\tau, 0) = \tau^+$, $\tau_2 = \max(-\tau, 0) = \tau^-$, and the value $v(P(x))$ is monotone and piecewise linear w.r.t. τ. More precisely, we can extract from the GTF integers $k_2, \ldots, k_d$ such that $1 \leq k_j \leq j$ and
$$v(P(x)) = \min(\nu_0,\ \nu_1 + \delta + \tau',\ \nu_2 + 2\delta + k_2\tau', \ldots, \nu_d + d\delta + k_d\tau')$$
where $\tau' = \max(\epsilon_1\tau, 0)$.

1.4 Constructible subsets of the real line

We introduce here the notion of $(\leq, \preceq)$*–constructible sets* in the real valuative affine space. This notion corresponds to sets that are definable in the language of ordered valued fields. These sets are analogous to Zariski-constructible sets in algebraic geometry and to semi-algebraic sets in real algebraic geometry.

Definition 1.4.1 *Let $(\mathbf{K}, \mathbf{V}, \mathbf{P})$ be an ordered valued field, and consider a finite family $(x_j)_{j=1,\ldots,m}$ of elements of $\mathbf{K}^{\mathrm{rc}}$. Let us call a* valued sign condition (a vsc fort short) for the family *any condition of the following type*
$$\bigwedge_{j \in J} \operatorname{sign}(x_j) = \sigma_j \quad \wedge \quad \bigwedge_{\ell \in L} \operatorname{sign}\left(\sum_{j \in J,\ \sigma_j \neq 0} \ell_j v(x_j)\right) = \sigma'_\ell$$

where $J \subseteq \{1,\dots,m\}$, $\ell \in L$ *(*L *is a finite subset of* $\mathbb{Z}^{\{j\,:\,j\in J,\,\sigma_j\neq 0\}}$*) and* $\sigma_j, \sigma'_\ell \in \{-1,0,1\}$.

Let N *be a positive integer. We call an* N-complete system of valued sign conditions on the family $(x_j)_{j=1,\dots,m}$ *a system of vsc's that gives all the signs* $\mathrm{sign}(x_j)$ *and all the signs* $\mathrm{sign}\left(\sum_{x_j\neq 0}\ell_j v(x_j)\right)$ *for all* $\ell \in \{-N,\dots,0,\dots,N\}^{\{j\,:\,1\leq j\leq m,\,x_j\neq 0\}}$.

An alternative definition could use $\mathrm{sign}\left(\sum_{j\in J,}\ \ell_j v(x_j)\right)$ even when $v(x_j)=\infty$ for some j's. But there should be no natural way to give a sign to an expression containing $\infty-\infty$.

Definition 1.4.2 *Let* $(\mathbf{K},\mathbf{V},\mathbf{P})$ *be an ordered valued subfield of a real closed valued field* $(\mathbf{R}, \mathbf{V_R}, \mathbf{P_R})$*, and consider a finite family* $(P_j)_{j=1,\dots,m}$ *of polynomials in* $\mathbf{K}[X_1,\dots,X_n]$.

- *The subset of* $\mathbf{R}^n$ *made of the* $\underline{x}=(x_1,\dots,x_n)$ *such that the* $P_j(\underline{x})$*'s verify some given system of vsc's is called a* basic $(\leq,\preceq)$–constructible set *defined over* $(\mathbf{K},\mathbf{V},\mathbf{P})$.
- *A* (general) $(\leq,\preceq)$–constructible set defined over $(\mathbf{K},\mathbf{V},\mathbf{P})$ *is any boolean combination* S *of basic* $(\leq,\preceq)$*–constructible sets defined over* $(\mathbf{K},\mathbf{V},\mathbf{P})$*. If* $(P_j)_{j=1,\dots,m}$ *is a family of polynomials such that any basic component of* S *is defined as in the first item, we say that* S is described from $(P_j)_{j=1,\dots,m}$.
- *Let* $S\subseteq\mathbf{R}^n$ *be a* $(\leq,\preceq)$*–constructible set. A map* $f: S\to\mathbf{R}^p$ *is called a* $(\leq,\preceq)$–constructible map *if its graph is a* $(\leq,\preceq)$*–constructible subset of* $\mathbf{R}^{n+p}$.

Let us recall that the order topology and the valued topology are identical in a real closed valued field.

Notation 1.4.3 *Let* $(\mathbf{K},\mathbf{V},\mathbf{P})$ *be an ordered valued subfield of a real closed valued field* $(\mathbf{R}, \mathbf{V_R}, \mathbf{P_R})$*. We shall use the following notations for some convex open* $(\leq,\preceq)$*–constructible subsets of the real line. They are basic* $(\leq,\preceq)$*–constructible sets defined over* $(\mathbf{K}^{\mathrm{rc}},\mathbf{V}^{\mathrm{rc}},\mathbf{P}^{\mathrm{rc}})$.

$$
\begin{aligned}
\mathbb{I}^+(a,\alpha) &= \{x\in\mathbf{R}\,:\,x=a+t,\ 0<t,\ v(t)=\alpha\}\\
&\quad \text{with } a\in\mathbf{K}^{\mathrm{rc}},\ \alpha\in\Gamma_{\mathbf{K}}^{dh}.\\
\mathbb{I}^-(a,\alpha) &= \{x\in\mathbf{R}\,:\,x=a-t,\ 0<t,\ v(t)=\alpha\}\\
&\quad \text{with } a\in\mathbf{K}^{\mathrm{rc}},\ \alpha\in\Gamma_{\mathbf{K}}^{dh}.\\
\mathbb{I}^+(a,\alpha,\beta) &= \{x\in\mathbf{R}\,:\,x=a+t,\ 0<t,\ \alpha<v(t)<\beta\}\\
&\quad \text{with } a\in\mathbf{K}^{\mathrm{rc}},\ \alpha<\beta \text{ in } \Gamma_{\mathbf{K}}^{dh}\cup\{\pm\infty\}.\\
\mathbb{I}^-(a,\alpha,\beta) &= \{x\in\mathbf{R}\,:\,x=a-t,\ 0<t,\ \alpha<v(t)<\beta\}\\
&\quad \text{with } a\in\mathbf{K}^{\mathrm{rc}},\ \alpha<\beta \text{ in } \Gamma_{\mathbf{K}}^{dh}\cup\{\pm\infty\}.\\
\mathbb{J}^+(a,b,\alpha) &= \{x\in\mathbf{R}\,:\,x=a+t(b-a),\ 0<t,\ v(t)=\alpha\}\\
&\quad \text{with } a<b\in\mathbf{K}^{\mathrm{rc}},\ 0<\alpha\in\Gamma_{\mathbf{K}}^{dh}.\\
\mathbb{J}^-(a,b,\alpha) &= \{x\in\mathbf{R}\,:\,x=b-t(b-a),\ 0<t,\ v(t)=\alpha\}\\
&\quad \text{with } a<b\in\mathbf{K}^{\mathrm{rc}},\ 0<\alpha\in\Gamma_{\mathbf{K}}^{dh}.\\
\mathbb{J}^+(a,b,\alpha,\beta) &= \{x\in\mathbf{R}\,:\,x=a+t(b-a),\ 0<t,\ \alpha<v(t)<\beta\}\\
&\quad \text{with } a<b\in\mathbf{K}^{\mathrm{rc}},\ 0\leq\alpha<\beta\in\Gamma_{\mathbf{K}}^{dh}\cup\{+\infty\}.\\
\mathbb{J}^-(a,b,\alpha,\beta) &= \{x\in\mathbf{R}\,:\,x=b-t(b-a),\ 0<t,\ \alpha<v(t)<\beta\}\\
&\quad \text{with } a<b\in\mathbf{K}^{\mathrm{rc}},\ 0\leq\alpha<\beta\in\Gamma_{\mathbf{K}}^{dh}\cup\{+\infty\}.\\
\mathbb{J}(a,b) &= \{x\in\mathbf{R}\,:\,x=a+t(b-a),\ 0<t<1,\ v(t)=v(1-t)=0\}\\
&\quad \text{with } a<b\in\mathbf{K}^{\mathrm{rc}}.
\end{aligned}
$$

These subsets will be called $(<,\preceq)$–intervals defined over $(\mathbf{K},\mathbf{V},\mathbf{P})$.

Some remarks.

- The subsets of $\mathbf{R}$ given in definition 1.4.2 are a priori basic $(\leq, \preceq)$–constructible sets defined over $(\mathbf{K}^{\mathrm{rc}}, \mathbf{V}^{\mathrm{rc}}, \mathbf{P}^{\mathrm{rc}})$. But they are also general $(\leq, \preceq)$–constructible sets defined over $(\mathbf{K}, \mathbf{V}, \mathbf{P})$: this is a consequence of Remark 3.1.2 (2).

- In $\mathbb{J}^+(a,b,\alpha)$, $\mathbb{J}^-(a,b,\alpha)$, $\mathbb{J}^+(a,b,\alpha,\beta)$ and $\mathbb{J}^-(a,b,\alpha,\beta)$ we have $0 < t < 1$ (in fact $t <$ any positive rational number) since $t > 0$ and $v(t) > 0$.

- Except when $\beta = \infty$, any $(<, \preceq)$–interval is closed.

- We have

$$\begin{array}{rcl}]a,\infty[& = & \mathbb{I}^+(a,-\infty,\infty), \\ ]a,b[& = & \mathbb{J}^+(a,b,0,\infty) \cup \mathbb{J}(a,b) \cup \mathbb{J}^-(a,b,0,\infty), \\ \mathbb{I}^+(a,\alpha,\gamma) & = & \mathbb{I}^+(a,\alpha,\beta) \cup \mathbb{I}^+(a,\beta) \cup \mathbb{I}^+(a,\beta,\gamma) \quad \text{if } \alpha < \beta < \gamma, \end{array}$$

  and similar results with $\mathbb{I}^-$, $\mathbb{J}^+$ and $\mathbb{J}^-$.

- When $t > 0$, $\alpha < \beta \in \Gamma_{\mathbf{K}}^{dh} \cup \{+\infty\}$, $c > 0 \in \mathbf{K}$ and $v(c) = \alpha + \beta$ we have the following equivalences

$$\begin{array}{rcl} \alpha < v(t) < \beta & \iff & \alpha < \min(v(t), v(c/t)) \iff \\ \alpha < v(t + c/t) & \iff & \alpha + v(t) < v(t^2 + c). \end{array}$$

- Concerning $\mathbb{J}(a,b)$ we have

$$\mathbb{J}(a,b) = \{x \in \mathbf{R} \,:\, x = a + t(b-a),\ 0 < t(1-t),\ v(t(1-t)) = 0\}.$$

- All $\mathbb{J}$'s could be considered as particular cases of $\mathbb{I}$'s, e.g., $\mathbb{J}^+(a,b,\alpha,\beta) = \mathbb{I}^+(a,\alpha',\beta')$ with $\alpha' = \alpha + v(b-a)$ and $\beta' = \beta + v(b-a)$.

- We could introduce

$$\begin{array}{rcl} \mathbb{J}(a,b,\alpha) & = & \{x \in \mathbf{R} \,:\, x = a + t(b-a),\ 0 < t < 1,\ v(t/(1-t)) = \alpha\} \\ & & \text{with } a < b \in \mathbf{K}^{\mathrm{rc}},\ \alpha \in \Gamma_{\mathbf{K}}^{dh}, \\ \mathbb{J}(a,b,\alpha,\beta) & = & \{x \in \mathbf{R} \,:\, x = a + t(b-a),\ 0 < t < 1,\ \alpha < v(t/(1-t)) < \beta\} \\ & & \text{with } a < b \in \mathbf{K}^{\mathrm{rc}},\ \alpha < \beta \text{ in } \Gamma_{\mathbf{K}}^{dh} \cup \{\pm\infty\}. \end{array}$$

  We should have $\mathbb{J}^+(a,b,\alpha) = \mathbb{J}(a,b,\alpha)$, $\mathbb{J}^-(a,b,\alpha) = \mathbb{J}(a,b,-\alpha)$, $\mathbb{J}^+(a,b,\alpha,\beta) = \mathbb{J}(a,b,\alpha,\beta)$, $\mathbb{J}^-(a,b,\alpha,\beta) = \mathbb{J}(a,b,-\beta,-\alpha)$ and $\mathbb{J}(a,b) = \mathbb{J}(a,b,0)$.

An easy corollary of Theorem 1.3.6 is the following description of $(\leq, \preceq)$–constructible subsets of the real line.

Theorem 1.4.4 *Let $(\mathbf{K}, \mathbf{V}, \mathbf{P})$ be an ordered valued subfield of a real closed valued field $(\mathbf{R}, \mathbf{V}_{\mathbf{R}}, \mathbf{P}_{\mathbf{R}})$. Any $(\leq, \preceq)$–constructible set of $\mathbf{R}$ defined over $(\mathbf{K}, \mathbf{V}, \mathbf{P})$ is a finite disjoint union of points in $\mathbf{K}^{\mathrm{rc}}$ and of $(<, \preceq)$–intervals defined over $(\mathbf{K}, \mathbf{V}, \mathbf{P})$ as in Notations 1.4.3.*

W e give a sketch of the proof on an example. Assume that the $(\leq, \preceq)$–constructible set S is defined from vsc's on 3 polynomials P_1, P_2, P_3 of degrees 5, introduce all real roots of these polynomials and of all their derivatives. Consider two consecutive roots a, b. We want to understand what $S \cap]a,b[$ is.

First let us see what $S \cap \mathbb{J}^+(a,b,0,\infty)$ looks like. We know that each $\mathrm{sign}(P_j(x))$ is constant on $]a,b[$. Concerning the valuations $v(P_j(x))$, we know from Examples 1.3.4 and 1.3.5 and

Theorem 1.3.6 that they are piecewise linear functions of $\tau_1 = v(x-a)/v(b-a)$, e.g., of the following forms

$$\begin{aligned} v(P_1(x)) &= \min(\mu_0, \mu_1+\tau_1, \mu_2+2\tau_1), \\ v(P_2(x)) &= \min(\eta_0, \eta_1+\tau_1, \eta_3+3\tau_1), \\ v(P_3(x)) &= \min(\lambda_0, \lambda_1+\tau_1, \lambda_2+2\tau_1, \lambda_4+4\tau_1). \end{aligned}$$

Note that τ_1 varies on $]0,+\infty[$. These piecewise linear functions have polygonal graphs inside $(\Gamma_{\mathbf{K}}^{dh} \cap]0,+\infty[) \times \Gamma_{\mathbf{K}}^{dh}$. It is possible to compute the vertices of these three polygonal graphs. E.g., if $\lambda_4 < \lambda_1 < \lambda_0$ and $3\lambda_2 > 2\lambda_1 + \lambda_4$ we have two vertices on the polygonal graph of $v(P_3)$ at the points with coordinates

$$\begin{aligned} \tau_{1,1} = \beta_1 = (\lambda_1 - \lambda_4)/3, \qquad & v(P_3(x)) = \lambda_1 + \beta_1 = \lambda_4 + 4\beta_1, \\ \tau_{1,2} = \beta_2 = \lambda_0 - \lambda_1, \qquad & v(P_3(x)) = \lambda_0 = \lambda_1 + \beta_2. \end{aligned}$$

All these vertices give a finite number of valuations for τ_1: $\alpha_1 < \cdots < \alpha_n$. Let $\alpha_0 = 0$, $\alpha_{n+1} = \infty$. On each $\mathbb{J}^+(a,b,\alpha_i,\alpha_{i+1})$ $(0 \le i \le n)$ and on each $\mathbb{J}^+(a,b,\alpha_i)$ $(1 \le i \le n)$, we know that each $v(P_j(x))$ $(1 \le j \le 3)$ is a fixed "affine function" of τ_1. So, the same is true for any linear combination

$$\ell_1 v(P_1(x)) + \ell_2 v(P_2(x)) + \ell_3 v(P_3(x)),$$

and we can compute the valuation τ_1 for which such an expression changes sign.

So the intersection $S \cap \mathbb{J}^+(a,b,0,\infty)$ is a finite disjoint union of $\mathbb{J}^+(a,b,\alpha,\beta)$ and $\mathbb{J}^+(a,b,\alpha)$ subsets.

In a similar way $S \cap \mathbb{J}(a,b)$ is either empty or equal to $\mathbb{J}(a,b)$, and $S \cap \mathbb{J}^-(a,b,0,\infty)$ is a finite disjoint union of $\mathbb{J}^-(a,b,\alpha,\beta)$ and $\mathbb{J}^-(a,b,\alpha)$ subsets.

Finally the intersection of S with the final (resp. initial) open interval is computed in a similar way as a finite union of $\mathbb{I}^+$ (resp. $\mathbb{I}^-$) intervals. □

2 Computing in the real closure of an ordered valued field

2.1 Codes à la Thom and valuations in the value group

The real closure $\mathbf{K}^{\mathrm{rc}}$ of an ordered field $(\mathbf{K},\mathbf{P})$ is unique up to unique $(\mathbf{K},\mathbf{P})$–isomorphism. This fact allows us to give an explicit construction of the real closure $\mathbf{K}^{\mathrm{rc}}$ (this is "well-known" from Tarski or even from Sturm and Sylvester, for a fully constructive proof see [7]).

E.g., it is possible to describe any element x of $\mathbf{K}^{\mathrm{rc}}$ by a so-called *code à la Thom* (see [3, 4]):

Definition 2.1.1 *A pair (P,σ) where $P \in \mathbf{K}[X]$ is a monic polynomial of degree d and $\sigma = (\sigma_1,\ldots,\sigma_{d-1}) \in \{1,-1\}^{d-1}$ codes the root x of P in $\mathbf{K}^{\mathrm{rc}}$ when one has*

$$P(x) = 0 \qquad \text{and} \qquad \sigma_i \cdot P^{(i)}(x) \ge 0 \quad \text{for } i = 1,\ldots,d-1.$$

The pair (P,σ) is called a code à la Thom (over $\mathbf{K}$) for x.

There are algorithms that use only the algebraic structure of $(\mathbf{K},\mathbf{P})$ and give the codes à la Thom corresponding to the roots of P in $\mathbf{K}^{\mathrm{rc}}$. It is possible to make explicit algebraic computations and sign's tests for such elements that are coded à la Thom. See e.g., [3, 4] or Proposition 2.4.2.

On the other hand, the Newton polygon algorithm allows us to determine the valuation $v(x)$ for any x in the algebraic closure of $\mathbf{K}$. How can we match these algorithms?

2.2 Three basic computational problems in the real closure of an ordered valued field

Consider an ordered valued field $(\mathbf{K}, \mathbf{V}, \mathbf{P})$. Since its real closure (with valuation) is determined up to unique $(\mathbf{K}, \mathbf{V}, \mathbf{P})$-isomorphism, the following computational problems makes sense:

Computational Problem 1
Let $(\mathbf{K}, \mathbf{V}, \mathbf{P})$ be an ordered valued field.
Input: *A code à la Thom (P, σ) over $\mathbf{K}$ for an element x of $\mathbf{K}^{\mathrm{rc}}$.*
Output: *The valuation $v(x)$ of x in $\Gamma_{\mathbf{K}}^{dh} \cup \{+\infty\}$. More precisely, compute some $a \in \mathbf{K}$ and a positive integer n such that $n \times v(x) = v(a)$.*

Remark 2.2.1 *Assume that the leading coefficient of $P \in \mathbf{V}[X]$ is a unit. The real zeroes of P are in $\mathbf{V}^{\mathrm{rc}}$. Let us denote by $\overline{x}$ the residue in $\overline{\mathbf{K}^{\mathrm{rc}}}$ of the zero x and by $\overline{P}$ the residue in $\overline{\mathbf{K}}[X]$ of the polynomial P. Then it is clear that $(\overline{P}, \sigma)$ is a code à la Thom over $\overline{\mathbf{K}}$ for $\overline{x}$ since the residual field $\overline{\mathbf{K}^{\mathrm{rc}}}$ can be identified with the real closure $\overline{\mathbf{K}}^{\mathrm{rc}}$ of $\overline{\mathbf{K}}$.*

More generally, we can ask for algorithms solving general existential problems.

Computational Problem 2
Let $(\mathbf{K}, \mathbf{V}, \mathbf{P})$ be an ordered valued field, and consider a finite family of polynomials, $(F_j)_{j=1,\dots,m}$ in $\mathbf{K}[X]$. Let $(x_h)_{h=1,\dots,p}$ be the ordered family of the zeroes of the (F_j)'s in $\mathbf{K}^{\mathrm{rc}}$. Recall that the number p and all the signs $\mathrm{sign}(F_j(x))$, for x equal to some x_h or inside some corresponding open interval, can be determined by computations in the ordered field $(\mathbf{K}, \mathbf{P})$.
Input: *The family $(F_j)_{j=1,\dots,m}$.*
Output: *All the valuations $v(F_j(x_h))$ $(h = 1, \dots, p)$ and $v(x_{h+1} - x_h)$ $(h = 1, \dots, p-1)$ in $\Gamma_{\mathbf{K}}^{dh} \cup \{+\infty\}$.*

Computational Problem 3
Let $(\mathbf{K}, \mathbf{V}, \mathbf{P})$ be an ordered valued field.
Input: *A finite family $(F_j)_{j=1,\dots,m}$ in $\mathbf{K}[X]$. A finite family $(\ell_k)_{k=1,\dots,r}$ of elements of $\mathbb{Z}^m$.*
Output: *All occurring systems of valued sign conditions of the following type for the family $(F_j(x))_{j=1,\dots,m}$ when $x \in \mathbf{K}^{\mathrm{rc}}$:*

$$\left((\mathrm{sign}(F_j(x)))_{j=1,\dots,m},\ \left(\mathrm{sign} \left(\sum_{j \in \{1,\dots,m\},\ F_j(x) \neq 0} \ell_{k,j}\, v(F_j(x)) \right) \right)_{k=1,\dots,r} \right).$$

Remark 2.2.2 *Assume that the family is stable under derivation. From Theorem 1.3.6 (see e.g., the proof of Theorem 1.4.4) it is clear that Computational Problem 3 can be solved by using the solution of Computational Problem 2. In fact we can describe in a finite way all occurring lists*

$$\left((\mathrm{sign}(F_j(x)))_{j=1,\dots,m},\ (v(F_j(x)))_{j=1,\dots,m} \right)$$

when $x \in \mathbf{K}^{\mathrm{rc}}$: for x on any $(<, \preceq)$–interval I used in the proof of Theorem 1.4.4 we have $v(F_j(x)) = \mu_{I,j} + m_{I,j} v(t)$ where t is either $(x - x_h)/(x_{h+1} - x_h)$, or $(x_{h+1} - x)/(x_{h+1} - x_h)$, or $x_1 - x$ or $x - x_p$.

2.3 Solving the first problem

Algorithm RCVF1 solving Problem 1. Recall that (P,σ) is a code à la Thom for a root x of $P \in \mathbf{K}[X]$. We can assume w.l.o.g. that $P(0) \neq 0$, $x > 0$ (else replace P by $P(-X)$) and that P is monic. Let $(x_i)_{i=1,\dots,d}$ be the roots of P in $\mathbf{K}^{\mathrm{ac}}$. Using the Newton Polygon algorithm, we compute the multiset $[\, v(x_i) \mid i = 1,\dots,n\,]$. So we can express the set of valuations $v(x_i)$ as $(v(c_j)/n_j)_{j=1,\dots,r}$ for some r-tuple $(c_j,n_j)_{j=1,\dots,r}$ with $c_j > 0$ in $\mathbf{K}$, $n_j \in \mathbb{N}$ and $v(c_j)/n_j < v(c_{j+1})/n_{j+1}$ for $j = 1,\dots,r-1$.
Consider the LCM n of denominators n_j and "replace each x_i by $z_i = x_i^n$": i.e., compute $Q(X) = \prod_i (X - z_i)$ and compute a code à la Thom (Q,σ') for $z = x^n$. Let $b_j = c_j^{n/n_j}$. Then $v(b_j) = (n/n_j)v(c_j)$ for $j = 1,\dots,r$ and

$$v(b_1) < \cdots < v(b_r).$$

So we have also

$$b_1 > \cdots > b_r > 0.$$

By rational computations in $(\mathbf{K},\mathbf{P})$ we can settle one of the three following inequalities in $\mathbf{K}^{\mathrm{rc}}$

$$\begin{array}{ll} & z \geq b_1, \\ b_j \geq z \geq b_{j+1} & \text{with some } j \in \{1,\dots,r-1\}, \\ & b_r \geq z > 0. \end{array}$$

In the first case we conclude that $v(z) = v(b_1)$. In the last case $v(z) = v(b_r)$. In the remaining case we know that

$$v(b_j) \leq v(z) \leq v(b_{j+1}) \qquad \text{so} \quad v(z) = v(b_j) \quad \text{or} \quad v(z) = v(b_{j+1}).$$

We have to find the exact valuation. Consider $c \in \mathbf{P}$ verifying

$$\begin{aligned} 0 < v(c) \leq \min\left(v\left(\frac{b_j}{b_{j-1}}\right), v\left(\frac{b_{j+1}}{b_j}\right)\right) \quad & \text{if } j > 1 \\ 0 < v(c) = v\left(\frac{b_2}{b_1}\right) \quad & \text{if } j = 1 \end{aligned}$$

(if $j > 1$, c can be chosen as b_j/b_{j-1} or b_{j+1}/b_j). Next consider the linear fractional change of variable

$$y \longmapsto \varphi(y) = \frac{y}{1 + cy^2}$$

We have
— If $v(y) \geq 0$ then $v(\varphi(y)) = v(y)$.
— If $v(y) \leq -v(c)$ then, letting $y' = 1/y$ we get

$$v(y') \geq v(c) > 0,\ \varphi(y) = \frac{y'}{c + y'^2} \quad \text{and} \quad v(\varphi(y)) = v(y') - v(c) \geq 0.$$

So the monic polynomial

$$R(Y) = \prod_i \left(Y - \varphi\left(\frac{z_i}{b_j}\right)\right)$$

has coefficients in $\mathbf{V}$. Moreover $v(z/b_j) \geq 0$, so $\varphi(z/b_j)$ is a unit iff $v(b_j) = v(z)$ since $v(\varphi(z/b_j)) = v(z/b_j)$.

We can compute a code à la Thom (R, σ'') for $\varphi(z/b_j)$. This gives a code à la Thom $(\overline{R}, \sigma'')$ for $\overline{\varphi(z/b_j)}$ (i.e., $\varphi(z/b_j)$ considered as an element of $\overline{\mathbf{K}}^{\mathrm{rc}}$). Finally we test whether this code is verified by $\overline{0}$ (which is a root of $\overline{R}$). In case of negative answer then $v(z) = v(b_j)$. Otherwise $v(z) = v(b_{j+1})$. ∎

Remarks 2.3.1

1) In a more explicit view, we should ask for computing two nonnegative elements a and b of $\mathbf{K}$ and an integer n such that $a \leq |x|^n \leq b$ and $v(a) = v(b)$.

*2) Clearly algorithm **RCVF1** allows us to run sure computations inside $(\mathbf{K}^{\mathrm{rc}}, \mathbf{V}^{\mathrm{rc}}, \mathbf{P}^{\mathrm{rc}})$ when we know how to compute inside $(\mathbf{K}, \mathbf{V}, \mathbf{P})$.*

2.4 Solving the second problem

First we recall the Cohen-Hörmander algorithm for ordered fields (see e.g., [1] chapter 1).

Definition 2.4.1 *Let $(\mathbf{K}, \mathbf{P})$ be an ordered field and (F_j) a finite family of univariate polynomials in $\mathbf{K}[X]$. A* complete tableau of signs for the family (F_j) *is the following* discrete data *T:*

- *The ordered list $(x_k)_{k=1,\ldots,r}$ of all the roots of all the F_j's in $\mathbf{K}^{\mathrm{rc}}$.*
- *The signs ($\in \{-1, 0, +1\}$) of all the F_j's at all the x_k's.*
- *The signs of all the F_j's in each interval $]-\infty, x_1[$, $]x_k, x_{k+1}[$ $(1 \leq k \leq r-1)$ and $]x_r, +\infty[$.*

We call an x_k a point of the tableau T. *Similarly an interval $]-\infty, x_1[$ or $]x_k, x_{k+1}[$ or $]x_r, +\infty[$ is called* an interval of the tableau T.

In this tableau x_k is merely a name for the corresponding root, it may be coded by the number k or in another way.

Proposition 2.4.2 (Cohen-Hörmander's algorithm for computing the complete tableau of signs for a finite family of univariate polynomials) *Let $(\mathbf{K}, \mathbf{P})$ be an ordered subfield of a real closed field $(\mathbf{R}, \mathbf{P}_{\mathbf{R}})$. Let $L = (F_1, \ldots, F_k)$ be a list of polynomials in $\mathbf{K}[Y]$. Let L' be the family of polynomials generated by the elements of L and by the operations $P \mapsto P'$ and $(P, Q) \mapsto \mathrm{Rem}(P, Q)$ for $\deg(P) \geq \deg(Q) \geq 1$. Then L' is finite and one can compute the complete tableau of signs for L' in terms of the following data:*

- *the degree of each polynomial in the family L',*
- *the diagrams of operations $P \mapsto P'$ and $(P, Q) \mapsto \mathrm{Rem}(P, Q)$,*
- *the signs of constants $\in L'$.*

L et us remark that in this algorithm the zero polynomial can appear in L' as a remainder $\mathrm{Rem}(P, Q)$ where $\deg(P) \geq \deg(Q) \geq 1$. The degree of the zero polynomial is -1.

The list L' is finite: one makes systematically the operation "derivation of every previously obtained polynomial" and "remainders of all previously obtained couple of polynomials", and one gets a finite family at the end since degrees are decreasing.

Let us number the polynomials in L' with an order compatible with the order on the degrees. Let L'_m be the subfamily of L' made of polynomials numbered from 1 to m. This

family is obviously stable under the operations "derivation" and "remainder by a division" which decrease strictly the degrees. Denote lastly by T_m the corresponding complete tableau of signs.

We are going to prove, by induction on m, that the complete tableau of signs of the polynomials in the family L'_m can be obtained by using only the authorized informations. As long as polynomials are of degree 0, this is clear. Suppose it is true up to m. Let P be the polynomial of number $m+1$ in L'. On each interval of T_m, the polynomial P is strictly monotonic. Every point a of T_m is either $+\infty$, or $-\infty$, or a root of a certain polynomial Q with number $\leq m$, and in this case, if $R = \mathrm{Rem}(P, Q)$, we have $P(a) = R(a)$. The sign of $P(a)$ is hence known in every case from the authorized informations. This allows us to know on which open intervals of T_m the polynomial P has a root in $\mathbf{R}$. Let x be such a root of P on one of these open intervals $I =]a, b[$. If Q is a polynomial of number $\leq m$ in P, its sign on the interval I is known. This means we know its sign at the point x, and on intervals $]a, x[$ and $]x, b[$. With respect to P, its signs on $]a, x[$ and on $]x, b[$ are also known since P is strictly monotonic on the interval. The complete tableau of signs for L'_{m+1} is thus known from the authorized informations and the complete tableau of signs for L'_m. □

In this algorithm we remark that each zero of the tableau is obtained with a Thom's encoding.

An extension of previous algorithm will solve Problem 2. First we give a valued version for the complete tableau of signs.

Definition 2.4.3 *Let* $(\mathbf{K}, \mathbf{V}, \mathbf{P})$ *be an ordered valued field and* $(F_j)_{j\in J}$ *a finite family of univariate polynomials in* $\mathbf{K}[X]$. *A* complete tableau of vsc's for the family (F_j) *is the following data* T*:*

- *The ordered list* $(x_k)_{k=1,\dots,r}$ *of all the roots of all the* F_j*'s in* $\mathbf{K}^{\mathrm{rc}}$.
- *The complete tableau of signs for the family* $(F_j)_{j\in J}$.
- *All the valuations* $v(x_{k+1} - x_k)$ $(k = 1, \dots, r-1)$.
- *All the valuations* $v(F_j(x_k))$ $(j \in J,\ k = 1, \dots, r)$.

Algorithm RCVF2 solving Problem 2. A first possibility is to use algorithm **RCVF1**. We think that it is interesting to indicate another possibility which goes in the same spirit as the Cohen-Hörmander algorithm for ordered fields. This gives us also simple proofs for theorems in sections 3 and 4. Call (P_j) the list L' in Proposition 2.4.2. Call $(x_{m,k})_{k=1,\dots,r_m}$ the ordered list of all roots of $L'_m = (P_j)_{j=1,\dots,m}$. We replace in the proof of Proposition 2.4.2 the complete tableau of signs T_m of L' by $S_m = T_m \cup V_m$ where V_m collects the valuations $v(P_j(x_{m,k}))$ $(j \in \{1, \dots, m\},\ k \in \{1, \dots, r_m\})$ and $v(x_{m,k+1} - x_{m,k})$ $(k \in \{1, \dots, r_m - 1\}.)$

Suppose we have done the job up to m. Let $P = P_{m+1}$ be the polynomial of index $m+1$ in L'. The tableau T_{m+1} is computed as in Proposition 2.4.2. It remains to compute missing informations in V_{m+1}.

At every root $a = x_{m,k}$ of a polynomial $Q = P_\ell$ with index $\ell \leq m$, if $R = \mathrm{Rem}(P, Q)$, we have $P(a) = R(a)$ and R is in L'_m, so the valuation $v(P(a))$ is known from V_m.

Let $x = a + t_1(b-a)$ be a root of P on an open interval $I =]x_{m,k}, x_{m,k+1}[=]a, b[$ of T_m. In order to compute all the $v(P_j(x))_{j=1,\dots,m}$ it is sufficient to compute $v(t_1) = \tau_1$ and $v(t_2) = \tau_2$ $(t_2 = 1 - t_1)$: Theorem 1.3.6 says us how to get the valuations $v(P_j(x))_{j=1,\dots,m}$ from V_m, τ_1 and τ_2.

In order to compute $\tau_1 = v(t_1)$ we use a GTF that expresses $P(x) = P(a+t_1(b-a)) = 0$ as

$$P(a) + t_1 \cdot \left(\sum_{j=1}^{d} \epsilon_j \cdot e^j \cdot G_{j,\varepsilon}(t_1, t_2) \cdot P^{[j]}(a_j) \right) \qquad (a_j = a \text{ or } b)$$

where $e = b - a$, $t_1 \cdot G_{j,\varepsilon}(t_1, t_2) = H_{j,\varepsilon}(t_1, t_2)$ and

$$\operatorname{sign}(\epsilon_j P^{[j]}(a_j)) = \operatorname{sign}(-P(a)) \ \ (1 \le j \le d).$$

Moreover, the valuations $v(P(a) = \nu$, $v(P^{[j]}(a_j)) = \nu_j$ and $\delta = v(b-a)$ are known. From the properties of $H_{j,\varepsilon}$, we know that $G_{j,\varepsilon}(t_1, t_2)$ is a unit if $\tau_1 = 0$, so its valuation in $\Gamma_{\mathbf{K}}^{dh} \cup \{+\infty\}$ depends only on τ_1. So we get

$$v(P(a)) = \nu = \min(\nu_1 + \delta + \tau_1,\ \nu_2 + 2\delta + k_2\tau_1, \ldots, \nu_d + d\delta + k_d\tau_1)$$

($\tau_1 \ge 0$, and some ν_k's may be infinite). The right hand side is an increasing piecewise linear function of τ_1 so we have a unique and explicit solution τ_1. With $\mu_i = \nu_i + i\delta$ we precisely get

$$\tau_1 = \max\left(\nu - \mu_1, \frac{\nu - \mu_2}{k_2}, \ldots, \frac{\nu - \mu_d}{k_d}\right).$$

Finally τ_2 is computed analogously and we can fill up V_{m+1}.

Remark also that if x is on the last interval $]x_{m,r_m}, +\infty[=]a, +\infty[$ of T_m, we can compute $v(x-a)$ in a similar way by using the usual Taylor formula. ∎

Definition 2.4.4 *In an additive divisible ordered group G we consider terms built from variables α_j by $\mathbb{Q}$-linear combinations and by using the operations* min *and* max. *We call such a term a* $\mathbb{Q}$-semilinear term. *The function defined by such a term is called a* $\mathbb{Q}$-semilinear function of the α_j's.

We get the following theorem, similar to Proposition 2.4.2.

Theorem 2.4.5 (An algorithm à la Cohen-Hörmander for computing the complete tableau of vsc's for a finite family of univariate polynomials) *Let $(\mathbf{K}, \mathbf{V}, \mathbf{P})$ be an ordered valued subfield of a real closed valued field $(\mathbf{R}, \mathbf{V_R}, \mathbf{P_R})$. Let $L = (F_1, \ldots, F_k)$ be a list of polynomials in $\mathbf{K}[Y]$. Let L' be the (finite) family of polynomials generated by the elements of L and by the operations $P \mapsto P'$ and $(P, Q) \mapsto \operatorname{Rem}(P, Q)$ for $\deg(P) \ge \deg(Q) \ge 1$. Call (c_j) the list of constants $\in L'$.*

Then one can compute the complete tableau of vsc's for L' in terms of the following data:

- *the degree of each polynomial in the family,*
- *the diagrams of operations $P \mapsto P'$ and $(P, Q) \mapsto \operatorname{Rem}(P, Q)$ in L',*
- *the signs* $\operatorname{sign}(c_j)$,
- *the valuations $v(c_j)$.*

Moreover, all the valuations $v(x_{k+1} - x_k)$ and all the valuations $v(P_j(x_k))$ are given as fixed $\mathbb{Q}$-semilinear functions of the $v(c_j)$'s: each such $\mathbb{Q}$-semilinear function is a fixed $\mathbb{Q}$-semilinear term (in the "variables" $v(c_j)$'s) that depends only on the complete tableau of signs of L'.

T his theorem is an extension of Proposition 2.4.2. The proof is similar. In fact we get all results by a close inspection of Algorithm **RCVF2**. □

2.5 Solving the third problem

Algorithm RCVF3 solving Problem 3. We run Algorithm **RCVF2** and we apply Theorem 1.3.6: see Remark 2.2.2. ∎

Definition 2.5.1 *Let $(F_j)_{j\in J}$ be a finite family of univariate polynomials in $\mathbf{K}[X]$ (where $(\mathbf{K}, \mathbf{V}, \mathbf{P})$ is an ordered valued field). We assume the family to be stable under derivation. Let M be a positive integer.*

An M-complete tableau of vsc's for the family (F_j) *is the following* discrete data T*:*

- *The ordered list $(x_k)_{k=1,\dots,r}$ of all the roots of all the F_j's in $\mathbf{K}^{\mathrm{rc}}$.*
- *For each $k = 1, \dots, r$, the M-complete system of vsc's (see Definition 1.4.1) for the family $(F_j(x_k))_{j\in J}$.*
- *For each $k = 1, \dots, r-1$*
  - *The M-complete system of vsc's for the family $(F_j(x))_{j\in J}$ for $x \in \mathbb{J}(x_k, x_{k+1})$.*
  - *A partition of $\mathbb{J}^+(x_k, x_{k+1}, 0, \infty)$ as a finite union of $2n_k + 1$ $(<, \preceq)$–intervals*

$$\bigcup_{i=0,n_k} \mathbb{J}^+(x_k, x_{k+1}, \alpha_{k,i}, \alpha_{k,i+1}) \ \cup \ \bigcup_{i=1,n_k} \mathbb{J}^+(x_k, x_{k+1}, \alpha_{k,i}),$$

  (where $\alpha_{k,0} = 0$ and $\alpha_{k,n_k+1} = \infty$) and for each $(<, \preceq)$–interval A of this partition, the M-complete system of vsc's for the family $(F_j(x))_{j\in J}$ which is the same one for any $x \in A$.
  - *A similar data concerning $\mathbb{J}^-(x_k, x_{k+1}, 0, \infty)$.*
- *Similar data concerning $\mathbb{I}^-(x_1, -\infty, \infty)$ and $\mathbb{I}^+(x_r, -\infty, \infty)$.*

In this tableau the $\alpha_{k,i}$'s $(0 < \alpha_{k,1} < \cdots < \alpha_{k,n_k} < \infty)$ are purely formal and n_k is the only relevant information concerning $\alpha_{k,1}, \dots, \alpha_{k,n_k}$.

We now state a result that precises the output of Algorithm **RCVF3**.

Theorem 2.5.2 (An algorithm à la Cohen-Hörmander for computing an M-complete tableau of vsc's for a finite family of univariate polynomials)
Let $(\mathbf{K}, \mathbf{V}, \mathbf{P})$ be an ordered valued subfield of a real closed valued field $(\mathbf{R}, \mathbf{V_R}, \mathbf{P_R})$. Let M be a positive integer. Let $L = (F_1, \dots, F_k)$ be a list of polynomials in $\mathbf{K}[Y]$. Let L' be the family of polynomials generated by the elements of L and by the operations $P \mapsto P'$ and $(P, Q) \mapsto \mathrm{Rem}(P, Q)$ for $\deg(P) \geq \deg(Q) \geq 1$. Call (c_j) the list of constants $\in L'$.

Then one can compute the M-complete tableau of vsc's for L' in terms of the following data:

- *the degree of each polynomial in the family,*
- *the diagrams of operations $P \mapsto P'$ and $(P, Q) \mapsto \mathrm{Rem}(P, Q)$ in L',*
- *the N-complete system of vsc's for the family (c_j),*

where N is an integer depending only on M and on the list of degrees in L.

3 Quantifier elimination algorithms

3.1 Parametrized computations

Algorithms **RCVF2** and **RCVF3** are uniform: they can be run when coefficients in the initial data are polynomials in other variables which are called *parameters* (instead of being in the base field).

A case by case discussion appears, and the straight-line algorithm is replaced by a branching one.

We describe this situation as a *parametrized algorithm* dealing with parametrized univariate polynomials.

Theorem 3.1.1 (parametrized version of Theorem 2.4.5) *Let* $(\mathbf{K}, \mathbf{V}, \mathbf{P})$ *be an ordered valued subfield of a real closed valued field* $(\mathbf{R}, \mathbf{V_R}, \mathbf{P_R})$. *Let* $L = (F_1, \ldots, F_k)$ *be a list of parametrized univariate polynomials of degrees* $d_1, \ldots, d_k$ *in some variable* X. *Let us run the algorithm* ***RCVF2*** *and let us open two branches in the computation any time we have to know if a given element is zero or nonzero when computing a remainder. Moreover, replace remainders by pseudoremainders in order to avoid denominators.*

Consider the family (c_j) *of all "constants" in all* L'*'s that appear at the leaves of the tree (these constants are* $\mathbf{K}$*–polynomials in the parameters).*

Finally consider that the computed valuations $v(x_{k+1} - x_k)$ *and* $v(P_j(x_k))$ *at any leave of the tree are given as* $\mathbb{Q}$*-semilinear functions of the "variables"* $v(c_j)$*'s.*

Then this global parametrized algorithm is finite and therefore gives a finite number of possibilities for its output: the complete tableau of vsc's for L.

More precisely when the signs of the "constants" c_j*'s are known, the complete tableau of signs is known and all the valuations* $v(x_{k+1} - x_k)$ *and* $v(P_j(x_k))$ *are given as explicit* $\mathbb{Q}$*-semilinear functions in the "variables"* $v(c_j)$*'s.*

T he proof of Proposition 2.4.2 (Cohen-Hörmander algorithm) works as well in the parametrized case. In each branch so created, the proof of Theorem 2.4.5 works as well. □

Remarks 3.1.2

1) An important case is obtained when all coefficients of the F_i*'s are independent parameters and* $(\mathbf{K}, \mathbf{V}, \mathbf{P}) = (\mathbb{Q}, \mathbb{Q}, \mathbb{Q}^{\geq 0})$. *This "generic case" gives the complete description of all situations occurring with a fixed number of polynomials of known degrees.*

2) Another interesting particular case is the following one, with only one parameter subject to certain constraints. We start with a list of polynomials $L = (F_1, \ldots, F_k)$ *in* $\mathbf{K}[Y]^n$, *we get an extended list* L' *and the complete tableau of signs. Let* a *and* b *be two consecutive roots in this tableau. Now we want to make computations with an element* x *of the interval* $]a, b[$. *Consider* x *as a parameter verifying some sign constraints, namely the Thom's sign conditions that define* $]a, b[$. *We add the polynomial* $Y - x$ *to* L *and we run the parametrized version of* ***RCVF2****. Only one root is added:* x. *The new polynomials appearing are only "constants" of the form* $Q(x)$ *(where* Q *is in* L'*). The process go on only trough one branch. We get the following result: the valuations* $v(x - a)$ *and* $v(b - x)$ *are given as* $\mathbb{Q}$*-semilinear functions of some* $v(Q(x))$*'s. From this we also get a similar result concerning* $v(x - x_j)$ *where* x_j *is any root in the tableau. Naturally, there is also a parametrized version for this result.*

Similarly we have a parametrized version of Theorem 2.5.2.

Theorem 3.1.3 (parametrized version of Theorem 2.5.2)
*Let $L = (F_1, \ldots, F_k)$ be a list of parametrized univariate polynomials of degrees $d_1, \ldots, d_k$ in some variable X. Let M be a positive integer. Let us run the algorithm **RCVF2** and let us open two branches in the computation any time we have to know if a given element is zero or nonzero when computing a remainder. Moreover, replace remainders by pseudoremainders in order to avoid denominators. Let us call (c_j) the family of all "constants" in all L''s that appear at the leaves of the tree (these constants are $\mathbf{K}$–polynomials in the parameters).*

*Finally when applying Theorem 1.3.6 in order to get the output of **RCVF3** from the one of **RCVF2**, we open three branches any time we have to know the sign of some $\mathbb{Z}$-linear combination of $v(c_j)$'s.*

Then this global parametrized algorithm is finite and therefore gives a finite number of possibilities for its output: the M-complete tableau of vsc's for L.

Moreover, these outputs depend on the following data:

- *the signs of the "constants" c_j's,*
- *the sign test inside a finite subset of the subgroup generated by the $v(c_j)$'s; which are exactly divisibility tests between monomials in the c_j's).*

Remark 3.1.4 *Since the computation in the previous theorem is purely formal, certain systems of conditions corresponding to the data given by the two last items may be impossible. If we want to know what are these impossible systems, we have to use the quantifier elimination algorithm given in Theorem 3.2.2. Nevertheless, one can verify that there is no circular argument.*

3.2 Quantifier elimination

We now give some corollaries of previous computations for quantifier elimination. We recall that these results are well known, see e.g., [2].

We consider the first order theory of real closed valued fields based on the language of ordered fields $(0, 1, +, -, \times, =, \leq)$ to which we add the predicate $x \preceq y$. So, all constants and variables represent elements in $\mathbf{K}$ (this corresponds to our previously explained computability assumptions).

Here is a corollary of Theorem 3.1.3.

Theorem 3.2.1 *Let $\Phi(\underline{a}, \underline{x})$ be a quantifier free formula in the first order theory of real closed valued fields. We view the a_i's as parameters and the x_j's as variables. Then one can give a quantifier free formula $\Psi(\underline{a})$ such that the two formulae $\exists \underline{x}\ \Phi(\underline{a}, \underline{x})$ and $\Psi(\underline{a})$ are equivalent in the formal theory. (The terms appearing in the formulae Φ and Ψ are $\mathbb{Z}$–polynomials in the parameters, and, in the case of Φ, also in the variables.)*

U se recursively Theorem 3.1.3 and eliminate the x_j's one after the other. □

We also get the following corollary.

Theorem 3.2.2 *Let $(\mathbf{K}, \mathbf{V}, \mathbf{P})$ be an ordered valued subfield of a real closed valued field $(\mathbf{R}, \mathbf{V_R}, \mathbf{P_R})$. Assume that the sign test and the divisibility test are explicit inside $(\mathbf{K}, \mathbf{V}, \mathbf{P})$. Then there is a uniform quantifier elimination algorithm for the first order theory of real closed valued fields extending $(\mathbf{K}, \mathbf{V}, \mathbf{P})$.*

3.3 An abstract form of quantifier elimination

An abstract form of Theorem 3.1.3 is the following theorem, that was given the first time by M.J. De la Puente in [9].

First, we need some definitions of the abstract objects.

Definition 3.3.1 *Let us denote the* real-valuative spectrum *of a commutative ring A by* Sperv$A$*: an element of* Sperv$A$ *is given by a ring homomorphism φ from A to a real closed valued field K, and two such homomorphisms φ, φ' define the same element of* Sperv$A$ *iff there exists an isomorphism of ordered valued fields $\psi : R \to R'$ such that $\psi \circ \varphi = \varphi'$, where R and R' are the real closed valued fields generated by $\varphi(A)$ and $\varphi'(A)$. Alternatively, an element of* Sperv$A$ *is given by a prime ideal Q of A and a structure of ordered valued field upon the fraction field of A/Q. A* constructible subset *of* Sperv$A$ *is by definition a boolean combination of* elementary constructible subsets $U_x := \{\varphi \in \text{Sperv}A \ : \ \varphi(x) > 0\}$ *and* $V_{x,y} := \{\varphi \in \text{Sperv}A \ : \ \varphi(x) \preceq \varphi(y)\}$*, where $x, y \in A$.*

Theorem 3.3.2 *The canonical mapping from* Sperv$A[X]$ *to* Sperv$A$ *transforms any $(\leq, \preceq)$–constructible subset into a $(\leq, \preceq)$–constructible subset.*

A $(\leq, \preceq)$–constructible subset in Sperv(B) is a finite union of basic $(\leq, \preceq)$–constructible subsets, that are defined as

$$\{\varphi \in \text{Sperv}(B) \ : \\ \bigwedge_i \varphi(a_i) = 0 \wedge \bigwedge_j \varphi(b_j) > 0 \wedge \bigwedge_k v(\varphi(c_k)) = v(\varphi(d_k)) \wedge \bigwedge_\ell v(\varphi(e_\ell)) > v(\varphi(f_\ell))\Big\}$$

where conjunctions are finite and all elements are in B. Searching the canonical image of a basic constructible subset S of Sperv$A[X]$ (defined by elements $a_i, b_j, c_k, d_k, e_\ell, f_\ell$ in $A[X]$) inside Sperv$A$, is the same thing that analyzing the conditions on the coefficients of the polynomials $a_i, b_j, c_k, d_k, e_\ell, f_\ell$ allowing the existence of an x where the defining conditions of S are verified. So Theorem 3.1.3 gives the answer. □

Another consequence of Theorem 3.1.3 is a *relativized version* of Theorem 3.3.2. This generalization is obtained by giving some *constraints* on the ring homomorphism φ from A to a real closed valued field K. We give e.g., a subring B of A, an ideal M of B, a multiplicative monoid S in A and a semi ring P in A ($P + P \subseteq P$, $P \times P \subseteq P$). We want to allow only homomorphisms ϕ (from A or $A[X]$ to a real closed valued field) verifying that $\phi(B)$ is in the valuation ring, $\phi(M)$ is in the maximal ideal, elements of $\phi(S)$ are nonzero and elements of $\phi(P)$ are nonnegative. If we write C the constraints (B, M, S, P) and if we write Sperv(A, C) the part of Sperv$A$ satisfying the constraints, we get: the canonical mapping from Sperv$(A[X], C)$ to Sperv(A, C) transforms any $(\leq, \preceq)$–constructible subset in a $(\leq, \preceq)$–constructible subset.

In [9] the relativized version is settled with one constraint B.

4 Constructible subsets in the real valuative affine space

4.1 Tarski-Seidenberg-Chevalley

We now give a geometric form for Theorems 3.1.3 and 3.2.2.

Theorem 4.1.1 *Let $(\mathbf{K}, \mathbf{V}, \mathbf{P})$ be an ordered valued subfield of a real closed valued field $(\mathbf{R}, \mathbf{V_R}, \mathbf{P_R})$. Let π the canonical projection from $\mathbf{R}^{n+r}$ onto $\mathbf{R}^n$. Let $S \subseteq \mathbf{R}^{n+r}$ be any $(\leq, \preceq)$–constructible set defined over $(\mathbf{K}, \mathbf{V}, \mathbf{P})$. Assume that the sign test and the divisibility test*

are explicit inside the ring generated by the coefficients of the polynomials that appear in the definition of S. Then a description of the projection $\pi(S) \subseteq \mathbf{R}^n$ can be computed in a uniform way by an algorithm that uses only rational computations, sign tests and divisibility tests.

In particular, the complexity of a description of $\pi(S)$ is explicitly bounded in terms of the complexity of a description of S.

Here *rational computations* mean computations in the ring generated by the coefficients of the polynomials occurring in the description of S. A *description of S* is a quantifier free formula in disjunctive normal form describing S. The *complexity* of such a description of S can be defined as a 5-tuple (n, d, k, ℓ, m) where n is the number of variables, d is the maximum of the degrees, k is the number of polynomials, ℓ is the number of $\vee$ and m is the bound for the numbers of $\wedge$ inside a disjunct.

Corollary 4.1.2 *Let $(\mathbf{K}, \mathbf{V}, \mathbf{P})$ be an ordered valued subfield of a real closed valued field $(\mathbf{R}, \mathbf{V_R}, \mathbf{P_R})$. Let $S \subseteq \mathbf{R}^n$ be a $(\leq, \preceq)$–constructible set and let $f : S \to \mathbf{R}^p$ be a $(\leq, \preceq)$–constructible map.*

- *The interior and the adherence of S inside $\mathbf{R}^n$ for the order topology are $(\leq, \preceq)$–constructible sets.*
- *$f(S) \subseteq \mathbf{R}^p$ is a $(\leq, \preceq)$–constructible set.*
- *Let T be a $(\leq, \preceq)$–constructible set containing $f(S)$ and let $g : T \to \mathbf{R}^q$ be a $(\leq, \preceq)$–constructible map. Then $g \circ f$ is a $(\leq, \preceq)$–constructible map.*
- *Let $T' \subseteq \mathbf{R}^p$ be a $(\leq, \preceq)$–constructible set. Then $f^{-1}(T') \subseteq \mathbf{R}^n$ is a $(\leq, \preceq)$–constructible set.*

4.2 Stratifications and applications

We think that the results of this section could allow to get most of the results obtained by Frank Mausz in his Doctoral dissertation [8] with a different approach.

Łojaziewicz stratification à la Cohen-Hörmander

We recall here a result about stratifying families ([1] chapter 9).

Definition and notation 4.2.1 *Consider a general monic polynomial of degree d as a point of $\mathbf{R}^d$. Let $\sigma = (\sigma_1, \ldots, \sigma_d) \in \{-1, +1\}^d$. Let*

$$U_\sigma = \left\{ P \in \mathbf{R}^d \ : \ \exists x \in \mathbf{R} \ \left(P(x) = 0 \ \wedge \ \bigwedge_{i=1}^{d} \operatorname{sign}(P^{(i)}(x)) = \sigma_i \right) \right\}.$$

It is easily seen that U_σ is a connected open semialgebraic subset of $\mathbf{R}^d$ (see e.g., [5]) and that

$$\overline{U_\sigma} = \left\{ P \in \mathbf{R}^d \ : \ \exists x \in \mathbf{R} \ \left(P(x) = 0 \ \wedge \ \bigwedge_{i=1}^{d} \operatorname{sign}(P^{(i)}(x)) \in \{\sigma_i, 0\} \right) \right\}.$$

For $P \in U_\sigma$ we call $\rho_\sigma(P)$ the zero which is coded à la Thom by (P, σ). Then $P \mapsto \rho_\sigma(P)$ is Nash on U_σ and admits a continuous semialgebraic extension on $\overline{U_\sigma}$, that we note also by ρ_σ. Such a function will be called a Thom's root function*, or simply a* root function.

More generally, if $\varphi : \mathbf{R}^{k-1} \to \mathbf{R}^d$ is a polynomial function, we can consider $\rho_\sigma \circ \varphi$ as defined over $\varphi^{-1}(\overline{U_\sigma})$. We also call such a function a root function*. This function is Nash*

over $\varphi^{-1}(U_\sigma)$. If $f(x_1,\dots,x_k)=\varphi(x_1,\dots,x_{k-1})(x_k)$ is the corresponding monic polynomial in k variables, we denote $\rho_\sigma\circ\varphi$ by $\rho_\sigma(f)$.

Finally if a polynomial $g\in\mathbf{K}[x_1,\dots,x_k]=\mathbf{K}[x_1,\dots,x_{k-1}][x_k]$ has a leading coefficient w.r.t. x_k which is a nonzero element c of $\mathbf{K}$, we say that g is quasi monic in x_k, *and we let $\rho_\sigma(g)=\rho_\sigma(g/c)$.*

For more details about root functions see [5].

Theorem 4.2.2 *([1] chap. 9) Let $(\mathbf{K},\mathbf{P})$ be an ordered subfield of a real closed field $(\mathbf{R},\mathbf{P_R})$. Let $g_1,\dots,g_s$ be nonzero polynomials in $\mathbf{K}[x_1,\dots,x_n]$. After a suitable linear change of variables there exists a family of polynomials*

$$(f_{i,j})_{i=1,\dots,n;j=1,\dots,\ell_i}$$

with the following properties (we will continue denoting the new variables by x_i).

(1) *First we have*

- $(g_1,\dots,g_s)\subseteq(f_{n,j})_{j=1,\dots,\ell_n}$
- *Each $f_{k,j}$ is a nonzero polynomial in $\mathbf{K}[x_1,\dots,x_k]$ which is quasimonic in x_k.*
- *For each index k the family $(f_{k,j})_{j=1,\dots,\ell_k}$ is stable under derivation w.r.t. x_k (excluding the zero derivative).*

(2) *Let us denote $I_k=\{(i,j)\ :\ i=1,\dots,k;j=1,\dots,\ell_i\}$. Call $\mathcal{C}_k$ the family of nonempty semialgebraic subsets of $\mathbf{R}^k$ that can be defined as some*

$$C_\varepsilon=\left\{(\xi_1,\dots,\xi_k)\in\mathbf{R}^k\ ;\ \bigwedge_{(i,j)\in I_k}\operatorname{sign}(f_{i,j}(\xi_1,\dots,\xi_k))=\epsilon_{i,j}\right\}\neq\emptyset$$

(where $\varepsilon=(\epsilon_{i,j})_{(i,j)\in I_k}$ is any family in $\{-1,0,+1\}$). It is clear that the C_ε's in $\mathcal{C}_k$ give a partition of $\mathbf{R}^k$. We have

(a) *The canonical projection $\pi_k(C_\varepsilon)$ of any element $C_\varepsilon\in\mathcal{C}_k$ on $\mathbf{R}^{k-1}$ is an element of $\mathcal{C}_{k-1}$: it is obtained as $C_{\varepsilon'}$ where ε' is the restriction of the family ε to I_{k-1}.*

(b) *The adherence $\overline{C_\varepsilon}$ of C_ε (recall we assume $C_\varepsilon\neq\emptyset$) is a union of elements of $\mathcal{C}_k$, it is obtained by relaxing strict inequalities in the definition of C_ε.*

(c) *If in the definition of $C_\varepsilon\in\mathcal{C}_k$ there is one equality $f_{k,i}(\xi_1,\dots,\xi_k)=0$ then C_ε is the graph of a root function $\rho_\sigma(f_{k,j})$ (here $f_{k,j}$ is seen as a polynomial in x_k, it is equal to $f_{k,i}$ or to some $f_{k,i}^{(\ell)}$ and σ is extracted from ε) which is Nash over $\pi_k(C_\varepsilon)$. Moreover, $\rho_\sigma(f_{k,i})$ is defined over $\overline{\pi_k(C_\varepsilon)}$ and the graph of this root function is $\overline{C_\varepsilon}$.*

(d) *Call $\pi_{n,k}$ the canonical projection $\mathbf{R}^n\to\mathbf{R}^k$. Let E be a k dimensional semialgebraic subset of $\mathbf{R}^n$ defined from the polynomials $g_1,\dots,g_s$. Then for any $C_\varepsilon\in\mathcal{C}_n$ which is contained in E, $\pi_{n,k}$ maps homeomorphically $\overline{C_\varepsilon}$ on its image.*

Definition 4.2.3 *Such a change of variables together with such a family $(f_{i,j})$ will be called a* stratification *for $(g_1,\dots,g_s)$ and for any semialgebraic subset of $\mathbf{R}^n$ defined from this family. The family $(f_{i,j})_{i=1,\dots,n;j=1,\dots,\ell_i}$ will be called a* stratifying family *for the initial family $(g_1,\dots,g_s)$. The semialgebraic subsets C_ε are called the* strata of the stratification.

We shall precisely consider the following way of constructing a stratifying family, à la Cohen-Hörmander (it is the one suggested in [1].) First we make a linear change of variables in order to make $g_1, \dots, g_s$ quasi monic in the new variable x_n. We add all the derivatives of each g_i w.r.t. x_n. This gives us the family $(f_{n,j})_{j=1,\dots,\ell_n}$.

We apply Cohen-Hormander's algorithm to this family and we call $h_1, \dots, h_\ell$ the "constants" given by this algorithm (these constants are polynomials in $(x_1, \dots, x_{n-1})$).

We make a new linear change of variables on $(x_1, \dots, x_{n-1})$ in order to make $h_1, \dots, h_\ell$ quasi monic in the new variable x_{n-1}. We make the same linear change of variables inside $(f_{n,j})_{j=1,\dots,\ell_n}$: this family remains quasimonic in x_n and stable under derivation w.r.t. x_n, and $h_1, \dots, h_\ell$ remain the "constants" given by the Cohen-Hormander's algorithm when applied to this family.

We add all the derivatives of each h_i w.r.t. x_{n-1}. This gives us the family $(f_{n-1,j})_{j=1,\dots,\ell_{n-1}}$. And so on.

With this kind of stratifying family, we can apply recursively Theorem 3.1.3. So we get a precise description of the variation of the valuations $v(f_{k,j}(x_1, \dots, x_k))$ when $(x_1, \dots, x_k) \in C_\varepsilon$ for any k and any $C_\varepsilon \in \mathcal{C}_k$. Let us see an example.

Example 4.2.4 *Assume $n = 3$. Consider a cell $C \in \mathcal{C}_3$. Assume that $C'' = \pi_{3,1}(C)$ is an interval $]a, b[$, that $C' = \pi_{3,2}(C)$ is the graph of a root function $h_1 = \rho_\sigma(f_{2,1})$ defined on $[a, b]$, and that C is the part of $C' \times \mathbf{R}$ between two root functions $h_2 = \rho_{\sigma'}(f_{3,1})$ and $h_3 = \rho_{\sigma''}(f_{3,2})$, so*

$$\begin{aligned} C &= \{(x, y, z) \,:\, a < x < b,\ y = h_1(x),\ h_2(x, y) < z < h_3(x, y)\} \\ &= \{(x, y, z) \,:\, a < x < b,\ y = h_1(x),\ h'_2(x) < z < h'_3(x)\}\,. \end{aligned}$$

We consider for $(x, y, z) \in C$, the parameters $t = (x - a)/(b - x)$, $\tau = v(t)$, $t' = (z - h'_2(x))/(h'_3(x) - z)$ and $\tau' = v(t')$. We get:

- *The map $h : (t, t') \mapsto (x, y, z) \in C$ is a Nash isomorphism from $(\mathbf{R}^+)^2$ onto C.*
- *For any $f_{k,j}$ in the stratifying family $v(f_{k,j}(x, y, z)) = \varphi_{k,j}(\tau, \tau')$ is a $\mathbb{Q}$-semilinear function of τ, τ' (here we use recursively Theorem 3.1.3).*
- *So, if we look at $C \cap S$ where S is any $(\leq, \preceq)$–constructible subset described from the $f_{k,j}$'s, we find that $C \cap S$ is a finite union of sets $h(L_i)$ where each L_i is defined as*

$$\left\{ (t, t') \in (\mathbf{R}^+)^2 \ :\ \bigwedge_\ell a_\ell(\tau, \tau') = \alpha_\ell \ \wedge \ \bigwedge_m b_m(\tau, \tau') > \beta_m \right\}$$

  where a_ℓ's and b_m's are $\mathbb{Z}$-linear forms and $\alpha_\ell,\ \beta_m \in \Gamma_{\mathbf{K}}^{dh}$.

- *Now we should like to have some rational expression of τ and τ' that uses only polynomials in (x, y, z). This is possible in the following way, as in Remark 3.1.2. Consider that the formal variables are X, Y, Z and that x, y, z are three parameters. Add to the list g_i the three polynomials $X - x$, $Y - y$, $Z - z$ and reconstruct the stratification, using the information that (x, y, z) is in the semialgebraic set C. You get that τ* and *τ'* are fixed $\mathbb{Q}$-semilinear functions in the $v(c_j)$'s and in some $v(F_j(x, y, z))$'s*: the c_j's are the old constants, and the $F_j(x, y, z)$ are the new "constants" that are constructed by the algorithm ($F_j(x, y, z) \in \mathbf{K}[x, y, z]$).*

The following "cell decomposition theorem" is merely the generalization of what we have seen on this example. It is obtained by applying Theorem 1.3.6 to a stratification à la Cohen-Hörmander. The last assertion is obtained as in Remark 3.1.2.

Theorem 4.2.5 (Cell decomposition theorem) *Let* $(\mathbf{K}, \mathbf{V}, \mathbf{P})$ *be an ordered valued subfield of a real closed valued field* $(\mathbf{R}, \mathbf{V_R}, \mathbf{P_R})$. *Let* $g_1, \ldots, g_s$ *be nonzero polynomials in* $\mathbf{K}[x_1, \ldots, x_n]$. *Consider a linear change of variables together with a family* $(f_{i,j})_{i=1,\ldots,n;j=1,\ldots,\ell_i}$ *that give a stratification for* $(g_1, \ldots, g_s)$. *Assume that this stratification is constructed à la Cohen-Hörmander, as explained above (after Definition 4.2.3). Consider any* k*-dimensional stratum* C_ε *corresponding to this stratification (see Theorem 4.2.2). Then there is a Nash isomorphism*

$$h : (\mathbf{R}^+)^k \longrightarrow C_\varepsilon, \quad (t_1, \ldots, t_k) \longmapsto h(t_1, \ldots, t_k)$$

with the following property.

If S *is any* $(\leq, \preceq)$*–constructible subset described from* $g_1, \ldots, g_s$, *then* $S \cap C_\varepsilon$ *is a finite union of cells* $h(L_i)$, *where each* L_i *can be defined as*

$$\left\{ (t_1, \ldots, t_k) \in (\mathbf{R}^+)^k \ : \ \bigwedge_\ell a_\ell(\tau) = \alpha_\ell \ \wedge \ \bigwedge_m b_m(\tau) > \beta_m \right\}$$

where $\tau = (\tau_1, \ldots, \tau_k) = (v(t_1), \ldots, v(t_k))$, *the* a_ℓ*'s and* b_m*'s are* $\mathbb{Z}$*-linear forms w.r.t.* τ, *and* $\alpha_\ell, \ \beta_m \in \Gamma_{\mathbf{K}}^{dh}$.

Moreover, each τ_i *is a* $\mathbb{Q}$*-semilinear function in some* $v(F_j(x_1, \ldots, x_n))$*'s (with* F_j*'s explicitly computable elements of* $\mathbf{K}[x_1, \ldots, x_n]$*).*

References

[1] Bochnak J., Coste M., Roy M.-F. *Géométrie algébrique réelle.* Springer-Verlag (1987). English version *Real Algebraic Geometry.* Springer-Verlag (1998) 4, 15, 22, 23, 24

[2] Cherlin, Dickmann M. A., *Real closed rings II. Model Theory.* Ann. of Pure and Applied Logic **25**, (1993) 213–231. 3, 20

[3] Cohen A., Cuypers H., Sterk H. (eds) *Some Tapas of Computer Algebra.* Springer Verlag (1999). 12

[4] Coste M., Roy M.-F. *Thom's Lemma, the coding of real algebraic numbers and the computation of the topology of semi-algebraic sets.* J. of Symbolic Computation **5** (1988), 121-129. 12

[5] González-Vega L., Lombardi H., Mahé L. *Virtual roots of real polynomials.* J. of Pure and Applied Algebra **124**, (1998) 147–166. 22, 23

[6] Lombardi H. *Une borne sur les degrés pour le Théorème des zéros réel effectif.* in: Real Algebraic Geometry. Lecture Notes in Math. n°1524. Eds.: Coste M., Mahé L., Roy M.-F.. Springer-Verlag, (1992), pp. 323–345. 6

[7] Lombardi H., Roy M.-F. *Constructive elementary theory of ordered fields.* in Effective Methods in Algebraic Geometry. Eds.: Mora T., Traverso C.. Birkhäuser. Basel. 1991. Progress in Math. n°94. pp. 249–262. 12

[8] Mausz F. *Definierbare Mengen über bewerteten reel abgeschlossenen Körpen*, Doctoral Dissertation, Univ. Köln, 1995. 22

[9] De la Puente M.J. *Specializations and a local homeomorphism theorem for real Riemann surfaces of rings.* Pacific J. of Math. **176** (2), (1996) 427–442. 21

[10] Warou H. *An algorithm and bounds for the real effective Nullstellensatz in one variable.* Progress in Math. n°143, Birkhäuser. Basel. 1996. pp. 373–387. 6

[11] Warou H. *Formules de Taylor Généralisées et applications.* Preprint Université de Niamey (1999). 6

Contents

Introduction **1**

1 Basic material **4**
1.1 The Newton Polygon 4
1.2 Generalized Tschirnhaus transformation 5
1.3 Generalized Taylor Formulas 5
1.4 Constructible subsets of the real line 9

2 Computing in the real closure of an ordered valued field **12**
2.1 Codes à la Thom and valuations in the value group 12
2.2 Three basic computational problems in the real closure of an ordered valued field 13
2.3 Solving the first problem 14
2.4 Solving the second problem 15
2.5 Solving the third problem 18

3 Quantifier elimination algorithms **19**
3.1 Parametrized computations 19
3.2 Quantifier elimination 20
3.3 An abstract form of quantifier elimination 21

4 Constructible subsets in the real valuative affine space **21**
4.1 Tarski-Seidenberg-Chevalley 21
4.2 Stratifications and applications 22