An Algorithm for Computing Analytic Branches of Space Curves at Singular Points

M.E.Alonso
T. Mora
G. Niesi
M. Raimondo*

Introduction

We discuss an algorithmical approach to the problem of authomatic parametrization of a curve in n-dimensional space, which is defined by implicit polynomial equations. The focus of our interest is the structure of the curve near singular points.

Let us be given a curve $\Gamma \subset \mathbf{C}^n$ defined by s polynomials $P_1, \ldots, P_s$ in $\mathbf{C}[X_1, \ldots, X_n]$ and let $(\alpha_1, \ldots, \alpha_n) \in \Gamma$ be a singular point of the curve. We assume that Γ is not contained in the hyperplane $X_1 - \alpha_1 = 0$; there is no loss of generality in doing this, since otherwise by the substitution $X_1 = \alpha_1$ in $P_1, \ldots, P_s$ we can reduce to a problem in one variable less.

It is then known that the analytic branches of Γ have a parametrization:

$$X_1 - \alpha_1 = t^{a_1}, X_2 - \alpha_2 = f_2(t), \ldots, X_n - \alpha_n = f_n(t)$$

with $a_1 \in \mathbf{N} - \{0\}, f_2, \ldots, f_n$ non-invertible power series in $\mathbf{C}[[t]]$. Our aim is to explicitly "compute" such parametrizations.

More exactly for each analytic branch we intend to compute integers $a_1, \ldots, a_n$, polynomials $T_2(t), \ldots, T_n(t)$, polynomials $S_2(t, X_2, \ldots, X_n)$,..., $S_n(t, X_2, \ldots, X_n)$ such that:

1) the Jacobian $(\frac{\delta S_i}{\delta X_j})_{ij}$ is non-zero at the origin.

*First author's address: Departamento de Algebra, Facultad de Ciencias Matematicas, Universidad Complutense, Madrid, SPAIN. Other authors' address: Dipartimento di Matematica, Università di Genova, ITALY.

2) denoting $Q_2(t), \ldots, Q_n(t)$ the unique formal power series s.t.

$$\forall i \; S_i(t, Q_2(t), \ldots, Q_n(t)) = 0$$

a parametrization of the analytic branch is given by:

$$X_1 - \alpha_1 = t^{a_1}, X_2 - \alpha_2 = T_2(t) + t^{a_2} Q_2(t), \ldots, X_n - \alpha_n = T_n(t) + t^{a_n} Q_n(t).$$

The problem is not only a typical one in Effective Algebraic Geometry; it has interesting applications in Geometric Modeling. There, space curve tracing is needed and numerical techniques fail near singular points; for curve tracing near a singular point, symbolic computations based on resolutions of singularities have been proposed ([12], [4]). The approach we are developing leads to symbolic tracing of approximations of Puiseux expansions for each branch; we hope it could provide a useful alternative for curve tracing near singularities. An approach for plane curves, which is similar to the one we propose here, has been given in [8].

The theory behind this problem is well settled since long time (cf.[17] and for more recent algorithmic approaches [18] and [5]) and we don't claim to have original results. Our effort has been devoted to taylor the theoretical results into an algorithm which takes advantage of the most recent state of the art in polynomial system solving, which allows an easy and robust conversion of the symbolic output to a numerical one (in view of the Geometric Modeling applications) and which is easily integrable in a general Polynomial System Solver (as the one who is the core of the Esprit POSSO Project).

It is mainly based on the Tangent Cone Algorithm for standard bases computations ([20]), weak models for the arithmetics of algebraic numbers as advocated by Duval ([9]) and seminumerical techniques for real zeroes of 0-dimensional systems ([7]). There is no current implementation of our algorithm, but we will present some promising experimentations performed by means of CoCoA 1.5.3 ([10]).

A version of this paper appeared as [1]; we refer to it for the proofs which have been omitted.

1 Branches of a Curve at a Singular Point

We begin by recalling some algebraic facts and fixing some notations.

A *Puiseux series* in X over a field K (all fields considered in this paper are of characteristic 0) is a formal expression:

$$P(X) = \sum_{i=0}^{\infty} c_i X^{\nu_i/\nu}$$

with $c_i \in K$, $c_0 \neq 0$, $\nu_i \in \mathbf{Z}$, $\nu \in \mathbf{N}$, $\gcd(\nu, \nu_0, \ldots, \nu_i, \ldots) = 1$ and $\nu_0 < \nu_1 < \ldots$.

Remark that there are at most finitely many negative exponents ν_i/ν in the Puiseux series $P(X)$, while there can be finitely or infinitely many positive exponents having non-zero coefficients. The value ν_0/ν is called the *order* of P, $\mathrm{ord}\,(P) = \nu_0/\nu$, while ν is called its *index*, $\mathrm{ind}\,(P) = \nu$, order and index of the zero series being undefined.

By the usual definition of sum and product, and by the canonical conventions for dealing with exponents, the set of all Puiseux series is turned into an integral domain. For each non-zero Puiseux series $P(X)$, there is a unique Puiseux series $P^{-1}(X)$ such that $P(X)P^{-1}(X) = 1$; for such a series, necessarily, $\mathrm{ord}\,(P^{-1}) = -\mathrm{ord}\,(P)$; moreover if $\mathrm{ind}\,(P) = 1$, i.e. the exponents of P are all integers, then $\mathrm{ind}\,(P^{-1}) = 1$ too. As a consequence the set of all Puiseux series in X over K is a field, which we denote by $K((X))_{\mathrm{Puis}}$. The subset of $K((X))_{\mathrm{Puis}}$ consisting of those series $P(X)$ such that $\mathrm{ord}\,(P) \geq 0$ (i.e. none among the exponents with non zero coefficient is negative) is closed under sums and products and is therefore an integral domain which we will denote as $K[[X]]_{\mathrm{Puis}}$. Units of $K[[X]]_{\mathrm{Puis}}$ are then the elements of order zero. The Puiseux series $P(X) = \sum_{i=0}^{\infty} c_i X^{\nu_i/\nu}$ with index 1, i.e. with integer exponents, are easily seen to be both a subfield of $K((X))_{\mathrm{Puis}}$ and the field of fractions of $K[[X]]$; it will be denoted by $K((X))$.

The most important property of Puiseux series is given by Puiseux Theorem which states that, if K is algebraically closed, then the field $K((X))_{\mathrm{Puis}}$ is algebraically closed.

Since a polynomial can be canonically identified with a (finite) Puiseux series with non-negative order and integer exponents, so that $K[X] \subset K[[X]]_{\mathrm{Puis}}$, one concludes that $K(X) \subset K((X))_{\mathrm{Puis}}$, so that, by Puiseux Theorem, $\mathbf{K}((X))_{\mathrm{Puis}}$ contains the algebraic closure of $K(X)$, where $\mathbf{K}$ is the algebraic closure of K.

Let $\Gamma \subset \mathbf{C}^n$ be a curve defined by

$$F_1(X_1, \ldots, X_n) = 0, \ldots, F_s(X_1, \ldots, X_n) = 0$$

where F_i is a polynomial in $K[X_1,\ldots,X_n]$, the field K is some finite extension of $\mathbf{Q}$ and $\mathbf{K}\subset\mathbf{C}$ denotes its algebraic closure; let $I\subset K[X_1,\ldots,X_n]$ be the ideal generated by $F_1,\ldots,F_s$ and let us denote $K[x_1,\ldots,x_n]:=K[X_1,\ldots,X_n]/I$ the coordinate ring of Γ. Let us also consider the ideal I^e generated by $F_1,\ldots,F_s$ in the larger ring $K(X_1)[X_2,\ldots,X_n]$.

Let us assume that none of the irreducible components of Γ is contained in some hyperplane $X_1=\alpha$; this implies that x_1 is not algebraic over K. Under this assumption, the ideal I^e (i.e. the system of equations $F_1=\ldots=F_s=0$) has only finitely many solutions in the $(n-1)$-dimensional affine space over the algebraical closure of $K(X_1)$, which is contained in $\mathbf{K}((X_1))_{\mathrm{Puis}}$. Then there are finitely many Puiseux series $P_{jk}(X_1)\in\mathbf{K}((X_1))_{\mathrm{Puis}}$, $j=1\ldots,r$, $k=2\ldots n$ such that:

$$F_i(X_1,P_{j2}(X_1),\ldots,P_{jn}(X_1))=0 \quad \text{for all } i,j$$

each of the $(n-1)$-tuples $(P_{j2}(X_1),\ldots,P_{jn}(X_1))$ being a solution of the system. Moreover each $P_{jk}(X_1)$ converges in a neighborhood of $X_1=0$. It is important to remark that, for each such solution, there is a finite algebraic extension K_j of K such that $P_{jk}(X_1)\in K_j((X_1))_{\mathrm{Puis}}$.

There are therefore, a fortiori, at most finitely many solutions

$$(P_{j2}(X_1),\ldots,P_{jn}(X_1))$$

such that $\mathrm{ord}\,(P_{jk})>0$ for all k. We will call them *the solutions centered at the origin* of $I^e=(F_1,\ldots,F_s)$.

Let

$$P_2(X_1):=\sum_{i=0}^{\infty}c_{i2}X^{\nu_{i2}/\nu_2},\ldots,P_n(X_1):=\sum_{i=0}^{\infty}c_{in}X^{\nu_{in}/\nu_n}$$

be one of these solutions; let $\nu:=\mathrm{lcm}\,(\nu_2,\ldots,\nu_n)$, let $\mu_{ij}:=\nu_{ij}\nu/\nu_j$; for $\xi\in\mathbf{K}$ let

$$R_j(\xi,t):=\sum_{i=0}^{\infty}c_{ij}\xi^{\mu_{ij}}t^{\mu_{ij}}\in\mathbf{K}[[\,t\,]]$$

and let $R_j(t):=R_j(1,t)$. Then $P_j\in\mathbf{K}[[X_1^{1/\nu}]]$ and it is the image of $R_j(\xi,t)$ under the isomorphism between $\mathbf{K}[[X_1^{1/\nu}]]$ and $\mathbf{K}[[t]]$ given by the identification $t=\xi^{-1}X_1^{1/\nu}$.

Since $(P_2,\ldots,P_n)$ is such that each P_i is convergent, then there is $\varepsilon>0$ such that for all $\xi\in\mathbf{K}$ and for all $t\in U_{\varepsilon|\xi|^{-1}}:=\{t\in\mathbf{C}:|t|<\varepsilon|\xi|^{-1}\}$ we have

$$(\xi^\nu t^\nu,R_2(\xi,t),\ldots,R_n(\xi,t))\in\Gamma.$$

Moreover the sets $\{(\xi^\nu t^\nu, R_2(\xi,t),\dots,R_n(\xi,t)) : t \in U_{\varepsilon|\xi|^{-1}}\}$ are the same for all $\xi \in \mathbf{K}$.

In particular, if ζ is a ν^{th}-root of unity, $\zeta^\nu = 1$, the automorphism of $\mathbf{K}((t))$ given by $t \mapsto \zeta t$ leaves fixed $X_1 = t^\nu$ and so $\mathbf{K}(X_1)$. As a consequence, if

$$Q_2(X_1) := \sum_{i=0}^{\infty} c_{i2}\zeta^{\mu_{i2}} X^{\nu_{i2}/\nu_2}, \dots, Q_n(X_1) := \sum_{i=0}^{\infty} c_{in}\zeta^{\mu_{in}} X^{\nu_{in}/\nu_n}$$

then $(Q_2,\dots,Q_n)$ is another solution of the system, while the sets

$$\{(t^\nu, R_2(t),\dots,R_n(t)) : t \in U_\varepsilon\} = \{(t^\nu, P_2(t^\nu),\dots,P_n(t^\nu)) : t \in U_\varepsilon\}$$

and

$$\{(t^\nu, R_2(\zeta,t),\dots,R_n(\zeta,t)) : t \in U_\varepsilon\} = \{(t^\nu, Q_2(t^\nu),\dots,Q_n(t^\nu)) : t \in U_\varepsilon\}$$

are the same.

In other words, solutions centered at the origin of the ideal $(F_1,\dots,F_s)$ of $K(X_1)[X_2,\dots,X_n]$ can be divided in cycles; each cycle contains, for some ν, exactly ν solutions, related each other as specified above. This motivates the following definition.

Definition 1 An *analytic branch* of Γ (at the origin) is a cycle of solutions $(P_2,\dots,P_n)$ with $\mathrm{ord}\,(P_i) > 0$ for all i, of $(F_1,\dots,F_s)$. The *order* of branch is the length ν of the corresponding cycle, i.e. the least common multiple of the indexes of the P_i's. Each n-tuple $(\xi^\nu t^\nu, R_2(\xi,t),\dots,R_n(\xi,t))$ is called *a parametrization* of the branch.

Assume moreover that for each neighborhood U of zero such that, for all i, the series $R_i(t)$ is convergent for each $t \in U$, one has

$$\{(t^\nu, R_2(t),\dots,R_n(t)) : t \in U\} \cap \mathbf{R}^n \neq (0,\dots,0).$$

Then the corresponding analytic branch is called *real.*

Clearly if a solution $(P_2,\dots,P_n)$ is such that $P_i \in \mathbf{R}[[X_1]]_{\mathrm{Puis}}$ for all i, then the corresponding branch is real. The converse is however false as it is shown by the following trivial example.

Let $F(X,Y) = X + Y^2 \in \mathbf{Q}[X,Y]$. The equation $F = 0$ has two solutions centered at the origin in $\mathbf{C}[[X]]_{\mathrm{Puis}}$, which are $Y = iX^{1/2}$ and $Y = -iX^{1/2}$; they form a cycle of length 2, being related by the transformation

$t \mapsto -t$, where $t = X^{1/2}$ and therefore they give the single branch $\{(t^2, it) : t \in \mathbf{C}\}$. This branch is real as it is easily realized by the transformation $t \mapsto -iu$, which gives a parametrization of the branch as $\{(-u^2, u) : u \in \mathbf{C}\}$, which satisfies $\{(-u^2, u) : u \in \mathbf{C}\} \cap \mathbf{R}^2 = \{(-u^2, u) : u \in \mathbf{R}\}$.

One proves that each real analytic branch has either a parametrization $(t^\nu, R_2(t), \dots, R_n(t))$ or a parametrization $(-t^\nu, R_2(t), \dots, R_n(t))$ where $R_i(t) \in \mathbf{R}[[t]]$ for all i.

Finally recall that the origin is a simple point for Γ if and only if there is only an analytic branch of Γ at the origin, this branch being of order 1, i.e. if and only if there is a single solution centered at the origin of $(F_1, \dots, F_s)$. Otherwise the origin is singular.

Let $I = (F_1, \dots, F_s) \subset K[X_1, \dots, X_n]$ be a polynomial ideal over some finite extension K of $\mathbf{Q}$ and let $\mathbf{K} \subset \mathbf{C}$ denote the algebraic closure of K; let

$$\Gamma := \{(\alpha_1, \dots, \alpha_n) \in \mathbf{K}^n : F_1(\alpha_1, \dots, \alpha_n) = \dots = F_s(\alpha_1, \dots, \alpha_n) = 0\}$$

We will assume that

1. I is radical, so that

   $$I = \{F \in K[X_1, \dots, X_n] \text{ s.t. } F(\alpha_1, \dots, \alpha_n) = 0 \ \forall (\alpha_1, \dots, \alpha_n) \in \Gamma\}$$

2. I is unmixed of dimension 1, i.e. all irreducible components of Γ are curves and Γ has only finitely many singular points

3. $x_1 \in K[x_1, \dots, x_n] = K[X_1, \dots, X_n]/I$ is not algebraic over K, i.e. none of the irreducible components of Γ is contained in some hyperplane $X_1 = \alpha_1$

and we will say that I *defines an admissible curve*

Let $(\alpha_1, \dots, \alpha_n) \in \Gamma$ be a singular point of the curve. By the translation $\phi : K[X_1, \dots, X_n] \to K[X_1, \dots, X_n]$ defined by $\phi(X_i) = X_i + \alpha_i$ we can assume w.l.o.g. the singular point to be the origin. Since the origin is singular, there is more than one solution centered at the origin of $(F_1, \dots, F_s)$, corresponding to either several branches or to a single branch of order greater than 1. By back-translating, each such solution $(P_2(X_1), \dots, P_n(X_1))$ will give rise to the corresponding solution $(\alpha_2 + P_2(X_1 - \alpha_1), \dots, \alpha_n + P_n(X_1 - \alpha_1))$ "centered at $(\alpha_1, \dots, \alpha_n)$", each branch will give rise to a branch, and if $(\alpha_1, \dots, \alpha_n) \in \mathbf{R}^n$ each real branch to a real branch.

Our aim is to "compute" all branches (and all real branches) centered at the singular points of Γ, by "computing" an element $(\alpha_2 + P_2(X_1 - \alpha_1), \ldots, \alpha_n + P_n(X_1 - \alpha_1))$ in each cycle giving a branch, or, equivalently, a parametrization

$$(\alpha_1 \pm t^\nu, \alpha_2 + R_2(t), \ldots, \alpha_n + R_n(t))$$

such that $R_i(t) \in \mathbf{R}[[\,t\,]]$ if the branch is real.

Since the problem is a local one, i.e. one needs only to be able to "compute" solutions centered at the origin, we need to formulate the problem in local terms, by considering the behaviour of Γ only near singular points.

We say therefore that $I = (F_1, \ldots, F_s)$ *locally defines an admissible curve* if, denoting $I_0 := IK[X_1, \ldots, X_n]_0$, then:

1. I_0 is radical, i.e. all irreducible components of Γ passing through the origin are simple
2. I_0 is unmixed of dimension 1, i.e. all irreducible components of Γ passing through the origin are curves
3. $x_1 \in K[x_1, \ldots, x_n]_0 = K[X_1, \ldots, X_n]_0 / I_0$ is not algebraic over K, i.e. none of the irreducible components of Γ passing through the origin is contained in the hyperplane $X_1 = 0$

2 Tools

2.1 Arithmetics

The algorithm we are going to describe in this paper requires extensive recourse to solving systems of polynomial equations with finitely many roots and to dealing with the arithmetics of algebraic numbers. Efficient techniques for both problems are therefore crucial for the performance of the algorithms we are discussing.

The current theoretical state of the art of polynomial system solving is much advanced in respect of the currently available implementations (not only in general purpose symbolic computation systems, but even in fairly specialized ones), and further advances will be available in the next future (see [6]). Implementations reflecting these theoretical advances are to be considered as forthcoming (a specialized symbolic computation system for polynomial system solving will be produced within the ESPRIT Basic

Research Action POSSO) and will have then an impact on the practical performance of our proposals.

The general philosophy underlying all recent advances in polynomial system solving is that there is no need to actually compute zeroes $(\eta_1, \dots, \eta_n)$ of a 0-dimensional ideal $I \subset K[X_1, \dots, X_n]$ (i.e. s.t. it has finitely many roots in $\mathbf{K}^n$) provided that one is able to perform arithmetical operations in $K(\eta_1, \dots, \eta_n)$, so that the effort is mainly devoted to devising effective (and efficient) schemes to perform arithmetics in $K(\eta_1, \dots, \eta_n)$ when only a 0-dimensional ideal I is given which has $(\eta_1, \dots, \eta_n)$ as a zero.

This philosophy was first advocated by Duval ([9]) in her model for algebraic number arithmetics, where an algebraic number α is defined, not by giving its minimal polynomial over $\mathbf{Q}$, as in the classical computational models, but just a squarefree polynomial $f(X) \in \mathbf{Q}[X]$ s.t. $f(\alpha) = 0$. Elements in the field $\mathbf{Q}(\alpha)$ are then represented (in a non-unique way) by elements in $\mathbf{Q}[X]/(f)$, so that $\mathbf{Q}[X]/(f)$ is used to represent all the fields $\mathbf{Q}(\alpha)$ where α is any one of the roots of f. Sums and products in $\mathbf{Q}(\alpha)$ are then performed as usual by modular arithmetics in $\mathbf{Q}[X]/(f)$. Problems obviously arise with inverse computation, since a same expression $g \in \mathbf{Q}[X]/(f)$ can be zero for some roots of f and non-zero for some other roots; the basic idea behind Duval's model is that $g(\alpha)$ is:

zero if α is root of $f_0(X) := GCD(f(X), g(X))$

non-zero if α is root of $f_1(X) := f(X)/f_0(X)$

so that each time a zero-checking and/or an inverse computation is required, while performing some algorithm requiring arithmetics over $\mathbf{Q}(\alpha)$, it gives a partial factorization of f into f_0 and f_1 and a splitting of $\mathbf{Q}[X]/(f)$ into $\mathbf{Q}[X]/(f_0)$ and $\mathbf{Q}[X]/(f_1)$; the algorithm is then to be performed separately over both $\mathbf{Q}[X]/(f_0)$ and $\mathbf{Q}[X]/(f_1)$.

Extensions of Duval approach to systems of polynomial equations are theoretically known ([14], [15], and the forthcoming paper [22]); let us sketch here the basic ideas of [22]:

Let $(\eta_1, \dots, \eta_n)$ be a zero of a 0-dimensional ideal $I \subset K[X_1, \dots, X_n]$; then:

1. there is a surjection from $K[X_1, \dots, X_n]/I$ to $K(\eta_1, \dots, \eta_n)$;

2. $K[X_1, \dots, X_n]/I$ is a K-vector space of finite dimension $h = \mathrm{mult}(I)$;

3. a Gröbner basis of I determines a vector subspace V of $K[X_1, \dots, X_n]$ isomorphic to $K[X_1, \dots, X_n]/I$

4. therefore each element of $K(\eta_1, \ldots, \eta_n)$ can be represented (not in a unique way) by an element of V.

5. linear algebra algorithms can be used to perform sums and products of elements of $K[X_1, \ldots, X_n]/I$ and so of the corresponding elements of $K(\eta_1, \ldots, \eta_n)$;

6. moreover if $g \in V$, denoting $I_0 := I + (g)$ and $I_1 := I : g^h$, then the zeroes of I_0 are exactly those zeroes $(\eta_1, \ldots, \eta_n)$ of I such that $g(\eta_1, \ldots, \eta_n) = 0$, while the zeroes of I_1 are exactly those zeroes $(\eta_1, \ldots, \eta_n)$ of I such that $g(\eta_1, \ldots, \eta_n) \neq 0$.

7. given a a Gröbner basis of I, linear algebra algorithms can be used to compute Gröbner bases of both I_0 and I_1 and so vectorial representations of both $K[X_1, \ldots, X_n]/I_0$ and $K[X_1, \ldots, X_n]/I_1$

8. therefore , exactly as in Duval model, if some algorithm is applied to the zeroes of I, each zero-checking will give rise to a splitting of $K[X_1, \ldots, X_n]/I$.

With reference to the model of [22] (or to any other model based on Duval techniques), we will say that $(I_1, \ldots, I_t)$ is a *splitting* of a 0-dimensional ideal $I \subset K[X_1, \ldots, X_n]$ if:

1. $\forall j \ \ I_j \subset K[X_1, \ldots, X_n]$ is a 0-dimensional ideal

2. the roots of I are the disjoint union of the roots of $I_j \ \ \forall j$

We are still left to discuss how to deal with real roots. Our proposal is to use the multivariate versions of Sturm Theorem ([23]) to decide whether a 0-dimensional ideal I has real zeroes; is such is the case, while still performing arithmetics with them in the model described above, we also use the seminumerical techniques advocated in [7] to obtain floating point approximations of all real algebraic numbers we are computing with.

2.2 Standard Bases and Multiplicities

Let us fix a non-zero vector of integer non-negative weights $(a_1, \ldots, a_n)$. Let us consider the morphism $\psi : K[X_1, \ldots, X_n] \to K[X_1, \ldots, X_n, t]$ defined by $\psi(X_i) = t^{a_i} X_i$. Then if $F(X_1, \ldots, X_n) \in K[X_1, \ldots, X_n]$, one has:

$$\begin{aligned} \psi(F) &= F(t^{a_1} X_1, \ldots, t^{a_n} X_n) \\ &= t^d G(X_1, \ldots, X_n) + t^{d+1} H(t, X_1, \ldots, X_n). \end{aligned}$$

The *initial form* of $F(X_1,\dots,X_n)$ (w.r.t. the weights $(a_1,\dots,a_n)$) is defined to be the polynomial $G(X_1,\dots,X_n)$ and we put $\mathrm{in}\,(F) = G$.

An alternative way of describing it is as follows: assigning to the variable X_i the weight a_i, a weight is then defined on $\mathbf{T} := \langle X_1,\dots,X_n\rangle$, the set of terms in $K[X_1,\dots,X_n]$, by:

$$wt(X_1^{e_1}\cdots X_n^{e_n}) = \sum_{i=1}^{n} a_i e_i$$

A pseudohomogenous form F of weight d, $wt(F) = d$, is then a polynomial $F = \sum_{t\in\mathbf{T}} c_t t$ s.t. $wt(t) = d\ \forall t$ s.t. $c_t \neq 0$. Each non-zero polynomial $G(X_1,\dots,X_n)$ can be written uniquely as a finite sum of non-zero pseudohomogeneous forms of different weights; $\mathrm{in}\,(G)$ is the form of least weight in this representation, and the weight of G is defined as $wt(G) := wt(\mathrm{in}\,(G))$.

Let I be an ideal in $K[X_1,\dots,X_n]$. Let us denote by $\mathrm{in}\,(I)$ the ideal in $K[X_1,\dots,X_n]$ generated by $\{\mathrm{in}\,(F) : F \in I\}$. It is easy to verify that $\mathrm{in}\,(I)$ is pseudohomogeneous (i.e. if a polynomial belongs to $\mathrm{in}\,(I)$, then each pseudohomogeneous form in its representation belongs to $\mathrm{in}\,(I)$ too) and that a pseudohomogeneous element in $\mathrm{in}\,(I)$ is the initial form of some polynomial in I.

In general if $(F_1,\dots,F_s)$ is a basis of I, then $(\mathrm{in}\,(F_1),\dots,\mathrm{in}\,(F_s))$ may not be a basis of $\mathrm{in}\,(I)$.

Definition 2 A *standard basis* of an ideal I (w.r.t. $(a_1,\dots,a_n)$) is a set of elements $\{G_1,\dots,G_t\}$ of I such that the ideal $\mathrm{in}\,(I)$ is generated by $(\mathrm{in}\,(G_1),\dots,\mathrm{in}\,(G_t))$.

There is a generalization of Buchberger Algorithm, the Tangent Cone Algorithm ([20]), which, given any set of generators of an ideal I, allows to compute a standard basis $(G_1,\dots,G_t)$ of I; moreover, for any prescribed term-ordering $<$, the algorithm returns a standard basis $(G_1,\dots,G_t)$ such that $(\mathrm{in}\,(G_1),\dots,\mathrm{in}\,(G_t))$ is a Gröbner basis of $\mathrm{in}\,(I)$ w.r.t. $<$.

It is important to remark that standard bases are a local tool, intended to describe the structure of a variety near the origin; in fact the ideal generated by a standard basis of I in the polynomial ring $K[X_1,\dots,X_n]$ can be different from I; however the extensions of the two ideals in $K[X_1,\dots,X_n]_0$, the localization of $K[X_1,\dots,X_n]$ at the origin, are the same. In geometrical terms this means that the irreducible components passing through the origin of the varieties defined by the two ideals are the same and have the same multiplicity.

In what follows we will restrict the weights a_i to be all positive, and w.l.o.g. we will assume $\gcd(a_i) = 1$. Under this assumption a standard basis of I satisfies the following properties:

1. the ideal $\mathrm{in}(I)$ is pseudohomogeneous; therefore if $(\eta_1, \ldots, \eta_n)$ is a zero of $\mathrm{in}(I)$ then, for all t, $(t^{a_1}\eta_1, \ldots, t^{a_n}\eta_n)$ is also a zero of $\mathrm{in}(I)$.
2. The dimension of $\mathrm{in}(I)$ is the local dimension of I, i.e. the maximal dimension of the irreducible components passing through the origin of the variety defined by the ideal.
3. If I locally defines a curve (i.e. the irreducible components of the variety defined by I passing through the origin are curves), then $\mathrm{in}(I)$ locally defines a curve too; in this case we can conclude that $\mathrm{in}(I)$ defines the union of the curves whose generic points are $(t^{a_1}\eta_1, \ldots, t^{a_n}\eta_n)$, where $(\eta_1, \ldots, \eta_n)$ runs among the zeroes of $\mathrm{in}(I)$; in particular those curves which do not lie in the plane $X_1 = 0$ are uniquely determined by the zeroes $(\eta_1, \ldots, \eta_n)$ of $\mathrm{in}(I)$, with $\eta_1 = 1$.
4. A curve $(t^{a_1}\eta_1, \ldots, t^{a_n}\eta_n)$ satisfies the equations of $\mathrm{in}(I)$ if and only if it is tangent at the origin to the curve defined by I.

Let us recall the notion of multiplicity for a root $(\omega_1, \ldots, \omega_n) \in L^n$ of a 0-dimensional ideal $I = (H_1, \ldots, H_s) \in K[X_1, \ldots, X_n]$, where $K \subset L \subset \mathbf{K}$. Let us denote by Δ the L-vector space generated by all the partial derivations $\frac{\partial^{i_1+\cdots+i_n}}{\partial X_1^{i_1}\cdots\partial X_1^{i_n}}$ and by $\Delta(\omega, I) \subset \Delta$ the subvector space

$$\Delta(\omega, I) := \{\partial \in \Delta \text{ s.t. } \partial(F)(\omega_1, \ldots, \omega_n) = 0 \ \forall F \in I\}$$

Definition 3 The *multiplicity* of a root $\omega = (\omega_1, \ldots, \omega_n) \in L^n$ of a 0-dimensional ideal $I \in K[X_1, \ldots, X_n]$, where $K \subset L \subset \mathbf{K}$, is $Mult(\omega, I) = dim_L(\Delta(\omega, I))$

Let us immediately remark the following Lemma which we will need in the sequel:

Lemma 1 *Let $K \subset L \subset \mathbf{K}$; let $(H_1, \ldots, H_s) \in K[X_1, \ldots, X_n]$ be a 0-dimensional ideal, and let $(\omega_1, \ldots, \omega_n) \in L^n$ be a root of I. Then $(\omega_1, \ldots, \omega_n)$ is a multiple root if and only if there are $\zeta_1, \ldots, \zeta_n \in L$ such that, denoting:*

$$\Delta(H) := \zeta_1 \partial H/\partial X_1 + \ldots + \zeta_n \partial H/\partial X_n \text{ for } H \in L[X_1, \ldots, X_n]$$

then $\Delta(H_i)(\omega_1, \ldots, \omega_n) = 0$ *for all* i.

Standard bases are a useful tool in studying multiplicities because of the following:

Proposition 1 *Let* I *be an ideal of dimension* 0*; then* $\mathrm{in}\,(I)$ *is a proper ideal if and only if the origin is among the zeroes of* I*; in this case:*

$$mult(0, I) = mult(0, \mathrm{in}\,(I)) = dim_K(K[X_1, \ldots, X_n]/I)$$

Furthermore we can count multiplicities of roots of a 0-dimensional ideal $I \subset K[X_1, \ldots, X_n]$ other than the origin as follows: let $\alpha := (\alpha_1, \ldots, \alpha_n)$ be a zero of I of multiplicity h and let $\phi_\alpha : K[X_1, \ldots, X_n] \to K[X_1, \ldots, X_n]$ be the morphism defined by $\phi_\alpha(X_i) = X_i + \alpha_i$; then the origin is a zero for $\phi_\alpha(I)$ of multiplicity h and this multiplicity can be computed by means of standard bases. Moreover the sum of the multiplicities of the zeroes of a 0-dimensional ideal I is equal to the K-dimension of $K[X_1, \ldots, X_n]/I$ and is called the *multiplicity* of I.

The notion of multiplicity is insufficient for some of our purposes and we need to give a stronger notion; let J be a 0-dimensional ideal and let $\alpha := (\alpha_1, \ldots, \alpha_n)$, $\beta := (\beta_1, \ldots, \beta_n)$ be two zeroes of J. We will say that α and β are *equivalent zeroes* of J if $\mathrm{in}\,(\phi_\alpha(J)) = \mathrm{in}\,(\phi_\beta(J))$; two equivalent zeroes have obviously the same multiplicity.

If α is a zero of I and β is a zero of J (where I and J are 0-dimensional), we will also say that α (as a zero of I) and β (as a zero of J) are equivalent if $\mathrm{in}\,(\phi_\alpha(I)) = \mathrm{in}\,(\phi_\beta(J))$.

If I is a 0-dimensional ideal and we apply the arithmetical models described in Section 2.1 for computing a standard basis of $\phi_\alpha(I)$ for a root α of I by performing arithmetics over $K[\alpha] := K[X_1, \ldots, X_n]/I$, the output will be

- a splitting $(I_1, \ldots, I_u)$
- $\forall i = 1, \ldots, u$ a set of polynomials in $K_j[X_1, \ldots, X_n]$ where $K_j := K[X_1, \ldots, X_n]/I_j$, which are a standard basis of $\phi_\alpha(I)$ for each root α of I_j.

so that two non-equivalent roots of I will be separated, but a single computation has been performed for equivalent ones.

2.3 Critical Tropisms

Let us fix weights $(a, b, \ldots, b)$ on $K[X_1, \ldots, X_n]$ with $a > 0$ and let $\nu := b/a$. Clearly in (F) is invariant if the weights are scaled by a positive quantity, so we will denote $\text{in}_\nu(F)$, $\text{in}_\nu(I)$ to denote in (F), in (I) for weights $(a, b, \ldots, b)$ with $b/a = \nu$.

Definition 4 We say that $\nu \in \mathbf{Q}^+ = \{\nu \in \mathbf{Q} : \nu > 0\}$ is a *critical tropism* for the ideal I if

$$\forall \varepsilon > 0 \ \exists \mu \text{ s.t. } |\mu - \nu| < \varepsilon \text{ and } \text{in}_\nu(I) \neq \text{in}_\mu(I)$$

In other words, ν is *not* a critical tropism if $\text{in}_\mu(I)$ is constant in a neighborhood of ν. A result by Lejeune and Tessier ([16]) states that an ideal has only finitely many critical tropisms; we give here a proof of this fact based on the notion of Gröbner Fan ([21]) which allows to adapt an algorithm by Assi ([3]) for their computation.

We start by imposing a bigraduation on $\mathbf{T} := \langle X_1, \ldots, X_n \rangle$ by defining:

$$wt_2(X_1^{e_1} \cdots X_n^{e_n}) = (e_1, \sum_{i=2}^{n} e_i) \in \mathbf{N}^2$$

and we fix a semigroup well-ordering $<$ on $\mathbf{N}^2$. A bihomogenous form F of weight (d_1, d_2), $wt_2(F) = (d_1, d_2)$, is then a polynomial $F = \sum_{t \in \mathbf{T}} c_t t$ s.t. $wt_2(t) = (d_1, d_2)$ $\forall t$ s.t. $c_t \neq 0$. Each non-zero polynomial $G(X_1, \ldots, X_n)$ can be written uniquely as a finite sum of non-zero bihomogeneous forms of different weights; $B(G)$ is the form of least weight w.r.t. $<$ in this representation, and the weight of G is defined as $wt(G) := wt(B(G))$.

If I is an ideal in $K[X_1, \ldots, X_n]$, we denote by $B(I)$ the ideal in $K[X_1, \ldots, X_n]$ generated by $\{B(F) : F \in I\}$. It is easy to verify that $B(I)$ is bihomogeneous (i.e. if a polynomial belongs to $B(I)$, then each bihomogeneous form in its representation belongs to $B(I)$ too).

We will call a *B-standard basis* of an ideal I (w.r.t. $<$) a set of elements $\{G_1, \ldots, G_t\} \subset I$ such that $B(I)$ is generated by $(B(G_1), \ldots, B(G_t))$.

To each semigroup well-ordering $<$ on $\mathbf{N}^2$, a linear form is associated (uniquely up to a positive scaling) $L(d_1, d_2) = ad_1 + bd_2$ with a, b non-negative integers and not both of them zero s.t. if $L(d_1, d_2) < L(e_1, e_2)$ then $(d_1, d_2) < (e_1, e_2)$. If L is as above, let us pose $wt(<) := \nu := b/a$ if $a > 0$, $wt(<) := \nu := \infty$ if $a = 0$ and $L_\nu := L$.

Moreover there are exactly two semigroup orderings $<$ s.t. $L_\nu = L$ which we will denote by $<_{\nu^+}$ and $<_{\nu^-}$, and which are defined as follows:

$$
\begin{aligned}
(d_1, d_2) <_{\nu^+} (e_1, e_2) \iff & L_\nu(d_1, d_2) < L_\nu(e_1, e_2) \quad \text{or} \\
& (L_\nu(d_1, d_2) = L_\nu(e_1, e_2) \quad \text{and} \quad e_1 < e_2)
\end{aligned}
$$

$$
\begin{aligned}
(d_1, d_2) <_{\nu^-} (e_1, e_2) \iff & L_\nu(d_1, d_2) < L_\nu(e_1, e_2) \quad \text{or} \\
& (L_\nu(d_1, d_2) = L_\nu(e_1, e_2) \quad \text{and} \quad e_1 > e_2)
\end{aligned}
$$

The only one among these orderings which is not a well-ordering is $<_{0^-}$. By $B_{\nu^+}(\cdot)$ (resp. $B_{\nu^-}(\cdot)$) we will denote $B(\cdot)$ w.r.t. $<_{\nu^+}$ (resp. $<_{\nu^-}$).

It is clear that:
a) if $wt(<) := \nu$ then $B(\mathrm{in}_\nu(F)) = B(F)$, $B(\mathrm{in}_\nu(I)) = B(I)$.
b) if $(G_1, \ldots, G_s)$ is a B-standard basis of I w.r.t. $<$, then $(\mathrm{in}_\nu(G_1), \ldots, \mathrm{in}_\nu(G_s))$ is a B-standard basis of $\mathrm{in}_\nu(I)$, so that in particular $(G_1, \ldots, G_s)$ is a standard basis of I with respect to the weights $(a, b, \ldots, b)$.

The Tangent Cone Algorithm , given any set of generators of I, can be applied to compute a B-standard basis $(G_1, \ldots, G_t)$ of I; moreover, for any prescribed term-ordering $<$, the algorithm returns a B-standard basis $(G_1, \ldots, G_t)$ such that $(B(G_1), \ldots, B(G_t))$ is a Gröbner basis of $B(I)$ w.r.t. $<$.

Lemma 2 *If* $\mathrm{in}_\nu(I)$ *is bihomogeneous, then* $B_{\nu^+}(I) = \mathrm{in}_\nu(I) = B_{\nu^-}(I)$

Proposition 2 *There are rational* $0 = \nu_0 < \nu_1 < \ldots < \nu_s < \nu_{s+1} = \infty$ *s.t.*

$\forall j = 0 \ldots s$, $\forall \nu \in (\nu_j, \nu_{j+1})$ *for each ordering* $<$ *s.t.* $wt(<) := \nu$, $B(I) = \mathrm{in}_\nu(I)$ *is independent on* $<$.

if $\nu = \nu_j$ *then* $B_{\nu^+}(I) = \mathrm{in}_{\nu+\varepsilon}(I)$, $B_{\nu^-}(I) = \mathrm{in}_{\nu-\varepsilon}(I)$ *for each sufficiently small* $\varepsilon > 0$

Proof: it is an easy generalization of [21] and a suitable specialization of [19], IV.3 and VII.5

Lemma 3 $\mathrm{in}_\nu(I)$ *is bihomogeneous if and only if* $\mathrm{in}_{\nu+\varepsilon}(I) = \mathrm{in}_{\nu-\varepsilon}(I)$ *for each sufficiently small* $\varepsilon > 0$

Proof: Let $g \in \mathrm{in}_\nu(I)$ and not bihomogenous, so that $g = B_{\nu^+}(g) + h$ with $h \neq 0$.

Since there are standard bases $(G_1, \ldots, G_s)$ of I s.t. $(B(G_1), \ldots, B(G_s))$ is a Groebner basis for $B_{\nu^+}(I)$, by applying an obvious modification of Buchberger reduction, we can moreover assume that no bihomogeneous form in the representation of h is in $B_{\nu^+}(I)$.

Since $B_{\nu^+}(h) <_{\nu^+} B_{\nu^+}(g)$, one has $B_{\nu^+}(g) <_{\nu^-} B_{\nu^+}(h)$, since the two orderings are the reverse of each other on pseudohomogeneous elements. Therefore $B_{\nu^-}(h) = B_{\nu^-}(g) \in B_{\nu^-}(I)$, $B_{\nu^-}(h) \notin B_{\nu^+}(I)$, so that $B_{\nu^+}(I) \neq B_{\nu^-}(I)$.

Conversely if $\mathrm{in}_\nu(I)$ is bihomogeneous, then for each sufficiently small $\varepsilon > 0$, $\mathrm{in}_{\nu+\varepsilon}(I) = B_{\nu^+}(I) = \mathrm{in}_\nu(I) = B_{\nu^-}(I) = \mathrm{in}_{\nu-\varepsilon}(I)$

Corollary 1 *If for a sufficiently small $\varepsilon > 0$, $\mathrm{in}_{\nu+\varepsilon}(I) = \mathrm{in}_{\nu-\varepsilon}(I)$, then* $\mathrm{in}_\nu(I) = \mathrm{in}_{\nu+\varepsilon}(I) = \mathrm{in}_{\nu-\varepsilon}(I)$

Proof: In fact, by the assumption, $\mathrm{in}_\nu(I)$ is bihomogeneous, so that $\mathrm{in}_\nu(I) = B_{\nu^-}(I) = \mathrm{in}_{\nu-\varepsilon}(I)$

Proposition 3 *There are only finitely many critical tropisms $0 = \nu_0 < \nu_1 < \ldots < \nu_t < \infty$ for I; if $\nu \in (\nu_i, \nu_{i+1})$, where we put $\nu_{t+1} = \infty$, then $\mathrm{in}_\nu(I)$ is bihomogeneous, while $\mathrm{in}_{\nu_i}(I)$ is not bihomogeneous for $i = 1 \ldots t$.*

Proof: It is an obvious corollary of the results above.

Lemma 4 *Let $\nu := b/a \in \mathbf{Q}^+$ be such that $\mathrm{in}_\nu(I)$ is bihomogeneous; let $(G_1, \ldots, G_s)$ be a standard basis of I w.r.t. to the weights $(a, b, \ldots, b)$. Let $0 \leq \nu_- < \nu < \nu_+ \leq \infty$ be s.t.*

$$\forall i \ \forall \mu \in (\nu_-, \nu_+), \mathrm{in}_\nu(G_i) = \mathrm{in}_\mu(G_i)$$

$$\exists i, j \text{ s.t. } \mathrm{in}_\nu(G_i) \neq \mathrm{in}_{\nu_-}(G_i), \ \mathrm{in}_\nu(G_j) \neq \mathrm{in}_{\nu_+}(G_j)$$

Then $\mathrm{in}_\mu(I) = \mathrm{in}_\nu(I) \ \forall \mu \in (\nu_-, \nu_+)$.

Moreover, both ν_- and ν_+ are critical tropisms (unless they are resp. 0 *or* ∞*)*

Proof: Assume there is $\mu \in (\nu_-, \nu_+)$ s.t. $\mathrm{in}_\mu(I)$ is not bihomogeneous. We will discuss only the case $\mu > \nu$, the other case requiring only trivial modifications. Let us choose the minimal such μ. Let $F \in I$ be s.t. $G := \mathrm{in}_\mu(F) = B_{\mu^-}(G) + H$ is not bihomogeneous. As above, we can assume that no bihomogeneous form in H is in $B_{\mu^-}(I)$ Also $B_{\mu^-}(G) = \mathrm{in}_{\mu-\varepsilon}(G) = \mathrm{in}_\nu(G) \in \mathrm{in}_\nu(I) \subset \mathrm{in}_\mu(I)$. Therefore $H \in \mathrm{in}_\mu(I)$, $B_{\mu^-}(H) \in B_{\mu^-}(I)$, contrary to the assumption.

As a corollary one obtains the following algorithm to compute all the critical tropisms of I (cf. [3]):

> Compute a B-standard basis $(G_1, \ldots, G_s)$ for I w.r.t. $<_{0^+}$
> % $\mathrm{in}_\varepsilon(I) = B_{0^+}(I) = (B_{0^+}(G_1), \ldots, B_{0^+}(G_s))$
> $i = 0, \nu_0 = 0$
> **While** $\exists \nu\ \exists j : \mathrm{in}_\nu(G_j) \neq B_{\nu_i^+}(G_j)$ **do**
> $\nu_{i+1} := min(\nu : \exists j : \mathrm{in}_\nu(G_j) \neq B_{\nu_i^+}(G_j))$
> $i := i + 1$
>   % $\mathrm{in}_{\nu_i+\varepsilon}(I) = B_{\nu_i^+}(I) = (B_{\nu_i^+}(G_1), \ldots, B_{\nu_i^+}(G_s))$

2.4 Transformations on a curve

Let $I = (F_1, \ldots, F_s)$ locally define an admissible curve Γ. First of all we need some more notation; if $(P_2, \ldots, P_n)$ is a solution centered at the origin of I, then

$$P_2(X_1) = \varepsilon_2 X_1^{\nu_2} + X_1^{\nu_2} Q_2(X_1), \ldots, P_n(X_1) = \varepsilon_n X_1^{\nu_n} + X_1^{\nu_n} Q_n(X_1)$$

with $\varepsilon_i \neq 0$, $\mathrm{ord}\,(Q_i) > 0$ for all i; let $\nu := \min(\nu_i)$; $\eta_i := \varepsilon_i$ if $\nu_i = \nu$, $\eta_i := 0$ if $\nu_i > \nu$. Then we say that:

ν is the *initial exponent* of $(P_2, \ldots, P_n)$

$(\eta_2 X_1^\nu, \ldots, \eta_n X_1^\nu)$ is the *initial approximation* of $(P_2, \ldots, P_n)$.

Let us fix weights $(a, b, \ldots, b)$ and let $\nu := b/a$. Let $\bar\eta := (\eta_2, \ldots, \eta_n) \in L^{n-1}$, where L is a finite algebraic extension of K. Let

$$\psi_{\bar\eta} : L[X_1, \ldots, X_n] \to L[t, X_2, \ldots, X_n]$$

be the morphism defined by:

$$X_1 = t^a,\ X_2 = (\eta_2 + X_2)t^b, \ldots, X_n = (\eta_n + X_n)t^b.$$

For a polynomial $F(X_1, \ldots, X_n) \in K[X_1, \ldots, X_n]$, denote

$$G(X_2, \ldots, X_n) := \mathrm{in}_\nu(F)(1, X_2, \ldots, X_n)$$

and $d(F)$ the weight of F. Then:

$$\psi_{\bar\eta}(F) = t^{d(F)} G(\eta_2 + X_2, \ldots, \eta_n + X_n) + t^{d(F)+1} H(t, \eta_2 + X_2, \ldots, \eta_n + X_n)$$

so that $\psi_{\bar\eta}(F)$ is divisible by $t^{d(F)}$, but not by a higher power of t.

Lemma 5 *Let* $F \in K[X_1, \ldots, X_n]$ *and* $P_2(X_1), \ldots, P_n(X_1) \in \mathbf{K}[[X_1]]_{\mathrm{Puis}}$ *be such that:*

a) $F(X_1, P_2(X_1), \ldots, P_n(X_1)) = 0$

b) $\mathrm{ord}\,(P_i) \geq \nu$ *for all* i*, so that*

c) $P_i(X_1) := \eta_i X_1^\nu + X_1^\nu Q_i(X_1)$ *for all* i *with* $Q_i(X_1) \in \mathbf{K}[[X_1]]_{\mathrm{Puis}}$ *and* $\mathrm{ord}\,(Q_i) > 0$.

Denote $\bar\eta := (\eta_2, \ldots, \eta_n)$ *and* $R(t, X_2, \ldots, X_n) := \psi_{\bar\eta}(F)/t^{d(F)}$. *Then:*

1. $\mathrm{in}_\nu(F)(1, \eta_2, \ldots, \eta_n) = 0$*;*

2. $R(t, Q_2(t^a), \ldots, Q_n(t^a)) = 0$.

Lemma 6 *Let* $F \in K[X_1, \ldots, X_n]$, $\bar\eta := (\eta_2, \ldots, \eta_n) \in \mathbf{K}^{n-1}$. *Let* $R(t, X_2, \ldots, X_n) := \psi_{\bar\eta}(F)/t^{d(F)}$, *and* $Q_2(t), \ldots, Q_n(t) \in \mathbf{K}[[t]]_{\mathrm{Puis}}$, *such that* $\mathrm{ord}\,(Q_i) > 0$ *and* $R(t, Q_2(t), \ldots, Q_n(t)) = 0$. *Let* $P_i(X_1) = \eta_i X_1^\nu + X_1^\nu Q_i(X_1^{1/a})$. *Then*

$$F(X_1, P_2(X_1), \ldots, P_n(X_1)) = 0.$$

Theorem 1 *Let* $F_1, \ldots, F_s$ *be a standard basis of the ideal* I *for the weights* $(a, b, \ldots b)$, $\nu := b/a$. *Let* $G_i(X_2, \ldots, X_n) := \mathrm{in}_{nu}(F_i)(1, X_2, \ldots, X_n)$ *and let* d_i *be the weight of* F_i. *Then:*

1. The ideal $(G_1, \ldots, G_s)$ *is either the whole ring (i.e. it has no roots) or a* 0*-dimensional ideal (i.e. it has finitely many roots only).*

2. There is a solution centered at the origin of $(F_1, \ldots, F_s)$ *with initial approximation*

$$X_2 = \eta_2 X_1^\nu, \ldots, X_n = \eta_n X_1^\nu$$

if and only if $(\eta_2, \ldots, \eta_n)$ *is a root of* $(G_1, \ldots, G_s)$.

Let $\bar\eta := (\eta_2, \ldots, \eta_n)$ *be a a root of* $(G_1, \ldots, G_s)$ *and* $R_i(t, X_2, \ldots, X_n) := \psi_{\bar\eta}(F_i)/t^{d_i}$. *Then:*

3. $(R_1, \ldots, R_s)$ *locally defines an admissible curve* $\Gamma_{\bar\eta}$ *(the* $\bar\eta$*-transformation of* Γ*).*

4. The solutions of $(F_1,\dots,F_s)$ *with initial approximation*

$$X_2=\eta_2X_1^\nu,\dots,X_n=\eta_nX_1^\nu$$

are $(P_2(X_1),\dots,P_n(X_1))$, *with* $P_i(X_1)=\eta_iX_1^\nu+X_1^\nu Q_i(X_1)$ *and* $(Q_2(t^a),\dots,Q_n(t^a))$ *a solution centered at the origin of* $(R_1,\dots,R_s)$.

Proof: 1) The ideal $\mathrm{in}_\nu(I)=(\mathrm{in}_\nu(F_1),\dots,\mathrm{in}_\nu(F_s))$ has dimension 1, so its zeroes are finitely many curves $(t^a\eta_1,t^b\eta_2,\dots,t^b\eta_n)$. The roots of $(G_1,\dots,G_s)$ are the points which satisfy $\mathrm{in}_\nu(F_1)=\dots=\mathrm{in}_\nu(F_s)=0$ and moreover $X_1=1$. Therefore there is a root of $(G_1,\dots,G_s)$, for each curve $(t^{a_1}\eta_1,\dots,t^{a_n}\eta_n)$, which is not in the hyperplane $X_1=0$.

2) If $(P_2(X_1),\dots,P_n(X_1))$ is a solution of $(F_1,\dots,F_s)$ centered at the origin with initial approximation

$$X_2=\eta_2X_1^\nu,\dots,X_n=\eta_nX_1^\nu$$

then $(\eta_2,\dots,\eta_n)$ is a root of $(G_1,\dots,G_s)$, as a consequence of Lemma 5. Conversely, since $(F_1,\dots,F_s)$ is a standard basis, if $(\eta_2,\dots,\eta_n)$ is a zero of $(G_1,\dots,G_s)$, then $(t^a,t^b\eta_2,\dots,t^b\eta_n)$ is tangent to Γ, and so there is a solution of $(F_1,\dots,F_s)$ centered at the origin with initial approximation

$$X_2=\eta_2X_1^\nu,\dots,X_n=\eta_nX_1^\nu.$$

3) Since $(F_1,\dots,F_s)$ locally defines a curve and so it has finitely many solutions centered at the origin with initial approximation

$$X_2=\eta_2X_1^\nu,\dots,X_n=\eta_nX_1^\nu$$

Lemmata 5 and 6 prove that $(R_1,\dots,R_s)$ has finitely many zeroes over $\mathbf{K}[[t]]_{\mathrm{Puis}}$, i.e. it locally defines a curve. If $(R_1,\dots,R_s)$ had components in the hyperplane $t=0$, then $(R_1,\dots,R_s,t)$ would have infinitely many solutions in $\mathbf{K}^n$. However $(R_1,\dots,R_s,t)=(G_1,\dots,G_s,t)$ is 0-dimensional. We must prove that all the solutions centered at the origin of $(R_1,\dots,R_s)$ are simple. Let $\zeta_2(t),\dots,\zeta_n(t)\in\mathbf{K}((t))_{\mathrm{Puis}}$ and denote

$$\Delta(H):=\zeta_2\partial H/\partial X_2+\dots+\zeta_n\partial H/\partial X_n$$

for $H\in\mathbf{K}[t,X_2,\dots,X_n]$.

Let $\omega_i(X_1):=\zeta_i(X_1^{1/a})$ and denote

$$\Delta(F):=\omega_2\partial F/\partial X_2+\dots+\omega_n\partial F/\partial X_n$$

for $F \in \mathbf{K}[X_1, X_2, \ldots, X_n]$.

A direct verification shows that for all i and j:

$$t^{d_i} \partial R_i / \partial X_j = t^b \psi_{\bar{\eta}}(\partial F_i / \partial X_j)$$

so that for all i

$$t^{d_i} \Delta(R_i) = t^b \psi_{\bar{\eta}}(\Delta(F_i)).$$

By Lemmata 5 and 6 $(Q_2(t), \ldots, Q_n(t))$ is a root of $(\Delta(R_1), \ldots, \Delta(R_s))$, if and only if $(P_2(X_1), \ldots, P_n(X_1))$ is a root of $(\Delta(F_1), \ldots, \Delta(F_s))$, i.e. $(Q_2(t), \ldots, Q_n(t))$ is a multiple root of $(R_1, \ldots, R_s)$ if and only if $(P_2(X_1), \ldots, P_n(X_1))$ is a multiple root of $(F_1, \ldots, F_s)$. Since the solutions centered at the origin of $(F_1, \ldots, F_s)$ are all simple, the same is necessarily true for those of $(R_1, \ldots, R_s)$.

4) It is an immediate consequence of Lemmata 5 and 6.

Corollary 2 *Given a standard basis $(F_1, \ldots, F_s)$ of I w.r.t. the weights $(a, b, \ldots b)$, let $\nu := b/a$, let d_i be the weight of* $\mathrm{in}(F_i)$*, let $\bar{\eta} := (\eta_2, \ldots, \eta_n)$ be a zero of*

$$\mathrm{in}_\nu(F_1)(1, X_2, \ldots, X_n) = \ldots = \mathrm{in}_\nu(F_s)(1, X_2, \ldots, X_n) = 0$$

and let

$$R_i(t, X_2, \ldots, X_n) := \psi_{\bar{\eta}}(F_i)/t^{d_i}.$$

Let $(u^c, V_2(u), \ldots, V_n(u))$, $V_i \in \mathbf{K}[[u]]$ be a parametrization of a branch of $\Gamma_{\bar{\eta}}$. Then

$$(u^{ac}, \eta_2 u^{bc} + u^{bc} V_2(u), \ldots, \eta_n u^{bc} + u^{bc} V_n(u))$$

is a parametrization of a branch of Γ.

Moreover each branch of Γ has a parametrization obtained as above.

It is useful to have some more insight into the conjugacy classes of the roots of $(G_1, \ldots, G_s)$. Let $\pi : K[X_1, \ldots, X_n] \to K[X_2, \ldots, X_n]$ be the projection given by $\pi(X_1) = 1$, $\pi(X_i) = X_i$. Let ζ be a primitive a^{th}-root of unity, $\zeta^a = 1$.

Let $J = \mathrm{in}_\nu(I) = (\mathrm{in}_\nu(F_1), \ldots, \mathrm{in}_\nu(F_s))$, so that $\pi(J) = (G_1, \ldots, G_s)$. Let $\bar{\eta} := (\eta_2, \ldots, \eta_n)$ be a zero of $\pi(J)$. Then $(t^a, \eta_2 t^b, \ldots, \eta_n t^b)$ is the generic zero of an irreducible component of the variety defined by J. Since $(t^a, \eta_2 \zeta^{ib} t^b, \ldots, \eta_n \zeta^{ib} t^b)$ is also a generic zero of the same component, $\bar{\eta}_i :=$

$(\eta_2\zeta^i, \ldots, \eta_n\zeta^i)$ is a zero of $\pi(J)$. It is possible to show that the $\bar{\eta}_i$'s are equivalent zeroes of $\pi(J)$.

Finally denote $\tau_i : \mathrm{K}[t, X_2, \ldots, X_n] \to \mathrm{K}[t, X_2, \ldots, X_n]$ the morphism such that $\tau_i(t) = \zeta^i t$ and $\tau_i(X_j) = \zeta^{-i} X_j$. One has $\psi_{\bar{\eta}_i} = \tau_i \psi_{\bar{\eta}}$ so that the the ideals of the $\bar{\eta}_i$-transformations of Γ are isomorphic. In conclusion:

Proposition 4 *Let $\bar{\eta} := (\eta_2, \ldots, \eta_n)$ be a root of $(G_1, \ldots, G_s)$, and let $\bar{\eta}_i := (\eta_2\zeta^i, \ldots, \eta_n\zeta^i)$, where ζ is a primitive a^{th}-root of unity. Then:*

1. *$\bar{\eta}_i$ is a zero of $(G_1, \ldots, G_s)$.*
2. *The $\bar{\eta}_i$'s are equivalent zeroes of $(G_1, \ldots, G_s)$*

Let us now refine the theorems above to discuss in details the real analytic branches.

Proposition 5 *Let $(P_2(X_1), \ldots, P_n(X_1))$ be a solution centered at the origin of $(F_1, \ldots, F_s)$, with*

$$P_2(X_1) = \sum c_{i2} X_1^{\nu_{i2}/\nu}, \ldots, P_n(X_1) = \sum c_{in} X_1^{\nu_{in}/\nu}$$

with $c_{ij} \neq 0$ $\nu, \nu_{ij} \in \mathbf{N}$, $\gcd(\nu_{ij}, \nu) = 1$, so that if ζ is a primitive ν-th root of 1, the ν solutions in the cycle of $(P_2, \ldots, P_n)$ are

$$P_{2j}(X_1) = \sum c_{i2} \zeta^{j\nu_{i2}} X_1^{\nu_{i2}/\nu}, \ldots, P_{nj}(X_1) = \sum c_{in} \zeta^{j\nu_{in}} X_1^{\nu_{in}/\nu}.$$

If ν is odd, consider the ν parametrizations of the branch

$$X_1 = t^\nu, X_2 = \sum c_{i2} \zeta^{j\nu_{i2}} t^{\nu_{i2}}, \ldots, X_n = \sum c_{in} \zeta^{j\nu_{in}} t^{\nu_{in}}$$

There is at most one such parametrization, which is "real" in the sense that all coefficients $c_{ik}\zeta^{j\nu_{ik}}$ are real, and there is exactly one if and only if the branch is real.

If ν is even let ξ be a primitive 2ν-root of 1 and consider the 2ν parametrizations of the branch:

$$X_1 = t^\nu, X_2 = \sum c_{i2} \xi^{j\nu_{i2}} t^{\nu_{i2}}, \ldots, X_n = \sum c_{in} \xi^{j\nu_{in}} t^{\nu_{in}} \quad j \text{ even}$$

$$X_1 = -t^\nu, X_2 = \sum c_{i2} \xi^{j\nu_{i2}} t^{\nu_{i2}}, \ldots, X_n = \sum c_{in} \xi^{j\nu_{in}} t^{\nu_{in}} \quad j \text{ odd}$$

There are either none or two real parametrizations; there are two if and only if the branch is real. In this case they are transformed into each other by the substitution $t \mapsto -t$.

In order to consider parametrizations of the kind

$$(-t^{\nu}, \sum c_{i2}t^{\nu_{i2}}, \ldots, \sum c_{in}t^{\nu_{in}})$$

we have to modify accordingly the results stated above.

Let $I = (F_1, \ldots, F_s)$ locally define an admissible curve Γ. Let us fix weights $(a, b, \ldots, b)$, where a is even and b is odd, and let $\nu := b/a$. Let us assume moreover that $(F_1, \ldots, F_s)$ is a standard basis of I for the weights $(a, b, \ldots b)$. Let ξ be a $2a^{th}$-primitive root of unity.

Let $\bar{\eta} := (\eta_2, \ldots, \eta_n) \in \mathbf{K}^{n-1}$, let $L := K(\eta_2, \ldots, \eta_n, \xi)$ and let $\psi_{\bar{\eta}} : L[X_1, \ldots, X_n] \to L[t, X_2, \ldots, X_n]$ be the morphism defined by the transformation

$$X_1 = t^a,\ X_2 = (\eta_2 + X_2)t^b,\ \ldots,\ X_n = (\eta_n + X_n)t^b$$

so that, for $F(X_1, \ldots, X_n) \in K[X_1, \ldots, X_n]$, denoting $d(F)$ the weight of $\mathrm{in}\,(F)$, one has:

$$\psi_{\bar{\eta}}(F) = t^{d(F)}\,\mathrm{in}\,(F)(1, \eta_2 + X_2, \ldots, \eta_n + X_n) + \ldots$$

Let $\rho : L[t, X_2, \ldots, X_n] \to L[t, X_2, \ldots, X_n]$ be the morphism such that

$$\rho(t) = \xi t, \quad \rho(X_i) = \xi^{-b}X_i \quad \text{for all } i$$

so that $\rho\psi_{\bar{\eta}} : L[X_1, \ldots, X_n] \to L[t, X_2, \ldots, X_n]$ is given by the transformation:

$$X_1 = -t^a,\ X_2 = (\xi^b\eta_2 + X_2)t^b,\ \ldots,\ X_n = (\xi^b\eta_n + X_n)t^b$$

and

$$\rho\psi_{\bar{\eta}}(F) = t^{d(F)}\,\mathrm{in}\,(F)(-1, \xi^b\eta_2 + X_2, \ldots, \xi^b\eta_n + X_n) + \ldots$$

Let now $\sigma : K[X_1, \ldots, X_n] \to K[X_1, \ldots, X_n]$ be the morphism such that

$$\sigma(X_1) = -X_1, \quad \sigma(X_i) = X_i \text{ for } i > 1$$

and let

$$\bar{\eta}^* := (\xi^b\eta_2, \ldots, \xi^b\eta_n).$$

It is immediate that

$$\rho\psi_{\bar{\eta}} = \psi_{\bar{\eta}^*}\sigma.$$

Let $\pi : K[X_1, \ldots, X_n] \to K[X_2, \ldots, X_n]$ be the projection such that $\pi(X_1) = 1,\ \pi(X_i) = X_i$. Let $J = \mathrm{in}\,(I) = (\mathrm{in}\,(F_1), \ldots, \mathrm{in}\,(F_s))$, so that

$$\pi(J) = (\mathrm{in}\,(F_1)(1, X_2, \ldots, X_n), \ldots, \mathrm{in}\,(F_s)(1, X_2, \ldots, X_n)).$$

Let $\bar\eta := (\eta_2, \ldots, \eta_n)$ be a zero of $\pi(J)$ so that $\bar\eta_{2i} := (\eta_2\xi^{2i}, \ldots, \eta_n\xi^{2i})$ is a zero of $\pi(J)$ for each i and $(t^a, \eta_2 t^b, \ldots, \eta_n t^b)$ is the generic zero of an irreducible component of the variety defined by J. Then $(-t^a, \eta_2\xi^b t^b, \ldots, \eta_n\xi^b t^b)$ is the generic zero of an irreducible component of the variety defined by $\sigma(J)$, so that, for each i, $\bar\eta_{2i+1} := (\eta_2\xi^{2i+1}, \ldots, \eta_n\xi^{2i+1})$ is a zero of $\pi\sigma(J) = (\mathrm{in}\,(F_1)(1, X_2, \ldots, X_n), \ldots, \mathrm{in}\,(F_s)(1, X_2, \ldots, X_n))$.

Extending the results of Proposition 4, we have:

Proposition 6 *The zeroes $\bar\eta_{2i}$ of $\pi(J)$ and the zeroes $\bar\eta_{2i+1}$ of $\pi\sigma(J)$ are equivalent. Moreover the $\bar\eta_{2i}$-transformations of Γ and the $\bar\eta_{2i+1}$-transformations of $\sigma(\Gamma)$ are all isomorphic. In particular this holds for the $\bar\eta$-transformation of Γ and the η^*-transformation of $\sigma(\Gamma)$.*

We have then the following generalization of Theorem 1:

Proposition 7 *Let $F_1, \ldots, F_s$ be a standard basis of I for the weights $(a, b, \ldots b)$, let $\nu := b/a$, with a even. Let*

$$G_i(X_2, \ldots, X_n) := \mathrm{in}_\nu(F_i)(-1, X_2, \ldots, X_n)$$

and let d_i be the weight of $\mathrm{in}_\nu(F_i)$. Then:

1) The ideal $(G_1, \ldots, G_s)$ is either the whole ring (i.e. it has no roots) or a 0-dimensional ideal.
Let $\bar\eta := (\eta_2, \ldots, \eta_n)$ be a zero of $(G_1, \ldots, G_s)$ and let $R_i(t, X_2, \ldots, X_n) = \psi_{\bar\eta}\sigma(F_i)/t^{d_i}$. Then:

2) $R_1, \ldots, R_s$ locally define an admissible curve $\Gamma_{\bar\eta}$.

3) $F_i(-t^a, \eta_2 t^b + t^b Q_2(t), \ldots, \eta_n t^b + t^b Q_n(t)) = 0$ for all i, if and only if

$$R_i(t, Q_2(t), \ldots, Q_n(t)) = 0$$

for all i and for $Q_i(t) \in \mathbf{K}[[t]]_{\mathrm{Puis}}$.

Corollary 3 *Let $(F_1, \ldots, F_s)$ be a standard basis of I w.r.t. the weights $(a, b, \ldots, b)$, let $\nu := b/a$, let d_i be the weight of $\mathrm{in}_\nu(F_i)$, let $\bar\eta := (\eta_2, \ldots, \eta_n)$ be a real zero of*

$$\mathrm{in}_\nu(F_1)(1, X_2, \ldots, X_n) = \ldots = \mathrm{in}_\nu(F_s)(1, X_2, \ldots, X_n) = 0$$

and let

$$R_i(t, X_2, \ldots, X_n) := \psi_{\bar\eta}(F_i)/t^{d_i}.$$

Let $((-1)^j u^c, V_2(u), \ldots, V_n(u))$, $V_i \in \mathbf{R}[[u]]$ *be a real parametrization of a real branch of* $\Gamma_{\bar\eta}$.

Then

$$((-1)^{aj}u^{ac}, (-1)^{bj}\eta_2 u^{bc} + (-1)^{bj}u^{bc}V_2(u), \ldots, (-1)^{bj}\eta_n u^{bc} + (-1)^{bj}u^{bc}V_n(u))$$

is a real parametrization of a real branch of Γ.

Let now a *be even, let* $\bar\eta := (\eta_2, \ldots, \eta_n)$ *be a real zero of*

$$\mathrm{in}_\nu(F_1)(-1, X_2, \ldots, X_n) = \ldots = \in_{nu}(F_s)(-1, X_2, \ldots, X_n) = 0$$

and let $R_i(t, X_2, \ldots, X_n) := \psi_{\bar\eta}\sigma(F_i)/t^{d_i}$. *Let* $((-1)^j u^c, V_2(u), \ldots, V_n(u))$, $V_i \in \mathbf{R}[[u]]$ *be a real parametrization of a real branch of* $\Gamma_{\bar\eta}$. *Then*

$$(-u^{ac}, (-1)^{bj}\eta_2 u^{bc} + (-1)^{bj}u^{bc}V_2(u), \ldots, (-1)^{bj}\eta_n u^{bc} + (-1)^{bj}u^{bc}V_n(u))$$

is a real parametrization of a real branch of Γ.

Moreover a real branch of Γ *has a parametrization obtained as above.*

We conclude this section by analyzing the case in which the $\bar\eta$-transformation of Γ has the origin as a simple point.

Proposition 8 *Assume* $(F_1, \ldots, F_s)$ *are a standard basis for the weights* $(a, b, \ldots, b)$ *which locally define an admissible curve* Γ. *Let* $G_i(X_2, \ldots, X_n)$ *be the polynomial* $\mathrm{in}(F_i)(1, X_2, \ldots, X_n)$, d_i *the pseudodegree of* $\mathrm{in}(F_i)$. *Let* $(\eta_2, \ldots, \eta_n)$ *be a simple zero of* $(G_1, \ldots, G_s)$, $L := K(\eta_2, \ldots, \eta_n)$.

Let $R_i(t, X_2, \ldots, X_n) = F_i(t^a, t^b(\eta_2 + X_2), \ldots, t^b(\eta_n + X_n))/t^{d_i}$. *Then the Jacobian matrix* $(\partial R_i/\partial X_j)_{ij}$ *has maximal rank at the origin. As a consequence there are* $n-1$ *linear combinations of the* R_i*'s,* $S_2, \ldots, S_n$ *such that*

1. $S_i(t, X_2, \ldots, X_n) = X_i + T_i(t, X_2, \ldots, X_n)$ *with* $T_i \in (t) + (X_2, \ldots, X_n)^2$;
2. *there are unique power series* $Q_j(t) \in L[[t]]$ *such that*

$$S_i(t, Q_2(t), \ldots, Q_n(t)) = 0;$$

3 $(Q_2, \ldots, Q_n)$ *is the unique solution centered at the origin of* $(R_1, \ldots, R_s)$.

Proof: First of all remark that $R_i(0, X_2, \ldots, X_n) = G_i(\eta_2 + X_2, \ldots, \eta_n + X_n)$, so that $\partial R_i/\partial X_j(0, X_2, \ldots, X_n) = \partial G_i/\partial X_j(\eta_2 + X_2, \ldots, \eta_n + X_n)$. Therefore the Jacobian matrix $(\partial R_i/\partial X_j)_{ij}$ has maximal rank at the origin if and only if the Jacobian matrix $(\partial G_i/\partial X_j)_{ij}$ has maximal rank at

$(\eta_2, \ldots, \eta_n)$. If the latter matrix has not maximal rank, then there are $c_2, \ldots, c_n \in L$, not all zero such that $c_2 \partial G_i/\partial X_2 + \ldots + c_n \partial G_i/\partial X_n$ vanishes at $(\eta_2, \ldots, \eta_n)$ for all i, against the assumption that $(\eta_2, \ldots, \eta_n)$ is a simple zero of $(G_1, \ldots, G_s)$. The other statement is an elementary consequence of the Implicit Function Theorem.

3 Outline of the Algorithm

We are now in a position to specify what we meant in Section 2.1 by "computing" all branches (and all real branches) centered at the singular points of Γ.

Assume that we are given $n-1$ polynomials

$$S_2(u, X_2, \ldots, X_n), \ldots, S_n(u, X_2, \ldots, X_n)$$

such that the Jacobian $(\partial S_i/\partial X_j)_{ij}$ is non-zero at the origin. Then by the Implicit Function Theorem, there are unique formal power series $Q_2(u), \ldots, Q_n(u)$ such that $S_i(u, Q_2(u), \ldots, Q_n(u)) = 0$ for all i; moreover any approximation of these series can be explicitly obtained by back substitution in the S_i.

Therefore we say that an analytic branch of Γ is given if we are given integers a, b, polynomials $T_2(t), \ldots, T_n(t)$, polynomials

$$S_2(t, X_2, \ldots, X_n), \ldots, S_n(t, X_2, \ldots, X_n)$$

such that:

1. the Jacobian $(\partial S_i/\partial X_j)_{ij}$ is non-zero at the origin.
2. denoting $Q_2(t), \ldots, Q_n(t)$ the unique formal power series such that, for all i, $S_i(t, Q_2(t), \ldots, Q_n(t)) = 0$ and $U_i(t) := T_i(t) + t^b Q_i(t)$ then $(t^a, U_2(t), \ldots, U_n(t))$ is a parametrization of the branch.

Analogously, we say that a real analytic branch of Γ is given if we are given integers j, k, a, b, real polynomials $T_2(t), \ldots, T_n(t)$, real polynomials $S_2(t, X_2, \ldots, X_n), \ldots, S_n(t, X_2, \ldots, X_n)$ such that:

1. the Jacobian $(\partial S_i/\partial X_j)_{ij}$ is non-zero at the origin.
2. denoting $Q_2(t), \ldots, Q_n(t)$ the unique formal power series such that, for all i, $S_i(t, Q_2(t), \ldots, Q_n(t)) = 0$ and $U_i(t) := T_i(t) + (-1)^k t^b Q_i(t)$ then $((-1)^j t^a, U_2(t), \ldots, U_n(t))$ is a real parametrization of the branch.

The algorithm by which, given a basis $(F_1, \ldots, F_s)$ of an ideal $I \in K[X_1, \ldots, X_n]$ defining an admissible curve Γ, we intend to compute all (real) analytic branches of Γ can be outlined at follows:

1. Check if I defines an admissible curve Γ
2. Compute the 0-dimensional ideal J whose roots are the singular points of Γ
3. Compute a splitting $(J_1, \ldots, J_t)$ of J s.t. $\forall i$ all the roots of J_i are equivalent and, denoting $K_i := K[X_1, \ldots, X_n]/J_i$, a set of polynomials in $K_i[X_1, \ldots, X_n]$ which are a standard basis of $\phi_\alpha(I)$ for each root α of J_i.
4. For each root α of J:
   (a) Compute all initial exponents ν of (real) solutions centered at α.
   (b) For each initial exponent ν:
      i. Compute a parametrization for each (real) solution centered at α with initial exponent ν.

Remark that the phrasing "*For each root α of J*" has been chosen just to avoid being unnecessarily cumbersome: computation of initial exponents and of analytic branches is not to be performed separately for each root of J but just for each "generic" root of J_i; if different roots of J_i have different patterns for initial exponents or analytic branches, this will be revealed by an appropriate splitting of J_i.

The actual output of the algorithm will be

1. a splitting $(J_1, \ldots, J_u)$ of J;
2. for all i, a set of "parametrizations"

   $$\{(\pm t_\lambda^a, U_{2\lambda}(t), \ldots, U_{n\lambda}(t))\},$$

   with $U_{j\lambda}(t)$ a formal power series with coefficients in $K[X_1, \ldots, X_n]/J_i$ such that if for each root $\alpha := (\alpha_1, \ldots, \alpha_n)$ of the ideal J_i, we denote $\pi_\alpha : K[X_1, \ldots, X_n]/J_i \mapsto K(\alpha_1, \ldots, \alpha_n)$ the canonical projection, then $\forall \alpha$ root of J_i,

   $$\{(\pm t_\lambda^a, \pi_\alpha(U_{2\lambda}(t)), \ldots, \pi_\alpha(U_{n\lambda}(t)))\}$$

   gives a parametrization for each solution centered at α.

It is obvious that a single computation is required for each set of K-conjugate roots of J, but even roots which are not conjugate are possibly not splitted by the algorithm, and even in case non-conjugate roots are completely separated by the algorithm, this is performed with no need of decomposing J by a primary decomposition algorithm. In particular moreover, only one parametrization for each cycle is explicitly computed, since solutions within the same cycle will never be splitted in this model.

4 The Algorithm

4.1 Testing the Algebraic Conditions and Computing Singular Points

We discuss here briefly how to test whether the ideal $I := (F_1, \ldots, F_s) \in K[X_1, \ldots, X_n]$, where K is a finite algebraic extension of the rationals, defines an admissible curve Γ.

First we compute a Gröbner basis of I, by which we can read the dimension of I. If the dimension of I is 1, we can then test whether I is radical and unmixed, by computing its top-radical $toprad(I)$, i.e. the intersection of the prime components of I of maximal dimension (remark that most of the algorithms for computing the radical of an ideal, actually need the computation of the top-radical as an intermediate step). The knowledge of a Gröbner basis of the $toprad(I)$ w.r.t. suitable (elimination) orderings, allows also to check whether $x_1 \in K[x_1, \ldots, x_n] = K[X_1, \ldots, X_n]/I$ is algebraic over K.

If $dim(I) = 1$ and x_1 is not algebraic over K, then $toprad(I)$ defines an admissible curve Γ which is the union of the irreducible curve components of the variety defined by I; in this case, if $I = toprad(I)$, then I satisfies the assumptions; otherwise, the algorithm can still be applied to $toprad(I)$.

If x_1 is algebraic over K, this is revealed by a polynomial $f \in toprad(I) \cap K[X_1]$. Then $toprad(I) : (f)^* = \{g : \exists d \; f^d g \in toprad(I)\}$ defines the admissible curve consisting of the irreducible components of the variety defined by $toprad(I)$ not contained in some hyperplane $X_1 = \alpha_1$. Moreover if α is a root of f, then $toprad(I) + (X_1 - \alpha)$ defines the admissible curve consisting of the irreducible components of the variety defined by $toprad(I)$ contained in the hyperplane $X_1 = \alpha$. So the algorithm can be applied separately to $toprad(I) : (f)^*$ and $toprad(I) + (X_1 - \alpha)$.

Assuming now that I defines an admissible curve Γ, the singular points of Γ are the roots of the 0-dimensional ideal generated by $(F_1, \ldots, F_s)$ and by the maximal minors of the Jacobian matrix $(\partial F_i / \partial X_j)_{ij}$.

4.2 Finding Initial Exponents

To compute the initial exponents of branches of I at a singular point α, by applying the morphism ϕ_α, we can assume w.l.o.g. that α is the origin.

The computation of initial exponents can then be reduced to the computation of the critical tropisms of I, because of the following results:

Proposition 9 *Let $\nu \in \mathbf{Q}^+$. If ν is the initial exponent of an analytic branch of I at the origin, then $in_\nu(I)$ is not bihomogeneous.*

Proof: Let a, b be positive integers s.t. $\nu = b/a$. Let $(F_1, \dots, F_s)$ be a standard basis of I w.r.t. the weights $(a, b, \dots, b)$ and let $G_i := in_\nu(F_i)(1, X_2, \dots, X_n)$. If the ideal $in_\nu(I)$ is bihomogeneous, then the ideal $(G_1, \dots, G_s) \subset K[X_2, \dots, X_n]$ is homogeneous. Since it has at most finitely roots because of Theorem 1, then its only root is the origin, so that ν is not an initial exponent of an analytic branch of I.

Corollary 4 *If ν is the initial exponent of an analytic branch of I at the origin, then ν is a critical tropism of I.*

We can therefore apply the algorithm sketched in Section 2.3 to compute the critical tropisms of I. Remark that the output of Step 3 of the algorithm is exactly what one needs for the critical tropism computation.

4.3 Finding all Solutions with a given Initial Exponent

Let us now fix a positive rational ν and let us show how to compute parametrizations for all analytic branches at the origin with initial exponent ν of $I = (F_1, \dots, F_s)$. Let $a, b \in \mathbf{N}$ be such that $b/a = \nu$, $\gcd(a, b) = 1$.

1. Compute a standard basis $(H_1, \dots, H_t)$ of the ideal $(F_1, \dots, F_s)$ w.r.t. the weights $(a, b, \dots, b)$.

   The standard basis computation can be performed by means of the Tangent Cone Algorithm [20], which has the advantage of returning a Gröbner basis of the ideal $J_0 = (G_1, \dots, G_t)$.

2. Let $G_i := \mathrm{in}_\nu(H_i)(1, X_2, \dots, X_n)$ and $d_i := wt(H_i)$ and let $J_0 := (G_1, \dots, G_t)$

   The ideal J_0 has at most finitely many roots and its roots are the coefficients of the initial approximations of the solutions centered at the origin with initial exponent ν.

3. Compute the ideal $J := J_0 : \mathbf{m}^* = \bigcup_{d=1}^{\infty} J_0 : \mathbf{m}^d$.

   The roots of J are exactly the non-zero roots of the ideal J_0 and they have the same multiplicity in the two ideals. A Gröbner basis for the ideal J can be obtained from the Gröbner basis $(G_1, \ldots, G_t)$ either by several Gröbner basis computations (there are different schemes to do that [24]) or more efficiently by a linear algebra algorithm [13, 22].

4. Compute a splitting $(J_1, \ldots, J_u)$ of J s.t. $\forall i$ all the roots of J_i are equivalent, the roots of J_1 being the simple roots of J

5. Denoting $(\eta_2, \ldots, \eta_n)$ the generic root of the ideal J_1, compute $R_i(t, X_2, \ldots, X_n) := H_i(t^a, t^b(\eta_2+X_2), \ldots, t^b(\eta_n+X_n))/t^{d_i}$; $S_2, \ldots, S_n$ satisfying the conditions of Proposition 8; return:

$$[(t^a, \eta_2 t^b, \ldots, \eta_n t^b);\ t^b;\ (S_2, \ldots, S_n)].$$

   Since the roots of J_1 are the simple roots of J, Proposition 8 implies that:

   - there are unique formal power series $Q_i(t)$ such that:

$$R_j(t, Q_2(t), \ldots, Q_n(t)) = 0 \quad \forall\, j$$

   - $(t^a, \eta_2 t^b + t^b Q_2(t), \ldots, \eta_2 t^b + t^b Q_2(t))$ is a parametrization of the unique analytic branch with initial approximation $(\eta_2 t^\nu, \ldots \eta_n t^\nu)$.

   As it was specified in section 3, the returned information is what we intend by "computing" a solution centered at the origin, and it is sufficient to compute polynomial approximations of any order.

6. For each $i = 2, \ldots, u$, denoting $(\eta_2, \ldots, \eta_n)$ the generic root of J_i:

   (a) compute

$$R_i(t, X_2, \ldots, X_n) := H_i(t^a, t^b(\eta_2 + X_2), \ldots, t^b(\eta_n + X_n))/t^{d_i}$$

   (b) compute a parametrization for each solution centered at the origin of $(R_1, \ldots, R_t)$, i.e. compute all

$$[(u^c, T_2(u), \ldots, T_n(u));\ u^d;$$

$$(S_2(u, X_2, \ldots, X_n), \ldots, S_n(u, X_2, \ldots, X_n))]$$

such that $(u^c, T_2(u) + u^d Q_2(u), \ldots, T_n(u) + u^d Q_n(u))$ is a parametrization of a solution centered at the origin of $(R_1, \ldots, R_t)$, where $Q_i(u)$ denote the unique formal power series such that, for all j, $S_i(u, Q_2(u), \ldots, Q_n(u)) = 0$.

(c) For each parametrization

$$[(u^c, T_2(u), \ldots, T_n(u));\ u^d;$$
$$(S_2(u, X_2, \ldots, X_n), \ldots, S_n(u, X_2, \ldots, X_n))]$$

return

$$[(u^{ac}, \eta_2 u^{bc} + u^{bc} T_2(u), \ldots, \eta_n u^{bc} + u^{bc} T_n(u));\ u^{bc+d};$$
$$(S_2(u, X_2, \ldots, X_n), \ldots, S_n(u, X_2, \ldots, X_n))]$$

so that

$$(u^a c, \eta_2 u^{bc} + u^{bc} T_2(u) + u^{bc+d} Q_2(u), \ldots,$$
$$\eta_n u^{bc} + u^{bc} T_n(u) + u^{bc+d} Q_n(u))$$

is a parametrization of a branch of Γ, denoting again $Q_i(u)$ the unique formal power series such that, for all j:

$$S_j(u, Q_2(u), \ldots, Q_n(u)) = 0.$$

Here we apply instead Theorem 1 which implies that

$$(u^a c, \eta_2 u^{bc} + u^{bc} T_2(u) + u^{bc+d} Q_2(u), \ldots, \eta_n u^{bc} + u^{bc} T_n(u) + u^{bc+d} Q_n(u))$$

is a parametrization of a solution centered at the origin of $(F_1, \ldots, F_s)$, if and only if

$$(u^c, T_2(u) + u^d Q_2(u), \ldots, T_n(u) + u^d Q_n(u))$$

is a parametrization of a solution centered at the origin of $(R_1, \ldots, R_t)$

Let us describe the modifications in the algorithm needed to compute only the real analytic branches; the modifications apply only to Steps (5) and (6) which are to be modified as follows:

5a) If J_1 has real roots, denoting $(\eta_2, \dots, \eta_n)$ the generic root of J_1, compute $R_i(t, X_2, \dots, X_n) := H_i(t^a, t^b(\eta_2 + X_2), \dots, t^b(\eta_n + X_n))/t^{d_i}$; $S_2, \dots, S_n$ satisfying the conditions of Proposition 8; return:

$[(t^a, \eta_2 t^b, \dots, \eta_n t^b);\ t^b;\ (S_2, \dots, S_n)]$

5b) If a is even, let ξ be a primitive $2a^{th}$-root of unity and let L_1 be the ideal whose roots, all simple, are:

$$\{(\eta_2 \xi^b, \dots, \eta_n \xi^b) : (\eta_2, \dots, \eta_n) \text{ a root of} J_1\}.$$

If L_1 has real roots, denoting $(\eta_2, \dots, \eta_n)$ its generic root, compute $R_i(t, X_2, \dots, X_n) = H_i(-t^a, t^b(\eta_2 + X_2), \dots, t^b(\eta_n + X_n))/t^{d_i}$; and $S_2, \dots, S_n$ satisfying the conditions of Proposition 4; return:

$$[(-t^a, \eta_2 t^b, \dots, \eta_n t^b);\ t^b;\ (S_2, \dots, S_n)]$$

6a) For each $i = 2, \dots, u$, s.t. J_i has real roots, denoting $(\eta_2, \dots, \eta_n)$ the generic root of J_i:

(a) compute

$$R_i(t, X_2, \dots, X_n) := H_i(t^a, t^b(\eta_2 + X_2), \dots, t^b(\eta_n + X_n))/t^{d_i}$$

(b) compute a parametrization for each real solution centered at the origin of $(R_1, \dots, R_t)$, i.e. compute all

$$[((-1)^j u^c, T_2(u), \dots, T_n(u));\ (-1)^k u^d;$$

$$(S_2(u, X_2, \dots, X_n), \dots, S_n(u, X_2, \dots, X_n))]$$

where T_i, S_i have real coefficients and are such that

$$((-1)^j u^c, T_2(u) + (-1)^k u^d Q_2(u), \dots, T_n(u) + (-1)^k u^d Q_n(u))$$

is a real parametrization of a real solution centered at the origin of $(R_1, \dots, R_t)$, where $Q_i(u)$ denote the unique formal power series such that, for all j, $S_i(u, Q_2(u), \dots, Q_n(u)) = 0$.

(c) For each real parametrization

$$[((-1)^j u^c, T_2(u), \dots, T_n(u));\ (-1)^k u^d;$$

$$(S_2(u, X_2, \dots, X_n), \dots, S_n(u, X_2, \dots, X_n))]$$

return:

$$[((-1)^{aj}u^{ac}, (-1)^{bj}\eta_2 u^{bc} + (-1)^{bj}u^{bc}T_2(u), \dots,$$
$$(-1)^{bj}\eta_n u^{bc} + (-1)^{bj}u^{bc}T_n(u));$$
$$(-1)^{bj+k}u^{bc+d};\ (S_2(u, X_2, \dots, X_n), \dots, S_n(u, X_2, \dots, X_n))]$$

6b) If a is even, let ξ be a primitive $2a^{th}$-root of unity and let L_i be the ideal whose roots are $\{(\eta_2\xi^b, \dots, \eta_n\xi^b) : (\eta_2, \dots, \eta_n) \text{ is a root of } J_i\}$. If L_1 has real roots, denoting $(\eta_2, \dots, \eta_n)$ its generic root:

(a) compute

$$R_i(t, X_2, \dots, X_n) := H_i(-t^a, t^b(\eta_2 + X_2), \dots, t^b(\eta_n + X_n))/t^{d_i}$$

(b) compute a parametrization for each real solution centered at the origin of $(R_1, \dots, R_t)$, i.e. compute all

$$[((-1)^j u^c, T_2(u), \dots, T_n(u));\ (-1)^k u^d;$$
$$(S_2(u, X_2, \dots, X_n), \dots, S_n(u, X_2, \dots, X_n))]$$

(c) For each real parametrization

$$[((-1)^j u^c, T_2(u), \dots, T_n(u));\ (-1)^k u^d;$$
$$(S_2(u, X_2, \dots, X_n), \dots, S_n(u, X_2, \dots, X_n))]$$

return:

$$[(-u^{ac}, (-1)^{bj}\eta_2 u^{bc} + (-1)^{bj}u^{bc}T_2(u), \dots,$$
$$(-1)^{bj}\eta_n u^{bc} + (-1)^{bj}u^{bc}T_n(u));$$
$$(-1)^{bj+k}u^{bc+d};\ (S_2(u, X_2, \dots, X_n), \dots, S_n(u, X_2, \dots, X_n))]$$

There are some comments to make about the modifications to the algorithm to adapt it to the real case:

1) We use the multivariate versions of Sturm Theorem ([23]) to decide whether a 0-dimensional ideal J_i has real zeroes

2) To compute L_i from J_i we do the following: we homogeneize a basis of J_i w.r.t. the variable X_1, obtaining a pseudohomogeneous ideal I_i such that $J_i = \pi(I_i)$; then L_i is simply obtained by $L_i = \pi\sigma(I_i)$.

3) The recursive calls of the algorithm are performed in the computational model for algebraic numbers described in Section 2.1; so they are done once for all roots of J_i (resp. L_i) provided that J_i (resp. L_i) has at least one real root. However when returning the results in the outmost level of recursion, we use the seminumerical techniques advocated in [7] to obtain floating point approximations of all real algebraic numbers appearing as coefficients.

4) Therefore in particular the polynomials S_i will have floating point coefficients and the computation of polynomial approximations of the formal power series solutions of the S_i will be performed numerically, so that our final output will be polynomial approximations of Puiseux series with floating point coefficients.

5 Correctness of the Algorithm

Let $I = (F_1, \ldots, F_s)$ locally define an admissible curve Γ, so that I has actually solutions centered at the origin.

To guarantee the correctness of the algorithm we need to show that all solutions centered at the origin are found by it. This is a consequence of the following:

Proposition 10 *With notation and assumptions of Theorem 1, if $\bar{\eta}$ is a root of $(G_1, \ldots, G_s)$ with multiplicity h then $(R_1, \ldots, R_s)$ has exactly h solutions centered at the origin (because of Theorem 1, the h solutions are simple and so are all distinct).*

Correctness of the algorithm follows now immediately; in fact: at Step 5) for each simple root $\bar{\eta}$ of J_1 the Algorithm returns the single solution of the $\bar{\eta}$-transformation of a curve; at Step 6), for a root $\bar{\eta}$ of J with multiplicity h, the Algorithm is called recursively to the ideal $(R_1, \ldots, R_s)$ which has exactly h solutions centered at the origin, and by an inductive argument, all such solutions are necessarily returned.

As an immediate consequence of Theorem 1 and Proposition 10, we get the following rigorous formulation of an argument by MacMillan [17] to count the number of solutions centered at the origin with a given initial exponent ν:

Theorem 2 *Let* $(F_1,\ldots,F_s)$ *locally define an admissible curve* Γ *and moreover be a standard basis for the weights* $(a,b,\ldots,b)$. *Let* $\nu := b/a$. *Let* $G_i(X_2,\ldots,X_n) = \mathrm{in}_\nu(F_i)(1,X_2,\ldots,X_n)$. *Then:*

1. *the multiplicity of the ideal* $(G_1,\ldots,G_s)$ *is the number of solutions centered at the origin with initial exponent* $\mu \geq \nu$;

2. *the multiplicity of the origin as a zero of* $(G_1,\ldots,G_s)$ *is the number of solutions centered at the origin with initial exponent* $\mu > \nu$;

3. *if* $(\eta_2,\ldots,\eta_n)$ *is a zero of* $(G_1,\ldots,G_s)$, *different from the origin, with multiplicity* h, *then* h *is the number of solutions centered at the origin with initial approximation* $X_2 = \eta_2 X_1^{b/a},\ldots,X_n = \eta_n X_1^{b/a}$.

Moreover, the multiplicity of the origin as a root of $I + (X_1)$ *is the number of solutions of* I *centered at the origin.*

This allows, while performing the computation of branches with initial exponent ν, to control the number of solutions with initial exponents equal, greeater then, lesser than ν. As a consequence we are allowed greater flexibility in looking for initial exponents than the one given by the algorithm in Section 2.3. Remark in fact that Lemma 4 allows to find critical tropisms as well from below, as in the algorithm, as from above. We made use of this flexibility in the examples reported in Section 8

6 Termination of the Algorithm

We have yet to prove termination of the algorithm; the only possibility for the algorithm to continue forever is that the recursive call in Step 6.b) is performed infinitely many times. We would have therefore an infinite sequence of:

- admissible curves $\Gamma_1,\ldots,\Gamma_r,\ldots$
- polynomial sets $\{F_{i1},\ldots,F_{is_i}\}$
- exponents $\nu_i = b_i/a_i$
- points $\bar{\eta}_i = (\eta_{2i},\ldots,\eta_{ni}) \in \mathbf{K}^{n-1}$
- integers h_i

related as follows:

$\{F_{i1},\ldots,F_{is_i}\}$ is a standard basis of Γ_i w.r.t. the weights $(a_i,b_i,\ldots,b_i)$.

$(1,\eta_{2i},\ldots,\eta_{ni})$ is a zero of $\mathrm{in}\,(F_{i1})=\ldots=\mathrm{in}\,(F_{is_i})=0$ of multiplicity h_i.

Γ_{i+1} is generated by $\psi_{\bar{\eta}_i}(F_{ij})/t^{d(F_{ij})}$ and has exactly h_i solutions centered at the origin.

We can then make the following remarks:

1. the sequence of the h_i's is non increasing, so it must stabilize to a common minimal value h;
2. moreover $h>1$ (otherwise termination is assured);
3. if $a_i>1$ then $(1,\zeta\eta_{2i},\ldots,\zeta\eta_{ni})$ is a zero of $\mathrm{in}\,(F_{i1})=\ldots=\mathrm{in}\,(F_{is_i})$ for each ζ such that $\zeta^{a_i}=1$;
4. therefore if $a_i>1$ then $h_{i-1}\geq a_ih_i>h_i$;
5. so there is N such that for $i\geq N$ we have $a_i=1$, $h_i=h>1$.

The admissible curves Γ_i have therefore h distinct solutions centered at the origin,

$$(P_{2ij}(X_1),\ldots,P_{nij}(X_1))_{j=1\ldots h}$$

with $P_{lij}(X_1)\in\mathbf{K}[[X_1]]$. Moreover

$$P_{lij}(X_1)=\eta_{li}X_1^{b_i}+X_1^{b_i}P_{l(i+1)j}(X_1)$$

for each l,i,j. Therefore if we set $c_N:=b_N$, $c_i:=c_{i-1}+b_i$ for all $i>N$ one has that $\sum_{i=N}^{M}\eta_{li}X_1^{c_i}$ is an approximation of P_{lNj} of order c_M for all j,M, against the assumption that the solutions of Γ_N are distinct.

7 A Complete Example

We apply now our algorithm to compute the analytic branches of the curve Γ defined by $I=(F_1,F_2)\in\mathbf{Q}[x,y,z]$ with:

$$F_1=(x^4-x^2y+y^4-2y^3+y^2)(x^4+x^2y-x^2+y^4-2y^3+y^2)=$$

$$=y^8+2y^4x^4+x^8-4y^7-4y^3x^4+6y^6-y^4x^2+y^2x^4-x^6-4y^5+2y^3x^2+yx^4+y^4-y^2x^2$$

$$F_2=z^2+y^2+x^2-y-3/4=z^2+(y-1/2)^2+x^2-1$$

where we look for Puiseux expansions in $\mathbf{C}[[z]]_{\mathrm{Puis}}$.

The suspicious reader will have already noticed that we are cheating but we pray him to go on, waiting for our apologies at the end of the Section.

The singular points of Γ are the 8 roots of the radical ideal

$$J = (z^2 - 3/4, x^3 - 1/4x, y^2 + x^2 - y, yx - 1/2x).$$

Let therefore $K = \mathbf{Q}[a, b, c] = \mathbf{Q}[x, y, z]/J$, $\phi : K[x, y, z] \mapsto K[x, y, z]$ be defined by:

$$\phi(x) = x + a, \phi(y) = y + b, \phi(z) = z + c$$

A standard basis computation of $\phi(I)$ w.r.t. weights $(0, 0, 1)$ gives the following splitting of J:

$$J_1 = (z^2 - 3/4, y - 1/2, x^2 - 1/4)$$

$$J_2 = (z^2 - 3/4, y^2 - y, x)$$

and, denoting $K_i := \mathbf{Q}[a, b, c] = \mathbf{Q}[x, y, z]/J_i$, the following sets of polynomials which are a standard basis of $\phi(I)$ in $K_1[x, y, z]$, $K_2[x, y, z]$, resp.:

$(y^8 + 2y^4x^4 + x^8 + 8by^7 - 4y^7 + 8ay^4x^3 + 8by^3x^4 - 4y^3x^4 + 8ax^7 - 28a^2y^6 + 6y^6 + 12a^2y^4x^2 - y^4x^2 - 12a^2y^2x^4 + y^2x^4 + 28a^2x^6 - x^6 + 8by^5 - 4y^5 - 4by^3x^2 + 2y^3x^2 - 8ay^2x^3 - 2byx^4 + yx^4 + 8ax^5 - 3a^2y^4 + y^4 - 6a^2y^2x^2 - y^2x^2 + 4a^2x^4 - ay^2x - 1/4a^2y^2$,
$2az^2 + 2ay^2 + 2ax^2 + 4caz + x)$

$(-z^8 - 4z^6y^2 - 6z^4y^4 - 4z^2y^6 + 6z^4x^4 + 12z^2y^2x^4 + 8y^4x^4 + 8z^2x^6 + 8y^2x^6 + 4x^8 - 8cz^7 - 8bz^6y + 4z^6y - 24cz^5y^2 - 24bz^4y^3 + 12z^4y^3 - 24cz^3y^4 - 24bz^2y^5 + 12z^2y^5 - 8czy^6 + 24cz^3x^4 + 24bz^2yx^4 - 12z^2yx^4 + 24czy^2x^4 + 32by^3x^4 - 16y^3x^4 + 16czx^6 + 16byx^6 - 8yx^6 - 18z^6 - 48cbz^5y + 24cz^5y - 42z^4y^2 - 96cbz^3y^3 + 48cz^3y^3 - 30z^2y^4 - 48cbzy^5 + 24czy^5 + z^4x^2 + 2z^2y^2x^2 + 19z^2x^4 + 48cbzyx^4 - 24czyx^4 + 8y^2x^4 - x^6 - 24cz^5 - 72bz^4y + 36z^4y - 48cz^3y^2 - 80bz^2y^3 + 40z^2y^3 - 24czy^4 + 4cz^3x^2 + 4bz^2yx^2 - 2z^2yx^2 + 4czy^2x^2 + 2czx^4 - 9z^4 - 48cbz^3y + 24cz^3y - 18z^2y^2 - 16cbzy^3 + 8czy^3 + 3z^2x^2 + 8cbzyx^2 - 4czyx^2$,
$2bz^2 - z^2 + 2by^2 - y^2 + 2bx^2 - x^2 + 4cbz - 2cz + y)$

We discuss now separately the two cases.

For the 4 singular points (a, b, c) which are roots of J_1, from the standard basis we read the first critical tropism $\nu = 1$. Moreover evaluating the standard basis at $z = 0$ we obtain that a basis of $\mathrm{in}(\phi(I), z)$ is (y^2, x) so that the origin has multiplicity 2 as a root of $(\phi(I), z)$, i.e. there are two solutions centered at each (a, b, c).

We then compute a basis of $\mathrm{in}_1(\phi(I))$ and evaluate it at $z = 1$, obtaining $(y^2, 4ca + x)$ i.e. the double root $y = 0, x = -4ac$. We apply then the transformation obtaining:

$(-32caz^6y^4x^3 - 32caz^6x^7 + z^6y^8 + 2z^6y^4x^4 + z^6x^8 - 96caz^6y^4x + 8az^5y^4x^3 - 672caz^6x^5 + 8az^5x^7 - 24cz^5y^4x^2 + 36z^6y^4x^2 - 56cz^5x^6 + 84z^6x^6 - 16caz^4y^4x + 72az^5y^4x - 2016caz^6x^3 + 32caz^4y^2x^3 - 144caz^4x^5 + 504az^5x^5 - 24cz^5y^4 + 18z^6y^4 - z^4y^6 + 2z^4y^4x^2 - 840cz^5x^4 + 630z^6x^4 - 2z^4y^2x^4 + 6z^4x^6 - 864caz^6x + 96caz^4y^2x - 1440caz^4x^3 + 2520az^5x^3 - 8az^3y^2x^3 + 8az^3x^5 + 6z^4y^4 - 1512cz^5x^2 + 756z^6x^2 + 24cz^3y^2x^2 - 36z^4y^2x^2 - 40cz^3x^4 + 270z^4x^4 - 1296caz^4x + 1512az^5x + 20caz^2y^2x - 72az^3y^2x - 16caz^2x^3 + 240az^3x^3 - 216cz^5 + 81z^6 + 24cz^3y^2 - 18z^4y^2 + 1/4z^2y^4 - 240cz^3x^2 + 810z^4x^2 - 5/2z^2y^2x^2 + z^2x^4 - 48caz^2x + 360az^3x - azy^2x - 72cz^3 + 162z^4 + czy^2 - 15/2z^2y^2 + 18z^2x^2 + 9z^2 - 1/16y^2,$

$2/3czy^2 + 2/3czx^2 + 4/3cax - 4azx + 8/3cz)$

which is is easily seen to be a standard basis for the weights $(1,1,1)$ of the ideal I_1 it generates. Evaluating $\mathrm{in}_1(I_1)$ at $z=1$ we obtain the ideal $(9-1/16y^2, 8a+x)$, which has two simple roots, corresponding to two distinct solutions.

Therefore at each of the 4 singular points (a,b,c) which are roots of J_1 we find two solutions with initial exponent 1,

$$x = -4acz - 8az^2 + \dots, \quad y = \pm 12z^2 + \dots$$

corresponding to two distinct branches of order 1, which are tangent each other. These branches can be expressed by formal power series over the field $\mathbf{Q}[a,b,c]$; since the four roots of J_1 are easily seen to be all real, the eight branches we have found are real.

Let us now consider the behaviour of Γ at one of the 4 singular points (a,b,c) which are roots of J_2. In this case, from the standard basis, we obtain that the first critical tropism is $\nu = 1/3$. Moreover evaluating the standard basis at $z=0$ we obtain that a basis of $\mathrm{in}(\phi(I),z)$ is is $(8y^2x^4 - x^6, y)$ so that the origin has multiplicity 6 as a root of $(\phi(I),z)$, i.e. there are six solutions centered at each (a,b,c).

Computing $\mathrm{in}_{1/3}(\phi(I))$ and evaluating at $z=1$ we obtain the ideal (y,x^6), whose only root is the origin with multiplicity 6; so the critical tropism $1/3$ doesn't correspond to an inital exponent.

This computation gives us also the next critical tropism $\nu = 1/2$. We compute then $\mathrm{in}_{1/2}(\phi(I))$ and evaluate it at $z=1$, obtaining $(-x^6 - 2cx^4 - 3x^2, y)$, which has the origin as a double root; removing the origin we obtain $(x^4 + 2cx^2 + 3, y)$, which has four simple roots (all of them complex), each of them giving a solution with initial exponent $1/2$ and so in total two (complex) branches of order 2.

The next critical tropism is $\nu = 1$; The evaluation of $\mathrm{in}_{1/2}(\phi(I))$ at $z=1$ is $(4cb - 2c + y, x^2 - 3)$ giving two non-zero simple roots ans so two solutions with initial exponent 1 corresponding to two branches of order 1, both of them real.

As we hinted above, we have been cheating; what we did was to take the tachnode in the (x, y)-plane with equation $x^4 - x^2y + y^4 - 2y^3 + y^2 = 0$ which has singular points at the origin, with two (complex) branches of order 2, and at $(0, 1)$ with two real branches of order 1, crossing each other transversally. We then rotated it of π around $(0, 1/2)$ so that the singular points were mapped one into the other. The union of the two curves has now two singular points, each of them being the center of two complex branches of order 2 and two real branches of order 1; the branches centered at one point are mapped in those centered at the other point by the rotation. Two more singular points appear in the other two intersection points of the two tachnodes, which are $(\pm 1/2, 1/2)$; in these two points the two tachnodes are cotangent.

We then took the intersection of the cylinder in the direction of the z-axis generated by the union of the two tachnodes, with the sphere of center $(0, 1/2, 0)$ and radius 1. Each of the four singular points gives rise to two singular points on on each emisphere; the eight singular points are:

$$(0, 0, \sqrt{3}/2) \quad (0, 0, -\sqrt{3}/2) \quad (0, 1, \sqrt{3}/2) \quad (0, 1, -\sqrt{3}/2)$$

$$(1/2, 1/2, \sqrt{3}/2) \quad (1/2, 1/2, -\sqrt{3}/2) \quad (-1/2, 1/2, \sqrt{3}/2) \quad (-1/2, 1/2, -\sqrt{3}/2)$$

They are conjugate in pairs, but it is obvious that the group of the four rotations of the space around the center of the sphere which map the curve in itself has two orbits on the set of singular points. Therefore for any two points in the same orbit, there is a rotation in the group which maps the branches centered at one point in those centered at the other point.

This explains our choice of the example:

- while our algorithm is completely unaware of all of this, the human reader can easily verify the correctness of the computation, , with this simple theoretical argument;
- moreover we have supported the claim of the superiority of a "weak" model for algebraic number arithmetics over the "classical" one; we needed to perform only a single computation for each set of points in the same orbit, while in the classical model a computation for each class of conjugate points would be needed (and it could have been easy to modify the example, just by suitably choosing the radius of the sphere, so that all eight singular points would be rational, and eight distinct computations would be required)

8 Some Experimentations in CoCoA

While the algorithm outlined here is not implemented, we have performed some experimentation in CoCoA (version 1.5.3), a system for symbolic computations in Commutative Algebra and Algebraic Geometry developed at the Mathematics Department of the University of Genoa by A. Giovini and G. Niesi [2, 10]. This system, written partly in Pascal and partly in C, runs on any computer of the Macintosh or MS-DOS family. It allows to compute Gröbner bases and standard bases of polynomial ideals over $\mathbf{Q}$ or $\mathbf{Z}_p$, to perform ideal operations and to compute invariants of ideals. In particular it computes multiplicities of ideals. It must be remarked that the algorithms to perform these operations are not (in the 0-dimensional case) the efficient linear algebra ones, but are founded on Gröbner basis computations; in particular the division $J_0 : \mathbf{m}^*$ requires n Gröbner basis computations and can be quite costly. CoCoA allows also to compute Gröbner bases for polynomial ideals over a field $\mathbf{Q}(\eta_2, \ldots, \eta_n)$ where $(\eta_2, \ldots, \eta_n)$ is a root of a zero-dimensional ideal I, at least in the case in which the surjection $\mathbf{Q}[X_2, \ldots, X_n]/I \to \mathbf{Q}(\eta_2, \ldots, \eta_n)$ is actually a bijection. Standard basis computations in this setting are not available in CoCoA 1.5.3, but are present in an experimental version. In both cases, the algorithms can be applied also in case the surjection is not a bijection, but then a careful interpretation of the output is needed. CoCoA has no facility to recognize real roots of systems not for multiplicity handling. Therefore it can be used for all steps of the algorithm outlined in section 7 except Step (4) and real-root recognition where ad hoc hand-driven computations are required.

Here we focus on Steps (1) to (3) which can be performed by the following instructions in CoCoA.

$h = \mathsf{TangentCone}(i)$; $h = h[z = 1]$; $\mathsf{Mult}(R/h)$
computes the standard basis $(H_1, \ldots, H_t)$ of $(F_1, \ldots, F_s)$, returns J_0 and computes its multiplicity.

$j = h : \mathsf{ideal}(x^m, y^m)$; $k = \mathsf{gbasis}(j)$; $\mathsf{Mult}(R/j)$
removes the null root, counts the number of non zero roots, with multiplicity, and gives the ideal J; m is the multiplicity of J_0.

The tables below report an outline of the computation (with timings in secs.) for two examples discussed in MacMillan [17], i.e. the curves in $\mathbf{Q}[Z, X, Y]$ with equations, respectively:

$$X^9 + Y^9 + (X^6 + Y^6)Z + XYZ^2 + Z^5, \quad Y^{10} + X^4Z + Y^2(X - Y)Z + Z^3$$

and

$$X^3 + (X^2 - Y^2)Z + Z^4, \quad Y^3 + (X^2 - Y^2)Z - Z^4$$

where we looked for Puiseux expansions in $\mathbf{R}[[Z]]_{\text{Puis}}$. The subset of initial exponents which have been tested (in the order in which they have been reported) has been chosen using the flexibility allowed us by Theorem 2.

Both examples have been computed on a Macintosh SE, with 2MB RAM, which is among the slowest computers in the Macintosh family.

Invariants & Timings

Initial exp. ν	1/7	2/7	2/3	1/2	1/3	4/13
# roots, μ	90	27	3	7	7	20
# non-zero roots,μ_1	63	7	3	4	0	13
mult(0), μ_0	27	20	0	3	7	7
h=TangentCone(i)	0.86	2.59	2.15	1.98	5.50^+	5.50^+
$h = h[z = 1]$	0.16	0.20	0.25	0.13	0.21	0.20
Mult(R/h)	0.96	1.14	0.94	1.01	1.04	0.98
$j = h : \text{ideal}(x^m, y^m)$	5.91	4.38	2.36	2.95		2.56
$k = \text{gbasis}(j)$	1.79	0.73	0.75	0.66		0.56
Mult(S/j)	0.50	0.21	0.18	0.20		0.23

Initial exp. ν	1	3/2	4/3	9/7	5/4
# roots, μ	9	0	3	3	7
# non-zero roots,μ_1	2		3	0	4
mult(0), μ_0	7		0	3	3
h=TangentCone(i)	0.26	0.41	0.78	0.71	0.75
$h = h[z = 1]$	0.20	0.18	0.25	0.20	0.23
Mult(R/h)	0.30	0.26	0.31	0.36	0.43
$j = h : \text{ideal}(x^m, y^m)$	1.79		0.51		0.83
$k = \text{gbasis}(j)$	0.31		0.15		0.15
Mult(S/j)	0.18		0.20		0.18

+ the standard basis computation has been truncated.

References

[1] M.E. Alonso, T. Mora, G. Niesi and M. Raimondo Local Parametrization of Space Curves at Singular Points In Computer Graphics and Mathematics, eds.B. Falcidieno, I. Herman and C. Pienovi, EurographicSeminar Series, Springer Verlag ,1992 to appear

[2] E. Armando, A. Giovini, and G. Niesi. *CoCoA User's Manual, (v. 1.5).* Dipartimento di Matematica, Università di Genova, 1991.

[3] A. Assi Standard Bases and Flatness Preprint, 1991

[4] C.L.Bajaj, C.M.Hoffmann, R.E.Lynch, and J.E. Hopcroft. Tracing surfaces intersections. *Computer Aided Geometric Design*, 5:285–307, 1988.

[5] A. D. Bruno and A. Soleev. The local uniformization of branches of a curve. Preprint IHES 34, 1990.

[6] G. Cardanus jr. POSSO: a report on the expected state of the art in POlynomial System SOlving. in preparation.

[7] P. Cellini, P. Gianni, and C. Traverso. Algorithms for the shape of semialgebraic sets. A new approach. In *Proc. AAECC 9*, number 539 in Lect. Notes in Comp. Sci., pages 1–18. Springer-Verlag, 1991.

[8] F. Cucker, L.Pardo, T.Recio, M.F.Roy, and M.Raimondo. On the computation of the local and global branches of real algebraic curves. In *Proc. AAECC 6*, number 356 in Lect. Notes in Comp. Sci., pages 161–181. Springer-Verlag, 1989.

[9] D. Duval Diverses questions relatives au calcul formel avec de nombres algebriques These d'etat, Grenoble, 1987.

[10] A. Giovini and G. Niesi. CoCoA: A User-Friendly System for Commutative Algebra. In *Proc. DISCO 90*, number 429 in Lect. Notes in Comp. Sci., pages 20–29. Springer-Verlag, 1990.

[11] W. Groebner. *Algebraische Geometrie.* Bibliographisches Institut Mannheim, 1968-70.

[12] C. M .Hoffmann. Algebraic curves. In *Mathematical aspects of Scientific Software*, number 14 in IMA Volumes in Mathematics and Applications, pages 101–122. Springer-Verlag, 1988.

[13] Y. Lakshman. *On the complexity of computing Groebner bases for zero dimensional polynomial ideals.* PhD thesis, Rensselaer Polytechnique Institute, 1991.

[14] D. Lazard Solving zero-dimensional algebraic systems Preprint, 1989

[15] D. Lazard A new method for solving algebraic systems of positive dimension Proc. AAECC 7, Disc. Appl. Math., 1991

[16] M. Lejeune-Jalabert, B. Tessier Transversalitè, polygone de Newton et installations Astérisque, 7-8: 75-119 (1973)

[17] W. D. MacMillan. A method for determining the solutions of a system of analytic functions in the neighborhood of a branch point. *Math.Ann.*, 72:180–202, 1912.

[18] J. Maurer. Puiseux expansions for space curves. *Manuscripta Math.*, 32:91–100, 1980.

[19] T. Mora Seven variations on Standard Bases Dipartimento di Matematica, Università di Genova, 1988

[20] T.Mora, G.Pfister, and C.Traverso. An introduction to the tangent cone algorithm. In *Issues in robotics and non-linear geometry.* JAI Press, 1992.

[21] T. Mora and L. Robbiano The Groebner Fan of an Ideal J. Symb. Comp. 6, 1988, 183-208

[22] T.Mora and C. Traverso. Representing algebraic numbers by Groebner bases. (in preparation).

[23] P. Pedersen, M.F. Roy and A. Szpirglas Counting Real Zeros in the Multivariate Case Proceedings MEGA 92.

[24] C. Traverso. Communication at the workshop Computing in Algebraic Geometry. Cortona, 1991.