5 Local Parametrization of Space Curves at Singular Points

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

ABSTRACT
We propose a symbolic computation algorithm for computing local parametrization of analytic branches and real analytic branches of a curve in n-dimensional space, which is defined by implicit polynomial equations. The algorithm can be used in space curve tracing near a singular point, as an alternative to symbolic computations based on resolutions of singularities.

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:

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

with $\alpha_1 \in \mathbf{N} - 0, f_2, \ldots, f_n$ 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 $S_2(t, X_2, \ldots, X_n), \ldots, S_n(t, X_2, \ldots, X_n)$ s.t.

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

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:

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

. Since the problem is a local problem, we can assume without loss of generality that the singular point is the origin, reducing ourselves to this case by means of a translation.

While the problem is a typical problem in Computer Algebra and we are going to use fairly standard symbolic computation techniques, we understand that the problem could have 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 ([9], [5]). 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 [6].

Local parametrization of a curve has been studied in a paper by Maurer ([13]); his approach is not completely algorithmical, but it could be made such by recurring to standard basis computations by means of the Tangent Cone Algorithm [14]. The algorithm requires however too many standard basis computations to result in an efficient algorithm. There is a much older (it goes back to 1912) computational approach to the same problem due to Mac Millan [12]; it is algorithmic only under some assumptions of regularity which represent a major restriction to its applicability; whenever these regularity conditions are not satisfied, Mac Millan recours to an impressive and clever set of tricks, which however fail to produce a complete algorithm.

Our proposal, while mainly based on Mac Millan's ideas, makes a complete algorithm out of them, by making use of the Tangent Cone Algorithm and other symbolic computation techniques. For another recent symbolic approach to the same problem see [2]

Our method requires extensive recourse to solving systems of polynomial equations with finitely many solutions and dealing with the arithmetics of algebraic numbers. We discuss a possible approach to this problems based on the most recent state of the art. There is no current implementation of our algorithm, but we will present some promising experimentations performed by means of CoCoA 1.5.3.

5.1 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 is a formal expression:

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

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

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, $\operatorname{ord}(P) = \nu_0/\nu$, while ν is called its *index*, $\operatorname{ind}(P) = \nu$, order and index of the zero series being undefined.

By the usual definition of sum and product, the set of all Puiseux series is turned into an integral domain; what is less obvious, is that 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, $\operatorname{ord}(P^{-1}) = -\operatorname{ord}(P)$; moreover if the exponents of P are all integers, the same is true for those of P^{-1}. 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 $\operatorname{ord}(P) \geq 0$ (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 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.

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 $K((X))_{\text{Puis}}$ and the field of fractions of $K[[X]]$; it will be denoted by $K((X))$.

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 $I^e \subset K(X_1)[X_2, \ldots, X_n]$ 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 $\mathbf{K}((X_1))_{\text{Puis}}$. Then there are finitely many Puiseux series $P_{jk}(X_1) \in \mathbf{K}((X_1))_{\text{Puis}}$, $j = 1 \ldots, r$, $k = 2 \ldots n$ 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 $P_{jk}(X_1) \in K_j((X_1))_{\text{Puis}}$.

There are therefore, a fortiori, at most finitely many solutions $(P_{j2}(X_1), \ldots, P_{jn}(X_1))$ such that $\text{ord}\,(P_{jk}) > 0$ for all k. We will call them *the solutions centered at the origin.*

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 $\nu := \text{lcm}\,(\nu_2, \ldots, \nu_n)$, let $\mu_{ij} := \nu_{ij}\nu/\nu_j$ and let

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

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

There are ν automorphisms of $\mathbf{K}((t))$ which leave fixed $X_1 = t^\nu$ and so $\mathbf{K}(X_1)$; they are given by $t \mapsto \zeta t$, where ζ is a ν^{th}-root of unity, $\zeta^\nu = 1$. As a consequence, if

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

then $(Q_2, \ldots, Q_n)$ is another solution of the system. In other words, solutions centered at the origin of a system of equations $F_1 = \ldots = F_s = 0$, $F_i \in K(X_1)[X_2, \ldots, X_n]$ can be divided in cycles; each cycle contains, for some ν, exactly ν solutions, related each other as specified above. Since any of these solutions, say $(P_2, \ldots, P_n)$, is such that each P_i is convergent, then there is an open disk $U_\varepsilon := \{t \in \mathbf{C} : |t| < \varepsilon\}$ such that for each $t \in U_\varepsilon$, $(t^\nu, R_2(t), \ldots, R_n(t))$ is a point of Γ.

Clearly if ζ is a primitive ν^{th}-root of unity, then the sets $\{(t^\nu, R_2(\zeta^\lambda t), \ldots, R_n(\zeta^\lambda t)) : t \in U_\varepsilon\}_{\lambda=1,\ldots,\nu}$ are the same. This motivates the following definition.

Definition 1 An *analytic branch* of Γ (at the origin) is a cycle of solutions $(P_2, \ldots, P_n)$ with $\mathrm{ord}\,(P_i) > 0$ for all i, of the system $F_1 = \ldots = F_s = 0$. 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. The n-tuple $(t^\nu, R_2(t), \ldots, R_n(t))$ 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 $\{(t^\nu, R_2(t), \ldots, R_n(t)) : t \in U\} \cap \mathbf{R}^n \neq (0, \ldots, 0)$. Then the corresponding analytic branch is called *real.*

Clearly if a solution $(P_2, \ldots, P_n)$ 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 a 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 $\{(-u^2, u) : u \in \mathbf{C}\} \cap \mathbf{R}^2 = \{(-u^2, u) : u \in \mathbf{R}\}$.

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

Recall, finally, 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 the system $F_1 = \ldots = F_s = 0$. Otherwise the origin is singular.

5.2 Local Parametrization at the Origin

Let $\Gamma \subset \mathbf{C}^n$ be a curve defined by s polynomials $F_1(X_1, \ldots, X_n), \ldots, F_s(X_1, \ldots, X_n)$ in $K[X_1, \ldots, X_n]$, where K is a finite algebraic extension of the rationals. We do not require the curve to be irreducible, but only that its irreducible components are all simple. Under this assumption the curve has only finitely many singular points.

Let then $(\alpha_1, \ldots, \alpha_n) \in \Gamma$ be a singular point of the curve. We assume that none of the irreducible components of Γ passing through $(\alpha_1, \ldots, \alpha_n)$ is contained in the hyperplane $X_1 - \alpha_1 = 0$. We refer to Appendix A to discuss how these properties can be tested, how to deal in case the last assumption fails, how to compute singular points.

By the translation $\phi : K[X_1, \ldots, X_n] \to K[X_1, \ldots, X_n]$ defined by $\phi(X_i) = X_i - \alpha_i$ we can assume w.l.o.g. the singular point to be the origin. As remarked above, since the origin is singular, there is more than one solution centered at the origin of the system $F_1 = \ldots = F_s = 0$, corresponding to either several branches or to a single branch of order greater than 1. By back-translating, each such solution $(P_2(X_1), \ldots, P_n(X_1))$ will give rise to the corresponding solution $(\alpha_2 + P_2(X_1 - \alpha_1), \ldots, \alpha_n + P_n(X_1 - \alpha_1))$ "centered at $(\alpha_1, \ldots, \alpha_n)$", each branch will give rise to a branch, and if $(\alpha_1, \ldots, \alpha_n) \in \mathbf{R}^n$ 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.

It is clear that our problem is a local problem, since, if the singular points of Γ are known, by means of a translation, we need only to be able to "compute" solutions centered at the origin. For technical reasons, we need to formulate the problem in local terms, by considering the behaviour of Γ only near the origin. In the following we will therefore assume to be given polynomials $F_1, \ldots, F_s$, which:

1. define locally a curve, i.e. all irreducible components of the variety

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

   passing through the origin are curves;

2. all irreducible components of Γ passing through the origin are simple;

3. none of the irreducible components of Γ passing through the origin is contained in the hyperplane $X_1 = 0$.

If these assumptions are satisfied we will say that $F_1, \ldots, F_s$ locally define an *admissible curve.*

We need obviously to clarify what we mean by computing a Puiseux series. 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 $Q_2(u), \ldots, Q_n(u)$ s.t. $S_i(u, Q_2(u), \ldots, Q_n(u)) = 0$ for all i; moreover any approximation of these series can be explicitly obtained by back substitution in the S_i.

Therefore we say that a solution centered at the origin $(P_2(X_1), \ldots, P_n(X_1))$ of the system $F_1 = \ldots = F_s = 0$ is given if we are given integers $a_1, \ldots, a_n$, polynomials $T_2(u), \ldots, T_n(u)$, polynomials $S_2(u, X_2, \ldots, X_n), \ldots, S_n(u, X_2, \ldots, X_n)$ such that:

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

2. denoting $Q_2(u), \ldots, Q_n(u)$ the unique formal power series such that, for all i, $S_i(u, Q_2(u), \ldots, Q_n(u)) = 0$ and $U_i(u) := T_i(u) + u^{a_i} Q_i(u)$ then $P_i(X_1) = U_i(X_1^{1/a_1})$.

5.3 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:

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

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

An alternative way of describing it is as follows: assign to the variable X_i the pseudodegree a_i and extend this notion of pseudodegree to the whole polynomial ring. Then each non-zero polynomial $F(X_1, \ldots, X_n)$ can be written uniquely as a finite sum of non-zero pseudohomogeneous forms of different pseudodegrees; $\mathrm{in}\,(F)$ is the form of least pseudodegree in this representation.

Let I be an ideal in $K[X_1, \ldots, X_n]$. Let us denote by $\mathrm{in}\,(I)$ the ideal in $K[X_1, \ldots, X_n]$ 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 in(I) too) and that a pseudohomogeneous element in in(I) is the initial form of some polynomial in I.

In general it is false that if $F_1, \ldots, F_s$ is a basis of I, then (in$(F_1), \ldots,$in(F_s)) is a basis of in(I).

To show an easy example consider the ring $K[X_1, X_2, X_3]$ and the ideal $I = (X_1^2 - X_2^3, X_1^2 - X_3^4)$. With weights $a_i = 1$, the notion of pseudodegree coincides with the one of usual degree and the initial form of a polynomial is the homogeneous form of least degree in its expansion. So we have:

$$\text{in}\,(X_1^2 - X_2^3) = X_1^2, \quad \text{in}\,(X_1^2 - X_3^4) = X_1^2, \quad \text{in}\,(X_2^3 - X_3^4) = X_2^3\,.$$

Since $X_2^3 - X_3^4 \in I$, the form X_2^3 belong to in(I), but it does not belong to $(X_1^2) = (\text{in}\,(X_1^2 - X_2^3), \text{in}\,(X_1^2 - X_3^4))$.

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

It is important to remark that standard bases are a local tool, intended to describe the structure of a variety near the origin.

First we have to phrase our geometry in algebraic terms; if I is an ideal of the ring $K[X_1, \ldots, X_n]$, then the set of points in $\mathbf{K}^n$ which satisfy all the polynomials in I are (by definition) an algebraic variety V, which can be splitted as the union of irreducible varieties; there is more than one ideal whose set of zeroes is the algebraic variety V; it is however possible to define a notion of multiplicity, so that each ideal corresponds uniquely to a union of irreducible varieties each of them with a prescribed multiplicity.

The dimension of an ideal will denote the maximal dimension of the irreducible components of the algebraic variety defined by the ideal. The local dimension of an ideal will denote the maximal dimension of the irreducible components passing through the origin of the algebraic variety defined by the ideal.

As already remarked in the previous paragraph, the object of our study will be an ideal locally defining a curve; the reason why we need this relaxing is that the ideal generated by a standard basis of I can be different from I; however the irreducible components passing through the origin of the variety 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 in(I) is pseudohomogeneous; therefore if $(\eta_1, \ldots, \eta_n)$ is a zero of in(I) then, for all t, $(t^{a_1}\eta_1, \ldots, t^{a_n}\eta_n)$ is also a zero of in(I).

2) The dimension of in(I) is the local dimension of I.

3) If I locally defines a curve, the algebraic variety defined by in(I) is the composition of irreducible curves through the origin; in this case we can conclude that 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 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 in(I), with $\eta_1 = 1$.

4) A curve $(t^{a_1}\eta_1, \ldots, t^{a_n}\eta_n)$ satisfies the equations of in(I) if and only if it is tangent at the origin to the curve defined by I.

When parametrizing a plane curve $F(X, Y) = 0$, solutions centered at the origin are then solutions of an univariate equation in $\mathbf{K}((X))_{\text{Puis}}[Y]$. Multiplicities of roots of a univariate equation, as well know, are related with the vanishing of derivatives. In our context we will have to deal with a notion of multiplicity for zeroes of systems of multivariate equations. Without entering in details here and referring the reader to the treatment of the problem in [8], we simply remark that in this case the multiplicity of a zero can be characterized in terms of the vanishing of linear combinations of partial higher derivatives. In particular we will need the following result:

Let L be a field of characteristic 0, let $H_1, \ldots, H_s \in L[X_1, \ldots, X_n]$, be such that the system $H_1 = \ldots = H_s = 0$ has only finitely many solutions, and let $(\omega_1, \ldots, \omega_n) \in L^n$ be a zero of the system. Then $(\omega_1, \ldots, \omega_n)$ is a multiple zero if and only if there are $\zeta_1, \ldots, \zeta_n \in L$ such that, denoting: $\Delta(H) := \zeta_1 \partial H/\partial X_1 + \ldots + \zeta_n \partial H/\partial X_n$ 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 results:

Let I be an ideal of dimension 0, i.e. which has only finitely many zeroes in $\mathbf{K}^n$; then $\mathrm{in}(I)$ *is a proper ideal if and only if the origin is among the zeroes of I; in this case the multiplicity of the origin as a zero of I is the same as its multiplicity as the only zero of* $\mathrm{in}(I)$.

Let us pursue further this point: an ideal I has dimension 0 if and only if in the ring $K[x_1, \ldots, x_n] := K[X_1, \ldots, X_n]/I$ each x_i is algebraic over K, if and only if $K[x_1, \ldots, x_n]$ is a finite dimensional K-vector space.

It is possible to show that the multiplicity of the origin as the zero of $\mathrm{in}(I)$ is exactly the K-dimension of $K[X_1, \ldots, X_n]/\mathrm{in}(I)$.

Furthermore we can count multiplicities of zeroes of I 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. Finally 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 $\mathrm{in}(\phi_\alpha(J)) = \mathrm{in}(\phi_\beta(J))$; by what we remarked above, this implies that α and β have the same multiplicity, but is not equivalent to it.

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 $\mathrm{in}(\phi_\alpha(I)) = \mathrm{in}(\phi_\beta(J))$.

Standard bases are an important tool in the algorithm we are describing here, so it is important to remark that there is an algorithm which, given any set of generators of an ideal, allows to compute a standard basis $(G_1, \ldots, G_t)$ of the ideal; moreover, for any prescribed term-ordering $<$, the algorithm returns a standard basis $(G_1, \ldots, G_t)$ such that $(\mathrm{in}(G_1), \ldots, \mathrm{in}(G_t))$ are a Gröbner basis w.r.t. $<$.

5.4 The Main Transformation

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

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

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:

$(\nu_2, \ldots, \nu_n)$ is the *vector of initial exponents* of $(P_2, \ldots, P_n)$

$(\varepsilon_2 X_1^{\nu_2}, \ldots, \varepsilon_n X_1^{\nu_n})$ is the *monomial approximation* of $(P_2, \ldots, P_n)$

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 $\eta := (\eta_2, \ldots, \eta_n) \in L^{n-1}$, where L is a finite algebraic extension of K. Let $\psi_\eta : L[X_1, \ldots, X_n] \to L[t, X_2, \ldots, X_n]$ 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

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

and $d(F)$ the pseudodegree of $\mathrm{in}\,(F)$. Then:

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

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

Lemma 1 *Let $F \in K[X_1, \ldots, X_n]$ and let $P_2(X_1), \ldots, P_n(X_1) \in \mathbf{K}[[X_1]]_{\mathrm{Puis}}$ 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 $\eta := (\eta_2, \ldots, \eta_n)$ and $R(t, X_2, \ldots, X_n) := \psi_\eta(F)/t^{d(F)}$. Then:

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

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

Proof: 1) One has:

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

and so, by the transformation $X_1 \to t^a$,

$$F(t^a, \eta_2 t^b + t^b Q_2(t^a), \ldots, \eta_n t^b + t^b Q_n(t^a)) = 0.$$

Decomposing the equality according to the different powers of t, one then obtains that $t^{d(F)} G(\eta_2, \ldots, \eta_n) = 0$.

2) One has:

$$t^{d(F)} R(t, X_2, \ldots, X_n) = \psi(F) = F(t^a, (\eta_2 + X_2)t^b, \ldots, (\eta_n + X_n)t^b)$$

and

$$P_i(t^a) = \eta_i t^b + t^b Q_i(t^a).$$

Then

$$t^{d(F)} R(t, Q_2(t^a), \ldots, Q_n(t^a)) = F(t^a, P_2(t^a), \ldots, P_n(t^a)) = 0.$$

Lemma 2 *Let $F \in K[X_1, \dots, X_n]$, $\eta := (\eta_2, \dots, \eta_n) \in \mathbf{K}^{n-1}$, $R(t, X_2, \dots, X_n) := \psi_\eta(F)/t^{d(F)}$, $Q_2(t), \dots, Q_n(t) \in \mathbf{K}[[t]]_{\mathrm{Puis}}$, $\mathrm{ord}\,(Q_i) > 0$ such that $R(t, Q_2(t), \dots, Q_n(t)) = 0$. Let $P_i(X_1) = \eta_i X_1^\nu + X_1^\nu Q_i(X_1^{1/a})$. Then*

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

Proof: Since:

$$t^{d(F)} R(t, X_2, \dots, X_n) = \psi(F) = F(t^a, (\eta_2 + X_2)t^b, \dots, (\eta_n + X_n)t^b)$$

$$P_i(t^a) = \eta_i t^b + t^b Q_i(t^a)$$

then:

$$F(t^a, P_2(t^a), \dots, P_n(t^a)) = t^{d(F)} R(t, Q_2(t^a), \dots, Q_n(t^a)) = 0.$$

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

1. *The system $G_1 = \dots = G_s = 0$ has either no solutions or finitely many solutions only.*
2. *There is a solution of $F_1 = \dots = F_s = 0$ centered at the origin with initial approximation*

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

   if and only if $(\eta_2, \dots, \eta_n)$ is a zero of $G_1 = \dots = G_s = 0$.

Let now $\bar\eta := (\eta_2, \dots, \eta_n)$ be a zero of $G_1 = \dots = G_s = 0$ and $R_i(t, X_2, \dots, X_n) := \psi_\eta(F_i)/t^{d_i}$. Then:

3. *$R_1, \dots, R_s$ locally define an admissible curve (the $\bar\eta$-transformation of Γ).*
4. *The solutions of the system $F_1 = \dots = F_s = 0$ with initial approximation $X_2 = \eta_2 X_1^\nu, \dots, X_n = \eta_n X_1^\nu$ are $(P_2(X_1), \dots, P_n(X_1))$, with $P_i(X_1) = \eta_i X_1^\nu + X_1^\nu Q_i(X_1)$ and $(Q_2(t^a), \dots, Q_n(t^a))$ a solution centered at the origin of $R_1 = \dots = R_s = 0$.*

Proof: 1) The ideal $\mathrm{in}\,(I) = (\mathrm{in}\,(F_1), \dots, \mathrm{in}\,(F_s))$ has dimension 1, so its solutions are finitely many curves $(t^a\eta_1, t^b\eta_2, \dots, t^b\eta_n)$. The solutions of $G_1 = \dots = G_s = 0$ are the points which satisfy $\mathrm{in}\,(F_1) = \dots = \mathrm{in}\,(F_s) = 0$ and moreover $X_1 = 1$. Therefore there is a solution of $G_1 = \dots = G_s = 0$, 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 $F_1 = \dots = F_s = 0$ centered at the origin with initial approximation

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

then $(\eta_2, \dots, \eta_n)$ is a zero of $G_1 = \dots = G_s = 0$, as a consequence of Lemma 1. Conversely, since $(F_1, \dots, F_s)$ is a standard basis, if $(\eta_2, \dots, \eta_n)$ is a zero of $G_1 = \dots = G_s = 0$, then $(t^a, t^b\eta_2, \dots, t^b\eta_n)$ is tangent to $F_1 = \dots = F_s = 0$, and so there is a solution of $F_1 = \dots = F_s = 0$ centered at the origin with initial approximation

$$X_2 = \eta_2 X_1^\nu, \dots, X_n = \eta_n X_1^\nu.$$

3) Since $F_1, \ldots, F_s$ locally define a curve and so have finitely many solutions centered at the origin with initial approximation

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

Lemmata 1 and 2 prove that $R_1 = \ldots = R_s = 0$ has finitely many zeroes over $\mathbf{K}[[t]]_{\mathrm{Puis}}$, i.e. $R_1, \ldots, R_s$ locally define a curve. If $R_1, \ldots, R_s$ had components in the hyperplane $t = 0$, then the system $R_1 = \ldots = R_s = t = 0$ would have infinitely many solutions in $\mathbf{K}^n$. However this system is equivalent to $G_1 = \ldots = G_s = t = 0$ which has only finitely many solutions. Finally we must prove that all the solutions centered at the origin of $R_1 = \ldots R_s = 0$ are simple. Let $\zeta_2(t), \ldots, \zeta_n(t) \in \mathbf{K}((t))_{\mathrm{Puis}}$ and denote

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

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

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

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

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

A direct verification shows that for all i and j:

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

so that for all i

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

By Lemmata 1 and 2 $(Q_2(t), \ldots, Q_n(t))$ is a zero of $\Delta(R_1) = \ldots = \Delta(R_s) = 0$, if and only if $(P_2(X_1), \ldots, P_n(X_1))$ is a zero of $\Delta(F_1) = \ldots = \Delta(F_s) = 0$, i.e. $(Q_2(t), \ldots, Q_n(t))$ is a multiple zero of $R_1 = \ldots = R_s = 0$ if and only if $(P_2(X_1), \ldots, P_n(X_1))$ is a multiple zero of $F_1 = \ldots = F_s = 0$. Since the solutions centered at the origin of $F_1 = \ldots = F_s = 0$ are all simple, the same is necessarily true for those of $R_1 = \ldots = R_s = 0$.

4) It is an immediate consequence of Lemmata 1 and 2.

It is useful to have some more insight into the conjugacy classes of the roots of the system $G_1 = \ldots = G_s = 0$. 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 $J = \mathrm{in}\,(I) = (\mathrm{in}\,(F_1), \ldots, \mathrm{in}\,(F_s))$, 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 $\psi_{\bar\eta_i} = \tau_i \psi_\eta$ so that the the ideals of the $\bar\eta_i$-transformations of Γ are isomorphic. In conclusion:

Proposition 1 *Let $\bar\eta := (\eta_2, \ldots, \eta_n)$ be a zero of $G_1 = \ldots G_s = 0$, 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 $G_1 = \ldots G_s = 0$.*
2. *The $\bar\eta_i$'s are equivalent zeroes of $G_1 = \ldots = G_s = 0$.*
3. *The ideals of the $\bar\eta_i$-transformations of Γ are isomorphic.*

5.5 Counting the Number of Roots

Let $F_1, \ldots, F_s$ locally define an admissible curve Γ, so that the system $F_1 = \ldots = F_s = 0$ has actually solutions centered at the origin, i.e. solutions $(P_2, \ldots, P_n)$ such that $ord(P_i) > 0$ for all i. Our first aim is to count them, which we will achieve by using different but equivalent notions of multiplicity.

First of all we recall that the multiplicity of intersection of the hyperplane $X_1 = 0$ with an analytic branch at the origin is the order of the branch, and so the number of solutions whose cycle gives the branch itself. Therefore the multiplicity of intersection at the origin of the hyperplane $X_1 = 0$ with the curve Γ is exactly the number of solutions centered at the origin of the system $F_1 = \ldots = F_s = 0$. The same number is however also the multiplicity of the origin as a solution of the system $X_1 = F_1 = \ldots = F_s = 0$. Since no component of the curve is contained in the hyperplane $X_1 = 0$, this new system is such to have only finitely many points in $\mathbf{K}^n$ as solutions and therefore the multiplicity of the origin as a zero of it is the multiplicity of any standard basis of the ideal $(X_1, F_1, \ldots, F_s) \subset K[X_1, \ldots, X_n]$ or equivalently of the ideal $(F_1(0, X_2, \ldots, X_n), \ldots, F_s(0, X_2, \ldots, X_n)) \subset K[X_2, \ldots, X_n]$. Hence we have proved:

Lemma 3 *Let $F_1, \ldots, F_s$ locally define an admissible curve Γ. Then the system*

$$F_1(0, X_2, \ldots, X_n) = \ldots = F_s(0, X_2, \ldots, X_n) = 0$$

has finitely many solutions. The multiplicity of the origin as a solution of this system is the number of solutions of $F_1 = \ldots = F_s = 0$ centered at the origin.

Remark that since we assume Γ to be admissible, and so in particular with no multiple component, the multiplicity at the origin of the system above counts the number of *distinct* solutions centered at the origin.

Lemma 4 *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 $G_i(X_2, \ldots, X_n) = \mathrm{in}\,(F_i)(1, X_2, \ldots, X_n)$ and d_i the pseudodegree of $\mathrm{in}\,(F_i)$. Let $(\eta_2, \ldots, \eta_n)$ be a zero of $G_1 = \ldots = G_s = 0$ with multiplicity h and 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 $R_1 = \ldots = R_s = 0$ has exactly h solutions centered at the origin (again, because of Theorem 1, the h solutions are simple and so are all distinct).

Proof: Remark that $G_i(\eta_2 + X_2, \ldots, \eta_2 + X_n) = R_i(0, X_2, \ldots, X_n)$. Since $(\eta_2, \ldots, \eta_n)$ is a zero of $G_1 = \ldots = G_s = 0$ with multiplicity h, the origin is a solution of the system $R_1(0, X_2, \ldots, X_n) = \ldots = R_s(0, X_2, \ldots, X_n) = 0$, with multiplicity h. By Lemma 3, then, $R_1 = \ldots = R_s = 0$ has exactly h solutions centered at the origin.

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 $G_i(X_2, \ldots, X_n) = \mathrm{in}\,(F_i)(1, X_2, \ldots, X_n)$. Then:*

1. *the multiplicity of the ideal $(G_1, \ldots, G_s)$ is the number of solutions centered at the origin with initial exponent $\mu \geq b/a$;*
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 $\mu > b/a$;*
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 $X_2 = \eta_2 X_1^{b/a}, \ldots, X_n = \eta_n X_1^{b/a}$.*

Proof: the result is an immediate consequence of Theorem 1 and Lemma 4.

Proposition 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 $G_i(X_2, \ldots, X_n) = \mathrm{in}\,(F_i)(1, X_2, \ldots, X_n)$, d_i the pseudodegree of $\mathrm{in}\,(F_i)$. Let $(\eta_2, \ldots, \eta_n)$ be a simple zero of $G_1 = \ldots = G_s = 0$, $L := K(\eta_2, \ldots, \eta_n)$. 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 $R_1 = \ldots = R_s = 0$.*

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 $G_1 = \ldots = G_s = 0$. The other statement is an elementary consequence of the Implicit Function Theorem.

5.6 Finding Initial Exponents

A basic step of the algorithm we are developing is finding the set of the initial exponents of the solutions centered at the origin of $F_1 = \ldots = F_s = 0$. In his paper [13], Maurer proposed a necessary condition for a vector $(\nu_2, \ldots, \nu_n)$ to be a vector of initial exponents.

Assume that $(\varepsilon_2 X_1^{\nu_2}, \ldots, \varepsilon_n X_1^{\nu_n})$ is the monomial approximation of a solution centered at the origin, so that $\varepsilon_i \neq 0$ for all i. Let $(a, b_2, \ldots, b_n)$ be integer weights with $\nu_i = b_i/a$. By an argument similar to that of Lemma 1, one proves that $(1, \varepsilon_2, \ldots, \varepsilon_n)$ must be a zero of $\mathrm{in}\,(F)$, for each polynomial F in I, where $\mathrm{in}\,(F)$ is computed with respect to the weights $(a, b_2, \ldots, b_n)$. Since $\varepsilon_i \neq 0$ for all i , then, for each polynomial F in I, $\mathrm{in}(F)$ cannot consist of a monomial, so that $(a, b_2, \ldots, b_n)$ must be orthogonal to an edge of the Newton polyhedron of F, for each F in I.

Because of this result, Maurer suggests the following approach: take $n-1$ among the F_i; compute their Newton polyhedra; for each possible $(n-1)$-tuple of edges, one for each polyhedron, compute "the" orthogonal direction. The list of vectors of exponents so found contains then all possible vectors of initial exponents.

An obvious improvement over this approach is to test this list with the Newton polyhedra of the other basis elements and of any other polynomial in the ideal produced during the algorithm, discarding those vectors which are not orthogonal to at least one edge of the polyhedron. Call *Maurer vectors* the resulting vectors. Also, if $(\nu_2, \ldots, \nu_n)$ is a Maurer vector, call $\nu := min(\nu_i)$ a *Maurer exponent.*

There are however two problems with Maurer's approach.

First of all it is possible that for some choice of an edge for each of s different Newton polyhedra (even for s larger than $n-1$), the s edges so chosen span a vector space of dimension less than $n-1$ so that there are infinitely many directions orthogonal to all of them and so infinitely many Maurer vectors. A quite inefficient remedy to this is based on the fact that there are bounds on the integers a, b_i such that $(b_2/a, \ldots, b_n/a)$ are vectors of initial exponents.

A second problem is however that the list of Maurer vectors is quite too large; a standard basis computation with weights $(a, b_2, \ldots, b_n)$ with $b_i/a = \nu_i$ is necessary in order to find (if there exist) monomial approximations $(\varepsilon_2 X_1^{\nu_2}, \ldots, \varepsilon_n X_1^{\nu_n})$, by means of an obvious generalization of Theorem 1; since standard basis computations are the most time-expensive part of a local parametrization algorithm, one cannot afford to compute too many of them.

A different proposal which searches for initial exponents and initial approximations only is contained in MacMillan's paper [12].

Let $\pi : \mathbf{N}^n \to \mathbf{N}^2$ given by $\pi(a_1, \ldots, a_n) = (a_1, a_2 + \ldots + a_n)$; consider the Newton polygons of the projections by π of the Newton polyhedra of the F_i's. MacMillan proves that, **if** a certain condition is verified, ν is the initial exponent of a solution centered at the origin, if and only if $-1/\nu$ is the slope of an edge of at least one of these Newton polygons. Call each such value ν a *MacMillan exponent.*

MacMillan's condition, which he states in terms of resultant theory, can be formulated in more modern language and then it states that $F_1, \ldots, F_s$ is a standard basis for each weight $(a, b \ldots, b)$ such that b/a is a MacMillan exponent. In general such a condition, as remarked by MacMillan himself, does not hold, so that MacMillan's list does not produce all initial exponents. There is however an advantage (and this remark again is due to MacMillan) in working with initial exponents instead of vectors of initial exponents, which is given by the counting argument of Theorem 2.

If $\nu_1 = b/a$ and $\nu_2 = d/c$, $\nu_1 < \nu_2$, are consecutive values in the list of MacMillan's exponent, standard basis computations w.r.t. the weights $(a, b, \ldots, b)$ and $(c, d, \ldots d)$ allow to compute the number of solutions with initial exponent $\nu > \nu_1$ and the number of solutions with initial exponent $\nu \geq \nu_2$; if the two numbers are different, their difference gives the number of solutions with initial exponent ν, $\nu_1 < \nu < \nu_2$. In this case, we can make use of Maurer exponents in the interval (ν_1, ν_2); the same counting argument allows to perform some kind of binary search in the list of Maurer exponents, so decreasing the number of standard basis computations required.

Properties of standard bases suggest to use the following heuristics instead.

For each polynomial in the standard basis of $(F_1, \ldots, F_s)$ w.r.t. the weights $(a, b, \ldots b)$ with $b/a = \nu_1$, compute its Newton polyhedron, and the Newton polygon of its projection by π; from the list of values ν, $\nu_1 < \nu < \nu_2$, such that $-1/\nu$ is the slope of an edge of one of these polygons, (if not empty) select the one of minimal value.

In the same way, for each polynomial in the standard basis of $(F_1, \ldots, F_s)$ w.r.t. the weights $(c, d, \ldots, d)$ with $d/c = \nu_2$, compute its Newton polyhedron, and the Newton polygon of its projection by π; from the list of values ν, $\nu_1 < \nu < \nu_2$, such that $-1/\nu$ is the slope of an edge of one of these polygons, (if not empty) select the one of maximal value.

Only in case this procedure fails, i.e. both lists are empty, perform one step of binary search in the list of Maurer exponents in the interval (ν_1, ν_2).

5.7 Finding all Solutions with a given Initial Exponent

Let us now fix a positive rational ν and let us show how to compute all solutions of $F_1 = \ldots = F_s = 0$ with initial exponent ν. Let $a, b \in \mathbf{N}$ be such that $b/a = \nu$, $\gcd(a, b) = 1$.

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

2. Let $G_i := \mathrm{in}(H_i)(1, X_2, \ldots, X_n)$ and d_i be the pseudodegree of $\mathrm{in}(H_i)$.
3. Compute the multiplicity μ of the ideal $J_0 = (G_1, \ldots, G_t)$.
4. Compute the ideal $J := (G_1, \ldots, G_t) : (X_2^\mu, \ldots, X_n^\mu)$.
5. Compute its multiplicity μ_1 and let $\mu_0 := \mu - \mu_1$.
6. Compute ideals $J_1, \ldots, J_u$ such that:

   i) the union of the roots of the J_i's gives the roots of J:

   $$\{(\eta_2, \ldots, \eta_n) : F(\eta_2, \ldots, \eta_n)\ \forall F \in J\} = \cup_i \{(\eta_2, \ldots, \eta_n) : F(\eta_2, \ldots, \eta_n)\ \forall F \in J_i\}$$

   ii) if $(\eta_2, \ldots, \eta_n)$ and $(\varepsilon_2, \ldots, \varepsilon_n)$ are roots of a same ideal J_i then they are equivalent zeroes of J;

   iii) the roots of J_1 are the simple roots of J.
7. For each root $(\eta_2, \ldots, \eta_n)$ of J_1:
   (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 $S_2, \ldots, S_n$ satisfying the conditions of Proposition 2;
   (c) return $[(t^a, \eta_2 t^b, \ldots, \eta_n t^b);\ t^b;\ (S_2, \ldots, S_n)]$.
8. For each root $(\eta_2, \ldots, \eta_n)$ of J_i, $i > 1$:
   (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 all solutions of $R_1(t, X_2, \ldots, X_n) = \ldots = R_t(t, X_2, \ldots, X_n) = 0$, 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 , denoting $Q_i(u)$ the unique formal power series such that, for all i, $S_i(u, Q_2(u), \ldots, Q_n(u)) = 0$ and putting:

   $$U_i(u) := T_i(u) + u^d Q_i(u),$$

   one has:

   $$R_1(u^c, U_2(u), \ldots, U_n(u)) = \ldots = R_t(u^c, U_2(u), \ldots, U_n(u)) = 0.$$

   (c) For each solution

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

   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, denoting $Q_i(u)$ the unique formal power series such that, for all i, $S_i(u, Q_2(u), \ldots, Q_n(u)) = 0$ and putting:

   $$V_i(u) := T_i(u) + u^d Q_i(u),$$

$$U_i(u) := \eta_i u^{bc} + u^{bc} V_i(u) = \eta_i u^{bc} + u^{bc} T_i(u) + u^{bc+d} Q_i(u)$$

one has:

$$R_1(u^c, V_2(u), \ldots, V_n(u)) = \ldots = R_t(u^c, V_2(u), \ldots, V_n(u)) = 0$$

and

$$H_1(u^{ac}, U_2(u), \ldots, U_n(u)) = \ldots = H_t(u^{ac}, U_2(u), \ldots, U_n(u)) = 0$$

Let us comment on each step of this algorithm.

1. The standard basis computation can be performed by means of the Tangent Cone Algorithm [14], which has the advantage of returning a Gröbner basis of the ideal $J_0 = (G_1, \ldots, G_t)$. Since the standard basis computation is the most time-consuming part of the Algorithm, we will discuss in an Appendix possible ways of improving this step of the algorithm, by truncating the standard basis computation.

2. 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. The multiplicity of $J_0 = (G_1, \ldots, G_t)$ can be easily computed if $(G_1, \ldots, G_t)$ is a Gröbner basis and it gives the sum of the multiplicities of the roots of J_0, i.e. the number of solutions centered at the origin with initial exponent $\nu_1 \geq \nu$.

4. The roots of the ideal $J := (G_1, \ldots, G_t) : (X_2^{\mu}, \ldots, X_n^{\mu})$ are exactly the same as 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 [16]; the technique is not efficient but has the advantage to be easily available in any system with the Gröbner basis algorithm) or by a linear algebra algorithm [11,15] which requires $n^2\mu^3$ arithmetical operations in the field K (this last approach is much more efficient, but we don't know of any existing implementation).

5. The knowledge of a Gröbner basis of J allows to compute easily its multiplicity. By Theorem 2, one then has that μ_1 is the number of solutions centered at the origin with initial exponent ν, while μ_0 is the number of solutions centered at the origin with initial exponent $\nu_1 > \nu$. The knowledge of μ_1 and μ_0 is required for the computation of initial exponents as sketched in the previous paragraph.

6. We agree that the formulation of this step is quite odd. An easier formulation would be: *compute all roots of J*. The reason why we have chosen this formulation is that, while we need to separate roots which are not equivalent, there is no need to actually compute them, as it will be made more clear in section 5.10, to which we refer, postponing the discussion of this point.

7. Since the roots of J_1 are the simple roots of J we can apply Proposition 2. Because of it, we know that there are unique formal power series $Q_i(t)$ such that $R_j(t, Q_2(t), \ldots, Q_n(t)) = 0$ for all j and that $(t^a, \eta_2 t^b + t^b Q_2(t), \ldots, \eta_2 t^b + t^b Q_2(t))$ corresponds to the unique solution centered at the origin with initial approximation $(\eta_2 t^{\nu}, \ldots \eta_n t^{\nu})$ by the substitution $t = X^{1/a}$. As it was specified in section 5.2, 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.

8. Here we apply instead Theorem 1 which implies that

$$R_1(u^c, V_2(u), \ldots, V_n(u)) = \ldots = R_t(u^c, V_2(u), \ldots, V_n(u)) = 0$$

   if and only if

$$H_1(u^{ac}, U_2(u), \ldots, U_n(u)) = \ldots = H_t(u^{ac}, U_2(u), \ldots, U_n(u)) = 0.$$

5.8 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 8.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:

1. $\{F_{i1}, \ldots, F_{is_i}\}$ is a standard basis of Γ_i w.r.t. the weights $(a_i, b_i, \ldots, b_i)$.
2. $(1, \eta_{2i}, \ldots, \eta_{ni})$ is a zero of $\mathrm{in}(F_{i1}) = \ldots = \mathrm{in}(F_{is_i}) = 0$ of multiplicity h_i.
3. $\Gamma_{i+1}$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 $h_{i-1} \geq a_i h_i > h_i$;
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.

5.9 Finding Real Analytic Branches

Our final aim is however not to find all solutions centered at the origin, and not even all analytic branches (which would require choosing a solution for each cycle), but to find the real analytic branches. To do so we make use of the following result:

Proposition 3 *Let $(P_2(X_1),\dots,P_n(X_1))$ be a solution centered at the origin of the system $F_1=\dots=F_s=0$, with*

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

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 $(P_2,\dots,P_n)$ are

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

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

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

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:

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

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

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 $(-t^\nu,\sum c_{i2}t^{\nu_{i2}},\dots,\sum c_{in}t^{\nu_{in}})$ we have to modify accordingly the results of section 5.4.

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

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

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

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

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

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

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

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

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

and

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

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

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

It is immediate that

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

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 1, we have:

Proposition 4 *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 analogon of Theorem 1:

Proposition 5 *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 $G_i(X_2,\ldots,X_n) := \mathrm{in}\,(F_i)(-1,X_2,\ldots,X_n)$ and let d_i be the pseudodegree of $\mathrm{in}\,(F_i)$. Then:*

1) $G_1 = \ldots = G_s = 0$ has either no solutions or finitely many solutions only.
Let $\bar\eta := (\eta_2,\ldots,\eta_n)$ be a zero of $G_1 = \ldots = G_s = 0$ 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.

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 1 *Given a standard basis $F_1,\ldots,F_s$ of I for the weights $(a,b,\ldots b)$, let $\nu := b/a$, let d_i be the pseudodegree of $\mathrm{in}\,(F_i)$, let $\eta := (\eta_2,\ldots,\eta_n)$ be a real zero of*

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

and let

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

Let $((-1)^j u^c, V_2(u), \ldots, V_n(u))$, $V_i \in \mathbf{R}[[u]]_{\mathrm{Puis}}$ *be a real parametrization of a real branch of* $R_1 = \ldots = R_s = 0$, *i.e.*

$$R_1((-1)^j u^c, V_2(u), \ldots, V_n(u)) = \ldots = R_s((-1)^j u^c, V_2(u), \ldots, V_n(u)) = 0.$$

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 $F_1 = \ldots = F_s = 0$.

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

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

and let $R_i(t, X_2, \ldots, X_n) := \psi_\eta \sigma(F_i)/t^{d_i}$. *Let* $((-1)^j u^c, V_2(u), \ldots, V_n(u))$, $V_i \in \mathbf{R}[[u]]_{\mathrm{Puis}}$ *be a real parametrization of a real branch of* $R_1 = \ldots = R_s = 0$. *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 $F_1 = \ldots = F_s = 0$.

Moreover a real branch of $F_1 = \ldots = F_s = 0$ *has a parametrization obtained as above.*

We are now able to describe the modifications we need to perform to the algorithm sketched in section 5.7, to compute only the real analytic branches; the modifications apply only to Steps (7) and (8) which are to be modified as follows:

7) For each *real* root $(\eta_2, \ldots, \eta_n)$ of J_1:

   (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 $S_2, \ldots, S_n$ satisfying the conditions of Proposition 1

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

8) 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 $\{(\eta_2\xi^b, \ldots, \eta_n\xi^b) : (\eta_2, \ldots, \eta_n)$ a root of $J_1\}$. For each real root $(\eta_2, \ldots, \eta_n)$ of L_1:

   (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 $S_2, \ldots, S_n$ satisfying the conditions of Proposition 1.

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

9) For each real root $(\eta_2, \ldots, \eta_n)$ of J_i, $i > 1$:

   (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 all real solutions of $R_1(t, X_2, \ldots, X_n) = \ldots = R_t(t, X_2, \ldots, X_n) = 0$, i.e. compute all

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

   where T_i, S_i have real coefficients and are such that, denoting $Q_i(u)$ the unique formal power series such that, for all i, $S_i(u, Q_2(u), \ldots, Q_n(u)) = 0$ and $V_i(u) := T_i(u) + (-1)^k u^d Q_i(u)$, one has:

$$R_1((-1)^j u^c, V_2(u), \ldots, V_n(u)) = \ldots = R_t((-1)^j u^c, V_2(u), \ldots, V_n(u)) = 0.$$

(c) For each real solution

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

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

return

$$[((-1)^{aj} u^{ac}, (-1)^{bj} \eta_2 u^{bc} + (-1)^{bj} u^{bc} T_2(u), \ldots, (-1)^{bj} \eta_n u^{bc} + (-1)^{bj} u^{bc} T_n(u));$$

$$(-1)^{bj+k} u^{bc+d};\ (S_2(u, X_2, \ldots, X_n), \ldots, S_n(u, X_2, \ldots, X_n))]$$

so that, letting

$$U_i(u) := (-1)^{bj} \eta_i u^{bc} + (-1)^{bj} u^{bc} V_i(u) =$$

$$(-1)^{bj} \eta_i u^{bc} + (-1)^{bj} u^{bc} T_i(u) + (-1)^{bj+k} u^{bc+d} Q_i(u)$$

one has:

$$F_1((-1)^{aj} u^{ac}, U_2(u), \ldots, U_n(u)) = \ldots = F_s((-1)^{aj} u^{ac}, U_2(u), \ldots, U_n(u)) = 0.$$

10) If a is even, let ξ be a primitive $2a^{th}$-root of unity and let L_i be the ideal whose roots, all simple, are $\{(\eta_2 \xi^b, \ldots, \eta_n \xi^b) : (\eta_2, \ldots, \eta_n)$ is a root of $J_i\}$. For each real root $(\eta_2, \ldots, \eta_n)$ of L_i, $i > 1$:

(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 all real solutions of $R_1(t, X_2, \ldots, X_n) = \ldots = R_t(t, X_2, \ldots, X_n) = 0$:

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

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

(c) For each real solution

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

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

return

$$[(-u^{ac}, (-1)^{bj} \eta_2 u^{bc} + (-1)^{bj} u^{bc} T_2(u), \ldots, (-1)^{bj} \eta_n u^{bc} + (-1)^{bj} u^{bc} T_n(u));$$

$$(-1)^{bj+k} u^{bc+d};\ (S_2(u, X_2, \ldots, X_n), \ldots, S_n(u, X_2, \ldots, X_n))].$$

5.10 The Algebraic Computations

Our algorithm requires extensive recourse to solving 0-dimensional systems of polynomial equations 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. However we have chosen here to avoid discussing how to deal with these questions and just to give the existence of algorithms for both problems as granted.

The reason is that not only 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), but that even in this respect, according to the major experts in the area, further advances will be available in the next future (see [10]). Implementations reflecting these theoretical advances are to be considered as forthcoming 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 $(\eta_2, \ldots, \eta_n)$ of a 0-dimensional ideal $I \subset K[X_2, \ldots, X_n]$ provided that one is able to perform arithmetical operations in $K(\eta_2, \ldots, \eta_n)$, so that the effort is in devising effective (and efficient) schemes to perform arithmetics in $K(\eta_2, \ldots, \eta_n)$ when only a 0-dimensional ideal I is given which has $(\eta_2, \ldots, \eta_n)$ as a zero.

Here we discuss briefly how to use for our algorithm some recent ideas in this direction which are contained in the forthcoming paper [15], together with the use of seminumerical techniques for real roots, advocated in [4] and [3].

The basic ideas of [15] are the following:

1) there is a surjection from $K[X_2, \ldots, X_n]/I$ to $K(\eta_2, \ldots, \eta_n)$;

2) $K[X_2, \ldots, X_n]/I$ is a K-vector space of finite dimension $h = \mathrm{mult}(I)$;

3) if I is given by a Gröbner basis, then a subvector space of $V \subset K[X_2, \ldots, X_n]$ can be given which is isomorphic to $K[X_2, \ldots, X_n]/I$;

4) therefore each element of $K(\eta_2, \ldots, \eta_n)$ 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 $K[X_2, \ldots, X_n]/I$ and so of the corresponding elements of $K(\eta_2, \ldots, \eta_n)$;

6) moreover if $g \in V$, linear algebra algorithms can be used to compute Gröbner bases (and so vectorial representations) of both $K[X_2, \ldots, X_n]/I_0$ and $K[X_2, \ldots, X_n]/I_1$, where $I_0 := I + (g)$ and $I_1 := I : g$.

While sums and products in $K(\eta_2, \ldots, \eta_n)$ can be computed because of 5), computing inverses is less trivial. Let in fact $g(X_2, \ldots, X_n) \in V$, $g \neq 0$. Not only (because of non-uniqueness of representation) it is possible that $g(\eta_2, \ldots, \eta_n) = 0$ but, what is worse, $g(\eta_2, \ldots, \eta_n)$ could be 0 for some zeroes of I, while being different from 0 for other zeroes of I.

However it is possible to prove that denoting $I_0 := I + (g)$ and $I_1 := I : g^h$, the zeroes of I_0 are exactly those zeroes $(\eta_2, \ldots, \eta_n)$ of I such that $g(\eta_2, \ldots, \eta_n) = 0$, while the zeroes of I_1 are exactly those zeroes $(\eta_2, \ldots, \eta_n)$ of I such that $g(\eta_2, \ldots, \eta_n) \neq 0$. Moreover by 6) it is possible to compute Gröbner bases of both I_0 and I_1 and (again by linear algebra) a polynomial h such that $gh = 1 \bmod I_1$ so that $h(\eta_2, \ldots, \eta_n)$ is the inverse of $g(\eta_2, \ldots, \eta_n)$ in $K(\eta_2, \ldots, \eta_n)$ for each zero $(\eta_2, \ldots, \eta_n)$ of I_1.

Particular care must be devoted to polynomial arithmetics over $K(\eta_2, \ldots, \eta_n)$ if performed in this model; in fact a polynomial in $K(\eta_2, \ldots, \eta_n)[Z]$ is represented by a polynomial in Z whose coefficients are polynomials in $V \subset K[X_2, \ldots, X_n]$; such coefficients could be zero for some value of $(\eta_2, \ldots, \eta_n)$ and not zero for others; since polynomial division requires taking the non-zero coefficient of highest degree in a polynomial, a polynomial division algorithm will perform differently for different zeroes of I. This means that, while performing polynomial division, several zero-checkings and inverse computations are required, each of them gives a splitting of I into I_0 and I_1; the polynomial division algorithm is then to be performed both over $K[X_2, \ldots, X_n]/I_0$ and $K[X_2, \ldots, X_n]/I_1$.

To make this point more clear, let us compute the squarefree polynomial $\mathrm{SQFR}(f)$ associated to $f = Z^3 - bZ^2 + 2aZ$, where (a, b) is a root of $I = (X^2 + X, XY - X, Y^2 - Y)$, i.e. is either $(0, 0)$, $(0, 1)$ or $(-1, 1)$. To do this we have to compute $h = \gcd(f, f')$, since

SQFR$(f) = f/h$. Since $f' = 3Z^2 - 2bZ + 2a$ and its leading coefficient is not zero in $\mathbf{Q}(a,b)$, we perform pseudodivision of f by f', obtaining $9f = q(Z)f' + g(Z)$, for a suitable $q(Z)$ and for $g(Z) = (12a - 2b)Z + 2a$.

One has:

$$I_0 := I + (12X - 2Y) = (X, Y);$$

for (a,b) a root of I_0, one has $g = 0$, $h := \gcd(f, f') = Z^2$, SQFR$(f) = f/h = Z$,

$$I_1 := I : (12X - 2Y) = (X^2 + X, Y - 1)$$

and

$$(12a - 2b)(-1/2 - 3/7a) = -6a - 36/7a^2 + b + 6/7ab = -6a + 36/7a + 1 + 6/7a = 1$$

for (a,b) a root of I_1.

Performing division of f' by g one obtains

$$f' = q'(Z)g + 81/49a$$

and then:

$$I_{10} := I_1 + (X) = (X, Y - 1);$$
$$I_{11} := I_1 : X = (X + 1, Y - 1);$$

for (a,b) a root of I_{10}, one has: $81/49a = 0$, so $h := \gcd(f, f') = g(Z) = -2Z$, SQFR$(f) = X^2 - X$; for (a,b) a root of I_{11}, one has: $81/49a \neq 0$, so $\gcd(f, f') = 1$ and SQFR$(f) = f$.

In fact the only root of I_0 is $(0,0)$ for which $f = X^3$, SQFR$(f) = X$; the only root of I_{10} is $(0,1)$ for which $f = X^3 - X^2$, SQFR$(f) = X^2 - X$; the only root of I_{11} is $(-1,1)$ for which $f = X^3 - X^2 - 2X$ is squarefree.

An advantage of this approach is that if, in our algorithm, we represent the roots of J by using a Gröbner basis of J (obtained in Step 4), according to the scheme described here, and we directly compute in this model

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

for all i and then a standard basis of $(R_1, \ldots, R_t)$ the ideal J will be naturally splitted into ideals J_i so that:

1. the union of the zeroes of J_i gives the zeroes of J;
2. for each J_i we will obtains polynomials $S_i(z_2, \ldots, z_n, t, X_2, \ldots, X_n)$, $i = 1 \ldots t_i$ such that for each zero $\eta := (\eta_2, \ldots, \eta_n)$ of J_i a standard basis of $R_1, \ldots, R_t$ is given by
$$\{S_i(\eta_2, \ldots, \eta_n, t, X_2, \ldots, X_n\}_{i=1\ldots t_i}$$
3. since $\{S_i(\eta_2, \ldots, \eta_n, t, X_2, \ldots, X_n\}$, $i = 1 \ldots t_i$ is a standard basis of in$(\phi_\eta(J_i))$ the zeroes of J_i are equivalent as required in Step 6).

This hopefully explains why we chose a so careful formulation of step 6) instead of the conceptually simpler, but computationally less efficient, formulation “Compute all roots of J”.

We are still left to discuss how to deal with real roots. Our proposal is the following:

1) There are multivariate versions of Sturm Theorem to decide whether a 0-dimensional ideal J_i has real zeroes; we use such techniques and we apply Steps 7) and 9) only if J_i has real zeroes, and Steps 8) and 10) only if L_i has real zeroes.

2) To compute L_i from J_i we do the following: since J_i is known through a Gröbner basis, there are techniques to compute 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 still performed in the computational model for algebraic numbers described above; so they are done for all roots of J_i (resp. L_i) provided that J_i (resp. L_i) has at least one real root. However when performing Steps 7.c), 8.c), 9.c) and 10.c) in the outmost level of recursion, we use the seminumerical techniques advocated in [4,3] to obtain floating point approximations of all real algebraic numbers appearing as coefficients.

4) Therefore in particular the poynomials 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.

5.11 A Complete Example

We apply our algorithm now to compute the real branches of the fourth curve discussed in MacMillan's paper, which is generated by the following polynomials in $\mathbf{Q}[z,x,y]$:

$$F_1 := (x^9 + y^9) + (x^6 + y^6)z + xyz^2 + z^5$$

$$F_2 := y^{10} + x^4 z + y^2(x-y)z + z^3$$

We are looking for Puiseux expansions in $\mathbf{R}[[z]]_{\mathrm{Puis}}$.

The computations have been performed partially by hand and mainly by using the system CoCoA developed in Genova (see Section 5.12).

The multiplicity of the origin as a zero of

$$(F_1(0,x,y),\ F_2(0,x,y)) = (x^9 + y^9,\ y^{10})$$

is 90 so we have altogether 90 solutions centered at the origin. MacMillan's exponents are 1/7, 2/7, 2/3, 3/2.

A standard basis computation shows that (F_1, F_2) is a standard basis for the weights $(7,1,1)$. The ideal

$$J_0 = (x^9 + y^9,\ y^{10} + xy^2 - y^3)$$

has multiplicity 90, so all solutions have initial exponent $\nu \geq 1/7$. The ideal

$$J := (x^9 + y^9,\ y^{10} + xy^2 - y^3) : (x^{90},\ y^{90})$$

is equal to the ideal

$$(x + y^8 - y,\ y^{63} - 9y^{56} + 36y^{49} - 84y^{42} + 126y^{35} - 126y^{28} + 84y^{21} - 36y^{14} + 9y^7 - 2).$$

Its roots are all simple and its multiplicity is 63; so there are 63 solutions with initial exponent $\nu \geq 1/7$ corresponding to 9 branches and 27 solutions with initial exponent $\nu > 1/7$. Only one of these 9 branches is real and has initial approximation $\eta := (-\sqrt[7]{2}, \sqrt[7]{2})$. Substitution gives the polynomials:

$t^{11} + 210b^6y^4 + 252b^5y^5 + 210b^4y^6 + 120b^3y^7 + 45b^2y^8 + 10by^9 + y^{10} + b^4t - 4b^3tx + 6b^2tx^2 - 4btx^3 + tx^4 + b^2x + 15b^2y + 2bxy + 86by^2 + 239y^3$

$t^{26}+2b^6t^4-6b^5t^4x+15b^4t^4x^2-20b^3t^4x^3+15b^2t^4x^4-6bt^4x^5+t^4x^6+6b^5t^4y+15b^4t^4y^2+20b^3t^4y^3+15b^2t^4y^4+6bt^4y^5+t^4y^6-b^2t^7+bt^7x+84b^6x^3-126b^5x^4+126b^4x^5-84b^3x^6+36b^2x^7-9bx^8+x^9-bt^7y+t^7xy+84b^6y^3+126b^5y^4+126b^4y^5+84b^3y^6+36b^2y^7+9by^8+y^9+18bx-72x^2+18by+72y^2$,

where b denotes $\sqrt[7]{2}$, from which we obtain:

$1/2b^5t^{11}+5b^6y^9+1/2b^5y^{10}-2b^6tx^3+1/2b^5tx^4+b^6xy+43b^6y^2+1/2b^5xy^2+239/2b^5y^3+210b^4y^4+252b^3y^5+210b^2y^6+120by^7+45y^8+b^2t-4btx+6tx^2+x+15y$,

$-1/504b^6t^{26}+1/28b^5t^{11}-1/504b^6t^4x^6-1/504b^6t^4y^6-1/504b^6x^9-1/504b^6t^7xy+179/504b^6y^9+1/28b^5y^{10}-1/7b^6tx^3+1/28b^5tx^4-1/126b^5t^4+1/42b^4t^4x-5/84b^3t^4x^2+5/63b^2t^4x^3-5/84bt^4x^4+1/42t^4x^5-1/42b^4t^4y-5/84b^3t^4y^2-5/63b^2t^4y^3-5/84bt^4y^4-1/42t^4y^5+1/252bt^7-1/252t^7x+1/7b^6x^2-1/3b^5x^3+1/2b^4x^4-1/2b^3x^5+1/3b^2x^6-1/7bx^7+1/28x^8+1/252t^7y+1/14b^6xy+41/14b^6y^2+1/28b^5xy^2+689/84b^5y^3+29/2b^4y^4+35/2b^3y^5+44/3b^2y^6+59/7by^7+89/28y^8+1/14b^2t-2/7btx+3/7tx^2+y$

which allow to apply the Implicit Function Theorem.

We now investigate the next initial exponent $2/7$. A standard basis for the weights $(7,2,2)$ is given by:

$F_1=(x^9+y^9)+(x^6+y^6)z+xyz^2+z^5$,

$F_2=y^{10}+x^4z+y^2(x-y)z+z^3$,

$F_3=y^2z^6-x^8z^3-x^7yz^3-x^6y^2z^3-x^5y^3z^3-x^4y^4z^3-x^3y^5z^3-x^2y^6z^3-xy^7z^3-y^8z^3-x^8y^{10}-x^7y^{11}-x^6y^{12}-x^5y^{13}-x^4y^{14}-x^3y^{15}-x^2y^{16}-xy^{17}-y^{18}-x^{12}z-x^{11}yz-x^{10}y^2z-x^9y^3z-x^8y^4z-x^7y^5z-x^6y^6z-x^5y^7z-x^4y^8z+x^6y^2z^2+y^8z^2+2y^{11}z+xy^3z^3$.

The ideal J_0 has multiplicity 27 (so that there are no solutions with initial exponent ν, $1/7<\nu<2/7$). The ideal J is $(x-y,\ y^7+1/2)$ and has multiplicity 7. There are therefore 20 solutions with initial exponent $\nu>2/7$ and 7 solutions (corresponding to a single branch) with initial exponent $2/7$.

The ideal J has the single real root $\eta:=(-1/\sqrt[7]{2},-1/\sqrt[7]{2})$ which is simple. Step 7 gives then:

$2/7b^6t^{17}-10b^6t^7y^9-b^5t^7y^{10}+2/7b^6x^9+45/2b^6t^7y^2+60b^5t^7y^3+105b^4t^7y^4+126b^3t^7y^5+105b^2t^7y^6+60bt^7y^7+45/2t^7y^8+2/7b^6y^9-b^5t^8+2/7b^6tx^6+2/7b^6ty^6-4b^6t^2x^3-b^5t^2x^4-1/4bt^7-36/7b^6x^2-12b^5x^3-18b^4x^4-18b^3x^5-12b^2x^6-36/7bx^7-9/7x^8-5/2t^7y-12/7b^6xy-22/7b^6y^2-b^5xy^2-11b^5y^3-18b^4y^4-18b^3y^5-12b^2y^6-36/7by^7-9/7y^8-2/7b^5t-6/7b^4tx-15/7b^3tx^2-20/7b^2tx^3-15/7btx^4-6/7tx^5-6/7b^4ty-15/7b^3ty^2-20/7b^2ty^3-15/7bty^4-6/7ty^5+1/2b^2t^2+2bt^2x+3t^2x^2+x$

$2/7b^6t^{17}+10b^6t^7y^9+b^5t^7y^{10}+2/7b^6x^9-45/2b^6t^7y^2-60b^5t^7y^3-105b^4t^7y^4-126b^3t^7y^5-105b^2t^7y^6-60bt^7y^7-45/2t^7y^8+2/7b^6y^9+b^5t^8+2/7b^6tx^6+2/7b^6ty^6+4b^6t^2x^3+b^5t^2x^4+1/4bt^7-36/7b^6x^2-12b^5x^3-18b^4x^4-18b^3x^5-12b^2x^6-36/7bx^7-9/7x^8+5/2t^7y+16/7b^6xy-50/7b^6y^2+b^5xy^2-13b^5y^3-18b^4y^4-18b^3y^5-12b^2y^6-36/7by^7-9/7y^8-2/7b^5t-6/7b^4tx-15/7b^3tx^2-20/7b^2tx^3-15/7btx^4-6/7tx^5-6/7b^4ty-15/7b^3ty^2-20/7b^2ty^3-15/7bty^4-6/7ty^5-1/2b^2t^2-2bt^2x-3t^2x^2+y$

where $b=-1/\sqrt[7]{2}$.

We now investigate the initial exponent $2/3$. A standard basis for the weights $(3,2,2)$ is:

$F_1=x^9+y^9+x^6z+y^6z+z^5+xyz^2$,

$F_2=-x^6y^{10}-y^{16}-y^{10}z^4-xy^{11}z+x^{13}+x^4y^9+x^{10}y^2-x^9y^3+xy^{11}-y^{12}+x^9z^2+y^9z^2$,

$F_3=y^{10}+x^4z+xy^2z-y^3z+z^3$,

$F_4 = -y^{10}z + x^9y + y^{10} + x^6yz + y^7z + yz^5 - x^4z^2 + y^3z^2 - z^4,$

$F_5 = xy^{10}z - x^{10}y + x^9y^2 - xy^{10} + y^{11} - x^7yz + x^6y^2z - xy^7z + y^8z - xyz^5 + y^2z^5 + x^5z^2 + xz^4.$

The ideal J_0 has multiplicity 3 (so that there are 17 solutions with initial exponent ν, $2/7 < n < 2/3$). The ideal J is $(x,\ y^3 - 1)$ which has multiplicity 3 and has only simple roots, the only real one being $(0, 1)$, which corresponds to a real analytic branch of index 3 and intial exponent $2/3$. Step 7 gives then:

$t^8x^9 + t^8y^9 + 9t^8y^8 + 36t^8y^7 + 84t^8y^6 + 126t^8y^5 + 126t^8y^4 + t^5x^6 + 84t^8y^3 + t^5y^6 + 36t^8y^2 + 6t^5y^5 + 9t^8y + 15t^5y^4 + t^8 + 20t^5y^3 + 15t^5y^2 + 6t^5y + 2t^5 + xy + x$

$-1/3t^{11}y^{10} - 10/3t^{11}y^9 - 15t^{11}y^8 - 40t^{11}y^7 + 1/3t^8x^9 - 70t^{11}y^6 + 1/3t^8y^9 - 84t^{11}y^5 + 3t^8y^8 - 70t^{11}y^4 + 12t^8y^7 - 40t^{11}y^3 + 28t^8y^6 - 15t^{11}y^2 + 42t^8y^5 - 10/3t^{11}y + 42t^8y^4 - 1/3t^{11} + 1/3t^5x^6 + 28t^8y^3 + 1/3t^5y^6 + 12t^8y^2 + 2t^5y^5 + 3t^8y + 5t^5y^4 + 1/3t^8 + 20/3t^5y^3 + 5t^5y^2 - 1/3t^2x^4 + 2t^5y + 2/3t^5 - 1/3xy^2 + 1/3y^3 - 1/3xy + y^2 + y$

Since the origin is not a solution of J_0 there are no solution with initial exponent $\nu > 2/3$. We have yet to find the 17 solutions with initial exponent ν, $2/7 < \nu < 2/3$. The standard basis for the weights $(3, 2, 2)$ gives a potential MacMillan exponent $\nu = 1/2$, while the standard basis for the weights $(7, 2, 2)$ does not introduce new initial exponents in the range $(2/7, 2/3)$. Computing a standard basis for the weights $(1, 1, 2)$ gives:

$F_1 = x^9 + y^9 + x^6z + y^6z + z^5 + xyz^2,$

$F_2 = -x^6y^{10} - y^{16} - xy^{11}z + x^4z^5 + z^7 + x^{13} + x^4y^9 + x^9z^2 + y^9z^2 + xy^2z^5 - y^3z^5 + x^{10}y^2 - x^9y^3 + xy^{11} - y^{12},$

$F_3 = y^{10} + x^4z + xy^2z - y^3z + z^3,$

$F_4 = -y^{10}z + x^9y + y^{10} + x^6yz + y^7z + yz^5 - x^4z^2 + y^3z^2 - z^4\ ,$

$F_5 = xy^{10}z - x^{10}y + x^9y^2 - xy^{10} + y^{11} - x^7yz + x^6y^2z - xy^7z + y^8z - xyz^5 + y^2z^5 + x^5z^2 + xz^4.$

The ideal J_0 has multiplicity 7 and the ideal $J = (y,\ x^4 + 1)$ multiplicity 4. Therefore there are 13 solutions with initial exponent ν, $2/7 < \nu < 1/2$, 3 with initial exponent $\nu > 1/2$ (which are the ones already found with initial exponent $\nu = 2/3$) and 4 with initial exponent $1/2$. The sistem $y = x^4 + 1 = 0$ has no real solution. Homogeneization of J gives the ideal ${}^hJ = (y,\ x^4 + z^2)$, so $\sigma({}^h(J)) = {}^hJ$, and the ideal whose roots are $\{(\xi\eta_2, \xi\eta_3) : (\eta_2, \eta_3) \text{ root of } J\}$, where ξ is a 4^{th}-root of 1, is again J. In fact the roots of J are $\{(\zeta^{2i+1}, 0) : i = 0 \ldots 3\}$ where ζ^8 is a primitive 8^{th}-root of 1; we can choose $\xi = \zeta^2$ so that $(\xi\zeta^{2i+1}, 0) = (\zeta^{2i+3}, 0)$. The two branches with initial exponent $1/2$ are therefore both complex.

We have still to find the 13 solutions with initial exponent in the range $(7/2, 1/2)$. The standard basis for the weights $(2, 1, 1)$ gives a new candidate exponent $1/3$. Computing a standard basis for the weights $(3, 1, 1)$ we obtain that J_0 has the origin as its only root of multiplicity 7, so that the missing thirteen solutions have initial exponent in the range $(7/2, 1/3)$. The standard basis also introduces the new candidate exponent $4/13$. With respect to the weights $(13, 4, 4)$ we obtain that J_0 has multiplicity 20 and that $J = (y, x^{13} + 1)$ has multiplicity 13. The single branch of index 13 and initial exponent $4/13$ is real since J has the single real root $(-1, 0)$, to which Step 7 can be applied. In conclusion there are 4 real branches of indexes 7, 7, 3, 13 and initial exponents $1/7$, $2/7$, $2/3$, $4/13$. Moreover there are 8 complex branches of index 7 and initial exponent $1/7$ and 2 complex branches of index 2 and initial exponent $1/2$.

Since in the previous example, we never needed to perform our "main" transformation, since we never encountered multiple roots, we perform here a partial computation on the second MacMillan example, where multiple roots are met.

The ideal is in $\mathbf{Q}[u,x,y,z]$ and we look for Puiseux expansions in $\mathbf{K}[[u]]_{\mathrm{Puis}}$. It is generated by

$$(x^3+(x+y+z)u+u^2,\ y^4+(x-y+z)u-u^3,\ z^5+(x^2+y^2+zx)u+xu^2+u^4)$$

We look for Puiseux expansions of initial exponent $1/3$. The ideal

$$J_0=(x^3,\ y^4+x-y+z,\ z^5+x^2+y^2+xz)$$

has multiplicity 60, the origin as a root of multiplicity 6 and other 18 triple roots which are the roots of the ideal

$$J_1=(x,\ y-z^{10}-z,\ z^{18}+2z^9+z^3+1).$$

We perform therefore the transformation: $x=xt,\ y=(b+y)t,\ z=(c+z)t,\ u=t^3$ where (b,c) is a root of $(b-c^{10}-c, c^{18}+2c^9+c^3+1)$ and we obtain the curve defined by the polynomials:

$c^{10}t+2ct+x^3+xt+yt+zt+t^3$,

$-4c^{15}y+4c^{10}y^3-4c^6y-6c^5y^2+4cy^3+x+y^4-y+z-t^5$,

$2c^{10}y+5c4z+10c^3z^2+10c^2z^3+cx+2cy+5cz^4+x^2+xz+xt^2+y^2+z^5+t^7$.

We choose the MacMillan exponent $1/3$ and we compute a standard basis for the weights $(3,1,1,1)$. The ideal J is generated by:

$x^3+c^{10}+2c$,

$z-14357/49781xc^{15}+10250/149343xc^{12}-4920/49781xc^9-84800/149343xc^6+22550/149343xc^3-25181/49781x$,

$y-29651/149343xc^{15}+10250/49781xc^{12}-14760/49781xc^9-55276/149343xc^6+22550/49781xc^3-25762/49781x$

where c satisfies $c^{18}+2c^9+c^3+1$. For each of the 18 values of c there are exactly 3 simple roots of the system.

Remark that a single computation is all we need to perform Step 7 for all 4-tuples (c,x,y,z) satisfying the conditions above.

5.12 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 [1,7]. 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 $J:(X_2^h,\dots,X_n^h)$ requires n Gröbner basis computations and can be quite costly. CoCoA allows also to compute Gröbner bases for polynomial ideals over a field $\mathbf{Q}(\eta_2,\dots,\eta_n)$ where $(\eta_2,\dots,\eta_n)$ is a root of a zero-dimensional ideal I, at least in the case in which the surjection $\mathbf{Q}[X_2,\dots,X_n]/I\to\mathbf{Q}(\eta_2,\dots,\eta_n)$

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 (6) and real-root recognition where ad hoc hand-driven computations are required.

Here we focus on Steps (1) to (5) which can be performed by the following instructions in CoCoA.

h = TangentCone(i); $h = h[z = 1]$

computes the standard basis $(H_1, \ldots, H_t)$ of $(F_1, \ldots, F_s)$ and returns J_0.

Mult(R/h)

counts the number of roots with multiplicity.

$j = h$: ideal(x^m, y^m); k = gbasis(j); Mult(S/j)

removes the null root, counts the number of non zero roots, with multiplicity, and gives the ideal J; m is the number of roots with multiplicity.

The tables below report an outline of the computation (with timings in secs.) for the example discussed in the previous paragraph and for another example in MacMillan, i.e. the curve with equations:

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

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

TABLE 5.1. 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
$j = h$: ideal(x^m, y^m)	5.91	4.38	2.36	2.95		2.56
k = 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

* the initial exponent has been derived by slopes derived from a standard basis computation.

\+ the standard basis computation has been truncated (cf. Appendix B).

5.13 Appendix A. Algebraic Preprocessing

Throughout the paper we have assumed that our input is a set of polynomials $F_1, \ldots, F_s$ in $K[X_1, \ldots, X_n]$, where K is a finite algebraic extension of the rationals, which define a curve Γ, whose irreducible components are all simple. To test this, by symbolic computation methods, we have first to compute a Gröbner basis of $I = (F_1, \ldots, F_s)$, by which we can read the dimension of I; if the dimension of I is 1 then the components of Γ are only curves and points.

It is then possible to compute the top-radical of $I := (F_1, \ldots, F_s)$ which is the ideal defining a variety whose irreducible components are all simple and are the components of Γ

TABLE 5.2. Invariants & Timings

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		0	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
$j = h$: ideal(x^m, y^m)	1.79		0.51		0.83
k = gbasis(j)	0.31		0.15		0.15
Mult(S/j)	0.18		0.20		0.18

* the initial exponent has been derived by slopes derived from a standard basis computation.

of maximal dimension. If I coincides with its top-radical, then I satisfies the assumptions; otherwise the algorithm can be applied to the top-radical of I.

Assuming now that I defines a curve Γ with no multiple irreducible components, the singular points of Γ, which are finite in number are the roots of the 0-dimensional ideal generated by $(F_1, \ldots, F_s)$ and by the maximal minors of the Jacobian matrix $(\partial F_i/\partial X_j)_{ij}$.

If $\alpha := (\alpha_1, \ldots, \alpha_n)$ is a singular point of the curve, by the translation $X_i \to X_i - \alpha_i$,we can assume that α is the origin. Our final assumption is then that none of the irreducible components of Γ passing through the origin is contained in the hyperplane $X_1 = 0$.

To check this, let $\pi : K[X_1, \ldots, X_n] \to K[X_2, \ldots, X_n]$ be the projection such that $\pi(X_1) = 0$, $\pi(X_i) = X_i$ for $i > 1$. The local dimension of $\pi(I)$ is 1 if and only if there are components of Γ passing through the origin and contained in the hyperplane $X_1 = 0$. Then the ideal $J := I : \pi(I)$ locally defines a curve whose components are the components of I not contained in the hyperplane $X_1 = 0$. We can then apply our algorithm separately to J and to $\pi(I)$.

5.14 Appendix B. Truncated Standard Basis Computations

In the example presented in Section 5.11, the standard basis computation for weights $(3, 1, 1)$ and $(13, 4, 4)$ has been truncated after five elements have been computed; there are at least two more elements in it, but a complete computation failed after approx. 20 mins. for memory overflow. In both cases however the missing elements would not change the ideal J_0. In fact the only possible effects of truncating a standard basis computation are that the resulting ideal J_0 has higher multiplicity than the correct output, i.e.:

1) the resulting ideal has some more zeroes than the correct output; this will be detected when applying recursively the algorithm to the transformed ideal: a complete standard basis computation of the R_i's will produce in this case an ideal with no zeroes;

2) the resulting ideal has some zeroes in common with the correct output, but with higher multiplicity; again a complete standard basis computation of the R_i's will allow to find the correct multiplicity;

3) the multiplicity of the origin in the resulting ideal is higher than μ_0; this can be tested by comparing the resulting μ_0 with the value of μ for the next higher initial exponent; if the two values are equal, then the obtained value for μ_0 is the correct one; otherwise the standard basis computation must be resumed.

In our example, for the weights $(3, 1, 1)$ we obtain $\mu = 7$; since this is the maximal possible value for for the multiplicity of J_0, we must have obtained the correct output. For the weights $(4, 4, 13)$ we obtain $\mu_1 = 13$; it could be that the correct value is less (so that there are solutions with initial exponent ν, $2/7 < \nu < 13/4$). Since each root however returns a solution (as it is checked at the next recursion level), this is not the case.

It is to be remarked that a common feature of standard (and Gröbner) basis computations is that the most expensive part of the algorithm often occurs after a standard basis has been obtained and is only necessary to certify the result. Moreover standard basis elements entering late in the output have higher chances to modify the standard basis only but not the ideal J_0. It would be worthwhile to investigate how much it is possible to make recourse in an automatic way to truncated standard basis computations, while recovering missing informations on the number of solutions by backtracking through the recursion levels.

5.15 References

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

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

3 P. Cellini, P. Gianni, and C. Traverso. ??? In *???*, ???, page ??? ???, 1991.

4 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.

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

6 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.

7 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.

8 W. Groebner. *Algebraische Geometrie*. Bibliographisches Institut Mannheim, 1968-70.

9 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.

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

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

12 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.

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

14 T.Mora, G.Pfister, and C.Traverso. An introduction to the tangent cone algorithm. In *Issuses in robotics and non-linear geometry*. JAI Press, 1991.

15 T.Mora and C. Traverso. Representing algebraic numbers by Groebner bases. Proc. MEGA 92. (submitted).

16 C. Traverso. Communication at the workshop Computing in Algebraic Geometry. Cortona, 1991.