Algebraic Extensions in the Resolution of Curve-Singularities [1]

Peter Stadelmeyer

Research Institute for Symbolic Computation
Johannes Kepler Universität
Linz, Austria

Peter.Stadelmeyer@risc.uni-linz.ac.at

Abstract

Let $\mathcal{C} \subset \mathbf{A}^2_K$ be an irreducible algebraic curve in the affine plane and let $\mathfrak{z}$ be a curve-branch of $\mathcal{C}$. In this paper we compare the algebraic extensions necessary to resolve $\mathfrak{z}$ either by quadratic transformations or Puiseux-series expansions.

It is well known that the residual field of $\mathfrak{z}$ is isomorphic to the coefficient field of a rational Puiseux-expansion of $\mathfrak{z}$. We will show, that this is also true for the coefficient field of quadratic transformations of $\mathfrak{z}$. This allows us to give an a-priory bound for the degree of the field extension necessary to resolve $\mathfrak{z}$.

We will also present an alternative definition of rational Puiseux-expansions based on the implicit function theorem and quadratic transformations.

Contents

1. Introduction	2
2. Resolution	2
3. Algebraic Extensions	7
Appendix A. Algorithms	11
References	14

[1] Supported by the Austrian Fonds zur Förderung der wissenschaftlichen Forschung project number P11160-TEC "HySaX".

1. Introduction

Let $\mathcal{C} \subset \mathbf{A}^2_K$ be an irreducible algebraic curve in the affine plane defined by a polynomial $f(x,y) \in k[x,y]$ and let $\mathfrak{z}$ be a curve-branch of $\mathcal{C}$. In Section 2 we describe two well-known standard methods to resolve $\mathfrak{z}$, namely quadratic transformations and Puiseux-series expansions.

We then compare the algebraic extensions necessary to resolve $\mathfrak{z}$ by each of these methods in Section 3. As shown in [Duval, 1989] the coefficient field of a rational Puiseux-expansion is equal to the residual field of $\mathfrak{z}$. This is optimal in the sense of a minimal field extension over the ground field k where $f(x,y)$ is defined. We will see that when resolving $\mathfrak{z}$ by quadratic transformations all computations can also be done in the residual field of $\mathfrak{z}$. This allows us to give an a-priory bound for the degree of the field extension necessary to resolve $\mathfrak{z}$.

Using the fact that both resolution methods yield the same field extension, namely the before-mentioned residual field, we present an alternative way of defining rational Puiseux-expansions based on the implicit function theorem and quadratic transformations.

In Appendix A a resolution algorithm using quadratic transformation is described. An algorithm to compute a system of rational Puiseux-series can be found in [Duval, 1989].

2. Resolution

Throughout this paper, let k be a commutative field with characteristic 0, e.g. the rational numbers, and let K be its algebraic closure. The rings of formal power-series over k and K in the indeterminate t are denoted by $k[[t]]$ and $K[[t]]$, respectively. The algebraically closed field of Puiseux-series over K in the indeterminate t is written as $K\langle\langle t\rangle\rangle$.

Let $f(x,y) \in k[x,y]$ be a polynomial of y-degree n and monic in y, i.e.

$$f(x,y) = y^n + a_{n-1}(x)y^{n-1} + \cdots + a_1(x)y + a_0(x),$$

where $a_i(x) \in k[x]$, for $0 \le i < n$. We assume that $f(x,y)$ is absolutely irreducible, i.e. irreducible in $K[x,y]$.

The polynomial $f(x,y)$ defines a plane algebraic curve $\mathcal{C}$ in the affine plane $\mathbf{A}^2_K$, namely the set of points given by

$$\mathcal{C} = \{(x_0,y_0) \in \mathbf{A}^2_K \mid f(x_0,y_0) = 0\}.$$

A point $q = (q_x, q_y) \in \mathbf{A}^2_K$ has *multiplicity* m *w.r.t.* $\mathcal{C}$ *(or* $f(x,y)$*)*, written as $\nu_q(\mathcal{C}) = m$ (or $\nu_q(f) = m$), if

$$\frac{\partial^{i+j} f}{\partial x^i \partial y^j}(q_x,q_y) = 0 \quad \text{, for all } i+j < m,$$
$$\frac{\partial^{i+j} f}{\partial x^i \partial y^j}(q_x,q_y) \neq 0 \quad \text{, for some } i+j = m.$$

We say that q is a point of the curve $\mathcal{C}$ if $\nu_q(\mathcal{C}) > 0$. The point q is called a *singular point of* $\mathcal{C}$ if $\nu_q(\mathcal{C}) > 1$.

From now on let $q \in \mathbf{A}^2_K$ be a point with multiplicity $m > 0$ w.r.t. $\mathcal{C}$. W.l.o.g. we can assume that the coordinate system is chosen in such a way that $q = (0, 0)$. The polynomial $f(x, y)$ can then be written as

$$f(x, y) = \sum_{d \geq m} f_d(x, y),$$

where $f_d(x, y) \in k[x, y]$, for $d \geq m$, are homogenous polynomials of degree d.

In the following two subsections we will shortly describe two standard methods to resolve curve singularities, namely quadratic transformations and Puiseux-series expansions. No new results will be presented there.

2.1. **Quadratic Transformations.** It is well known that any plane curve singularity can be resolved by a finite sequence of quadratic transformations. For details and proofs we refer to [Abhyankar, 1983], [Abhyankar, 1990] and [Brieskorn and Knörrer, 1986].

Definition 1. A *quadratic transformation (QT) with the origin as center* is defined as one of the following two transformations

$$\begin{aligned} \sigma' \colon \mathbf{A}^2_K \to \mathbf{A}^2_K, &\quad (x, y) \mapsto (x, xy), \\ \sigma'' \colon \mathbf{A}^2_K \to \mathbf{A}^2_K, &\quad (x, y) \mapsto (xy, y). \end{aligned}$$

We call the QT σ' a *QT of type I* and σ'' a *QT of type II.*

If we apply σ' to $f(x, y)$ we get

$$\begin{aligned} (f \circ \sigma')(x, y) &= f(x, xy) \\ &= f_m(x, xy) + f_{m+1}(x, xy) + \cdots + f_d(x, xy) + \cdots \\ &= x^m f_d(1, y) + x^{m+1} f_{m+1}(1, y) + \cdots + x^d f_d(1, y) + \cdots \\ &= x^m \left(f_m(1, y) + x f_{m+1}(1, y) + \cdots + x^{d-m} f_d(1, y) + \cdots \right) \\ &= x^m f'(x, y) = f^*(x, y). \end{aligned}$$

Definition 2. The curve defined by $f^*(x, y)$ is called the *total transform of* $\mathcal{C}$ and will be denoted by $\mathcal{C}^*$. It factors into the curve $\mathcal{C}'$, called the *proper transform of* $\mathcal{C}$, defined by $f'(x, y)$ and the line $\mathcal{E}'$ defined by $e(x, y) = x^m$, called the *exceptional line.* The exceptional line meets the proper transform in a certain number of points, called the *neighboring points of the origin*, which are the common solutions of $e(x, y) = 0$ and $f'(x, y) = 0$. The coordinates of the neighboring points are therefore given by $(0, \xi)$, where ξ is a root of $f_m(1, y)$.

For a QT of type II the total and proper transform of $\mathcal{C}$ are defined analogously, with the difference that the exceptional line $\mathcal{E}'$ is now given by $e(x,y) = y^m$ and the coordinates of the neighboring points are $(\xi, 0)$, where ξ is a root of $f_m(x,1)$.

Translating the coordinate system of the transformed curve in such a way that a neighboring point is in the origin, we can again apply a QT (now to the transformed curve). Iterating this process we get a sequence which is defined by the types of the QTs and the coordinates of the neighboring points.

Definition 3. A *sequence* γ *of QTs of length* H is defined as

$$\gamma = (\sigma_1, \dots, \sigma_H; f', e'),$$

where σ_h, for $1 \le h \le H$, is either of the form

$$\sigma_h = (I, \xi_h) \qquad\qquad \text{(QT of type I, and coordinate } (0, \xi_h))$$

or

$$\sigma_h = (II, \xi_h) \qquad\qquad \text{(QT of type II, and coordinate } (\xi_h, 0)).$$

The proper transform and the exceptional line of $\mathcal{C}$ w.r.t. the QTs σ_1, ..., σ_H are given by f' and e'.

The *coefficient field* k^γ *of* γ is defined as $k^\gamma = k(\xi_1, \dots, \xi_H)$.

Definition 4. We say that $\mathcal{C}$ has *normal crossings at* q if it defined by $f(x,y) = g(x,y)z_1(x,y)^a z_2(x,y)^b$, where a, b are non-negative integers, $\nu_q(g) = 0$ and $\nu_q(z_1) = \nu_q(z_2) = 1$. In addition to that, the tangent of the curve defined by $z_1(x,y)$ at q has to be different from the tangent of the curve defined by $z_2(x,y)$ at q.

We can now formulate the main theorem about resolution by quadratic transformations.

Theorem 1 (Total Resolution Theorem for Plane Curves). *There always exists a sequence of QTs of finite length such that the total transform of $\mathcal{C}$ has only normal crossings.*

Proof. See e.g. [Abhyankar, 1990]. □

Theorem 1 guarantees termination (and hence correctness) of the QT-resolution algorithm given in Appendix A.1.

2.2. **Puiseux-series Expansions.** As mentioned above, another possibility to resolve plane curve singularities is by using Puiseux-series expansions. Again, for more details we refer the reader to [Abhyankar, 1990], [Brieskorn and Knörrer, 1986], [Duval, 1989] and [Walker, 1978]. For a discussion about the close connection between QTs and Puiseux-series expansions see also [Stadelmeyer and Winkler, 1997] and [Stadelmeyer, 2000].

According to *Newton's Theorem* [Newton, 1660] the polynomial $f(x, y)$ can be factored into

$$f(x, y) = \prod_{i=1}^{n} (y - \mathfrak{B}_i(x)), \text{ where}$$
$$\mathfrak{B}_i(x) = \sum_{h>0} \mathfrak{b}_{i,h} x^{h/e_i}.$$

We assume that each $e_i > 0$ is as small as possible, i.e. $\gcd(\{h \mid \mathfrak{b}_{i,h} \neq 0\}) = 1$, for $1 \leq i \leq n$.

The series $\mathfrak{B}_i(x) \in K\langle\langle x \rangle\rangle$, for $1 \leq i \leq n$, are called the *Puiseux-series of* $f(x, y)$ *at the origin*. The numbers e_i are called the *ramification indices of the series* $\mathfrak{B}_i(x)$.

Definition 5. A *local parameterization* δ *of the curve* C *at the origin* is a pair $\delta = (A(t), B(t))$, where $A(t) = \sum_{h>0} a_h t^h$, $B(t) = \sum_{h>0} b_h t^h \in K[[t]]$, and $f(A(t), B(t)) = 0$. The *coefficient field* k^δ *of* δ *over* k is defined as the field $k^\delta = k(a_1, b_1, a_2, b_2, \ldots)$.

We say that two local parameterizations $(A(t), B(t))$ and $(A'(t), B'(t))$ are *equivalent w.r.t.* k' if there exists a power-series $T(t) \in k'[[t]]$ with $\mathbf{o}_t(T(t)) = 1$ such that $A(t) = A'(T(t))$ and $B(t) = B'(T(t))$. If we simply say equivalent we mean equivalent w.r.t. K.

It surely holds that $f(x, \mathfrak{B}_i(x)) = 0$, for $1 \leq i \leq n$. So each Puiseux-series $\mathfrak{B}_i(x)$ yields a local parameterization δ_i of C at the origin, called a *Puiseux parameterization*, of the following special form

$$\delta_i = (A_i(t), B_i(t)) = (t^{e_i}, \mathfrak{B}_i(t^{e_i})) = (t^{e_i}, \sum_{h>0} \mathfrak{b}_{i,h} t^h).$$

The sets $\mathfrak{z}_i \subset \mathbf{A}_K^2$ of points defined by

$$\mathfrak{z}_i = \{(A_i(t), B_i(t)) \in \mathbf{A}_K^2 \mid t \in K\}$$

are called the *curve-branches of* C *at the origin*. As can easily be seen, equivalent local parameterizations define the same curve-branch.

The *ramification index of the curve-branch* $\mathfrak{z}_i$ is defined as the ramification index of $\mathfrak{B}_i(x)$, i.e. e_i.

Let J be the number of different curve-branches of C at the origin. The set $\mathbf{I} = \{1, \ldots, n\}$ can then be partitioned into subsets $\mathbf{I}_j$, for $1 \leq j \leq J$, such that all δ_i, for $i \in \mathbf{I}_j$, are equivalent.

If we assume that the Puiseux parameterizations are labeled in such a way that $j \in \mathbf{I}_j$ holds, for $1 \leq j \leq J$, we have $|\mathbf{I}_j| = e_j$ and $n = \sum_{1 \leq j \leq J} e_j$.

Definition 6. A *generalized Puiseux parameterization* δ *of* $\mathcal{C}$ *at the origin* is a local parameterization of $\mathcal{C}$ at the origin of the form

$$\delta = (A(t), B(t)) = (at^e, \sum_{h>0} b_h t^h), \text{ with } a \neq 0.$$

Definition 7. A *system* Δ *of rational Puiseux parameterizations of* $\mathcal{C}$ *at the origin over* k is a set $\Delta = \{\delta_1, \ldots, \delta_J\}$ of non-equivalent generalized Puiseux parameterizations of $\mathcal{C}$ which is invariant under the action of the Galois group $\mathcal{G} = \mathrm{Gal}(K/k)$.

We will also call a pair δ_j, $1 \leq j \leq J$, a *rational Puiseux-series* of $f(x, y)$.

Let G denote the number of $\mathcal{G}$-orbits in a system $\Delta = \{\delta_1, \ldots, \delta_J\}$ of rational Puiseux parameterizations of $\mathcal{C}$ over k and let k^{δ_j}, for $1 \leq j \leq J$, be the corresponding coefficient fields. We define the numbers ϵ_j as $\epsilon_j = [k^{\delta_j} : k]$.

If we assume that δ_g, for $1 \leq g \leq G$, belong to different $\mathcal{G}$-orbits, then it holds that $n = \sum_{1 \leq g \leq G} e_g \epsilon_g$, since parameterizations in the same $\mathcal{G}$-orbit have the same ramification index.

3. Algebraic Extensions

In this section we show that the algebraic extensions needed to resolve a curve-branch by QTs are basically the same as those needed to compute a *rational* Puiseux parameterization of it. This allows us to use the well known connection between algebraic extensions and the (topological) structure of a singularity in the case of Puiseux parameterizations (see e.g. the paper of [Duval, 1989]) also for QTs.

Another consequence of this is an alternative characterization of rationality of a local parameterization in terms of QTs.

Let $\mathfrak{z}$ be a curve-branch of $\mathcal{C}$ with origin q and let $\gamma = (\sigma_1, \ldots, \sigma_H; f', e')$ be a sequence of QTs such that $\mathfrak{z}$ is totally resolved (as a curve-branch of $\mathcal{C}$). As usually, the coefficient field of γ is denoted by k^γ.

3.1. Quadratic Transformations.

Lemma 1. *For any local parameterization δ of $\mathfrak{z}$ it holds that $k^\gamma \subseteq k^\delta$, where k^δ is the coefficient field of δ.*

Proof. Let $\delta = \delta_0 = (A_0(t), B_0(t))$. We will show that $\xi_h \in k^\delta$, for all $1 \leq h \leq H$, and hence $k^\gamma \subseteq k^\delta$. To do so, we assume that $\xi_1, \ldots, \xi_{h-1} \in k^\delta$ and we show that $\xi_h \in k^\delta$.

Depending on which type σ_h is, we define the local parameterization $\delta_h = (A_h(t), B_h(t))$ as:

- The QT σ_h is of type I:
  Since this is equivalent to $\mathbf{o}_t(A_{h-1}(t)) \leq \mathbf{o}_t(B_{h-1}(t))$, we define

$$\begin{aligned} A_h(t) &= A_{h-1}(t), \\ B'_h(t) &= \frac{B_{h-1}(t)}{A_{h-1}(t)}, \\ B_h(t) &= B'_h(t) - B'_h(0). \end{aligned}$$

  Obviously, $A_h(t)$, $B'_h(t)$, $B_h(t) \in k^\delta[[t]]$ and $\delta_h = (A_h(t), B_h(t))$ is the proper transform of δ_{h-1} w.r.t. σ_h. Further it holds that $\xi_h = B'_h(0)$ and hence $\xi_h \in k^\delta$ (see e.g. [Stadelmeyer, 2000]).

- The QT σ_h is of type II:
  In this case $\mathbf{o}_t(A_{h-1}(t)) > \mathbf{o}_t(B_{h-1}(t))$ and the proper transform δ_h of δ_{h-1} w.r.t. σ_h is given by

$$\begin{aligned} A_h(t) &= \frac{A_{h-1}(t)}{B_{h-1}(t)}, \\ B_h(t) &= B_{h-1}(t). \end{aligned}$$

  Since $\mathbf{o}_t(A_{h-1}(t)) > \mathbf{o}_t(B_{h-1}(t))$ we have $\xi_h = A_h(0) = 0 \in k^\delta$.

$\square$

3.2. **Puiseux-series Expansion.**

Lemma 2. *Let* $A(t) = \sum_{h\geq 0} a_h t^h \in k(\alpha)[[t]]$ *be a power-series with* $\mathbf{o}_t\,(A(t)) = m \geq 1$*. Then there exists a power-series* $B(t) \in k(\alpha)[[t]]$ *with* $\mathbf{o}_t\,(B(t)) = 1$ *such that* $A(B(t)) = a_m t^m$*.*

Proof. Let $A(t) = \sum_{h\geq m} a_h t^h$, $a_m \neq 0$ and let $B(t) = \sum_{h\geq 1} b_h t^h$. For $A(B(t)) = \sum_{h\geq m} c_h t^h$ we require that

$$c_h = \begin{cases} a_h & \text{if } h = m, \\ 0 & \text{if } h > m. \end{cases}$$

For $h = m$, since $c_m = a_m b_1^m$ we can set $b_1 = 1$.

For $h > m$, the coefficients c_h are equal to

$$c_h = \sum_{i=m}^{h} a_i\, f_{h,i} \quad \text{, where}$$

$$f_{h,i} = \sum_{\substack{i_1+2\,i_2+\cdots+h\,i_h=h,\\ i_1+i_2+\cdots+i_h=i}} \binom{i!}{i_1!\;i_2!\cdots i_h!} b_1^{i_1} b_2^{i_2}\cdots b_h^{i_h}.$$

From this it can be seen that $f_{h,i}$ depends on b_i, for $1 \leq i \leq h-i+1$, and therefore c_h depends on b_i, for $1 \leq i \leq h-m+1$. The coefficient b_{h-m+1} occurs exactly once in the sum c_h, namely as $a_m m b_1^{m-1} b_{h-m+1}$. Hence, setting $c_h = 0$ one gets a *linear* equation for b_{h-m+1}.

The coefficients of $B(t)$ can now be obtained iteratively by setting $c_h = 0$ and solving for b_{h-m+1}, for $h = m+1, m+2, \ldots$. ∎

Remark: In general there does not exist a power-series $B(t) \in k(\alpha)[[t]]$ such that $A(B(t)) = t^m$, because this would require setting $b_1 = (a_m)^{\frac{1}{m}}$ which may not be possible in $k(\alpha)$. This corresponds exactly to the difference of Puiseux parameterizations and generalized Puiseux parameterizations.

Lemma 3. *There exists a generalized Puiseux parameterization* δ *of* $\mathfrak{z}$ *with coefficient field* k^δ*, such that* $k^\delta \subseteq k^\gamma$*.*

Proof. Since $\bar{f}_H = \bar{f}$ has normal-crossings and $\mathbf{o}_t\left(\bar{f}_H(0,t)\right) = 1$, a local parameterization $(A'_H(t), B'_H(t))$ of $\bar{f}_H$ can be computed using the *implicit function theorem*. So we know that $A'_H(t), B'_H(t) \in k^\gamma[[t]]$ and $\mathbf{o}_t\,(A'_H(t)) = 1$. According to Lemma 2 there exists a reparameterization $T_H(t) \in k^\gamma[[t]]$ such that

$$A_H(t) = A'_H(T(t)) = a^{[H]} t,$$
$$B_H(t) = B'_H(T(t)),$$

and $A_H(t)$, $B_H(t) \in k^\gamma[[t]]$. Hence we have shown that there exists a generalized Puiseux parameterization $(A_H(t), B_H(t))$ for $\bar{f}_H$.

Now assume, for some $1 \le h \le H$, we already computed a generalized Puiseux parameterization $(A_h(t), B_h(t))$ of $\bar{f}_h$ such that $A_h(t)$, $B_h(t) \in k^\gamma[[t]]$.

A local parameterization of $\bar{f}_{h-1}$ is then either given by:

- The QT σ_h is of type I:

$$A'_{h-1}(t) = A_h(t)$$
$$B'_{h-1}(t) = A_h(t)(B_h(t) - \xi_h)$$

- The QT σ_h is of type II:

$$A'_{h-1}(t) = B_h(t)(A_h(t) - \xi_h)$$
$$B'_{h-1}(t) = B_h(t).$$

In both cases there exists a reparameterization $T_{h-1}(t) \in k^\gamma[[t]]$ such that $(A_{h-1}(t), B_{h-1}(t)) = (A'_{h-1}(T(t)), B'_{h-1}(T(t)))$ is a generalized Puiseux parameterization for $\bar{f}_{h-1}$ and $A_{h-1}(t)$, $B_{h-1}(t) \in k^\gamma[[t]]$.

But this means, we have shown that there exists a generalized Puiseux parameterization $(A_0(t), B_0(t))$ of $\mathfrak{z}$ whose coefficient field is a subfield of k^γ. □

Because a rational Puiseux parameterization δ of a curve-branch $\mathfrak{z}$ has the smallest possible coefficient field among all local parameterizations of $\mathfrak{z}$ we get $k^\gamma \subseteq k^\delta \subseteq k^\gamma$, which implies $k^\gamma = k^\delta$.

Lemma 4. *The coefficient field k^γ generated by a sequence γ of QTs which totally resolves a curve-branch $\mathfrak{z}$ is equal to the residual field of $\mathfrak{z}$.*

Proof. Follows from $k^\gamma = k^\delta$, where δ is a rational Puiseux parameterization of $\mathfrak{z}$ and the fact that k^δ is equal to the coefficient field of $\mathfrak{z}$ (see [Duval, 1989]). □

It can easily be seen, that the property of being *rational* for a system of generalized Puiseux parameterization only depends on the coefficient fields of the parameterizations. Using Lemma 3 we can characterize rational Puiseux parameterizations also as follows.

Lemma 5. *Let δ be a local parameterization of a curve-branch $\mathfrak{z}$. The parameterization δ is rational if and only if there exists a local parameterization δ' of $\mathfrak{z}$ as constructed in the proof of Lemma 3 (pull-back of QTs) which is equivalent to δ w.r.t. $k^{\delta'}$.*

Proof. From Lemma 4 we know that $k^{\delta'}$ is equal to the residual field of $\mathfrak{z}$. As mentioned above, the local parameterization δ is therefore rational if and only if k^{δ} is equal to $k^{\delta'}$. Since δ and δ' are parameterizing the same curve-branch $\mathfrak{z}$ (i.e. they are equivalent w.r.t. K) the fields k^{δ} and $k^{\delta'}$ are equal if and only if δ and δ' are equivalent w.r.t. $k^{\delta'}$. □

3.3. **Degree of Algebraic Extension.** For this subsection let γ be again a sequence of QTs which totally resolves $\mathfrak{z}$ and $\delta = (at^e, B(t))$ a rational Puiseux parameterization of $\mathfrak{z}$, where $\mathfrak{z}$ is a curve-branch of $\mathcal{C}$.

Lemma 6. *The degree of an algebraic extension necessary to resolve a curve-branch of a curve C by QTs (or Puiseux-series expansions) is less than or equal to the y-degree of the defining polynomial of C.*

Proof. From the previous subsection we know that $[k^{\gamma} : k] = [k^{\delta} : k]$. Let ϵ be the degree of the algebraic extensions. Using the fact that $e\epsilon \leq n$, where n is the y-degree of the defining polynomial of $\mathcal{C}$ (see Subsection 2.2), we have $\epsilon \leq n$. □

One way to deal with multiple algebraic extensions like $k(\alpha_1, \alpha_2)$ occuring in the resolution algorithms is to compute a primitive element α^* such that $k(\alpha^*) = k(\alpha_1, \alpha_2)$. An algorithm to compute α^* together with normal representations of α_1 and α_2 in $k(\alpha^*)$ can be found in [Winkler, 1996].

A direct consequence of Lemma 6 is that at most $\log(n)$ primitive elements have to be computed in the resolution algorithms.

Appendix A. Algorithms

Let $\mathcal{C}$ be a curve defined by $f(x,y) \in k[x,y]$ and let $\mathfrak{z}_j$, for $1 \le j \le J$, be the curve-branches of $\mathcal{C}$ with origin $(0,0)$.

A.1. **Resolution by Quadratic Transformations.** In the following we describe an algorithm to compute the total resolution sequences γ_j of $\mathfrak{z}_j$, for $1 \le j \le J$, together with their proper transforms, exceptional divisors and coefficient fields k^{γ_j}. The coefficient field is represented by a primitve element α, such that $k^{\gamma_j} = k(\alpha)$.

Function: `resolveQT`
In: $f(x,y) \in k[x,y]$.
Out: A list of proper transforms and exceptional divisors of the totally resolved curve defined by $f(x,y)$ together with their resolution sequences and primitive elements for their coefficient fields.

```
resolveQT(f)
begin
   return applyQT(f, 1, 1)
end
```

Function: `applyQT`
In: $f(x,y)$, $e(x,y) \in k(\alpha)[x,y]$
Out: Apply QTs of type I and type II.

```
applyQT(f, e, α)
begin
   return conc(applyQT1(f, e, α), applyQT2(f, e, α))
end
```

Function: `applyQT1`
In: $f(x,y)$, $e(x,y) \in k(\alpha)[x,y]$.
Out: Apply QTs of type I.

```
applyQT1(f, e, α)
begin
   res := [ ]
   d := ν_0(f)

   f' := x^{-d} f(x, xy)
   e' := x^d e(x, xy)
   for ξ ∈ K root of f'(0, y) ∈ k(α) do
      f'' := f'(x, y + ξ)
      e'' := e'(x, y + ξ)
      if (ξ = 0) or (o_t (f(0, t)) > 1) then
         res' := resolveQT(f'', e'', primitiveElement(α, ξ))
```

```
        for r in res' do
            res := append(res, [['I', d, ξ], r])
        od
    else
        res := append(res, [['I', d, ξ], f'', e'', α])
    fi
od

return res
end
```

Function: applyQT2
In: $f(x, y)$, $e(x, y) \in k(\alpha)[x, y]$.
Out: Apply QTs of type II.

```
applyQT2(f, e, α)
begin
  res := [ ]
  d := ν_0(f)

  f' := y^{-d} f(xy, y)
  e' := y^d e(xy, y)
  for ξ ∈ K root of f'(x, 0) ∈ k(α) do
      f'' := f'(x + ξ, y)
      e'' := e'(x + ξ, y)
      if (ξ = 0) or (o_t (f(t, 0)) > 1) then
          res' := resolveQT(f'', e'', primitiveElement(α, ξ))
          for r in res' do
              res := append(res, [['II', d, ξ], r])
          od
      else
          res := append(res, [['II', d, ξ], f'', e'', α])
      fi
  od

  return res
end
```

As explained e.g. in [Brieskorn and Knörrer, 1986] the QTs of type I and type II are in some sense overlapping. As a consequence of this, it may happen that one curve-branch has more than one resolution sequence. One way to get uniqueness in QT-resolution for curve-branches is to consider for QTs of type II only the case where $\xi = 0$. This is exactly the case which is missing, when applying QTs of type I. For a more detailed argumentation about this see also [Teitelbaum, 1990].

A modified version of algorithm applyQT2 called applyQT2' is given below.

Function: `applyQT2'`
In: $f(x,y)$, $e(x,y) \in k(\alpha)[x,y]$.
Out: Apply QTs of type II only for neigboringpoints with coordinates $(0,0)$. This way one gets a one-to-one correspondence between QT-resolution sequences and curve-branches.

```
applyQT2'(f, e, α)
begin
   res := [ ]
   d := ν_0(f)

   f' := y^{-d} f(xy, y)
   e' := y^d e(xy, y)
   if 0 root of f'(x, 0) then
      res' := resolveQT(f', e', α)
      for r in res' do
         res := append(res, [['II', d, 0], r])
      od
   fi

   return res
end
```

A.2. **Resolution by Puiseux-series Expansion.** An algorithm for computing a system of rational Puiseux-series is described in [Duval, 1989] as algorithm `newton`.

Function: `resolvePE`
In: $f(x,y) \in k[x,y]$.
Out: A system $\Delta = \{\delta_1, \ldots, \delta_J\}$ of rational Puiseux series over k together with their coefficient fields k^{δ_j}.

```
resolvePE(f)
begin
   return newton('rational', f, 0)
end
```

References

[Abhyankar, 1983] Abhyankar, S. S. (1983). Desingularization of plane curves. In *American Mathematical Society Proceedings of Symposia in Pure Mathematics*, volume 40, Part 1, pages 1–45.

[Abhyankar, 1990] Abhyankar, S. S. (1990). *Algebraic Geometry for Scientists and Engineers*. American Mathematical Society.

[Brieskorn and Knörrer, 1986] Brieskorn, E. and Knörrer, H. (1986). *Plane Algebraic Curves*. Birkhäuser.

[Duval, 1989] Duval, D. (1989). Rational puiseux expansion. *Compositio Math.*, 70:119–154.

[Newton, 1660] Newton, I. (1660). *Geometria Analitica.*

[Stadelmeyer, 2000] Stadelmeyer, P. (2000). Computing the system of adjoint plane curves by puiseux expansion, part ii: Algorithm. Technical Report 00-04, RISC – Linz, Johannes Kepler Universität, 4040 Linz, Austria, Europe.

[Stadelmeyer and Winkler, 1997] Stadelmeyer, P. and Winkler, F. (1997). Computing the system of adjoint plane curves by puiseux expansion. Technical Report 97-38, RISC – Linz, Johannes Kepler Universität, 4040 Linz, Austria, Europe.

[Teitelbaum, 1990] Teitelbaum, J. (1990). The computational complexity of the resolution of plane curve singularities. *Mathematics of Computation*, pages 797–837.

[Walker, 1978] Walker, R. J. (1978). *Algebraic curves.* Springer.

[Winkler, 1996] Winkler, F. (1996). *Polynomial Algorithms in Computer Algebra.* Springer.