Johann Radon Institute for
Computational and Applied Mathematics
Austrian Academy of Sciences (ÖAW)

RICAM
JOHANN·RADON·INSTITUTE
FOR COMPUTATIONAL AND APPLIED MATHEMATICS

Formal Desingularization of Surfaces – The Jung Method Revisited –

T. Beck

FORMAL DESINGULARIZATION OF SURFACES
– THE JUNG METHOD REVISITED –

TOBIAS BECK

ABSTRACT. In this paper we propose the concept of *formal desingularizations* as a substitute for the resolution of algebraic varieties. Though a usual resolution of algebraic varieties provides more information on the structure of singularities there is evidence that the weaker concept is enough for many computational purposes. We give a detailed study of the Jung method and show how it facilitates an efficient computation of formal desingularizations for projective surfaces over a field of characteristic zero, not necessarily algebraically closed. The paper includes a generalization of Duval's Theorem on rational Puiseux parametrizations to the multivariate case and a detailed description of a system for multivariate algebraic power series computations.

CONTENTS

1. INTRODUCTION

Smooth varieties are (in general) well-understood. By contrast (or simply because of that) the objects of interest are often singular varieties. From the theoretical point of view, a remedy for this situation is the celebrated Theorem of Hironaka [20] (or [19] for a more modern treatment) on the resolution of singularities which is ubiquitous in algebraic geometry: If X is a variety over a field of characteristic

zero, then there always exists a smooth variety Y and a proper birational morphism $\pi : Y \to X$. So for proving theorems and defining birational invariants, one can often argue on Y rather than on X and finally transfer the result back to the singular variety. This theorem has been made constructive by Villamayor [37], Bierstone-Milman [5] and others. There are also two implementations of the desingularization algorithm in `Singular` [16], one by Bodnár and Schicho [6] and another one by Frübis-Krüger [14]. In principal this makes many theoretical results algorithmic, but any algorithm relying on a desingularization suffers from the high computational complexity of the desingularization process. There are also specialized constructive methods for the surface case (for a list see [9] and [24, Chp. 2]), in particular, the Method of Jung which originates in [22] and has been further developed in [38] and [21]. But – to the best of our knowledge – there are no implementations available.

From the computational point of view, it is not always necessary to describe a desingularization completely. In the case of algebraic curves over a field $\mathbb{E}$, series expansions have proven to be an important algorithmic tool. Here the preimage of the singular locus w.r.t. a desingularization is a finite set of points. The idea is to describe the desingularization by power series expansions that determine "formal neighborhoods" of these points. If $\mathbb{E}$ has characteristic zero, Puiseux expansions can be used, and the Newton-Puiseux algorithm is implemented in many computer algebra systems including `Magma` [7], `Maple` and `Singular`. The latter system also has an implementation of Hamburger-Noether expansions [8] that provides a similar tool for positive characteristic. Applications are for example the computation of an integral basis of the function field [36] or Riemann-Roch spaces of divisors [17].

The purpose of this paper is to provide a similar tool for hypersurfaces of $\mathbb{P}^3_{\mathbb{E}}$, where $\mathbb{E}$ is a field of characteristic zero. We emphasize algorithmic aspects and proceed as follows: In Section 2 we define formal desingularizations for schemes of arbitrary dimension. They can be interpreted as sufficiently large sets of local parametrizations by formal maps. Formal desingularization offer a lot of flexibility because during computation one can always to switch to formally isomorphic schemes. Then in Section 3 we show how to compute them for surfaces using the method of Jung that depends crucially on the Theorem of Jung-Abhyankar. We define and use rational Puiseux parametrizations whose existence and computability we assume for that moment. We also give a description of the algorithm in mathematical pseudo-code. Finally Section 4 shows in detail how to implement a system that represents and computes with multivariate algebraic power series in `Magma`. (Locally smooth systems, as proposed in [1], were insufficient from the complexity point of view.) Folklore knew that the concept of rational Puiseux parametrizations introduced by Duval [12] should be extensible to multivariate quasi-ordinary polynomials. We give a new and more elementary proof of that fact and show how to compute parametrizations using our representation. We end with an open problem and an outlook in Section 5. In a short appendix we collect results from local commutative algebra for reference.

Before we proceed we recall and fix some notions. Let $\mathbb{E}$ be a field of characteristic zero and X and Y *integral* $\mathbb{E}$-*schemes*. By $\mathbb{E}(X)$ and $\mathbb{E}(Y)$ we denote the respective function fields. A *rational map* $\pi : Y \dashrightarrow X$ is given by a tuple (V, π) s.t. $V \subseteq Y$ is open and $\pi : V \to X$ is a regular morphism. Note that we do not restrict to schemes of finite type here. In particular all regular morphisms are rational maps. Two tuples (V_1, π_1) and (V_2, π_2) are *equivalent*, or define the same rational map, if $\pi_1|_{V_1 \cap V_2} = \pi_2|_{V_1 \cap V_2}$.

Assume that two maps send the generic point of Y to $p \in X$ (its image is always defined for rational maps). Then (V_1, π_1) and (V_2, π_2) are equivalent iff the induced

inclusions of fields $\mathcal{O}_{X,p}/\mathfrak{m}_{X,p} \hookrightarrow \mathbb{E}(Y)$ are the same (where $\mathfrak{m}_{X,p} \subset \mathcal{O}_{X,p}$ is the maximal ideal). In particular if π is *dense*, *i.e.*, p is the generic point of X, we get an inclusion $\mathbb{E}(X) \hookrightarrow \mathbb{E}(Y)$ determining π.

Note, however, that not all such field inclusions yield rational maps under our assumption since we have not yet restricted to schemes of finite type over $\mathbb{E}$. *E.g.*, let $X := \operatorname{Spec} \mathbb{E}[x]$, $Y := \operatorname{Spec} \mathbb{E}[x]_{\langle x \rangle}$ and $\pi : Y \to X$ be the morphism induced by localization. Then π induces an isomorphism of function fields $\mathbb{E}(X) \cong \mathbb{E}(Y)$. Nevertheless π has no rational inverse. A rational map with inverse is called *birational* (or also a *birational transformation*).

Further it is easy to see that dense rational maps may be composed. A rational map has a *domain of definition*, which is the maximal open set on which it can be defined (equivalently, the union of all such open sets).

2. Formal Desingularizations

For this section we denote by X and Y *separated, integral schemes of finite type over* $\mathbb{E}$. Further we assume that both are of *dimension n*. All (rational) maps will be relative over $\mathbb{E}$.

Let $(A, \mathfrak{m})$ be a valuation ring of $\mathbb{E}(X)$ over $\mathbb{E}$ (where $\mathfrak{m}$ is the maximal ideal). If A is discrete of rank 1 and the transcendence degree of $A/\mathfrak{m}$ over $\mathbb{E}$ is $n - 1$ then it is called a *divisorial valuation ring of* $\mathbb{E}(X)$ *over* $\mathbb{E}$ or a *prime divisor of* $\mathbb{E}(X)$ (see, *e.g.*, [33, Def. 2.6]). It is an *essentially finite*, regular, local $\mathbb{E}$-algebra of Krull-dimension 1 (*i.e.*, the localization of a finitely generated $\mathbb{E}$-algebra at a prime ideal, see [40, Thm. VI.14.31]).

Let $(A, \mathfrak{m})$ be a divisorial valuation ring of $\mathbb{E}(X)$ over $\mathbb{E}$. By [18, Lem. II.4.4.] the inclusion $A \subset \mathbb{E}(X)$ defines a unique morphism $\operatorname{Spec} \operatorname{QF}(A) \to X$ and therefore a rational map $\operatorname{Spec} A \dashrightarrow X$ sending generic point to generic point. Composing this with the morphism obtained by the $\mathfrak{m}$-adic completion $A \to \widehat{A}$ we get a rational map $\operatorname{Spec} \widehat{A} \dashrightarrow X$.

Definition 2.1 (Formal Prime Divisor)**.** Let $(A, \mathfrak{m})$ be a divisorial valuation ring of $\mathbb{E}(X)$ over $\mathbb{E}$. Assume that the rational map $\operatorname{Spec} \widehat{A} \dashrightarrow X$ (as above) is actually a *morphism* $\varphi : \operatorname{Spec} \widehat{A} \to X$ (*i.e.*, defined also at the closed point). Then φ is a representative for a class of schemes up to X-isomorphism. This class (and, by abuse of notation, any representative) will be called a *formal prime divisor* on X.

Hence we may compose a representative φ with an isomorphism $\operatorname{Spec} B \to \operatorname{Spec} \widehat{A}$ to get another representative for the same formal prime divisor. We have an isomorphism $\widehat{A} \cong \mathbb{F}_\varphi[\![t]\!]$ with $\mathbb{F}_\varphi := \widehat{A}/\mathfrak{m}\widehat{A} \cong A/\mathfrak{m}$. In the sequel we will sometimes assume that $\widehat{A}$ is already of this form, *i.e.*, $\varphi : \operatorname{Spec} \mathbb{F}_\varphi[\![t]\!] \to X$. The isomorphism is an instance of *Cohen's Structure Theorem* for regular rings, see Theorem A.1.

Formal prime divisors provide an algorithmic way for dealing with divisorial valuations; A formal prime divisor yields an inclusion of function fields $\mathbb{E}(X) \hookrightarrow \mathbb{F}_\varphi(\!(t)\!)$. Vice versa, by what was said above, φ is determined by this inclusion. So it is this piece of information one has to represent. Composing this inclusion with the order function $\operatorname{ord}_t : \mathbb{F}_\varphi(\!(t)\!) \to \mathbb{Z}$ we get the corresponding divisorial valuation.

We want to single out a special class of formal prime divisors.

Definition 2.2 (Realized Formal Prime Divisors)**.** Let $p \in X$ be a regular point of codimension 1. The formal prime divisor

$$\operatorname{Spec} \widehat{\mathcal{O}_{X,p}} \to X$$

(given by composing the canonic morphism $\operatorname{Spec} \mathcal{O}_{X,p} \to X$ with the morphism induced by the completion $\mathcal{O}_{X,p} \to \widehat{\mathcal{O}_{X,p}}$) is called *realized*.

If X is *normal* then all generic points of closed subsets of codimension 1 are necessarily regular [18, Thm II.8.22A]. Therefore there is a one-one correspondence of realized formal prime divisors and prime Weil divisors. Another important fact is that we can compare formal prime divisors of birationally equivalent schemes under certain conditions.

Lemma 2.3 (Pullback of Formal Prime Divisors)**.** *Let X and Y be S-schemes with structure morphisms $\rho_X : X \to S$, $\rho_Y : Y \to S$ and assume that ρ_Y is proper. Let $\pi : Y \dashrightarrow X$ be a birational transformation of S-schemes (meaning that $\rho_Y = \rho_X \pi$ as rational maps).*

Then each formal prime divisor $\varphi : \operatorname{Spec} \widehat{A} \to X$ lifts uniquely to a formal prime divisor on Y, i.e., there is a unique formal prime divisor $\pi^* \varphi : \operatorname{Spec} \widehat{A} \to Y$ s.t. $\pi(\pi^* \varphi) = \varphi$ as rational maps.

Proof. Consider the commuting diagram

$$
\begin{array}{ccccc}
\operatorname{Spec} \operatorname{QF}(\widehat{A}) & \longrightarrow & \operatorname{Spec} \mathbb{E}(X) & \longrightarrow & \operatorname{Spec} \mathbb{E}(Y) \\
\downarrow & & \downarrow & & \downarrow \\
\operatorname{Spec} \widehat{A} & \xrightarrow{\varphi} & X & \dashrightarrow{\pi^{-1}} & Y \\
& & {\scriptstyle \rho_X} \searrow & & \swarrow {\scriptstyle \rho_Y} \\
& & & S &
\end{array}
$$

where the vertical arrows are given by restricting identity maps to the germs at the generic points and the upper arrows are induced by φ and π^{-1} respectively. The two squares trivially commute and the triangle commutes because π was assumed to be a birational transformation of S-schemes.

Now assume that a lift $\pi^* \varphi$ as in the claim exists, then we must have $\pi^* \varphi = \pi^{-1} \varphi$ because π is birational. This (a priori only *rational*) map would fit into the following contracted diagram:

$$
\begin{array}{ccc}
\operatorname{Spec} \operatorname{QF}(\widehat{A}) & \longrightarrow & Y \\
\downarrow & {\scriptstyle \pi^* \varphi} \nearrow & \downarrow {\scriptstyle \rho_Y} \\
\operatorname{Spec} \widehat{A} & \xrightarrow{\rho_X \varphi} & S
\end{array}
$$

Now there exists a unique *regular* morphism $\psi : \operatorname{Spec} \widehat{A} \to Y$ which fits into this diagram by applying the valuative criterion of properness to ρ_Y (see [18, Thm. II.4.7]). Since a rational map is uniquely determined by the inclusion of function fields we see that $\pi^* \varphi = \psi$. $\square$

Corollary 2.4 (Pullback along Proper Morphisms)**.** *Let $\pi : Y \to X$ be a proper, birational morphism. A formal prime divisor on X lifts to a unique formal prime divisor on Y. Vice versa a formal prime divisor on Y extends to a unique formal prime divisor on X, hence π^* is a bijection.*

Proof. This is obtained by applying Lemma 2.3 to π and π^{-1} where $S := X$. $\square$

We will apply the operator π^* also to sets of formal prime divisors.

Definition 2.5 (Center and Support)**.** Let $\varphi : \operatorname{Spec} \widehat{A} \to X$ be a formal prime divisor. We define its *center*, in symbols $\operatorname{center}(\varphi)$, to be the image of the closed point. Further the *support* of a *finite* set of formal prime divisors $\mathcal{S}$ is defined as $\operatorname{supp}_X(\mathcal{S}) := \overline{\{\operatorname{center}(\varphi) \mid \varphi \in \mathcal{S}\}}$, i.e., the closure of the set of all centers.

Example 2.6. Let $X := \operatorname{Spec} A$ with $A := \mathbb{Q}[x, y, z]/\langle x^2 + y^2 - z^2 \rangle$ be the cone over the circle and $Y := \operatorname{Spec} B$ with $B := \mathbb{Q}[x', y', z']/\langle x'^2 + y'^2 - 1 \rangle$ the cylinder. The

strict transform π under the blow up of the origin has an affine chart $Y \to X$ given by the homomorphism $A \to B : x \mapsto x'z', y \mapsto y'z', z \mapsto z'$. The generic point of the exceptional divisor in Y is the prime ideal $\langle z' \rangle$. In this case we have a trivial isomorphism $\widehat{B_{\langle z' \rangle}} \cong \mathrm{QF}(\mathbb{Q}[x', y']/\langle x'^2 + y'^2 - 1 \rangle)[\![z']\!]$. Then a formal prime divisor is induced by the homomorphism

$$A \to \mathrm{QF}(\mathbb{Q}[x', y']/\langle x'^2 + y'^2 - 1 \rangle)[\![z']\!] : x \mapsto x'z', y \mapsto y'z', z \mapsto z'.$$

We can compose this homomorphism with an arbitrary isomorphism of rings to get another representative of the same formal prime divisor. *E.g.*, since the circle is a rational curve we can change the coefficient field by $\mathrm{QF}(\mathbb{Q}[x', y']/\langle x'^2 + y'^2 - 1 \rangle) \to \mathbb{Q}(s) : x' \mapsto \frac{2s}{1+s^2}, y' \mapsto \frac{-1+s^2}{1+s^2}$ and map, say, $z' \mapsto t + t^2 + \dots$. Now a formal prime divisor $\varphi : \mathrm{Spec}\, \mathbb{Q}(s)[\![t]\!] \to X$ is induced by

$$A \to \mathbb{Q}(s)[\![t]\!] : x \mapsto \frac{2s(t + t^2 + \dots)}{1+s^2}, y \mapsto \frac{(-1+s^2)(t+t^2+\dots)}{1+s^2}, z \mapsto t + t^2 + \dots.$$

One finds $\mathrm{center}_X(\varphi) = \langle x, y, z \rangle$ (which is the preimage of the prime ideal $\langle t \rangle$) and by construction we know that $\pi^*\varphi$ is realized with center $\langle z' \rangle$ in Y.

Now we are in the situation to define formal desingularizations.

Definition 2.7 (Formal Description of a Desingularization). Let $\pi : Y \to X$ be a *desingularization*, *i.e.*, π is proper, birational and Y is regular. Let $\mathcal{S}$ be a *finite* set of formal prime divisors on X. We say that $\mathcal{S}$ is a *formal description* of π iff

(1) all divisors in $\pi^*\mathcal{S}$ are realized,
(2) $\pi^{-1}(\mathrm{supp}_X(\mathcal{S})) = \mathrm{supp}_Y(\pi^*\mathcal{S})$ and
(3) the induced morphism $Y \setminus \mathrm{supp}_Y(\pi^*\mathcal{S}) \to X \setminus \mathrm{supp}_X(\mathcal{S})$ is an isomorphism.

The set $\mathcal{S}$ itself consists of formal prime divisors on X and makes no reference to the morphism π. By another definition we can *avoid* mentioning an *explicit* π.

Definition 2.8 (Formal Desingularization). Let $\mathcal{S}$ be a finite set of formal prime divisors on X. Then $\mathcal{S}$ is called a *formal desingularization* of X iff there *exists some* desingularization π s.t. $\mathcal{S}$ is a formal description of it.

Informally speaking the set $\mathcal{S}$ makes it possible to treat divisors on Y effectively, although we haven't explicitly represented Y as a whole; Indeed, realized formal prime divisors correspond bijectively to usual prime divisors on the regular scheme Y. The set of formal prime divisors now divides into two classes: those within $\pi^*\mathcal{S}$ and those with center in $Y \setminus \mathrm{supp}_Y(\pi^*\mathcal{S})$. The latter can be dealt with on the isomorphic scheme $X \setminus \mathrm{supp}_X(\mathcal{S})$. Therefore formal descriptions are an appropriate algorithmic tool to work with invertible sheaves on Y.

In the case of surfaces it is easy to see that the existentially quantified π in the above definition is actually unique up to isomorphism. Therefore $\mathcal{S}$ really identifies a desingularization in the common sense. Vice versa, every desingularization can be described formally by completing the stalks along the exceptional divisors.

Theorem 2.9 (Uniqueness of Surface Desingularization). *Let $\mathcal{S}$ be a formal desingularization of X. If $\pi_1 : Y_1 \to X$ and $\pi_2 : Y_2 \to X$ are two desingularizations described by $\mathcal{S}$ (in the sense of Definition 2.7) then Y_1 and Y_2 are isomorphic as X-schemes.*

Proof. Let $b^{(0)} : X^{(0)} \to X$ be a minimal desingularization (see [26, Cor. 27.3]) of X and let $\mathcal{S}^{(0)}$ be obtained from $(b^{(0)})^*\mathcal{S}$ by subtracting all realized formal prime divisors. Then π_1 and π_2 factor through $X^{(0)}$ yielding a commuting diagram

$$Y_1 \dashrightarrow^{\left(\pi_2^{(0)}\right)^{-1}\pi_1^{(0)}} Y_2$$

$$\pi_1^{(0)} \searrow \qquad \swarrow \pi_2^{(0)}$$

$$X^{(0)}$$

and $\pi_1^{(0)}$ and $\pi_2^{(0)}$ are both described by $\mathcal{S}^{(0)}$.

Moreover these maps are proper, birational morphisms between regular surfaces, so they factor into a finite sequence of point blow ups (see [18, Cor. V.5.4] which holds also for the case of a non-closed ground field). The set of possible centers for the first blow up is exactly $\mathrm{supp}_{X^{(0)}}(\mathcal{S}^{(0)})$. Choose a center, compute the blow up $b^{(1)} : X^{(1)} \to X^{(0)}$ and set $\mathcal{S}^{(1)}$ to be the set $(b^{(1)})^*\mathcal{S}^{(0)}$ excluding the unique formal prime divisor that is turned realized and centered along the exceptional divisor. Again $\pi_1^{(0)}$ and $\pi_2^{(0)}$ factor through morphisms $\pi_1^{(1)} : Y_1 \to X^{(1)}$ and $\pi_2^{(1)} : Y_2 \to X^{(1)}$ described by $\mathcal{S}^{(1)}$. Going on like this and setting $l := \#\mathcal{S}^{(0)}$, we find that $\pi_1^{(l)}$ and $\pi_2^{(l)}$ are described by $\mathcal{S}^{(l)} = \emptyset$ and hence are isomorphisms by Definition 2.7. □

It is not so clear whether a similar statement holds in higher dimensions when minimal resolutions are not available.

Remark 2.10 (Formal Desingularization of Reduced Schemes). The above definitions can and will be used in a more general setting. Namely, if $X = \bigcup_i X_i$ is the decomposition of a *reduced, equidimensional* (no longer integral) scheme into irreducible closed subschemes then any morphism $\mathrm{Spec}\,\mathbb{F}[\![t]\!] \to X$ is actually a morphism to one of the X_i. We call it a formal prime divisor if the corresponding $\mathrm{Spec}\,\mathbb{F}[\![t]\!] \to X_i$ is a formal prime divisor. We call it again realized iff it corresponds to the completion at the germ of a regular codimension 1 point in X (not in X_i!). Lemma 2.3 and Corollary 2.4 remain valid in this setting (where a birational morphism between two reduced schemes is a morphism that induces birational morphisms on all irreducible components). The definitions of center, support and formal desingularization carry over straight forward.

3. The Method of Jung Revisited

In this section we describe the desingularization of surfaces after Jung.

3.1. **Theory of the Method.** First we will view a projective surface as a certain covering of a smooth surface. Then we modify the covering such that after passing to the integral closure the remaining singularities are very simple and can be resolved by point blow ups.

3.1.1. *Projective Surfaces as Ramified Coverings of the Plane.* Consider a projective hypersurface $X \subseteq \mathbb{P}_{\mathbb{E}}^3$. We want to view X in a slightly different way. Let $p_0 \in \mathbb{P}_{\mathbb{E}}^3 \setminus X$ be a closed *rational* point (*i.e.*, its residue field is isomorphic to $\mathbb{E}$) and $\pi : W \to V$ the linear projection from p_0 where $W := \mathbb{P}_{\mathbb{E}}^3 \setminus p_0$ and $V := \mathbb{P}_{\mathbb{E}}^2$. This projection defines a line bundle. Its restriction $\pi\mid_X : X \to V$ is a Noether normalization of X, *i.e.*, a *finite morphism* onto the projective plane. We subsume the governing properties in the following definition:

Definition 3.1 (Ramified Coverings). Let $\pi : W \to V$ be a *line bundle* s.t. V is a *regular, integral* surface over $\mathbb{E}$. Further let $X \subset W$ be a *reduced hypersurface* s.t. $\pi|_X : X \to V$ is *finite*. The tuple (π, X) is then called a *ramified covering*.

That is our notion of ramified covering comprises that we are dealing with surfaces and that the covering surface is embedded in a line bundle over the base. Now
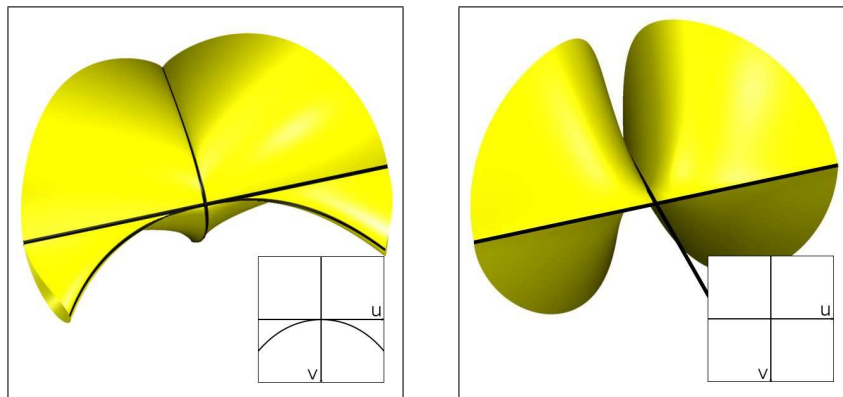
FIGURE 1. Embedded Desingularization of the Discriminant

The left side shows the local picture of the example surface X together with its discriminant curve. On the right we depict a chart X_0 obtained from the embedded desingularization of the discriminant curve.

we want to define the ramification locus of such a covering, *i.e.*, the locus where the covering $\pi|_X$ is "not locally trivial" (more precisely, not étale). Since π is a line bundle and $\pi|_X$ is finite, we can find a covering $\{U_i\}_i$ of V by affine open subsets s.t. $\mathcal{O}_W(\pi^{-1}(U_i)) \cong \mathcal{O}_V(U_i)[z]$ is a polynomial ring in one variable and X is given by a monic, squarefree polynomial $f_i \in \mathcal{O}_V(U_i)[z]$.

Definition 3.2 (Discriminant Curve). Let $(\pi : W \to V, X)$ be a ramified covering. Let $\{U_i\}_i$ be a covering of V as above and $f_i \in \mathcal{O}_V(U_i)[z]$ a set of polynomials defining X. The ideals $\langle \mathrm{disc}_z(f_i) \rangle \subseteq \mathcal{O}_V(U_i)$ define an invertible sheaf of ideals and the corresponding subscheme is called the *discriminant curve* $D_{\pi|_X} \subseteq V$.

The discriminant curve is actually a concept independent of the concrete covering and embedding of X into W. It depends only on $\pi|_X$. Further the covering is locally trivial except over $D_{\pi|_X}$.

Example 3.3. Consider the surface $X \subset \mathbb{P}^3_{\mathbb{Q}}$ given by $F = 0$ with $F := x_0^6 + 3x_0^4 x_2 x_3 + x_0^3 x_1^2 x_2 + 3x_0^2 x_2^2 x_3^2 + x_2^3 x_3^3 \in \mathbb{Q}[x_0, x_1, x_2, x_3]$. Since F is monic in x_0 the surface X doesn't contain the point $p := (1 : 0 : 0 : 0)$. The line bundle defined by the projection of $X \setminus \{p\}$ to the plane $x_0 = 0$ is given by dehomogenizing with respect to x_1, x_2 and x_3.

In the last chart, the defining equation has the form $f := w^6 + 3vw^4 + u^2 vw^3 + 3v^2 w^2 + v^3 \in \mathbb{Q}[u, v][w]$ where we have mapped $x_0 \mapsto w$, $x_1 \mapsto u$, $x_2 \mapsto v$ and $x_3 \mapsto 1$. We have the local discriminant $\mathrm{disc}_w(f) = 729u^8 v^{12}(u^4 - 64v)$. Figure 1 left displays the surface.

3.1.2. *Embedded Desingularization of the Discriminant Curve.* We would like to give a more detailed study of the covering, but for general ramified coverings (π, X) this is hard. The complexity of X resp. of the covering map is partially reflected in the discriminant curve $D_{\pi|_X}$. Recall that a closed point p is called *normal crossing* for the embedded curve $D_{\pi|_X} \subseteq V$ if the curve is locally defined by $d_x^{e_x} d_y^{e_y} u \in \mathcal{O}_{V,p}$ where u is a unit, $\{d_x, d_y\}$ is a local system of parameters and $e_x, e_y \geq 0$. The whole curve is called normal crossing if it is normal crossing at every closed point.

Definition 3.4 (Nicely Ramified Coverings). Let (π, X) be a ramified covering. If $D_{\pi|_X}$ is normal crossing then we call (π, X) *nicely ramified*.

We can always modify a ramified covering to become nicely ramified. If we speak of *normal crossing singularities* of the discriminant curve of a nicely ramified covering, we mean the closed points where two components intersect.

Lemma 3.5 (Simplification of Coverings). *Let $(\pi : W \to V, X)$ be a ramified covering. There is a* proper, *birational morphism $\rho : V' \to V$ s.t. the ramified covering $(\pi' : W' \to V', X')$ is* nicely ramified *(where $W' := W \times_V V'$ and $X' := X \times_W W'$). Further ρ is given by a finite succession of blow ups in closed points.*

Proof. The theorem on embedded desingularization of curves (see [24, Thm. 1.47]) shows the existence of the morphism ρ; Indeed it says that after a finite number of blow ups in the singular points of the reduced curve the pullback of $D_{\pi|_X}$ is normal crossing. For showing the lemma it remains to prove that constructing the discriminant curve commutes with base extension. This is left to the reader. $\quad\square$

Example 3.3 (continued). The curve defined by $\mathrm{disc}_w(f)$ has a complicated singularity at the origin which needs to be resolved. One of the chart maps is given by $u \mapsto uv$, $v \mapsto u^2v^3$ and transforms $\mathrm{disc}_w(f)$ to $729u^{34}v^{47}(u^2v - 64)$ which describes a curve with a normal crossing intersection at the origin.

The embedded desingularization of the discriminant curve can be applied to the surface X (by mapping $w \mapsto w$) to obtain a surface with chart X_0. We obtain the new local equation $f_0 = w^6 + 3u^2v^3w^4 + u^4v^5w^3 + 3u^4v^6w^2 + u^6v^9$ with $\mathrm{disc}_w(f_0) = 729u^{34}v^{47}(u^2v - 64)$, see Figure 1 right.

3.1.3. *Desingularization of Toroidal Surface Singularities.* The structure of nicely ramified coverings depends crucially on the celebrated Theorem of Jung-Abhyankar (see Theorem A.5). A polynomial fulfilling the conditions of the theorem is called *quasi-ordinary.* In its original form the theorem is not precise enough for our purposes, for example, because the statement doesn't involve the coefficient fields of the power series solutions. In the sequel $\mathbb{E}[\![\underline{x}^\Gamma]\!]$ will denote the ring of power series with coefficients in a field $\mathbb{E}$, variables $x_1, \ldots, x_n$ and exponents in $\Gamma \cap \mathbb{R}^n_{\geq 0}$ (the non-negative orthant of a full rational lattice). We need the concept of rational parametrizations (for a refined version see Definition 4.9):

Definition 3.6 (Parametrizations). *Let $f \in \mathbb{E}[\![x_1, \ldots, x_n]\!][z]$ be quasi-ordinary. I.e., f is monic, squarefree and s.t. $\mathrm{disc}_z(f) = x_1^{e_1} \cdots x_n^{e_n} u(\underline{x})$ where $u(0, \ldots, 0) \neq 0$.*

We call (σ, α) with $\sigma \in \mathrm{Aut}(\mathbb{E}'[\![x_1, \ldots, x_n]\!] \mid \mathbb{E}')$ and $\alpha \in \mathbb{E}'[\![\underline{x}^\Gamma]\!]$ a *parametrization* of f if $\mathbb{E} \subseteq \mathbb{E}'$, $\mathbb{Z}^n \subseteq \Gamma$ and $\sigma^{\uparrow z}(f)(\alpha) = 0$. Let $g|f$ be an irreducible factor s.t. $\sigma^{\uparrow z}(g)(\alpha) = 0$. We call (σ, α) *rational* if the induced homomorphism $\mathrm{IC}(\mathbb{E}[\![x_1, \ldots, x_n]\!][z]/\langle g \rangle) \to \mathbb{E}'[\![\underline{x}^\Gamma]\!]$ which maps $z \mapsto \alpha$ and $\gamma \mapsto \sigma(\gamma)$ for $\gamma \in \mathbb{E}[\![x_1, \ldots, x_n]\!]$ is an isomorphism. A set of rational parametrizations for f is called *complete* if it is in bijective correspondence with the irreducible factors of f.

Here we used $\sigma^{\uparrow z}$ for the lifting of the automorphism to the polynomial ring by coefficient-wise application. We will show later, that we can actually compute such rational parametrizations.

Theorem 3.7 (Existence of Rational Parametrizations). *Let $f \in \mathbb{E}[\![x_1, \ldots, x_n]\!][z]$ be a quasi-ordinary polynomial. Then a complete set of rational parametrizations of f exists and can be computed. Moreover, if actually $\mathrm{disc}_z(f) = x_1^{e_1} \cdots x_m^{e_m} u(\underline{x})$ where $m \leq n$ and $u(0, \ldots, 0) \neq 0$ then the exponent lattices of the power series rings will be of the form $\Gamma \times \mathbb{Z}^{n-m}$ for some m-dimensional rational lattice Γ.*

Proof. For the first statement see Algorithm 11 and Corollary 4.15 of Section 4.1. In Lemma 4.14 the relation between the computed parametrizations and the fractionary power series roots of f is explored. Together with Theorem A.5 this gives the statement about the exponent lattice. $\quad\square$

Example 3.3 (continued). The transformed polynomial $f_0 \in \mathbb{Q}[u, v][w]$ is quasi-ordinary. In this case a complete set of rational parametrizations is given by only

a single parametrization (σ, α) with $\sigma : \mathbb{Q}[\![u, v]\!] \to \mathbb{Q}[\![u, v]\!] : u \mapsto -8u, v \mapsto -v$ and

$$\alpha := -8u^{\frac{6}{6}} v^{\frac{9}{6}} + 8u^{\frac{8}{6}} v^{\frac{10}{6}} - 4u^{\frac{10}{6}} v^{\frac{11}{6}} + u^{\frac{14}{6}} v^{\frac{13}{6}} - \frac{1}{2} u^{\frac{18}{6}} v^{\frac{15}{6}} + \frac{5}{16} u^{\frac{22}{6}} v^{\frac{17}{6}} - \frac{7}{32} u^{\frac{26}{6}} v^{\frac{19}{6}} + \dots$$

We will see later that the simple form of σ is no coincidence. We further have $\alpha \in \mathbb{Q}[\![(u, v)^\Gamma]\!]$ with $\Gamma := \mathbb{Z}(0, \frac{1}{2}) + \mathbb{Z}(\frac{1}{3}, \frac{1}{6})$. This lattice is shown in Figure 2 below.

Complete sets of rational parametrizations describe very explicitly the structure of the integral closure of $\mathbb{E}[\![x_1, \dots, x_n]\!][z]/\langle f \rangle$.

Lemma 3.8 (Decomposition Induced by Rational Parametrizations). *Let $f \in \mathbb{E}[\![x_1, \dots, x_n]\!][z]$ be a quasi-ordinary polynomial and $\mathcal{P} = \{(\sigma_i, \alpha_i)\}_i$ with $(\sigma_i, \alpha_i) \in \mathrm{Aut}(\mathbb{E}_i[\![x_1, \dots, x_n]\!] \mid \mathbb{E}_i) \times \mathbb{E}_i[\![\underline{x}^{\Gamma_i}]\!]$ a complete set of rational parametrizations of f. Then the homomorphisms*

$$\psi_i : \mathbb{E}[\![x_1, \dots, x_n]\!][z]/\langle f \rangle \to \mathbb{E}_i[\![\underline{x}^{\Gamma_i}]\!] : \gamma \mapsto \sigma_i(\gamma) \text{ for } \gamma \in \mathbb{E}[\![x_1, \dots, x_n]\!] \text{ and } z \mapsto \alpha_i$$

can be composed to a homomorphism

$$\psi : \mathbb{E}[\![x_1, \dots, x_n]\!][z]/\langle f \rangle \to \prod_i \mathbb{E}_i[\![\underline{x}^{\Gamma_i}]\!] : a \mapsto (\dots, \psi_i(a), \dots)$$

which lifts to an isomorphism $\psi : \mathrm{IC}(\mathbb{E}[\![x_1, \dots, x_n]\!][z]/\langle f \rangle) \to \prod_i \mathbb{E}_i[\![\underline{x}^{\Gamma_i}]\!]$.

Sketch of Proof. By the definition of rational parametrizations it is enough to show

$$\mathrm{IC}(\mathbb{E}[\![x_1, \dots, x_n]\!][z]/\langle f \rangle) \cong \prod_i \mathrm{IC}(\mathbb{E}[\![x_1, \dots, x_n]\!][z]/\langle f_i \rangle)$$

where the righthand side runs over all irreducible factors f_i of f. By [13, Exer. 2.26] this can be shown using orthogonal idempotents. More precisely, if $f = h_1 h_2$ where h_1 and h_2 are factors without common divisor then set $e_1 := h_2/(h_1 + h_2)$ and $e_2 := h_1/(h_1 + h_2)$ to be elements in $\mathrm{QF}(\mathbb{E}[\![x_1, \dots, x_n]\!][z]/\langle f \rangle)$. (For this one checks that the denominators are no zero-divisors.) Then one easily computes $e_1 + e_2 = 1$, $e_1 e_2 = 0$ and $e_i = e_i(e_1 + e_2) = e_i^2 + e_1 e_2 = e_i^2$. The idempotency relations imply in particular that $e_1, e_2 \in \mathrm{IC}(\mathbb{E}[\![x_1, \dots, x_n]\!][z]/\langle f \rangle)$. So the integral closure splits:

$$\mathrm{IC}(\mathbb{E}[\![x_1, \dots, x_n]\!][z]/\langle f \rangle) \cong e_1 \mathrm{IC}(\mathbb{E}[\![x_1, \dots, x_n]\!][z]/\langle f \rangle) \times e_2 \mathrm{IC}(\mathbb{E}[\![x_1, \dots, x_n]\!][z]/\langle f \rangle)$$

Finally one shows $e_i \mathrm{IC}(\mathbb{E}[\![x_1, \dots, x_n]\!][z]/\langle f \rangle) \cong \mathrm{IC}(\mathbb{E}[\![x_1, \dots, x_n]\!][z]/\langle h_i \rangle)$. $\quad\square$

Corollary 3.9 (Singularities of Ramified Coverings). *Let (π, X) be a ramified covering, $\nu : \widetilde{X} \to X$ the normalization morphism. Then the (isolated) singular points of $\widetilde{X}$ lie over the singularities of the (reduced) discriminant curve. Moreover, over normal crossing singularities the singularities of $\widetilde{X}$ are toroidal.*

Proof. Let $q \in \widetilde{X}$ be a closed point and $p := \pi(\nu(q))$. Assume that p either does not lie at all on $D_{\pi|_X}$, or lies on a regular point of the reduced curve, or is a normal crossing singularity. In each of these cases $D_{\pi|_X}$ can locally be defined by $d_x^{e_x} d_y^{e_y} u \in \mathcal{O}_{V,p}$ where $\{d_x, d_y\}$ is a local system of parameters and $e_x \geq 0$, $e_y \geq 0$. There is an isomorphism between the completion of $\mathcal{O}_{V,p}$ and $\mathbb{F}[\![x, y]\!]$ (where $\mathbb{F}$ is the residue field of $\mathcal{O}_{V,p}$) which maps $d_x \mapsto x$ and $d_y \mapsto y$, see Theorem A.1. We can as well assume that $\widehat{\mathcal{O}_{V,p}} = \mathbb{F}[\![x, y]\!]$, $d_x = x$ and $d_y = y$.

The completion of the fiber of $\pi|_X$ can be defined by the vanishing of a polynomial $f \in \mathbb{F}[\![x, y]\!][z]$ which is quasi-ordinary. Building the integral closure commutes with completion, see Lemma A.3. Then Lemma 3.8 implies that the completion of $\mathcal{O}_{\widetilde{X}, q}$ is isomorphic to a power series ring with fractional exponents. But those are the completions of the distinguished stalks of affine toric surfaces, hence, all such points q can at most be toroidal.

If p does not lie on $D_{\pi|_X}$ then $e_x = e_y = 0$. If it is a regular point of $D_{\pi|_X}$ then, say, $e_x > 0$ and $e_y = 0$. By Theorem 3.7, in both cases, the power series rings in
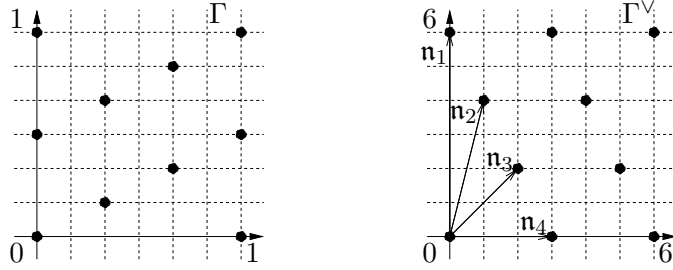
FIGURE 2. Lattice and Dual Lattice

We show the non-negative quadrant of a lattice Γ and its dual $\Gamma^\vee$ (*i.e.*, the set of all linear forms to $\mathbb{Z}$ identified via scalar multiplication of vectors). In the dual we have inscribed an minimal sequence of generators $\mathfrak{n}_1, \ldots, \mathfrak{n}_4$. Indices are chosen s.t. subsequent pairs correspond to neighboring vectors.

the parametrizations have exponent lattices of the form $(\frac{1}{e}\mathbb{Z}) \times \mathbb{Z}$. These rings are regular and by faithful flatness $\mathcal{O}_{\widetilde{X},q}$ must be regular itself. $\square$

Example 3.3 (continued). For our example this means that the integral closure of $\mathbb{Q}[\![u,v]\!][w]/\langle f_0 \rangle$ is isomorphic to $\mathbb{Q}[\![(u,v)^\Gamma]\!]$. This fits well to the picture in Figure 1 that suggests that the surface X_0, though singular, has only a single analytic branch at the origin.

Modifying a ramified covering to become nicely ramified is constructive, since embedded desingularization of curves is. Passing to the normalization of a scheme of finite type over $\mathbb{E}$ is constructive, since computing the integral closure of finitely generated $\mathbb{E}$-algebras is (see, *e.g.*, [11]). By the above corollary we are left with the task of desingularizing normal toroidal surface singularities.

These singularities have first been studied by Jung [22]. As noted in [9, Lect. 2, §2] a normal toric surface can be desingularized by a finite sequence of point blow ups. This property can be transferred to toroidal singularities by Lemma A.4. So we could obtain a desingularization by computing a sequence of point blow ups of the normalization $\widetilde{X}$ and, hence, Jung's method is already constructive.

However, computing normalizations is not cheap. Lemma 3.8 shows that rational parametrizations anyway describe the integral closure. In the following section we will therefore follow a different approach, always with formal desingularizations in mind. We will also benefit in other places from the additional flexibility obtained by applying formal isomorphisms.

The final lemma of this section has its origins in Hirzebruch [21] (see also [25]) who first gave explicit formulas for the desingularization of toric surface singularities using continued fractions. Afterwards the arrival of toric geometry (*cf.* [15]) has introduced new terminology and means of description. Recall that the *dual* $\Gamma^\vee$ of a full lattice $\Gamma \subset \mathbb{Q}^n$ is the set of all linear forms $\mathfrak{n} \in \mathbb{Q}^n$ with $\mathfrak{n}(\mathfrak{m}) \in \mathbb{Z}$ for all $\mathfrak{m} \in \Gamma$.

Lemma 3.10 (Formal Desingularization of Toric Surfaces)**.** *Let* $\operatorname{Spec} \mathbb{E}[\underline{x}^\Gamma]$ *for some rational lattice* $\Gamma \subset \mathbb{Q}^2$ *be a toric surface and* $\mathfrak{n}_1, \ldots, \mathfrak{n}_l \in \Gamma^\vee \cap \mathbb{R}_{\geq 0}^2$ *an ordered and minimal sequence of monoid generators as in Figure 2. Then the set of morphisms* $\psi_i : \operatorname{Spec} \mathbb{E}(s)[\![t]\!] \to \operatorname{Spec} \mathbb{E}[\underline{x}^\Gamma]$ *given by the* $\mathbb{E}$-*algebra homomorphisms*

$$\mathbb{E}[\underline{x}^\Gamma] \to \mathbb{E}(s)[\![t]\!] : \underline{x}^{\mathfrak{m}} \mapsto s^{\mathfrak{n}_i(\mathfrak{m})} t^{\mathfrak{n}_{i+1}(\mathfrak{m})}$$

for $1 \leq i \leq l-2$ *is a formal desingularization of* $\operatorname{Spec} \mathbb{E}[\underline{x}^\Gamma]$.

Proof. Desingularizations of toric schemes can be constructed using special fans in the dual cone and lattice $\Gamma^\vee \cap \mathbb{R}_{\geq 0}^2$ (see, *e.g.*, [15, 10]). Applying this construction to the fan whose one-dimensional faces are given by the $\mathfrak{n}_i$ one obtains a desingularization π. In fact the morphisms $\pi_i : \operatorname{Spec} \mathbb{E}[s,t] \to \operatorname{Spec} \mathbb{E}[\underline{x}^\Gamma]$ given

by $\mathbb{E}[\underline{x}^\Gamma] \to \mathbb{E}[s,t] : \underline{x}^{\mathfrak{m}} \mapsto s^{\mathfrak{n}_i(\mathfrak{m})} t^{\mathfrak{n}_{i+1}(\mathfrak{m})}$ for $1 \le i \le l-1$ are isomorphic to the restriction of π to an open covering by affine charts.

The exceptional locus (*i.e.*, the π-preimage of the isolated singularity) is a finite union of divisors. We get a formal description of π by completing the local rings along these divisors. They are given, for example, by the prime ideals $\langle t \rangle \subset \mathbb{E}[s,t]$ in each of the charts $1, \ldots, l-2$. For the completions of the local rings we then have trivially $\widehat{\mathbb{E}[s,t]_{\langle t \rangle}} \cong \mathbb{E}(s)[\![t]\!]$. $\square$

Remark 3.11 (Minimal Desingularization by Point Blow Ups). The desingularization described by the above set of morphisms is the *minimal* one obtained (up to isomorphism) by subsequently blowing up isolated singular points. To show this one observes that every single such blow up gives (non-affine) toric surfaces that are described by fans in $\Gamma^\vee \cap \mathbb{R}^2_{\ge 0}$. Elementary arguments about the lattice and its dual show that the one-dimensional faces of these lattices are always given by one of the vectors $\mathfrak{n}_i$. On the other hand any fan defined by a proper subset of the generators is associated to a still singular surface.

Example 3.3 (continued). This lemma can be applied as follows. The normalization $\widetilde{X_0}$ of X_0 has an isolated singularity which is formally isomorphic to the distinguished germ of a toric surface with coordinate ring $\mathbb{Q}[(u,v)^\Gamma]$.

The lemma says that this toric surface is formally desingularized by mapping $(u,v)^{\mathfrak{m}} \mapsto s^{\mathfrak{n}_i(\mathfrak{m})} t^{\mathfrak{n}_{i+1}(\mathfrak{m})} \in \mathbb{Q}(s)[\![t]\!]$ for $i \in \{1,2\}$ with $\mathfrak{n}_i$ as in Figure 2. Let's look at this for $i = 1$ in terms of algebra generators $v^{1/2}, u^{1/3}v^{1/6}, u \in \mathbb{Q}[(u,v)^\Gamma]$. We have to map

$$v^{\frac{1}{2}} \mapsto s^{\langle (0,6),(0,1/2) \rangle} t^{\langle (1,4),(0,1/2) \rangle} = s^3 t^2,$$

$$u^{\frac{1}{3}} v^{\frac{1}{6}} \mapsto s^{\langle (0,6),(1/3,1/6) \rangle} t^{\langle (1,4),(1/3,1/6) \rangle} = st,$$

$$u \mapsto s^{\langle (0,6),(1,0) \rangle} t^{\langle (1,4),(1,0) \rangle} = t.$$

Composing with the homomorphism induced by the rational parametrization (σ, α) we get homomorphisms $\varphi_i : \mathbb{Q}[u,v][w]/\langle f_0 \rangle \to \mathbb{Q}(s)[\![t]\!]$:

$$\varphi_1 : u \mapsto -8s^6 t, v \mapsto -t^4, w \mapsto -8s^6 t^7 + 8s^8 t^8 - 4s^{10} t^9 + s^{14} t^{11} - \tfrac{1}{2} s^{18} t^{13} + \ldots,$$

$$\varphi_2 : u \mapsto -8st^2, v \mapsto -s^4 t^2, w \mapsto -8s^7 t^5 + 8s^8 t^6 - 4s^9 t^7 + s^{11} t^9 - \tfrac{1}{2} s^{13} t^{11} + \ldots$$

The two induced morphisms $\operatorname{Spec} \mathbb{Q}(s)[\![t]\!] \to X_0$ are the formal prime divisors centered at the origin that become realized on a desingularization of $\widetilde{X_0}$ by point blow ups.

But this is not yet a formal desingularization of X_0. As can be seen in Figure 1, the singular locus of X_0 is the union of the u-axis and the v-axis. So there should also be formal prime divisors supported on these lines. Let's first consider $u = 0$. By mapping $u \mapsto t$ and $v \mapsto s$ we transform f_0 to $w^6 + 3s^3 t^2 w^4 + s^5 t^4 w^3 + 3s^6 t^4 w^2 + s^9 t^6 \in \mathbb{Q}(s)[t][w]$. Now we compute a univariate rational parametrization (σ, α):

$$\sigma : t \mapsto \tfrac{-8}{s^5} t, \; \alpha = -\tfrac{8}{s^5} \gamma t^{\frac{1}{2}} - \tfrac{8}{s^5} t^{\frac{2}{3}} + \tfrac{4}{s^8} \gamma t^{\frac{5}{6}} + \tfrac{1}{s^{11}} \gamma t^{\frac{7}{6}} + \tfrac{1}{2s^{14}} \gamma t^{\frac{3}{2}} + \cdots \in \mathbb{Q}(s)[\gamma][\![t^{(1/6)\mathbb{Z}}]\!]$$

Here γ is an algebraic element satisfying $\gamma^2 + s^3 = 0$. Canceling exponent denominators this yields a homomorphism $\varphi_0 : \mathbb{Q}[u,v][w]/\langle f_0 \rangle \to \mathbb{Q}(s)[\gamma][\![t]\!]$:

$$\varphi_0 : u \mapsto \tfrac{-8}{s^5} t^6, v \mapsto s, w \mapsto -\tfrac{8}{s^5} \gamma t^3 - \tfrac{8}{s^5} t^4 + \tfrac{4}{s^8} \gamma t^5 + \tfrac{1}{s^{11}} \gamma t^7 + \tfrac{1}{2s^{14}} \gamma t^9 + \ldots$$

This homomorphism corresponds to completing the germ at a generic point in $\widetilde{X_0}$ above $u = 0$ by Lemma A.3. This germ is not modified by subsequent point blow ups. So we get a further formal prime divisor. A last one is supported on $v = 0$:

$$\varphi_3 : u \mapsto s, v \mapsto -64s^{10} t^6, w \mapsto -512s^{16} t^9 + 512s^{18} t^{10} - 256s^{20} t^{11} + 64s^{24} t^{13} + \ldots$$

Note that this procedure explicitly produces the residue fields at the generic points of the exceptional divisors in a desingularization. They correspond to the coefficient fields of the power series. Finally, composing all four formal prime divisors with the morphism $X_0 \to X$ which was obtained by the desingularization of the discriminant curve, we get a part of a formal desingularization of X.

3.2. **A Divide and Conquer Approach.** Now we want to cast the theory of the previous paragraph into explicit algorithms. We want to give a formal description of a Jung desingularization of a ramified covering $(\pi : W \to V, X)$. Note that such a desingularization is always relative to an embedded desingularization $\rho : V_\rho \to V$ of the discriminant curve $D_{\pi|_X}$. Because then $(\pi_\rho : W_\rho \to V_\rho, X_\rho)$ for $W_\rho := W \times_V V_\rho$ and $X_\rho := X \times_W W_\rho$ is a nicely ramified covering and we can define the Jung desingularization $\Pi_\rho : Y_\rho \to X$ to be obtained by normalizing X_ρ and successively blowing up singular points, see Remark 3.11.

If we wanted to avoid redundant blow ups, we could already fix the embedded desingularization ρ to be minimal, *i.e.*, obtained by blowing up a point of the discriminant curve only when it is a non-normal crossing singularity. For computational reasons, we choose a slightly different desingularization, see Remark 3.17 below. Also, the definition of a formal description $\mathcal{S}$ of Π_ρ leaves a bit of choice for $\mathcal{S}$, *e.g.*, one may always add formal prime divisors which are realized on the desingularization. We get rid of this ambiguity by requiring that $\mathrm{supp}_X(\mathcal{S}) = \pi^{-1}(D_{\pi|_X})$ and say we compute a *formal description of Π_ρ above $D_{\pi|_X}$*.

Remark 3.12 (Divide and Conquer Paradigm). We will desingularize the discriminant curve and compute the formal prime divisors for the surface at the same time. The substitutions involved in computing the curve desingularization make the defining equations more complicated. Therefore our paradigm must be to compute formal prime divisors "as early" as possible. In other words, if we know that the surface (resp. its normalization) remains unchanged in a subset (up to isomorphism) by further blow ups of the discriminant curve we immediately compute the formal prime divisors centered in that set.

Let $\rho : V_\rho \to V$ be an embedded desingularization of the discriminant curve. Our divide and conquer approach (in particular Algorithm 3 below) relies on the following facts:

- Let $p \in D_{\pi|_X}$ be a point s.t. ρ is not an isomorphism at p. Let $\rho_0 : V' \to V$ be the blow up at p and $(\pi' : W' \to V', X')$ the induced ramified covering. Then ρ factors as $\rho = \rho_1 \rho_0$ where $\rho_1 : V_\rho \to V'$ is an embedded desingularization of $D_{\pi'|_{X'}}$, $X_\rho \to X$ factors through $X' \to X$ and also $\pi'^{-1}(D_{\pi'|_{X'}})$ must be equal to the support of the pullback of $\mathcal{S}$. So it is equivalent to compute the formal description of Π_{ρ_1} above $D_{\pi'|_{X'}}$.
- Now ρ_0 is an isomorphism everywhere except at p. We can split the computation of the formal desingularization Π_ρ into two parts; the computation of formal prime divisors which are not centered above p on the one hand and those which are centered above p, or equivalently, whose pullbacks (see Corollary 2.4) are centered above the exceptional divisor $\rho_0^{-1}(p)$. Computing the latter will be delegated to a recursive call.
- When blowing up the (not necessarily rational) point p we may first apply a morphism to the projection plane that induces a formal isomorphism at p because of Lemma A.3 and Lemma A.4, compare Remark 3.14 below.

Finally, Example 3.3 has shown that in the case of nicely ramified coverings we have to compute formal prime divisors in two ways: Those which are centered above the components of the discriminant curve are obtained using Lemma 3.8 with

$n = 1$, and those which are centered above the normal crossings of the discriminant curve using a combination of Lemma 3.8 with $n = 2$, Lemma 3.10 and Lemma A.4.

3.3. **The Algorithm.** In the following algorithmic descriptions we allow subsets of a set A, which in our notation will be elements of 2^A, as data types. These will either be finite sets or they will be finitely generated ideals of a ring A. So it is clear that they can be represented. For simplicity of notation, we also allow passing of homomorphisms from polynomial rings in a finite number of variables. They can obviously be represented by the images of their generators. We assume that we can represent power series which will be explained later in Section 4.1. If $\phi : A \to B$ is a homomorphism of rings, we write again $\phi^{\uparrow w} : A[w] \to B[w]$ for its lifting to the corresponding polynomial rings by coefficient-wise application and $\mathbf{map}_\phi : 2^A \to 2^B$ for the function on subsets defined by element-wise application.

Let $X \subset \mathbb{P}^3_\mathbb{E}$ be a closed hypersurface. Following Section 3.1.1, we first have to produce a ramified covering. This is done in algorithm `DesingGlobal`. By $\overline{\mathbb{E}}$ (resp. $\overline{\mathbb{E}(s)}$) we denote the algebraic closure of $\mathbb{E}$ (resp. of the rational function field). If it shows up in the return type of a signature we actually mean that the result involves some finite field extension (of transcendence degree 1), *i.e.*, we do not rely on a system for computing with algebraic closures.

The algorithm will be formulated for reduced surfaces, see Remark 2.10. This is due to the fact that we will transform our surface by extending the base field in certain steps and cannot assure that the transformed surface remains integral, even when the original surface was, see Remark 3.14 below.

Algorithm 1 `DesingGlobal`$(F : \mathbb{E}[x_0, \ldots, x_3]) : 2^{\mathbb{E}[x_0, \ldots, x_3] \to \overline{\mathbb{E}(s)}[\![t]\!]}$

Require: A squarefree homogeneous polynomial $F \neq 0$.
Ensure: A finite set of homomorphisms $\mathbb{E}[x_0, \ldots, x_3] \to \mathbb{F}[\![t]\!]$ factoring through $\mathbb{E}[x_0, \ldots, x_3]/\langle F \rangle$ s.t. the induced morphisms $\operatorname{Spec} \mathbb{F}[\![t]\!] \to \operatorname{Proj} \mathbb{E}[x_0, \ldots, x_3]/\langle F \rangle$ are a formal desingularization.
1: Let $\phi : \mathbb{E}[x_0, \ldots, x_3] \to \mathbb{E}[x_0, \ldots, x_3]$ be a linear automorphism s.t. $\phi(F)(1, 0, 0, 0) \neq 0$;
2: $\psi_1 : \mathbb{E}[x_0, \ldots, x_3] \to \mathbb{E}[u, v][w] : x_0 \mapsto w, x_1 \mapsto 1, x_2 \mapsto u, x_3 \mapsto v$;
3: $S := \mathbf{map}_{\rho \mapsto \rho \psi_1 \phi} \texttt{DesingLocal}(\psi_1 \phi(F), \langle 0 \rangle)$;
4: $\psi_2 : \mathbb{E}[x_0, \ldots, x_3] \to \mathbb{E}[u, v][w] : x_0 \mapsto w, x_1 \mapsto v, x_2 \mapsto 1, x_3 \mapsto u$;
5: $S := S \cup \mathbf{map}_{\rho \mapsto \rho \psi_2 \phi} \texttt{DesingLocal}(\psi_2 \phi(F), \langle v \rangle)$;
6: $\psi_3 : \mathbb{E}[x_0, \ldots, x_3] \to \mathbb{E}[u, v][w] : x_0 \mapsto w, x_1 \mapsto u, x_2 \mapsto v, x_3 \mapsto 1$;
7: $S := S \cup \mathbf{map}_{\rho \mapsto \rho \psi_3 \phi} \texttt{DesingLocal}(\psi_3 \phi(F), \langle u, v \rangle)$;
8: **return** S;

In line 1 we choose a linear automorphism of $\mathbb{P}^3_\mathbb{E}$ (represented by ϕ) s.t. the preimage of X under this automorphism is Noether normalized by a projection onto the plane $x_0 = 0$.

Remark 3.13. The automorphism maps $(1, 0, 0, 0)$ to a point $p \notin X$. In an actual implementation one should find p s.t. most of its coordinates are zero and the rest are small integers. This preserves sparsity in $\phi(F)$ and keeps coefficients small.

For convenience of description, we will actually assume that ϕ is the identity. Then the ramified covering $(\pi : W \to V, X)$ is given as follows: We set $W := \mathbb{P}^3_\mathbb{E} \setminus \{(1 : 0 : 0 : 0)\}$, V is the plane $x_0 = 0$, π is the corresponding linear projection and X is defined by the vanishing of F monic in x_0.

The algorithm produces a set of homomorphisms S representing a formal desingularization. Therefore we cover V by open subsets $x_i \neq 0$ (given by the ψ_i) for

$1 \leq i \leq 3$ and call algorithm `DesingLocal` for each of those in lines 2 to 7. The latter algorithm produces formal desingularizations of the respective affine subsets. Because of the huge overlaps we add *focus* ideals to each call.

Algorithm 2 `DesingLocal`$(f : \mathbb{E}[u,v][w], \mathcal{F} : 2^{\mathbb{E}[u,v]}) : 2^{\mathbb{E}[u,v][w] \to \overline{\mathbb{E}(s)}[\![t]\!]}$

Require: A squarefree polynomial $f \neq 0$, monic in w, and a focus ideal $\mathcal{F}$.

Ensure: A finite set of homomorphisms $\mathbb{E}[u,v][w] \rightarrow \mathbb{F}[\![t]\!]$ factoring through $\mathbb{E}[u,v][w]/\langle f \rangle$ s.t. the induced morphisms $\operatorname{Spec} \mathbb{F}[\![t]\!] \to \operatorname{Spec} \mathbb{E}[u,v][w]/\langle f \rangle$ form the subset of a formal desingularization which is centered above the closed subset defined by $\mathcal{F}$.

1: $d := \texttt{SquareFreePart}(\operatorname{disc}_w(f)); E := \texttt{IrredFactors}(d);$
2: $S := \bigcup_{e \in E \text{ with } \mathcal{F} \subseteq \langle e \rangle} \texttt{DivisorsAboveCurve}(f, e);$
3: **for** $(u_0, v_0) \in \texttt{ZeroSet}(\mathcal{F} + \langle d, \partial d/\partial u, \partial d/\partial v \rangle)$ **do**
4:     $\psi : \mathbb{E}[u,v] \to \mathbb{E}'[u,v] : u \mapsto u + u_0, v \mapsto v + v_0;$
5:     $S := S \cup \mathbf{map}_{\rho \mapsto \rho \psi^{\uparrow w}} \texttt{DesingRec}(\psi^{\uparrow w}(f), \{\psi(e) \mid e \in E \text{ and } \psi(e)(0,0) = 0\});$
6: **return** $S;$

In line 1 we compute the defining equation d of the *reduced* discriminant curve and its factors E. For all $e \in E$ the prime ideal $\langle e \rangle$ corresponds to the generic point $p \in V$ of an irreducible component of the discriminant curve.

No matter how the desingularization $\rho : V_\rho \to V$ of the discriminant curve looks like, it is always a succession of point blow ups. Therefore p will be isomorphically contained in V_ρ. The same holds for points in the normalization of X lying above p. According to our paradigm in Remark 3.12 we compute the formal prime divisors centered above these p already at this stage of the algorithm, see line 2, by calling algorithm `DivisorsAboveCurve` (see Algorithm 4) for each $e \in E$ which is in focus.

In line 3 we compute the singular locus of the reduced discriminant curve, more precisely, that part which is in focus. For each of its closed points p we want to find the formal prime divisors centered above p. Therefore we apply the homomorphism ψ of line 4 (which corresponds to moving p to the origin) and then call algorithm `DesingRecursive` in line 5.

Remark 3.14 (Exploiting Formal Isomorphisms). At this point we would like to mention that ψ may involve an algebraic field extension, namely, by the residue field $\mathbb{E}'$ of p. Therefore ψ, which looks like a mere translation, is not an isomorphism. Nevertheless the induced morphism of schemes $\operatorname{Spec} \mathbb{E}'[u,v] \to \operatorname{Spec} \mathbb{E}[u,v]$ is formally isomorphic at p by Corollary A.2. (Note that we can choose a system $f_1, f_2 \in \mathbb{E}[u,v]$ of generators of the maximal ideal corresponding to p s.t. $f_1 \in \mathbb{E}[u]$ is irreducible and the image of f_2 in $(\mathbb{E}[u]/\langle f_1 \rangle)[v]$ is also irreducible.) But for computing a formal desingularization, we may well pass to a formally isomorphic scheme as a consequence of Lemma A.3 and Lemma A.4. Note that the introduction of a field extension may further split the defining equation, *i.e.*, $\psi^{\uparrow w}(f)$ may be reducible even though f is not. Also the discriminant factors might split again. This is another (more important) reason for computing the formal prime divisors above the components of the discriminant already in line 2.

Remark 3.15 (Auxiliary Functions). The above algorithm depends on a couple of auxiliary functions which we are not giving in detail, their names are mainly self-explanatory: `SquareFreePart` should compute the squarefree part of a polynomial and `IrredFactors` is supposed to produce the set of irreducible factors of a polynomial. A comment on `ZeroSet` is in order. It expects a zero-dimensional ideal $\mathcal{F} \subseteq \mathbb{E}[x_1, \ldots, x_n]$. It should return a finite set of n-tuples s.t. for each maximal

ideal $\mathfrak{f}$ containing $\mathcal{F}$ there is exactly one tuple $(\xi_1, \ldots, \xi_n) \in (\mathbb{E}')^n$ s.t. $\mathbb{E} \subseteq \mathbb{E}'$ and the induced homomorphism $\mathbb{E}[x_1, \ldots, x_n] \to \mathbb{E}' : x_i \mapsto \xi_i$ lifts to an isomorphism from $\mathbb{E}[x_1, \ldots, x_n]/\mathfrak{f}$.

Remark 3.16. Computing the squarefree part and factorization was done in Algorithm 2 to keep the number of parameters small. Of course it would fit more naturally in Algorithm 1 to avoid multiple computations.

The recursive algorithm `DesingRecursive` now implements the *divide and conquer* paradigm, see again Remark 3.12.

Algorithm 3 $\texttt{DesingRecursive}(f : \mathbb{E}[u,v][w], E : 2^{\mathbb{E}[u,v]}) : 2^{\mathbb{E}[u,v][w] \to \overline{\mathbb{E}(s)}[\![t]\!]}$

Require: A squarefree polynomial $f \neq 0$, monic in w, and a set of polynomials E s.t. $e(0,0) = 0$ for all $e \in E$ and $\prod_{e \in E} e$ is the squarefree part of $\operatorname{disc}_w(f)$ in the local ring $\mathbb{E}[u,v]_{\langle u,v \rangle}$.

Ensure: A finite set of homomorphisms $\mathbb{E}[u,v][w] \to \mathbb{F}[\![t]\!]$ factoring through $\mathbb{E}[u,v][w]/\langle f \rangle$ s.t. the induced morphisms $\operatorname{Spec} \mathbb{F}[\![t]\!] \to \operatorname{Spec} \mathbb{E}[u,v][w]/\langle f \rangle$ form the subset of a formal desingularization which is centered above the origin.

1: **if** $\texttt{IsNormalCrossing}(E)$ **then**
2:     **return** $\texttt{DivisorsAboveCrossing}(f, E)$;
3: $\phi_u : \mathbb{E}[u,v] \to \mathbb{E}[u,v] : u \mapsto uv, v \mapsto v$; $\phi_v : \mathbb{E}[u,v] \to \mathbb{E}[u,v] : u \mapsto v, v \mapsto uv$;
4: $f_u := \phi_u{}^{\uparrow w}(f)$; $f_v := \phi_v{}^{\uparrow w}(f)$;
5: $E_u := \mathbf{map}_{e \mapsto \phi_u(e)/v^{\operatorname{ord}(e)}}(E)$; $E_v := \mathbf{map}_{e \mapsto \phi_v(e)/v^{\operatorname{ord}(e)}}(E)$;
6: $S := \mathbf{map}_{\rho \mapsto \rho \phi_u{}^{\uparrow w}} \texttt{DivisorsAboveCurve}(f_u, v)$;
7: **for** $(u_0, v_0) \in \texttt{ZeroSet}(\langle \prod_{e \in E_u} e, v \rangle)$ **do**
8:     $\psi : \mathbb{E}[u,v] \to \mathbb{E}'[u,v] : u \mapsto u + u_0, v \mapsto v + v_0$;
9:     $S := S \cup \mathbf{map}_{\rho \mapsto \rho \psi^{\uparrow w} \phi_u{}^{\uparrow w}} \texttt{DesingRecursive}(\psi^{\uparrow w}(f_u),$
                                       $\{\psi(e) \mid e \in E_u \text{ and } \psi(e)(0,0) = 0\} \cup \{v\})$;
10: **if** exists $e \in E_v$ s.t. $e(0,0) = 0$ **then**
11:     $S := S \cup \mathbf{map}_{\rho \mapsto \rho \phi_v{}^{\uparrow w}} \texttt{DesingRecursive}(f_v,$
                                       $\{e \mid e \in E_v \text{ and } e(0,0) = 0\} \cup \{v\})$;
12: **return** S;

In line 1 we check, whether the origin of the reduced discriminant curve is a normal crossing. If this is the case we know (see Corollary 3.9) that the points above the origin in the normalization are toroidal singularities that can be desingularized by a succession of blow ups in isolated singular points. The corresponding formal prime divisors are computed by algorithm `DivisorsAboveCrossing` (see Algorithm 6) and returned.

Otherwise we have to modify the discriminant curve by blowing up the origin. The two charts of the blow up are computed in lines 3 to 5: We determine the defining equations f_u and f_v of the transformed surface and also modify the discriminant factors accordingly.

Note that the homomorphisms are such that the exceptional divisor is given by $v = 0$ in *both* charts. Over this exceptional divisor there are centered a couple of formal prime divisors. By the same reasoning as for Algorithm 2 (see Remark 3.14) we compute them immediately by calling `DivisorsAboveCurve` in line 6.

Now we have to consider the points on the exceptional divisor which are singular. In one of the charts they are given by the set of line 7. As in Algorithm 2 we move these points to the origin and go into recursion, see lines 8 and 9. Now there is possibly one singular point left to consider, namely, the origin of the other chart. It is treated in line 11.

To complete the algorithm, it remains to show how to compute the formal prime divisors which are centered above irreducible components or normal crossings of the reduced discriminant curve.

3.3.1. *Divisors above Generic Points of the Discriminant Curve.* We now give an algorithm for computing the formal prime divisors which are centered above generic points of the discriminant curve. This is easy by what we have developed so far.

Algorithm 4 $\mathtt{DivisorsAboveCurve}(f : \mathbb{E}[u,v][w], e : \mathbb{E}[u,v]) : 2^{\mathbb{E}[u,v][w] \to \overline{\mathbb{E}(s)}[\![t]\!]}$

Require: A squarefree polynomial $f \neq 0$, monic in w, and an irreducible factor e of $\mathrm{disc}_w(f)$.
Ensure: A finite set of homomorphisms $\mathbb{E}[u,v][w] \to \mathbb{F}[\![t]\!]$ factoring through $\mathbb{E}[u,v][w]/\langle f \rangle$ s.t. the induced morphisms $\mathrm{Spec}\,\mathbb{F}[\![t]\!] \to \mathrm{Spec}\,\mathbb{E}[u,v][w]/\langle f \rangle$ form the subset of a formal desingularization which is centered above $\langle e \rangle$.
 1: $\mathbb{F}_0 := \mathrm{QF}(\mathbb{E}[u,v]/e)$; Let $u_0, v_0 \in \mathbb{F}_0$ be the natural images of u, v;
 2: **if** $\partial e/\partial v \neq 0$ **then**
 3:     $\phi : \mathbb{E}[u,v] \to \mathbb{F}_0[t] : u \to u_0, v \to v_0 + t$;
 4: **else**
 5:     $\phi : \mathbb{E}[u,v] \to \mathbb{F}_0[t] : u \to u_0 + t, v \to v_0$;
 6: $S := \emptyset$;
 7: **for** $(\sigma, \alpha) \in \mathtt{Param}(\phi^{\uparrow w}(f))$ **do**
 8:     $\psi : \mathbb{F}[\![t^{(1/e)\mathbb{Z}}]\!] \to \mathbb{F}[\![t]\!] : \gamma \mapsto \mathtt{Evaluate}(\gamma, (e), t)$; {assuming $\alpha \in \mathbb{F}[\![t^{(1/e)\mathbb{Z}}]\!]$}
 9:     $S := S \cup \{\mathbb{E}[u,v][w] \to \mathbb{F}[\![t]\!] : u \mapsto \psi\sigma\phi(u), v \mapsto \psi\sigma\phi(v), w \mapsto \psi(\alpha)\}$;
10: **return** S;

In lines 1 to 5 we construct a homomorphism $\phi : \mathbb{E}[u,v] \to \mathbb{F}_0[t]$ inducing an isomorphism from the completed localization at $\langle e \rangle$ to $\mathbb{F}_0[\![t]\!]$, see Corollary A.2. Therefore the completions of the localizations of $\mathrm{IC}(\mathbb{E}[u,v][w]/\langle f \rangle)$ at prime ideals above $\langle e \rangle$ are isomorphic to those of $\mathrm{IC}(\mathbb{F}_0[\![t]\!]/\langle \phi^{\uparrow w}(f) \rangle)$ above $\langle t \rangle$ by Lemma A.3. Lemma 3.8 tells us how these completions can be computed using a complete set of rational parametrizations. This is done in lines 7 to 9 using the results of a call to $\mathtt{Param}$ (see Algorithm 11 in Section 4.3). The homomorphism ψ defined via $\mathtt{Evaluate}$ (see Algorithm 8) is just mapping $t^{1/e} \mapsto t$ for cosmetic reasons, *i.e.*, getting rid of denominators.

3.3.2. *Divisors above Normal Crossings of the Discriminant Curve.* First we fill a gap in Algorithm 3 and show how to test the normal crossing property for a set of curves.

Algorithm 5 $\mathtt{IsNormalCrossing}(E : 2^{\mathbb{E}[u,v]}) : \mathtt{Boolean}$

Require: A set of squarefree polynomials E s.t. $e(0,0) = 0$ for all $e \in E$.
Ensure: $\mathtt{true}$ iff the curves defined by E are *considered* normal crossing at the origin.
 1: **if** E is not of the form $\{v, e\}$ **then**
 2:     **return** $\mathtt{false}$;
 3: **else**
 4:     **return** $\partial e/\partial u(0,0) \neq 0$;

Note that in general E describes a set of curves with normal crossing at the origin when $E = \{e_1, e_2\}$ and $\det(\partial(e_1, e_2)/\partial(u, v))(0, 0) \neq 0$. But this algorithm returns $\mathtt{true}$ only for the special situation that one of the curves is actually $v = 0$.

Remark 3.17 (Almost Minimal Jung Desingularizations)*.* Although Algorithm 5 does in fact test for normal crossings of a special form the overall algorithm will eventually terminate; Computing the point blow ups as in Algorithm 3 guarantees that the exceptional divisor is always of the form $v = 0$ in both charts. It is known (see [24, Thm. 1.47]) that one can compute an embedded desingularization by a finite number of point blow ups. If one of the normal crossings is not of the above form, then our algorithm computes an additional blow up but terminates at the next level. In other words, the computed Jung desingularization belongs to an *almost minimal* embedded desingularization of the discriminant curve. The benefit is that the homomorphism in line 2 of the next algorithm is so easy to compute. One could also use usual normal crossings and compute more complicated homomorphisms.

Algorithm 6 `DivisorsAboveCrossing`$(f : \mathbb{E}[u, v][w], E : 2^{\mathbb{E}[u,v]}) : 2^{\mathbb{E}[u,v][w] \to \overline{\mathbb{E}}(s)[\![t]\!]}$

Require: A squarefree polynomial $f \neq 0$, monic in w, and a set of polynomials $E = \{v, e\}$ s.t. $e(0, 0) = 0$, $\partial e/\partial u(0, 0) \neq 0$ and ve is the squarefree part of $\mathrm{disc}_w(f)$ in the local ring $\mathbb{E}[u, v]_{\langle u,v \rangle}$.
Ensure: A finite set of homomorphisms $\mathbb{E}[u, v][w] \to \mathbb{F}[\![t]\!]$ factoring through $\mathbb{E}[u, v][w]/\langle f \rangle$ s.t. the induced morphisms $\mathrm{Spec}\,\mathbb{F}[\![t]\!] \to \mathrm{Spec}\,\mathbb{E}[u, v][w]/\langle f \rangle$ form the subset of a formal desingularization which is centered above the origin.
1: Let $g := e(z, v') - u' \in \mathbb{E}[u', v'][z]$;
2: $\phi : \mathbb{E}[u, v] \to \mathbb{E}[\![u', v']\!] : v \mapsto v', u \mapsto \texttt{ImplicitFunction}(g)$;
3: $S := \emptyset$;
4: **for** $(\sigma, \alpha) \in \texttt{Param}(\phi^{\uparrow w}(f))$ **do**
5:     Let $\mathfrak{n}_1, \ldots, \mathfrak{n}_l \in \mathbb{Z}^2$ be the sequence of generators of $\Gamma^\vee \cap \mathbb{R}^2_{\geq 0}$;
      {assuming $\alpha \in \mathbb{E}'[\![(u', v')^\Gamma]\!]$ and ordering generators as in Figure 2}
6:     **for** $1 \leq i \leq l - 2$ **do**
7:       $\psi : \mathbb{E}'[\![(u', v')^\Gamma]\!] \to \mathbb{E}'(s)[\![t]\!] : \gamma \mapsto \texttt{Evaluate}(\gamma, (\mathfrak{n}_i, \mathfrak{n}_{i+1}), (s, t))$;
      {where $s, t \in \mathbb{E}'(s)[\![t]\!]$}
8:       $S := S \cup \{\mathbb{E}[u, v][w] \to \mathbb{F}[\![t]\!] : u \mapsto \psi\sigma\phi(u), v \mapsto \psi\sigma\phi(v), w \mapsto \psi(\alpha)\}$;
9: **return** S;

This algorithm expects that the discriminant curve of the input surface has a normal crossing at the origin, more precisely, the discriminant of the defining equation is $v^{d_1} e^{d_2}$ times a local unit. We want to compute bivariate parametrizations above the origin, but f is not yet normal crossing. We first have to apply a formal isomorphism ϕ, see line 2, that maps $v \mapsto v'$ and $e \mapsto u'$, because then the discriminant becomes $v'^{d_1} u'^{d_2}$ up to a unit and the defining equation $\phi^{\uparrow w}(f)$ is quasi-ordinary. To this end the image of u must fulfill the equation $e(\phi(u), v') - u' = 0$ which has a unique solution by the implicit function theorem and is computed by a call to `ImplicitFunction` (see Algorithm 9 in Section 4.2).

By the same reasoning as for Algorithm 6 the completions of the localizations of $\mathrm{IC}(\mathbb{E}[u, v][w]/\langle f \rangle)$ at prime ideals above the origin can be computed by bivariate rational parametrization using a call to `Param`, see line 4. Now assume such a completion is given by $\mathbb{E}'[\![(u', v')^\Gamma]\!]$.

We know how to compute a formal description of a special desingularization of $\mathrm{Spec}\,\mathbb{E}'[(u', v')^\Gamma]$, namely, the one obtained by a minimal number of point blow ups, see Lemma 3.10 and Remark 3.11. We compute the corresponding homomorphisms $\mathbb{E}'[\![(u', v')^\Gamma]\!] \to \mathbb{E}'(s)[\![t]\!] : (u', v')^\mathfrak{m} \mapsto s^{\mathfrak{n}_i(\mathfrak{m})} t^{\mathfrak{n}_{i+1}(\mathfrak{m})}$ by calls to `Evaluate` in line 7. This desingularization commutes with completion by Lemma A.4, hence, we get a formal desingularization of the toroidal singularity by composing these homomorphisms with the one given by the parametrization, compare line 8.

4. Computing with Multivariate Algebraic Power Series

In order to implement the above algorithms we have to represent multivariate, fractionary, algebraic power series, *i.e.*, power series with coefficients in a field $\mathbb{E}$, variables $x_1, \ldots, x_n$ and exponents in $\Gamma \cap \mathbb{R}^n_{\geq 0}$ (the non-negative orthant of a full rational lattice) that are roots of non-zero polynomials in $\mathbb{E}[x_1, \ldots, x_n][z]$. In the sequel we denote this ring by $\mathbb{E}[\![\underline{x}^\Gamma]\!]$ (hence, this notation from now means *algebraic*, not formal power series). We must be able to perform a couple of operations:

(1) We have to expand power series up to arbitrary order.
(2) We have to compute the power series arising in complete sets of rational parametrizations for quasi-ordinary polynomials and solve equations fulfilling the conditions of the implicit function theorem.
(3) Let $\hom(\Gamma, \mathbb{E}^*)$ denote the (commutative, multiplicative) group of homomorphisms from the lattice Γ to the multiplicative group $\mathbb{E}^*$ with group operation given by multiplication in the codomain. With $\sigma \in \hom(\Gamma, \mathbb{E}^*)$ we associate the automorphism $\mathbb{E}[\![\underline{x}^\Gamma]\!] \to \mathbb{E}[\![\underline{x}^\Gamma]\!]$ mapping $\underline{x}^{\mathfrak{m}} \mapsto \sigma(\mathfrak{m})\underline{x}^{\mathfrak{m}}$ and $c \mapsto c$ for $c \in \mathbb{E}$. This action of $\hom(\Gamma, \mathbb{E}^*)$ on $\mathbb{E}[\![\underline{x}^\Gamma]\!]$ should be computable.
(4) If $\alpha \in \mathbb{E}_1[\![\underline{x}^{\Gamma_1}]\!]$ is a power series, $\mathfrak{n}_1, \ldots, \mathfrak{n}_l$ are vectors in $\Gamma_1^\vee \cap \mathbb{R}^m_{\geq 0}$ and $(\xi_1, \ldots, \xi_l)$ are power series in $\mathbb{E}_2[\![\underline{x}^{\Gamma_2}]\!]$ where $\mathbb{E}_2$ is a field extension of $\mathbb{E}_1$, we want to compute the image of α under the homomorphism $\phi : \mathbb{E}_1[\![\underline{x}^{\Gamma_1}]\!] \to \mathbb{E}_2[\![\underline{x}^{\Gamma_2}]\!]$ which maps $\underline{x}^{\mathfrak{m}} \mapsto \prod_{1 \leq i \leq l} \xi_i^{\mathfrak{n}_i(\mathfrak{m})}$ and $c \mapsto c$ for $c \in \mathbb{E}_1$ if such ϕ is well-defined.

Remark 4.1 (Origin of Requirements). Requirement (1) just means that (in order to return values) we need a representation in finite terms of series which a priori are infinite objects.

Requirement (2) is obvious. We have to compute rational parametrizations in Algorithms 4 and 6 in order to compute formal prime divisors in the case of nicely ramified coverings. The first line of the latter algorithm also implies solving an equation that fulfills the conditions of the implicit function theorem.

Further it would be nice to express certain homomorphisms $\mathbb{E}_1[\![\underline{x}^{\Gamma_1}]\!] \to \mathbb{E}_2[\![\underline{x}^{\Gamma_2}]\!]$. In general these are given by specifying the images of generators $\underline{x}^{\mathfrak{m}}$ in a consistent way. But such general homomorphisms are not easy to compute. Instead we concentrate on the two special cases (3) and (4).

Computing the action induced by lattice homomorphisms becomes relevant when computing rational parametrizations. So we need (3) to accomplish (2).

In line 7 of Algorithm 6, we find a transformation which is a special case of requirement (4). Another special case of that requirement is substitution of power series $\xi_i \in \mathbb{E}_2[\![\underline{x}^{\Gamma_2}]\!]$ into a polynomial or power series $g \in \mathbb{E}_1[\![x_1, \ldots, x_n]\!]$ which is an instance with $\Gamma_1 = \Gamma_1^\vee = \mathbb{Z}^n$ and $\mathfrak{n}_i$ the standard basis vectors. Such substitutions occur when we compute the composite of two homomorphisms, *e.g.*, in line 9 of Algorithm 4.

Also note that an even more special case of the last requirement is effectivity of addition and multiplication (with $g = x_1 + x_2$ resp. $g = x_1 x_2$).

Computations with algebraic power series usually involve studying the support and the *Newton Polygon* of the defining equation (see [39, 29, 4, 35]), which live in $\mathbb{Q}^n \times \mathbb{Z}$ resp. $\mathbb{R}^{n+1}$. In order to allow for a nice implementation, we will consider a *flattened* support by assuming that $\mathbb{Q}^n$ is ordered as a group and considering $\mathbb{Q}^n \times \mathbb{Z}$ a "plane". In this setting, one can do a fair amount of "convex geometry".

In fact we will work with two different orderings. Let $q_1, q_2 \in \mathbb{Q}^n$. We have a partial ordering on $\mathbb{Q}^n$ by comparing the total degrees $|q_1|$ and $|q_2|$ (*i.e.*, the sum of their components) via $\leq$ as rational numbers. Further we assume a total ordering

$\preccurlyeq$ which is a refinement of it, *i.e.*, $|q_1| \leq |q_2|$ implies $q_1 \preccurlyeq q_2$. For a power series $0 \neq \alpha = \sum_{\mathfrak{m}} \alpha_{\mathfrak{m}} \underline{x}^{\mathfrak{m}} \in \mathbb{E}[\![\underline{x}^{\Gamma}]\!]$ we can therefore define two supports and two orders, namely, $\mathrm{supp}_{\leq}(\alpha) := \{ |\mathfrak{m}| \in \mathbb{Q} \mid \alpha_{\mathfrak{m}} \neq 0 \}$, $\mathrm{supp}_{\preccurlyeq}(\alpha) := \{ \mathfrak{m} \in \mathbb{Q}^n \mid \alpha_{\mathfrak{m}} \neq 0 \}$, $\mathrm{ord}_{\leq}(\alpha) := \min_{\leq}(\mathrm{supp}_{\leq}(\alpha))$ and $\mathrm{ord}_{\preccurlyeq}(\alpha) := \min_{\preccurlyeq}(\mathrm{supp}_{\preccurlyeq}(\alpha))$. W.r.t. the finer ordering, we will also need the initial term $\mathrm{it}_{\preccurlyeq}(\alpha) := \alpha_{\mathrm{ord}_{\preccurlyeq}(\alpha)} \underline{x}^{\mathrm{ord}_{\preccurlyeq}(\alpha)}$. The degree compatibility is important because it implies that we can easily expand series up to an arbitrary order w.r.t the fine ordering if and only if we can expand up to arbitrary total degree.

We also have to study polynomials with power series coefficients. Consider

$$0 \neq g = \sum_{0 \leq i \leq d} \left(\sum_{\mathfrak{m}} g_{\mathfrak{m},i} \underline{x}^{\mathfrak{m}} \right) z^i \in \mathbb{E}_0[\![\underline{x}^{\Gamma_0}]\!][z].$$

Its *support* is $\mathrm{supp}_{\preccurlyeq}(g) := \{ (\mathfrak{m}, i) \in \mathbb{Q}^n \times \mathbb{Z} \mid g_{\mathfrak{m},i} \neq 0 \}$. We define linear maps

$$\varphi_{\mathfrak{n}} : \mathbb{Q}^n \times \mathbb{Z} \to \mathbb{Q}^n : (\mathfrak{m}, i) \mapsto \mathfrak{m} + i\mathfrak{n}$$

for all $\mathfrak{n} \in \mathbb{Q}_{\geq 0}^n$ and set $\mathrm{ord}_{\preccurlyeq,\mathfrak{n}}(g) := \min_{\preccurlyeq} \{ \varphi_{\mathfrak{n}}(\mathfrak{m}, i) \mid (\mathfrak{m}, i) \in \mathrm{supp}_{\preccurlyeq}(g) \}$. We say that $\mathrm{supp}_{\preccurlyeq}(g)$ has an *non-trivial* edge of slope $\mathfrak{n}$ iff $\varphi_{\mathfrak{n}}$ attains its minimum for *at least two* arguments in $\mathrm{supp}_{\preccurlyeq}(g)$. Further we define the $\mathfrak{n}$-th *edge equation* as

$$\mathrm{edge}_{\preccurlyeq,\mathfrak{n}}(g) := \sum_{\substack{(\mathfrak{m},i) \in \mathrm{supp}_{\preccurlyeq}(g) \text{ and} \\ \varphi_{\mathfrak{n}}(\mathfrak{m},i) = \mathrm{ord}_{\preccurlyeq,\mathfrak{n}}(g)}} g_{\mathfrak{m},i} \underline{x}^{\mathfrak{m}} z^i.$$

Then $\mathrm{supp}_{\preccurlyeq}(g)$ has a non-trivial edge of slope $\mathfrak{n}$ iff the $\mathfrak{n}$-th edge equation is not a single term, *i.e.*, it is also non-trivial.

Note that $\mathrm{supp}_{\preccurlyeq}(g)$ has at most finitely many non-trivial edges. Indeed, assume $g = \sum_{l \leq i \leq k} \gamma_i z^i$ with $\gamma_l \neq 0$ and $\gamma_k \neq 0$ and let $\mathfrak{o}_i := \mathrm{ord}_{\preccurlyeq}(\gamma_i)$ whenever $\gamma_i \neq 0$. Then the only possible slopes are $(i-j)^{-1}(\mathfrak{o}_j - \mathfrak{o}_i)$ for $i > j$ and $\mathfrak{o}_j \succ \mathfrak{o}_i$ with $\gamma_i \neq 0$, $\gamma_j \neq 0$. Denoting the slopes that occur by $\mathfrak{n}_m$ we could define the "Newton Polygon" of g as the set $\{ (\mathfrak{m}, i) \in \mathbb{Q}^n \times \mathbb{Z} \mid l \leq i \leq k \text{ and } \varphi_{\mathfrak{n}_m}(\mathfrak{m}) \succcurlyeq \mathrm{ord}_{\preccurlyeq,\mathfrak{n}_m}(g) \text{ for all } m \}$.

4.1. **Representing Algebraic Power Series.** In the sequel we suggest a representation which is suitable for the computer algebra system MAGMA [7] and facilitates all of the above operations. We only highlight the essential points. MAGMA, like most other computer algebra systems, does not provide polynomials $f \in \mathbb{E}[\underline{x}^{\Gamma}]$ with fractionary exponents directly. For simplicity of reading, we nevertheless use such polynomials, an implementation being straightforward. We also assume that given f we can ask for its coefficient field $\mathbb{E}$ and exponent lattice Γ and that an implicit conversion mechanism is provided for $\mathbb{E}_1[\underline{x}^{\Gamma_1}] \subseteq \mathbb{E}_2[\underline{x}^{\Gamma_2}]$ whenever $\mathbb{E}_1 \subseteq \mathbb{E}_2$ and $\Gamma_1 \subseteq \Gamma_2$. Further it should be understood that a tuple defining a series may recursively depend on other series or even on polynomials with series coefficients. We represent algebraic power series using a *hybrid lazy-exact approach* by finite, acyclic, directed and rooted graphs with nodes of two types:

Type A: We represent an algebraic power series $\alpha \in \mathbb{E}_2[\![\underline{x}^{\Gamma_2}]\!]$ by a tuple

(4.1)
$$(\alpha_0, f)$$

where $\alpha_0 \in \mathbb{E}_2[\underline{x}^{\Gamma_2}]$ is an initial segment of α w.r.t. $\preccurlyeq$ and $f = \sum_{0 \leq i \leq d} \varphi_i z^i \in \mathbb{E}_1[\![\underline{x}^{\Gamma_1}]\!][z]$ are such that $\mathbb{E}_1 \subseteq \mathbb{E}_2$, $\Gamma_1 \subseteq \Gamma_2$ and $f \neq 0$ is squarefree (when considered as a polynomial over $\mathrm{QF}(\mathbb{E}_1[\![\underline{x}^{\Gamma_1}]\!])$) and vanishing on α.

Such a node in general has as $d+1$ descendants, namely, the coefficients φ_i. As a special case we allow $f \in \mathbb{E}_1[\underline{x}^{\Gamma_1}][z]$. In this case we store f itself, there are no descendants and the node is terminal.

We also need a technical condition to ensure that α_0 identifies α uniquely amongst the roots of f.

Algorithm 7 $\texttt{Series}(\alpha_0 : \mathbb{E}_2[\underline{x}^{\Gamma_2}], f : \mathbb{E}_1[\![\underline{x}^{\Gamma_1}]\!][z]) : \mathbb{E}_2[\![\underline{x}^{\Gamma_2}]\!]$

Require: A tuple as in (4.1) fulfilling Condition 4.3.
Ensure: The power series α defined by it.
 1: Encapsulate data and return object of type "algebraic power series";

Type B: The second type of node is given by a tuple

$$(4.2) \qquad\qquad\qquad (\alpha, \underline{\mathfrak{n}}, \underline{\xi})$$

and represents the image $\beta := \phi(\alpha)$ under the homomorphism described in the third requirement. It has $l + 1$ descendants, namely, the ξ_i and α. Also in this case we need a technical condition necessary for ϕ being well-defined.

Algorithm 8 $\texttt{Evaluate}(\alpha : \mathbb{E}_1[\![\underline{x}^{\Gamma_1}]\!], \underline{\mathfrak{n}} : (\Gamma_1^\vee \cap \mathbb{R}_{\geq 0}^n)^l, \underline{\xi} : \mathbb{E}_2[\![\underline{x}^{\Gamma_2}]\!]) : \mathbb{E}_2[\![\underline{x}^{\Gamma_2}]\!]$

Require: A tuple as in (4.2) fulfilling Condition 4.6.
Ensure: The power series β defined by it.
 1: Encapsulate data and return object of type "algebraic power series";

Nodes of type B facilitate explicitly the operation of requirement (4) from our list. The following sections describe how to implement the remaining requirements using algorithms based on an idea in [3] which is similar in spirit to [35].

Remark 4.2 (Representation Paradigm). The reason for calling this representation *lazy-exact* is the following: In order to expand a series up to some order, we will recursively expand its descendants (maybe storing precomputed values) and then compute the approximation of the series under consideration in a *lazy* fashion. On the other hand, using elimination theory and traversing the representation graph recursively, one can compute a (minimal) defining polynomial for any series represented as above. Therefore zero-equality and polynomiality/rationality are decidable. In this sense we speak of an *exact* representation. Since in particular all polynomials (including 0 and 1) are representable we get a *computationally effective* ring. All this (and a little bit more) is included in the `MAGMA` implementation. Note, however, that it is advisable to avoid the effective decision algorithms because they depend on nested resultant computations and can be very expensive.

4.2. **Expanding Algebraic Power Series.** Now we show how to expand power series in a lazy fashion. For more efficient computations with lazy power series, see [34]. For expanding a power series α given by a tuple (4.1), we consider

$$(4.3) \quad g := f(z + \alpha_0) = \sum_{i=0}^{d} \gamma_i z^i, \alpha_1 := \alpha - \alpha_0, \mathfrak{n} := \operatorname{ord}_{\preccurlyeq}(\alpha_1) \text{ and } \mathfrak{c} := \operatorname{ord}_{\preccurlyeq}(\gamma_1).$$

First we want to find implications of the fact that $g(\alpha_1) = 0$. The case $\alpha_1 = 0$ happens if and only if $g(0) = 0$ or, equivalently, $\gamma_0 = 0$. Let's assume $\alpha_1 \neq 0$ and set $\alpha' := \operatorname{it}_{\preccurlyeq}(\alpha_1)$. Next we study the contribution of the terms $\gamma_i z^i$ to the result under the substitution $z \mapsto \alpha_1$. Whenever $\gamma_i \neq 0$ we find

$$\gamma_i \alpha_1^i = \gamma_i(\alpha' + (\alpha_1 - \alpha'))^i = \operatorname{it}_{\preccurlyeq}(\gamma_i)\alpha'^i + \dots \text{ (higher order terms)}.$$

The minimal order of these expressions is

$$\min_{\preccurlyeq}\{\underbrace{\operatorname{ord}_{\preccurlyeq}(\operatorname{it}_{\preccurlyeq}(\gamma_i)\alpha'^i)}_{\operatorname{ord}_{\preccurlyeq}(\gamma_i)+i\mathfrak{n}} \mid 0 \leq i \leq d \text{ and } \gamma_i \neq 0\} = \operatorname{ord}_{\preccurlyeq,\mathfrak{n}}(g).$$

Since $g(\alpha_1) = 0$ and $\alpha' \neq 0$ it follows that the terms of order $\mathrm{ord}_{\preccurlyeq,\mathfrak{n}}(g)$ must sum up to zero. In particular, there have to be at least two indices i s.t. the terms $\mathrm{it}_{\preccurlyeq}(\gamma_i)\alpha'^i$ are of order $\mathrm{ord}_{\preccurlyeq,\mathfrak{n}}(g)$. In other words, the $\mathfrak{n}$-th edge equation of g must be non-trivial and α' must be a root of it.

If we can make sure that the data in (4.1) implies that the $\mathfrak{n}$-th edge is linear of the form $\mathrm{it}_{\preccurlyeq}(\gamma_1)z + \mathrm{it}_{\preccurlyeq}(\gamma_0) = 0$ then α' is uniquely determined and easy to compute.

Condition 4.3 (Valid Representations of Type A). *With definitions as in* (4.3) *we require for valid representations of type A that either* $\gamma_0 = 0$ *or* $\mathrm{edge}_{\preccurlyeq,\mathfrak{n}}(g)$ *is linear.*

Now substitute $\alpha_0 \mapsto \alpha_0 + \alpha'$, $\alpha_1 \mapsto \alpha_1 - \alpha'$ and $g \mapsto g(z + \alpha')$. A careful analysis of the exponent structure shows that under the above condition $\mathrm{it}_{\preccurlyeq}(\gamma_1)$ doesn't change and Condition 4.3 remains valid. Hence we can repeat the argument and compute successively as many terms as needed.

Example 4.4. Let $f := z^6 - 3x_2z^4 - \frac{1}{64}x_1^2x_2^3z^3 + 3x_2^2z^2 - x_2^3$. Then f has a power series root α starting with $\alpha_0 = x_2^{1/2} + \frac{1}{8}x_1^{2/3}x_2$. We work with the degree graded lexicographical ordering $\preccurlyeq$. First we translate f as in (4.3):

$$f(z + \alpha_0) = z^6 + (-6x_2^{1/2} + \tfrac{3}{4}x_1^{2/3}x_2)z^5 +$$
$$(+12x_2 - \tfrac{15}{4}x_1^{2/3}x_2^{3/2} + \tfrac{15}{64}x_1^{4/3}x_2^2)z^4 +$$
$$(-8x_2^{3/2} + 6x_1^{2/3}x_2^2 - \tfrac{15}{16}x_1^{4/3}x_2^{5/2} + \tfrac{3}{128}x_1^2x_2^3)z^3 +$$
$$(-3x_1^{2/3}x_2^{5/2} + \tfrac{9}{8}x_1^{4/3}x_2^3 - \tfrac{9}{128}x_1^2x_2^{7/2} - \tfrac{9}{4096}x_1^{8/3}x_2^4)z^2 +$$
$$(-\tfrac{3}{8}x_1^{4/3}x_2^{7/2} + \tfrac{3}{64}x_1^2x_2^4 + \tfrac{9}{2048}x_1^{8/3}x_2^{9/2} - \tfrac{9}{16384}x_1^{10/3}x_2^5)z +$$
$$(-\tfrac{3}{1024}x_1^{8/3}x_2^5 + \tfrac{9}{16384}x_1^{10/3}x_2^{11/2} - \tfrac{7}{262144}x_1^4x_2^6)$$

We find that $f(z+\alpha_0)$ has a linear edge of slope $(\frac{4}{3}, \frac{3}{2})$ and extract the edge equation $-\frac{3}{8}x_1^{4/3}x_2^{7/2}z - \frac{3}{1024}x_1^{8/3}x_2^5 = 0$. The solution is the next term $-\frac{1}{128}x_1^{4/3}x_2^{3/2}$ in the expansion of α. Next we consider $f(z + \alpha_0 - \frac{1}{128}x_1^{4/3}x_2^{3/2})$ and find that it has a linear edge of slope $(\frac{8}{3}, \frac{5}{2})$. Solving the edge equation $-\frac{3}{8}x_1^{4/3}x_2^{7/2} + \frac{3}{262144}x_1^4x_2^6 = 0$ we find the next term $\frac{1}{32768}x_1^{8/3}x_2^{5/2}$, and so on:

$$\alpha = -x_2^{1/2} + \tfrac{1}{8}x_1^{2/3}x_2 - \tfrac{1}{128}x_1^{4/3}x_2^{3/2} + \tfrac{1}{32768}x_1^{8/3}x_2^{5/2} - \tfrac{1}{4194304}x_1^4x_2^{7/2} + \ldots$$

Obviously we do not need to know g completely to do this computation. More precisely, we can expand α up to order less than $\mathfrak{o}$, if we have approximated g sufficiently well. All the terms of order less than $\mathfrak{o}$ are determined by a linear edge equation of the form $\mathrm{it}_{\preccurlyeq}(\gamma_1)z + \cdots = 0$. Therefore, it is sufficient to know the constant term up to order less than $\mathrm{ord}_{\preccurlyeq,\mathfrak{o}}(\mathrm{it}_{\preccurlyeq}(\gamma_1)z) = \mathfrak{c} + \mathfrak{o}$ with $\mathfrak{c}$ as in (4.3). Hence, for approximating g it is sufficient to expand the coefficients of f up to order less than $\mathfrak{c} + \mathfrak{o}$.

For example, Condition 4.3 is true when considering a power series defined by the implicit function theorem. Therefore solving such equations is trivial:

Algorithm 9 `ImplicitFunction`$(g : \mathbb{E}_1[\![\underline{x}^{\Gamma_1}]\!][z]) : \mathbb{E}_1[\![\underline{x}^{\Gamma_1}]\!]$

Require: A polynomial g s.t. $g(0, \ldots, 0, 0) = 0$ and $\partial g/\partial z(0, \ldots, 0, 0) \neq 0$.
Ensure: The unique root α of g s.t. $\alpha(0, \ldots, 0) = 0$.
  1: **return** `Series`$(0, g)$;

Indeed, if g is equal to $\sum_{i=0}^{d} \gamma_i z^i$, $g(0,\ldots,0,0) = 0$ and $\partial g/\partial z(0,\ldots,0,0) \neq 0$ then $\mathrm{ord}_{\preccurlyeq}(\gamma_0) \succ 0$ (or $\gamma_0 = 0$) and $\mathrm{ord}_{\preccurlyeq}(\gamma_1) = 0$. If $\gamma_0 \neq 0$ then $\mathrm{edge}_{\preccurlyeq,\mathfrak{n}}(g)$ must be linear where $\mathfrak{n} = \mathrm{ord}_{\preccurlyeq}(\gamma_0) = \mathrm{ord}_{\preccurlyeq}(\alpha)$.

Remark 4.5 (Universality of Type A). Note that for any algebraic power series α there is, by definition, a squarefree polynomial f with polynomial coefficients vanishing on it. This implies that $f(z + \alpha)$ vanishes at $z = 0$ with multiplicity one or that the constant coefficient of $f(z+\alpha)$ is zero whereas its linear coefficient does not vanish. This means that the initial term of the linear coefficient is fixed if we consider translations $f(z + \alpha_0)$ by sufficiently large initial segments α_0 of α. As a consequence we can always find an initial segment α_0 s.t. Condition 4.3 is fulfilled and every algebraic power series is representable by a single node of type A.

So our representation is already universal. But computing efficiently the last operation of our requirement list is not easy in this representation. So for algorithmic purposes we also allow the second type of node.

The previous discussion showed how to expand power series represented by a graph consisting of nodes of type A. Since $\preccurlyeq$ is compatible with total degree this implies that we can expand such series up to arbitrary total degree. Now we consider a power series β represented by a tuple (4.2). Indeed what comes next is best explained in the total degree ordering.

Assume we want to expand β up to order less than $o \in \mathbb{Q}$. Therefore we first compute approximations $\widetilde{\xi}_i$ of the descendants ξ_i up to order less than o. Then we apply the map $\underline{x}^{\mathfrak{m}} \mapsto \prod_{1 \leq i \leq l} \widetilde{\xi}_i^{\mathfrak{n}_i(\mathfrak{m})}$ to each term in an expansion of α, sum up the intermediate results and finally truncate at order o. For this truncation to be correct, we have to use a sufficiently large expansion of α, say, up to order less than o'. The only remaining question is how to determine o' from o.

To this end let

$$(4.4) \qquad \widetilde{\mathfrak{n}} := \left(\sum_{1 \leq i \leq l} \mathrm{ord}_{\leq}(\xi_i)\, \mathfrak{n}_i \right) = (\widetilde{\mathfrak{n}}_1, \ldots, \widetilde{\mathfrak{n}}_n) \text{ and } c := \min_{\leq}\{\widetilde{\mathfrak{n}}_j \mid 1 \leq j \leq n\}$$

where $\mathrm{ord}_{\leq}(0) := \infty$. Let ϕ denote the homomorphism $\underline{x}^{\mathfrak{m}} \mapsto \prod_{1 \leq i \leq l} \xi_i^{\mathfrak{n}_i(\mathfrak{m})}$ then

$$\mathrm{ord}_{\leq}(\phi(\underline{x}^{\mathfrak{m}})) = \mathrm{ord}_{\leq}\left(\prod_{1 \leq i \leq l} \xi_i^{\mathfrak{n}_i(\mathfrak{m})} \right) = \left(\sum_{1 \leq i \leq l} \mathrm{ord}_{\leq}(\xi_i)\, \mathfrak{n}_i(\mathfrak{m}) \right) = \widetilde{\mathfrak{n}}(\mathfrak{m})$$

$$= \sum_{1 \leq j \leq n} \widetilde{\mathfrak{n}}_j \mathfrak{m}_j \geq \sum_{1 \leq j \leq n} c\mathfrak{m}_j = c|\mathfrak{m}|.$$

This calculation shows two things: First, if $c > 0$ then for any $\gamma = \sum_{\mathfrak{m}} \gamma_{\mathfrak{m}} \underline{x}^{\mathfrak{m}}$ the sum $\sum_{\mathfrak{m}} \gamma_{\mathfrak{m}} \phi(\underline{x}^{\mathfrak{m}})$ converges, so $\phi(\gamma)$ is well defined. This is an analogue to the usual condition when substituting formal power series into each other.

Condition 4.6 (Valid Representations of Type B). *For valid representations of type B we require $c > 0$ for c defined as in* (4.4).

Second, under this condition, if $\alpha = \sum_{\mathfrak{m}} \alpha_{\mathfrak{m}} \underline{x}^{\mathfrak{m}}$ then the terms $\alpha_{\mathfrak{m}} \underline{x}^{\mathfrak{m}}$ with $|\mathfrak{m}| \geq o/c$ contribute terms to $\phi(\alpha)$ of order greater or equal o, so we can choose $o' := o/c$.

Remark 4.7 (Contraction Constants). We can give a nice theoretical meaning to the two technical conditions and the deduced algorithms. Namely, the values $\mathfrak{c}$ and c may be understood as additive resp. multiplicative *contraction constants* for certain continuous maps between power series domains with the usual metrics. In the case of Condition 4.1 this map is contractive only in a small enough neighborhood

(determined by $\mathrm{ord}_{\preccurlyeq}(\alpha - \alpha_0)$) of the root α. Contractivity makes the represented series well-defined.

In both cases the constants determine how far the descendants of a node have to be expanded. An implementation could store them together with the representing tuples (4.1) and (4.2). We would also like to mention that for an efficient implementation it is *crucial to truncate intermediate results* (e.g. defining polynomials or approximations of descendants) as often as possible to a sufficient precision. The bounds are computed by similar calculations as above. We omit them from the presentation and show only the essentials of the algorithm.

4.3. **Rational Parametrizations for Quasi-Ordinary Polynomials.** A quite intricate thing is the computation of complete sets of rational parametrizations. In requirement (3) we have introduced the action of the group $\mathrm{hom}(\Gamma, \mathbb{E}^*)$ on $\mathbb{E}[\![\underline{x}^\Gamma]\!]$. We write this as a left action using again functional notation, *i.e.*, for $\sigma \in \mathrm{hom}(\Gamma, \mathbb{E}^*)$ and $\alpha \in \mathbb{E}[\![\underline{x}^\Gamma]\!]$ we simply write $\sigma(\alpha)$. This is an *exponent structure preserving* automorphism in the sense that $\mathrm{supp}_{\preccurlyeq}(\alpha) = \mathrm{supp}_{\preccurlyeq}(\sigma(\alpha))$. Let's convince ourselves that this action can effectively be carried out in our representation.

Remark 4.8 (Effectivity of Actions Induced by Lattice Homomorphisms). Since such an automorphism is structure preserving, it is easily computed in our representation: If a power series is represented by a tuple (4.1), then we apply the automorphism to the initial segment α_0 and to the coefficients of the defining equation f, possibly recursing to the descendants. If a power series is represented by a tuple (4.2), we apply the automorphism recursively to the ξ_i.

Definition 4.9 (Rational Parametrizations). We call (σ, α) with $\alpha \in \mathbb{E}_1[\![\underline{x}^{\Gamma_1}]\!]$ and $\sigma \in \mathrm{hom}(\Gamma_0, \mathbb{E}_1^*)$ a *parametrization* of a monic polynomial $f \in \mathbb{E}_0[\![\underline{x}^{\Gamma_0}]\!][z]$ iff $\mathbb{E}_0 \subseteq \mathbb{E}_1$, $\Gamma_0 \subseteq \Gamma_1$ and $\sigma^{\uparrow z}(f)(\alpha) = 0$. The *order* of the parametrization is defined to be $\mathrm{ord}_{\preccurlyeq}(\alpha)$.

Let $g | f$ be an irreducible factor s.t. $\sigma^{\uparrow z}(g)(\alpha) = 0$. We call (σ, α) *rational* if the induced homomorphism $\mathrm{IC}(\mathbb{E}_0[\![\underline{x}^{\Gamma_0}]\!][z]/\langle g \rangle) \to \mathbb{E}_1[\![\underline{x}^{\Gamma_1}]\!]$ which maps $z \mapsto \alpha$ and $\gamma \mapsto \sigma(\gamma)$ for $\gamma \in \mathbb{E}_0[\![\underline{x}^{\Gamma_0}]\!]$ is an isomorphism.

Intuitively, rational parametrizations are distinguished by minimal field and lattice extensions. The induced homomorphism exists due to the universal property of integrally closed domains. If this homomorphism is an isomorphism then the irreducible polynomial g from above at least has to be prime. (Mind that $\mathbb{E}_0[\![\underline{x}^{\Gamma_0}]\!]$ is in general no UFD!)

Remark 4.10 (Irreducible Monic Polynomials). Let $g \in \mathbb{E}_0[\![\underline{x}^{\Gamma_0}]\!][z]$ be a monic irreducible polynomial. We want to prove that g is prime. The following arguments are taken from [28]. It is sufficient to show primality in $\mathrm{QF}(\mathbb{E}_0[\![\underline{x}^{\Gamma_0}]\!])[z]$; Indeed, if $hg \in \mathbb{E}_0[\![\underline{x}^{\Gamma_0}]\!][z]$ for some $h \in \mathrm{QF}(\mathbb{E}_0[\![\underline{x}^{\Gamma_0}]\!])[z]$ then a Gaussian style inductive argument shows that $h \in \mathbb{E}_0[\![\underline{x}^{\Gamma_0}]\!][z]$. So $g\ \mathbb{E}_0[\![\underline{x}^{\Gamma_0}]\!][z] = (g\ \mathrm{QF}(\mathbb{E}_0[\![\underline{x}^{\Gamma_0}]\!])[z]) \cap \mathbb{E}_0[\![\underline{x}^{\Gamma_0}]\!][z]$, *i.e.*, it is the preimage of a prime ideal and therefore prime itself.

Let $g' \in \mathrm{QF}(\mathbb{E}_0[\![\underline{x}^{\Gamma_0}]\!])[z]$ be an irreducible (and hence prime) monic polynomial factor of g. We show $g' = g$. Being also roots of g, all roots of g' (in some splitting field) are integral over $\mathbb{E}_0[\![\underline{x}^{\Gamma_0}]\!]$. The coefficients of g' (being polynomials in these roots) are also integral over $\mathbb{E}_0[\![\underline{x}^{\Gamma_0}]\!]$ and elements of $\mathrm{QF}(\mathbb{E}_0[\![\underline{x}^{\Gamma_0}]\!])$. Then $g' \in \mathbb{E}_0[\![\underline{x}^{\Gamma_0}]\!][z]$ because $\mathbb{E}_0[\![\underline{x}^{\Gamma_0}]\!]$ is integrally closed. By the above argument $g'|g$ also in $\mathbb{E}_0[\![\underline{x}^{\Gamma_0}]\!][z]$ and so $g' = g$ because g is irreducible.

This also implies that a monic polynomial $f \in \mathbb{E}_0[\![\underline{x}^{\Gamma_0}]\!][z]$ has a unique (up to permutation) factorization into monic irreducibles.

Let now $f \in \mathbb{E}_0[\![\underline{x}^{\Gamma_0}]\!][z]$ be quasi-ordinary and assume we want to compute a *complete set of rational parametrizations*. Let's be more general and say we want

to compute a complete set of rational parametrizations of order greater than some value $\mathfrak{n}_0 \in \mathbb{Q}^n$. (With the choice $\mathfrak{n}_0 := (-1, \ldots, -1)$ this includes the original task.)

First assume we are given a parametrization (σ, α) of f s.t. $\alpha \neq 0$ and $\mathfrak{n} := \mathrm{ord}_{\preccurlyeq}(\alpha) \succ \mathfrak{n}_0$. Write $g := \sigma^{\uparrow z}(f)$ and $\alpha' := \mathrm{it}_{\preccurlyeq}(\alpha)$. By the same reasoning as in the beginning of Section 4.2 (with α in place of α_1), we find that the $\mathfrak{n}$-th edge equation of g must be non-trivial and α' must be a root of it.

Now assume we have to find (σ, α) as above using a recursive approach. As a first step we have to determine the initial term of α (up to some isomorphism). From the previous discussion it follows that its slope will be $\mathfrak{n} \succ \mathfrak{n}_0$ s.t. f has a non-trivial $\mathfrak{n}$-th edge equation. If the tuple (σ, α) is meant to be a rational parametrization, then we have to solve this equation economically, *i.e.*, using a field extension of least degree, and at the same time determine σ partially. Duval's trick [12] adapted to the multivariate case gives an optimal choice.

To this end let $\mathfrak{m}_i$ for $1 \leq i \leq n$ be a basis of Γ_0. Let $b \in \mathbb{Z}_{>0}$ be the size of Γ'/Γ_0 where $\Gamma' := \Gamma_0 + \mathbb{Z}\mathfrak{n}$, *i.e.*, b is minimal s.t. $b\mathfrak{n} \in \Gamma_0$. Now we can write

$$\mathrm{edge}_{\preccurlyeq, \mathfrak{n}}(f) = \sum_{l \leq i \leq k} f_i \underline{x}^{\mathfrak{m}_i} z^i = \underline{x}^{\mathfrak{m}_l} z^l \sum_{0 \leq j \leq (k-l)/b} f_{l+jb} \underline{x}^{-jb\mathfrak{n}} z^{jb}$$

with $f_l \neq 0$ and $f_k \neq 0$. Further we can express $b\mathfrak{n} = \sum_{1 \leq i \leq n} c_i \mathfrak{m}_i$, where necessarily $\gcd(b, c_1, \ldots, c_n) = 1$ since b was chosen minimally, and compute Bézout coefficients u and v_i s.t. $ub + \sum_{1 \leq i \leq n} v_i c_i = 1$. (Note that this choice is not unique.) If r is a *non-zero* root in a minimal field extension $\mathbb{E}'$ s.t.

$$\sum_{0 \leq j \leq (k-l)/b} f_{l+jb} r^j = 0$$

then we can define the homomorphism $\sigma' : \Gamma_0 \to \mathbb{E}'^* : \mathfrak{m}_i \mapsto r^{-v_i}$ and the initial term $\alpha' := r^u \underline{x}^{\mathfrak{n}}$. With these definitions one checks

$$\mathrm{edge}_{\preccurlyeq, \mathfrak{n}}(\sigma'^{\uparrow z}(f))(\alpha') = \sigma'^{\uparrow z}(\mathrm{edge}_{\preccurlyeq, \mathfrak{n}}(f))(r^u \underline{x}^{\mathfrak{n}})$$

$$= \sigma'(\underline{x}^{\mathfrak{m}_l}) z^l \sum_{0 \leq j \leq (k-l)/b} f_{l+jb} \sigma'(\underline{x}^{-jb\mathfrak{n}})(r^u \underline{x}^{\mathfrak{n}})^{jb}$$

$$= (\ldots) \sum_{0 \leq j \leq (k-l)/b} f_{l+jb} \left(\sigma'(\underline{x}^{-\sum_{1 \leq i \leq n} c_i \mathfrak{m}_i}) r^{ub} \underline{x}^{b\mathfrak{n}} \right)^j$$

$$= (\ldots) \sum_{0 \leq j \leq (k-l)/b} f_{l+jb} \left(r^{\sum_{1 \leq i \leq n} v_i c_i} \underline{x}^{-b\mathfrak{n}} r^{ub} \underline{x}^{b\mathfrak{n}} \right)^j$$

$$= (\ldots) \sum_{0 \leq j \leq (k-l)/b} f_{l+jb} \left(r^{ub + \sum_{1 \leq i \leq n} v_i c_i} \underline{x}^{-b\mathfrak{n} + b\mathfrak{n}} \right)^j$$

$$= (\ldots) \sum_{0 \leq j \leq (k-l)/b} f_{l+jb} r^j = 0.$$

This finishes the description of how to choose the first term (up to isomorphism) and part of the structure preserving automorphism. The remainder of course has to be chosen via recursion. More precisely, define $f' := \sigma'^{\uparrow z}(f)(z + \alpha')$ and compute a parametrization $(\sigma'', \alpha'') \in \hom(\Gamma', \mathbb{E}_1^*) \times \mathbb{E}_1[\![\underline{x}^{\Gamma_1}]\!]$ of f' with $\mathrm{ord}_{\preccurlyeq}(\alpha'') \succ \mathfrak{n}$. Then we may just set $\alpha := \sigma''(\alpha') + \alpha'' \in \mathbb{E}_1[\![\underline{x}^{\Gamma_1}]\!]$ and $\sigma := \sigma''\sigma' \in \hom(\Gamma_0, \mathbb{E}_1^*)$. (Note that we have an inclusion $\hom(\Gamma_0, \mathbb{E}'^*) \to \hom(\Gamma_0, \mathbb{E}_1^*)$ and a surjection $\hom(\Gamma', \mathbb{E}_1^*) \to \hom(\Gamma_0, \mathbb{E}_1^*)$, hence, we can build $\sigma''\sigma' \in \hom(\Gamma_0, \mathbb{E}_1^*)$.) Now trivially

$$0 = \sigma''^{\uparrow z}(f')(\alpha'') = \sigma''^{\uparrow z}(\sigma'^{\uparrow z}(f)(z + \alpha'))(\alpha'')$$
$$= \sigma''^{\uparrow z}(\sigma'^{\uparrow z}(f))(z + \sigma''(\alpha'))(\alpha'') = \sigma''^{\uparrow z}(\sigma'^{\uparrow z}(f))(\sigma''(\alpha') + \alpha'') = \sigma^{\uparrow z}(f)(\alpha).$$

Example 4.11. Let $f_0 := z^6 + 3x_2z^4 + x_1^2x_2^3z^3 + 3x_2^2z^2 + x_2^3$. Its discriminant is $\text{disc}_z(f_0) = 729x_1^8x_2^{21}(x_1^4x_2^3 - 64)$ and, hence, it is quasi-ordinary. We again use the degree graded lexicographical ordering $\preccurlyeq$.

The only rational slope of a non-trivial edge is $\mathfrak{n}_1 := (0, \frac{1}{2})$ with edge equation $z^6 + 3x_2z^4 + 3x_2^2z^2 + x_2^3 = 0$. We see that only even powers of z have a non-vanishing coefficient which corresponds to the fact that $2\mathfrak{n}_1 \in \mathbb{Z}^2$, *i.e.*, $b_1 = 2$. Let r_1 be a solution of $0 = r^3 + 3r^2 + 3r + 1 = (r+1)^3$, hence, $r_1 = -1$. The standard lattice has basis $\mathfrak{m}_{1,1} = (1,0)$ and $\mathfrak{m}_{1,2} = (0,1)$. Then $2\mathfrak{n}_{1,1} = 0\mathfrak{m}_{1,1} + 1\mathfrak{m}_{1,2}$, hence, $c_{1,1} = 0$ and $c_{1,2} = 1$. One verifies the Bézout relation $0b_1 + 0c_{1,1} + 1c_{1,2} = 1$ and we have $u_1 = 0$, $v_{1,1} = 0$ and $v_{1,2} = 1$. Therefore we define the first term $\alpha_1 := r_1^{u_1}x_2^{1/2} = x_2^{1/2}$ and the homomorphism to be $\sigma_1 : \mathfrak{m}_{1,1} \mapsto r_1^{-v_{1,1}} = 1, \mathfrak{m}_{1,2} \mapsto r_1^{-v_{1,2}} = -1$ with corresponding action $x_1 \mapsto x_1, x_2 \mapsto -x_2$. We set

$$f_1 := \sigma_1^{\uparrow z}(f_0)(z + x_2^{\frac{1}{2}}) =$$
$$z^6 + 6x_2^{\frac{1}{2}}z^5 + 12x_2z^4 + (8x_2^{\frac{3}{2}} - x_1^2x_2^3)z^3 - 3x_1^2x_2^{\frac{7}{2}}z^2 - 3x_1^2x_2^{\frac{8}{2}}z - x_1^2x_2^{\frac{9}{2}}.$$

For f_1 we now find two rational slopes of non-trivial edges, namely, $\mathfrak{n}_1$ from above and $\mathfrak{n}_2 = (\frac{2}{3}, 1)$. The extended exponent lattice at this point is $\mathbb{Z}\mathfrak{m}_{2,1} + \mathbb{Z}\mathfrak{m}_{2,2}$ where $\mathfrak{m}_{2,1} = (1,0)$ and $\mathfrak{m}_{2,2} = (0, \frac{1}{2})$. We have $3\mathfrak{n}_2 = 2\mathfrak{m}_{2,1} + 6\mathfrak{m}_{2,2}$, *i.e.*, $b_2 = 3$, $c_{2,1} = 2$ and $c_{2,2} = 6$. From a Bézout relation we get $u_2 = 1$, $v_{2,1} = -1$ and $v_{2,2} = 0$. The edge equation is $8x_2^{3/2}z^3 - x_1^2x_2^{9/2} = 0$. Let r_2 be the root of $8r - 1 = 0$, *i.e.*, $r_2 = \frac{1}{8}$. Hence, we define a new homomorphism $\sigma_2 : \mathfrak{m}_{2,1} \mapsto r_2^{-v_{2,1}} = \frac{1}{8}, \mathfrak{m}_{2,2} \mapsto r_2^{-v_{2,2}} = 1$ with action $x_1 \mapsto \frac{1}{8}x_1, x_2^{1/2} \mapsto x_2^{1/2}$. We also define a new initial segment $\alpha_2 := \sigma_2(\alpha_1) + r_2^{u_2}x_1^{2/3}x_2 = x_2^{1/2} - \frac{1}{8}x_1^{2/3}x_2$ and set $f_2 := \sigma_2^{\uparrow z}(f_1)(z - \frac{1}{8}x_1^{2/3}x_2)$.

From now on the edge equation will always be linear and we have determined a parametrization. More precisely, the overall automorphism is $\sigma_2\sigma_1$ and acts by $x_1 \mapsto \frac{1}{8}x_1, x_2 \mapsto -x_2$. The power series starts with α_2 and is a root of $\sigma_2\sigma_1^{\uparrow z}(f_0)$. We have seen its expansion in Example 4.4.

This discussion yields the following algorithm. The return type $\overline{\mathbb{E}_0}[\![\underline{x}^{\mathbb{Q}^n}]\!]$ means algebraic power series with coefficients in some finite algebraic extension $\mathbb{E}_0$ and exponents in some rational lattice containing $\mathbb{Z}^n$.

Algorithm 10 $\texttt{ParamRec}(f : \mathbb{E}_0[\![\underline{x}^{\Gamma_0}]\!][z], \mathfrak{n}_0 \in \mathbb{Q}^n) : 2^{\hom(\Gamma_0, \overline{\mathbb{E}_0}^*) \times \overline{\mathbb{E}_0}[\![\underline{x}^{\mathbb{Q}^n}]\!]}$

Require: A quasi-ordinary polynomial f and an order $\mathfrak{n}_0$.
Ensure: A set of rational parametrizations of f of order greater $\mathfrak{n}_0$.
1: $S := \{\mathfrak{n} \in \mathbb{Q}_{\geq 0}^n \mid \mathfrak{n} \succ \mathfrak{n}_0 \text{ and } \text{edge}_{\preccurlyeq,\mathfrak{n}}(f) \text{ is non-trivial}\}$; $\mathcal{P} := \emptyset$;
2: **if** $(\forall \mathfrak{n} \in S : \text{ord}_z(\text{edge}_{\preccurlyeq,\mathfrak{n}}(f)) \geq 1)$ or $(\exists \mathfrak{n} \in S : \deg_z(\text{edge}_{\preccurlyeq,\mathfrak{n}}(f)) = 1)$ **then**
3: $\quad S := S \setminus \{\mathfrak{n} \in S \mid \deg_z(\text{edge}_{\preccurlyeq,\mathfrak{n}}(f)) = 1\}$; $\mathcal{P} := \mathcal{P} \cup \{(1, \texttt{Series}(0, f))\}$;
4: **for** $\mathfrak{n} \in S$ **do**
5: $\quad$ Let $b \in \mathbb{Z}_{>0}$ be minimal s.t. $b\mathfrak{n} \in \Gamma_0$; Let $\mathfrak{m}_i$ for $1 \leq i \leq n$ be a basis of Γ_0;
6: $\quad$ Write $b\mathfrak{n} = \sum_{1 \leq i \leq n} c_i\mathfrak{m}_i$ and compute $u, v_i \in \mathbb{Z}$ s.t. $ub + \sum_{1 \leq i \leq n} v_ic_i = 1$;
7: $\quad$ Write $\text{edge}_{\preccurlyeq,\mathfrak{n}}(f) = \underline{x}^{\mathfrak{m}_l}z^l \sum_{0 \leq j \leq k} f_j\underline{x}^{-jb\mathfrak{n}}z^{jb}$ with $f_0 \neq 0$ and $f_k \neq 0$;
8: $\quad R := \texttt{ZeroSet}(\langle \sum_{0 \leq j \leq k} f_jz^j \rangle)$;
9: $\quad$ **for** $r \in R$ **do**
10: $\quad\quad \alpha' := r^u\underline{x}^{\mathfrak{n}}$; $\sigma' : \Gamma_0 \to \mathbb{E}'^* : \mathfrak{m}_i \mapsto r^{-v_i}$; {assuming $r \in \mathbb{E}'^*$}
11: $\quad\quad \mathcal{P} := \mathcal{P} \cup \textbf{map}_{(\sigma'', \alpha'') \mapsto (\sigma''\sigma', \sigma''(\alpha') + \alpha'')}\texttt{ParamRec}(\sigma'^{\uparrow z}(f)(z + \alpha'), \mathfrak{n})$;
12: **return** $\mathcal{P}$;

For the definition of the auxiliary function `ZeroSet` see Remark 3.15. Applying structure preserving automorphisms and translating the defining polynomial in z preserves quasi-ordinariness. Therefore the arguments to the recursive call always fit to the input description. Although the algorithm never makes explicit use of Theorem A.5 (the Theorem of Jung-Abhyankar) it depends crucially on f being quasi-ordinary. For example, the power series constructed in line 3 are well-defined in that case; Otherwise there might not be any power series root of f which is supported on the positive orthant and whose initial term is a root of the linear edge of f. Recursion in this algorithm ends when the set S is empty when entering line 4. Termination is assured by the very argument of Remark 4.5.

Remark 4.12 (And a Little Bit of Engineering...). In line 1 of the above algorithm we compute the "Newton Polygon" of $f = \sum_i \varphi_i z^i$. Since f is monic, one of the non-trivial edges contains the point $((0, \ldots, 0), \deg_z(f))$. Now z divides f either with multiplicity 0 or 1 (because of squarefreeness). So for computing the non-trivial edges it will be enough to expand the coefficients φ_i until the initial term of φ_1 or φ_0 appears depending on whether z divides f or not. In other words we would have to check, whether $\varphi_0 = 0$. In principle this is possible, see Remark 4.2, but from the point of efficiency it is not advisable.

On the other hand it doesn't matter if z divides f or if f has a linear edge equation (compare to the condition in line 2). In both cases we return `Series`$(0, f)$ which might be zero. So an engineering solution might be to compute either all non-trivial edges or only a set of non-trivial edges with lowest vertex at linear level and make sure that the constant term (if existent) has large enough order.

Another approach would be to modify the above algorithm to allow approximate input with polynomial coefficients only but also include error reporting when an approximation was not accurate enough.

Further it is advisable to choose a short vector $(u, v_1, \ldots, v_n) \in \mathbb{Z}^{n+1}$ using for example the LLL-algorithm. For practical purposes the additional complexity is negligible compared to the grow of coefficients if a larger vector is chosen.

We didn't include the technical tricks into the description because the algorithm is easier to read and to argue about when written up as above.

Setting now $\mathfrak{n}_0 := (-1, \ldots, -1)$ we get a set of parametrizations of f:

Algorithm 11 `Param`$(f : \mathbb{E}_0[\![\underline{x}^{\Gamma_0}]\!][z]) : 2^{\hom(\Gamma_0, \overline{\mathbb{E}_0}^*) \times \overline{\mathbb{E}_0}[\![\underline{x}^{\mathbb{Q}^n}]\!]}$

Require: A quasi-ordinary polynomial f.
Ensure: A complete set of rational parametrizations of f.
  1: **return** `ParamRec`$(f, (-1, \ldots, -1))$;

We have to show that the computed parametrizations are rational and complete.

Lemma 4.13 (Bounding Extensions). *Let Algorithm 10 be called with a quasi-ordinary polynomial $f \in \mathbb{E}_0[\![\underline{x}^{\Gamma_0}]\!][z]$ and $\mathfrak{n}_0 \in \mathbb{Q}^n$ and write $(\sigma_i, \alpha_i) \in \hom(\Gamma_0, \mathbb{E}_i^*) \times \mathbb{E}_i[\![\underline{x}^{\Gamma_i}]\!]$ for the computed parametrizations. Then we may bound the extensions from above by*

$$\sum_i [\mathbb{E}_i : \mathbb{E}_0] \ \#(\Gamma_i/\Gamma_0) \leq \max\{\deg_z(\mathrm{edge}_{\preccurlyeq, \mathfrak{n}}(f)) \mid \mathfrak{n} \succ \mathfrak{n}_0\}.$$

Proof. Assume the condition in line 2 holds. Then either f has a zero root, *i.e.*, $z | f$ or we have found a linear edge equation. In both cases we construct one parametrization of f as in line 3. The involved series is an element of $\mathbb{E}_0[\![\underline{x}^{\Gamma_0}]\!]$ and the lattice remains unchanged. This parametrization contributes a summand 1 to the lefthand side of the inequality.

Now set $d := \max\{\deg_z(\text{edge}_{\preccurlyeq,\mathfrak{n}}(f)) \mid \mathfrak{n} \succ \mathfrak{n}_0\} - 1$ if the condition in line 2 was true, $d := \max\{\deg_z(\text{edge}_{\preccurlyeq,\mathfrak{n}}(f)) \mid \mathfrak{n} \succ \mathfrak{n}_0\}$ otherwise. We have to ensure that the sum modified by running only over the parametrizations constructed in the loop is bounded from above by d. To this end assume that S contains o slopes $\mathfrak{n}_j$ when entering line 4. Let ℓ_j denote the height of the edge equation of slope $\mathfrak{n}_j$, *i.e.*, the difference of its z-degree and its z-order. Then $\sum_{1 \le j \le o} \ell_j \le d$.

Fix an edge, *i.e.*, a value of j. Then we compute an integer b_j in line 5 and a number of roots $r_{j,k} \in \mathbb{E}_{j,k}$ with multiplicities, say, $m_{j,k}$ for $1 \le k \le s_j$ in line 8. It follows that $b_j = \#(\Gamma_j / \Gamma_0)$ with $\Gamma_j := \Gamma_0 + \mathbb{Z}\mathfrak{n}_j$ measures the extension of the exponent lattice and $\ell_j = b_j(\sum_{1 \le k \le s_j}[\mathbb{E}_{j,k} : \mathbb{E}_0] \, m_{j,k})$.

Fix a root, *i.e.*, a value of k and let $f_{j,k}$ be the polynomial used as parameter in the recursive call in line 11. Now $m_{j,k}$ is also the multiplicity of the root of the corresponding edge equation. After translation zero becomes an $m_{j,k}$-fold root, hence, the z-order of $\text{edge}_{\preccurlyeq,\mathfrak{n}_j}(f_{j,k})$ is equal to $m_{j,k}$. This can serve as an upper bound in the statement for the recursive call, which returns, say, $t_{j,k}$ different parametrizations.

Assuming that the lemma is true for recursive calls (see $(*)$ below) one computes:

$$d \ge \sum_{1 \le j \le o} \ell_j = \sum_{1 \le j \le o} b_j \sum_{1 \le k \le s_j} [\mathbb{E}_{j,k} : \mathbb{E}_0] \, m_{j,k}$$

$$\overset{(*)}{\ge} \sum_{1 \le j \le o} \#(\Gamma_j/\Gamma_0) \sum_{1 \le k \le s_j} [\mathbb{E}_{j,k} : \mathbb{E}_0] \sum_{1 \le l \le t_{j,k}} [\mathbb{E}_{j,k,l} : \mathbb{E}_{j,k}] \, \#(\Gamma_{j,k,l}/\Gamma_j)$$

$$= \sum_{1 \le j \le o} \sum_{1 \le k \le s_j} \sum_{1 \le l \le t_{j,k}} [\mathbb{E}_{j,k,l} : \mathbb{E}_{j,k}][\mathbb{E}_{j,k} : \mathbb{E}_0] \, \#(\Gamma_{j,k,l}/\Gamma_j)\#(\Gamma_j/\Gamma_0)$$

$$= \sum_{1 \le j \le o} \sum_{1 \le k \le s_j} \sum_{1 \le l \le t_{j,k}} [\mathbb{E}_{j,k,l} : \mathbb{E}_0] \, \#(\Gamma_{j,k,l}/\Gamma_0)$$

For each tuple of indices (j, k, l) appearing in that sum, the loop now produces exactly one parametrization with coefficient field $\mathbb{E}_{j,k,l}$ and exponent lattice $\Gamma_{j,k,l}$. $\square$

For what follows we assume that $\mathbb{E}_0 \subseteq \mathbb{E}_i \subseteq \overline{\mathbb{E}_0}$. A parametrization $(\sigma_i, \alpha_i) \in \hom(\Gamma_0, \mathbb{E}_i^*) \times \mathbb{E}_i[\![\underline{x}^{\Gamma_i}]\!]$ is very close to a root of f in $\overline{\mathbb{E}_0}[\![\underline{x}^{\Gamma_i}]\!]$. It provided a root if we could reverse the effects of σ_i. Precisely, let $\tau \in \hom(\Gamma_i, \overline{\mathbb{E}_0})$ be an extension of the inverse of σ_i to Γ_i, in other words, $\tau|_{\Gamma_0} = \sigma_i^{-1}$. Then we call $\beta := \tau(\alpha_i)$ an *associated root* to (σ_i, α_i), because applying τ to the equation $0 = \sigma_i^{\uparrow z}(f)(\alpha_i)$ yields $0 = (\tau\sigma_i)^{\uparrow z}(f)(\tau(\alpha_i)) = (\sigma_i^{-1}\sigma_i)^{\uparrow z}(f)(\beta) = f(\beta)$. It is not hard to show that σ_i^{-1} can always be extended to $\hom(\Gamma_i, \overline{\mathbb{E}_0})$ because $\overline{\mathbb{E}_0}$ is algebraically closed.

The next lemma says, that we do not miss any associated roots.

Lemma 4.14 (Completeness). *Let Algorithm 10 be called with a quasi-ordinary polynomial $f \in \mathbb{E}_0[\![\underline{x}^{\Gamma_0}]\!][z]$ and $\mathfrak{n}_0 \in \mathbb{Q}^n$ and write $(\sigma_i, \alpha_i) \in \hom(\Gamma_0, \mathbb{E}_i^*) \times \mathbb{E}_i[\![\underline{x}^{\Gamma_i}]\!]$ for the computed parametrizations. Then each root $\beta \in \overline{\mathbb{E}_0}[\![\underline{x}^{\mathbb{Q}^n}]\!]$ of f with $\text{ord}_{\preccurlyeq}(\beta) \succ \mathfrak{n}_0$ is associated to at least one (σ_i, α_i).*

Proof. Let β be a root of f of order $\mathfrak{n} \succ \mathfrak{n}_0$. If $\beta = 0$ or if $\beta \ne 0$ and $\text{edge}_{\preccurlyeq,\mathfrak{n}}(f)$ is a linear equation then we consider the parametrization constructed in line 3: The involved series is already β and the involved automorphism is the identity.

Otherwise assume the outer loop is processing slope $\mathfrak{n}$, set $\Gamma' := \Gamma_0 + \mathbb{Z}\mathfrak{n}$ and write $\beta = \beta' + \beta''$ where $\beta' := \text{it}_{\preccurlyeq}(\beta)$. Then β' must be a root of $\text{edge}_{\preccurlyeq,\mathfrak{n}}(f)$. Setting $\beta' = o\underline{x}^{\mathfrak{n}}$ for some $o \in \overline{\mathbb{E}_0}$ we have that $r := o^b$ is a root of $\sum_{0 \le j \le k} f_j z^j$, compare line 8.

Assume now we are in the inner loop processing this $r \in \mathbb{E}'^*$ and let $f' := \sigma'^{\uparrow z}(f)(z + \alpha')$ be the polynomial in the arguments to the recursive call in line 11. Let $\tau' \in \hom(\Gamma', \overline{\mathbb{E}_0})$ be defined via $\tau'|_{\Gamma_0} = \sigma'^{-1}$ and $\mathfrak{n} \mapsto r^{-u}o$. We have to check that this is well-defined, more precisely, since $b\mathfrak{n} \in \Gamma_0$ (with b minimal) we must have that $(r^{-u}o)^b$ coincides with $\sigma'^{-1}(b\mathfrak{n})$; Indeed

$$(r^{-u}o)^b = r^{1-bu} = r^{\sum_{1 \le i \le n} v_i c_i} = \prod_{1 \le i \le n}(r^{v_i})^{c_i} = \sigma'^{-1}(\textstyle\sum_{1 \le i \le n} c_i \mathfrak{m}_i) = \sigma'^{-1}(b\mathfrak{n}).$$

In particular $\tau'(\alpha') = \tau'(r^u \underline{x}^{\mathfrak{n}}) = o\underline{x}^{\mathfrak{n}} = \beta'$ and applying τ'^{-1} to $0 = f(\beta)$ we get $0 = (\tau'^{-1})^{\uparrow z}(f)(\tau'^{-1}(\beta') + \tau'^{-1}(\beta'')) = (\sigma')^{\uparrow z}(f)(\alpha' + \tau'^{-1}(\beta'')) = f'(\tau'^{-1}(\beta''))$. So $\tau'^{-1}(\beta'')$ is a root of f' of order greater $\mathfrak{n}$.

Assuming that the statement holds for the recursive call, we get a parametrization $(\sigma'', \alpha'') \in \hom(\Gamma_0, \mathbb{E}''^*) \times \mathbb{E}''[\![\underline{x}^{\Gamma''}]\!]$ which is associated to $\tau'^{-1}(\beta'')$ via, say, τ'' with $\tau''|_{\Gamma'} = \sigma''^{-1}$. This is combined to a returned parametrization $(\sigma''\sigma', \sigma''(\alpha') + \alpha'')$. We claim that this parametrization is associated to β via $\tau'\tau''$. Indeed $\tau'\tau''$ restricts to the inverse of $\sigma''\sigma'$:

$$(\tau'\tau'')|_{\Gamma_0} = (\tau'|_{\Gamma_0})(\tau''|_{\Gamma_0}) = \sigma'^{-1}(\sigma''^{-1}|_{\Gamma_0}) = (\sigma''\sigma')^{-1}$$

It remains to show that it maps $\sigma''(\alpha') + \alpha''$ to β:

$$\tau'\tau''(\sigma''(\alpha') + \alpha'') = \tau'(\tau''\sigma'')(\alpha') + \tau'(\tau''(\alpha'')) =$$
$$\tau'(\sigma''^{-1}\sigma'')(\alpha') + \tau'(\tau'^{-1}(\beta'')) = \tau'(\alpha') + \beta'' = \beta' + \beta'' = \beta \quad \square$$

Now if β_1 and β_2 are roots of f associated to (σ_i, α_i) via τ_1 and τ_2, then $\tau_1 \tau_2^{-1}$ restricts to the identity in $\hom(\Gamma_0, \overline{\mathbb{E}_0})$, hence, maps Γ_0 to 1. In other words $\tau_1 \tau_2^{-1}$ acts as an automorphism on $\overline{\mathbb{E}_0}[\![\underline{x}^{\Gamma_i}]\!]$ fixing $\overline{\mathbb{E}_0}[\![\underline{x}^{\Gamma_0}]\!]$. Therefore, the roots which are associated to one and the same parametrization are all conjugate and, hence, roots of the same irreducible factor. This gives an injection from the irreducible factors (with roots of order greater $\mathfrak{n}_0$) to parametrizations (of order greater $\mathfrak{n}_0$).

Corollary 4.15 (Complete Sets of Rational Parametrizations). *Let Algorithm 11 be called with a quasi-ordinary polynomial $f \in \mathbb{E}_0[\![\underline{x}^{\Gamma_0}]\!][z]$ and write $(\sigma_i, \alpha_i) \in \hom(\Gamma_0, \mathbb{E}_i^*) \times \mathbb{E}_i[\![\underline{x}^{\Gamma_i}]\!]$ for the computed parametrizations, then:*
- $\deg_z(f) = \sum_i [\mathbb{E}_i : \mathbb{E}_0] \ \#(\Gamma_i/\Gamma_0)$
- *All computed parametrizations are rational and in bijective correspondence with the irreducible factors of f.*

Proof. To show this, we apply the above two lemmata with $\mathfrak{n}_0 := (-1, \ldots, -1)$ each. In Lemma 4.13, clearly, $\deg_z(f)$ is an upper bound for the righthand side of the inequality, so $\deg_z(f) \ge \sum_i [\mathbb{E}_i : \mathbb{E}_0] \ \#(\Gamma_i/\Gamma_0)$.

Now let $f_j | f$ be the irreducible factors. By Lemma 4.14 and the previous discussion we may assume that there is an injection $j \mapsto i_j$ s.t. f_j is parametrized by $(\sigma_{i_j}, \alpha_{i_j})$. Then we have chains of field inclusions

$$\mathrm{QF}(\mathbb{E}_0[\![\underline{x}^{\Gamma_0}]\!]) \subseteq \mathrm{QF}(\mathbb{E}_0[\![\underline{x}^{\Gamma_0}]\!][z]/\langle f_j \rangle) \subseteq \mathrm{QF}(\mathbb{E}_{i_j}[\![\underline{x}^{\Gamma_{i_j}}]\!]),$$

where the second inclusion is given by $(\sigma_{i_j}, \alpha_{i_j})$. The extensions are algebraic of degrees $[\mathrm{QF}(\mathbb{E}_0[\![\underline{x}^{\Gamma_0}]\!][z]/\langle f_j \rangle) : \mathrm{QF}(\mathbb{E}_0[\![\underline{x}^{\Gamma_0}]\!])] = \deg_z(f_j)$ respectively $[\mathrm{QF}(\mathbb{E}_{i_j}[\![\underline{x}^{\Gamma_{i_j}}]\!]) : \mathrm{QF}(\mathbb{E}_0[\![\underline{x}^{\Gamma_0}]\!])] = [\mathbb{E}_{i_j} : \mathbb{E}_0] \ \#(\Gamma_{i_j}/\Gamma_0)$ and therefore

$$\deg_z(f) = \sum_j \deg_z(f_j) \le \sum_j [\mathbb{E}_{i_j} : \mathbb{E}_0] \ \#(\Gamma_{i_j}/\Gamma_0) \le \sum_i [\mathbb{E}_i : \mathbb{E}_0] \ \#(\Gamma_i/\Gamma_0).$$

Together we have proven equality. In fact, since all summands are positive we find that the map $j \mapsto i_j$ is a bijection and for each chain of inclusions as above equality of degrees must hold. This gives the second statement. $\square$

5. Conclusion

We have introduced the concept of formal desingularizations and shown how to compute them for hypersurfaces of $\mathbb{P}^3_{\mathbb{E}}$. The algorithm has been implemented and found to run very well. We can compute formal desingularizations faster by magnitudes than the general algorithms for desingularization. The reason is that our algorithm doesn't depend on Groebner basis computations. It relies only on linear algebra and polynomial factorization.

Here, we would like to point out an application of our algorithm. Namely, formal desingularizations can be used to compute adjoint sheaves. We will describe how to do that in another paper. Adjoint sheaves in arbitrary dimension are defined to be the direct image of the tensor powers of the canonic sheaf w.r.t. an arbitrary desingularization. Adjoint spaces for projective schemes (*i.e.*, graded components of the associated graded ring to that sheaf) are the keystone to the rational parametrization of curves. In [32] it has been shown that they are of equal importance for the computation of rational surface parametrizations. For example, they facilitate the computation of the arithmetic genus and the plurigenera of the surface. Thus, we can effectively check Castelnuovo's Criterion for the parametrizability of surfaces. Moreover, adjoint spaces can be used to construct certain rational maps that reduce the parametrization problem to a set of base cases. The final goal is an efficient implementation to rationally parametrize hypersurface in $\mathbb{P}^3_{\mathbb{Q}}$ (with or without introducing field extensions).

We finish with an open problem. With our current definition, a formal desingularization is just a loosely related set of formal prime divisors. For some applications, however, it would be nice to know the dual graph of the surface desingularization, *i.e.*, an annotated graph with one vertex for each exceptional divisor and edges whenever two divisors intersect. Such a graph could be the starting point for an algorithm to compute the minimal formal desingularization. In our method it would be easy to keep track of the dual graph of the embedded curve desingularization and in a certain sense the dual graph of the resolution projects to it. Such graph coverings have been studied in [30, 31]. The problem is that we get formal prime divisors from two sources, namely, Algorithm 4 and Algorithm 6. However, it is not clear how the corresponding prime divisors intersect.

The algorithm of this paper as well as the method for the computation of adjoint spaces is available as a `Magma`-package and can be downloaded via this link:

<center>http://www.ricam.oeaw.ac.at/software/symcomp/adjoints.tar.gz</center>

It will probably become part of the next major `Magma`-release.

Acknowledgment

Appendix A. Some Local Algebra

In this appendix we gather a few results from local commutative algebra and present them in a form suitable for our needs. Again $\mathbb{E}$ denotes a field of characteristic zero which need not be algebraically closed. We are dealing with completions of stalks of regular schemes of finite type over $\mathbb{E}$. Therefore we first give a famous structure theorem in this setting. Recall that an *essentially finite* local $\mathbb{E}$-algebra is the localization of a finitely generated $\mathbb{E}$-algebra at a prime ideal.

Theorem A.1 (Cohen Structure Theorem). *Let $(\widehat{A}, \mathfrak{m})$ be the completion of an essentially finite, regular, local $\mathbb{E}$-algebra of Krull dimension s. Set $\mathbb{F}_0 := \widehat{A}/\mathfrak{m}$ with canonic projection $\pi : \widehat{A} \to \mathbb{F}_0$. Further let*

- $\{u_i\}_{1 \leq i \leq r} \subset \widehat{A}$ *be a set projecting to a transcendence basis of* $\mathbb{F}_0$ *over* $\mathbb{E}$ *and*
- $\{v_j\}_{1 \leq j \leq s} \subset \mathfrak{m}$ *a minimal set of generators.*

Then there is a unique coefficient field $\mathbb{F} \subseteq \widehat{A}$ *containing* $\mathbb{E}$ *and* $\{u_i\}_{1 \leq i \leq r}$ *s.t.* π *restricts to an isomorphism* $\mathbb{F} \to \mathbb{F}_0$ *and*

$$\mathbb{F}[\![x_1, \ldots, x_s]\!] \to \widehat{A} : \begin{cases} f \mapsto f & \text{for } f \in \mathbb{F}, \\ x_j \mapsto v_j & \text{for } 1 \leq j \leq s \end{cases}$$

is also an isomorphism.

Proof. The existence of a unique field $\mathbb{F}$ fulfilling the first assertion is the content of [27, Thm. 28.3] and its proof (where references to differential bases can be substituted by transcendence bases in characteristic zero). Since $\{v_j\}_{1 \leq j \leq s}$ is a set of generators for $\mathfrak{m}$ one easily sees that the homomorphism in the second assertion is surjective, *cf.* [2, Lem. 10.23]. The rings on both sides have the same dimension. Therefore the kernel must be trivial by [2, Cor. 11.18]. □

We actually need a constructive version of a kind of inverse of the above isomorphism in a special case.

Corollary A.2 (Completion at Points in Affine n-Space). *Let* $\mathfrak{p} := \langle f_1, \ldots, f_r \rangle \subset \mathbb{E}[x_1, \ldots, x_n]$ *be a prime ideal of height* $l \leq \min(r, n)$,

$$\mathcal{J} := \frac{\partial(f_1, \ldots, f_r)}{\partial(x_1, \ldots, x_n)} \in \mathbb{E}[x_1, \ldots, x_n]^{r \times n}$$

the Jacobian matrix, $\mathbb{F}_0 := \mathrm{QF}(\mathbb{E}[x_1, \ldots, x_n]/\mathfrak{p})$ *the residue field,* $\pi : \mathbb{E}[x_1, \ldots, x_n] \to \mathbb{F}_0$ *the canonic projection and*

$$\phi : \mathbb{E}[x_1, \ldots, x_n] \to \mathbb{F}_0[t_1, \ldots, t_l] : x_i \mapsto \pi(x_i) + M_i(t_1, \ldots, t_l)^T,$$

where M_i *are row vectors with entries in* $\{0, 1\}$. *Write* $M := (M_i)_{1 \leq i \leq n}$.

Then ϕ *extends uniquely to a homomorphism* $\mathbb{E}[\widehat{x_1, \ldots, x_n}]_{\mathfrak{p}} \to \mathbb{F}_0[\![t_1, \ldots, t_l]\!]$. *Moreover we can choose* M *s.t.* $\pi(\mathcal{J})M \in \mathbb{F}_0^{r \times l}$ *has rank* l *and then the extended homomorphism becomes an isomorphism.*

Proof. The homomorphism ϕ trivially extends to $\mathbb{F}_0[\![t_1, \ldots, t_l]\!]$. Then for any $g \in \mathbb{E}[x_1, \ldots, x_n]$ one computes for the image

$$\phi(g) \in \pi(g) + \pi(\partial g/\partial(x_1, \ldots, x_n))M(t_1, \ldots, t_l)^T + \mathfrak{m}^2$$

where $\mathfrak{m} := \langle t_1, \ldots, t_l \rangle$. Now the above equation shows that if $g \in \mathbb{E}[x_1, \ldots, x_n] \setminus \mathfrak{p}$ then we have $\pi(g) \neq 0$ for the constant part. Therefore the image is a unit and the homomorphism lifts uniquely to $\mathbb{E}[x_1, \ldots, x_n]_{\mathfrak{p}}$. Impose the $\mathfrak{p}$-adic topology on the domain and the $\mathfrak{m}$-adic topology on the codomain. Writing down the long expansion one sees that the homomorphism is even uniformly continuous. Since the codomain is already complete we have a unique lifting to $\mathbb{E}[\widehat{x_1, \ldots, x_n}]_{\mathfrak{p}}$.

Since $\mathbb{E}[x_1, \ldots, x_n]$ is regular the Jacobian image $\pi(\mathcal{J})$ has rank l equal to the height of the prime. Let $(j_1, \ldots, j_l)$ be the column indices of a non-vanishing $l \times l$-minor and choose $M := (e_{j_1}, \ldots, e_{j_l})$. Here e_j denotes the column vector with 1 in position j and 0 otherwise. Since multiplication by M extracts exactly the columns of this minor also $\pi(\mathcal{J})M$ has rank l.

Applying the above formula to the components of the vector $(f_1, \ldots, f_r)^T$ of generators of $\mathfrak{p}$ we find that its π-image is of the form

$$\underbrace{(\pi(f_1), \ldots, \pi(f_r))^T}_{=(0, \ldots, 0)} + \underbrace{\pi(\mathcal{J})M(t_1, \ldots, t_l)^T}_{=:L(f_1, \ldots, f_r)} + \text{(higher order terms)}.$$

The rank condition assures that the components of $L(f_1, \ldots, f_r)$ generate $\mathfrak{m}/\mathfrak{m}^2$ as $\mathbb{F}_0$-vector space. Hence $\mathfrak{m} = \langle \phi(f_1), \ldots, \phi(f_r) \rangle$ by Nakayama's lemma.

Now let $\mathbb{F} \subseteq \mathbb{E}[\widehat{x_1, \ldots, x_n}]_{\mathfrak{p}}$ be a coefficient field in the sense of Theorem A.1., *i.e.*, restricting the canonic projection to $\mathbb{F}$ gives an isomorphism

$$\mathbb{F} \cong \mathbb{E}[\widehat{x_1, \ldots, x_n}]_{\mathfrak{p}} / \mathfrak{p}\mathbb{E}[\widehat{x_1, \ldots, x_n}]_{\mathfrak{p}} \cong \mathbb{F}_0.$$

But then also $\phi(\mathbb{F})$ is a coefficient field of $\mathbb{F}_0[\![t_1, \ldots, t_l]\!]$. Now we proceed as in the proof of Theorem A.1. The paragraph above shows that ϕ is surjective and comparing dimensions one proves injectivity. $\qquad\square$

To show correctness of our algorithms we need that completion commutes with two common operations, namely, building the integral closure and computing the blow up algebra.

Lemma A.3 (Integral Closure and Completion)**.** *Let A be a finitely generated $\mathbb{E}$-algebra, $f \in A[z]$ a monic polynomial, $\mathfrak{p} \subset A$ a prime ideal and consider the following diagram:*

$$\begin{array}{ccc} \mathrm{IC}(A[z]/\langle f \rangle) & \longrightarrow & \mathrm{IC}(\widehat{A_{\mathfrak{p}}}[z]/\langle f \rangle) \\ \uparrow & & \uparrow \\ \\ A & \longrightarrow & \widehat{A_{\mathfrak{p}}} \end{array}$$

Then $\mathfrak{q} \mapsto \mathfrak{q}' := \mathfrak{q}\,\mathrm{IC}(\widehat{A_{\mathfrak{p}}}[z]/\langle f \rangle)$ gives a bijective correspondence between prime ideals $\mathfrak{q} \subset \mathrm{IC}(A[z]/\langle f \rangle)$ above $\mathfrak{p}$ and prime ideals $\mathfrak{q}' \subset \mathrm{IC}(\widehat{A_{\mathfrak{p}}}[z]/\langle f \rangle)$ above $\mathfrak{p}\widehat{A_{\mathfrak{p}}}$, and the induced homomorphisms $\mathrm{IC}(\widehat{A[z]/\langle f \rangle})_{\mathfrak{q}} \to \mathrm{IC}(\widehat{A_{\mathfrak{p}}[z]/\langle f \rangle})_{\mathfrak{q}'}$ are isomorphisms.

Proof. The fact that building the integral closure and completion commutes is known as Zariski's Main Theorem, see, *e.g.*, [40, Thm. VIII.33]. $\qquad\square$

Lemma A.4 (Blowing up and Completion)**.** *Let A be a finitely generated $\mathbb{E}$-algebra, $\mathfrak{p} \subset A$ a prime ideal and consider the diagram*

$$\begin{array}{ccc} B & \longrightarrow & B' := \widehat{A_{\mathfrak{p}}} \otimes_A B \\ \uparrow & & \uparrow \\ \\ A & \longrightarrow & \widehat{A_{\mathfrak{p}}} \end{array}$$

where B is a coordinate ring of an affine chart of the blow up of $\operatorname{Spec} A$ at $\mathfrak{p}$.

Then B' is a coordinate ring of an affine chart of the blow up of $\operatorname{Spec} \widehat{A_{\mathfrak{p}}}$ at $\mathfrak{m}\widehat{A_{\mathfrak{p}}}$. Further $\mathfrak{q} \mapsto \mathfrak{q}' := \mathfrak{q}B'$ gives a bijective correspondence between prime ideals $\mathfrak{q} \subset B$ above $\mathfrak{p}$ and prime ideals $\mathfrak{q}' \subset B'$ above $\mathfrak{m}\widehat{A_{\mathfrak{p}}}$, and the induced homomorphisms $\widehat{B_{\mathfrak{q}}} \to \widehat{B'_{\mathfrak{q}'}}$ are isomorphisms.

Proof. This is an algebraic transcription of [23, Prop. A.14.7] which holds analogously for ground fields which are not algebraically closed. $\qquad\square$

Finally we state the theorem which provides the theoretical basis for the whole formal desingularization procedure.

Theorem A.5 (Theorem of Jung-Abhyankar)**.** *Let $f \in \mathbb{E}[\![x_1, \ldots, x_n]\!][z]$ be a monic, squarefree polynomial s.t. $\mathrm{disc}_z(f) = x_1^{e_1} \cdots x_m^{e_m} u(x_1, \ldots, x_n)$ where $m \leq n$ and $u(0, \ldots, 0) \neq 0$. Then there is a natural number $d \geq 1$ and there are $\deg_z(f)$ distinct power series $\alpha_i \in \overline{\mathbb{E}}[\![x_1^{1/d}, \ldots, x_m^{1/d}, x_{m+1}, \ldots, x_n]\!]$ solving f, i.e., $f(x_1, \ldots, x_n, \alpha_i) = 0$ for $1 \leq i \leq \deg_z(f)$.*

Proof. An irreducible factor of f must again be monic and its discriminant must be a factor of $\text{disc}_z(f)$, hence, can also be written as above. Now the statement can be found in [23, Prop. 3.2.5]. □

References

1. María E. Alonso, Teo Mora, and Mario Raimondo, *A computational model for algebraic power series*, J. Pure Appl. Algebra **77** (1992), no. 1, 1–38.
2. Michael F. Atiyah and Ian G. Macdonald, *Introduction to commutative algebra*, Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969.
3. Tobias Beck and Josef Schicho, *Approximate Roots in Graded Rings*, Tech. Report 2005-03, RICAM, March 2005.
4. Frédéric Beringer and Françoise Richard-Jung, *Multi-variate polynomials and Newton-Puiseux expansions*, Symbolic and numerical scientific computation (Hagenberg, 2001), Lecture Notes in Comput. Sci., vol. 2630, Springer, Berlin, 2003, pp. 240–254.
5. Edward Bierstone and Pierre D. Milman, *A simple constructive proof of canonical resolution of singularities*, Effective methods in algebraic geometry (Castiglioncello, 1990), Progr. Math., vol. 94, Birkhäuser Boston, Boston, MA, 1991, pp. 11–30.
6. Gábor Bodnár and Josef Schicho, *A computer program for the resolution of singularities*, Resolution of singularities (Obergurgl, 1997), Progr. Math., vol. 181, Birkhäuser, Basel, 2000, pp. 231–238.
7. Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, Computational algebra and number theory (London, 1993). MR MR1484478
8. Antonio Campillo and José I. Farrán, *Symbolic Hamburger-Noether expressions of plane curves and applications to AG codes*, Math. Comp. **71** (2002), no. 240, 1759–1780 (electronic).
9. Vincent Cossart, Jean Giraud, and Ulrich Orbanz, *Resolution of surface singularities*, Lecture Notes in Mathematics, vol. 1101, Springer-Verlag, Berlin, 1984, With an appendix by H. Hironaka.
10. David A. Cox, *Toric varieties and toric resolutions*, Resolution of singularities (Obergurgl, 1997), Progr. Math., vol. 181, Birkhäuser, Basel, 2000, pp. 259–284.
11. Theo de Jong, *An algorithm for computing the integral closure*, JSC **26** (1998), 273–277.
12. Dominique Duval, *Rational Puiseux expansions*, Compositio Math. **70** (1989), no. 2, 119–154.
13. David Eisenbud, *Commutative algebra*, Graduate Texts in Mathematics, vol. 150, Springer-Verlag, New York, 1995, With a view toward algebraic geometry.
14. Anne Frühbis-Krüger and Gerhard Pfister, *Practical aspects of algorithmic resolution of singularities*, Reports on Computer Algebra, no. 33, Centre for Computer Algebra, University of Kaiserslautern, October 2004, Online available at http://www.mathematik.uni-kl.de/ zca.
15. William Fulton, *Introduction to toric varieties*, Annals of Mathematics Studies, vol. 131, Princeton University Press, Princeton, NJ, 1993, The William H. Roever Lectures in Geometry.
16. Gert-Martin Greuel and Gerhard Pfister, *A **Singular** introduction to commutative algebra*, Springer-Verlag, Berlin, 2002, With contributions by Olaf Bachmann, Christoph Lossen and Hans Schönemann, With 1 CD-ROM (Windows, Macintosh, and UNIX).
17. Gaétan Haché and Dominique Le Brigand, *Effective construction of algebraic geometry codes*, IEEE Trans. Inform. Theory **41** (1995), no. 6, part 1, 1615–1628, Special issue on algebraic geometry codes.
18. Robin Hartshorne, *Algebraic geometry*, Springer-Verlag, New York, 1977, Graduate Texts in Mathematics, No. 52.
19. Herwig Hauser, *The Hironaka theorem on resolution of singularities (or: A proof we always wanted to understand)*, Bull. Amer. Math. Soc. (N.S.) **40** (2003), no. 3, 323–403 (electronic).
20. Heisuke Hironaka, *Resolution of singularities of an algebraic variety over a field of characteristic zero. I, II*, Ann. of Math. (2) 79 (1964), 109–203; ibid. (2) **79** (1964), 205–326.
21. Friedrich Hirzebruch, *Über vierdimensionale Riemannsche Flächen mehrdeutiger analytischer Funktionen von zwei komplexen Veränderlichen*, Math. Ann. **126** (1953), 1–22.
22. H. W. E. Jung, *Darstellung der Funktionen eines algebraischen Körpers zweier unabhängigen Veränderlichen x, y in der Umgebung x = a, y = b*, J. für Math. **133** (1908), 289–314 (German).
23. Karl-Heinz Kiyek and José L. Vicente, *On the Jung-Abhyankar theorem*, Arch. Math. (Basel) **83** (2004), no. 2, 123–134.
24. János Kollár, *Lectures on resolution of singularities*, Annals of Mathematics Studies, vol. 166, Princeton University Press, Princeton, NJ, 2007.

25. Henry B. Laufer, *Normal two-dimensional singularities*, Princeton University Press, Princeton, N.J., 1971, Annals of Mathematics Studies, No. 71.
26. Joseph Lipman, *Rational singularities, with applications to algebraic surfaces and unique factorization*, Inst. Hautes Études Sci. Publ. Math. (1969), no. 36, 195–279.
27. Hideyuki Matsumura, *Commutative ring theory*, second ed., Cambridge Studies in Advanced Mathematics, vol. 8, Cambridge University Press, Cambridge, 1989, Translated from the Japanese by M. Reid.
28. Stephen McAdam, *Unique factorization of monic polynomials*, Comm. Algebra **29** (2001), no. 10, 4341–4343.
29. John McDonald, *Fiber polytopes and fractional power series*, J. Pure Appl. Algebra **104** (1995), no. 2, 213–233.
30. András Némethi, *Resolution graphs of some surface singularities. I. Cyclic coverings*, Singularities in algebraic and analytic geometry (San Antonio, TX, 1999), Contemp. Math., vol. 266, Amer. Math. Soc., Providence, RI, 2000, pp. 89–128.
31. András Némethi and Ágnes Szilárd, *Resolution graphs of some surface singularities. II. Generalized Iomdin series*, Singularities in algebraic and analytic geometry (San Antonio, TX, 1999), Contemp. Math., vol. 266, Amer. Math. Soc., Providence, RI, 2000, pp. 129–164.
32. Josef Schicho, *Rational parametrization of surfaces*, J. Symbolic Comput. **26** (1998), no. 1, 1–29.
33. Mark Spivakovsky, *Valuations in function fields of surfaces*, Amer. J. Math. **112** (1990), no. 1, 107–156.
34. Joris van der Hoeven, *Relax, but don't be too lazy*, JSC **34** (2002), 479–542.
35. _____, *Transseries and real differential algebra*, Springer-Verlag, Berlin, 2006, Lecture Notes in Mathematics, Vol. 1888.
36. Mark van Hoeij, *An algorithm for computing an integral basis in an algebraic function field*, J. Symbolic Comput. **18** (1994), no. 4, 353–363.
37. Orlando Villamayor, *Constructiveness of Hironaka's resolution*, Ann. Sci. École Norm. Sup. (4) **22** (1989), no. 1, 1–32.
38. Robert J. Walker, *Reduction of the singularities of an algebraic surface*, Ann. of Math. (2) **36** (1935), no. 2, 336–365.
39. _____, *Algebraic curves*, Springer-Verlag, New York, 1978, Reprint of the 1950 edition.
40. Oscar Zariski and Pierre Samuel, *Commutative algebra. Vol. II*, Springer-Verlag, New York, 1975, Reprint of the 1960 edition, Graduate Texts in Mathematics, No. 29.

TOBIAS BECK, SYMBOLIC COMPUTATION GROUP, JOHANN RADON INSTITUTE FOR COMPUTATIONAL AND APPLIED MATHEMATICS, AUSTRIAN ACADEMY OF SCIENCES, ALTENBERGERSTRASSE 69, A-4020 LINZ, AUSTRIA

E-mail address: `Tobias.Beck@ricam.oeaw.ac.at`