Local to global algorithms for the Gorenstein adjoint ideal of a curve

Janko Böhm and Wolfram Decker and Santiago Laplagne and Gerhard Pfister

Abstract We present new algorithms for computing adjoint ideals of curves and thus, in the planar case, adjoint curves. With regard to terminology, we follow Gorenstein who states the adjoint condition in terms of conductors. Our main algorithm yields the Gorenstein adjoint ideal $\mathfrak{G}$ of a given curve as the intersection of what we call local Gorenstein adjoint ideals. Since the respective local computations do not depend on each other, our approach is inherently parallel. Over the rationals, further parallelization is achieved by a modular version of the algorithm which first computes a number of the characteristic p counterparts of $\mathfrak{G}$ and then lifts these to characteristic zero. As a key ingredient, we establish an efficient criterion to verify the correctness of the lift. Well-known applications are the computation of Riemann-Roch spaces, the construction of points in moduli spaces, and the parametrization of rational curves. We have implemented different variants of our algorithms together with Mnuk's approach in the computer algebra system SINGULAR and give timings to compare the performance.

Janko Böhm
Fachbereich Mathematik, Universität Kaiserslautern, Postfach 3049, D-67653 Kaiserslautern, Germany, e-mail: boehm@mathematik.uni-kl.de

Wolfram Decker
Fachbereich Mathematik, Universität Kaiserslautern, Postfach 3049, D-67653 Kaiserslautern, Germany, e-mail: decker@mathematik.uni-kl.de

Santiago Laplagne
Departamento de Matemática, Facultad de Ciencias Exactas y Naturales, (1428) Pabellón I - Ciudad Universitaria, Buenos Aires, Argentina, e-mail: slaplagn@dm.uba.ar

Gerhard Pfister
Fachbereich Mathematik, Universität Kaiserslautern, Postfach 3049, D-67653 Kaiserslautern, Germany, e-mail: pfister@mathematik.uni-kl.de

1 Introduction

In classical algebraic geometry, starting from Riemann's paper on abelian functions [56], the adjoint curves of an irreducible plane curve Γ have been used as an essential tool in the study of the geometry of Γ. The defining property of an *adjoint curve* is that it passes with "sufficiently high" multiplicity through the singularities of Γ. There are several ways of making this precise, developed in classical papers by [15], [17, 1893], and [54], and in more recent work by [37, 28] and [60, 43]. We refer to [42],[30], [31], and [21] for results comparing the different notions: whereas the adjoint condition given by Brill and Noether is more restrictive, the notions of adjoint curves given by the other authors above coincide.

In this paper, we always consider adjoint curves in the less restrictive sense. In fact, we rely on Gorenstein's algebraic definition which states the adjoint condition at a singular point $P \in \Gamma$ by considering the conductor of the local ring $\mathcal{O}_{\Gamma,P}$ in its normalization. It is a well-known consequence of Max Noether's Fundamentalsatz that the adjoint curves of any given degree m cut out, residual to a fixed divisor supported on the singular locus of Γ, a complete linear series. Of fundamental importance is the case $m = \deg\Gamma - 3$ which, as shown by Gorenstein, yields the canonical series.

The ideal generated by the defining forms of the adjoint curves of Γ is called the *adjoint ideal* of Γ. In [2], the concept of adjoint ideals is extended to the non-planar case: consider a non-degenerate integral curve $\Gamma \subset \mathbb{P}^r_k = \mathrm{Proj}(S)$, and let I be a saturated homogeneous ideal of S properly containing the ideal of Γ. Then I is an adjoint ideal of Γ if its homogeneous elements of degree $m \gg 0$ cut out, residual to a fixed divisor whose support contains the singular locus, a complete linear series. As pointed out in [2], the existence of adjoint ideals is implicit in classical papers: examples are the Castelnuovo adjoint ideal and the Petri adjoint ideal. In [21], it is shown that Gorenstein's condition leads to the largest possible adjoint ideal, supported on the singular locus and containing all other adjoint ideals, and referred to as the *Gorenstein adjoint ideal* $\mathfrak{G} = \mathfrak{G}(\Gamma)$. See [21] for some remarks on how the different concepts of adjoint ideals compare in the non-planar case.

With regard to practical applications, adjoint curves enter center stage in the classical Brill-Noether algorithm for computing Riemann-Roch spaces, which in turn can be used to construct Goppa codes (see [46]). Furthermore, linear series cut out by adjoint curves allow us to construct explicit examples of smooth curves via singular plane models; a typical application is the experimental study of moduli spaces of curves. If the geometric genus of a plane curve Γ is zero, then the adjoint curves of degree $\deg\Gamma - 2$ specify a birational map to a rational normal curve. Based on this, we can find an explicit parametrization of Γ over its field of definition, starting either from the projective line or a conic. See [6] and the implementation in the SINGULAR library [9]. Algorithms for parametrization, in turn, have applications in computer aided design, for example, to compute intersections of curves with other algebraic varieties. See also [58].

A well-known algorithm for computing the Gorenstein adjoint ideal $\mathfrak{G} = \mathfrak{G}(\Gamma)$ in the planar case is due to [52]. This algorithm makes use of linear algebra to

obtain $\mathfrak{G}$ from an integral basis for the normalization $\overline{k[C]}$, where C is an affine part of Γ containing all singularities of Γ. Efficient ways of finding integral bases rely on Puiseux series techniques (see [61], [12]). This somewhat limits Mnuk's approach to characteristic zero. The same applies to the algorithm of [41], which also computes the Gorenstein adjoint ideal of a plane curve from an integral basis of $\overline{k[C]}$. The approach of [53], on the other hand, is limited to curves with ordinary multiple points only.

In this paper, we present a new algorithm for computing $\mathfrak{G}$. This algorithm is highly efficient and not restricted to the planar case, special types of singularities, or to characteristic zero. The basic idea is to compute $\mathfrak{G}$ as the intersection of "local Gorenstein ideals", one for each singular point of Γ. Each local ideal is obtained via Gröbner bases, starting from a "local contribution" to the normalization $\overline{k[C]}$ at the respective singular point. To find these contributions, we use the algorithm from [7] which is a local variant of the normalization algorithm designed in [33].

Our approach is already faster per se. In addition, it can take advantage of handling special classes of singularities in an ad hoc way. Above all, it is inherently parallel. For input over the rationals, further parallelization is achieved by a modular version of the algorithm which first computes a number of characteristic p counterparts of $\mathfrak{G}$ and then lifts these to characteristic zero. This allows us, in addition, to avoid intermediate coefficient growth over the rationals. To apply the general rational reconstruction scheme from [10], we prove an efficient criterion to verify the correctness of the lift. Note that the local-to-global approach is particularly useful when combined with modular methods: By Chebotarev's density theorem [19], the primes p for which the singular locus decomposes over $\mathbb{F}_p$ have positive density among all primes, provided the singular locus is decomposable over $\overline{\mathbb{Q}}$.

Our paper is organized as follows: In Section 2, we discuss algorithmic normalization. In Section 3, we review the definition of adjoint ideals and some related facts. In Section 4, we describe global algorithmic approaches to obtain $\mathfrak{G}$. We first discuss Mnuk's approach. Then we describe a global approach which relies on normalization and Gröbner bases. In Sections 5 and 6, we present our local to global algorithm for finding $\mathfrak{G}$ via normalization and Gröbner bases. Section 7 pays particular attention to the planar case, commenting on the direct treatment of special types of singularities. In Sections 8 and 9, we discuss the modular version of our algorithm. Finally, in Section 10, we compare the performance of the different approaches, relying on our implementations in the computer algebra system SINGULAR, and running various examples coming from algebraic geometry.

2 Algorithms for normalization

We begin with some general remarks on normalization and the role played by the conductor. For these, let A be any reduced Noetherian ring, and let $\mathrm{Q}(A)$ be its total ring of fractions. Then $\mathrm{Q}(A)$ is again a reduced Noetherian ring. We write

$$\mathrm{Spec}(A) = \{P \subset A \mid P \text{ prime ideal}\}$$

for the *spectrum* of A. The *vanishing locus* of an ideal J of A is the set $V(J) = \{P \in \mathrm{Spec}(A) \mid P \supset J\}$.

The *normalization* of A, written $\overline{A}$, is the integral closure of A in $\mathrm{Q}(A)$. We call A *normalization-finite* if $\overline{A}$ is a finite A-module, and we call A *normal* if $A = \overline{A}$.

We denote by

$$N(A) = \{P \in \mathrm{Spec}(A) \mid A_P \text{ is not normal}\}$$

the *non-normal locus* of A, and by

$$\mathrm{Sing}(A) = \{P \in \mathrm{Spec}(A) \mid A_P \text{ is not regular}\}$$

the *singular locus* of A.

Remark 1. Note that $N(A) \subset \mathrm{Sing}(A)$. Equality holds if A is of pure dimension one. Indeed, a Noetherian local ring of dimension one is normal iff it is regular (see [26, Thm. 4.4.9]).

Definition 1. If $R \subset S$ is an extension of rings, the *conductor* of A in B is

$$\mathscr{C}_{S/R} = \mathrm{Ann}_R(S/R) = \{r \in R \mid rS \subset R\}.$$

Note that $\mathscr{C}_{S/R}$ is the largest ideal of R which is also an ideal of S.

Remark 2. Specializing to the normalization, we write

$$\mathscr{C}_A = \mathscr{C}_{\overline{A}/A} = \mathrm{Ann}_A(\overline{A}/A) = \{a \in A \mid a\overline{A} \subset A\}.$$

Note that $\mathscr{C}_A$ can be naturally identified with $\mathrm{Hom}_A(\overline{A}, A)$ (see [62, Lemma 2.4.2]).

Lemma 1. *We have $N(A) \subset V(\mathscr{C}_A)$. Furthermore, A is normalization-finite iff $\mathscr{C}_A$ contains a non-zerodivisor of A. In this case, $N(A) = V(\mathscr{C}_A)$.*

Proof. See [36, Lemmas 3.6.1, 3.6.3].

Remark 3 (Splitting of Normalization). Finding the normalization can be reduced to the case of integral domains: If $P_1 \ldots, P_s$ are the minimal primes of A, then

$$\overline{A} \cong \overline{A/P_1} \times \cdots \times \overline{A/P_s}$$

(see [26, Thm. 1.5.20]).

Remark 4. Let k be a field. An *affine k-domain* is a finitely generated k-algebra which is an integral domain. By Emmy Noether's finiteness theorem (see [27, Cor. 13.13]), any such domain is normalization-finite, and its normalization is an affine k-domain as well. Geometrically, by gluing, this implies that any integral algebraic variety X over k admits a (unique) *normalization map* $\pi : \overline{X} \to X$, where π

is a finite morphism and, hence, the normal scheme $\overline{X}$ is an algebraic variety over k as well (see, for example, [47, Sec. 4.1.2]). Specifically, by Remark 1, if Γ is an integral algebraic curve over k, we get the *nonsingular model* $\pi : \overline{\Gamma} \to \Gamma$.

Definition 2. A homomorphism $A \to B$ of reduced Noetherian rings is called *normal* if it is flat and if for every $P \in \operatorname{Spec}(A)$ and every field extension L of A_P/PA_P, the ring $B \otimes_A L$ is normal.

Remark 5 (Base Change). Let $\ell \subset k$ be a separable field extension, and let A be a finitely generated reduced ℓ-algebra. Then $A \to A \otimes_\ell k$ is a normal homomorphism, so that $\overline{A} \otimes_\ell k$ is a normal ring (see [62, Propositions 19.1.1, 19.1.2, Thm. 19.4.2]). On the other hand, by [62, Thm. 19.5.1], we may identify $\overline{A} \otimes_\ell k$ with the integral closure of $A \otimes_\ell k$ in $\mathrm{Q}(A) \otimes_\ell k$. In turn, since every non-zerodivisor of A is a non-zerodivisor of $A \otimes_\ell k$, we may regard $\mathrm{Q}(A) \otimes_\ell k$ as a subring of $\mathrm{Q}(A \otimes_\ell k)$, and thus $\overline{A} \otimes_\ell k$ as a subring of $\overline{A \otimes_\ell k}$. Since $\overline{A} \otimes_\ell k$ is already normal, we conclude that $\overline{A \otimes_\ell k} = \overline{A} \otimes_\ell k$. In particular,

$$\begin{aligned}\mathscr{C}_{A\otimes_\ell k} &\cong \operatorname{Hom}_{A\otimes_\ell k}(\overline{A \otimes_\ell k}, A \otimes_\ell k) = \operatorname{Hom}_{A\otimes_\ell k}(\overline{A} \otimes_\ell k, A \otimes_\ell k) \\ &= \operatorname{Hom}_{A\otimes_\ell k}(\overline{A} \otimes_A (A \otimes_\ell k), A \otimes_A (A \otimes_\ell k)) \cong \operatorname{Hom}_A(\overline{A}, A) \otimes_\ell k \\ &\cong \mathscr{C}_A \otimes_\ell k\end{aligned}$$

(see [27, Prop. 2.10] for the second to last identity).

Now, we briefly discuss algorithmic normalization. We begin by recalling the normalization algorithm of Greuel, Laplagne, and Seelisch [33], which is an improvement of de Jong's algorithm (see [25], [22]). This algorithm, to which we refer as the GLS Algorithm, is based on the normality criterion of Grauert and Remmert. To state this criterion, we need:

Lemma 2. *Let A be a reduced Noetherian ring, and let $J \subset A$ be an ideal which contains a non-zerodivisor g of A. Then:*

1. *If $\varphi \in \operatorname{Hom}_A(J,J)$, the fraction $\varphi(g)/g \in \overline{A}$ is independent of the choice of g, and φ is multiplication by $\varphi(g)/g$.*
2. *There are natural inclusions of rings*

$$A \subset \operatorname{Hom}_A(J,J) \cong \frac{1}{g}(gJ :_A J) \subset \overline{A} \subset Q(A),\ a \mapsto \varphi_a,\ \varphi \mapsto \frac{\varphi(g)}{g},$$

where φ_a is multiplication by a.

Proof. See [36, Lemmas 3.6.1, 3.6.3].

Proposition 1 (Grauert and Remmert Criterion). *Let A be a reduced Noetherian ring, and let $J \subset A$ be a radical ideal which contains a non-zerodivisor g of A and satisfies $V(\mathscr{C}_A) \subset V(J)$. Then A is normal iff $A \cong \operatorname{Hom}_A(J,J)$ via the map which sends a to multiplication by a.*

Proof. See [29], [36, Prop. 3.6.5].

Definition 3. A pair (J,g) as in the proposition is called a *test pair* for A, and J is called a *test ideal* for A.

If k is a field and A is an affine k-domain, then test pairs exist by Lemma 1 and Emmy Noether's finiteness theorem. If, in addition, k is perfect, an explicit test pair can be found by applying the Jacobian criterion (see [27, Thm. 16.19] for this criterion). In fact, in this case, we may choose the radical of the Jacobian ideal M together with any non-zero element g of M as a test pair. Given a test pair (J,g), the basic idea of finding $\overline{A}$ is to enlarge A by a sequence of finite extensions of affine k-domains

$$A_{i+1} = \mathrm{Hom}_{A_i}(J_i,J_i) \cong \frac{1}{g}(gJ_i :_{A_i} J_i) \subset \overline{A} \subset \mathrm{Q}(A),$$

with $A_0 = A$ and test ideals $J_i = \sqrt{JA_i}$, until the Grauert and Remmert criterion allows one to stop. According to [33], each A_i can be represented as a quotient $\frac{1}{d_i}U_i \subset \mathrm{Q}(A)$, where $U_i \subset A$ is an ideal and $d_i \in U_i$ is non-zero. In this way, all computations except those of the radicals J_i may be carried through in A.

Example 1. For

$$A = \mathbb{C}[x,y] = \mathbb{C}[X,Y]/\langle X^5 - Y^2\,(Y-1)^3\rangle,$$

the radical of the Jacobian ideal is

$$J := \langle x, y\,(y-1)\rangle_A\,,$$

so that we can take (J,x) as a test pair. Then, in its first step, the normalization algorithm yields

$$A_1 = \frac{1}{x}U_1 = \frac{1}{x}\left\langle x, y(y-1)^2\right\rangle_A.$$

In the next steps, we get

$$A_2 = \frac{1}{x^2}U_2 = \frac{1}{x^2}\left\langle x^2, xy(y-1), y(y-1)^2\right\rangle_A$$

and

$$A_3 = \frac{1}{x^3}U_3 = \frac{1}{x^3}\left\langle x^3, x^2y(y-1), xy(y-1)^2, y^2(y-1)^2\right\rangle_A.$$

In the final step, we find that A_3 is normal and, hence, equal to $\overline{A}$.

Next, we describe the local to global variant of the GLS algorithm given in [7]. This variant is a considerable enhancement of the algorithm which serves as a motivation for our local to global approach to compute the Gorenstein adjoint ideal. It is based on the following two observations from [7]: First, the normalization $\overline{A}$ can be computed as the sum of local contributions $A \subset A^{(i)} \subset \overline{A}$, and second, local contributions can be obtained efficiently by a local variant of the GLS algorithm. For our purposes, it is enough to present the relevant results in a special case. Here,

as usual, if P is a prime of a ring R, and M is an R-module, we write M_P for the localization of M at $R \setminus P$.

Proposition 2. *Let A be an affine domain of dimension one over a field k, and let $\mathrm{Sing}(A) = \{P_1, \ldots, P_s\}$ be its singular locus. For $i = 1, \ldots, s$, let an intermediate ring $A \subset A^{(i)} \subset \overline{A}$ be given such that $A^{(i)}_{P_i} = \overline{A_{P_i}}$. Then*

$$\sum_{i=1}^{s} A^{(i)} = \overline{A}.$$

Proof. See [7, Prop. 15].

Definition 4. A ring $A^{(i)}$ as above is called a *local contribution* to $\overline{A}$ at P_i. It is called a *minimal local contribution* if $A^{(i)}_{P_j} = A_{P_j}$ for $j \neq i$.

The computation of local contributions is based on the modified version of the Grauert and Remmert criterion below:

Proposition 3. *Let A be an affine domain of dimension one over a field k, let $A \subset A'$ be a finite ring extension, let $P \in \mathrm{Sing}(A)$, and let $J' = \sqrt{PA'}$. If*

$$A' \cong \mathrm{Hom}_{A'}(J', J')$$

via the map which sends a' to multiplication by a', then A'_P is normal.

Proof. See [7, Prop. 16].

Considering an affine domain A of dimension one over a perfect field k, let $P \in \mathrm{Sing}(A)$. Choose P together with a non-zero element $g \in P$ instead of a test pair as in Definition 3. Then, proceeding as before, we get a chain of affine k-domains

$$A \subset A_1 \subset \cdots \subset A_m \subset \overline{A}$$

such that A_m is a local contribution to $\overline{A}$ at P.

Remark 6. Given A as above, a finite ring extension $A \subset A'$, and a prime $P \in \mathrm{Sing}(A)$, let $Q \in \mathrm{Sing}(A)$ be a prime different from P, and let $J' = \sqrt{PA'}$. Then

$$\begin{aligned} \mathrm{Hom}_{A'}(J', J')_Q &\cong \mathrm{Hom}_{A'_Q}(J'_Q, J'_Q) \\ &\cong \mathrm{Hom}_{A'_Q}(A'_Q, A'_Q) \cong A'_Q \end{aligned}$$

(see [27, Proposition 2.10] for the first identity). Inductively, this shows that the algorithm outlined above computes a minimal local contribution to $\overline{A}$ at P. Note that such a contribution is uniquely determined since, by definition, its localization at each $Q \in \mathrm{Spec}(A)$ is determined.

Example 2. In Example 1, there are two singularities, namely $P_1 = \langle x, y\rangle$ and $P_2 = \langle x, y-1\rangle$. Geometrically, these are a singularity of type A_4 at $(0,0)$ and a 3-fold point of type E_8 at $(0,1)$. For P_1, the local normalization algorithm yields $\overline{A_{P_1}} = (\frac{1}{d_1}U_1)_{P_1}$, where

$$d_1 = x^2 \text{ and } U_1 = \left\langle x^2,\ y(y-1)^3\right\rangle_A.$$

For P_2, we get $\overline{A_{P_2}} = (\frac{1}{d_2}U_2)_{P_2}$, where

$$d_2 = x^3 \text{ and } U_2 = \left\langle x^3,\ x^2y^2(y-1),\ y^2(y-1)^2\right\rangle_A.$$

Combining the local contributions, we get

$$\frac{1}{d}U = \frac{1}{d_1}U_1 + \frac{1}{d_2}U_2,$$

with $d = x^3$ and

$$U = \left\langle x^3,\ xy(y-1)^3,\ x^2y^2(y-1),\ y^2(y-1)^2\right\rangle_A.$$

Note that U coincides with the ideal U_3 computed in Example 1.

In the following sections we will use the notation below:

Notation 1 *Given an affine algebraic curve $C \subset \mathbb{A}^r_k$ over a field k with vanishing ideal $I(C)$ and a point*[1] *$P \in C$, if $I \subset k[X_1,\ldots,X_r]$ is an ideal properly containing $I(C)$, we will write $I_P = I\mathcal{O}_{C,P}$ for the* local ideal *of I at P. Similarly for a projective algebraic curve $\Gamma \subset \mathbb{P}^r_k$ and a homogeneous ideal $I \subset k[X_0,\ldots,X_r]$.*

3 Adjoint ideals

Let k be a field, and let $\Gamma \subset \mathbb{P}^r_k$ be an integral non-degenerate projective algebraic curve. Write $S = k[X_0,...,X_r]$ for the homogeneous coordinate ring of $\mathbb{P}^r_k$, $I(\Gamma) \subset S$ for the homogeneous vanishing ideal of Γ, $k[\Gamma] = S/I(\Gamma)$ for the homogeneous coordinate ring of Γ, and $\mathrm{Sing}(\Gamma)$ for the singular locus of Γ.

Let $\pi : \overline{\Gamma} \to \Gamma$ be the normalization map, let P be a point of Γ, and let $\mathcal{O}_{\Gamma,P}$ be the local ring of Γ at P. Then the normalization $\overline{\mathcal{O}_{\Gamma,P}}$ is a semi-local ring whose maximal ideals correspond to the points of $\overline{\Gamma}$ lying over P. Furthermore, $\overline{\mathcal{O}_{\Gamma,P}}$ is finite over $\mathcal{O}_{\Gamma,P}$, so that $\overline{\mathcal{O}_{\Gamma,P}}/\mathcal{O}_{\Gamma,P}$ is a finite-dimensional k-vector space. The dimension

$$\delta_P(\Gamma) = \delta(\mathcal{O}_{\Gamma,P}) = \dim_k \overline{\mathcal{O}_{\Gamma,P}}/\mathcal{O}_{\Gamma,P}$$

is called the *delta invariant* of Γ at P. The *arithmetic genus* of Γ is $p_a(\Gamma) = 1 - \mathrm{P}_\Gamma(0)$, where P_Γ is the Hilbert polynomial of $k[\Gamma]$. Making use of the (global) *delta*

[1] The term *point* will always refer to a closed point.

invariant

$$\delta(\Gamma) = \sum_{P \in \mathrm{Sing}(\Gamma)} \delta_P(\Gamma)$$

of Γ, the *geometric genus* $p(\Gamma)$ of Γ is given by

$$p(\Gamma) = p(\overline{\Gamma}) = p_a(\Gamma) - \delta(\Gamma)$$

(see [39]). If Γ is a plane curve of degree n, we have $p_a(\Gamma) = \binom{n-1}{2}$.

Following the presentation in [20], we now recall the definition and characterization of adjoint ideals due to [2] and [21]. Let $I = \bigoplus_{m \geq 0} I_m \subset S = k[X_0, \ldots, X_r]$ be a saturated homogeneous ideal properly containing $I(\Gamma)$. Pulling back $\mathrm{Proj}(S/I)$ via π, we get an effective divisor $\Delta(I)$ on $\overline{\Gamma}$. Let H be a divisor on $\overline{\Gamma}$ given as the pull-back of a hyperplane in $\mathbb{P}^r_k$. Then, since any divisor on $\overline{\Gamma}$ cut out by a homogeneous polynomial in I is of the form $D + \Delta(I)$ for some effective divisor D, we have natural linear maps

$$\rho_m : I_m \to H^0\left(\overline{\Gamma}, \mathscr{O}_{\overline{\Gamma}}(mH - \Delta(I))\right),$$

for all $m \geq 0$.

Remark 7. Consider the exact sequence

$$0 \to \widetilde{I}\mathscr{O}_\Gamma \to \pi_*(\widetilde{I}\mathscr{O}_{\overline{\Gamma}}) \to \mathscr{F} \to 0,$$

where $\widetilde{I}$ is the ideal sheaf on $\mathbb{P}^r_k$ associated to I, and $\mathscr{F}$ is the cokernel. Twisting by $m \gg 0$ and taking global sections, we get the exact sequence

$$0 \to H^0\big(\Gamma, \widetilde{I}\mathscr{O}_\Gamma(m)\big) \to H^0\big(\overline{\Gamma}, \widetilde{I}\mathscr{O}_{\overline{\Gamma}}(mH)\big) \to H^0\left(\Gamma, \mathscr{F}\right) \to 0.$$

Indeed, $\mathscr{F}$ has finite support and, since the normalization map π is finite, we have $H^0\big(\overline{\Gamma}, \widetilde{I}\mathscr{O}_{\overline{\Gamma}}(mH)\big) \cong H^0\big(\Gamma, \pi_*(\widetilde{I}\mathscr{O}_{\overline{\Gamma}})(m)\big)$. Since $\widetilde{I}\mathscr{O}_{\overline{\Gamma}}(mH) = \mathscr{O}_{\overline{\Gamma}}\big(mH - \Delta(I)\big)$ and, for $m \gg 0$, $H^0\big(\Gamma, \widetilde{I}\mathscr{O}_\Gamma(m)\big) = I_m/I(\Gamma)_m$, we get, for $m \gg 0$, the exact sequence

$$0 \to I_m/I(\Gamma)_m \xrightarrow{\overline{\rho_m}} H^0\left(\overline{\Gamma}, \mathscr{O}_{\overline{\Gamma}}(mH - \Delta(I))\right) \to H^0\left(\Gamma, \mathscr{F}\right) \to 0.$$

In particular, for $m \gg 0$,

$$\ker(\rho_m) = I(\Gamma)_m.$$

Definition 5. With notation and assumptions as above, the ideal I is called an *adjoint ideal* of Γ if the maps

$$\rho_m : I_m \to H^0\left(\overline{\Gamma}, \mathscr{O}_{\overline{\Gamma}}(mH - \Delta(I))\right)$$

are surjective for $m \gg 0$.

As already remarked in the introduction, the existence of adjoint ideals is classical. Locally, adjoint ideals are characterized by the following criterion:

Theorem 2. *The ideal I is an adjoint ideal of Γ iff $I_P = I_P\overline{\mathscr{O}_{\Gamma,P}}$ for all $P \in \mathrm{Sing}(\Gamma)$.*

Proof. Using the notation from Remark 7, we have, for $m \gg 0$,

$$\dim_k \operatorname{coker} \rho_m = h^0(\Gamma, \mathscr{F}) = \sum_{P \in \operatorname{Sing}(\Gamma)} \ell(I_P \overline{\mathscr{O}_{\Gamma,P}} / I_P).$$

Hence, ρ_m is surjective iff $I_P \overline{\mathscr{O}_{\Gamma,P}} = I_P$ for all $P \in \operatorname{Sing}(\Gamma)$.

Corollary 1. *If I is an adjoint ideal of Γ and $P \in \operatorname{Sing}(\Gamma)$, then $I_P \subsetneqq \mathscr{O}_{\Gamma,P}$.*

Proof. Suppose $I_P = \mathscr{O}_{\Gamma,P}$. Then $I_P \subsetneqq I_P \overline{\mathscr{O}_{\Gamma,P}}$, a contradiction to Theorem 2.

Corollary 2. *The support of* $\operatorname{Proj}(S/I)$ *contains* $\operatorname{Sing}(\Gamma)$.

Proof. Follows immediately from Corollary 1.

Theorem 3. *There is a unique largest homogeneous ideal $\mathfrak{G} \subset S$ which satisfies*

$$\mathfrak{G}_P = \mathscr{C}_{\mathscr{O}_{\Gamma,P}} \text{ for all } P \in \operatorname{Sing}(\Gamma).$$

The ideal $\mathfrak{G}$ is an adjoint ideal of Γ containing all other adjoint ideals of Γ. In particular, $\mathfrak{G}$ is saturated and $\operatorname{Proj}(S/\mathfrak{G})$ *is supported on* $\operatorname{Sing}(\Gamma)$.

Proof. For the conductor ideal sheaf $\mathscr{C} = \operatorname{Ann}_{\mathscr{O}_\Gamma}(\pi_* \mathscr{O}_{\overline{\Gamma}} / \mathscr{O}_\Gamma)$ on Γ, we have $\mathscr{C}_P = \mathscr{C}_{\mathscr{O}_{\Gamma,P}}$ for all $P \in \Gamma$. If $j : \Gamma \to \mathbb{P}^r_k$ is the inclusion, then the graded S-module $\mathfrak{G} = \bigoplus_{n \in \mathbb{Z}} H^0(\mathbb{P}^r_k, j_* \mathscr{C}(n))$ associated to $j_* \mathscr{C}$ is the unique largest homogeneous ideal with $\mathfrak{G}_P = \mathscr{C}_{\mathscr{O}_{\Gamma,P}}$ for all $P \in \operatorname{Sing}(\Gamma)$. By Theorem 2 and the properties of the conductor, $\mathfrak{G}$ is an adjoint ideal. Moreover, if I is any other adjoint ideal, then $I_P \subset \mathfrak{G}_P$ for all $P \in \Gamma$, hence $I \subset \mathfrak{G}$.

Definition 6. With notation as in Theorem 3, the ideal $\mathfrak{G}$ is called the *Gorenstein adjoint ideal* of Γ. We also write $\mathfrak{G}(\Gamma) = \mathfrak{G}$.

For repeated subsequent use, we introduce the following notation:

Notation 4 *Given an integral non-degenerate projective algebraic curve $\Gamma \subset \mathbb{P}^r_k$, let C be the affine part of Γ with respect to the chart*

$$\mathbb{A}^r_k \hookrightarrow \mathbb{P}^r_k, \ (X_1, \ldots, X_r) \mapsto (1 : X_1 : \cdots : X_r).$$

Let $I(C) \subset k[X_1, \ldots, X_r]$ be the vanishing ideal of C, let $k[C] = k[x_1, \ldots, x_r] = k[X_1, \ldots, X_r]/I(C)$ be its coordinate ring, and let $\operatorname{Sing}(C)$ *be the set of singular points of C.*

Proposition 4. *Let C be the affine part of Γ in the chart $X_0 \neq 0$ as in Notation 4, and let $\overline{\mathfrak{G}}$ be the ideal of $k[C]$ obtained by dehomogenizing $\mathfrak{G}$ with respect to X_0 and mapping the result to $k[C]$. Then*

$$\overline{\mathfrak{G}} = \mathscr{C}_{k[C]}.$$

If Γ has no singularities at infinity and $\mathscr{C}_{k[C]} = \langle g_i(x_1, \ldots, x_r) \mid i = 1, \ldots, m \rangle_{k[C]}$, with polynomials $g_i \in k[X_1, \ldots, X_r]$, then $\mathfrak{G}$ is the homogenization of the ideal

$$\langle g_i(X_1,...,X_r) \mid i=1,\ldots,m\rangle_{k[X_1,...,X_r]} + I(C)$$

with respect to X_0.

Proof. The first assertion is obtained by localizing at the points of C:

$$\overline{\mathfrak{G}}_P = \mathscr{C}_{\mathscr{O}_{C,P}} = (\mathscr{C}_{k[C]})_P \text{ for each } P \in C.$$

Here, the first equality is clear from the definition of $\mathfrak{G}$ (see Theorem 3). The second equality holds since forming the conductor commutes with localization since $k[C]$ is normalization-finite (see [63, Ch. V, § 5]).

The second assertion follows from the first one since there are no singularities at infinity, $\mathfrak{G}$ is saturated, and the support of $\mathfrak{G}$ is contained in C.

Remark 8 (Base Change). Suppose that Γ is defined over a subfield ℓ of k such that $\ell \subset k$ is separable, and let $\Gamma(\ell) \subset \mathbb{P}^r_\ell$ be the set of ℓ-rational points of Γ. Then it follows from Remark 5 and Proposition 4 that

$$\delta(\Gamma(\ell)) = \delta(\Gamma) \text{ and } \mathfrak{G}(\Gamma(\ell))k[X_0,\ldots,X_n] = \mathfrak{G}(\Gamma).$$

We now take a moment to specialize to plane curves.

Remark 9. Assume Γ is a plane curve. Then, by Max Noether's Fundamentalsatz, the maps $\rho_m : \mathfrak{G}_m \to H^0\left(\overline{\Gamma}, \mathscr{O}_{\overline{\Gamma}}(mH - \Delta(\mathfrak{G}))\right)$ are surjective for *all* m. Referring to each homogeneous polynomial in $\mathfrak{G}$ not contained in $I(\Gamma)$ as an *adjoint curve* to Γ, this means that residual to $\Delta(\mathfrak{G})$, the adjoint curves of any degree m cut out the complete linear series $\mathscr{A}_m = |mH - \Delta(\mathfrak{G})|$. See [60, § 49].

Theorem 5. *Assume Γ is a plane curve of degree n. Then, residual to $\Delta(\mathfrak{G})$, the elements of $\mathfrak{G}_{n-3}$ cut out the complete canonical linear series. Equivalently,*

$$\deg \Delta(\mathfrak{G}) = 2\delta(\Gamma). \tag{1}$$

Proof. See [28, Thm. 9].

Recall that the dimension of the canonical linear series is $\dim \mathscr{A}_{n-3} = p(\Gamma) - 1$.

Remark 10. Assume Γ is a plane curve of degree n. If $p(\Gamma) = 0$, that is, Γ is rational, then $\dim \mathscr{A}_{n-2} = \deg \mathscr{A}_{n-2} = n-2$, and the image of Γ under $\mathscr{A}_{n-2}$ is a rational normal curve $\Gamma_{n-2} \subset \mathbb{P}^{n-2}_k$ of degree $n-2$. Via the birational morphism $\Gamma_{n-2} \to \Gamma$, the problem of parametrizing Γ is reduced to parametrizing the smooth curve Γ_{n-2}. For the latter, we may successively decrease the degree of the rational normal curve by 2 via the anti-canonical linear series. This yields an isomorphism from Γ_{n-2} either to $\mathbb{P}^1$ or to a plane conic, depending on whether n is odd or even.

We will now return to the general case and discuss a version of Equation (1) which is also valid if Γ is not necessarily planar. In fact, this equation characterizes adjoint ideals. We use the following notation: If $I \subset S$ is a homogeneous ideal, write $\deg I = \deg \mathrm{Proj}(S/I)$. That is, $\deg I$ is $(\dim I - 1)!$ times the leading coefficient of the Hilbert polynomial of S/I.

Lemma 3. *Let $I \subset S$ be a saturated homogeneous ideal with $I(\Gamma) \subsetneq I$. Then*

$$\deg \Delta(I) \leq \deg I + \delta(\Gamma),$$

and I is an adjoint ideal of Γ iff

$$\deg \Delta(I) = \deg I + \delta(\Gamma).$$

Proof. Let $\mathrm{P}_\Gamma(t) = (\deg \Gamma)\cdot t - p_a(\Gamma) + 1$ be the Hilbert polynomial of $k[\Gamma]$. Denote by I_Γ the image of I in $k[\Gamma]$. Then, for $m \gg 0$,

$$\deg I = \dim_k(S_m/I_m) = \dim_k(k[\Gamma]_m/(I_\Gamma)_m) = P_\Gamma(m) - \dim_k(I_\Gamma)_m.$$

Moreover, by Remark 7 and with notation as in that remark,

$$h^0\left(\overline{\Gamma}, \mathscr{O}_{\overline{\Gamma}}(mH - \Delta(I))\right) = \dim_k(I_\Gamma)_m + h^0\left(\Gamma, \mathscr{F}\right) \geq \dim_k(I_\Gamma)_m$$

for $m \gg 0$. Hence, by Riemann-Roch, we have

$$\begin{aligned}(\deg \Gamma)\cdot m - \deg \Delta(I) &= \deg |mH - \Delta(I)| = \dim |mH - \Delta(I)| + p(\Gamma)\\ &\geq \dim_k(I_\Gamma)_m - 1 + p(\Gamma)\\ &= \mathrm{P}_\Gamma(m) - \deg I - 1 + p(\Gamma)\\ &= (\deg \Gamma)\cdot m - \delta(\Gamma) - \deg I\end{aligned}$$

for $m \gg 0$ since $|mH - \Delta(I)|$ is non-special for large m by reason of its degree. For such m, equality holds iff ρ_m is surjective.

Remark 11. In the case where Γ is a plane curve and $I = \mathfrak{G}$ is its Gorenstein adjoint ideal, Lemma 3 shows that Equation (1) may be rewritten as

$$\deg \mathfrak{G} = \delta(\Gamma). \tag{2}$$

Note that (1) and (2) may not hold in the non-planar case:

Example 3 (26, Example 5.2.5]. Let $\Gamma \subset \mathbb{P}^3_{\mathbb{C}}$ be the image of the parametrization

$$\mathbb{P}^1_{\mathbb{C}} \longrightarrow \mathbb{P}^3_{\mathbb{C}},\ (s:t) \mapsto (s^5 : t^3 s^2 : t^4 s : t^5).$$

Then Γ has exactly one singularity at $(1:0:0:0)$. Furthermore, $p(\Gamma) = 0$ and $p_a(\Gamma) = 2$, hence $\delta(\Gamma) = 2$. However, $\mathfrak{G} = \langle X_1, X_2, X_3\rangle \subset \mathbb{C}[X_0, \ldots, X_3]$, hence $\deg \mathfrak{G} = 1$.

Remark 12. If $\Gamma \subset \mathbb{P}^r_k$ is any curve as in Notation 4, with affine part C and no singularities at infinity, then it follows from Proposition 4 that

$$\deg \mathfrak{G} = \dim_k\left(k[C]/\mathscr{C}_{k[C]}\right) = \textstyle\sum_{P \in \mathrm{Sing}(C)} \dim_k(\mathscr{O}_{C,P}/\mathscr{C}_{\mathscr{O}_{C,P}}).$$

Lemma 4. *If* $\mathrm{char}\, k = 0$, *then* $\dim_k(\mathscr{O}_{\Gamma,P}/\mathscr{C}_{\mathscr{O}_{\Gamma,P}}) \leq \delta_P(\Gamma)$ *for any point* $P \in \Gamma$.

Proof. This follows from the case $k = \mathbb{C}$ proved in [32, 2.4] by base change (see Remark 5).

Now recall that a point $P \in \mathrm{Sing}(\Gamma)$ is called a *Gorenstein singularity* if

$$\dim_k(\mathscr{O}_{\Gamma,P}/\mathscr{C}_{\mathscr{O}_{\Gamma,P}}) = \delta_P(\Gamma).$$

Example 4. Plane curve singularities are Gorenstein (see, for example, [26, Corollary 5.2.9]).

Corollary 3. *We have:*

1. *If* $\mathrm{char}\, k = 0$*, then* $\deg \mathfrak{G} \leq \delta(\Gamma)$.
2. *If* Γ *has only Gorenstein singularities, then*

$$\deg \mathfrak{G} = \delta(\Gamma) \;\; \textit{and} \;\; \deg \Delta(\mathfrak{G}) = 2\delta(\Gamma).$$

Proof. This is clear from the discussion above.

We now begin with the discussion of how to compute the Gorenstein adjoint ideal. One possible way of finding $\mathfrak{G}$ is to apply the global algorithms presented in Section 4.2 below, starting from the normalization $\overline{k[C]}$, and relying on Proposition 4. To compute $\overline{k[C]}$, in turn, we may use the local to global approach outlined in Section 2. As we will see, however, it is more efficient to directly proceed with a local to global approach for finding $\mathfrak{G}$, computing local Gorenstein adjoint ideals at the singular points, and obtaining $\mathfrak{G}$ as their intersection. This will be the theme of Sections 5 and 6, while in Section 7, focusing on the case of plane curves, we will write down explicit generators for the local Gorenstein adjoint ideals at various types of singularities.

Remark 13. With regard to implementing Proposition 4 as a part of the global algorithms, we note that if k is infinite, then the assumption on the singularities can always be achieved by a projective change of coordinates defined over k. If k is infinite, however, we may have to replace k by an algebraic extension field of k. Our local to global algorithm, on the other hand, does not require a coordinate change. If Γ is defined over a subfield ℓ of k such that $\ell \subset k$ is separable, then it follows from Remark 8 that we may find the Gorenstein ideal by computations over ℓ.

If Γ is defined over $\mathbb{Q}$, we will use the equality

$$\deg \mathfrak{G} = \deg \Delta(\mathfrak{G}) - \delta(\Gamma)$$

from Lemma 3 to compute $\deg \mathfrak{G}$ without actually knowing $\mathfrak{G}$, and apply this in the final verification step of our modularized adjoint ideal algorithm (see Sections 8 and 9). In fact, we will present a modular approach to computing $\deg \Delta(\mathfrak{G})$, and we will use standard techniques to compute $\delta(\Gamma)$. For the latter, first note that the delta invariant of Γ differs from that of a plane model of Γ by the quantity $p_a(\Gamma) - \binom{\deg \Gamma - 1}{2}$. The delta invariant of a plane curve, in turn, can be computed locally at

the singular points, either from the semigroups of values of the analytic branches of the singularity (see [26], [35]), or from a formula relating the local delta invariant to the Milnor number (see Remark 19 in Section 7).

Remark 14. Let $\Gamma \subset \mathbb{P}^r_k$ be a curve with affine part C as in Notation 4 and no singularities at infinity. Then computing $\deg \Delta(\mathfrak{G})$ also means to compute the dimension $\dim_k\left(\overline{k[C]}/\mathscr{C}_{k[C]}\right)$:

$$\begin{aligned}\deg \Delta(\mathfrak{G}) &= \delta(\Gamma) + \deg \mathfrak{G} \\ &= \dim_k\left(\overline{k[C]}/k[C]\right) + \dim_k\left(k[C]/\mathscr{C}_{k[C]}\right) \\ &= \dim_k\left(\overline{k[C]}/\mathscr{C}_{k[C]}\right).\end{aligned}$$

4 Global approaches

4.1 Computing the conductor via the trace matrix

We will require some facts from classical ideal theory (see [63, Ch. V] for details and proofs): Let R be an integral domain, and let $K = \mathrm{Q}(R)$ be its quotient field. A *fractionary ideal* of R is an R-submodule $\mathfrak{b}$ of K admitting a common denominator: there is an element $0 \neq d \in R$ such that $d\,\mathfrak{b} \subset R$.

Example 5. The extensions A_i computed by the normalization algorithms from Section 2 are fractionary ideals of the given affine domain A.

If $\mathfrak{b}, \mathfrak{b}'$ are two fractionary ideals of R, with $\mathfrak{b}'$ non-zero, then $\mathfrak{b} : \mathfrak{b}' = \{z \in K \mid z\,\mathfrak{b}' \subset \mathfrak{b}\}$ is a fractionary ideal of R as well. A fractionary ideal $\mathfrak{b}$ of R is *invertible* if there is a fractionary ideal $\mathfrak{b}'$ of R such that $\mathfrak{b} \cdot \mathfrak{b}' = R$. In this case, $\mathfrak{b}'$ is uniquely determined and equal to $R : \mathfrak{b}$.

Suppose in addition that R is normal. Let K' be a finite separable extension of K, and let R' be an integral extension of R such that $K' = \mathrm{Q}(R')$. Moreover, let

$$\mathrm{Tr}_{K'/K} : K' \to K,\ z \mapsto \sum_{g \in \mathrm{Gal}(K'/K)} g(z),$$

be the corresponding *trace map*. Then the *complementary module*

$$\mathfrak{C}_{R'/R} := \left\{z \in K' \mid \mathrm{Tr}_{K'/K}\left(zR'\right) \subset R\right\}$$

of R' with respect to R is a *fractionary ideal* of R' containing R'. Hence, the *different*

$$\begin{aligned}\mathfrak{D}_{R'/R} = R' : \mathfrak{C}_{R'/R} &= \left\{z \in K' \mid z\,\mathfrak{C}_{R'/R} \subset R'\right\} \\ &= \left\{z \in K' \mid zx \in R' \text{ for all } x \in K' \text{ with } \mathrm{Tr}_{K'/K}\left(xR'\right) \subset R\right\}\end{aligned}$$

of R' over R is a non-zero ideal of R'.

Now, keeping our assumptions, we focus on the case where R is a Dedekind domain, and where R' is the integral closure of R in K'. Then R' is a Dedekind domain as well, which implies that every non-zero fractionary ideal of R' is invertible. On the other hand, by the primitive element theorem, there is an element $y \in R'$ with $K' = K(y)$. Denote by $f(Y) \in K[Y]$ the minimal polynomial of y over K. Then, as shown in [63, Ch. V],

$$f'(y)R' = \mathscr{C}_{R'/R[y]}\mathfrak{D}_{R'/R},$$

hence

$$\mathscr{C}_{R'/R[y]} = f'(y)\mathfrak{C}_{R'/R}. \tag{3}$$

We now fix the following setup:

Notation 6 *Let k be a field, and let $\Gamma \subset \mathbb{P}^2_k$ be a plane curve of degree n defined by an irreducible polynomial $F \in k[X,Y,Z]$. Suppose that the equation $f \in k[X,Y]$ of the affine part C of Γ in the chart*

$$\mathbb{A}^2_k \hookrightarrow \mathbb{P}^2_k,\ (X,Y) \mapsto (1:X:Y),$$

is monic in Y.

Write $k[C] = k[x,y] = k[X,Y]/\langle f(X,Y)\rangle$ for the affine coordinate ring of C and

$$k(C) = k(x,y) = k(X)[Y]/\langle f(X,Y)\rangle$$

for its function field. Then x is a separating transcendence basis of $k(C)$ over k, and y is integral over $k[x]$, with integral equation $f(x,y) = 0$. In particular, $k[C]$ is integral over $k[x]$, which implies that $\overline{k[C]}$ coincides with the integral closure $\overline{k[x]}$ of $k[x]$ in $k(C)$. Furthermore, $\overline{k[C]}$ is a free $k[x]$-module of rank

$$n := \deg_y(f) = [k(C) : k(x)].$$

Definition 7. An *integral basis* for $\overline{k[C]}$ is a set $b_0, \ldots, b_{n-1}$ of free generators for $\overline{k[C]}$ over $k[x]$:

$$\overline{k[C]} = k[x]b_0 \oplus \cdots \oplus k[x]b_{n-1}.$$

Remark 15. Since $k(C) = k(x,y) = k(X)[Y]/\langle f\rangle$, any element $\alpha \in k(C)$ can be represented as a polynomial in $k(X)[Y]$ of degree less than $n = \deg f$. Hence, we may associate to α a well-defined degree $\deg_y(\alpha)$ in y and a smallest common denominator in $k[x]$ of the coefficients of α. In particular, $\overline{k[C]}$ has an integral basis (b_i) in triangular form, that is, with $\deg_y(b_i) = i$, for $i = 0, \ldots, n-1$ (see [12, Remark 1.4]. If not stated otherwise, all integral bases considered here will be of this form. In principle, such a basis can be found by applying one of the normalization algorithms discussed earlier (see [12, Remark 1.5]). However, in the characteristic zero case, methods relying on Puiseux series techniques are much more efficient (see [12] and [61]). Note that when using these methods, we temporarily may have to pass to an algebraic extension field of k.

Example 6. An integral basis for the curve considered in Examples 1, 2 is given below:

$$1, y, \frac{y(y-1)}{x}, \frac{y(y-1)^2}{x^2}, \frac{y^2(y-1)^2}{x^3}.$$

Using Proposition 4 and Equation (3), with $R = k[x]$, $R' = \overline{k[C]}$, $K = k(x)$, and $K' = k(C)$, we get Algorithm 1.

Algorithm 1 Gorenstein adjoint ideal via linear algebra (see [52])

Input: A plane curve Γ over a perfect field k with affine part C as in Notation 6 and no singularities at infinity.

Output: The Gorenstein adjoint ideal $\mathfrak{G}$ of Γ.

1: Compute an integral basis $(b_i)_{i=0,\ldots,n-1}$ for $\overline{k[C]}$.

2: Compute the (symmetric and invertible) trace matrix

$$T = \left(\mathrm{Tr}_{k(C)/k(x)}\left(b_i b_j\right)\right)_{i,j=0,\ldots,n-1} \in k(x)^{n\times n}.$$

3: Compute a decomposition $L \cdot R = P \cdot T$, where L is left triangular matrix with diagonal entries equal to one, R is a right triangular matrix, and P is a permutation matrix.

4: For $j = 0, \ldots, n-1$, use forward and backward substitution to compute

$$\eta_j = \sum_{i=0}^{n-1} s_{ij} b_i,$$

where $(s_{ij}) = T^{-1}$. The η_j are $k[x]$-module generators for $\mathfrak{C}_{\overline{k[C]}/k[x]}$. By Equation (3), $\mathscr{C}_{k[C]} = \langle \frac{\partial f}{\partial Y}(x,y)\,\eta_j \mid j = 0, \ldots, n-1 \rangle$.

5: Let $\mathscr{C}$ be the ideal of $k[X,Y]$ generated by representatives of minimal y-degree of the $\frac{\partial f}{\partial Y}(x,y)\,\eta_j$, $j = 0, \ldots, n-1$.

6: **return** the homogenization of $\mathscr{C}$ with respect to X_0.

Example 7. Let $\Gamma \subset \mathbb{P}^2_{\mathbb{C}}$ be the projetive closure of the curve C with affine equation

$$X^5 - Y^2(1-Y)^3 = 0$$

as in Examples 1, 2, and 6. From the integral basis

$$1, y, \frac{y(y-1)}{x}, \frac{y(y-1)^2}{x^2}, \frac{y^2(y-1)^2}{x^3}.$$

given in Example 6, we compute the trace matrix

$$T = \begin{pmatrix} 5 & 3 & 0 & 0 & 0 \\ 3 & 3 & 0 & 0 & -5x^2 \\ 0 & 0 & 0 & -5x^2 & -3x \\ 0 & 0 & -5x^2 & -3x & 0 \\ 0 & -5x^2 & -3x & 0 & 0 \end{pmatrix},$$

which yields by forward and backward substitution

$$\mathscr{C}_{\mathbb{C}[C]} = \left\langle x^3,\, x^2\,(y-1)\,,\, xy\,(x-1)\,,\, y\,(y-1)^2 \right\rangle_{\mathbb{C}[C]}.$$

Homogenization gives the Gorenstein ideal $\mathfrak{G}$ which can be decomposed using primary decomposition:

$$\mathfrak{G} = \left\langle X^2, Y \right\rangle \cap \left\langle X^3, X\,(Y-Z)\,, (Y-Z)^2 \right\rangle.$$

Note the two ideals on the right hand side correspond to the two singularities of C. This somewhat motivates the local to global algorithm discussed in Sections 5 and 6 below, where $\mathfrak{G}$ will be found as the intersection of local Gorenstein ideals.

4.2 Computing the adjoint ideal via ideal quotients

The algorithm presented in what follows relies on normalization and ideal quotients. It is not limited to plane curves.

Proposition 5. *Let $\Gamma \subset \mathbb{P}^r_k$ be a curve with affine part C as in Notation 4. Write $\overline{k[C]} = \frac{1}{d}U$, where $U \subset k[C]$ is an ideal and $d \in U$ is non-zero. Then the conductor is*

$$\mathscr{C}_{k[C]} = \langle d \rangle_{k[C]} : U.$$

Proof. By definition,

$$\begin{aligned} \mathscr{C}_{k[C]} &= \left\{ s \in k[C] \mid s \cdot \overline{k[C]} \subset k[C] \right\} \\ &= \left\{ s \in k[C] \mid s \cdot g \in \langle d \rangle_{k[C]} \text{ for all } g \in U \right\} \\ &= \langle d \rangle_{k[C]} : U. \end{aligned}$$

Using once more Proposition 4, we get Algorithm 2.

Example 8. In Example 7,

$$a_0 = X^3,\ a_1 = X^2Y(Y-1),\ a_2 = XY(Y-1)^2,\ a_3 = Y^2(Y-1)^2,$$

and $d = X^3$. Hence,

$$\langle d, f \rangle : \langle a_0, ..., a_3, f \rangle = \left\langle X^3,\, X^2\,(Y-1)\,,\, XY\,(Y-1)\,,\, Y\,(Y-1)^2 \right\rangle.$$

Algorithm 2 Gorenstein adjoint ideal via ideal quotients

Input: A curve $\Gamma \subset \mathbb{P}^r_k$ over a perfect field k with affine part C as in Notation 4 and no singularities at infinity.

Output: The Gorenstein adjoint ideal $\mathfrak{G}$ of Γ.

1: Normalization: Compute polynomials $d, a_0, \ldots, a_s \in k[X_1, ..., X_r]$ such that the fractions $\frac{a_i(x_1,...,x_r)}{d(x_1,...,x_r)}$ generate $\overline{k[C]}$ as a $k[C]$-module.

2: Compute the ideal quotient

$$\mathscr{C} = (\langle d \rangle + I(C)) : (\langle a_0, ..., a_s \rangle + I(C)) \subset k[X_1, ..., X_r].$$

3: **return** the homogenization of $\mathscr{C}$ with respect to X_0.

5 A Local to global approach

In this section, motivated by the local to global approach for normalization, we introduce local Gorenstein adjoint ideals of a given curve Γ and show how to find the Gorenstein adjoint ideal $\mathfrak{G}$ of Γ as their intersection. Together with the algorithm presented in the next section, which computes the local ideals, this yields a local to global approach for finding $\mathfrak{G}$. As we will see in Section 10, this approach is per se faster than the algorithms discussed so far. In addition, it is well-suited for parallel computations.

We consider a curve $\Gamma \subset \mathbb{P}^r_k$ as in Notation 4.

Definition 8. Let $W \subset \mathrm{Sing}(\Gamma)$ be any set of singular points of Γ. The *local Gorenstein adjoint ideal* of Γ at W is defined to be the largest homogeneous ideal $\mathfrak{G}(W) \subset S$ which satisfies

$$\mathfrak{G}(W)_P = \mathscr{C}_{\mathscr{O}_{\Gamma,P}} \text{ for all } P \in W. \tag{4}$$

For a single point $P \in \mathrm{Sing}(\Gamma)$, we write $\mathfrak{G}(P) := \mathfrak{G}(\{P\})$.

Remark 16. Since $\mathfrak{G}(W)$ is the largest homogeneous ideal satisfying (4), it is saturated and $\mathrm{Proj}(S/\mathfrak{G}(W))$ is supported on W.

Proposition 6. *Let $W \subset \mathrm{Sing}(\Gamma)$. Then*

$$\mathfrak{G}(W) = \textstyle\bigcap_{P \in W} \mathfrak{G}(P).$$

Proof. This is immediate from the definition: If $\mathfrak{G}' := \bigcap_{P \in W} \mathfrak{G}(P)$, then $\mathrm{Proj}(S/\mathfrak{G}')$ and $\mathrm{Proj}(S/\mathfrak{G}(W))$ have the same support W, and

$$\mathfrak{G}'_Q = \mathfrak{G}(Q)_Q = \mathscr{C}_{\mathscr{O}_{\Gamma,Q}} = \mathfrak{G}(W)_Q$$

for all $Q \in W$, hence $\mathfrak{G}(W) = \mathfrak{G}'$.

Proposition 6 yields Algorithm 3.

Algorithm 3 Gorenstein adjoint ideal, local to global

Input: A curve $\Gamma \subset \mathbb{P}^r_k$ over a perfect field k as in Notation 4.
Output: The Gorenstein adjoint ideal $\mathfrak{G}$ of Γ.
1: Compute $\mathrm{Sing}(\Gamma) = \{P_1, ..., P_s\}$.
2: Apply Algorithm 4 in Section 6 below to compute $\mathfrak{G}(P_i)$ for all i.
3: **return** $\bigcap_{i=1}^{s} \mathfrak{G}(P_i)$.

Remark 17. It is clear from Proposition 6 that we may choose any partition $\mathrm{Sing}(\Gamma) = \bigcup_{i=1}^{s} W_i$ of $\mathrm{Sing}(\Gamma)$ and have

$$\mathfrak{G} = \bigcap_{i=1}^{s} \mathfrak{G}(W_i).$$

This is useful in that for some subsets W_i, specialized approaches or a priori knowledge may ease the computation of $\mathfrak{G}(W_i)$. In Section 7, focusing on plane curves, we will present some ideas in this direction.

6 Computing local adjoint ideals

In this section, we modify Algorithm 2 so that it computes the local Gorenstein adjoint ideal of Γ at a point P from a minimal local contribution to $\overline{k[C]}$ at P via ideal quotients.

Fix a curve $\Gamma \subset \mathbb{P}^r_k$ as in Notation 4, a point $P \in \mathrm{Sing}(\Gamma)$, and an affine chart containing P. For simplicity of the presentation, we stick with the chart $X_0 \neq 0$, and let C be the affine part of Γ as before. Consider an ideal $U \subset k[C]$ and a non-zero element $d \in U$ such that $\frac{1}{d}U$ is the minimal local contribution to $\overline{k[C]}$ at P.

Proposition 7. *With notation as above, and given $Q \in C$, we have*

$$(\langle d \rangle_{k[C]} : U)_Q = \begin{cases} \mathscr{C}_{\mathscr{O}_{C,Q}} & \text{if } Q = P, \\ \mathscr{O}_{C,Q} & \text{if } Q \neq P. \end{cases}$$

Proof. By the minimality assumption, we have

$$\left(\frac{1}{d}U\right)_Q = \begin{cases} \overline{\mathscr{O}_{C,Q}} & \text{if } Q = P, \\ \mathscr{O}_{C,Q} & \text{if } Q \neq P. \end{cases}$$

The claim follows since localization commutes with forming the conductor:

$$\left(\langle d \rangle_{k[C]} : U\right)_Q = \left(\mathscr{C}_{(\frac{1}{d}U)\,/\,k[C]}\right)_Q = \mathscr{C}_{(\frac{1}{d}U)_Q\,/\,k[C]_Q}.$$

Now, we argue as in the proof of Proposition 4: From Proposition 7 and Remark 16, it follows that $\langle d \rangle_{k[C]} : U$ coincides with the ideal obtained by dehomogenizing $\mathfrak{G}(P)$ with respect to X_0 and mapping the result to $k[C]$. Hence, since $\mathfrak{G}(P)$ is saturated, Algorithm 4 below indeed computes $\mathfrak{G}(P)$.

Algorithm 4 Local Gorenstein adjoint ideal from a local contribution

Input: A curve $\Gamma \subset \mathbb{P}^r_k$ over a perfect field k with affine part C as in Notation 4 and a point $P \in \mathrm{Sing}(C) \subset \mathrm{Sing}(\Gamma)$.

Output: The local Gorenstein adjoint ideal $\mathfrak{G}(P)$ of Γ.

1: Compute polynomials $d, a_0, \ldots, a_s \in k[X_1, ..., X_r]$ such that the fractions $\frac{a_i(x_1,\ldots,x_r)}{d(x_1,\ldots,x_r)}$ generate the minimal local contribution to $\overline{k[C]}$ at P as a $k[C]$-module.

2: Compute the ideal quotient

$$\mathscr{C} = (\langle d \rangle + I(C)) : (\langle a_0, ..., a_s \rangle + I(C)) \subset k[X_1, ..., X_r].$$

3: **return** the homogenization of $\mathscr{C}$ with respect to X_0.

Example 9. Let $\Gamma \subset \mathbb{P}^2_{\mathbb{C}}$ be the projetive closure of the curve C with affine equation

$$X^5 - Y^2(1-Y)^3 = 0$$

as in Examples 1, 2, 6, and 8. We compute the local Gorenstein adjoint ideals. For the A_4-singularity P_1, we know from Example 2 that

$$d_1 = x^2 \text{ and } U_1 = \left\langle x^2,\ y(y-1)^3 \right\rangle_{\mathbb{C}[C]},$$

so that

$$\mathfrak{G}(P_1) = \left\langle X^2,\ Y \right\rangle.$$

For the E_8 singularity P_2, in turn, we have

$$d_2 = x^3 \text{ and } U_2 = \left\langle x^3,\ x^2y^2(y-1),\ y^2(y-1)^2 \right\rangle_{\mathbb{C}[C]},$$

leading to

$$\mathfrak{G}(P_2) = \left\langle X^3,\ X(Y-Z), (Y-Z)^2 \right\rangle.$$

Note that $\mathfrak{G}(P_1)$ and $\mathfrak{G}(P_2)$ are the ideals already obtained in Example 7.

7 Improvements to the local strategy for plane curves

In this section, we focus on the case of a plane curve Γ with affine part $C = V(f)$ and $\mathrm{Sing}(\Gamma) = \mathrm{Sing}(C)$ as in Notation 6. *For simplicity of the presentation, we suppose throughout the section that our ground field $k = \mathbb{C}$.*

As explained in Section 5, the Gorenstein adjoint ideal $\mathfrak{G}$ can be computed as the intersection of local Gorenstein ideals via a partition of $\mathrm{Sing}(C)$. To begin with, consider the following partition:

$$\mathrm{Sing}(C) = W_2 \cup W_3 \cup \cdots \cup W_r \cup W', \tag{5}$$

where, for each i, W_i denotes the locus of ordinary i-fold points (ordinary multiple points of multiplicity i)[2] and where W' collects the remaining singularities of C. In particular, W_2 is the set of nodes of C. Note that in many practical examples $W' = \emptyset$.

Lemma 5. *Let $P \in \mathrm{Sing}(C)$, and let $\mathfrak{m}_P \subset k[X,Y]$ be the corresponding maximal ideal. If P is an ordinary i-fold point of C, then*

$$\mathfrak{G}(P) = \mathfrak{m}_P^{i-1}.$$

Proof. Since C is a plane curve and P is an ordinary i-fold point of C, the conductor $\mathscr{C}_{\mathscr{O}_{C,P}} = \mathfrak{m}_{C,P}^{i-1}$, where $\mathfrak{m}_{C,P}$ is the maximal ideal of $\mathscr{O}_{C,P}$ (see [49], [30]). The result follows from the very definition of $\mathfrak{G}(P)$.

Applying the lemma to the partition (5), we get the intersection of ideals

$$\mathfrak{G} = I(W_2) \cap I(W_3)^2 \cap \cdots \cap I(W_r)^r \cap \mathfrak{G}(W'). \tag{6}$$

Hence, in the case where Γ is known to have ordinary multiple points as singularities only (that is, $W' = \emptyset$), we can compute $\mathfrak{G}$ in a very efficient way by using Algorithm 5 below (see [6]).

Algorithm 5 Gorenstein adjoint ideal, ordinary multiple points only

Input: A plane curve Γ of degree n with defining polynomial F as in Notation 6 with only ordinary multiple points as singularities.

Output: The Gorenstein adjoint ideal $\mathfrak{G}$ of Γ.

$J_1 = \left\langle \frac{\partial F}{\partial X}, \frac{\partial F}{\partial Y}, \frac{\partial F}{\partial Z} \right\rangle$ (the ideal defining $\mathrm{Sing}(\Gamma)$)
$i = 1$
while $(J_i : \langle X,Y,Z\rangle^\infty) \neq \langle 1\rangle$ **do**
  $i = i+1$
  $J_i = \left\langle \frac{\partial^{j+l+m} F}{\partial X^j \partial Y^l \partial Z^m} \mid j+l+m = i;\ j,l,m \in \mathbb{N} \right\rangle$
$B = \langle X,Y,Z\rangle^{n-i}$
while $i > 0$ **do**
  $I_i = (J_{i-1} : B^\infty)$ (the ideal of the i-fold points of Γ)
  $B = ((B \cap I_i^{i-1}) : \langle X,Y,Z\rangle^\infty)$
  $i = i-1$
return B

In the general case, Equation (6) allows us to reduce the computation of $\mathfrak{G}$ to the less involved task of computing $\mathfrak{G}(W')$ as soon as we have detected the ordinary i-fold points. To begin with treating these, here is how to find the nodes:

[2] Recall that an ordinary multiple point of multiplicity i is a singularity where the lowest non-vanishing jet of f factors into i distinct linear factors.

Remark 18. We know how to find *all* singularities: $\mathrm{Sing}(C)$ is given by the ideal

$$J = \left\langle f, \frac{\partial f}{\partial X}, \frac{\partial f}{\partial Y} \right\rangle.$$

Now consider the Hessian matrix $\mathrm{Hess}(f)$ formed by the second partial derivatives of f. By the Morse lemma (see [51]), a point $P \in \mathrm{Sing}(C)$ is a node iff $\mathrm{Hess}(f)$ is non-degenerate at P. That is, P is a node iff

$$I(P) + \langle \det(\mathrm{Hess}(f)) \rangle = k[X,Y].$$

This gives us a fast way of computing W_2.

Carrying our efforts one step further, we discuss the local analysis of the singularities via invariants. This yields an efficient method not only for finding the delta invariant, but also for detecting the ordinary i-fold points, for each i:

Remark 19. Let $P \in \mathrm{Sing}(C)$. After a translation, we may assume that $P = (0,0)$ is the origin. Write m_P for the multiplicity and

$$\mu_P = \dim_k \left(k[[X,Y]] \Big/ \left\langle \frac{\partial f}{\partial X}, \frac{\partial f}{\partial Y} \right\rangle \right)$$

for the *Milnor number* of C at P. Then $m_P = \deg h_p$, where h_P is the lowest degree homogeneous summand of the Taylor expansion of f at P. Recall that μ_P can be computed via standard bases (see [36]). Furthermore, if the Newton polygon of f is non-degenerate (otherwise, successively blow up), the *number r_P of branches* of f at P can be computed as

$$r_P = \sum_{j=1}^{s-1} \gcd\left(V_X^{(j+1)} - V_X^{(j)},\ V_Y^{(j+1)} - V_Y^{(j)} \right),$$

where $V^{(1)}, \ldots, V^{(s)}$ are the (ordered) vertices of the Newton polygon (and X and Y refer to their respective coordinates). This is immediate from [14, Section 8.4, Lemma 3]. The delta invariant of C at P is then obtained as

$$\delta_P = \frac{1}{2}(\mu_P + r_P - 1)$$

(see, for example, [35, Chapter 1, Proposition 3.34]). Furthermore, P is an ordinary i-fold point iff h_P is square-free and $m_P = i$. Equivalently,

$$(m_P, r_P, \delta_P) = \left(i,\ i,\ \binom{i}{2} \right).$$

See [35, Chapter 1, Proposition 3.33].

The local analysis of the singularities may be used to further refine our partition of $\mathrm{Sing}(C)$. For example, singularities of type *ADE* can be identified as follows:

Remark 20. With notation as in Remark 19, the point $P = (0,0) \in \mathrm{Sing}(C)$ is

1. of type A_n, $n \geq 2$, iff $h_P = l_1^2$, with $l_1 \in k[X,Y]$ linear, and $\mu_P = n$,
2. of type D_n, $n \geq 4$, iff $h_P = l_1 l_2 l_3$ or $h_P = l_1^2 l_2$, with pairwise different linear polynomials $l_j \in k[X,Y]$, and $\mu_P = n$, and
3. of type E_n, $n = 6,7,8$, iff $h_P = l_1^3$, with $l_1 \in k[X,Y]$ linear, and $\mu_P = n$.

Here, in (2), h_P splits into three different linear factors iff P is of type D_4. See, for example, [35, Chapter 1, Theorems 2.48, 2.51, 2.54].

To describe the local Gorenstein adjoint ideal at a singularity of type A, D, or E, we use the following notation:

Notation 7 *For any element $g \in k[[X,Y]]$, let $g_j = \mathrm{taylor}\,(g,j) \in k[X,Y]$ be the Taylor expansion of g at $P = (0,0)$ modulo $O(j+1)$.*[3]

If C has a singularity of type A_n at $P = (0,0)$, we may write f in the form $f = T^2 + W^{n+1}$, where $T, W \in k[[X,Y]]$ is a regular system of parameters. Let $s = \left\lfloor \frac{n+1}{2} \right\rfloor$ (the meaning of s will become clear in the proof of Lemma 6). We may compute the Taylor expansion $T_{s-1} \in k[X,Y]$ as follows. If n and thus s is equal to 1, set $T_0 = 0$. Otherwise, inductively solve f for T: Start by choosing a linear form $T_1 \in k[X,Y]$ such that $\mathrm{taylor}(f,2) = T_1^2$. Supposing that $1 < j < s-1$ and $T_j = T + O(j+1)$ has already been computed, write

$$\mathrm{taylor}(f - T_j^2,\ j+2) = 2T_1 \cdot m,$$

with $m \in k[X,Y]$ homogeneous of degree $j+1$, and set $T_{j+1} = T_j + m$.

Lemma 6. *Let C have a singularity of type A_n, $n \geq 1$, at $P = (0,0)$. Set $s = \left\lfloor \frac{n+1}{2} \right\rfloor$, and let T_{s-1} be defined as above. Then $\mathfrak{G}(P)$ is the homogenization of*

$$\langle X^s,\ T_{s-1},\ Y^s \rangle \subset k[X,Y]$$

with respect to Z.

Proof. The case $n = 1$ is clear, so we may suppose $n \geq 2$. If $\mathfrak{G}' = \langle X^s,\ T_{s-1},\ Y^s \rangle \subset k[X,Y]$, then $\mathfrak{G}'_Q = \mathscr{O}_{C,Q}$ for all $Q \in C \setminus \{P\}$, so it suffices to show that $\mathfrak{G}'_P = \mathscr{C}_B$, where $B = \mathscr{O}_{C,P}$. For this, we pass to the completion

$$\widehat{B} = k[[x,y]] = k[[X,Y]]/\langle f(X,Y) \rangle,$$

and consider the isomorphism

$$A = k[[t,w]] = k[[T,W]]/\left\langle T^2 + W^{n+1} \right\rangle \to \widehat{B},\ t \mapsto T(x,y), w \mapsto W(x,y).$$

An analysis of the normalization algorithm applied to A shows that

[3] The notation $O(m)$ stands for terms of degree $\geq m$.

$$\overline{A} = \sum_{i=0}^{n-s} k[[t]] \cdot w^i + \sum_{i=n-s+1}^{n} k[[t]] \cdot \frac{w^i}{t},$$

and that it takes $s = \left\lfloor \frac{n+1}{2} \right\rfloor$ steps to reach $\overline{A}$ (see [11, Sect. 4]). Hence,

$$\mathscr{C}_A = \langle t, w^s \rangle_A, \text{ so that } \mathscr{C}_{\widehat{B}} = \langle T(x,y), W(x,y)^s \rangle_{\widehat{B}}.$$

Working in $k[[X,Y]]$, we write

$$T = aX + bY \text{ and } W = cX + dY,$$

where $a,b,c,d \in k[[X,Y]]$ are such that $ad-bc$ is a unit in $k[[X,Y]]$. Since $\langle X,Y\rangle = \langle T,W\rangle$, it follows that $\langle X,Y\rangle^s = \langle T,W\rangle^s \subset \langle T,W^s\rangle$. Since $\langle X,Y\rangle = \langle X,T\rangle$ or $\langle X,Y\rangle = \langle T,Y\rangle$, we have $W^s \in \langle X,Y\rangle^s \subset \langle X^s,T,Y^s\rangle$. We conclude that

$$\langle X^s, T, Y^s \rangle = \langle T, W^s \rangle.$$

If $s > 1$, then $\langle X,Y\rangle = \langle X,T_{s-1}\rangle$ or $\langle X,Y\rangle = \langle T_{s-1},Y\rangle$. Hence, for any s, we have $\langle X,Y\rangle^s \subset \langle X^s,T_{s-1},Y^s\rangle$. We conclude that

$$\langle X^s, T_{s-1}, Y^s \rangle = \langle X^s, T, Y^s \rangle.$$

Now recall that B is an excellent ring, which implies that $\overline{\widehat{B}} = \widehat{\overline{B}}$ (see, for example, [11, Sect. 1]). It follows that

$$\mathscr{C}_{\widehat{B}} = \mathrm{Hom}_{\widehat{B}}\left(\overline{\widehat{B}}, B\right) = \mathrm{Hom}_B\left(\overline{B}, B\right) \otimes_B \widehat{B} = \mathscr{C}_B \otimes_B \widehat{B}. \tag{7}$$

Since completion is faithfully flat in the case considered here, we conclude that

$$\mathscr{C}_B = \langle x^s, T_{s-1}(x,y), y^s \rangle_B.$$

Remark 21. In particular, if P is a cusp, then $\mathfrak{G}(P) = \langle X, Y\rangle$. So in Equation (6), nodes and cusps may be treated simultaneously.

If C has a singularity of type D_n at $P = (0,0)$, we may write f in the form $f = W \cdot \left(T^2 + W^{n-2}\right)$, where $T, W \in k[[X,Y]]$ is a regular system of parameters. Let $s = \left\lfloor \frac{n}{2} \right\rfloor$. We may compute the Taylor expansion $T_{s-2} \in k[X,Y]$ as follows. If $n = 4$, set $T_0 = 0$. If $n \geq 5$, choose linear forms $T_1, W_1 \in k[X,Y]$ such that $\mathrm{taylor}(f,3) = T_1^2 \cdot W_1$. For $j \leq s-2$, determine $W_j = W + O(j+1)$ as the Puiseux expansion up to order j of f corresponding to W_1. Supposing that $1 < j < s-2$ and $T_j = T + O(j+1)$ has already been computed, write

$$\mathrm{taylor}(f - T_j^2 \cdot W_{j+1},\ j+3) = 2Z_1 \cdot W_1 \cdot m,$$

with $m \in k[X,Y]$ homogeneous of degree $j+1$, and set $T_{j+1} = T_j + m$.

Lemma 7. *Let C have a singularity of type D_n, $n \geq 4$, at $P = (0,0)$. Set $s = \left\lfloor \frac{n}{2} \right\rfloor$, and let T_{s-2} be defined as above. Then $\mathfrak{G}(P)$ is the homogenization of*

$$\langle X,\ Y\rangle \cdot \left\langle X^{s-1},\ T_{s-2},\ Y^{s-1}\right\rangle \subset k[X,Y]$$

with respect to Z.

Proof. We have an isomorphism

$$A \to \widehat{B},\ q \mapsto T(x,y),\ w \mapsto W(x,y),$$

where $B = \mathscr{O}_{C,P}$ and

$$A = k[[t,w]] = k[[T,W]]/\left\langle W \cdot \left(T^2 + W^{n-2}\right)\right\rangle.$$

This time, the normalization is

$$\overline{A} = \sum_{i=0}^{n-2-s} k[[t]] \cdot w^i + \sum_{i=n-1-s}^{n-3} k[[t]] \cdot \frac{w^i}{t} + k[[t]] \cdot \frac{w^{n-2}}{t^2},$$

and it takes $s = \left\lfloor \frac{n}{2} \right\rfloor$ steps to reach $\overline{A}$ (see again [11, Sect. 4]). Hence,

$$\mathscr{C}_A = \left\langle t^2, tw, w^s\right\rangle.$$

Write

$$T = aX + bY \text{ and } W = cX + dY,$$

where $a,b,c,d \in k[[X,Y]]$ are such that $ad - bc$ is a unit in $k[[X,Y]]$. Since $\langle X,Y\rangle = \langle T,W\rangle$, we have $\langle XT,YT\rangle = \left\langle T^2,TW\right\rangle$ and $\langle X,Y\rangle^s = \langle T,W\rangle^s \subset \left\langle T^2,TW,W^s\right\rangle$. Hence,

$$\langle X,Y\rangle \cdot \left\langle X^{s-1},T,Y^{s-1}\right\rangle \subset \left\langle T^2,TW,W^s\right\rangle.$$

For the other inclusion, observe that $\langle X,Y\rangle = \langle X,T\rangle$ or $\langle X,Y\rangle = \langle T,Y\rangle$, so that $\langle X,Y\rangle^{s-1} \subset \left\langle X^{s-1},T,Y^{s-1}\right\rangle$. Hence,

$$W^s \in \langle X,Y\rangle^s \subset \langle X,Y\rangle \cdot \left\langle X^{s-1},T,Y^{s-1}\right\rangle.$$

If $s > 2$, then $\langle X,Y\rangle = \langle X,T_{s-2}\rangle$ or $\langle X,Y\rangle = \langle T_{s-2},Y\rangle$. Hence, for any s, we have $\langle X,Y\rangle^{s-1} \subset \left\langle X^{s-1},T_{s-2},Y^{s-1}\right\rangle$. We conclude that

$$\left\langle X^{s-1},T_{s-2},Y^{s-1}\right\rangle = \left\langle X^{s-1},T,Y^{s-1}\right\rangle.$$

To summarize,

$$\left\langle T^2,TW,W^s\right\rangle = \langle X,Y\rangle \cdot \left\langle X^{s-1},T,Y^{s-1}\right\rangle = \langle X,Y\rangle \cdot \left\langle X^{s-1},T_{s-2},Y^{s-1}\right\rangle,$$

so that

$$\mathscr{C}_{\widehat{B}} = \langle x,y\rangle \cdot \left\langle x^{s-1},T_{s-2}(x,y),y^{s-1}\right\rangle \subset \widehat{B}.$$

Then the claim follows as before.

Lemma 8. *Let C have a singularity of type E_n, $n = 6,7,8$, at $P = (0,0)$. Set $s = \left\lfloor \frac{n-1}{2} \right\rfloor$, and let l_1 be as in Remark 20. Then $\mathfrak{G}(P)$ is the homogenization of*

$$\langle X,\, Y\rangle \cdot \left\langle X^{s-1},\, l_1,\, Y^{s-1}\right\rangle \subset k[X,Y]$$

with respect to Z.

Proof. Depending on $n \in \{6,7,8\}$, we have an isomorphism

$$A \to \widehat{B},\, q \mapsto T(x,y),\, w \mapsto W(x,y),$$

where $B = \mathscr{O}_{C,P}$ and

$$\begin{aligned} A = k[[t,w]] &= k[[T,W]]/\left\langle T^3 + W^4 \right\rangle \text{ or} \\ A = k[[t,w]] &= k[[T,W]]/\left\langle T\left(T^2 + W^3\right)\right\rangle \text{ or} \\ A = k[[t,w]] &= k[[T,W]]/\left\langle T^3 + W^5 \right\rangle. \end{aligned}$$

In each case, by [11, Sect. 4],

$$\overline{A} = k[[w]] \cdot 1 + k[[w]] \cdot \frac{t}{w} + k[[w]] \cdot \frac{t^2}{w^s},$$

which implies that

$$\mathscr{C}_A = \left\langle t^2, tw, w^s \right\rangle.$$

The same argument as in the proof of Lemma 7 shows that

$$\mathscr{C}_{\widehat{B}} = \langle x,y\rangle \cdot \left\langle x^{s-1}, T_{s-2}(x,y), y^{s-1}\right\rangle \subset \widehat{B},$$

and the claim follows as before. Note that $T_{s-2} = 0$ if $s = 2$, and $T_{s-2} = l_1$ if $s = 3$.

In principle, we could pursue a similar strategy for all singularities classified by Arnold in [5]. However, in [12], we give an algorithm which, for plane curves in characteristic zero, allows us to compute the local contributions to the normalization for a broad class of singularities in a direct way. Combining the approach of Section 6 with this algorithm or with modular techniques and normalization as described in Section 8 below, we already get a very efficient algorithm for computing $\mathfrak{G}$.

8 Parallel computation using modular techniques

Algorithm 3 is parallel in nature since the computations of the local adjoint ideals do not depend on each other. In this section, in the case where the given curve is defined over $\mathbb{Q}$, we describe a modular way of parallelizing Algorithm 3 even further. One possible approach is to replace the computations of the Gröbner bases involved,

the computation of the (minimal) associated primes in the singular locus, and the computations yielding the normalizations by their modular variants as introduced in [4], [40], and [7]. These variants are either probabilistic or require expensive tests to verify the results at the end. To reduce the number and complexity of the verification tests, we provide a direct modularization for the adjoint ideal algorithm. The approach we propose requires only the verification of the final result: In the next section, we give efficient conditions for checking whether the result obtained is indeed the Gorenstein adjoint ideal.

Our approach relies on the general scheme for modular computations presented in [10] and provided, in fact, motivation for developing the scheme. This is based on error tolerant rational reconstruction (a short account of which will be given in Remark 23 below) and can handle *bad primes*[4], provided there are only finitely many such primes. Referring to [10] for details, we will now outline the main ideas behind the scheme.

Fix a global monomial ordering $>$ on the monoid of monomials in the variables $X = \{X_0, \ldots, X_r\}$. Consider the polynomial rings $R = \mathbb{Q}[X]$ and, given an integer $N \geq 2$, $R_N = (\mathbb{Z}/N\mathbb{Z})[X]$. If $H \subset R$ or $H \subset R_N$ is a set of polynomials, then denote by $\mathrm{LM}(H) := \{\mathrm{LM}(h) \mid h \in H\}$ its set of leading monomials.

If $\frac{a}{b} \in \mathbb{Q}$ with $\gcd(a,b) = 1$ and $\gcd(b,N) = 1$, set $\left(\frac{a}{b}\right)_N := (a + N\mathbb{Z})\,(b + N\mathbb{Z})^{-1} \in \mathbb{Z}/N\mathbb{Z}$. If $f \in R$ is a polynomial such that N is coprime to any denominator of a coefficient of f, then its *reduction modulo* N is the polynomial $f_N \in R_N$ obtained by mapping each coefficient c of f to c_N. If $H = \{h_1, \ldots, h_s\} \subset R$ is a set of polynomials such that N is coprime to any denominator of a coefficient of any h_i, set $H_N = \{(h_1)_N, \ldots, (h_s)_N\}$. If $J \subset R$ is an ideal, we write

$$J_0 = J \cap \mathbb{Z}[X] \text{ and } J_N = \langle f_N \mid f \in J_0 \rangle \subset R_N,$$

and call J_N *the reduction of* J *modulo* N. We also write $(R/J)_N = R_N/J_N$.

As a first step towards the modular algorithm, we explain how to compute the reduction of a given ideal $J \subset R$ modulo a prime, supposing that a Gröbner basis for J is already known.

Lemma 9. *With notation as above, let $J \subset R$ be an ideal, let $H = \{h_1, \ldots, h_s\}$ be a Gröbner basis for J with elements $h_i \in \mathbb{Z}[X]$, and let p be a prime not dividing any of the leading coefficients* $\mathrm{LC}(h_i)$. *Then for every $f \in J \cap \mathbb{Z}[X]$, there exists an integer $d \in \mathbb{Z}$ not divisible by p, and such that $df \in \langle H \rangle_{\mathbb{Z}[X]}$.*

Proof. Let $f \in J \cap \mathbb{Z}[X]$. Then, since H is a Gröbner basis for J, there exists an $h_i \in H$ such that $\mathrm{LM}(f)$ is divisible by $\mathrm{LM}(h_i)$. We hence have a representation $\mathrm{LC}(h_i) \cdot f = m \cdot h_i + f^{(1)}$ with $f^{(1)} \in J \cap \mathbb{Z}[X]$, and such that $\mathrm{LM}(f) > \mathrm{LM}(f^{(1)})$. Proceeding with $f^{(1)}$ instead of f and continuing that way, we get an integer $d \in \mathbb{Z}$ and a representation $df = \sum_{i=1}^{s} \xi_i h_i$ as desired.

Corollary 4. *If J, H, and p are as above, then $J_p = \langle H_p \rangle_{\mathbb{F}_p[X]}$.*

[4] In our context, a prime p is *bad* if Algorithm 3, applied to the modulo p values of the input over the rationals, does not return the reduction of the characteristic zero result.

Proof. Given $f \in J \cap \mathbb{Z}[X]$, let $df = \sum_{i=1}^{s} \xi_i h_i$ be a representation as above. Then $d_p f_p = \sum_{i=1}^{s} (\xi_i)_p (h_i)_p$. We conclude that $f_p \in \langle H_p \rangle_{\mathbb{F}_p[X]}$.

Corollary 5. *With J and H as above, let p be a prime such that H_p is a Gröbner basis with* $\mathrm{LM}(H) = \mathrm{LM}(H_p)$. *Then* $J_p = \langle H_p \rangle_{\mathbb{F}_p[X]}$.

We now fix the following setup for the rest of this section:

Notation 8 *Let $\Gamma \subset \mathbb{P}^r_{\mathbb{Q}}$ be an integral non-degenerate projective algebraic curve, let $I(\Gamma)$ be the ideal of Γ in R, and let $G(0) \subset R$ be the reduced Gröbner basis of $\mathfrak{G}(\Gamma)$. If p is a prime such that* $\mathrm{LM}(I(\Gamma)) = \mathrm{LM}(I(\Gamma)_p)$, *and $I(\Gamma)_p$ is radical and defines an integral non-degenerate projective algebraic curve in $\mathbb{P}^r_{\mathbb{F}_p}$, then write Γ_p for this curve and $G(p) \subset R_p$ for the reduced Gröbner basis of $\mathfrak{G}(\Gamma_p)$.*

Remark 22. There are only finitely many primes p for which the desired conditions on $I(\Gamma)_p$ in Notation 8 are not satisfied. Since these conditions can be checked using Gröbner bases and square-free decomposition, we may reject such a prime if we encounter it in the modular algorithm. In the following discussion, we will ignore these bad primes for simplicity of the presentation. In particular, we will assume that the Gröbner bases $G(p)$ are defined for all primes p.

The basic idea of the modular adjoint ideal algorithm can now be described as follows: First, choose a set of primes $\mathscr{P}$ and compute $G(p)$ for each $p \in \mathscr{P}$. Second, lift the $G(p)$ coefficientwise to a set of polynomials $G \subset R$. Provided that $\mathfrak{G}(\Gamma)_p = \mathfrak{G}(\Gamma_p)$ for each $p \in \mathscr{P}$, we then expect that G is a Gröbner basis which coincides with our target Gröbner basis $G(0)$.

The lifting process consists of two steps. First, use Chinese remaindering to lift the $G(p) \subset R_p$ to a set of polynomials $G(N) \subset R_N$, with $N := \prod_{p \in \mathscr{P}} p$. Second, compute a set of polynomials $G \subset R$ by lifting the coefficients occurring in $G(N)$ to rational coefficients. Here, to identify Gröbner basis elements corresponding to each other, we require that $\mathrm{LM}(G(p)) = \mathrm{LM}(G(q))$ for all $p, q \in \mathscr{P}$. This leads to condition (L2) in the definition below:

Definition 9. With notation as above, a prime p is called *lucky* if

(L1) $\mathfrak{G}(\Gamma)_p = \mathfrak{G}(\Gamma_p)$ and
(L2) $\mathrm{LM}(G(0)) = \mathrm{LM}(G(p))$.

Otherwise p is called *unlucky*.

Lemma 10. *All but finitely many primes are lucky.*

Proof. As is clear from the proof of [10, Lemma 5.5], it is enough to show that condition (L1) is true for all but finitely many primes. For this, we may assume that Γ does not have singularities at $X_0 = 0$. Then for all but finitely many primes p, the curve Γ_p does not have singularities at $X_0 = 0$.

Let C be the affine part of Γ in the chart $X_0 \neq 0$. Write $A = \mathbb{Q}[X_1, \ldots, X_r]/I(C)$. Using a Gröbner basis argument as summarized in [10, Remark 5.3], it is shown

in [7, Section 4] that $(\overline{A})_p = \overline{A_p}$ for all but finitely many primes p. So if we write $\overline{A} = \frac{1}{d}U$, with an ideal $U \subset A$ and an element $0 \neq d \in A$, and $\overline{A_p} = \frac{1}{d(p)}U(p)$, with an ideal $U(p) \subset A_p$ and an element $0 \neq d(p) \in A_p$, then

$$(d_p : U_p) = (d(p) : U(p))$$

for all but finitely many primes p.

Computing an ideal quotient amounts to another Gröbner basis computation. Hence, we may again apply [10, Remark 5.3] to conclude that

$$(d : U)_p = (d_p : U_p)$$

for all but finitely many primes p.

Summing up, the result follows from Propositions 4 and 5.

When performing the modular algorithm, condition (L1) can only be checked a posteriori: We compute $G(p)$ and, thus, $\mathfrak{G}(\Gamma_p)$ on our way, but $\mathfrak{G}(\Gamma)_p$ is only known to us after $G(0)$ and, thus, $\mathfrak{G}(\Gamma)$ has been computed. This is not a problem, however, since the finitely many primes where $\mathfrak{G}(\Gamma)_p \neq \mathfrak{G}(\Gamma_p)$ will not influence the final result if we apply error tolerant rational reconstruction as discussed now.

Remark 23. Let N' and M be integers with $\gcd(N', M) = 1$, let $N = N' \cdot M$, and let $\frac{a}{b} \in \mathbb{Q}$ with $\gcd(a,b) = \gcd(N', b) = 1$. Set $\bar{r}_1 := \left(\frac{a}{b}\right)_{N'} \in \mathbb{Z}/N'\mathbb{Z}$, let $\bar{r}_2 \in \mathbb{Z}/M\mathbb{Z}$ be arbitrary, and denote by $\bar{r}$, with $0 \leq r \leq N-1$, the image of $(\bar{r}_1, \bar{r}_2)$ under the isomorphism

$$\mathbb{Z}/N'\mathbb{Z} \times \mathbb{Z}/M\mathbb{Z} \to \mathbb{Z}/N\mathbb{Z}.$$

Lifting $\bar{r}$ to a rational number by Gaussian reduction, starting from $(a_0, b_0) = (N'M, 0)$ and $(a_1, b_1) = (r, 1)$, we create the sequence (a_i, b_i) obtained by

$$(a_{i+2}, b_{i+2}) = (a_i, b_i) - q_i(a_{i+1}, b_{i+1}),$$

with

$$q_i = \left\lfloor \frac{\langle (a_i, b_i), (a_{i+1}, b_{i+1}) \rangle}{\|(a_{i+1}, b_{i+1})\|^2} \right\rceil.$$

Computing this sequence until $\|(a_{i+2}, b_{i+2})\| \geq \|(a_{i+1}, b_{i+1})\|$, we return `false` if $\|(a_{i+1}, b_{i+1})\|^2 \geq N$, and $\frac{a_{i+1}}{b_{i+1}}$, otherwise. By [10, Lemma 4.3], this algorithm will return $\frac{a_{i+1}}{b_{i+1}} = \frac{a}{b}$, provided that N is large enough and $M \ll N'$. More precisely, we ask that $N' > (a^2 + b^2) \cdot M$.

Definition 10. If $\mathscr{P}$ is a finite set of primes, set

$$N' = \prod_{p \in \mathscr{P} \text{ lucky}} p \quad \text{and} \quad M = \prod_{p \in \mathscr{P} \text{ unlucky}} p.$$

Then $\mathscr{P}$ is called *sufficiently large* if

$$N' > (a^2 + b^2) \cdot M$$

for any coefficient $\frac{a}{b}$ of any polynomial in $G(0)$ (assume $\gcd(a,b)=1$).

Lemma 11. *If $\mathscr{P}$ is a sufficiently large set of primes satisfying condition* (L2)*, then the reduced Gröbner bases $G(p)$, $p \in \mathscr{P}$, lift via Chinese remaindering and error tolerant rational reconstruction to the reduced Gröbner basis $G(0)$.*

Proof. By Lemma 10, condition (L1) holds for all but finitely many primes p. Hence, since $\mathscr{P}$ is sufficiently large, the result follows as in the proof of [10, Lemma 5.6] from [10, Lemma 4.3].

Lemma 10 guarantees, in particular, that a sufficiently large set $\mathscr{P}$ of primes satisfying condition (L2) exists. So from a theoretical point of view, the idea of finding $G(0)$ is now as follows: Consider such a set $\mathscr{P}$, compute the reduced Gröbner bases $G(p)$, $p \in \mathscr{P}$, and lift the results to $G(0)$.

From a practical point of view, however, we face the problem that condition (L2) can only be checked a posteriori. On the other hand, as already pointed out, we need that the $G(p)$, $p \in \mathscr{P}$, have the same set of leading monomials in order to identify corresponding Gröbner basis elements in the lifting process. To remedy this situation, we suggest to proceed in a randomized way: First, fix an integer $t \geq 1$ and choose a set of t primes $\mathscr{P}$ at random. Second, compute $\mathscr{G} = \{G(p) \mid p \in \mathscr{P}\}$, and use a majority vote on the set of lead monomials to choose a subset of $\mathscr{G}$ such that all Gröbner bases in the subset have the same set of lead monomials:

DELETEBYMAJORITYVOTE: *Define an equivalence relation on $\mathscr{P}$ by setting $p \sim q :\Longleftrightarrow \mathrm{LM}(G(p)) = \mathrm{LM}(G(q))$. Then replace $\mathscr{P}$ by the equivalence class of largest cardinality,*[5] *and change $\mathscr{G}$ accordingly.*

Now, all $G(p)$, $p \in \mathscr{P}$, have the same set of leading monomials. Hence, we can apply the error tolerant lifting algorithm to the coefficients of the Gröbner bases in $\mathscr{G}$. If this algorithm returns `false` at some point, we enlarge the set $\mathscr{P}$ by t primes not used so far, and repeat the whole process. Otherwise, the lifting yields a set of polynomials $G \subset R$. Furthermore, if $\mathscr{P}$ is sufficiently large, all primes in $\mathscr{P}$ satisfy condition (L2). Since we cannot check, however, whether $\mathscr{P}$ is sufficiently large, a final verification step over $\mathbb{Q}$ is required. We will establish such a test in Section 9 below. Since this test is particularly expensive if $G \neq G(0)$, we first perform a test in positive characteristic in order to increase our chances that the two sets are equal:

PTEST: *Randomly choose a prime $p \notin \mathscr{P}$ which does neither divide the numerator nor the denominator of any coefficient occurring in any polynomial in G. Return* `true` *if $G_p = G(p)$, and* `false` *otherwise.*

If PTEST returns `false`, then $\mathscr{P}$ is not sufficiently large (or the extra prime chosen in PTEST is bad). In this case, we enlarge $\mathscr{P}$ as above and repeat the process. If PTEST returns `true`, however, then most likely $G = G(0)$. Only now, we verify the result over $\mathbb{Q}$. If the verification fails, we again enlarge $\mathscr{P}$ and repeat the process.

[5] We have to use a weighted cardinality count: when enlarging $\mathscr{P}$, the total weight of the elements already present must be strictly smaller than the total weight of the new elements. Otherwise, though highly unlikely in practical terms, it may happen that only unlucky primes are accumulated.

9 Verification

Throughout this section, we consider a curve $\Gamma \subset \mathbb{P}^r_{\mathbb{Q}}$ with Gorenstein adjoint ideal $\mathfrak{G} = \mathfrak{G}(\Gamma) \subset R = \mathbb{Q}[X]$ as in Notation 8. Our goal is to derive a criterion which, in combination with the procedure pTEST from the previous section, provides an effective way of checking whether the result of our modular algorithm is correct. The verification is based on the following observation obtained from Lemma 3:

If $I \subset R$ is a homogeneous ideal, then $I = \mathfrak{G}$ iff the following hold:

1. I is saturated and $I(\Gamma) \subsetneqq I$,
2. $\deg \Delta(I) = \deg I + \delta(\Gamma)$, and
3. $\deg I = \deg \mathfrak{G}$.

To turn this into an algorithmic criterion, we need some preparations. If A is any reduced Noetherian algebra over a field k, then, as a direct generalization of the definition from Section 3, we can associate to A the delta invariant

$$\delta_k(A) = \dim_k \overline{A}/A.$$

Proposition 8. *Let $B \to A$ be a homomorphism of reduced Noetherian rings. Suppose:*

1. *$(B, \mathfrak{m})$ is a normal local domain with perfect residue class field k;*
2. *the natural homomorphism $B \to \widehat{B}$ from B to its completion $\widehat{B}$ is normal;*
3. *A is a formally equidimensional Nagata ring;*
4. *A is a flat B-algebra, $\mathfrak{m}A$ is contained in every maximal ideal of A, the ring $A/\mathfrak{m}A$ is reduced, and $\delta_k(A/\mathfrak{m}A) < \infty$;*
5. *$\overline{A}/A$ is a finite B-module;*
6. *the unique map $\overline{A}/\mathfrak{m}\overline{A} \to \overline{A/\mathfrak{m}A}$ which factorizes the normalization map $A/\mathfrak{m}A \to \overline{A/\mathfrak{m}A}$ as*
$$A/\mathfrak{m}A \to \overline{A}/\mathfrak{m}\overline{A} \to \overline{A/\mathfrak{m}A}$$
is injective.

Then

$$\delta_{\mathrm{Q}(B)}(A \otimes_B \mathrm{Q}(B)) \leq \delta_k(A/\mathfrak{m}A).$$

Proof. See [44, Prop. 2.1.1(i)] for the factorization in (6) and [44, Prop. 3.3] for the proof of the proposition.

Corollary 6. *With notation as above, let p be a prime such that $I(\Gamma)_p$ is radical and defines an integral non-degenerate curve $\Gamma_p \subset \mathbb{P}^r_{\mathbb{F}_p}$. Then*

$$\delta(\Gamma) \leq \delta(\Gamma_p).$$

Proof. Write $X' = \{X_1, \ldots, X_r\}$. We may assume that Γ has no singularities at $X_0 = 0$. Let C be the affine part of Γ in the chart $X_0 \neq 0$ as before. Write

$$J = I(C) \cap \mathbb{Z}[X'] \text{ and } I(C)_p = \left\langle f_p \mid f \in J \right\rangle \subset \mathbb{F}_p[X'].$$

Then J is a prime ideal of height $r-1$, $\langle p,J\rangle$ is a prime ideal, and $J\cap\mathbb{Z}=\langle 0\rangle$. The claim follows by applying Proposition 8 to $(B,\mathfrak{m})=(\mathbb{Z}_{\langle p\rangle},\langle p\rangle)$ and $A=\mathbb{Z}_{\langle p\rangle}[X']/J\,\mathbb{Z}_{\langle p\rangle}[X']$ since, in this case, $A\otimes_B \mathrm{Q}(B)=\mathbb{Q}[X']/I(C)$, $A/\mathfrak{m}A=\mathbb{F}_p[X']/I(C)_p$, and conditions (1) through (6) of the proposition are satisfied. Indeed, this is clear for (1), while (2) holds since B is excellent. We have (3) since A is of finite type over B and $J\mathbb{Z}_{\langle p\rangle}[X']$ is a prime ideal. Moreover, (4) is satisfied since A is a torsion-free B-module, $\langle p,J\rangle$ is a prime ideal, and $\mathrm{Spec}(A/\mathfrak{m}A)$ is a curve. We get (5) since $A/\mathscr{C}_A$ is a finite B-module and $\overline{A}/\mathscr{C}_A$ is a finite $A/\mathscr{C}_A$-module. Finally, condition (6) holds by Lemma 12 below: Taking into account that $\mathrm{Q}(A)=\mathrm{Q}(\mathbb{Z}[X']/J)$, the lemma gives us a canonical map

$$\overline{A}\to\overline{A/mA},\ \alpha=\frac{\overline{a}}{\overline{b}}\mapsto\frac{a \bmod \langle p,J\rangle}{b \bmod \langle p,J\rangle},$$

where $a,b\in\mathbb{Z}[X']$, with $b\notin\langle p,J\rangle$, and where $\overline{a},\overline{b}$ denote the images of a,b in A. Since $\alpha=\frac{\overline{a}}{\overline{b}}$ is in the kernel of this map iff $a\in\langle p,J\rangle$, we get an injective map $\overline{A}/\mathfrak{m}\overline{A}\to\overline{A/\mathfrak{m}A}$ which factorizes the normalization map as desired.

Before deriving Lemma 12, we illustrate condition (6) by an example.

Example 10. Let $(B,\mathfrak{m})=(\mathbb{Z}_{\langle 3\rangle},\langle 3\rangle)$ and $A=\mathbb{Z}_{\langle 3\rangle}[X,Y]/\left\langle X^3+Y^3+Y^5\right\rangle$. Then $\overline{A/\mathfrak{m}A}=\left\langle 1,\frac{x}{y},\frac{(x+y)^2}{y^3}\right\rangle_{A/\mathfrak{m}A}$ and $\overline{A}=\left\langle 1,\frac{x}{y},\frac{x^2}{y^2}\right\rangle_A$. We compute $\delta_{\mathbb{Q}}(A\otimes_B\mathbb{Q})=3$ and $\delta_{\mathbb{F}_3}(A/\mathfrak{m}A)=4$, and find that

$$\overline{A}/\mathfrak{m}\overline{A}=\left\langle 1,\frac{x}{y},\frac{x^2}{y^2}\right\rangle_{A/\mathfrak{m}A}\subsetneq\left\langle 1,\frac{x}{y},\frac{(x+y)^2}{y^3}\right\rangle_{A/\mathfrak{m}A}=\overline{A/\mathfrak{m}A}.$$

Lemma 12. *With notation as in the proof of Corollary 6, for any $\alpha\in\overline{A}$, there exist $a,b\in\mathbb{Z}[X']$ with $b\notin\langle p,J\rangle$ and $\alpha=\frac{\overline{a}}{\overline{b}}\in\mathrm{Q}(A)=\mathrm{Q}(\mathbb{Z}[X']/J)$.*

Proof. For $\alpha\in\overline{A}$, there are $a,b\in\mathbb{Z}[X']$ with $b\notin J$ and $\alpha=\frac{a \bmod J}{b \bmod J}$, and there are $a_0,\ldots,a_{m-1}\in\mathbb{Z}[X']$ and $d\in\mathbb{Z}$ with $p\nmid d$ and

$$\alpha^m+\frac{a_{m-1} \bmod J}{d}\alpha^{m-1}+\ldots+\frac{a_0 \bmod J}{d}=0.$$

Then $d\cdot a^m+a_{m-1}\cdot ba^{m-1}+\ldots+a_0\cdot b^m\in J$.

If $b_0=b\in\langle p,J\rangle$, then $d\cdot a^m\in\langle p,J\rangle$. Hence, since (p,J) is prime, $a\in\langle p,J\rangle$. Then $a=pa_1+c_1$ and $b=pb_1+d_1$ for some $a_1,b_1\in\mathbb{Z}[X']$ and some $c_1,d_1\in J$. If $b_1\in\langle p,J\rangle$, we can iterate the process. Inductively, as long as $b_{s-1}\in\langle p,J\rangle$, we obtain $a_s,b_s\in\mathbb{Z}[X']$ and $c_s,d_s\in J$ with $a=p^sa_s+c_s$ and $b=p^sb_s+d_s$. If b_s were in $\langle p,J\rangle$ for all s, then $b\in\bigcap_s\langle p^s,J\rangle=J$, contradicting our assumption on b. Thus, there is an s with $b_s\notin\langle p,J\rangle$. Then

$$\alpha=\frac{a \bmod J}{b \bmod J}=\frac{p^sa_s \bmod J}{p^sb_s \bmod J}=\frac{a_s \bmod J}{b_s \bmod J}.$$

Notation 9 *Let $I \subset R$ be a saturated homogeneous ideal such that $I(\Gamma) \subsetneqq I$, let m be an integer, and let $g \in I$ be a homogeneous polynomial of degree m not contained in $I(\Gamma)$. Let* $\operatorname{div}(g)$ *be the divisor cut out by g on $\overline{\Gamma}$, let $D(g) = \operatorname{div}(g) - \Delta(I)$ be the corresponding divisor in $|mH - \Delta(I)|$, and let $d(g) = \deg D(g)$. Furthermore, write $\widetilde{d}(g)$ for the degree of the part of $D(g)$ away from* $\operatorname{Sing}(\Gamma)$.

Given a prime p, use the same notation for Γ_p and g_p if these are defined.

Note that $\deg \operatorname{div}(g) = m \cdot \deg \Gamma$ and $\widetilde{d}(g) \leq d(g)$.

Theorem 10. *Let $I \subset R$ be a saturated homogeneous ideal such that $I(\Gamma) \subsetneqq I$, let m be an integer, let $g \in I$ be a homogeneous polynomial of degree m not contained in $I(\Gamma)$, and let p be a prime. With notation as above, suppose:*

1. *$I(\Gamma)_p$ is radical and defines an integral non-degenerate curve $\Gamma_p \subset \mathbb{P}^r_{\mathbb{F}_p}$;*
2. *g_p is defined and non-zero;*
3. *Γ and Γ_p have the same Hilbert polynomial;*
4. *I_p is an adjoint ideal of Γ_p;*
5. *$\deg I = \deg I_p$;*
6. *m is large enough to ensure that $\left|mH_p - \Delta(I_p)\right|$ is nonspecial;*
7. *$\widetilde{d}(g_p) = (\deg \Gamma) \cdot m - \deg I_p - \delta(\Gamma)$.*

Then

$$\delta(\Gamma) = \delta(\Gamma_p),\ \widetilde{d}(g) = d(g),\ \textit{and}\ \deg \Delta(I) = \deg \Delta(I_p).$$

Moreover, I is an adjoint ideal of Γ, and we have

$$\deg \Delta(I) = (\deg \Gamma) \cdot m - \widetilde{d}(g_p).$$

Proof. By (3), we have

$$\deg(\Gamma) = \deg(\Gamma_p) \ \text{ and } \ p_a(\Gamma) = p_a(\Gamma_p). \tag{8}$$

Moreover, since (1) holds, it follows from Corollary 6 that $\delta(\Gamma) \leq \delta(\Gamma_p)$. Hence, taking (4) and Lemma 3 into account, we get

$$\begin{aligned} \widetilde{d}(g_p) \leq d(g_p) &= (\deg \Gamma_p) \cdot m - \deg \Delta(I_p) \\ &= (\deg \Gamma) \cdot m - \deg I_p - \delta(\Gamma_p) \\ &\leq (\deg \Gamma) \cdot m - \deg I_p - \delta(\Gamma). \end{aligned}$$

By (6), this chain of inequalities is an equality, so that

$$\widetilde{d}(g_p) = d(g_p) = (\deg \Gamma_p) \cdot m - \deg \Delta(I_p) \tag{9}$$

and

$$\delta(\Gamma) = \delta(\Gamma_p). \tag{10}$$

Together with Lemma 3 and conditions (4) and (5), this implies that

$$\deg \Delta(I_p) = \deg I_p + \delta(\Gamma_p) = \deg I + \delta(\Gamma) \geq \deg \Delta(I), \tag{11}$$

or equivalently that

$$d(g_p) \leq d(g). \tag{12}$$

Next, in the main part of the proof, we show equality in (12). For this, we consider the closed subscheme

$$X = V(I(\Gamma)_0) \subset \mathbb{P}^r_{\mathbb{Z}} \xrightarrow{\Pi} \operatorname{Spec}\mathbb{Z}$$

with projection Π and fibers $X_q = X \times_{\operatorname{Spec}\mathbb{Z}} \operatorname{Spec}\kappa(\langle q\rangle)$. Then the fiber over the generic point $\langle 0\rangle \in \operatorname{Spec}\mathbb{Z}$ is $X_0 = \Gamma$, while over $\langle p\rangle$ we have $X_p = \Gamma_p$. Since Γ and Γ_p have the same Hilbert polynomial by (3), there is a Zariski open subset $V \subset \operatorname{Spec}\mathbb{Z}$ containing p and such that the Hilbert polynomial is constant on V. It follows that the restriction map $\Pi_V : X_V = \Pi^{-1}(V) \to V$ constitutes a flat family (see [38, Ch. III, Thm. 9.9]).

Since $\delta(\Gamma_p) = \delta(\Gamma)$, the δ-constant criterion for simultaneous normalization (see [44, Cor. 3.3.1]) implies that there is a Zariski open subset $U \subset V \subset \operatorname{Spec}\mathbb{Z}$ containing p and such that $\pi_U : X_U = \Pi^{-1}(U) \to U$ is equinormalizable. That is, there is a finite map $\nu : \overline{X} \to X_U$ such that $\overline{\Pi} := \Pi_U \circ \nu$ is flat with non-empty geometrically normal fibers, and such that for each $\langle q\rangle \in U$ the induced map of fibers $\nu_q : \overline{X}_q \to X_q$ is the normalization map.

By construction of I, the family of sheaves defined by $I_0 = I \cap \mathbb{Z}[X]$ is flat over a Zariski open subset of U containing both $\langle 0\rangle$ and $\langle p\rangle$. Hence, the semi-continuity theorem (see, for example, [47, Ch. 5, Thm. 3.20]) implies that the dimensions of the linear series induced by I on $\overline{\Gamma}$ and I_p on $\overline{\Gamma}_p$ satisfy

$$h^0\left(\overline{\Gamma}_p, \mathscr{O}_{\overline{\Gamma}_p}(mH_p - \Delta(I_p))\right) \geq h^0\left(\overline{\Gamma}, \mathscr{O}_{\overline{\Gamma}}(mH - \Delta(I))\right).$$

Hence $d(g_p) \geq d(g)$ by condition (7) and Riemann-Roch, and since $p(\Gamma_p) = p(\Gamma)$ by (8) and (10). Taking (9) and (12) into account, it follows that

$$\widetilde{d}(g_p) = d(g_p) = d(g).$$

The second equality translates into $\deg\Delta(I_p) = \deg\Delta(I)$, so that I is an adjoint ideal by Lemma 3 and (11). Finally,

$$(\deg\Gamma)\cdot m - \deg\Delta(I) = (\deg\Gamma_p)\cdot m - \deg\Delta(I_p) = \widetilde{d}(g_p).$$

Corollary 7. *In the situation of Theorem 10, suppose that all assumptions of the theorem are satisfied. Suppose in addition that I_p is the Gorenstein adjoint ideal of Γ_p. Then I is the Gorenstein adjoint ideal of Γ.*

Proof. Theorem 10 already tells us that I is an adjoint ideal of Γ. In particular, $I \subset \mathfrak{G}$ and, thus, $\deg I \geq \deg\mathfrak{G}$. This implies that

$$\deg\Delta(\mathfrak{G}) = \deg\mathfrak{G} + \delta(\Gamma) \leq \deg I + \delta(\Gamma) = \deg\Delta(I) = \deg\Delta(I_p), \tag{13}$$

where the last equality holds by the theorem. On the other hand, since we suppose that I_p is the Gorenstein adjoint ideal of Γ_p, we have

$$\dim\left|mH_p - \Delta(I_p)\right| \geq \dim|mH - \Delta(\mathfrak{G})|$$

for m large enough by semi-continuity. Hence, by Riemann-Roch and since $\delta(\Gamma_p) = \delta(\Gamma)$ by the theorem, we have

$$\deg \Delta(I_p) \leq \deg \Delta(\mathfrak{G})$$

(see Lemma 3 and its proof). This shows that (13) is an equality. In particular,

$$\deg I = \deg \mathfrak{G}.$$

We conclude that $I = \mathfrak{G}$.

Remark 24. In the final verification step of our modular algorithm for computing $\mathfrak{G}$, if G denotes the result of the lifting process as in the previous section, we randomly choose one of the primes $p \in \mathscr{P}$ already used in the lifting process, and apply Theorem 10 to the ideal $I = \langle G \rangle$. For this, we need to know whether the assumptions of the theorem hold. Checking condition (2) is trivial, while conditions (1) and (3) are fulfilled by construction (see Remark 22 and step 6 of Algorithm 6 below, where we in particular check that $\mathrm{LM}(I(\Gamma)) = \mathrm{LM}(I(\Gamma)_p)$). Similarly conditions (4) and (5) are fulfilled since by construction $G_p = G(p)$ and thus $I_p = \mathfrak{G}(\Gamma_p)$. With respect to condition (6), we will comment on how to choose m in Lemma 13 below. Finally, since we know how to compute $\delta(\Gamma)$, we can also check condition (7) (see step 18 of Algorithm 6).

In the situation above, if all assumptions of Theorem 10 are fulfilled, then by the assertions of the theorem, we may rewrite the formula in condition (7) as

$$\widetilde{d}(g) = \deg(\Gamma) \cdot m - \deg \Delta(\mathfrak{G}). \tag{14}$$

So in order to expect that condition (7) holds for a given m and randomly chosen $g \in I_m$ and $p \in \mathscr{P}$, the degree m needs to be large enough so that equation (14) is satisfied. The following lemma specifies an appropriate bound for m, which is also sufficient to guarantee that condition (6) is fulfilled.

Lemma 13. *Consider an integer m such that $\mathrm{P}_\Gamma(m) - 1 \geq p_a(\Gamma)$, and suppose that $g \in \mathfrak{G}_m$ is generic. Then* (14) *is satisfied, and $|mH - \Delta(\mathfrak{G})|$ is nonspecial.*

Proof. By assumption and since $\mathrm{P}_\Gamma(m) = (\deg \Gamma) \cdot m - p_a(\Gamma) + 1$, we have

$$(\deg \Gamma) \cdot m \geq 2p_a(\Gamma).$$

On the other hand, by Lemma 3 and Corollary 3,

$$\deg \Delta(\mathfrak{G}) \leq 2\delta(\Gamma).$$

Putting these inequalities together, we get

$$(\deg \Gamma) \cdot m - \deg \Delta(\mathfrak{G}) \geq 2p_a(\Gamma) - 2\delta(\Gamma) = 2p(\Gamma).$$

In particular, $|mH - \Delta(\mathfrak{G})|$ is base-point free, which implies that $d(g) = \widetilde{d}(g)$ since g is generic. Furthermore, by reason of its degree, $|mH - \Delta(\mathfrak{G})|$ is nonspecial.

Remark 25. For a plane curve Γ of degree n the condition $\mathrm{P}_\Gamma(m) - 1 \geq p_a(\Gamma)$ means that $n \cdot m \geq (n-1)(n-2)$, which is satisfied for $m \geq n-2$.

We summarize our approach in Algorithm 6.

Algorithm 6 Modular adjoint ideal

Input: A curve $\Gamma \subset \mathbb{P}^r_{\mathbb{Q}}$ satisfying the conditions of Notation 8.
Output: The Gorenstein adjoint ideal $\mathfrak{G}(\Gamma)$.

choose an integer $t \geq 1$
$\mathscr{P} = \mathscr{G} = \emptyset$
loop
  choose a list $\mathscr{Q}$ of t random primes not used so far
  for all $p \in \mathscr{Q}$ **do**
    if $I(\Gamma)_p$ satisfies the conditions of Notation 8 **then**
      compute the reduced Gröbner basis $G(p)$ of $\mathfrak{G}(\Gamma_p) \subset R_p$ (via Alg. 3)
      $\mathscr{P} = \mathscr{P} \cup \{p\}$, $\mathscr{G} = \mathscr{G} \cup \{G(p)\}$
  $(\mathscr{G}, \mathscr{P}) = \text{DELETEBYMAJORITYVOTE}(\mathscr{G}, \mathscr{P})$
  lift $(\mathscr{G}, \mathscr{P})$ to a set of polynomials $G \subset R$ via the Chinese remainder theorem and Gaussian reduction
  if the lifting succeeds **and** $\text{PTEST}(I(\Gamma), G, \mathscr{P})$ **then**
    if G is a Gröbner basis **and** $\langle G \rangle$ is saturated **then**
      choose m such that $\mathrm{P}_\Gamma(m) - 1 \geq p_a(\Gamma)$
      choose $g \in \langle G \rangle_m$ at random
      choose a prime $p \in \mathscr{P}$
      if g_p is defined and non-zero **then**
        M_p = Jacobian ideal of $I(\Gamma)_p$
        compute $\widetilde{d}(g_p) = \deg\left((I(\Gamma_p) + \langle g_p \rangle) : M_p^\infty\right)$
        compute $\delta(\Gamma)$
        if $\widetilde{d}(g_p) = \deg(\Gamma) \cdot m - \deg\langle G(p) \rangle - \delta(\Gamma)$ **then**
          return $\langle G \rangle$

Remark 26. In Algorithm 6, the $G(p)$, $p \in \mathscr{P}$, can be computed in parallel. Each individual computation, in turn, can be parallelized by partitioning the singular loci.

Remark 27. The most expensive step of the verification is the computation of $\delta(\Gamma)$. If we skip the verification, the algorithm will become probabilistic. That is, the output can only be expected to be the Gorenstein adjoint ideal, with high probability.

Skipping the verification usually accelerates the algorithm considerably. This gives us, in particular, a fast probabilistic way to compute both the geometric genus $p(\Gamma)$ and $\deg \Delta(\mathfrak{G}) = \dim_{\mathbb{Q}} \left(\overline{\mathbb{Q}[C]}/\mathscr{C}_{\mathbb{Q}[C]} \right)$.

10 Timings

The algorithms for adjoint ideals presented in this paper are implemented in the SINGULAR library `adjointideal.lib` (see [13]). They make use of the normalization algorithm of Section 2 either in its local or local to global variant, as appropriate. These variants, in turn, are part of the SINGULAR library `locnormal.lib` (see [8]).

In this section, we compare the performance of the different algorithms. Specifically, we consider

`LA`	Mnuk's global linear algebra approach (Algorithm 1),
`IQ`	the global ideal quotient approach (Algorithm 2),
`locIQ`	the local ideal quotient approach (Algorithm 3 using Algorithm 4),
`locIQP2`	the local ideal quotient approach for plane curves with the improvements of Section 7 concerning ordinary multiple points and singularities of type *ADE*, and
`modLocIQ`	the modular local ideal quotient strategy (Algorithm 6).

For the modular approach, we do not make use of a local analysis of the singular locus except for computing the invariants needed in the verification step.

To quantify the improvement in computation time obtained by omitting the verification step in the modular approach, we give timings for the *resulting, now probabilistic, version of Algorithm 6 (denoted by* `modLocIQ'` *in the tables)*. Note that in all examples where we could check the output of the modular algorithm by computing the desired Gröbner basis also directly over $\mathbb{Q}$, the result was indeed correct.

To quantify the contributions of the different normalization algorithms and to provide a lower bound for any adjoint ideal algorithm using them, we also specify the computation times for the normalization step in SINGULAR via the local to global approach outlined in Section 2 (denoted by `locNormal`), and for finding an integral basis in MAPLE via the algorithm of van Hoeij (denoted by `Maple-IB`). Once being fully implemented in SINGULAR, we expect further improvements of the performance by computing the local contribution or just an integral basis of the local ring by the algorithm discussed in [12]. Since this algorithm and van Hoeij's algorithm rely on Puiseux series, they work in characteristic zero only.

All timings are in seconds on an AMD Opteron 6174 machine with 48 cores, 2.2GHz, and 128GB of RAM running a Linux operating system. A dash indicates that the computation did not finish within 10000 seconds. The *timings for parallel computations are marked by the symbol * and the maximum number of cores used in parallel is indicated in brackets*.

Remark 28. All examples are defined over the field of rationals. For `locIQ`*, the number of cores used corresponds to the number of components of the decomposition of the singular locus over $\mathbb{Q}$. For `modLocIQ`*, the number of cores used in a given iteration of the algorithm is obtained by summing up the number of components modulo p over all primes $p \in \mathscr{Q}$ chosen in Step 4 of Algorithm 6.

To show the power of the modular algorithm, we give simulated parallel timings even if the number of processes exceeds the number of cores available on our machine (which is a valid approach since the algorithm has basically zero communication overhead). For the single-core timings of `modLocIQ`, we *indicate in square brackets the number of primes used by the algorithm.*

Now we turn to explicit examples. First we consider rational plane curves defined by a random parametrization of degree n. These curves have $\binom{n-1}{2}$ ordinary double points. Their defining equations $f_{1,n}$ were generated by the function `randomRatCurve` from the SINGULAR library `paraplanecurves.lib` (see [9]), using the random seed 1 and a random parametrization with coefficients of bitlength 15. For the resulting timings, see Table 1. We observe that the detection

Table 1 Timings for curves given by a random parametrization.

	$f_{1,5}$	$f_{1,6}$	$f_{1,7}$
deg	5	6	7
`locNormal`	2.1	56	-
`Maple-IB`	5.1	47	318
`LA`	98	4400	-
`IQ`	2.1	56	-
`locIQ`	1.3	54	3800
`locIQ`*	1.3 (1)	54 (1)	3800 (1)
`locIQP2`	.18	1.2	49
`locIQP2`*	.18 (1)	1.2 (1)	49 (1)
`modLocIQ`	6.4 [33]	19 [53]	150 [75]
`modLocIQ'`	6.2 [33]	18 [53]	104 [75]
`modLocIQ`*	.36 (74)	1.6 (153)	51 (230)
`modLocIQ'`*	.21 (74)	.48 (153)	5.2 (230)

of special types of singularities is fast and yields the best performance among the non-probabilistic algorithms, while the modular local strategy provides a very fast probabilistic algorithm.

To compare the algorithms at a single singularity, we consider plane curves with exactly one A_n respectively D_n singularity at the origin of the affine chart $\{Z \neq 0\}$ (ignoring singularities at infinity). For the modular approach, we omit verification since this step relies on global properties of the curve. The curves with affine equation $f_{2,n,d} = Y^2 + X^{n+1} + Y^d$, $n \geq 1$, $d \geq 3$, have precisely one singularity of type A_n at the origin. The curves with affine equation $f_{3,n,d} = X(X^{n-1} + Y^2) + Y^d$, $n \geq 2$, $d \geq 3$, have exactly one singularity of type D_n at the origin. For timings, see Tables 2 and 3, respectively. In both examples, the best strategy is `IQ` since we consider only one singularity and since no coefficients of large bitlength occur.

Table 2 Timings for curves with one singularity of type A_n.

	$f_{2,5,10}$	$f_{2,5,100}$	$f_{2,5,500}$	$f_{2,50,100}$	$f_{2,50,500}$	$f_{2,400,500}$
deg	10	100	500	100	500	500
`locNormal`	.12	.12	.12	.51	.51	3.6
`Maple-IB`	.08	1.5	96	4.7	150	630
`LA`	.18	140	-	150	-	-
`IQ`	.12	.12	.12	.51	.51	3.6
`modLocIQ'`	.20 [2]	.22 [2]	.96 [2]	1.1 [2]	2.0 [2]	11 [2]
`modLocIQ'*`	.10 (2)	.13 (2)	.48 (2)	.54 (2)	1.2 (2)	5.8 (2)

Table 3 Timings for curves with one singularity of type D_n.

	$f_{3,5,10}$	$f_{3,5,100}$	$f_{3,5,500}$	$f_{3,50,100}$	$f_{3,50,500}$	$f_{3,400,500}$
deg	10	100	500	100	50	500
`locNormal`	.15	.15	.15	.67	.67	4.9
`Maple-IB`	.05	1.7	100	34	1830	-
`LA`	.20	140	-	140	-	-
`IQ`	.15	.15	.15	.67	.67	5.0
`modLocIQ'`	.22 [2]	.23 [2]	.23 [2]	1.5 [2]	1.5 [2]	24 [2]
`modLocIQ'*`	.09 (2)	.10 (2)	.10 (2)	.74 (2)	.77 (2)	17 (2)

The plane curves with defining equations

$$f_{4,n} = \left(X^{n+1}+Y^{n+1}+Z^{n+1}\right)^2 - 4\left(X^{n+1}Y^{n+1}+Y^{n+1}Z^{n+1}+Z^{n+1}X^{n+1}\right)$$

were given in [Hirano 1992] and have $3(n+1)$ singularities of type A_n if n is even. To ensure that all singularities of the curves are in the affine chart $\{Z \neq 0\}$, we substitute $Z = 2X - 3Y + 1$. For timings, see Table 4.

Table 4 Timings for curves with many A_n-singularities.

	$f_{4,4}$	$f_{4,6}$	$f_{4,8}$
deg	10	14	18
`locNormal`	1.6	-	-
`Maple-IB`	2.2	14	70
`LA`	89	-	-
`IQ`	2.5	-	-
`locIQ`	.96	-	-
`locIQ*`	.36 (6)	-	-
`locIQP2`	1.0	-	-
`locIQP2*`	.38 (6)	-	-
`modLocIQ`	3.7 [3]	23 [4]	190 [4]
`modLocIQ'`	3.3 [3]	20 [4]	170 [4]
`modLocIQ*`	.63 (27)	4.4 (48)	50 (48)
`modLocIQ'*`	.38 (27)	2.2 (48)	30 (48)

To conclude this section, we present examples of curves in higher-dimensional projective space. As above, we first consider curves with only one singularity in a given affine chart: let L_n be the ideal of the image of

$$\mathbb{A}^1 \longrightarrow \mathbb{A}^3, t \mapsto (t^{n-2}, t^{n-1}, t^n).$$

Second, denote by I_n the ideal of the image in $\mathbb{P}^5$ under the degree-2 Veronese embedding of the curve $\{f_{4,n} = 0\}$. For the resulting timings, see Table 5.

Table 5 Timings for non-planar curves.

	L_{25}	L_{50}	I_4	I_6
deg	25	50	20	28
`locNormal`	3.9	84	21	-
`IQ`	3.9	84	30	-
`locIQ`	3.9	84	18	-
`locIQ`*	3.9 (1)	84 (1)	7.5 (6)	-
`modLocIQ'`	6.5 [2]	220 [2]	74 [5]	2600 [5]
`modLocIQ'`*	3.3 (2)	140 (2)	4.0 (45)	59 (69)

To summarize, we observe that the ideal quotient approach is faster than the linear algebra one. To some extent, this is due to the lack of efficiency of the rational function arithmetic in SINGULAR. The local strategy is faster than the global one if there is more than one component in the decomposition of the singular locus over $\mathbb{Q}$. In addition, the local algorithm can be run in parallel and is, then, even faster. In most examples, especially when the coefficients have large bitlength, the fastest approach is the modular local strategy, which parallelizes in a two-fold way, via localization and modularization. Note that, even if the singular locus of the curve is irreducible over the rationals, by Chebotarev's density theorem the singular locus is likely to decompose when passing to a finite field (see, for example, $f_{1,7}$). In contrast to other modular algorithms (such as modular normalization), the verification step is usually very fast.

Acknowledgements. We would like to thank Gert-Martin Greuel, Christoph Lossen, Thomas Markwig, Mathias Schulze, and Frank Seelisch for helpful discussions.

References

1. Adams, W. W.; Loustaunau, P.: *An introduction to Gröbner bases*, Graduate Studies in Mathematics, 3, AMS (1994).
2. Arbarello, E.; Ciliberto, C.: *Adjoint hypersurfaces to curves in $\mathbb{P}^r$ following Petri*, in Commutative Algebra, Lecture Notes in Pure and Applied Mathematics, vol. 84, Dekker, New York, 1-21 (1983).
3. Arbarello, E.; Cornalba M.; Griffiths, P. A.; Harris, J.: *Geometry of Algebraic Curves*, Volume I. Springer (1985).

4. Arnold, E. A.: *Modular algorithms for computing Gröbner bases*, Journal of Symbolic Computation 35, 403-419 (2003).
5. Arnold, V.I.; Gusein-Zade, S.M.; Varchenko, A.N.: *Singularities of Differential Maps*, Volume I. Birkhäuser (1995).
6. Böhm, J.: *Parametrisierung rationaler Kurven*. Diploma thesis, Institut für Mathematik und Physik der Universität Bayreuth (1999).
7. Böhm, J.; Decker, W.; Laplagne, S.; Pfister, G.; Steenpaß, A.; Steidel, S.: *Parallel Algorithms for Normalization*. J. Symbolic Comput. 51, 99-114 (2013).
8. Böhm, J.; Decker, W.; Laplagne, S.; Pfister, G.; Steenpaß, A.; Steidel, S.: *locnormal.lib - A* SINGULAR *4-1-0 library for computing integral bases of algebraic function fields*. SINGULAR distribution, http://www.singular.uni-kl.de.
9. Böhm, J.; Decker, W.; Laplagne, S.; Seelisch, F.: *paraplanecurves.lib - A* SINGULAR *4-0-2 library for computing parametrizations of rational curves*. SINGULAR distribution, http://www.singular.uni-kl.de.
10. Böhm, J.; Decker, W.; Fieker, C.; Pfister, G.: *The use of bad primes in rational reconstruction*, Math. Comp. 84, 3013-3027 (2015).
11. Böhm, J.; Decker, W.; Schulze, M.: *Local analysis of Grauert-Remmert-type normalization algorithms*. Internat. J. Algebra Comput. 24-1, 69–94 (2014).
12. Böhm, J.; Decker, W.; Laplagne, S.; Pfister, G.: *Computing integral bases via localization and Hensel lifting*. http://arxiv.org/abs/1505.05054 (2015).
13. Böhm, J.; Decker, W.; Laplagne, S.; Seelisch, F.: *adjointideal.lib - A* SINGULAR *library for computing adjoint ideals of curves*. SINGULAR distribution, http://www.singular.uni-kl.de.
14. Brieskorn, N.: *Plane algebraic curves*. Birkhäuser (1986).
15. Brill, A.; Noether, M.: *Über die algebraischen Functionen und ihre Anwendung in der Geometrie*. Math. Ann. 7, 269-310 (1874).
16. Buchweitz, R.; Greuel, G.-M: *The Milnor Number and Deformations of Complex Curve Singularities*. Inventiones Math. 58, 241-281 (1980).
17. Castelnuovo, G.: *Massima dimensione dei sistemi lineari di curve piane di dato genere*. Ann. Mat. (2) 18, 119-128 (1890).
18. Castelnuovo, G.: *Sui multipli di una serie lineare di gruppi di punti appartenenti ad una curva algebrica*. Rend. Circ. Mat. Palermo 7, 89-110 (1893).
19. Tschebotareff (Chebotarev), N.: Die Bestimmung der Dichtigkeit einer Menge von Primzahlen, welche zu einer gegebenen Substitutionsklasse gehören. Math. Ann. 95, 191-228 (1925).
20. Chiarli, N.: *Deficiency of linear series on the normalization of a space curve*. Comm. Algebra 12, 2231-2242 (1984).
21. Ciliberto, C.; Orecchia, F.: *Adjoint Ideals to Projective Curves are Locally Extended Ideals*. Bollettino U.M.I. (6) 3-B, 39-52 (1984).
22. Decker, W.; Greuel, G.-M.; Pfister, G.; de Jong, T.: *The normalization: a new algorithm, implementation and comparisons*. In: Computational methods for representations of groups and algebras (Essen, 1997), Birkhäuser (1999).
23. Decker, W.; Greuel, G.-M.; Pfister, G.; Schönemann, H.: SINGULAR *4-1-0 — A computer algebra system for polynomial computations*. http://www.singular.uni-kl.de.
24. Dieudonne, J.: *Topics in local algebra*, Notre Dame Mathematical Lectures (1967).
25. De Jong, T.: *An algorithm for computing the integral closure*. Journal of Symbolic Computation 26, 273-277 (1998).
26. De Jong, T.; Pfister, G.: *Local Analytic Geometry*. Vieweg (2000).
27. Eisenbud, D.: *Commutative Algebra with a View Toward Algebraic Geometry*. Springer (1995).
28. Gorenstein, D.: *An Arithmetic Theory of Adjoint Plane Curves*. Trans. Am. Math. Soc 72, 414-436 (1952).
29. Grauert, H.; Remmert, R.: *Analytische Stellenalgebren*. Unter Mitarbeit von O. Riemenschneider, Die Grundlehren der mathematischen Wissenschaften, Band 176. Springer (1971).
30. Greco, S.; Valabrega, P.: *On the theory of adjoints*. Lect. Notes in Math. 732, 99-123 (1979).

31. Greco, S.; Valabrega, P.: *On the theory of adjoints II*. Rendiconti del Circolo Matematico di Palermo, Serie II, Tomo XXXI, 5-15 (1982).
32. Greuel, G.-M.: *On deformations of curves and a formula of Deligne*, Algebraic Geometry (La Rábida 1981), Lecture Notes in Math. 961 (1982).
33. Greuel, G.-M.; Laplagne, S.; Seelisch, F.: *Normalization of rings*. J. Symbolic Comput. 45, no. 9, 887-901 (2010).
34. Greuel, G.-M.; Laplagne, S.; Pfister, G.: *normal.lib – A* SINGULAR *library for computing the normalization of affine rings*. SINGULAR distribution, http://www.singular.uni-kl.de.
35. Greuel, G.-M.; Lossen, C.; Shustin, E.: *Introduction to Singularities and Deformations*. Springer (2007).
36. Greuel, G.-M.; Pfister, G.: *A Singular Introduction to Commutative Algebra*. Springer (2008).
37. Gröbner, W.: *Idealtheoretischer Aufbau der algebraischen Geometrie, Teil I*. Teubner (1941).
38. Hartshorne, R.: *Algebraic Geometry*, Springer (1977).
Hirano 1992. Hirano, A.: *Construction of plane curves with cusps*. Saitama Mathematical Journal 10, 21-24 (1992).
39. Hironaka, H.: *On the arithmetic genera and the effective genera of algebraic curves*, Mem. College Sci. Univ. Kyoto Ser. A Math. Volume 30, Number 2, 177-195 (1957).
40. Idrees, N.; Pfister, G.; Steidel, S.: *Parallelization of Modular Algorithms*. Journal of Symbolic Computation 46, 672-684 (2011).
41. El Kahoui, M.; Moussa, Z. Y.: *An algorithm to compute the adjoint ideal of an affine plane curve*, Math. Comput. Sci. 8, 289-298 (2014).
42. Keller, O.: *Die verschiedenen Definitionen des adjungierten Ideals einer ebenen algebraischen Kurve*. Math. Ann. 159, 130-144 (1965).
43. Keller, O.: *Vorlesungen über algebraische Geometrie*. Akademische Verlagsgesellschaft (1974).
44. Lipman, J.: *A numerical criterion for simultaneous normalization*. Duke Math. J. 133 (2), 347-390 (2006).
45. Kornerup, P.; Gregory, R. T.: *Mapping Integers and Hensel Codes onto Farey Fractions*. BIT Numerical Mathematics 23(1), 9-20 (1983).
46. Le Brigand, D.; Risler, J. J. : *Algorithme de Brill-Nother et codes de Goppa*. Bulletin de la S. M. F. 116, 231-253 (1988).
47. Liu, Q.: *Algebraic Geometry and Arithmetic Curves*, Oxford University Press (2002).
48. MAPLE (Waterloo MAPLE Inc.): MAPLE. http: //www.maplesoft.com/ (2012).
49. Matlis, E.: *1-dimensional Cohen-Macaulay rings*. Lecture Notes in Mathematics 327. Springer (1970).
50. Milne, J. S.: *Étale cohomology*, Princeton University Press (1980).
51. Milnor, T.: *Singular Points of Complex Hypersurfaces*. Ann. of Math. Studies 61. Princeton (1968).
52. Mnuk, M.: *An algebraic approach to computing adjoint curves*. J. Symbolic Comput., 23(2-3), 229-240 (1997).
53. Orecchia, F.; Ramella, I.: On the Computation of the Adjoint Ideal of Curves with Ordinary Singularities, Appl. Math. Sciences Vol. 8, no. 136, 6805-6812 (2014).
54. Petri, K.: *Über Spezialkurven I*. Math. Ann. 93, 182-209 (1924).
55. Pfister, G.; Sahin, N.; Viazovska, M.: *curvepar.lib – A* SINGULAR *library for invariants of space curve singularities*. SINGULAR distribution, http://www.singular.uni-kl.de.
56. Riemann, B.: *Theorie der Abel'schen Functionen*. Journal für reine und angew. Math., Bd. 54, Nr. 14, 115-155 (1857).
57. Sendra, J. R.; Winkler, F.: *Parametrization of algebraic curves over optimal field extensions. Parametric algebraic curves and applications* (Albuquerque, NM, 1995). J. Symbolic Comput. 23, no. 2-3, 191-207 (1997).
58. Sendra, J. R.; Winkler, F.; Perez-Diaz, S.: *Rational Algebraic Curves*. Algorithms and Computation in Mathematics, Vol. 22. Springer (2008).
59. Shafarevich, I. R.: *Algebraic Geometry I*, Springer (1994).
60. van der Waerden, B. L.: *Einführung in die algebraische Geometrie*. Die Grundlehren der Mathematischen Wissenschaften (1939).

61. van Hoeij, M.: *An algorithm for computing an integral basis in an algebraic function field*. J. Symbolic Comput. 18, no. 4, 353-363 (1994).
62. Swanson, I.; Huneke, C.: *Integral closure of ideals, rings, and modules*. Cambridge University Press (2006).
63. Zariski, O.; Samuel, P.: *Commutative Algebra I*. Springer (1975).