Journal of Symbolic Computation 51 (2013) 99–114

Contents lists available at SciVerse ScienceDirect

Journal of Symbolic Computation

www.elsevier.com/locate/jsc

Parallel algorithms for normalization

Janko Böhm [a], Wolfram Decker [a], Santiago Laplagne [b], Gerhard Pfister [a], Andreas Steenpaß [a], Stefan Steidel [a]

[a] *Department of Mathematics, University of Kaiserslautern, Erwin-Schrödinger-Str., 67663 Kaiserslautern, Germany*
[b] *Departamento de Matemática, FCEN, Universidad de Buenos Aires, Ciudad Universitaria, Pabellón I, (C1428EGA) Buenos Aires, Argentina*

ARTICLE INFO

Article history:
Received 14 October 2011
Accepted 23 March 2012
Available online 4 July 2012

Keywords:
Normalization
Integral closure
Test ideal
Grauert–Remmert criterion
Modular computation
Parallel computation

ABSTRACT

Given a reduced affine algebra A over a perfect field K, we present parallel algorithms to compute the normalization $\overline{A}$ of A. Our starting point is the algorithm of Greuel et al. (2010), which is an improvement of de Jong's algorithm (de Jong, 1998; Decker et al., 1999). First, we propose to stratify the singular locus $\mathrm{Sing}(A)$ in a way which is compatible with normalization, apply a local version of the normalization algorithm at each stratum, and find $\overline{A}$ by putting the local results together. Second, in the case where $K = \mathbb{Q}$ is the field of rationals, we propose modular versions of the global and local-to-global algorithms. We have implemented our algorithms in the computer algebra system SINGULAR and compare their performance with that of the algorithm of Greuel et al. (2010). In the case where $K = \mathbb{Q}$, we also discuss the use of modular computations of Gröbner bases, radicals, and primary decompositions. We point out that in most examples, the new algorithms outperform the algorithm of Greuel et al. (2010) by far, even if we do not run them in parallel.

1. Introduction

Normalization is an important concept in commutative algebra, with applications in algebraic geometry and singularity theory. We are interested in computing the normalization $\overline{A}$ of a reduced affine K-algebra A, where K is a perfect field. For this, a number of algorithms have been proposed, but not all of them are of practical interest (see the historical account in Greuel et al., 2010). A milestone is

E-mail addresses: boehm@mathematik.uni-kl.de (J. Böhm), decker@mathematik.uni-kl.de (W. Decker), slaplagn@dm.uba.ar (S. Laplagne), pfister@mathematik.uni-kl.de (G. Pfister), steenpass@mathematik.uni-kl.de (A. Steenpaß), steidel@mathematik.uni-kl.de (S. Steidel).

0747-7171/$ – see front matter
http://dx.doi.org/10.1016/j.jsc.2012.07.002

de Jong's algorithm (de Jong, 1998; Decker et al., 1999), which is based on the normality criterion of Grauert and Remmert (1971), and which has been implemented in SINGULAR (see Decker et al., 2012), MACAULAY2 (see Grayson and Stillman, 2010), and MAGMA (see Bosma et al., 1997). The algorithm of Greuel et al. (2010) (*GLS normalization algorithm* for short), which is also based on the Grauert and Remmert criterion, is an improvement of de Jong's algorithm. It is implemented in SINGULAR. The algorithm proposed by Leonard and Pellikaan (2003) and Singh and Swanson (2009) is designed for the characteristic p case. It is implemented in SINGULAR and MACAULAY2 and works well for small p.

In view of modern multi-core computers, the parallelization of fundamental algorithms becomes increasingly important. Our objective in this paper is to present parallel versions of the GLS normalization algorithm in that we reduce the general problem to computational problems which are easier and do not depend on each other. It turns out that in most cases, the new algorithms outperform the GLS algorithm by far, even if we do not run them in parallel.

We start in Section 2 by reviewing the basic ideas of the GLS algorithm. In particular, we recall the normality criterion of Grauert and Remmert. In Section 3, we present a local version of the normality criterion which applies to a stratification of the singular locus $\mathrm{Sing}(A)$ of A. This allows us to find $\overline{A}$ by a local-to-global approach. Section 4 contains a discussion of modular methods for the GLS algorithm and its local-to-global version. Timings are presented in Section 5.

2. The GLS normalization algorithm

Referring to Greuel et al. (2010) and Greuel and Pfister (2007) for details and proofs, we sketch the GLS normalization algorithm. We begin with some general remarks. For these, A may be any reduced Noetherian ring.

Definition 1. Let A be a reduced Noetherian ring. The *normalization* of A, written $\overline{A}$, is the integral closure of A in its total ring of fractions $\mathrm{Q}(A)$. We call A *normal* if $A = \overline{A}$.

We write

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

for the *spectrum* of A and $V(J) = \{P \in \mathrm{Spec}(A) \mid P \supseteq J\}$ for the *vanishing locus* of an ideal J of A. If $P \in \mathrm{Spec}(A)$, then A_P denotes the localization of A at P. More generally, if S is a multiplicatively closed subset of A and M is an A-module, then $S^{-1}M$ denotes the localization of M at S.

Taking into account that normality is a local property, we call

$$N(A) = \left\{P \in \mathrm{Spec}(A) \;\middle|\; A_P \text{ is not normal}\right\}$$

the *non-normal locus* of A. Furthermore, we write

$$\mathrm{Sing}(A) = \left\{P \in \mathrm{Spec}(A) \;\middle|\; A_P \text{ is not regular}\right\}$$

for the *singular locus* of A. Then $N(A) \subseteq \mathrm{Sing}(A)$.

Remark 2. A Noetherian local ring of dimension one is normal if and only if it is regular. See de Jong and Pfister (2000, Theorem 4.4.9).

Definition 3. Let A be a reduced Noetherian ring. The *conductor* of A in $\overline{A}$ is the ideal

$$\mathcal{C}_A = \mathrm{Ann}_A(\overline{A}/A) = \{a \in A \mid a\overline{A} \subseteq A\}.$$

Lemma 4. *Let A be a reduced Noetherian ring. Then $N(A) \subseteq V(\mathcal{C}_A)$. Furthermore, $\overline{A}$ is module-finite over A if and only if $\mathcal{C}_A$ contains a non-zerodivisor of A. In this case, $N(A) = V(\mathcal{C}_A)$.*

To state the aforementioned Grauert and Remmert criterion, we need:

Lemma 5. *Let A be a reduced Noetherian ring, and let $J \subseteq A$ be an ideal containing a non-zerodivisor g of A. Then the following hold:*

(1) *If $\varphi \in \operatorname{Hom}_A(J, J)$, then 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*

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

where $\varphi_a : J \to J$ denotes the multiplication by $a \in A$.

Proposition 6. *(See Grauert and Remmert, 1971.) Let A be a reduced Noetherian ring, and let $J \subseteq A$ be an ideal satisfying the following conditions:*

(1) *J contains a non-zerodivisor g of A,*
(2) *J is a radical ideal,*
(3) *$V(\mathcal{C}_A) \subseteq V(J)$.*

Then A is normal iff $A \cong \operatorname{Hom}_A(J, J)$ via the map which sends a to φ_a.

Definition 7. A pair (J, g) as in Proposition 6 is called a *test pair* for A, and J is called a *test ideal* for A.

By Lemma 4, test pairs exist iff $\overline{A}$ is module-finite over A. Given such a pair (J, g), the idea of finding $\overline{A}$ is to successively enlarge A until the normality criterion allows us to stop (since A is Noetherian, this will eventually happen in the module-finite case). Starting from $A_0 = A$, we get a chain of extensions of reduced Noetherian rings

$$A = A_0 \subseteq \cdots \subseteq A_{i-1} \subseteq A_i \subseteq \cdots \subseteq A_m = \overline{A}.$$

Here, $A_{i+1} = \operatorname{Hom}_{A_i}(J_i, J_i) \cong \frac{1}{g}(gJ_i :_{A_i} J_i)$, where J_i is the radical of the extended ideal JA_i, for $i \geqslant 1$. Note that (J_i, g) is indeed a test pair for A_i:

Remark 8. (See Greuel et al., 2010, Prop. 3.2.) Let A be a reduced Noetherian ring such that $\overline{A}$ is module-finite over A, and let $A \subseteq A' \subseteq \overline{A}$ be an intermediate ring. Clearly, every non-zerodivisor $g \in A$ of A is a non-zerodivisor of $\mathrm{Q}(A)$. In particular, it is a non-zerodivisor of A'. Furthermore, if $\mathcal{C}_{A'}$ is the conductor of A' in $\overline{A'} = \overline{A}$, then $\mathcal{C}_{A'} \supseteq \mathcal{C}_A$. It follows that every prime ideal $Q \in N(A') = V(\mathcal{C}_{A'})$ contracts to a prime ideal $P = Q \cap A \in N(A) = V(\mathcal{C}_A)$. Hence, if (J, g) is a test pair for A, then $P \supseteq J$, which implies that $Q \supseteq \sqrt{JA'} =: J'$. We conclude that (J', g) is a test pair for A'.

Explicit computations rely on explicit representations of the A_i as A-algebras. These will be obtained as an application of Lemma 9 below. To formulate the lemma, we use the following notation. Let $J \subseteq A$ be an ideal containing a non-zerodivisor g of A, and let A-module generators $u_0 = g, u_1, \ldots, u_s$ for $gJ :_A J$ be given. Choose variables $T_1, \ldots, T_s$, and consider the epimorphism

$$\Phi : A[T_1, \ldots, T_s] \to \frac{1}{g}(gJ :_A J), \quad T_i \mapsto \frac{u_i}{g}.$$

The kernel of Φ describes the A-algebra relations on the u_i/g. We single out two types of relations:

- Each A-module syzygy

$$\alpha_0 u_0 + \alpha_1 u_1 + \cdots + \alpha_s u_s = 0, \quad \alpha_i \in A,$$

gives an element $\alpha_0 + \alpha_1 T_1 + \cdots + \alpha_s T_s \in \ker \Phi$, which we call a *linear relation*.

- Developing each product $\frac{u_i}{g}\frac{u_j}{g}$, $1 \leqslant i \leqslant j \leqslant s$, as a sum $\frac{u_i}{g}\frac{u_j}{g} = \sum_k \beta_{ijk}\frac{u_k}{g}$, we get elements $T_iT_j - \sum_k \beta_{ijk}T_k$ in $\ker\Phi$, which we call *quadratic relations*.

It is easy to see that these linear and quadratic relations already generate $\ker\Phi$. We thus have:

Lemma 9. *Let A be a reduced Noetherian ring, and let $J \subseteq A$ be an ideal containing a non-zerodivisor g of A. Then, given A-module generators $u_0 = g, u_1, \dots, u_s$ for $gJ :_A J$, we have an isomorphism of A-algebras*

$$A[T_1, \dots, T_s]/R \cong \frac{1}{g}(gJ :_A J), \quad T_i \mapsto \frac{u_i}{g},$$

where R is the ideal generated by the linear and quadratic relations described above.

The following result from Greuel et al. (2010) will allow us to find the normalization in a way such that all calculations except the computation of the radicals $\sqrt{J_i}$ can be carried through in the original ring A:

Theorem 10. *Let A be a reduced Noetherian ring, let $J \subseteq A$ be an ideal containing a non-zerodivisor g of A, let $A \subseteq A' \subseteq \mathrm{Q}(A)$ be an intermediate ring such that A' is module-finite over A, and let $J' = \sqrt{JA'}$. Let U and H be ideals of A and $d \in A$ such that $A' = \frac{1}{d}U$ and $J' = \frac{1}{d}H$, respectively. Then*

$$\left(gJ' :_{A'} J'\right) = \frac{1}{d}(dgH :_A H) \subseteq \mathrm{Q}(A).$$

Remark 11. In the case where $A = K[X_1 \dots, X_n]/I$ is a reduced affine algebra over a field K, let $P_1, \dots, P_r$ be the associated primes of the radical ideal I. Then

$$\overline{A} \cong \overline{K[X_1, \dots, X_n]/P_1} \times \dots \times \overline{K[X_1, \dots, X_n]/P_r},$$

and $\overline{A}$ is module-finite over A by Emmy Noether's finiteness theorem (see Swanson and Huneke, 2006). Thus, using techniques for primary decomposition as in Greuel et al. (2010, Remark 4.6), the computation of normalization can be reduced to the case where A is an affine domain (that is, I is a prime ideal). When writing our algorithms in pseudocode, we will always start from a domain A. Talking about a non-zerodivisor then just means to talk about a non-zero element.

Remark 12. If A is an affine domain over a perfect field K, we can apply the Jacobian criterion (see Eisenbud, 1995): If M is the Jacobian ideal[1] of A, then M is non-zero and contained in the conductor $\mathcal{C}_A$ (see Greuel et al., 2010, Lemma 4.1). Hence, we may choose $\sqrt{M}$ together with any non-zero element g of $\sqrt{M}$ as an initial test pair. Implementing all this, the GLS normalization algorithm will find an ideal $U \subseteq A$ and a denominator $d \in \mathcal{C}_A$ such that

$$\overline{A} = \frac{1}{d}U \subseteq \mathrm{Q}(A).$$

Since M is contained in $\mathcal{C}_A$, any non-zero element of M is valid as a denominator: If $0 \neq c \in M$, then $c \cdot \frac{1}{d}U =: U'$ is an ideal of A, so that $\frac{1}{d}U = \frac{1}{c}U'$.

For the purpose of comparison with the local approach of the next section, we illustrate the GLS algorithm by an example:

[1] The *Jacobian ideal* of A is generated by the images of the $c \times c$ minors of the Jacobian matrix $(\frac{\partial f_i}{\partial x_j})$, where c is the codimension, and $f_1, \dots, f_r$ are polynomial generators for I.

Example 13. For

$$A = K[x, y] = K[X, Y]/\langle X^4 + Y^2(Y-1)^3\rangle,$$

the radical of the Jacobian ideal is

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

and we can take $g := x \in J$ as a non-zerodivisor of A. In its first step, starting with the initial test pair (J, x), the normalization algorithm produces the following data:

$$U^{(1)} := xJ :_A J = \langle x, y(y-1)^2\rangle_A \quad \text{and} \quad A_1 := A[t_1] := A[T_1]/I_1 \cong \frac{1}{x}U^{(1)},$$

with relations and isomorphism given by

$$I_1 = \langle -T_1 x + y(y-1)^2, T_1 y(y-1) + x^3, T_1^2 + x^2(y-1)\rangle_{A[T_1]}$$

and

$$t_1 \mapsto \frac{y(y-1)^2}{x},$$

respectively. In the next step we find

$$\begin{aligned} J_1 &:= \sqrt{\langle x, y(y-1)\rangle_{A_1}} = \langle x, y(y-1), t_1\rangle_{A_1} \\ &= \frac{1}{x}\langle x^2, xy(y-1), y(y-1)^2\rangle_A =: \frac{1}{x}H_1. \end{aligned}$$

Using the test pair (J_1, x) and applying Theorem 10 and Lemma 9, we get

$$\begin{aligned} \frac{1}{x}(xJ_1 :_{A_1} J_1) &= \frac{1}{x^2}\left(x^2 H_1 :_A H_1\right) \\ &= \frac{1}{x^2}\langle x^2, xy(y-1), y(y-1)^2\rangle_A =: \frac{1}{x^2}U^{(2)} \end{aligned}$$

and

$$A_2 := A[t_2, t_3] := A[T_2, T_3]/I_2 \cong \frac{1}{x^2}U^{(2)},$$

with relations and isomorphism given by

$$\begin{aligned} I_2 = \langle &T_2 x - T_3(y-1), -T_3 x + y(y-1), T_2 y(y-1) + x^2, T_2 y^2(y-1)^2 + T_3 x^3, \\ &T_2^2 + (y-1), T_2 T_3 + x, T_3^2 - T_2 y\rangle \end{aligned}$$

and

$$t_2 \mapsto \frac{y(y-1)^2}{x^2}, \qquad t_3 \mapsto \frac{y(y-1)}{x},$$

respectively. In the final step, we find that A_2 is normal, so that $\overline{A} = A_2$.

3. Normalization via localization

In this section, we discuss a local-to-global approach for computing normalization. Our starting point is the following result:

Proposition 14. *Let A be a reduced Noetherian ring. Suppose that the singular locus* $\operatorname{Sing}(A) = \{P_1, \dots, P_s\}$ *is finite. For $i = 1, \dots, s$, let $S_i = A \setminus P_i$, and let an intermediate ring $A \subset A^{(i)} \subset \overline{A}$ be given such that $S_i^{-1}A^{(i)} = \overline{S_i^{-1}A}$. Then*

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

Proof. We will show a more general result in Proposition 15 below. $\square$

That $\operatorname{Sing}(A)$ is finite is, for example, true if A is the coordinate ring of a curve. Whenever $\operatorname{Sing}(A) = \{P_1, \dots, P_s\}$ is finite, the proposition allows us to find $\overline{A}$ by normalizing locally at each P_i using Proposition 16 below, and putting the local results together. In the case where $\operatorname{Sing}(A)$ is not finite, working just with the (finitely many) minimal primes in $\operatorname{Sing}(A)$ will not give the correct result. However, it is still possible to obtain $\overline{A}$ as a finite sum of local contributions: The idea is to stratify $\operatorname{Sing}(A)$ in a way which is compatible with normalization. For this, if $P \in \operatorname{Sing}(A)$, set

$$L_P = \bigcap_{P \supseteq \widetilde{P} \in \operatorname{Sing}(A)} \widetilde{P}.$$

We stratify $\operatorname{Sing}(A)$ according to the values of the function $P \mapsto L_P$. That is, if

$$\mathcal{L} = \left\{ L_P \;\middle|\; P \in \operatorname{Sing}(A) \right\}$$

denotes the set of all possible values, then the strata are the sets

$$V_L = \left\{ P \in \operatorname{Sing}(A) \;\middle|\; L_P = L \right\}, \quad L \in \mathcal{L}.$$

We write $\operatorname{Strata}(A) = \{V_L \mid L \in \mathcal{L}\}$ for the set of all strata. If $P_1, \dots, P_r$ denote the minimal primes in $\operatorname{Sing}(A)$, we have

$$\mathcal{L} \subseteq \left\{ \bigcap_{i \in \Gamma} P_i \;\middle|\; \Gamma \subseteq \{1, \dots, r\} \right\}.$$

Hence, the set of strata is finite. By construction, the singular locus is the disjoint union of all strata. For $V \in \operatorname{Strata}(A)$, write L_V for the constant value of $P \mapsto L_P$ on V.

We can now state and prove a result which is more general than Proposition 14:

Proposition 15. *Let A be a reduced Noetherian ring with stratification of the singular locus* $\operatorname{Strata}(A) = \{V_1, \dots, V_s\}$. *For $i = 1, \dots, s$, let an intermediate ring $A \subseteq A^{(i)} \subseteq \overline{A}$ be given such that $S^{-1}A^{(i)} = \overline{S^{-1}A}$ for each $S = A \setminus P$, $P \in V_i$. Then*

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

Proof. By construction, $B := \sum_{i=1}^{s} A^{(i)} \subseteq \overline{A}$. We wish to show equality. It suffices to show that if $P \in \operatorname{Spec}(A)$ is a prime ideal and $S = A \setminus P$, then $S^{-1}B = S^{-1}\overline{A}$. If $P \in \operatorname{Sing}(A)$, then $P \in V_i$ for some i. Hence, $S^{-1}A^{(i)} = \overline{S^{-1}A}$, and the local equality is obtained from the chain of inclusions

$$S^{-1}A^{(i)} \subseteq S^{-1}B \subseteq S^{-1}\overline{A} = \overline{S^{-1}A}.$$

If $P \notin \operatorname{Sing}(A)$, then $S^{-1}A$ is normal, and the local equality follows likewise from the chain of inclusions

$$S^{-1}A \subseteq S^{-1}B \subseteq S^{-1}\overline{A} = \overline{S^{-1}A}. \qquad \square$$

For a given stratum $V = V_i$, the modification of the Grauert and Remmert criterion below will allow us to find a ring $A^{(i)}$ as above along the lines of the previous section:

Proposition 16. *Let A be a reduced Noetherian ring such that $\overline{A}$ is module-finite over A, and let $A \subseteq A' \subseteq \overline{A}$ be an intermediate ring. Let $V \in \operatorname{Strata}(A)$, and let $J' = \sqrt{L_V A'}$. Suppose that L_V contains a non-zerodivisor g of A. If*

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

via the map which sends a' to $\varphi_{a'}$, then the localization $S^{-1}A'$ with $S = A \setminus P$ is normal for each $P \in V$.

Proof. The assumption and Eisenbud (1995, Proposition 2.10) give

$$S^{-1}A' \cong S^{-1}\big(\operatorname{Hom}_{A'}\big(J', J'\big)\big) \cong \operatorname{Hom}_{S^{-1}A'}\big(S^{-1}J', S^{-1}J'\big).$$

Hence, the result will follow from the Grauert and Remmert criterion (Proposition 6) applied to $S^{-1}A'$ once we show that the localized ideal $S^{-1}J'$ satisfies the three conditions of the criterion. First, since forming radicals commutes with localization, $S^{-1}J'$ is a radical ideal. Second, the image of g in $S^{-1}A'$ is a non-zerodivisor of $S^{-1}A'$ contained in $S^{-1}J'$. Third, we show that $V(\mathcal{C}_{S^{-1}A'}) = N(S^{-1}A') \subseteq V(S^{-1}J')$. For this, we first note that

$$V(\mathcal{C}_{S^{-1}A}) = N\big(S^{-1}A\big) = \big\{S^{-1}\widetilde{P} \bigm| \widetilde{P} \in N(A),\ \widetilde{P} \subseteq P\big\}.$$

Indeed, prime ideals of $S^{-1}A$ correspond to prime ideals of A contained in P. Let now $Q \in N(S^{-1}A')$. Then, as shown in Remark 8, Q contracts to some $S^{-1}\widetilde{P} \subseteq S^{-1}A$ with $\widetilde{P} \in N(A)$, $\widetilde{P} \subseteq P$. This implies that

$$Q \supseteq \sqrt{\big(S^{-1}\widetilde{P}\big)\big(S^{-1}A'\big)} = \sqrt{S^{-1}\big(\widetilde{P}A'\big)} = S^{-1}\big(\sqrt{\widetilde{P}A'}\big) \supseteq S^{-1}J',$$

as desired. $\square$

In the situation of Proposition 16, let a non-zerodivisor $g \in L_V$ of A be known. Then, using (L_V, g) instead of a test pair as in Definition 7, and proceeding as in the previous section, we get a chain of rings

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

such that $S^{-1}(A_m)$ is normal and, hence, equal to $S^{-1}\overline{A} = \overline{S^{-1}A}$ for all $S = A \setminus P$, $P \in V$.

Summing up, we are lead to Algorithms 1 and 2 below.

Algorithm 1 Normalizing the localizations

Input: An affine domain $A = K[X_1, \ldots, X_n]/I$ over a perfect field K, a stratum $V \in \operatorname{Strata}(A)$, and $0 \neq g \in L_V$.
Output: An ideal $U \subseteq A$ and $d \in A$ with $\frac{1}{d}U \subseteq \overline{A}$ and $S^{-1}(\frac{1}{d}U) = \overline{S^{-1}A}$ for all $S = A \setminus P$, $P \in V$.
1: **return** the result of the GLS normalization algorithm applied to (L_V, g);

Algorithm 2 Normalization via localization

Input: An affine domain $A = K[X_1, \ldots, X_n]/I$ over a perfect field K.
Output: An ideal $U \subseteq A$ and $d \in A$ such that $\overline{A} = \frac{1}{d}U \subseteq \mathrm{Q}(A)$.
1: $J := \sqrt{M}$, where M is the Jacobian ideal of A;
2: choose $0 \neq g \in J$;
3: compute the strata of the singular locus $\mathrm{Strata}(A) = \{V_1, \ldots, V_s\}$;
4: **for all** i **do**
5: apply Algorithm 1 to (V_i, g) to find an ideal $U_i \subseteq A$ and a power $d_i = g^{m_i}$ with $A \subseteq \frac{1}{d_i}U_i \subseteq \overline{A}$ and $S^{-1}(\frac{1}{d_i}U_i) = \overline{S^{-1}A}$ for all $S = A \setminus P$, $P \in V_i$;
6: $m := \max\{m_1, \ldots, m_s\}$, $d := g^m$, $U := \sum_i g^{m-m_i}U_i$;
7: **return** (U, d);

Remark 17. In Algorithm 2, it may be more efficient to choose possibly different non-zero elements $g_i \in L_{V_i}$. In Step 5, the algorithm computes, then, pairs (U_i', d_i) with ideals $U_i' \subseteq A$ and powers $d_i = g_i^{m_i}$. As explained in Greuel et al. (2010, Remark 4.3), starting from the (U_i', d_i), we may always find a denominator $d \in M$ and ideals $U_i \subseteq A$ such that $\frac{1}{d}U_i = \frac{1}{d_i}U_i'$ for all i. Then, the desired result is $(\sum_i U_i, d)$.

Remark 18. In Algorithm 2, it is sufficient to consider the minimal strata, that is, the strata V such that L_V is minimal with respect to inclusion. Denote, as above, the minimal primes of the singular locus of A by $P_1, \ldots, P_r$. We can obtain the minimal L_V as all possible intersections $\bigcap_{i\in\Gamma} P_i$, with subsets $\Gamma \subseteq \{1, \ldots, r\}$ which are maximal with the property that $\sum_{i\in\Gamma} P_i \neq \langle 1\rangle$.

Example 19. We come back to the coordinate ring A of the curve C with defining polynomial $f(X, Y) = X^4 + Y^2(Y-1)^3$ from Example 13 to discuss normalization via localization. The curve C has a double point of type A_3 at $(0, 0)$ and a triple point of type E_6 at $(0, 1)$. We illustrate Algorithm 2, using for both singular points the non-zerodivisor $g = x$: For the A_3-singularity, consider

$$P_1 = \langle x, y\rangle_A \quad \text{and} \quad S_1 = A \setminus P_1.$$

The local normalization algorithm yields $\overline{S_1^{-1}A} = S_1^{-1}(\frac{1}{d_1}U_1)$, where

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

For the E_6-singularity, considering

$$P_2 = \langle x, y-1\rangle_A \quad \text{and} \quad S_2 = A \setminus P_2,$$

we get $\overline{S_2^{-1}A} = S_2^{-1}(\frac{1}{d_2}U_2)$, where

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

Combining the local contributions, we get

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

with $d = x^2$ and

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

A moment's thought shows that U coincides with the ideal $U^{(2)}$ found in Example 13.

The local-to-global approach is usually much faster than the global algorithm even when not run in parallel. The reason is that the minimal primes of the singular locus are much simpler than the singular locus itself. Therefore, in the local-to-global case, the intermediate rings are much easier to handle. Most notably, the representations of the intermediate rings as affine rings involve considerably less variables than in the global case. In the following example, we exemplify this difference.

Example 20. Consider the *projective* plane curve defined by the polynomial

$$f_{1,4} = \left(X^5 + Y^5 + Z^5\right)^2 - 4\left(X^5Y^5 + X^5Z^5 + Y^5Z^5\right) \in \mathbb{Q}[X, Y, Z],$$

which will be reconsidered in Section 5 with respect to timings. After the coordinate transformation $Z \mapsto 3X - 2Y + Z$, all singularities of the projective curve lie in the affine chart $Z \neq 0$. Write

$$f = f_{1,4}(X, Y, 3X - 2Y + 1) \in \mathbb{Q}[X, Y] =: W$$

for the defining polynomial of the affine curve, and let $A = \mathbb{Q}[x, y] = W/\langle f\rangle$.

The curve has 15 singular points: the radical of the Jacobian ideal M decomposes as

$$\begin{aligned}\sqrt{M} = &\left\langle y, 121x^4 + 142x^3 + 64x^2 + 13x + 1\right\rangle \cap \langle y, 2x + 1\rangle \\ &\cap \left\langle 211y^4 - 131y^3 + 51y^2 - 11y + 1, 3x - 2y + 1\right\rangle \\ &\cap \left\langle 11y^4 - 23y^3 + 19y^2 - 7y + 1, x\right\rangle \cap \langle y + 1, x + 1\rangle \cap \langle 3y - 1, x\rangle.\end{aligned}$$

We compare the global approach to the local strategy at the singularity corresponding to the test ideal $J = \langle y, 2x + 1\rangle$.

In the local setting, we use the non-zerodivisor $g = y$ and compute the ideal quotient

$$\begin{aligned}U_1 &= gJ : J \\ &= \left\langle y, 29282x^9 + 83369x^8 + 105668x^7 + 78296x^6 + 37382x^5 + 11926x^4 + 2542x^3 \right.\\ &\qquad \left. + 349x^2 + 28x + 1\right\rangle.\end{aligned}$$

We observe that in addition to y, the ideal U_1 requires only one more generator. Hence, the representation of $A_1 \cong \frac{1}{g}(gJ : J)$ as an affine ring $A_1 = A[T_1]/I_1$ requires only one additional variable T_1. The ideal I_1 is generated by 10 linear relations and one quadratic relation. Next, we compute the radical of the image of J in A_1. Technically, this means to compute the radical $\sqrt{J + I_1}$ in the polynomial ring $W[T_1]$ (here, by abuse of notation, we denote the preimage of J in the polynomial ring also by J). The ideal I_1 is quite complicated. Since J is generated by linear polynomials, however, the reduced Gröbner basis of $J + I_1$ is very simple. It is easily computed as

$$J + I_1 = \left\langle Y, 2X + 1, 16384T_1^2 - T_1 + 625\right\rangle.$$

As a consequence, the computation of the radical

$$J_1 = \sqrt{J + I_1} = \langle Y, 2X + 1, 128T_1 - 25\rangle$$

is cheap as well. In the next step, A_2 can be represented as an affine algebra over A with, again, only one new variable. Hence, verifying that A_2 is already a local contribution to $\overline{A}$ at the singularity corresponding to J is also cheap.

In contrast, the global approach uses the test ideal $J = \sqrt{M}$, which is generated by one polynomial of degree 3 and three polynomials of degree 6. As a non-zerodivisor, we consider the lowest degree generator $g = 3x^2y - 2xy^2 + xy$. As in the local case, the first ideal quotient $gJ : J$ is easily obtained. However, in addition to g, it requires three more generators. Hence, as an affine algebra over A, it is represented as $A_1 = A[T_1, T_2, T_3]/I_1$, where the ideal of relations $I_1 \subseteq A[T_1, T_2, T_3]$ is generated by 6 linear and 6 quadratic relations. No significant reduction occurs in $J + I_1$ since J does not contain any linear polynomial. The complexity of Buchberger's algorithm grows doubly-exponentially in the number of variables. Compared to the local case, this increase in complexity makes the computation of $\sqrt{J + I_1}$ considerably more expensive. In fact, Singular does not compute the corresponding Gröbner basis within 2000 seconds.

4. Modular methods

Algorithm 2 from Section 3 is parallel in nature since the computations of the local normalizations do not depend on each other. In this section, we describe a modular way of parallelizing both the GLS normalization algorithm from Section 2 and the local-to-global algorithm from Section 3 in the case where $K = \mathbb{Q}$ is the field of rationals. One possible approach is to just replace *all* involved Gröbner basis respectively radical computations by their modular variants as introduced by Arnold (2003) and Idrees et al. (2011). These variants are either probabilistic or require rather expensive tests to verify the results at the end. In order to reduce the number of verification tests, we provide a direct modularization for the normalization algorithms. The approach we propose requires, in principle, only one verification at the end. In the local-to-global setup, however, it is reasonable to additionally handle the Gröbner basis computation for the Jacobian ideal, the subsequent primary decomposition, and the recombination of the local results by modular techniques. We exemplarily describe the modularization of the GLS normalization algorithm as outlined in Section 2. Each of the local normalizations in Algorithm 2 from Section 3 can be modularized similarly.

Fix a global monomial ordering $>$ on the semigroup of monomials in the set of variables $X = \{X_1, \ldots, X_n\}$. Consider the polynomial rings $W = \mathbb{Q}[X]$ and, given an integer $N \geqslant 2$, $W_N = (\mathbb{Z}/N\mathbb{Z})[X]$. If $T \subseteq W$ or $T \subseteq W_N$ is a set of polynomials, then denote by $\mathrm{LM}(T) := \{\mathrm{LM}(f) \mid f \in T\}$ its set of leading monomials. If $\frac{a}{b} \in \mathbb{Q}$ with $\gcd(a,b) = 1$ and $\gcd(b,N) = 1$, set $(\frac{a}{b})_N := (a + N\mathbb{Z})(b + N\mathbb{Z})^{-1} \in \mathbb{Z}/N\mathbb{Z}$. If $f \in W$ is a polynomial such that N is coprime to any denominator of a coefficient of f, then $f_N \in W_N$ is the polynomial obtained by reducing each coefficient modulo N as just described. If $H = \{h_1, \ldots, h_t\}$ is a Gröbner basis in W such that N is coprime to any denominator in any h_i, then write $H_N = \{(h_1)_N, \ldots, (h_t)_N\}$. Given an ideal $I \subseteq W$, set $I_N = \langle f_N \mid f \in I \cap \mathbb{Z}[X]\rangle \subseteq W_N$ and $(W/I)_N = W_N/I_N$.

Remark 21. For practical purposes, the ideal $I \subseteq W$ is given by a set of generators $f_1, \ldots, f_r$. Then for all but finitely many primes p, the ideal I_p can be realized via the equality

$$I_p = \big\langle (f_1)_p, \ldots, (f_r)_p \big\rangle \subseteq W_p.$$

When performing the modular algorithm described below, we reject a prime p if the ideal on the right hand side is not well-defined. Otherwise, we work with this ideal instead of I_p. The finitely many primes where the two ideals differ will not influence the result if we apply error tolerant rational reconstruction (see Remark 22).

From a practical point of view, we work with ideals of the polynomial ring W containing I, but think of them as ideals of the quotient ring $A = W/I$. Therefore, we simplify our notation as follows: If $I \subseteq J \subseteq W$ are ideals, then we denote the ideal induced by J in A also by J. Vice versa, if $J \subseteq A$ is an ideal, then its preimage in W is also denoted by J. Similarly for W_N.

From now on, $I = \langle f_1, \ldots, f_r \rangle \subseteq W$ will be a prime ideal. We wish to compute the normalization of the affine domain $A = W/I$ using modular methods. For this, we fix a polynomial $d \in W$ which represents a non-zero element in the Jacobian ideal M of A. This element of M will also be denoted by d. It will serve as a "universal denominator" for all normalizations in positive characteristic as well as for the final normalization in characteristic zero (see Remark 12 for the choice of denominators). In characteristic zero, we write $U(0)$ for the ideal of A which satisfies $\frac{1}{d}U(0) = \overline{A}$, and $G(0)$ for the reduced Gröbner basis[2] of $U(0)$. Furthermore, we write $V(0) \subseteq A[T_1, \ldots, T_s]$ for the ideal[3] of relations on the elements of $\frac{1}{d}G(0)$ which represents $\overline{A}$ as an A-algebra as in Lemma 9. We denote the reduced Gröbner basis of $V(0)$ by $R(0)$. In the same way, if p is a prime number which does not divide any

[2] Recall that reduced Gröbner bases are uniquely determined. For practical purposes, however, we do not need to reduce the Gröbner bases involved since the lifting process described below only requires that the result is uniquely determined by the algorithm.

[3] With respect to ideals of $W[T_1, \ldots, T_s]$ and $A[T_1, \ldots, T_s]$, we use the same setup and notation as for ideals of W and A.

denominator in the reduced Gröbner basis of I and such that A_p is a domain and d_p is non-zero and contained in the conductor[4] of A_p, we use $U(p)$, $G(p)$, $V(p)$, and $R(p)$ in characteristic p.

Note that $G(0)_p$ is not necessarily equal to $G(p)$. However, as we will show in Lemma 25 below, equality holds for all but finitely many primes p. Relying on this fact, the basic idea of the modular normalization algorithm can be described as follows. First, compute the Jacobian ideal M of A and choose a polynomial $d \in W$ representing a non-zero element $d \in M$. Second, choose a set $\mathcal{P}$ of prime numbers at random, and compute, for each $p \in \mathcal{P}$, reduced Gröbner bases $G(p) \subseteq W_p$ such that $\frac{1}{d_p}\langle G(p)\rangle \subseteq \mathrm{Q}(A_p)$ is the normalization of A_p. Third, lift the modular Gröbner bases to a set of polynomials $G \subseteq W$ and define $U := \langle G\rangle$. We then expect that $U = U(0)$ and $G = G(0)$.

The lifting process has two steps. First, assuming that all $\mathrm{LM}(G(p))$, $p \in \mathcal{P}$, are equal, we can lift the Gröbner bases in the set $\mathcal{GP} := \{G(p) \mid p \in \mathcal{P}\}$ to a set of polynomials $G(N) \subseteq W_N$, with $N := \prod_{p\in\mathcal{P}} p$. For this, apply the Chinese remainder algorithm to the coefficients of the corresponding polynomials occurring in the $G(p)$, $p \in \mathcal{P}$. Second, compute a set of polynomials $G \subseteq W$ by lifting the modular coefficients occurring in $G(N)$ to rational coefficients as described in Böhm et al. (2012):

Remark 22. Rational reconstruction via the Chinese remainder theorem and Gaussian reduction is error-tolerant in the following sense: Let N_1 and N_2 be integers with $\gcd(N_1, N_2) = 1$, and let $\frac{a}{b} \in \mathbb{Q}$ with $\gcd(a, b) = \gcd(N_1, b) = 1$. Set $r_1 := (\frac{a}{b})_{N_1} \in \mathbb{Z}/N_1\mathbb{Z}$, let $r_2 \in \mathbb{Z}/N_2\mathbb{Z}$ be arbitrary, and denote by r the image of (r_1, r_2) under the isomorphism

$$\mathbb{Z}/N_1\mathbb{Z} \times \mathbb{Z}/N_2\mathbb{Z} \to \mathbb{Z}/(N_1N_2)\mathbb{Z}.$$

Lifting r to a rational number via Gaussian reduction will generate, starting from $(a_0, b_0) = (N_1N_2, 0)$ and $(a_1, b_1) = (r, 1)$, a sequence of rational numbers (a_i, b_i) obtained by setting

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

where q_i is chosen such that (a_i, b_i) has minimal Euclidean length. Computing this sequence until the Euclidean length does not decrease strictly any more, we obtain a tuple (a_i, b_i) with $\frac{a_i}{b_i} = \frac{a}{b}$, provided that $N_2 \ll N_1$. For details, see Böhm et al. (2012).

Just as for $\mathcal{GP}$, we proceed for the set of reduced Gröbner bases $\mathcal{RP} := \{R(p) \mid p \in \mathcal{P}\}$ giving the modular algebra relations.

As for other modular algorithms based on Chinese remaindering, we need suitably adapted notions of a lucky prime and a sufficiently large set of lucky primes:

Definition 23. Using the notation introduced above, we define:

(1) A prime number p is called *lucky* for A if $U(0)_p = U(p)$, $V(0)_p = V(p)$, and the following hold:
   (a) A_p is a domain.
   (b) d_p is a non-zero element in the conductor of A_p.
   (c) $\mathrm{LM}(G(0)) = \mathrm{LM}(G(p))$.
   (d) $\mathrm{LM}(R(0)) = \mathrm{LM}(R(p))$.
   Otherwise p is called *unlucky* for A.

(2) A finite set $\mathcal{P}$ of lucky primes for A is called *sufficiently large* for A if

$$\prod_{p\in\mathcal{P}} p \geqslant \max\left\{2\cdot|c|^2 \;\middle|\; \begin{array}{l} c \text{ a denominator or numerator of a} \\ \text{coefficient occurring in } G(0) \text{ or } R(0)\end{array}\right\}.$$

[4] From a practical point of view, we check whether d_p is in the Jacobian ideal of A_p.

Remark 24. A modular algorithm for the basic task of computing Gröbner bases is presented in Arnold (2003) and Idrees et al. (2011). In contrast to our situation here, where we wish to find the ideal $U(0)$ by computing its reduced Gröbner basis $G(0)$, Arnold's algorithm starts from an ideal which is already given. If p is a prime number, $J \subset W$ is an ideal, $H(0)$ is the reduced Gröbner basis of J, and $H(p)$ the reduced Gröbner basis of J_p, then p is lucky for J in the sense of Arnold if $\mathrm{LM}(H(0)) = \mathrm{LM}(H(p))$. It is shown in Arnold (2003, Thms. 5.12 and 6.2) that if p is lucky for J in this sense, then $H(0)_p$ is well-defined and equal to $H(p)$. By Arnold (2003, Cor. 5.4 and Thm. 5.13), all but finitely many primes are Arnold–lucky for J. Moreover, if $\mathcal{P}$ is a set of primes satisfying Arnold's condition $\mathrm{LM}(H(0)) = \mathrm{LM}(H(p))$ for all $p \in \mathcal{P}$, and such that $\mathcal{P}$ is sufficiently large with respect to the coefficients occurring in $H(0)$, then the $H(p)$, $p \in \mathcal{P}$, lift to $H(0)$.

In our situation, if p is a prime number, we find $U(p)$ on our way, but $U(0)_p$ is only known to us after $U(0)$ has been computed. Therefore, the condition $U(0)_p = U(p)$ in our definition of lucky can only be checked a posteriori. Similarly for $V(0)_p = V(p)$. However, when performing our modular algorithm, by part 1 of Lemma 25 below and Remark 22, there are only finitely many primes not satisfying these conditions and these primes will not influence the result of the algorithm.

Lemma 25. *With notation as above, we have*:

(1) *All but a finite number of primes are lucky for A.*
(2) *If $\mathcal{P}$ is a sufficiently large set of lucky primes for A, then the reduced Gröbner bases $G(p)$, $p \in \mathcal{P}$, lift to the reduced Gröbner basis $G(0)$. In the same way, the $R(p)$, $p \in \mathcal{P}$, lift to $R(0)$.*

Proof. With respect to part 1, it is clear that conditions (1a) and (1b) in our definition of lucky are true for all but finitely many primes. Moreover, $\frac{1}{d_p}U(0)_p$ is integral over A_p for all but finitely many p. Since testing normality via the Grauert and Remmert criterion amounts to a Gröbner basis computation, and since reducing a Gröbner basis modulo a sufficiently general prime p gives a Gröbner basis of the reduced ideal, we conclude that $U(0)_p = U(p)$ for all but finitely many primes. Furthermore, if $U(0)_p = U(p)$, condition (1c) from our definition of lucky is equivalent to asking that p is lucky for $U(0)$ in the sense of Arnold, so that also this condition holds for all but finitely many primes. For $V(0)_p = V(p)$ and condition (1d), we may argue similarly since finding the ideal of algebra relations amounts to another Gröbner basis computation.

For part 2, let $\mathcal{P}$ be a sufficiently large set of lucky primes for A. Then, as pointed out above, $G(0)_p$ is well-defined and equal to $G(p)$ for all $p \in \mathcal{P}$. Furthermore, since $\mathcal{P}$ is sufficiently large, the $G(0)_p$, $p \in \mathcal{P}$, lift to $G(0)$. In the same way, we may argue for the relations. $\square$

From a theoretical point of view, the idea of the algorithm is now as follows: Consider a sufficiently large set $\mathcal{P}$ of lucky primes for A, compute the reduced Gröbner bases $G(p)$, $p \in \mathcal{P}$, and lift the results to the reduced Gröbner basis $G(0)$ as described above.

From a practical point of view, we face the problem that the conditions (1c), (1d), and (2) from Definition 23 cannot be tested a priori. To remedy the situation, we proceed in a randomized way. First, we fix an integer $t \geqslant 1$ and choose a set of t primes $\mathcal{P}$ at random. Second, we delete all primes p from $\mathcal{P}$ which do not satisfy conditions (1a) and (1b). Third, we compute $\mathcal{GP} = \{G(p) \mid p \in \mathcal{P}\}$ and $\mathcal{RP} = \{R(p) \mid p \in \mathcal{P}\}$, and use the following test to modify $\mathcal{P}$ so that all primes in $\mathcal{P}$ satisfy (1c) and (1d) with high probability:

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

Only now, we lift the Gröbner bases in $\mathcal{GP}$ and $\mathcal{RP}$ to sets of polynomials G and R, respectively. Since we do not know whether all primes in the chosen equivalence class are indeed lucky and

[5] If applicable, take Remark 27 below into account.

whether the class is sufficiently large, a final verification step is needed: We have to check whether $\frac{1}{d}\langle G\rangle$ is integral over A and normal. Since this can be expensive, especially if the result is false, we test the result at first in positive characteristic:

pTestNormal: *Randomly choose a prime number $p \notin \mathcal{P}$ such that A_p is a domain, d_p is a non-zero element in the conductor of A_p, and p does not divide the numerator and denominator of any coefficient occurring in a polynomial in G, R, or $\{f_1, \ldots, f_r\}$. Return true if $\frac{1}{d_p}\langle G_p\rangle$ is the normalization of A_p and satisfies the relations R_p, and false otherwise.*

If pTestNormal returns false, then $\mathcal{P}$ is not sufficiently large for A or not all primes in $\mathcal{P}$ are lucky (or the extra prime chosen in pTestNormal is unlucky). In this case, we enlarge the set $\mathcal{P}$ by t primes not used so far and repeat the whole process. On the other hand, if pTestNormal returns true, then most likely $G = G(0)$ and, thus, $\frac{1}{d}\langle G\rangle = \overline{A}$. It makes, then, sense to verify the result over the rationals by applying the following lemma. If the verification fails, we enlarge $\mathcal{P}$ and repeat the process.

Lemma 26. *With notation as above, the ring $\frac{1}{d}\langle G\rangle \subseteq \mathrm{Q}(A)$ is the normalization of A if and only if the following two conditions hold*:

(1) *The ring $\frac{1}{d}\langle G\rangle$ is integral over A. This holds if G and R are Gröbner bases, and the elements of $\frac{1}{d}G$ satisfy the relations R.*
(2) *The ring $\frac{1}{d}\langle G\rangle$ is normal. Equivalently, $\frac{1}{d}\langle G\rangle$ satisfies the conditions of the Grauert and Remmert criterion.*

Proof. If $\frac{1}{d}\langle G\rangle$ is integral over A, then $\frac{1}{d}\langle G\rangle \subseteq \overline{A}$. If $\frac{1}{d}\langle G\rangle$ is also normal, then equality holds. Note that if R is a Gröbner basis, then $\dim\langle R\rangle = \dim\langle R(p)\rangle$ for all $p \in \mathcal{P}$. Hence, if the elements of $\frac{1}{d}G$ satisfy the relations R, and G is a Gröbner basis, then $\frac{1}{d}\langle G\rangle$ is integral over A. □

We summarize modular normalization in Algorithm 3.

Algorithm 3 Modular normalization

Input: A prime ideal $I \subseteq \mathbb{Q}[X]$.
Output: A Gröbner basis $G \subseteq \mathbb{Q}[X]$ and $d \in \mathbb{Q}[X]$ such that $\frac{1}{d}\langle G\rangle \subseteq \mathrm{Q}(A)$ is the normalization of $A = \mathbb{Q}[X]/I$.

1: compute M, the Jacobian ideal of A;
2: choose a polynomial $d \in \mathbb{Q}[X]$ representing a non-zero element $d \in M$;
3: choose $\mathcal{P}$, a list of random primes;
4: $\mathcal{GP} = \emptyset$, $\mathcal{RP} = \emptyset$;
5: **loop**
6:   **for** $p \in \mathcal{P}$ **do**
7:     **if** A_p is not a domain or $d_p \in A_p$ is zero or d_p is not contained in the conductor of A_p **then**
8:       delete p;
9:     **else**
10:       use the GLS algorithm to compute $G(p)$, the reduced Gröbner basis such that $\frac{1}{d_p}\langle G(p)\rangle \subseteq \mathrm{Q}(A_p)$ is the normalization of A_p, and $R(p)$, the reduced Gröbner basis of the ideal of algebra relations;
11:       $\mathcal{GP} = \mathcal{GP} \cup \{G(p)\}$, $\mathcal{RP} = \mathcal{RP} \cup \{R(p)\}$;
12:   $(\mathcal{GP}, \mathcal{RP}, \mathcal{P}) =$ deleteUnluckyPrimesNormal$(\mathcal{GP}, \mathcal{RP}, \mathcal{P})$;
13:   lift $(\mathcal{GP}, \mathcal{RP}, \mathcal{P})$ to $G \subseteq \mathbb{Q}[X]$ and $R \subseteq W[T_1, \ldots, T_s]$ via Chinese remaindering and Gaussian reduction;
14:   **if** the lift succeeds and pTestNormal$(I, d, G, R, \mathcal{P})$ **then**
15:     **if** $\frac{1}{d}\langle G\rangle \subseteq \mathrm{Q}(A)$ is integral over A **then**
16:       **if** $\frac{1}{d}\langle G\rangle \subseteq \mathrm{Q}(A)$ is normal **then**
17:         **return** (G, d);
18:   enlarge $\mathcal{P}$;

Remark 27. If the loop in Algorithm 3 requires more than one round, we have to apply deleteUnluckyPrimesNormal in Step 12 with some care. Otherwise, it may happen that always classes containing only unlucky primes are selected. To avoid this problem, when determining the cardinality of the classes considered in a certain round of the loop, we count all prime numbers in the class selected in the previous round as just one element. Then $\mathcal{P}$ will eventually contain lucky primes and termination of the algorithm is ensured by Lemma 25 and Remark 22.

Remark 28. In Algorithm 3, the normalizations $\frac{1}{d_p}\langle G(p)\rangle$ can be computed in parallel. Furthermore, we can parallelize the final verifications of integrality and normality.

Remark 29. Algorithm 3 is also applicable without the final tests (that is, without the verification that $\frac{1}{d}\langle G\rangle \subseteq Q(A)$ is integral over A and normal). In this case, the algorithm is probabilistic, that is, the output $\frac{1}{d}\langle G\rangle \subseteq Q(A)$ is the normalization of A only with high probability. This usually accelerates the algorithm considerably.

Remark 30. The computation of the algebra structure R of the normalization via lifting of the relations $R(p)$ may require a large number of primes. Hence, if the number of cores available is limited, a better choice is to obtain just G by the modular approach and then compute the relations $R(0)$ over the rationals. For this approach, the initial ideals of the relations need not be tested in deleteUnluckyPrimesNormal and pTestNormal.

5. Timings

We compare the GLS normalization algorithm[6] (denoted in the tables below by `normal`) with Algorithm 2 from Section 3 (`locNormal`) and Algorithm 3 from Section 4 (`modNormal`).[7] For all modular computations, we use the simplified algorithm as specified in Remark 30. Note that at this writing, modularized versions of `locNormal` have not yet been implemented.

In many cases, it turns out that the final verification is a time consuming step of `modNormal`. To quantify the improvement of computation times by omitting the verification, we give timings for the resulting, now probabilistic, version of Algorithm 3 (denoted by `modNormal*` in the tables). In all examples computed so far, the result of the probabilistic algorithm is indeed correct.

All timings are in seconds on an AMD Opteron 6174 machine with 48 cores, 2.2 GHz, and 128 GB of RAM, running a Linux operating system. Computations which did not finish within 2000 seconds are marked by a dash. The maximum number of cores used is written in square brackets. For the single core version of `modNormal`, we indicate the number of primes used by the algorithm in brackets.

So far, in Singular, the computation of associated primes via fast modular methods has only been implemented for the zero-dimensional case. As the computation of associated primes is required by the local approach, we first focus on the case of curves, where the singular locus is zero-dimensional.

The projective plane curves defined by the equations

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

were constructed in Hirano (1992). They have $3(k+1)$ singularities of type A_k, provided that k is even. If k is odd, the curves are reducible, in which case the normalization algorithms still work in the same way as in the irreducible case as long as they do not detect a zerodivisor. After the coordinate transformation $Z \mapsto 3X - 2Y + Z$, all singularities of the projective curves lie in the affine chart $Z \neq 0$. We apply the algorithm to the affine curves. The timings for $k = 2, \ldots, 5$ are shown in Table 1.

Both the local and the probabilistic modular approaches have a better performance than the GLS algorithm, and they improve further in their parallel versions. The modular algorithm with final verification is slower, but can still handle much bigger examples than GLS.

[6] We use the implementation available in the Singular library `normal.lib`.

[7] To implement our algorithms, we have created the Singular libraries `modnormal.lib` and `locnormal.lib`.

Table 1
Timings for plane curves with many A_k singularities.

	$f_{1,2}$	$f_{1,3}$	$f_{1,4}$	$f_{1,5}$
`normal[1]`	.34	14	–	–
`locNormal[1]`	.57	2.0	2.1	38
`locNormal[20]`	.42	1.3	1.4	11
`modNormal[1]`	4.4 (3)	73 (4)	250 (5)	–
`modNormal[10]`	4.1	68	240	–
`modNormal*[1]`	.57 (3)	7.4 (4)	11 (5)	–
`modNormal*[10]`	.31	2.1	2.5	–

Table 2
Timings for plane curves with various types of singularities.

	$f_{2,7}$	$f_{2,8}$	$f_{2,9}$	f_3	f_4	f_5
`normal[1]`	7.7	12	383	–	474	1620
`locNormal[1]`	4.4	13	118	1.9	19	1.2
`locNormal[20]`	1.4	3.3	31	1.4	18	.93
`modNormal[1]`	38 (3)	69 (3)	146 (3)	142 (3)	–	50 (8)
`modNormal[10]`	38	69	146	84	–	43
`modNormal*[1]`	.70 (3)	1.2 (3)	1.2 (3)	88 (3)	9.8 (3)	7.0 (8)
`modNormal*[10]`	.47	.70	.74	30	4.7	.98

Timings for the affine plane curves defined by

$$\begin{aligned}
f_{2,k} &= \big((X-1)^k - Y^3\big)\big((X+1)^k - Y^3\big)\big(X^k - Y^3\big)\big((X-2)^k - Y^3\big)\big((X+2)^k - Y^3\big) + Y^{15},\\
f_3 &= X^{10} + Y^{10} + (X-2Y+1)^{10} + 2\big(X^5(X-2Y+1)^5 - X^5Y^5 + Y^5(X-2Y+1)^5\big),\\
f_4 &= \big(Y^5 + 2X^8\big)\big(Y^3 + 7(X-1)^4\big)\big((Y+5)^7 + 2X^{12}\big) + Y^{11},\\
f_5 &= 9127158539954X^{10} + 3212722859346X^8Y^2 + 228715574724X^6Y^4\\
&\quad - 34263110700X^4Y^6 - 5431439286X^2Y^8 - 201803238Y^{10} - 134266087241X^8\\
&\quad - 15052058268X^6Y^2 + 12024807786X^4Y^4 + 506101284X^2Y^6 - 202172841Y^8\\
&\quad + 761328152X^6 - 128361096X^4Y^2 + 47970216X^2Y^4 - 6697080Y^6\\
&\quad - 2042158X^4 + 660492X^2Y^2 - 84366Y^4 + 2494X^2 - 474Y^2 - 1,
\end{aligned}$$

are presented in Table 2.

In Table 3, we consider surfaces in $\mathbb{A}^3$ cut out by

$$\begin{aligned}
f_{6,k} &= XY(X-Y)(X+Y)(Y-1)Z + \big(X^k - Y^2\big)\big(X^{10} - (Y-1)^2\big),\\
f_{7,k} &= Z^2 - \big(Y^2 - 1234X^3\big)^k\big(15791X^2 - Y^3\big)\big(1231Y^2 - X^2(X+158)\big)\big(1357Y^5 - 3X^{11}\big),\\
f_8 &= Z^5 - \big((13X-17Y)\big(5X^2 - 7Y^3\big)\big(3X^3 - 2Y^2\big)\big(19Y^2 - 23X^2(X+29)\big)\big)^2.
\end{aligned}$$

We omit the verification step in the modular algorithm, as this is too time consuming. Note that the performance of the local approach will be considerably improved as soon as modular primary decomposition in higher dimension will be available in Singular.

Timings for the curves in $\mathbb{A}^3$ defined by the ideals

$$I_{9,k} = \big\langle Z^3 - \big(19Y^2 - 23X^2(X+29)\big)^2,\, X^3 - \big(11Y^2 - 13Z^2(Z+1)\big)^k \big\rangle$$

and the surface in $\mathbb{A}^4$ defined by

$$I_{10} = \big\langle Z^2 - \big(Y^3 - 123456W^2\big)\big(15791X^2 - Y^3\big)^2,\, WZ - \big(1231Y^2 - X(111X+158)\big)\big\rangle$$

are given in Table 4.

Table 3
Timings for the normalization of surfaces in $\mathbb{A}^3$.

	$f_{6,11}$	$f_{6,12}$	$f_{6,13}$	$f_{7,2}$	$f_{7,3}$	f_8
`normal[1]`	2.6	11	6.4	–	–	–
`locNormal[1]`	.25	.26	.29	80	113	70
`locNormal[20]`	.21	.22	.24	80	113	70
`modNormal*[1]`	2.2 (2)	.60 (2)	.78 (2)	12 (5)	17 (5)	2.3 (2)
`modNormal*[10]`	1.5	.52	.67	3.5	4.7	1.7

Table 4
Timings for curves in $\mathbb{A}^3$ and a surface in $\mathbb{A}^4$.

	$I_{9,1}$	$I_{9,2}$	I_{10}
`normal[1]`	3.2	–	150
`locNormal[1]`	4.2	36	83
`locNormal[20]`	4.1	35	82
`modNormal[1]`	–	–	28 (4)
`modNormal[10]`	–	–	14
`modNormal*[1]`	8.9 (5)	–	8.4 (4)
`modNormal*[10]`	2.1	–	2.5

To summarize, both the local and the probabilistic modular approaches provide a significant improvement over the GLS algorithm in computation times and size of the examples covered. The probabilistic method is very stable in the sense that it produces the correct result in all examples computed so far. As usual, the verification step in the modular setup is the most time consuming task, and a refinement of this step will be the focus of further research. The modular technique parallelizes completely, the local approach parallelizes best if the complexity distributes evenly over the minimal strata of the singular locus. In general, the localization technique, even when not run in parallel, is a major improvement to the GLS algorithm. Note, that the local contribution can also be obtained by other means. See, for example, Böhm et al. (in preparation) for a fast method in the case of curves, using Hensel lifting and Puiseux series.

References

Arnold, E.A., 2003. Modular algorithms for computing Gröbner bases. Journal of Symbolic Computation 35, 403–419.

Böhm, J., Decker, W., Laplagne, S., Seelisch, F., in preparation. Computing integral bases via localization and Hensel lifting.

Böhm, J., Decker, W., Fieker, C., Pfister, G., 2012. The use of bad primes in rational reconstruction. Preprint, available at http://arxiv.org/abs/1207.1651.

Bosma, W., Cannon, J., Playoust, C., 1997. The Magma algebra system. I. The user language. Journal of Symbolic Computation 24, 235–265.

Decker, W., Greuel, G.-M., Pfister, G., de Jong, T., 1999. The normalization: A new algorithm, implementation and comparisons. In: Computational Methods for Representations of Groups and Algebras. Essen, 1997. Birkhäuser.

Decker, W., Greuel, G.-M., Pfister, G., Schönemann, H., 2012. SINGULAR 3-1-4 — A computer algebra system for polynomial computations. http://www.singular.uni-kl.de.

Eisenbud, D., 1995. Commutative Algebra with a View Toward Algebraic Geometry. Springer.

Grauert, H., Remmert, R., 1971. Analytische Stellenalgebren. Springer.

Grayson, D.R., Stillman, M.E., 2010. MACAULAY2 — A software system for research in algebraic geometry. http://www.math.uiuc.edu/Macaulay2/.

Greuel, G.-M., Laplagne, S., Seelisch, F., 2010. Normalization of rings. Journal of Symbolic Computation 45, 887–901.

Greuel, G.-M., Pfister, G., 2007. A SINGULAR Introduction to Commutative Algebra, second edition. Springer.

Hirano, A., 1992. Construction of plane curves with cusps. Saitama Mathematical Journal 10, 21–24.

Idrees, N., Pfister, G., Steidel, S., 2011. Parallelization of modular algorithms. Journal of Symbolic Computation 46, 672–684.

de Jong, T., 1998. An algorithm for computing the integral closure. Journal of Symbolic Computation 26, 273–277.

de Jong, T., Pfister, G., 2000. Local Analytic Geometry. Vieweg.

Leonard, D.A., Pellikaan, R., 2003. Integral closures and weight functions over finite fields. Finite Fields and their Applications 9, 479–504.

Singh, A., Swanson, I., 2009. An algorithm for computing the integral closure. Preprint, available at http://arxiv.org/abs/0901.0871.

Swanson, I., Huneke, C., 2006. Integral Closure of Ideals, Rings, and Modules. Cambridge University Press.