Normalization of Rings

Gert-Martin Greuel

Department of Mathematics, University of Kaiserslautern - P.O. Box 3049 - (67653) Kaiserslautern, Germany

Santiago Laplagne

Departamento de Matemática, FCEN, Universidad de Buenos Aires - Ciudad Universitaria, Pabellón I - (C1428EGA) - Buenos Aires, Argentina

Frank Seelisch

Department of Mathematics, University of Kaiserslautern - P.O. Box 3049 - (67653) Kaiserslautern, Germany

Abstract

We present a new algorithm to compute the integral closure of a reduced Noetherian ring in its total ring of fractions. A modification, applicable in positive characteristic, where actually all computations are over the original ring, is also described. The new algorithm of this paper has been implemented in SINGULAR, for localizations of affine rings with respect to arbitrary monomial orderings. Benchmark tests show that it is in general much faster than any other implementation of normalization algorithms known to us.

Key words: normalization, integral closure, test ideal, Grauert-Remmert criterion

1. Introduction

Computing the normalization of a ring is a major tool in commutative algebra, with applications in algebraic geometry and singularity theory. The first general algorithms were proposed by Stolzenberg (1968) and Seidenberg (1970, 1975). However, the tools involved, such as extensions of the ground field and addition of new indeterminates, make them unsuitable for most practical applications.

Email addresses: `greuel@mathematik.uni-kl.de` (Gert-Martin Greuel), `slaplagn@dm.uba.ar` (Santiago Laplagne), `seelisch@mathematik.uni-kl.de` (Frank Seelisch).

In recent years several new and more practicable algorithms using Groebner bases have been proposed. The basic approach, continuing the line of the works mentioned before, is to compute an increasing chain of rings from the original ring to its normalization. This is carried out in the works of Traverso (1986), Vasconcelos (1991, 1998), Brennan and Vasconcelos (2001). To our knowledge none of these algorithms has been implemented and it remains unclear how practical they are. Also de Jong (1998), Decker et al. (1999) follow this path, applying as a new ingredient a criterion for normality due to Grauert and Remmert (1971). In Decker et al. (1999) they report an effective implementation of their algorithm in SINGULAR (Greuel et al., 2009b). It became the standard algorithm for normalization in computer algebra systems, being now implemented also in Macaulay2 (Grayson and Stillman, 2009) and Magma (Bosma et al., 1997). A good review on most of these algorithms can be found in Swanson and Huneke (2006, Chapter 15).

Another approach, presented in Gianni and Trager (1997), is to use Noether normalization, reduce the problem to the one dimensional case, and apply existing special algorithms for that case (Ford, 1987; Cohen, 1993). Unfortunately, we do not now of any implementation of these algorithms.

A more recent approach taken in Leonard and Pellikaan (2003) and Singh and Swanson (2008) is to compute a decreasing chain of finitely generated modules over the original ring containing the normalization. Their algorithm works only in the case when the base field is of positive characteristic p, where they can use the Frobenius map. It has been implemented in Macaulay2 and SINGULAR, and it turns out to be very fast for small p. However the computation of the Frobenius makes it impracticable when p is large.

There are also very efficient methods for computing the normalization in some special cases. For example, for toric rings, one can apply fast combinatorial techniques, as explained in Bruns and Koch (2001).

The algorithm we propose in this paper is a general algorithm and it is based on de Jong (1998) and Decker et al. (1999). In their algorithm, as we mentioned before, they construct an increasing chain of affine rings. They enlarge the rings by computing the endomorphism ring of a test ideal (see below), adding new variables for each module generator of the endomorphism ring and dividing out the relations among them. Then the algorithm is applied recursively to this new affine ring. Due to the increasing number of variables and relations this can produce a big slow-down in the performance of the algorithm already when the number of intermediate rings is 2 or 3. For a larger number, it usually makes the algorithm unusable, as the Groebner bases of the ideals of relations grow extensively. Our approach avoids the increasing complexity when enlarging the rings, benefiting from the finitely generated A-module structure of the normalization. We are able to do most computations over the original ring without adding new variables or relations.

The main new results of this paper are presented in Section 3. In Section 4 we describe the algorithm and show, as an application, how the δ-invariant of the ring can be computed. Section 5 contains several benchmark examples and a comparison with previously known algorithms, while Section 6 is devoted to an extension of the algorithm to non-global monomial orderings.

2. Basic definitions and tools

Let A be a reduced Noetherian ring.[1] The *normalization* $\bar{A}$ of A is the integral closure of A in the total ring of fractions $Q(A)$, which is the localization of A with respect to the non-zerodivisors on A. A is called *normal* if $A = \bar{A}$.

The *conductor* of A in $\bar{A}$ is $C = \{a \in Q(A) \mid a\bar{A} \subset A\} = \mathrm{Ann}_A(\bar{A}/A)$.

Lemma 2.1. *$\bar{A}$ is a finitely generated A-module if and only if C contains a non-zerodivisor on A.*

Proof. If $p \in C$ is a non-zerodivisor then $\bar{A} \cong p\bar{A} \subset A$ is module-finite over A, since A is Noetherian. Conversely, if $\bar{A}$ is module-finite over A then any common multiple of the denominators of a finite set of generators is a non-zerodivisor on A contained in C. $\square$

We recall the Grauert and Remmert criterion of normality.

Proposition 2.2. *Let A be a Noetherian reduced ring and $J \subset A$ an ideal satisfying the following conditions:*
  (1) J contains a non-zerodivisor on A,
  (2) J is a radical ideal,
  (3) $N(A) \subset V(J)$, where

$$N(A) = \{P \subset A, \ prime \ ideal \ \mid A_P \ is \ not \ normal\}$$

  is the non-normal locus of A.
Then A is normal if and only if $A \cong \mathrm{Hom}_A(J, J)$, via the canonical map which maps $a \in A$ to the multiplication by a.

Definition 2.3. An ideal $J \subset A$ satisfying properties $(1)-(3)$ is called a *test ideal* (for the normalization) of A. A pair (J, p) with J a test ideal and $p \in J$ a non-zerodivisor on A is called a *test pair* for A.

By Lemma 2.1, test pairs exist if and only if $\bar{A}$ is module-finite over A. We can choose any radical ideal J such that $p \in J \subseteq \sqrt{C}$.

Our algorithm computes the normalization of A when a test pair for A is known. If A is a reduced, finitely generated k-algebra with k a perfect field, then C contains a non-zerodivisor which can be computed by using the Jacobian ideal (cf. Lemma 4.1 and Remark 4.6). The same holds for localizations of such k-algebras w.r.t. any monomial ordering. Indeed, our algorithm is slightly more general, working whenever the Jacobian ideal does not vanish.

If A is not normal, we get a proper ring extension $A \subsetneq \mathrm{Hom}_A(J, J) =: A_1$.

If A_1 is not normal, which is checked by applying Proposition 2.2 to A_1, we obtain a new ring A_2 by that same proposition, which then has to be tested for normality, and so on. That is, we get a chain of inclusions of rings

$$A \subset A_1 \subset A_2 \subset \dots$$

(with $A_i = A[t_1, \dots, t_{s_i}]/I_i$, I_i ideal in A_i, and natural maps $\psi_i : A \hookrightarrow A_i$).

---

[1] We assume that all rings are commutative with 1 and that morphisms map 1 to 1.

If at some point, we get a normal ring A_N, then $A_N \cong \bar{A}$ by Lemma 2.6. This guarantees that if $\bar{A}$ is a finitely generated A-module, the chain will become stationary with A_N normal, giving an algorithm to compute the normalization.

The fact which makes the whole algorithm practicable, is the isomorphism

$$\operatorname{Hom}_A(J, J) \cong 1/p \cdot (pJ :_A J),$$

allowing us to compute $\operatorname{Hom}_A(J, J)$ over A. This fact, not contained in de Jong (1998), was found by the first named author during the implementation of the algorithm in SINGULAR and first published in Decker et al. (1999) (see also Greuel and Pfister (2008, Lemma 3.6.1) and Gianni and Trager (1997) for related statements). We shall prove a generalization of this isomorphism in Lemma 3.1, which will be needed in the new algorithm.

The following lemma describes the A-algebra structure of $1/p \cdot (pJ :_A J)$. This will allow us to compute the normalization of A recursively.

Lemma 2.4. *Let A be a reduced Noetherian ring, and (J, p) a test pair for A. Let $\{u_0 = p, u_1, \ldots, u_s\}$ be a system of generators for the A-module $pJ :_A J$. If $t_1, \ldots, t_s$ denote new variables, then $t_j \mapsto u_j/p$, $1 \le j \le s$, defines an isomorphism of A-algebras*

$$A_1 := A[t_1, \ldots, t_s]/I_1 \xrightarrow{\cong} \frac{1}{p}(pJ :_A J),$$

where I_1 is the kernel of the map $t_j \mapsto u_j/p$ from $A[t_1, \ldots, t_s] \to \frac{1}{p}(pJ :_A J)$.

See Greuel and Pfister (2008, Lemma 3.6.7) for the computational aspects of this lemma.

Example 2.5. Let $I = \left\langle x^2 - y^3 \right\rangle \subset k[x, y]$ and $A = k[x, y]/I$. We take the test pair (J, p), with $J := \langle x, y \rangle_A$ (the radical of the singular locus of A) and $p := x$ (see Algorithm 1). Then $pJ :_A J = \left\langle x, y^2 \right\rangle_A$ and $1/p \cdot (pJ :_A J) = 1/x \cdot \left\langle x, y^2 \right\rangle_A \cong A_1 := A[t]/I_1$ where $I_1 = \left\langle t^2 - y, yt - x, y^2 - xt \right\rangle_{A[t]}$. The isomorphism is given by $t \mapsto y^2/x$.

The following easy lemma gives a normalization criterion for ring extensions. It provides a convenient way to prove correctness of our normalization algorithm, or any modification, because it is independent of the intermediate steps.

Lemma 2.6. *Let $\psi : A \to B$ be a map between reduced Noetherian rings satisfying the following conditions:*
(1) ψ is injective,
(2) ψ is finite,
(3) B is contained in $Q(\psi(A))$.
Then ψ induces isomorphisms $Q(A) \to Q(B)$ and $\bar{A} \to \bar{B}$. In particular, if B is integrally closed, then $\bar{A}$ is isomorphic to B.

Proof. Since $A \hookrightarrow B$ is injective, so is $Q(A) \hookrightarrow Q(B)$ and hence $\bar{A} \hookrightarrow \bar{B}$. The isomorphism $Q(A) \to Q(B)$ is clear by 3. The finiteness of ψ implies that B (and therefore $\bar{B}$) is integral over A. Since $\psi(A) \subseteq B \subseteq \bar{B} \subseteq Q(B) = Q(\psi(A))$, we conclude that $\bar{B}$ is the normalization of $\psi(A)$, which immediately implies the isomorphism $\bar{A} \to \bar{B}$. $\quad\square$

3. Computing over the original ring

It has already been noticed by many authors (see for example the comments preceding Prop. 6.65 of Vasconcelos (2005)) that the chain of rings mentioned in last section, or similar constructions where the number of variables and relations increase in each step, behaves poorly in practice. (See also Remark 5.1.)

There has been therefore a search for algorithms carrying out most of the computations in the original ring. In Vasconcelos (2000) they propose to use

$$B = \bigcup_{n \geq 1} \mathrm{Hom}_S(I^n, I^n),$$

where S is a hypersurface ring over which A is finite and birational and I is the annihilator of the S-module A/S. However, as mentioned in that same paper, computing B is still the hard part of the algorithm and there is no indication on how to do it.

In this section we show that a chain of ring as used in Decker et al. (1999) can be constructed doing most computations over the original ring. In this way we obtain an algorithm that is usually much faster in practice.

The purpose of this section is not only to show that the computations over the original ring are possible. The proofs which we provide show also how these computations can be done and thus prepare the algorithms presented in the next section.

We start with a generalization of the isomorphism from the previous section, expressing $\mathrm{Hom}_A(J, J)$ as an ideal quotient, to be used later. We formulate a more general version than needed. For a related statement see Swanson and Huneke (2006).

Lemma 3.1. *Let A be a reduced (not necessarily Noetherian) ring, $Q(A)$ its total ring of fractions, and I, J two A-submodules of $Q(A)$. Assume that I contains a non-zerodivisor p on A.*

(1) The map

$$\Phi : \mathrm{Hom}_A(I, J) \xrightarrow{\cong} \frac{1}{p}(pJ :_{Q(A)} I) = J :_{Q(A)} I, \quad \varphi \mapsto \frac{\varphi(p)}{p},$$

is independent of the choice of p and an isomorphism of A-modules.

(2) If $J \subset A$ then

$$pJ :_{Q(A)} I = pJ :_A I.$$

Proof. (1) Let $q \in I$ be another non-zerodivisor on A. Write $p = p_1/p_0$ and $q = q_1/q_0$, with p_0, q_0 non-zerodivisors contained in A and $p_1, q_1 \in A$.

Then $c := p_0 q_0 \in A$ is a non-zerodivisor and $cp, cq \in A$ with $cpq \in I$. Since $\varphi \in \mathrm{Hom}_A(I, J)$ is A-linear, we can write

$$cp\varphi(q) = \varphi(cpq) = cq\varphi(p),$$

whence $\varphi(p)/p = \varphi(q)/q$ in $Q(A)$, showing that Φ is independent of p.

Moreover, for any $f \in I$ we have

$$\frac{\varphi(p)}{p} \cdot f = \frac{\varphi(cp)}{cp} \cdot f = \frac{\varphi(cpf)}{cp} = \frac{cp\varphi(f)}{cp} = \varphi(f) \in J,$$

in particular $\varphi(p) \cdot f \in pJ$. This shows that the image $\Phi(\varphi)$ is in $1/p \cdot (pJ :_{Q(A)} I)$. It also shows that $\varphi(p) = 0 \Leftrightarrow \forall f \in I \; \varphi(f) = 0 \Leftrightarrow \varphi = 0$ and hence that Φ is injective.

To see that Φ is surjective, let $q \in Q(A)$ satisfy $qI \subset J$. Denote by $m_q \in \operatorname{Hom}_A(I, J)$ the multiplication by q. Then $\Phi(m_q) = qp/p = q$ showing that Φ is surjective.

(2) During the proof of (1) we have seen that

$$pJ :_{Q(A)} I = \{\varphi(p) \mid \varphi \in \operatorname{Hom}_A(I, J)\}.$$

Hence, the claimed equality holds if and only if $\varphi(p) \in A$ for all $\varphi \in \operatorname{Hom}_A(I, J)$, which is clearly true if $J \subset A$. $\quad\square$

Recall the chain of extension rings from last section $A \subset A_1 \subset A_2 \subset \ldots$ We have seen that we can compute the normalization of A by computing the normalization of A_i (Lemma 2.6). The next proposition explains how to obtain a test pair in A_i from a given test pair in A. This is the only computation to be carried out in A_i.

Proposition 3.2. *Let A be a reduced Noetherian ring, $A' = A[t_1, \ldots, t_s]/I'$ a finite extension ring, with natural inclusion $\psi : A \hookrightarrow A'$. If (J, p) is a test pair for A then setting $J' = \sqrt{\langle \psi(J) \rangle_{A'}}$, $(J', \psi(p))$ is a test pair for A'.*

Proof. Let C be the conductor of A in $Q(A)$ and C' the conductor of A' in $Q(A')$. We know that $N(A') = V(C')$, $N(A) = V(C)$ and $\psi(C) \subset C'$. Therefore $V(C') \subset V(C)$, which proves that $N(A') \subset N(\psi(A))$ since $\psi(A) \cong A$. We have $N(A) \subset V(J)$ by definition of J, and hence $N(A') \subset V(\psi(J))$. Now $\psi(p) \in J'$ is a non-zerodivisor on A' and $(J', \psi(p))$ is a test pair for A'. $\quad\square$

Example 3.3. Recall Example 2.5. We started with $A = k[x, y]/\langle x^2 - y^3 \rangle$ and test pair $(J, p) = (\langle x, y \rangle, x)$ and obtained $A_1 := A[t]/I_1 \cong 1/d_1 \cdot U_1$ where $I_1 = \langle t^2 - y, yt - x, y^2 - xt \rangle$, $d_1 = x$ and $U_1 = \langle x, y^2 \rangle_A$.

We now compute $J_1 = \sqrt{\langle \psi_1(J) \rangle_{A_1}} = \sqrt{\langle x, y \rangle_{A_1}} = \langle x, y, t \rangle_{A_1} = \langle t \rangle_{A_1}$ (since $t^2 = y$ and $t^3 = x$ in A_1). Therefore $(\langle t \rangle, x)$ is a test pair for A_1.

For the remainder of this section, let R be a Noetherian ring, $I \subset R$ a radical ideal and $A = R/I$.

We are mainly interested in $R = k[x_1, \ldots, x_n]$ with k a field (which the reader may assume in the following), or $R = k[x_1, x_2, \ldots, x_n]_>$ with $>$ an arbitrary monomial ordering. However the proposed method works quite generally, whenever a test pair is known.

In the new algorithm, we will compute ideals $U_1, U_2, \ldots, U_N$ of A and non-zerodivisors $d_i \in U_i, 1 \leq i \leq N$, on A such that

$$A \subset \frac{1}{d_1} U_1 \subset \frac{1}{d_2} U_2 \subset \cdots \subset \frac{1}{d_N} U_N = \bar{A}.$$

From the construction we know that $1/d_i \cdot U_i$ is a finitely generated R-algebra and hence there is a surjection

$$R_i := R[t_1, t_2, \ldots, t_{s_i}] \twoheadrightarrow \frac{1}{d_i} U_i, \quad t_j \mapsto u_j,$$

where $\{d_i, u_1, \ldots, u_{s_i}\}$ is a set of R-module generators of U_i. If I_i denotes the kernel of this map, we get a ring map

$$\varphi_i : A_i := R_i/I_i \xrightarrow{\cong} \frac{1}{d_i} U_i \subset Q(A).$$

(Note that the definition of I_i is now slightly different from the one given in 2.4.)

Example 3.4. Carrying on with Example 3.3, we compute $\varphi_1(J_1) = \varphi_1(\langle t \rangle)$.

Note that $\varphi_1(t) = y^2/x$. However the A-module $\langle y^2/x \rangle_A \subsetneq \varphi_1(\langle t \rangle)$. For example, we have seen that $y \in \langle t \rangle_{A_1}$ and clearly $\varphi_1(y) = yx/x$, but $yx \notin \langle y^2 \rangle_A$.

This shows that in order to obtain A-module generators of $\varphi_i(J_i)$ it is not enough to compute the images of the generators of J_i. In Algorithm 2 we will show how to compute the generators. In this example, it turns out that $\varphi_1(\langle t \rangle) = \langle yx/x, y^2/x \rangle$ as A-module.

Once we have computed a test pair (J_i, p_i) in A_i, the next step is to compute the quotient $pJ_i :_{A_i} J_i$. The following theorem shows that this computation can be carried out in the original ring A.

Theorem 3.5. *Let* $A = R/I$, $A' = A[t_1, \ldots, t_s]/I'$ *a finite ring extension and maps* $\psi : A \hookrightarrow A'$, $\varphi : A' \hookrightarrow Q(A)$. *Let* (J, p) *be a test pair for* A *and* (J', p') *a test pair for* A', *with* $p' = \psi(p)$. *Let* U, H *be ideals of* A *and* $d \in A$ *such that* $\varphi(A') = \dfrac{1}{d}U$ *and* $\varphi(J') = \dfrac{1}{d}H$. *Then*

$$(p'J') :_{A'} J' = \frac{1}{d}(dpH :_A H).$$

Proof. The proof is an easy consequence of Lemma 3.1. Omitting φ and ψ in the following notations and applying Lemma 3.1 to $p \in J \subset A$ we get

$$(p'J') :_{A'} J' = (p'J') :_{Q(A)} J' = pH :_{Q(A)} H,$$

since $Q(A') = Q(A)$ and $J' = 1/d \cdot H$.

On the other hand, we can apply Lemma 3.1 to $dp \in H \subset A$ and get

$$\frac{1}{d}(dpH :_A H) = \frac{1}{d}(dpH :_{Q(A)} H) = pH :_{Q(A)} H. \qquad \square$$

Using Theorem 3.5 together with the previous results, once we have computed an intermediate ring A_i, we can compute A_{i+1}, the next ring in the chain. If $A_i = A_{i+1}$, we have finished and A_i is the normalization of the original ring A, by Lemma 2.6. If not, we proceed by induction to compute the normalization.

We continue with the above example.

Example 3.6. We have $p = d_1 = x$ and $H_1 = \langle xy, y^2 \rangle_A$. We compute $d_1 p H_1 :_A H_1 = x^2 \langle xy, y^2 \rangle :_A \langle xy, y^2 \rangle = \langle x^2, xy^2 \rangle$.

Then
$$\mathrm{Hom}_{A_1}(J_1, J_1) \cong \frac{1}{x^2}\langle x^2, xy^2 \rangle = \frac{1}{x}\langle x, y^2 \rangle.$$

This is equal to A_1. Therefore, the ring A_1 was already normal, and hence equal to the normalization of A.

Modification 3.7. We have seen that the only computation performed in A_i is the radical of $\psi_i(J)$. However, when the characteristic of the base field is $q > 0$ it is possible to compute also this radical over the original ring. For this, we use the Frobenius map, as described in Matsumoto (2001).

7

Let $G = \psi_i(J) \subset A_i$. By definition,

$$J_i = \sqrt{G} = \{f \in A_i \mid f^m \in G \text{ for some } m \in \mathbb{N}\}.$$

Mapping to $Q(A)$, we obtain

$$\varphi_i(J_i) = \left\{ \tilde{f}/d_i \ \middle| \ \tilde{f} \in U_i, \ \left(\tilde{f}/d_i \right)^m \in \varphi_i(G) \text{ for some } m \in \mathbb{N} \right\} = \bigcup_{m \geq 1} G_m,$$

where $G_m := \left\{ \tilde{f}/d_i \ \middle| \ \tilde{f} \in U_i, \ \left(\tilde{f}/d_i \right)^m \in \varphi_i(G) \right\}$. Then

$$d_i G_q = \{\tilde{f} \in U_i \mid \tilde{f}^q \in d_i^q \varphi_i(G)\}.$$

Now $d_i^q \varphi_i(G)$ is an ideal of A and $d_i G_q$ is the so-called q-th root of $d_i^q \varphi_i(G)$. This ideal can be computed over A using the Frobenius map (cf. Matsumoto (2001)).

By iteratively computing the q-th root of the output, until no new polynomials are added, we obtain $\varphi_i(J_i)$ as desired.

Computing the radical in this way, we get another algorithm (in positive characteristic) which is similar to the one proposed in Singh and Swanson (2008). In their algorithm they start with the inclusion $\bar{A} \subset \frac{1}{c}A$, where c is an element of the conductor and compute a decreasing chain of A-modules

$$\frac{1}{c}A = \frac{1}{c}U_0' \supset \frac{1}{c}U_1' \supset \cdots \supset \frac{1}{c}U_N' = \bar{A}.$$

In our algorithm we compute an increasing chain

$$A \subset \frac{1}{d_1}U_1 \subset \cdots \subset \frac{1}{d_N}U_N = \bar{A}.$$

The most difficult computational task for both algorithms is the Frobenius map. However, in our algorithm we start with a small denominator d_1 and therefore the computations might be in some cases easier. This modification has not yet been tested.

4. Algorithms and application

We describe the algorithm in general terms. Since we compute an increasing sequence of subrings of the integral closure the algorithm terminates, for a Noetherian ring A, if and only if $\bar{A}$ is a finitely generated A-module. By Lemma 2.1 this is equivalent to the existence of a test pair. We now deal with the problem of constructing an initial test pair.

Lemma 4.1. *Let k be a perfect field, and $A = k[x_1, x_2, \ldots, x_n]/I$ with $I = \langle f_1, f_2, \ldots, f_t \rangle$ a reduced equidimensional ring of dimension r. Let M be the Jacobian ideal of I, that is, the ideal in A generated by the images of the $(n-r) \times (n-r)$-minors of the Jacobian matrix $(\partial f_i / \partial x_j)_{i,j}$. Then M is contained in the conductor of A and contains a non-zerodivisor on A.*

Proof. Let $I = P_1 \cap P_2 \cap \ldots \cap P_s$ with $P_1, P_2, \ldots, P_s$ the minimal associated primes of I. Since A is equidimensional, $\dim(A) = \text{height}(P_i) = r$ for $1 \leq i \leq s$. Hence,

the image of M in $A_i = k[x_1, x_2, \ldots, x_n]/P_i$ is contained in the Jacobian ideal M_i of P_i. By the Lipman-Sathaye theorem (cf. Swanson and Huneke (2006) and Singh and Swanson (2008, Remark 1.5)) M_i and hence M is contained in the conductor of A_i. Since $\bar{A} = \bar{A}_1 \oplus \bar{A}_2 \oplus \cdots \oplus \bar{A}_s$, M is then also in the conductor of A. Moreover, the image of M in A_i is not zero since A_i is reduced. This follows from the Jacobian criterion and by Serre's condition for reducedness (cf. Greuel and Pfister (2008, Section 5.7)). As a consequence, M is not contained in the union of the minimal associated primes of A and hence contains a non-zerodivisor on A. $\quad\square$

Note that both, the Lipman-Sathaye theorem and the Jacobian criterion, require k to be perfect.

The ideal $J := \sqrt{M}$ from last lemma can be used as an initial test ideal. To construct a test pair, we need to find in addition a non-zerodivisor of A in J. An element $p \in A$ is a non-zerodivisor if and only if $0 :_A \langle p \rangle = 0$, hence the non-zerodivisor test is effective. However, it is not sufficient to apply the test to the generators of J. (E.g., if $I = \langle xy \rangle$, the polynomials x, y generate J and are zerodivisors on A, but $x + y$ is not.) Since we cannot test all elements of J there seems to be a problem to find a test pair if I is not prime. We address this problem as well as the perfectness and the equidimensionality assumptions in Remark 4.6.

We first describe in Algorithm 1 how to compute the initial test pair (J, p) in A, assuming that we are able to find a non-zerodivisor.

Remark 4.2. Only for this step we need the assumption that $R = k[x_1, x_2, \ldots, x_n]_>$ with k perfect and that I is equidimensional. All further steps do not require this assumption. If, by whatever means, an initial test pair (J, p) for A is known, we can start with the computation of U_1 and then all further steps are correct, and the loop terminates with the computation of $\bar{A}$. Hence, for any reduced ring $A = R/I$ with given test pair (J, p), the algorithm is effective when Gröbner bases, ideal quotients, and radicals can be computed in rings of the form $R[t_1, t_2, \ldots, t_s]$.

Algorithm 1 Initial test pair (J, p)

Input: $I \subset R$, an equidimensional radical ideal, with $R = k[x_1, x_2, \ldots, x_n]_>$ and k a
    perfect field.
Output: (J, p) a test pair for $A := R/I$.
  $r := \dim(I)$
  $M' :=$ the Jacobian ideal of I, i.e., the ideal in R generated by the
    $(n - r) \times (n - r)$-minors of the Jacobian matrix of I
  $M :=$ the image of M' in A
  $J := \sqrt{M} \subset A$
  choose $p \in J$ such that p is a non-zerodivisor on A
  return (J, p)

We now explain how to perform some auxiliary tasks, that will be needed in the main algorithm.

We have seen in the previous section that if $A = R/I$ and $A' = R[t_1, \ldots, t_n]/I'$ a finite extension ring with $I \subset I'$, then there exist a non-zerodivisor $d \in A$, an ideal $U \subset A$ and

a map $\varphi : A' \to 1/d \cdot U$ such that $A' \xrightarrow{\cong} 1/d \cdot U$. For computations, we need to know how to move from one representation to the other.

Remark 4.3. If we know d and generators $\{d, u_1, \ldots, u_s\}$ of U, we can explicitly compute $\varphi(q)$ for any $q \in A'$. Let $\tilde{q} \in R'$ be a representative, and substitute all the variables t_j in $\tilde{q}$ by the corresponding fraction u_j/d. This results in an element $f/d^e \in Q(A)$ for some $f \in A$ and $e \in \mathbb{Z}_{\geq 0}$. Now we need to find $f' \in A$ such that $f/d^e = f'/d$ in $Q(A)$, which is equivalent to $f = f'd^{e-1} + g$ in R, with $g \in I$. We can find f' by solving the (extended) ideal membership problem $f \in I + \langle d^{e-1} \rangle$ in R, e.g. by using the SINGULAR command `lift`, cf. Greuel and Pfister (2008, Example 1.8.2).

We will need also to compute A-module generators of ideals $J' \subset A'$ given by generators in A'. It is clear that for any such J' there exist an ideal $H \subset A$ such that $\varphi(J') = 1/d \cdot H$. So the problem is equivalent to finding elements $h_1, \ldots, h_l$ in A that generate H as an A-ideal. In Algorithm 2 we explain how do it.

Algorithm 2 A-module generators

Input: $A = R/I$, with $R = k[x_1, \ldots, x_n]$ and $I \subset R$ ideal; $A' = R'/I'$ a ring extension of A, with $R' = R[t_1, \ldots, t_s]$ and $I' \subset R'$ an ideal; $d \in A'$ a non-zerodivisor and $U' = \langle u_0 = d, u_1, \ldots, u_s \rangle_A$ such that $A' \cong \frac{1}{d}U$, with map $\varphi : A' \xrightarrow{\cong} \frac{1}{d}U$; $J' = \langle f_1, \ldots, f_m \rangle_{A'}$, an ideal of A'.

Output: $H = \langle h_1, \ldots, h_l \rangle_A$ such that $\varphi(J') = 1/d \cdot H$

  for $j = 1, \ldots, m$ **do**
    compute h_j such that $\varphi_i(f_j) = h_j/d$ (cf. Remark 4.3)
  end for
  set $S = \{h_1, \ldots, h_m\}$
  for $j = 1, \ldots, m$; $k = 1, \ldots, s$ **do**
    compute $h_{j,k} \in A$ such that $h_{j,k}/d = u_k/d \cdot h_j/d$ in $Q(A)$ (again by Remark 4.3)
    if $h_{j,k} \notin \langle S \rangle_A$ **then**
      $S = S \cup \{h_{j,k}\}$
    end if
  end for
  return $H := \langle S \rangle$

Lemma 4.4. *Let $A = R/I$, with $R = k[x_1, \ldots, x_n]$ and $I \subset R$ ideal; $A' = R'/I'$ a ring extension of A, with $R' = R[t_1, \ldots, t_s]$ and $I' \subset R'$ an ideal; $d \in A'$ a non-zerodivisor and $U' = \langle u_0 = d, u_1, \ldots, u_s \rangle_A$ such that $A' \cong \frac{1}{d}U$, with map $\varphi : A' \xrightarrow{\cong} \frac{1}{d}U$; $J' = \langle f_1, \ldots, f_m \rangle_{A'}$, an ideal of A'. The output ideal $H = \langle h_1, \ldots, h_l \rangle_A$ of Algorithm 2 satisfies $\varphi(J') = 1/d \cdot H$.*

Proof. This follows since the A-module $\langle 1 = u_0/d, u_1/d_i, \ldots, u_s/d \rangle_A = \varphi(A')$ and the A'-module $\langle h_1/d, h_2/d, \ldots, h_m/d \rangle_{A'} = \varphi(J')$ ($h_1, \ldots, h_m$ as in the algorithm). Therefore the products $u_k/d \cdot h_j/d$, $0 \leq k \leq s, 1 \leq j \leq m$, generate $\varphi(J')$ as A-module. Hence $\{h_j \mid 1 \leq j \leq l\}$ generates H as A-module, or equivalently as A-ideal. $\square$

Example 4.5. We apply the algorithm to compute the A-module generators of $\varphi_1(J_1)$ from Example 3.4. Recall that $J_1 = \langle t \rangle_{A_1}$, $U_1 = \langle x, y^2 \rangle_A$ and $d = x$. We start with $h_1 = \varphi_1(t) = y^2/x$ and $S = \{h_1\}$. In the first step, we compute $x/x \cdot y^2/x = y^2/x$, therefore $h_{1,0} = y^2$. Since $y^2 \in \langle y^2 \rangle$, we do not do anything. In the second step we compute $y^2/x \cdot y^2/x = y^4/x^2 = x^2y/x^2 = xy/x$, therefore $h_{1,1} = xy$. Since $xy \notin \langle y^2 \rangle$, we add it to S. We finish with $H = \langle xy, y^2 \rangle$, as mentioned in Example 3.4.

We are now ready to present in Algorithm 3 the main algorithm to compute the normalization.

Termination follows from Lemma 2.1 and the discussion after Definition 2.3, correctness follows from Lemma 2.6.

Algorithm 3 Normalization of R/I

Input: $I \subset R$, an equidimensional radical ideal

Output: generators of an ideal $U \subset R$, and $d \in R$ such that $\overline{A} = \dfrac{1}{d}U \subset Q(A)$,
    with $A := R/I$.
  compute (J, p), an initial test ideal
  $U_1 := (pJ :_A J) \subset A$
  $d_1 := p$
  if $\langle d_1 \rangle = U_1$ **then**
    return $(\langle 1 \rangle, 1)$
  end if
  $i := 1$
  loop
    write $U_i = \left\langle d_i, u_1^{(i)}, u_2^{(i)}, \ldots, u_s^{(i)} \right\rangle_A$
    set $R_i := R[t_1, \ldots, t_s]$, $\pi_i : R_i \to \frac{1}{d_i}U_i \subset \frac{1}{d_i}A$ the map $t_j \mapsto u_j^{(i)}/d_i$
    $I_i := \ker(\pi_i)$ (cf. Lemma 2.4)
    set $A_i = R_i/I_i$
    $J_i := \sqrt{\psi_i(J)} \subset A_i$, with $\psi_i : A \hookrightarrow A_i$
    compute $\{f_1, \ldots, f_k\} \subset A$ such that $H_i := \langle f_1, f_2, \ldots, f_k \rangle_A = d_i\varphi_i(J_i)$,
        with $\varphi_i : A_i \xrightarrow{\cong} \frac{1}{d_i}U_i$ (cf. Lemma 4.4)
    compute generators of $U_{i+1} := (pd_iH_i) :_A H_i$
    if $d_iU_i \subset U_{i+1}$ **then**
      return (U_i, d_i)
    end if
    $d_{i+1} := pd_i$
    $i := i + 1$
  end loop

Remark 4.6. Let us comment on some variations and generalizations of Algorithm 3. For this let k be *any* field, $R = k[x_1, x_2, \ldots, x_n]_>$, and $I \subset R$ a radical ideal.
(1) If I is not (or not known to be) equidimensional we can start with an algorithm to compute the minimal associated primes (cf. Greuel and Pfister (2008, Algorithm 4.3.4, Algorithm 4.4.3)) or the equidimensional parts (cf. Greuel and Pfister (2008, Algorithm 4.4.9)) of I, where the latter is often faster. The corresponding ideals $I_1, I_2, \ldots, I_r$ are

equidimensional and we have $\overline{R/I} \cong \overline{R/I_1} \oplus \overline{R/I_2} \oplus \cdots \oplus \overline{R/I_r}$. Hence the problem is reduced to the case of I being prime or equidimensional.

(2) Now let I be equidimensional and M the Jacobian ideal. Since regular rings are normal, it follows from the Jacobian criterion that $N(R/I) \subset V(M)$. Let us assume that $M \neq 0$ and choose $p \in M \setminus \{0\}$.

a) If $I_1 := I :_R \langle p \rangle \subset I$ then p is a non-zerodivisor on A and $J = \sqrt{M}$ is a test ideal. This is always the case if I is prime.

b) If $I_1 \not\subset I$ we compute $I_2 := I :_R I_1$ and obtain a splitting $I = I_1 \cap I_2$ (cf. Greuel and Pfister (2008, Lemma 1.8.14(3))) and $\overline{R/I} \cong \overline{R/I_1} \oplus \overline{R/I_2}$. Hence we can continue with the ideals I_1 and I_2 separately which have both fewer minimal associated primes than I. Consequently, after finitely many splittings, the corresponding ideal is prime or we have found a non-zerodivisor. This provides us with test ideals as in case a).

(3) The above arguments show that (even if k is not perfect) Algorithm 3 works for prime ideals if and only if the Jacobian ideal M is not zero. This is always the case for k perfect. However, if k is not perfect, $M = 0$ may occur. For example, consider $k = (\mathbb{Z}/q)(t)$ with q a prime number, and $I = \langle x^q + y^q + t \rangle \subset k[x, y]$. For a method to compute a non-zero element in the conductor of R/I if I is prime and if $Q(R/I)$ is separable over k, see Swanson and Huneke (2006, Exercise 12.12).

4.1.   The δ-invariant

As an application of the normalization algorithm we show how to compute the δ-invariant of a reduced Noetherian k-algebra $A = k[x_1, x_2, \ldots, x_n]_>/I$,

$$\delta(A) := \dim_k(\bar{A}/A).$$

$\delta(A)$ may be infinite but it is finite if the algebraic variety $V(I)$ defined by I has isolated non-normal points, e.g. for reduced curves, i.e. $\dim(A) = 1$. In this case, δ is important as it is the difference between the arithmetic and the geometric genus of a curve. Moreover, the δ-invariant is one of the most important numerical invariants for curve singularities (cf. Campillo et al. (2007)), that is, for 1-dimensional complete local rings A. The extension of our algorithm to non-global orderings in Section 6 has the immediate consequence that it allows to compute δ for affine rings as well as for local rings of singularities, noting that $\delta(k[x_1, x_2, \ldots, x_n]_>/I) = \delta(k[[x_1, x_2, \ldots, x_n]]/I)$ if $>$ is a local ordering.

Lemma 4.7. *Let R be a reduced Noetherian ring, $I \subset R$ be a radical ideal, and $I = P_1 \cap \cdots \cap P_r$ its prime decomposition. Write $I = I_1 \cap \cdots \cap I_s$, where $I_i = \bigcap_{j \in N_i} P_j$ and $\{N_1, \ldots, N_s\}$ is a partition of $\{1, \ldots, r\}$. Let U_i, d_i be the output of the normalization algorithm for $A_i = R/I_i$. Then*

(1) $\delta(A_i) = \dim_k(U_i/d_i U_i)$, $1 \leq i \leq s$,

(2) $\delta(R/I) = \displaystyle\sum_{i=1}^{s} \delta(A_i) + \sum_{i=1}^{s-1} \dim_k(R/(I + I^{(i)}))$, where $I^{(i)} = I_{i+1} \cap \cdots \cap I_s$.

In particular $\delta(R/I) < \infty$ iff every summand on the right hand side of (2) is finite.

Proof. This follows by induction on s, and by repeatedly applying the following sequence of inclusions for $s = 2$, i.e. $I = I_1 \cap I_2$,

$$R/I \hookrightarrow R/I_1 \oplus R/I_2 \hookrightarrow \overline{R/I_1} \oplus \overline{R/I_2} \cong \overline{R/I},$$

and the exact sequence

$$0 \to R/I \to R/I_1 \oplus R/I_2 \to R/(I_1 + I_2) \to 0. \qquad \qquad \square$$

Note that $\dim_k R/(I_i + I^{(i)})$ can be computed from a standard basis of $I_i + I^{(i)}$ and $\dim_k(U_i/d_i U_i)$ from a standard basis of a presentation matrix of $U/d_i U_i$ via `modulo` (cf. Greuel and Pfister (2008, SINGULAR Example 2.1.26)). An algorithm to compute δ is also implemented in SINGULAR (Greuel et al., 2009b).

5. Examples and comparisons

In Table 1 we see a comparison of the implementations in SINGULAR of the new algorithm `normal` and other existing algorithms. `normalC` is an implementation based on the algorithm Decker et al. (1999) (see also Greuel and Pfister (2008, Section 3.6)) and `normalP` is an implementation of the algorithm of Leonard and Pellikaan (2003), Singh and Swanson (2008) for positive characteristic. All these implementations are now available in the SINGULAR library `normal.lib` (Greuel et al., 2009a). Computations were performed on a compute server running a 1.60GHz Dual AMD Opteron 242 with 8GB ram.

∗ indicates that the algorithm had not finished after 20 minutes,

- indicates that the algorithm is not applicable (i.e., using `normalP` in characteristic 0).

We try several examples over the fields $k = \mathbb{Q}$ and $k = \mathbb{Z}_p, p \in \{2, 3, 5, 11, 13, 32003\}$, when the ideal is prime in the corresponding ring. We see that the new algorithm is extremely fast compared to the other algorithms. Only the algorithm `normalP` is sometimes faster for very small characteristic.

In columns 3 and 4 we give additional information on how the new algorithm works. The column "non-zerodivisor" indicates which non-zerodivisor is chosen. The column "steps" indicates how many loop steps are needed to compute the normalization. We see that our new algorithm performs well compared to the classic algorithm especially when the number of steps needed is large.

We use the following examples:

- $I_1 = \langle (x - y)x(y + x^2)^3 - y^3(x^3 + xy - y^2) \rangle \subset k[x, y]$,
- $I_2 = \langle 55x^8 + 66y^2x^9 + 837x^2y^6 - 75y^4x^2 - 70y^6 - 97y^7x^2 \rangle \subset k[x, y]$,
- $I_3 = \langle y^9 + y^8x + y^8 + y^5 + y^4x + y^3x^2 + y^2x^3 + yx^8 + x^9 \rangle \subset k[x, y]$,
- $I_4 = \langle (x^2 + y^2 - 1)^3 + 27x^2y^2 \rangle \subset k[x, y]$,
- $I_5 = \langle -x^{10} + x^8y^2 - x^6y^4 - x^2y^8 + 2y^{10} - x^8 + 2x^6y^2 + x^4y^4 - x^2y^6 - y^8 + 2x^6 - x^4y^2 + x^2y^4 + 2x^4 + 2x2y^2 - y^4 - x^2 + y^2 - 1 \rangle \subset k[x, y]$,
- $I_6 = \langle z^3 + zyx + y^3x^2 + y^2x^3, uyx + z^2, uz + z + y^2x + yx^2, u^2 + u + zy + zx, v^3 + vux + vz^2 + vzyx + vzx + uz^3 + uz^2y + z^3 + z^2yx^2 \rangle \subset k[x, y, z, u, v]$.
- $I_7 = \langle x^2 + zw, y^3 + xwt, xw^3 + z^3t + ywt^2, y^2w^4 - xy^2z^2t - w^3t^3 \rangle \subset k[x, y, z, w, t]$.

Remark 5.1. As mentioned before, the main drawback of the algorithm Decker et al. (1999) is the increasing complexity of the new rings that are constructed. A direct implementation of the algorithm turns out to be so slow that it does not even finish for most of the examples analyzed in this paper (after 1 hour). For example, in the second example (I_2) over $\mathbb{Z}_3$, the fifth ring constructed in the chain has 12 variables and 76 generators for the ideal of relations. The sixth ring could not be computed using this direct approach.

13

Table 1. Timings

No.	char	normal data		seconds		
		non-zerodivisor	steps	normal	normalP	normalC
1	0	y	7	0	-	72
1	2	y	7	0	0	0
1	5	y	7	1	73	0
1	11	$x - 2y$	7	1	12	$*$
1	32003	y	7	0	$*$	1
2	0	y	7	1	-	$*$
2	3	y	8	0	0	3
2	13	y	7	0	$*$	10
2	32003	y	7	0	$*$	10
3	0	y	6	2	-	$*$
3	2	y	13	1	0	$*$
3	5	y	6	1	7	$*$
3	11	$x + 4y$	6	1	$*$	$*$
3	32003	y	6	1	$*$	$*$
4	0	$2x^2y - y^3 + y$	1	0	-	0
4	5	$x^2y + 2y^3 - 2y$	1	0	3	0
4	11	$x^2y + 5y^3 - 5y$	1	0	$*$	0
4	32003	$x^2y + 16001y^3 - 16001y$	1	0	$*$	0
5	0	y	1	0	-	0
5	5	$x^3y + xy$	3	1	$*$	$*$
5	11	y	1	0	0	0
5	32003	y	1	1	$*$	0
6	2	v	2	6	24	172
7	0	y	6	12	-	582
7	2	y	6	11	0	35
7	5	y	6	12	3	358
7	11	y	6	11	43	503
7	32003	y	6	11	$*$	617

14

A partial solution to this problem, used in implementations, is to eliminate as far as possible redundant variables, that is, variables than can be expressed in term of the others through the relations in the ring. This is what is done in `normalC`, and it is sometimes a good improvement. However detecting the redundant variables becomes more and more difficult as the relations get more and more complex, adding a new expensive task to the computation, that does not always succeeds in detecting all the relations.

The algorithm proposed in this paper avoids this problem in a natural way.

We have also compared our implementation with the normalization procedures in Macaulay2 (they use the algorithms Decker et al. (1999) and Singh and Swanson (2008)) and in Magma (they say that they use Decker et al. (1999) for the general case; however it seems to work only in characteristic 0 and the code is not accessible). Our new algorithm is always faster and succeeds where the other implementations do not finish. We do not know implementations in other computer algebra systems.

6. Extension to non-global orderings

In this section, let $>$ be any monomial ordering on the set $\mathrm{Mon}(x_1, \ldots, x_n)$ of monomials in $x = (x_1, \ldots, x_n)$. That is, $>$ is a total ordering which satisfies

$$\forall \alpha, \beta, \gamma \in \mathbb{Z}_+^n \quad x^\alpha > x^\beta \Rightarrow x^{\alpha+\gamma} > x^{\beta+\gamma},$$

but we do not require that $>$ is a well ordering. The main reference for this section is Greuel and Pfister (2008) where the theory of standard basis for such monomial orderings was developed.

We consider the multiplicatively closed set

$$S_> := \{u \in k[x] \smallsetminus \{0\} \mid \mathrm{LM}(u) = 1\},$$

where LM denotes the leading monomial. The localization of $k[x]$ w.r.t. $S_>$ is denoted as

$$k[x]_> := S_>^{-1} k[x] = \left\{ \frac{f}{u} \;\middle|\; f, u \in k[x], \mathrm{LM}(u) = 1 \right\}.$$

It is shown in Greuel and Pfister (2008, Section 1.5) that $k[x]_>$ is a regular Noetherian ring satisfying

$$k[x] \subset k[x]_> \subset k[x]_{\langle x \rangle},$$

where $k[x]_{\langle x \rangle}$ denotes the localization of $k[x]$ w.r.t. the maximal ideal $\langle x \rangle = \langle x_1, \ldots, x_n \rangle$. Note that
- $k[x]_> = k[x] \iff >$ is global (i.e. $x_i > 1$, $i = 1, \ldots, n$), and
- $k[x]_> = k[x]_{\langle x \rangle} \iff >$ is local (i.e. $x_i < 1$, $i = 1, \ldots, n$).

In applications, in particular in connection with elimination in local rings, we need also *mixed* orderings, where some of the variables are greater than and others smaller than 1. An important case is the product ordering $> = (>_1, >_2)$ on $\mathrm{Mon}(x_1, \ldots, x_n, y_1, \ldots, y_m)$ where $>_1$ is global on $\mathrm{Mon}(x_1, x_2, \ldots, x_n)$ and $>_2$ is arbitrary on $\mathrm{Mon}(y_1, y_2, \ldots, y_m)$. Then

$$k[x, y]_> = (k[y]_{>_2})[x] = k[y]_{>_2} \otimes_k k[x],$$

(cf. Greuel and Pfister (2008, Examples 1.5.3)), which will be used in the extension of our algorithm to non-global orderings.

We now show that for any monomial ordering $>$ and any radical ideal $I \subset k[x]_>$, the normalization of the ring $k[x]_>/I$ is a finitely generated $k[x]_>/I$-module and how to extend Algorithm 3 from Section 4 to this general situation.

For any ideal $I \subset k[x]_>$ we have $I = I'k[x]_>$, with $I' = I \cap k[x]$. Let $(k[x]/I')_>$ (resp. $\overline{(k[x]/I')_>}$) denote the localization w.r.t. the image of $S_>$ in $k[x]/I'$ (resp. in $\overline{k[x]/I'}$). We have $k[x]_>/I \cong (k[x]/I')_>$.

Lemma 6.1. *With the above notations, we have an isomorphism*

$$\overline{k[x]_>/I} \cong \overline{(\overline{k[x]/I'})_>}$$

of $k[x]_>$-algebras. In particular, $\overline{k[x]_>/I}$ is a finitely generated $k[x]_>/I$-module.

Moreover, let $\overline{k[x]/I'} \cong k[x,t]/H$ as $k[x]$-algebras with new variables $t = (t_1, \ldots, t_s)$ and H an ideal in $k[x,t]$. Then

$$\overline{k[x]_>/I} \cong (k[x]_>)[t] \, / \, H(k[x]_>)[t].$$

Proof. The first statement follows immediately from the well-known fact that localization commutes with normalization. Since $\overline{k[x]/I'}$ is module-finite over $k[x]/I'$ the same holds for the localization $(\overline{k[x]/I'})_>$ over $(k[x]/I')_>$. The last statement follows since the image of $S_>$ in $k[x,t]$ localizes $k[x,t]$ only w.r.t. the x variables. □

Remark 6.2. Let $f_1, f_2, \ldots, f_s \in k[x]$ generate $I = \langle f_1, f_2, \ldots, f_s \rangle k[x]_>$ and let I' denote the ideal generated by $f_1, f_2, \ldots, f_s$ in $k[x]$. We can compute $\overline{k[x]_>/I}$ in two different ways.

The first method is to compute a test ideal J and $\mathrm{Hom}_{k[x]_>/I}(J, J)$ in the same manner as described in the previous sections, just w.r.t. the ordering $>$, i.e. in $k[x]_>$. When adding new variables t_i (corresponding to $k[x]_>$-module generators of $\mathrm{Hom}_{k[x]_>/I}(J, J)$) we define on $k[t, x]$ a block ordering $(>_1, >)$ with $>_1$ a global ordering on the (first) t-block (i.e. $t_i > 1$ for all i and $t_i > x_j$ for all i, j) and $>$ the given ordering on the (second) x-block. Then we continue with this new ring and monomial ordering.

This algorithm is correct (by applying Prop. 2.6 to $A = k[x]_>/I$) and terminates because $\overline{k[x]_>/I}$ is finitely generated over $k[x]_>/I$ by Corollary 6.1.

The second method is to compute the normalization of $k[x]/I'$ as in the previous section, with all variables greater than 1. Then we map the result to $k[t, x]_{>_1, >}$ with block ordering $(>_1, >)$ as for the first method. By Corollary 6.1 both methods give the same result, hence the second algorithm is also correct.

If we start with an equidimensional decomposition $I' = \bigcap_{i=1}^r I_i$, then of course we only need to compute the normalization for those ideals I_i for which a standard basis of I_i w.r.t. the ordering $>$ does not contain 1.

Example 6.3. To see the difference between both methods, let

$$I = \langle y^2 - x^2(x+1)^2(x+2) \rangle \subset R := k[x, y]_>,$$

with $>$ a local ordering (i.e. $k[x, y]_> \cong k[x, y]_{\langle x, y \rangle}$). Let $I' = I \cap k[x, y]$. In Figure 1 we can see the real part of the curve $\mathbf{V}(I')$. This curve has two singularities, at the points $P_1 = (0, 0)$ and $P_2 = (-1, 0)$.
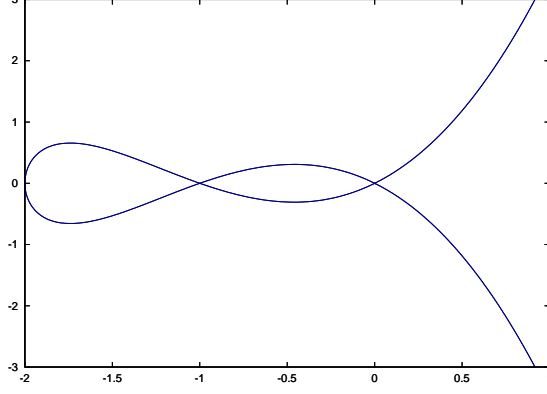
Fig. 1. $y^2 - x^2(x+1)^2(x+2)$

We carry out the first method, setting $A = R/I$. The singular locus of I is $J = \langle x, y \rangle$, which is radical. This is the first test ideal. We take as non-zerodivisor $p := y$ and compute the quotient

$$U_1 := yJ :_A J = \langle x, y \rangle.$$

Since $U_1 \neq \langle y \rangle$ we go on. The ring structure of $1/y \cdot U_1$ is $A_1 = k[t, x, y]_{>_1,>}/I_1$, with block ordering $(>_1, >)$ ($>_1$ any ordering) and $I_1 = \langle tx^4 + 4tx^3 + 5tx^2 + 2tx - y, -ty + x, t^2(x+1)^2(x+2) - 1, x^5 + 4x^4 + 5x^3 + 2x^2 - y^2 \rangle$.

We compute $J_1 := \sqrt{\varphi_1(\langle x, y \rangle)} = \langle x, y, 2t^2 - 1 \rangle_{A_1}$.

Mapping J_1 to $Q(A)$ using $d_1 = y$ as denominator, we get $J_1 \cong 1/y \cdot H_1$, with $H_1 := \langle yx, y^2 \rangle$. (The image of $2t^2 - 1$ in $Q(A)$ is $(-10xy - 8x^2y - 2x^3y)/y$, which is already in $1/y \cdot \langle yx, y^2 \rangle$.) We compute the quotient

$$U_2 := y^2 \langle yx, y^2 \rangle :_A \langle yx, y^2 \rangle = \langle xy, y^2 \rangle.$$

We see that $yU_1 = U_2$. This means that A_1 was already normal and isomorphic to the normalization of A, which is therefore $1/y \cdot \langle x, y \rangle_A$.

Let us now apply the second method. We set $R' := k[x, y]$ and $A' = R'/I'$. The singular locus of I' is $J = \langle x^2 + x, y \rangle$, which is radical. J serves as first test ideal. As non-zerodivisor we choose $p := y$ and compute the quotient

$$U_1 := yJ :_{A'} J = \langle y, x^3 + 3x^2 + 2x \rangle.$$

As $U_1 \neq \langle y \rangle$, we continue. We compute A_1', the ring structure of $1/y \cdot U_1$, $A_1' = k[t, x, y]/\langle tx^2 + tx - y, -ty + x^3 + 3x^2 + 2x, t^2 - x - 2, x^5 + 4x^4 + 5x^3 + 2x^2 - y^2 \rangle$, and $J_1 = \sqrt{\varphi_1(\langle x^2 + x, y \rangle)} = \langle x^2 + x, y \rangle$.

Mapping J_1 to $Q(A')$ using $d_1 = y$ as denominator, we obtain $J_1 \cong 1/y \cdot H_1$, with $H_1 := \langle y(x^2 + x), y^2 \rangle$. We compute the quotient

$$U_2 := y^2 \langle y(x^2 + x), y^2 \rangle :_{A'} \langle y(x^2 + x), y^2 \rangle = \langle y^2, y(x^3 + 3x^2 + 2x) \rangle.$$

Now we have $yU_1 = U_2$, and thus A_1' was already normal and isomorphic to the normalization of A'. Therefore, the normalization $\bar{A}$ equals $1/y \cdot \langle y, x^3 + 3x^2 + 2x \rangle_A = 1/y \cdot \langle y, x \rangle_A$, as before.

17

Remark 6.4. In the previous example, using the first method yields simpler test ideals and quotients. However, our experience is that in general, computations with non-global orderings are often slower than computations with global orderings, and therefore the second method should be preferred at least if the input ideal is prime. On the other hand the computation should be faster with the first method if the ideal, or its jacobian ideal, has complicated components which vanish in the localization.

References

Bosma, W., Cannon, J. J., Playoust, C., 1997. The Magma algebra system. I. The user language. J. Symbolic Comput. 24 (3–4), 235–265.

Brennan, J. P., Vasconcelos, W. V., 2001. On the structure of closed ideals. Math. Scand. 88 (1), 3–16.

Bruns, W., Koch, R., 2001. Computing the integral closure of an affine semigroup. Univ. Iagel. Acta Math. (39), 59–70.

Campillo, A., Greuel, G.-M., Lossen, C., 2007. Equisingular calculations for plane curve singularities. J. Symbolic Comput. 42, 89–114.

Cohen, H., 1993. A course in computational algebraic number theory. Vol. 138 of Graduate Texts in Mathematics. Springer-Verlag, Berlin.

de Jong, T., 1998. An algorithm for computing the integral closure. J. Symbolic Comput. 26 (3), 273–277.

Decker, W., de Jong, T., Greuel, G.-M., Pfister, G., 1999. The normalization: a new algorithm, implementation and comparisons. In: Computational methods for representations of groups and algebras (Essen, 1997). Vol. 173 of Progr. Math. Birkhäuser, Basel, pp. 177–185.

Ford, D. J., 1987. The construction of maximal orders over a Dedekind domain. J. Symbolic Comput. 4 (1), 69–75.

Gianni, P., Trager, B., 1997. Integral closure of Noetherian rings. In: Proceedings of the 1997 International Symposium on Symbolic and Algebraic Computation (Kihei, HI). ACM, New York, pp. 212–216 (electronic).

Grauert, H., Remmert, R., 1971. Analytische Stellenalgebren. Springer-Verlag, Berlin, unter Mitarbeit von O. Riemenschneider, Die Grundlehren der mathematischen Wissenschaften, Band 176.

Grayson, D. R., Stillman, M. E., 2009. Macaulay2 1.2, a software system for research in algebraic geometry. Available at http://www.math.uiuc.edu/Macaulay2/.

Greuel, G.-M., Laplagne, S., Pfister, G., 2009a. `normal.lib`, a SINGULAR library for computing the normalization of affine rings.

Greuel, G.-M., Pfister, G., 2008. A **Singular** introduction to commutative algebra, extended Edition. Springer, Berlin, with contributions by Olaf Bachmann, Christoph Lossen and Hans Schönemann, With 1 CD-ROM (Windows, Macintosh and UNIX).

Greuel, G.-M., Pfister, G., Schönemann, H., 2009b. Singular 3.1.0 — A computer algebra system for polynomial computations. http://www.singular.uni-kl.de.

Leonard, D. A., Pellikaan, R., 2003. Integral closures and weight functions over finite fields. Finite Fields Appl. 9 (4), 479–504.

Matsumoto, R., 2001. Computing the radical of an ideal in positive characteristic. J. Symbolic Comput. 32 (3), 263–271.

Seidenberg, A., 1970. Construction of the integral closure of a finite integral domain. Rend. Sem. Mat. Fis. Milano 40, 100–120.

Seidenberg, A., 1975. Construction of the integral closure of a finite integral domain. II. Proc. Amer. Math. Soc. 52, 368–372.

Singh, A., Swanson, I., 2008. An algorithm for computing the integral closure. Preprint available at arXiv, http://arxiv.org/abs/0901.0871.

Stolzenberg, G., 1968. Constructive normalization of an algebraic variety. Bull. Amer. Math. Soc. 74, 595–599.

Swanson, I., Huneke, C., 2006. Integral closure of ideals, rings, and modules. Vol. 336 of London Mathematical Society Lecture Note Series. Cambridge University Press, Cambridge.

Traverso, C., 1986. A study on algebraic algorithms: the normalization. Rend. Sem. Mat. Univ. Politec. Torino (Special Issue), 111–130 (1987), conference on algebraic varieties of small dimension (Turin, 1985).

Vasconcelos, W., 2005. Integral closure. Springer Monographs in Mathematics. Springer-Verlag, Berlin, rees algebras, multiplicities, algorithms.

Vasconcelos, W. V., 1991. Computing the integral closure of an affine domain. Proc. Amer. Math. Soc. 113 (3), 633–638.

Vasconcelos, W. V., 1998. Computational methods in commutative algebra and algebraic geometry. Vol. 2 of Algorithms and Computation in Mathematics. Springer-Verlag, Berlin, with chapters by David Eisenbud, Daniel R. Grayson, Jürgen Herzog and Michael Stillman.

Vasconcelos, W. V., 2000. Divisorial extensions and the computation of integral closures. J. Symbolic Comput. 30 (5), 595–604.