An algorithm for computing the integral closure

Anurag K. Singh and Irena Swanson

We present an algorithm for computing the integral closure of a reduced ring that is finitely generated over a finite field.

Leonard and Pellikaan [2003] devised an algorithm for computing the integral closure of weighted rings that are finitely generated over finite fields. Previous algorithms proceed by building successively larger rings between the original ring and its integral closure [de Jong 1998; Seidenberg 1970; 1975; Stolzenberg 1968; Vasconcelos 1991; 2000]; the Leonard–Pellikaan algorithm instead starts with the first approximation being a finitely generated module that contains the integral closure, and successive steps produce submodules containing the integral closure. The weights in [Leonard and Pellikaan 2003] impose strong restrictions, and play a crucial role in various steps of their algorithm; see Remark 1.7. We present a modification of the Leonard–Pellikaan algorithm that works in much greater generality: it computes the integral closure of a reduced ring that is finitely generated over a finite field.

We discuss an implementation of the algorithm in Macaulay 2, and provide comparisons with de Jong's algorithm [1998].

1. The algorithm

Our main result is the following theorem; see Remark 1.5 for an algorithmic construction of an element D as below when R is a domain, and for techniques for dealing with the more general case of reduced rings.

Theorem 1.1. *Let R be a reduced ring that is finitely generated over a computable field of characteristic $p > 0$. Set $\bar{R}$ to be the integral closure of R in its total ring of fractions. Suppose D is a nonzerodivisor in the conductor ideal of R, that is, D is a nonzerodivisor with $D\bar{R} \subseteq R$.*

(1) *Set $V_0 = \frac{1}{D}R$, and inductively define $V_{e+1} = \{f \in V_e \mid f^p \in V_e\}$ for $e \geqslant 0$. Then the modules V_e are algorithmically constructible.*

(2) *The descending chain $V_0 \supseteq V_1 \supseteq V_2 \supseteq V_3 \supseteq \cdots$ stabilizes. If $V_e = V_{e+1}$, then V_e equals $\overline{R}$.*

The prime characteristic enables us to use the Frobenius or pth power map; this is what makes the modules V_e algorithmically constructible.

Remark 1.2. For each integer $e \geqslant 0$, the module DV_e is an ideal of R; we set $U_e = DV_e$ and use this notation in the proof of Theorem 1.1 as well as in the Macaulay 2 code in the following section. The inductive definition of V_e translates to $U_0 = R$ and $U_{e+1} = \{r \in U_e \mid r^p \in D^{p-1}U_e\}$ for $e \geqslant 0$.

Proof of Theorem 1.1. (1) By Remark 1.2, it suffices to establish that the ideals U_e are algorithmically constructible. This follows inductively since

$$U_{e+1} = U_e \cap \ker\left(R \xrightarrow{\ F\ } R \xrightarrow{\ \pi\ } R/D^{p-1}U_e\right) \quad \text{for } e \geqslant 0,$$

where F is the Frobenius endomorphism of R, and π the canonical surjection.

(2) By construction, one has $V_{e+1} \subseteq V_e$ for each e. Moreover, it is a straightforward verification that

$$V_e = \{f \in V_0 \mid f^{p^i} \in V_0 \text{ for each } i \leqslant e\}.$$

Suppose $f \in \overline{R}$. Then $f^{p^i} \in \overline{R}$ for each $i \geqslant 0$, so $Df^{p^i} \in R$. It follows that $f \in V_e$ for each e.

If $V_{e+1} = V_e$ for some positive integer e, then it follows from the inductive definition that $V_{e+i} = V_e$ for each $i \geqslant 1$.

Let $v_1, \ldots, v_s \colon R \longrightarrow \mathbb{Z} \cup \{\infty\}$ be the Rees valuations of the ideal DR, that is, v_i are valuations such that for each $n \in \mathbb{N}$, the integral closure of the ideal $D^n R$ equals $\{r \in R \mid v_i(r) \geqslant nv_i(D) \text{ for each } i\}$. Let e be an integer such that $p^e > v_i(D)$ for each i. Suppose $r/D \in V_e$. Then $(r/D)^{p^e} \in V_0$, so $r^{p^e} \in D^{p^e-1}R$. It follows that $p^e v_i(r) \geqslant (p^e - 1)v_i(D)$ for each i, and hence that

$$v_i(r) \geqslant v_i(D) - v_i(D)/p^e > v_i(D) - 1$$

for each i. Since $v_i(r)$ is an integer, it follows that $v_i(r) \geqslant v_i(D)$ for each i, and therefore $r \in \overline{DR}$. But then r belongs to the integral closure of the ideal $D\overline{R}$ in $\overline{R}$. Since principal ideals are integrally closed in $\overline{R}$, it follows that $r \in D\overline{R}$, whence $r/D \in \overline{R}$. $\qquad\square$

Remark 1.3. If R is an integral domain satisfying the Serre condition S_2, then each module V_e is S_2 as well:

Proceed by induction on e. Without loss of generality, assume R is local. Let x, y be part of a system of parameters for R. Suppose $yv \in xV_{e+1}$ for an element

$v \in V_{e+1}$. Then $yv/x \in V_{e+1}$, that is, $yv/x \in V_e$ and $y^p v^p / x^p \in V_e$, or equivalently, $yv \in xV_e$ and $y^p v^p \in x^p V_e$. Since V_e is S_2 by the inductive hypothesis, it follows that $v \in xV_e$ and $v^p \in x^p V_e$, hence $v \in xV_{e+1}$.

Remark 1.4. In the notation of Theorem 1.1, suppose e is an integer such that $V_e = V_{e+1}$. We claim that the integral closure of a principal ideal aR is

$$\{r \in R \mid Dr^{p^i} \in a^{p^i} R \text{ for each } i \leqslant e+1\}.$$

To see this, suppose r is an element of the ideal displayed above. Then $Dr^p = ga^p$ for some $g \in R$. Since

$$D(r/a)^{p^i} \in R \quad \text{for each } i \leqslant e+1,$$

it follows that

$$D(g/D)^{p^i} \in R \quad \text{for each } i \leqslant e.$$

But then $g/D \in V_e$, which implies that $g/D \in V_i$ for each i. Hence $D(r/a)^{p^i} \in R$ for each i, equivalently $r \in \overline{aR}$.

Remark 1.5. Let R be a reduced ring that is finitely generated over a perfect field K of prime characteristic p. We describe how to algorithmically obtain a nonzerodivisor D in the conductor ideal of R.

Case 1. Suppose R is an integral domain. Consider a presentation of R over K, say $R = K[x_1, \ldots, x_n]/(f_1, \ldots, f_m)$. Set $h = \text{height}(f_1, \ldots, f_m)$. Then the determinant of each $h \times h$ submatrix of the Jacobian matrix $(\partial f_i / \partial x_j)$ multiplies $\overline{R}$ into R; this may be concluded from the Lipman–Sathaye Theorem [1981] (also found as Theorem 12.3.10 in [Huneke and Swanson 2006]), as discussed in the following paragraph. At least one such determinant has nonzero image in R, and can be chosen as the element D in Theorem 1.1. Other approaches to obtaining an element D are via the proof of [Huneke and Swanson 2006, Theorem 3.1.3], or equivalently, via the results from [Stichtenoth 1993].

Let J be the ideal of R generated by the images of the $h \times h$ submatrices of $(\partial f_i / \partial x_j)$. We claim that J is contained in the conductor of R. By passing to the algebraic closure, assume K is algebraically closed. After a linear change of coordinates, assume that the x_i are in general position, specifically, that for any $n - h$ element subset Λ of $\{x_1, \ldots, x_n\}$, the extension $K[\Lambda] \subseteq R$ is a finite integral extension, equivalently that $K[\Lambda]$ is a Noether normalization of R. By the Lipman–Sathaye Theorem, the relative Jacobian $J_{R/K[\Lambda]}$ is contained in the conductor ideal. The claim now follows since, as Λ varies, the relative Jacobian ideals $J_{R/K[\Lambda]}$ generate the ideal J.

Even when R is not necessarily an integral domain, the ideal J, as defined above, is not contained in any minimal prime of R; this follows from the Jacobian criterion, see, for example, [Huneke and Swanson 2006, Theorem 4.4.9].

Case 2. In the case where R is a reduced equidimensional ring, one may proceed as above and choose D to be the determinant of an $h \times h$ submatrix of $(\partial f_i / \partial x_j)$, and then test to see whether D is a nonzerodivisor. If it turns out that D is a nonzero zerodivisor, set $I_1 = (0 :_R D)$ and $I_2 = (0 :_R I_1)$. Then each of R/I_1 and R/I_2 is a reduced equidimensional ring, with fewer minimal primes than R, and $\overline{R} = \overline{R/I_1} \times \overline{R/I_2}$. Hence $\overline{R}$ may be computed by computing the integral closure of each R/I_i.

Case 3. If R is a reduced ring that is not necessarily equidimensional, one may compute the minimal primes $P_1, \ldots, P_n$ of R using an algorithm for primary decomposition—admittedly an expensive step—and then compute $\overline{R}$ using Case 1 and the fact that $\overline{R} = \overline{R/P_1} \times \cdots \times \overline{R/P_n}$.

Remark 1.6. Theorem 1.1 may be extended as follows. Suppose a reduced ring R has an endomorphism φ with the property that for each valuation $\upsilon : R \longrightarrow \mathbb{Z} \cup \{\infty\}$, there exists an integer $k \geqslant 2$ such that

$$\upsilon(\varphi(r)) = k\upsilon(r) \quad \text{for each } r \in R. \tag{1.6.1}$$

Let D be a nonzerodivisor in the conductor of R. Set $V_0 = \frac{1}{D} R$ and

$$V_{e+1} = \{f \in V_e \mid \varphi(f) \in V_e\} \quad \text{for } e \geqslant 0.$$

Imitating the proof of Theorem 1.1, one sees that the descending chain

$$V_0 \supseteq V_1 \supseteq V_2 \supseteq V_3 \supseteq \cdots$$

stabilizes at $\overline{R}$. If colon ideals and kernels of endomorphisms are computable in R, then each V_e is algorithmically constructible.

As an example, consider a polynomial ring $A = \mathbb{F}[x_1, \ldots, x_k]$ over a field $\mathbb{F}$. Let R be a subring of A that is generated, as an $\mathbb{F}$-algebra, by finitely many monomials. Fix an integer $k \geqslant 2$. The $\mathbb{F}$-algebra endomorphism of A with $x_i \mapsto x_i^k$ restricts to an endomorphism φ of R satisfying property (1.6.1). Thus, one obtains an algorithm for computing the integral closure of affine semigroup rings; see Bruns and Koch [2001] for another algorithm.

Remark 1.7. The Leonard–Pellikaan algorithm [2003] is based on earlier work of Leonard [2001]. These papers make use of the Frobenius endomorphism along with a *weighted total-degree monomial ordering*; this is a monomial ordering under which there are only finitely many elements preceding any given element, and this is an essential ingredient in proving the convergence of their algorithm. The affine domains considered in [Leonard and Pellikaan 2003] are constructed as towers in the following sense: R_0 is a finite field; if R_{j-1} is given with a weight function wt_{j-1}, then R_j is the integral closure of $R_{j-1}[x_j]/(\varphi_j(x_j))$ in $F_{j-1}[x_j]/(\varphi_j(x_j))$,

as computed by their algorithm; here F_{j-1} is the field of fractions of R_{j-1}, and

$$\varphi_j(x_j) = x_j^{m_j} + u_j \prod_{i=1}^{j-1} x_i^{\alpha_{i,j}} + g_j(x_j, \ldots, x_1)$$

is an element of $R_{j-1}[x_j]$ that is irreducible and monic in x_j, such that u_j is a nonzero element of R_0, and the weight function satisfies

$$\mathrm{wt}_j(g_j(x_j, \ldots, x_1)) < \mathrm{wt}_j(x_j^{m_j}) = \mathrm{wt}_j\left(\prod_{i=1}^{j-1} x_i^{\alpha_{i,j}}\right),$$

where wt_j is a modification (not a simple extension) of wt_{j-1} that requires further technical assumptions on the m_j and $\alpha_{i,j}$. A complexity analysis of some aspects of the Leonard–Pellikaan algorithm is carried out in [Hu and Maharaj 2008].

2. Implementation and examples

Here is our code in Macaulay 2 [Grayson and Stillman], which uses this algorithm to compute the integral closure.

Input: An integral domain R that is finitely generated over a finite field, and, optionally, a nonzero element D of the conductor ideal of R.

Output: A set of generators for $\bar{R}$ as a module over R.

Macaulay 2 function:

```
icFracP = method(Options=>{conductorElement => null})
icFracP Ring := List => o -> (R) -> (
    P := ideal presentation R;
    c := codim P;
    S := ring P;
    if o.conductorElement === null then (
       J := promote(jacobian P,R);
       n := 1;
       det1 := ideal(0_R);
       while det1 == ideal(0_R) do (
          det1 = minors(c,J);
          n = n+1
       );
       D := det1_0;
    ) else D = o.conductorElement;
    p := char(R);
    K := ideal(1_R);
    U := ideal(0_R);
    F := apply(generators R, i-> i^p);
```

```
while (U != K) do (
   U = K;
   L := U*ideal(D^(p-1));
   f := map(R/L,R,F);
   K = intersect(kernel f, U);
);
U = mingens U;
if numColumns U == 0 then {1_R}
else apply(numColumns U, i-> U_(0,i)/D)
)
```

Since the Leonard–Pellikaan algorithm uses the Frobenius endomorphism, it is less efficient when the characteristic of the ring is a large prime. In the examples that follow, the computations are performed on a MacBook Pro computer with a 2 GHz Intel Core Duo processor; the time units are seconds. The comparisons are with de Jong's algorithm [1998] as implemented in the program ICfractions in Macaulay 2, version 1.1.

Example 2.1. Let $\mathbb{F}_2[x, y, t]$ be a polynomial ring over the field $\mathbb{F}_2$, and set $R = \mathbb{F}_2[x, y, x^2t, y^2t]$. Then R has a presentation $\mathbb{F}_2[x, y, u, v]/(x^2v - y^2u)$, which shows, in particular, that x^2 is an element of the conductor ideal. Setting $D = x^2$, the algorithm above computes that the integral closure of R is generated, as an R-module, by the elements 1 and xyt. Tracing the algorithm, one sees that V_0 is not equal to V_1, that V_1 is not equal to V_2, and that $V_2 = V_3$. Indeed, these R-modules are

$$V_0 = \frac{1}{x^2}R, \qquad V_1 = \frac{1}{x}R + ytR, \qquad V_e = R + ytR \text{ for } e \geqslant 2.$$

As is to be expected, the algorithm is less efficient as the characteristic of the ground field increases:

characteristic p	2	3	5	7	11	13	17	37	97
icFracP	0.04	0.03	0.04	0.04	0.04	0.05	0.05	0.13	0.59
icFractions	0.08	0.09	0.09	0.09	0.14	0.15	0.15	0.15	0.15

Integral closure of $\mathbb{F}_p[x, y, u, v]/(x^2v - y^2u)$.

We remark that R is an affine semigroup ring, so its integral closure may also be computed using the program normaliz of Bruns and Koch [2001].

Example 2.2. Consider the hypersurface

$$R = \mathbb{F}_p[u, v, x, y, z]/(u^2x^4 + uvy^4 + v^2z^4).$$

It is readily verified that R is a domain, and that $t = ux^4/v$ is integral over R. The ring $R[t]$ has a presentation $\mathbb{F}_p[u, v, x, y, z, t]/I$, where I is the ideal generated

by the 2×2 minors of the matrix

$$\begin{pmatrix} u & t & -z^4 \\ v & x^4 & t+y^4 \end{pmatrix}.$$

Since the entries of the matrix form a regular sequence in $\mathbb{F}_p[u, v, x, y, z, t]$, the ring $R[t]$ is Cohen–Macaulay. Moreover, if $p \neq 2$, then the singular locus of $R[t]$ is $V(t, y, xz, vz, ux)$ which has codimension 2, so $R[t]$ is normal.

If $p = 2$ then the ring $R[t]$ is not normal; indeed, in this case, the integral closure of R is generated, as an R-module, by the elements

$$1, \qquad \sqrt{uv}, \qquad \frac{ux + z\sqrt{uv}}{y}, \qquad \frac{vz + x\sqrt{uv}}{y}, \qquad \frac{uxz + z^2\sqrt{uv}}{uy}.$$

For small values of p, these computations may be verified on Macaulay 2 using either algorithm; some computations times are recorded next. (Here and in the next table $*$ means that the computation did not terminate within six hours.)

characteristic p	2	3	5	7	11
icFracP		0.07	0.22	9.67	143	12543
icFractions	1.16	$*$	$*$	$*$	$*$

Integral closure of $\mathbb{F}_p[u, v, x, y, z]/(u^2x^4 + uvy^4 + v^2z^4)$.

Example 2.3. Consider the hypersurface

$$R = \mathbb{F}_p[u, v, x, y, z]/(u^2x^p + 2uvy^p + v^2z^p),$$

where p is an odd prime. We shall see that $\bar{R}$ has $p+1$ generators as an R-module, but first some comparisons:

characteristic p	3	5	7	11	13	17	19	23
icFracP	0.07	0.09	0.27	1.81	4.89	26	56	225
icFractions	1.49	75.00	4009	$*$	$*$	$*$	$*$	$*$

Integral closure of $\mathbb{F}_p[u, v, x, y, z]/(u^2x^p + 2uvy^p + v^2z^p)$.

We claim that $\bar{R}$ is generated, as an R-module, by the elements

$$1, \qquad \sqrt{y^2 - xz}, \qquad \text{and} \qquad u^{i/p}v^{(p-i)/p} \text{ for } 1 \leqslant i \leqslant p-1. \tag{2.3.1}$$

It is immediate that these elements are integral over R; to see that they belong to the fraction field of R, note that

$$\sqrt{y^2 - xz} = \pm \frac{uy^p + vz^p}{u(y^2 - xz)^{(p-1)/2}}$$

and that, by the quadratic formula, one also has

$$\left(\frac{u}{v}\right)^{1/p} = \frac{-y \pm \sqrt{y^2 - xz}}{x}. \tag{2.3.2}$$

Moreover, using (2.3.2), it follows that

$$v^{1/p}\sqrt{y^2 - xz} = \pm(xu^{1/p} + yv^{1/p}),$$

and hence the R-module generated by the elements (2.3.1) is indeed an R-algebra. It remains to verify that the ring

$$A = R\left[\sqrt{y^2 - xz}, u^{i/p}v^{(p-i)/p} \mid 1 \leqslant i \leqslant p - 1\right]$$

is normal. For this, it suffices to verify that

$$B = R\left[\sqrt{y^2 - xz}, u^{1/p}, v^{1/p}\right]$$

is normal, since A is a direct summand of B as an A-module: use the grading on B where $\deg x = \deg y = \deg z = 0$ and $\deg u^{1/p} = 1 = \deg v^{1/p}$, in which case A is the pth Veronese subring $\bigoplus_{i \in \mathbb{N}} B_{ip}$. The ring B has a presentation $\mathbb{F}_p[x, y, z, d, s, t]/I$, where I is generated by the 2×2 minors of the matrix

$$\begin{pmatrix} y+d & z & s \\ x & y-d & -t \end{pmatrix},$$

and $s \mapsto u^{1/p}$, $t \mapsto v^{1/p}$, $d \mapsto \sqrt{y^2 - xz}$. But then — after a change of variables — B is a determinantal ring, and hence normal.

Acknowledgment

References

[Bruns and Koch 2001] W. Bruns and R. Koch, "Computing the integral closure of an affine semi-group", *Univ. Iagel. Acta Math.* **39** (2001), 59–70. MR 2002m:20095 Zbl 1006.20045

[Grayson and Stillman] D. R. Grayson and M. E. Stillman, Macaulay 2, a software system for research in algebraic geometry, Available at http://www.math.uiuc.edu/Macaulay2.

[Hu and Maharaj 2008] X. Hu and H. Maharaj, "On the qth power algorithm", *Finite Fields Appl.* **14**:4 (2008), 1068–1082. MR 2009g:14028 Zbl 1153.14022

[Huneke and Swanson 2006] C. Huneke and I. Swanson, *Integral closure of ideals, rings, and modules*, London Mathematical Society Lecture Note Series **336**, Cambridge University Press, 2006. MR 2008m:13013 Zbl 1117.13001

[de Jong 1998] T. de Jong, "An algorithm for computing the integral closure", *J. Symbolic Comput.* **26**:3 (1998), 273–277. MR 99d:13007 Zbl 0932.13021

[Leonard 2001] D. A. Leonard, "Finding the defining functions for one-point algebraic-geometry codes", *IEEE Trans. Inform. Theory* **47**:6 (2001), 2566–2573. MR 2003d:94122 Zbl 1019.94030

[Leonard and Pellikaan 2003] D. A. Leonard and R. Pellikaan, "Integral closures and weight functions over finite fields", *Finite Fields Appl.* **9**:4 (2003), 479–504. MR 2005d:13015 Zbl 1085.11059

[Lipman and Sathaye 1981] J. Lipman and A. Sathaye, "Jacobian ideals and a theorem of Briançon-Skoda", *Michigan Math. J.* **28**:2 (1981), 199–222. MR 83m:13001 Zbl 0438.13019

[Seidenberg 1970] A. Seidenberg, "Construction of the integral closure of a finite integral domain", *Rend. Sem. Mat. Fis. Milano* **40** (1970), 100–120. MR 45 #3396 Zbl 0218.14023

[Seidenberg 1975] A. Seidenberg, "Construction of the integral closure of a finite integral domain. II", *Proc. Amer. Math. Soc.* **52** (1975), 368–372. MR 54 #12741 Zbl 0333.13004

[Stichtenoth 1993] H. Stichtenoth, *Algebraic function fields and codes*, Springer, Berlin, 1993. MR 94k:14016 Zbl 0816.14011

[Stolzenberg 1968] G. Stolzenberg, "Constructive normalization of an algebraic variety", *Bull. Amer. Math. Soc.* **74** (1968), 595–599. MR 37 #201 Zbl 0164.04202

[Vasconcelos 1991] W. V. Vasconcelos, "Computing the integral closure of an affine domain", *Proc. Amer. Math. Soc.* **113**:3 (1991), 633–638. MR 92b:13013 Zbl 0739.13014

[Vasconcelos 2000] W. V. Vasconcelos, "Divisorial extensions and the computation of integral closures", *J. Symbolic Comput.* **30**:5 (2000), 595–604. MR 2001k:13017 Zbl 0999.13004

singh@math.utah.edu   *University of Utah, Department of Mathematics, 155 South 1400 East, Salt Lake City, UT 84112-0090, United States* http://www.math.utah.edu/~singh/

iswanson@reed.edu   *Reed College, Department of Mathematics, 3203 SE Woodstock Boulevard, Portland, OR 97202-8199, United States* http://people.reed.edu/~iswanson/