COMPUTING THE INTEGRAL CLOSURE OF AN AFFINE DOMAIN

WOLMER V. VASCONCELOS

(Communicated by Louis J. Ratliff, Jr.)

ABSTRACT. Let $A = k[x_1, \dots, x_n]/P$ be an affine domain over a field k , with P given by a set of generators. We give a method to find the defining ideal of its integral closure B as an affine domain $B = k[y_1, \dots, y_m]/Q$.

INTRODUCTION

The problem of describing constructively the integral closure of an affine domain has been dealt with previously in [10], and particularly in [9]. Our reasons for revisiting the question are to propose an effective method that makes use of resources that have since become available. Among these is a better recognition of the algebraic techniques which have a smoother merging with computational techniques based on the Buchberger algorithm.

1. SERRE'S CRITERION

The setting we use is that provided by the normality criterion of Serre [7, Theorem 39], which for convenience is stated for the case of an integral domain.

Theorem 1.1. *Let A be a Noetherian integral domain. A is integrally closed if and only if the following conditions hold:*

- (a) *For each prime $\wp$ of codimension one, $A_{\wp}$ is a discrete valuation domain.*
- (b) *Every ideal I of codimension two contains a regular sequence on A with two elements.*

An equivalent way of stating (b) is: Principal ideals of A do not have embedded primary components. It is known as condition S_2 , while (a) is the condition R_1 .

The task is, given an affine domain A , to find an integral rational extension B that satisfies both S_2 and R_1 . The integral closure B will be determined by

Received by the editors May 14, 1990 and, in revised form, June 4, 1990.

1980 *Mathematics Subject Classification* (1985 Revision). Primary 13B20; Secondary 13-04, 13C15.

The author was partially supported by the NSF.

two types of extensions: first, through a preprocessing that enables S_2 , followed by a sequence of extensions of a second kind. We are going to see that if A already satisfies R_1 , then B can be computed in a single step.

We will not be specific about which software/hardware was used. It suffices to say that all the better known packages (e.g. *Macaulay*, *Macsyma*, *Maple*, *Reduce*), in a variety of platforms, were employed. All the techniques are based on Gröbner bases calculations. (See [1] for a discussion of fundamental algorithms, and their capabilities.)

2. THE DOUBLE DUAL

We assume that we have a Noether normalization of A (see [6] for details):

$$R = k[z] = k[z_1, \dots, z_d] \hookrightarrow A.$$

A is a torsion free R -module, and the process that gives the Noether normalization also yields a presentation of A as an R -module:

$$R^p \xrightarrow{\varphi} R^q \rightarrow A \rightarrow 0.$$

The double dual, or bidual, of A is the module

$$A^{**} = \text{Hom}_R(\text{Hom}_R(A, R), R).$$

Proposition 2.1. A^{**} is a subring of B .

Proof. It follows from the description by Samuel [8] of the bidual of a finitely generated torsion-free module M over a normal domain R :

Proposition 2.2.

$$M^{**} = \bigcap M_{\varphi}, \quad \text{height } \varphi = 1.$$

The intersection is taken in the vector space $V = M \otimes R_{(0)}$.

As a consequence of Theorem 1.1, it follows that B is a reflexive R -module.

We must now find a finite formula for A^{**} , for which purpose we make use of the presentation of A .

For an ideal I of an integral domain A , $I^{-1} = A : I$ has the usual meaning:

$$I^{-1} = \{x \in \text{field of fractions of } A \mid x \cdot I \subset A\}.$$

I^{-1} is an A -module, canonically isomorphic to $\text{Hom}_A(I, A)$. As an R -module I^{-1} is reflexive if A is a reflexive R -module. To see this, it is enough to show that I^{-1} is the R -dual of some R -module. Thus, since $A = \text{Hom}_R(A^*, R)$ we have by adjointness

$$\text{Hom}_A(I, A) = \text{Hom}_A(I, \text{Hom}_R(A^*, R)) = \text{Hom}_R(I \otimes_A A^*, R).$$

Let J be the first nonvanishing Fitting ideal of A as an R -module. Since A is a torsion-free R -module, $\text{height } J \geq 2$. Pick f, g , two relatively prime polynomials in J . Define

$$C = \bigcup_{i \geq 1} (A : (f, g)^i).$$

Proposition 2.3. $A^{**} = C$.

Proof. From Proposition 2.2, it follows that the right-hand side of this formula is contained in A^{**} . (At the same time, this shows that the right-hand side has a stable value, since B is a finitely generated R -module.) Conversely, let $x \in A^{**}$ and denote by L the R -conductor of A^{**} into C , that is,

$$L = \{r \in R \mid rx \in C\}.$$

L is an ideal of R whose radical contains J . Indeed, if $\wp$ is a prime containing L but not J , $A_{\wp}$ is a free $R_{\wp}$ -module and therefore coincides with $A_{\wp}^{**}$. But $A_{\wp} \subset C_{\wp}$ contradicts the definition of L . This means that for some integer t , $(f, g)^t \cdot x \in A$ and therefore $x \in C$. $\square$

The point of this construction is that A^{**} will satisfy condition S_2 . The other overrings to be constructed will also preserve this property. We have the following:

Theorem 2.4. If A satisfies the condition R_1 , then $B = C$.

Proof. C , being a finite, rational extension of A , clearly inherits the condition R_1 from it. $\square$

Remark 2.5. In many cases it is unnecessary to find the Noether normalization, since it is only used to provide the elements f and g . It is clearly enough that they define part of a normalizing system of parameters and lie in the ideal that defines the Cohen-Macaulay locus of A .

There remains to obtain a presentation of $A^{**} = k[y_1, \dots, y_m]/Q$. Once that is done, we replace A by A^{**} .

We use a method developed in [11], exploiting the fact that the transform is computed relative to a two-generated ideal. There will be two steps to consider:

Algorithm 2.6. Let A be an affine domain and let f, g be a regular sequence as above.

(a) The formula

$$\begin{aligned} A(t) &:= A : (f, g)^t = \left(\bigcap_{1 \leq i \leq t} (A f^t :_A g^i f^{t-i}) \right) f^{-t} \\ &= \left(\bigcap_{1 \leq i \leq t} (A f^i :_A g^i) \right) f^{-t} \end{aligned}$$

yields $a_1 f^{-r}, \dots, a_s f^{-r}$, such that $A^{**} = A[a_1 f^{-r}, \dots, a_s f^{-r}]$, where r is the stable value of t .

(b) For each $a_i f^{-r}$ consider the linear polynomial $f^r U_i - A_i$, where the U_i are indeterminates and A_i is a representative in $k[x_1, \dots, x_n]$ of a_i . Let $K = (P, f^r U_1 - A_1, \dots, f^r U_s - A_s)$. Let Q be the “rational

closure" of K :

$$Q = \bigcup_{t \geq 1} (K :_{k[x_1, \dots, x_n, U_1, \dots, U_s]} f^t).$$

Then

$$A^{**} = k[x_1, \dots, x_n, U_1, \dots, U_s]/Q.$$

The proof of correctness is clear from the discussion. An advantage of computing the transforms $A(t)$ lies in the convenience of testing for stabilization.

In the sequel, when we replace A by a larger ring C , C will always be a reflexive A -module, and therefore S_2 passes from A to C .

Example 2.7. The affine domain defined by the prime ideal of [2, Example 4.7] fits nicely here. $A = k[a, b, c, d, e]/P$ satisfies the condition of the theorem. Its integral closure is $B = k[a, b, c, d, e, u, v]/Q$, with Q generated by the polynomials (where P is the radical of the ideal generated by the first three polynomials):

$$\begin{aligned} & ab^3c + bc^3d + a^3be + cd^3e + ade^3, \\ & a^2bc^2 + b^2cd^2 + a^2d^2e + ab^2e^2 + c^2de^2, \\ & a^5 + b^5 + c^5 + d^5 - 5abcde + e^5, \\ & a^4bc - ab^4e - 2b^2c^2de + a^2cde^2 + bd^3e^2 + du, \\ & a^3b^2c - bc^2d^3 - b^5e - d^5e + 2abcde^2 - ev, \\ & a^2b^2cd + b^2c^3e + a^4de - 2bcd^2e^2 - abe^4 - cu, \\ & bc^5 - 2ab^2cde + c^3d^2e - a^3de^2 + be^5 - bv, \\ & b^5c + a^2b^3e - abc^2de - ad^3e^2 + cv, \\ & ab^2c^3 + abcd^2e - a^2be^3 - de^5 + dv, \\ & abc^2d^2 - b^3c^2e + ad^4e - a^2bce^2 + b^2d^2e^2 - cde^4 + bu, \\ & b^3c^2d - cd^2e^3 - av, \\ & bcd^4 - c^4de - au, \\ & abc^4 - b^4cd - a^2b^2de + ac^2d^2e + b^2c^2e^2 - bd^2e^3 - eu, \\ & ab^4c^2e^3 - a^4b^3c^2d + a^2b^3c^4e + a^6bcde + ab^6cde + 3b^4c^3d^2e \\ & \quad - a^3b^4de^2 - 3a^2b^2c^2d^2e^2 - b^3cd^4e^2 + a^2bd^4e^3 - b^5c^5 - a^3b^2ce^4 \\ & \quad + bc^2d^3e^4 - abcde^6 - b^2cd^2u + a^2d^2eu + c^2de^2u - abcdev + e^5v - v^2, \\ & b^4cde^4 + 2a^3d^3e^4 + 4a^2b^2de^5 - ac^2d^2e^5 + 2bd^2e^7 + abcdeu \\ & \quad + ac^2d^2v - b^2c^2ev - 4a^2ce^2v - bd^2e^2v + uv, \\ & ab^3c^6 + a^5bc^3d - a^2b^4c^2de - 2ab^2c^4d^2e + a^5cd^3e \\ & \quad - a^2b^3d^3e^2 - 2abc^2d^4e^2 - a^2b^2c^3e^3 + ad^6e^3 - a^2bcd^2e^4 - cd^3e^6, \\ & \quad + b^2c^2eu - bd^2e^2u - u^2 + bc^3dv - cd^3ev - ade^3v. \end{aligned}$$

3. JACOBIAN IDEALS

We must find a way to further enlarge A , if necessary, into its integral closure B . We bring in the Jacobian ideal of A . Here we restrict ourselves to characteristic zero. As it turns out, Jacobian ideals already have large numbers of generators, and the cost of bringing in mixed Jacobians is much too high.

Let $S = k[x_1, \dots, x_n]$, k is a perfect field, and let $I = (f_1, \dots, f_m)$ be an ideal of S . We shall recall some basic properties of the module of Kähler differentials of the algebra $A = S/I$. Our basic references will be [4] and [7].

The module of k -differentials of the algebra A will be denoted by $\Omega_{A/k}$. Although this module is independent of how it is presented as a quotient of a polynomial ring, it can be conveniently described by the exact sequence of modules of differentials

$$I/I^2 \xrightarrow{d} \Omega_{S/k} \otimes_S A \rightarrow \Omega_{A/k} \rightarrow 0,$$

where d is the universal derivation $df = \sum_{i=1}^n \frac{\partial f}{\partial x_i} dx_i$.

The Jacobian ideals of I are the determinantal ideals of the matrix

$$\varphi = \left(\frac{\partial(f_1, \dots, f_p)}{\partial(x_1, \dots, x_n)} \right) \bmod I.$$

The Jacobian ideal proper is the ideal of $m \times m$ minors of φ , $m = \text{codim } I$; it shall be denoted by J . In other words, they are the Fitting ideals of the module $\Omega_{A/k}$, and therefore behave well with regard to many processes, particularly localization and completion.

We have the following criterion of Lipman [5]:

Theorem 3.1. *If J is an invertible ideal, then A is regular.*

While the usual Jacobian criterion requires $J = A$, this permits one to work with much less. It will provide the required approach.

We introduce the following notation: $J^{-1} = \text{Hom}_A(J, A)$, and $C = (J \cdot J^{-1})^{-1}$. Both J^{-1} and C are A -modules, contained in the field of fractions of A . We note that C is a ring. Indeed, if $x \in C$, the equation

$$x \cdot J \cdot J^{-1} = x \cdot J^{-1} \cdot J \subset A$$

implies that $x \cdot J^{-1} \subset J^{-1}$, and therefore x belongs to $\text{Hom}_A(J^{-1}, J^{-1})$. On the other hand, every element of this endomorphism ring is realized by multiplication by an element in the field of fractions of A , so that if $z \cdot J^{-1} \subset J^{-1}$, we have $z \cdot J^{-1} \cdot J \subset J^{-1} \cdot J \subset A$, and thus $z \in C$.

Algorithm 3.2. *Let A be an affine domain satisfying Serre's condition S_2 , and let J be its Jacobian ideal.*

- (a) *If height $J \geq 2$, then $B = A$.*
- (b) *If height $J = 1$, then C is a subring of B properly containing A .*
- (c) *Replace A by C until (a) is realized.*

Proof. If height $J \geq 2$, A satisfies R_1 and is therefore normal by Theorem 1.1.

If height $J = 1$, we claim that $A \neq C \subset B$. Indeed, the ideal $J \cdot J^{-1}$ must have depth 1, as otherwise $J_{\mathfrak{p}}$ would be invertible for each prime $\mathfrak{p}$ of height 1; by Theorem 3.1 $A_{\mathfrak{p}}$ would be regular. But an ideal I of a Noetherian domain A has depth 1 if and only if $I^{-1} \neq A$ (see [3, Exercise 2, p. 102]), and therefore C is a proper extension of A . Moreover, since $C = \text{Hom}_A(J \cdot J^{-1}, A)$, it inherits S_2 from A . $\square$

Remark 3.3. The ideal $I \cdot I^{-1}$ is the so-called *trace ideal* of I . If computation of syzygies is possible over the ring A , it can be obtained as follows. Let

$$A^m \xrightarrow{\varphi} A^n \rightarrow I \rightarrow 0$$

be a presentation of I . Let ψ be the $n \times p$ matrix, whose columns generate the relations of φ^* (the transpose of φ). Then $I \cdot I^{-1} = I_1(\psi)$. We leave the straightforward proof to the reader.

For curves, and some low-dimensional rings, this method gives a reasonable performance. However, its practice is not always successful, a primary reason being the large number of generators of Jacobian ideals. (Sometimes we wonder whether such ideals live in Noetherian rings.)

REFERENCES

1. B. Buchberger, *Gröbner bases: An algorithmic method in polynomial ideal theory*, Recent Trends in Mathematical Systems Theory (N. K. Bose, ed.), D. Reidel, Dordrecht, 1985, pp. 184–232.
2. S. Huckaba and C. Huneke, *Powers of ideals having small analytic deviation*, preprint.
3. I. Kaplansky, *Commutative rings*, University of Chicago Press, Chicago, 1974.
4. E. Kunz, *Kähler differentials*, Vieweg, Wiesbaden, 1986.
5. J. Lipman, *On the Jacobian ideal of the module of differentials*, Proc. Amer. Math. Soc. **21** (1969), 422–426.
6. A. Logar, *A computational proof of the Noether normalization lemma*, Applied Algebra, Algebraic Algorithms and Error-Correcting Codes (T. Mora, ed.), Lecture Notes in Comput. Sci., vol. 357, Springer-Verlag, Heidelberg, 1989, pp. 259–273.
7. H. Matsumura, *Commutative algebra*, Benjamin/Cummings, Reading, MA, 1980.
8. P. Samuel, *Anneaux gradués factoriels et modules réflexifs*, Bull. Soc. Math. France **92** (1964), 237–249.
9. A. Seidenberg, *Construction of the integral closure of a finite integral domain II*, Proc. Amer. Math. Soc. **52** (1975), 368–372.
10. G. Stolzenberg, *Constructive normalization of an algebraic variety*, Bull. Amer. Math. Soc. **74** (1968), 595–599.
11. W. V. Vasconcelos, *Symmetric algebras and factoriality*, Commutative Algebra (M. Hochster, C. Huneke, and J. D. Sally, eds.), Springer-Verlag, New York, 1989, pp. 467–496.

DEPARTMENT OF MATHEMATICS, RUTGERS UNIVERSITY, NEW BRUNSWICK, NEW JERSEY 08903