Integral Closure of Noetherian Rings

P. Gianni
Dipartimento di Matematica
Universitá di Pisa, Italy
gianni@dm.unipi.it

B. Trager*
IBM Research
Yorktown Heights, NY
bmt@watson.ibm.com

Abstract

After giving a proposition which reduces the problem of computing the integral closure of a general noetherian ring to the three problems:

- Compute a universal denominator d (element in the conductor).
- Compute radical of the ideal generated by d.
- Compute ideal quotients

we show that for the common case of affine domains, i.e. domains which are finitely generated over fields, of characteristic zero, we can use an effective localization in order to perform most of the computation in one dimensional rings where it can be done with linear algebra.

1 Introduction

The problem of computing the integral closure of a ring is a very basic construction in commutative algebra. It is a canonical way of removing singularities in codimension one. In the case of one dimensional rings, this gives a complete desingularization. This problem was addressed by Stolzenberg and Seidenberg in a series of papers in the case where the base ring was an affine domain, ([S], [S2], [ST]). Stolzenberg gave a construction that assumes the base ring separably generated while Seidenberg generalized it to rings which are finitely generated over fields satisfying his "condition P". Their constructions freely made use of algebraic extensions of the ground field and adjunctions of new indeterminates yielding algorithms which were not practical. The problem was revisited by Traverso, ([T]) and Vasconcelos, ([V]). They gave more effective algorithms using constructions based on Gröbner bases. On the other hand this problem had also been addressed in the context of one dimensional rings by Ford, ([F]), and Trager, ([Tr]) where the problem was reduced performing linear algebra over principal ideal domains, i.e. a sequence of hermite normal form computations. The one dimensional case was also revisited by Cohen, ([CO]), who added some computational improvements.

We first give a very general proposition which shows that one can compute the integral closure of any noetherian ring where one can solve the following three problems:

- Compute a universal denominator d (element in the conductor).
- Compute radical of the ideal generated by d.
- Compute ideal quotients

We then return to the problem of computing the integral closure of an affine domain and show that by an effective use of localization we can reduce the majority of the calculation to the efficient one dimensional algorithm presented by Ford, Trager, and Cohen.

*This research benefited from the contribution of C.N.R., M.U.R.S.T. and ESPRIT reactive LTR 21024 FRISCO

2 Notations and preliminary results

All rings are commutative, with unit and noetherian.

Definition 1 *Let S be a ring.*

- *An element $x \in S$ is a regular element iff $xy = 0 \Longrightarrow y = 0$.*
- *An ideal in S is a regular ideal if it contains at least one regular element*
- *If $T = \{x \in S \mid x \text{ is regular}\}$ then the total quotient ring of S, $Q(S)$ is defined as $Q(S) = T^{-1}S$.*

Definition 2 *Let S be a ring and $S \subset S'$ be an extension of S. An element $\alpha \in S'$ is integral over S if there exists a monic polynomial $f(x) \in S[x]$ such that $f(\alpha) = 0$.*

Definition 3 *We define the integral closure of S as the set*

$$\overline{S} = \{y \in Q(S) \mid y \text{ is integral over } S\}$$

We remark that, in general, the integral closure is not finitely generated over the original ring. In this paper we will present an algorithm to compute the integral closure of a noetherian ring S, under the assumption that it is finitely generated.

The construction we present relies on the following definitions and results:

Definition 4 *Let $I \subset S$ be a regular ideal then the idealizer of I is the ring $Idl(I) = [I :_{Q(S)} I] = \{y \in Q(S) | yI \subset I\}$.*

Proposition 1 *Let $I \subset S$ be a regular ideal then the idealizer of I is integral over S.*

Proof. Let $a_1, \dots, a_k$ be a set of generators of I. If $uI \subset I$ then $ua_i = \sum_j r_{ij} a_j$ with $r_{ij} \in S$. Let M be the matrix $r_{ij} - \delta_{ij} u$ where δ_{ij} is the Kronecker index. Then after multiplying by its adjoint we see that $det(M)$ annihilates I. Since I contains a regular element $det(M) = 0$ and this gives an integral relation for u over S.

Proposition 2 *S is integrally closed if and only if $Idl(I) = S$ for every regular ideal I.*

Proof. Let $x = \frac{y}{d} \in Q(S)$ be integral over S. Consider the integral relation for x, $x^n = \sum c_i x^i$, where $c_i \in S$. By multiplying it by d^n we get $y^n = \sum c_i d^{n-i} y^i$. Now consider the the ideal $L = (d^n, yd^{n-1}, \dots, y^{n-1}d)$. Because of the properties of the generators, we have $xL \subset L$ and hence $x \in S$. Since the other implication is trivial the proof is accomplished.

Proposition 3 *If $\overline{S}$ is finitely generated as S module there exists $t \in S$ regular element such that $t\overline{S} \subset S$. We will refer to such t as a universal denominator.*

We will discuss later how to compute such elements.

Proposition 4 *Let $d \in S$ be an element such that $[I :_{Q(S)} I] \subseteq \frac{1}{d}S$, then $Idl(I) = \frac{1}{d}[dI : I]$, where the last quotient is the usual quotient.*

Proof. $Idl(I) = [I :_{Q(S)} I] = \frac{1}{d}\{x \in S \mid \frac{x}{d} I \subseteq I\} = \frac{1}{d}\{x \in S \mid xI \subseteq dI\} = \frac{1}{d}[dI : I]$.

Proposition 5 *Let $v \in I$ be a regular element, then $[I :_{Q(S)} I] \subset \frac{1}{v}S$,*

Proof. For any $x \in [I :_{Q(S)} I]$, $xv \in I$ so $x \in \frac{1}{v}I \subset \frac{1}{v}S$.

Thus given a universal denominator or a regular element of I, the problem of computing idealizers is reduced to the usual computation of ideal quotients over S.

Proposition 6 *If S is not integrally closed and t is an universal denominator then:*

$$S \subset Idl(\sqrt{tS}) \subseteq \overline{S}$$

Proof. By proposition 1, it is enough to prove that if S is not integrally closed then S is properly contained in $Idl(\sqrt{tS})$.

Consider the non-zero quotient module $\overline{S}/S$, and let p be one of its associated primes. Thus there exists $c \in \overline{S} \setminus S$ such that $p = \{s \in S \mid sc \in S\}$. Since $tc \in S$, $t \in p$ and therefore $\sqrt{tS} \subset p$. c is integral so satisfies $c^n = \sum_i r_i c^i$. If $y \in \sqrt{tS} \subset p$, then $yc \in S$. By multiplying the integral relation for c by y^n we get $(yc)^n = y(\sum_i r_i (yc)^i y^{n-i-1})$, this implies $yc \in \sqrt{tS}$ and hence $c \in Idl(\sqrt{tS})$.

This proposition furnishes an algorithm to compute the integral closure: it is enough to be able to construct the universal denominator and compute quotients and radicals of ideals. We iterate replacing S by $Idl(\sqrt{tS})$ until reaching stability. The existence of the universal denominator along with the fact that S is noetherian guarantees that this process terminates.

This algorithm though is not very efficient. There exists an efficient algorithm for rings which are integral over principal ideal domains, ([Tr]). The aim of the rest of the paper is to be able to arrive at a more efficient algorithm doing the majority of the work with one dimensional rings. For this purpose we will restrict ourselves to consider affine domains of characteristic zero.

We will assume for the rest of this paper that the ring S is presented using Noether normalization, e.g. as done in [LO].

$$R = K[x_1, \dots, x_m]$$

$$S \cong R[s_1, \dots, s_t] \cong R[y_1, \dots, y_t]/I$$

where I is a prime ideal and K is a field characteristic zero, R is a polynomial ring over K and S is integral over R.

We recall that in this hypothesis, the integral closure can be characterized by the following criterion (Serre's criterion) ([E],[M]):

Theorem 1 *An integral domain S is integrally closed if and only if the following condition hold :*

- *$[R_1]$ For each prime p of codimension 1, S_p is a discrete valuation domain.*
- *$[S_2]$ Every ideal I of codimension two contains a regular sequence on S with two elements.*

3 Computation of a universal denominator

Given S the first problem to solve , in order to construct $\overline{S}$, is to find a universal denominator, i.e. and element d such that $d\overline{S} \subset S$. The ideal of such elements is called the conductor of $\overline{S}$ into S. The conductor is non-zero if and only if $\overline{S}$ is finitely generated over S. We will in fact require a non-zero element from the base ring R which lies in the conductor.

The standard approaches to this construction use discriminants.

- Since $Q(R) \subset Q(S)$ is a separable algebraic extension, compute a primitive element $\alpha \in S$, such that $Q(S) \cong Q(R)(\alpha)$. If f_α denotes the minimum polynomial of α, then the discriminant of f_α = Resultant(f_α, f_α') = Norm(f_α'), belongs to the conductor, ([ST]).
- If we wish to avoid primitive element constructions we can choose a basis $\alpha_1, \dots, \alpha_s$ of $Q(S)$ over $Q(R)$ such that $\alpha_i \in S$. Define the trace matrix $M = (m_{ij})$, $m_{ij} = tr(\alpha_i \alpha_j)$. Then the determinant of M is an element of the conductor which belongs to R, ([S]).

An alternative approach is based on jacobian ideals. Since the singular locus includes the non-normal locus, it is easy to see that some power of the jacobian ideal lies in the conductor. In our particular case, Theorem 2 from ([L]) implies that the relative jacobian of S over R is in fact contained in the conductor ideal.

- Compute the relative jacobian ideal of S over R, i.e. given a set of generators $\{g_1, \ldots, g_n\}$ for the defining ideal I, construct the $n \times t$ matrix $M = (m_{ij})$, $m_{ij} = (\partial g_i / \partial y_j)$. The relative jacobian ideal J is generated by the set of $t \times t$ determinants of M. If we let d_0 be one of these determinants which is non-zero, then $Norm_{Q(S)/Q(R)} d_0$ belongs to R and lies in the conductor. Alternatively we could directly compute $J \cap R$ and take a generator with a small number of prime factors.

We use the element d in order to reduce ourselves to the one dimensional case. Since R is a polynomial ring over a field, it is an abstract Unique Factorization Domain. Let $d = \prod_i d_i^{e_i}$ be a factorization of d into irreducibles so that (d_i) are prime ideals of R. Then the set $D = R \setminus \cup_i (d_i)$ is a multiplicative set and localizing by this set we have that R_D is a semilocal one dimensional domain. Since S is integral over R, S_D is integral over R_D and this implies that S_D is also a one dimensional semilocal ring.

Proposition 7 *Let $\overline{S}$ be the integral closure of S, and d be as previously defined, then:*

- (i) *S_d is integrally closed*
- (ii) $\overline{S} = \overline{S}_D \cap S_d$

Proof. (i) Since $\overline{S} \subseteq S_d$, $\overline{S}_d = S_d$ and thus S_d is integrally closed since localizations of integrally closed rings are integrally closed.

(ii) Let P be the set of height one primes in $\overline{S}$. Since $\overline{S}$ is integrally closed, $\overline{S}$ can be expressed as $\overline{S} = \bigcap_{p \in P} \overline{S}_p$, ([E], [M]). Let $P = P_1 \cup P_2 = \{p \in P \mid d \in p\} \cup \{p \in P \mid d \notin p\}$. We notice that $\overline{S}_d = S_d = \bigcap_{P_2} S_p$. Since we have also $\overline{S}_D = \bigcap_{P_1} \overline{S}_p$ the thesis holds.

In this way in order to compute $\overline{S}$ we have to compute the integral closure of a semilocal one dimensional ring S_D.

4 Integral Closure of S_D

Proposition 8 *R_D is an effective principal ideal domain.*

Proof. Let $a, b \in R_D$ and let $g = gcd(a, b)$. Considering $a_1 = \frac{a}{g}$ and $b_1 = \frac{b}{g}$, we are reduced to finding a linear combination of a_1 and b_1 which is relatively prime to d and thus containded in D. In practice since our ground field is infinite, a random linear combination would do, but we can also give a deterministic construction. In R_D there are only a finite number of maximal ideals $(d_1), \ldots, (d_t)$ and a_1 and b_1 belong to disjoint sets of (d_i)'s, let $q = \prod_Q d_r$ where $Q = \{p | p \text{ irreducible } p \not| a_1 \text{ and } p \not| b_1\}$, ($q = 1$ if Q is empty). Then $a_1 + qB_1 = s \in D$ i.e. $gcd(a_1 + qb_1, d) = 1$.

S_D is integral over R_D and torsion free so is a free module of rank $[Q(S) : Q(R)]$. Relative to a chosen basis elements of S_D can be represented as vectors of elements of R_D, and fractional ideals in S_D can have an arbitrary set of generators constructively reduced to a free basis using Hermite normal form computations for matrices over R_D. Thus we can effectively compute in S_D even though the multiplicative set D is only implicitly defined.

To compute the integral closure of S_D, we now give suitably specialized algorithms for computing $\sqrt{dS_D}$ and its idealizer. Since our ground field has characteristic zero, one can show that the problem of computing radicals can be reduced to the so-called trace radical which can be computed using linear algebra.

Proposition 9 ([Tr]) *If p is an irreducible element in R_D, (i.e. equal to a prime factor of d), then*

$$\sqrt{pS_D} = \{u \in S_D \mid p | tr(uw) \quad \forall w \in S_D\}$$

Corollary 1 *Let dd be the product of the distinct prime factors of d then*

$$\sqrt{dS_D} = \{u \in S_D \mid dd | tr(uw) \quad \forall w \in S_D\}$$

Relative to fixed basis $\alpha_1, \ldots, \alpha_n$ for S_D over R_D, we can represent elements in S_D as $\sum u_i \alpha_i$ with $r_i \in R_D$. To guarantee that $dd \mid tr(uw) \quad \forall w \in S_D$, it is enough that $dd \mid \sum_i r_i tr(\alpha_i \alpha_j)$ for $1 \leq j \leq n$. If we construct the matrix $M = (tr(\alpha_i \alpha_j))$, then we need to solve the matrix equation $Mu \in dd\, R_D^n$. As shown in [Tr] this can be done by forming the $2n \times n$ matrix with the matrix M in the first n rows and dd times the $n \times n$ identity matrix in the next n rows. Since R_D is a constructive P.I.D., we can use the Hermite row reduction algorithm to reduce the matrix to an upper triangular matrix. The columns of the inverse of this triangular matrix form a basis for the solutions to the linear system, and thus give us our free module generators for the trace radical.

The computation of the idealizer can also be reduced to a linear system. We form the n multiplication matrices associated with the basis for our ideal, then we perform Hermite row reduction on the $n^2 \times n$ matrix composed of a vertical stacking of these multiplication matrices. After again performing Hermite row reduction, we get a triangular matrix whose inverse yield a basis for the idealizer.

As in the first section we continue replacing our ring S_D with the idealizer of the radical of the ideal (dS_D) until the ring doesn't change. Since we are always working with free R_D modules it is easy to check when the process stabilizes. At the end of the process we have $\overline{S}_D$ presented as a free R_D module. We can assume the generators are of the form s/d where $s \in S$, since any factor of the denominator which is relatively prime to d is a unit in S_D and thus can be discarded.

Remark 1 *The algorithm described does not depend on the ability to factor d. However if we know the factorization of d, we are able to improve the performance of the Hermite reduction process.*

Let $d = \prod_i^k d_i^{e_i}$, and let $D_i = R \setminus (d_i)$. We can consider $R_D = R_{D_1} \cap \ldots \cap R_{D_k}$. In this case R_{D_i} is a discrete valuation ring. Thus given any two elements of R_{D_i}, one must divide the other. The algorithm of Hermite row reduction for matrices over discrete valuation rings becomes essentially equivalent to simple gaussian elimination. There is always one element in each column which divides all the others and thus can be used to zero out the column.

To use this improved version of Hermite row reduction we let $\overline{S}_D = \overline{S}_{D_1} \cap \ldots \cap \overline{S}_{D_t}$, so we have now to compute the intersection . We can assume $\overline{S}_{D_i} \cong R_{D_i}[\frac{a_{i1}}{d_i^{e_i}}, \ldots, \frac{a_{i,n}}{d_i^{e_i}}]$ and then $\overline{S}_D \cong R_D[\frac{a_{1,1}}{d_1^{e_1}}, \ldots, \frac{a_{t,n}}{d_k^{e_k}}]$ is simply the ring obtained by adjoining all these generators since each denominator d_j is a unit in all the other rings R_{D_i}. At the end we should reduce our set of generators to a free basis in order to minimize the number of module generators. This can be done by another application of hermitian row reduction over R_D. This process finds $s_1, \ldots, s_n \in S$ such that $\overline{S}_D \cong R_D[\frac{s_1}{d}, \ldots, \frac{s_n}{d}]$. By construction each $\frac{s_i}{d}$ is integral over R_D, but a stronger statement is true:

Proposition 10 *With notation as above, each $\frac{s_i}{d}$ is integral over S.*

Proof. We have seen that $\overline{S} = \overline{S}_D \bigcap S_d$. Thus since each $\frac{s_i}{d}$ is contained in both $\overline{S}_D$ and S_d, it is contained in $\overline{S}$.

For simplicity of notation we put :

$$T = S[\frac{s_1}{d}, \ldots, \frac{s_n}{d}]$$

Remark 2 *T nonsingular in codimension one and satisfies Serre's conditon R_1.*

5 Construction of $\overline{S}$

In order to complete the algorithm and construct $\overline{S}$ we have to compute $\overline{S}_D \cap S_d = T_D \cap T_d$. Three algorithms are possible. The first is due to Vasconcelos [V] who shows that if T satisfies Serre's condition R_1 then $\mathrm{Hom}_R(\mathrm{Hom}_R(T, R), R)$ is integrally closed since it also satisfies Serre's condition S_2. In addition he gives an algorithm for computing this double dual.

Seidenberg and Stolzenberg require computing the isolated components of a primary decomposition for the ideal dT and then dividing the generators by d.

We propose a third way which is in fact a more efficient way to do the computation proposed by Seidenberg and Stolzenberg. In the notation introduced at the end of the previous section we need to compute $T_D \cap T_d$, since $T_d = S_d$. We will do this using the following observation:

Proposition 11 $T_D \cap T_d = \frac{1}{d}(dT_D \cap T)$.

Proof. As we already remarked, the integral closure of T is contained in $\frac{1}{d}T$, so $T_D \cap T_d = T_D \cap \frac{1}{d}T = \frac{1}{d}(dT_D \cap T)$.

$(dT_D \cap T)$ is exactly the extension of the ideal d to T_D and followed by its contraction to T. This can be easily done via Gröbner bases, but first we need a presentation of T as a polynomial ring modulo an ideal, i.e. we need to find the ideal of relations among the generators of T. We already have S presented as

$$S = R[y_1, \ldots, y_t]/I$$

and we have T presented as

$$T = S[\frac{s_1}{d}, \ldots, \frac{s_n}{d}]$$

where $s_i \in S$, $d \in R$. To get the ideal of relations for T, we can select new variables $z_1, \ldots, z_n$ and one addition variable u to represent the inverse of d. We form the ideal

$$I + (ud - 1, z_1 - s_1 u, \ldots, z_n - s_n u)$$

in

$$K[x_1, \ldots, x_m, y_1, \ldots, y_t, z_1, \ldots, z_n, u].$$

Then we can compute a groebner basis with an elimination ordering for u, i.e. we choose an ordering which is some refinement of the ordering by degree in u. The subideal generated by the groebner basis generators which are free of u gives a presentation of T as a polynomial ring modulo an ideal.

To compute $(dT_D \cap T)$, we use the following straightforward generalization of Proposition 3.7 in [GTZ]. We use $R[\mathbf{z}]$ to denote a polynomial ring in several variables over R.

Proposition 12 *Let $(di) \subset R$ be a collection of principal prime ideals. Let $D = R \setminus \cup_i(d_i)$ a multiplicative set. For any given ideal $I \subset R[\mathbf{z}]$, we can find a $s \in D$ such that*

$$IR_D[\mathbf{z}] \cap R[\mathbf{z}] = IR_s[\mathbf{z}] \cap R[\mathbf{z}].$$

Essentially one computes a relative Gröbner basis, computes the product of the leading coefficients of the generators with all factors of d removed. If we let s be this element, then $(dT_D \cap T) = (dT_s \cap T)$. The latter can be computed by adding a generator of the form $us - 1$ where u is a new variable and then contracting back to the original ring.

6 Algorithm summary

- Compute a noether normal presentation of the ring $R = K[x_1, \ldots, x_m]$, $S = R[y_1, \ldots, y_t]/I$ where R is a polynomial ring over a field and S is integral over R.
- Compute a universal denominator $d \in R$ such that $d\overline{S} \subseteq S$ by one of the algorithms in section 3.
- Let D be the set of polynomials in R which are relatively prime to d. R_D is an effective PID and we compute a basis for S_D over R_D. Note that we only use D implicitly in the sense that any denominator relatively prime to d is automatically a unit.

  Remark 3 *If we use the factorization of d to improve the performance of the hermite normal form construction, then we need to add an outer iteration over the factors of d here replacing D with D_i the set of polynomials in R which are not divisible by d_i.*

- perform the next 2 steps until the ring stabilizes:

  compute the ideal $\sqrt{dS_D}$ using the trace radical construction in section 4.

  compute an R_D basis for the idealizer of this ideal, discarding factors of the denominators which are relatively prime to d. If this ring properly contains S_D, then consider this as the new S_D and repeat.

- Let $T = S[s_1/d, \ldots, s_n/d]$ be the ring we have computed so far. This ring is non-singular in codimension one. To complete the construction we find a presentation of T as a polynomial ring modulo an ideal. Then we compute $dT_D \cap T$. The resulting ideal generators divided by d generate the integral closure of S.

Remark 4 *One of the referees made us aware of a paper by Beukers and Couveignes [BC], which takes an essentially similar approach to computing normalizations. They also* *use localizations to reduce the problem to several integral closure computations in one-dimensional rings. They compute the final normalization by directly computing the intersection of this collection of locally integrally closed rings, using the fact that they are all free R-modules.*

References

[BC] Beukers, F., Couveignes, J-M., *Computing normalizations of coverings of the sphere*, manuscript, 1996.

[CO] Cohen, H., *A Course in Computational Algebraic Number Theory*, Springer–Verlag, 1993, pag. 297–306.

[E] Eisenbud, D., *Commutative Algebra with a view toward Algebraic Geometry*, Springer–Verlag, 1995.

[F] Ford, D.J., *On the Computation of the Maximal Order in a Dedekind Domain*, Ph.D. Thesis, Ohio State University, Dept. of Mathematics,(1978).

[GTZ] Gianni, P., Trager, B., Zacharias, G., *Gröbner Bases and Primary Decomposition of Polynomial Ideals*, J. Symbolic Computation **6** (1988), 149–167.

[L] Lipman, J., Sathaye, A., *Jacobian Ideals and a theorem of Briançon–Skoda*, Michigan Math.J., **28** (1981), 199–222.

[LO] Logar, A., *A computational proof of the Noether normalization lemma*, Applied Algebra, Algebraic Algorithms and Error-correcting Codes (T. Mora, ed.), LNCS **357** Springer-Verlag, (1989), 259–173.

[M] Matsumura, H., *Commutative algebra*, Benjamin /Cummings, Reading, MA, 1980.

[S] Seidenberg, A., *Construction of the integral closure of a finite integral domain*, Rend.Sem.Mat.Fis. Milano **40** (1970) 101–120.

[S2] Seidenberg, A., *Construction of the integral closure of a finite integral domain II*, Proc.Amer.Math.Soc **52** (1975), 368–372.

[ST] Stolzenberg, G., *Constructive normalization of an algebraic variety*, Bull.Amer.Math.Soc **74** (1968), 595–599.

[Tr] Trager, B.M., *Integration of Algebraic Functions*, Ph.D. Thesis, M.I.T., (1984)

[T] Traverso, C., *A study on algebraic algorithms: the normalization*, in "Algebraic varieties of small dimension",Rend. Sem. Mat. Torino, 1986

[V] Vasconcelos, W.V., *Computing the integral closure of an affine domain*, Proc.Amer.Math.Soc Vol.113, N0.3, 1991 , 633–638.