

APPENDIX: ALGORITHMS FOR COMPUTING SATURATIONS OF IDEALS IN FINITELY GENERATED COMMUTATIVE RINGS

MATTHIAS ASCHENBRENNER

Consider the following basic task:

Given a finitely generated commutative \mathbb{Z} -algebra A (specified by generators and relations) and a finite list of generators for an ideal I of A , compute a finite list of generators for the inverse image of the ideal $I \otimes \mathbb{Q}$ under the natural morphism $A \rightarrow A \otimes \mathbb{Q}$.

The existence of such an algorithm is well-known, and the purpose of this appendix is to briefly describe two different procedures for the task at hand, and to make some additional related remarks. Before this, we observe that representing the \mathbb{Z} -algebra A as a quotient $A = \mathbb{Z}[X]/J$ where J is an ideal of the polynomial ring $\mathbb{Z}[X] = \mathbb{Z}[X_1, \dots, X_N]$ (where N and generators for J are part of the input data) one sees that it suffices to consider the case where A is a polynomial ring over \mathbb{Z} . In this case, the pullback ideal in question may also simply be described as the *saturation* $I\mathbb{Q}[X] \cap \mathbb{Z}[X]$ of I with respect to the multiplicative subset $\mathbb{Z} \setminus \{0\}$ of $\mathbb{Z}[X]$. That is, we need to give an algorithm which does the following:

Given $N \in \mathbb{N}$ and generators f_1, \dots, f_n for an ideal I of $\mathbb{Z}[X] = \mathbb{Z}[X_1, \dots, X_N]$, compute a finite list of generators for the ideal $I\mathbb{Q}[X] \cap \mathbb{Z}[X]$ of $\mathbb{Z}[X]$.

In fact, both algorithms below compute a nonzero integer δ such that $(I : \delta) = I\mathbb{Q}[X] \cap \mathbb{Z}[X]$ as well as a finite list of generators for the ideal $(I : \delta)$.

Algorithm 1. This algorithm, from [1], uses Gröbner bases in polynomial rings over \mathbb{Z} . For basic facts about Gröbner bases in this context, see [1]. One may proceed as follows:

- (1) Compute a Gröbner basis G of I with respect to an arbitrary monomial ordering of the monomials in X . Let s be the least common multiple of the leading coefficients of the elements of G , with $s = 1$ if $I = \{0\}$ (and hence $G = \emptyset$). Then we have

$$I\mathbb{Q}[X] \cap \mathbb{Z}[X] = I\mathbb{Z}[\frac{1}{s}][X] \cap \mathbb{Z}[X]$$

by [1, Proposition 4.4.4]. (The integer s also has the property that $(\mathbb{Z}[X]/I)[\frac{1}{s}]$ is a free $\mathbb{Z}[\frac{1}{s}]$ -module [8, Theorem 2.1]; this is a particular instance of Grothendieck's "generic freeness lemma".)

- (2) Next, let Y be a new indeterminate, distinct from X_1, \dots, X_N . Then

$$I\mathbb{Z}[\frac{1}{s}][X] \cap \mathbb{Z}[X] = (I, Ys - 1) \cap \mathbb{Z}[X]$$

by [1, Proposition 4.4.1]. Fix an arbitrary monomial ordering $<_X$ of the monomials $X^\alpha = X_1^{\alpha_1} \cdots X_N^{\alpha_N}$ ($\alpha = (\alpha_1, \dots, \alpha_N) \in \mathbb{N}^N$) in X . Compute

The author was partially supported by National Science Foundation grant DMS-0556197.

a Gröbner basis G_s for the ideal $(I, Ys - 1)$ of $\mathbb{Z}[X, Y]$ with respect to the monomial ordering given by

$$X^\alpha Y^a < X^\beta Y^b \iff a < b, \text{ or } a = b \text{ and } X^\alpha <_X X^\beta.$$

Then the finite set $G_s \cap \mathbb{Z}[X]$ is a Gröbner basis for $(I, Ys - 1) \cap \mathbb{Z}[X] = IQ[X] \cap \mathbb{Z}[X]$, by [1, Theorem 4.3.6].

As a bonus, if we choose a nonzero integer δ such that $\delta g \in I$ for all $g \in G_s \cap \mathbb{Z}[X]$, then $IQ[X] \cap \mathbb{Z}[X] = (I : \delta)$. (We may take δ to be a power of s .)

Algorithm 2. This algorithm, implicit in [2], uses the natural division of the problem posed into two subproblems:

- (P1) Compute an integer δ such that $(I : \delta) = IQ[X] \cap \mathbb{Z}[X]$.
- (P2) Compute, given $g \in \mathbb{Z}[X]$, a finite list of generators for the ideal $(I : g)$.

First, as a byproduct of Hermann's classical algorithm [7] for deciding ideal membership in polynomial rings over fields, one obtains a procedure for computing a polynomial $P(c) \in \mathbb{Z}[C]$ in the coefficient tuple c of f_1, \dots, f_n such that $\delta = P(c)$ has the property in (P1); see [2, Section 3]. Subproblem (P2) is approached by specifying an algorithm which accomplishes the following:

- (P2') Given $g_1, \dots, g_m \in \mathbb{Z}[X]$, compute a finite generating set for the $\mathbb{Z}[X]$ -submodule of $\mathbb{Z}[X]^m$ consisting of the solutions to the homogeneous linear equation $y_1 g_1 + \dots + y_m g_m = 0$.

To see how this solves (P2), given $g \in \mathbb{Z}[X]$, consider the homogeneous linear equation

$$y_1 f_1 + \dots + y_n f_n = y_{n+1} g.$$

Then the projection onto the $(n+1)$ st components of every generating set for the $\mathbb{Z}[X]$ -module of solutions to this equation in $\mathbb{Z}[X]^{n+1}$ is a generating set for the ideal $(I : g)$. An algorithm for (P2'), based on an adaptation of Hermann's algorithm from $\mathbb{Q}[X]$ to $\mathbb{Z}[X]$, may be found in [2, Section 4]. (Of course, (P2') may also be solved using Gröbner bases: it suffices to note that given a Gröbner basis G for the ideal (g_1, \dots, g_m) of $\mathbb{Z}[X]$ with respect to an arbitrary monomial ordering, the representations of the S -polynomials of G in normal form with respect to G give rise to a finite generating set for the syzygies of g_1, \dots, g_m ; see [1, Theorem 4.3.16].)

Remarks. Algorithm 1 seems better suited for practical computations. However, unlike in the case of fields, the precise worst-case behavior of the analogue of Buchberger's algorithm for computing Gröbner bases over $\mathbb{Z}[X]$ is as of yet still unclear. (For very weak bounds see [6], and for further discussion the forthcoming [3].) Algorithm 2 has the advantage of coming with explicit (doubly-exponential) complexity bounds: for example, suppose $d \in \mathbb{N}$ is an upper bound on the (total) degree of f_i for $i = 1, \dots, n$; then $IQ[X] \cap \mathbb{Z}[X] = (g_1, \dots, g_m)$ where $\deg(g_j) \leq (2d)^{2^{N \log(N+1)}}$ for $j = 1, \dots, m$, cf. [2, Theorem B]. (Note that this bound only depends on the bound d on the degrees and not on the particular coefficients of the f_i .)

In connection with (P1), we remark that the *smallest* positive integer δ such that $(I : \delta) = IQ[X] \cap \mathbb{Z}[X]$ agrees with the exponent of the torsion subgroup of the additive group of $\mathbb{Z}[X]/I$. (The torsion subgroup of the additive group of a Noetherian ring always has finite exponent.) The algorithms indicated above, together with a procedure for deciding equality of ideals in $\mathbb{Z}[X]$ (found in [1, 2]),

give rise to a procedure for computing this exponent in an obvious way; another algorithm was given by Clivio [5] (based on earlier work of Ayoub [4]).

REFERENCES

1. Adams, W., and Loustanaunau, P., *An Introduction to Gröbner Bases*, Graduate Studies in Mathematics, vol. 3, American Mathematical Society, Providence, RI, 1994.
2. Aschenbrenner, M., *Ideal membership in polynomial rings over the integers*, J. Amer. Math. Soc. **17** (2004), no. 2, 407–441 (electronic).
3. ———, *Uniform degree bounds for Gröbner bases*, in preparation.
4. Ayoub, C., *On constructing bases for ideals in polynomial rings over the integers*, J. Number Theory **17** (1983), no. 2, 204–225.
5. Clivio, A., *Algorithmic aspects of $\mathbf{Z}[x_1, \dots, x_n]$ with applications to tiling problems*, Z. Math. Logik Grundlag. Math. **36** (1990), no. 6, 493–515.
6. Gallo, G., and Mishra, B., *A solution to Kronecker's problem*, Appl. Algebra in Engrg. Comm. Comput. **5** (1994), no. 6, 343–370.
7. Hermann, G., *Die Frage der endlich vielen Schritte in der Theorie der Polynomideale*, Math. Ann. **95** (1926), 736–788.
8. Vasconcelos, W. V., *Flatness testing and torsionfree morphisms*, J. Pure Appl. Algebra **122** (1997), no. 3, 313–321.

UNIVERSITY OF CALIFORNIA, LOS ANGELES, CA 90095, U.S.A.
E-mail address: matthias@math.ucla.edu