Advances in Mathematics of Communications
Volume 3, No. 1, 2009, 1–11
doi:10.3934/amc.2009.3.1

A WEIGHTED MODULE VIEW OF INTEGRAL CLOSURES OF AFFINE DOMAINS OF TYPE I

Douglas A. Leonard

Department of Mathematics and Statistics
Auburn University
Auburn, AL 36849-5307, USA

(Communicated by Tom Hoeholdt)

Abstract. A type I presentation $S = R/J$ of an affine (order) domain has a weight function injective on the monomials in the footprint $\Delta(J)$. This can be extended naturally to a presentation, $\overline{R}/\overline{J}$, of the integral closure $ic(S)$. This presentation over $P := F[x_n, \ldots, x_1]$ as an affine P-algebra relative to a corresponding grevlex-over-weight monomial ordering is shown to have a minimal, reduced Gröbner basis (for the ideal of relations $\overline{J}$) consisiting only of P-quadratic relations defining the multiplication of the P-module generators and possibly some P-linear relations if those generators are not independent over P. There then may be better choices for P to minimize the number of P-module generators needed. The intended coding theory application is to the description of one-point AG codes, not only from curves (with $P = F[x_1]$) but also from higher-dimensional varieties.

1. Introduction

To properly describe a curve $\mathcal{X}$ to be used to define a one-point AG code, it is necessary to put it in special position relative to that one special point P_∞, with variables corresponding to rational homogeneous functions modulo $\mathcal{X}$, with no poles except possibly at P_∞. Then the generator and/or parity-check functions come from the vector space $L(mP_\infty)$ of said functions with pole order at most m, contained in the ring $L(\infty P_\infty)$ of all such functions. The footprint $\Delta(J)$ of the affine domain $S = R/J$ of type I defining the curve does not usually define all of $L(\infty P_\infty)$, but the footprint of its integral closure (in its field of fractions) does. So there is a compelling reason to study integral closures in the context of AG coding.

If one views the pole orders as corresponding to the (negatives of the) trailing exponents in the Laurent series expansions in terms of a local parameter t_∞ at P_∞, then the obvious generalization to n-dimensional surfaces is in terms of the trailing exponent vector $\underline{\alpha} \in \mathbf{N}_0^n$ in an expansion involving n independent local parameters.

The view in this paper is to start with a polynomial ring $P := \mathbf{F}[x_n, \ldots, x_1]$ with a monomial ordering (which can be viewed as a weight function wt_P injective on the set of monomials), deal with type I integral extensions $S := P[y]/\langle f(y)\rangle$ so that wt_P can be naturally extended to a weight function wt_S, which naturally induces a weight function on the integral closure $ic(S)$ of S. While similar to the general theory of order domains in [5], there are two important differences here. The view there is that one starts with S, may or may not care about P, (since the weight

2000 *Mathematics Subject Classification:* Primary: 11T71, 13B22, 94B27.
Key words and phrases: AG codes, integral closure, normalization, order domains.

function on S may not be a monomial ordering on every choice of P), and the Δ-set is viewed as an infintie-dimensional vector space over $\mathbf{F}$, not in terms of a finite P-module generating set.

The presentation of $ic(S) = \overline{R}/\overline{J}$ desired here is relative to this P-module generating set $y_0 := 1, y_1, \ldots y_{s-1}$, so that $\overline{J}$ has a minimal, reduced Gröbner basis with elements of the form

$$y_i y_j - \sum_k c_{i,j,k} y_k,\ c_{i,j,k} \in P$$

defining the algebra multiplication, and possibly some elements of the form

$$a_{j,i} y_i - a_{i,j} y_j - \sum_{k \neq i,j} b_{i,j,k} y_k,\ a_{j,i}, a_{i,j}, b_{i,j,k} \in P$$

if the P-module generators are not independent over P. (This means that, in general, s is not necessarily the same as the degree of the integral extension.)

This is followed by a possible minimization of such a presentation by making a more enlightened choice for P. After all, when $n = 1$, it is known ([10]) that there is an $\mathbf{F}[f_\rho]$-module basis, ρ being the smallest positive pole order, with one basis element of smallest positive pole order congruent to $i \ mod\ \rho$ for each i. This leaves open the question of what the minimum number of P-module generators is when $n > 1$, not only because it may not be easy to see whether an example is minimized, but also because there is no longer any definite relation between the degree of the extension and that number even when the problem is given as a minimized integral extension.

But what is missing from the *generic* presentations of integral closures given by most current implementations is a nice description of the monomials in the footprint. Here the footprint necessarily has monomials all of the form $y_i \underline{x}^{\underline{\alpha}}$ for y_i one of the P-module generators, and $\underline{x}^{\underline{\alpha}}$ a monomial of P, whether or not a complete minimization is found.

Section 2 will be primarily concerned with notation and the implications of said notation. Section 3 contains as small an example as known by the author in which the P-module generators are not independent. Section 4 gives the theorem summarizing the structure of S and $ic(S)$. Section 5 gives some discussion of the limitations of various implementations. Section 6 contains examples of minimization and a theorem guaranteeing the the structure is not compromised by minimization. Examples here and on the website were done using an implementation of the author's qth-power algorithm [9], [11], written in MAGMA [12] and available on the `http://www.dms.auburn.edu/~leonada` website. [There are also examples on the website of input and output of current implementations, which may be useful in understanding the following commentary in this section, as well as other points made later on.]

Before proceeding, we should note that this approach is definitely not taken by anyone else. Weight functions, fundamental to the study of order domains [5], [8], are virtually unused or actively ignored in the study of integral closures. The result is usually a generic form of integral closure presentation, with a default monomial ordering, having little to do with the original monomial order of the ring. It is perhaps more surprising, however, that there is never any coherent attempt to give a readable presentation for the integral closure, such as the one suggested here, which is, after all, along the lines of structure constant algebras defined by s^3 structure constants (from P). (It is even more surprising given that current algorithms are based on producing sequences of rings each defined in terms of quadratic and linear relations over the previous ring.) But then again, the prevailing viewpoint, at least for $n > 1$, is not relative to P, and sometimes not relative to a presentation at all, but merely relative to a set of fractions generating $ic(S)$ over S. At the very least, one might have hoped for a presentation consisting of:

- a ring $\overline{R} := \mathbf{F}[y_{s-1}, \dots, y_1; x_n, \dots, x_1]$ as an extension of $P := \mathbf{F}[x_n, \dots, x_1]$;
- an ideal of relations $\overline{J}$, so that $ic(S) = \overline{R}/\overline{J}$;
- an inclusion map $\phi : S \to ic(S)$ describing what the variables in S look like in $ic(S)$;
- an element c of the conductor, and an inclusion map $\psi : ic(S) \to \frac{1}{c} ic(S)$ describing what the new variables look like in terms of the field of fractions of S.

even if one doesn't ask for $c \in P$, $(y_0 := 1, y_1, \dots y_{s-1})$ to be P-module generators, $\overline{J}$ to have the particularly nice form above, or a weight function injective on the monomials of the footprint $\Delta(\overline{J})$.

2. Notation

Let $\mathbf{F}$ be a *field* (which here and in the intended applications is either a finite field or the algebraic closure of a finite field) and $P := \mathbf{F}[x_n, \dots, x_1]$ a *multivariate polynomial ring* over $\mathbf{F}$ in n *independent* variables.

Consider the following adaptation of more standard definitions of *weight functions* in *order domains* [5], written in terms of the ring R and ideal J instead of implicitly in terms of the quotient ring $S = R/J$.

Definition 2.1. Let $S = R/J$ be an affine domain. A function

$$wt_S := R \to \mathbf{N}_0^n \cup \{-\infty\}$$

(with $-\infty \prec \underline{\alpha}$ for all $\underline{\alpha} \in \mathbf{N}_0^n$) is a *weight function* on S iff:

1. $wt_S(f) = -\infty$ iff $f \in J$;
2. $wt_S(f) = 0$ iff $f = c + J,\ c \in \mathbf{F}\backslash\{0\}$;
3. $wt_S(fg) = wt_S(f) + wt_S(g)$ for all $f, g \notin J$;
4. $wt_S(\alpha f + \beta g) \leq\ max\{wt_S(f), wt_S(g)\}$ for all $\alpha, \beta \in \mathbf{F}$;
5. if $wt_S(f) = wt_S(g) \succ \underline{0}$, then $wt_S(f - \lambda g) \prec wt_S(g)$ for an unique $\lambda \in \mathbf{F}$.

Let A_P be a non-singular $n \times n$ matrix over $\mathbf{N}_0$ defining the (*global*) *monomial ordering* on P (with the default here being the *grevlex* ordering, $x_n \succ \cdots \succ x_1$), and hence a weight function given by $wt_P(\underline{x}^{\underline{\alpha}}) := A_P \underline{\alpha}^t$, with distinct monomials obviously having distinct weights (since A_P defines a total order on monomials, or equivalently since it is non-singular).

Let $f(T) := \sum_{i=0}^{d} f_i T^i \in P[T]$ be a *monic*, *absolutely irreducible* polynomial of degree d. Use it to define an *integral extension*, the *affine domain* $S := P[y]/J$ for $J := \langle f(y) \rangle$. To extend wt_P to a weight function wt_S on S, define $wt_S(\underline{x}^{\underline{\alpha}}) := d \cdot wt_P((\underline{x}^{\underline{\alpha}})$, and $wt_S(y) := max\{\frac{wt_S(f_i)}{d-i} : 0 \leq i < d\}$. If that max is taken on at only one value of i, that value is $i = 0$, $LM(f_0) := \underline{x}^{\underline{\alpha}}$, and

$$gcd\{d,\ gcd\{\alpha_i : 0 \leq i < d\}\} = 1,$$

then S is said to be *type I*. (This terminology probably dates back to [4], but with a more rudimentary definition. The current definiton can be found at least as early as [11].)

The standard *grevlex* order is defined by the $s\times s$ $(0,1)$ matrix $G^{(s)}$, with $G^{(s)}_{i,j} := 1$ iff $1 \leq i + j \leq s + 1$. Regarless of monomial order, $NF(g, I)$ will always mean the *normal form* of g, meaning the remainder after division by elements of I, $LC(g)$, $LM(g)$, and $LT(g) = LC(g)LM(g)$, the *leading coefficient*, *leading monomial*, and *leading term* of g (relative to the given ordering). $SP(f, g)$ will denote the *spolynomial* of f and g.

For W_{ind} a non-singular $n \times n$ matrix over $\mathbf{N}_0$, and W_{dep} some $n \times s$ matrix over $\mathbf{N}_0$, we introduce *grevlex-over-weight* order defined by the matrix

$$M := \begin{pmatrix} G^{(s)} & 0 \\ W_{dep} & W_{ind} \end{pmatrix};$$

and *weight-over-grevlex* orders defined by the matrix

$$M := \begin{pmatrix} W_{dep} & W_{ind} \\ G^{(s)} & 0 \end{pmatrix},$$

with the former emphasizing the P-module structure, the latter the weights. In either case, define the *weight* of the monomial $\underline{y}^{\underline{\gamma}}, \underline{x}^{\underline{\alpha}}$ as $W_{dep}\underline{\gamma}^t + W_{ind}\underline{\alpha}^t$. The monomial ordering on the extension S of P above, is given by $A_S := \begin{pmatrix} 1 & \underline{0} \\ wt_S(y)^t & dA_P \end{pmatrix}$.

The following short lemma is included here only because it explains the use of the gcd condition in the definition of type I above.

Lemma 2.2 (**Folklore**). *The (standard) monomials in the footprint $\Delta(J)$ of a type I affine domain have distinct weights.*

Proof. Suppose, for some $0 \leq j < i < d$,

$$wt_S(y^i \underline{x}^{\underline{\alpha}}) = wt_S(y^j \underline{x}^{\underline{\beta}})$$

for these two distinct monomials in the footprint $\Delta(J)$. Then

$$(i - j)wt_S(y) = wt_S(\underline{x}^{\underline{\beta}}) - wt_S(\underline{x}^{\underline{\alpha}}) = d(wt_P(\underline{x}^{\underline{\beta}}) - wt_P(\underline{x}^{\underline{\alpha}})).$$

But because of the gcd condition, this forces either $d|i - j$ or $\underline{\alpha} = \underline{\beta}$. ☐

Example 1. The *Klein quartic* is most often given in terms of the affine model (with 2 points at infinity) $\mathbf{F}_2[y, x]/\langle y^3 + x^3y + x\rangle$, probably because this has nice symmetry in its homogeneuos form. It is already integrally closed. If one were dealing with 2-point codes here, it would be possible to write this as

$$ic(S) = S = \mathbf{F}_2[y_2, y_1; x_1]/J,\ J := \langle y_1^2 - y_2,\ y_2y_1 - (y_1x_1^3 + x_1),\ y_2^2 - (y_2x_1^3 + y_1x_1)\rangle;$$

While one can try to define a weight function with $wt(y) := 3$, and $wt(x) := 2$, both $y^2 = y_2$ and $x^3 = x_2^3$ are standard monomials with the same weight, 6. This happened because $wt(y^3) = wt(yx^3) > wt(x)$ instead of $wt(y^3) = wt(x) > wt(yx^3)$.

The one-point description: $\mathbf{F}_2[f_5; f_3]/\langle f_5^3 + f_3^5 + f_5f_3\rangle$, gotten by using $f_5 := yx$ and $f_3 := y$, is not integrally closed since $f_7 := f_5^2/f_3$ is integral over $\mathbf{F}_2[f_3]$. The integral closure $\mathbf{F}_2[f_7, f_5; f_3]/\langle f_5^2 + f_7f_3,\ f_7f_5 + f_5 + f_3^4,\ f_7^2 + f_7 + f_5f_3^3\rangle$, has the obvious weight function (implied by the subscripts used), with standard monomials of the forms f_3^i, $f_5f_3^i$, and $f_7f_3^i$, $i \geq 0$, having all possible distinct weights different (those different from $1, 2, 4$). And the original 2-point presentation can be recovered from this readily by resubstitution.

Example 2. The presentation $S := \mathbf{F}_2[y,x]/\langle x^{10}+y^4+y\rangle$, is clearly an integral extension of $P := \mathbf{F}_2[x]$, and is already integrally closed. It has a weight function defined by $wt_S(y) := 10$ and $wt_S(x) := 4$, so it is an order domain, but not with semi-group $\Gamma = \langle 4, 10\rangle$. Similarly it is *not* a type I presentation because $gcd(4,10) = 2 \neq 1$, meaning that y_{10}^2 and x_4^5 are both standard monomials with the same weight, 20. But $z := y_{10}^2 + x_4^5$ satisfies $z^2 = y_{10}$; so $weight(z) = 5$.

This gives a type I presentation $\mathbf{F}_2[z_5; x_4]/\langle z_5^4 + z_5 + x_4^5\rangle$. Depending on the monomial ordering chosen, this can have footprint either $\{x^i z^j : 0 \leq i < 5, 0 \leq j\}$ or $\{z^i x^j : 0 \leq i < 4, 0 \leq j\}$, both infinite, but the latter having fewer (4 rather than 5) P-module generators. So the presentation suggested here is relative to the $\mathbf{F}_2[x_4]$-module basis $y_0 := 1$, $y_1 := z_5$, $y_2 := z_{10} := z_5^2$, and $y_3 := z_{15} := z_5^3$, with the ideal

$$\begin{aligned}&\langle z_5^2 - z_{10},\ z_{10}z_5 - z_{15},\ z_{10}^2 - (z_5 + x_4^5),\\ &\ z_{15}z_5 - (z_5 + x_4^5),\ z_{15}z_{10} - (z_{10} + z_5 x_4^5),\ z_{15}^2 - (z_{15} + z_{10}x_4^5)\rangle.\end{aligned}$$

(Note that the common module orderings generally referred to as TOP (Term-Over-Position) and POT (Position-Over-Term), at least in the standard text [1] in the section on Gröbner bases for modules, assume no interplay between module positions and terms in those positions, whereas we have a monomial ordering on a ring viewed as a module. There are many places where block orders are implemented and used, but not so for orderings of the type suggested here, which can only be used in various computational algebra packages by defining the whole matrix.)

3. Example

The following example, which could be defined as a single type I extension directly, will be given as two such instead. It is the smallest example known to the author in which the P-module generators are not independent. (Such an example, of course, cannot occur when $n = 1$, but it is conceivable that there is an example of degree less than the $d = 9$ here.)

Start with the polynomial ring $P := \mathbf{F}_2[x_2, x_1]$ (with the *grevlex* order). The monic polynomial $f(T) := T^3 + x_2x_1T + \left(x_2^3x_1^2 + x_2^2x_1^3\right)$ can be used to define a *type I integral extension* $S_1 := P[y]/\langle f(y)\rangle$ with grevlex-over-weight monomial order defined by $\begin{pmatrix} 1 & 0 & 0\\ 5 & 3 & 3\\ 3 & 3 & 0\end{pmatrix}$.

As a P-module, $S_1 = \mathbf{F}_2[y,x]/\langle y^3 + yx_2x_1 + x_2^3x_1^2 + x_2^2x_1^3\rangle$ has standard P-module basis $(1, y, y^2)$. S_1 happens *not* to be *integrally closed*, since $\left(\frac{y^2}{x_2x_1}\right)^3 + \left(\frac{y^2}{x_2x_1}\right) + \left(x_2^3x_1 + x_2x_1^3\right) = 0$. The integral closure $ic(S_1)$ is, in fact a subset of $\delta^{-1}S_1$ for $\delta := x_2x_1$, which also has a P-module basis $(\delta^{-1}y^0, \delta^{-1}y^1, \delta^{-1}y^2)$. So the obvious hope is that $ic(S_1)$ will have a P-module basis of the form $(y_0 := 1, y_1, y_2) = (\delta^{-1}f_{0,0}(y), \delta^{-1}f_{1,0}(y), \delta^{1-}f_{2,0}(y))$ with $deg(f_{i,0}(y)) = i$. $ic(S_1)$ can be written in the form $ic(S_1) = \mathbf{F}_2[y_2, y_1; x_2, x_1]/\overline{J_1}$ for $y_1 := y$, $y_2 := y^2/(x_2x_1)$, and $\overline{J}_1$ the ideal of induced realtions describing the polynomial multiplication ignored when viewing $ic(S_1)$ merely as a P-module, in that

$$\overline{J}_1 = \langle y_1^2 + y_2x_2x_1,\ y_2y_1 + y_1 + x_2^2x_1 + x_2x_1^2,\ y_2^2 + y_2 + y_1(x_2 + x_1)\rangle$$

corresponds to

$$\begin{array}{llll} NF(y_1 \cdot y_1) = 0 & \cdot 1 + 0 & \cdot y_1 + (x_2x_1) & \cdot y_2, \\ NF(y_2 \cdot y_1) = (x_2^2x_1 + x_2x_1^2) & \cdot 1 + 1 & \cdot y_1 + 0 & \cdot y_2, \\ NF(y_2 \cdot y_2) = 0 & \cdot 1 + (x_2 + x_1) & \cdot y_1 + 1 & \cdot y_2. \end{array}$$

Now let

$$h(T) := T^3 + (y_2 + y_1)(x_2 + 1)x_1T + (y_2(x_2x_1 + 1) + y_1(x_2 + x_1))x_2^2x_1,$$

define a further integral extension $S_2 := ic(S_1)[z]/\langle h(z)\rangle$.

$$\begin{aligned} S_2 = \mathbf{F}_2&[z, y_2, y_1, x_2, x_1]/ \\ &\langle \overline{J}_1, z^3 + (y_2 + y_1)(x_2 + 1)x_1z + (y_2(x_2x_1 + 1) + y_1(x_2 + x_1))x_2^2x_1\rangle \end{aligned}$$

has a standard P-module basis $(z^0y_0, z^0y_1, z^0y_2, z^1y_0, z^1y_1, z^1y_2, z^2y_0, z^2y_1, z^2y_2)$. Again S_2 happens *not* to be integrally closed. But this time, not only is the conjectured form of the variables used to define $ic(S_2)$ wrong, there are more variables than the 9 above that describe S_2. Such a set of dependent variables is:

$$\begin{aligned} f_{0,0} &:= y_0; \\ f_{15,9} &:= y_1; \\ f_{12.9} &:= y_2; \\ f_{19,12} &:= zy_0; \\ f_{34,21} &:= zy_1; \\ x_1f_{34,30} &:= zy_1x_2 + zy_2 + zy_0; \\ f_{31,21} &:= zy_2; \\ \delta f_{29,24} &:= z^2y_0(x_2^3x_1^2 + x_2^2x_1^3 + x_2^3x_1 + x_2x_1^3 + x_2x_1 + 1) \\ &\quad + z^2y_2(x_2x_1 + 1) + z^2y_1(x_2 + x_1); \\ \delta f_{26,24} &:= z^2y_1(x_2^2x_1 + x_2x_1^2 + x_2x_1 + x_1^2 + x_2 + x_1) \\ &\quad + z^2y_2(x_2^2x_1 + x_2x_1 + x_1 + 1) \\ &\quad + z^2y_0(x_2^3x_1 + x_2^2x_1^2 + x_2^2x_1 + x_2x_1 + x_1 + 1); \\ \delta f_{23,15} &:= z^2y_2(x_2x_1^2 + x_1) + z^2y_1(x_2x_1 + x_1^2) + z^2y_0(x_2^2x_1^2 + x_2x_1^3 + x_2x_1^2 + x_1) \end{aligned}$$

for $\delta := (x_2 + x_1)(x_2 + 1)x_2(x_1 + 1)x_1^2$. The integral closure is then of the form

$$ic(S_2) = \mathbf{F}_2[f_{34,30}, f_{34,21}, f_{31,21}, f_{29,24}, f_{26,24}, f_{23,15}, f_{19,12}, f_{15,9}, f_{12,9}; f_{9,9}, f_{9,0}]/\overline{J}_2$$

with $\overline{J}_2$ the ideal of induced relations most of the form $f_if_j - NF(f_if_j, \overline{J}_2)$ except for the first, of the form $SP(f_{34,30}, f_{34,21}) - NF(SP(f_{34,30}, f_{34,21}), \overline{J}_2)$. That one describes the dependence between $f_{34,30}$ and $f_{34,21}$:

$$f_{34,30}f_{9,0} + f_{34,21}(f_{9,9} + f_{9,0}) + f_{31,21}(1) + f_{19,12}(1) = 0.$$

An example of the others is:

$$f_{12,9}f_{12,9} + f_{15,9}(f_{9,9} + f_{9,0}) + f_{12,9}(1) = 0$$

describing a multiplication of $f_{12,9}$ and $f_{12,9}$. (A full list of all the 45+1 relations for this example can be found on the website.)

4. Weighted basis theorem

To define the P-linear relation hypothesis, it is necessary to introduce non-standard notation, to write $LM(f) = \underline{x}^{\underline{\alpha}} LM_P(f)$, to split $LM(f)$ over P into a "coefficient" $\underline{x}^{\underline{\alpha}}$ from P and a "monomial" $LM_P(f)$. (These correspond to a leading coefficient and a leading monomial only if one is working with P as the coefficient ring and allows a weight function to deal with all the variables that occur, whether or not they are variables defined over P or variables in P itself. This is *not* the view taken currently in any computational algebra packages.)

Theorem 4.1. *Let $P := \mathbf{F}[x_n, \dots, x_1]$ be a polynomial ring in n independent variables over the field $\mathbf{F}$. Let*

$$Q := P[y_{m-1}, \dots, y_1]/I = \mathbf{F}[y_{m-1}, \dots, y_1; x_n, \dots, x_1]/I$$

be an integrally closed *extension of P (with $Q = P$ corresponding to the case $m = 1$), with grevlex-over-weight monomial order defined by the matrix M.*

Let $f(T) \in Q[T]$ be a monic, (absolutely irreducible) polynomial (of some degree d) define an integral extension *$S := Q[z]/\langle f(z)\rangle$, with grevlex-over-weight monomial order an extension of that on Q so that $LM(f) = z^d$.*

Suppose that $\Delta \in P$ satisfies $S \subseteq ic(S) \subseteq \Delta^{-1}S$.

Then $ic(S) = \mathbf{F}[w_{s-1}, \dots, w_1; x_n, \dots, x_1]/J$ with J having Gröbner basis B with elements $w_i w_j - NF(w_i w_j, \overline{J})$ for all i, j, and $SP(w_i, w_j) - NF(SP(w_i, w_j), \overline{J})$ when $LP(w_i) = LP(w_j)$, with $LP(w_i)$ denoting the leading monomial of w_i if Q is viewed with coefficients from P.

Proof. Since $ic(S)$ is a ring, the minimal, reduced Gröbner basis will have to contain elements of the form $w_i w_j = \sum_k c_{i,j,k} w_k =: NF(w_i w_j, \overline{J})$ for some *structure constants* $c_{i,j,k} \in P$. Any other elements in a Gröbner basis for $ic(S)$ must be P-linear combinations of the w's. Since $SP(w_i, w_j) = \sum_k b_{i,j,k} w_k =: NF(SP(w_i, w_j), \overline{J})$, when $LM_P(w_i) = LM_P(w_j)$, the minimal P-linear combinations will be of the form $SP(w_i, w_j) - NF(SP(w_i, w_j), \overline{J})$, with $LM_P(w_i) = LM_P(w_j)$. ∎

5. Integral closure algorithms

Integral closure algorithms are based on some version of

$$S \subseteq ic(S) \subseteq M = \Delta^{-1}S$$

for some Δ, not necessarily in P. Most are based on finding an increasing sequence of rings

$$S = R_0 \subset \cdots \subset R_l = R_{l+1} = ic(S)$$

with the elements in R_{i+1} of the form f_i/d_i for $f_i \in R_i$ and $d_1 \cdots d_i | \Delta$. The qth power algorithm [11] on the other hand is based on finding a sequence of P-modules

$$\Delta^{-1}S = M_0 \supset \cdots \supset M_L = M_{L+1} = ic(S)$$

with $M_{i+1} := \{\Delta^{-1}f \in M_i : NormalForm(\Delta^{-1}f)^q \in M_i\}$. (This works best when all the coefficients involved are in $\mathbf{F}_q$, since it is then a linear algorithm with major cost in computing the normal forms involved.)

But other than choosing $\Delta \in P$ it is not so important which type of algorithm is used. What is more important is choosing to find a large enough set of variables, as above, so that the leading terms are all of degree at most 2 in the dependent variables. And secondarily, the monomial order of the base ring should extend to the integral closure. (The algorithm used to produce output for this paper is, however, based on the qth-power algorithm.)

[There is an example on the website which is a thinly disguised example of a simple Hermitian curve worked out in MAGMA, SINGULAR, and MACAULAY 2, showing the limitations of each implementation. This example was used to show that there were bugs in the stopping criteria in the latter two implementations.]

In the example given, the `normal.lib` function of SINGULAR [6] produces

$$\begin{aligned}
&T(1) := z,\ T(2) := y_1,\ T(3) := y_2,\ T(4) := x_2,\ T(5) := x_1,\\
&\delta := (x_2+x_1)(x_2+1)x_2(x_1+1)x_1^2,\\
&\delta\left(T(6) + (x_2+1)x_1\right) := z^2y_2\left(x_2x_1 + x_2^2\right) + z^2y_1\left(x_2x_1^2 + x_1\right)\\
&\qquad\qquad\qquad\qquad + z^2\left(x_2^3x_1^2 + x_2(x_1^3 + x_1^2) + x_1\right),\\
&\delta\left(T(7) + y_2(x_2+1) + y_1(x_2+1)x_1 + x_2^2x_1 + x_2x_1^2 + x_2x_1 + x_1^2\right)\\
&:= z^2y_2\left(x_2^2x_1^2 + x_2(x_1^3 + x_1^2) + x_1^3\right)\\
&\quad + z^2y_1\left(x_2^2x_1 + x_2x_1^2 + x_2x_1 + x_1^2\right)\\
&\quad + z^2\left(x_2^3x_1^2 + x_2^2(x_1^3 + x_1^2 + x_1) + x_2(x_1^3 + x_1^2 + x_1) + x_1^2\right),\\
&\delta(T(8) + zy_2 + zy_1(x_2+1) + z(x_2^2 + x_2x_1 + x_2 + x_1 + 1)\\
&\qquad + y_2(x_2^3 + x_2^2x_1 + x_2^2 + x_2 + 1) + y_1(x_2^3 + x_2x_1 + x_1)\\
&\qquad + x_2^4x_1 + x_2^3(x_1^2 + x_1) + x_2^2(x_1^2 + x_1) + x_2(x_1^2 + x_1) + x_1^2)\\
&:= +z^2y_2\left(x_2^2x_1^2 + x_2(x_1^3 + x_1^2) + x_1^3\right) + z^2y_1\left(x_2^2x_1 + x_2(x_1^2 + x_1) + x_1^2\right)\\
&\quad + z^2\left(x_2^3x_1^2 + x_2^2(x_1^3 + x_1^2 + x_1) + x_2(x_1^3 + x_1^2 + x_1) + x_1^2\right)\\
&\quad + zy_2\left(x_2^4(x_1^2 + x_1) + x_2^3(x_1^2 + x_1) + x_2^2(x_1^4 + x_1^2) + x_2(x_1^4 + x_1^3)\right)\\
&\quad + zy_1\left(x_2^3(x_1^2 + x_1) + x_2^2(x_1^3 + x_1) + x_2(x_1^3 + x_1^2)\right)\\
&\quad + z\left(x_2^3(x_1^2 + x_1) + x_2^2(x_1^3 + x_1) + x_2(x_1^3 + x_1^2)\right),\\
&\delta(T(9) + zy_2 + zy_1(x_2+1) + z(x_2^2 + x_2x_1 + x_2 + x_1 + 1)\\
&\qquad + y_2(x_2^3 + x_2^2x_1 + x_2^2 + x_2 + 1) + y_1(x_2^3 + x_2x_1 + x_2 + x_1 + 1)\\
&\qquad + x_2^4x_1 + x_2^3(x_1^2 + x_1) + x_2^2(x_1^2 + x_1) + x_2(x_1^2 + 1) + x_1 + 1))\\
&:= +z^2y_2\left(x_2^2(x_1^2 + x_1) + x_2(x_1^3 + x_1 + 1) + x_1^3 + x_1^2 + x_1\right)\\
&\quad + z^2y_1\left(x_2x_1^2 + x_1^2 + x_1 + 1\right)\\
&\quad + z^2\left(x_2^3(x_1^2 + x_1) + x_2^2x_1^3 + x_2(x_1^3 + x_1^2) + x_1^2 + x_1 + 1\right)\\
&\quad + zy_2\left(x_2^4(x_1^2 + x_1) + x_2^3(x_1^2 + x_1) + x_2^2(x_1^4 + x_1^3) + x_2(x_1^4 + x_1^3)\right)\\
&\quad + zy_1\left(x_2^3(x_1^2 + x_1) + x_2^2(x_1^3 + x_1) + x_2(x_1^3 + x_1^2)\right)\\
&\quad + z\left(x_2^3(x_1^2 + x_1) + x_2^2(x_1^3 + x_1) + x_2(x_1^3 + x_1^2)\right).
\end{aligned}$$

though the last 4 are not given explicitly, and the first 5 are only given explicitly in that the embedding map from S maps z, y_1, y_2, x_2, and x_1 onto $T(1)$, $T(2)$, $T(3)$, $T(4)$, and $T(5)$ respectively. The Gröbner basis elements are an unpredictable mess, since the order is grevlex on $(T(1),\ldots,T(9))$. Our suggested form would be $ic(S) = \mathbf{F}_2[z_9, z_8, z_7, z_6, z_5, z_4, z_3, z_2, z_1; x_2, x_1]/\overline{I}$ with weight function given by the weight matrix $\overline{M} := \left(\begin{smallmatrix} 34 & 34 & 31 & 29 & 26 & 23 & 19 & 12 & 15 & 9 & 9\\ 30 & 21 & 21 & 24 & 24 & 15 & 12 & 9 & 9 & 9 & 0\end{smallmatrix}\right)$ and order gotten by completing this to a grevlex-over-weight order.

6. Minimization

Given that this procedure preserves the recursively generated monomial order, it is sometimes possible to minimize the result if some independent variable x_j is integral over some different choice $P^* := \mathbf{F}[x_n^*, \ldots, x_1^*]$.

Example 3. Consider

$$Q := P := \mathbf{F}_2[x_2, x_1],\ wt(Q) := \begin{pmatrix} | & 1 & 1 \\ | & 1 & 0 \end{pmatrix},$$
$$f(T) := T^4 + T^2 x_2 x_1 + T^0 x_2^3 x_1^2,$$
$$S := Q[z]/\langle f(z)\rangle,\ wt(S) = \begin{pmatrix} 5 & | & 4 & 4 \\ 3 & | & 4 & 0 \end{pmatrix},$$
$$\Delta := x_2^3 x_1^2,$$
$$ic(S) = \mathbf{F}_2[z_3, z_2, z_1; x_2, x_1]/\overline{I},\ wt(ic(S)) = \begin{pmatrix} 3 & 2 & 5 & | & 4 & 4 \\ 1 & 2 & 3 & | & 4 & 0 \end{pmatrix},$$
$$\overline{I} = \big\langle z_1^2 + z_2 x_2 x_1, z_2 z_1 + z_3 x_2 + z_1, z_2^2 + z_2 + x_2,$$
$$z_3 z_1 + x_2 x_1, z_3 z_2 + z_1, z_3^2 + z_2 x_1 + x_1 \big\rangle,$$
$$\delta := x_2^2 x_1,\ z_3\delta := z^3 + z x_2 x_1,\ z_2\delta := z^2 x_2,\ z_1\delta := z\delta,$$

$x_2 = z_2^2 + z_2$ is integral over $\mathbf{F}_2[z_2, x_1]$ and $z_1 = z_3 z_2$.

$$ic(S) = \mathbf{F}_2[\overline{z_1}; \overline{x}_2, \overline{x}_1]/\overline{J},\ wt(ic(S)) = \begin{pmatrix} 3 & | & 2 & 4 \\ 1 & | & 2 & 0 \end{pmatrix},$$
$$\overline{J} = \big\langle \overline{z}_1^2 + \overline{x}_2\overline{x}_1 + \overline{x}_1 \big\rangle,$$
$$\delta := x_2^2 x_1,\ \overline{z}_1\delta := z^3 + z x_2 x_1,\ \overline{x}_2\delta := z^2 x_2,\ \overline{x}_1 := x_1\delta,$$
$$\psi((\overline{z}_1,\ \overline{x}_2,\ \overline{x}_1)\delta) = (z^3 + z x_2 x_1,\ z^2 x_2,\ x_1\delta),$$
$$\phi(z,\ x_2,\ x_1) = (\overline{z}_1\overline{x}_2,\ \overline{x}_2^2 + \overline{x}_2,\ \overline{x}_1).$$

This is an especially important step in some applications where the original ring is described in terms of variables which are not necessarily those of most interest in the final ring (such as the example above having 12 or 5 variables in a module generating set).

There is an example on the website, with elements of weights 25 and 21 in characteristic 2 which exceeded the 4GB storage ceiling in SINGULAR, but for which MAGMA, almost immediately produces a module basis with 21 elements, (too messy to include here) with respective weights

$$354, 358, 341, 324, 337, 333,\ 25j, 14 \geq j \geq 0.$$

It is straightforward, but tedious, to produce the simpler 7 elements of weights [16,15,13,12,11,10;7] from this. This takes at most 358*21 reductions. (If this reduction is not immediately clear, see [13].) It is much harder to produce the corresponding ideal, since, among other things, MAGMA thinks this should be an $\mathbf{F}_2(y_{21})$-module computation, not an $\mathbf{F}_2(y_7)$-module one.

Example 4. Consider a slight variation on example 9.5 of [5], namely

$$X_1^4 - X_2^3 + X_3^2 = 0.$$

There are numerous ways to view this as an integral extension problem as considered here. Their weight function is $wt(X_1) := (3, 0)$, $wt(X_2) := (4, 0)$ and $wt(X_3) :=$

$(0,1)$; their point being that (X_1,X_2) is a set of independent variables, but their weights aren't. Here that means that this weight function would be perfectly fine if this is viewed as a type I integral extension of $P := \mathbf{F}[X_2,X_3]$, integrally closed with P-module basis $(1,X_1,X_1^2,X_1^3)$, but not if it is viewed as a type I integral extension of $P := \mathbf{F}[X_2,X_1]$. However, for this extension the default $wt(X_3) := (3,3)$, $wt(X_2) := (2,2)$, $wt(X_1) := (1,0)$. is fine, giving P-module basis $(1,X_1)$.

But in either case the weight of the first variable is not really dependent on the weight of the third. So maybe using weights won't be the best way to see that the latter gives a smaller presentation in terms of the $\mathbf{F}[y,x]$-module basis $(1,z)$ than the former, with $\mathbf{F}[y,z]$-module basis $(1,x,x^2,x^3)$.

But there are times when it is possible to use the weights to determine a minimal presentation, including the important case $n=1$.

Theorem 6.1. *Suppose that both presentations*

$$S = \mathbf{F}[x_n,\dots,x_1][y]/\langle f_1(y)\rangle \text{ and } S = \mathbf{F}[y,x_{n-1},\dots,x_1][x_n]/\langle f_2(x_n)\rangle$$

are type I integral extensions with the same weight function wt_s. Then $wt_S(y)$ and $wt_S(x_n)$ are scalar multiples of each other.

Proof.

$$d_1 wt_S(y) = a_n wt_S(x_n) + \sum_{i=1}^{n-1} a_i x_i,\ d_2 wt_s(x_n) = b_n wt_S(y) + \sum_{i=1}^{n-1} b_i wt_S(x_i)$$

for some non-negative integers a_i and b_i, and some positive integers d_1 and d_2. But then

$$(d_1 d_2 - a_n b_n) wt_S(x_n) = \sum_{i=1}^{n-1} (b_n a_i + d_1 b_i) wt_S(x_i).$$

This is clearly a dependence among independent weights, so $b_n a_i + d_1 b_i = 0$ for $1 \le i < n$. But this forces $b_i = 0$ for $1 \le i < n$, and $d_2 wt_S(x_n) = b_n wt_S(y)$. $\square$

This gives the known (certainly implicitly understood as long ago as the early 1990's) result for $n=1$:

Corollary 6.2 (Folklore). *For curves (the case $n=1$), there is an $\mathbf{F}[x_1]$-module basis $(y_0 := 1, y_1, \dots, y_{\rho-1})$ with $x_1 := f_\rho$ of smallest positive pole order ρ at P_∞, and $y_i := f_{\rho_i}$ with $\rho_i \equiv i (mod\ \rho)$ (also smallest). In particular $\mathcal{L}(\infty P_\infty)$ has vector-space generators $f_{\rho_i} f_\rho^j$ for $0 \le i < \rho$, and $0 \le j$ over $\mathbf{F}$.*

We have seen by the example above that, for higher dimensional varieties $(n>1)$, it may be the case that a weight function for S viewed as a type I integral extension relative to one choice of P, cannot possibly be used for S viewed similarly relative to some other choice of P. If $f(T) = T^d + \cdots + f_0$ with $f_0 = \underline{x}^{\underline{\alpha}}$, and $\alpha_i \ne 0$ for $1 \le i \le n$, then it would seem that the above theorem would not apply, since x_n would not be integral over $\mathbf{F}[y,x_{n-1},\dots,x_1]$, but consider the following example:

Example 5. $S := \mathbf{F}_2[y;x_2,x_1]/\langle y^6 + yx_2^3x_1^4 + x_2^5x_1^3\rangle$, with $wt_S(x_1) := (6,0)$, $wt_S(x_2) := (12,12)$, and $wt_S(y) := (13,10)$. Then there is an $\mathbf{F}_2[x_2,x_1]$-module basis $(1,y,z,zy,z^2,w)$ for $z := y^2/(x_2x_1)$ and $w := y^5/(x_2^3x_1^2)$; but since $wt_s(z) = (8,8)$, and $3(8,8) = 2(12,12)$ there is an $\mathbf{F}_2[z,x_1]$-module basis $(1,x_2,y,w)$ with $s=4$ instead of $s=6$.

Example 6. $S := \mathbf{F}_2[y;x,z]/\langle y^7 + y^6z + x^6 + x^5z\rangle$ has an integral closure with $\mathbf{F}_2[x,z]$-module basis of size 7, whereas it has $\mathbf{F}_2[y,z]$-module basis of size 6, with no clue from the weights: $(0,0)$, $(6,5)$, $(12,10)$, $(11,8)$, $(10,6)$, $(9,4)$, $(8,2)$; $(7,7)$, $(7,0)$, in the former and $(0,0)$, $(7,6)$, $(8,6)$, $(9,6)$, $(10,6)$, $(11,6)$; $(6,6)$, $(6,0)$, in the latter. However using weights $(6,0)$,$(7,0)$,and $(0,7)$ in place of $(6,5)$, $(7,7)$, $(7,0)$, would make it simple to apply the theorem.

REFERENCES

[1] W. Adams and P. Loustaunau, "An Introduction to Gröbner Bases," American Mathematical Society, Providence, RI, 1994.

[2] H. Cohen, "A Course in Computational Algebraic Number Theory," Springer, Berlin, 1993.

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

[4] G.-L. Feng and T. R. N. Rao, *A simple approach for construction of algebraic-geometric codes from affine plane curves*, IEEE Trans. Infrom. Theory, **40** (1994), 1003–1012.

[5] O. Geil and R. Pellikaan, *On the structure of order domains*, Finite Fields Appl., **8** (2002), 369–396.

[6] G.-M. Greuel and G. Pfister, `normal.lib` A SINGULAR 3.0 Library for Computing the Normalization of Affine Rings, 2005.

[7] G.-M. Greuel, G. Pfister and H. Schönemann, SINGULAR 3.0.4 A Computer Algebra System for Polynomial Computations, Centre for Computer Algebra, University of Kaiserslautern, 2007.

[8] T. Høholdt, J. H. van Lint and R. Pellikaan, "Algebraic Geometry of Codes," North-Holland, Amsterdam, (1998), 871–961.

[9] D. A. Leonard, *Finding the defining functions for one-point algebraic-geometric codes*, IEEE Trans. Infrom. Theory, **47** (2001), 2566–2573.

[10] D. A. Leonard, *Prototype I representations of AG codes*, in "Proceedings of the 40th Allerton Conference," U. of Illinois, (2002), 1007–1016.

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

[12] The MAGMA Computational Algebra System for Algebra, Number Theory and Geometry, the university of Sydney computational algebra group, `http://magma.maths.usyd.edu.au/magma`.

[13] R. Matsumoto, *Constructing algebraic geometry codes on the normalization of a singular C_{ab} curve*, IEICE Trans. Fundamentals, **E82-A** (1999), 1981–1986.

Received June 2008; revised January 2009.

E-mail address: leonada@auburn.edu