TU Kaiserslautern

Bachelor thesis

Greatest common divisors using homological algebra

Author:
Florian Diebold

Supervisor:
PD Dr. Mohamed Barakat

August 19, 2011

Contents

1. Introduction

Building on ideas from Northcott's book *Finite Free Resolutions* [**5**], T. Coquand and C. Quitté [**3**] presented a proof of the fact that if the ideal generated by some elements $a_1, \dots, a_n$ of a commutative ring has a finite free resolution, there exists a greatest common divisor of $a_1, \dots, a_n$. As they mention, the proof is constructive, giving an algorithm to compute this greatest common divisor. I wrote an implementation of this algorithm, and of some other ideas used in the proof, for the HOMALG project [**4**] [**2**], an algorithmic homological algebra project implemented in GAP4. In this bachelor thesis, I reproduce the proof for the algorithm and discuss its implementation.

The code for this implementation is completely contained in the files `ExteriorAlgebra.gd` and `ExteriorAlgebra.gi` in the `Modules` package [**1**] of HOMALG.

In the following, let R be a commutative ring with one.

2. Regularity

Definition 1. We say that $a \in R^n$ is *regular* if for $x \in R$, $ax = 0$ implies $x = 0$.

Similarly, for an R-module E, we say that $a \in R^n$ is *E-regular* if for $x \in E$, $a_1 x = \ldots = a_n x = 0$ implies $x = 0$.

This definition can be rephrased to give a way to define higher-order regularity. First we define, again for $a \in R^n$, the map

$$d_a : R \to R^n,\ x \mapsto ax. \tag{1}$$

Given an R-module E, using the tensor product, we also get the map

$$d_a : E \to E^n,\ x \mapsto ax. \tag{2}$$

Obviously, a is (E-) regular exactly if $\ker d_a = 0$. Now, to define higher-order versions of these maps, we need the *exterior algebra*.

3. Exterior Algebra

Let M be an R-module.

Definition 2. The *exterior algebra* $\bigwedge(M)$ is the free algebra with a map $i\colon M \to \bigwedge(M)$ satisfying $i(x) \wedge i(x) = 0$ for all $x \in M$.

In this case, all we need is the exterior algebra over a free module $M = R^n$. This allows us to concretely represent $\bigwedge(M)$ as a free R-module of rank 2^n: We write $e_I, I \subseteq \{1, \dots, n\}$ for the 2^n elements of the basis of $\bigwedge(M) = R^{2^n}$, and define

$$e_I \wedge e_J := e_{I \cup J} \prod_{(i,j) \in I \times J} (i, j), \tag{3}$$

where $(i, j) = 1$ if $i < j$, $(i, j) = 0$ if $i = j$, and $(i, j) = -1$ if $i > j$. This operation can be extended to $\bigwedge(M)$ using bilinearity. It is then obvious that the resulting operation makes $\bigwedge(M)$ into an associative algebra; and, using $i\colon M \to \bigwedge(M)$, $(a_1, \dots, a_n) \mapsto \sum_{i=1}^n a_i e_{\{i\}}$, satisfies Definition 2.

In the following, we will identify a and $i(a)$ for $a \in R^n$.

This construction also makes it obvious that $\bigwedge(R^n)$ is a *graded* algebra; each graded part $\bigwedge^p(R^n)$ is a free R-module of rank $\binom{n}{p}$, using the elements e_I, where $|I| = p$, as basis. We will call $\bigwedge^p(M)$ the *p-th exterior power* of M.

In HOMALG, $\bigwedge^p(M)$ can be constructed using `ExteriorPower(p, M)`. This caches the exterior powers of `M` in the attribute `ExteriorPowers`. The exterior powers themselves get the following properties and attributes:

Attribute	Value
`IsExteriorPower`	`true`
`ExteriorPowerExponent`	`p`
`ExteriorPowerBaseModule`	`M`

TABLE 1. exterior power attributes

Elements of modules marked with `IsExteriorPower` will then be automatically (using an immediate method) marked as `IsExteriorPowerElement`. The $\wedge$ operator is implemented in the operation `Wedge`. Two helper functions, `_Homalg_IndexCombination` and `_Homalg_CombinationIndex`, help converting the sets used to index the canonical basis of $\bigwedge^p(R^n)$ from and to normal (1-based) natural number indices.

4. Koszul complex and Grade

It is easy to see that $\bigwedge^0(R^n) \cong R$, and $\bigwedge^1(R^n) \cong R^n$. Thus, our map d_a from Equation 1 could be seen to go from $\bigwedge^0(R^n)$ to $\bigwedge^1(R^n)$. As promised, this gives us higher-order versions of d_a:

$$d_{a,p} : \bigwedge^p(R^n) \to \bigwedge^{p+1}(R^n),\ x \mapsto a \wedge x. \tag{4}$$

Since, for $x \in \bigwedge^p(R^n)$, $(d_{a,p+1} \circ d_{a,p})(x) = a \wedge (a \wedge x) = (a \wedge a) \wedge x = 0 \wedge x = 0$, this gives rise to a complex.

Definition 3. The cohomological complex $K^\bullet(a) := (\bigwedge^\bullet(R^n), d_{a,\bullet})$ is called the *Koszul complex*:

$$0 \to R \xrightarrow{d_{a,0}} R^n \xrightarrow{d_{a,1}} \bigwedge^2(R^n) \xrightarrow{d_{a,2}} \cdots \xrightarrow{d_{a,n-1}} \bigwedge^n(R^n) \to 0$$

By taking the tensor product with the R-module E, we obtain the *E-valued Koszul complex* $K^\bullet(a;E) := (\bigwedge^\bullet(R^n) \otimes E, d_{a,\bullet}) = (\bigwedge^\bullet(E), d_{a,\bullet})$.

This construction is implemented in the `Modules` package of HOMALG as the operation `KoszulComplex(a, E)`; where `a` is passed as a list.

Note that constructing the Koszul complex is an exact functor in the second argument, i.e. any map of R-modules $E \to F$ induces a chain map $K^\bullet(a;E) \to K^\bullet(a;F)$, and if $E \to F \to G$ is exact, then so is $K^\bullet(a;E) \to K^\bullet(a;F) \to K^\bullet(a;G)$. Coquand and Quitté make heavy use of this fact and the long exact sequence this induces (via the zig-zag lemma).

In the following, we will denote the cohomology modules of these complexes by $H^p(a)$ and $H^p(a;E)$, respectively. Obviously, $K^\bullet(a) = K^\bullet(a;R)$.

Definition 4. We now define the *grade of a on E* by requiring that $\mathrm{grade}(a;E) \geq k$ if $H^p(a;E) = 0$ for all $p < k$.

We will write $\mathrm{grade}(a)$ for $\mathrm{grade}(a;R)$.

In HOMALG, this is implemented as `Grade_UsingKoszulComplex`. As we will show later, the grade depends only on the ideal $\langle a_1, \dots, a_n \rangle$; thus, the HOMALG operation works both on lists of ring elements and on ideals. For both argument types, the module E can be passed as a second parameter. This also provides a method for the HOMALG operation `Grade(I, E)`, where `I` is an ideal and `E` a module.

This definition gives the desired higher-order regularity:

Remark. Let $a = (a_1, \dots, a_n) \in R^n$.

(1) $\operatorname{grade}(a;E) \geq 1$ if and only if a is E-regular.
(2) $\operatorname{grade}(a;E) \geq 2$ if a is E-regular and for each $(x_1,\dots,x_n) \in E^n$ with $a_i x_j - a_j x_i = 0$ for all i,j, there exists an $x' \in E$ such that $x_i = a_i x'$.

Proof. (1): $\operatorname{grade}(a;E) \geq 1$ means that $H^0(a;E) = 0$, i.e. $\ker d_{a,0} = 0$.

(2): $\operatorname{grade}(a;E) \geq 2$ iff additionally $H^1(a;E) = 0$, i.e. $\operatorname{im} d_{a,0} = \ker d_{a,1}$.

Let $x \in \ker d_{a,1}$; that means $x = (x_1,\dots,x_n) \in E^n$ and $a \wedge x = d_{a,1}(x) = 0$. Looking at the components of $a \wedge x$ in the canonical basis $e_{\{i,j\}}$, that is equivalent to the fact that for all $\{i,j\} \subseteq \{1,\dots,n\}$, we have $a_i x_j - a_j x_i = 0$.

On the other hand, $x \in \operatorname{im} d_{a,0}$ is equivalent to the condition that there is an $x' \in E$ such that $x_i = a_i x'$. □

If we have $a, x \in R^n$ satisfying the condition in (2) (i.e., $a_i x_j - a_j x_i = 0$ for all i,j), we call them *proportional*; thus, if a and x are proportional and $\operatorname{grade}(a) \geq 2$, then x is a multiple of a.

We will make use of this property of grade 2 through the following lemma:

Lemma 1. *Let $(a_1,\dots,a_n) \in R^n$ be regular and $g, b_1,\dots,b_n \in R$ such that $(a_1,\dots,a_n) = g(b_1,\dots,b_n)$. If $\operatorname{grade}(b_1,\dots,b_n) \geq 2$, then g is regular and is the greatest common divisor of $a_1,\dots,a_n$.*

Proof. Were g not regular, there would have to exist an $x \in R, x \neq 0$ such that $xg = 0$. But that would imply that $xa = xgb = 0$, contrary to the assumption that a is regular.

Now let $s \in R$ be another element which divides all a_i, i.e. $a = sc$ for some $c = (c_1,\dots,c_n) \in R^n$. By the same reasoning as above, s is regular, and thus b and c are proportional. Since $\operatorname{grade}(b) \geq 2$, this implies that c is a multiple of b, i.e. there exists a $t \in R$ such that $c = tb$. We conclude $gb = a = sc = stb$, and since b is regular, $g = st$. □

5. Other operations on the exterior algebra

For the algorithm, we will need several other operations on exterior algebra elements, which we will define now.

We start with a generalization of the interior product:

Definition 5. For $a, b \in R^n$, we have $a \cdot b = \sum a_i b_i$. Using induction on k, we define

$$a \cdot e_{i_0 \dots i_k} := a_{i_o} e_{i_1 \dots i_k} - e_{i_0} \wedge (a \cdot e_{i_1 \dots i_k}),$$

and then $a \cdot \omega \in \bigwedge^k(R^n)$ for $\omega \in \bigwedge^{k+1}(R^n)$ by linearity.

This immediately gives the following equation, again for $a, b \in R^n$ and $\omega \in \bigwedge^{k+1}(R^n)$:

$$a \cdot (b \wedge \omega) = (a \cdot b)\omega - b \wedge (a \cdot \omega) \tag{5}$$

Since $\bigwedge^k(R^n)$ has a canonical basis, we can also define the direct analogon to the dot product in R^n:

Definition 6. For $\omega = \sum \omega_I e_I, \nu = \sum \nu_I e_I \in \bigwedge^k(R^n)$, we define

$$(\omega \mid \nu) := \sum \omega_I \nu_I.$$

Note that $(\omega \mid e_I)$ simply means the component of ω with the index I in the canonical basis. It is easy (if a bit tedious) to see that

$$e_i \cdot e_I = \begin{cases} (-1)^{|\{k \in I | k < i\}|} e_{I \setminus \{i\}} & \text{if } i \in I \\ 0 & \text{otherwise.} \end{cases}$$

This implies $(e_i \cdot e_I \mid e_J) = (e_i \wedge e_J \mid e_I) = (e_I \mid e_i \wedge e_J)$, which thanks to linearity then gives

$$(a \cdot \omega \mid \nu) = (\omega \mid a \wedge \nu). \tag{6}$$

Two other operations are left:

Definition 7. Since $\bigwedge^n(R^n)$ is a free module of rank 1, we define for $\omega \in \bigwedge^n(R^n)$

$$[\omega] := (\omega \mid e_{\{1,\dots,n\}}),$$

i.e. the single component of ω in the canonical basis.

Let $p+q=n$. To any $\omega \in \bigwedge^p(R^n)$ we associate

$$\omega^* := \sum_{|I|=q} [e_I \wedge \omega] e_I \in \bigwedge^q(R^n).$$

These two operations are directly used in the algorithm. In `Modules`, $[a]$ is implemented as `SingleValueOfExteriorPowerElement(a)`, and a^* is `ExteriorPowerElementDual(a)`.

Now we can prove the main tool for the correctness proof of the algorithm. We first give two lemmata and then prove the main theorem.

Lemma 2. *Let $v \in R^n$ be orthogonal to $u_1, \dots, u_p \in R^n$. Then $u_1 \wedge \dots \wedge u_p$ is orthogonal to any $v \wedge \beta$ for $\beta \in \bigwedge^{p-1}(R^n)$ (i.e., $(u_1 \wedge \dots \wedge u_p \mid v \wedge \beta) = 0$).*

Proof. We have $v \cdot (u_1 \wedge \dots \wedge u_p) = 0$ by induction on p since

$$v \cdot (u_1 \wedge \omega) = (v \cdot u_1)\omega - u_1 \wedge (v \cdot \omega)$$

. Thus, $(u_1 \wedge \dots \wedge u_p \mid v \wedge \beta) = (v \cdot (u_1 \wedge \dots \wedge u_p) \mid \beta) = 0$. $\square$

Lemma 3. *For $a_1, \dots, a_n, b_1, \dots, b_p \in R^n$, write $r_{i_1 \dots i_p}$ for the element $[a_1 \wedge \dots \wedge a_n]$ where a_{i_k} is replaced by b_k for $1 \le i_1 < \dots < i_p \le n$. We then have*

$$[a_1 \wedge \dots \wedge a_n] b_1 \wedge \dots \wedge b_p = \sum r_{i_1 \dots i_p} a_{i_1} \wedge \dots \wedge a_{i_p}.$$

Proof. We show this in the case that $R = \mathbb{Z}[X]$. From this, the general case follows via tensor product. In this case, we have a fraction field K. The vectors $a_1, \dots, a_n$ can be assumed to be linearly independent, since otherwise $a_1 \wedge \dots \wedge a_n = 0$ and the statement is thus trivial. Hence, $a_1, \dots, a_n$ form a basis of K^n, and because both sides of the equation are linear in $b_1, \dots, b_p$, we just need to check the case where $b_1, \dots, b_p$ are basis vectors, i.e. $b_1 = a_{j_1}, \dots, b_p = a_{j_p}$. In this case, the equality becomes trivial, since $r_{i_1 \dots i_p} = 0$ except when $i_1 = j_1, \dots, i_p = j_p$. $\square$

Theorem 4. *Let $u_1, \dots, u_p, v_1, \dots, v_q \in R^n$ pairwise orthogonal, i.e. $u_i \cdot v_j = 0$ for all i, j, and $p+q=n$. Then the elements $\omega := u_1 \wedge \dots \wedge u_p$ and $\beta := v_1 \wedge \dots \wedge v_q$ are such that ω and β^* are proportional.*

Proof. ω and β^* being proportional means that for any two subsets I and J of N_n with $|I| = |J| = p$, we have

$$\begin{aligned} 0 &= (\beta^* \mid e_I)(\omega \mid e_J) - (\beta^* \mid e_J)(\omega \mid e_I) \\ &= [e_I \wedge \beta](\omega \mid e_J) - [e_J \wedge \beta](\omega \mid e_I) \\ &= (\omega \mid [e_I \wedge \beta] e_J - [e_J \wedge \beta] e_I). \end{aligned}$$

Write $i_1 < \dots < i_p \in I$ and $j_1 < \dots < j_p \in J$. Using Lemma 3, we see that $[e_I \wedge \beta] e_J = [e_{i_1} \wedge \dots \wedge e_{i_p} \wedge v_1 \wedge \dots \wedge v_q] e_{j_1} \wedge \dots \wedge e_{j_p}$ is a sum of elements of the form $v_l \wedge \alpha_l$, plus the element $r_{1 \dots p} e_{i_1} \wedge \dots \wedge e_{i_p} = [e_{j_1} \wedge \dots \wedge e_{j_p} \wedge v_1 \wedge \dots \wedge v_q] e_{i_1} \wedge \dots \wedge e_{i_p} = [e_J \wedge \beta] e_I$, which is cancelled. From Lemma 2, it follows that ω is orthogonal to each of these summands and hence the entire sum. $\square$

6. The inductive definition of grade

In *Finite Free Resolutions*, Northcott gives a different (but equivalent) definition of the grade. We need this definition to prove a small lemma.

Lemma 5. *Let $a = (a_1, \ldots, a_n) \in R^n$. The multiplication by any element $x \in \langle a_1, \ldots, a_n \rangle$ kills each $H^l(a; E)$.*

Proof. Let $x \in \langle a_1, \ldots, a_n \rangle$; then we can write $x = b \cdot a$ for some $b \in R^n$. Furthermore, let $\overline{\alpha} \in H^l(a; E)$, which implies $\alpha \in \ker d_{a,l} \implies a \wedge \alpha = 0$. Using the generalized interior product, and Equation 5 in particular, we get

$$\begin{aligned} x\alpha &= b \cdot (a \wedge \alpha) + a \wedge (b \cdot \alpha) \\ &= a \wedge (b \cdot \alpha) \in \operatorname{im} d_{a,l-1} \\ &\implies x\overline{\alpha} = 0. \end{aligned}$$

□

Lemma 6. *If x is an E-regular element in $\langle a_1, \ldots, a_n \rangle$, then we have a short exact sequence*

$$0 \to H^i(a; E) \to H^i(a; E/xE) \to H^{i+1}(a; E) \to 0.$$

In particular, $\operatorname{grade}(a; E) \geq k + 1$ *exactly if* $\operatorname{grade}(a; E/xE) \geq k$.

Proof. Since x is E-regular, we have a short exact sequence

$$0 \to E \xrightarrow{x} E \to E/xE \to 0.$$

This induces a short exact sequence of complexes

$$0 \to K^\bullet(a; E) \xrightarrow{x} K^\bullet(a; E) \to K^\bullet(a; E/xE) \to 0,$$

to which we can associate a long exact sequence

$$\cdots \to H^i(a; E) \xrightarrow{x} H^i(a; E) \to H^i(a; E/xE) \to H^{i+1}(a; E) \xrightarrow{x} H^{i+1}(a; E) \cdots .$$

Because of Lemma 5, the multiplication with x in this sequence is simply the zero map, which finally yields

$$0 \to H^i(a; E) \to H^i(a; E/xE) \to H^{i+1}(a; E) \to 0.$$

The exactness of this complex implies that

$$H^i(a; E/xE) = 0 \implies H^{i+1}(a; E) = 0$$

and

$$H^{i+1}(a; E) = H^i(a; E) = 0 \implies H^i(a; E/xE) = 0,$$

which proves $\operatorname{grade}(a; E) \geq k + 1 \iff \operatorname{grade}(a; E/xE) \geq k$. □

As Coquand and Quitté remark, the grade does not change if we add indeterminates to the ring. This is useful because of the following theorem, which is proved in *Finite Free Resolutions* [**5**]:

Theorem 7. *If $a = (a_1, \ldots, a_n) \in R^n$ is regular, then for any sequence of distinct monomials $m_1, \ldots, m_n$, the polynomial $a_1 m_1 + \ldots + a_n m_n$ is regular.*

Proof. Suppose that $f = a_1 m_1 + \ldots + a_n m_n$ is not regular, i.e. a zero divisor. Then there is a polynomial $g = b_1 l_1 + \ldots + b_k l_k$ with monomials l_i such that $fg = 0$. Choose g such that its number of monomials is minimal. We assume that $m_1 > m_2 > \ldots > m_n$ and $l_1 > l_2, \ldots, l_n$ in lexicographical order. Then $a_1 b_1$ has to be 0. This implies that $a_1 g$ has fewer monomials than g, and because $f a_1 g = 0$, the polynomial $a_1 g$ has to be 0. Thus, $(f - a_1 m_1) g = 0$. This implies $a_2 b_1 = 0$, and by repeating this argument, we get $a_1 b_1 = a_2 b_1 = \ldots = a_n b_1 = 0$, which means that a is not regular. □

For instance, $a_1 + a_2X + \ldots + a_nX^{n-1}$ is regular in $R[X]$. Thus, every regular ideal (i.e., the ideal $\langle a_1, \ldots, a_n \rangle$ if a is regular) contains a regular element, at least in a polynomial extension of R; this is called a *latent regular element*.

Now we can give the inductive definition of the grade from *Finite Free Resolutions*:

Theorem 8. *The following statements are equivalent:*

- $\operatorname{grade}(a; E) \geq k + 1$
- *for all regular elements* $x \in \langle a_1, \ldots, a_n \rangle$, *we have* $\operatorname{grade}(a; E/xE) \geq k$
- *there is a regular (maybe latent) element* $x \in \langle a_1, \ldots, a_n \rangle$ *such that* $\operatorname{grade}(a; E/xE) \geq k$.

Proof. This follows directly from Lemma 6, using the latent regular element from Theorem 7. □

We can now easily show the following lemma, which also implies that the grade only depends on the ideal $\langle a_1, \ldots, a_n \rangle$:

Lemma 9. *Let* $b := (b_1, \ldots, b_m) \in R^m$ *with* $b_1, \ldots, b_n \in \langle a_1, \ldots, a_n \rangle$, *and* $\operatorname{grade}(b; E) \geq k$. *Then we have* $\operatorname{grade}(a; E) \geq k$.

Proof. This is obvious for $k = 0$.

Let $k > 0$. $\operatorname{grade}(b; E) \geq k$ implies that there exists a regular (maybe latent) element $x \in \langle b_1, \ldots, b_m \rangle \subseteq \langle a_1, \ldots, a_n \rangle$ such that $\operatorname{grade}(b; E/xE) \geq k - 1$. By induction, we then have $\operatorname{grade}(a; E/xE) \geq k - 1$ and thus $\operatorname{grade}(a; E) \geq k$. □

7. The Cayley determinant

Now we come to the *Cayley determinant* of a complex, which will be our greatest common divisor. The following applies to a complex of free modules

$$F_m \xrightarrow{A_m} F_{m-1} \xrightarrow{A_{m-1}} F_{m-2} \to \cdots \to F_1 \xrightarrow{A_1} F_0, \tag{7}$$

where

$$F_m = R^{r_m}, F_{m-1} = R^{r_m + r_{m-1}}, F_{m-2} = R^{r_{m-1}+r_{m-2}}, \ldots, F_1 = R^{r_2+r_1}, F_0 = R^{r_1}.$$

Also, we require that $\operatorname{grade}(\Delta_{r_i}(A_i)) \geq 2$ for $i = m, \ldots, 2$ and $\operatorname{grade}(\Delta_{r_1}(A_1)) \geq 1$.

We will see the elements of $\bigwedge^p(R^n)$ as column vectors (in the canonical basis). In the HOMALG implementation, this depends on whether R^n is given as a left or right module; it takes care to switch rows and columns when a complex of left modules is given.

For a matrix $A \in R^{m\times n}$, we can see the columns of A as column vectors $u_1, \ldots, u_n$ in R^m. We write $\wedge^p(A)$ for the matrix having the wedge products $u_{i_1} \wedge \ldots \wedge u_{i_p}, 1 \leq i_1 < \ldots < i_p \leq n$ as columns. To help with this calculation, the function `WedgeMatrixBaseImages(A, J, M)` was implemented, which computes the wedge product of the columns (resp. rows for left modules) of the matrix `A` indexed by the list `J`, treating them as elements of the module `M`. Note that the matrix $\wedge^p(A)$ has the p-minors $\Delta_p(A)$ as its elements. This is easy to see by checking the definition of the determinant.

The Cayley determinant is the last element of an inductively defined sequence. We calculate this sequence $\beta_m, \beta_{m-1}, \ldots, \beta_1$, where $\beta_i \in \bigwedge^{r_i}(F_{i-1})$, using the following steps:

- $\beta_m := \wedge^{r_m}(A_m)$.
- To calculate β_i for $i < m$:
  1. Let $p := r_{i+1}$, $q := r_i$, $s := r_{i-1}$, and write the columns of the matrix A_i^T as column vectors $v_1, \ldots, v_{q+s} \in F_i = R^{p+q}$.

(2) For every subset $J = j_1 < \ldots < j_q \subseteq N_{q+s}$, compute $v_J := v_{j_1} \wedge \ldots \wedge v_{j_q} \in \bigwedge^q(F_i)$. Then find a $\gamma_J \in R$ such that $v_J^* = \gamma_J \beta_{i+1}$ (we will prove that such a γ_J is guaranteed to exist).

(3) Finally, the element β_i is constructed by $\beta_i = \sum \gamma_J e_J$.

Repeat these steps to calculate $\beta_{m-1}, \beta_{m-2}, \ldots, \beta_1$.

Since $\beta_1 \in \bigwedge^{r_1}(R^{r_1})$, we have an element $[\beta_1] \in R$. This is called the *Cayley determinant* of the complex (7). Now, we show that the γ_J from step 2 actually exists:

Lemma 10. *With the above definitions, the following holds:*

- $\wedge^{r_i}(A_i) = \beta_i(\beta_{i+1}^*)^T$ *for* $i = m, \ldots, 1$ *(setting* $\beta_{m+1} := 1$*)*
- $\mathrm{grade}(\beta_i) \geq 2$ *for* $i = m, \ldots, 2$
- γ_J *exists for all subsets* J *in every step.*

Proof. The first part is trivial for $i = m$.

Let $i < m$, and assume $\wedge^{r_{i+1}}(A_{i+1}) = \beta_{i+1}(\beta_{i+2}^*)^T$ with $\mathrm{grade}(\beta_{i+1}) \geq 2$ and β_{i+2} regular. We define $r := r_{i+2}$; thus we have

$$R^{r+p} \xrightarrow{A_{i+1}} R^{p+q} \xrightarrow{A_i} R^{q+s}.$$

Since (7) is a complex, we have $A_i A_{i+1} = 0$. Writing the columns of A_{i+1} as vectors $u_1, \ldots, u_{r+p}$, this implies $u_i \cdot v_j = 0$ for all i, j. Using Theorem 4, we get, for subsets $I = i_1 < \ldots < i_p$ of N_{r+p} and $J = j_1 < \ldots < j_q$ of N_{q+s}, that $u_I := u_{i_1} \wedge \ldots \wedge u_{i_p}$ and $v_J^* = (v_{j_1} \wedge \ldots \wedge v_{j_q})^*$ are proportional. By assumption, we have

$$u_I = (\beta_{i+2}^* \mid e_I)\beta_{i+1}.$$

Thus, since β_{i+2}^* is regular, β_{i+1} and v_J^* are proportional, and since $\mathrm{grade}(\beta_{i+1}) \geq 2$, there exists a γ_J such that $v_J^* = \gamma_J \beta_{i+1}$. This is equivalent to $v_J = \gamma_J \beta_{i+1}^*$, and (remembering that $\gamma_J = (\beta_i \mid e_J)$ by definition) hence we get $\wedge^q(A_i^T) = \beta_{i+1}^* \beta_i^T$, i.e. $\wedge^q(A_i) = \beta_i(\beta_{i+1}^*)^T$.

This also implies that $\Delta_q(A_i) \subseteq \langle \beta_i \rangle$, and thus by Lemma 9 $\mathrm{grade}(\beta_i) \geq 2$ if $\mathrm{grade}(\Delta_q(A_i)) \geq 2$. □

Since we have that $\Delta_{r_1}(A_1)$ is regular, $\Delta_{r_1}(A_1) = \wedge^{r_1}(A_1) = \beta_1(\beta_{i+1}^*)^T$ and $\mathrm{grade}(\beta_{i+1}^*) \geq 2$, by Lemma 1 $[\beta_1]$ is a greatest common divisor of $\Delta_{r_1}(A_1)$.

In homalg, the inductive step of the above algorithm is implemented in the global function `CayleyDeterminant_Step(beta, d, p, q, s)` (`beta` is the element calculated in the previous step, i.e. β_{i+1} when calculating β_i, and `d` is the map represented by the matrix A_i). The calculation of v_J is done using the function `WedgeMatrixBaseImages` mentioned above. Note that this could be done more efficiently, since many subproducts are calculated several times for different sets J and could instead be reused. The function then finds the factor γ_J by simply dividing by the first non-zero component of β_{i+1}. Also note that the elements β_i are never really used as exterior power elements in the algorithm itself; only their components are accessed. For this reason, they are stored simply as lists.

The Cayley determinant itself is then calculated by the operation `CayleyDeterminant(C)`, which just goes through the morphisms in the complex, calculating the sequence r_i and calling `CayleyDeterminant_Step` to compute β_i.

8. Application to finite free resolutions

We still need to prove that certain complexes satisfy the conditions given for the complex (7). This requires some new tools:

Lemma 11. *Let* $(a_1, \ldots, a_n) \in R^n$ *be regular and* $J = \langle b_1, \ldots, b_m \rangle \subseteq R$ *a finitely generated ideal. If* $J = 0$ *in each localization* $R[1/a_i]$*, then* $J = 0$ *in* R*; and if* $(b_1, \ldots, b_m)$ *is regular in each localization* $R[1/a_i]$*, then* $(b_1, \ldots, b_m)$ *is regular in* R*.*

Proof. We can assume each a_i not to be a zero divisor. Then $x \in J$ implies $x = 0$ in each $R[1/a_i]$, which implies $\frac{a_i x}{a_i} = 0 \implies a_i x = 0$ and thus, because of the regularity of $(a_1, \ldots, a_n)$, we get $x = 0$ in R.

Now let $x \in R$ such that $xb_1 = \ldots = xb_m = 0$; this implies $x = 0$ in each localization, and hence $x = 0$ in R by the same argument as above. □

This directly implies the following lemma:

Lemma 12. *Let* $(x_1, \ldots, x_m) \in R^m$ *be regular and* $\operatorname{grade}(a; E) \geq k$ *in each localization* $R[1/x_i]$*. Then* $\operatorname{grade}(a; E) \geq k$ *in* R*.*

Two other statements are required:

Theorem 13. *(MacCoy) If* A *represents an injective linear map* $R^p \to R^q$*, then* $\Delta_p(A)$ *is regular.*

Proof. We look at the first column $a_1, \ldots, a_q$ of A. Since A is injective, $(a_1, \ldots, a_q)$ has to be regular. Thus, using Lemma 11, we just need to check $\Delta_p(A)$ over each $R[1/a_i]$. But in this case, the matrix A is equivalent to a matrix of the form

$$\begin{pmatrix} 1 & 0 \\ 0 & B \end{pmatrix},$$

where B is injective itself, and $\Delta_{p-1}(B) = \Delta_p(A)$. Thus, $\Delta_p(A)$ is regular by induction. □

Lemma 14. *If the sequence*

$$E \xrightarrow{A} F \xrightarrow{B} G \xrightarrow{C} H$$

is exact, and $a \in R$ *is* H*-regular, then*

$$E \xrightarrow{A} F \xrightarrow{B} G$$

is exact modulo $\langle a \rangle$*.*

Proof. Let $y \in F$ such that $By = 0$ modulo $\langle a \rangle$; i.e. there exists a $z \in G$ such that $By = az$. This implies $CBy = Caz = aCz = 0 \implies Cz = 0$, since a is H-regular. Hence, because the first complex is exact, there exists a $y_1 \in F$ such that $z = By_1$. We then have $B(y - ay_1) = 0$, which (again because of exactness) implies that $y - ay_1$ is in the image of A, i.e. y is in the image of A modulo $\langle a \rangle$. □

Now we can prove this useful theorem:

Theorem 15. *If the sequence*

$$0 \to F_m \xrightarrow{A_m} F_{m-1} \xrightarrow{A_{m-1}} F_{m-2} \to \cdots \to F_1 \xrightarrow{A_1} F_0,$$

with $F_i = R^{p_i}$*, is exact, then either the ring is trivial or we can define the sequence* $r_m := p_m, r_{m-1} := p_{m-1} - r_m, \ldots, r_0 := p_0 - r_1$ *with* $r_i \geq 0$ *and* $\operatorname{grade}(\Delta_{r_k}(A_k)) \geq k$*.*

Proof. By Theorem 13, $\Delta_{r_m}(A_m)$ is regular. Using Lemma 14, we have that

$$0 \to F_m \xrightarrow{A_m} F_{m-1} \xrightarrow{A_{m-1}} F_{m-2} \to \cdots \to F_1$$

is still exact modulo any regular element of $\Delta_{r_m}(A_m)$, i.e. $\Delta_{r_m}(A_m)$ is still regular and thus $\mathrm{grade}(\Delta_{r_m}(A_m)) \geq 2$. We can iterate this argument to get $\mathrm{grade}(\Delta_{r_m}(A_m)) \geq m$. Now let δ be an r_m-minor of A_m; then the matrix A_m is over $R[1/\delta]$ equivalent to a matrix of the form

$$\begin{pmatrix} I_{r_m} \\ B_m \end{pmatrix}.$$

The matrix A_{m-1} is then of the form $(0 \quad B_{m-1})$, which gives the exact sequence

$$R^{r_{m-1}} \xrightarrow{B_{m-1}} F_{m-2} \to \ldots \to F_1 \xrightarrow{A_1} F_0.$$

By induction, we then have $\mathrm{grade}(\Delta_{r_{m-1}}(A_{m-1})) = \mathrm{grade}(\Delta_{r_{m-1}}(B_{m-1})) \geq m-1$ and $\mathrm{grade}(\Delta_{r_i}(A_i)) \geq i$ for $i = m-2, \ldots, 1$. Since this holds in $R[1/\delta]$ for any δ and $\Delta_{r_m}(A_m)$ is regular, it follows in R via Lemma 12. □

This gives the following corollary:

Theorem 16. *Let $I = \langle a_1, \ldots, a_n \rangle$ be an ideal with a finite free resolution*

$$0 \to F_m \to \cdots \to F_1 \xrightarrow{(a_1,\ldots,a_n)} I \to 0,$$

with $F_m = R^{p_m}$, then the elements $a_1, \ldots, a_n$ have a greatest common divisor which is regular.

Proof. Using Theorem 15, the complex

$$F_m \to \cdots \to F_1 \xrightarrow{(a_1,\ldots,a_n)} R$$

satisfies the conditions to have a Cayley determinant. This gives a greatest common divisor of $\Delta_1(a_1, \ldots, a_n) = (a_1, \ldots, a_n)$. □

Thus, we really have a way to calculate greatest common divisors using the Cayley determinant: first compute a finite free resolution of the ideal using syzygies, and then its Cayley determinant. I implemented the homalg function `Gcd_UsingCayleyDeterminant` to do just this.

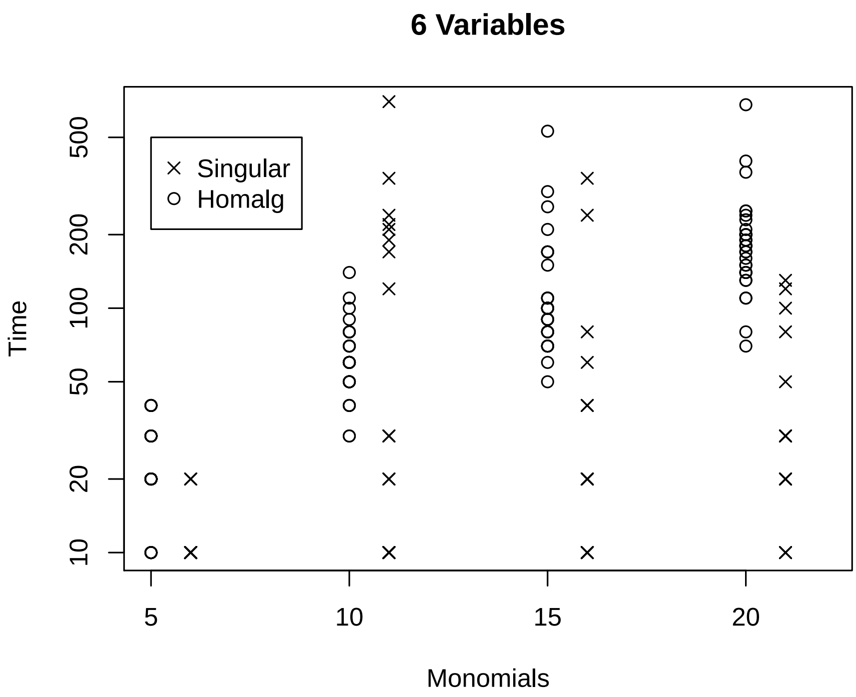
9. Performance measurements

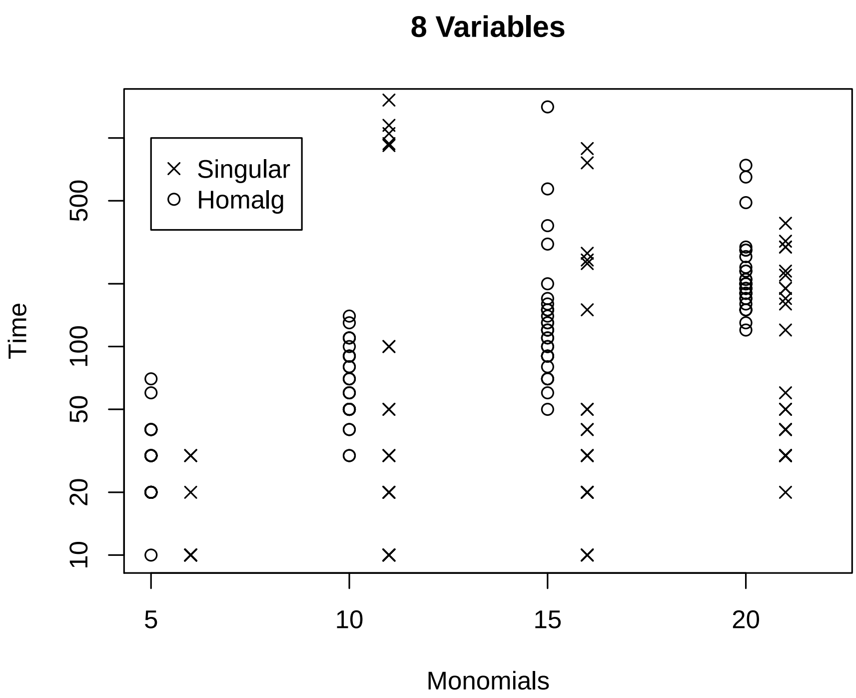
To get an idea of the performance characteristics of this algorithm, I conducted some quantitative comparisons with SINGULAR's `gcd` function. For several combinations of monomial count m and variable count v, polynomials were computed by generating m random monomials (per polynomial) of degree up to 5 and with variables $x_1, \ldots, x_v$ and adding them. These polynomials were split into triples f, g, h to get pairs fg, fh with non-trivial greatest common divisor. Then, the greatest common divisor of each of the resulting 100 pairs was computed using SINGULAR's `gcd` and using my implementation, but still using SINGULAR as the backend CAS for the syzygy calculation. Obviously, this methodology is not flawless, but it did at least yield some surprising first measurements: While SINGULAR's algorithm is consistently faster for low variable count, it became slower when handling some polynomials with 8 or 10 variables, while the Cayley determinant-based algorithm didn't show as severe slowdowns.

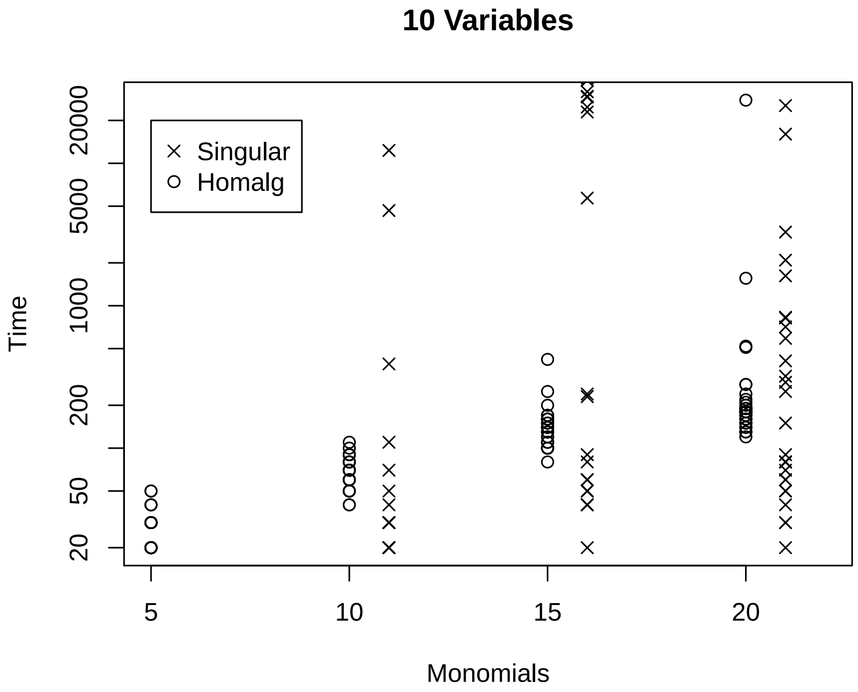
Variables	Monomials	Homalg mean	Singular mean	Homalg σ	Singular σ
6	5	23	6.2	10.1	6.8
8	5	29	7.0	12.6	9.5
10	5	28	2.3	8.7	4.3
6	10	65	152.0	23.6	290.8
8	10	72	496.7	29.0	1205.5
10	10	69	599.7	17.6	2368.2
6	15	129	235.7	95.6	786.4
8	15	186	1550.3	254.2	3901.7
10	15	146	13501.0	62.2	18508.3
6	20	200	312.0	114.7	1056.0
8	20	242	525.0	141.9	2264.3
10	20	1169	5346.0	5031.1	14096.8

TABLE 2. Measured gcd calculation times and standard deviations, in ms

The following figures show the distribution of the calculation times for 6, 8 and 10 variables.


6 Variables
Singular
Homalg
Time
500
200
100
50
20
10
5
10
15
20
Monomials


8 Variables
Singular
Homalg
Time
500
100
50
20
10
5
10
15
20
Monomials


10 Variables
Singular
Homalg
Time
20000
5000
1000
200
50
20
5
10
15
20
Monomials

Bibliography

[1] Mohamed Barakat, Florian Diebold, and Markus Lange-Hegermann. *The* `Modules` *package – A* `homalg` *based package for the Abelian category of finitely presented modules over computable rings*, 2007-2011. (`http://homalg.math.rwth-aachen.de/index.php/core-packages/modules`).

[2] Mohamed Barakat and Daniel Robertz. `homalg` – A meta-package for homological algebra. *J. Algebra Appl.*, 7(3):299–317, 2008. (`arXiv:math.AC/0701146`).

[3] Thierry Coquand and Claude Quitté. Constructive finite free resolutions. *manuscripta mathematica*, pages 1–15, 2011.

[4] The homalg project authors. *The* `homalg` *project*, 2003-2011. (`http://homalg.math.rwth-aachen.de/`).

[5] Douglas Geoffrey Northcott. *Finite free resolutions*. Cambridge Univ. Press, Cambridge [u.a.], 1976.