An Algorithm for the Traverso-Swan theorem on seminormal rings

Sami Barhoumi ([1]), Henri Lombardi ([2])

June 4, 2008

Abstract

We give an algorithm for an explicit implementation of Traverso-Swan's theorem, saying that a reduced ring $\mathbf{A}$ is seminormal if and only if the canonical map: $\operatorname{Pic}\mathbf{A} \to \operatorname{Pic}\mathbf{A}[x]$ is an isomorphism.

MSC 2000 : 13C10, 19A13, 14Q20, 03F65.

Keywords : Seminormal ring, Picard Group, Constructive Mathematics, Traverso-Swan theorem, Resultant ideal, Subresultant module.

1 Introduction

In [2] T. Coquand obtained a constructive proof of the fact that a reduced ring $\mathbf{A}$ is seminormal if and only if the canonical map:

$$\operatorname{Pic}\mathbf{A} \to \operatorname{Pic}\mathbf{A}[x]$$

is an isomorphism. This theorem is due to Swan [8], generalizing a result of Traverso [9].

We recall [8] that a ring $\mathbf{A}$ is seminormal if when $b^2 = c^3$ then there exists $a \in \mathbf{A}$ such that $b = a^3$ and $c = a^2$. This is a remarkably simple condition. Similarly the statement that the canonical map $\operatorname{Pic}\mathbf{A} \to \operatorname{Pic}\mathbf{A}[x]$ is an isomorphism can also be formulated in an elementary way. Swan's original definition includes that $\mathbf{A}$ is reduced, but, as noticed by Costa [4], reduceness follows from seminormality: if $d^2 = 0$ then $d^2 = 0^3 = 0$ and so there exists $a \in \mathbf{A}$ such that $a^3 = d$ and $a^2 = 0$. So $d = 0$.

When $\mathbf{A} \subseteq \mathbf{B}$ are commutative rings, the *seminormal closure* of $\mathbf{A}$ in $\mathbf{B}$ is the smallest subring $\mathbf{A}_1$ of $\mathbf{B}$ containing $\mathbf{A}$ such that if $x \in \mathbf{B}$, $x^2 \in \mathbf{A}_1$ and $x^3 \in \mathbf{A}_1$ then $x \in \mathbf{A}_1$.

In this paper, we give an algorithm for an explicit implementation of Traverso-Swan's theorem. More precisely let $\mathbf{C}$ be a reduced ring and $f_1, \dots, f_n, g_1, \dots, g_n$ polynomials in $\mathbf{C}[X]$ such that $f_1 \cdot g_1 + \cdots + f_n \cdot g_n = 1$, $f_1(0) = g_1(0) = 1$ and $f_i(0) = g_i(0) = 0$ for $i \geq 2$. Let $\mathbf{A}$ be the ring generated by the coefficients of $m_{ij} = f_i \times g_j$ and $\mathbf{B}$ the ring generated by the coefficients of f_i and g_j. We construct finitely many elements $c_1, \dots, c_m \in \mathbf{B}$ such that $c_{i+1}^2, c_{i+1}^3 \in \mathbf{A}[c_1, \dots, c_i]$ and $\mathbf{B} = \mathbf{A}[c_1, \dots, c_m]$.

[1] Équipe de Mathématiques, UMR CNRS 6623, UFR des Sciences et Techniques, Université de Franche-Comté, 25030 BESANCON cedex, FRANCE, email: sami.barhoumi@univ-fcomte.fr.

[2] Same address, email: henri.lombardi@univ-fcomte.fr.

2 First steps for Traverso-Swan's theorem on seminormality

In this section we recall some steps in the constructive method of T. Coquand [2].

To any commutative ring $\mathbf{A}$ one associates the group of projective modules of rank one equipped with tensor product as group operation. This is the Picard group $\mathrm{Pic}\,\mathbf{A}$ of the ring $\mathbf{A}$. We can represent any finitely generated projective module P over $\mathbf{A}$ as the image of an $n \times n$ idempotent matrix M. The module $P \simeq \mathrm{Im}\,M$ is of rank one if and only if $\det(\mathrm{I}_n + xM) = 1 + x$. Equivalently $\mathrm{Tr}\,M = 1$ and any 2×2 minor of M equals 0. If $M \in \mathbf{A}^{n\times n}$ represents a projective $\mathbf{A}$-module P of rank one, we use the notation

$$M \simeq_{\mathbf{A}} \mathrm{I}_{1,n} = \begin{pmatrix} 1 & 0_{1,n-1} \\ 0_{n-1,1} & 0_{n-1,n-1} \end{pmatrix}$$

for expressing that P is a free module over $\mathbf{A}$. Precisely we have:

Lemma 1 *Let M be a projection matrix of rank one over a ring $\mathbf{A}$. Then $M \simeq_{\mathbf{A}} \mathrm{I}_{1,n}$ if and only if there exist f_i, $g_j \in \mathbf{A}$ such that $m_{ij} = f_i g_j$ for each i, j. If we write f the column vector (f_i) and g the row vector (g_j) this can be written as $M = fg$. Furthermore the column vector f and the row vector g are uniquely defined up to a unit by these conditions: if we have other vectors f' and row g' such that $M = f'g'$ then there exists a unit u of $\mathbf{A}$ such that $f = uf'$ and $g' = ug$.*

Note that in the reverse way when we have a column vector f and a row vector g, if $gf = 1$, then the matrix $M = fg$ is a projection matrix of rank 1.

Theorem 2 (Traverso-Swan-Coquand)
Let k be a positive integer. A reduced ring $\mathbf{A}$ is seminormal if and only if the canonical map $\mathrm{Pic}\,\mathbf{A} \to \mathrm{Pic}\,\mathbf{A}[x_1, \ldots, x_k]$ is an isomorphism.

The "only if part" is based on a Schanuel example. The proof of the "if part" is much more difficult. In this paper we give an algorithm for the following particular case ($k = 1$).

Theorem 3 *Le $\mathbf{A}$ be a seminormal ring. Then the canonical map $\mathrm{Pic}\,\mathbf{A} \to \mathrm{Pic}\,\mathbf{A}[x]$ is an isomorphism.*

The first author will propose in a following paper a direct algorithmic proof of the implication "$\mathbf{A}$ seminormal implies $\mathbf{A}[x]$ seminormal". Combined with the present paper this will give an algorithm for the general case (Theorem 2).

First steps in Coquand's proof are based on the following lemmas.

Lemma 4 *If $\mathbf{A}$ is a reduced ring, then the canonical map $\mathrm{Pic}\,\mathbf{A} \to \mathrm{Pic}\,\mathbf{A}[x]$ is an isomorphism if and only if for any $n \times n$ projection matrix $M(x) = (m_{ij}(x))$ of rank one over $\mathbf{A}[x]$ such that $M(0) = \mathrm{I}_{1,n}$, there exist $f_i, g_j \in \mathbf{A}[x]$ such that $f(0) = g(0) = 1$ and $m_{ij} = f_i g_j$.*

Let us recall that a ring is zero-dimensional and reduced if and only if every element a has a quasi-inverse, i.e. an element $a^\bullet$ such that

$$a^2 a^\bullet = a, \quad \text{and} \quad a(a^\bullet)^2 = a^\bullet.$$

Such a ring is often called a Von Neuman regular ring.

In constructive mathematics we say that a ring is a discrete field if we have the disjunction "any element is zero or invertible" in an explicit way (see [7] for basic concepts of constructive algebra). A discrete field is zero-dimensional and reduced.

Lemma 5 *If* $\mathbf{A}$ *is a reduced ring then* $\mathbf{A}$ *has a reduced zero-dimensional extension.*

For Lemma 5, if $\mathbf{A}$ is an integral domain, we can take the fraction field of $\mathbf{A}$.

Lemma 6 *If* $\mathbf{C}$ *is a reduced zero-dimensional ring, then any finitely generated projective module of rank one over* $\mathbf{C}[x]$ *is free.*

In case $\mathbf{C}$ is a discrete field we can use the following procedure for Lemma 6. We start with a projection matrix of rank one $M(x) = (m_{ij})$ such that $M(0) = \mathrm{I}_{1,n}$. We take for f_1 the gcd of the first row of M in $\mathbf{C}[x]$ with $f_1(0) = 1$. Then $g_j = \frac{m_{1j}}{f_1}$, $f_i = \frac{m_{i1}}{g_1}$.

Since lemmas 4, 5 and 6 are relatively easy, the more difficult part in the proof of Theorem 3 is given by Theorem 8 below.

Context: Let $\mathbf{B}$ be a reduced ring and f_i, g_i $(i = 1, \ldots, n)$ polynomials in $\mathbf{B}[x]$ such that $\sum f_i g_i = 1$, $f_1(0) = g_1(0) = 1$ and $f_i(0) = g_i(0) = 0$ for $i \geq 2$. Let $m_{ij}(x) = f_i(x)g_j(x)$. Let $\mathbf{A}$ be the ring generated by the coefficients of m_{ij}'s. We assume also that $\mathbf{B}$ is generated by the coefficients of f_i and g_i. We denote by $\mathbf{A}_1$ the seminormal closure of $\mathbf{A}$ in $\mathbf{B}$.

Remark 7 *Let us explain how to come within Context if we start with a projection matrix of rank one* $M(x) = (m_{ij})$ *such that* $M(0) = \mathrm{I}_{1,n}$*. Let* $\mathbf{A}$ *be the ring generated by the coefficients of* m_{ij}*'s. We consider a reduced zero-dimensional ring* $\mathbf{C}$ *containing* $\mathbf{A}$ *(Lemma 5). We find polynomials* f_i *and* g_i *in* $\mathbf{C}[x]$ *such that* $f_1(0) = 1 = g_1(0)$ *and* $m_{ij} = f_i g_j$ *for any* i, j *(Lemma 6). Then* $\mathbf{B}$ *is the ring generated by the coefficients of* f_i*'s and* g_i*'s. As already explained, in case the matrix has its coefficients in an integral ring this procedure is particularly simple.*

Using Lemma 4 and the previous remark (which is based on constructive proofs of Lemmas 5 and 6) it is clear that Theorem 3 is a consequence of the following more precise statement.

Theorem 8 *Within Context,* $\mathbf{A}_1 = \mathbf{B}$*. More precisely there are finitely many elements* $c_1, \ldots, c_m \in \mathbf{B}$ *such that* $c_{i+1}^2, c_{i+1}^3 \in \mathbf{A}[c_1, \ldots, c_i]$ $(i \in \{1, \ldots, m-1\})$ *and* $\mathbf{B} = \mathbf{A}[c_1, \ldots, c_m]$.

Lemma 9 *Within Context, the coefficients of* f_i *and* g_j *are integral over* $\mathbf{A}$*. So* $\mathbf{B}$ *is finite as an* $\mathbf{A}$*-module .*

Indeed, if u is a coefficient of f_i, it follows from $f_i g_j \in \mathbf{A}[x]$ that $ug_j(0)$ is integral over $\mathbf{A}$ for all j. This is a consequence of Kronecker's theorem [3, 5, 6] that states that if $P_1P_2 = Q \in \mathbf{A}[x]$ then any product u_1u_2, where u_i is a coefficient of P_i, is integral over the ring generated by the coefficients of Q. Since $g_1(0) = 1$, this implies that u is integral over $\mathbf{A}$.

In the sequel of the paper we explain how to get algorithmically Theorem 8.

In section 3 we give some preliminary lemmas for this construction. In section 4 we give the algorithm for a 2×2 projection matrix of rank one. In section 5 we give the general algorithm for an $n \times n$ projection matrix of rank one.

3 Preliminary Lemmas

Lemma 10 *Let $c \in \mathbf{B}$ and $m \in \mathbb{N}$ such that $c^n \in \mathbf{A}_1$ for any $n \geq m$, then $c \in \mathbf{A}_1$.*

Proof For example let $m = 2^4 = 16$. We have following:
since c^{16} and $c^{24} \in \mathbf{A}_1$ then $c^8 \in \mathbf{A}_1$, since c^{18} and $c^{27} \in \mathbf{A}_1$ then $c^9 \in \mathbf{A}_1$, and so on for any $n \geq 8$, $a^n \in \mathbf{A}_1$. Briefly we can pass from 2^4 to 2^3. In the same way we pass from 2^3 to 2^2, and from 2^2 to 2. Thus c^2 and $c^3 \in \mathbf{A}_1$, so $c \in \mathbf{A}_1$. □

Lemma 11 $\mathbf{A}$[*coefficients of* f_1] $= \mathbf{B}$

Proof Let $\mathbf{B}'$ be the ring generated by $\mathbf{A}$ and the coefficients of f_1. We have $m_{1j} = f_1 g_j$, $f_1(0) = 1$. Suppose that $\deg\, m_{1j} \leq d$. We divide m_{1j} by f_1 by ascending powers, we obtain $m_{1j} = q f_1 + x^{d+1} h$, $q,\, h \in \mathbf{A}[x]$. Necessarily $h = 0$, $q = g_j$ and thus the coefficients of g_j are polynomial combinations of those of m_{1j} and f_1. It follows that $g_j \in \mathbf{B}'[x]$. Since $g_1 \in \mathbf{B}'[x]$ we obtain in a similar way that $f_i \in \mathbf{B}'[x]$. So $\mathbf{B} = \mathbf{B}'$. □

Example 12 *Let $n = 2$, $f_1 = 1+ax+bx^2$, $f_2 = cx+dx^2$, $g_1 = 1+ex+fx^2$, $g_2 = gx+hx^2$, $m_{11} = f_1 g_1$, $m_{12} = f_1 g_2$, $m_{21} = f_2 g_1$, $m_{22} = f_2 g_2$. We have $\mathbf{B} = \mathbf{A}[a,\, b]$, and a, b are integral over $\mathbf{A}$.*

Lemma 13 *If $a \in \mathbf{A}$ and $af_1 \in \mathbf{A}[x]$ then there exists $k \in \mathbb{N}$ such that $a^k \mathbf{B} \subseteq \mathbf{A}$.*

Proof We have $\mathbf{B} = \mathbf{A}[b_1, \ldots, b_r]$ where $f_1 = 1 + b_1 x + \cdots + b_r x^r$ (Lemma 11). Every b_i is integral over $\mathbf{A}$. Let d_i be the degree of an integral dependence relation of b_i. Then $\mathbf{B} = \sum \mathbf{A} b^\delta$, with $b^\delta = b_1^{\delta_1} \ldots b_r^{\delta_r}$, $0 \leq \delta_i < d_i$. (δ means $\delta_1, \ldots, \delta_r$ and b^δ is a pure notation). If $af_1 \in \mathbf{A}[x]$ and $\sum(d_i - 1) = k$, then $a^k b^\delta = (ab_1)^{\delta_1} \cdots (ab_r)^{\delta_r} \cdot a^{k - \sum \delta_i}$ with $k - \sum \delta_i \geq 0$. So $a^k b^\delta \in \mathbf{A}$. Thus $a^k \mathbf{B} \subseteq \mathbf{A}$. □

Lemma 14 *If $a \in \mathbf{A}$ and $a^m \mathbf{B} \subseteq \mathbf{A}$ for some $m \in \mathbb{N}$, then $a\mathbf{B} \subseteq \mathbf{A}_1$.*

Proof For $b \in \mathbf{B}$ we have $(ab)^m \mathbf{B} \subseteq \mathbf{A}$. This implies that $(ab)^n \in \mathbf{A}_1$ for any $n \geq m$. Applying Lemma 10, we get $a\mathbf{B} \subseteq \mathbf{A}_1$. □

Lemma 15 *Let $a \in \mathbf{B}$ and $\ell \in \mathbb{N}$ such that $a^\ell f_1 \in \mathbf{A}[x]$, then $\sqrt{a\mathbf{B}} \subseteq \mathbf{A}_1$.*

Proof This follows from Lemma 13 and Lemma 14. □

Fact 16 *Let $\mathbf{C} \subseteq \mathbf{B}$ be two rings and $\mathcal{J}$ an ideal of $\mathbf{B}$. Then $\mathbf{C} + \mathcal{J}$ is a ring, $\mathcal{J}$ is an ideal of $\mathbf{C} + \mathcal{J}$, $\mathbf{C} \cap \mathcal{J}$ is an ideal of $\mathbf{C}$, and the isomorphism of $\mathbf{C}$-modules $(\mathbf{C} + \mathcal{J})/\mathcal{J} \simeq \mathbf{C}/(\mathbf{C} \cap \mathcal{J})$ is an isomorphism of rings.*

Lemma 17 *With Lemma 15 hypotheses, we have $\mathbf{A} + \sqrt{a\mathbf{B}} \subseteq \mathbf{A}_1$. Let $\mathcal{J} = \sqrt{a\mathbf{B}}$,*

$$\widetilde{\mathbf{A}} = (\mathbf{A} + \mathcal{J})/\mathcal{J} \subseteq \mathbf{A}_1/\mathcal{J} \quad \text{and} \quad \widetilde{\mathbf{B}} = \mathbf{B}/\mathcal{J},$$

then $\mathbf{A}_1/\mathcal{J}$ is the seminormal closure of $\widetilde{\mathbf{A}}$ in $\widetilde{\mathbf{B}}$.

Proof Let $\mathbf{C}$ be the seminormal closure of $\widetilde{\mathbf{A}}$ in $\widetilde{\mathbf{B}}$. We write $\mathbf{C} = \mathbf{A}_2/\mathcal{J}$ with $\mathcal{J} \subseteq \mathbf{A}_2$ as a subring of $\mathbf{B}/\mathcal{J}$. It is clear that $\mathbf{A}_1 \subseteq \mathbf{A}_2$. Let $x \in \mathbf{A}_2$ and assume first that $\bar{x}^2, \bar{x}^3 \in \widetilde{\mathbf{A}}$. Then $x^2, x^3 \in \mathbf{A}_1$, so $x \in \mathbf{A}_1$. Reasoning inductively, we replace $\mathbf{A}$ by $\mathbf{A}[x]$. Since any element in $\mathbf{C}$ can be reached in a finite number of steps, we see that $\mathbf{A}_2 = \mathbf{A}_1$. □

The concrete consequence of Lemma 17 for our computation is that, whenever we find an $a \in \mathbf{B}$ such that $a^\ell f_1 \in \mathbf{A}[x]$ for some integer ℓ, we are allowed to replace $\mathbf{A}$ and $\mathbf{B}$ by $\widetilde{\mathbf{A}}$ and $\widetilde{\mathbf{B}}$. Indeed, it is clear that hypotheses of Context remain true for these rings, and if forthcoming computations show that the seminormal closure of $\widetilde{\mathbf{A}}$ in $\widetilde{\mathbf{B}}$ is equal to $\widetilde{\mathbf{B}}$, Lemma 17 says that $\mathbf{A}_1 = \mathbf{B}$.

In short “we are allowed to continue the computation modulo $\mathcal{J}$”.

4 The Case 2×2

Resultant and subresultants

For two polynomials $P = a_p x^p + \cdots + a_0$ and $Q = b_q x^q + \cdots + b_0$ of formal degrees p and q, we denote by $\mathrm{Res}_x(P, p, Q, q)$ the resultant of P and Q; that is to say the determinant of the Sylvester Matrix:

$$\mathrm{Syl}_x(P,p,Q,q) \;=\; \begin{array}{c} \begin{pmatrix} a_0 & & & & & b_0 & & & \\ a_1 & a_0 & & & & b_1 & b_0 & & \\ \vdots & a_1 & \ddots & & & & b_1 & \ddots & \\ \vdots & & \ddots & \ddots & & \vdots & & \ddots & b_0 \\ a_p & & & \ddots & a_0 & & \vdots & & b_1 \\ & a_p & & & a_1 & b_q & & & \\ & & \ddots & & \vdots & & b_q & & \vdots \\ & & & \ddots & \vdots & & & \ddots & \\ & & & & a_p & & & & b_q \end{pmatrix} \\ \underbrace{\hphantom{a_0\;a_0\;\ddots\;\ddots\;a_0}}_{q \text{ columns}} \quad \underbrace{\hphantom{b_0\;b_0\;\ddots\;b_0}}_{p \text{ columns}} \end{array}$$

First we recall well known identities (see e.g., [1] chapter 3).

Fact 18 *Let $P, Q, Q_1, R, U \in \mathbf{A}[x]$ of formal degrees p, q, q_1, r, u. Assume that P is monic. Then*

- $\mathrm{Res}_x(R, r, Q, q) = (-1)^{qr} \mathrm{Res}_x(Q, q, R, r)$,
- $\mathrm{Res}_x(R, r, Q.Q_1, q + q_1) = \mathrm{Res}_x(R, r, Q, q)\mathrm{Res}_x(R, r, Q_1, q_1)$,
- $\mathrm{Res}_x(R, r, Q + UR, q) = \mathrm{Res}_x(R, r, Q, q)$ *if* $q \geq u + r$.
- $\mathrm{Res}_x(P, p, Q, q') = \mathrm{Res}_x(P, p, Q, q)$ *if* $q' \geq q$. *So when P is monic of degree p we can use the short notation* $\mathrm{Res}_x(P, p, Q)$.
- $\mathrm{Res}_x(P, p, Q + UP) = \mathrm{Res}_x(P, p, Q)$,

We recall now the definition of *subresultant polynomials.* Let $d = min(p,\, q)$. For any i, $(0 \leq i < d)$, the *subresultant of P and Q in degree i* is the determinant of the square matrix :

$$\begin{array}{c} \begin{pmatrix} a_p & & & & b_q & & & \\ \vdots & \ddots & & & \vdots & \ddots & & \\ \vdots & & & a_p & \vdots & & & b_q \\ \vdots & & & \vdots & \vdots & & & \vdots \\ a_{i+1-(q-i-1)} & & & a_{i+1} & b_{i+1-(p-i-1)} & & & b_{i+1} \\ x^{q-i-1}P(x) & \cdots & \cdots & P(x) & x^{p-i-1}Q(x) & \cdots & \cdots & Q(x) \end{pmatrix} \\ \underbrace{\hphantom{x^{q-i-1}P(x)\;\cdots\;\cdots\;P(x)}}_{(q-i) \text{ columns}} \quad \underbrace{\hphantom{x^{p-i-1}Q(x)\;\cdots\;\cdots\;Q(x)}}_{(p-i) \text{ columns}} \end{array}$$

We denote it by $\mathrm{Sres}_{i,x}(P, p, Q, q)$ or $\mathrm{Sres}_i(P, p, Q, q)$. It is easily shown that we can take $\mathrm{Sres}_i(P, p, Q, q)$ of formal degree i and that $\mathrm{Sres}_0(P, p, Q, q) = \mathrm{Res}(P, p, Q, q)$. Moreover each $\mathrm{Sres}_i(P, p, Q, q)$ belongs to the ideal $\langle P, Q \rangle$.

Examples 19 *Let* $p = 3$, $q = 4$, *and* $i = 2$ *then*

$$\mathrm{Sres}_{2,x}(P,3,Q,4) = \begin{vmatrix} a_3 & 0 & b_4 \\ a_2 & a_3 & b_3 \\ xP(x) & P(x) & Q(x) \end{vmatrix}.$$

Let $p = 4$, $q = 5$ *and* $i = 2$ *then*

$$\mathrm{Sres}_{3,x}(P,4,Q,5) = \begin{vmatrix} a_4 & 0 & 0 & b_5 & 0 \\ a_3 & a_4 & 0 & b_4 & b_5 \\ a_2 & a_3 & a_4 & b_3 & b_4 \\ a_1 & a_2 & a_3 & b_2 & b_3 \\ x^2P(x) & xP(x) & P(x) & xQ(x) & Q(x) \end{vmatrix}.$$

The following fact is a particular case of Theorem 80 (page 239) of [1].

Fact 20 *Let* P *be a monic polynomial of degree* p *and* Q_1, Q_2 *polynomials of formal degrees* q_1, q_2. *Let* $Sr_p = \mathrm{Sres}_p(PQ_1, p+q_1, PQ_2, p+q_2)$, *let* sr_p *be the coefficient of degree* p *of* Sr_p. *Then* $sr_p = \mathrm{Res}(Q_1, q_1, Q_2, q_2)$ *and* $sr_p \cdot P = Sr_p$.

Proof of Theorem 8 (case $n = 2$)

Within Context, with $n = 2$, we consider f_i and g_i as being of formal degree d. We define the formal reciprocal polynomials in degree d, $F_i = x^d f_i(\frac{1}{x})$ and $G_i = x^d g_i(\frac{1}{x})$. We remark that F_i and G_i can be taken of formal degree d for $i = 1$ and of formal degree $d-1$ for $i > 1$. Moreover F_1 and G_1 are monic, and $F_1G_1 + F_2G_2 = x^{2d}$.

For example with $d = 2$, $f_1 = 1 + ax + bx^2$, $f_2 = cx + kx^2$, $g_1 = 1 + ex + fx^2$, $g_2 = gx + hx^2$, we have $F_1 = b + ax + x^2$, $F_2 = k + cx$, $G_1 = f + ex + x^2$, $G_2 = h + gx$.

Applying Fact 20, we get

$$sr_d \cdot F_1 = \mathrm{Sres}_d(F_1G_1, 2d, F_1G_2, 2d-1) \in \mathbf{A}[x].$$

So *srd* satisfies the hypothesis of Lemma 15, with $\ell = 1$.

Applying Lemma 17 we may reason modulo $\sqrt{sr_d\mathbf{B}}$, i.e. we may suppose that $sr_d = 0$ and kill nilpotent elements. Moreover $sr_d = \mathrm{Res}(G_1, d, G_2, d-1)$.

We need the following lemma.

Lemma 21 *Let* a *be the constant coefficient of* F_i *or* G_i. *Then* $a^{2d} \equiv 0 \bmod sr_d$.

Proof E.g., let a_i the constant coefficient of G_i. We have $sr_d = \mathrm{Res}_x(G_1, d, G_2, d-1) = 0$. Moreover $f_1g_1 + f_2g_2 = 1$ gives $F_1G_1 + F_2G_2 = x^{2d}$. Then we get (because G_1 is monic)

$$\begin{aligned} a_1^{2d} &= \mathrm{Res}(G_1, d, x^{2d}, 2d) &&= \mathrm{Res}(G_1, d, F_1G_1 + F_2G_2, 2d) \\ &= \mathrm{Res}(G_1, d, F_2G_2, 2d) &&= \mathrm{Res}(G_1, d, F_2G_2, 2d-2) \\ &= \mathrm{Res}(G_1, d, G_2, d-1)\mathrm{Res}(G_1, d, F_2, d-1) &&\equiv 0 \bmod sr_d \end{aligned}$$

In a similar way (because $2d \geq 2d-2$):

$$\begin{aligned} a_2^{2d} &= \mathrm{Res}(G_2, d-1, x^{2d}, 2d) &&= \mathrm{Res}(G_2, d-1, F_1G_1 + F_2G_2, 2d) \\ &= \mathrm{Res}(G_2, d-1, F_1G_1, 2d) &&= \mathrm{Res}(G_2, d-1, G_1, d)\mathrm{Res}(G_2, d-1, F_1, d) \\ &\equiv 0 \bmod sr_d \end{aligned}$$

□

Conclusion: When we consider the case of f_i and g_i with formal degree d, $(1 \le i \le 2)$, any of their coefficients in degree d, let us denote a, verify $a^k \cdot \mathbf{B} \subseteq \mathbf{A}$ for some $k \in \mathbb{N}$ which we are able to clarify according to d.
More precisely the coefficients of f_1 of degree ≥ 1 verify an integral dependence relation of degree $\binom{2d}{d}$ over $\mathbf{A}$. Using the proof of Lemma 13 we get $sr_d^k \cdot \mathbf{B} \subseteq \mathbf{A}$ with $k = d\left(\binom{2d}{d} - 1\right)$. Since $a^{2d} \equiv 0 \mod sr_d$ in $\mathbf{A}$ we get $a^\ell \cdot \mathbf{B} \subseteq \mathbf{A}$, with $\ell = 2d^2\left(\binom{2d}{d} - 1\right)$. E.g., for $d = 3$, $\ell = 342$.
This gives a first approximation of $\mathbf{A}_1$ by $\mathbf{A}' = \mathbf{A} + \sqrt{\mathcal{I}}$ where $\mathcal{I}$ is the ideal of $\mathbf{B}$ generated by the coefficients of degree d of f_i's and g_i's. Since we are allowed to reason modulo $\sqrt{\mathcal{I}}$, we finish the algorithm by induction on d.

5 Generalization to the case $n \times n$

In this section we generalize the algorithm to the case of a matrix of size $n \times n$.

Resultant ideal and subresultant modules

In this paragraph we consider $C_0, C_1, \ldots, C_r \in \mathbf{A}[x]$ and assume that C_0 is monic of degree d.

For two polynomials P and Q of $\mathbf{A}[x]$, with Q monic we denote by $\mathrm{Rem}_x(P,Q)$ (or $\mathrm{Rem}(P,Q)$ if there is no ambiguity) the remainder of the euclidean division of P by Q. Now we recall the definition of the generalized Sylvester matrix.

Definition 22 *The* generalized Sylvester matrix *associated to the polynomials* $C_0, C_1, \ldots, C_r \in \mathbf{A}[x]$, *denoted by* $\mathrm{Syl}_x(C_0, d, C_1, \ldots, C_r)$ *is the matrix with the following columns:* $\mathrm{Rem}(C_1, C_0)$, …, $\mathrm{Rem}(C_r, C_0)$, …, $\mathrm{Rem}(x.C_1, C_0)$, …, $\mathrm{Rem}(x.C_r, C_0)$, …, $\mathrm{Rem}(x^{d-1}.C_1, C_0)$, …, $\mathrm{Rem}(x^{d-1}.C_r, C_0)$ *in the basis* $(x^{d-1}, \ldots, x, 1)$.

Fact 23 *Let* $A_d = \mathbf{A}[x]_d$ *be the* $\mathbf{A}$*-module of polynomials of degree* $< d$*, with basis* $(x^{d-1}, \ldots, x, 1)$ *and* $\varphi : \mathbf{A}^{dr} \longrightarrow A_d$ *the* $\mathbf{A}$*-linear map given by the matrix* $S = \mathrm{Syl}_x(C_0, d, C_1, \ldots, C_r)$. *Then* $\langle C_0, \ldots, C_r\rangle \cap A_d = \mathrm{Im}\,\varphi$.

Example 24 *Let* $C_0(x) = x^3 + 3x^2 + 4$, $C_1(x) = 4x^2 + 5x + 3$, $C_2(x) = -3x^2 + 2x + 3$, $C_3(x) = 2x^2 - x + 7$ *then*

$$\mathrm{Syl}_x(C_0, 3, C_1, C_2, C_3) = \begin{pmatrix} 4 & -3 & 2 & -7 & 11 & -7 & 20 & -27 & -16 \\ 5 & 2 & -1 & -1 & 6 & 5 & -9 & 1 & -1 \\ 3 & 3 & 7 & -16 & 12 & -8 & 28 & -44 & 28 \end{pmatrix}. \quad (1)$$

Remark 25 *We remark that* $\mathrm{Syl}_x(C_0, d, C_1, \ldots, C_r)$ *is a matrix of* d *rows and* $d.r$ *columns. Moreover if* $r = 1$ *the determinant of the matrix is equal to the resultant of* C_0 *and* C_1.

Definition 26 *Let* M *be a matrix in* $\mathbf{A}^{m\times n}$*, the* determinantal ideals $\mathcal{D}_k(M)$ *of the matrix* M *are the ideals generated by the minors of size* k *of the matrix* M*, with* $0 \le k \le \min(m, n)$.

Definition 27 *We define the* resultant ideal *of* $C_0, C_1, \ldots, C_r$*, denoted by* $\mathrm{Ires}_x(C_0, d, C_1, \ldots, C_r)$*: this is* $\mathcal{D}_d(\mathrm{Syl}_x(C_0, d, C_1, \ldots, C_r))$.

The importance of the resultant ideal comes from the fact it is equal to the elimination ideal, up to radical.

Lemma 28 *Let C_0 be a monic polynomial of degree d. Let $\mathcal{I}$ be the elimination ideal $\langle C_0, C_1, \ldots, C_r\rangle \cap \mathbf{A}$. Then*

$$\mathcal{I}^d \subseteq \mathrm{Ires}_x(C_0, d, C_1, \ldots, C_r) \subseteq \mathcal{I}.$$

Proof It is clear that $\mathrm{Ires}_x(C_0, d, C_1, \ldots, C_r) \subseteq \mathcal{I}$. Let $S = \mathrm{Syl}_x(C_0, d, C_1, \ldots, C_r)$. Let $y_i \in \mathcal{I} \cap \mathbf{A}$ $(1 \le i \le d)$. Then $y_i x^{i-1} \in \mathcal{I} \cap A_d = \mathrm{Im}\, S$ (Fact 23). This means that $\mathrm{Diag}(y_1, \ldots, y_d) = SH$ for some matrix H. Thus, by the Binet-Cauchy formula, $y_1 y_2 \cdots y_d$ (the determinant of $\mathrm{Diag}(y_1, \ldots, y_d)$) is in $\mathrm{Ires}_x(C_0, d, C_1, \ldots, C_r)$. □

Lemma 29

1. *Let $P \in \langle C_0, C_1, \ldots, C_r\rangle$. Then*

$$\mathrm{Res}_x(C_0, d, P) \in \mathrm{Ires}_x(C_0, d, C_1, \ldots, C_r).$$

2. *(conjecture) More generally consider the "generic" case where the coefficients of C_0, C_1, ..., C_r are indeterminates over a ring $\mathbf{C}$. So $\mathbf{A} = \mathbf{C}[\text{coeffs of } C_i's]$. Then*

$$\mathrm{Ires}_x(C_0, d, C_1, \ldots, C_r) = \langle C_0, C_1, \ldots, C_r\rangle \cap \mathbf{A}.$$

Proof
1) follows from 2): since $\mathrm{Res}_x(C_0, d, P, p)$ belongs to $\langle C_0, C_1, \ldots, C_r\rangle \cap \mathbf{A}$ in the generic case, it can be expressed as a member of $\mathrm{Ires}_x(C_0, d, C_1, \ldots, C_r)$ in the generic case. It remains to specialize this result.
Since we did not find a proof of 2) we give also a direct proof of 1).
For each $k < d$ we can write $Px^k = C_0 Q_k + \mathrm{Rem}_x(Px^k, C_0)$. The remainder is in $\langle C_0, \ldots, C_r\rangle \cap \mathbf{A}[x]_d$. So it is a linear combination of the columns of $S = \mathrm{Syl}_x(C_0, d, C_1, \ldots, C_r)$. So $\mathrm{Syl}_x(C_0, d, P) = ST$ for a suitable matrix T. We conclude by the Binet-Cauchy formula. □

We recall now the definition of the *subresultant modules.*

Let $k < d$. We make the following transformations in the Sylvester matrix $\mathrm{Syl}_x(C_0, d, C_1, \ldots, C_r)$:

- we suppress rows with degree $< k$,
- we suppress columns $\mathrm{Rem}(x^j.C_i, C_0)$ when $j > d - k - 1$,
- we replace the last row (corresponding to degree k) by the sequence $\mathrm{Rem}(C_1, C_0)$, ..., $\mathrm{Rem}(C_r, C_0)$, $\mathrm{Rem}(x.C_1, C_0)$, ..., $\mathrm{Rem}(x.C_r, C_0)$, ..., $\mathrm{Rem}(x^{d-k-1}.C_1, C_0)$, ..., $\mathrm{Rem}(x^{d-k-1}.C_r, C_0)$.

Then we obtain a matrix of size $(d-k) \times (d-k).r$ denoted $\mathrm{Syl}_{k,x}(C_0, d, C_1, \ldots, C_r)$.

Example 30 *We consider the matrix $\mathrm{Syl}_x(C_0, 3, C_1, C_2, C_3)$ of Example 24 and $k = 1$. If we suppress rows with degree < 1, and columns $\mathrm{Rem}(x^j.C_i, C)$ when $j > d - k - 1 = 1$ we obtain the matrix*

$$\begin{pmatrix} 4 & -3 & 2 & -7 & 11 & -7 \\ 5 & 2 & -1 & -1 & 6 & 5 \end{pmatrix}.$$

Finally we replace the last row by the vector $(C_1, C_2, C_3, r_1, r_2, r_3)$ *with* $r_1 = \mathrm{Rem}(xC_1, C_0)$, $r_2 = \mathrm{Rem}(x.C_2, C_0)$, $r_3 = \mathrm{Rem}(x.C_3, C_0)$. *Then*

$$\mathrm{Syl}_{1,x}(C_0, d, C_1, C_2, C_3) = \begin{pmatrix} 4 & -3 & 2 & -7 & 11 & -7 \\ C_1 & C_2 & C_3 & r_1 & r_2 & r_3 \end{pmatrix}.$$

In a similar way

$$\mathrm{Syl}_{0,x}(C_0, 3, C_1, C_2, C_3) = \begin{pmatrix} 4 & -3 & 2 & -7 & 11 & -7 & 20 & -27 & -16 \\ 5 & 2 & -1 & -1 & 6 & 5 & -9 & 1 & -1 \\ C_1 & C_2 & C_3 & r_1 & r_2 & r_3 & r'_1 & r'_2 & r'_3 \end{pmatrix}. \quad (2)$$

with $r'_1 = \mathrm{Rem}(x^2.C_1, C_0)$, $r'_2 = \mathrm{Rem}(x^2.C_2, C_0)$ *and* $r'_3 = \mathrm{Rem}(x^2.C_3, C_0)$

Definition 31 *For* $k < d$, *the subresultant module of degree* k *associated to the polynomials* $C_0, C_1, \ldots, C_r$, *denoted by* $\mathrm{Mres}_{k,x}(C_0, d, C_1, \ldots, C_r)$ *is the* $\mathbf{A}$*-module generated by the maximal minors of* $\mathrm{Syl}_{k,x}(C_0, d, C_1, \ldots, C_r)$.

Note that the generators of this module are polynomials with formal degree k. Remark also that comparing matrices (1) and (2) we obtain the equality

$$\mathrm{Mres}_{0,x}(C_0, d, C_1, \ldots, C_r) = \mathrm{Ires}_x(C_0, d, C_1, \ldots, C_r).$$

Lemma 32 *If* P *is monic of degree* p, *then*

$$\mathrm{Mres}_{p,x}(P.C_0, p + d, P.C_1, \ldots, P.C_r) = \mathrm{Ires}_x(C_0, d, C_1, \ldots, C_r) \cdot P.$$

First we give an example.

Example 33 *Let us first start by an example for a polynomial* P *of degree* 1. *Let* $P(x) = x - 2$, *and* C_0, C_1, C_2, C_3 *as in Example 24. The matrix* $\mathrm{Syl}_{1,x}(PC_0, 3+1, PC_1, PC_2, PC_3)$ *is equal to*

$$\begin{pmatrix} 4 & -3 & 2 & -7 & 11 & -7 & 20 & -27 & -16 \\ -3 & 8 & -5 & 13 & 28 & 19 & -49 & 55 & 31 \\ PC_1 & PC_2 & PC_3 & Pr_1 & Pr_2 & Pr_3 & Pr'_1 & Pr'_2 & Pr'_3 \end{pmatrix}.$$

We subtract from the second row (-2) *times the first, we obtain the matrix*

$$\begin{pmatrix} 4 & -3 & 2 & -7 & 11 & -7 & 20 & -27 & -16 \\ 5 & 2 & -1 & -1 & 6 & 5 & -9 & 1 & -1 \\ PC_1 & PC_2 & PC_3 & Pr_1 & Pr_2 & Pr_3 & Pr'_1 & Pr'_2 & Pr'_3 \end{pmatrix}. \quad (3)$$

Comparing this matrix to $\mathrm{Syl}_{0,x}(C_0, 3, C_1, C_2, C_3)$ *given in Equation (2) we see that it is the same one, except for the last row which is multiplied by* P. *In particular, any maximal minor of the matrix* $\mathrm{Syl}_{1,x}(PC_0, 3+1, PC_1, PC_2, PC_3)$ *can be written as a product of* P *and a maximal minor of* $\mathrm{Syl}_x(C_0, 3, C_1, C_2, C_3)$, *for instance*

$$\begin{vmatrix} 4 & -3 & 2 \\ 5 & 2 & -1 \\ PC_1 & PC_2 & PC_3 \end{vmatrix} = P \begin{vmatrix} 4 & -3 & 2 \\ 5 & 2 & -1 \\ C_1 & C_2 & C_3 \end{vmatrix} = P \begin{vmatrix} 4 & -3 & 2 \\ 5 & 2 & -1 \\ 3 & 3 & -7 \end{vmatrix}.$$

This implies $\mathrm{Mres}_{1,x}(P.C_0, 3+1, P.C_1, PC_2, P.C_3) = \mathrm{Ires}_x(C_0, 3, C_1, C_2, C_3) \cdot P$.

Proof of Lemma 32 Let us first demonstrate the relation for a polynomial P of degree 1. Let $P = x + s$, and $M = \mathrm{Syl}_{1,x}(PC_0, d+1, PC_1, \ldots, PC_r)$. By subtracting iteratively from each row s times the preceding row, starting at the second one and finishing at the last but one we obtain the same rows as those of the matrix $\mathrm{Syl}_x(C_0, d, C_1, \ldots, C_r)$. Except for the last row, where we have the vector $(\mathrm{Rem}(PC_1, PC_0), \ldots, \mathrm{Rem}(PC_r, PC_0), \ldots, \mathrm{Rem}(x.C_1P, PC_0), \ldots, \mathrm{Rem}(x.PC_r, PC_0), \ldots, \mathrm{Rem}(x^{d-1}.PC_1, PC_0), \ldots, \mathrm{Rem}(x^{d-1}.C_rP, PC_0))$. So the last row is merely multiplied by P. It follows that any minor of size d can be written as a product of P and a minor of M. We conclude that

$$\mathrm{Mres}_{1,x}(P.C_0, d+1, P.C_1, \ldots, P.C_r) = \mathrm{Mres}_{0,x}(C_0, d, C_1, \ldots, C_r) \cdot P.$$

A similar computation shows that

$$\mathrm{Mres}_{k+1,x}(P.C_0, d+1, P.C_1, \ldots, P.C_r) = \mathrm{Mres}_{k,x}(C_0, d, C_1, \ldots, C_r) \cdot P.$$

Finally, for P of degree > 1 we obtain the result by iteration, since P can be written as a product of linear factors in the splitting algebra of P. □

We need the following lemma.

Lemma 34 *Let $E_0, E_1, \ldots, E_r$ be polynomials in $\mathbf{A}[x]$ such that $C_0E_0 + C_1E_1 + \cdots + C_rE_r = x^\ell$. Assume that $\mathrm{Ires}_x(C_0, d, C_1, \ldots, C_r) = 0$. Let c_i be the constant coefficient of C_i.*

1. *We have $c_0^\ell = 0$.*
2. *Consider $i \in \{1, \ldots, r\}$*
   (a) *We have $c_i^{d\ell} = 0$.*
   (b) *Assume that E_0 is monic of degree e, $E_1, \ldots, E_r$ have formal degrees $\leq e$ and C_i have formal degrees $< d$ (so $\ell = e + d$). Assume also that the conjecture in Lemma 29 is true. Then $c_i^\ell = 0$.*

Proof 1) We apply Lemma 29 1). Since $x^\ell \in \langle C_0, \ldots, C_r \rangle$ we get

$$c_0^\ell = \mathrm{Res}(x^\ell, \ell, C_0) = \pm \mathrm{Res}(C_0, d, x^\ell) \in \mathrm{Ires}_x(C_0, d, C_1, \ldots, C_r).$$

2a) We have $c_i^\ell = \mathrm{Res}(x^\ell, \ell, C_i, d_i) = \pm\mathrm{Res}(C_i, d_i, x^\ell, \ell) \in \mathcal{I} = \langle C_0, \ldots, C_r \rangle \cap \mathbf{A}$ and $\mathcal{I}^d \subseteq \mathrm{Ires}_x(C_0, d, C_1, \ldots, C_r)$.
2b) We apply Lemma 29 2). Let $B = C_0E_0 + C_1E_1 + \cdots + C_rE_r$. In the generic case B is monic of degree ℓ and $\mathrm{Res}(B, \ell, C_i)$ is in the elimination ideal $\langle C_0, \ldots, C_r \rangle \cap \mathbf{A}$. This implies it is in the resultant ideal $\mathrm{Ires}(C_0, d, C_1, \ldots, C_r)$. After specialization, we get $B = x^\ell$ and we deduce $c_i^\ell = \mathrm{Res}(x^\ell, \ell, C_i) = 0$. □

Proof of Theorem 8

Within Context, we consider f_i's and g_i's as being of formal degree d. We define the formal reciprocal polynomials in degree d, $F_i = x^d f_i(\frac{1}{x})$ and $G_i = x^d g_i(\frac{1}{x})$.
By Lemma 32 we have

$$\mathrm{Ires}(G_1, d, G_2, \ldots, G_n) \cdot F_1 = \mathrm{Mres}_d(G_1F_1, d, G_2F_1, \ldots, G_nF_1) \subseteq \mathbf{A}[x].$$

So, applying Lemma 17 we are allowed to reason modulo $\mathrm{Ires}(G_1, d, G_2, \ldots, G_n)$, i.e, we can suppose that $\mathrm{Ires}_x(G_1, d, G_2, \ldots, G_n) = 0$.
In this situation, since $F_1G_1 + \ldots + F_nG_n = x^{2d}$, the coefficients of degree d of $g_i's$ satisfy Lemma 34. We conclude that any of the coefficients of g_i's in degree d, let us denote a, verify $a^k \cdot \mathbf{B} \subseteq \mathbf{A}$ for some $k \in \mathbb{N}$ which we are able to clarify according to d. By symmetry, we get the same result for any of the coefficients of f_i's in degree d. This gives a first approximation of $\mathbf{A}_1$ by $\mathbf{A}' = \mathbf{A} + \sqrt{\mathcal{I}}$ where $\mathcal{I}$ is the ideal of $\mathbf{B}$ generated by the coefficients of degree d of f_i's and g_i's. Since we are allowed to reason modulo $\sqrt{\mathcal{I}}$, we finish the algorithm by induction on d.

References

[1] F. Apéry, J.-P. Joualoulou, *Elimination: Le cas d'une variable*, Hermann (2006). 5, 6

[2] T. Coquand, *On Seminormality*, J. Algebra **305** (2006) 577–584. 1, 2

[3] T. Coquand, H. Persson, *Valuations and Dedeking Prague theorem*, J. Pure Appl. Algebra **155** (2001) 121–129. 3

[4] D. L. Costa, *Seminormality and projective module*, in: Séminaire d'algèbre Dubreil et Marie-Pole Mallivain, 34me année, vol. 924, 1982. 1

[5] H. Edwards, *Divisor Theory*, Birkhauser, Boston, MA, 1989. 3

[6] H. Lombardi, *Hidden constructions in abstract algebra. (1) Integral dependence relations*, J. Pure Appl. Agebra **167** (2002) 259–267. 3

[7] R. Mines, F. Richman, W. Ruitenburg *A Course in Constructive Algebra.* Universitext. Springer-Verlag, (1988). 2

[8] R. Swan, *On seminormality*, J. Algebra **67** (1980) 210–229 1

[9] C. Traverso, *Seminormality and Picard group*, Ann. Scuola Norm. Sup. Pisa **24** (1970) 585–595. 1