COLLOQUIUM MATHEMATICUM

VOL. 146 2017 NO. 1

SUSLIN'S LEMMA FOR RINGS CONTAINING AN INFINITE FIELD

BY

SAMIHA MONCEUR and IHSEN YENGUI (Sfax)

Abstract. A well-known lemma of Suslin says that for a commutative ring $\mathbf{A}$, if ${}^{\mathrm{t}}(v_1,\dots,v_n) \in \mathbf{A}[X]^{n\times 1}$ is unimodular where v_1 is monic of degree d and $n \geq 3$, then there exist $\gamma_1,\dots,\gamma_\ell \in \mathrm{E}_{n-1}(\mathbf{A}[X])$ such that, denoting by w_i the first coordinate of $\gamma_i\,{}^{\mathrm{t}}(v_2,\dots,v_n)$, we have

$$\langle \mathrm{Res}_X(v_1,w_1),\dots,\mathrm{Res}_X(v_1,w_\ell)\rangle = \mathbf{A}.$$

This lemma played a central role in Suslin's resolution of Serre's conjecture. In case $\mathbf{A}$ contains a set $E = \{y_0,\dots,y_{(n-2)d}\}$ such that $y_i - y_j \in \mathbf{A}^\times$ for $i \neq j$, we prove that the γ_i's can simply correspond to the elementary operations $L_1 \to L_1 + \sum_{j=2}^{n-1} y_i^{j-2} L_j$, $0 \leq i \leq (n-2)d$. These efficient elementary operations enable us to give a new and simple algorithm (for the Quillen–Suslin theorem) for reducing unimodular rows with entries in $\mathbf{K}[X_1,\dots,X_k]$ to ${}^{\mathrm{t}}(1,0,\dots,0)$, using elementary operations in case $\mathbf{K}$ is an infinite field. This work generalizes a previous paper by Lombardi and the second author which corresponds to the particular case $n = 3$.

1. Introduction. In 1955, J.-P. Serre remarked [Se1] that it was not known whether there exist finitely generated projective modules over $\mathbf{A} = \mathbf{K}[X_1,\dots,X_n]$, $\mathbf{K}$ a field, which are not free. This remark turned into the "Serre conjecture", stating that indeed there were no such modules. Proven independently by Quillen [Q] and Suslin [Su1, Su2], it became known subsequently as the Quillen–Suslin theorem. The book of Lam [Lam1] is a nice exposition about Serre's conjecture which has been updated recently in [Lam2]. An important related fact worth mentioning is that it was known [Se2] well before Serre's conjecture was settled that finitely generated projective modules over $\mathbf{A}$ are stably free, i.e., every finitely generated projective $\mathbf{A}$-module is isomorphic to the kernel of an $\mathbf{A}$-epimorphism $T : \mathbf{A}^n \to \mathbf{A}^\ell$. In that situation the matrix T is unimodular, that is, the maximal minors of T generate the unit ideal in $\mathbf{A}$.

Recall that a vector ${}^{\mathrm{t}}(b_1,\dots,b_n)$ over a ring $\mathbf{R}$ is said to be *unimodular* if $\langle b_1,\dots,b_n\rangle = \mathbf{R}$. The set of all unimodular vectors will be denoted by

2010 *Mathematics Subject Classification*: Primary 13Cxx, 13Pxx; Secondary 14Qxx.
Key words and phrases: Quillen–Suslin theorem, Suslin lemma, constructive mathematics, computer algebra.
Received 22 June 2013; revised 6 February 2015.
Published online 9 September 2016.

$\mathrm{Um}_n(\mathbf{R})$. It is worth pointing out the following precise criterion for the freeness of finitely generated stably free modules over a ring $\mathbf{R}$ in terms of unimodular vectors:

For any ring $\mathbf{R}$ *and integer* $d \geq 0$*, the following are equivalent:*

(i) *Any finitely generated stably free module of rank* $> d$ *is free.*
(ii) *Any unimodular vector over* $\mathbf{R}$ *of length* $\geq d+2$ *can be completed to an invertible matrix over* $\mathbf{R}$*.*
(iii) *For* $n \geq d+2$, $\mathrm{GL}_n(\mathbf{R})$ *acts transitively on* $\mathrm{Um}_n(\mathbf{R})$*.*

A well-known lemma of Suslin [Su2] says that for a commutative ring $\mathbf{A}$, if ${}^{\mathrm{t}}(v_1, \ldots, v_n) \in \mathbf{A}[X]^{n\times 1}$ is unimodular where v_1 is monic of degree d and $n \geq 3$, then there exist $\gamma_1, \ldots, \gamma_\ell \in \mathrm{E}_{n-1}(\mathbf{A}[X])$ such that, denoting by w_i the first coordinate of $\gamma_i\, {}^{\mathrm{t}}(v_2, \ldots, v_n)$, we have

$$\langle \mathrm{Res}_X(v_1, w_1)), \ldots, \mathrm{Res}_X(v_1, w_\ell)\rangle = \mathbf{A}.$$

This lemma played a central role in the resolution of Serre's conjecture. In case $\mathbf{A}$ contains a set $E = \{y_0, \ldots, y_{(n-2)d}\}$ such that $y_i - y_j \in \mathbf{A}^\times$ for $i \neq j$, we prove that the γ_i's can simply correspond to the elementary operations $L_1 \to L_1 + \sum_{j=2}^{n-1} y_i^{j-2} L_j$, $0 \leq i \leq (n-2)d$. These efficient elementary operations enable us to give a new and simple algorithm (for the Quillen–Suslin theorem) for reducing unimodular rows with entries in $\mathbf{K}[X_1, \ldots, X_k]$ to ${}^{\mathrm{t}}(1, 0, \ldots, 0)$, using elementary operations in case $\mathbf{K}$ is an infinite field. This work generalizes a previous paper [LY] by Lombardi and the second author which corresponds to the particular case $n = 3$.

There are several papers [FQ, FG, LW1, LW2, LS, LY, P, YP] in the literature proposing algorithms for the Quillen–Suslin theorem, but the first full implementation (a `MAPLE` package by Fabiańska) is available only recently [F].

Suslin's lemma cited above is the only nonconstructive step in Suslin's elementary proof of Serre's problem [Su2]. In the literature, in order to surmount the obstacle of this lemma which is true for any ring $\mathbf{A}$, constructive mathematicians interested in Suslin's techniques for Suslin's stability theorem and the Quillen–Suslin theorem are restricted to rings in which one knows effectively the form of all maximal ideals. For instance, in [FQ, FG, LW1, LS, P], the authors utilize the fact that for a discrete field $\mathbf{K}$, the ring $\mathbf{K}[X_1, \ldots, X_k]$ is Noetherian and has an effective Nullstellensatz (see [P, proof of Theorem 4.3]). In this paper, we avoid the heavy use of maximal ideals by using efficient elementary operations.

Let us fix some additional notation. We call an $n \times n$ matrix *elementary* if it has 1's on the diagonal and at most one nonzero off-diagonal entry. More precisely, if $a \in \mathbf{A}$ and $i \neq j$, $1 \leq i, j \leq n$, we define the elementary matrix $\mathrm{E}_{i,j}(a)$ to be the $n \times n$ matrix with 1's on the diagonal, with a in

the (i,j)-slot, and with 0's elsewhere. In other words, $\mathrm{E}_{i,j}(a)$ is the matrix corresponding to the elementary operation $L_i \to L_i + aL_j$. Moreover, $\mathrm{E}_n(\mathbf{A})$ will denote the subgroup of $\mathrm{SL}_n(\mathbf{A})$ generated by all elementary matrices.

All rings considered are unitary and commutative. The undefined terminology is standard as in [Lam2], and, for constructive algebra, in [LQ].

2. A reminder about the resultant. In this section, we give a brief outline of the *resultant*: an important idea in constructive algebra whose development owes considerably to famous pioneers such as Bézout, Cayley, Euler, Herman, Hurwitz, Kronecker, Macaulay, Noether, and Sylvester, among others.

This section will focus on the few properties of the resultant we need in this paper so that it becomes self-contained.

Definition 2.1. Let $\mathbf{R}$ be a ring, and let

$$f = a_0X^\ell + a_1X^{\ell-1} + \cdots + a_\ell \in \mathbf{R}[X], \qquad a_0 \neq 0,\ a_i \in \mathbf{R},$$
$$g = b_0X^m + b_1X^{m-1} + \cdots + b_m \in \mathbf{R}[X], \qquad b_0 \neq 0,\ b_i \in \mathbf{R}.$$

The *resultant* of f and g, denoted by $\mathrm{Res}_X(f,g)$, is the determinant of the $(m+\ell)\times(m+\ell)$ matrix below (called the *Sylvester matrix* of f and g with respect to X):

$$\mathrm{Syl}(f,g,X) = \underbrace{\begin{pmatrix} a_0 & & & & b_0 & & & \\ a_1 & a_0 & & & b_1 & b_0 & & \\ a_2 & a_1 & \ddots & & b_2 & b_1 & \ddots & \\ \vdots & & \ddots & a_0 & \vdots & & \ddots & b_0 \\ & \vdots & & a_1 & & \vdots & & b_1 \\ a_\ell & & & & b_m & & & \\ & a_\ell & & \vdots & & b_m & & \vdots \\ & & \ddots & & & & \ddots & \\ & & & a_\ell & & & & b_m \end{pmatrix}}_{\substack{m \text{ columns} \\ \qquad\qquad\qquad\qquad \ell \text{ columns}}}.$$

The resultant is an efficient tool for eliminating variables as can be seen in the following proposition. Applying this proposition in the particular case $\mathbf{R}[X] = \mathbf{K}[X_1,\ldots,X_n]$, $\mathbf{K}$ a field, we see that $\mathrm{Res}_{X_n}(f,g)$ is in the first elimination ideal $\langle f,g\rangle \cap \mathbf{K}[X_1,\ldots,X_{n-1}]$.

PROPOSITION 2.2 (see for example [CLO, Proposition 5.9]). *Let* $\mathbf{R}$ *be a ring. Then, for any* $f, g \in \mathbf{R}[X]$*, there exist* $h_1, h_2 \in \mathbf{R}[X]$ *such that*

$$h_1 f + h_2 g = \mathrm{Res}_X(f, g) \in \mathbf{R}$$

with $\deg(h_1) \leq m - 1$ *and* $\deg(h_2) \leq \ell - 1$.

PROPOSITION 2.3 (see for example [CLO, Corollary 6.2]). *Let* $\mathbf{K}$ *be a field and* $f, g \in \mathbf{K}[X] \setminus \{0\}$*. Then*

$$1 \in \langle f, g \rangle \;\Leftrightarrow\; \mathrm{Res}_X(f, g) \neq 0.$$

Proposition 2.3 can be generalized to rings as follows:

PROPOSITION 2.4 (see [LY, Lemma 2]). *Let* $\mathbf{R}$ *be a ring, and let* $f, g \in \mathbf{R}[X] \setminus \{0\}$ *with* f *monic. Then*

$$1 \in \langle f, g \rangle \text{ in } \mathbf{R}[X] \;\Leftrightarrow\; \mathrm{Res}_X(f, g) \in \mathbf{R}^{\times}.$$

3. Suslin's lemma, a particular case

THEOREM 3.1 (Suslin's lemma [Su2, Lemma 2.3]). *Let* $\mathbf{A}$ *be a commutative ring. If* $\langle v_1(X), \ldots, v_n(X) \rangle = \mathbf{A}[X]$ *where* v_1 *is monic and* $n \geq 3$*, then there exist* $\gamma_1, \ldots, \gamma_\ell \in \mathrm{E}_{n-1}(\mathbf{A}[X])$ *such that, denoting by* w_i *the first coordinate of* $\gamma_i \, {}^{\mathrm{t}}(v_2, \ldots, v_n)$*, we have*

$$\langle \mathrm{Res}_X(v_1, w_1), \ldots, \mathrm{Res}_X(v_1, w_\ell) \rangle = \mathbf{A}.$$

THEOREM 3.2 (Suslin's lemma, a particular case, new formulation). *Let* $\mathbf{A}$ *be a commutative ring, and let* $v_1, \ldots, v_n \in \mathbf{A}[X]$ *with* $n \geq 3$ *and* v_1 *monic of degree* d*. Suppose that* $\mathbf{A}$ *contains* $(n-2)d + 1$ *elements* $y_0, \ldots, y_{(n-2)d}$ *such that* $y_i - y_j \in \mathbf{A}^{\times}$ *for* $i \neq j$ *(for example if* $\mathbf{A}$ *contains an infinite field). Then*

$$1 \in \langle v_1, \ldots, v_n \rangle$$
$$\Leftrightarrow\; 1 \in \big\langle \mathrm{Res}_X(v_1, v_2 + y_i v_3 + \cdots + y_i^{n-2} v_n),\ 0 \leq i \leq (n-2)d \big\rangle.$$

Proof. The implication "$\Leftarrow$" is straightforward. Let us prove "$\Rightarrow$". Denote $w_i := v_2 + y_i v_3 + \cdots + y_i^{n-2} v_n$ and $r_i = \mathrm{Res}_X(v_1, w_i)$ for $0 \leq i \leq s = (n-2)d$, $\ell := d + 1$, and suppose that $1 \in \langle v_1, \ldots, v_n \rangle$.

A nonconstructive proof: To prove that $\langle r_0, \ldots, r_s \rangle = \mathbf{A}$ it suffices to prove that for each maximal ideal $\mathfrak{M}$ of $\mathbf{A}$ there exists $0 \leq i \leq s$ such that $r_i \notin \mathfrak{M}$. For this, let $\mathfrak{M}$ be a maximal ideal of $\mathbf{A}$, and for contradiction suppose that $\overline{r_0}, \ldots, \overline{r_s} = 0$ in the residue field $\mathbf{K} := \mathbf{A}/\mathfrak{M}$. Note that $\overline{\mathrm{Res}_X(v_1, w_i)} = \mathrm{Res}_X(\overline{v_1}, \overline{w_i})$ since v_1 is monic. This means that for each i there exists $\xi_i \in \overline{\mathbf{K}}$ (an algebraic closure of $\mathbf{K}$) such that $\overline{v_1}(\xi_i) = \overline{w_i}(\xi_i) = \overline{0}$. But since $\deg_X v_1 = d$, $\overline{v_1}$ has at most d distinct roots, and hence there exists at least one root among the ξ_i repeated $n - 1$ times. We can suppose that

$\xi_1 = \cdots = \xi_{n-1} =: \xi$. Thus, we have

$$\begin{pmatrix} 1 & y_1 & \dots & y_1^{n-2} \\ 1 & y_2 & \dots & y_2^{n-2} \\ \vdots & \vdots & \vdots & \vdots \\ 1 & y_{n-1} & \dots & y_{n-1}^{n-2} \end{pmatrix} \begin{pmatrix} v_2(\xi) \\ v_3(\xi) \\ \vdots \\ v_n(\xi) \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Since the matrix above is a Vandermonde matrix, its determinant is equal to

$$\prod_{1 \le i < j \le n-1} (y_j - y_i),$$

which is invertible in $\mathbf{A}$. Thus, $\overline{v}_1(\xi) = \cdots = \overline{v}_n(\xi) = 0$, in contradiction with $1 \in \langle v_1, \dots, v_n \rangle$.

A constructive proof: Let

$$\begin{aligned} &Z_0 = \cdots = Z_{n-3} = z_0, \\ &Z_{n-2} = \cdots = Z_{2n-5} = z_1, \\ &\vdots \\ &Z_{(n-2)k} = \cdots = Z_{(n-2)(k+1)-1} = z_k, \\ &\vdots \\ &Z_{(n-2)(d-1)} = \cdots = Z_{(n-2)d-1} = z_{d-1}, \\ &Z_{(n-2)d} = z_d \end{aligned}$$

be an enumeration of ℓ indeterminates over $\mathbf{A}$ with $n-2$ repetitions except the last one which is repeated once. Let us denote

$$I = \langle v_1(Z_i), w_i(Z_i) \mid 0 \le i \le s \rangle, \qquad \mathbf{A}_\ell = \mathbf{A}[Z_0, \dots, Z_s]/I.$$

First we prove that $1 = 0$ in $\mathbf{A}_\ell$. Letting $0 \le i_1 < \cdots < i_{n-1} \le s$, we have

$$\begin{pmatrix} 1 & y_{i_1} & \dots & y_{i_1}^{n-2} \\ 1 & y_{i_2} & \dots & y_{i_2}^{n-2} \\ \vdots & \vdots & \vdots & \vdots \\ 1 & y_{i_{n-1}} & \dots & y_{i_{n-1}}^{n-2} \end{pmatrix} \begin{pmatrix} v_2 \\ v_3 \\ \vdots \\ v_n \end{pmatrix} = \begin{pmatrix} w_{i_1} \\ w_{i_2} \\ \vdots \\ w_{i_{n-1}} \end{pmatrix}.$$

As the matrix above is a Vandermonde matrix, its determinant is equal to

$$\prod_{1 \le \ell < k \le n-1} (y_{i_k} - y_{i_\ell}),$$

which is invertible in $\mathbf{A}$. Thus, $v_2, \dots, v_n \in \langle w_{i_1}, \dots, w_{i_{n-1}} \rangle$ and a fortiori

$$v_2(Z_{i_1}), \dots, v_n(Z_{i_1}) \in I + \langle w_{i_2}(Z_{i_1}), \dots, w_{i_{n-1}}(Z_{i_1}) \rangle \subseteq I + \langle Z_{i_1} - Z_{i_2}, \dots, Z_{i_1} - Z_{i_{n-1}} \rangle,$$

and hence, using the fact that $1 \in \langle v_1, \dots, v_n \rangle$, we obtain

$$1 \in I + \langle Z_{i_1} - Z_{i_2}, \dots, Z_{i_1} - Z_{i_{n-1}} \rangle.$$

Thus, for $0 \le i < j \le d$,

$$1 \in I + \langle Z_{(n-2)i} - Z_{(n-2)i+1}, \dots, Z_{(n-2)i} - Z_{(n-2)(i+1)-1}, Z_{(n-2)i} - Z_{(n-2)j} \rangle = I + \langle z_i - z_j \rangle,$$

that is, $z_i - z_j$ is invertible in $\mathbf{A}_\ell$.

On the other hand, by clearing the denominators in the Lagrange interpolation formula, we obtain

$$v_1(X)\Big(\prod_{i \neq j}(z_i - z_j)\Big) \in \langle v_1(z_1), \dots, v_1(z_\ell) \rangle \subseteq \mathbf{A}[z_1, \dots, z_\ell][X]$$

(here we need the hypothesis $\ell = \deg v_1 + 1$). In $\mathbf{A}_\ell$, $\prod_{i \neq j}(z_i - z_j)$ is invertible, $v_1(z_1) = \cdots = v_1(z_\ell) = 0$, thus $v_1(X) = 0$ in $\mathbf{A}_\ell[X]$. Since v_1 is monic, we obtain $1 = 0$ in $\mathbf{A}_\ell$, that is, $1 \in I$.

For $0 \le k \le s$, denote $I_k = \langle v_1(Z_i), w_i(Z_i) \mid 0 \le i \le k \rangle$, $J_k = I_k + \langle r_i \mid k < i \le s \rangle$ and $\mathbf{A}_k = \mathbf{A}[Z_1, \dots, Z_k]/I_k$. Note that $I_s = I$, so $1 \in I_s = J_s$. Using Proposition 2.4, we deduce by induction on k from s to 0 that $1 \in J_k$: in order to go from $k+1$ to k consider the ring $\mathbf{B}_k = \mathbf{A}[Z_1, \dots, Z_k]/\langle r_{k+2}, \dots, r_s \rangle$ and apply Proposition 2.4 with $X = Z_{k+1}$, $a = v_1(Z_{k+1})$, $b = w_{k+1}(Z_{k+1})$. So $1 \in J_0 = \langle r_s, r_{s-1}, \dots, r_0 \rangle$. ∎

Note that [LY, Theorem 1] is a particular case of Theorem 3.2:

COROLLARY 3.3 ([LY, Theorem 1]). *Let $\mathbf{A}$ be a commutative ring and let $V, v, U, u, w \in \mathbf{A}[X]$ be such that $Vv + Uu + w = 1$ and v is monic. Denote $\ell = \deg v + 1$, and suppose that $\mathbf{A}$ contains a set $E = \{y_1, \dots, y_\ell\}$ such that $y_i - y_j$ is invertible for each $i \neq j$. For each $1 \le i \le \ell$, denoting $r_i = \mathrm{Res}_X(v, u + y_i w)$, we have $\langle r_1, \dots, r_\ell \rangle = \mathbf{A}$.*

Proof. Use Theorem 3.2 with $n = 3$, $v_1 = v$, $v_2 = u$, and $v_3 = w$. ∎

4. Suslin's algorithm for reduction of polynomial unimodular vectors. For any ring $\mathbf{B}$, when we say that a matrix $N \in \mathrm{M}_n(\mathbf{B})$ $(n \ge 3)$

is in $\mathrm{SL}_2(\mathbf{B})$, we mean that it is of the form

$$\begin{pmatrix} N' & 0 & \dots & 0 \\ 0 & 1 & & \\ \vdots & & \ddots & \\ 0 & & & 1 \end{pmatrix}$$

with $N' \in \mathrm{SL}_2(\mathbf{B})$.

From Theorem 3.2 ensues an algorithm for eliminating variables from unimodular polynomial vectors with coefficients in a ring containing an infinite field. First, let us recall the following lemma.

LEMMA 4.1 (Translation by the resultant [Su2, Lemma 2.1]). *Let* $\mathbf{R}$ *be a commutative ring. Let* $f_1, f_2 \in \mathbf{R}[X]$, $b, d \in \mathbf{R}$, *and* $r = \mathrm{Res}_X(f_1, f_2) \in \mathbf{R}$. *Then there exists* $B \in \mathrm{SL}_2(\mathbf{R}[X])$ *such that*

$$B \begin{pmatrix} f_1(b) \\ f_2(b) \end{pmatrix} = \begin{pmatrix} f_1(b + rd) \\ f_2(b + rd) \end{pmatrix}.$$

Proof. Take $g_1, g_2 \in \mathbf{R}[X]$ such that $f_1 g_1 + f_2 g_2 = r$ (use the proof of Proposition 2.2), denote by s_1, s_2, t_1, t_2 the polynomials in $\mathbf{R}[X, Y, Z]$ such that

$$\begin{aligned} f_1(X + YZ) &= f_1(X) + Y s_1(X, Y, Z), \\ f_2(X + YZ) &= f_2(X) + Y s_2(X, Y, Z), \\ g_1(X + YZ) &= g_1(X) + Y t_1(X, Y, Z), \\ g_2(X + YZ) &= g_2(X) + Y t_2(X, Y, Z), \end{aligned}$$

and set

$$\begin{aligned} B_{1,1} &= 1 + s_1(b, r, d)\, g_1(b) + t_2(b, r, d) f_2(b), \\ B_{1,2} &= s_1(b, r, d)\, g_2(b) - t_2(b, r, d) f_1(b), \\ B_{2,1} &= s_2(b, r, d)\, g_1(b) - t_1(b, r, d) f_2(b), \\ B_{2,2} &= 1 + s_2(b, r, d)\, g_2(b) + t_1(b, r, d) f_1(b). \end{aligned}$$

Then one can take $B = \left(\begin{smallmatrix} B_{1,1} & B_{1,2} \\ B_{2,1} & B_{2,2} \end{smallmatrix}\right)$. ∎

ALGORITHM 4.2 (An algorithm for eliminating variables from unimodular polynomial vectors with coefficients in a ring containing an infinite field).

INPUT: A column $\mathcal{V} = \mathcal{V}(X) = {}^{\mathrm{t}}(v_1(X), \dots, v_n(X)) \in \mathrm{Um}_n(\mathbf{A}[X])$ such that v_1 is monic of degree d, and $\mathbf{A}$ contains a set $E = \{y_0, \dots, y_{(n-2)d}\}$ such that $y_i - y_j \in \mathbf{A}^\times$ for $i \neq j$.

OUTPUT: A matrix $\mathcal{B} \in \mathrm{SL}_n(\mathbf{A}[X])$ such that $\mathcal{B}\mathcal{V} = \mathcal{V}(0)$.

STEP 1: For $0 \leq i \leq s = (n-2)d$, set $w_i = v_2 + y_i v_3 + \cdots + y_i^{n-2} v_n$, compute $r_i := \mathrm{Res}_X(v_1, w_i)$, and find $\alpha_0, \ldots, \alpha_s \in \mathbf{A}$ with $\alpha_0 r_0 + \cdots + \alpha_s r_s = 1$ (here we use Theorem 3.2).

For $0 \leq i \leq s$, compute $f_i, g_i \in \mathbf{A}[X]$ such that $f_i v_1 + g_i w_i = r_i$ (use the proof of Proposition 2.2).

STEP 2: Set

$$\begin{aligned} b_{s+1} &:= 0, \\ b_s &:= \alpha_s r_s X, \\ b_{s-1} &:= b_s + \alpha_{s-1} r_{s-1} X, \\ &\vdots \\ b_0 &:= b_1 + \alpha_0 r_0 X = X \end{aligned}$$

(the last equality follows from the fact that $X = \sum_{i=0}^{s} \alpha_i r_i X$).

STEP 3: For $1 \leq i \leq s+1$, find $\mathcal{B}_i \in \mathrm{SL}_n(\mathbf{A}[X])$ such that $\mathcal{B}_i \mathcal{V}(b_{i-1}) = \mathcal{V}(b_i)$. In more detail, let γ_i be the matrix corresponding to the elementary operation $L_2 \to L_2 + \sum_{j=3}^{n} y_i^{j-2} L_j$, that is,

$$\gamma_i := E_{2,n}(y_i^{n-2}) \cdots E_{2,3}(y_i).$$

For $3 \leq j \leq n$, set

$$F_{i,j} := \frac{v_j(b_{i-1}) - v_j(b_i)}{b_{i-1} - b_i} = \frac{v_j(b_{i-1}) - v_j(b_i)}{\alpha_i r_i X} \in \mathbf{A}[X],$$

so that

$$\begin{aligned} v_j(b_{i-1}) - v_j(b_i) &= \alpha_i r_i X F_{i,j} \\ &= \alpha_i X F_{i,j} f_i(b_{i-1}) v_1(b_{i-1}) + \alpha_i X F_{i,j} g_i(b_{i-1}) w_i(b_{i-1}) \\ &= \sigma_{i,j} v_1(b_{i-1}) + \tau_{i,j} w_i(b_{i-1}) \end{aligned}$$

with

$$\sigma_{i,j} := \alpha_i X F_{i,j} f_i(b_{i-1}), \qquad \tau_{i,j} := \alpha_i X F_{i,j} g_i(b_{i-1}) \in \mathbf{A}[X].$$

Let $\Gamma_i \in \mathrm{E}_n(\mathbf{A}[X])$ be the matrix corresponding to the elementary operations $L_j \to L_j - \sigma_{i,j} L_1 - \tau_{i,j} L_2$, $3 \leq j \leq n$, that is,

$$\Gamma_i := \prod_{j=3}^{n} E_{j,1}(-\sigma_{i,j}) E_{j,2}(-\tau_{i,j}).$$

Set

$$B_{i,2} := \Gamma_i\gamma_i \in \mathrm{E}_n(\mathbf{A}[X]), \quad \text{so that} \quad B_{i,2}\mathcal{V}(b_{i-1}) = \begin{pmatrix} v_1(b_{i-1}) \\ w_i(b_{i-1}) \\ v_3(b_i) \\ \vdots \\ v_n(b_i) \end{pmatrix}.$$

Following Lemma 4.1, set

$$\begin{aligned}
s_{i,1}(X,Y,Z) &:= \frac{v_1(X+YZ)-v_1(X)}{Y} \in \mathbf{A}[X,Y,Z],\\
s_{i,2}(X,Y,Z) &:= \frac{w_i(X+YZ)-w_i(X)}{Y} \in \mathbf{A}[X,Y,Z],\\
t_{i,1}(X,Y,Z) &:= \frac{f_i(X+YZ)-f_i(X)}{Y} \in \mathbf{A}[X,Y,Z],\\
t_{i,2}(X,Y,Z) &:= \frac{g_i(X+YZ)-g_i(X)}{Y} \in \mathbf{A}[X,Y,Z],\\
C_{i,1,1} &:= 1 + s_{i,1}(b_{i-1}, r_i, -\alpha_i X) f_i(b_{i-1})\\
&\qquad + t_{i,2}(b_{i-1}, r_i, -\alpha_i X) w_i(b_{i-1}) \in \mathbf{A}[X],\\
C_{i,1,2} &:= s_{i,1}(b_{i-1}, r_i, -\alpha_i X) g_i(b_{i-1}) - t_{i,2}(b_{i-1}, r_i, -\alpha_i X) v_1(b_{i-1}) \in \mathbf{A}[X],\\
C_{i,2,1} &:= s_{i,2}(b_{i-1}, r_i, -\alpha_i X) f_i(b_{i-1}) - t_{i,1}(b_{i-1}, r_i, -\alpha_i X) w_i(b_{i-1}) \in \mathbf{A}[X],\\
C_{i,2,2} &:= 1 + s_{i,2}(b_{i-1}, r_i, -\alpha_i X) g_i(b_{i-1})\\
&\qquad + t_{i,1}(b_{i-1}, r_i, -\alpha_i X) v_1(b_{i-1}) \in \mathbf{A}[X],\\
C_i &:= \begin{pmatrix} C_{i,1,1} & C_{i,1,2} \\ C_{i,2,1} & C_{i,2,2} \end{pmatrix} \in \mathrm{SL}_2(\mathbf{A}[X]).
\end{aligned}$$

Note that

$$C_i \begin{pmatrix} v_1(b_{i-1}) \\ w_i(b_{i-1}) \end{pmatrix} = \begin{pmatrix} v_1(b_i) \\ w_i(b_i) \end{pmatrix}.$$

Set

$$B_{i,1} := \gamma_i^{-1} \begin{pmatrix} C_i & 0 \\ 0 & I_{n-2} \end{pmatrix} \quad \text{with} \quad \gamma_i^{-1} = E_{2,3}(-y_i)\cdots E_{2,n}(-y_i^{n-2}).$$

Set

$$\mathcal{B}_i := B_{i,1}B_{i,2} \in \mathrm{SL}_n(\mathbf{A}[X]), \quad \text{so that} \quad \mathcal{B}_i\mathcal{V}(b_{i-1}) = \mathcal{V}(b_i).$$

STEP 4: $\mathcal{B} := \mathcal{B}_{s+1}\cdots\mathcal{B}_1$.

EXAMPLE 4.3. Now, let

$$\mathcal{V} = \begin{pmatrix} x + y^2 - 1 \\ -x + y^2 - 2xy \\ x - y^3 + 2 \end{pmatrix} \in \mathrm{Um}_3(\mathbb{Q}[x, y]).$$

Algorithm 4.2 has been implemented using the Computer Algebra System `MAPLE`. The code of our algorithm `UnimodElimination` gives a matrix B in $\mathrm{SL}_3(\mathbb{Q}[x, y])$ eliminating one variable. In this example, $B\mathcal{V} = \mathcal{V}(0, y)$.

```
> V := matrix([[x + y^2 − 1], [−x + y^2 − 2 ∗ x ∗ y], [x − y^3 + 2]]);
> B := UnimodElimination(V, x);
B := matrix([[1+27/151∗x−56/151∗x∗y−24/151∗x∗y^2−8/151∗y^3∗x, −35/151∗
x−4/151∗x∗y^2−14/151∗x∗y, −62/151∗x−8/151∗x∗y^2−28/151∗x∗y], [2/151∗
x∗y+56/151∗y^3∗x+16/151∗y^4∗x+136/151∗x∗y^2−27/151∗x, 1+84/151∗x∗y+
8/151∗y^3∗x+32/151∗x∗y^2+35/151∗x, 152/151∗x∗y+16/151∗y^3∗x+64/151∗x∗
y^2+62/151∗x], [−56/151∗x∗y−8/151∗y^3∗x−24/151∗x∗y^2+27/151∗x, −35/151∗
x − 4/151 ∗ x ∗ y^2 − 14/151 ∗ x ∗ y, 1 − 62/151 ∗ x − 8/151 ∗ x ∗ y^2 − 28/151 ∗ x ∗ y]])
> VV := expandvector(multiply(B, V));
VV := matrix([[−1 + y^2], [y^2], [2 − y^3]])
```

Let us fix an infinite sequence (y_i) of pairwise distinct elements in an infinite field $\mathbf{K}$, and use the notation $\underline{X} = (X_1, \ldots, X_k)$.

ALGORITHM 4.4 (An algorithm for the Quillen–Suslin theorem: case of $\mathbf{K}[X_1, \ldots, X_k]$ where $\mathbf{K}$ is an infinite field).

INPUT: A column $\mathcal{V} = \mathcal{V}(\underline{X}) = {}^{\mathrm{t}}(v_1(\underline{X}), \ldots, v_n(\underline{X})) \in \mathrm{Um}_n(\mathbf{K}[\underline{X}])$ with $\max_{1 \le i \le n}\{\deg v_i\} = d$ (here by degree we mean total degree), where $d \ge 2$.

OUTPUT: A matrix G in $\mathrm{SL}_n(\mathbf{K}[\underline{X}])$ such that $G\mathcal{V} = {}^{\mathrm{t}}(1, 0, \ldots, 0)$.

For j from k to 1 perform Steps 1 and 2:

STEP 1: Make a linear change of variables (or a change of variables à la Nagata) so that v_1 becomes monic at X_j.

STEP 2: Perform Algorithm 4.2 with $\mathbf{A} = \mathbf{K}[X_1, \ldots, X_{j-1}]$ and $X = X_j$. Output the new $\mathcal{V}$.

EXAMPLE 4.5 (Example 4.3 continued). Let

$$\mathcal{V} = \begin{pmatrix} v_1 \\ v_2 \\ v_3 \end{pmatrix} = \begin{pmatrix} x + y^2 - 1 \\ -x + y^2 - 2xy \\ x - y^3 + 2 \end{pmatrix} \in \mathrm{Um}_3(\mathbb{Q}[x, y]).$$

Recall that the syzygy module of (v_1, v_2, v_3) is

$$\mathrm{Syz}(v_1, v_2, v_3) := \{ {}^{\mathrm{t}}(w_1, w_2, w_3) \in \mathbb{Q}[x, y]^3 \mid w_1 v_1 + w_2 v_2 + w_3 v_3 = 0\}.$$

Recall also that since ${}^{\mathrm{t}}(v_1, v_2, v_3) \in \mathrm{Um}_3(\mathbb{Q}[x, y])$, $\mathrm{Syz}(v_1, v_2, v_3)$ is a projective $\mathbb{Q}[x, y]$-module which is free of rank 2 by the Quillen–Suslin theorem [Q, Su1].

We have implemented Algorithm 4.4 using `MAPLE`. It computes a matrix $G \in \mathrm{SL}_3(\mathbb{Q}[x, y])$ such that $G\mathcal{V} = {}^{\mathrm{t}}(1, 0, 0)$.

```
G := matrix([[-1+60/151*x*y^3+540/151*x*y^2+62/151*x*y-108/151*x+2*
y^2-128/151*x*y^5-272/151*x*y^4-32/151*x*y^6,-40/151*x*y^2+266/151*x*
y+140/151*x-72/151*x*y^4-172/151*x*y^3+3-2*y^2-16/151*x*y^5,248/151*
x-48/151*x*y^2+484/151*x*y-144/151*x*y^4-312/151*x*y^3-32/151*x*
y^5],[-y^2+64/151*x*y^5+144/151*x*y^4+2/151*x*y^3-190/151*x*y^2+27/151*
x-2/151*x*y+16/151*x*y^6,36/151*x*y^4+90/151*x*y^3+38/151*x*y^2-1-
35/151*x-84/151*x*y+y^2+8/151*x*y^5,60/151*x*y^2+72/151*x*y^4+164/151*
x*y^3-152/151*x*y-62/151*x+16/151*x*y^5],[2-190/151*x*y^3-344/151*x*
y^2-172/151*x*y+135/151*x-y^3+64/151*x*y^6+160/151*x*y^5+26/151*x*
y^4+16/151*x*y^7,-76/151*x*y^2-210/151*x*y-175/151*x+36/151*x*y^5+
98/151*x*y^4+54/151*x*y^3-2+y^3+8/151*x*y^6,-310/151*x-152/151*x*y^2-
388/151*x*y+92/151*x*y^3+72/151*x*y^5+180/151*x*y^4+16/151*x*y^6+1]])
```

Thus, if we denote

$$\epsilon_1 = \begin{pmatrix} -151y^2 + 64xy^5 + 144xy^4 + 2xy^3 - 190xy^2 + 27x - 2xy + 16xy^6 \\ 36xy^4 + 90xy^3 + 38xy^2 - 151 - 35x - 84xy + 151y^2 + 8xy^5 \\ 60xy^2 + 72xy^4 + 164xy^3 - 152xy - 62x + 16xy^5 \end{pmatrix},$$

$\epsilon_2 =$

$$\begin{pmatrix} 302 - 190xy^3 - 344xy^2 - 172xy + 135x - 151y^3 + 64xy^6 + 160xy^5 + 26xy^4 + 16xy^7 \\ -76xy^2 - 210xy - 175x + 36xy^5 + 98xy^4 + 54xy^3 - 302 + 151y^3 + 8xy^6 \\ -310x - 152xy^2 - 388xy + 92xy^3 + 72xy^5 + 180xy^4 + 16xy^6 + 151 \end{pmatrix},$$

then (ϵ_1, ϵ_2) is a free basis for $\mathrm{Syz}(v_1, v_2, v_3)$. A minimal parametrization of the set $\mathcal{E}$ of all inverses of $\mathcal{V}$ is

$$\begin{aligned} \mathcal{E} &:= \{\mathcal{U} = (u_1, u_2, u_3) \in \mathbb{Q}[x, y]^{1\times 3} \mid \mathcal{U}\mathcal{V} = 1\} \\ &= \{\epsilon_0 + \alpha\epsilon_1 + \beta\epsilon_2 \mid \alpha, \beta \in \mathbb{Q}[x, y]\}, \end{aligned}$$

where

$$\epsilon_0 = \frac{1}{151}\begin{pmatrix} -151 + 60xy^3 + 540xy^2 + 62xy - 108x + 302y^2 - 128xy^5 - 272xy^4 - 32xy^6 \\ -40xy^2 + 266xy + 140x - 72xy^4 - 172xy^3 + 453 - 302y^2 - 16xy^5 \\ 248x - 48xy^2 + 484xy - 144xy^4 - 312xy^3 - 32xy^5 \end{pmatrix}.$$

REFERENCES

[CLO] D. Cox, J. Little and D. O'Shea, *Ideals, Varieties and Algorithms*, 2nd ed., Springer, New York, 1997.

[F] A. Fabiańska, A Maple QuillenSuslin package: http://wwwb.math.rwth-aachen.de/QuillenSuslin/.

[FQ] A. Fabiańska and A. Quadrat, *Applications of the Quillen–Suslin theorem to the multidimensional systems theory*, in: Gröbner Bases in Control Theory and Signal Processing, H. Park and G. Regensburger (eds.), Radon Ser. Comput. Appl. Math. 3, de Gruyter, 2007, 23–106.

[FG] N. Fitchas et A. Galligo, *Nullstellensatz effectif et conjecture de Serre (Théorème de Quillen–Suslin) pour le calcul formel*, Math. Nachr. 149 (1990), 231–253.

[Lam1] T. Y. Lam, *Serre's Conjecture*, Lecture Notes in Math. 635, Springer, Berlin, 1978.

[Lam2] T. Y. Lam, *Serre's Problem on Projective Modules*, Springer Monogr. Math., Springer, 2006.

[LW1] R. C. Laubenbacher and C. J. Woodburn, *An algorithm for the Quillen–Suslin theorem for monoid rings*, J. Pure Appl. Algebra 117–118 (1997), 395–429.
, .

[LW2] R. C. Laubenbacher and C. J. Woodburn, *A new algorithm for the Quillen–Suslin theorem*, Beiträge Algebra Geom. 41 (2000), 23–31.

[LS] A. Logar and B. Sturmfels, *Algorithms for the Quillen–Suslin theorem*, J. Algebra 145 (1992), 231–239.

[LQ] H. Lombardi et C. Quitté, *Algèbre commutative. Méthodes constructives. Modules projectifs de type fini. Cours et exercices*, Calvage et Mounet, 2011.

[LY] H. Lombardi and I. Yengui, *Suslin's algorithms for reduction of unimodular rows*, J. Symbolic Comput. 39 (2005), 707–717.

[P] H. Park and C. Woodburn, *An algorithmic proof of Suslin's stability theorem for polynomial rings*, J. Algebra 178 (1995), 277–298.

[Q] D. Quillen, *Projective modules over polynomial rings*, Invent. Math. 36 (1976), 167–171.

[Se1] J.-P. Serre, *Faisceaux algébriques cohérents*, Ann. of Math. 61 (1955), 191–278.

[Se2] J.-P. Serre, *Modules projectifs et espaces fibrés à fibre vectorielle*, Sém. Dubreil–Pisot, exp. 23, Paris, 1957/58.

[Su1] A. A. Suslin, *Projective modules over a polynomial ring are free*, Soviet Math. Dokl. 17 (1976), 1160–1164.

[Su2] A. A. Suslin, *On the structure of the special linear group over polynomial rings*, Math. USSR-Izv. 11 (1977), 221–238.

[YP] D. C. Youla and P. F. Pickel, *The Quillen–Suslin theorem and the structure of n-dimensional elementary polynomial matrices*, IEEE Trans. Circuits Systems 31 (1984), 513–518.

Samiha Monceur, Ihsen Yengui
Department of Mathematics
Faculty of Sciences
University of Sfax
3000 Sfax, Tunisia
E-mail: ihsen.yengui@fss.rnu.tn