Suslin's algorithms for reduction of unimodular rows

Henri Lombardi [a],

[a] *Laboratoire de Mathématiques, UMR CNRS 6623, UFR des Sciences et Techniques, Université de Franche-Comté, 25030 BESANCON cedex, FRANCE*

Ihsen Yengui [b]

[b] *Département de Mathématiques, Faculté des Sciences de Sfax, 3018 Sfax, TUNISIA*

Abstract

A well-known lemma of Suslin says that for a commutative ring $\mathbf{A}$ if $(v_1(X), \ldots, v_n(X)) \in (\mathbf{A}[X])^n$ is unimodular 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 the ideal generated by $\mathrm{Res}(v_1, e_1.\gamma_1\,{}^{\mathrm{t}}(v_2, \ldots, v_n))$, $\ldots$, $\mathrm{Res}(v_1, e_1.\gamma_\ell\,{}^{\mathrm{t}}(v_2, \ldots, v_n))$ equals $\mathbf{A}$. This lemma played a central role in the resolution of Serre's conjecture. In case $\mathbf{A}$ contains a set E of cardinality greater than $\deg v_1 + 1$ such that $y - y'$ is invertible for each $y \neq y'$ in E, we prove that the γ_i can simply correspond to the elementary operations $L_1 \to L_1 + y_i \sum_{j=2}^{n-1} u_{j+1} L_j$, $1 \leq i \leq \ell = \deg v_1 + 1$, where $u_1 v_1 + \cdots + u_n v_n = 1$. These efficient elementary operations enable us to give new and simple algorithms 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. Another feature of this paper is that it shows that the concrete local-global principles can produce competitive complexity bounds.

Key words: Quillen-Suslin's Theorem, Suslin's Stability Theorem, Constructive Mathematics, Computer Algebra.
1991 MSC: 13C10, 19A13, 14Q20, 03F65

Email addresses: henri.lombardi@univ-fcomte.fr (Henri Lombardi), ihsen.yengui@fss.rnu.tn. (Ihsen Yengui).
URL: http://hlombardi.free.fr/ (Henri Lombardi).

1 Introduction

One principal motivation is to obtain a constructive proof of a lemma of Suslin which played a central role in the Suslin's solution of Serre's conjecture.

Sulsin's Lemma (Suslin, 1977, Lemma 2.3)
Let $\mathbf{A}$ *be a commutative ring* $\mathbf{A}$ *and* $(v_1(X), \ldots, v_n(X)) \in (\mathbf{A}[X])^n$ *a unimodular row with* v_1 *monic and* $n \geq 3$. *Then there exist finitely many* $\gamma_i \in \mathrm{E}_{n-1}(\mathbf{A}[X])$ *such that*

$$\langle \mathrm{Res}(v_1, e_1.\gamma_i\, {}^{\mathrm{t}}(v_2, \ldots, v_n)) \mid 1 \leq i \leq \ell \rangle = \mathbf{A}.$$

where $e_1.x$ *is the first coordinate of* $x \in \mathbf{A}^n$.

In case $\mathbf{A}$ contains a set E of cardinality greater than $\deg v_1 + 1$ such that $y - y'$ is invertible for each $y \neq y'$ in E, we prove that the γ_i can simply correspond to the elementary operations

$$L_1 \to L_1 + y_i \sum_{j=2}^{n-1} u_{j+1} L_j,\ 1 \leq i \leq \ell = \deg v_1 + 1,$$

where the $u_j \in \mathbf{A}[X]$ satisfy $u_1 v_1 + \cdots + u_n v_n = 1$. These efficient elementary operations enable us to give a new and simple algorithm for reducing unimodular columns 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.

We think that this kind of operations may bring useful simplifications to the existing algorithms for the Quillen-Sulin and Suslin's stability theorems based on unimodular completion and will facilitate their implementation (Fitchas and Galligo, 1990; Logar and Sturmfels, 1992; Park and Woodburn, 1995).

The undefined terminology is standard as in Kunz (1991); Lam (1978).

2 Efficient elementary operations

The following theorem gives under a stronger hypothesis a more precise formulation of Suslin's lemma.

Theorem 1 (Suslin's Lemma, particular case)
Let $\mathbf{A}$ *be a commutative ring,* $V, v, U, u, w \in \mathbf{A}[X]$ *such that* $Vv + Uu + w = 1$ *and* v *is monic. Denote* $\ell = \deg v + 1$ *and suppose that* $\mathbf{A}$ *contains a set*

$E = \{y_1, \ldots, y_\ell\}$ such that $y_i - y_j$ is invertible for each $i \neq j$. For each $1 \leq i \leq \ell$, denoting $r_i = \mathrm{Res}(v, u + y_i w)$, then $\langle r_1, \ldots, r_\ell \rangle = \mathbf{A}$, that is, there exist $\alpha_1, \ldots, \alpha_\ell \in \mathbf{A}$ such that $\alpha_1 r_1 + \cdots + \alpha_\ell r_\ell = 1$.

Furthermore, supposing that $\mathbf{A}$ is a polynomial ring in a finite number of variables over a basic ring $\mathbf{B}$ and that $\deg V$, $\deg U \leq D$, $1 + \deg v$, $1 + \deg u \leq d$ (where $d \geq 2$) and $\deg w \leq d + D$, then for each $1 \leq i \leq \ell$, $\deg(\alpha_i) \leq \frac{d^4}{4}(\frac{d}{2} + D + 1)^2$ and $\deg(\alpha_i r_i) \leq \frac{d^4}{4}(d + D + 1)^2$ (here, by degree we mean total degree).

Proof Let $Z_1, \ldots, Z_\ell$ be ℓ indeterminates over $\mathbf{A}$ and denote

$$I = \langle v(Z_i), u(Z_i) + y_i w(Z_i) \mid 1 \leq i \leq \ell \rangle, \quad \mathbf{A}_\ell = \mathbf{A}[Z_1, \ldots, Z_\ell]/I\,.$$

First we prove that $1 = 0$ in $\mathbf{A}_\ell$.

Observe that for $i \neq j$, $(y_i - y_j)w(Z_i) \in \langle Z_i - Z_j \rangle + I$. Indeed,

$$(y_i - y_j)w(Z_i) = (y_i w(Z_i) + u(Z_i)) - (y_j w(Z_j) + u(Z_j)) + (u(Z_j) - u(Z_i)) + y_j(w(Z_j) - w(Z_i)).$$

Since $y_i - y_j$ is invertible, $w(Z_i) \in \langle Z_i - Z_j \rangle + I$. Thus,

$$u(Z_i) = -y_i\, w(Z_i) + (u(Z_i) + y_i w(Z_i)) \in \langle Z_i - Z_j \rangle + I.$$

Since $v(Z_i) \in I$ and $Vv + Uu + w = 1$, we get $1 \in \langle Z_i - Z_j \rangle + I$, 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

$$v(X)\ \left(\prod\nolimits_{i \neq j}(Z_i - Z_j)\right) \in \langle v(Z_1), \ldots, v(Z_\ell) \rangle\ \subseteq\ \mathbf{A}[Z_1, \ldots, Z_\ell][X]$$

(here we need the hypothesis $\ell = \deg v + 1$).

In $\mathbf{A}_\ell$, $\prod_{i \neq j}(Z_i - Z_j)$ is invertible, $v(Z_1) = \cdots = v(Z_\ell) = 0$, thus $v(X) = 0$ in $\mathbf{A}_\ell[X]$. Since v is monic, we obtain $1 = 0$ in $\mathbf{A}_\ell$, that is $1 \in I$.

For $0 \leq k \leq \ell$, denote $I_k = \langle v(Z_i), u(Z_i) + y_i w(Z_i) \mid 1 \leq i \leq k \rangle$, $J_k = I_k + \langle r_i \mid k < i \leq \ell \rangle$ and $\mathbf{A}_k = \mathbf{A}[Z_1, \ldots, Z_k]/I_k$. Note that $I_\ell = I$, so $1 \in I_\ell = J_\ell$. Using Lemma 2 below we get by induction on k from ℓ to 0 that $1 \in J_k$: in order to go from $k+1$ to k consider the ring $\mathbf{B}_k = \mathbf{A}[Z_1, \ldots, Z_k]/\langle r_{k+2}, \ldots, r_\ell \rangle$ and apply the lemma with $X = Z_{k+1}$, $a = v(Z_{k+1})$, $b = u(Z_{k+1}) + y_{k+1} w(Z_{k+1})$. So $1 \in J_0 = \langle r_\ell, \ldots, r_1 \rangle$.

For the degree bounds, as seen above, for $i \neq j$, we can write $(y_i - y_j)w(Z_i)$ in the form

$$(y_i - y_j)w(Z_i) = (Z_i - Z_j)A_{i,j} + B_{i,j},$$

where $A_{i,j} \in \mathbf{A}[Z_1, \ldots, Z_\ell]$, $B_{i,j} \in I$, $\deg((Z_i - Z_j)A_{i,j}) \leq d+D$, and $\deg B_{i,j} \leq d+D$.

In the same way, we can write $(y_i - y_j)u(Z_i)$ in the form

$$(y_i - y_j)u(Z_i) = (Z_i - Z_j)C_{i,j} + D_{i,j},$$

where $C_{i,j} \in \mathbf{A}[Z_1, \ldots, Z_\ell]$, $D_{i,j} \in I$, $\deg((Z_i - Z_j)C_{i,j}) \leq d+D$, and $\deg D_{i,j} \leq d+D$.

Thus, since $y_i - y_j = (y_i - y_j)V(Z_i)v(Z_i) + (y_i - y_j)U(Z_i)u(Z_i) + (y_i - y_j)w(Z_i)$, we have:

$$1 = (Z_i - Z_j)E_{i,j} + F_{i,j},$$

where $E_{i,j} \in \mathbf{A}[Z_1, \ldots, Z_\ell]$, $F_{i,j} \in I$, $\deg((Z_i - Z_j)E_{i,j}) \leq d + 2D$, and $\deg F_{i,j} \leq d + 2D$.

Hence, we have an identity of the form:

$$\left(\prod_{i \neq j}(Z_i - Z_j)\right) A = 1 + B,$$

where $A \in \mathbf{A}[Z_1, \ldots, Z_\ell]$, $B \in I$, $\deg A \leq \binom{d}{2}(d + 2D) \leq d^2(\frac{d}{2} + D)$, and $\deg B \leq \binom{d}{2}(d + 2D) \leq d^2(\frac{d}{2} + D)$.

Multiplying the Lagrange interpolation formula by A, we obtain an identity of the form:

$$v(X) = -Bv(X) + A\,(v(Z_1)g_1 + \cdots + v(Z_\ell)g_\ell),$$

where $g_i \in \mathbf{A}[Z_1, \ldots, Z_\ell, X]$, and $\deg g_i \leq d$.

By identifying the leading coefficients in both sides, since v is monic and $B, v(Z_1), \ldots, v(Z_\ell) \in I$, we obtain an identity of the form:

$$1 = \theta_1 + \cdots + \theta_m,$$

where $\theta_i \in I$, and $\deg \theta_i \leq 2d + d^2(\frac{d}{2} + D) \leq d^2(\frac{d}{2} + D + 1)$ $(d \geq 2)$.

Applying Lemma 2 and following the proof above, there exists $\alpha_\ell \in \mathbf{A}_{\ell-1}$ and $\gamma_\ell \in I_{\ell-1}$ such that $\alpha_\ell r_\ell + \gamma_\ell = 1$, with $\deg(\alpha_\ell) \leq \frac{d^4}{4}(\frac{d}{2} + D + 1)^2$, and so on, we find that for each $1 \leq i \leq \ell$, $\deg(\alpha_i) \leq \frac{d^4}{4}(\frac{d}{2} + D + 1)^2$.

More explicitly, using the equality $1 = \theta_1 + \cdots + \theta_m$, we can write

$$1 = v(Z_\ell)\gamma_{1,\ell} + (u(Z_\ell) + y_\ell w(Z_\ell))\gamma_{2,\ell} + \gamma_\ell,$$

where $\gamma_{i,\ell} \in \mathbf{A}[Z_1, \ldots, Z_\ell]$, $\gamma_\ell \in I_{\ell-1}$, $\deg(v(Z_\ell)\gamma_{1,\ell}), \deg((u(Z_\ell)+y_\ell w(Z_\ell))\gamma_{2,\ell}), \deg \gamma_\ell \leq d^2(\frac{d}{2}+D+1)$.

By Lemma 2, we have

$$r_\ell \operatorname{Res}_{Z_\ell}(v(Z_\ell), \gamma_{2,\ell}) = \operatorname{Res}_{Z_\ell}(v(Z_\ell), 1-\gamma_\ell) = 1-\gamma_\ell.$$

Thus, it suffices to take $\alpha_\ell = \operatorname{Res}_{Z_\ell}(v(Z_\ell), \gamma_{2,\ell})$ so that $r_\ell\alpha_\ell + \gamma_\ell = 1$. Now, let us explain how to pass from step $k+1$ to step k. Suppose that we have already found an equality of the form

$$\alpha_\ell r_\ell + \cdots + \alpha_{k+1} r_{k+1} + \gamma_{k+1} = 1,$$

where $\gamma_{k+1} \in I_k$. Write

$$\gamma_{k+1} = v(Z_k)\gamma_{1,k} + (u(Z_k) + y_k w(Z_k))\gamma_{2,k} + \gamma_k,$$

where $\gamma_{i,k} \in \mathbf{A}[Z_1, \ldots, Z_k]$, $\gamma_k \in I_{k-1}$, and $\deg(v(Z_k)\gamma_{1,k})$, $\deg((u(Z_k) + y_k w(Z_k))\gamma_{2,k})$, $\deg \gamma_k \leq d^2(\frac{d}{2}+D+1)$.

Since $r_k \operatorname{Res}_{Z_k}(v(Z_k), \gamma_{2,k}) = 1 - \alpha_\ell r_\ell - \cdots - \alpha_{k+1} r_{k+1} - \gamma_k$, it suffices to take $\alpha_k = \operatorname{Res}_{Z_k}(v(Z_k), \gamma_{2,k})$.

Moreover, since $\deg r_i \leq d(d+D)$, then

$$\deg(\alpha_i r_i) \leq \frac{d^4}{4}(\frac{d}{2}+D+1)^2 + d(d+D) \leq \frac{d^4}{4}(d+D+1)^2.$$

Indeed, $\frac{d^4}{4}(d+D+1)^2 - \frac{d^4}{4}(\frac{d}{2}+D+1)^2 - d(d+D) = \frac{d}{4}(\frac{3}{4}d^5 + (d^4-4)D + d(d^3-4)) \geq 0$.

□

Lemma 2 (basic elimination lemma)
Let $a, b \in \mathbf{B}[X]$ with a monic. Then

$$\langle a, b\rangle = \langle 1\rangle \text{ in } \mathbf{B}[X] \quad \Longleftrightarrow \quad \langle \operatorname{Res}_X(a,b)\rangle = \langle 1\rangle \text{ in } \mathbf{B}$$

More precisely if $ca + db = 1$ in $\mathbf{B}[X]$ then $\operatorname{Res}(a,b)\operatorname{Res}(a,d) = 1$ in $\mathbf{B}$.
Furthermore, supposing that $\mathbf{B}$ is a polynomial ring in a finite number of variables over a basic ring $\mathbf{A}$, $\deg(a) \leq \delta$ and $\deg(d) \leq \delta_1$, then $\deg(\operatorname{Res}(a,d)) \leq \delta\delta_1$. In particular, if $\deg(ad) \leq \delta'$, then $\deg(\operatorname{Res}(a,d)) \leq \frac{\delta'^2}{4}$.

Proof Since a is monic, we have $\operatorname{Res}(a, db) = \operatorname{Res}(a,d)\operatorname{Res}(a,b)$ and

$$\operatorname{Res}(a, db) = \operatorname{Res}(a, ca+db) = \operatorname{Res}(a, 1) = 1.$$

The fact that $\deg(\operatorname{Res}(a,d)) \leq \delta\delta_1$ is classical. □

The following formulation of Theorem 1 will be the main key mathematical result used in the algorithm for unimodular reduction.

Corollary 3 *Let* $\mathbf{A}$ *be a commutative ring,* $v_1, \ldots, v_n, u_1, \ldots, u_n \in \mathbf{A}[X]$ *such that* $u_1v_1 + \cdots + u_nv_n = 1$, v_1 *is monic and* $n \geq 3$. *Denote* $\ell = \deg v_1 + 1$ *and suppose that* $\mathbf{A}$ *contains a set* $E = \{y_1, \ldots, y_\ell\}$ *such that* $y_i - y_j$ *is invertible for each* $i \neq j$. *For each* $1 \leq i \leq \ell$, *denoting* $r_i = \mathrm{Res}(v_1, v_2 + y_i \sum_{j=3}^{n} u_j v_j)$, *then* $\langle r_1, \ldots, r_\ell \rangle = \mathbf{A}$, *that is, there exist* $\alpha_1, \ldots, \alpha_\ell \in \mathbf{A}$ *such that* $\alpha_1 r_1 + \cdots + \alpha_\ell r_\ell = 1$.

Furthermore, supposing that $\mathbf{A}$ *is a polynomial ring in a finite number of variables over a basic ring* $\mathbf{B}$, $1 + \max_{1 \leq i \leq n}\{\deg v_i\} = d$ *(where* $d \geq 2$*), and* $\max_{1 \leq i \leq n}\{\deg u_i\} = D$, *then for each* $1 \leq i \leq \ell$, $\deg(\alpha_i r_i) \leq \frac{d^4}{4}(d + D + 1)^2$.

Proof Let $v = v_1$, $u = v_2$, $w = u_3v_3 + \cdots + u_nv_n$ and apply Theorem 1. □

Remark. The second author has given in Yengui (2004) a general constructive proof of the lemma of Suslin cited in the introduction without any restriction on the ring $\mathbf{A}$. With the degree bounds and notations of Corollary 3, the general constructive proof involves 2^d matrices γ_j in $\mathrm{E}_{n-1}(\mathbf{A}[X])$, the subgroup of $\mathrm{SL}_{n-1}(\mathbf{A}[X])$ generated by elementary matrices, instead of d in Corollary 3. Moreover, in the general constructive proof, each γ_j is the product of at most $2d$ elementary matrices while in Corollary 3 it is the product of $n - 2$ elementary matrices.

3 Reduction of unimodular rows

For any ring $\mathbf{A}$ and $n \geq 1$, $\mathrm{Um}_n(\mathbf{A})$ denotes the set of unimodular rows in $\mathbf{A}$, that is $\mathrm{Um}_n(\mathbf{A}) = \{(x_1, \ldots, x_n) \in \mathbf{A}^n \text{ such that } \langle x_1, \ldots, x_n \rangle = \mathbf{A}\}$. $\mathrm{E}_n(\mathbf{A})$ denotes the subgroup of $\mathrm{SL}_n(\mathbf{A})$ generated by elementary matrices. For $i \neq j$, $E_{i,j}(a)$ is the matrix corresponding to the elementary operation $L_i \to L_i + aL_j$.

From now on, we suppose that n is an integer ≥ 3. All the considered matrices are square of size n.

The algorithms are based on Lombardi and Quitté (2003) and on Theorem 1.

An algorithm for unimodular completion: general case.

Input: Two columns $\mathcal{V} = \mathcal{V}(X) = {}^{\mathrm{t}}(v_1(X), \ldots, v_n(X))$, $\mathcal{U} = \mathcal{U}(X) = {}^{\mathrm{t}}(u_1(X), \ldots, u_n(X)) \in \mathbf{A}[X]^n$ such that v_1 is monic and $\mathcal{V}\,{}^{\mathrm{t}}\mathcal{U} = 1$. We assume the "size" of an element $a \in \mathbf{A}$ is measured by $\deg(a) \in \mathbb{N}$, the function

deg sharing the usual properties of a total degree function in a polynomial ring: $\deg(a+b) \leq \max(\deg(a), \deg(b))$, $\deg(ab) \leq \deg(a) + \deg(b)$. We assume $1 + \max_{1 \leq i \leq n}\{\deg v_i\} \leq d$ (where $d \geq 2$) and $\max_{1 \leq i \leq n}\{\deg u_i\} \leq D$. We assume the ring $\mathbf{A}$ integral and contains infinitely many y_i of degree 0 such that $y_i - y_j$ is invertible for $i \neq j$.

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

Step 1: For $1 \leq i \leq \ell = \deg_X v_1 + 1$, set $w_i := v_2 + y_i(u_3 v_3 + \cdots + u_n v_n)$, compute $r_i := \mathrm{Res}_X(v_1, w_i)$ and find $\alpha_1, \ldots, \alpha_\ell \in \mathbf{A}$ such that $\alpha_1 r_1 + \cdots + \alpha_\ell r_\ell = 1$ (here we use the constructive proof of Theorem 1).

For $1 \leq i \leq \ell$, compute $f_i, g_i \in \mathbf{A}[\underline{X}]$ such that $f_i v_1 + g_i w_i = r_i$.

Step 2: For $1 \leq i \leq \ell$,

$$H_i := E_{n,1}(-1)E_{1,n}(1)E_{n-1,n}(-v_{n-1}) \cdots E_{3,n}(-v_3)E_{2,n}(-w_i)E_{1,n}(-v_1)$$
$$E_{n,2}(-r_i^{-1}(v_n - 1)g_i)E_{n,1}(-r_i^{-1}(v_n - 1)f_i)E_{2,n}(y_i u_n) \cdots E_{2,3}(y_i u_3).$$

(Comment: Of course, we consider only the r_i which are nonzero and we have $H_i\mathcal{V} = {}^{\mathrm{t}}(1, 0, \ldots, 0)$).

Set $\tilde{H}_i := H_i(0)^{-1} H_i(X)$ so that $\tilde{H}_i \mathcal{V}(X) = \mathcal{V}(0)$.

Note that the coefficients of H_i are in the module $\mathbf{A}[X]\frac{1}{r_i}$ and those of $\tilde{H}_i$ are in $\mathbf{A}[X]\frac{1}{r_i^2}$.

Step 3: For $1 \leq i \leq \ell$, find $k_i \in \mathbb{N}$ and $G_i \in \mathrm{SL}_n(\mathbf{A}[X, Y])$ such that $G_i \mathcal{V}(X + r_i^{k_i} Y) = \mathcal{V}(X)$ (see Lombardi and Quitté, 2003, Lemma 15).

In more details,

$$\tilde{H}_i(X)\ \mathcal{V}(X) = \mathcal{V}(0) = \tilde{H}_i(X + r_i^{2n}Y)\ \mathcal{V}(X + r_i^{2n}Y),$$

and so

$$\tilde{H}_i(X)^{-1}\ \tilde{H}_i(X + r_i^{2n}Y)\ \mathcal{V}(X + r_i^{2n}Y)\ =\ \mathcal{V}(X).$$

Thus, we take $k_i = 2n$ and $G_i = \tilde{H}_i(X)^{-1}\ \tilde{H}_i(X + r_i^{2n}Y)$.

Moreover, since all the coefficients of $r_i^2 \tilde{H}_i$ are in $\mathbf{A}[X, Y]$ then $G_i \in \mathrm{SL}_n(\mathbf{A}[X, Y])$ (see Lemma 4).

To sum up, the main properties of G_i are

$$\begin{cases} G_i \in \mathrm{SL}_n(\mathbf{A}[X,Y]) \\ G_i \mathcal{V}(X + r_i^{2n} Y) = \mathcal{V}(X). \end{cases}$$

Step 4: Find $\tilde{G} = \tilde{G}(X,Y) \in \mathrm{SL}_n(\mathbf{A}[X,Y])$ such that $\tilde{G}\mathcal{V}(X+Y) = \mathcal{V}(X)$.

More precisely, let $\beta_1, \ldots, \beta_\ell \in \mathbf{A}$ such that $\beta_1 r_1^{2n} + \cdots + \beta_\ell r_\ell^{2n} = 1$ ($\beta_1, \ldots, \beta_\ell$ are deduced from the identity $(\alpha_1 r_1 + \cdots + \alpha_\ell r_\ell)^{2n\ell} = 1$).

Set

$$\tilde{G} = \prod_{i=2}^{\ell} G_i(X + (\beta_1 r_1^{2n} + \cdots + \beta_{i-1} r_{i-1}^{2n})Y, \beta_i Y).$$

Remark that

$$G_\ell(X + (\beta_1 r_1^{2n} + \cdots + \beta_{\ell-1} r_{\ell-1}^{2n})Y, \beta_\ell Y)\ \mathcal{V}(X+Y)$$

$$= G_\ell(X + (\beta_1 r_1^{2n} + \cdots + \beta_{\ell-1} r_{\ell-1}^{2n})Y, \beta_\ell Y)\ \mathcal{V}(X + (\beta_1 r_1^{2n} + \cdots + \beta_{\ell-1} r_{\ell-1}^{2n})Y + \beta_\ell r_\ell^{2n} Y)$$

$$= \mathcal{V}(X + (\beta_1 r_1^{2n} + \cdots + \beta_{\ell-1} r_{\ell-1}^{2n})Y),$$

and so on until getting

$$\tilde{G}\mathcal{V}(X+Y) = \mathcal{V}(X).$$

Step 5: $G := \tilde{G}(0, X)$.

(Comment: Since $\tilde{G}\mathcal{V}(X+Y) = \mathcal{V}(X)$, then $G\mathcal{V}(X) = \mathcal{V}(0)$).

For sake of completeness, we add the following lemma which is a more precise formulation of a lemma originally given in Lombardi and Quitté (2003) and was used in Step 3 of the above algorithm.

Lemma 4 (Lombardi and Quitté, 2003, Lemma 15) *Let* $\mathbf{A}$ *be an integral domain,* $b \in \mathbf{A}$, $H(X) \in \mathrm{SL}_n(\mathbf{A}[\frac{1}{b}][X])$ *such that* $b^m H(X) \in \mathrm{M}_n(\mathbf{A}[X])$ *for some* $m \in \mathbb{N}$. *Then*

$$H(X + b^{mn} Y) H(X)^{-1} \in \mathrm{SL}_n(\mathbf{A}[X,Y]).$$

So, with the notations of the algorithm for unimodular completion, we get the following complexity bounds.

Proposition 5 (complexity bounds, 1)
The matrix G is the product of at most d matrices in $\mathrm{SL}_n(\mathbf{A}[X])$ obtained as the product of at most $4d(2n+1) = \mathrm{O}(n\,d)$ elementary matrices $M_i \in \mathrm{M}_n(\mathbf{A}[X]\frac{1}{r_i})$ where $r_i = \mathrm{Res}_X(v_1(X), w_i(X))$, $1 \leq i \leq \deg_X v_1 + 1$, and $w_i = v_2 + y_i(u_3v_3 + \cdots + u_nv_n)$. Moreover,

$$\deg G \leq 2(\frac{1}{2}nd^5(d+D+1)^2+1)d^2(d+D)^2(2nd(d+D)+1) = \mathrm{O}(n^2d^8(d+D)^5)$$

and the sequential complexity of this algorithm amounts to $\mathrm{O}(n^4d)$ arithmetic operations in $\mathbf{A}$ on elements of degree bounded by $\mathrm{O}(n^2d^8(d+D)^5)$.

Proof

In Step 1: $\deg w_i \leq d+D$, $\deg(\alpha_i r_i) \leq \frac{d^4}{4}(d+D+1)^2$ (see Corollary 3), $\deg f_i \leq d+D$ and $\deg g_i \leq d$.

In Step 2: H_i is the product of $2n+1$ elementary matrices in $\mathrm{M}_n(\mathbf{A}[X]\frac{1}{r_i})$, $r_iH_i \in \mathrm{M}_n(\mathbf{A}[X])$ and $\deg(r_iH_i) \leq d(d+D)^2$. Thus, $\tilde{H}_i$ is the product of $2(2n+1)$ elementary matrices in $\mathrm{M}_n(\mathbf{A}[X]\frac{1}{r_i})$, $r_i^2\tilde{H}_i \in \mathrm{M}_n(\mathbf{A}[X])$ and $\deg(r_i^2\tilde{H}_i) \leq 2d(d+D)^2$.

In Step 3: G_i is the product of $4(2n+1)$ elementary matrices in $\mathrm{M}_n(\mathbf{A}[X]\frac{1}{r_i})$. Moreover,

$$\deg(r_i^2\tilde{H}_i(X + r_i^{2n}Y)) \leq 2d(d+D)^2(2nd(d+D))$$

and

$$\deg(r_i^2\tilde{H}_i(X))^{-1} \leq 2d(d+D)^2.$$

Thus,

$$\deg G_i \leq 2d(d+D)^2(2nd(d+D)+1).$$

In Step 4: $\deg(\beta_i r_i^{2n}) \leq 2n\frac{d^5}{4}(d+D+1)^2 = \frac{1}{2}nd^5(d+D+1)^2$,

$$\deg G_i(X + (\beta_1 r_1^{2n} + \cdots + \beta_{i-1}r_{i-1}^{2n})Y, \beta_i Y) \leq$$

$$\left(\frac{1}{2}nd^5(d+D+1)^2+1\right)2d(d+D)^2(2nd(d+D)+1).$$

Thus,

$$\deg \tilde{G} \leq (\frac{1}{2}nd^5(d+D+1)^2+1)2d^2(d+D)^2(2nd(d+D)+1) = \mathrm{O}(n^2d^8(d+D)^5).$$

Moreover, $\tilde{G}$ is the product of at most $4d(2n+1)$ elementary matrices in $\mathrm{M}_n(\mathbf{A}[X]\frac{1}{r_i})$.

Of course, for the complexity of this algorithm, we did not consider the possibility of a fast matrix multiplication process. □

Note that, contrary to the papers Logar and Sturmfels (1992); Park and Woodburn (1995), our algorithm for unimodular reduction does not use the fact that the basic ring is Noetherian.

An algorithm for unimodular completion: case of $\mathbf{K}[X_1, \ldots, X_k]$ *where* $\mathbf{K}$ *is an infinite field.*

In the following algorithm $\mathbf{K}$ will denote an infinite field (e.g. $\mathrm{Char}\,\mathbf{K} = 0$), with an infinite sequence of pairwise distinct elements (y_i).

We also use $\underline{X} = (X_1, \ldots, X_k)$.

Input: Two columns $\mathcal{V} = \mathcal{V}(\underline{X}) = {}^{\mathrm{t}}(v_1(\underline{X}), \ldots, v_n(\underline{X}))$, $\mathcal{U} = \mathcal{U}(\underline{X}) = {}^{\mathrm{t}}(u_1(\underline{X}), \ldots, u_n(\underline{X})) \in \mathbf{K}[\underline{X}]^n$ such that $\mathcal{V}\,{}^{\mathrm{t}}\mathcal{U} = 1$, with $1+\max_{1\leq i\leq n}\{\deg v_i\} = d$ (where $d \geq 2$) and $\max_{1\leq i\leq n}\{\deg u_i\} = D$.

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

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

Step 1: Make a linear change of variables so that v_1 becomes monic at X_j.

Step 2 Perform the general algorithm with $\mathbf{A} = \mathbf{K}[X_1, \ldots, X_{j-1}]$ and $X = X_j$. Output the new $\mathcal{V}$ and $\mathcal{U}$.

Note that if D is deduced from d by the effective Nullstellensatz Fitchas and Galligo (1990), that is if only $\mathcal{V} = \mathcal{V}(\underline{X}) = {}^{\mathrm{t}}(v_1(\underline{X}), \ldots, v_n(\underline{X})) \in \mathrm{Um}_n(\mathbf{K}[\underline{X}])$ is given as input, then $D = d^k$.

So we get the following complexity bounds. In Proposition 6 we treat the case where both of $\mathcal{V}$ and $\mathcal{U}$ are given as input as well as the case where only $\mathcal{V}$ is given as input.

Proposition 6 (complexity bounds, 2)

(1) The matrix G *obtained after the first iteration (that is, after eliminating* X_k*) is the product of at most* d *matrices in* $\mathrm{SL}_n(\mathbf{K}[\underline{X}])$ *obtained as the product of at most* $4d(2n+1) = \mathrm{O}(n\,d)$ *elementary matrices* $M_{i,k} \in \mathrm{M}_n(\mathbf{K}[\underline{X}]_{\frac{1}{r_{i,k}}})$ *where* $r_{i,k} = \mathrm{Res}_{X_k}(v_1(\underline{X}), w_i(\underline{X}))$, $1 \leq i \leq \deg_{X_k} v_1 + 1$,

and $w_i = v_2 + y_i(u_3v_3 + \cdots + u_nv_n)$. *Moreover,*

$$\deg G \leq 2(\frac{1}{2}nd^5(d+D+1)^2+1)d^2(d+D)^2(2nd(d+D)+1) = \mathrm{O}(n^2d^8(d+D)^5)$$

and the sequential complexity of this algorithm amounts to $(nd(d+D))^{\mathrm{O}(k)} = (nd)^{\mathrm{O}(k^2)}$ *field operations in* $\mathbf{K}$.

(2) The final matrix M *obtained after* k *iterations is the product of at most* dk *matrices in* $\mathrm{SL}_n(\mathbf{K}[\underline{X}])$ *obtained as the product of at most* $4dk(2n+1) = \mathrm{O}(k\,n\,d)$ *elementary matrices* $M_{i,j} \in \mathrm{M}_n(\mathbf{K}[\underline{X}]\frac{1}{r_{i,j}})$ *where*
$r_{i,j} = \mathrm{Res}_{X_j}(v_1(X_1,\ldots,X_j,0,\ldots,0), w_i(X_1,\ldots,X_j,0,\ldots,0))$,
$1 \leq i \leq \deg_{X_j} v_1(X_1,\ldots,X_j,0,\ldots,0)+1$, $1 \leq j \leq k$ *and*
$w_i = v_2 + (i-1)(u_3v_3 + \cdots + u_nv_n)$.
Moreover,

$$\deg M \leq 2k(\frac{1}{2}nd^5(d+D+1)^2+1)d^2(d+D)^2(2nd(d+D)+1) = \mathrm{O}(kn^2d^8(d+D)^5)$$

and the sequential complexity of this algorithm amounts to $(nd(d+D))^{\mathrm{O}(k)} = (nd)^{\mathrm{O}(k^2)}$ *field operations in* $\mathbf{K}$.

Proof. Note that $\mathcal{V}(X_1,\ldots,X_{j-1},0)\,{}^t\mathcal{U}(X_1,\ldots,X_{j-1},0) = 1$,

$$1 + \max_{1\leq i\leq n}\{\deg v_i(X_1,\ldots,X_{j-1},0)\} \leq d$$

and $\max_{1\leq i\leq n}\{\deg u_i(X_1,\ldots,X_{j-1},0)\} \leq D$. So it suffices to give the bound for Step 2 and to raise at the power k.

Since the product of two matrices in $\mathrm{M}_n(\mathbf{K}[\underline{X}])$ of degree $\leq d'$ requires $\mathrm{O}(n^3(d')^{2k})$ field operations, we infer from Proposition 5 that the complexity of the algorithm computing G amounts to $(nd(d+D))^{\mathrm{O}(k)}$ ($d' = n^2d^8(d+D)^5$). □

Remark.
1) As explained in Fitchas and Galligo (1990); Logar and Sturmfels (1992); Park and Woodburn (1995), our algorithm for unimodular completion can be used to obtain an algorithm for the Quillen-Suslin theorem. Precise bounds have been computed by some authors concerning algorithms for the Quillen-Suslin theorem based on Suslin's proof of Serre's Conjecture. The best bounds are given in Caniglia et al. (1993) and have been already announced in Fitchas and Galligo (1990). Note that in Caniglia et al. (1993), the authors treat globally unimodular matrices since treating a unimodular matrix column by column produces doubly exponential bounds. So, a comparison between our algorithm and theirs can only be made in the unimodular completion case. As mentioned in Caniglia et al. (1993), the orders of degree and complexity bounds they obtained cannot be improved. Contrary to the algorithms found in Caniglia et al. (1993) and Fitchas and Galligo (1990) which use essentially

Suslin's method Suslin (1977) (A transitivity theorem) and are similar to the formulation given below, our algorithm follows the concrete local-global principle descibed in Lombardi and Quitté (2003) and the form of the obtained factors is different. The main feature of our algorithm is its simplicity which will certainly facilitate its implementation and the fact that it considerably reduces the number of factors occuring in the computation of M. Moreover, by this algorithm, we show that the concrete local-global principles Lombardi and Quitté (2003) can produce competitive complexity bounds.

2) Another alternative would be to follow what Suslin did in Paragraph 2 (A transitivity theorem) of Suslin (1977). This has been explained constructively in Fitchas and Galligo (1990) (Theorem 15). With analogous calculation to what Fitchas and Galligo did in Fitchas and Galligo (1990), we can then obtain the following formulation and bounds (with a number of factors lower than the one obtained in Fitchas and Galligo (1990) and Caniglia et al. (1993), similar degree bound, and slightly better complexity bound):

Let $\mathbf{K}$ *be an infinite field,* $\mathcal{V} = {}^{\mathrm{t}}(v_1(\underline{X}), \ldots, v_n(\underline{X})) \in \mathrm{Um}_n(\mathbf{K}[\underline{X}])$ *such that* $1 + \max_{1 \leq i \leq n}\{\deg v_i\} = d$ *(where* $d \geq 2$*). Then, there exists a matrix* $M \in \mathrm{SL}_n(\mathbf{K}[\underline{X}])$ *satisfying the following properties*

(i) $M\mathcal{V} = {}^{\mathrm{t}}(1, 0, \ldots, 0)$.

(ii) $\deg M = d^{\mathrm{O}(k)}$.

(iii) M *has a representation* $M = N_1 \cdots N_p$ *as a product of* $p \leq 2knd$ *matrices* $N_h \in \mathbf{K}[\underline{X}]^{n \times n}$

such that for $1 \leq h \leq p$, $\deg N_h = d^{\mathrm{O}(k)}$, N_h *is an elementary matrix or has the form*

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

with $N'_h \in \mathrm{SL}_2(\mathbf{K}[\underline{X}])$.

(iv) M *can be computed in sequential time* $n^3 d^{\mathrm{O}(k^2)}$.

3) Using Corollary 3 and some classical steps used in Kunz (1991), Lam (1978), Lombardi and Quitté (2003), Park and Woodburn (1995), or Suslin (1977), we

can obtain an algorithm for reducing unimodular rows by elementary matrices. As shown in Park and Woodburn (1995) (Section 4), an algorithm for the Suslin's stability theorem ($\mathrm{SL}_n(\mathbf{K}[\underline{X}]) = \mathrm{E}_n(\mathbf{K}[\underline{X}])$) can be obtained by $n-3$ iterations of this algorithm coupled with an algorithm for the Suslin's stability theorem in the particular case the given unimodular matrix has the form

$$\begin{pmatrix} p & q & 0 \\ r & s & 0 \\ 0 & 0 & 1 \end{pmatrix} \in \mathrm{SL}_3(\mathbf{K}[\underline{X}]),$$

where p is monic in the last variable X_k. Unfortunately, these iterations produce an explosion of the degree of the considered unimodular matrix and produce a double-exponential complexity.

References

Caniglia, L., Cortinas, G., Danon, S., Heintz, J., Krick, T., Solerno, P., 1993. Algorithmic aspects of Suslin's proof of Serre's conjecture. Comput. Complexity 3, 31–55.

Fitchas, N., Galligo, A., 1990. Nullstellensatz effectif et conjecture de Serre (théorème de Quillen-Suslin) pour le calcul formel. Math. Nachr. 149, 231–253.

Kunz, E., 1991. Introduction to Commutative Algebra and Algebraic Geometry. Birkhäuser.

Lam, T., 1978. Serre's conjecture. Vol. 635 of Lecture Notes in Mathematics. Springer-Verlag, Berlin-New York.

Logar, A., Sturmfels, B., 1992. Algorithms for the Quillen-Suslin Theorem. J. Algebra 145 (1), 231–239.

Lombardi, H., Quitté, C., 2003. Constructions cachées en algèbre abstraite (2) le principe local-global. In: Fontana, M., Kabbaj, S.-E., Wiegand, S. (Eds.), Commutative ring theory and applications. Vol. 231 of Lecture notes in pure and applied mathematics. M. Dekker, pp. 461–476.

Park, H., Woodburn, C., 1995. An algorithmic proof of Suslin's stability theorem for polynomial rings. J. Algebra 178, 277–298.

Suslin, A., 1977. On the structure of the special linear group over polynomial rings. Math. USSR-Izv. 11, 221–238.

Yengui, I., 2004. Making the use of maximal ideals constructive, [preprint].