An Algorithmic Proof of Suslin's Stability Theorem for Polynomial Rings

Hyungju Park* Cynthia Woodburn†

Abstract

Let k be a field. Then Gaussian elimination over k and the Euclidean division algorithm for the univariate polynomial ring $k[x]$ allow us to write any matrix in $SL_n(k)$ or $SL_n(k[x])$, $n \geq 2$, as a product of elementary matrices. Suslin's stability theorem states that the same is true for $SL_n(k[x_1, \ldots, x_m])$ with $n \geq 3$ and $m \geq 1$. In this paper, we present an algorithmic proof of Suslin's stability theorem, thus providing a method for finding an explicit factorization of a given polynomial matrix into elementary matrices. Gröbner basis techniques may be used in the implementation of the algorithm.

1 Introduction

Immediately after proving the famous Serre's Conjecture (which is now known as the Quillen-Suslin theorem) in 1976 [Sus76], A.A. Suslin went on to prove the following K_1-analogue of Serre's Conjecture [Sus77].

> **Suslin's Stability Theorem.** Let R be a commutative Noetherian ring and $n \geq \max(3, \dim(R) + 2)$. Then, any $n \times n$ matrix $A = (f_{ij})$ of determinant 1, with f_{ij} elements of the polynomial ring $R[x_1, \ldots, x_m]$, can be written as a product of elementary matrices over $R[x_1, \ldots, x_m]$.

*Dept. of Mathematics, University of California, Berkeley, CA 94720; e-mail: park@math.berkeley.edu

†Dept. of Mathematics, Pittsburg State University, Pittsburg, KS 66762; e-mail: cwoodbur@mail.pittstate.edu

Recall that for any ring R, an $n \times n$ elementary matrix $E_{ij}(a)$ over R is a matrix of the form $I + a \cdot e_{ij}$ where $i \neq j, a \in R$ and e_{ij} is the $n \times n$ matrix whose (i, j) entry is 1 and all other entries are zero. Let $SL_n(R)$ be the group of all the $n \times n$ matrices of determinant 1 whose entries are elements of R, and let $E_n(R)$ be the subgroup of $SL_n(R)$ generated by the elementary matrices. Then Suslin's stability theorem can be expressed as

$$SL_n(R[x_1, \ldots, x_m]) = E_n(R[x_1, \ldots, x_m]) \quad \text{for all } n \geq \max(3, \dim(R) + 2).$$

In this paper, we develop an algorithmic proof of the above assertion over a field $R = k$. For a given $A \in SL_n(k[x_1, \ldots, x_m])$ with $n \geq 3$, the algorithm produces elementary matrices $E_1, \ldots, E_t \in E_n(k[x_1, \ldots, x_m])$ such that $A = E_1 \cdots E_t$. Implementation of this algorithm involves use of the method of Gröbner bases, an important tool in computational algebra and computational algebraic geometry. See [CLO92] and [Mis93] for more information on Gröbner bases and applications.

Definition 1.1 *A square matrix A over a ring R is called* **realizable**, *if A can be written as a product of elementary matrices over R.*

The contents of this paper are as follows:

- In Section 2, an algorithmic proof of the normality of $E_n(k[x_1, \ldots, x_m])$ in $SL_n(k[x_1, \ldots, x_m])$ for $n \geq 3$ is given.
- In Section 3, we give an algorithm for the *Quillen Induction Process*, a standard way of reducing a given problem over a ring to an easier problem over a local ring. Using this *Quillen Induction Algorithm*, we reduce our realization problem over the polynomial ring $R[x_m]$ to one over $R_{\mathcal{M}}[x_m]$'s, where $R = k[x_1, \ldots, x_{m-1}]$ and $\mathcal{M}$ ranges over a finite set of a maximal ideals of R.
- In Section 4, an algorithmic proof of the *Elementary Column Property*, a stronger version of the *Unimodular Column Property*, is given, and we note that this algorithm gives another constructive proof of the Quillen-Suslin theorem. Using the *Elementary Column Property*, we

show that a realization algorithm for $SL_n(k[x_1, \ldots, x_m])$ is obtained from a realization algorithm for matrices of the special form

$$\begin{pmatrix} p & q & 0 \\ r & s & 0 \\ 0 & 0 & 1 \end{pmatrix} \in SL_3(k[x_1, \ldots, x_m]),$$

where p is monic in the last variable x_m.

- In Section 5, in view of the results in the preceding two sections, we note that a realization algorithm over $k[x_1, \ldots, x_m]$ can be obtained from a realization algorithm for the matrices of the special form $\begin{pmatrix} p & q & 0 \\ r & s & 0 \\ 0 & 0 & 1 \end{pmatrix}$ over $R[X]$, where R is now a local ring and p is monic in X. A realization algorithm for this case was already found by M.P. Murthy in [GM80]. We reproduce Murthy's algorithm in this section.

- In Section 6, we suggest using the Steinberg relations from algebraic K-theory to lower the number of elementary matrix factors in a factorization produced by our algorithm. We also mention an ongoing effort of using our algorithm in Signal Processing.

2 $E_n(k[x_1, \ldots, x_m]) \trianglelefteq SL_n(k[x_1, \ldots, x_m])$, for $n \geq 3$

Lemma 2.1 *The Cohn matrix* $A = \begin{pmatrix} 1+xy & x^2 \\ -y^2 & 1-xy \end{pmatrix}$ *is not realizable, but* $\begin{pmatrix} A & 0 \\ 0 & 1 \end{pmatrix} \in SL_3(k[x,y])$ *is.*

Proof: The nonrealizability of A was first proved by P. M. Cohn in [Coh66], and a complete algorithmic criterion for the realizability of matrices in $SL_2(k[x_1, \ldots, x_m])$ was recently developed in [THK94]. Now consider

$$\begin{pmatrix} A & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1+xy & x^2 & 0 \\ -y^2 & 1-xy & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Noting that $\begin{pmatrix} 1+xy & x^2 & 0 \\ -y^2 & 1-xy & 0 \\ 0 & 0 & 1 \end{pmatrix} = I + \begin{pmatrix} x \\ -y \\ 0 \end{pmatrix} \cdot (y, x, 0)$, we see that the realizability of this matrix is a special case of Lemma 2.3 below. $\square$

Definition 2.2 *Let $n \geq 2$. A* **Cohn-type matrix** *is a matrix of the form*

$$I + a\mathbf{v} \cdot (v_j \mathbf{e_i} - v_i \mathbf{e_j})$$

where $\mathbf{v} = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \in (k[x_1, \ldots, x_m])^n$, $i < j \in \{1, \ldots, n\}$, $a \in k[x_1, \ldots, x_m]$, *and* $\mathbf{e_i} = (0, \ldots, 0, 1, 0, \ldots, 0)$ *with* 1 *occurring only at the* i*-th position.*

Lemma 2.3 *Any Cohn-type matrix for $n \geq 3$ is realizable.*

Proof: First, consider the case $i = 1, j = 2$. In this case,

$$\begin{aligned}
B &= I + a \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \cdot (v_2, -v_1, 0, \ldots, 0) \\
&= \begin{pmatrix} 1 + av_1v_2 & -av_1^2 & 0 & \cdots & 0 \\ av_2^2 & 1 - av_1v_2 & 0 & \cdots & 0 \\ av_3v_2 & -av_3v_1 & & & \\ \vdots & \vdots & & I_{n-2} & \\ av_nv_2 & -av_nv_1 & & & \end{pmatrix} \\
&= \begin{pmatrix} 1 + av_1v_2 & -av_1^2 & 0 & \cdots & 0 \\ av_2^2 & 1 - av_1v_2 & 0 & \cdots & 0 \\ 0 & 0 & & & \\ \vdots & \vdots & & I_{n-2} & \\ 0 & 0 & & & \end{pmatrix} \prod_{l=3}^{n} E_{l1}(av_lv_2)E_{l2}(-av_lv_1).
\end{aligned}$$

So, it is enough to show that

$$A = \begin{pmatrix} 1 + av_1v_2 & -av_1^2 & 0 \\ av_2^2 & 1 - av_1v_2 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

is realizable for any $a, v_1, v_2 \in k[x_1, \ldots, x_m]$. Let "$\rightarrow$" indicate that we are applying elementary operations, and consider the following:

$$
\begin{aligned}
A &= \begin{pmatrix} 1+av_1v_2 & -av_1^2 & 0 \\ av_2^2 & 1-av_1v_2 & 0 \\ 0 & 0 & 1 \end{pmatrix} \rightarrow \begin{pmatrix} 1+av_1v_2 & -av_1^2 & v_1 \\ av_2^2 & 1-av_1v_2 & v_2 \\ 0 & 0 & 1 \end{pmatrix} \\
&\rightarrow \begin{pmatrix} 1 & -av_1^2 & v_1 \\ 0 & 1-av_1v_2 & v_2 \\ -av_2 & 0 & 1 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 0 & v_1 \\ 0 & 1 & v_2 \\ -av_2 & av_1 & 1 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 0 & v_1 \\ 0 & 1 & v_2 \\ 0 & av_1 & 1+av_1v_2 \end{pmatrix} \\
&\rightarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & v_2 \\ 0 & av_1 & 1+av_1v_2 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & v_2 \\ 0 & 0 & 1 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.
\end{aligned}
\tag{2.1}
$$

Keeping track of all the elementary operations involved in 2.1, we get

$$A = E_{13}(-v_1)E_{23}(-v_2)E_{31}(-av_2)E_{32}(av_1)E_{13}(v_1)E_{23}(v_2)E_{31}(av_2)E_{32}(-av_1).$$

In general (i.e., for arbitrary $i < j$),

$$B = I + a \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \cdot (0, \ldots, 0, v_j, 0, \ldots, 0, -v_i, 0, \ldots, 0)$$

with v_j occuring at the i-th position and $-v_i$ occuring at the j-th position. Therefore, we have

$$
B = \begin{pmatrix}
1 & \cdots & av_1v_j & \cdots & -av_1v_i & \cdots & 0 \\
 & \ddots & \vdots & & \vdots & & 0 \\
 & & 1+av_iv_j & & -av_i^2 & & \\
 & & \vdots & & \vdots & & \\
 & & av_j^2 & & 1-av_iv_j & & \\
 & & \vdots & & \vdots & & \\
 & & v_nv_j & & -v_nv_i & & 1
\end{pmatrix}
$$

$$
= \begin{pmatrix} 1 & \cdots & 0 & \cdots & 0 & \cdots & 0 \\ & \ddots & \vdots & & \vdots & & 0 \\ & & 1+av_iv_j & & -av_i^2 & & \\ & & \vdots & & \vdots & & \\ & & av_j^2 & & 1-av_iv_j & & \\ & & \vdots & & \vdots & & \\ & & 0 & & 0 & & 1 \end{pmatrix} \cdot \prod_{\substack{1\le l\le n \\ l\ne i,j}} E_{li}(av_lv_j)E_{lj}(-av_lv_i)
$$

$$
\begin{aligned}
= \; & E_{it}(-v_i)E_{jt}(-v_j)E_{ti}(-av_j)E_{tj}(av_i)E_{it}(v_i)E_{jt}(v_j)E_{ti}(av_j)E_{tj}(-av_i) \\
& \cdot \prod_{\substack{1\le l\le n \\ l\ne i,j}} E_{li}(av_lv_j)E_{lj}(-av_lv_i),
\end{aligned}
$$

where $t \in \{1,\ldots,n\}$ can be chosen to be any number other than i or j. $\square$

Since a Cohn-type matrix is realizable, any product of Cohn-type matrices is also realizable. This observation motivates the following generalization of the above lemma.

Definition 2.4 *Let R be a ring and $\mathbf{v} = (v_1,\ldots,v_n)^t \in R^n$ for some $n \in I\!N$. Then* $\mathbf{v}$ *is called a* **unimodular column vector** *if its components generate R, i.e. if there exist $g_1,\ldots,g_n \in R$ such that $v_1g_1 + \cdots + v_ng_n = 1$.*

Remark 2.5 When $R = k[x_1,\ldots,x_m]$ is a polynomial ring and $\mathbf{v} \in R^n$ is a unimodular vector, we can explicitly find these g_i's by either using the effective Nullstellensatz (see [FG90]) or Gröbner bases (see [CLO92]).

Lemma 2.6 *Suppose that $A \in SL_n(k[x_1,\ldots,x_m])$ with $n \ge 3$ can be written in the form $A = I + \mathbf{v}\cdot\mathbf{w}$ for a unimodular column vector $\mathbf{v}$ and a row vector $\mathbf{w}$ over $k[x_1,\ldots,x_m]$ such that $\mathbf{w}\cdot\mathbf{v} = 0$. Then A is realizable.*

Proof: Since $\mathbf{v} = (v_1,\ldots,v_n)^t$ is unimodular, we can find $g_1,\ldots,g_n \in k[x_1,\ldots,x_m]$ such that $v_1g_1 + \cdots + v_ng_n = 1$. This, combined with $\mathbf{w}\cdot\mathbf{v} = w_1v_1 + \cdots + w_nv_n = 0$, yields a new expression for $\mathbf{w}$:

$$
\mathbf{w} \;=\; \sum_{i<j} a_{ij}(v_j\mathbf{e_i} - v_i\mathbf{e_j})
$$

where $a_{ij} = w_i g_j - w_j g_i$. Now,

$$\begin{aligned} A &= I + \mathbf{v} \cdot \left(\sum_{i<j} a_{ij}(v_j \mathbf{e_i} - v_i \mathbf{e_j}) \right) \\ &= I + \sum_{i<j} \mathbf{v} \cdot a_{ij}(v_j \mathbf{e_i} - v_i \mathbf{e_j}) \\ &= \prod_{i<j} \left(I + \mathbf{v} \cdot a_{ij}(v_j \mathbf{e_i} - v_i \mathbf{e_j}) \right). \end{aligned}$$

Each factor on the right hand side of this equation is a Cohn-type matrix and thus realizable, so A is also realizable. □

Corollary 2.7 *$BE_{ij}(a)B^{-1}$ is realizable for any $B \in GL_n(k[x_1, \ldots, x_m])$ with $n \geq 3$ and $a \in k[x_1, \ldots, x_m]$.*

Proof: Note that $i \neq j$, and

$$BE_{ij}(a)B^{-1} = I + (i\text{-th column vector of } B) \cdot a \cdot (j\text{-th row vector of } B^{-1}).$$

Let $\mathbf{v}$ be the i-th column vector of B and $\mathbf{w}$ be a times the j-th row vector of B^{-1}. Then (i-th row vector of B^{-1}) $\cdot \mathbf{v} = 1$ implies $\mathbf{v}$ is unimodular, and $\mathbf{w} \cdot \mathbf{v}$ is clearly zero since $i \neq j$. Therefore, $BE_{ij}(a)B^{-1} = I + \mathbf{v} \cdot \mathbf{w}$ satisfies the condition of the above lemma, and is thus realizable. □

Corollary 2.8 *For $n \geq 3$, $E_n(k[x_1, \ldots, x_m])$ is a normal subgroup of $SL_n(k[x_1, \ldots, x_m])$.*

Proof: Let $A \in SL_n(k[x_1, \ldots, x_m])$ and $E \in E_n(k[x_1, \ldots, x_m])$. Then the above corollary gives us an algorithm for finding elementary matrices $E_1, \ldots, E_t$ such that $A^{-1}EA = E_1 \cdots E_t$. □

3 Gluing of Local Realizability

Let $R = k[x_1, \ldots, x_{m-1}]$, $X = x_m$ and $\mathcal{M} \in \mathrm{Max}(R)$ ={maximal ideals of R}. For $A \in SL_n(R[X])$, we let $A_{\mathcal{M}} \in SL_n(R_{\mathcal{M}}[X])$ be its image under the canonical mapping $SL_n(R[X]) \to SL_n(R_{\mathcal{M}}[X])$. We will occasionally write $A = A(X)$ to emphasize that we are viewing the entries of the matrix A as polynomials in one variable. Now consider the following analogue of Quillen's patching theorem for elementary matrices:

> Suppose $n \geq 3$ and $A \in SL_n(R[X])$. Then A is realizable over $R[X]$ if and only if $A_{\mathcal{M}} \in SL_n(R_{\mathcal{M}}[X])$ is realizable over $R_{\mathcal{M}}[X]$ for every $\mathcal{M} \in \mathrm{Max}(R)$.

While a non-constructive proof of this assertion is given in [Sus77] and a more general functorial treatment of this Quillen Induction Process can be found in [Knu91], we will give a constructive proof for it here, thus providing a patching algorithm with input certain local factorizations of a given matrix A and output a global factorization of A into elementary matrices. Since the necessity of the condition is clear, we have to prove the following theorem.

Theorem 3.1 *(Quillen Induction Algorithm) Let $A \in SL_n(R[X])$. If $A_{\mathcal{M}} \in E_n(R_{\mathcal{M}}[X])$ for every $\mathcal{M} \in \mathrm{Max}(R)$, then $A \in E_n(R[X])$.*

Proof: Let $\mathbf{a_1} = (0, \ldots, 0) \in k^{m-1}$, and let $\mathcal{M}_1 = \{g \in k[x_1, \ldots, x_{m-1}] \mid g(\mathbf{a_1}) = 0\}$ be the corresponding maximal ideal. Then by assumption, $A_{\mathcal{M}_1}$ is realizable over $R_{\mathcal{M}_1}[X]$. Hence, we can write

$$A_{\mathcal{M}_1} = \prod_j E_{s_j t_j}\left(\frac{c_j}{d_j}\right) \tag{2.2}$$

where $c_j, d_j \in R, d_j \notin \mathcal{M}_1$. Letting $r_1 = \prod_j d_j \notin \mathcal{M}_1$, we can rewrite 2.2 as

$$A_{\mathcal{M}_1} = \prod_j E_{s_j t_j}\left(\frac{c_j \prod_{k \neq j} d_k}{r_1}\right) \in E_n(R_{r_1}) \subset E_n(R_{\mathcal{M}_1}).$$

Denote an algebraic closure of k by $\bar{k}$. Inductively, let $\mathbf{a_j} \in \bar{k}^{m-1}$ be a common zero of $r_1, \ldots, r_{j-1}$ and $\mathcal{M}_j = \{g \in k[x_1, \ldots, x_{m-1}] \mid g(\mathbf{a_j}) = 0\}$ be the corresponding maximal ideal of R for each $j \geq 2$. (See [CLO92] for details and references for using Gröbner bases to find a common zero of a finite set of polynomials.) Define $r_j \notin \mathcal{M}_j$ in the same way as r_1 above, so that

$$A_{\mathcal{M}_j} \in E_n(R_{r_j}[X]).$$

Since $\mathbf{a_j}$ is a common zero of $r_1, \ldots, r_{j-1}$ in this construction, we immediately see that $r_1, \ldots, r_{j-1} \in \mathcal{M}_j = \{g \in R \mid g(\mathbf{a_j}) = 0\}$. But noting $r_j \notin \mathcal{M}_j$, we conclude that $r_j \notin r_1 R + \cdots + r_{j-1} R$. Now, since R is Noetherian, we will get to some l after a finite number of steps such that $r_1 R + \cdots + r_l R = R$. (We can use Gröbner bases to determine when 1_R is in the ideal $r_1R + \cdots + r_lR$, e.g. see [CLO92].)

Let d be a natural number. Then since $r_1^dR + \cdots + r_l^dR = R$, we can find $g_1, \ldots, g_l \in R$ such that $r_1^dg_1 + \cdots + r_l^dg_l = 1$. Now, we express $A(X) \in SL_n(R[X])$ in the following way:

$$\begin{aligned}
A(X) &= A(X - Xr_1^dg_1) \cdot [A^{-1}(X - Xr_1^dg_1)A(X)] \\
&= A(X - Xr_1^dg_1 - Xr_2^dg_2) \cdot [A^{-1}(X - Xr_1^dg_1 - Xr_2^dg_2)A(X - Xr_1^dg_1)] \\
&\quad \cdot [A^{-1}(X - Xr_1^dg_1)A(X)] \\
&= \cdots \\
&= A(X - \sum_{i=1}^{l} Xr_i^dg_i) \cdot [A^{-1}(X - \sum_{i=1}^{l} Xr_i^dg_i)A(X - \sum_{i=1}^{l-1} Xr_i^dg_i)] \cdots \\
&\quad \cdots [A^{-1}(X - Xr_1^dg_1)A(X)].
\end{aligned}$$

Note here that the first matrix $A(X - \sum_{i=1}^{l} Xr_i^dg_i) = A(0)$ on the right hand side is in $E_n(R)$ by the induction hypothesis. We will now show that for a sufficiently large d, each bracketed expression in the above equation is actually in $E_n(R[X])$, so that A itself is in $E_n(R[X])$. To this end, we let $A_{\mathcal{M}_i} = A_i$ and identify $A \in SL_n(R[X])$ with $A_i \in SL_n(R_{\mathcal{M}_i}[X])$. Then each bracketed expression is of the form

$$A_i^{-1}(cX)A_i((c + r_i^dg)X).$$

Claim: For any $c, g \in R$, we can find a sufficiently large d such that $A_i^{-1}(cX)A_i((c + r_i^dg)X) \in E_n(R[X])$ for $i = 1, \ldots, l$.
Let

$$D_i(X, Y, Z) = A_i^{-1}(Y \cdot X)A_i((Y + Z) \cdot X) \in E_n(R_{r_i}[X, Y, Z])$$

and write D_i in the form

$$D_i = \prod_{j=1}^{h} E_{s_jt_j}(b_j + Zf_j)$$

where $b_j \in R_{r_i}[X, Y]$ and $f_j \in R_{r_i}[X, Y, Z]$. ¿From now on, the elementary matrix $E_{s_jt_j}(a)$ will be simply denoted as $E^j(a)$ for notational convenience.

For $p = 1, \ldots, h$, define C_p by

$$C_p = \prod_{j=1}^{p} E^j(b_j) \in E_n(R_{r_i}[X, Y]).$$

Then the C_p's satisfy the following recursive relations:

$$\begin{array}{rcl} E^1(b_1) &=& C_1, \\ E^p(b_p) &=& C_{p-1}^{-1} C_p \quad (2 \leq p \leq h), \\ C_h &=& I. \end{array}$$

Hence, using the fact that $E_{ij}(a + b) = E_{ij}(a)E_{ij}(b)$, we have

$$\begin{array}{rcl} D_i &=& \prod_{j=1}^{h} E^j(b_j + Zf_j) \\ &=& \prod_{j=1}^{h} E^j(b_j)E^j(Zf_j) \\ &=& [E^1(b_1)E^1(Zf_1)][E^2(b_2)E^2(Zf_2)] \ \cdots \ [E^h(b_h)E^h(Zf_h)] \\ &=& [C_1E^1(Zf_1)][C_1^{-1}C_2E^2(Zf_2)] \ \cdots \ [C_{h-1}^{-1}C_hE^h(Zf_h)] \\ &=& \prod_{j=1}^{h} C_jE^j(Zf_j)C_j^{-1}. \end{array}$$

Now in the same way as in the proof of Lemma 2.6 and Corollary 2.7, we can write $C_jE^j(Zf_j)C_j^{-1}$ as a product of Cohn-type matrices, i.e. for any given $j \in \{1, \ldots, h\}$, let $\mathbf{v} = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}$ be the s_j-th column vector of C_j. Then

$$C_jE_{s_jt_j}(Zf_j)C_j^{-1} = \prod_{1 \leq \gamma < \delta \leq n} [I + \mathbf{v} \cdot Zf_j \cdot a_{\gamma\delta}(v_\gamma \mathbf{e}_\delta - v_\delta \mathbf{e}_\gamma)]$$

for some $a_{\gamma\delta} \in R_{r_i}[X, Y]$. Also, we can find a natural number d such that

$$v_\gamma = \frac{v'_\gamma}{r_i^d}, \quad a_{\gamma\delta} = \frac{a'_{\gamma\delta}}{r_i^d}, \quad f_j = \frac{f'_j}{r_i^d}$$

for some $v'_\gamma, a'_{\gamma\delta} \in R[X,Y]$, $f'_j \in R[X,Y,Z]$. Now, replacing Z by $r_i^{4d}g$, we see that all the Cohn-type matrices in the above expression for $C_jE^j(Zf_j)C_j^{-1}$ have denominator-free entries. Therefore,

$$C_jE^j(r_i^{4d}gf_j)C_j^{-1} \in E_n(R[X,Y]).$$

Since this is true for each j, we conclude that for a sufficiently large d,

$$D_i(X,Y,r_i^d g) = \prod_{j=1}^{h} C_jE^j(r_i^d g f_j)C_j^{-1} \in E_n(R[X,Y]).$$

Now, setting $Y = c$ proves the claim, and completes the proof of the theorem. □

4 Reduction to $SL_3(k[x_1, \ldots, x_m])$

Let $A \in SL_n(k[x_1,\ldots,x_m])$ with $n \geq 3$, and let $\mathbf{v}$ be its last column vector. Then $\mathbf{v}$ is unimodular. (Recall that the cofactor expansion along the last column gives a required relation.) Now, if we can reduce $\mathbf{v}$ to $\mathbf{e_n} = (0,0,\ldots,0,1)^t$ by applying elementary operations, i.e. if we can find $B \in E_n(k[x_1,\ldots,x_m])$ such that $B\mathbf{v} = \mathbf{e_n}$, then

$$BA = \begin{pmatrix} & & & 0 \\ & \tilde{A} & & \vdots \\ & & & 0 \\ p_1 & \ldots & p_{n-1} & 1 \end{pmatrix}$$

for some $\tilde{A} \in SL_{n-1}(k[x_1,\ldots,x_m])$ and $p_i \in k[x_1,\ldots,x_m]$ for $i = 1,\ldots,n-1$. Hence,

$$BAE_{n1}(-p_1)\cdots E_{n(n-1)}(-p_{n-1}) = \begin{pmatrix} \tilde{A} & 0 \\ 0 & 1 \end{pmatrix}.$$

Therefore, our problem of expressing $A \in SL_n(k[x_1,\ldots,x_m])$ as a product of elementary matrices is now reduced to the same problem for $\tilde{A} \in SL_{n-1}(k[x_1,\ldots,x_m])$. By repeating this process, we get to the problem of expressing $A = \begin{pmatrix} p & q & 0 \\ r & s & 0 \\ 0 & 0 & 1 \end{pmatrix} \in SL_3(k[x_1, \ldots, x_m])$ as a product of elementary matrices, which is the subject of the next section. In this section, we will develop an algorithm for finding elementary operations that reduce a given unimodular column vector $\mathbf{v} \in (k[x_1, \ldots, x_m])^n$ to $\mathbf{e_n}$. Also, as a corollary to this Elementary Column Property, we give an algorithmic proof of the Unimodular Column Property which states that for any given unimodular column vector $\mathbf{v} \in (k[x_1, \ldots, x_m])^n$, there exists a unimodular matrix B, i.e. a matrix with constant nonzero determinant, over $k[x_1, \ldots, x_m]$ such that $B\mathbf{v} = \mathbf{e_n}$. Recently, *A. Logar, B. Sturmfels* in [LS92] and *N. Fitchas, A. Galligo* in [FG90], [Fit93] have given different algorithmic proofs of this Unimodular Column Property, thereby giving algorithmic proofs of the Quillen-Suslin theorem. Therefore, our algorithm gives another constructive proof of the Quillen-Suslin theorem. The second author has given a different algorithmic proof of the Elementary Column Property based on a localization and patching process in [Woo94].

Definition 4.1 *For a ring R, $\mathrm{Um}_n(R) = \{$n-dimensional unimodular column vectors over $R\}$.*

As in Section 3, let $R = k[x_1, \ldots, x_{m-1}]$ and $X = x_m$. Then $k[x_1, \ldots, x_m] = R[X]$. By identifying $A \in SL_2(R[X])$ with $\begin{pmatrix} A & 0 \\ 0 & I_{n-2} \end{pmatrix} \in SL_n(R[X])$, we can regard $SL_2(R[X])$ as a subgroup of $SL_n(R[X])$. As before, we use the notation $A = A(X)$ and $\mathbf{v} = \mathbf{v}(X)$ to emphasize that we are viewing the entries of a matrix A or a vector $\mathbf{v}$ as polynomials in one variable. Now consider the following lemma and theorem, which will be used to prove the Elementary Column Property.

Lemma 4.2 *Let $f_1, f_2, b, d \in R[X]$ and let r be the resultant of f_1 and f_2. Then there exists $B \in SL_2(R[X])$ 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: By a property of the resultant of two polynomials, we can find $g_1, g_2 \in R[X]$ such that $f_1 g_1 + f_2 g_2 = r$. (See [CLO92] or [GM80] for details.) Let

$s_1, s_2, t_1, t_2 \in R[X, Y, Z]$ be the polynomials defined by

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

Now, define

$$\begin{aligned} B_{11} &= 1 + s_1(b,r,d)\cdot g_1(b) + t_2(b,r,d)\cdot f_2(b), \\ B_{12} &= s_1(b,r,d)\cdot g_2(b) - t_2(b,r,d)\cdot f_1(b), \\ B_{21} &= s_2(b,r,d)\cdot g_1(b) - t_1(b,r,d)\cdot f_2(b), \\ B_{22} &= 1 + s_2(b,r,d)\cdot g_2(b) + t_1(b,r,d)\cdot f_1(b). \end{aligned}$$

Then one checks easily that $B = \begin{pmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{pmatrix}$ satisfies the desired property and that $B \in SL_2(R[X])$. $\square$

Theorem 4.3 *Suppose* $\mathbf{v}(X) = \begin{pmatrix} v_1(X) \\ \vdots \\ v_n(X) \end{pmatrix} \in \mathrm{Um}_n(R[X])$, *and* $v_1(X)$ *is monic in* X. *Then there exists* $B_1 \in SL_2(R[X])$ *and* $B_2 \in E_n(R[X])$ *such that* $B_1 B_2 \cdot \mathbf{v}(X) = \mathbf{v}(0)$.

Proof: Let $\mathbf{a_1} = (0, \ldots, 0) \in k^{m-1}$. Define $\mathcal{M}_1 = \{g \in k[x_1, \ldots, x_{m-1}] \mid g(\mathbf{a_1}) = 0\}$ and $k_1 = R/\mathcal{M}_1$ as the corresponding maximal ideal and residue field, respectively. By hypothesis $\mathbf{v} \in (R[X])^n$ is a unimodular column vector, so its image $\bar{\mathbf{v}}$ in $(k_1[X])^n = ((R/\mathcal{M}_1)[X])^n$ is also unimodular. Since $k_1[X]$ is a principal ideal ring, the ideal $< \bar{v}_2, \ldots, \bar{v}_n >$ is generated by a single element, $G_1 = \gcd(\bar{v}_2, \ldots, \bar{v}_n)$. Then $\bar{v}_1$ and G_1 generate the unit ideal in $k_1[X]$ since $\bar{v}_1, \bar{v}_2, \ldots, \bar{v}_n$ generate the unit ideal. Using the Euclidean division algorithm for $k_1[X]$, we can find $E_1 \in E_{n-1}(k_1[X])$ such that

$$E_1 \begin{pmatrix} \bar{v}_2 \\ \vdots \\ \bar{v}_n \end{pmatrix} = \begin{pmatrix} G_1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

By identifying k_1 with a subring of R, we may regard E_1 as an element of $E_n(R[X])$ and G_1 as an element of $R[X]$. Then,

$$\begin{pmatrix} 1 & 0 \\ 0 & E_1 \end{pmatrix} \mathbf{v} = \begin{pmatrix} v_1 \\ G_1 + q_{12} \\ q_{13} \\ \vdots \\ q_{1n} \end{pmatrix}$$

for some $q_{12}, \ldots, q_{1n} \in \mathcal{M}_1[X]$. Now, define $r_1 \in R$ by $r_1 = \mathrm{Res}(v_1, G_1 + q_{12})$, the resultant of v_1 and $G_1 + q_{12}$, and find $f_1, h_1 \in R[X]$ such that

$$f_1 \cdot v_1 + h_1 \cdot (G_1 + q_{12}) = r_1.$$

Since v_1 is monic, and $\bar{v}_1$ and $G_1 \in k_1[X]$ generate the unit ideal, we have

$$\begin{aligned} \bar{r}_1 &= \overline{\mathrm{Res}(v_1, G_1 + q_{12})} \\ &= \mathrm{Res}(\bar{v}_1, G_1) \\ &\neq 0. \end{aligned}$$

Therefore, $r_1 \notin \mathcal{M}_1$. Denote an algebraic closure of k by $\bar{k}$. Inductively, let $\mathbf{a_j} \in \bar{k}^{m-1}$ be a common zero of $r_1, \ldots, r_{j-1}$ and $\mathcal{M}_j$ be the corresponding maximal ideal of R for each $j \geq 2$. Define $r_j \notin \mathcal{M}_j$ in the same way as above. Define also, $E_j \in E_{n-1}(k_j[X]), G_j \in k_j[X], f_j, h_j \in R[X]$, and $q_{j2}, \ldots, q_{jn} \in \mathcal{M}_j[X]$ in an analogous way. As we saw in the proof of Theorem 3.1, there is a finite l such that $r_1R + \cdots + r_lR = R$. Find g_i's in R such that $r_1g_1 + \cdots + r_lg_l = 1$. Now, define $b_0, b_1, \ldots, b_l \in R[X]$ as

$$\begin{aligned} b_0 &= 0 \\ b_1 &= r_1g_1X \\ b_2 &= r_1g_1X + r_2g_2X \\ &\vdots \\ b_l &= r_1g_1X + r_2g_2X + \cdots + r_lg_lX = X. \end{aligned}$$

Then these b_i's satisfy the recursive relations:

$$\begin{aligned} b_0 &= 0 \\ b_i &= b_{i-1} + r_ig_iX \quad \text{for } i = 1, \ldots, l. \end{aligned}$$

Claim: For each $i \in \{1, \ldots, l\}$, there exists $B_i \in SL_2(R[X])$ and $B_i' \in E_n(R[X])$ such that $\mathbf{v}(b_i) = B_i B_i' \mathbf{v}(b_{i-1})$.

Using this and the fact that $E_n(R[X]) \cdot SL_2(R[X]) \subseteq SL_2(R[X]) \cdot E_n(R[X])$ (Corollary 2.7), we inductively get

$$\begin{aligned} \mathbf{v}(X) &= \mathbf{v}(b_l) \\ &= B_l B_l' \mathbf{v}(b_{l-1}) \\ &\vdots \\ &= BB'\mathbf{v}(b_0) \\ &= BB'\mathbf{v}(0) \end{aligned}$$

for some $B \in SL_2(R[X])$ and $B' \in E_n(R[X])$. Therefore, it is enough to prove the above claim.

Proof of claim: Let $\tilde{G}_i = G_i + q_{i2}$. Then

$$\begin{pmatrix} 1 & 0 \\ 0 & E(X) \end{pmatrix} \mathbf{v}(X) = \begin{pmatrix} v_1(X) \\ \tilde{G}_i(X) \\ q_{i3}(X) \\ \vdots \\ q_{in}(X) \end{pmatrix}.$$

For $3 \leq j \leq n$, we have

$$q_{ij}(b_i) - q_{ij}(b_{i-1}) \in (b_i - b_{i-1}) \cdot R[X] = r_i g_i X \cdot R[X].$$

Since $r_i \in R$ doesn't depend on X, we have

$$\begin{aligned} r_i &= f_i(X)v_1(X) + h_i(X)\tilde{G}_i(X) \\ &= f_i(b_{i-1})v_1(b_{i-1}) + h_i(b_{i-1})\tilde{G}_i(b_{i-1}) \\ &= \text{a linear combination of } v_1(b_{i-1}) \text{ and } \tilde{G}_i(b_{i-1}) \text{ over } R[X]. \end{aligned}$$

Therefore, we see that for $3 \leq j \leq n$,

$$q_{ij}(b_i) = q_{ij}(b_{i-1}) + \text{a linear combination of } v_1(b_{i-1}) \text{ and } \tilde{G}_i(b_{i-1}) \text{ over} R[X].$$

Hence we can find $C \in E_n(R[X])$ such that

$$C \begin{pmatrix} 1 & 0 \\ 0 & E(b_{i-1}) \end{pmatrix} \mathbf{v}(b_{i-1}) = C \begin{pmatrix} v_1(b_{i-1}) \\ \tilde{G}_i(b_{i-1}) \\ q_{i3}(b_{i-1}) \\ \vdots \\ q_{in}(b_{i-1}) \end{pmatrix} = \begin{pmatrix} v_1(b_{i-1}) \\ \tilde{G}_i(b_{i-1}) \\ q_{i3}(b_i) \\ \vdots \\ q_{in}(b_i) \end{pmatrix}.$$

Now, by Lemma 4.2, we can find $\tilde{B} \in SL_2(R[X])$ such that

$$\tilde{B} \begin{pmatrix} v_1(b_{i-1}) \\ \tilde{G}_i(b_{i-1}) \end{pmatrix} = \begin{pmatrix} v_1(b_i) \\ \tilde{G}_i(b_i) \end{pmatrix}.$$

Finally, define $B \in SL_n(R[X])$ as follows:

$$B = \begin{pmatrix} 1 & 0 \\ 0 & E(b_i)^{-1} \end{pmatrix} \begin{pmatrix} \tilde{B} & 0 \\ 0 & I_{n-2} \end{pmatrix} \cdot C \cdot \begin{pmatrix} 1 & 0 \\ 0 & E(b_i) \end{pmatrix}.$$

Then this B satisfies

$$B\mathbf{v}(b_{i-1}) = \mathbf{v}(b_i),$$

and, by using the normality of $E_n(R[X])$ again, we see that

$$B \in SL_2(R[X])E_n(R[X]),$$

which proves the claim and completes the proof of the theorem. □

Remark 4.4 Note that the groups $GL_n(k[x_1, \ldots, x_m])$ and $E_n(k[x_1, \ldots, x_m])$ act on the set $\mathrm{Um}_n(k[x_1, \ldots, x_m])$ by matrix multiplication. If the group action of $E_n(k[x_1, \ldots, x_m])$ on $\mathrm{Um}_n(k[x_1, \ldots, x_m])$ is transitive, then we get a desired algorithm in the following way: For any n-dimensional unimodular column vectors $\mathbf{v}, \mathbf{v}'$ over $k[x_1, \ldots, x_m]$, we can find $B \in E_n(k[x_1, \ldots, x_m])$ such that $B\mathbf{v} = \mathbf{v}'$. Now, let $\mathbf{v}' = \mathbf{e_n}$.

Theorem 4.5 *(Elementary Column Property) For $n \geq 3$, the group $E_n(k[x_1, \ldots, x_m])$ acts transitively on the set $Um_n(k[x_1, \ldots, x_m])$.*

Corollary 4.6 *(Unimodular Column Property)* *For $n \geq 2$, the group $GL_n(k[x_1, \dots, x_m])$ acts transitively on the set $Um_n(k[x_1, \dots, x_m])$.*

Proof: For $n \geq 3$, the Elementary Column Property clearly implies the Unimodular Column Property since a product of elementary matrices is always unimodular, i.e. has a constant nonzero determinant.

If $n = 2$, for any $\mathbf{v} = (v_1, v_2)^t \in \mathrm{Um}_2(k[x_1, \dots, x_m])$, by using Buchberger's algorithm for computing a Gröbner basis, we can find $g_1, g_2 \in k[x_1, \dots, x_m]$ such that $v_1 g_1 + v_2 g_2 = 1$. Then the unimodular matrix $U_{\mathbf{v}} = \begin{pmatrix} v_2 & -v_1 \\ g_1 & g_2 \end{pmatrix}$ satisfies $U_{\mathbf{v}} \cdot \mathbf{v} = \mathbf{e_2}$. Therefore we see that, for any $\mathbf{v}, \mathbf{w} \in \mathrm{Um}_2(k[x_1, \dots, x_m])$, $U_{\mathbf{w}}^{-1} U_{\mathbf{v}} \cdot \mathbf{v} = \mathbf{w}$ where $U_{\mathbf{w}}^{-1} U_{\mathbf{v}} \in GL_2(k[x_1, \dots, x_m])$. □

Proof of Theorem 4.5: Since the Euclidean division algorithm for $k[x_1]$ proves the theorem for $m = 1$, we may assume by induction the statement of the theorem for $R = k[x_1, \dots, x_{m-1}]$. Let $X = x_m$ and $\mathbf{v} = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \in \mathrm{Um}_n(R[X])$. We may also assume that v_1 is monic by applying a change of variables (as in the proof of the Noether Normalization Lemma). Now by Theorem 4.3, we can find $B_1 \in SL_2(R[X])$ and $B_2 \in E_n(R[X])$ such that

$$B_1 B_2 \cdot \mathbf{v}(X) \quad = \quad \mathbf{v}(0) \in R.$$

Then by the inductive hypothesis, we can find $B' \in E_n(R)$ such that

$$B' \cdot \mathbf{v}(0) \quad = \quad \mathbf{e_n}.$$

Therefore, we get

$$\mathbf{v} \quad = \quad B_2^{-1} B_1^{-1} B'^{-1} \mathbf{e_n}.$$

By the normality of $E_n(R[X])$ in $SL_n(R[X])$ (Corollary 2.7), we can write $B_1^{-1} B'^{-1} = B'' B_1^{-1}$ for some $B'' \in E_n(R[X])$. Since

$$B_1^{-1} = \begin{pmatrix} p & q & 0 & \dots & 0 \\ r & s & 0 & \dots & 0 \\ 0 & 0 & & & \\ \vdots & \vdots & & I_{n-2} & \\ 0 & 0 & & & \end{pmatrix}$$

for some $p, q, r, s \in R[X]$, we have

$$\begin{aligned}
\mathbf{v} &= B_2^{-1}B_1^{-1}B'^{-1}\mathbf{e_n} \\
&= (B_2^{-1}B'')B_1^{-1}\mathbf{e_n} \\
&= (B_2^{-1}B'')\begin{pmatrix} p & q & 0 & \dots & 0 \\ r & s & 0 & \dots & 0 \\ 0 & 0 & & & \\ \vdots & \vdots & & I_{n-2} & \\ 0 & 0 & & & \end{pmatrix}\begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix} \\
&= (B_2^{-1}B'')\mathbf{e_n}
\end{aligned}$$

where $B_2^{-1}B'' \in E_n(R[X])$. Since we have this relationship for any $\mathbf{v} \in \mathrm{Um}_n(R[X])$, we get the desired transitivity. $\square$

5 Realization Algorithm for $SL_3(R[X])$

Now, we give a realization algorithm for matrices of the form $\begin{pmatrix} p & q & 0 \\ r & s & 0 \\ 0 & 0 & 1 \end{pmatrix}$ $\in SL_3(k[x_1, \dots, x_m])$. Again, by applying a change of variables, we may assume that $p \in k[x_1, \dots, x_m]$ is a monic polynomial in the last variable x_m. In view of the Quillen Induction Algorithm developed in Section 3, we see that it is enough to develop a realization algorithm for matrices of the form $\begin{pmatrix} p & q & 0 \\ r & s & 0 \\ 0 & 0 & 1 \end{pmatrix} \in SL_3(R[X])$, in the case where R is a commutative local ring and $p \in R[X]$ is a monic polynomial. A realization algorithm for this case was obtained by M.P. Murthy [GM80]. We present below a slightly modified version.

Lemma 5.1 *Let L be a commutative ring, and $a, a', b \in L$. Then, the following are true.*

1. *(a, b) and (a', b) are unimodular over L if and only if (aa', b) is unimodular over L.*

2. *For any $c, d \in L$ such that $aa'd - bc = 1$, there exist $c_1, c_2, d_1, d_2 \in L$ such that $ad_1 - bc_1 = 1$, $a'd_2 - bc_2 = 1$, and*

$$\begin{pmatrix} aa' & b & 0 \\ c & d & 0 \\ 0 & 0 & 1 \end{pmatrix} \equiv \begin{pmatrix} a & b & 0 \\ c_1 & d_1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} a' & b & 0 \\ c_2 & d_2 & 0 \\ 0 & 0 & 1 \end{pmatrix} \pmod{E_3(L)}.$$

Proof: (1) If (aa', b) is unimodular over L, there exist $h_1, h_2 \in L$ such that $h_1 \cdot (aa') + h_2 \cdot b = 1$. Now $(h_1 a') \cdot a + h_2 \cdot b = 1$ implies (a, b) is unimodular, and $(h_1 a) \cdot a' + h_2 \cdot b = 1$ implies (a', b) is unimodular.

Suppose, now, that (a, b) and (a', b) are unimodular over L. Then, we can find $h_1, h_2, h_1', h_2' \in L$ such that $h_1 a + h_2 b = 1$, $h_1' a' + h_2' b = 1$. Now, let $g_1 = h_1 h_1'$, $g_2 = h_2' + a' h_2 h_1'$, and consider

$$\begin{aligned} g_1 aa' + g_2 b &= h_1 h_1' aa' + (h_2' + a' h_2 h_1') b \\ &= h_1' a' (h_1 a + h_2 b) + h_2' b \\ &= h_1' a' + h_2' b \\ &= 1. \end{aligned}$$

So we have a desired unimodular relation.

(2) If $c, d \in L$ satisfy $aa'd - bc = 1$, then (aa', b) is unimodular, which in turn implies that (a, b) and (a', b) are unimodular. Therefore, we can find $c_1, d_1, d_1, d_2 \in L$ such that $ad_1 - bc_1 = 1$ and $a'd_2 - bc_2 = 1$. For example, we can let

$$c_1 = c_2 = c, \quad d_1 = a'd, \quad d_2 = ad.$$

Now, consider

$$\begin{aligned} \begin{pmatrix} aa' & b & 0 \\ c & d & 0 \\ 0 & 0 & 1 \end{pmatrix} &= E_{21}(cd_1d_2 - d(c_2 + a'c_1d_2)) \begin{pmatrix} aa' & b & 0 \\ c_2 + a'c_1d_2 & d_1d_2 & 0 \\ 0 & 0 & 1 \end{pmatrix} \\ &= E_{21}(cd_1d_2 - d(c_2 + a'c_1d_2)) E_{23}(d_2 - 1) E_{32}(1) E_{23}(-1) \\ &\quad \cdot \begin{pmatrix} a & b & 0 \\ c_1 & d_1 & 0 \\ 0 & 0 & 1 \end{pmatrix} E_{23}(1) E_{32}(-1) E_{23}(1) \begin{pmatrix} a' & b & 0 \\ c_2 & d_2 & 0 \\ 0 & 0 & 1 \end{pmatrix} \\ &\quad \cdot E_{23}(-1) E_{32}(1) E_{23}(a - 1) E_{31}(-a'c_1) E_{32}(-d_1). \end{aligned}$$

This explicit expression shows that

$$\begin{pmatrix} aa' & b & 0 \\ c & d & 0 \\ 0 & 0 & 1 \end{pmatrix} \equiv \begin{pmatrix} a & b & 0 \\ c_1 & d_1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} a' & b & 0 \\ c_2 & d_2 & 0 \\ 0 & 0 & 1 \end{pmatrix} \pmod{E_3(L)}.$$

$\square$

Theorem 5.2 *Suppose* $(R, \mathcal{M})$ *is a commutative local ring, and* $A = \begin{pmatrix} p & q & 0 \\ r & s & 0 \\ 0 & 0 & 1 \end{pmatrix}$ $\in SL_3(R[X])$ *where* p *is monic. Then* A *is realizable over* $R[X]$.

Proof: We induct on $\deg(p)$. If $\deg(p) = 0$, then $p = 1$, and A is clearly realizable. Now, suppose $\deg(p) = d > 0$ and $\deg(q) = l$. Since $p \in R[X]$ is monic, we can find $f, g \in R[X]$ such that

$$q = fp + g, \quad \deg(g) < d.$$

Then,

$$AE_{12}(-f) = \begin{pmatrix} p & q - fp & 0 \\ r & s - fr & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} p & g & 0 \\ r & s - fr & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Hence we may assume $\deg(q) < d$. Now, we note that either $p(0)$ or $q(0)$ is a unit in R, otherwise, we would have $p(0)s(0) - q(0)r(0) \in \mathcal{M}$, which contradicts the fact that $ps - qr = p(0)s(0) - q(0)r(0) = 1$. Consider these two cases separately.

Case 1: Suppose that $q(0)$ is a unit.
We have

$$AE_{21}(-q(0)^{-1}p(0)) = \begin{pmatrix} p - q(0)^{-1}p(0)q & q & 0 \\ r - q(0)^{-1}p(0)s & s & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

So, we may assume $p(0) = 0$. Now, write $p = Xp'$. Then, by Lemma 5.1, we can find $c_1, d_1, c_2, d_2 \in R[X]$ such that $Xd_1 - qc_1 = 1$, $p'd_2 - qc_2 = 1$ and

$$\begin{pmatrix} p & q & 0 \\ r & s & 0 \\ 0 & 0 & 1 \end{pmatrix} \equiv \begin{pmatrix} X & q & 0 \\ c_1 & d_1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} p' & q & 0 \\ c_2 & d_2 & 0 \\ 0 & 0 & 1 \end{pmatrix} \pmod{E_3(R[X])}$$

Since p' is monic and $\deg(p') < d$, the second matrix on the right hand side is realizable by the induction hypothesis. As for the first matrix, we may assume that q is a unit of R since we can assume $\deg(q) < \deg(X) = 1$ and $q(0)$ is a unit. Then invertibility of q leads easily to an explicit factorization of $\begin{pmatrix} X & q & 0 \\ c_1 & d_1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ into elementary matrices.

Case 2: Suppose that $q(0)$ is not a unit.
First we claim that there exist $p', q' \in R[X]$ such that $\deg(p') < l, \deg(q') < d$ and $p'p - q'q = 1$. To prove this claim, we let $r \in R$ be the resultant of p and q. Then there exist $f, g \in R[X]$ with $\deg(f) < l, \deg(g) < d$ such that $fp + gq = r$. Since p is monic and $p, q \in R[X]$ generate the unit ideal, we see that $r \notin \mathcal{M}$, hence r is a unit or R. Now, setting $p' = f/r$, $q' = -g/r$ proves the claim. Also note that since $p'(0)p(0) - q'(0)q(0) = 1$ and $q(0) \in \mathcal{M}$, then $p'(0) \notin \mathcal{M}$. This means that $q(0) + p'(0)$ is a unit. Now, we have that

$$\begin{aligned} \begin{pmatrix} p & q & 0 \\ r & s & 0 \\ 0 & 0 & 1 \end{pmatrix} &= E_{21}(rp' - sq') \begin{pmatrix} p & q & 0 \\ q' & p' & 0 \\ 0 & 0 & 1 \end{pmatrix} \\ &= E_{21}(rp' - sq')E_{12}(-1) \begin{pmatrix} p + q' & q + p' & 0 \\ q' & p' & 0 \\ 0 & 0 & 1 \end{pmatrix}. \end{aligned}$$

Noting that the last matrix on the right hand side is realizable by Case 1, since $q(0) + p'(0)$ is a unit and $\deg(p + q') = d$, we see that $\begin{pmatrix} p & q & 0 \\ r & s & 0 \\ 0 & 0 & 1 \end{pmatrix}$ is also realizable. $\square$

6 Eliminating Redundancies

When applied to a specific matrix, the algorithm presented in this paper will produce a factorization into elementary matrices, but this factorization may not have minimal length. The Steinberg relations [Mil71] from algebraic K–theory provide a method for improving a given factorization by eliminating some of the unnecessary factors. The Steinberg relations which elementary matrices satisfy are

1. $E_{ij}(0) = I$;
2. $E_{ij}(a)E_{ij}(b) = E_{ij}(a+b)$;
3. For $i \neq l$, $[E_{ij}(a), E_{jl}(b)] = E_{ij}(a)E_{jl}(b)E_{ij}(-a)E_{jl}(-b) = E_{il}(ab)$;
4. For $j \neq l$, $[E_{ij}(a), E_{li}(b)] = E_{ij}(a)E_{li}(b)E_{ij}(-a)E_{li}(-b) = E_{lj}(-ab)$;
5. For $i \neq p$, $j \neq l$, $[E_{ij}(a), E_{lp}(b)] = E_{ij}(a)E_{lp}(b)E_{ij}(-a)E_{lp}(-b) = I$.

The realization algorithm of this paper can be implemented together with a Redundancy Elimination Algorithm based on the above set of relations, using existing computer algebra systems. As suggested in [THK94], an algorithm of this kind has application in Signal Processing since it gives a way of expressing a given multidimensional filter bank as a cascade of simpler filter banks called elementary ladder steps.

Acknowledgements

The authors wish to thank A. Kalker, T.Y. Lam, R. Laubenbacher, B. Sturmfels and M. Vetterli for all the valuable support, insightful discussions and encouragement.

References

[Coh66] P.M. Cohn. On the structure of the GL_2 of a ring. *Inst. Hautes Études Sci. Publ. Math. No. 30*, 365–413, 1966.

[CLO92] D. Cox, J. Little and D. O'Shea. Ideals, Varieties and Algorithms Springer, 1992.

[FG90] N. Fitchas and A. Galligo. Nullstellensatz effectif et conjecture de Serre (théorème de Quillen-Suslin) pour le calcule formel. *Math. Nachr 149*, 232–253, 1990.

[Fit93] N. Fitchas. Algorithmic aspects of Suslin's proof of Serre's conjecture. *Comput. Complexity 3*, 31–55, 1993.

[GM80] S.K. Gupta and M.P. Murthy. Suslin's work on linear groups over polynomial rings and Serre problem, *Indian Statistical Institute Lecture Notes Series* 8. MacMillan, New Delhi, 1980.

[HO89] A. Hahn and O.T. O'Meara. The classical groups and K-theory. Springer, 1989.

[Knu91] M.A. Knus. Quadratic and Hermitian Forms over Rings. Springer, 1991.

[Lam78] T.Y. Lam. Serre's conjecture, *Lecture Notes in Mathematics* 635. Springer, 1978.

[LS92] A. Logar and B. Sturmfels. Algorithms for the Quillen-Suslin theorem. *J. Algebra* 145, 231–239, 1992.

[Mil71] J. Milnor. Introduction to Algebraic K-Theory, *Annals of Mathematics Studies* 72. Princeton University Press, 1971.

[Mis93] B. Mishra. Algorithmic Algebra. Springer, 1993.

[Sus76] A.A. Suslin. Projective modules over a polynomial ring are free. *Soviet Math. Dokl.* 17, 1160–1164, 1976.

[Sus77] A.A. Suslin. On the structure of the special linear group over polynomial rings. *Math. USSR Izv.* 11, 221–238, 1977.

[THK94] L. Tolhuizen, H. Holmann, and A. Kalker. A design method for bi-orthogonal, m-dimensional 2-band filter banks. to appear in IEEE Transactions on Signal Processing, 1994.

[Woo94] C. Woodburn. An Algorithm for Suslin's Stability Theorem. Ph.D Dissertation, New Mexico State University, 1994.