An Algorithmic Proof of Suslin’s Stability Theorem over 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 the multivariate polynomial ring $SL_n(k[x_1, \ldots, x_m])$ with $n \geq 3$. As Gaussian elimination gives us an algorithmic way of finding an explicit factorization of the given matrix into elementary matrices over a field, we develop a similar algorithm over polynomial rings.

1 Introduction

Immediately after proving the famous Serre’s Conjecture (the Quillen-Suslin theorem, nowadays) in 1976 [11], A. Suslin went on [12] to prove the following $K_1$-analogue of Serre’s Conjecture which is now known as 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 $f_{ij}$ being 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; park@math.berkeley.edu
†Dept. of Mathematics, Pittsburg State University; cwoodburn@mail.pittstate.edu
**Definition 1** 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 $(i, j)$ component is 1 and all other components are zero.

For a ring $R$, 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

$$SL_n(R[x_1, \ldots, x_m]) = E_n(R[x_1, \ldots, x_m]) \quad \text{for all } n \geq \max(3, \dim(R) + 2).$$  \hspace{1cm} (1)

In this paper, we develop an algorithmic proof of the above assertion over a field $k$. By implementing this algorithm, for a given $A \in SL_n(k[x_1, \ldots, x_m])$ with $n \geq 3$, we are able to find those elementary matrices $E_1, \ldots, E_t \in E_n(k[x_1, \ldots, x_m])$ such that $A = E_1 \cdots E_t$.

**Remark 1** If a matrix $A$ can be written as a product of elementary matrices, we will say $A$ is realizable.

- 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, which will be used in the rest of paper.

- In section 3, we develop 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 $R[X]$ to one over $R_M[X]$’s, where $R = k[x_1, \ldots, x_{m-1}]$ and $M$ is a maximal ideal 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 the matrices of the following 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 [4]. 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 Normality of \(E_n(k[x_1, \ldots, x_m])\) in \(SL_n(k[x_1, \ldots, x_m])\)

Lemma 1 The Cohn matrix \(A = \begin{pmatrix} 1 + xy & x^2 \\ -y^2 & 1 - xy \end{pmatrix}\) is not realizable, but \( \begin{pmatrix} A & 0 \\ 0 & 1 \end{pmatrix} \) is.

Proof: The nonrealizability of \(A\) is proved in [1], and a complete algorithmic criterion for the realizability of matrices in \(SL_2(k[x_1, \ldots, x_m])\) is developed in [13]. 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 the following Lemma 3. □

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

\[
I + a v \cdot (v_i e_j - v_j e_i)
\]

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

**Lemma 2** Any Cohn-type matrix for \( n \geq 3 \) is realizable.

**Proof:** First, let's consider the case \( i = 1, j = 2 \). In this case,

\[
B = I + a \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \cdot (v_2, -v_1, 0, \ldots, 0)
\]

\[
= \begin{pmatrix}
1 + av_1 v_2 & -av_1^2 & 0 & \cdots & 0 \\
av_1^2 & 1 - av_1 v_2 & 0 & \cdots & 0 \\
& av_3 v_2 & -av_3 v_1 & I_{n-2} \\
& \vdots & \vdots & \vdots & \vdots \\
& av_n v_2 & -av_n v_1 & \\
1 + av_1 v_2 & -av_1^2 & 0 & \cdots & 0 \\
av_1^2 & 1 - av_1 v_2 & 0 & \cdots & 0 \\
0 & 0 & \vdots & \vdots & \vdots \\
& \vdots & \vdots & \vdots & \vdots \\
0 & 0 & 0 & \cdots & 1
\end{pmatrix}
\]

\[
= \prod_{l=3}^n E_{l1}(av_1 v_2) E_{l2}(-av_1 v_1), (3)
\]

So, it's enough to show that

\[
A = \begin{pmatrix}
1 + av_1 v_2 & -av_1^2 & 0 \\
av_1^2 & 1 - av_1 v_2 & 0 \\
0 & 0 & 1
\end{pmatrix}
\]

4
is realizable for any $a, v_1, v_2 \in k[x_1, \ldots, x_m]$. Let "→" indicate that we are applying elementary operations, and consider the following:

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

(5)

Keeping track of all the elementary operations involved, we get

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

(6)

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

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

(Here, $v_j$ occurs at the $i$-th position and $-v_i$ occurs at the $j$-th position.)

\[
\begin{pmatrix}
1 & \cdots & av_1 v_j & \cdots & -av_1 v_i & \cdots & 0 \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & 0 \\
1 + av_i v_j & -av_i^2 \\
\vdots & \vdots & \vdots \\
av_j^2 & 1 - av_i v_j \\
\vdots & \vdots & \vdots \\
v_n v_j & -v_n v_i & 1
\end{pmatrix}
\]
In the above, $t \in \{1, \ldots, n\}$ can be chosen to be any number other than $i$ and $j$. \hfill \Box

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 3** Let $R$ be a ring and $v = (v_1, \ldots, v_n)^t \in R^n$ for some $n \in \mathbb{N}$. Then $v$ 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 $v_1g_1 + \cdots + v_ng_n = 1$.

**Corollary 1** Suppose that $A \in SL_n(k[x_1, \ldots, x_m])$ with $n \geq 3$ can be written in the form $A = I + v \cdot w$ for a unimodular column vector $v$ and a row vector $w$ over $k[x_1, \ldots, x_m]$ such that $w \cdot v = 0$. Then $A$ is realizable.

**Proof:** Since $v = (v_1, \ldots, v_n)^t$ is unimodular, we can find $g_1, \ldots, g_n \in k[x_1, \ldots, x_m]$ such that $v_1g_1 + \cdots + v_ng_n = 1$. We can use the effective Nullstellensatz to explicitly find these $g_i$’s (See \[3\]). This combined with $w \cdot v = w_1v_1 + \cdots + w_nv_n = 0$ yields a new expression for $w$:

$$ w = \sum_{i<j} a_{ij}(v_j e_i - v_i e_j) \quad \text{(8)} $$
where \( a_{ij} = w_i g_j - w_j g_i \). Now,
\[
A = \prod_{i<j} (I + v \cdot a_{ij} (v_j e_i - v_i e_j)).
\] (9)

Each component on the right hand side of this equation is a Cohn-type matrix and thus realizable, so \( A \) is also realizable.

**Corollary 2** \( BE_{ij}(a)B^{-1} \) 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 \( v \) be the \( i\text{-th column vector of } B \) and \( w \) be \( a \) times the \( j\text{-th row vector of } B^{-1} \). Then \((i\text{-th row vector of } B^{-1}) \cdot v = 1\) implies \( v \) is unimodular, and \( w \cdot v \) is clearly zero since \( i \neq j \). Therefore, \( BE_{ij}(a)B^{-1} = I + v \cdot w \) satisfies the condition of the above corollary, and is thus realizable.

**Remark 2** One important consequence of this corollary is that for \( n \geq 3 \), \( E_n(k[x_1, \ldots, x_m]) \) is a normal subgroup of \( SL_n(k[x_1, \ldots, x_m]) \), i.e. if \( A \in SL_n(k[x_1, \ldots, x_m]) \) 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 Glueing of Local Realizability

Let \( R = k[x_1, \ldots, x_{m-1}] \), \( X = x_m \) and \( M \in \text{Max}(R) = \{ \text{maximal ideals of } R \} \). For \( A \in SL_n(R[X]) \), we let \( A_M \in SL_n(R_M[X]) \) be its image under the canonical mapping \( SL_n(R[X]) \rightarrow SL_n(R_M[X]) \). Also, by induction, we may assume \( SL_n(R) = E_n(R) \) for \( n \geq 3 \). Now consider the following analogue of Quillen’s 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 \( A_M \in SL_n(R_M[X]) \) is realizable over \( R_M[X] \) for every \( M \in \text{Max}(R) \).
While a non-constructive proof of this assertion is given in [12] and a more general functorial treatment of this Quillen Induction Process can be found in [6], we will attempt to give a constructive proof for it here. Since the necessity of the condition is clear, we have to prove the following:

**Theorem 1** (Quillen Induction Algorithm) For any given $A \in SL_n(R[X])$, if $A_M \in E_n(R_M[X])$ for every $M \in \text{Max}(R)$, then $A \in E_n(R[X])$.

**Remark 3** In view of this theorem, for any given $A \in SL_n(R[X])$, now it’s enough to have a realization algorithm for each $A_M$ over $R_M[X]$.

**Proof:** Let $a_1 = (0, \ldots, 0) \in k^{m-1}$, and $M_1 = \{g \in k[x_1, \ldots, x_{m-1}] \mid g(a_1) = 0\}$ be the corresponding maximal ideal. Then by the condition of the theorem, $A_{M_1}$ is realizable over $R_{M_1}[X]$. Hence, we can write

$$A_{M_1} = \prod_j E_{s_j t_j} \left(\frac{c_j}{d_j}\right)$$

(10)

where $c_j, d_j \in R, d_j \notin M_1$. Letting $r_1 = \prod_j d_j \notin M_1$, we can rewrite this as

$$A_{M_1} = \prod_j E_{s_j t_j} \left(\frac{c_j \prod_{k \neq j} d_k}{r_1}\right) \in E_n(R_{r_1}) \subset E_n(R_{M_1}).$$

(11)

Denote an algebraic closure of $k$ by $\bar{k}$. Inductively, let $a_j \in \bar{k}^{m-1}$ be a common zero of $r_1, \ldots, r_{j-1}$ and $M_j = \{g \in k[x_1, \ldots, x_{m-1}] \mid g(a_j) = 0\}$ be the corresponding maximal ideal of $R$ for each $j \geq 2$. Define $r_j \notin M_j$ in the same way as in the above so that

$$A_{M_j} \in E_n(R_{r_j}[X]).$$

(12)

Since $a_j$ is a common zero of $r_1, \ldots, r_{j-1}$ in this construction, we immediately see $r_1, \ldots, r_{j-1} \in M_j = \{g \in R \mid g(a_j) = 0\}$. But noting $r_j \notin M_j$, we conclude that $r_j \notin r_1 R + \cdots + r_{j-1} R$. Now, since the Noetherian condition on $R$ guarantees that 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 the usual Ideal Membership Algorithm to determine when $1_R$ is in the ideal $r_1 R + \cdots + r_L R$.

Let $l$ be a large natural number (It will soon be clear what large means). Then since $r^l_1 R + \cdots + r^l_L R = R$, we can use the effective Nullstellensatz.
to find $g_1, \ldots, g_L \in R$ such that $r_1^l g_1 + \cdots + r_L^l g_L = 1$. Now, we express $A(X) \in SL_n(R[X])$ in the following way:

$$A(X) = A(X - Xr_1^l g_1) \cdot [A^{-1}(X - Xr_1^l g_1)A(X)]$$

$$= A(X - Xr_1^l g_1 - Xr_2^l g_2) \cdot [A^{-1}(X - Xr_1^l g_1 - Xr_2^l g_2)A(X - Xr_1^l g_1)]$$

$$\cdot [A^{-1}(X - Xr_1^l g_1)A(X)]$$

$$= \cdots$$

$$= A(X - \sum_{i=1}^L Xr_i^l g_i) \cdot [A^{-1}(X - \sum_{i=1}^L Xr_i^l g_i)A(X - \sum_{i=1}^{L-1} Xr_i^l g_i)] \cdots$$

$$\cdots [A^{-1}(X - Xr_1^l g_1)A(X)].$$

(13)

Note here that the first matrix $A(X - \sum_{i=1}^L Xr_i^l g_i) = A(0)$ on the right hand side is in $SL_n(R) = E_n(R)$ by the induction hypothesis. What we will be shown now is that for a sufficiently large $l$, each expression in the brackets in the above equation for $A$ is actually in $E_n(R[X])$, so that $A$ itself is in $E_n(R[X])$. To this end, by letting $A_M = A_i$ and identifying $A \in SL_n(R[X])$ with $A_i \in SL_n(R_M[X])$, note that each expression in the brackets is in the following form:

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

(14)

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

Let

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

(15)

and write $D_i$ in the form

$$D_i = \prod_{j=1}^h E_{s_j,t_j}(b_j + Z f_j)$$

(16)

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 $E_{s_j,t_j}(a)$ will be simply denoted as $E^j(a)$ for notational convenience. Now define $C_p$ by

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

(17)
Then the $C_p$’s satisfy the following recursive relations:

\[
E^1(b_1) = C_1 \\
E^p(b_p) = C_{p-1}^{-1}C_p \quad (2 \leq p \leq h) \\
C_h = I.
\]  

(18)

Hence, using $E_{ij}(a + b) = E_{ij}(a)E_{ij}(b)$,

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

(19)

Now in the same way as in the proof of Corollary 1 and Corollary 2 of section 2, 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 $v = \left( \begin{array}{c} v_1 \\ \vdots \\ v_n \end{array} \right)$ be the $s_j$-th column vector of $C_j$. Then

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

(20)

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

\[
v_\gamma = \frac{v'_\gamma}{r'_i}, \quad a_{\gamma\delta} = \frac{a'_{\gamma\delta}}{r'_i}, \quad f_j = \frac{f'_j}{r'_i}
\]  

(21)

for some $v'_\gamma, a'_{\gamma\delta} \in R[X,Y]$, $f'_j \in R[X,Y,Z]$. Now, replacing $Z$ by $r_i\cdot g$, 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,

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

(22)
Since this is true for each \( j \), we conclude that for a sufficiently large \( l \),

\[
D_i(X, Y, r^i g) = \prod_{j=1}^{h} C_j E_j (r^i g f_j) C_j^{-1} \in E_n(R[X, Y]).
\] (23)

Now, letting \( Y = c \) proves the claim. \( \square \)

### 4 Reduction to \( SL_3(\mathbb{K}[x_1, \ldots, x_m]) \)

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

\[
BA = \begin{pmatrix}
\tilde{A} & 0 \\
\vdots & 0 \\
p_1 & \cdots & p_{n-1} & 1
\end{pmatrix}
\] (24)

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

\[
BA E_{n1}(-p_1) \cdots E_{n(n-1)}(-p_{n-1}) = \begin{pmatrix}
\tilde{A} & 0 \\
0 & 1
\end{pmatrix}.
\] (25)

Therefore our problem of expressing \( A \in SL_n(\mathbb{K}[x_1, \ldots, x_m]) \) as a product of elementary matrices is now reduced to the same problem for \( \tilde{A} \in SL_{n-1}(\mathbb{K}[x_1, \ldots, x_m]) \). By repeating this process, we get to the problem of expressing \( \tilde{A} = \begin{pmatrix}
p & q & 0 \\
r & s & 0 \\
0 & 0 & 1
\end{pmatrix} \in SL_3(\mathbb{K}[x_1, \ldots, x_m]) \) 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 \( v \in (\mathbb{K}[x_1, \ldots, x_m])^n \) to \( e_n \). 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 $v \in (k[x_1, \ldots, x_m])^n$, there exists a unimodular matrix $B$, i.e. a matrix of constant determinant, over $k[x_1, \ldots, x_m]$ such that $Bv = e_n$.

Lately, A. Logar, B. Sturmfels in [8] and N. Fitchas, A. Galligo in [3], [2] 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 [14].

**Definition 4** For a ring $R$, $\text{Um}_n(R) = \{n$-dimensional unimodular column vectors over $R\}$.

**Remark 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 $\text{Um}_n(k[x_1, \ldots, x_m])$ by matrix multiplication.

**Theorem 2** (*Elementary Column Property*) For $n \geq 3$, the group $E_n(k[x_1, \ldots, x_m])$ acts transitively on the set $\text{Um}_n(k[x_1, \ldots, x_m])$.

**Remark 5** According to this theorem, if $v, v'$ are $n$-dimensional unimodular column vectors over $k[x_1, \ldots, x_m]$, then we can find $B \in E_n(k[x_1, \ldots, x_m])$ such that $Bv = v'$. Letting $v' = e_n$ gives a desired algorithm.

**Corollary 3** (*Unimodular Column Property*) For $n \geq 2$, the group $GL_n(k[x_1, \ldots, x_m])$ acts transitively on the set $\text{Um}_n(k[x_1, \ldots, x_m])$.

**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 determinant.

If $n = 2$, for any $v = (v_1, v_2)^t \in \text{Um}_2(k[x_1, \ldots, x_m])$, find $g_1, g_2 \in k[x_1, \ldots, x_m]$ such that $v_1g_1 + v_2g_2 = 1$. Then the unimodular matrix $U_v = \begin{pmatrix} v_2 & -v_1 \\ g_1 & g_2 \end{pmatrix}$ satisfies $U_v \cdot v = e_2$. Therefore we see that, for any $v, w \in \text{Um}_2(k[x_1, \ldots, x_m]), U_w^{-1}U_v \cdot v = w$ where $U_w^{-1}U_v \in GL_2(k[x_1, \ldots, x_m])$. □
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 \( \begin{pmatrix} A & 0 \\ 0 & \text{I}_{n-2} \end{pmatrix} \) $\in SL_n(R[X])$, we can regard $SL_2(R[X])$ as a subgroup of $SL_n(R[X])$. Now consider the following theorem.

**Theorem 3** Suppose $v(X) = \begin{pmatrix} v_1(X) \\ \vdots \\ v_n(X) \end{pmatrix} \in \text{Um}_n(R[X])$, 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 $B_1B_2 \cdot v(X) = v(0)$.

**Proof:** Later \( \Box \)

We will use this theorem to prove the **Theorem 2** now.

**Proof of Theorem 2:** Since the *Euclidean division algorithm* for $k[x_1]$ proves the theorem for $m = 1$ case, by induction, we may assume the statement of the theorem for $R = k[x_1, \ldots, x_{m-1}]$. Let $X = x_m$ and $v = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \in \text{Um}_n(R[X])$. We may also assume that $v_1$ is monic by applying a change of variables (as in the well-known proof of the *Noether Normalization Lemma*). Now by the above **Theorem 3**, we can find $B_1 \in SL_2(R[X])$ and $B_2 \in E_n(R[X])$ such that

\[
B_1B_2 \cdot v(X) = v(0) \in R. \quad (26)
\]

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

\[
B' \cdot v(0) = e_n. \quad (27)
\]

Therefore, we get

\[
v = B_2^{-1}B_1^{-1}B'^{-1}e_n. \quad (28)
\]
By the normality of $E_n(R[X])$ in $SL_n(R[X])$ (Corollary 2), we can write $B_{1}^{-1}B_{1}^{'}^{-1} = B_{1}^{''}B_{1}^{-1}$ for some $B_{1}^{''} \in E_{n}(R[X])$. Since

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

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

$$v = B_{2}^{-1}B_{1}^{-1}B_{1}^{'}^{-1}e_{n}$$

$$= (B_{2}^{-1}B_{1}^{''})B_{1}^{-1}e_{n}$$

$$= (B_{2}^{-1}B_{1}^{''}) \begin{pmatrix} p & q & 0 & \ldots & 0 \\ r & s & 0 & \ldots & 0 \\ 0 & 0 \\ \vdots & \vdots & I_{n-2} \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}$$

$$= (B_{2}^{-1}B_{1}^{''})e_{n}$$  \hspace{1cm} (30)

where $B_{2}^{-1}B_{1}^{''} \in E_{n}(R[X])$. Since we have this relationship for any $v \in Um_{n}(R[X])$, we get the desired transitivity. \hspace{1cm} \blacksquare

Now, we need one lemma to construct an algorithm for the Theorem 3.

**Lemma 3** Let $f_1, f_2, b, d \in R[X]$ and $r$ be the resultant of $f_1$ and $f_2$. Then there exists $B \in SL_{2}(R[X])$ such that

$$B \begin{pmatrix} f_1(b) \\ f_2(b) \end{pmatrix} = \begin{pmatrix} f_1(b + rd) \\ f_2(b + rd) \end{pmatrix}.$$  \hspace{1cm} (31)

**Proof:** By the property of the resultant of two polynomials, we can find $g_1, g_2 \in R[X]$ such that $f_1g_1 + f_2g_2 = r$. Also let $s_1, s_2, t_1, t_2 \in R[X, Y, Z]$ be the polynomials defined by

$$f_1(X + Y Z) = f_1(X) + Y s_1(X, Y, Z)$$
$$f_2(X + Y Z) = f_2(X) + Y s_2(X, Y, Z)$$
$$g_1(X + Y Z) = g_1(X) + Y t_1(X, Y, Z)$$
$$g_2(X + Y Z) = g_2(X) + Y t_2(X, Y, Z).$$  \hspace{1cm} (32)
Now, let
\[ B_{11} = 1 + s_1(b, r, d) \cdot g_1(b) + t_2(b, r, d) \cdot f_2(b) \]
\[ B_{12} = s_1(b, r, d) \cdot g_2(b) - t_2(b, r, d) \cdot f_1(b) \]
\[ B_{21} = s_2(b, r, d) \cdot g_1(b) - t_1(b, r, d) \cdot f_2(b) \]
\[ B_{22} = 1 + s_2(b, r, d) \cdot g_2(b) + t_1(b, r, d) \cdot f_1(b). \] (33)

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

Proof of Theorem 3: Let \( a_1 = (0, \ldots, 0) \in k^{m-1}. \) Define \( M_1 = \{ g \in k[x_1, \ldots, x_{m-1}] \mid g(a_1) = 0 \} \) and \( k_1 = R/M_1 \) as the corresponding maximal ideal and residue field, respectively. Since \( v \in (R[X])^n \) is a unimodular column vector, its image \( \overline{v} \) in \( (k_1[X])^n = ((R/M_1)[X])^n \) is also unimodular. Since \( k_1[X] \) is a principal ideal ring, the minimal Gröbner basis of its ideal \( < \overline{v}_2, \ldots, \overline{v}_n > \) consists of a single element, \( G_1. \) Then \( \overline{v}_1 \) and \( G_1 \) generate the unit ideal in \( k_1[X] \) since \( \overline{v}_1, \overline{v}_2, \ldots, \overline{v}_n \) 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
\[ E_1 \begin{pmatrix} \overline{v}_2 \\ \vdots \\ \overline{v}_n \end{pmatrix} = \begin{pmatrix} G_1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}. \] (34)

By identifying \( k_1 \) with a subring of \( R, \) we may regard \( E_1 \) to be an element of \( E_n(R[X]) \) and \( G_1 \) to be an element of \( R[X]. \) Then,
\[ \begin{pmatrix} 1 & 0 \\ 0 & E_1 \end{pmatrix} v = \begin{pmatrix} v_1 \\ G_1 + q_{12} \\ q_{13} \\ \vdots \\ q_{1n} \end{pmatrix} \] (35)
for some \( q_{12}, \ldots, q_{1n} \in M_1[X]. \) Now, define \( r_1 \in R \) by
\[ r_1 = \text{Res}(v_1, G_1 + q_{12}) = \text{the resultant of } v_1 \text{ and } G_1 + q_{12} \] (36)
and find $f_1, h_1 \in R[X]$ such that

$$f_1 \cdot v_1 + h_1 \cdot (G_1 + q_{12}) = r_1.$$  \hfill (37)

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

$$\bar{r}_1 = \text{Res}(v_1, G_1 + q_{12}) = \text{Res}(\bar{v}_1, G_1) \neq 0.$$  \hfill (38)

Therefore, $r_1 \notin M_1$. Denote an algebraic closure of $k$ by $\bar{k}$. Inductively, let $a_j \in \bar{k}^{m-1}$ be a common zero of $r_1, \ldots, r_{j-1}$ and $M_j$ be the corresponding maximal ideal of $R$ for each $j \geq 2$. Define $r_j \notin M_j$ in the same way as in the 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 $q_{j2}, \ldots, q_{jn} \in M_j[X]$ in an analogous way. Since we let $a_j$ be a common zero of $r_1, \ldots, r_{j-1}$ in this construction, we see $r_1, \ldots, r_{j-1} \in M_j = \{ g \in R \mid g(a_j) = 0 \}$. But noting $r_j \notin M_j$, we conclude that $r_j \notin r_1 R + \cdots + r_{j-1} R$. Now, since $R$ is Noetherian, after a finite number of steps, we will get to some $L$ such that $r_1 R + \cdots + r_L R = R$. We can use the *effective Nullstellensatz* to explicitly find those $g_i$'s in $R$ such that $r_1 g_1 + \cdots + r_L g_L = 1$. Define, now, $b_0, b_1, \ldots, b_L \in R[X]$ in the following way:

$$b_0 = 0$$
$$b_1 = r_1 g_1 X$$
$$b_2 = r_1 g_1 X + r_2 g_2 X$$
$$\vdots$$
$$b_L = r_1 g_1 X + r_2 g_2 X + \cdots + r_L g_L X = X.$$  \hfill (39)

Then these $b_i$'s satisfy the recursive relations:

$$b_0 = 0$$
$$b_i = b_{i-1} + r_i g_i X \quad \text{for } i = 1, \ldots, L.$$  \hfill (40)

*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 $v(b_i) = B_i B_i' v(b_{i-1})$. 

16
If this claim is true, then using \( E_n(R[X]) \cdot SL_2(R[X]) \subseteq SL_2(R[X]) \cdot E_n(R[X]) \) (Normality of \( E_n(R[X]) \); **Corollary 2**), we inductively get
\[
\mathbf{v}(X) = \mathbf{v}(b_L) = B_L B'_L \mathbf{v}(b_{L-1}) = \cdots = BB' \mathbf{v}(0) \tag{41}
\]
for some \( B \in SL_2(R[X]) \) and \( B' \in E_n(R[X]) \). Therefore it’s enough to prove the above claim. For this purpose, let \( \tilde{G}_i = G_i + q_{i2} \). Then
\[
\begin{pmatrix} 1 & 0 & 0 \\ 0 & E(X) \end{pmatrix} \mathbf{v}(X) = \begin{pmatrix} v_1(X) \\ \tilde{G}_i(X) \\ q_{i3}(X) \\ \vdots \\ q_{in}(X) \end{pmatrix}. \tag{42}
\]
For \( 3 \leq l \leq n \), we have
\[
q_{il}(b_i) - q_{il}(b_{i-1}) \in (b_i - b_{i-1}) \cdot R[X] = r_i g_i X \cdot R[X]. \tag{43}
\]
Since \( r_i \in R \) doesn’t depend on \( X \), we have
\[
r_i = f_i(X)v_1(X) + h_i(X) \tilde{G}_i(X) = f_i(b_{i-1})v_1(b_{i-1}) + h_i(b_{i-1}) \tilde{G}_i(b_{i-1}) = \text{a linear combination of } v_1(b_{i-1}) \text{ and } \tilde{G}_i(b_{i-1}) \text{ over } R[X]. \tag{44}
\]
Therefore, we see that for \( 3 \leq l \leq n \),
\[
q_{il}(b_i) = q_{il}(b_{i-1}) + \text{a linear combination of } v_1(b_{i-1}) \text{ and } \tilde{G}_i(b_{i-1}) \text{ over } R[X].
\]
Hence we can find \( C \in E_n(R[X]) \) such that
\[
C \begin{pmatrix} 1 & 0 & 0 \\ 0 & E(b_{i-1}) \end{pmatrix} \mathbf{v}(b_{i-1}) = C \begin{pmatrix} v_1(b_{i-1}) \\ \tilde{G}_i(b_{i-1}) \\ q_{i3}(b_{i-1}) \\ \vdots \\ q_{in}(b_{i-1}) \end{pmatrix}
\]
\[
\begin{pmatrix}
v_1(b_{i-1}) \\
\tilde{G}_i(b_{i-1}) \\
q_3(b_i) \\
\vdots \\
q_m(b_i)
\end{pmatrix}.
\] (45)

Now, by the Lemma 3, we can find \( \tilde{B} \in SL_2(R[X]) \) such that
\[
\tilde{B} \begin{pmatrix} v_1(b_{i-1}) \\ \tilde{G}_i(b_{i-1}) \end{pmatrix} = \begin{pmatrix} v_1(b_i) \\ \tilde{G}_i(b_i) \end{pmatrix}.
\] (46)

Finally, define \( B \in SL_n(R[X]) \) as follows:
\[
B = \begin{pmatrix} 1 & 0 & 0 \\ 0 & E(b_i)^{-1} & 0 \\ 0 & 0 & I_{n-2} \end{pmatrix} \cdot \tilde{B} \begin{pmatrix} 1 & 0 \\ 0 & E(b_i) \end{pmatrix} \cdot C \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & E(b_i) & 0 \\ 0 & 0 & 1 \end{pmatrix}.
\] (47)

Then this \( B \) satisfies
\[
Bv(b_{i-1}) = v(b_i),
\] (48)

and by using the normality of \( E_n(R[X]) \) again, we see that
\[
B \in SL_2(R[X])E_n(R[X])
\] (49)

and this proves the claim. \( \square \)

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

Now, we want to find a realization algorithm for the matrices of the special type in \( SL_3(k[x_1, \ldots, x_m]) \), i.e. matrices of the form
\[
\begin{pmatrix}
p & q & 0 \\
r & s & 0 \\
0 & 0 & 1
\end{pmatrix} \in SL_3(k[x_1, \ldots, x_m]).
\]
Again, by applying a change of variables, we may assume that \( p \in k[x_1, \ldots, x_m] \) is a monic polynomial in the last variable \( x_m \).

In view of the Quillen Induction Algorithm developed in the section 3, we see that it’s enough to develop a realization algorithm for the matrices of
the form \[
\begin{pmatrix}
p & q & 0 \\
r & s & 0 \\
0 & 0 & 1
\end{pmatrix}
\in SL_3(R[X]),
\]
where \(R\) is now 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, and we present in the below a slightly modified version of the Lemma 3.6 in [4] Suslin’s Work on Linear Groups over Polynomial Rings and Serre Problem by S.K. Gupta and M.P. Murthy.

**Lemma 4** Let \(L\) be a commutative ring, and \(a, a', b \in L\). Then, the followings 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 \((h_1a') \cdot a + h_2 \cdot b = 1\) implies \((a, b)\) is unimodular, and \((h_1a) \cdot a' + h_2 \cdot b = 1\) 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 \(h_1a + h_2b = 1\), \(h_1'a' + h_2'b = 1\). Now, let \(g_1 = h_1h_1'\), \(g_2 = h_2'h_2\), and consider

\[
g_1aa' + g_2b = h_1h_1'aa' + (h_2' + a'h_2h_1')b = h_1'a'(h_1a + h_2b) + h_2'b = h_1'a' + h_2'b = 1.
\]

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
\[
c_1 = c_2 = c, \quad d_1 = a'd, \quad d_2 = ad. \tag{51}
\]

Now, consider
\[
\begin{pmatrix}
aa' & b & 0 \\
c & d & 0 \\
0 & 0 & 1
\end{pmatrix}
= E_{21}(cd_1d_2 - d(c_2 + a'c_1d_2)) \begin{pmatrix}
aa' & b & 0 \\
c_2 + a'c_1d_2 & d_1d_2 & 0 \\
0 & 0 & 1
\end{pmatrix}
= E_{21}(cd_1d_2 - d(c_2 + a'c_1d_2))E_{23}(d_2 - 1)E_{32}(1)E_{23}(-1)
\begin{pmatrix}
a & b & 0 \\
c_1 & d_1 & 0 \\
0 & 0 & 1
\end{pmatrix}
E_{23}(1)E_{32}(-1)E_{23}(1)
\begin{pmatrix}
a' & b & 0 \\
c_2 & d_2 & 0 \\
0 & 0 & 1
\end{pmatrix}
E_{23}(-1)E_{32}(1)E_{23}(a - 1)E_{31}(-a'c_1)E_{32}(-d_1). \tag{52}
\]
This explicit expression tells us that
\[
\begin{pmatrix}
aa' & b & 0 \\
c & d & 0 \\
0 & 0 & 1
\end{pmatrix}
\equiv \begin{pmatrix}
a & b & 0 \\
c_1 & d_1 & 0 \\
0 & 0 & 1
\end{pmatrix}
\begin{pmatrix}
a' & b & 0 \\
c_2 & d_2 & 0 \\
0 & 0 & 1
\end{pmatrix}
\pmod{E_3(L)}. \tag{53}
\]

\[\square\]

**Theorem 4** Suppose \((R, M)\) 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:** By induction on \(\deg(p)\). If \(\deg(p) = 0\), then \(p = 0\) or 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
\[
q = fp + g, \quad \deg(g) < d. \tag{54}
\]
Then,
\[
AE_{12}(-f) = \begin{pmatrix}
p & q - fp & 0 \\
r & s - fr & 0 \\
0 & 0 & 1
\end{pmatrix}
= \begin{pmatrix}
p & g & 0 \\
r & s - fr & 0 \\
0 & 0 & 1
\end{pmatrix}
\tag{55}
\]
Hence we may assume \( \text{deg}(q) < d \). Now, we note that either \( p(0) \) or \( q(0) \) is a unit in \( R \), otherwise, we would have \( p(0)s(0) - q(0)r(0) \in M \) that contradicts to \( ps - qr = p(0)s(0) - q(0)r(0) = 1 \). Let’s consider these two cases, separately.

Case 1: When \( q(0) \) is a unit.
Using the invertibility of \( q(0) \), we have

\[
AE_{21}(-q(0)^{-1}p(0)) = \begin{pmatrix} p - q(0)^{-1}p(0)q & q & 0 \\ r - q(0)^{-1}p(0)s & s & 0 \\ 0 & 0 & 1 \end{pmatrix}
\] (56)

So, we may assume \( p(0) = 0 \). Now, write \( p = Xp' \). Then, by the above Lemma 3, 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

\[
\begin{pmatrix} p & q & 0 \\ r & s & 0 \\ 0 & 0 & 1 \end{pmatrix} \equiv \begin{pmatrix} X & q & 0 \\ c_1 & d_1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} p' & q & 0 \\ c_2 & d_2 & 0 \\ 0 & 0 & 1 \end{pmatrix} \pmod{E_3(R[X])} \] (57)

Since \( \text{deg}(p') < d \), the second matrix on the right hand side is realizable by the induction hypothesis. As for the first one, we may assume that \( q \) is a unit of \( R \) since we can assume \( \text{deg}(q) < \text{deg}(X) = 1 \) and \( q(0) \) is a unit. And 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: When \( q(0) \) is not a unit.
First we claim the following; there exist \( p', q' \in R[X] \) such that \( \text{deg}(p') < l, \text{deg}(q') < d \) 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 \( \text{deg}(f) < l, \text{deg}(g) < d \) such that \( fp + gq = r \). Since \( p \) is monic and \( p, q \in R[X] \) generate the unit ideal, we see that \( r \notin M \), i.e. \( r \in A^* \). Now, letting \( p' = f/r, q' = -g/r \) shows the claim. Also note that the two relations, \( p'(0)p(0) - q'(0)q(0) = 1 \) and \( q(0) \in M, \) imply \( p'(0) \notin M \). This means \( q(0) + p'(0) \) is a unit. Now, consider the following.

\[
\begin{pmatrix} p & q & 0 \\ r & s & 0 \\ 0 & 0 & 1 \end{pmatrix} = E_{21}(rp' - sq') \begin{pmatrix} p & q & 0 \\ q' & p' & 0 \\ 0 & 0 & 1 \end{pmatrix}
\]
\[
E_{21}(rp' - sq')E_{12}(-1) \begin{pmatrix}
p + q' & q + p' & 0 \\
q' & p' & 0 \\
0 & 0 & 1
\end{pmatrix}.
\] (58)

Noting that the last matrix on the right hand side is realizable by the Case 1 since \(q(0) + p'(0)\) is a unit and \(\text{deg}(p + q') = d\), 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 contain more factors than is necessary. The Steinberg relations \([9]\) from algebraic \(K\)-theory provide a method for improving a given factorization by eliminating some of the unnecessary factors. The Steinberg relations that 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 \(j \neq l\), \([E_{ij}(a), E_{li}(b)] = E_{ij}(a)E_{li}(b)E_{ij}(-a)E_{li}(-b) = E_{ij}(-ab)\)
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 first author is in the process of implementing the realization algorithm of this paper, together with a Redundancy Elimination Algorithm based on the above set of relations, using existing computer algebra systems. As suggested in \([8]\), 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.
Acknowledgement

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

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

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

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

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

[5] A. Hahn and O.T.O’Meara. *The classical groups and K-theory*. Springer, 1989.

[6] M.A. Knus. *Quadratic and hermitian forms over rings*. Springer, 1991.

[7] T.Y. Lam. *Serre’s conjecture*, volume 635 of *Lecture Notes in Mathematics*. Springer, 1978.

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

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

[10] B. Mishra. *Algorithmic Algebra*. Springer, 1993.

[11] A.A. Suslin. Projective modules over a polynomial ring are free. *Soviet Math. Dokl.*, 17:1160–1164, 1976.
[12] A.A. Suslin. On the structure of the special linear group over polynomial rings. *Math. USSR Izv.*, 11:221–238, 1977.

[13] L. Tolhuizen, H. Holmann, and A. Kalker. A design method for bi-orthogonal, m-dimensional 2-band filter banks. *to appear in IEEE Journal*, 1994.

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