Bounded reduction of invertible matrices over polynomial rings by addition operations

By Leonid Vaserstein

Introduction

Kazhdan [15] introduced a property T for topological groups and proved it for the discrete groups $SL_r\mathbf{Z}$ with $n \geq 3$. Here $\mathbf{Z}$ stands for the ring of integers. He also proved that the group $SL_2\mathbf{Z}$ did not enjoy the T-property. He believed that neither $SL_3(\mathbf{Z}[x])$ did.

The T-property was related with other group properties (cf., e.g., [28]). For example, here are two properties of $G = SL_r\mathbf{Z}, r \geq 3$, which $G = SL_2\mathbf{Z}$ does not have:

every matrix in G is a product of a bounded number of elementary matrices [8];

every subgroup of a finite index in G contains a congruence subgroup and hence has no infinite commutative factor groups [25], [3].

Shalom [29] (cf. also [10]) proved that if every matrix in the group $SL_r(\mathbf{Z}[x_1, \ldots, x_n])$ can be reduced to a smaller size $\begin{pmatrix} * & 0 \\ 0 & 1 \end{pmatrix}$ by a bounded number of addition operations, then this discrete group has the T-property. He also observed that such a bounded reduction is possible when $r \geq n + 3$ by methods of Bass [1], using Bass' estimate $\mathrm{sr}(\mathbf{Z}[x_1, \ldots, x_n]) \leq n + 2$ for the stable rank.

Vaserstein [33] proved that $\mathrm{sr}(\mathbf{Z}[x_1, \ldots, x_n]) = n + 1$ for $n \geq 2$ and that in the case $n = 1$, when $\mathrm{sr}(\mathbf{Z}[x_1]) = 3$, the bounded reduction is still possible for $SL_3(\mathbf{Z}[x_1])$. So $SL_r(\mathbf{Z}[x_1, \ldots, x_n])$ has the T-property for $r \geq \max(3, n + 2)$.

In this paper, we show that the bounded reduction is possible when $r \geq 3$ for any n. Therefore the groups $SL_r(\mathbf{Z}[x_1, \ldots, x_n])$ have the T-property for all $r \geq 3$ and all n..

Note that that the congruence subgroup problem has negative solution for the groups $SL_r(\mathbf{Z}[x_1, \ldots, x_n])$ for all $n \geq 1$ and $r \geq 2$ (I wrote this to Kassabov in response to his question).

For any $r \geq 3$ and any n, it is known [30] (cf. also [14]) that every matrix in $SL_r(\mathbf{Z}[x_1, \ldots, x_n])$ is a product of elementary matrices but it is unknown (even for $n = 1$ and any $r \geq 3$) whether the number of elementary matrices can be bounded.

Replacing the coefficient ring $\mathbf{Z}$ by an arbitrary commutative Noetherian ring C of finite Krull dimension $\dim(C)$ (note that $\dim(\mathbf{Z}) = 1$) we obtain a more general result:

THEOREM 1.   *Let C be a commutative Noetherian ring and $\dim(C) < \infty$. Then for any $r \geq \max(3, \dim(C) + 2)$, every matrix in $SL_r(C[x_1, \ldots, x_n])$ can be reduced to the subgroup* $\begin{pmatrix} SL_{r-1}(C[x_1, \ldots, x_n]) & 0 \\ 0 & 1 \end{pmatrix}$ *by*

$$n(21n - 79)/2 + 33nr + 4r - 4$$

row addition operations.

By induction on r, we obtain

COROLLARY 2.   *Let C be a commutative Noetherian ring and $\dim(C) < \infty$. Then for any $r \geq \max(3, \dim(C) + 2)$, every matrix in $SL_r(C[x_1, \ldots, x_n])$ can be reduced to the subgroup* $\begin{pmatrix} SL_s C[x_1, \ldots, x_n]) & 0 \\ 0 & 1_{r-s} \end{pmatrix}$, *where*

$$s = \max(2, \dim(C) + 1),$$

by

$$n(21n-79)(r-s)/2 + (33n+4)(r-s)(r+s+1)/2 - 4(r-s) < 11n^2 + 17(n+1)r^2$$

row addition operations.

For example, when $C = F$ is a field, then $\dim(C) = 0$ and each matrix in the group $SL_r(F[x_1, \ldots, x_n])$ with $r \geq 3$ can be reduced to the subgroup $\begin{pmatrix} SL_2(F[x_1, \ldots, x_n]) & 0 \\ 0 & 1_{r-2} \end{pmatrix}$ by $11n^2 + 17(n+1)r^2$ addition operations. When $n = 0$, the further reduction is possible. In fact, every matrix in $SL_r F$ is a product of r^2 elementary matrices, and for any r there is a matrix in $SL_r F$ which is not a product of $r^2 - 2$ elementary matrices.

By an *elementary matrix* over a ring A we mean a matrix $a^{i,j}$ where $a \in A$ and $i \neq j$. It differs from the identity matrix 1_r at at most one off-diagonal position. Multiplication by an elementary matrix on the left is a row addition operation. In some publications (but not in the present paper), any matrix in $E_r A$, i.e., any product of elementary matrices is called an elementary matrix.

When $n \geq 1$ and $r = 2$, by Cohn [7], the *elementary length* in the group $E_2(F[x_1, \ldots, x_n])$ is unbounded, i.e., there are arbitrary long product of elementary matrices which cannot be shorten; furthermore, $SL_2(F[x_1, \ldots, x_n]) \neq E_2(F[x_1, \ldots, x_n])$ when $n \geq 2$.

Also when $F = \mathbf{C}$, the complex numbers, or $F = \mathbf{R}$, the real numbers, the elementary length in $SL_r[F[x_1]) = E_r(F[x_1])$ is unbounded for every $r \geq 2$ [31]] On the other hand, when F is finite or algebraic over a finite field, every

matrix in $SL_r(F[x_1])$ is a product of a bounded number of elementary matrices provided that $r \geq 3$ [16].

When $F = \mathbf{Q}$, the rational numbers, then for any $n \geq 1$ and any $r \geq 3$, it is unknown whether every matrix in $SL_r(F[x_1, \ldots, x_n])$ is a bounded product of elementary matrices.

Under the conditions of Theorem 1 and the additional condition that C is regular, reduction from $SL_r(C[x_1, \ldots, x_n])$ to SL_rC by addition operations is possible [30] but [30] does not give any upper bound for the number of operations, and, as mentioned above, no upper bound dependent only on n, r exists in the cases $C = \mathbf{C}$ and $C = \mathbf{R}$.

Decomposition in polynomial matrices into products of elementary matrices is important in digital signal processing, and there are many publications (cf, e.g., [5], [4], [6], [9], [11], [12], [13], [17], [22],[18], [20], [19], [21], [23], [24], [27], [26], [34]) about algorithmic ways to do this,. Most of them, give no bounds on the number of elementary matrices (or their degrees). A notable exception is [9], which gives, on page 34, representation of any matrix $\alpha \in SL_r(F[x_1, \ldots, x_n])$ as a product of $O(n^2 r^2 (\deg(\alpha)+1)^2)$ matrices each of them being elementary or belonging to the subgroup $\begin{pmatrix} SL_2(F[x_1, \ldots, x_n]) & 0 \\ 0 & 1_{r-2} \end{pmatrix}$, provided that F is an infinite field. The constant in O is not given, and the bound is obviously wrong when $n = 0$. Our Corollary 1 removes the dependence on the matrix, gives an explicit constant, and works also for finite fields.

In Section 1, we reduce Theorem 1 to Theorem 1.2 which we prove in Section 2.

Now we point out two consequences of Corollary 2.

COROLLARY 3. *Let A be a a commutative ring generated by n elements and $r \geq 3$. Then every matrix in $E_n A$ can be reduced to a matrix in $\begin{pmatrix} SL_2 A & 0 \\ 0 & 1_{r-2} \end{pmatrix}$ by $11n^2 r + 17(n + 1)r^2$ row addition operations.*

Proof. We have a ring morphism $\mathbf{Z}[x_1, \ldots, x_n] \to A$ taking 1 to 1. Every matrix $\alpha \in E_r A$ is the image of a matrix $\beta \in SL_r(\mathbf{Z}[x_1, \ldots, x_n])$. Reducing the matrix β to the subgroup $\begin{pmatrix} SL_2(\mathbf{Z}[x_1, \ldots, x_n]) & 0 \\ 0 & 1_{r-2} \end{pmatrix}$ by Corollary 1 with $C = \mathbf{Z}$, we reduce its image α to $\begin{pmatrix} SL_2 A & 0 \\ 0 & 1_{r-2} \end{pmatrix}$.

COROLLARY 4. *Let A be a a commutative algebra over a field F generated by n elements and $r \geq 3$. Then every matrix in $E_n A$ can be reduced to a matrix in $\begin{pmatrix} SL_2 A & 0 \\ 0 & 1_{r-2} \end{pmatrix}$ by $11n^2 r + 17(n + 1)r^2$ row addition operations.*

Proof. We have a ring morphism $F[x_1, \ldots, x_n] \to A$ taking 1 to 1. Every matrix in $\alpha \in E_r A$ is the image of a matrix in $\beta \in SL_r(F[x_1, \ldots, x_n])$. Reducing the matrix β to the subgroup $\begin{pmatrix} SL_2(F[x_1, \ldots, x_n]) & 0 \\ 0 & 1_{r-2} \end{pmatrix}$ by Corollary 1 with $C = F$, we reduce its image α to $\begin{pmatrix} SL_2 A & 0 \\ 0 & 1_{r-2} \end{pmatrix}$.

Acknowledgments. I discussed polynomial matrices with several mathematicians. Particularly encouraging were conversations with A.Suslin, E.Knill, I.Daubechies , and Y. de Cornulier.

1. Reduction of Theorem 1 to Theorem 1.2

Following [33], we denote by $Um_r A$ the set of unimodular columns over a ring A with 1. Obviously, $(GL_r A)e_r \subset Um_r A$, where e_r is the last column of the identity matrix 1_r.

Since every matrix $\alpha = \begin{pmatrix} \beta & 0 \\ * & 1 \end{pmatrix} \in GL_r A$ can be reduced to $\begin{pmatrix} \beta & 0 \\ 0 & 1 \end{pmatrix}$ by $r - 1$ row (or column) addition operations, Theorem 1 follows trivially from the following result.

THEOREM 1.1.   *Under the conditions of Theorem 1, let $D = \dim(C)$, $A = C[x_1, \ldots, x_n]$. Then every column $b \in Um_r A$ can be reduced to the last column e_r of the identity matrix 1_r by*

$$21n(n+1)/2 + (22D + 10r - 6)n + D + 2r - 1 \leq n(21n - 79)/2 + 33nr + 3r - 3$$

row addition operations.

The rest of this section is about reducing Theorem 1.1 to the following result involving univariate polynomials.

THEOREM 1.2.   *Let B is a commutative ring with 1 such that the space $Specm(B)$ of maximal ideals is Notherian and $\mathrm{Bdim}(B) = \delta < \infty$. Let $r \geq 3, A = B[y], b = (b_i) \in Um_r A$, and b_1 be monic. Then, by*

$$21\delta + 9r + 15$$

addition operations, the polynomial column $b = b(y)$ can be reduced to the constant column $b(0)$.

Here we use the Bass dimension $\mathrm{Bdim}(B)$ which is defined as the least δ such that

the space $Specm(B)$ of all maximal ideals of B is a finite union of subspaces of Krull dimension $\leq \delta$ each.

Clearly, $\mathrm{Bdim}(B) \le \dim(B)$ for any Noetheria ring B. Bass [1], [2] proved that

$\mathrm{sr}((B) \le \mathrm{Bdim}(B) + 1$ when $B \ne 0$.

(For the zero ring, $\dim(0) = \mathrm{Bdim}(0) = -\infty$.)

We will prove Theorem 1.2 in the next section, using a "semi-localization and patching" method. In the end of this section, we will use Theorem 1.2 to obtain Theorem 1.1 by induction on the number of variables n. In other words, we eliminate one variable after another. To eliminate a variable (using Theorem 1.2), we have to create a monic polynomial. We do this, following Suslin [33], by $\dim(C) + 1 + r$ addition operations and an invertible change of variables, using the condition $r \ge \dim(C) + 2$.

Now we describe how to create a monic polynomial.

LEMMA 1.3.   *Let C be a Noetherian ring with $\dim(C) = D < \infty, n \ge 1, A = C[x_1, \ldots, x_n]$. Let $r \ge D + 2$. Let $b = (b_i) \in Um_r A$. Then there are $c_i \in A$ and an invertible change of variables $x_1, \ldots, x_n \leftrightarrow y_1, \ldots, y_n$ such that $c_i = 0$ for $i \ge D + 2$ and the ideal*

$$A(b_1 + c_1 b_r) + \cdots + A(b_{r-1} + c_{r-1} b_r)$$

contains a monic polynomial in y_r with coefficients in $C[y_1, \ldots, y_{r-1}]$.

Proof. By Corollary 9.3 of [33], multiplying the column b by elementary matrices $a^{i,j}$ with $i \le j - 1, D + 1$, we can arrange that the first $D + 1$ entries form a prime (regular) sequence. In other words, there is an upper triangular matrix $\alpha \in GL_r A$ with ones along the main diagonal which may differ from 1_r only in the first $D + 1$ rows such that the entries $d_1, \ldots, d_{D+1}$ of the column $(d_i) = \alpha b$ form a prime sequence.

By Lemma 9.1 of [33], the hight of the ideal $J = Ad_1 + \cdots + Ad_{D+1}$ admits the lower bound $\mathrm{ht}(J) \ge D + 1$. Lemma 10.5 of [33] asserts that there is an invertible change of variables $x_1, \ldots, x_n \leftrightarrow y_1, \ldots, y_n$ such that the ideal J contains a monic polynomial in y_r with coefficients in $C[y_1, \ldots, y_{r-1}]$.

Let $(c_1, \ldots, c_{r-1}, 1)^T$ be the last column of the matrix α. Then $c_i = 0$ for $i \ge D + 2$ and $J = A(b_1 + c_1 b_r) + \cdots + A(b_{r-1} + c_{r-1} b_r)$.

COROLLARY 1.4.   *Under the conditions of Lemma 1.3, by $D + r$ addition operations, we can make the first entry of the column b to be monic in $y = y_r$ with coefficients in $B = C[x_1, \ldots, y_{n-1}]$.*

Proof. Applying Lemma 1.3 (to the column obtained from b by switching the first and last components), after $D + 1$ addition operations, we obtain a column (d_i) such that the ideal $J = Ad_2 + \cdots + Ad_r$ contains a monic polynomial. Then by adding to $b_1 = d_1$ an element of J which can be accomplished

by $r - 1$ addition operations, we make the first entry monic. The total number of addition operations is $D + 1 + r - 1 = D + r$.   □

Now we can prove Theorem 1.1.

First by Corollary 1.3 we make the first entry monic using $D + r$ addition operations. Then we can eliminate the variable $y = y_r$ by Theorem 1.2 using

$$21\delta + 9r + 15 \leq 21(n + D - 1) + 9r + 15$$

addition operations. We used that $\delta = \mathrm{Bdim}(B) \leq \dim(B) = D + n - 1$. So the total number of addition operation to eliminate one variable is at most $21n + 22D + 10r - 6$.

After n steps, using at most $21n(n + 1)/2 + (22D + 10r - 6)n$ addition operations, we can eliminate all n variables, i.e., obtain a column in Um_rC.

Since $\mathrm{sr}(C) \leq \mathrm{Bdim}(C) + 1 \leq D + 1 \leq r - 1$, we can reduce this column over C to e_r by at most $D + 1 + 2(r - 1)$ addition operations. So it takes at most

$$21n(n + 1)/2 + (22D + 10r - 6)n + D + 2r - 1 \leq n(21n - 79)/2 + 33nr + 3r - 3$$

addition operations to reduce b to e_r (we used that $D \leq r - 2$).

2. Proof of Theorem 1.2

Definition 2.1. Let A be an associative ring with 1, s a central element of A, $r \geq 2$, $v \in A^{r-1}$ (a column over A), $u \in A^{r-1\ T}$ (a row over A). We define an r by r matrix over A by

$$\mu(u, s, v) = \begin{pmatrix} 1_{r-1} + vsu & vs^2 \\ -uvu & 1 - uvs \end{pmatrix}.$$

If $s \in GL_1A$, then

$$\mu(u, s, v) = \begin{pmatrix} 1_{r-1} & 0 \\ -u/s & 1 \end{pmatrix} \begin{pmatrix} 1_{r-1} & vs^2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1_{r-1} & 0 \\ u/s & 1 \end{pmatrix}$$

is a product of $3(r - 1)$ elementary matrices.

A direct computation shows that

$$\mu(u, s, v)\mu(u, s, v') = \mu(u, s, v + v')$$

and $\mu(u, s, 0) = 1_r$, hence $\mu(u, s, v) \in GL_rA$.

LEMMA 2.2.   When $r \geq 3$, the matrix $\mu(u, s, v)$ is a product of $7r - 3$ elementary matrices in GL_rA.

Proof. We write $v = \begin{pmatrix} v_1 \\ v' \end{pmatrix}$ and $u = (u_1, u')$. Then

$$\mu(u, s, v) = \mu(u, s, e_1 v_1)\mu\left(u, s, \begin{pmatrix} 0 \\ v' \end{pmatrix}\right).$$

The second factor in detail is

$$\begin{pmatrix} 1 & 0 & 0 \\ v'su_1 & 1_{r-2} + v'su' & v's^2 \\ -u'v'u_1 & -u'v'u' & 1 - u'v's \end{pmatrix}.$$

By $r - 1$ row (or column) addition operations we can change the first column and obtain

$$\begin{pmatrix} 1 & 0 & 0 \\ v's & 1_{r-2} + v'su' & v's^2 \\ -u'v' & -u'v'u' & 1 - u'v's \end{pmatrix}.$$

Adding the first column multiplied by $-s$ to the last column we obtain the matrix

$$\begin{pmatrix} 1 & 0 & -s \\ v's & 1_{r-2} + v'su' & 0 \\ -u'v' & -u'v'u' & 1 \end{pmatrix}.$$

Adding the last row multiplied by s to the first row we obtain the matrix

$$\begin{pmatrix} 1 - u'sv' & -u'v'u's & 0 \\ v's & 1_{r-2} + v'su' & 0 \\ -u'v' & -u'v'u' & 1 \end{pmatrix}.$$

Now we can kill the first two entries in the last row by $r - 1$ row addition operations and obtain $\begin{pmatrix} \mu(u', 1, v's) & 0 \\ 0 & 1 \end{pmatrix}$ which is a product of $3(r-2)$ elementary matrices. So the second factor is a product of $5r - 6$ elementary matrices.

The first factor looks similar:

$$\mu(u, s, e_1 v_1) = \begin{pmatrix} 1 + v_1 s u_1 & v_1 s u' & v_1 s^2 \\ 0 & 1_{r-2} & 0 \\ -u_1 v_1 u_1 & u_1 v_1 u' & 1 - u_1 v_1 s \end{pmatrix}.$$

After conjugation by a permutation matrix, it takes the form

$$\begin{pmatrix} 1_{r-2} & 0 & 0 \\ v_1 s u' & 1 + v_1 s u_1 & v_1 s^2 \\ u_1 v_1 u' & -u_1 v_1 u_1 & 1 - u_1 v_1 s \end{pmatrix}.$$

After $2(r - 3)$ row addition operations, it takes the form

$$\begin{pmatrix} 1_{r-3} & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & * & 1 + v_1 s u_1 & v_1 s^2 \\ 0 & * & -u_1 v_1 u_1 & 1 - u_1 v_1 s \end{pmatrix}.$$

Now we treat the southeast 3 by 3 block in the same way as we treated the second factor above and write it as the product of $5 \cdot 3 - 6 = 9$ elementary matrices. So $\mu(u, s, e_1 v_1)$ is a product of $2(r - 3) + 9 = 2r + 3$ elementary matrices.

Thus, $\mu(u, s, v)$ is a product of $7r - 3$ elementary matrices.

COROLLARY 2.3.   *Let A be an associative ring with 1, s a central element of A, $r \geq 2$, $b', v \in A^{r-1}$, $u \in A^{r-1\ T}$, $b_r \in A$. Assume that $ub' = (1 - b_r)s$. Then we can transform the column $\begin{pmatrix} b' \\ b_r \end{pmatrix}$ to $\begin{pmatrix} b' + vs^2 \\ b_r - usv \end{pmatrix}$ by $7r - 3$ addition operations.*

Proof. We have $\mu(u, s, v) \begin{pmatrix} b' \\ b_r \end{pmatrix} = \begin{pmatrix} b' + vs^2 \\ b_r - usv \end{pmatrix}.$

COROLLARY 2.4.   *Let B be a commutative ring with 1, $A = B[y], r \geq 3, b = b(y) = (b_i) \in A^r, s \in B \cap (Ab_1 + \cdots + Ab_{r-1})$. Then the column $b(y + s^2 z)$ can be reduced to $b(x)$ by $8r - 4$ addition operations over $A[z]$.*

Proof. We write $b = b(y) = (b_i)$ as $b = \begin{pmatrix} b' \\ b_r \end{pmatrix}$. By Corollary 2.3, the column

$$b(y + s^2 z) = \begin{pmatrix} b'(y + s^2 z) \\ b_r(y + s^2 z) \end{pmatrix} \in A[z]^r$$

can be reduced to $\begin{pmatrix} b'(y) \\ b_r(y) + sw \end{pmatrix}$ by $7r - 3$ addition operations, for some $w \in A[z]$. We used that $s \in B \cap (A[z]b_1(t) + \cdots + A[z]b_{r-1}(t))$ for $t = y + s^2 z$ and that $b'(y + s^2 z) \equiv b'(y) \pmod{s^2 A[z]}$.

Now $\begin{pmatrix} b'(y) \\ b_r(y) + sw \end{pmatrix}$ can be reduced to $b(y) = \begin{pmatrix} b'(y) \\ b_r(y) \end{pmatrix}$ by $r - 1$ addition operations. $\qquad\square$

LEMMA 2.5.   *Let B be a commutative ring with 1, $A = B[y], r \geq 3, b = (b_i) \in Um_r A$, and J an ideal of B. Assume that b_1 is monic and that $\mathrm{Specm}(B/J)$ is Noetherian. Then there are $c_i \in A$ such that*
$$\mathrm{Bdim}(B/(J + B \cap (Ab_1 + A(b_2 + \textstyle\sum_{i=3}^r c_i b_i)))) \leq \mathrm{Bdim}(B/J) - 1.$$

Proof. We identify $P \in \mathrm{Specm}(B/J)$ with $P \in \mathrm{Specm}(B)$ containing J. There are only finitely many maximal irreducible components in $\mathrm{Specm}(B/J)$. We choose a maximal ideal P at each component.

For each P we can find $c_i \in A$ such that b_1 and $b_2 + \sum_{i=3}^r c_i b_i$ do not have a common zero at P (modulo P, we work with polynomials over a field), i.e., the resultant $\mathrm{res}(b_1, b_2 + \sum_{i=3}^r c_i b_i) \in B$ does not belong to P.

We use that b_1 is monic, which makes the resultant independent on the degree of the second polynomial. In general, the definition of the resultant

involves the degrees of polynomials which can degrees after reduction modulo an ideal.

By the Chinese Remainder Theorem, we can find $c_i \in A$ as above which work for every P (chosen on the irreducible components). Then passing from B/J to

$$B/(J + B \cap (Ab_1 + A(b_2 + \sum_{i=3}^{r} c_i b_i)))$$

replaces every component by a proper subset which reduces the dimension Bdim by at least 1. (When $B/J = 0$, i.e., $\mathrm{Bdim}(B/J) = -\infty$, the dimension stays $-\infty$; when $\mathrm{Bdim}(B/J) = \infty$, it may stay ∞.) $\square$

COROLLARY 2.6. *Under the conditions of Lemma 2.8, for every j such that $1 \le j \le r - 2$ there are $d_i \in B$ such that $d_1 = d_i = 0$ for $i > j$ and* $\mathrm{Bdim}(B/(B \cap \sum_{i=2}^{r-1} A(b_i + d_i b_r))) \le \mathrm{Bdim}(B/J) - j$.

Proof. When $j = 1$ this is Lemma 2.8 (observe that the addition operations not involving b_1 and b_r do not change the ideal $\sum_{i=2}^{r-1} Ab_i$).

When $j > 1$ (hence $r > 4$), we change b_3 by addition operations to get further reduction of the dimension, etc. $\square$

COROLLARY 2.7. *Let B be a commutative ring with 1 and $A = B[y]$. Assume that $\mathrm{Specm}(B)$ is Noetherian and $\delta = \mathrm{Bdim}(B) < \infty$. We write $\delta + 1 = \delta_0 + (r-2)\delta_1$ with $\delta_1 = \lfloor \delta/(r-2) \rfloor$. Let $r \ge 3, b = (b_i) \in Um_r A, b_1$ is monic. Then there are $c_{i,j} \in A$, where $2 \le i \le r-1, 0 \le j \le \delta_1$ such that $c_{i,\delta_1} = 0$ for $i \ge \delta_0 + 1$ and*

$$\sum_{j=0}^{\delta_1} (B \cap \sum_{i=2}^{r-1} A(b_i + c_{i,j} b_r)) = B.$$

Proof. This follows from Corollary 2.9 by induction on δ_1. Note that $\mathrm{Bdim}(B/J) < 0$ if and only if $J = B$. $\square$

PROPOSITION 2.8. *Under the conditions of Corollary 2.10, the polynomial column $b = b(y)$ can be reduced to the constant column $b(0)$ by*

$$(9r - 6)(\delta_1 + 1) + \delta_0$$

addition operations.

Proof. Let $c_{i,j}$ be as in Corollary 2.7. We find $s_j \in B \cap \sum_{i=2}^{r-1} A(b_i + c_{i,j} b_r)$ such that $\sum_{j=0}^{\delta_1} s_j = 1$.

For $j = 0, \ldots, \delta_1$, we set $b^{(j)} = (b_i + c_{i,j} b_r) \in Um_r A$, where $c_{1,j} = c_{r,r} = 0$. By Corollary 2.4, the polynomial column $b^{(j)}(y)$ can be reduced to $b^{(j)}(y + s_j^2 z_j)$

by $8r - 4$ addition operations over $A[z_j]$. We write this fact as follows:

$$b^{(j)}(y) \underset{8r-4}{\rightarrow} b^{(j)}(y + s_j^2 z_j).$$

Now we combine this with the fact that $b(y)$ can be reduced to $b^{(j)}(y)$ by $r - 2$ addition operations:

$$b(y) \underset{r-2}{\rightarrow} b^{(j)}(y) \underset{8r-4}{\rightarrow} b^{(j)}(y + s_j^2 z_j)$$

(when $j = \delta_1$, the number $r - 2$ can be replaced by $\delta_0 \leq r - 3$).

Combining the addition operations, we obtain:

$$b(y) \underset{r-2}{\rightarrow} b^{(0)}(y) \underset{8r-4}{\rightarrow} b^{(0)}(y + s_0^2 z_0) \underset{r-2}{\rightarrow} b^{(1)}(y + s_0^2 z_0) \underset{8r-4}{\rightarrow} b^{(1)}(y + s_0^2 z_0 + s_1^2 z_1)$$

$$\cdots \underset{8r-4}{\rightarrow} b^{(\delta_1)}(y + s_0^2 z_0 + \cdots + s_{\delta_1}^2 z_{\delta_1}) \underset{\delta_0}{\rightarrow} b(y + s_0^2 z_0 + \cdots + s_{\delta_1}^2 z_{\delta_1}).$$

Thus, $b(y)$ can be reduced to $b(y + s_0^2 z_0 + \cdots + s_{\delta_1}^2 z_{\delta_1})$ by $(9r - 6)(\delta_1 + 1) + \delta_0$ addition operations over the the polynomial ring ring $A[z_0, \ldots, z_{\delta_1}]$.

Since $\sum s_j = 1$, $\sum B s_j^2 = B$. Specializing the indeterminates z_j to elements in yB, we make $y + s_0^2 z_0 + \cdots + s_{\delta_1}^2 z_{\delta_1}$ zero. $\qquad\square$

Now we can finish our proof of Theorem 1.2. Using that $\delta_0 \geq 0, \delta = (r - 2)\delta_1 + \delta_0$, and $r \geq 3$ (hence $13r\delta_1 \geq 36\delta_1$), we get that

$$9(r - 6)(\delta_1 + 1) + \delta_0 \leq 21\delta + 9r + 15.$$

So Theorem 1.2 follows from Proposition 2.8.

Remark. If $\delta_1 = 0$ in Proposition 2.8, i.e., $\delta \leq r - 3$ in Theorem 1.2, then the bound $9r - 6 + \delta$ in Proposition 2.8 (resp., $9r + 15$ in Theorem 1.2) can be easily improved to the bound $2\delta + r + 1$ (resp., $3r - 5$).

3. Concluding remarks

By Vaserstein [33] §5, for any commutative ring A and any $r \geq 1$, if every $b \in Um_{2r}A$ can be reduced to e_{2r} by a bounded number of addition operations, then this can be done by a bounded number of elementary symplectic operations. Therefore, it is trivial to extend our results to the symplectic groups $Sp_{2r}A$ with some bounds, but getting good bounds requires some work.

Also similar results can be obtained by similar methods for orthogonal and other simple isotropic algebraic groups.

In conclusion, it is interesting to compare results of the present paper with those of [32]. Let X be a topological space, $A = \mathbf{R}^X$ (resp., $A = \mathbf{C}^X$) the ring of continuous real (resp., complex) functions on X. Assume that X is finitely-dimensional (i.e., $\mathrm{sr}A) < \infty$). It is shown in [32] that every matrix in $E_r A$ can be reduced to the subgroup $\begin{pmatrix} SL_2 A & 0 \\ 0 & 1_{r-2} \end{pmatrix}$ by a bounded number of addition operations and that (in the case $A = \mathbf{R}^X$ and $r = 2$) the further bounded reduction to 1_r is not always possible.

This is similar to Corollary 1 above. However, when $A = \mathbf{C}^X$ or $r \geq 3$, every matrix in $E_r A$ is a product of a bounded number (depending only on r and $\mathrm{sr}(A)$) of elementary matrices which contrasts with the situation for $A = \mathbf{R}[x]$ or $\mathbf{C}[x]$. A philosophical explanation is that while the fundamental group of $SL_n \mathbf{R}$ is finite for $r \geq 3$ (which was used in [32]), an algebraic version of the fundamental group is $K_2 \mathbf{R}$ which is infinitely generated (which was used in [31]).

PENN STATE, UNIVERSITY PARK, PA

REFERENCES

[1] H. BASS, K-theory and stable algebra. Inst. Hautes Études Sci. Publ. Math. No. 22 (1964), 5–60.

[2] ———, Algebraic K-theory. W. A. Benjamin, Inc., New York-Amsterdam 1968 xx+762 pp.

[3] ———, J. MILNOR, and J.-P. SERRE, Solution of the congruence subgroup problem for SL_n ($n \geq 3$) and Sp_{2n} ($n \geq 2$). Inst. Hautes Études Sci. Publ. Math. No. 33 (1967), 59–137. Erratum by J.-P. SERRE: Inst. Hautes Études Sci. Publ. Math. No. 44 (1974), 241–244.

[4] N.K. BOSE (Ed.), Multidimensional Systems Theory: Progress, Directions and Open Problems, Reidel, Dordrecht, The Netherlands, 1985.

[5] ———and S. LERTRATTANAPANICH, Polynomial matrix factorization, multidimensional filter banks, and wavelets. Sampling, wavelets, and tomography, 137–156, Appl. Numer. Harmon. Anal., Birkhäuser Boston, Boston, MA, 2004.

[6] S. BASU and A.C. TAN, On a generalized factorization problem for structurally passive synthesis of digital filters, IEEE Trans. Circuits Systems 36 (1989), 1529–1543.

[7] P. M. COHN, On the structure of the GL_2 of a ring. Inst. Hautes Études Sci. Publ. Math. No. 30 1966, 5–53.

[8] D. CARTER and G. KELLER, Elementary expressions for unimodular matrices. Comm. Algebra 12 (1984), no. 3-4, 379–389.

[9] L. CANIGLIA, G. CORTIAS, S. DANÓN, J. HEINTZ, T. KRICK, and P. SOLERNÓ, Algorithmic aspects of Suslin's proof of Serre's conjecture. Comput. Complexity 3 (1993), no. 1, 31–55.

[10] Y. DE CORNULIER, Property T for linear groups over rings, after Shalom, preprint 2006, 4 pages.

[11] E. Fornasini and M.E. Valcher, nD Polynomial matrices with applications to multidimensional signal analysis, Multidimensional Systems Signal Process. 8 (1997), 387–408.

[12] J. Gago-Vargas, Constructions in $R[x_1, \ldots, x_n]$: applications to K-theory. J. Pure Appl. Algebra 171 (2002), no. 2-3, 185–196.

[13] _____, On Suslin's stability theorem for $R[x_1, \ldots, x_m]$. (English summary) Ring theory and algebraic geometry (Len, 1999), 203–210, Lecture Notes in Pure and Appl. Math., 221, Dekker, New York, 2001.

[14] F. Grunewald, J. Mennicke, and L. Vaserstein, On symplectic groups over polynomial rings. Math. Z. 206 (1991), no. 1, 35–56.

[15] D. Kazhdan, On the connection of the dual space of a group with the structure of its closed subgroups, Funk. Anal. Pril. 1 (1967), 71–74.

[16] H.W. Lenstra, Jr., On Artin's conjecture and Euclid's algorithm in global fields. Invent. Math. 42 (1977), 201–224.

[17] H. Lombardi and I. Yengui, Suslin's algorithms for reduction of unimodular rows. J. Symbolic Comput. 39 (2005), no. 6, 707–717.

[18] Z. Lin, Notes on n-D polynomial matrix factorizations. Multidimens. Systems Signal Process. 10 (1999), no. 4, 379–393.

[19] _____, Further results on n-D polynomial matrix factorizations. Multidimens. Systems Signal Process. 12 (2001), no. 2, 199–208.

[20] _____, N.K. Bose, Some conjectures on multivariate polynomial matrices. The Second International Workshop on Multidimensional (nD) Systems (Czocha Castle, 2000), 165–170, Tech. Univ. Press, Zielona Góra, 2000.

[21] _____, N.K. Bose, A generalization of Serre's conjecture and some related issues. Linear Algebra Appl. 338 (2001), 125–138.

[22] _____, J. Q. Ying, and L. Xu, Factorizations for nD polynomial matrices. Circuits Systems Signal Process. 20 (2001), no. 6, 601–618.

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

[24] R.C. Laubenbacher and C. J. Woodburn, A new algorithm for the Quillen-Suslin theorem. Beiträge Algebra Geom. 41 (2000), no. 1, 23–31.

[25] J. L. Mennicke, Finite factor groups of the unimodular group. Ann. of Math. (2) 81 (1965), 31–37.

[26] H. Park, A realization algorithm for $\mathrm{SL}_2(R[x_1, \cdots, x_m])$ over the Euclidean domain. SIAM J. Matrix Anal. Appl. 21 (1999), no. 1, 178–184 (electronic).

[27] _____ and C. Woodburn, An Algorithmic Proof of Suslin's Stability Theorem for Polynomial Rings. J. Algebra 178 (1995), 277–298.

[28] Y. Shalom, Bounded generation and Kazhdan's property (T). Inst. Hautes Études Sci. Publ. Math. No. 90 (1999), 145–168 (2001).

[29] _____, Algebraization of Kazhdan's property (T), preprint, 2006, 26 pp.

[30] A. A. Suslin, The structure of the special linear group over rings of polynomials. Izv. Akad. Nauk SSSR Ser. Mat. 41 (1977), no. 2, 235–252, 477.

[31] W. van der Kallen, $\mathrm{SL}_3(C[X])$ does not have bounded word length. Algebraic K-theory, Part I (Oberwolfach, 1980), pp. 357–361, Lecture Notes in Math., 966, Springer, Berlin-New York, 1982.

[32] L.N. Vaserstein, Reduction of a matrix depending on parameters to a diagonal form by addition operations. Proc. Amer. Math. Soc. 103 (1988), no. 3, 741–746.

[33] _____ and A. A. Suslin, Serre's problem on projective modules over polynomial rings, and algebraic K-theory. (Russian) Izv. Akad. Nauk SSSR Ser. Mat. 40 (1976), no. 5, 993–1054, 1199.

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