ON THE COMPLEXITY OF BILINEAR FORMS OVER ASSOCIATIVE ALGEBRAS

Nader H. Bshouty

Department of Computer Science, Technion-I.I.T, Haifa, Israel
Department of Computer Science, University of Calgary
2500 University Drive N.W.
Calgary, Alberta, Canada T2N 1N4
e-mail: bshouty@cpsc.ucalgary.ca

ABSTRACT:

Let F be a field and let $Q(\alpha) = q_1^{d_1}(\alpha)\cdots q_k^{d_k}(\alpha) \in F[\alpha]$ be a polynomial of degree n where $q_1(\alpha),\cdots,q_k(\alpha)$ are distinct irreducible polynomials. Let $y_1(\alpha),\cdots,y_r(\alpha)$, $x_1(\alpha),\cdots,x_s(\alpha)$ be $r+s$, $n-1$-degree polynomials. It is shown that if $Card(F) \geq \max_{1\leq i\leq k} 2deg\ q_i^{d_i}(\alpha) - 2$ then the number of nonscalar multiplications/ divisions required to compute the coefficients of $x_i(\alpha)y_1(\alpha)\ mod\ Q(\alpha), i = 1,\cdots,s$ by straight line algorithms is $s(2n-k)$. We also prove that if H is a $s\times r$ matrix with entries from F then the number of nonscalar multiplications/ divisions required to compute the coefficients of $(x_1(\alpha),\cdots,x_s(\alpha))H(y_1(\alpha),\cdots,y_r(\alpha))^T$ by straight line algorithms is $rank(H)(2n-k)$. All those systems satisfy the direct sum conjecture strongly. For some other algebras that are direct sum of local algebras the above results are also hold.

1. INTRODUCTION

Let F be a field and let $x = (x_1,\cdots,x_n)^T$ be a vector of indeterminates . Let $Q_x = \{x^TQ_1x,\cdots,x^TQ_mx\}$ be a set of quadratic forms on $x_1,\cdots,x_n$ over F where Q_i is a $n\times n$ matrix with entries from F. A *straight*

line algorithm that computes Q_x is a sequence of rational functions $\sigma_1, \cdots, \sigma_L$ where

1) For every $1 \leq j \leq L$ we have $\sigma_j = w_{j,1} \circ w_{j,2}$ where $\circ \in \{\times, \div\}$

$$w_{j,1}, w_{j,2} \in \left(F + \sum_{i=1}^{n} F x_i + \sum_{i=1}^{j-1} F\sigma_i\right) \backslash F$$

or $\circ = \div$, $w_{j,1} \in F$ and $w_{j,2} \in \left(F + \sum_{i=1}^{n} F x_i + \sum_{i=1}^{j-1} F\sigma_i\right) \backslash F$.

2) We have

$$Q_x \subseteq F + \sum_{i=1}^{n} F x_i + \sum_{i=1}^{L} F\sigma_i.$$

We call the operation $\circ$ in 1) a *non-scalar* $\circ$. Therefore in this model we count only non-scalar multiplications/ divisions.

The minimal L is denoted by $L(Q_x)$ or $L_F(Q_x)$ and called the *multiplicative complexity* of Q_x.

When we compute Q_x by an algorithm $\sigma_1, \cdots, \sigma_\mu$ where $\sigma_j = w_{j,1} \times w_{j,2}$, $w_{j,1}, w_{j,2} \in \sum_{i=1}^{n} F x_i$ then we call the algorithm *quadratic algorithm* . The minimal μ is denoted by $\mu(Q_x)$ or $\mu_F(Q_x)$ and is called the *quadratic complexity* of Q_x. In [17] Strassen proved that for infinite fields F

$$L_F(Q_x) = \mu_F(Q_x). \tag{1}$$

Let $u = (u_1, \cdots, u_n)^T$ be a vector of new indeterminates and

$$Q_x^1 = \{x^T Q_1 x, \cdots, x^T Q_{m_1} x\}, \qquad Q_u^2 = \{u^T Q_{m_1+1} u, \cdots, u^T Q_{m_2} u\}$$

be two sets of quadratic forms. It is obvious that

$$\mu(Q_x^1 \cup Q_u^2) \leq \mu(Q_x^1) + \mu(Q_u^2). \tag{2}$$

In [9], [17] and [18] Fiduccia- Zalcstein, Strassen and Winograd , respectively, conjecture that for every two sets of quadratic forms Q_x^1, Q_u^2 we have

$$\mu(Q_x^1 \cup Q_u^2) = \mu(Q_x^1) + \mu(Q_u^2), \tag{3}$$

and every minimal quadratic algorithm $\sigma_1, \cdots, \sigma_\mu$ for $(Q_x^1 \cup Q_u^2)$ can be separated in to two minimal algorithms

$$s_1 = (\sigma_i)_{i \in I}, \qquad s_2 = (\sigma_i)_{i \in J}, \tag{4}$$

where $I \cup J = \{1, \cdots, \mu\}$, $I \cap J = \emptyset$, and s_1 and s_2 are minimal quadratic algorithms for Q_x^1 and Q_u^2, respectively. The set $Q_x^1 \cup Q_u^2$ is called the *direct sum* of Q_x^1 and Q_u^2. We also denote it by $Q_x^1 \oplus Q_u^2$.

When (3) is satisfied for Q_x^1 and Q_u^2 then we say that Q_x^1 and Q_u^2 satisfy the *direct sum conjecture* in the model of quadratic algorithms. We define DSC_{QA} or $DSC_{QA}(F)$ to be the set of all pairs (Q_x^1, Q_u^2) such that Q_x^1 and Q_u^2 satisfy the direct sum conjecture in the quadratic algorithms model. When (4) is

satisfied for Q_x^1 and Q_u^2 then we say that Q_x^1 and Q_u^2 satisfy the *direct sum conjecture strongly* in the model of quadratic algorithms. We define $DSCS_{QA}$ or $DSCS_{QA}(F)$ to be the set of all pairs (Q_x^1, Q_u^2) such that Q_x^1 and Q_u^2 satisfy the direct sum conjecture strongly in the quadratic algorithms model. If for every Q_u^2 we have $(Q_x^1, Q_u^2) \in DSCS_{QA}$ then we write $Q_x^1 \in DSCS_{QA}$.

Similarly, we define the classes DSC_{SLA} and $DSCS_{SLA}$ for the straight line model. It is obvious that

$$DSC_M \subseteq DSCS_M$$

for every model of computation M. By the results of Strassen in [17] and Bshouty in [8], for infinite fields F, we also have

$$DSC_{SLA}(F) = DSC_{QA}(F), \qquad DSCS_{SLA}(F) = DSCS_{QA}(F).$$

Let $x = (x_1, \cdots, x_n)^T$ and $y = (y_1, \cdots, y_m)^T$ be vectors of indeterminates. Let $B_{x,y}$ be a set of bilinear forms $\{x^T B_1 y, \cdots, x^T B_k y\}$. A *bilinear algorithm* that computes $B_{x,y}$ is a quadratic algorithm $\sigma_1, \cdots, \sigma_\delta$ where $\sigma_i = w_{j,1} \times w_{j,2}$, $w_{j,1} \in \sum_{i=1}^n F x_i$ and $w_{j,2} \in \sum_{i=1}^m F y_i$. In a similar manner we define $\delta(B_{x,y})$ the *bilinear complexity* of $B_{x,y}$. Obviously, $\mu(B_{x,y}) \leq \delta(B_{x,y})$. We also define DSC_{BA} and $DSCS_{BA}$.

Let $\mathbf{A}$ be an associative algebra of dimension k with a unity element 1 and let $\{a_1, \cdots, a_k\}$ be a base of $\mathbf{A}$. We denote by $[xy]_{\mathbf{A}} = \{x^T B_1 y, \cdots, x^T B_k y\}$ the set of bilinear forms defined by the product of two elements in the algebra $\mathbf{A}$, i.e,

$$\sum_{i=1}^{k} (x^T B_i y) a_i = \left(\sum_{i=1}^{k} x_i a_i \right) \left(\sum_{i=1}^{k} y_i a_i \right).$$

In a similar manner we can define $[x_1 y, x_2 y, \cdots, x_n y]_{\mathbf{A}}$ and $[x_1 y_1 + \cdots + x_n y_n]_{\mathbf{A}}$ or more general $[x^T C_1 y, \cdots, x^T C_j y]_{\mathbf{A}}$ where $x = (x_1, \cdots, x_n)^T \in \mathbf{A}^n$, $y = (y_1, \cdots, y_m)^T \in \mathbf{A}^m$ and $C_1, \cdots, C_j$ are $n \times m$ matrices.

Obviously, $[\ ]_F$ depends on the chooses bases $\{a_1, \cdots, a_k\}$. By Feduccia-Zalcstein [9] and section 3 results, the complexity of $[\ ]_F$ does not depend on the bases.

In [4], Alder and Strassen proved that for every set of quadratic forms Q_u we have

$$\mu([xy]_{\mathbf{A}} \oplus Q_u) \geq 2\ dim\ \mathbf{A} - I_{\mathbf{A}} + \mu(Q_u)$$

where $I_{\mathbf{A}}$ is the number of the maximal two side ideals of $\mathbf{A}$. This result have been generalized by Auslander-Winograd [5] and Hartman [13]. They proved that if $\mathbf{A}$ is a direct sum of division algebras then

$$\mu([x_1 y, x_2 y, \cdots, x_n y]_{\mathbf{A}}) \geq (2dim\ \mathbf{A} - I_{\mathbf{A}})n.$$

If $\mu([x_1 y, x_2 y, \cdots, x_n y]_{\mathbf{A}}) \leq (2dim\ \mathbf{A} - I_{\mathbf{A}})n$ then we call $\mathbf{A}$ an algebra of $n-$*minimal complexity* and if $\delta([x_1 y, x_2 y, \cdots, x_n y]_{\mathbf{A}}) \leq (2dim\ \mathbf{A} - I_{\mathbf{A}})n$, then we call $\mathbf{A}$ an algebra of $n-$*minimal rank*. Obviously, if $\mathbf{A}$ is an algebra of 1-minimal complexity (rank) then it is an algebra of n-minimal complexity (rank) for every n. In [10] De-Groote proved that a division algebra $\mathbf{A}$ is an algebras of 1-minimal complexity if and only if

$\mathbf{A}$ is a field with $|F| \geq 2dim\ \mathbf{A}$. Other characterization of 1-minimal rank algebras can be found in [12] and [15].

In this paper we generalize all the results in [4], [5], [6], [13] and [18]. We prove the following:

Theorem I . Let $\mathbf{A} = \mathbf{A}_1 \times \cdots \times \mathbf{A}_k$ be an algebra where each $\mathbf{A}_i$ is local commutative algebra and there exist $d_i \in \mathbf{A}_i$ such that $\{a | a\ rad\mathbf{A}_i = 0\} = d_i\mathbf{A}_i$, or $\mathbf{A}_i$ is a division algebra. Then for every set of quadratic forms C we have

$$\mu([x_1y, \cdots, x_ny]_{\mathbf{A}} \oplus C) \geq (2dim\mathbf{A} - k)n + \mu(C).$$

If $\mathbf{A}$ is an algebra of n-minimal complexity then

$$[x_1y, \cdots, x_ny]_{\mathbf{A}} \in DSCS_{SLA}.$$

Theorem II . Let $\mathbf{A} = \mathbf{A}_1 \times \cdots \times \mathbf{A}_k$ be an algebra where $\mathbf{A}_i$ is local algebra. Then for every set of bilinear forms B we have

$$\delta([x_1y, \cdots, x_ny]_{\mathbf{A}} \oplus B) \geq (2dim\mathbf{A} - k)n + \delta(B).$$

If $\mathbf{A}$ is an algebra of n-minimal rank then

$$[x_1y, \cdots, x_ny]_{\mathbf{A}} \in DSCS_{BA}.$$

Theorem III . Let $\mathbf{A}$ be a commutative algebra. Let H be a $n \times m$ matrix. Then

$$\mu([x^THy]_{\mathbf{A}}) \geq (2dim\mathbf{A} - I_{\mathbf{A}})rank(H).$$

If $\mathbf{A}_1$ and $\mathbf{A}_2$ are commutative algebras of $rank(H_1)$- minimal rank and $rank(H_2)$-minimal rank, respectively, then

$$([x^TH_1y]_{\mathbf{A}_1}, [x^TH_2y]_{\mathbf{A}_2}) \in DSCS_{SLA}.$$

Theorem IV . Let $\mathbf{A} = \mathbf{A}_1 \times \cdots \times \mathbf{A}_k$ be an algebra where $\mathbf{A}_i$ is local. Let H be an $n \times m$ matrix. Then for every set of bilinear form B we have

$$\delta([x^THy]_{\mathbf{A}} \oplus B) \geq (2dim\mathbf{A} - k)rank(H) + \delta(B).$$

If $\mathbf{A}$ is an algebra of $rank(H)$-minimal rank then

$$[x^THy]_{\mathbf{A}} \in DSCS_{BA}.$$

Since by Artinian theorem, every commutative algebra is a direct sum of local commutative algebras, Theorem II and IV are true for commutative algebras. In this case we have $k = I_{\mathbf{A}}$.

We also prove lower bounds for some other bilinear systems over direct sum of local algebras.

Theorems I,II,III and IV follows:

Let $\mathbf{A} = F[\alpha]/(p(\alpha))$ where $p(\alpha) = p_1^{d_1}(\alpha)\cdots p_k^{d_k}(\alpha) \in F[\alpha]$ is a polynomial of degree n where $p_1, \cdots, p_k$ are distinct irreducible polynomials. Then $[xy]_{\mathbf{A}}$ is equivalent to the problem of computing the product of two $n-1$-degree polynomials modulo $p(\alpha)$. By theorem I and II we have:

Corollary I . Let $\mathbf{A} = F[\alpha]/(p(\alpha))$ where $p = p_1^{d_1}\cdots p_k^{d_k}$, $p_1, \cdots, p_k$ are distinct irreducible polynomials and $|F| \geq 2\max_{1\leq i\leq k}\ deg\ p_i^{d_i}(\alpha) - 2$. Then for every set of quadratic forms C and bilinear forms B we have

$$\mu([x_1y, \cdots, x_ny]_{\mathbf{A}} \oplus C) = (2deg\ p - k)n + \mu(C),$$

$$\delta([x_1y, \cdots, x_ny]_{\mathbf{A}} \oplus B) = (2deg\ p - k)n + \delta(B),$$

and

$$[x_1y, \cdots, x_ny]_{\mathbf{A}} \in DSCS_{SLA}, DSCS_{BA}.$$

Notice that when F is finite field we need more restricted conditions on C and B. For details see [8].

For sets of quadratic forms Q_x^1 and Q_u^2, [bilinear forms $B_{x,y}$], let $Alg_{SLA}(Q_x^1)$, $[Alg_{BA}(B_{x,y})]$, denote the set of all minimal straight line algorithms, [bilinear algorithms], that computes Q_x^1, $[B_{x,y}]$. We denote by $Alg_{SLA}(Q_x^1) \oplus Alg_{SLA}(Q_u^2)$ the set of all straight line algorithms $\sigma_1, \cdots, \sigma_t$ such that there exist sets $I, J \subset \{1, \cdots, t\}$, $I \cup J = \{1, \cdots, t\}$ and $I \cap J = \emptyset$, where $(\sigma_i)_{i\in I} \in Alg_{SLA}(Q_x^1)$ and $(\sigma_i)_{i\in J} \in Alg_{SLA}(Q_u^2)$. Obviously, $(Q_x^1, Q_u^2) \in DSCS_{SLA}$ if and only if $Alg_{SLA}(Q_x^1 \oplus Q_u^2) = Alg_{SLA}(Q_x^1) \oplus Alg_{SLA}(Q_u^2)$. By corollary I we have

Corollary II . Let $\mathbf{A} = F[\alpha]/(p(\alpha))$ where $p = p_1^{d_1}\cdots p_k^{d_k}$, $p_1, \cdots, p_k$ are distinct irreducible polynomials and $|F| \geq 2\max_{1\leq i\leq k}\ deg\ p_i^{d_i}(\alpha) - 2$. Then for a base $\{a_1, \cdots, a_n\}$ that represent $\mathbf{A}$ as $F[\alpha]/(p_1^{d_1}(\alpha)) \times \cdots \times F[\alpha]/(p_k^{d_k}(\alpha))$ we have

$$Alg_{SLA}([x_1y, \cdots, x_ny]_{\mathbf{A}}) = Alg_{SLA}([x_1y, \cdots, x_ny]_{F[\alpha]/(p_1^{d_1}(\alpha))}) \oplus \cdots \oplus Alg_{SLA}([x_1y, \cdots, x_ny]_{F[\alpha]/(p_k^{d_k}(\alpha))}),$$

and

$$Alg_{BA}([x_1y, \cdots, x_ny]_{\mathbf{A}}) = Alg_{BA}([x_1y, \cdots, x_ny]_{F[\alpha]/(p_1^{d_1}(\alpha))}) \oplus \cdots \oplus Alg_{BA}([x_1y, \cdots, x_ny]_{F[\alpha]/(p_k^{d_k}(\alpha))}).$$

Notice that section 3 shows that the classification of all minimal algorithms for $[\ ]_{\mathbf{A}}$ for some base gives the classification of all minimal algorithms for this system for any base.

This corollary shows that a classification of all minimal straight line algorithms, [bilinear algorithms], for $[x_1y, \cdots, x_ny]_{\mathbf{A}}$ where $\mathbf{A} = F[\alpha]/(p^{d_i}(\alpha))$, $p(\alpha)$ is irreducible gives a classification for all the minimal straight line algorithms, [bilinear algorithms], for $[x_1y, \cdots, x_ny]_{\mathbf{A}}$ where $\mathbf{A} = F[\alpha]/(p(\alpha))$, for any polynomial $p(\alpha)$. A classification of all minimal bilinear algorithms in the case where $n = 1$ is completely studied in [2] and [3].

Theorems III and IV follows:

Corollary III . Let $\mathbf{A} = F[\alpha]/(p(\alpha))$ where $p = p_1^{d_1} \cdots p_k^{d_k}$, $p_1, \cdots, p_k$ are distinct irreducible polynomials and $|F| \geq 2\max_{1 \leq i \leq k} \ deg \ p_i^{d_i}(\alpha) - 2$. Then for every set of bilinear forms B we have

$$\mu([x^T H y]_{\mathbf{A}}) = (2deg \ p(\alpha) - k) rank(H),$$

$$\delta([x^T H y]_{\mathbf{A}} \oplus B) = (2deg \ p(\alpha) - k) rank(H) + \delta(B)$$

and

$$[x^T H y]_{\mathbf{A}} \in DSCS_{BA}.$$

As in corollary II we have

Corollary IV . Let $\mathbf{A} = F[\alpha]/(p(\alpha))$ where $p = p_1^{d_1} \cdots p_k^{d_k}$, $p_1, \cdots, p_k$ are distinct irreducible polynomials and $|F| \geq 2\max_{1 \leq i \leq k} \ deg \ p_i^{d_i}(\alpha) - 2$. Then for a base $\{a_1, \cdots, a_n\}$ that represent $\mathbf{A}$ as $F[\alpha]/(p_1^{d_1}(\alpha)) \times \cdots \times F[\alpha]/(p_k^{d_k}(\alpha))$ we have

$$Alg_{SLA}([x^T H y]_{\mathbf{A}}) = Alg_{SLA}([x^T H y]_{F[\alpha]/(p_1^{d_1}(\alpha))}) \oplus \cdots \oplus Alg_{SLA}([x^T H y]_{F[\alpha]/(p_k^{d_k}(\alpha))})$$

and

$$Alg_{BA}([x^T H y]_{\mathbf{A}}) = Alg_{BA}([x^T H y]_{F[\alpha]/(p_1^{d_1}(\alpha))}) \oplus \cdots \oplus Alg_{BA}([x^T H y]_{F[\alpha]/(p_k^{d_k}(\alpha))}).$$

In section 2 we give preliminary results in the bilinear and quadratic complexity theory. In section 3 we study some of the properties of the regular representation of associative algebras and in section 4 we use these properties to classify some minimal bilinear and quadratic algorithms. In section 5 and section 6 we study the complexity of $[x_1 y, \cdots, x_n y]_{\mathbf{A}}$ and $[x^T H y]_{\mathbf{A}}$, respectively. The technique we use can be used to prove lower bounds for many other bilinear systems over associative algebras.

2. PRELIMINARY RESULTS

In this section we give some preliminary results

Definition 1. Let $B = \{B_1, \cdots, B_k\}$ be a set of $n \times m$ matrices. We define the *$T-dual$* and *$D-$ dual sets* B^T and B^D of B as follows:

$$B^T = \{B_1^T, \cdots, B_k^T\} \quad , \quad B^D = \{C_1, \cdots, C_m\},$$

Here B_i^T is the transpose of B_i and B^D denotes the set of $n \times k$ matrices that satisfy

$$C_i^j = B_j^i, i, = 1, \cdots, m \ , \ j, = 1, \cdots, k,$$

where B_i^j is the j-th column of B_i, i.e

$$C_i = [B_1 e_{m,i} | \cdots | B_k e_{m,i}].$$

where $e_{m,i}$ is the i-th column unit vector of order m.

We also define $B^E = B^{TDT}$, i.e $B^E = \{D_1, \cdots, D_n\}$ where

$$D_i = \begin{bmatrix} e_{n,i}^T B_1 \\ \vdots \\ e_{n,i}^T B_k \end{bmatrix}.$$

Definition 2. Let $B = \{B_1, \cdots, B_k\}$ be a set of $n \times m$ matrices. Let M, N and $K = (K_{i,j})$ be $m \times m'$, $n' \times n$ and $k' \times k$ matrices, respectively. We define

$$NBM = \{NB_1M, \cdots, NB_kM\}, \quad B[K] = \left\{ \sum_{j=1}^{k} K_{1,j} B_j, \cdots, \sum_{j=1}^{k} K_{k',j} B_j \right\}.$$

Definition 3. Let $B = \{B_1, \cdots, B_k\}$ and $C = \{C_1, \cdots, C_{k'}\}$ be sets of $n \times m$ and $n' \times m'$ matrices, respectively. We define

$$B \oplus C = \{\tilde{B}_1, \cdots, \tilde{B}_k, \tilde{C}_1, \cdots, \tilde{C}_{k'}\}$$

where

$$\tilde{B}_i = \begin{pmatrix} B_i & 0_{n \times m'} \\ 0_{n' \times m} & 0_{n' \times m'} \end{pmatrix} \quad , \quad \tilde{C}_j = \begin{pmatrix} 0_{n \times m} & 0_{n \times m'} \\ 0_{n' \times m} & C_j \end{pmatrix}$$

and $0_{s \times r}$ denotes the zero $s \times r$ matrix.

Define

$$B \otimes C = \left\{ B_i \otimes C_j \middle| \ i = 1, \cdots, k, j = 1, \cdots, k' \right\}.$$

where $\otimes$ is the Kronecker product of matrices. If $k = k'$ then

$$diag(B, C) = \{diag(B_1, C_1), \cdots, diag(B_k, C_k)\}$$

where

$$diag(B_i, C_i) = \begin{pmatrix} B_i & \\ & C_i \end{pmatrix}.$$

Lemma 1. *[7]. Let A_1, A_2 and A be sets of k_1, k_2 and k, $n_1 \times m_1$, $n_2 \times m_2$ and $n \times m$ matrices, respectively, and I_r be the identity matrix of order r. Then*

(1) $A^{TT} = A$, $A^{DD} = A$, $A^{EE} = A$, $A^E = A^{TDT} = A^{DTD}$.

(2) $A[K][J] = A[JK]$, $(NAM)[K] = N(A[K])M$.

(3) $(NAM)^T = M^T A^T N^T$, $(A[K])^T = A^T[K]$

(4) $(NA)^D = NA^D$, $(AM)^D = A^D[M^T]$, $(A[K])^D = A^D K^T$.

(5) $(A_1 \oplus A_2)^T = A_1^T \oplus A_2^T$, $(A_1 \oplus A_2)^D = A_1^D \oplus A_2^D$.

(6) $(A_1 \otimes A_2)^T = A_1^T \otimes A_2^T$, $(A_1 \otimes A_2)^D = A_1^D \otimes A_2^D$.

(7) $A_1[K] \oplus A_2 = (A_1 \oplus A_2)[diag(K, I_{k_2})]$, $NA_1M \oplus A_2 = diag(N, I_{n_2})(A_1 \oplus A_2)diag(M, I_{m_2})$.

(8) $A_1[K] \otimes A_2 = (A_1 \otimes A_2)[K \otimes I_{k_2}]$, $NA_1M \otimes A_2 = (N \otimes I_{n_2})(A_1 \otimes A_2)(M \otimes I_{m_2})$

(9) $A \otimes (A_1 \oplus A_2) = (A \otimes A_1) \oplus (A \otimes A_2)$.

If we add $A^I = A$ then the set $\{I, T, D, TD, DT, E\}$ is a group that is isomorphic to the symetric group $S_3 = \{(\ ), (1,2), (2,3), (1,3,2), (1,2,3), (1,3)\}$.

Definition 4. For two k-sets of $n \times m$ matrices B and C we write $B \equiv C$, B is *equivalent* to C, if there exist nonsingular matrices N, M and K such that

$$B = N(C[K])M.$$

Obviously, this relation is an equivalence relation.

Lemma 2. *[7]. Let $A_1, \cdots, A_j, B_1, \cdots, B_j$ be sets of matrices. Then*

(1) *If $A_1 \equiv B_1$ then $A_1^D \equiv B_1^D$ and $A_1^T \equiv B_1^T$.*

(2) *$B_1 \oplus \cdots \oplus B_j \equiv B_{\phi(1)} \oplus \cdots \oplus B_{\phi(j)}$ and $B_1 \otimes \cdots \otimes B_j \equiv B_{\phi(1)} \otimes \cdots \otimes B_{\phi(j)}$ for any permutation ϕ on $\{1, \cdots, j\}$.*

(3) *If $A_i \equiv B_i$, $i = 1, \cdots, j$ then $A_1 \oplus \cdots \oplus A_j \equiv B_1 \oplus \cdots \oplus B_j$ and $A_1 \otimes \cdots \otimes A_j \equiv B_1 \otimes \cdots \otimes B_j$.*

Definition 5. We denote by $M_{n,m,p}$ the set of matrices defined by the product of $n \times m$ and $m \times p$ matrices. It is known that

$$M_{n,m,p} = I_n \otimes I_m^D \otimes I_p^E.$$

This follows

$$M_{n,m,p}^D \equiv M_{m,n,p}, M_{n,m,p}^E \equiv M_{p,m,n} \quad , \quad M_{n,m,p} \otimes M_{n',m',p'} \equiv M_{nn',mm',pp'}.$$

and by the results in [7] we can find the exact relation between the above systems.

Definition 6. Let $A = \{A_1, \cdots, A_k\}$ be a set of matrices. We define

$$rowrank(A) = rank[A_1|\cdots|A_k], \qquad colrank(A) = rank[A_1^T|\cdots|A_k^T],$$

and

$$dim(A) = dim\ L(A).$$

where $L(A)$ is the linear space spanned by the elements of A.

It can be easily prove

Lemma 3. *We have*

(1) *$rowrank(A) = dim(A^E)$, $colrank(A) = dim(A^D)$.*

(2) *For nonsingular matrices N, M and K we have*

$$rowrank(NAM[K]) = rowrank(A), \qquad colrank(NAM[K]) = colrank(A).$$

Following [8], [14] and [16] we have

Lemma 4. *We have*

(1) *$\mu(A) \leq \delta(A) < 2\mu(A)$.*

(2) $\delta(A) = \delta(A^T) = \delta(A^D), \quad \mu(A) = \mu(A^T)$.

(3) $\mu(NAM[K]) = \mu(A)$, *for every nonsingular matrices* N, M *and* K.

(4) $\mu(A \oplus B) \leq \mu(A) + \mu(B)$ *and* $\mu(I_t \otimes A) \leq \mu(\oplus_{i=1}^{t} A) \leq t\mu(A)$.

(5) $\mu(A \otimes B) \leq \mu(A)\mu(B)$.

(6) $\mu(A) \geq \frac{1}{2}\delta(diag(A, A^T))$.

(7) $DSC_{SLA} = DSC_{QA}, DSCS_{SLA} = DSCS_{QA}$.

(3),(4) and (5) are also true for the bilinear complexity δ.

Lemma 5. *[6]. Let* A *be a set of matrices. If for every nonsingular matrix* N *there exist* $A_1, \cdots, A_s \in A[N]$ *such that*

$$rank[A_1|\cdots|A_s] \geq t \qquad \text{or} \qquad rank[A_1^T|\cdots|A_s^T] \geq t$$

then

$$\mu(A) \geq dim\ A + t - s.$$

Definition 7. We denote by $NB^*(r)$ the collection of sets of matrices A such that there exist a linear subspace A_1 of $L(A)$ and integers s and t where:

(1) For every nonsingular matrix N and for every $B_1 \in (L(A)\backslash A_1) \cap A[N]$ there exist $s-1$ matrices $B_2, \cdots, B_s \in (L(A)\backslash A_1) \cap A[N]$ such that

$$rank[B_1|\cdots|B_s] \geq t \qquad \text{or} \qquad rank[B_1^T|\cdots|B_s^T] \geq t.$$

(2) $\mu(A) = dim(A) + t - s + r$.

In [6], we proved the following two lemmas

Lemma 6.

(1) *If* $A \in NB^*(0)$ *then* $A \in DSCS_{SLA}$.

(2) *If* $A \in NB^*(1)$ *then* $A \in DSC_{SLA}$.

(3) *If* $A \in NB^*(r), r > 1$ *then for every set of matrices* B *we have*

$$\mu(A \oplus B) \geq dim(A) + t - s + 1 + \mu(B).$$

Notice that all the results in lemma 5 and 6 are also true for bilinear algorithms.

Lemma 7. *We have:* $A \in DSCS_{BA}$ *if and only if* $A^D \in DSCS_{BA}$ *if and only if* $A^E \in DSCS_{BA}$.

Using the results in [16] we prove

Lemma 8. *Let* $A = \{A_1, \cdots, A_k\}$ *and* $B = \{B_1, \cdots, B_{k'}\}$ *be sets of matrices. If*

(1) $(diag(A, A^T), diag(B, B^T)) \in DSCS_{BA}$,

(2) $\delta(diag(A, A^T)) = 2\delta(A)$ *and* $\delta(diag(B, B^T)) = 2\delta(B)$.

Then $(A, B) \in DSCS_{SLA}$.

Proof . If $(A, B) \notin DSCS_{SLA}$ then by [8, lemmas 2,8] there exist a minimal quadratic algorithm $\sigma_1, \cdots, \sigma_t$ for $\{x^T A_1 y, \cdots, x^T A_k y, u^T B_1 v, \cdots, u^T B_{k'} v\}$ where $\sigma_{i_0} \in F[x, y, u, v]\backslash(F[x, y] \cup F[u, v])$.

Let

$$\sigma_i = (a_{i,1}(x) + a_{i,2}(y) + a_{i,3}(u) + a_{i,4}(v))(b_{i,1}(x) + b_{i,2}(y) + b_{i,3}(u) + b_{i,4}(v)).$$

It is known [16] that the algorithm $(\tilde{\sigma}_{i,j})_{i=1,\cdots,t,j=1,2}$ where

$$\tilde{\sigma}_{i,1} = (a_{i,1}(x) + a_{i,2}(x') + a_{i,3}(u) + a_{i,4}(u'))(b_{i,1}(y') + b_{i,2}(y) + b_{i,3}(v') + b_{i,4}(v)),$$

and

$$\tilde{\sigma}_{i,2} = (b_{i,1}(x) + b_{i,2}(x') + b_{i,3}(u) + b_{i,4}(u'))(a_{i,1}(y') + a_{i,2}(y) + a_{i,3}(v') + a_{i,4}(v)),$$

is a bilinear algorithm that computes $D = diag(A, A^T) \oplus diag(B, B^T)$. Because

$$\delta(diag(A, A^T) \oplus diag(B, B^T)) = \delta(diag(A, A^T)) + \delta(diag(B, B^T)) = 2\delta(A) + 2\delta(B).$$

we have $\{\tilde{\sigma}_{i,j}\}_{i=1,\cdots,t,j=1,2}$ is a minimal algorithm for D. By (1) and since

$$\tilde{\sigma}_{i_0,1} \in F[x, x', y, y', u, u', v, v']\backslash(F[x, x', y, y'] \cup F[u, u', v, v']),$$

we have a contradiction to [8, lemma 2]. This contradiction follows the result. ○

3. REGULAR REPRESENTATION OF ALGEBRAS

In this section we give the results in [7] that will be used in the next sections.

Let $\mathbf{A}$ be an associative algebra with unit element 1 and $\{a_1, \cdots, a_n\}$ be a base of the algebra $\mathbf{A}$. Let

$$a_i a_j = \sum_{k=1}^{n} \gamma_{i,j,k} a_k$$

with $\gamma_{i,j,k} \in F$, $i, j, k = 1, \cdots, n$. Then for $x = \sum_{i=1}^{n} x_i a_i$ and $y = \sum_{j=1}^{n} y_j a_j$ we have

$$xy = \left(\sum_{i=1}^{n} x_i a_i\right)\left(\sum_{j=1}^{n} y_j a_j\right) = \sum_{k=1}^{n}\left(\sum_{i=1}^{n}\sum_{j=1}^{n} \gamma_{i,j,k} x_i y_j\right) a_k.$$

Let $a_i y = \sum_{k=1}^{n} \sigma_{i,k} a_k$ and define $A_y = (\sigma_{i,k})$ an $n \times n$ square matrix. Then it can be easily shown that $\sigma_{i,k} = \sum_{j=1}^{n} \gamma_{i,j,k} y_j$ and $\mathbf{RR}_l(\mathbf{A}) = \{A_a | a \in \mathbf{A}\}$ form an algebra over F that is isomorphic to $\mathbf{A}$ under the corresponding $a \to A_a$, $\{A_{a_1}, \cdots, A_{a_n}\}$ is a base for the algebra $\mathbf{RR}_l(\mathbf{A})$, $A_\lambda = \lambda I_n$, $A_a A_b = A_{ab}$, $A_a + A_b = A_{a+b}$, $\lambda A_a = A_{\lambda a}$ for $\lambda \in F$ and if $ab = 1$ then $A_a^{-1} = A_b$. The algebra $\mathbf{RR}_l(\mathbf{A})$ is called the *left regular representation* of $\mathbf{A}$. The left regular representation $\mathbf{RR}_l(\mathbf{A})$ of $\mathbf{A}$ is depending on the chooses bases $B = \{a_1, \cdots, a_n\}$. when we want to emphasize this dependency we write $\mathbf{RR}_l(\mathbf{A}, B)$.

Let $x a_i = \sum_{j=1}^{n} \delta_{j,i} a_j$ and define $A^x = (\delta_{j,i})$ an $n \times n$ square matrix. Then $\mathbf{RR}_r(\mathbf{A}) = \{A^a | a \in \mathbf{A}\}$ form an algebra over F that is isomorphic to $\mathbf{A}$ under the corresponding $a \to A^a$. The algebra $\mathbf{RR}_r(\mathbf{A})$ is called the *right regular representation* of $\mathbf{A}$.

We define

$$\mathbf{B}(\mathbf{A}) = \{B_1, \cdots, B_n\}$$

where for $\mathbf{x} = (x_1, \cdots, x_n)^T$, $\mathbf{y} = (y_1, \cdots, y_n)^T$ we have

$$\mathbf{x}^T B_i \mathbf{y} = \sum_{i=1}^{n} \sum_{j=1}^{n} \gamma_{i,j,k} x_i y_j.$$

i.e. the $i-$th coefficient of the product xy.

Let $\mathbf{C}_l(\mathbf{A}) = \{A_{a_1}, \cdots, A_{a_n}\}$ and $\mathbf{C}_r(\mathbf{A}) = \{A^{a_1}, \cdots, A^{a_n}\}$. In [7] we gave the following connection between $\mathbf{B}(\mathbf{A})$, $\mathbf{C}_l(\mathbf{A})$ and $\mathbf{C}_r(\mathbf{A})$.

Lemma 9. *We have*

$$\mathbf{C}_l(\mathbf{A})^D = \mathbf{B}(\mathbf{A}), \mathbf{C}_r(\mathbf{A})^E = \mathbf{B}(\mathbf{A}), \mathbf{C}_r(\mathbf{A}) = \mathbf{C}_l(\mathbf{A})^{TD}.$$

Obviously, $\mathbf{C}_l(\mathbf{A})$, $\mathbf{C}_r(\mathbf{A})$ and $\mathbf{B}(\mathbf{A})$ depend on the chooses bases $B = \{a_1, \cdots, a_n\}$. When we want to emphasis this dependency we write $\mathbf{C}_l(\mathbf{A}, B)$, $\mathbf{C}_r(\mathbf{A}, B)$ and $\mathbf{B}(\mathbf{A}, B)$.

Lemma 10. *Let* $\mathbf{A}$ *and* $\mathbf{A}'$ *be algebras. If* $\mathbf{A}$ *is isomorphic to* $\mathbf{A}'$ *then there exist bases* $A = \{a_1, \cdots, a_n\}$ *and* $A' = \{a'_1, \cdots, a'_n\}$ *for* $\mathbf{A}$ *and* $\mathbf{A}'$*, respectively, such that*

$$\mathbf{C}_l(\mathbf{A}, A) = \mathbf{C}_l(\mathbf{A}', A'), \mathbf{B}(\mathbf{A}, A) = \mathbf{B}(\mathbf{A}', A').$$

Lemma 11. *Let* $A = \{a_1, \cdots, a_n\}$ *and* $B = \{b_1, \cdots, b_n\}$ *be bases for the algebra* $\mathbf{A}$*. If* $B = A[M]$ *then*

$$\mathbf{B}(\mathbf{A}, B) = M\mathbf{B}(\mathbf{A}, A)[(M^T)^{-1}]M^T \ , \ \mathbf{C}_l(\mathbf{A}, B) = M\mathbf{C}_l(\mathbf{A}, A)[M]M^{-1}.$$

and

$$\mathbf{C}_r(\mathbf{A}, B) = (M^T)^{-1}\mathbf{C}_r(\mathbf{A}, A)[M]M^T.$$

Lemma 12. *Let* $\mathbf{A}$ *and* $\mathbf{A}'$ *be algebras. If* $\mathbf{A}$ *is isomorphic to* $\mathbf{A}'$ *then there exist a nonsingular matrix* M *such that*

$$\mathbf{RR}_l(\mathbf{A}) = M\mathbf{RR}_l(\mathbf{A}')M^{-1}.$$

Also for $B = A[M]$ *where* A *and* B *are as in lemma 11 we have*

$$\mathbf{RR}_l(\mathbf{A}, B) = M\mathbf{RR}_l(\mathbf{A}, A)M^{-1}.$$

Lemma 13. *Let* $\mathbf{A}_1$ *and* $\mathbf{A}_2$ *be algebras. Then*

$$\mathbf{C}_l(\mathbf{A}_1 \times \mathbf{A}_2) \equiv \mathbf{C}_l(\mathbf{A}_1) \oplus \mathbf{C}_l(\mathbf{A}_2), \quad \mathbf{B}(\mathbf{A}_1 \times \mathbf{A}_2) \equiv \mathbf{B}(\mathbf{A}_1) \oplus \mathbf{B}(\mathbf{A}_2),$$

$$\mathbf{C}_l(\mathbf{A}_1 \otimes \mathbf{A}_2) \equiv \mathbf{C}_l(\mathbf{A}_1) \otimes \mathbf{C}_l(\mathbf{A}_2), \quad \mathbf{B}(\mathbf{A}_1 \otimes \mathbf{A}_2) \equiv \mathbf{B}(\mathbf{A}_1) \otimes \mathbf{B}(\mathbf{A}_2).$$

Let $\mathbf{A}$ be an algebra. The *reciprocal algebra* $\mathbf{A}^-$ of $\mathbf{A}$ is an algebra with elements of $\mathbf{A}$ and the multiplication $*$ such that $a * b = ba$. We have

Lemma 14. *Let* $\{a_1, \cdots, a_n\}$ *be a base for* $\mathbf{A}$. *Then*

$$\mathbf{B}(\mathbf{A}^-) = \mathbf{B}(\mathbf{A})^T, \mathbf{C}_l(\mathbf{A}^-) = \mathbf{C}_l(\mathbf{A})^E, \mathbf{C}_r(\mathbf{A}^-) = \mathbf{C}_r(\mathbf{A})^D \ , \ \mathbf{C}_r(\mathbf{A}^-) = \mathbf{C}_l(\mathbf{A})^T.$$

Observe that when $\mathbf{A}$ is commutative algebra then $\mathbf{A}^- = \mathbf{A}$ and therefore we have

Lemma 15. *We have* $\mathbf{C}_l(\mathbf{A}) = \mathbf{C}_l(\mathbf{A})^E$ *iff* $\mathbf{C}_r(\mathbf{A}) = \mathbf{C}_r(\mathbf{A})^T$ *iff* $\mathbf{B}(\mathbf{A}) = \mathbf{B}(\mathbf{A})^T$ *iff* $\mathbf{A}$ *is commutative algebra.*

Definition 8. Let $\mathbf{A}$ be an algebra. For $W \in \{D, T, DT, TD, E\}$ we say that $\mathbf{A}$ is *W-algebra* (*W^--algebra*) if

$$\mathbf{C}_l(\mathbf{A})^W \equiv \mathbf{C}_l(\mathbf{A}), \quad (\mathbf{C}_l(\mathbf{A})^W \equiv \mathbf{C}_l(\mathbf{A}^-)).$$

We say that $\mathbf{A}$ is *W-isomorphic algebra* (*W^--isomorphic algebra*) if there exist matrices N and M such that $NL(\mathbf{C}_l(\mathbf{A})^W)M$ is an algebra that is isomorphic $\mathbf{A}$ (to $\mathbf{A}^-$) [Recall that $L(H)$ is the linear space spanned by the elements of H]. Obviously

$$W - algebra \implies W - isomorphic \ \ algebra.$$

$$W^- - algebra \implies W^- - isomorphic \ \ algebra.$$

and the following lemma follows

Lemma 16. *Let* $W, W_1, W_2 \in \{D, T, TD, DT, E\}$. *Then*

(*i*) *If* $\mathbf{A}$ *is* W_1*-algebra and* W_2*-algebra then* $\mathbf{A}$ *is* W_1W_2*-algebra.*

(*ii*) $\mathbf{A}$ *is* W^-*-algebra iff* $\mathbf{A}$ *is* WE*-algebra iff* $\mathbf{A}$ *is* EW*-algebra.*

(*iii*) $\mathbf{A}$ *is* W^-*-isomorphic algebra iff* $\mathbf{A}$ *is* WT*-isomorphic algebra.*

Lemma 16 follows

Lemma 17. *For every algebra* $\mathbf{A}$ *one of the following can happen*

(*i*) $\mathbf{A}$ *is* W*-algebra for every* $W \in \{D, T, TD, E\}$.

(*ii*) $\mathbf{A}$ *is* W*-algebra for only one* $W \in \{D, T, TD, E\}$.

(*iii*) $\mathbf{A}$ *is not* W*-algebra for every* $W \in \{D, T, TD, E\}$.

Lemma 18. *Every algebra* $\mathbf{A}$ *is* TD*-isomorphic algebra.*

For E-algebras we proved

Lemma 19. $\mathbf{A}$ *is* E*-algebra iff* $\mathbf{A}$ *is* E*- isomorphic algebra iff* $\mathbf{A}$ *is* T*- isomorphic algebra iff* $\mathbf{A}$ *is isomorphic to* $\mathbf{A}^-$.

For T and D-algebras we proved

Lemma 20. *We have*

(*i*) $\mathbf{A}$ *is* D*-algebra iff* $\mathbf{A}^-$ *is* T*-algebra.*

(*ii*) *If* $\mathbf{A}$ *is* D*-algebra then* $\mathbf{A}$ *is isomorphic to* $\mathbf{A}^-$.

For TD and DT-algebras we proved

Lemma 21.

(i) $\mathbf{A}$ *is DT-algebra iff* $\mathbf{A}$ *is TD-algebra iff* $\mathbf{A}^-$ *is DT-algebra.*

(ii) $\mathbf{A}$ *is DT-algebra iff There exist a regular matrix* N *such that* $\mathbf{RR}_r(\mathbf{A}) = N\mathbf{RR}_l(\mathbf{A})N^{-1}$.

Lemma 22. *If* $\mathbf{A}_1$ *and* $\mathbf{A}_2$ *are W-algebra (W-isomorphic algebra) then are the algebras* $\mathbf{A}_1 \times \mathbf{A}_2$ *and* $\mathbf{A}_1 \otimes \mathbf{A}_2$.

Let $\mathbf{M}_n$ be the total matrix algebra of order n. For semisimple algebras we proved

Lemma 23. *Let* $\mathbf{A} = \times_{i=1}^{l} \mathbf{M}_{n_i} \otimes \mathbf{D}_i$ *be a semisimple algebra. Then*

(1) $\mathbf{A}$ *is DT-algebra and TD-algebra.*

(2) $\mathbf{A}$ *is E-algebra iff* $\mathbf{A}$ *is D-algebra iff* $\mathbf{A}$ *is T-algebra iff there exist a permutation* ϕ *on* $\{1, \cdots, l\}$ *such that*

$$n_i = n_{\phi(i)}, \qquad \mathbf{D}_i \cong \mathbf{D}_{\phi(i)}^-, i = 1, \cdots, l.$$

($\cong$ = isomorphic).

This lemma implies that every semisimple algebra over the complex field or the real field is W-algebra for all $W \in \{E, D, T, DT, TD\}$.

For local commutative algebras we proved

Lemma 24. *Let* $\mathbf{A}$ *be a local commutative algebra. Then*

(1) $\mathbf{A}$ *is E-algebra.*

(2) $\mathbf{A}$ *is DT-algebra iff* $\mathbf{A}$ *is TD-algebra iff* $\mathbf{A}$ *is D-algebra iff* $\mathbf{A}$ *is T-algebra iff there exist* $d \in \mathbf{A}$ *such that*

$$\{a | a \ rad \ \mathbf{A} = 0\} = d\mathbf{A}.$$

By Artinian theorem, every commutative algebra is a direct sum of local commutative algebra. For commutative algebra we proved

Lemma 25. *Let* $\mathbf{A} = \mathbf{A}_1 \oplus \cdots \oplus \mathbf{A}_l$ *be a commutative algebra where* $\mathbf{A}_i$ *are local commutative algebras. Then*

(1) $\mathbf{A}$ *is E-algebra.*

(2) $\mathbf{A}$ *is DT-algebra iff* $\mathbf{A}$ *is TD-algebra iff* $\mathbf{A}$ *is D-algebra iff* $\mathbf{A}$ *is T-algebra iff* $A_1, \cdots, A_l$ *are D-algebras.*

Using lemma 25 it can be easily prove

Lemma 26. *Every algebra* $\mathbf{A} = F[\alpha]/(p(\alpha))$, *where* $p(\alpha)$ *is a polynomial, is W-algebra for every* $W \in \{E, D, T, DT, TD\}$.

This lemma follows that every semisimple algebra over a finite field is W-algebras for all $W \in \{D, T, TD, DT, E\}$.

Let $C = \{C_1, \cdots, C_k\}$ be a set of $n \times m$ matrices, $\mathbf{A}$ be an algebra. The *quadratic complexity of* C *over the algebra* $\mathbf{A}$ is $\mu(C \otimes \mathbf{B}(\mathbf{A}))$, i.e the complexity of $\{x^T C_1 y, \cdots, x^T C_k y\}$ where $x = (x_1, \cdots, x_n)^T$, $y = (y_1, \cdots, y_m)^T$ and x_i, y_j are elements in the algebra $\mathbf{A}$. In the same manner we can define the bilinear complexity of C over the algebra $\mathbf{A}$ as $\delta(C \otimes \mathbf{B}(\mathbf{A}))$. By lemma 4, 7, 9 and 14 we have

Lemma 27.

(*1*) $\delta(C \otimes \mathbf{B}(\mathbf{A})) = \delta(C^D \otimes \mathbf{C}_l(\mathbf{A})) = \delta(C^E \otimes \mathbf{C}_r(\mathbf{A}))$.

(*2*) *If* $\mathbf{A}$ *is D-algebra then* $\delta(C \otimes \mathbf{B}(\mathbf{A})) = \delta(C^D \otimes \mathbf{B}(\mathbf{A}))$

(*3*) *If* $\mathbf{A}$ *is T-algebra then* $\delta(C \otimes \mathbf{B}(\mathbf{A})) = \delta(C^E \otimes \mathbf{B}(\mathbf{A}))$

(*4*) *If* $\mathbf{A}$ *is TD-algebra then* $\delta(C \otimes \mathbf{B}(\mathbf{A})) = \delta(C^{DT} \otimes \mathbf{B}(\mathbf{A}))$

(*5*) *If* $\mathbf{A}$ *is D-algebra then* $\mu(C \otimes \mathbf{B}(\mathbf{A})) = \mu(C \otimes \mathbf{C}_l(\mathbf{A})) = \mu(C^T \otimes \mathbf{C}_r(\mathbf{A}^-))$

(*6*) *If* $\mathbf{A}$ *is T-algebra then* $\mu(C \otimes \mathbf{B}(\mathbf{A})) = \mu(C \otimes \mathbf{C}_r(\mathbf{A})) = \mu(C^T \otimes \mathbf{C}_l(\mathbf{A}^-))$

(*7*) *If* $\mathbf{A}$ *is TD-algebra then* $\mu(C \otimes \mathbf{B}(\mathbf{A})) = \mu(C \otimes \mathbf{C}_l(\mathbf{A}^-)) = \mu(C^T \otimes \mathbf{C}_l(\mathbf{A}))$

before we leave this section we shall prove the the following lemma

Lemma 28. *Let* $\mathbf{A}$ *be a local algebra. There exist a base* $\{a_1, \cdots, a_k, a_{k+1}, \cdots, a_{rk}\}$ *for* $\mathbf{A}$ *where* $a_1, \cdots, a_k \notin rad\mathbf{A}$, $a_{k+1}, \cdots, a_{rk} \in rad\mathbf{A}$,

$$A_{a_i} = \begin{pmatrix} \tilde{A}_i & & * \\ & \ddots & \\ 0 & & \tilde{A}_i \end{pmatrix}, \qquad i = 1, \cdots, k, \tag{5}$$

$\mathbf{C}(\mathbf{A}/rad\mathbf{A}) = \{\tilde{A}_i\}_{i=1,\cdots,k}$ *and*

$$A_{a_i} = \begin{pmatrix} 0_{k\times k} & & * \\ & \ddots & \\ 0 & & 0_{k\times k} \end{pmatrix}, \qquad i = k+1, \cdots, rk. \tag{6}$$

Proof . Let $\mathbf{A} = L \oplus_F rad\mathbf{A}$ and $\{a_1, \cdots, a_k\}$ be a base for L. Since $\mathbf{A}$ is local, all the elements in L are invertible. Let i_0 be the least integer such that $(rad\mathbf{A})^{i_0} \neq 0$ and $(rad\mathbf{A})^{i_0+1} = 0$. We choose an element $b_1 \in (rad\mathbf{A})^{i_0}$. Then $b_1 L \subseteq (rad\mathbf{A})^{i_0}$ because L contains invertible elements. Let $b_2 \in (rad\mathbf{A})^{i_0} \backslash b_1 L$. Then $b_2 L \subseteq (rad\mathbf{A})^{i_0}$. If $b_2 L \cap b_1 L \neq 0$ then there exist $a_1, a_2 \notin rad\mathbf{A}$ such that $b_2 a_2 = b_1 a_1$, which implies $b_2 = b_1 a_1 a_2^{-1} \in b_1 \mathbf{A} = b_1(L \oplus_F rad\mathbf{A}) = b_1 L$. A contradiction. Therefore $b_1 L \oplus_F b_2 L \subseteq (rad\mathbf{A})^{i_0}$. By induction hypothesis we can prove that there exist $b_1, \cdots, b_{k_0} \in (rad\mathbf{A})^{i_0}$ such that

$$L_{i_0} = b_1 L \oplus_F \cdots \oplus_F b_{k_0} L = (rad\mathbf{A})^{i_0}$$

and $\{b_i a_j\}_{\substack{i=1,\cdots,k_0 \\ j=1,\cdots,k}}$ is a base for $(rad\mathbf{A})^{i_0}$.

We now handle $(rad\mathbf{A})^{i_0-1}$. Let $b_{k_0+1} \in (rad\mathbf{A})^{i_0-1} \backslash (rad\mathbf{A})^{i_0}$. Then $b_{k_0+1} L \subseteq (rad\mathbf{A})^{i_0-1} \backslash (rad\mathbf{A})^{i_0}$ and therefore $b_{k_0+1} L \cap L_{i_0} = 0$. Assume $b_{k_0+2} \in ((rad\mathbf{A})^{i_0-1} \backslash (rad\mathbf{A})^{i_0}) \backslash b_{k_0+1} L$. If $b_{k_0+2} L \cap (b_{k_0+1} L \oplus_F L_{i_0}) \neq 0$ then there exist $a_1, a_2 \in L$ and $c \in L_{i_0}$ such that $b_{k_0+2} a_2 = b_{k_0+1} a_1 + c$. Then $b_{k_0+2} = b_{k_0+1} a_1 a_2^{-1} + c a_2$. Since $a_1 a_2^{-1}$ is invertible we have $a_1 a_2^{-1} = a + w$ where $a \in L$ and $w \in rad\mathbf{A}$ and then $b_{k_0+2} = b_{k_0+1} a + b_{k_0+1} w + c a_2$. Now $b_{k_0+1} w + c a_2 \in (rad\mathbf{A})^{i_0}$, $a \in L$ and therefore $b_{k_0+2} \in b_{k_0+1} L + L_{i_0}$. A contradiction. In this way we can find $b_{k_0+1}, \cdots, b_{k_1}$ such that

$$b_1 L \oplus_F \cdots \oplus_F b_{k_1} L = (rad\mathbf{A})^{i_0-1}.$$

Therefore we have (By induction hypothethis)

$$\mathbf{A} = L \oplus_F b_1 L \oplus_F \cdots \oplus_F b_r L$$

such that if $b_{i_1} \in (rad\mathbf{A})^{j_1} \backslash (rad\mathbf{A})^{j_1-1}$, $b_{i_2} \in (rad\mathbf{A})^{j_2} \backslash (rad\mathbf{A})^{j_2-1}$ and $i_2 > i_1$ then $j_2 \leq j_1$.

We want now to find the regular representation $\mathbf{C}_l(\mathbf{A}, B)$ where $B = \{a_1, \cdots, a_k\} \cup \{b_{r-i+1} a_j\}_{\substack{i=1,\cdots,r \\ j=1,\cdots,k}}$.

Let $\phi : \mathbf{A} \rightarrow \mathbf{A}/rad\mathbf{A}$ be a canonical projection. Then $c_i = \phi(a_i)$, $i = 1, \cdots, k$ is a base of $\mathbf{A}/rad\mathbf{A}$. If

$$c_i c_j = \sum_{l=1}^{k} \gamma_{i,j,l} c_l \tag{7}$$

then since $\phi(a_i a_j) = c_i c_j = \sum_{l=1}^{k} \gamma_{i,j,l} c_l = \phi\left(\sum_{l=1}^{k} \gamma_{i,j,l} a_l\right)$, we have

$$a_i a_j = \sum_{l=1}^{k} \gamma_{i,j,l} a_l + w, \qquad w \in rad\mathbf{A}.$$

Assume that

$$w \in (rad\mathbf{A})^{n_w} \backslash (rad\mathbf{A})^{n_w+1}.$$

and

$$b_i \in (rad\mathbf{A})^{n_{b_i}} \backslash (rad\mathbf{A})^{n_{b_i}+1}.$$

Now since $(b_0 = 1)$

$$(b_t a_i) a_j = \sum_{l=1}^{k} \gamma_{i,j,l} b_t a_l + b_t w$$

and $b_t w \in (rad\mathbf{A})^{n'} \backslash (rad\mathbf{A})^{n'+1}$, $n' > n_{b_t}$ and by (7) we have (5) where $\tilde{A}_i = A_{c_i}$ in $\mathbf{C}(\mathbf{A}/rad\mathbf{A}, \{c_1, \cdots, c_k\})$.

Since for $r, s > 0$, $e = \min(r, s)$ we have $(b_r a_i)(b_s a_j) \in b_{e-1} L \oplus_F \cdots \oplus_F b_1 L$ then (6) follows. ○

4. CLASSIFICATION

In this section we show how a classification of all minimal quadratic [bilinear] algorithms for some bilinear systems can give a classification of minimal quadratic [bilinear] algorithms for other bilinear systems. This section is independent on the next sections. The reader who are interesting only in the proofs of the results in the abstract can leave this section.

Let $P = \{P_1, \cdots, P_k\}$ be a set of $n \times m$ matrices. It is well known that every quadratic and bilinear algorithm for $x^T P y = \{x^T P_1 y, \cdots x^T P_k y\}$ can be written as

$$E((Ax + By) \circ (Cx + Dy)) \qquad , \qquad G(Hx \circ Jy),$$

respectively, where A, B, C, D, E, H, G and J are $\mu(P) \times n$, $\mu(P) \times m$, $\mu(P) \times n$, $\mu(P) \times m$, $k \times \mu(P)$, $k \times \delta(P)$, $\delta(P) \times n$ and $\delta(P) \times m$ matrices, respectively, with entries from the field F, and $\circ$ is a componentwise product.

We shall simply write (E, A, B, C, D) and (G, H, J) for quadratic and bilinear algorithms, respectively. We also define $Alg_M(P)$ the set of all minimal M algorithms for P, $M \in \{QA, BA\}$.

By the results in [9], [14] and [18] we have

Lemma 29. *Let P be a set of matrices and let N, M and K be nonsingular matrices. Then*

(1) $(E, A, B, C, D) \in Alg_{QA}(P)$ *iff* $(KE, AN, BM, CN, DM) \in Alg_{QA}(NP[K]M)$.

(2) $(G, H, J) \in Alg_{BA}(P)$ *iff* $(KG, HN, JM) \in Alg_{BA}(P)$.

(3) $(E, A, B, C, D) \in Alg_{QA}(P)$ *iff* $(E, B, A, D, C) \in Alg_{QA}(P^T)$.

(4) $(G, H, J) \in Alg_{BA}(P)$ *iff* $(H, G, J) \in Alg_{BA}(P^D)$ *iff* $(G, J, H) \in Alg_{BA}(P)$.

For sets of matrices Q_1 and Q_2, we denote by $Alg_M(Q_1) \oplus Alg_M(Q_2)$ the set of all M algorithms $\sigma_1, \cdots, \sigma_t$ such that there exist sets $I, J \subset \{1, \cdots, t\}$, $I \cup J = \{1, \cdots, t\}$ and $I \cap J = \emptyset$, where $(\sigma_i)_{i \in I} \in Alg_M(Q_1)$ and $(\sigma_i)_{i \in J} \in Alg_M(Q_2)$. Obviously, $(Q_1, Q_2) \in DSCS_M$ if and only if $Alg_M(Q_1 \oplus Q_2) = Alg_M(Q_1) \oplus Alg_M(Q_2)$.

Now we prove

Lemma 30. *The complexity and the strong direct sum conjecture of a set of bilinear form C over the algebra $\mathbf{A}$ do not depend on the chooses bases. A classification of all minimal quadratic [bilinear] algorithms for C over $\mathbf{A}$ for one representation gives a classification of all minimal quadratic [bilinear] algorithms for any representation.*

Proof . In other words we have to prove that

$$\mu(C \otimes B(\mathbf{A}, E_1)) = \mu(C \otimes B(\mathbf{A}, E_2)),$$

where E_1, E_2 are any sets of bases of $\mathbf{A}$. Also we should find nonsingular matrices N, M and K such that

$$C \otimes B(\mathbf{A}, E_1) = N(C \otimes B(\mathbf{A}, E_2))M[K].$$

Now both results are easily follows from lemma 11, 27 and 29. ○

This lemma follows

Lemma 31. *Let $\mathbf{A} = \mathbf{A}_1 \times \cdots \times \mathbf{A}_n$ be an algebra. Then*

$$\mu(C \otimes B(\mathbf{A})) = \mu\left(\oplus_{i=1}^{n}(C \times B(\mathbf{A}_i))\right).$$

In particular we have

$$\mu(C \otimes F[\alpha]/(p(\alpha))) = \mu(\oplus_{i=1}^{k}(C \otimes F[\alpha]/(p_i^{d_i}(\alpha))),$$

where $p(\alpha) = \prod_{i=1}^{k} p_i^{d_i}(\alpha)$, and p_i are distinct irreducible polynomials.

Now for the bilinear complexity we have

Lemma 32. *If $\mathbf{A}$ is W-algebra for $W \in \{D, T, TD\}$ then the classification of all bilinear algorithms for $[x^T H y]_{\mathbf{A}}$ where $x = (x_1, \cdots, x_n)$ and $y = (y_1, \cdots, y_m)$ and H is a $n \times m$ matrix of rank r, gives a classification of all bilinear algorithms for $[xy_1, \cdots, xy_n]_{\mathbf{A}}$ and conversly.*

Proof . Let (A_1, B_1, C_1) be a bilinear algorithm for $[x^T H y]_{\mathbf{A}} = H \otimes \mathbf{B}(\mathbf{A})$. It is well known that there exist $r \times m$ and $n \times r$ matrices N and M with rank r such that $NHM = I_r$. Therefore

$$(N \otimes I_k)(H \otimes \mathbf{B}(\mathbf{A}))(M \otimes I_k) \equiv I_r \otimes \mathbf{B}(\mathbf{A})$$

and therefore $(A_2, B_2, C_2) = (A_1, B_1(N \otimes I_k), C_1(M \otimes I_k))$ is minimal bilinear algorithm for $I_r \otimes \mathbf{B}(\mathbf{A})$.

If $\mathbf{A}$ is D-algebra then by definition 8, there exist nonsingular matrices U, V and W such that

$$\mathbf{B}(\mathbf{A})^D = U\mathbf{B}(\mathbf{A})V[W].$$

By lemma 1 and 29 (A_2, B_2, C_2) is a minimal bilinear algorithm for $I_r \otimes \mathbf{B}(\mathbf{A})$ if and only if (B_2, A_2, C_2) is a minimal bilinear algorithm for

$$(I_r \otimes \mathbf{B}(\mathbf{A}))^D = I_r^D \otimes \mathbf{B}(\mathbf{A})^D = (I_r \otimes U)(I_r^D \otimes \mathbf{B}(\mathbf{A}))(I_r \otimes V)[I_r \otimes W]$$

if and only if $((I_r \otimes W)B_2, A_2(I_r \otimes U), C_2(I_r \otimes V))$ is a minimal bilinear algorithm for $I_r^D \otimes \mathbf{B}(\mathbf{A}) = [x_1 y, \cdots, x_r y]_{\mathbf{A}}$. ○

5. COMPLEXITY OF $X_1 Y, \cdots, X_N Y$ IN ALGEBRAS

In this section we investigate the complexity of computing $x_1 y, ..., x_n y$ in algebras which are direct sum of local algebras. This problem is equivalent to the complexity of $\{e_{n,1}, \cdots, e_{n,n}\}$ over the algebra $\mathbf{A}$. I.e

$$\mu(x_1 y, \cdots, x_n y) = \mu(I_n^D \otimes \mathbf{B}(\mathbf{A})).$$

Since $(I_n^D \otimes \mathbf{B}(\mathbf{A}))^D = I_n \otimes \mathbf{C}_l(\mathbf{A}) = \left\{ I_n \otimes A_{a_i} \middle| \{a_i\}_{i=1,\cdots,k} \text{ is a base for } A \right\}$ we have

$$I_n^D \otimes \mathbf{B}(\mathbf{A}) = \left\{ [(I_n \otimes A_{a_1})e_{nk,i} | \cdots | (I_n \otimes A_{a_n})e_{nk,i}] \middle| i = 1, \cdots, nk \right\}$$

where $k = dim\ \mathbf{A}$.

For $v \in F^{nk}$ we denote by

$$B(v) = \left[(I_n \otimes A_{a_1})v \middle| \cdots \middle| (I_n \otimes A_{a_k})v \right].$$

Observe that

$$\lambda_1 B(v_1) + \lambda_2 B(v_2) = B(\lambda_1 v_1 + \lambda_2 v_2). \tag{8}$$

We first investigate the case where $\mathbf{A}$ is division algebra.

Lemma 33. *Let $\mathbf{A}$ be a division algebra of dimension k, $v_1, \cdots, v_l \in F^{nk}$ and let*

$$s = dim\ L\left\{ (I_n \otimes A_{a_i})v_j \middle| i = 1, \cdots, k, j = 1, \cdots, l \right\}$$

Then for every nonsingular matrix N and every $B(u_1) \in \{B(v_1), \cdots, B(v_l)\}[N]$ there exist $\frac{s}{k} - 1$ matrices $B(u_2), \cdots, B(u_{s/k})$ in $\{B(v_1), \cdots, B(v_l)\}[N]$ such that

$$rowrank(\{B(u_1), \cdots, B(u_{s/k})\}) = s.$$

Proof . By (8) we have for every nonsingular matrix N

$$\{B(v_1), \cdots, B(v_l)\}[N] = \{B(w_1), \cdots, B(w_l)\}$$

for $\{w_1, \cdots, w_l\} = \{v_1, \cdots, v_l\}[N] \subset F^{nk}$. Since $L(w_1, \cdots, w_l) = L(v_1, \cdots, v_l)$ we have

$$dim\ L\{(I_n \otimes A_{a_i})w_j | i = 1, \cdots, k, j = 1, \cdots, l\} = s. \tag{9}$$

If $l = s/k$ then by lemma 3 we have

$$rowrank(\{B(w_1), \cdots, B(w_l)\}) = rank[B(w_1)| \cdots |B(w_l)]$$

$$= dimL\{(I_n \otimes A_{a_i})w_j | i = 1, \cdots, k, j = 1, \cdots, l\} = s,$$

and then the proof is completed.

If $l > s/k$ then the set $\{(I_n \otimes A_{a_i})w_j | i = 1, \cdots, k\ , j = 1, \cdots, l\}$ contains $lk > s$ vectors and therefore there exist one vector that is depending on the other. Assume (w.l.o.g) that

$$\sum_{i=1}^{k} \lambda_i (I_n \otimes A_{a_i})w_1 = \sum_{i=1}^{k} \sum_{j=2}^{l} \delta_{i,j} (I_n \otimes A_{a_i})w_j \tag{10}$$

where not all λ_i are zero. Then for $a = \sum_{i=1}^{k} \lambda_i a_i$, we obtain

$$(I_n \otimes A_a)w_1 = \sum_{i=1}^{k} \sum_{j=2}^{l} \delta_{i,j} (I_n \otimes A_{a_i})w_j.$$

Since A is division algebra we have A_a nonsingular and then

$$w_1 = \sum_{i=1}^{k} \sum_{j=2}^{l} \delta_{i,j} (I_n \otimes A_{a^{-1}a_i})w_j = \sum_{i=1}^{k} \sum_{j=2}^{l} \delta'_{i,j} (I_n \otimes A_{a_i})w_j$$

then for every $d = 1, \cdots, k$ we have

$$(I_n \otimes A_{a_d})w_1 = \sum_{i=1}^{k} \sum_{j=2}^{l} \delta^d_{i,j} (I_n \otimes A_{a_i})w_j$$

which implies that

$$dim\ L\{(I_n \otimes A_{a_i})w_j | i = 1, \cdots, k, j = 2, \cdots, l\} = s.$$

By induction hypothesis it can be proved that there exist $j_1, \cdots, j_{s/k}$ such that

$$dim\ L\{(I_n \otimes A_i)w_{j_q} | i = 1, \cdots, k, q = 1, \cdots, s/k\} = s.$$

Then as before

$$rowrank(\{B(w_{j_1}),\cdots,B(w_{j_{s/k}})\}) = s.$$

It is obvious from (10) that we can always assume that $j' \in \{j_1,\cdots,j_{s/k}\}$ for any $j' \in \{1,\cdots,l\}$. ○

For $v_1,\cdots,v_l \in F^{nk}$ we denote by

$$L_{\mathbf{A}}(v_1,\cdots,v_l) = L\big(\{(I_n \otimes A_{a_i})v_j \big| i = 1,\cdots,k\ ,\ j = 1,\cdots,l\}\big).$$

The following theorem gives a lower bound for computing a subset $B \subseteq L(I_n^D \otimes \mathbf{B}(\mathbf{A}))$

Theorem 1. *Let* $\mathbf{A}$ *be a division algebra,* $V = \{v_1,\cdots,v_l\} \subseteq F^{n\ dim\mathbf{A}}$ *and* $B = \{B(v_1),\cdots,B(v_l)\}$. *Then*

$$\mu(B) \geq \mu_0 = dim\ L(V) + \left(1 - \frac{1}{dim\mathbf{A}}\right) dim\ L_{\mathbf{A}}(V).$$

(1) If $\mu(B) = \mu_0$ *then* $B \in DSCS_{SLA}$.

(2) If $\mu(B) = \mu_0 + 1$ *then* $B \in DSC_{SLA}$.

(3) If $\mu(B) > \mu_0 + 1$ *then for every set of matrices* C *we have*

$$\mu(B \oplus C) \geq \mu_0 + 1 + \mu(C).$$

Proof . We shall prove that $B \in NB^*$. Let $A_1 = \emptyset$. By lemma 33, for every nonsingular matrix N and every $B(w_1) \in B[N]$ there exist $r - 1 = (dim\ L_A(v_1,\cdots,v_l)/dim\mathbf{A}) - 1$ matrices $B(w_2),\cdots,B(w_r) \in B[N]$ such that

$$rowrank(\{B(w_1),\cdots,B(w_r)\}) \geq dim\ L_{\mathbf{A}}(v_1,\cdots,v_l).$$

Then by lemma 5

$$\mu(B) \geq dim(B) + \left(1 - \frac{1}{dim\mathbf{A}}\right) dim\ L_{\mathbf{A}}(V) = dim\ L(V) + \left(1 - \frac{1}{dim\mathbf{A}}\right) dim\ L_{\mathbf{A}}(V)$$

By lemma 6 the result follows. ○

Theorem 2. *Let* $\mathbf{A}$ *be a direct sum of division algebras* $\mathbf{D}_1 \times \cdots \times \mathbf{D}_w$. *Then*

$$\mu((I_n^D \otimes \mathbf{B}(\mathbf{A})) \oplus C) \geq \sum_{i=1}^{w} (2dim\ \mathbf{D}_i - 1)n + \mu(C)$$

If the bound is tight then $I_n^D \otimes \mathbf{B}(\mathbf{A}) \in DSCS_{SLA}$.

Proof . By theorem 1 we have for $B = I_n^D \otimes \mathbf{B}(\mathbf{A}_i)$, $dim\ B = n\ dim\mathbf{D}_i$ and $dim L_{\mathbf{D}_i}(V) = n\ dim\mathbf{D}_i$ and therefore

$$\mu((I_n^D \otimes \mathbf{B}(\mathbf{D}_i)) \oplus C) \geq (2dim(\mathbf{D}_i) - 1)n + \mu(C).$$

Since by lemma 1 and 13 we have $I_n^D \otimes \mathbf{B}(\mathbf{A}) = \oplus_{i=1}^{w}(I_n^D \otimes \mathbf{B}(\mathbf{D}_i))$ the result follows. ○

For a matrix S we denote by $L_{col}(S)$ and $L_{row}(S)$ the linear space spanned by the columns and the rows of S, respectively. We have

Lemma 34. *Let* $\mathbf{A}$ *be a division algebra of dimension* k. *Then for every nonsingular matrix* N *and for every* $C_1 \in (I_n^D \otimes \mathbf{C}_l(\mathbf{A}))[N]$ *there exist* $n-1$ *matrices* $C_2, \cdots, C_n \in (I_n^D \otimes \mathbf{C}_l(\mathbf{A}))[N]$ *such that*

$$L_{col}[C_1|\cdots|C_n] = F^{nk}.$$

Proof . Since $\mathbf{A}$ is a division algebra, by lemma 23, $\mathbf{A}$ is DT-algebra and therefore

$$I_n^D \otimes \mathbf{C}_l(\mathbf{A}) \equiv I_n^D \otimes \mathbf{C}_l(\mathbf{A})^{DT} = I_n^D \otimes \mathbf{B}(\mathbf{A}^-).$$

Therefore by lemma 33 the result follows. ○

Lemma 35. *Let* $\mathbf{A}$ *be a local algebra and* $A = I_n^D \otimes \mathbf{C}_l(\mathbf{A})$. *There exist a linear space* $A_1 \subseteq L(A)$ *such that for every nonsingular matrix* N *and every* $C_1 \in A[N] \cap (L(A) \backslash A_1)$ *there exist* $C_2, \cdots, C_n \in A[N] \cap (L(A) \backslash A_1)$ *where*

$$rowrank\{C_1, \cdots, C_n\} \geq n \ dim \ \mathbf{A}.$$

Proof . We shall use the base in lemma 28. Let $\mathbf{C}_l(\mathbf{A}) = \{A_{a_1}, \cdots, A_{a_k}, A_{a_{k+1}}, \cdots, A_{a_{rk}}\}$, $A_1 = I_n^D \otimes L\{A_{a_{k+1}}, \cdots, A_{a_{rk}}\}$ and $A_2 = (L(A) \backslash A_1)$. Let N be any nonsingular matrix. Observing the first k columns of the matrices in $(I_n^D \otimes \mathbf{C}_l(\mathbf{A}))[N]$ we conclude by lemma 34 that for every $C_1 \in (I_n^D \otimes \mathbf{C}_l(\mathbf{A}))[N] \cap A_2$ there exist $C_2, \cdots, C_n \in (I_n^D \otimes \mathbf{C}_l(\mathbf{A}))[N] \cap A_2$ such that $L_{col}(\text{first } k \text{ columns in } C_1, \cdots, C_n) = nk$. Actually, it can be easy verify that

$$L_{col}(\text{first } k \text{ columns in } C_1, \cdots, C_n) =$$

$$\left\{(v_1, 0_{dim\mathbf{A}-k}, v_2, 0_{dim\mathbf{A}-k}, \cdots, v_n, 0_{dim\mathbf{A}-k})^T | (v_1, v_2, \cdots, v_n) \in F^{nk}\right\}.$$

Since $[C_1|\cdots|C_n]$ is of the form

$$\begin{pmatrix}
C_{1,1} & & * & C_{1,2} & & * & & C_{1,n} & & * \\
& C_{1,1} & & & C_{1,2} & & \cdots & & C_{1,n} & \\
& & \ddots & & & \ddots & \cdots & & & \ddots \\
0 & & C_{1,1} & 0 & & C_{1,2} & & 0 & & C_{1,n} \\
C_{2,1} & & * & C_{2,2} & & * & & C_{2,n} & & * \\
& C_{2,1} & & & C_{2,2} & & \cdots & & C_{2,n} & \\
& & \ddots & & & \ddots & \cdots & & & \ddots \\
0 & & C_{2,1} & 0 & & C_{2,2} & & 0 & & C_{2,n} \\
& \vdots & & & \vdots & & \vdots & & \vdots & \\
& \vdots & & & \vdots & & \vdots & & \vdots & \\
& \vdots & & & \vdots & & \vdots & & \vdots & \\
C_{n,1} & & * & C_{n,2} & & * & & C_{n,n} & & * \\
& C_{n,1} & & & C_{n,2} & & \cdots & & C_{n,n} & \\
& & \ddots & & & \ddots & \cdots & & & \ddots \\
0 & & C_{n,1} & 0 & & C_{n,2} & & 0 & & C_{n,n}
\end{pmatrix}$$

We have

$$L_{col}(i\text{-th } k \text{ columns of } C_1, \cdots, C_n) =$$

$$\left\{(*_{(i-1)k}, v_1, 0_{i(dim\mathbf{A}-k)}, *_{(i-1)k}, v_2, 0_{i(dim\mathbf{A}-k)}, \cdots, *_{(i-1)k}, v_n, 0_{i(dim\mathbf{A}-k)})^T \middle| (v_1, v_2, \cdots, v_n) \in F^{nk}\right\},$$

where $*_{(i-1)k}$ is $(i-1)k$ entries with some possible nonzero elements from the field. Then obviously,

$$\begin{aligned} L_{col}(C_1, \cdots, C_n) = & L_{col}(\text{first } k \text{ columns of } C_1, \cdots, C_n) \oplus_F \\ & L_{col}(\text{second } k \text{ columns of } C_1, \cdots, C_n) \oplus_F \\ & \vdots \\ & L_{col}(\text{last } k \text{ columns of } C_1, \cdots, C_n) = F^{n\ dim\mathbf{A}} \end{aligned}$$

This follows the result. ○

Lemma 35 follows

Theorem 3. *Let $\mathbf{A} = \mathbf{A}_1 \times \cdots \times \mathbf{A}_k$ be an algebra where $\mathbf{A}_i$ is local algebra. If $\mathbf{A}$ is W-algebra for some $W \in \{D, T, TD, DT\}$ then for every set of matrices C we have*

$$\mu([x_1y, \cdots, x_ny]_{\mathbf{A}} \oplus C) \geq (2dim\mathbf{A} - k)n + \mu(C). \tag{11}$$

If $\mathbf{A}$ is an algebra of n-minimal complexity then equation hold in (11) and

$$[x_1y, \cdots, x_ny]_{\mathbf{A}} \in DSCS_{SLA}. \tag{12}$$

Proof . If A is D, T, TD or DT-algebra then $I_n^D \otimes B(A) \equiv I_n^D \otimes \mathbf{C}_l(\mathbf{A}), I_n^D \otimes \mathbf{C}_l(\mathbf{A}^-)^T, I_n^D \otimes \mathbf{C}_l(\mathbf{A}^-), I_n^D \otimes \mathbf{C}_l(\mathbf{A}^-)$, respectively. Then by lemma 35 the result follows. ○

Theorem 4. *Let $\mathbf{A} = \mathbf{A}_1 \times \cdots \times \mathbf{A}_k$ be an algebra where $\mathbf{A}_i$ is local algebra. Then for every set of matrices C we have*

$$\delta([x_1y, \cdots, x_ny]_{\mathbf{A}} \oplus C) \geq (2dim\mathbf{A} - k)n + \delta(C). \tag{13}$$

If $\mathbf{A}$ is an algebra of n-minimal rank then equation hold in (13) and

$$[x_1y, \cdots, x_ny]_{\mathbf{A}} \in DSCS_{BA}.$$

Proof . By Theorem 11 we have

$$\delta((I_n^D \otimes \mathbf{C}_l(\mathbf{A})) \oplus C^E) \geq (2dim\mathbf{A} - k) + \delta(C^E).$$

Then by lemma 27 and since $I_n^{DE} = I_n^D$ we have

$$\delta((I_n^D \otimes \mathbf{B}_l(\mathbf{A})) \oplus C) \geq (2dim\mathbf{A} - k) + \delta(C).$$

If $\mathbf{A}$ is of minimal rank then $I_n^D \otimes \mathbf{C}_l(\mathbf{A}) \in DSCS_{BA}$ and therefore by lemma 7, $I_n^D \otimes \mathbf{B}_l(\mathbf{A}) \in DSCS_{BA}$. ○

6. COMPLEXITY OF ONE BILINEAR FORM OVER ALGEBRAS

In this section we shall study the complexity of one bilinear form over algebras.

Let H be a $n \times m$ matrix and $\mathbf{A}$ be an algebra. Then

Lemma 36. *$\mu(H \otimes \mathbf{B}(\mathbf{A})) = \mu(I_r \otimes \mathbf{B}(\mathbf{A}))$ where $r = rank(H)$.*

Proof . Let N and M be a nonsingular matrices such that $NHM = diag(I_r, 0)$. Then

$$(N \otimes I_k)(H \otimes \mathbf{B}(\mathbf{A}))(M \otimes I_k) = diag(I_r, 0) \otimes \mathbf{B}(\mathbf{A})$$

which implies the result. ○

In this section we prove

Theorem 5. *Let $\mathbf{A} = \mathbf{A}_1 \times \cdots \times \mathbf{A}_k$ be an algebra where $\mathbf{A}_i$ is local. Let H be a $n \times m$ matrix. Then for every set of matrices C we have*

$$\delta([x^T H y]_{\mathbf{A}} \oplus C) \geq (2dim\mathbf{A} - k)rank(H) + \delta(C).$$

If $\mathbf{A}$ is an algebra of $rank(H)$-minimal rank then

$$[x^T H y]_{\mathbf{A}} \in DSCS_{BA}.$$

Proof . Let $r = rank(H)$. In lemma 35 we prove this theorem for $I_r^D \otimes \mathbf{C}_l(\mathbf{A})$. Then by lemma 7, 9, 27 and 36 it is also true for

$$(I_r^D \otimes \mathbf{C}_l(\mathbf{A}))^D = I_r \otimes \mathbf{B}(\mathbf{A}) = [x_1 y_1 + \cdots + x_n y_n]_{\mathbf{A}} \equiv [x^T H y]_{\mathbf{A}}. \quad ○$$

Theorem 6. *Let $\mathbf{A}$ be a commutative algebra. Let H be $n \times m$ matrix. Then*

$$\mu([x^T H y]_{\mathbf{A}}) \geq (2dim\mathbf{A} - I_{\mathbf{A}})rank(H).$$

If $\mathbf{A}_1$ and $\mathbf{A}_2$ are commutative algebras of minimal rank then

$$([x^T H_1 y]_{\mathbf{A}_1}, [x^T H_2 y]_{\mathbf{A}_2}) \in DSCS_{SLA}.$$

Proof . Let $r = rank(H)$. By lemma 4 and 36 we have

$$\mu([x^T H y]_{\mathbf{A}}) = \mu(I_r \otimes \mathbf{B}(\mathbf{A})) \geq \frac{1}{2}\delta(diag((I_r \otimes \mathbf{B}(\mathbf{A})), (I_r \otimes \mathbf{B}(\mathbf{A}))^T)).$$

Since $\mathbf{A}$ is commutative we have by lemma 15, $\mathbf{B}(\mathbf{A})^T = \mathbf{B}(\mathbf{A})$, and by theorem 5

$$\mu([x^T H y]_{\mathbf{A}}) \geq \frac{1}{2}\delta(I_{2r} \otimes \mathbf{B}(\mathbf{A})) = (2dim\mathbf{A} - k)rank(H).$$

Now by lemma 8, $([x^T H_1 y]_{\mathbf{A}_1}, [x^T H_2 y]_{\mathbf{A}_2}) \in DSCS_{SLA}$. ○

REFERENCES

[1] A. A. Albert, Structure of algebras, American Mathematical Society Colloquium Publications, Vol XXIV, (1939).

[2] A. Averbuch, Z. Galil, S. Winograd, Classification of all the minimal bilinear algorithm for computing the coefficient of the product of two polynomials modulo a polynomial in the algebra $G[u]/ < u^n >$.

[3] A. Averbuch, Z. Galil, S. Winograd, Classification of all the minimal bilinear algorithm for computing the coefficient of the product of two polynomials modulo a polynomial in the algebra $G[u]/ < Q(u)^l > \quad l > 1$, *Theoretical Computer Science* **58** (1988), 17-56.

[4] A. Alder, V. Strassen, On the algorithmic complexity of associative algebras, *Theoret. Compute. Sci.* **15** (1981):201-211.

[5] L. Auslander, S. Winograd The multiplicative complexity of certain semilinear systems defined by polynomials, *Adv. in App. Math.* **1** (1980), 157-299.

[6] N. H. Bshouty, On the exteded direct sum conjecture, Proceedings 21st Annual ACM Symposium on Theory of Computing, (May 1989).

[7] N. H. Bshouty, On the regular representation of algebras, TR 89/365/27, University of Calgary.

[8] N. H. Bshouty, On the direct sum conjecture in the straight line model.

[9] C.M. Feduccia, Y. Zalcstein, Algebras having linear multiplicative complexity, *J. ACM,* **24** (1977), 311-331.

[10] H. F. Groote, Characterization of division algebras of minimal rank and the structure of their algorithm varieties, *SIAM J. Comput.* **12** (1983), 101-117.

[11] H. G. Groote, Lectures on the complexity of bilinear problems. *LN Comput. Sci.* **245** , Springer, Berline 1987.

[12] H. F. Groote, J. Heintz, Commutative algebra of minimal rank, *Linear Algebra and its Applications,* **55** (1983), 37-68.

[13] W. Hartmann, On the multiplicative complexity of modules over associative algebras, *SIAM J. Appl. Math.* **14** (1985), 383-395.

[14] J. Hopcroft, J. Munsinski, Duality applied to the complexity of matrix multiplication, *SIAM J. Comput.* **2** (1973), 159-173.

[15] J. Heintz, J. Morgenstern, On associative algebras of minimal rank, *Proc. of the AAECC-2 Conference*(Grenoble 1988).

[16] J. Ja'Ja' On the complexity of bilinear forms with commutativity, *SIAM. J.Comput* **9, 4,** (1980), 713-728.

[17] V. Strassen, Vermeidung von Divisionen, *J. Reine Angew. Math.* **264** (1973), 184-202.

[18] S. Winograd, On the Number of Multiplications Necessary to Compute Certain Functions, *Comm. Pure and Appl. Math.* **23** (1970), 165-179.