

MULTIPLICATIVE COMPLEXITY OF DIRECT SUM OF QUADRATIC SYSTEMS

Nader H. Bshouty

Department of Computer Science

Technion - IIT, Haifa, Israel

and

Department of Computer Science

University of Calgary, Calgary, Canada

ABSTRACT

We consider the quadratic complexity of certain sets of quadratic forms. We study classes of direct sums of quadratic forms. For these classes of problems we show that the complexity of one direct sum is the sum of the complexities of the summands and that every minimal quadratic algorithm for computing the direct sums is a direct-sum algorithm.

Key Words : multiplicative complexity, direct sum, quadratic algorithms, bilinear algorithms, algebras.

1. INTRODUCTION

Let F be a field, for $\mathbf{x} = (x_1, \dots, x_n)^T$ let $F[\mathbf{x}]$ be the ring of polynomials in x_1, \dots, x_n over the field F , and $\mathbf{z} = (z_1, \dots, z_k)^T$ be vectors of indeterminates. Let $Q^{\mathbf{x}} = (Q_1, \dots, Q_k) \in F[\mathbf{x}]^k$ be a vector of quadratic forms on x_1, \dots, x_n over the field F . The *quadratic system defined by $Q^{\mathbf{x}}$* is the polynomial $Q^{\mathbf{x}}\mathbf{z} = \sum_{i=1}^k Q_i z_i \in F[\mathbf{x}, \mathbf{z}]$. A *quadratic algorithm* that computes the quadratic system $Q^{\mathbf{x}}\mathbf{z}$ with *multiplicative complexity \mathbf{L}* is a set of triples $\{(a_i(\mathbf{z}), b_i(\mathbf{x}), c_i(\mathbf{x}))\}$ of size \mathbf{L} , where a_i, b_i and c_i are linear forms of the corresponding variables, and

$$Q^{\mathbf{x}}\mathbf{z} = \sum_{i=1}^{\mathbf{L}} a_i(\mathbf{z}) b_i(\mathbf{x}) c_i(\mathbf{x}). \quad (1)$$

The minimal integer \mathbf{L} in which (1) holds is denoted by $\mathbf{L} (Q^{\mathbf{x}\mathbf{z}})$ and then the quadratic algorithm is said to be *minimal*. It is known from [S1] that, when F is an infinite field, then $\mathbf{L} (Q^{\mathbf{x}\mathbf{z}})$ is the complexity of $Q^{\mathbf{x}\mathbf{z}}$ by means of straight-line algorithms.

Let $\mathbf{y} = (y_1, \dots, y_m)^T$ be a vector of indeterminates and let $Q^{\mathbf{x},\mathbf{y}} = (Q'_1, \dots, Q'_k) \in F[\mathbf{x}, \mathbf{y}]^k$ be a vector of bilinear forms on \mathbf{x} and \mathbf{y} . A *bilinear algorithm* that computes the *bilinear system* $Q^{\mathbf{x},\mathbf{y}\mathbf{z}}$ with multiplicative *rank* \mathbf{R} is a set of triples $\{(a_i(\mathbf{z}), b_i(\mathbf{x}), c_i(\mathbf{y}))\}$ of size \mathbf{R} where a_i, b_i and c_i are linear forms of the corresponding variables, and

$$Q^{\mathbf{x},\mathbf{y}\mathbf{z}} = \sum_{i=1}^{\mathbf{R}} a_i(\mathbf{z})b_i(\mathbf{x})c_i(\mathbf{y}). \quad (2)$$

The minimal integer \mathbf{R} for which (2) holds is denoted by $\mathbf{R} (Q^{\mathbf{x},\mathbf{y}\mathbf{z}})$. In [J1]¹ it was shown that

$$\mathbf{L} (Q^{\mathbf{x},\mathbf{y}\mathbf{z}}) \leq \mathbf{R} (Q^{\mathbf{x},\mathbf{y}\mathbf{z}}) < 2\mathbf{L} (Q^{\mathbf{x},\mathbf{y}\mathbf{z}}).$$

Since (1) and (2) uniquely determine the algorithms, for simplicity, we shall say that (1) and (2) are the quadratic and bilinear algorithm, respectively.

The *direct sum* of two quadratic systems $Q_1^{\mathbf{x}\mathbf{z}}$ and $Q_2^{\mathbf{y}\mathbf{z}}$ (respectively, two bilinear systems $Q_1^{\mathbf{x},\mathbf{y}\mathbf{z}}$ and $Q_2^{\mathbf{x},\mathbf{y}\mathbf{z}}$), denoted by $Q_1^{\mathbf{x}\mathbf{z}} \oplus Q_2^{\mathbf{y}\mathbf{z}}$ (respectively, $Q_1^{\mathbf{x},\mathbf{y}\mathbf{z}} \oplus Q_2^{\mathbf{x},\mathbf{y}\mathbf{z}}$), is $Q_1^{\mathbf{x}_1}\mathbf{z}_1 + Q_2^{\mathbf{x}_2}\mathbf{z}_2$ (respectively, $Q_1^{\mathbf{x}_1,\mathbf{y}_1}\mathbf{z}_1 + Q_2^{\mathbf{x}_2,\mathbf{y}_2}\mathbf{z}_2$) where $\mathbf{x}_i, \mathbf{y}_i, \mathbf{z}_i, i = 1, 2$ are distinct vectors of indeterminates. It is obvious that

$$\begin{aligned} \mathbf{R} (Q_1^{\mathbf{x}\mathbf{z}} \oplus Q_2^{\mathbf{y}\mathbf{z}}) &\leq \mathbf{R} (Q_1^{\mathbf{x}\mathbf{z}}) + \mathbf{R} (Q_2^{\mathbf{y}\mathbf{z}}), \\ \mathbf{L} (Q_1^{\mathbf{x}\mathbf{z}} \oplus Q_2^{\mathbf{y}\mathbf{z}}) &\leq \mathbf{L} (Q_1^{\mathbf{x}\mathbf{z}}) + \mathbf{L} (Q_2^{\mathbf{y}\mathbf{z}}). \end{aligned}$$

When equality holds for \mathbf{R} (respectively, for \mathbf{L}) for any bilinear system $Q_2^{\mathbf{x},\mathbf{y}\mathbf{z}}$ (respectively, quadratic system $Q_2^{\mathbf{y}\mathbf{z}}$), then we say that $Q_1^{\mathbf{x}\mathbf{z}}$ satisfies the *direct sum conjecture*, in short DSC, [S1], (respectively, then we say that $Q_1^{\mathbf{x}\mathbf{z}}$ satisfies the *extended direct sum conjecture*, in short EDSC).

We say that $Q_1^{\mathbf{x},\mathbf{y}\mathbf{z}}$ satisfies the *direct sum conjecture strongly*, in short DSCS, [W3] (respectively, $Q_1^{\mathbf{x}\mathbf{z}}$ satisfies the *extended direct sum conjecture strongly*, in short EDSCS) if for any bilinear system $Q_2^{\mathbf{x}_2,\mathbf{y}_2}\mathbf{z}_2$ (respectively, every quadratic system $Q_2^{\mathbf{x}_2}\mathbf{z}_2$), every minimal bilinear algorithm for $Q_1^{\mathbf{x}_1,\mathbf{y}_1}\mathbf{z}_1 + Q_2^{\mathbf{x}_2,\mathbf{y}_2}\mathbf{z}_2$ (respectively, every quadratic algorithm for $Q_1^{\mathbf{x}_1}\mathbf{z}_1 + Q_2^{\mathbf{x}_2}\mathbf{z}_2$) is of the form

¹ Obviously, quadratic algorithms can also compute bilinear systems, $Q^{\mathbf{x},\mathbf{y}\mathbf{z}} = \sum_{i=1}^{\mathbf{L}} a_i(\mathbf{z})b_i(\mathbf{x},\mathbf{y})c_i(\mathbf{x},\mathbf{y})$.

$$Q_1^{\mathbf{x}_1, \mathbf{y}_1} \mathbf{z}_1 + Q_2^{\mathbf{x}_2, \mathbf{y}_2} \mathbf{z}_2 = \sum_{i=1}^{\mathbf{R}_1} a_i(\mathbf{z}_1) b_i(\mathbf{x}_1) c_i(\mathbf{y}_1) + \sum_{i=1}^{\mathbf{R}_2} a'_i(\mathbf{z}_2) b'_i(\mathbf{x}_2) c'_i(\mathbf{y}_2)$$

(respectively,

$$Q_1^{\mathbf{x}_1} \mathbf{z}_1 + Q_2^{\mathbf{x}_2} \mathbf{z}_2 = \sum_{i=1}^{\mathbf{L}_1} a_i(\mathbf{z}_1) b_i(\mathbf{x}_1) c_i(\mathbf{x}_1) + \sum_{i=1}^{\mathbf{L}_2} a'_i(\mathbf{z}_2) b'_i(\mathbf{x}_2) c'_i(\mathbf{x}_2) \quad).$$

Here the first summand is a minimal bilinear algorithm for $Q_1^{\mathbf{x}_1, \mathbf{y}_1} \mathbf{z}_1$ (respectively, quadratic algorithm for $Q_1^{\mathbf{x}_1} \mathbf{z}_1$) and the second is a minimal bilinear algorithm for $Q_2^{\mathbf{x}_2, \mathbf{y}_2} \mathbf{z}_2$ (respectively, quadratic algorithm for $Q_2^{\mathbf{x}_2} \mathbf{z}_2$). In other words, every minimal algorithm for the direct sum system can be split into two algorithms. The first algorithm is minimal for the first system and the second algorithm is minimal for the second system.

Considerable attention has been given to the question of whether or not the direct sum conjecture properties are true for various systems. If we replace the ground field F by a ring R , then the results of Schonhage in [Sh] show that, when R is not an integral domain, the direct sum conjecture is not true. In the literature, the DSC, DSCS and EDSC properties have been proved for a few bilinear and quadratic systems. For details see [AFW], [ASt], [FW], [FZ], [Gr3], [Gr4], [JT1], [Mi] and [W3].

In this paper we define large classes of bilinear and quadratic forms and prove the direct sum conjecture properties for them.

2. NEW RESULTS

We will begin this section with some notation and definitions.

Let F be a field and let $\mathbf{x} = (x_1, \dots, x_n)^T$ and $\mathbf{y} = (y_1, \dots, y_m)^T$ be vectors of indeterminates. Let $Q^{\mathbf{x}, \mathbf{y}}$ be a k -vector of bilinear forms. Then, $Q^{\mathbf{x}, \mathbf{y}} = (\mathbf{x}^T A_1 \mathbf{y}, \dots, \mathbf{x}^T A_k \mathbf{y})$ where A_i are $n \times m$ -matrices with entries from F . For the matrix $Q(\mathbf{z}) = \sum_{i=1}^k A_i z_i$, which we call the *characteristic matrix* of $Q^{\mathbf{x}, \mathbf{y}}$, we have

$$Q^{\mathbf{x}, \mathbf{y}} \mathbf{z} = \sum_{i=1}^k (\mathbf{x}^T A_i \mathbf{y}) z_i = \mathbf{x}^T (\sum_{i=1}^k A_i z_i) \mathbf{y} = \mathbf{x}^T Q(\mathbf{z}) \mathbf{y}.$$

We define **row rank** $Q^{\mathbf{x}, \mathbf{y}} \mathbf{z}$ (respectively, **col rank** $Q^{\mathbf{x}, \mathbf{y}} \mathbf{z}$) to be the dimension of the linear space over F spanned by the rows of $Q(\mathbf{z})$ (respectively, columns of $Q(\mathbf{z})$) and

$$\mathbf{rank} Q^{\mathbf{x}, \mathbf{y}} \mathbf{z} = \mathbf{max} (\mathbf{col rank} Q^{\mathbf{x}, \mathbf{y}} \mathbf{z}, \mathbf{row rank} Q^{\mathbf{x}, \mathbf{y}} \mathbf{z}).$$

Finally we denote the linear space of bilinear forms spanned by the entries of $Q^{x,y}$ with $\mathbf{Span} (Q^{x,y})$, and its dimension with $\mathbf{dim} Q^{x,y}$. Then

$$\mathbf{dim} \mathbf{Span} (Q^{x,y}) = \mathbf{dim} \{Q^{x,y} u \mid u \in F^n\} = \mathbf{dim} \{Q(u) \mid u \in F^n\}.$$

In the remainder of the paper, we shall need the following definitions:

Definition I. For nonnegative integers τ and r we denote by $\mathbf{DS} (\tau, r)$, the collection of bilinear systems $Q^{x,y,z}$ such that: There exist integers $t \geq s \geq \tau$ such that the following conditions hold:

- (i) For every basis $\{Q_1, \dots, Q_k\}$ of the linear space $\mathbf{Span} (Q^{x,y})$ there exist $Q_{j_1}, \dots, Q_{j_{s-\tau}}$, $\tau+1 \leq j_i \leq k$, $i = 1, \dots, s - \tau$, such that

$$\mathbf{rank} ((Q_1, \dots, Q_\tau, Q_{j_1}, \dots, Q_{j_{s-\tau}}) \tilde{\mathbf{z}}) \geq t,$$

where $\tilde{\mathbf{z}} = (z_1, \dots, z_s)^T$.

and

- (ii) $\mathbf{L} (Q^{x,y,z}) = \mathbf{dim} Q^{x,y} + t - s + r$.

It follows at once from definition I that if $Q^{x,y,z} \in \mathbf{DS} (\tau, r)$, then condition (i) implies

- (i') For every basis $\{Q_1, \dots, Q_k\}$ of the linear space $\mathbf{Span} (Q^{x,y})$ there exist Q_{j_1}, \dots, Q_{j_s} , $1 \leq j_i \leq k$, $i = 1, \dots, s$, such that

$$\mathbf{rank} ((Q_{j_1}, \dots, Q_{j_s}) \tilde{\mathbf{z}}) \geq t.$$

It is well known (see, for example [BD1], [Fi], [FZ], [KB], [W2] and [W3]) that condition (i') implies

$$\mathbf{L} (Q^{x,y,z}) \geq \mathbf{dim} Q^{x,y} + t - s.$$

In the following we define a subset of $\mathbf{DS} (0, r)$ which is of special interest to the result of this paper.

Definition II. Let $Q^{x,y,z} \in \mathbf{DS} (0, r)$ with t and s of definition I. We say that $Q' \in \mathbf{Span} (Q^{x,y})$ is active if, for every basis $\{Q_1, \dots, Q_k\}$ of $\mathbf{Span} (Q^{x,y})$ that contains Q' , there exist Q_{i_2}, \dots, Q_{i_s} , $1 \leq i_j \leq k$, $j = 1, \dots, s$ such that

$$\mathbf{rank} ((Q', Q_{i_2}, \dots, Q_{i_s}) \tilde{\mathbf{z}}) \geq t.$$

where $\tilde{\mathbf{z}} = (z_1, \dots, z_s)^T$.

Definition III . Let $\mathbf{DS}^*(r)$ denote the collection of bilinear systems $Q^{x,y,z}$ in $\mathbf{DS}(0, r)$ which satisfy the following conditions:

(i) For every basis $\{Q_1, \dots, Q_k\}$ of $\mathbf{Span}(Q^{x,y})$ there exists an active element Q_{i_1} , $1 \leq i_1 \leq k$, such that for every non-active element Q_{i_2} , $1 \leq i_2 \leq k$, and every $f_1, f_2 \in F$, $f_1 \neq 0$, we have $f_1 Q_{i_1} + f_2 Q_{i_2}$ is active.

(ii) For the integers $t \geq s \geq 0$ of definition I we have: For every basis $\{Q_1, \dots, Q_k\}$ of $\mathbf{Span}(Q^{x,y})$, there exist s active elements Q_{i_1}, \dots, Q_{i_s} , $1 \leq i_j \leq k$, $j = 1, \dots, s$, such that

$$\mathbf{rank}((Q_{i_1}, \dots, Q_{i_s})\tilde{\mathbf{z}}) \geq t,$$

where $\tilde{\mathbf{z}} = (z_1, \dots, z_s)^T$.

Our main results are:

Theorem 1 . If $Q^{x,y,z} \in \mathbf{DS}(0, r)$, then for any quadratic system $Q^{x,z}$, we have

$$\mathbf{L}(Q^{x,y,z} \Theta Q^{x,z}) \geq \mathbf{L}(Q^{x,y,z}) + \mathbf{L}(Q^{x,z}) - r.$$

In particular, if $r = 0$, then $Q^{x,y,z}$ satisfies the EDSC.

Theorem 2 . If $Q^{x,y,z} \in \mathbf{DS}(1, 0)$, then $Q^{x,y,z}$ satisfies the EDSCS.

Theorem 3 . If $Q^{x,y,z} \in \mathbf{DS}(1, r)$, $r \geq 1$, then for any quadratic system $Q^{x,z}$, we have

$$\mathbf{L}(Q^{x,y,z} \Theta Q^{x,z}) \geq \mathbf{L}(Q^{x,y,z}) + \mathbf{L}(Q^{x,z}) - (r - 1).$$

In particular, if $r = 1$, then $Q^{x,y,z}$ satisfies the EDSC.

Theorem 4 . If $Q^{x,y,z} \in \mathbf{DS}^*(0)$, then $Q^{x,y,z}$ satisfies the EDSCS.

Theorem 5 . If $Q^{x,y,z} \in \mathbf{DS}^*(r)$, $r \geq 1$, then for any quadratic system $Q^{x,z}$, we have

$$\mathbf{L}(Q^{x,y,z} \Theta Q^{x,z}) \geq \mathbf{L}(Q^{x,y,z}) + \mathbf{L}(Q^{x,z}) - (r - 1).$$

In particular, if $r = 1$, then $Q^{x,y,z}$ satisfies the EDSC.

Notice that the results in the theorems are independent of the integers t and s in definitions I, II and III.

Remark . Theorem 1-5 are also true for the bilinear complexity, \mathbf{R} .

Examples of bilinear systems in $\mathbf{DS}(1, 0)$ include: bilinear systems $Q^{x,y} = (\mathbf{x}^T A \mathbf{y})$ with single

bilinear form; bilinear systems $Q^{x,y,z}$ that satisfy $\mathbf{L}(Q^{x,y,z}) = \mathbf{rank} Q^{x,y,z}$ or $\mathbf{L}(Q^{x,y,z}) = \mathbf{dim} Q^{x,y}$; bilinear systems defined by polynomial multiplication and their dual systems; and bilinear systems defined by the product of two polynomials, modulo a squarefree polynomial.

The set $\mathbf{DS}(1, 1)$ includes: bilinear systems $Q^{x,y,z}$ that satisfy $\mathbf{L}(Q^{x,y,z}) = \mathbf{rank} Q^{x,y,z} + 1$ or $\mathbf{L}(Q^{x,y,z}) = \mathbf{dim} Q^{x,y} + 1$; bilinear systems defined by the product of two quaternions; and bilinear systems defined by the product \mathbf{XY} and \mathbf{YX} of two 2×2 matrices.

The set $\mathbf{DS}^*(0)$ includes: bilinear systems defined by the product of two polynomials, modulo a fix polynomial; bilinear systems $Q^{x,y,z}$ that satisfy $\mathbf{L}(Q^{x,y,z}) \leq \mathbf{dim} Q^{x,y} + 1$; bilinear systems $Q^{x,y,z}$ with $\mathbf{row rank} Q^{x,y,z} = m$, $\mathbf{col rank} Q^{x,y,z} = n$ and $\mathbf{dim} Q^{x,y} \geq nm - 3$; bilinear systems defined by the product \mathbf{XY} and \mathbf{YX} of two quaternions; and bilinear systems defined by the product of two triangular 2×2 matrices.

The set $\mathbf{DS}^*(1)$ includes: bilinear systems $Q^{x,y,z}$ that satisfy $\mathbf{L}(Q^{x,y,z}) \geq \mathbf{dim} Q^{x,y} + 2$; bilinear systems $Q^{x,y,z}$ that satisfy $\mathbf{rank} Q^{x,y,z} \leq 3$; bilinear systems $Q^{x,y,z}$ with $\mathbf{row rank} Q^{x,y,z} = m$, $\mathbf{col rank} Q^{x,y,z} = n$ and $\mathbf{dim} Q^{x,y} = nm - 4$ or $nm - 5$; the bilinear system defined by the cross product of two 3-dimensional vector; the bilinear system defined by the product of two elements in the Lie algebra of 2×2 matrices; and the bilinear system defined by the multiplication of two triangular 3×3 -matrices.

For the next result we shall use the notation \mathbf{x}_n to denote the vector of indeterminates $(x_1, \dots, x_n)^T$ of length n , and similarly for \mathbf{y}_n and \mathbf{z}_n .

Let $Q = (A_1, \dots, A_k)$ be a vector of $n \times m$ -matrices with entries from F , and let $\mathbf{x}_n^T Q \mathbf{y}_m$ be the vector of bilinear forms $(\mathbf{x}_n^T A_1 \mathbf{y}_m, \dots, \mathbf{x}_n^T A_k \mathbf{y}_m)$. The D -dual and T -dual systems of $(\mathbf{x}_n^T Q \mathbf{y}_m)$, are $(\mathbf{x}_n^T Q^D \mathbf{y}_k)$ and $(\mathbf{x}_m^T Q^T \mathbf{y}_n)$ respectively, defined by

$$(\mathbf{x}_n^T Q \mathbf{y}_m) \mathbf{z}_k = (\mathbf{x}_n^T Q^D \mathbf{z}_k) \mathbf{y}_m = (\mathbf{y}_m^T Q^T \mathbf{x}_n) \mathbf{z}_k.$$

It follows that

$$Q^T = (A_1^T, \dots, A_k^T) \quad \text{and} \quad Q^D = (B_1, \dots, B_m),$$

where B_i are $n \times k$ matrices, $B_i = [A_1 e_i \mid \dots \mid A_k e_i]$ and $\{e_i\}$ is the standard basis of F^m .

Our main result for the bilinear complexity is:

Theorem 6 . Let $Q^{\mathbf{x},\mathbf{y}}\mathbf{z} = (\mathbf{x}_n^T Q \mathbf{y}_m) \mathbf{z}_k$ be a bilinear system. Then

(i) If $(\mathbf{x}_n^T Q \mathbf{y}_m) \mathbf{z}_k$ satisfies the DSCS (DSC), then so does each of the dual systems $(\mathbf{x}_n^T Q^D \mathbf{y}_k) \mathbf{z}_m$ and $(\mathbf{x}_m^T Q \mathbf{y}_n) \mathbf{z}_k$.

(ii) If for any bilinear system $Q^{\mathbf{x},\mathbf{y}}\mathbf{z}$ we have

$$\mathbf{R}((\mathbf{x}_n^T Q \mathbf{y}_m) \mathbf{z}_k \oplus Q^{\mathbf{x},\mathbf{y}}\mathbf{z}) \geq c + \mathbf{R}(Q^{\mathbf{x},\mathbf{y}}\mathbf{z}),$$

then for any bilinear systems, $Q_2^{\mathbf{x},\mathbf{y}}\mathbf{z}$ and $Q_3^{\mathbf{x},\mathbf{y}}\mathbf{z}$, we have

$$\mathbf{R}((\mathbf{x}_n^T Q^D \mathbf{y}_k) \mathbf{z}_m \oplus Q_2^{\mathbf{x},\mathbf{y}}\mathbf{z}) \geq c + \mathbf{R}(Q_2^{\mathbf{x},\mathbf{y}}\mathbf{z}),$$

$$\mathbf{R}((\mathbf{x}_m^T Q^T \mathbf{y}_n) \mathbf{z}_k \oplus Q_3^{\mathbf{x},\mathbf{y}}\mathbf{z}) \geq c + \mathbf{R}(Q_3^{\mathbf{x},\mathbf{y}}\mathbf{z}).$$

Let \mathbf{A} be an associative algebra of dimension k with a unit element 1, and let $\{a_1, \dots, a_k\}$ be a basis of \mathbf{A} . We denote by $Q_{\mathbf{A}}^{\mathbf{x},\mathbf{y}} = (Q_1, \dots, Q_k)$ the vector of bilinear forms defined by the product of two elements in \mathbf{A} , i.e.,

$$\sum_{i=1}^k Q_i a_i = \left[\sum_{i=1}^k x_i a_i \right] \left[\sum_{i=1}^k y_i a_i \right].$$

It has been shown in [FZ] that $\mathbf{L}(Q_{\mathbf{A}}^{\mathbf{x},\mathbf{y}}\mathbf{z})$ does not depend on the chosen basis.

A beautiful result of Alder and Strassen in [ASt] states: For any quadratic system $Q^{\mathbf{x},\mathbf{z}}$, we have

$$\mathbf{L}(Q_{\mathbf{A}}^{\mathbf{x},\mathbf{y}}\mathbf{z} \oplus Q^{\mathbf{x},\mathbf{z}}) \geq 2 \mathbf{dim} \mathbf{A} - t(\mathbf{A}) + \mathbf{L}(Q^{\mathbf{x},\mathbf{z}}),$$

where $t(\mathbf{A})$ is the number of two-sided maximal ideals of \mathbf{A} . If $\mathbf{L}(Q_{\mathbf{A}}^{\mathbf{x},\mathbf{y}}\mathbf{z}) = 2 \mathbf{dim} \mathbf{A} - t(\mathbf{A})$ (respectively, $\mathbf{R}(Q_{\mathbf{A}}^{\mathbf{x},\mathbf{y}}\mathbf{z}) = 2 \mathbf{dim} \mathbf{A} - t(\mathbf{A})$), then we say that the algebra is of *minimal complexity* (respectively, *minimal rank*).

Denote the radical of \mathbf{A} , i.e the maximal (two-sided) nilpotent ideal contained in \mathbf{A} , by $rad \mathbf{A}$. An algebra \mathbf{A} is called *local* if $\mathbf{A} / rad \mathbf{A}$ is a division algebra, and is called *clean* if $\mathbf{A} / rad \mathbf{A}$ is finite product of division algebras. For a direct product of division algebras $\mathbf{A} = \mathbf{A}_1 \times \dots \times \mathbf{A}_l$ we define $C_{\mathbf{A}}$ (respectively, $R_{\mathbf{A}}$) to be the number of \mathbf{A}_i which are not of minimal complexity (respectively, of minimal rank).

Our main results in the complexity of algebras are:

Corollary I

Let \mathbf{A} be a clean algebra. Then for any quadratic system $Q^{\mathbf{xz}}$ we have

$$L(Q_{\mathbf{A}}^{\mathbf{x}^y} \mathbf{z} \Theta Q^{\mathbf{xz}}) \geq 2 \dim \mathbf{A} - C_{\mathbf{A}/\text{rad } \mathbf{A}} + L(Q^{\mathbf{xz}}).$$

Corollary II

Let $\mathbf{A} = \mathbf{A}_1 \times \cdots \times \mathbf{A}_l$ be a direct product of division algebras. If \mathbf{A} is an algebra of minimal complexity, then $Q_{\mathbf{A}}^{\mathbf{x}^y}$ satisfies the EDSCS.

Corollary III

Let $\mathbf{A} = F[\alpha]/(p(\alpha))$ where $p(\alpha) \in F[\alpha]$ is a polynomial. Then $Q_{\mathbf{A}}^{\mathbf{x}^y}$ satisfies the EDSCS.

Corollary IV

Let \mathbf{A} be a clean algebra. If \mathbf{A} is an algebra of minimal rank, then $Q_{\mathbf{A}}^{\mathbf{x}^y} \mathbf{z}$ satisfies the DSCS.

Corollaries I, II and III have been proved by Feig and Winograd in [FW] for the bilinear complexity.

Characterization of division algebras \mathbf{A} of minimal complexity are studied in [Gr3] and [Fei]. It has been proved that division algebras of minimal complexity are simple field extensions of F with $|F| \geq 2 \dim \mathbf{A} - 2$. No results are known about non-division algebras of minimal complexity. Characterization of commutative algebras, local algebras, and clean algebras of minimal rank over a closed field are given in [GH1], [BC] and [HMo], respectively.

The paper is organized as follows. In sections 3 and 4 we prove some preliminary results needed for the proof of the theorems. In section 6 we prove Theorems 1, 2 and 3 and corollaries I and II. In section 7 we prove Theorems 4 and 5 and corollary III. In section 8 we prove Theorem 6. In section 6 we prove corollary IV. Finally, in section 9 we present some open problems in the area.

All the results in section 2, 3 and 4 are proved for the quadratic complexity. They are also valid for the bilinear complexity.

3. PRELIMINARY RESULTS

In this section we develop some lower bound techniques needed for the proof of our results.

Let $Q^{\mathbf{x}} = (Q_1, \dots, Q_k)$ be a k -vector of quadratic forms on $\mathbf{x} = (x_1, \dots, x_n)^T$ over the field F .

Each quadratic form in $Q^{\mathbf{x}}$ is

$$Q_l = \sum_{i=1}^n \sum_{j=i}^n a_{l,i,j} x_i x_j = \mathbf{x}^T A_l \mathbf{x},$$

where A_l is an upper triangular $n \times n$ -matrix. We define $Q = (A_1, \dots, A_k)$, and the *characteristic matrix* of Q is $Q(\mathbf{z}) = \sum_{i=1}^k A_i z_i$ where $\mathbf{z} = (z_1, \dots, z_k)$ is k -vector of indeterminates. It can be immediately seen that

$$\mathbf{x}^T Q(\mathbf{z}) \mathbf{x} = Q^{\mathbf{x}} \mathbf{z}.$$

The polynomial $Q^{\mathbf{x}} \mathbf{z}$ is called the *quadratic system* of $Q^{\mathbf{x}}$. For a vector of quadratic forms $Q^{\mathbf{x}}$, we define **Span** ($Q^{\mathbf{x}}$) to be the linear space of quadratic forms over F spanned by the entries of $Q^{\mathbf{x}}$, and define **dim** $Q^{\mathbf{x}}$ as its dimension. In a similar way, the bilinear system is defined by a vector of bilinear forms $Q^{\mathbf{x},\mathbf{y}}$. For a bilinear system $Q^{\mathbf{x},\mathbf{y}} \mathbf{z} = \mathbf{x}^T Q(\mathbf{z}) \mathbf{y}$ we define **row rank** $Q^{\mathbf{x},\mathbf{y}} \mathbf{z}$ (respectively, **col rank** $Q^{\mathbf{x},\mathbf{y}} \mathbf{z}$) to be the dimension of the linear space over F spanned by the rows (respectively, columns) of $Q(\mathbf{z})$. Finally, we let

$$\mathbf{rank} Q^{\mathbf{x},\mathbf{y}} \mathbf{z} = \max (\mathbf{col rank} Q^{\mathbf{x},\mathbf{y}} \mathbf{z}, \mathbf{row rank} Q^{\mathbf{x},\mathbf{y}} \mathbf{z}).$$

The following Lemma is frequently used in this paper.

Lemma 1 . *Let*

$$Q^{\mathbf{x}} \mathbf{z} = \sum_{i=1}^{\mathbf{L}_1} a_i(\mathbf{z}) b_i(\mathbf{x}) c_i(\mathbf{x})$$

and

$$Q^{\mathbf{x},\mathbf{y}} \mathbf{z} = \mathbf{x}^T Q_2(\mathbf{z}) \mathbf{y} = \sum_{i=1}^{\mathbf{L}_2} a_i'(\mathbf{z}) b_i'(\mathbf{x},\mathbf{y}) c_i'(\mathbf{x},\mathbf{y})$$

be minimal quadratic algorithms. Then the following are true

- (i) **dim Span** $\{a_1(\mathbf{z}), \dots, a_{\mathbf{L}_1}(\mathbf{z})\} \geq \mathbf{dim} Q^{\mathbf{x}}$.
- (ii) There exists a partition $\{I, J\}$ of $\{1, \dots, \mathbf{L}_2\}$ such that

$$\mathbf{dim Span} \{b_i'(0,\mathbf{y}), c_j'(0,\mathbf{y}) \mid i \in I, j \in J\} \geq \mathbf{col rank} Q^{\mathbf{x},\mathbf{y}} \mathbf{z}.$$

- (iii) $\mathbf{L}_1 \geq \mathbf{dim} Q^{\mathbf{x}}$.

(iv) $\mathbf{L}_2 \geq \text{col rank } Q^{\mathbf{x}, \mathbf{y}} \mathbf{z}$.

We remind the reader that $\text{Span}(A)$ denote the linear space spanned by the elements of the set A .

Proof. (i) and (ii) are proved in [AS] and (iii) and (iv) follow immediately from (i) and (ii), respectively. We shall give different proof for (i) and (ii) to illustrate the technique we will frequently use in the paper.

Let $Q^{\mathbf{x}} = (Q_1, \dots, Q_n)$, $\dim Q^{\mathbf{x}} = k$ and assume, without loss of generality, that Q_1, \dots, Q_k are linearly independent. We substitute in the algorithm $z_{k+1} = \dots = z_n = 0$ and obtain

$$Q^{\mathbf{x}, \mathbf{z}} \bar{\mathbf{z}} = \sum_{i=1}^{\mathbf{L}_1} \bar{a}_i(\bar{\mathbf{z}}) b_i(\mathbf{x}) c_i(\mathbf{x}),$$

where $Q^{\mathbf{x}, \mathbf{z}} = (Q_1, \dots, Q_k)$, $\bar{\mathbf{z}} = (z_1, \dots, z_k)$ and $\bar{a}_i(\bar{\mathbf{z}}) = a_i(\mathbf{z})|_{z_i=0, i=k+1, \dots, n}$.

Now we prove (i) by induction on k . The case $k=1$ is trivial. Assuming the result is true for $k-1$, we have: Since $Q_1 \neq 0$, the quadratic system $Q^{\mathbf{x}, \mathbf{z}} \bar{\mathbf{z}}$ is dependent on z_1 , and therefore, there exists $\bar{a}_i(\mathbf{z}) = \sum_{i=1}^k \lambda_i z_i$ that is dependent on z_1 , i.e., $\lambda_1 \neq 0$. Then substituting

$$z_1 = l(z_2, \dots, z_k) = -(1/\lambda_1) \sum_{i=2}^k \lambda_i z_i$$

we obtain

$$(Q_2 - (\lambda_2/\lambda_1)Q_1, \dots, Q_k - (\lambda_k/\lambda_1)Q_1) \tilde{\mathbf{z}} = \sum_{\substack{i=1 \\ i \neq i_0}}^{\mathbf{L}_1} \tilde{a}_i(\tilde{\mathbf{z}}) b_i(\mathbf{x}) c_i(\mathbf{x}).$$

Here $\tilde{\mathbf{z}} = (z_2, \dots, z_k)^T$ and

$$\tilde{a}_i(\tilde{\mathbf{z}}) = \bar{a}_i(\bar{\mathbf{z}})|_{z_1=l(z_2, \dots, z_k)} = \bar{a}_i(\bar{\mathbf{z}}) - \frac{\delta_{i,1}}{\lambda_1} \bar{a}_{i_0}(\bar{\mathbf{z}}),$$

where $\delta_{i,1}$ is the coefficient of z_1 in $\bar{a}_i(\bar{\mathbf{z}})$. Now by the induction hypothesis we have $\mathbf{L}_1 - 1 \geq k - 1$, so that $\mathbf{L}_1 \geq k$, as was to be shown.

Let $Q_2(\mathbf{z}) = [Q_2^{(1)}(\mathbf{z}), \dots, Q_2^{(m)}(\mathbf{z})]$ where $Q_2^{(i)}(\mathbf{z})$ is the i -th column of $Q_2(\mathbf{z})$. As above, we may assume that $Q_2^{(1)}(\mathbf{z}), \dots, Q_2^{(m)}(\mathbf{z})$ are linearly independent and we proceed to proof (ii) by induction on m . Since $Q_2^{(1)}(\mathbf{z}) \neq 0$, then $Q^{\mathbf{x}, \mathbf{y}} \mathbf{z} = \mathbf{x}^T Q_2(\mathbf{z}) \mathbf{y}$ depends on y_1 and therefore there exists b'_{j_0} (or c'_{j_0}) that depends on y_1 , that is,

$$b'_{j_0}(\mathbf{x}, \mathbf{y}) = \sum_{i=1}^n \lambda_i x_i + \sum_{j=1}^m \delta_j y_j,$$

where $\lambda_i, \delta_j \in F$ and $\delta_1 \neq 0$. Then substituting

$$y_1 = l'(\mathbf{x}, y_2, \dots, y_m) = -(1/\delta_1) \left(\sum_{i=1}^n \lambda_i x_i + \sum_{j=2}^m \delta_j y_j \right)$$

we obtain

$$\begin{aligned} \mathbf{x}^T [Q_2^{(2)}(\mathbf{z}) - (\delta_2/\delta_1)Q_2^{(1)}(\mathbf{z}), \dots, Q_2^{(m)}(\mathbf{z}) - (\delta_m/\delta_1)Q_2^{(1)}(\mathbf{z})] \tilde{\mathbf{y}} + \mathbf{x}^T K(\mathbf{z}) \mathbf{x} \\ = \sum_{\substack{i=1 \\ i \neq j_0}}^{\mathbf{L}_1} a'_i(\mathbf{z}) \tilde{b}_i(\mathbf{x}, \tilde{\mathbf{y}}) \tilde{c}_i(\mathbf{x}, \tilde{\mathbf{y}}) \end{aligned}$$

for some $K(\mathbf{z})$, where $\tilde{\mathbf{y}} = (y_2, \dots, y_m)^T$ and

$$\tilde{b}_i(\mathbf{x}, \tilde{\mathbf{y}}) = b'_i(\mathbf{x}, \mathbf{y})|_{y_1=l'(\mathbf{x}, y_2, \dots, y_m)}, \quad \tilde{c}_i(\mathbf{x}, \tilde{\mathbf{y}}) = c'_i(\mathbf{x}, \mathbf{y})|_{y_1=l'(\mathbf{x}, y_2, \dots, y_m)}.$$

By the induction hypothesis we have $\mathbf{L}_2 - 1 \geq m - 1$, so, $\mathbf{L}_2 \geq m$, as was to be shown. \square

Remark . In what follows, the results are true for **row rank** as well as **col rank**. The results are proved either for **row rank** or **col rank** for our convenience.

Throughout the paper we assume that $a_1(\mathbf{z}), \dots, a_k(\mathbf{z})$, $k = \mathbf{dim} Q^{\mathbf{x}}$, (respectively, $b_1(0, \mathbf{y}), \dots, b_m(0, \mathbf{y})$, $m = \mathbf{col rank} Q_2^{\mathbf{x}, \mathbf{y}}(\mathbf{z})$) are linearly independent.

Applying the argument used in the proof of Lemma 1, we will develop the following more general results:

Lemma 2 . Let $\mathbf{x}, \mathbf{y}, \mathbf{u}, \mathbf{v}, \mathbf{z}$ be distinct vectors of indeterminates and let $Q_1^{\mathbf{x}, \mathbf{u}} \mathbf{z} = \mathbf{x}^T Q_1(\mathbf{z}) \mathbf{u}$ be a bilinear system. Then for any quadratic system $\mathbf{y}^T Q_3(\mathbf{z}) \mathbf{y}$ and bilinear system $\mathbf{x}^T Q_2(\mathbf{z}) \mathbf{y}$ we have

$$\mathbf{L}(\mathbf{x}^T Q_1(\mathbf{z}) \mathbf{u} + \mathbf{x}^T Q_2(\mathbf{z}) \mathbf{y} + \mathbf{y}^T Q_3(\mathbf{z}) \mathbf{y}) \geq \mathbf{col rank} Q_1^{\mathbf{x}, \mathbf{u}} \mathbf{z} + \mathbf{L}(\mathbf{y}^T Q_3(\mathbf{z}) \mathbf{y}).$$

Therefore, for the bilinear systems $Q_1^{\mathbf{u}, \mathbf{x}} \mathbf{z} = \mathbf{u}^T Q_1(\mathbf{z}) \mathbf{x}$ and $Q_1^{\mathbf{u}, \mathbf{v}} \mathbf{z} = \mathbf{u}^T Q_1(\mathbf{z}) \mathbf{v}$ we have

$$\mathbf{L}(\mathbf{u}^T Q_1(\mathbf{z}) \mathbf{x} + \mathbf{x}^T Q_2(\mathbf{z}) \mathbf{y} + \mathbf{y}^T Q_3(\mathbf{z}) \mathbf{y}) \geq \mathbf{row rank} Q_1^{\mathbf{u}, \mathbf{x}} \mathbf{z} + \mathbf{L}(\mathbf{y}^T Q_3(\mathbf{z}) \mathbf{y}),$$

and

$$\mathbf{L}(\mathbf{u}^T Q_1(\mathbf{z}) \mathbf{v} + \mathbf{y}^T Q_3(\mathbf{z}) \mathbf{y}) \geq \mathbf{rank} Q_1^{\mathbf{u}, \mathbf{v}} \mathbf{z} + \mathbf{L}(\mathbf{y}^T Q_3(\mathbf{z}) \mathbf{y}).$$

Proof . Exactly as in the proof of lemma 1, we can find a substitution $u_1 = l(\mathbf{x}, \mathbf{y}, u_2, \dots, u_n)$ that will vanish at least one term in the quadratic algorithm. Applying this argument to u_2, \dots, u_n , respectively, (here $n = \mathbf{col rank} Q_1^{\mathbf{x}, \mathbf{u}} \mathbf{z}$), we obtain an algorithm for

$$\mathbf{x}^T A_1(\mathbf{z}) \mathbf{x} + \mathbf{x}^T A_2(\mathbf{z}) \mathbf{y} + \mathbf{x}^T Q_2(\mathbf{z}) \mathbf{y} + \mathbf{y}^T Q_3(\mathbf{z}) \mathbf{y},$$

for some $A_1(\mathbf{z})$ and $A_2(\mathbf{z})$, with multiplicative complexity

$$\mathbf{L}' = \mathbf{L} (\mathbf{x}^T Q_1(\mathbf{z}) \mathbf{u} + \mathbf{x}^T Q_2(\mathbf{z}) \mathbf{y} + \mathbf{y}^T Q_3(\mathbf{z}) \mathbf{y}) - \text{col rank } Q_1^{\mathbf{x}, \mathbf{u}} \mathbf{z}.$$

Now by substituting $\mathbf{x} = 0$ in the algorithm we obtain a quadratic algorithm for $\mathbf{y}^T Q_3(\mathbf{z}) \mathbf{y}$. Therefore

$$\mathbf{L}' \geq \mathbf{L} (\mathbf{y}^T Q_3(\mathbf{z}) \mathbf{y}) \text{ and the lemma is proved. } \square$$

The last two results of this section are well known. Lemma 3, is frequently used in the literature to obtain lower bounds for the complexity of bilinear systems. For example, see [W2], [W3] and [KB]. For the sake of completeness, a proof is given which illustrates our method. Lemma 4 is trivial and we shall refer to it in the remainder of the paper.

Lemma 3. *Let $Q^{\mathbf{x}} = (Q_1, \dots, Q_k)$ be a k -vector of quadratic forms. Suppose that, for any nonsingular $n \times n$ -matrix N , there exist s entries Q_{i_1}, \dots, Q_{i_s} of $Q^{\mathbf{x}N}$ such that for $\tilde{\mathbf{z}} = (z_1, \dots, z_s)^T$ we have*

$$\mathbf{L} ((Q_{i_1}, \dots, Q_{i_s}) \tilde{\mathbf{z}}) \geq t.$$

Then

$$\mathbf{L} (Q^{\mathbf{x}\mathbf{z}}) \geq \text{dim } Q^{\mathbf{x}} + t - s.$$

Proof. Let $\mathbf{L} = \mathbf{L} (Q^{\mathbf{x}\mathbf{z}})$. Then

$$Q^{\mathbf{x}\mathbf{z}} = \sum_{i=1}^{\mathbf{L}} a_i(\mathbf{z}) b_i(\mathbf{x}) c_i(\mathbf{x}).$$

By lemma 1, there exist $k = \text{dim } Q^{\mathbf{x}}$ independent $a_i(\mathbf{z})$ and therefore we can assume, without loss of generality, that there exists a nonsingular $n \times n$ -matrix M satisfying $a_1(M \mathbf{z}) = z_1, \dots, a_k(M \mathbf{z}) = z_k$ and hence

$$Q^{\mathbf{x}M\mathbf{z}} = \sum_{i=1}^k z_i b_i(\mathbf{x}) c_i(\mathbf{x}) + \sum_{i=k+1}^{\mathbf{L}} a_i(M \mathbf{z}) b_i(\mathbf{x}) c_i(\mathbf{x}).$$

Assume, without loss of generality, that the first entries Q_1, \dots, Q_s of $Q^{\mathbf{x}M} = (Q_1, \dots, Q_k)$ satisfy

$$\mathbf{L} ((Q_1, \dots, Q_s) \tilde{\mathbf{z}}) \geq t,$$

for $\tilde{\mathbf{z}} = (z_1, \dots, z_s)^T$. Then, by substituting $z_{s+1} = \dots = z_k = 0$, we get

$$\begin{aligned} & (Q_1, \dots, Q_s) \tilde{\mathbf{z}} = \\ & (Q_1, \dots, Q_s, 0, \dots, 0) \hat{\mathbf{z}} = \sum_{i=1}^s z_i b_i(\mathbf{x}) c_i(\mathbf{x}) + \sum_{i=k+1}^{\mathbf{L}} a_i(M \hat{\mathbf{z}}) b_i(\mathbf{x}) c_i(\mathbf{x}), \end{aligned}$$

where $\hat{\mathbf{z}} = (z_1, \dots, z_s, 0, \dots, 0)^T$. The last equation implies that

$$t \leq \mathbf{L} \left((Q_1, \dots, Q_s) \tilde{\mathbf{z}} \right) \leq \mathbf{L} - k + s,$$

and this completes the proof. \square

Lemma 4 . Let $\mathbf{x} = (x_1, \dots, x_n)^T$, $\tilde{\mathbf{x}} = (x_1, \dots, x_{n'})^T$, $\mathbf{z} = (z_1, \dots, z_k)^T$ and $\tilde{\mathbf{z}} = (z_1, \dots, z_{k'})^T$ and let N and K be $n \times n'$ and $k \times k'$ -matrices of rank n and k , respectively. Then

$$\mathbf{x}^T Q(\mathbf{z}) \mathbf{x} = \sum_{i=1}^{\mathbf{L}} a_i(\mathbf{z}) b_i(\mathbf{x}) c_i(\mathbf{x}) \quad (3)$$

is a minimal quadratic algorithm for $Q(\mathbf{z})$ if and only if

$$\tilde{\mathbf{x}}^T N^T Q(K \tilde{\mathbf{z}}) N \tilde{\mathbf{x}} = \sum_{i=1}^{\mathbf{L}} a_i(K \tilde{\mathbf{z}}) b_i(N \tilde{\mathbf{x}}) c_i(N \tilde{\mathbf{x}}) \quad (4)$$

is a minimal quadratic algorithm for $N^T Q(K \tilde{\mathbf{z}}) N$.

Proof . If (3) is true, then by substituting $\mathbf{x} = N \tilde{\mathbf{x}}$ and $\mathbf{z} = K \tilde{\mathbf{z}}$ we get (4). There exists a matrices N^- and K^- such that $N N^- = I_n$, and $K K^- = I_k$ where I_n is the identity $n \times n$ -matrix. Substituting $N^- \mathbf{x}$ for $\tilde{\mathbf{x}}$ and $K^- \mathbf{z}$ for $\tilde{\mathbf{z}}$ in (4) we obtain (3). \square

4. SEPARABLE ALGORITHMS

The main purpose of this section is to introduce the strong version of the direct sum conjecture (DSCS, EDSCS), and to analyze minimal quadratic algorithms for a direct sum of quadratic systems. We also find equivalent conditions for the strong direct sum conjecture which will be frequently used in this paper.

Let $\mathbf{x}_1 = (x_1, \dots, x_n)^T$, $\mathbf{x}_2 = (x_{n+1}, \dots, x_{n+m})^T$, $\mathbf{z}_1 = (z_1, \dots, z_r)^T$ and $\mathbf{z}_2 = (z_{r+1}, \dots, z_{r+s})^T$ be vectors of indeterminates and let $\mathbf{x} = (\mathbf{x}_1^T, \mathbf{x}_2^T)^T$ and $\mathbf{z} = (\mathbf{z}_1^T, \mathbf{z}_2^T)^T$. For two vectors of quadratic forms, $Q_1^{\mathbf{x}_1}$ and $Q_2^{\mathbf{x}_2}$, we say that the minimal quadratic algorithm

$$Q^{\mathbf{xz}} = Q_1^{\mathbf{x}_1} \mathbf{z}_1 + Q_2^{\mathbf{x}_2} \mathbf{z}_2 = \sum_{i=1}^{\mathbf{L}} a_i(\mathbf{z}) b_i(\mathbf{x}) c_i(\mathbf{x})$$

is *separable* if there exists a set $I \subseteq \{1, \dots, \mathbf{L}\}$ such that the following conditions hold:

(i) $Q_1^{\mathbf{x}_1} \mathbf{z}_1 = \sum_{i \in I} a_i(\mathbf{z}) b_i(\mathbf{x}) c_i(\mathbf{x})$, $Q_2^{\mathbf{x}_2} \mathbf{z}_2 = \sum_{i \notin I} a_i(\mathbf{z}) b_i(\mathbf{x}) c_i(\mathbf{x})$.

(ii) The first quadratic algorithm in (i) (respectively, the second) is a minimal quadratic algorithm for $Q_1^{\mathbf{x}_1} \mathbf{z}_1$ (respectively, $Q_2^{\mathbf{x}_2} \mathbf{z}_2$).

(iii) The terms $a_i(\mathbf{z}), b_i(\mathbf{x}), c_i(\mathbf{x}), i \in I$ (respectively, $i \notin I$) are linear forms of \mathbf{z}_1 and \mathbf{x}_1 (respectively, \mathbf{z}_2 and \mathbf{x}_2), that is, they are independent of \mathbf{z}_2 and \mathbf{x}_2 , (respectively, of \mathbf{z}_1 and \mathbf{x}_1).

We say that $Q_1^{\mathbf{x}_1} \mathbf{z}_1$ satisfies the *extended direct sum conjecture strongly* (EDSCS) if, for any quadratic system $Q_2^{\mathbf{x}_2} \mathbf{z}_2$, any minimal quadratic algorithm for $Q_1^{\mathbf{x}_1} \mathbf{z}_1 + Q_2^{\mathbf{x}_2} \mathbf{z}_2$ is separable.

The following lemma proves that condition (i) is sufficient for an algorithm to be separable. (The technique we use in our proof was used in [AFW] for the bilinear complexity).

Lemma 5. *If there exists a set $I \subseteq \{1, \dots, \mathbf{L}\}$ such that*

$$Q_1^{\mathbf{x}_1} \mathbf{z}_1 = \sum_{i \in I} a_i(\mathbf{z}) b_i(\mathbf{x}) c_i(\mathbf{x}),$$

then the algorithm is separable.

Proof. Obviously,

$$Q_2^{\mathbf{x}_2} \mathbf{z}_2 = Q^{\mathbf{x}} \mathbf{z} - Q_1^{\mathbf{x}_1} \mathbf{z}_1 = \sum_{i \notin I} a_i(\mathbf{z}) b_i(\mathbf{x}) c_i(\mathbf{x}).$$

If $|I| > \mathbf{L}(Q_1^{\mathbf{x}_1} \mathbf{z}_1)$, then, since $|N_{\mathbf{L}} - I| \geq \mathbf{L}(Q_2^{\mathbf{x}_2} \mathbf{z}_2)$, we have

$$\mathbf{L}(Q^{\mathbf{x}} \mathbf{z}) = |I| + |N_{\mathbf{L}} - I| > \mathbf{L}(Q_1^{\mathbf{x}_1} \mathbf{z}_1) + \mathbf{L}(Q_2^{\mathbf{x}_2} \mathbf{z}_2).$$

A contradiction. Therefore $|I| = \mathbf{L}(Q_1^{\mathbf{x}_1} \mathbf{z}_1)$ and (ii) follows.

Suppose that for some $i_0 \in I$, $a_{i_0}(\mathbf{z}) = \lambda z_{j_0} + \tilde{a}_{i_0}(\mathbf{z})$ depends on z_{j_0} (i.e. $\lambda \neq 0$) where $j_0 > r$. We remind the reader that $\mathbf{z}_1 = (z_1, \dots, z_r)$ and $\mathbf{z}_2 = (z_{r+1}, \dots, z_{r+s})$ so that if $j_0 > r$, then $a_{i_0}(\mathbf{z})$ is dependent on $z_{j_0}, j_0 > r$ and therefore $a_{i_0}(\mathbf{z})$ is dependent on \mathbf{z}_2 . Then substituting $z_{j_0} = -(1/\lambda) \tilde{a}_{i_0}(\mathbf{z})$ in the first algorithm we obtain

$$Q_1^{\mathbf{x}_1} \mathbf{z}_1 = \sum_{i \in I - \{i_0\}} \tilde{a}_i(\mathbf{z}) b_i(\mathbf{x}) c_i(\mathbf{x}),$$

where $\tilde{a}_i(\mathbf{z}) = a_i(\mathbf{z}) \big|_{z_{j_0} = -(1/\lambda) \tilde{a}_{i_0}(\mathbf{z})}$. Therefore $\mathbf{L}(Q_1^{\mathbf{x}_1} \mathbf{z}_1) \leq |I| - 1$, a contradiction. Interchanging the roles of a_i and b_i , (iii) follows. \square

Lemma 6. *If the algorithm is not separable, then there exists $a_i(\mathbf{z})$ that depends on \mathbf{z}_1 and \mathbf{z}_2 , and $b_i(\mathbf{x})$ or $c_i(\mathbf{x})$ that depends on \mathbf{x}_1 and \mathbf{x}_2 .*

Proof . Assume that each $a_i(\mathbf{z})$ depends on \mathbf{z}_1 or \mathbf{z}_2 , but not both. Let $I = \{i \mid a_i(\mathbf{z}) \text{ depends on } \mathbf{z}_1\}$.

Then by substituting $\mathbf{z}_2 = 0$ we get

$$Q_1^{\mathbf{x}_1} \mathbf{z}_1 = \sum_{i \in I} a_i(\mathbf{z}) b_i(\mathbf{x}) c_i(\mathbf{x}).$$

By lemma 5, the algorithm is seperable and the proof is completed. In a similar way we can prove the result for b_i and c_i . \square

Lemma 7 . Let $\mathbf{x}, \mathbf{z}, \tilde{\mathbf{x}}, \tilde{\mathbf{z}}, N$ and K be as in lemma 4. Then, $\mathbf{x}^T Q(\mathbf{z})\mathbf{x}$ satisfies the EDSCS if and only if $\tilde{\mathbf{x}}^T N^T Q(K\tilde{\mathbf{z}})N\tilde{\mathbf{x}}$ satisfies the EDSCS.

Proof . Assume that $\tilde{\mathbf{x}}^T N^T Q(K\tilde{\mathbf{z}})N\tilde{\mathbf{x}}$ does not satisfy the EDSCS. Then, by lemma 6, there exists a quadratic system $Q^{\mathbf{u}\mathbf{v}}$ and there exists a minimal quadratic algorithm

$$\tilde{\mathbf{x}}^T N^T Q(K\tilde{\mathbf{z}})N\tilde{\mathbf{x}} + Q^{\mathbf{u}\mathbf{v}} = \sum_{i=1}^L a_i(\tilde{\mathbf{z}}, \mathbf{u}) b_i(\tilde{\mathbf{x}}, \mathbf{v}) c_i(\tilde{\mathbf{x}}, \mathbf{v}),$$

such that $a_1(\tilde{\mathbf{z}}, \mathbf{u})$ depends on $\tilde{\mathbf{z}}$ and \mathbf{u} . Then substituting $\tilde{\mathbf{x}} = N^{-1}\mathbf{x}$ and applying lemma 4 we have that

$$\mathbf{x}^T Q(K\tilde{\mathbf{z}})\mathbf{x} + Q^{\mathbf{u}\mathbf{v}} = \sum_{i=1}^L a_i(\tilde{\mathbf{z}}, \mathbf{u}) b_i(N^{-1}\mathbf{x}, \mathbf{v}) c_i(N^{-1}\mathbf{x}, \mathbf{v}),$$

is a minimal quadratic algorithm. Note that $a_1(\tilde{\mathbf{z}}, \mathbf{u})$ is still dependent on $\tilde{\mathbf{z}}$ and \mathbf{u} and therefore $\mathbf{x}^T Q(K\tilde{\mathbf{z}})\mathbf{x}$ does not satisfy the EDSCS. By lemma 6, there exists (without loss of generality) a $b_{i_0}(N^{-1}\mathbf{x}, \mathbf{v})$ that depends on \mathbf{x} and \mathbf{v} . Substituting $\tilde{\mathbf{z}} = K^{-1}\mathbf{z}$ and applying lemma 4 again, we have that

$$\mathbf{x}^T Q(\mathbf{z})\mathbf{x} + Q^{\mathbf{u}\mathbf{v}} = \sum_{i=1}^L a_i(K^{-1}\mathbf{z}, \mathbf{u}) b_i(N^{-1}\mathbf{x}, \mathbf{v}) c_i(N^{-1}\mathbf{x}, \mathbf{v})$$

is a minimal quadratic algorithm. Since $b_{i_0}(N^{-1}\mathbf{x}, \mathbf{v})$ depends on \mathbf{x} and \mathbf{v} then by lemma 6 we have a contradiction to the fact that $\mathbf{x}^T Q(\mathbf{z})\mathbf{x}$ satisfies the EDSCS. \square

Remark . For bilinear systems $\mathbf{x}^T Q(\mathbf{z})\mathbf{y} = Q^{\mathbf{x},\mathbf{y}}\mathbf{z}$ with $\mathbf{x} = (x_1, \dots, x_n)^T$, $\mathbf{y} = (y_1, \dots, y_m)^T$ and $\mathbf{z} = (z_1, \dots, z_k)^T$ and matrices N, M, K of rank n, m, k respectively, lemma 4 and 7 hold for $\mathbf{x}^T Q(\mathbf{z})\mathbf{y}$ and $\mathbf{x}^T N^T Q(K\mathbf{z})M\mathbf{y}$. This follows because

$$\mathbf{x}^T N^T Q(K\mathbf{z})M\mathbf{y} = (\mathbf{x}^T, \mathbf{y}^T) \begin{pmatrix} N & 0 \\ 0 & M \end{pmatrix}^T \begin{pmatrix} 0 & Q(K\mathbf{z}) \\ 0 & 0 \end{pmatrix} \begin{pmatrix} N & 0 \\ 0 & M \end{pmatrix} \begin{pmatrix} \mathbf{x} \\ \mathbf{y} \end{pmatrix}.$$

Thus we can assume throughout the paper that

$$\text{row rank } Q^{\mathbf{x},\mathbf{y}}\mathbf{z} = n, \text{ col rank } Q^{\mathbf{x},\mathbf{y}}\mathbf{z} = m, \text{ dim } Q^{\mathbf{x},\mathbf{y}} = k.$$

Another equivalent condition for the quadratic algorithms to be separable is given in Lemma 8 below. Recall that $\mathbf{Span}(Q^{\mathbf{x}})$ is the linear space spanned by the entries of $Q^{\mathbf{x}}$, $\mathbf{x}_1 = (x_1, \dots, x_n)^T$, $\mathbf{x}_2 = (x_{n+1}, \dots, x_{n+m})^T$, $\mathbf{z}_1 = (z_1, \dots, z_r)^T$ and $\mathbf{z}_2 = (z_{r+1}, \dots, z_{r+s})^T$. We need the following definition.

Definition 1 . For $Q^{\mathbf{x}\mathbf{z}} = Q_1^{\mathbf{x}_1} \mathbf{z}_1 + Q_2^{\mathbf{x}_2} \mathbf{z}_2$ we say that a nonsingular $(r+s) \times (r+s)$ -matrix N does not mix $Q_1^{\mathbf{x}_1}$ with $Q_2^{\mathbf{x}_2}$ if each entry of $Q_1^{\mathbf{x}_1} N$ is either in $\mathbf{Span}(Q_1^{\mathbf{x}_1})$ or in $\mathbf{Span}(Q_2^{\mathbf{x}_2})$.

We say that the nonsingular $(r+s) \times (r+s)$ -matrix N normalize the minimal quadratic algorithm

$$Q^{\mathbf{x}\mathbf{z}} = \sum_{i=1}^{\mathbf{L}} a_i(\mathbf{z}) b_i(\mathbf{x}) c_i(\mathbf{x})$$

if

$$Q^{\mathbf{x}} N \mathbf{z} = \sum_{j_i \in I} z_i b_{j_i}(\mathbf{x}) c_{j_i}(\mathbf{x}) + \sum_{j \notin I} a_j(N \mathbf{z}) b_j(\mathbf{x}) c_j(\mathbf{x}),$$

where $I = \{j_1, \dots, j_{r+s}\}$ is a subset of $\{1, \dots, \mathbf{L}\}$ and $|I| = r+s$. That is, there exists a set of integers I of size $r+s$ such that for each $j_i \in I$, $i = 1, \dots, r+s$ we have $a_{j_i}(N \mathbf{z}) = z_i$.

Lemma 8 . Let $Q^{\mathbf{x}\mathbf{z}} = Q^{\mathbf{x}_1} \mathbf{z}_1 + Q^{\mathbf{x}_2} \mathbf{z}_2$ and let $Q^{\mathbf{x}\mathbf{z}} = \sum_{i=1}^{\mathbf{L}} a_i(\mathbf{z}) b_i(\mathbf{x}) c_i(\mathbf{x})$ be a minimal quadratic algorithm for $Q^{\mathbf{x}\mathbf{z}}$. If, for every nonsingular $(r+s) \times (r+s)$ -matrix N that normalizes the minimal algorithm, the matrix N does not mix $Q_1^{\mathbf{x}_1}$ with $Q_2^{\mathbf{x}_2}$, then the quadratic algorithm is separable.

Proof . Assume that the quadratic algorithm is not separable. Then, by lemma 6, (without loss of generality) $a_1(\mathbf{z}) = a_{1,1}(\mathbf{z}_1) + a_{1,2}(\mathbf{z}_2)$ where $a_{1,1}(\mathbf{z}_1) \neq 0$ and $a_{1,2}(\mathbf{z}_2) \neq 0$. Let N be a nonsingular $(r+s) \times (r+s)$ -matrix such that (without loss of generality, by reordering the terms of the sum)

$$Q^{\mathbf{x}} N \mathbf{z} = \sum_{i=1}^{r+s} z_i b_i(\mathbf{x}) c_i(\mathbf{x}) + \sum_{i=r+s+1}^{\mathbf{L}} a_i(N \mathbf{z}) b_i(\mathbf{x}) c_i(\mathbf{x}).$$

Notice that in this case $a_i(N \mathbf{z}) = z_i$, $i = 1, \dots, r+s$. Since N does not mix $Q_1^{\mathbf{x}_1}$ with $Q_2^{\mathbf{x}_2}$, the matrix N is of the form

$$N = \begin{bmatrix} N_1 & 0 \\ 0 & N_2 \end{bmatrix} E_\phi$$

for some permutation matrix E_ϕ , where $Q^{\mathbf{x}} N E_\phi^{-1} = (Q_1^{\mathbf{x}_1} N_1, Q_2^{\mathbf{x}_2} N_2)$. Since $a_1(N \mathbf{z}) = z_1$, we have

$$z_{\phi^{-1}(1)} = a_1(N E_\phi^{-1} \mathbf{z}) = a_{1,1}(N_1 \mathbf{z}_1) + a_{1,2}(N_2 \mathbf{z}_2)$$

and therefore $a_{1,1}(N_1\mathbf{z}_1) = 0$ or $a_{1,2}(N_2\mathbf{z}_2) = 0$. Since N is nonsingular, N_1 and N_2 are nonsingular and therefore $a_{1,1}(\mathbf{z}_1) = 0$ or $a_{1,2}(\mathbf{z}_2) = 0$. This is a contradiction. \square

5. DIRECT SUM OF SOME CLASSES

In this section we define some classes of quadratic systems and prove that they satisfy the EDSC and EDSCS.

Definition 2. For nonnegative integers τ and r we denote by $\mathbf{DS}(\tau, r)$, the collection of bilinear systems

$Q^{\mathbf{x},\mathbf{y}\mathbf{z}} = \sum_{i=1}^n Q'_i z_i$ such that: There exist integers $s \geq t \geq \tau$ such that the following conditions hold:

- (i) For every nonsingular $n \times n$ -matrix N and for every τ entries $Q_{i_1}, \dots, Q_{i_\tau}$ of $Q^{\mathbf{x},\mathbf{y}N}$, there exist $s - \tau$ entries $Q_{j_1}, \dots, Q_{j_{s-\tau}}$ of $Q^{\mathbf{x},\mathbf{y}N}$ such that

$$\mathbf{rank}((Q_{i_1}, \dots, Q_{i_\tau}, Q_{j_1}, \dots, Q_{j_{s-\tau}})\tilde{\mathbf{z}}) \geq t,$$

where $\tilde{\mathbf{z}} = (z_1, \dots, z_s)^T$.

- (ii) $\mathbf{L}(Q^{\mathbf{x},\mathbf{y}\mathbf{z}}) = \mathbf{dim} Q^{\mathbf{x},\mathbf{y}} + t - s + r$.

By lemma 3, if $Q^{\mathbf{x},\mathbf{y}\mathbf{z}}$ satisfies (i), then $\mathbf{L}(Q^{\mathbf{x},\mathbf{y}\mathbf{z}}) \geq \mathbf{dim} Q^{\mathbf{x},\mathbf{y}} + t - s$.

Remark . Definition 2 is equivalent to definition I in the introduction.

Our main results in this section are:

Theorem 1. If $Q^{\mathbf{x},\mathbf{y}\mathbf{z}} \in \mathbf{DS}(0, r)$, then for any quadratic system $Q^{\mathbf{x}\mathbf{z}}$ we have

$$\mathbf{L}(Q^{\mathbf{x},\mathbf{y}\mathbf{z}} \oplus Q^{\mathbf{x}\mathbf{z}}) \geq \mathbf{L}(Q^{\mathbf{x},\mathbf{y}\mathbf{z}}) + \mathbf{L}(Q^{\mathbf{x}\mathbf{z}}) - r.$$

In particular, if $r = 0$, then $Q^{\mathbf{x},\mathbf{y}\mathbf{z}}$ satisfies the EDSC.

Theorem 2. If $Q^{\mathbf{x},\mathbf{y}\mathbf{z}} \in \mathbf{DS}(1, 0)$, then $Q^{\mathbf{x},\mathbf{y}\mathbf{z}}$ satisfies the EDSCS.

Theorem 3. If $Q^{\mathbf{x},\mathbf{y}\mathbf{z}} \in \mathbf{DS}(1, r)$, $r \geq 1$, then for any quadratic system $Q^{\mathbf{x}\mathbf{z}}$ we have

$$\mathbf{L}(Q^{\mathbf{x},\mathbf{y}\mathbf{z}} \oplus Q^{\mathbf{x}\mathbf{z}}) \geq \mathbf{L}(Q^{\mathbf{x},\mathbf{y}\mathbf{z}}) + \mathbf{L}(Q^{\mathbf{x}\mathbf{z}}) - (r - 1).$$

In particular, if $r = 1$, then $Q^{\mathbf{x},\mathbf{y}\mathbf{z}}$ satisfies the EDSC.

Proof of Theorem 1 .

Let $Q^{x_1, y_1} \mathbf{z}_1 = Q_1 z_1 + \dots + Q_k z_k \in \mathbf{DS}(0, r)$ and $Q^{x_2} \mathbf{z}_2 = Q_{k+1} z_{k+1} + \dots + Q_{k+k'} z_{k+k'}$ be any quadratic system. Set $Q^x = (Q^{x_1, y_1}, Q^{x_2})$, $\mathbf{x} = (\mathbf{x}_1^T, \mathbf{y}_1^T, \mathbf{x}_2^T)^T$ and $\mathbf{z} = (\mathbf{z}_1^T, \mathbf{z}_2^T)^T$. Let N be any non-singular $(k+k') \times (k+k')$ -matrix and let

$$Q^x N = (Q'_1 + Q''_1, \dots, Q'_{k+k'} + Q''_{k+k'}),$$

where $Q'_1, \dots, Q'_{k+k'} \in \mathbf{Span}(Q^{x_1, y_1})$ and $Q''_1, \dots, Q''_{k+k'} \in \mathbf{Span}(Q^{x_2})$. Since N is a non-singular matrix, there exist $j_1, \dots, j_{k'}$ such that $\{Q''_{j_1}, \dots, Q''_{j_{k'}}\}$ is a basis for $\mathbf{Span}(Q^{x_2})$. Since $Q^{x_1, y_1} \mathbf{z}_1 \in \mathbf{DS}(0, r)$, there exist integers $t \geq s \geq 0$ and $Q'_{i_1}, \dots, Q'_{i_s}$ such that

$$\mathbf{rank}((Q'_{i_1}, \dots, Q'_{i_s}) \tilde{\mathbf{z}}_1) \geq t, \quad \mathbf{L}(Q^{x_1, y_1} \mathbf{z}_1) = k + t - s + r,$$

where $\tilde{\mathbf{z}}_1 = (z_1, \dots, z_s)^T$. Then for

$$(Q'_I + Q''_I, Q'_J + Q''_J) \stackrel{\Delta}{=} (Q'_{i_1} + Q''_{i_1}, \dots, Q'_{i_s} + Q''_{i_s}, Q'_{j_1} + Q''_{j_1}, \dots, Q'_{j_{k'}} + Q''_{j_{k'}})$$

and $\tilde{\mathbf{z}}_2 = (z_{s+r}, \dots, z_{s+k'})^T$ we have

$$\begin{aligned} \mathbf{L}((Q'_I + Q''_I) \tilde{\mathbf{z}}_1 + (Q'_J + Q''_J) \tilde{\mathbf{z}}_2) &= \mathbf{L}((Q'_I, Q'_J) \begin{bmatrix} \tilde{\mathbf{z}}_1 \\ \tilde{\mathbf{z}}_2 \end{bmatrix} + (Q''_I, Q''_J) \begin{bmatrix} \tilde{\mathbf{z}}_1 \\ \tilde{\mathbf{z}}_2 \end{bmatrix}) \\ &\geq \mathbf{rank}((Q'_I, Q'_J) \begin{bmatrix} \tilde{\mathbf{z}}_1 \\ \tilde{\mathbf{z}}_2 \end{bmatrix}) + \mathbf{L}((Q''_I, Q''_J) \begin{bmatrix} \tilde{\mathbf{z}}_1 \\ \tilde{\mathbf{z}}_2 \end{bmatrix}) \quad (\text{Lemma 2}) \end{aligned}$$

Since Q''_J is a basis for $\mathbf{Span}(Q^{x_2})$ and since $\tilde{\mathbf{z}}_1, \tilde{\mathbf{z}}_2$ are distinct vectors of indeterminates, we have

$$\geq \mathbf{rank}(Q'_I \tilde{\mathbf{z}}_1) + \mathbf{L}(Q^{x_2} \mathbf{z}_2) \geq t + \mathbf{L}(Q^{x_2} \mathbf{z}_2).$$

We have already proved that, for any nonsingular $(k+k') \times (k+k')$ -matrix N , there exist $s+k'$ entries of $Q^x N$ with rank $t + \mathbf{L}(Q^{x_2} \mathbf{z}_2)$. Now using lemma 3 and 4 we have

$$\begin{aligned} \mathbf{L}(Q^x \mathbf{z}) &= \mathbf{L}(Q^x N \mathbf{z}) \geq (k+k') + (t + \mathbf{L}(Q^{x_2} \mathbf{z}_2)) - (s+k') \\ &= k + t - s + \mathbf{L}(Q^{x_2} \mathbf{z}_2) = \mathbf{L}(Q^{x_1, y_1} \mathbf{z}_1) + \mathbf{Span}(Q^{x_2} \mathbf{z}_2) - r. \quad \square \end{aligned}$$

Proof of Theorems 2 and 3 .

Let $Q^x \mathbf{z}$, $Q^{x_1, y_1} \mathbf{z}_1$, $Q^{x_2} \mathbf{z}_2$, \mathbf{x} and \mathbf{z} be as in the proof of theorem 1. Let

$$Q^{x_1, y_1} \mathbf{z}_1 + Q^{x_2} \mathbf{z}_2 = Q^x \mathbf{z} = \sum_{i=1}^L a_i(\mathbf{z}) b_i(\mathbf{x}) c_i(\mathbf{x})$$

be any minimal quadratic algorithm for $Q^{\mathbf{x}\mathbf{z}}$ and N be any nonsingular matrix that normalizes the algorithm, *i.e*

$$Q^{\mathbf{x}}N\mathbf{z} = \sum_{j_i \in S} z_i b_{j_i}(\mathbf{x})c_{j_i}(\mathbf{x}) + \sum_{j \notin S} a_j(N\mathbf{z})b_j(\mathbf{x})c_j(\mathbf{x}),$$

where $S = \{j_1, \dots, j_{k+k'}\}$ is a subset of $\{1, \dots, \mathbf{L}\}$ and $|S| = k+k'$. If every matrix N that normalizes the algorithm does not mix $Q^{\mathbf{x}_1, \mathbf{y}_1}$ with $Q^{\mathbf{x}_2}$, then by lemma 8, $Q^{\mathbf{x}_1, \mathbf{y}_1}\mathbf{z}_1$ satisfies the EDSCS and the two theorems are proved.

Now, assume that some matrix N mixes $Q^{\mathbf{x}_1, \mathbf{y}_1}$ with $Q^{\mathbf{x}_2}$ and let

$$Q^{\mathbf{x}}N = (Q'_1 + Q''_1, \dots, Q'_{k+k'} + Q''_{k+k'}),$$

where $Q'_1, \dots, Q'_{k+k'} \in \mathbf{Span}(Q^{\mathbf{x}_1, \mathbf{y}_1})$ and $Q''_1, \dots, Q''_{k+k'} \in \mathbf{Span}(Q^{\mathbf{x}_2})$. Then there exists an entry $Q'_{j_1} + Q''_{j_1}$ of $Q^{\mathbf{x}}N$ such that $Q'_{j_1}, Q''_{j_1} \neq 0$, $Q'_{j_1} \in \mathbf{Span}(Q^{\mathbf{x}_2})$ and $Q''_{j_1} \in \mathbf{Span}(Q^{\mathbf{x}_1, \mathbf{y}_1})$. Since N is a nonsingular matrix, there exist $j_2, \dots, j_{k'}$ such that $Q''_{j_2}, \dots, Q''_{j_{k'}}$ is a basis for $\mathbf{Span}(Q^{\mathbf{x}_2})$. Since $Q^{\mathbf{x}_1, \mathbf{y}_1}\mathbf{z}_1 \in \mathbf{DS}(1, r)$, there exist integers $t \geq s \geq 1$ and $Q'_{i_1}, \dots, Q'_{i_{s-1}}$ such that

$$\mathbf{rank}((Q'_{j_1}, Q'_{i_1}, \dots, Q'_{i_{s-1}})\tilde{\mathbf{z}}_1) \geq t, \quad \mathbf{L}(Q^{\mathbf{x}_1, \mathbf{y}_1}\mathbf{z}_1) = k + t - s + r,$$

where $\tilde{\mathbf{z}}_1 = (z_1, \dots, z_s)^T$. Then for

$$(Q'_{I'} + Q''_{I'}, Q'_{J'} + Q''_{J'}) \stackrel{\Delta}{=} (Q'_{i_1} + Q''_{i_1}, \dots, Q'_{i_{s-1}} + Q''_{i_{s-1}}, Q'_{j_1} + Q''_{j_1}, \dots, Q'_{j_{k'}} + Q''_{j_{k'}})$$

we have (as in the proof of Theorem 1)

$$\mathbf{L}((Q'_{I'} + Q''_{I'})\tilde{\mathbf{z}}_1 + (Q'_{J'} + Q''_{J'})\tilde{\mathbf{z}}_2) \geq t + \mathbf{L}(Q^{\mathbf{x}_2}\mathbf{z}_2).$$

Substituting $z_i = 0$ for $i \notin I' \cup J = \{i_1, \dots, i_{s-1}, j_2, \dots, j_{k'}\}$ in the quadratic algorithm for $Q^{\mathbf{x}}N\mathbf{z}$ we obtain a quadratic algorithm for $(Q'_{I'} + Q''_{I'})\tilde{\mathbf{z}}_1 + (Q'_{J'} + Q''_{J'})\tilde{\mathbf{z}}_2$ with complexity $\mathbf{L} - (k + k' - (s + k' - 1))$. Then, by lemma 4, we have

$$\begin{aligned} \mathbf{L}(Q^{\mathbf{x}}\mathbf{z}) &= \mathbf{L}(Q^{\mathbf{x}}N\mathbf{z}) \geq (k + k') + (t + \mathbf{L}(Q^{\mathbf{x}_2}\mathbf{z}_2)) - (s + k' - 1) \\ &= k + t - s + 1 + \mathbf{L}(Q^{\mathbf{x}_2}\mathbf{z}_2) = \mathbf{L}(Q^{\mathbf{x}_1, \mathbf{y}_1}\mathbf{z}_1) + \mathbf{L}(Q^{\mathbf{x}_2}\mathbf{z}_2) - (r - 1). \end{aligned}$$

If $\mathbf{L}(Q^{\mathbf{x}_1, \mathbf{y}_1}\mathbf{z}_1) = k + t - s$, *i.e* $r = 0$, then we have a contradiction to the fact that

$$\mathbf{L}(Q^{\mathbf{x}}\mathbf{z}) = \mathbf{L}(Q^{\mathbf{x}_1, \mathbf{y}_1}\mathbf{z}_1 + Q^{\mathbf{x}_2}\mathbf{z}_2) \leq \mathbf{L}(Q^{\mathbf{x}_1, \mathbf{y}_1}\mathbf{z}_1) + \mathbf{L}(Q^{\mathbf{x}_2}\mathbf{z}_2)$$

and therefore $Q^{\mathbf{x}_1, \mathbf{y}_1}\mathbf{z}_1$ satisfies the EDSCS. On the other hand, if $\mathbf{L}(Q^{\mathbf{x}_1, \mathbf{y}_1}\mathbf{z}_1) \geq k + t - s + 1$, then the above equation is the result we need to prove. \square

In the following, $Q^{\mathbf{x}\mathbf{z}}$ is an arbitrary quadratic system.

Corollary 1 . Let $Q^{\mathbf{x},\mathbf{y}} = (Q_1)$ be a vector of a single bilinear form. Then $Q^{\mathbf{x},\mathbf{y}\mathbf{z}}$ satisfies the EDSCS.

Proof . Since $\mathbf{L} (Q^{\mathbf{x},\mathbf{y}\mathbf{z}}) = \mathbf{rank} Q^{\mathbf{x},\mathbf{y}\mathbf{z}}$, we have $Q^{\mathbf{x},\mathbf{y}\mathbf{z}} \in \mathbf{DS} (1, 0)$. \square

Corollary 2 . If $\mathbf{L} (Q^{\mathbf{x},\mathbf{y}\mathbf{z}}) = \mathbf{rank} Q^{\mathbf{x},\mathbf{y}\mathbf{z}}$ or $\mathbf{L} (Q^{\mathbf{x},\mathbf{y}\mathbf{z}}) = \mathbf{dim} Q^{\mathbf{x},\mathbf{y}}$, then $Q^{\mathbf{x},\mathbf{y}\mathbf{z}}$ satisfies the EDSCS.

Proof . If $\mathbf{L} (Q^{\mathbf{x},\mathbf{y}\mathbf{z}}) = \mathbf{rank} Q^{\mathbf{x},\mathbf{y}\mathbf{z}}$, then for every nonsingular matrix N we have $\mathbf{rank} (Q^{\mathbf{x},\mathbf{y}} N \mathbf{z}) = \mathbf{rank} (Q^{\mathbf{x},\mathbf{y}\mathbf{z}})$ and therefore $Q^{\mathbf{x},\mathbf{y}\mathbf{z}} \in \mathbf{DS} (1, 0)$. If $\mathbf{L} (Q^{\mathbf{x},\mathbf{y}\mathbf{z}}) = \mathbf{dim} Q^{\mathbf{x},\mathbf{y}}$, then for every nonsingular matrix N , any entry Q_i of $Q^{\mathbf{x},\mathbf{y}} N$ satisfies $\mathbf{rank} (Q_i z_i) \geq 1$. Therefore $Q^{\mathbf{x},\mathbf{y}\mathbf{z}} \in \mathbf{DS} (1, 0)$. \square

It follows from corollary 2 that:

Corollary 3 . If $\mathbf{L} (Q^{\mathbf{x},\mathbf{y}\mathbf{z}}) \geq \mathbf{rank} Q^{\mathbf{x},\mathbf{y}\mathbf{z}} + 1 = l$ or $\mathbf{L} (Q^{\mathbf{x},\mathbf{y}\mathbf{z}}) \geq \mathbf{dim} Q^{\mathbf{x},\mathbf{y}} + 1 = l$, then

$$\mathbf{L} (Q^{\mathbf{x},\mathbf{y}\mathbf{z}} \oplus Q^{\mathbf{x}\mathbf{z}}) \geq l + \mathbf{L} (Q^{\mathbf{x}\mathbf{z}}).$$

In particular, if $\mathbf{Span} (Q^{\mathbf{x},\mathbf{y}\mathbf{z}}) = \mathbf{rank} Q^{\mathbf{x},\mathbf{y}\mathbf{z}} + 1$ or $= \mathbf{dim} Q^{\mathbf{x},\mathbf{y}} + 1$, then $Q^{\mathbf{x},\mathbf{y}\mathbf{z}}$ satisfies the EDSC.

Let \mathbf{A} be an associative algebra of dimension k with a unit element 1 and let $\{a_1, \dots, a_k\}$ be a basis of \mathbf{A} . We denote by $Q_{\mathbf{A}}^{\mathbf{x},\mathbf{y}} = (Q_1, \dots, Q_k)$ the vector of bilinear forms defined by the product of two elements in \mathbf{A} , i.e.,

$$\sum_{i=1}^k Q_i a_i = \left[\sum_{i=1}^k x_i a_i \right] \left[\sum_{i=1}^k y_i a_i \right].$$

The result of Alder and Strassen in [AS t] states: for any quadratic system $Q^{\mathbf{x}\mathbf{z}}$ we have

$$\mathbf{L} (Q_{\mathbf{A}}^{\mathbf{x},\mathbf{y}} \mathbf{z} \oplus Q^{\mathbf{x}\mathbf{z}}) \geq 2 \mathbf{dim} \mathbf{A} - t(\mathbf{A}) + \mathbf{L} (Q^{\mathbf{x}\mathbf{z}}),$$

where $t(\mathbf{A})$ is the number of two-sided maximal ideals of \mathbf{A} . If $\mathbf{L} (Q_{\mathbf{A}}^{\mathbf{x},\mathbf{y}} \mathbf{z}) = 2 \mathbf{dim} \mathbf{A} - t(\mathbf{A})$ (respectively, $\mathbf{R} (Q_{\mathbf{A}}^{\mathbf{x},\mathbf{y}} \mathbf{z}) = 2 \mathbf{dim} \mathbf{A} - t(\mathbf{A})$), then we say that the algebra is of *minimal complexity* (respectively, *minimal rank*).

Denote the radical of \mathbf{A} , i.e the maximal (two-sided) nilpotent ideal contained in \mathbf{A} , by $\mathit{rad} \mathbf{A}$. An algebra \mathbf{A} is called *local* if $\mathbf{A} / \mathit{rad} \mathbf{A}$ is a division algebra, and is called *clean* if $\mathbf{A} / \mathit{rad} \mathbf{A}$ is a finite product of division algebras. For a direct product of division algebras $\mathbf{A} = \mathbf{A}_1 \times \dots \times \mathbf{A}_l$ we define $C_{\mathbf{A}}$ (respectively, $R_{\mathbf{A}}$) to be the number of \mathbf{A}_i which are not of minimal complexity (respectively, of minimal rank).

Our main results in the complexity of algebras are:

Corollary 4 . *Let \mathbf{A} be a division algebra. If \mathbf{A} is a simple field extension and $|F| \geq 2 \dim \mathbf{A} - 2$, then $Q_{\mathbf{A}}^{\mathbf{x},\mathbf{y}} \mathbf{z}$ satisfies the EDSCS. If \mathbf{A} is not a simple field extension or $|F| < 2 \dim \mathbf{A} - 2$, then*

$$\mathbf{L} (Q_{\mathbf{A}}^{\mathbf{x},\mathbf{y}} \mathbf{z} \oplus Q^{\mathbf{x}} \mathbf{z}) \geq 2 \dim \mathbf{A} + \mathbf{L} (Q^{\mathbf{x}} \mathbf{z}).$$

In particular, if $\mathbf{L} (Q_{\mathbf{A}}^{\mathbf{x},\mathbf{y}}) = 2 \dim \mathbf{A}$, then $Q_{\mathbf{A}}^{\mathbf{x},\mathbf{y}} \mathbf{z}$ satisfies the EDSC.

Proof . For every nonsingular matrix N each entry of $Q_{\mathbf{A}}^{\mathbf{x},\mathbf{y}} N$ has rank $k = \dim \mathbf{A}$. Therefore $Q_{\mathbf{A}}^{\mathbf{x},\mathbf{y}} \mathbf{z} \in \mathbf{DS} (1, r)$. In [Gr3], De Groote proved that $\mathbf{L} (Q_{\mathbf{A}}^{\mathbf{x},\mathbf{y}} \mathbf{z}) = 2 \dim \mathbf{A} - 1$ if and only if \mathbf{A} is a simple field extension and $|F| \geq 2 \dim \mathbf{A} - 2$. Now the claim follows immediately. \square

Remark . Corollary 4 with the results of [Fei] and [W4] classify all the minimal quadratic algorithms for $Q_{F(\alpha)/(p(\alpha))}^{\mathbf{x},\mathbf{y}} \mathbf{z}$ when $p(\alpha) = p_1(\alpha) \cdots p_k(\alpha) \in F[\alpha]$ are squarefree and $|F| \geq 2 \max_{1 \leq i \leq k} \deg p_i(\alpha) - 2$. For C_n the cyclic group of order n we have that $F[C_n]$ is isomorphic to $F[\alpha]/(\alpha^n - 1)$ and $\alpha^n - 1$ is squarefree for $\text{char } F \neq 0 \pmod{n}$.

Corollary 4 implies the following:

Corollary 5 . *Let \mathbf{A}_Q be the algebra of quaternions over the real field R and $\mathbf{A} = \prod_{i=1}^t \mathbf{A}_Q$, then*

$$\mathbf{L} (Q_{\mathbf{A}}^{\mathbf{x},\mathbf{y}} \mathbf{z} \oplus Q^{\mathbf{x}} \mathbf{z}) = 8t + \mathbf{L} (Q^{\mathbf{x}} \mathbf{z}).$$

Corollary 6 . *Let \mathbf{A} be a clean algebra. Then*

$$\mathbf{L} (Q_{\mathbf{A}}^{\mathbf{x},\mathbf{y}} \mathbf{z} \oplus Q^{\mathbf{x}} \mathbf{z}) \geq 2 \dim \mathbf{A} - C_{\mathbf{A}/\text{rad } \mathbf{A}} + \mathbf{L} (Q^{\mathbf{x}} \mathbf{z}).$$

Proof . In [ASt] it is shown that

$$\mathbf{L} (Q_{\mathbf{A}}^{\mathbf{x},\mathbf{y}} \mathbf{z} \oplus Q^{\mathbf{x}} \mathbf{z}) \geq 2 \dim \text{rad } \mathbf{A} + \mathbf{L} (Q_{\mathbf{A}/\text{rad } \mathbf{A}}^{\mathbf{x},\mathbf{y}} \mathbf{z} \oplus Q^{\mathbf{x}} \mathbf{z}).$$

Since $\mathbf{A}/\text{rad } \mathbf{A}$ is the direct sum of division algebras, from corollary 4, the result follows. \square

Corollary 7 . *Let F be a field with $\text{char } F \neq 2$. Let $Q^{\mathbf{x},\mathbf{y}} \mathbf{z}$ be the bilinear system defined by the product $\mathbf{X}\mathbf{Y}$ and $\mathbf{Y}\mathbf{X}$ of two 2×2 matrices. Then*

$$\mathbf{L} (Q^{\mathbf{x},\mathbf{y}} \mathbf{z} \oplus Q^{\mathbf{x}} \mathbf{z}) = \mathbf{L} (Q^{\mathbf{x},\mathbf{y}}) + \mathbf{L} (Q^{\mathbf{x}} \mathbf{z}).$$

Proof . It is known from [Gr2], that for fields F with $\text{char } F \neq 2$ we have $\mathbf{L} (Q^{\mathbf{x},\mathbf{y}} \mathbf{z}) \leq 9$, $\dim Q^{\mathbf{x},\mathbf{y}} = 7$ and every $Q \in \text{Span} (Q^{\mathbf{x},\mathbf{y}})$ satisfies $\text{rank } Qz = 2$. Therefore $Q^{\mathbf{x},\mathbf{y}} \mathbf{z} \in \mathbf{DS} (1, 1)$. \square

Corollary 8 . Let $Q^{x,yz}$ be the bilinear system defined by the product of two polynomials of degree n .

Then

(i) If $|F| \geq 2n$, then $Q^{x,yz}$ satisfies the EDSCS.

(ii) If $|F| < 2n \leq 2|F| + 2$, then

$$\mathbf{L}(Q^{x,yz} \Theta Q^{xz}) = 3n + 1 - \left\lfloor \frac{|F|}{2} \right\rfloor + \mathbf{L}(Q^{xz}).$$

(iii) If $|F| < n^{1/3}$, then

$$\mathbf{L}(Q^{x,yz} \Theta Q^{xz}) \geq 3n - \frac{n}{\log_{|F|} n - 3} + \mathbf{L}(Q^{xz}).$$

Proof . If $|F| \geq 2n$, then from [W3],

$$\mathbf{L}(Q^{x,yz}) = \mathbf{dim} Q^{x,y} = 2n - 1.$$

Using corollary 2, (i) follows. Then (ii) and (iii) follow from [ABK] and [KB, Lemma 4 and 5]. \square

6. DIRECT SUM OF $\mathbf{DS}(0, r)$.

In this section we define a subclass of $\mathbf{DS}(0, r)$ and prove that all quadratic systems in this subclass satisfy the EDSCS. This subclass contains $Q_{F[\alpha]^{1/(p(\alpha))}}^{x,y}z$ for any polynomial $p(\alpha) \in F[\alpha]$. We recall that the bilinear form $Q^{x,yz}$ is in $\mathbf{DS}(0, r)$ if there exist integers $t \geq s$ such that

(i) For every basis $\{Q_1, \dots, Q_k\}$ of the linear space $\mathbf{Span}(Q^{x,y})$ there exist Q_{j_1}, \dots, Q_{j_s} , $1 \leq j_i \leq k$, $i = 1, \dots, s$, such that

$$\mathbf{rank}((Q_{j_1}, \dots, Q_{j_s})\tilde{\mathbf{z}}) \geq t,$$

where $\tilde{\mathbf{z}} = (z_1, \dots, z_s)^T$, and

(ii)

$$\mathbf{L}(Q^{x,yz}) = \mathbf{dim} Q^{x,y} + t - s + r.$$

Throughout this section the integers s and t are the integers in (i) and (ii). When we wish to emphasize the dependence on s and t , we write $\mathbf{DS}_{s,t}(0, r)$. Similarly for other subclasses defined later.

Definition 3 . Let $Q^{x,yz} = \sum_{i=1}^k Q_i z_i$ be a bilinear system, where $Q^{x,yz} \in \mathbf{DS}(0, r)$. We say that

$Q'_{i_1} \in \mathbf{Span}(Q^{x,y})$ is active if, for every nonsingular $k \times k$ -matrix N , whenever Q'_{i_1} is one of the entries of $Q^{x,y}N = (Q'_{i_1}, \dots, Q'_{i_k})$, there exist $s-1$ entries $Q'_{i_2}, \dots, Q'_{i_s}$ of $Q^{x,y}N$, $1 \leq i_j \leq k$,

$j = 1, \dots, s$, such that

$$\mathbf{rank} ((Q_{i_1}, \dots, Q_{i_s}) \tilde{\mathbf{z}}) \geq t.$$

where $\tilde{\mathbf{z}} = (z_1, \dots, z_s)^T$.

Definition 4 . Let $\mathbf{DS}^*(r)$ denote the collection of bilinear systems $Q^{\mathbf{x},\mathbf{y}}\mathbf{z}$ in $\mathbf{DS}(0, r)$ such that:

(i) For any nonsingular matrix N there exists an active entry Q'_{i_1} , $1 \leq i_1 \leq k$, of $Q^{\mathbf{x},\mathbf{y}}N = (Q'_{i_1}, \dots, Q'_{i_k})$ such that, for every non-active entry Q'_{i_2} , $1 \leq i_2 \leq k$, of $Q^{\mathbf{x},\mathbf{y}}N$ and every $f_1, f_2 \in F$, $f_1 \neq 0$, we have that $f_1 Q'_{i_1} + f_2 Q'_{i_2}$ is also active.

(ii) For every nonsingular matrix N there exist s active entries $Q'_{i_1}, \dots, Q'_{i_s}$ of $Q^{\mathbf{x},\mathbf{y}}N$ such that

$$\mathbf{rank} ((Q'_{i_1}, \dots, Q'_{i_s}) \tilde{\mathbf{z}}) \geq t,$$

where $\tilde{\mathbf{z}} = (z_1, \dots, z_s)^T$.

Remark . Definitions 3 and 4 are equivalent to definitions II and III in the introduction.

It follows at once from definition 4 that the set of all nonactive bilinear forms is a sublinear space of $\mathbf{Span}(Q^{\mathbf{x},\mathbf{y}})$. Therefore, definition 4 is equivalent to the following:

There exists a subspace L' of $\mathbf{Span}(Q^{\mathbf{x},\mathbf{y}})$ such that: for any basis $\{Q_1, \dots, Q_k\}$ of $\mathbf{Span}(Q^{\mathbf{x},\mathbf{y}})$ there exist $Q_{i_1}, Q_{i_2}, \dots, Q_{i_s} \in \mathbf{Span}(Q^{\mathbf{x},\mathbf{y}}) - L'$, $1 \leq i_j \leq k$, $1 \leq j \leq s$, with

$$\mathbf{rank} ((Q_{i_1}, \dots, Q_{i_s}) \tilde{\mathbf{z}}) \geq t,$$

where $\tilde{\mathbf{z}} = (z_1, \dots, z_s)^T$.

In fact, L' is the set of all nonactive bilinear forms and $\mathbf{Span}(Q^{\mathbf{x},\mathbf{y}}) - L'$ is the set of all active bilinear forms.

When $s = 1$ an equivalent definition of $\mathbf{DS}_{1,t}^*(r)$ is given in the following

Lemma 9 . We have

$$\mathbf{DS}_{1,t}^*(r) = \mathbf{DS}_{1,t}(0, r).$$

Proof . We recall that if $Q^{\mathbf{x},\mathbf{y}}\mathbf{z} \in \mathbf{DS}_{1,t}(0, r)$ (with $s = 1$), then for every nonsingular matrix N there exists an entry Q_i of $Q^{\mathbf{x},\mathbf{y}}N$ such that $\mathbf{rank} Q_i z_1 \geq t$. Hence any active bilinear form is $Q_j \in \mathbf{Span}(Q^{\mathbf{x},\mathbf{y}})$ with $\mathbf{rank} Q_j z_1 \geq t$ (and any non-active bilinear form is $Q_j \in \mathbf{Span}(Q^{\mathbf{x},\mathbf{y}})$ with

rank $Q_j z_1 < t$).

Assume, toward contradiction, that for some nonsingular matrix N , and for every active entry Q'_i of $Q^{x,y}N$, there exists a non-active entry $Q'_{j(i)}$ in $Q^{x,y}N$ and $f_{j_1(i)}, f_{j_2(i)} \in F, f_{j_1(i)} \neq 0$ such that

$$(f_{j_1(i)}Q'_i + f_{j_2(i)}Q'_{j(i)}) \text{ is not active.} \quad (5)$$

Let $I = \{ i \mid Q'_i \text{ is active} \}$ and let N' be a $k \times k$ -matrix such that $Q^{x,y}N N' = (Q''_1, \dots, Q''_k)$,

where

$$Q''_i = \begin{cases} Q'_i & i \notin I, \\ Q'_i + (f_{j_2(i)}/f_{j_1(i)})Q'_{j(i)} & i \in I. \end{cases}$$

Since $j(i) \notin I$, we have $\{Q''_1, \dots, Q''_k\}$ is a basis for **Span** $(Q^{x,y})$ and therefore N' is nonsingular.

Now, $N N'$ is nonsingular; $Q''_i = Q'_i, i \notin I$, is not active; and by (5), $Q''_i, i \in I$, is also not active.

This is a contradiction to the fact that $Q^{x,y}z \in \mathbf{DS}_{1,t}(r)$, since it must be at least one active bilinear form in $Q^{x,y}N N'$. \square

In this section we prove the following:

Theorem 4. *If $Q^{x,y}z \in \mathbf{DS}^*(0)$, then $Q^{x,y}z$ satisfies the EDSCS.*

Theorem 5. *If $Q^{x,y}z \in \mathbf{DS}^*(r), r \geq 1$, then for any quadratic system $Q^x z$ we have*

$$\mathbf{L}(Q^{x,y}z \oplus Q^x z) \geq \mathbf{L}(Q^{x,y}z) + \mathbf{L}(Q^x z) - (r - 1).$$

In particular, if $r = 1$, then $Q^{x,y}z$ satisfies the EDSC.

Proof of Theorems 4 and 5.

Let $Q^{x_1, y_1} z_1 = Q_1 z_1 + \dots + Q_k z_k$ be a bilinear system in $\mathbf{DS}^*(r)$ and let $Q^{x_2} z_2 = Q_{k+1} z_{k+1} + \dots + Q_{k+k'} z_{k+k'}$ be an arbitrary quadratic system. Set $Q^x = (Q^{x_1, y_1}, Q^{x_2})$, $z = (z_1^T, z_2^T)^T$ and $x = (x_1^T, y_1^T, x_2^T)^T$. Let

$$Q^{x_1, y_1} z_1 + Q^{x_2} z_2 = Q^x z = \sum_{i=1}^L a_i(z) b_i(x) c_i(x)$$

be a minimal quadratic algorithm for $Q^x z$. If for any nonsingular $(k+k') \times (k+k')$ -matrix N that normalizes the minimal algorithm, that is, (without loss of generality)

$$Q^x N z = \sum_{i=1}^{k+k'} z_i b_i(x) c_i(x) + \sum_{i=k+k'+1}^L a_i(N z) b_i(x) c_i(x), \quad (6)$$

the matrix N does not mix Q^{x_1, y_1} with Q^{x_2} , then, by lemma 8 the the algorithm is seperable and the two theorems are proved. Assume, therefore, that there exists a nonsingular $(k+k') \times (k+k')$ matrix N that normalizes the minimal algorithm (*i.e* satisfies (6)) and mixes Q^{x_1, y_1} with Q^{x_2} . We shall prove that

$$\mathbf{L} (Q^{\mathbf{x}\mathbf{z}}) \geq \mathbf{L} (Q^{x_1, y_1} \mathbf{z}_1) + \mathbf{L} (Q^{x_2} \mathbf{z}_2) + (r-1). \quad (*)$$

For, if $Q^{x_1, y_1} \mathbf{z}_1 \in \mathbf{DS}^* (r)$, $r \geq 1$, then Theorem 5 follows, and if $Q^{x_1, y_1} \mathbf{z}_1 \in \mathbf{DS}^* (0)$, then we have a contradiction and Theorem 4 follows.

Let

$$Q^{\mathbf{x}} N = (Q'_1 + Q''_1, \dots, Q'_{k+k'} + Q''_{k+k'}),$$

where $Q'_i \in \mathbf{Span} (Q^{x_1, y_1})$ and $Q''_i \in \mathbf{Span} (Q^{x_2})$, $i = 1, \dots, k+k'$. Since $Q^{x_1, y_1} \mathbf{z} \in \mathbf{DS}^* (r)$, there exists $Q'_i + Q''_i$ in $Q^{\mathbf{x}} N$ such that Q'_i is active. Let

$$Z_1 = \{ w \mid Q'_w \text{ is active} \}$$

and define

$$Z_i = \{ w \mid \text{there exists } a_r (N \mathbf{z}), r > k+k', \\ \text{that depends on some } z_p \text{ with } p \in Z_{j-1}, \text{ and on } z_w \}.$$

Obviously, Z_i is a subset of Z_{i+1} . Let Z_l be the first set that satisfies $Z_l = Z_{l+1}$ (Obviously, $Z_{l+1} = Z_{l+2} = \dots$). We now distinguish between two cases:

Case I. There exists $i' \in Z_l$ such that $Q''_{i'} \neq 0$.

Let p be the smallest integer that satisfies: there exists $i' \in Z_p$ such that $Q''_{i'} \neq 0$. By the definition of Z_i , we can find a sequence $i_1, i_2, \dots, i_p = i'$ of length p such that $Q''_{i_j} = 0$, $1 \leq j < p$, $Q''_{i_p} \neq 0$, $i_q \in Z_q - Z_{q-1}$, $q = 2, \dots, p$ and $i_1 \in Z_1$. We now proceed with the proof of (*) by induction on p .

If $i_1 = i_p$ *i.e.* $Q''_{i_1} \neq 0$, then since Q'_{i_1} is active, we have

$$\mathbf{L} (Q^{\mathbf{x}\mathbf{z}}) \geq k + t - s + 1 + \mathbf{L} (Q^{x_2} \mathbf{z}_2) = \mathbf{L} (Q^{x_1, y_1} \mathbf{z}_1) + \mathbf{L} (Q^{x_2} \mathbf{z}_2) + (r-1).$$

(exactly as in the proof of theorem 2 and 3).

Suppose $p > 1$. Because p is the minimal integer such that $Q''_{i_p} \neq 0$ we have $Q''_{i_1} = \dots = Q''_{i_{p-1}} = 0$, and by the definition of Z_1 we have that $Q'_{i_2}, \dots, Q'_{i_p}$ are not active. By the definition of Z_q and p , there exists $a_{r_0} (N \mathbf{z})$ that depends on z_{i_1} and z_{i_2} and does not depend on z_{i_3}, \dots, z_{i_p} . *i.e.*

$a_{r_0}(N \mathbf{z}) = \lambda z_{i_2} + \delta z_{i_1} + \tilde{a}(\mathbf{z})$ where $\lambda, \delta \neq 0$ and $\tilde{a}(\mathbf{z})$ does not depend on z_{i_1}, \dots, z_{i_p} . By substituting

$$\frac{1}{\lambda} (z_{i_2} - \delta z_{i_1} - \tilde{a}(\mathbf{z}))$$

for z_{i_2} in (6), we obtain

$$\begin{aligned} Q N N' \mathbf{z} &= \sum_{\substack{i=1 \\ i \neq i_2}}^{k+k'} z_i b_i(\mathbf{x}) c_i(\mathbf{x}) + z_{i_2} b_{r_0}(\mathbf{x}) c_{r_0}(\mathbf{x}) \\ &+ \sum_{\substack{i=k+k' \\ i \neq r_0}}^{\mathbf{1}} a_i(N N' \mathbf{z}) b_i(\mathbf{x}) c_i(\mathbf{x}) + \frac{1}{\lambda} (z_{i_2} - \delta z_{i_1} - \tilde{a}(\mathbf{z})) b_{i_2}(\mathbf{x}) c_{i_2}(\mathbf{x}). \end{aligned}$$

Here the i_2 entry of $Q N N'$ is now

$$Q'_{i_1} - \frac{\delta}{\lambda} Q'_{i_2} - \frac{\delta}{\lambda} Q''_{i_2},$$

and the i_p, \dots, i_3 entries remain $Q'_{i_p}, \dots, Q'_{i_3}$, respectively. Since Q'_{i_1} is active and Q'_{i_2} is not active,

we have that $Q'_{i_1} - \frac{\delta}{\lambda} Q'_{i_2} \in \mathbf{Span}(Q^{\mathbf{x}_1, \mathbf{y}_1})$ is active. Note also that, there exists $a_i(N N' \mathbf{z})$ that

depends on z_{i_1} and z_{i_3} . (Actually, if $a_i(N \mathbf{z})$ depends on z_{i_2} and z_{i_3} , then $a_i(N N' \mathbf{z})$ depends on z_{i_1} and

z_{i_3}). The terms $a_i(N \mathbf{z})$ that depend on $z_j, j \in Z_1 - Z_2$ satisfies $a_i(N N' \mathbf{z}) = a_i(N \mathbf{z})$. So we have that

NN' normalizes the minimal algorithm, and now the new sequence i_1, i_3, \dots, i_p satisfies the above con-

ditions with the new sets $Z_1 \cup Z_2, Z_3, \dots, Z_p$. Assuming that (*) holds for $p - 1$, it follows that it holds

for p . This accomplishes the proof for this case.

Case II. For each $i \in Z_l$, we have $Q''_i = 0$. That is, each $a_i(N \mathbf{z})$ depends on $(z_q)_{q \in Z_l}$ or $(z_q)_{q \notin Z_l}$, but not both.

Let

$$P = \{i \mid a_i(N \mathbf{z}) \text{ is dependent on } (z_q)_{q \in Z_l}\}.$$

We now estimate the number of the terms $a_i(N \mathbf{z})$ that depend on $(z_q)_{q \in Z_l}$. Substituting $z_q = 0$ for all

$q \notin Z_l$ in the minimal algorithm, we obtain the algorithm

$$\sum_{i \in Z_l} z_i b_i(\mathbf{x}) c_i(\mathbf{x}) + \sum_{i \in P} a_i(N \mathbf{z}) b_i(\mathbf{x}) c_i(\mathbf{x}),$$

with complexity $|Z_p| + |P|$, that computes some bilinear system $\tilde{Q} \mathbf{z}$. The entries of \tilde{Q} are from

$\mathbf{Span}(Q^{\mathbf{x}_1, \mathbf{y}_1})$ because $Q''_i = 0$ for $i \in Z_l$. Since all the active entries are Q'_i with $i \in Z_1 \subseteq Z_l$, by

condition (ii) in Definition 5, there exist s active entries $Q'_{j_1}, \dots, Q'_{j_s}, \{j_1, \dots, j_s\} \in Z_1$ such that

rank $(Q'_{j_1}, \dots, Q'_{j_s}) \tilde{\mathbf{z}} \geq t$. Therefore, by lemma 3 we have

$$|Z_l| + |P| = \mathbf{L}(Q\tilde{\mathbf{z}}) \geq |Z_l| + t - s. \quad (7)$$

Let $P^C = \{k+k'+1, \dots, \mathbf{L}\} - P$ and $Z_l^C = \{1, \dots, k+k'\} - Z_l$. Now substituting $z_q = 0$, $q \in Z_l$, in the quadratic algorithm, we obtain

$$\sum_{i \notin Z_l} z_i b_i(\mathbf{x}) c_i(\mathbf{x}) + \sum_{i \in P} a_i(N\mathbf{z}) b_i(\mathbf{x}) c_i(\mathbf{x}). \quad (**)$$

Since $Q''_i = 0$ for $i \in Z_l$, the above algorithm computes $(Q^{x_1, y_1}, Q^{x_2}) M \tilde{\mathbf{z}}$ for some nonsingular matrix M , $\mathbf{Span}(Q^{x_1, y_1}) \subseteq \mathbf{Span}(Q^{x_1, y_1})$, $\tilde{\mathbf{z}} = (z_{r_1}, \dots, z_{r_w})^T$, $w = k+k' - |Z_l|$ and $\{r_1, \dots, r_w\} = Z_l^C$. If

$$\mathbf{L}(Q^{x_1, y_1} \tilde{\mathbf{z}}_1) \geq \dim \mathbf{Span}(Q^{x_1, y_1}) + 1 = k - |Z_l| + 1,$$

or if the algorithm in (**) is not minimal, then by corollary 3 we have

$$|Z_l^C| + |P^C| \geq \mathbf{L}(Q^{x_2} \mathbf{z}_2) + k - |Z_l| + 1. \quad (8)$$

Combining this with (7) we have

$$\begin{aligned} \mathbf{L}(Q^{\mathbf{xz}}) = \mathbf{L} &= |Z_l| + |Z_l^C| + |P| + |P^C| \geq \\ \mathbf{L}(Q^{x_2} \mathbf{z}_2) + k + t - s + 1 &= \mathbf{L}(Q^{x_1, y_1} \tilde{\mathbf{z}}_1) + \mathbf{L}(Q^{x_2} \mathbf{z}_2) + (r-1). \end{aligned}$$

Therefore, $\mathbf{L}(Q^{x_1, y_1} \tilde{\mathbf{z}}_1) = \dim \mathbf{Span}(Q^{x_1, y_1})$, and the algorithm in (**) is minimal. Then, by corollary 1, this algorithm is separable, and therefore so is the algorithm in (6). This contradicts the assumption that N mixes Q^{x_1, y_1} with Q^{x_2} . \square

Theorem 4 and 5 give the following results:

Corollary 9 . Let $\mathbf{A} = F[\alpha]/(p(\alpha))$ where $p(\alpha) = p_1(\alpha)^{d_1} \cdots p_k(\alpha)^{d_k}$ and $p_1(\alpha), \dots, p_k(\alpha)$ are distinct irreducible polynomials. Let $d = \max_{1 \leq i \leq k} \deg p_i(\alpha)^{d_i}$.

(i) If $|F| \geq 2d - 2$, then $Q_{\mathbf{A}}^{\mathbf{xy}} \mathbf{z}$ satisfies the EDSCS.

(ii) If $|F| < 2d - 2$, then for every quadratic system $Q^{\mathbf{xz}}$ we have

$$\mathbf{L}(Q_{\mathbf{A}}^{\mathbf{xy}} \mathbf{z} \oplus Q^{\mathbf{xz}}) \geq 2 \deg p(\alpha) - k + s_p + \mathbf{L}(Q^{\mathbf{xz}}),$$

where s_p is the number of $p_i(\alpha)$ that satisfy $|F| < 2 \deg p_i(\alpha) - 2$.

Proof . Since

$$F[\alpha]/(p(\alpha)) \equiv F[\alpha]/(p_1(\alpha)^{d_1}) \times \cdots \times F[\alpha]/(p_k(\alpha)^{d_k}),$$

it is enough to prove the theorem for the algebra $\mathbf{A}_1 = F[\alpha]/(p_1(\alpha)^{d_1})$. In [W3], Winograd proved that for every nonsingular matrix N there exists an entry Q'_i of $Q_{\mathbf{A}_1}^{\mathbf{x},\mathbf{y}} N$ with $\mathbf{rank}(Q'_i z_i) = \deg p_1(\alpha)^{d_1}$. In [FZ], Feduccia and Zalcstein proved that if $|F| \geq 2 \deg p_1(\alpha)^{d_1} - 2$, then $\mathbf{L}(Q_{\mathbf{A}_1}^{\mathbf{x},\mathbf{y}} \mathbf{z}) \leq 2 \deg p_1(\alpha)^{d_1} - 1$. Combining both results we get that $Q_{\mathbf{A}_1}^{\mathbf{x},\mathbf{y}} \in \mathbf{DS}^*(0)$ and (i) follows.

In [ASt] Alder and Strassen proved that $\mathbf{L}(Q_{\mathbf{A}_1}^{\mathbf{x},\mathbf{y}} \mathbf{z}) \geq 2 \deg p_1(\alpha)^{d_1-1} + \mathbf{L}(Q_{\mathbf{A}_1}^{\mathbf{x},\mathbf{y}} \mathbf{z})$, where $\overline{\mathbf{A}}_1 = F[\alpha]/(p_1(\alpha))$. If $|F| < 2 \deg p_1(\alpha) - 2$, then the results of Winograd in [W4] and De Groote in [Gr3] show that $\mathbf{L}(Q_{\overline{\mathbf{A}}_1}^{\mathbf{x},\mathbf{y}} \mathbf{z}) \geq 2 \deg p_1(\alpha)$, and therefore $\mathbf{L}(Q_{\mathbf{A}_1}^{\mathbf{x},\mathbf{y}} \mathbf{z}) \geq 2 \deg p_1(\alpha)^{d_1}$, which implies (ii). \square

Remark . Corollary 9 shows that to obtain the classification of all minimal quadratic algorithms for $F[\alpha]/(p(\alpha))$ for any polynomial $p(\alpha)$, it suffices to classify all minimal quadratic algorithms for $F[\alpha]/(p_1(\alpha)^{d_1})$ for an irreducible polynomial $p_1(\alpha)$. It is known from [Am] that minimal quadratic algorithms for $F[\alpha]/(p_1(\alpha)^{d_1})$ are not necessary bilinear. The classification of all minimal bilinear algorithms for $F[\alpha]/(p(\alpha))$, for any $p(\alpha)$, is completely studied in [AGW1], [AGW2], [Fel] and [FW].

Corollary 10 . *Let $Q^{\mathbf{x},\mathbf{y}}\mathbf{z}$ be a bilinear system. Then*

- (i) *If $\mathbf{L}(Q^{\mathbf{x},\mathbf{y}}\mathbf{z}) = \mathbf{dim} Q^{\mathbf{x},\mathbf{y}} + 1$, then $Q^{\mathbf{x},\mathbf{y}}\mathbf{z}$ satisfies the EDSCS.*
- (ii) *If $\mathbf{L}(Q^{\mathbf{x},\mathbf{y}}\mathbf{z}) = \mathbf{dim} Q^{\mathbf{x},\mathbf{y}} + 2$, then $Q^{\mathbf{x},\mathbf{y}}\mathbf{z}$ satisfies the EDSC.*
- (iii) *If $\mathbf{L}(Q^{\mathbf{x},\mathbf{y}}\mathbf{z}) \geq \mathbf{dim} Q^{\mathbf{x},\mathbf{y}} + 2$, then for every quadratic system $Q^{\mathbf{x}}\mathbf{z}$ we have*

$$\mathbf{L}(Q^{\mathbf{x},\mathbf{y}}\mathbf{z} \oplus Q^{\mathbf{x}}\mathbf{z}) \geq \mathbf{dim} Q^{\mathbf{x},\mathbf{y}} + 2 + \mathbf{L}(Q^{\mathbf{x}}\mathbf{z}).$$

Proof . If for some nonsingular matrix N , all the entries Q_i of $Q^{\mathbf{x},\mathbf{y}}N$ satisfy $\mathbf{rank} Q_i z_i = 1$, then it is well known that, $\mathbf{L}(Q^{\mathbf{x},\mathbf{y}}) = \mathbf{dim} Q^{\mathbf{x},\mathbf{y}}$. Therefore, for every nonsingular matrix N , there exists an entry Q'_i of $Q^{\mathbf{x},\mathbf{y}}N$ with $\mathbf{rank} Q'_i z_i \geq 2$. This, combined with lemma 9, proves the corollary. \square

An immediate generalization is:

Corollary 11 . Let $Q^{\mathbf{x},\mathbf{y}}\mathbf{z}$ be a bilinear system. If for every basis $\{Q'_1, \dots, Q'_k\}$ for $\mathbf{Span}(Q^{\mathbf{x},\mathbf{y}})$ there exists Q'_i such that $\mathbf{rank} Q'_i z_i \geq t$, then

- (i) If $\mathbf{L}(Q^{\mathbf{x},\mathbf{y}}\mathbf{z}) = k + t - 1$, then $Q^{\mathbf{x},\mathbf{y}}\mathbf{z}$ satisfies the EDSCS.
- (ii) If $\mathbf{L}(Q^{\mathbf{x},\mathbf{y}}\mathbf{z}) = k + t$, then $Q^{\mathbf{x},\mathbf{y}}\mathbf{z}$ satisfies the EDSC.
- (iii) If $\mathbf{L}(Q^{\mathbf{x},\mathbf{y}}\mathbf{z}) \geq k + t$, then for every quadratic system $Q^{\mathbf{x}}\mathbf{z}$ we have

$$\mathbf{L}(Q^{\mathbf{x},\mathbf{y}}\mathbf{z} \oplus Q^{\mathbf{x}}\mathbf{z}) \geq k + t + \mathbf{L}(Q^{\mathbf{x}}\mathbf{z}).$$

In particular we have

Corollary 12 . Let $F = C$, the complex field and let $\mathbf{A} = \{A_1, \dots, A_k\}$ be any set of $n \times m$ matrices where $n, m \leq 3$. Define the bilinear system $Q(\mathbf{A}) = (\mathbf{x}^T A_1 \mathbf{y}, \dots, \mathbf{x}^T A_k \mathbf{y})$. Then $Q(\mathbf{A})\mathbf{z}$ satisfies the EDSC.

Proof . Following [AS] we have $\mathbf{L}(Q(\mathbf{A})\mathbf{z}) \leq \mathbf{dim} Q(\mathbf{A}) + 2$ or $\mathbf{L}(Q(\mathbf{A})\mathbf{z}) \leq \mathbf{rank} Q(\mathbf{A})\mathbf{z} + 1$. \square

Remark . Corollary 12 can be applied to bilinear systems defined by the cross product of $(x_1, x_2, x_3)^T$ and $(y_1, y_2, y_3)^T$, (see [DL]); to the product of two elements in the Lie algebra of 2×2 -matrices, (see [Mi] and [GH2]); and to $Q_{\mathbf{A}}^{\mathbf{x},\mathbf{y}}$ where \mathbf{A} is an algebra of $\mathbf{dim} \mathbf{A} \leq 3$. Actually, the first two systems are in $\mathbf{DS}(1, 1)$ for any field F .

Corollary 13 . Let \mathbf{A}_i be a set of $m \times n - i$, $m \times n$ -matrices. If $0 \leq i \leq 3$, then $Q(\mathbf{A}_i)$ satisfies the EDSCS, and if $4 \leq i \leq 5$, then $Q(\mathbf{A}_i)$ satisfies the EDSC.

Proof . Following [AS, Theorem 2], [AL2], [B2] and [Gat2], we have $\mathbf{L}(Q(\mathbf{A}_i)\mathbf{z}) \leq \mathbf{dim} Q(\mathbf{A}_i) + 1$ for $0 \leq i \leq 3$, and $\mathbf{L}(Q(\mathbf{A}_i)\mathbf{z}) \leq \mathbf{dim} Q(\mathbf{A}_i) + 2$, for $4 \leq i \leq 5$. \square

Corollary 13 was first proved by Ja'ja' and Takche in [JT1], for bilinear algorithms for the case of $i = 1$.

Corollary 14 . Let $F = R$, the real field. Let $Q^{\mathbf{x},\mathbf{y}}\mathbf{z}$ be the bilinear system defined by the product $\mathbf{X}\mathbf{Y}$ and $\mathbf{Y}\mathbf{X}$ of the two quaternions \mathbf{X} and \mathbf{Y} . Then $Q^{\mathbf{x},\mathbf{y}}\mathbf{z}$ satisfies the EDSCS.

Proof . Following [Gr1], we have $\mathbf{L} (Q^{\mathbf{x},\mathbf{y}}\mathbf{z}) = 10$, $\mathbf{dim} Q^{\mathbf{x},\mathbf{y}} = 7$ and, for every nonsingular matrix N there exists an entry Q_i of $Q^{\mathbf{x},\mathbf{y}}N$ satisfying $\mathbf{rank} Q_i z_i = 4$. Therefore $Q^{\mathbf{x},\mathbf{y}}\mathbf{z} \in \mathbf{DS}^*(0)$ and the result follows. \square

7. BILINEAR ALGORITHMS

In this section we introduce some notation and prove Theorem 6.

Let $\mathbf{x}_n = (x_1, \dots, x_n)^T$, $\mathbf{y}_m = (y_1, \dots, y_m)^T$ and $\mathbf{z}_k = (z_1, \dots, z_k)^T$ be vectors of indeterminates. Throughout this section the subscripts n , m and k in \mathbf{x}_n , \mathbf{y}_m and \mathbf{z}_k will always denote the length of the vector. For a vector of $n \times m$ -matrices $Q = (A_1, \dots, A_k)$ we shall denote by $(\mathbf{x}_n^T Q \mathbf{y}_m) \mathbf{z}_k$ the bilinear system defined by Q , that is, $(\mathbf{x}_n^T A_1 \mathbf{y}_m, \dots, \mathbf{x}_n^T A_k \mathbf{y}_m) \mathbf{z}_k$. A *bilinear algorithm* that computes the bilinear system $(\mathbf{x}_n^T Q \mathbf{y}_m) \mathbf{z}_k$ with $\mathbf{rank} \mathbf{R}$ is

$$(\mathbf{x}_n^T Q \mathbf{y}_m) \mathbf{z}_k = \sum_{i=1}^{\mathbf{R}} a_i(\mathbf{z}_k) b_i(\mathbf{x}_n) c_i(\mathbf{y}_m), \quad (9)$$

where a_i , b_i and c_i are linear forms of the corresponding variables. The minimal integer \mathbf{R} in which equation (9) hold will be denoted by $\mathbf{R}((\mathbf{x}_n^T Q \mathbf{y}_m) \mathbf{z}_k)$ and will be called the *bilinear complexity* of $(\mathbf{x}_n^T Q \mathbf{y}_m) \mathbf{z}_k$. In [J1] it was shown that

$$\mathbf{L}((\mathbf{x}_n^T Q \mathbf{y}_m) \mathbf{z}_k) \leq \mathbf{R}((\mathbf{x}_n^T Q \mathbf{y}_m) \mathbf{z}_k) < 2 \mathbf{L}((\mathbf{x}_n^T Q \mathbf{y}_m) \mathbf{z}_k).$$

If for any bilinear system $(\mathbf{x}_n^T Q' \mathbf{y}_{m'}) \mathbf{z}_{k'}$,

$$\mathbf{R}((\mathbf{x}_n^T Q \mathbf{y}_m) \mathbf{z}_k \Theta (\mathbf{x}_n^T Q' \mathbf{y}_{m'}) \mathbf{z}_{k'}) = \mathbf{R}((\mathbf{x}_n^T Q \mathbf{y}_m) \mathbf{z}_k) + \mathbf{R}((\mathbf{x}_n^T Q' \mathbf{y}_{m'}) \mathbf{z}_{k'}),$$

then we say that $(\mathbf{x}_n^T Q \mathbf{y}_m) \mathbf{z}_k$ satisfies the *direct sum conjecture* (in short DSC). If each minimal bilinear algorithm for $(\mathbf{x}_n^T Q \mathbf{y}_m) \mathbf{z}_k \Theta (\mathbf{x}_n^T Q' \mathbf{y}_{m'}) \mathbf{z}_{k'}$ is separable, then we say that $(\mathbf{x}_n^T Q \mathbf{y}_m) \mathbf{z}_k$ satisfies the *direct sum conjecture strongly* (in short DSCS).

The *D-dual* and *T-dual* systems of $(\mathbf{x}_n^T Q \mathbf{y}_m) \mathbf{z}_k$ are $(\mathbf{x}_n^T Q^D \mathbf{y}_k) \mathbf{z}_m$ and $(\mathbf{x}_m^T Q^T \mathbf{y}_n) \mathbf{z}_k$, respectively, where

$$(\mathbf{x}_n^T Q \mathbf{y}_m) \mathbf{z}_k = (\mathbf{x}_n^T Q^D \mathbf{z}_k) \mathbf{y}_m = (\mathbf{y}_m^T Q^T \mathbf{x}_n) \mathbf{z}_k.$$

This means that, if $Q = (A_1, \dots, A_k)$, where A_i are $n \times m$ -matrices, then $Q^T = (A_1^T, \dots, A_k^T)$ and $Q^D = (B_1, \dots, B_m)$, where $B_i = [A_1 e_i \mid \dots \mid A_k e_i]$ and e_i is the i -th column vector of unity of order n . It follows immediately from the above definitions that $Q^{DD} = Q^{TT} = Q$ and

$$\mathbf{R}((\mathbf{x}_n^T Q \mathbf{y}_m) \mathbf{z}_k) = \mathbf{R}((\mathbf{x}_n^T Q^D \mathbf{y}_k) \mathbf{z}_m) = \mathbf{R}((\mathbf{x}_m^T Q^T \mathbf{y}_n) \mathbf{z}_k). \quad (10)$$

(for details see [HM])

Our main result in this section is given in the following.

Theorem 6. *Let $(\mathbf{x}_n^T Q \mathbf{y}_m) \mathbf{z}_k$ be a bilinear system. Then*

(i) *If $(\mathbf{x}_n^T Q \mathbf{y}_m) \mathbf{z}_k$ satisfies the DSCS (DSC), then, so do the dual systems $(\mathbf{x}_n^T Q^D \mathbf{y}_k) \mathbf{z}_m$ and $(\mathbf{x}_m^T Q^T \mathbf{y}_n) \mathbf{z}_k$.*

(ii) *Suppose that for any bilinear system $(\mathbf{x}_n^T Q' \mathbf{y}_{m'}) \mathbf{z}_{k'}$ we have*

$$\mathbf{R}((\mathbf{x}_n^T Q \mathbf{y}_m) \mathbf{z}_k \ominus (\mathbf{x}_n^T Q' \mathbf{y}_{m'}) \mathbf{z}_{k'}) \geq c + \mathbf{R}((\mathbf{x}_n^T Q' \mathbf{y}_{m'}) \mathbf{z}_{k'}).$$

Then, for any bilinear systems $(\mathbf{x}_n^T Q_1 \mathbf{y}_{m'}) \mathbf{z}_{k'}$ and $(\mathbf{x}_n^T Q_2 \mathbf{y}_{m'}) \mathbf{z}_{k'}$ we have

$$\mathbf{R}((\mathbf{x}_n^T Q^D \mathbf{y}_k) \mathbf{z}_m \ominus (\mathbf{x}_n^T Q_1 \mathbf{y}_{m'}) \mathbf{z}_{k'}) \geq c + \mathbf{R}((\mathbf{x}_n^T Q_1 \mathbf{y}_{m'}) \mathbf{z}_{k'}),$$

$$\mathbf{R}((\mathbf{x}_m^T Q^T \mathbf{y}_n) \mathbf{z}_k \ominus (\mathbf{x}_n^T Q_2 \mathbf{y}_{m'}) \mathbf{z}_{k'}) \geq c + \mathbf{R}((\mathbf{x}_n^T Q_2 \mathbf{y}_{m'}) \mathbf{z}_{k'}).$$

Proof. Suppose that $(\mathbf{x}_n^T Q \mathbf{y}_m) \mathbf{z}_k$ does not satisfy the DSCS. Then, by lemma 6, there exists a bilinear system $(\mathbf{x}'_n{}^T Q' \mathbf{y}'_{k'}) \mathbf{z}'_{m'}$ and a minimal bilinear algorithm

$$(\mathbf{x}_n^T Q^D \mathbf{y}_k) \mathbf{z}_m \ominus (\mathbf{x}'_n{}^T Q' \mathbf{y}'_{k'}) \mathbf{z}'_{m'} = \sum_{i=1}^{\mathbf{R}} a_i(\mathbf{z}_m, \mathbf{z}'_{m'}) b_i(\mathbf{x}_n, \mathbf{x}'_{n'}) c_i(\mathbf{y}_k, \mathbf{y}'_{k'}),$$

such that $a_1(\mathbf{z}_m, \mathbf{z}'_{m'})$ depends on \mathbf{z}_m and $\mathbf{z}'_{m'}$. Since $Q^{DD} = Q$, the D -dual system of the above is

$$(\mathbf{x}_n^T Q \mathbf{y}_m) \mathbf{z}_k \ominus (\mathbf{x}'_n{}^T Q'^D \mathbf{y}'_{m'}) \mathbf{z}'_{k'}$$

(for details see [HM] and [BF]). The minimal bilinear algorithm for this system is

$$(\mathbf{x}_n^T Q \mathbf{y}_m) \mathbf{z}_k \ominus (\mathbf{x}'_n{}^T Q'^D \mathbf{y}'_{m'}) \mathbf{z}'_{k'} = \sum_{i=1}^{\mathbf{R}} a_i(\mathbf{y}_m, \mathbf{y}'_{m'}) b_i(\mathbf{x}_n, \mathbf{x}'_{n'}) c_i(\mathbf{z}_k, \mathbf{z}'_{k'}) \quad (11)$$

Now since the term $a_1(\mathbf{z}_m, \mathbf{z}'_{m'})$ depends on \mathbf{z}_m and $\mathbf{z}'_{m'}$, it follows that $a_1(\mathbf{y}_m, \mathbf{y}'_{m'})$ in the new minimal algorithm must depend on \mathbf{y}_m and $\mathbf{y}'_{m'}$. Therefore, $(\mathbf{x}_n^T Q \mathbf{y}_m) \mathbf{z}_k$ does not satisfy the DSCS. This contradicts the assumption.

Part (ii) follows immediately from (10). \square

We remind the reader that all the theorems and corollaries in the previous sections also hold for the bilinear complexity.

The following corollaries are consequences of Theorem 6 and the results of the previous sections.

Corollary 15 . *Let*

$$r(Q) = \max \{ \dim \mathbf{x}_n^T Q \mathbf{y}_m, \mathbf{row\ rank}(\mathbf{x}_n^T Q \mathbf{y}_m)_{\mathbf{z}_k}, \mathbf{col\ rank}(\mathbf{x}_n^T Q \mathbf{y}_m)_{\mathbf{z}_k} \}.$$

We have

(i) *If $\mathbf{R}((\mathbf{x}_n^T Q \mathbf{y}_m)_{\mathbf{z}_k}) \leq r(Q) + 1$, then $(\mathbf{x}_n^T Q \mathbf{y}_m)_{\mathbf{z}_k}$ satisfies the DSCS.*

(ii) *If $\mathbf{R}((\mathbf{x}_n^T Q \mathbf{y}_m)_{\mathbf{z}_k}) = r(Q) + 2$, then $(\mathbf{x}_n^T Q \mathbf{y}_m)_{\mathbf{z}_k}$ satisfies the DSC.*

Proof . It can be easily shown that

$$\mathbf{col\ rank}(\mathbf{x}_n^T Q \mathbf{y}_m)_{\mathbf{z}_k} = \dim \mathbf{x}_n^T Q^D \mathbf{y}_k,$$

and

$$\mathbf{row\ rank}((\mathbf{x}_n^T Q \mathbf{y}_m)_{\mathbf{z}_k}) = \mathbf{col\ rank}((\mathbf{x}_m^T Q^T \mathbf{y}_n)_{\mathbf{z}_k}).$$

Now the result follows immediately from corollary 10 and theorem 6. \square

The following result follows from corollary 13.

Corollary 16 . *Let $\mathbf{A} = \{A_1, \dots, A_{k_1}\}$ be a set of $k_2 \times k_3$ -matrices. Consider the bilinear system*

$$(\mathbf{x}_{k_2}^T Q \mathbf{y}_{k_3})_{\mathbf{z}_{k_1}} = (\mathbf{x}_{k_2}^T A_1 \mathbf{y}_{k_3}, \dots, \mathbf{x}_{k_2}^T A_{k_1} \mathbf{y}_{k_3})_{\mathbf{z}_{k_1}}.$$

Then for $\{l, m, n\} = \{1, 2, 3\}$ we have:

(i) *If $k_l = k_m k_n - i$, $i \leq 3$, then $(\mathbf{x}_{k_2}^T Q \mathbf{y}_{k_3})_{\mathbf{z}_{k_1}}$ satisfies the DSCS.*

(ii) *If $k_l = k_m k_n - i$, $4 \leq i \leq 5$, then $(\mathbf{x}_{k_2}^T Q \mathbf{y}_{k_3})_{\mathbf{z}_{k_1}}$ satisfies the DSC.*

In [JT1], Ja'Ja' and Takche showed that for sufficient large fields, if $2 \in \{k_1, k_2, k_3\}$, then $(\mathbf{x}_{k_2}^T Q \mathbf{y}_{k_3})_{\mathbf{z}_{k_1}}$ satisfies the DSC.

8. DIRECT SUM OF ALGEBRAS

To acquaint the reader with the concepts in this section, we quickly review some notation.

Let F be a field. Let \mathbf{A} be an associative algebra over F of dimension $\mathbf{dim\ A} = k$, with unity element 1, and let a_1, \dots, a_k be a basis of the algebra \mathbf{A} . Suppose

$$a_i a_j = \sum_{l=1}^k \gamma_{i,j,l} a_l,$$

with $\gamma_{i,j,l} \in F$, $i, j, l = 1, \dots, k$. Then for the two elements $x = \sum_{i=1}^k x_i a_i$ and $y = \sum_{j=1}^k y_j a_j$ in the

algebra \mathbf{A} we have

$$x y = \left[\sum_{i=1}^k x_i a_i \right] \left[\sum_{j=1}^k y_j a_j \right] = \sum_{l=1}^k \left[\sum_{i=1}^k \sum_{j=1}^k \gamma_{i,j,l} x_i y_j \right] a_l.$$

Suppose $a_i y = \sum_{l=1}^k \sigma_{i,l} a_l$ where $\sigma_{i,l} \in F$. We define the $k \times k$ -matrix $A_y = (\sigma_{i,l})$. Then $\bar{\mathbf{A}} = \{A_a \mid a \in \mathbf{A}\}$ form an algebra over F isomorphic to \mathbf{A} under the correspondence $a \rightarrow A_a$ (for details see [A pp. 9-12]). The set of matrices $\{A_{a_1}, \dots, A_{a_k}\}$ is a basis for the algebra $\bar{\mathbf{A}}$; $A_1 = I_k$ the identity matrix of order k ; $A_a A_b = A_{ab}$; $A_a + A_b = A_{a+b}$; $\lambda A_a = A_{\lambda a}$ for $\lambda \in F$; and if $a b = 1$, then $A_a^{-1} = A_b$. The algebra $\bar{\mathbf{A}}$ is called the *regular representation* of \mathbf{A} .

Let $\mathbf{x} = (x_1, \dots, x_k)^T$, $\mathbf{y} = (y_1, \dots, y_k)^T$ and $\mathbf{z} = (z_1, \dots, z_k)^T$ be vectors of indeterminates and let $Q_{\mathbf{A}} = (Q_1, \dots, Q_k)$ be a k -vector of $k \times k$ matrices such that

$$\mathbf{x}^T Q_l \mathbf{y} = \sum_{i=1}^k \sum_{j=1}^k \gamma_{i,j,l} x_i y_j, \quad l = 1, \dots, k,$$

that is, $\mathbf{x}^T Q_l \mathbf{y}$ is the l -coefficient in the product

$$x y = \left[\sum_{i=1}^k x_i a_i \right] \left[\sum_{j=1}^k y_j a_j \right] = \sum_{l=1}^k (\mathbf{x}^T Q_l \mathbf{y}) a_l.$$

The bilinear system defined by the algebra \mathbf{A} is

$$Q_{\bar{\mathbf{A}}}^{\mathbf{x}^T \mathbf{y}} \mathbf{z} = (\mathbf{x}^T Q_{\mathbf{A}} \mathbf{y}) \mathbf{z} = (\mathbf{x}^T Q_1 \mathbf{y}, \dots, \mathbf{x}^T Q_k \mathbf{y}) \mathbf{z}.$$

In [FZ] it was proved that

$$(\mathbf{x}^T Q_{\bar{\mathbf{A}}}^D \mathbf{y}) \mathbf{z} = (\mathbf{x}^T A_{a_1} \mathbf{y}, \dots, \mathbf{x}^T A_{a_n} \mathbf{y}) \mathbf{z}. \quad (12)$$

In [ASt] Alder and Strassen proved the lower bound

$$\mathbf{R} (Q_{\bar{\mathbf{A}}}^{\mathbf{x}^T \mathbf{y}} \mathbf{z}) \geq 2 \dim \mathbf{A} - t(\mathbf{A}),$$

where $t(\mathbf{A})$ is the number of maximal two-sided ideals of \mathbf{A} . Following De Groote, cf. [Gr3], \mathbf{A} is said to be of *minimal rank* (respectively, *minimal complexity*) if

$$\mathbf{R} (Q_{\bar{\mathbf{A}}}^{\mathbf{x}^T \mathbf{y}} \mathbf{z}) = 2 \dim \mathbf{A} - t(\mathbf{A}), \quad (\mathbf{L} (Q_{\bar{\mathbf{A}}}^{\mathbf{x}^T \mathbf{y}} \mathbf{z}) = 2 \dim \mathbf{A} - t(\mathbf{A}).)$$

We say that \mathbf{A} is a *clean* algebra if $\mathbf{A} / \text{rad } \mathbf{A}$ is a direct product of division algebras. For a clean algebra \mathbf{A} with $\mathbf{A} / \text{rad } \mathbf{A} = \mathbf{A}_1 \times \dots \times \mathbf{A}_t$ where \mathbf{A}_i is a division algebra, ($t(\mathbf{A}) = t$), we define $R_{\mathbf{A} / \text{rad } \mathbf{A}} (C_{\mathbf{A} / \text{rad } \mathbf{A}})$ to be the number of algebras \mathbf{A}_i which are not of minimal rank (minimal complexity).

Let \mathbf{A} be an algebra over F and let E be an extension field of F . We will denote by \mathbf{A}^E the algebra \mathbf{A} over E .

To prove the main result of this section we need the following well known result (for details see [A]).

Lemma 10. *Let \mathbf{A} be a clean algebra. For any extension field $E = F(z_1, \dots, z_r)$ of F , with independent transcendental elements z_1, \dots, z_r , we have*

- (i) *The algebra \mathbf{A}^E is clean.*
- (ii) *$\text{rad } \mathbf{A}^E = (\text{rad } \mathbf{A})^E$.*
- (iii) *If $\mathbf{A} / \text{rad } \mathbf{A} \cong \mathbf{A}_1 \times \dots \times \mathbf{A}_t$ where $\mathbf{A}_i, 1 \leq i \leq t$, are division algebras, then*

$$\mathbf{A}^E / \text{rad } \mathbf{A}^E \cong \mathbf{A}_1^E \times \dots \times \mathbf{A}_t^E$$

and $\mathbf{A}_i^E, 1 \leq i \leq t$, are division algebras.

Our main result in this section is:

Corollary 17. *Let \mathbf{A} be a clean algebra. Then*

- (i) *If \mathbf{A} is an algebra of minimal rank, then $Q_{\mathbf{A}}^{\mathbf{x}, \mathbf{y}} \mathbf{z}$ satisfies the DSCS.*
- (ii) *If \mathbf{A} is not an algebra of minimal rank, then for any bilinear system $Q^{\mathbf{x}, \mathbf{y}} \mathbf{z}$, we have*

$$\mathbf{R}(Q_{\mathbf{A}}^{\mathbf{x}, \mathbf{y}} \mathbf{z} \oplus Q^{\mathbf{x}, \mathbf{y}} \mathbf{z}) \geq 2 \dim \mathbf{A} - t(\mathbf{A}) + 1 + \mathbf{R}(Q^{\mathbf{x}, \mathbf{y}} \mathbf{z}).$$

- (iii) *If \mathbf{A} is not an algebra of minimal rank, then for any bilinear system $Q^{\mathbf{x}, \mathbf{y}} \mathbf{z}$ we have*

$$\mathbf{R}(Q_{\mathbf{A}}^{\mathbf{x}, \mathbf{y}} \mathbf{z} \oplus Q^{\mathbf{x}, \mathbf{y}} \mathbf{z}) \geq 2 \dim \mathbf{A} - t(\mathbf{A}) + R_{\mathbf{A} / \text{rad } \mathbf{A}} + \mathbf{R}(Q^{\mathbf{x}, \mathbf{y}} \mathbf{z}).$$

In particular, if $\mathbf{R}(Q_{\mathbf{A}}^{\mathbf{x}, \mathbf{y}} \mathbf{z}) = 2 \dim \mathbf{A} - t(\mathbf{A}) + R_{\mathbf{A} / \text{rad } \mathbf{A}}$, then $Q_{\mathbf{A}}^{\mathbf{x}, \mathbf{y}} \mathbf{z}$ satisfies the DSC.

Proof. Corollary 6 implies (iii). Now, if we prove that $(\mathbf{x}^T Q_{\mathbf{A}}^D \mathbf{y}) \mathbf{z} \in \mathbf{DS}^*(r)$, then by lemma 6, (i) and (ii) follow.

From (12) we have

$$(\mathbf{x}^T Q_{\mathbf{A}}^D \mathbf{y}) \mathbf{z} = (\mathbf{x}^T A_{a_1} \mathbf{y}, \dots, \mathbf{x}^T A_{a_t} \mathbf{y}) \mathbf{z}.$$

Let N be any nonsingular $k \times k$ -matrix and let

$$(\mathbf{x}^T Q_{\mathbf{A}}^D \mathbf{y}) N = (\mathbf{x}^T (\sum_{i=1}^k \lambda_{i,1} A_{a_i}) \mathbf{y}, \dots, \mathbf{x}^T (\sum_{i=1}^k \lambda_{i,k} A_{a_i}) \mathbf{y}) = (Q_1, \dots, Q_k),$$

with $\lambda_{i,j} \in F$. Since N is a nonsingular matrix, the matrices $B_j = \sum_{i=1}^k \lambda_{i,j} A_{a_i}, j = 1, \dots, k$ form a basis for the algebra $\overline{\mathbf{A}}$ (the regular representation algebra).

For $a \in \overline{\mathbf{A}}$ let $r(a) \in \overline{\mathbf{A}}/rad \overline{\mathbf{A}}$ be its image under a canonical homomorphism $\overline{\mathbf{A}} \xrightarrow{r} \overline{\mathbf{A}}/rad \overline{\mathbf{A}}$. For $b \in \overline{\mathbf{A}}/rad \overline{\mathbf{A}}$ and $1 \leq \sigma \leq t$, let $[b]_{\sigma}$ denote the canonical projection of $\overline{\mathbf{A}}/rad \overline{\mathbf{A}}$ onto its σ -th component (of b) according to the decomposition $\overline{\mathbf{A}}/rad \overline{\mathbf{A}} = \overline{\mathbf{A}}_1 \times \dots \times \overline{\mathbf{A}}_t$, i.e., $[\]_{\sigma}: \overline{\mathbf{A}}/rad \overline{\mathbf{A}} \rightarrow \overline{\mathbf{A}}_{\sigma}$.

We will first prove that $(\mathbf{x}^T Q_{\mathbf{A}}^D \mathbf{y}) \in \mathbf{DS}(0, r)$. Since $\{B_j \mid j = 1, \dots, k\}$ form a basis for $\overline{\mathbf{A}}$, we have that $C_j = r(B_j), j = 1, \dots, k$ is a basis for $\overline{\mathbf{A}}/rad \overline{\mathbf{A}} = \overline{\mathbf{A}}_1 \times \dots \times \overline{\mathbf{A}}_t$. Therefore, for every $1 \leq \sigma \leq t$ there exists $C_{j_{\sigma}}$ such that $[C_{j_{\sigma}}]_{\sigma} \neq 0$. Consider the element $c = \sum_{\sigma=1}^t z_{\sigma} C_{j_{\sigma}}$ in $\overline{\mathbf{A}}^E / rad \overline{\mathbf{A}}^E$, where $E = F(z_1, \dots, z_t)$. Since $[c]_{\sigma} \neq 0$ for all $\sigma = 1, \dots, t$, the element c is a nonsingular element in the algebra $\overline{\mathbf{A}}^E / rad \overline{\mathbf{A}}^E$. Therefore, $\sum_{\sigma=1}^t z_{\sigma} B_{j_{\sigma}}$ is a nonsingular element in $\overline{\mathbf{A}}^E$, which implies that

$$\mathbf{rank}_E \sum_{\sigma=1}^t z_{\sigma} B_{j_{\sigma}} = \mathbf{dim} \overline{\mathbf{A}}^E = \mathbf{dim} \overline{\mathbf{A}} = \mathbf{dim} \mathbf{A},$$

where $\mathbf{rank}_E H$ is the dimension of the linear space spanned by the rows of H over E , (in this case, it is the rank of the matrix H over E). Now we have

$$\mathbf{rank}((Q_{j_1}, \dots, Q_{j_t})(z_1, \dots, z_t)^T) \geq \mathbf{rank}_F \sum_{\sigma=1}^t z_{\sigma} B_{j_{\sigma}} \geq \mathbf{rank}_E \sum_{\sigma=1}^t z_{\sigma} B_{j_{\sigma}} = \mathbf{dim} \mathbf{A}.$$

We have already proved that for any nonsingular $k \times k$ -matrix N , there exist t entries Q_{i_1}, \dots, Q_{i_t} in $(\mathbf{x}^T Q_{\mathbf{A}}^D \mathbf{y})N$ such that

$$\mathbf{rank}((Q_{i_1}, \dots, Q_{i_t})\tilde{\mathbf{z}}) \geq \mathbf{dim} \mathbf{A},$$

where $\tilde{\mathbf{z}} = (z_1, \dots, z_t)^T$. This proves that $(\mathbf{x}^T Q_{\mathbf{A}}^D \mathbf{y})\mathbf{z} \in \mathbf{DS}(0, r)$.

In the linear space $\mathbf{Span}(Q_{\mathbf{A}}^{\mathbf{x}^{\mathbf{y}}})$, the bilinear form $\mathbf{x}^T H_j \mathbf{y}$ is active if and only if $r(H_j) \neq 0$. Since $r(B_{j_{\sigma}}) = C_{j_{\sigma}} \neq 0$, the entries Q_{i_1}, \dots, Q_{i_t} are active. Actually, the set of all nonactive bilinear forms are the bilinear forms $\mathbf{x}^T H \mathbf{y}$, where $H \in rad \overline{\mathbf{A}}$.

We still have to prove the first condition of $\mathbf{DS}^*(r)$. That is, for any nonsingular $k \times k$ -matrix N , there exists an active entry Q'_{j_1} of $(\mathbf{x}^T Q_{\mathbf{A}}^D \mathbf{y})N$ such that for every non-active entry Q'_{j_2} of

$(\mathbf{x}^T Q_A^D \mathbf{y})N$, and every $f_1, f_2 \in F$ with $f_1 \neq 0$, we have that $f_1 Q'_{j_1} + f_2 Q'_{j_2}$ is also active.

The entry Q'_{j_1} is active and therefore $r(B_{j_1}) \neq 0$, which implies $B_{j_1} \notin \text{rad } \bar{\mathbf{A}}$. The entry Q'_{j_2} is non-active and therefore $r(B_{j_2}) = 0$, which implies $B_{j_2} \in \text{rad } \bar{\mathbf{A}}$. Now the desired condition follows because $f_1 Q'_{j_1} + f_2 Q'_{j_2} = \mathbf{x}^T (f_1 B_{j_1} + f_2 B_{j_2}) \mathbf{y}$ and $f_1 B_{j_1} + f_2 B_{j_2} \notin \text{rad } \bar{\mathbf{A}}$ for every $f_1 \neq 0$. \square

We now give some examples of clean algebras.

Example 1. The *simple generated local algebra* is $\mathbf{A} = F[\alpha]/(p(\alpha)^d)$ where $p(\alpha) \in F[\alpha]$ is an irreducible polynomial. This algebra satisfies

$$\text{rad } \mathbf{A} = (p(\alpha)) , \mathbf{A} / \text{rad } \mathbf{A} = F[\alpha]/(p(\alpha)).$$

If $|F| \geq 2 \deg p(\alpha)^d - 2$, then \mathbf{A} is an algebra of minimal rank. If $|F| \leq 2 \deg p(\alpha) - 2$, then \mathbf{A} is not an algebra of minimal rank.

Example 2. The local algebra $\mathbf{A} = F[\omega_1, \dots, \omega_d]$ where $\omega_i \omega_j = 0$ for every $i \neq j$. This algebra satisfies

$$\text{rad } \mathbf{A} = (\omega_1) + \dots + (\omega_d) , \mathbf{A} / \text{rad } \mathbf{A} = F.$$

When $\omega_i^2 = 0$, then \mathbf{A} is called the *null algebra*. This algebra is of minimal rank.

Remark . De Groote and Heintz proved in [GH1] that commutative local algebras of minimal rank are either the algebras in example 1 or example 2.

Example 3. Any commutative algebra is a direct sum of commutative local algebras (See [AM], the Artin theorem). Therefore commutative algebras are clean.

Example 4. Let $n_1 < n_2 < \dots < n_k < n$ be a natural numbers. Then

$$\mathbf{A} = F[x^{n_1}, \dots, x^{n_k}] / (F[x^{n_1}, \dots, x^{n_k}] \cap F[x]x^n)$$

is a commutative algebra. It has been proved in [GH1], that \mathbf{A} is of minimal rank if and only if $n_1 + n_2 \geq n$.

Example 5. The set of all upper triangular $N \times N$ -matrices $T_N(C)$ over the complex field C is a clean algebra. This algebra satisfies

$$\text{rad } T_N(C) = \bar{T}_N(C) \stackrel{\Delta}{=} \{ \text{strict upper triangular } N \times N \text{ - matrices} \}$$

and

$$T_N(C)/\text{rad } T_N(C) = C \times \overset{N \text{ times}}{\cdots} \times C.$$

Therefore by the Alder and Strassen bound we have

$$\mathbf{R}(Q_{T_N(C)}^{\mathbf{x}, \mathbf{y}}) \geq N^2.$$

Heintz and Morgenstern proved in [HMo] that $T_N(C)$ is of minimal rank if and only if $N = 2$. They also proved that $\mathbf{R}(Q_{T_3(C)}^{\mathbf{x}, \mathbf{y}}) = 10$.

By corollary 16 we have that $Q_{T_2(C)}^{\mathbf{x}, \mathbf{y}}$ satisfies the DSCS; $Q_{T_3(C)}^{\mathbf{x}, \mathbf{y}}$ satisfies the DSC; and for every $N \geq 3$ and any bilinear system $Q^{\mathbf{x}, \mathbf{y}, \mathbf{z}}$ we have

$$\mathbf{R}(Q_{T_N(C)}^{\mathbf{x}, \mathbf{y}} \mathbf{z} \Theta Q^{\mathbf{x}, \mathbf{y}, \mathbf{z}}) \geq N^2 + 1 + \mathbf{R}(Q^{\mathbf{x}, \mathbf{y}, \mathbf{z}}). \quad \square$$

Example 6 . The upper triangular $N \times N$ -matrix $T_N(D)$ over a division algebra D over a field F is a clean algebra. Obviously, $T_N(D) \equiv T_N(F) \otimes D$,

$$\text{rad } T_N(D) = \bar{T}_N(D) = \bar{T}_N(F) \otimes D,$$

and

$$T_N(D)/\text{rad } T_N(D) = D \times D \times \overset{N \text{ times}}{\cdots} \times D.$$

By the Alder and Strassen bound we have that for any bilinear system $Q^{\mathbf{x}, \mathbf{y}, \mathbf{z}}$,

$$\mathbf{R}(Q_{T_N(D)}^{\mathbf{x}, \mathbf{y}} \mathbf{z} \Theta Q^{\mathbf{x}, \mathbf{y}, \mathbf{z}}) \geq N^2 K + N K - N + \mathbf{R}(Q^{\mathbf{x}, \mathbf{y}, \mathbf{z}}),$$

where $K = \mathbf{dim } D$. By Corollary 17 we have

$$\mathbf{R}(Q_{T_N(D)}^{\mathbf{x}, \mathbf{y}} \mathbf{z} \Theta Q^{\mathbf{x}, \mathbf{y}, \mathbf{z}}) \geq N^2 K + N K - N + R_D N + \mathbf{R}(Q^{\mathbf{x}, \mathbf{y}, \mathbf{z}}),$$

where $R_D = 0$ if D is a division algebra of minimal rank, and $R_D = 1$ otherwise.

9. OPEN PROBLEMS

Finally, we shall give some open problems

- (1) Prove that for any associative algebra \mathbf{A} and any quadratic system $Q^{\mathbf{x}, \mathbf{z}}$ (respectively, bilinear system $Q^{\mathbf{x}, \mathbf{y}, \mathbf{z}}$), we have

$$\mathbf{L}(Q_{\mathbf{A}}^{\mathbf{x}, \mathbf{y}} \mathbf{z} \Theta Q^{\mathbf{x}, \mathbf{z}}) \geq 2 \mathbf{dim } \mathbf{A} - C_{\mathbf{A}/\text{rad } \mathbf{A}} + \mathbf{L}(Q^{\mathbf{x}, \mathbf{z}})$$

(respectively,

$$\mathbf{R}(Q_{\mathbf{A}}^{\mathbf{x}, \mathbf{y}} \mathbf{z} \Theta Q^{\mathbf{x}, \mathbf{y}, \mathbf{z}}) \geq 2 \mathbf{dim } \mathbf{A} - R_{\mathbf{A}/\text{rad } \mathbf{A}} + \mathbf{R}(Q^{\mathbf{x}, \mathbf{y}, \mathbf{z}})).$$

And if $\mathbf{L}(Q_{\mathbf{A}}^{\mathbf{x}, \mathbf{y}}) = 2 \mathbf{dim } \mathbf{A} - C_{\mathbf{A}/\text{rad } \mathbf{A}}$ (respectively, $\mathbf{R}(Q_{\mathbf{A}}^{\mathbf{x}, \mathbf{y}}) = 2 \mathbf{dim } \mathbf{A} - R_{\mathbf{A}/\text{rad } \mathbf{A}}$), *i.e.*

- \mathbf{A} is of minimal complexity (respectively, minimal rank), then $Q_{\mathbf{A}}^{x,y}$ satisfies the EDSCS (respectively, satisfies the DSCS).
- (2) Prove that the bilinear systems $Q^{x,y,z}$ in $\mathbf{DS}(2, i)$ satisfy the EDSCS (respectively, satisfy the DSCS) for $i = 0, 1$ and satisfy the EDSC for $i = 2$ (respectively, satisfy the DSC). Note that the bilinear system defined by the product of 2×2 matrices is in $\mathbf{DS}(2, 1)$.
- (3) Classify all the minimal quadratic (bilinear) algorithms for algebras of minimal complexity (minimal rank).
- (4) Find a lower bound $\alpha \dim \mathbf{A}$ for some algebra \mathbf{A} over an infinite field, with $\alpha > 2$. For finite fields, see [B1], [B3] and [LSW].

REFERENCES

- [A] A. A. Albert, *Structure of algebras*, American Mathematical Society Colloquium Publications, Vol XXIV, (1939).
- [ABK] A. Averbuch, N. H. Bshouty, M. Kaminski, Classification of polynomial multiplication of small degree over finite fields.
- [Am] A. Averbuch, private communication.
- [AGW1] A. Averbuch, Z. Galil, S. Winograd, Classification of all the minimal bilinear algorithms for computing the coefficient of the product of two polynomials modulo a polynomial in the algebra $G[u]/\langle u^n \rangle$.
- [AGW2] 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 $G[u]/\langle Q(u)^l \rangle$, $l > 1$, *Theoretical Computer Science* **58** (1988), 17-56.
- [AFW] L. Auslander, E. Feig, S. Winograd, Direct Sum of Bilinear Algorithm, *Linear Algebra and Its Application* **38** (1981), 175-192

- [AL2] M. D. Atkinson, S. Lloyd, The rank of $m \times n \times (m n - 2)$ tensors, *SIAM J. Compute.***12** (1983):611-615.
- [AM] M. F. Atiyah, I. G. Macdonald, *Introduction to commutative algebra.*, Addison-Wesley, London, 1969.
- [AS] M. D. Atkinson, N. M. Stephens, On the maximal multiplicative complexity of a family of bilinear forms, *Linear Algebra and Its Application* **27** (1979) , 1-8.
- [ASt] A. Alder, V. Strassen, On the algorithmic complexity of associative algebras, *Theoret. Compute. Sci.* **15** (1981):201-211.
- [B1] N. H. Bshouty, A lower bound for matrix multiplication, Proceedings 29th Annual Symposium on Foundations of Computer Science, (1988).
- [B2] N. H. Bshouty, Maximal rank of $m \times n \times (m n - k)$ tensors, TR, Technion.
- [B3] N. H. Bshouty, On the algorithmic complexity of associative algebras over finite fields. TR, Technion.
- [B4] N. H. Bshouty, On the complexity of bilinear forms over associative algebras, TR No. 89/373/35, University of Calgary.
- [BC] W. Büchi, M. Clausen, On a class of primary algebras of minimal rank, *Linear Algebra and Its Applications* **69** (1985), 249-268.
- [BD1] R.W. Brockett, D. Dobkin, On the Optimal Evaluation of a set of Bilinear Forms, *Linear Algebra and Its Applications* **19** (1978), 207-235.
- [DL] D. Dobkin, Jan Van Leeuwen, The complexity of vector-product, *Information Processing Letter*, **4**, (1976), 149-154.
- [Fei] E. Feig, On systems of bilinear forms whose minimal division-free algorithms are all bilinear, *Journal of Algorithms*, **2**, (1981), 261-281.
- [Fel] A. Fellmann, Optimal algorithms for finite dimensional simply generated algebras, *LN Comput. Sci.* **229**,(1986).

- [Fi] C. M. Fiduccia, Fast matrix multiplication, Proc. 3rd Annual ACM Symp. on theory of computing (1971), 45-49.
- [FW] E. Feig, S. Winograd, On the direct sum conjecture, *Linear Algebra and Its Application* **63** (1984), 193-219.
- [FZ] C.M. Feduccia, Y. Zalcstein, Algebras having linear multiplicative complexity, *J. ACM* **24** (1977), 311-331.
- [Gat1] J. von zur Gathen, Algebraic complexity theory. To appear in Annual Review of Computer Science **3** (1988). Tech. Rep. 207/88, Dept. of Computer Science, University of Toronto, 1988.
- [Gat2] J. von zur Gathen, Maximal bilinear complexity and codes. Preprint, University of Toronto, (1988).
- [Gr1] H. F. De Groote, On the complexity of quaternion multiplication, *Information Processing Letter* **3** (1975) 177-179.
- [Gr2] H. F. De Groote, On varieties of optimal algorithms for the computation of bilinear mapping III. Optimal algorithm for the computation of $x y$ and $y x$ where $x, y \in M_2(K)$, *Theoretical Computer Science* **7** (1978), 239-249.
- [Gr3] H. F. De Groote, Characterization of division algebras of minimal rank and the structure of their algorithm varieties, *SIAM J. Comput.* **12** (1983), 101-117.
- [Gr4] H. G. De Groote, Lectures on the complexity of bilinear problems. *LN Comput. Sci.* **245**, Springer, Berlin 1987.
- [GH1] H. F. De Groote, J. Heintz, Commutative algebras of minimal rank, *Linear Algebra and its Applications*, **55**(1983), 37-68.
- [GH2] H. F. De Groote, J. Heintz, A lower bound for the bilinear complexity of some semisimple Lie algebras, *Algebraic algorithms and error correcting codes. Proc. AAECC-3*, Grenoble 1985. *LN Comput. Sci.* **229**, (1986), 211-222.
- [HM] J. Hopcroft, J. Munsinski, Duality applied to the complexity of matrix multiplication, *SIAM J. Comput.* **2** (1973), 159-173.

- [HMo] J. Heintz, J. Morgenstern, On associative algebras of minimal rank, *Proc. of the AAECC-2 Conference (Grenoble 1984)*.
- [J1] J. Ja'Ja' On the complexity of bilinear forms with commutativity, *SIAM. J.Comput* **9, 4**, (1980), 713-728.
- [JT1] J. Ja'Ja', J. Takche, On the validity of the direct sum conjecture, *SIAM. J.Comput* **15, 4**, (1986), 1004-1020.
- [KB] M. Kaminski, N. H. Bshouty, Multiplicative complexity of polynomial multiplication over finite field, Proceedings 28th Annual Symposium on Foundations of Computer Science, (1987).
- [LSW] A. Lempel, G. Seroussi, S. Winograd, On the Complexity of Multiplication in Finite Fields, *Theoret. Comput. Sci.* **22** (1983), 285-296.
- [Mi] R. Mirwald, The algorithmic structure of $sl(2, k)$, *Algebraic algorithms and error correcting codes. AAECC-3 Grenoble 1985. LN Comput. Sci.* (1986), 274-287.
- [Sh] A. Schonhage, Partial and total matrix multiplication, *SIAM J. Compute* **10, 3**, (1981), 434-455.
- [S1] V. Strassen, Vermeidung von Divisionen, *J. Reine Angew. Math.* **264** (1973), 184-202.
- [W1] S. Winograd, On the Number of Multiplications Necessary to Compute Certain Functions, *Comm. Pure and Appl. Math.* **23** (1970), 165-179.
- [W2] S. Winograd, On multiplication of 2×2 matrices, *Linear Algebra and its Applications*, **4** (1971), 381-388.
- [W3] S. Winograd, Some Bilinear Forms Whose Multiplicative Complexity Depends on the Field Constants, *Math. System Theory* **10** (1976/77), 169-180.
- [W4] S. Winograd, On multiplication in algebraic extension field, *Theoret. Comput. Sci.*, **8** (1979), 359-377.