ON THE ALGORITHMIC COMPLEXITY OF ASSOCIATIVE ALGEBRAS OVER FINITE FIELDS

Nader H. Bshouty

Department of Computer Science

Technion - Israel Institute of Technology, Israel.

and

University of Calgary, Alberta, Canada.

ABSTRACT

The multiplicative complexity of a finite dimensional associative algebra **A** over a finite field F is the number of nonscalar multiplication needed to multiply two elements of the algebra **A**.

In this paper we generalize all the results known from the literature about lower bounds for the multiplicative complexity of associative algebras over finite fields.

Key Words : multiplicative complexity, bilinear algorithms, quadratic algorithms, associative algebras, Frobenuis algebra, linear codes.

1. INTRODUCTION

Let F be a field and let $\mathbf{B} = \{B_1, \ldots, B_k\}$ be a set of $n \times m$-matrices with entries from F. A *quadratic* algorithms over F that compute the bilinear forms $x^T \mathbf{B} y = \{x^T B_1 y, \ldots, x^T B_k y\}$, where $x = (x_1, \ldots, x_n)^T$ and $y = (y_1, \ldots, y_m)^T$ are vectors of indeterminates, are straightline algorithms over F for $x^T \mathbf{B} y$ that their nonscalar multiplications are of the shape $l(x,y) \times l'(x,y)$ where $l(x,y)$ and $l'(x,y)$ are linear forms of x and y. The *complexity* $\mathbf{L}_F(\mathbf{B})$ of $\mathbf{B}$ is the minimal number of nonscalar multiplications needed to compute $x^T \mathbf{B}\, y$ by quadratic algorithms over F. It is known from [S] that, when F is infinite field, then $\mathbf{L}_F(\mathbf{B})$ is the number of nonscalar multiplications divisions needed to compute $x^T \mathbf{B}\, y$ by straightline algorithms. When F is finite, then it is known from [W] that

$\mathbf{L}_F(\mathbf{B})$ is the number of nonscalar multiplications needed to compute $x^T\mathbf{B}y$ by a straightline algorithm without divisions.

When the indeterminates x_i and y_j do not commute then we can restrict the quadratic algorithms to *bilinear algorithms*, i.e. quadratic algorithms that their nonscalar multiplications are of the shape $l(x)\times l'(y)$ where $l(x)$ and $l'(y)$ are linear form of x and y, respectively, and this restriction does not increase the multiplicative complexity. We write $\mathbf{R}_F(\mathbf{B})$ for the minimal number of nonscalar multiplications needed to compute $x^T\mathbf{B}y$ by bilinear algorithms. The relation between the quadratic complexity and the bilinear complexity is, cf. [J], (when the indeterminates commute)

$$\mathbf{L}_F(\mathbf{B}) \le \mathbf{R}_F(\mathbf{B}) < 2\mathbf{L}_F(\mathbf{B}).$$

Throughout the paper we shall write $\mathbf{L}$ and $\mathbf{R}$ for $\mathbf{L}_F$ and $\mathbf{R}_F$, respectively.

Let $\mathbf{A}$ be an associative algebra of dimension k over a finite field F with identity element 1 and let $\{a_1, \ldots, a_k\}$ be a basis of $\mathbf{A}$. Let $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$ be vectors of indeterminates. Denote by $\mathbf{B}_{\mathbf{A}}$ the set of $k\times k$-matrices $\{B_1, \ldots, B_k\}$ such that

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

i.e. $x^T B_i y$, $i=1, \ldots, k$ are the coefficients of the product of two elements in $\mathbf{A}$. Then $\mathbf{L}(\mathbf{B}_{\mathbf{A}})$ is the multiplicative complexity of the product of two elements in $\mathbf{A}$. It is known from [FZ] that this complexity does not depend on the chosen basis, i.e. on $\{a_1, \ldots, a_n\}$.

We shall abbreviate $\mathbf{L}(\mathbf{B}_{\mathbf{A}})$ and $\mathbf{R}(\mathbf{B}_{\mathbf{A}})$ by $\mathbf{L}(\mathbf{A})$ and $\mathbf{R}(\mathbf{A})$, respectively.

The result of Alder-Strassen in [AS] states:

$$\mathbf{L}(\mathbf{A}) \ge 2\, dim\ \mathbf{A} - t(\mathbf{A}),$$

where $t(\mathbf{A})$ is the number of maximal (two-sided) ideals of $\mathbf{A}$.

The technique used in [AS] is the substitution technique. Many papers slightly improve this result, (see, for example, [B2], [BC], [FW], [G], [GH] and [HM]), but no example of algebra $\mathbf{A}$ over infinite field is known for which we can prove a lower bound $c\ dim\ \mathbf{A}$, with $c>2$, using the substitution technique.

For algebras over finite fields, Lemple-Winograd, Lemple-Seroussi-Winograd and Brokett-Dobkin in [LW], [LSW] and [BD], respectively, found a new method that gives better lower bounds. They use coding theory to prove the bounds

$$\mathbf{L}_{F_2}(F_{2^n}) \geq 3.52\,n \tag{1}$$

and

$$\mathbf{L}_{F_q}(F_{q^n}) \geq \left(2+\frac{1}{q-1}\right) n - O(\log(n)), \tag{2}$$

where F_q is the q-element field and F_{q^n} is the n-degree extention field of F_q.

For these algebras, Chudnovsky proved in [CC] the linear upper bound

$$\mathbf{L}_{F_2}(F_{2^n}) \leq 6n\,, \quad \mathbf{L}_{F_q}(F_{q^n}) \leq \left(2+O\left(\frac{1}{q^{1/2}}\right)\right) n. \tag{3}$$

In [B1] we used both techniques, the substitution and coding techniques, to prove the lower bound

$$\mathbf{L}_{F_2}(\mathbf{M}_n(F_2)) \geq 2.5\,n^2 - O(n \log n), \tag{4}$$

for the total matrix algebra $\mathbf{M}_n$ over the binary field F_2.

In this paper we shall unify and generalize these results for other algebras over finite fields.

For a polynomial $p \in F[\alpha]$, let $F(p) = F[\alpha]/(p(\alpha))$.

We first generalize the results in (1) and (2) as follows

Corollary I . Let $p \in F[\alpha]$ be a polynomial over a finite field F. Then

$$\mathbf{L}(F(p)) \geq \left(2+\frac{1}{|F|-1}\right) deg\, p - o(deg\, p). \tag{5}$$

The result of Chudnovsky in (3) implies the upper bound

$$\mathbf{L}(F(p)) \leq \left(2+O\left(\frac{1}{|F|^{1/2}}\right)\right) deg\, p\,. \tag{6}$$

Then we generalize our result in (4) as follows

Corollary II . Let $p \in F[\alpha]$ be an irreducible polynomials of degree d. If F is the binary field, then for any n and d that satisfy $d = o(\log n)$ or $d = O(\log n)$ or $\log n = o(d)$, we have

$$\mathbf{L}(\mathbf{M}_n(F) \otimes F(p)) \geq 2.5 n^2 deg\, p - o(n^2 deg\, p).$$

Finally, the result of Coppersmith-Winograd in [CW] and Chudnovsky, (6), implies

$$\mathbf{L}(\mathbf{M}_n(F) \otimes F(p)) \leq n^{2.376} \mathbf{L}(F(p)) \leq \left[2 + O\left[\frac{1}{|F|^{1/2}} \right] \right] n^{2.376} deg\, p .$$

In the paper we also show how to find new lower bounds for some algebras with nonzero radical, as algebras with one maximal ideal. For many algebras over the binary field the bound

$$2\frac{1}{2} dim\ \mathbf{A} + dim\ (rad\, \mathbf{A}) - o\,(dim\ \mathbf{A})$$

can be obtained.

2. PRELIMINARY RESULTS

This section contain a survey of some basic concept and results from [BF] that will be employed throughout the paper.

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

$$\mathbf{B}^T = \{B_1^T, \ldots, B_n^T\} \quad , \quad \mathbf{B}^D = \{C_1, \ldots, C_n\},$$

where, B_i^T is the transpose of the matrix B_i and

$$C_i = [B_1 e_i \mid \cdots \mid B_n e_i],$$

where e_i is the i-th column vector of unity.

Definition 2 . Let $\mathbf{B} = \{B_1, \ldots, B_n\}$ be a set of n, $n \times n$-matrices and M, N and $K = (K_{i,j})$ be $n \times n$-matrices. We define

$$N\,\mathbf{B}M = \{N B_1 M, \ldots, N B_n M\},\ \mathbf{B}[K] = \left\{ \sum_{j=1}^{n} K_{1,j} B_j, \ldots, \sum_{j=1}^{n} K_{n,j} B_j \right\}$$

Definition 3 . Let $\mathbf{B} = \{B_1, \ldots, B_n\}$ and $\mathbf{C} = \{C_1, \ldots, C_m\}$ be sets of n and m, $n \times n$- and $m \times m$-matrices, respectively. We define

$$\mathbf{B} \oplus \mathbf{C} = \{\tilde{B}_1, \ldots, \tilde{B}_n, \tilde{C}_1, \ldots, \tilde{C}_m\}$$

where

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

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

We also define

$$\mathbf{B}\otimes\mathbf{C}=\{B_i\otimes C_j \mid i=1,\ldots,n\ ,\ j=1,\ldots,m\}.$$

where $\otimes$ is the Kronecker product of matrices.

The following lemma proved in [BF]

Lemma 1 . Let $\mathbf{B}_1$, $\mathbf{B}_2$ and $\mathbf{B}$ be sets of n_1, n_2 and n, $n_1\times n_1$, $n_2\times n_2$ and $n\times n$-matrices, respectively, and K, J and M are matrices. Then

(i) $\mathbf{B}^{TT}=\mathbf{B}$, $\mathbf{B}^{DD}=\mathbf{B}$, $\mathbf{B}^{EE}=\mathbf{B}$, $\mathbf{B}^{E}=\mathbf{B}^{TDT}=\mathbf{B}^{DTD}$.

(ii) $\mathbf{B}[K][J]=\mathbf{B}[JK]$, $(N\mathbf{B}M)[K]=N(\mathbf{B}[K])M$.

(iii) $(N\mathbf{B}M)^T=M^T\mathbf{B}^TN^T$, $(\mathbf{B}[K])^T=\mathbf{B}^T[K]$

(iv) $(N\mathbf{B})^D=N\mathbf{B}^D$, $(\mathbf{B}M)^D=\mathbf{B}^D[M^T]$, $(\mathbf{B}[K])^D=(\mathbf{B}^DK^T)$.

(v) $(\mathbf{B}_1\oplus\mathbf{B}_2)^T=\mathbf{B}_1^T\oplus\mathbf{B}_2^T$, $(\mathbf{B}_1\oplus\mathbf{B}_2)^D=\mathbf{B}_1^D\oplus\mathbf{B}_2^D$.

(vi) $(\mathbf{B}_1\otimes\mathbf{B}_2)^T=\mathbf{B}_1^T\otimes\mathbf{B}_2^T$, $(\mathbf{B}_1\otimes\mathbf{B}_2)^D=\mathbf{B}_1^D\otimes\mathbf{B}_2^D$.

(vii) $\mathbf{B}_1[K]\oplus\mathbf{B}_2=(\mathbf{B}_1\oplus\mathbf{B}_2)[diag(K,I_{n_2})]$, $N\mathbf{B}_1M\oplus\mathbf{B}_2=diag(N,I_{n_2})(\mathbf{B}_1\oplus\mathbf{B}_2)diag(M,I_{n_2})$.

$(viii)$ $\mathbf{B}_1[K]\otimes\mathbf{B}_2=(\mathbf{B}_1\otimes\mathbf{B}_2)[K\otimes I_{n_2}]$, $N\mathbf{B}_1M\otimes\mathbf{B}_2=(N\otimes I_{n_2})(\mathbf{B}_1\otimes\mathbf{B}_2)(M\otimes I_{n_2})$

where

$$diag(B_1,B_2)=\begin{bmatrix}B_1 & 0\\ 0 & B_2\end{bmatrix}.$$

Definition 4 . For two n-sets of $n\times n$-matrices $\mathbf{B}$ and $\mathbf{C}$ we write $\mathbf{B}\equiv\mathbf{C}$ if there exist nonsingular $n\times n$-matrices N, M and K such that

$$\mathbf{B}=N(\mathbf{C}[K])M.$$

Obviously this relation is an equivalence relation.

Lemma 2 . [BF]. Let $\mathbf{B}_1,\ldots,\mathbf{B}_t,\mathbf{C}_1,\ldots,\mathbf{C}_t$ be sets of matrices. Then

(i) If $\mathbf{B}_1\equiv\mathbf{C}_1$, then $\mathbf{B}_1^D\equiv\mathbf{C}_1^D$ and $\mathbf{B}_1^T\equiv\mathbf{C}_1^T$.

(ii) For any permutation ϕ on $\{1,\ldots,t\}$ we have

$$\mathbf{B}_1 \oplus \cdots \oplus \mathbf{B}_t \equiv \mathbf{B}_{\phi(1)} \oplus \cdots \oplus \mathbf{B}_{\phi(t)}, \quad \mathbf{B}_1 \otimes \cdots \otimes \mathbf{B}_t \equiv \mathbf{B}_{\phi(1)} \otimes \cdots \otimes \mathbf{B}_{\phi(t)}$$

(iii) If $\mathbf{A}_i \equiv \mathbf{B}_i$, $i = 1, \ldots, t$, then

$$\mathbf{A}_1 \otimes \cdots \otimes \mathbf{A}_t \equiv \mathbf{B}_1 \otimes \cdots \otimes \mathbf{B}_t, \quad \mathbf{A}_1 \oplus \cdots \oplus \mathbf{A}_t \equiv \mathbf{B}_1 \oplus \cdots \oplus \mathbf{B}_t.$$

Let $\mathbf{A}$ be an associative algebra with identity element 1 and $\{a_1, \ldots, a_n\}$ be a basis of the algebra $\mathbf{A}$. Let

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

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

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

Let $a \in \mathbf{A}$, $a_i\, a = \sum_{k=1}^{n} \sigma_{i,k}\, a_k$, $i = 1, \ldots, n$, and define the square $n \times n$-matrix $A_a = (\sigma_{i,k})$. Then $\mathbf{RR}(\mathbf{A}) = \{A_a \mid a \in \mathbf{A}\}$ form an algebra over F that is isomorphic to $\mathbf{A}$ under the corresponding $a \to A_a$, $\{A_{a_1}, \ldots, A_{a_n}\}$ is a basis for the algebra $\mathbf{RR}(\mathbf{A})$, $A_1 = I_n$, $A_a\, A_b = A_{ab}$, $A_a + A_b = A_{a+b}$, $\lambda A_a = A_{\lambda a}$ for $\lambda \in F$ and if $a\, b = 1$ then $A_a^{-1} = A_b$. The algebra $\mathbf{RR}(\mathbf{A})$ is called the *(right) regular matrix representation* of $\mathbf{A}$. Since $\mathbf{RR}(\mathbf{A})$ is isomorphic to $\mathbf{A}$ we can consider the elements of $\mathbf{A}$ as $n \times n$-matrices in $\mathbf{RR}(\mathbf{A})$, i.e $\mathbf{A}=\mathbf{RR}(\mathbf{A})$ and $a = A_a$.

We define $\mathbf{B}_{\mathbf{A}} = \{B_1, \ldots, B_n\}$ where, for indeterminates $\mathbf{x} = (x_1, \ldots, x_n)$ and $\mathbf{y} = (y_1, \ldots, y_n)$,

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

i.e. the i-th coefficient of the product $x\, y = \left(\sum_{i=1}^{n} x_i\, a_i \right) \left(\sum_{i=1}^{n} y_i\, a_i \right)$.

Let $\mathbf{C}_{\mathbf{A}} = \{a_1, \ldots, a_n\}(=\{A_{a_1}, \ldots, A_{a_n}\})$. Obviously, $\mathbf{B}_{\mathbf{A}}$ and $\mathbf{C}_{\mathbf{A}}$ are dependent on the chosen basis. The connection between $\mathbf{B}_{\mathbf{A}}$ and $\mathbf{C}_{\mathbf{A}}$ is

Lemma 3 . [BF]. We have

$$\mathbf{C}_{\mathbf{A}}^{D} = \mathbf{B}_{\mathbf{A}}.$$

Lemma 4 . Let $\mathbf{A}_1$ and $\mathbf{A}_2$ be algebras. Then, there exist basis for $\mathbf{A}_1$, $\mathbf{A}_2$, $\mathbf{A}_1 \times \mathbf{A}_2$, $\mathbf{A}_1 \otimes \mathbf{A}_2$ such that

$$\mathbf{C}_{\mathbf{A}_1 \times \mathbf{A}_2} = \mathbf{C}_{\mathbf{A}_1} \oplus \mathbf{C}_{\mathbf{A}_2}, \quad \mathbf{B}_{\mathbf{A}_1 \times \mathbf{A}_2} = \mathbf{B}_{\mathbf{A}_1} \oplus \mathbf{B}_{\mathbf{A}_2},$$

$$\mathbf{C}_{\mathbf{A}_1 \otimes \mathbf{A}_2} = \mathbf{C}_{\mathbf{A}_1} \otimes \mathbf{C}_{\mathbf{A}_2}, \quad \mathbf{B}_{\mathbf{A}_1 \otimes \mathbf{A}_2} = \mathbf{B}_{\mathbf{A}_1} \otimes \mathbf{B}_{\mathbf{A}_2},$$

Let $\mathbf{A}$ be a finite dimentional associative algrebra over a field F with identity element. We say that $\mathbf{A}$ is Frobenuis algebra if there exists a non-degenerate bilinear form $f : \mathbf{A} \times \mathbf{A} \to F$ that satisfies

$$f(ab, c) = f(a, bc),$$

for all $a, b, c \in \mathbf{A}$. The reader can find other definitions and properties of Frobenuis algebras in [CR].

The following result that is proved in [BF] will be frequently used in the sequel

<u>**Lemma 5 .**</u> Let $\mathbf{A}$ be an algebra and $\mathbf{A}^-$ be the reciprocal algebra of $\mathbf{A}$. Then,

$$\mathbf{C}_{\mathbf{A}^-} \equiv \mathbf{B}_{\mathbf{A}}$$

if, and only if, $\mathbf{A}$ is Frobenuis algebra.

We now give some examples

<u>**Example 1 . Polynomial algebra**</u>

The *polynomial algebra* is the algebra $F(p) = F[\alpha]/(p(\alpha))$ where $p(\alpha) \in F[\alpha]$. It can be easily shown that, there exist a basis for $F(p)$ such that

$$\mathbf{C}_{F(p)} = \{C_p^0, C_p^1, \ldots, C_p^{deg\, p-1}\},$$

where C_p is the companion matrix of p. So that we can consider $F(p)$ as

$$F(p) = \{\lambda_0 C_p^0 + \cdots + \lambda_{d-1} C_p^{d-1} \mid (\lambda_0, \ldots, \lambda_{d-1}) \in F^d\}$$

where $d = deg\, p$. When p is irreducible, then $F(p)$ is a field and therefore the nonzero matrices in $F(p)$ are nonsingular.

Another property that will be used in the sequel is: Let p and q be two irreducible polynomials such that $gcd(deg\, p, deg\, q) = 1$, i.e $deg\, p$ and $deg\, q$ are relatively primes, then, the matrices

$$\mathbf{C}_{F(p)} \otimes \mathbf{C}_{F(q)} = \{C_p^i \otimes C_q^j \mid i = 0, \ldots, deg\, p - 1, j = 0, \ldots, deg\, q - 1\} \tag{7}$$

are linearly independent matrices and each matrix in $Span(\mathbf{C}_{F(p)} \otimes \mathbf{C}_{F(q)})$, (the linear space spanned by the elements of $\mathbf{C}_{F(p)} \otimes \mathbf{C}_{F(q)}$), has rank $(deg\, p)(deg\, q)$. This property follows from the fact $F_{q^r} \otimes F_{q^s} = F_{q^{rs}}$ when r and s are relatively prime and F_{q^r} is the r-degree extention of the q-element field F_q.

If $p(\alpha) = p_1(\alpha)^{d_1} \cdots p_r(\alpha)^{d_r}$ where $p_1(\alpha), \ldots, p_r(\alpha)$ are distinct irreducible polynomials, then

$$F(p) = F(p_1^{d_1}) \times \cdots \times F(p_r^{d_r}). \tag{8}$$

and it is well known from [CR] that

$$F(p_1^{d_1}) = F(p_1) \otimes F(\alpha^{d_1}). \tag{9}$$

This algebra also satisfies

Lemma 6 . The algebra $F(p)$ is Frobenius algebra.

In [BF] we proved

Lemma 7 .

(i) A commutative algebra $\mathbf{A}$ is Frobenius algebra if, and only if, $\mathbf{A}$ is a direct product of Frobenius commutative local algebras.

(ii) A local algebra $\mathbf{A}$ is Frobenius algebra if, and only if, there exist $d \in \mathbf{A}$ such that

$$\{a \mid a \, rad\, A = 0\} = d\,A.$$

Example 2 . Matrices over polynomial algebras .

The matrices over polynomial algebra $F(p)$ is the algebra

$$\mathbf{M}_n \otimes F(p),$$

where $\mathbf{M}_n$ is the total $n \times n$-matrix algebra. We shall consider $\mathbf{M}_n$ as (the regular matrix representation)

$$\mathbf{M}_n = \{I_n \otimes M \mid M \in F^{n \times n}\},$$

where $F^{n \times n}$ is the set of the square $n \times n$-matrices over the field F.

It is known from [CR] that matrices over Frobenius algebras are Frobenius algebras.

3. BOUNDS ON LINEAR CODES AND COMPLEXITY

Let n be an integer. A *linear code* over F of length n is a linear subspace C of F^n. If $dim\ C = k$, then C is called $[n, k]$ code. For $c \in C$ the *weight* of c, denoted by $wt(c)$, is the number of the nonzero components of c. The *minimal weight* of C is **min** $\{wt(c) \mid c \in C - \{0\}\}$. We say that C is a $[n, k, d]$ *code* if, $C \subseteq F^n$ is a code of dimension k and minimal weight d. Let $N_F(k, d)$ be the smallest integer such that there exist a $[N_F(k, d), k, d]$ code. When F is the binary field we simply write $N(k,d)$. The connection between the linear codes and the complexity of quadratic forms over F is given in the following lemma.

<u>Lemma 8 .</u> [BD], [LW] . Let $\mathbf{B} = \{B_1, \ldots, B_k\}$ be a set of $n \times m$ matrices and let $Span(\mathbf{B})$ be the linear space spanned by the elements of $\mathbf{B}$. Let $d = \min_{B' \in \mathbf{B}} \mathbf{rank}\ B'$ and $k = dim\ Span(\mathbf{B})$. Then

$$\mathbf{L}(\mathbf{B}) \geq N_F(k,d).$$

The next two lemmas give lower bounds for $N_F(k,d)$.

<u>Lemma 9 .</u> (Griesmer Bound [L, p. 59]). We have

$$N_F(k,d) \geq \sum_{i=0}^{k-1} \left\lceil \frac{d}{|F|^i} \right\rceil \geq \begin{cases} \left\lceil \left(1 + \frac{1}{|F|-1} - \frac{1}{|F|^{k-1}(|F|-1)}\right) d \right\rceil & \text{if } k \leq \log_{|F|} d \\ \left\lceil \left(1 + \frac{1}{|F|-1}\right) d + k - \log_{|F|} d - 3, \right. & \text{if } k > \log_{|F|} d. \end{cases}$$

When F is the binary field, then we have the following asymptotic bound

<u>Lemma 10 .</u> (MRRW [L]): For sufficient large $N(k,d)$ with $d/N(k,d) \to \delta$ we have

$$\frac{k}{N(k,d)} \leq H_2\left(\frac{1}{2} - \sqrt{\delta^2 - \delta}\right)(1 + o(1)).$$

where

$$H_2(x) = -x \log_2 x - (1-x)\log_2(1-x).$$

Another lower bound techniques known from the literature for the complexity of quadratic algorithms are

<u>Lemma 11 .</u> [BD]. Let $\mathbf{B} = \{B_1, \ldots, B_{k_1}\}$ and $\mathbf{C} = \{C_1, \ldots, C_{k_2}\}$ be sets of $n \times m$-matrices. Then

$$\mathbf{L}(\mathbf{C} \cup \mathbf{B}) \geq dim\ Span(\mathbf{C}) + \min_{\lambda_{i,j} \in F} \mathbf{L}(\{B_1 + \sum_{j=1}^{k_2} \lambda_{1,j} C_j, \ldots, B_{k_1} + \sum_{j=1}^{k_2} \lambda_{k_1,j} C_j\}),$$

where $Span(\mathbf{C})$ is the linear space spanned by the elements of $\mathbf{C}$.

Notice that the results in lemma 8 and 11 are also true for the bilinear complexity $\mathbf{R}$.

<u>Lemma 12 .</u> Let $\mathbf{B}$ and $\mathbf{C}$ be sets of matrices. If $\mathbf{B} \equiv \mathbf{C}$, then

$$\mathbf{L}(\mathbf{B}) = \mathbf{L}(\mathbf{C}), \quad \mathbf{R}(\mathbf{B}) = \mathbf{R}(\mathbf{C}).$$

If $Span(\mathbf{B}) \subseteq Span(\mathbf{C})$, then

$$\mathbf{L}(\mathbf{B}) \le \mathbf{L}(\mathbf{C}), \quad \mathbf{R}(\mathbf{B}) \le \mathbf{R}(\mathbf{C}).$$

The duality lemma is

Lemma 13 . [HMu]. Let $\mathbf{B} = \{B_1, \ldots, B_n\}$ and $\mathbf{C} = \{C_1, \ldots, C_n\}$ be sets of $n \times n$-matrices. If $\mathbf{B} \equiv \mathbf{C}^D$, then

$$\mathbf{R}(\mathbf{B}) = \mathbf{R}(\mathbf{C}).$$

Therefore, for any algebra **A**

$$\mathbf{R}(\mathbf{A}) = \mathbf{R}(\mathbf{B_A}) = \mathbf{R}(\mathbf{C_A}),$$

and for Frobenius algebras **A** we have

$$\mathbf{L}(\mathbf{A}) = \mathbf{L}(\mathbf{B_A}) = \mathbf{L}(\mathbf{C_A}).$$

4. LOWER BOUND FOR POLYNOMIAL ALGEBRAS

In this section we prove corollary I

We say that the set of independent matrices **B** is (k, l, d)–set if $|\mathbf{B}| = k$ and there exist $k-l$ matrices $B_1, \ldots, B_{k-l} \in \mathbf{B}$ such that: For every $B \notin Span(\mathbf{B})$, we have, (we remind the reader that $Span(\mathbf{B})$ is the linear space spanned by the elements of **B**)

$$\textbf{rank}\ B \ge d.$$

The following lemma will be used to find lower bounds for the complexity of direct product of algebras

Lemma 14 . If $\mathbf{B}^{(i)}$, are (k_i, l, d_i)–set, $i = 1, \ldots, s$, then

$$\mathbf{L}(\mathbf{B}^{(1)} \oplus \cdots \oplus \mathbf{B}^{(s)}) \ge \sum_{i=1}^{s} k_i - s\,l + N_F(l, \sum_{i=1}^{s} d_i).$$

Proof . Let $\mathbf{B}^{(i)} = \{B_1^{(i)}, \ldots, B_l^{(i)}, B_{l+1}^{(i)}, \ldots, B_{k_i}^{(i)}\}$, $i = 1, \ldots, s$, such that, for any $B \notin Span(\{B_{l+1}^{(i)}, \ldots, B_{k_i}^{(i)}\})$, $i = 1, \ldots, s$,

$$\textbf{rank}\ B \ge d_i.$$

Consider the following subsets of $\mathbf{B}^{(1)} \oplus \cdots \oplus \mathbf{B}^{(s)}$,

$$\mathbf{V}_1 = \{diag(B_i^{(1)}, B_i^{(2)}, \ldots, B_i^{(s)}) \mid i = 1, \ldots, l\}.$$

and

$$\mathbf{V}_2 = \{diag\,(B_{i_1}^{(1)}, \ldots, B_{i_s}^{(s)}) \mid i_\alpha = l+1, \ldots, k_\alpha, \alpha = 1, \ldots, s\}.$$

By lemma 11 and 12,

$$\mathbf{L}(\mathbf{B}^{(1)} \oplus \cdots \oplus \mathbf{B}^{(s)}) \geq \mathbf{L}(\mathbf{V}_1 \cup \mathbf{V}_2) \geq |\mathbf{V}_2| + \min_{\lambda \in F^{k_1 + \cdots + k_s}} \mathbf{L}(\mathbf{S}_\lambda) \tag{10}$$

where, for $\lambda = (\lambda_{1,1}, \ldots, \lambda_{1,k_1}, \lambda_{2,1}, \ldots, \lambda_{2,k_2}, \ldots, \lambda_{s,1}, \ldots, \lambda_{s,k_s})$, we have

$$\mathbf{S}_\lambda = \left\{ diag\,(B_i^{(1)} + \sum_{j=l+1}^{k_1} \lambda_{1,j} B_j^{(1)}, \ldots, B_i^{(s)} + \sum_{j=l+1}^{k_s} \lambda_{s,j} B_j^{(s)}) \;\middle|\; i = 1, \ldots, l \right\}.$$

Since every nonzero element in $Span\,(\mathbf{S}_\lambda)$ is of the form

$$P = diag\left[\sum_{i=1}^{l} \delta_{1,i} B_i^{(1)} + \sum_{j=l+1}^{k_1} \lambda'_{1,j} B_j^{(1)} \;, \ldots, \; \sum_{i=1}^{l} \delta_{1,i} B_i^{(s)} + \sum_{j=l+1}^{k_s} \lambda'_{s,j} B_j^{(s)} \right]$$

where not all $\delta_{1,i}$ are zero, and since

$$G_i = \sum_{i=1}^{l} \delta_{1,i} B_i^{(h)} + \sum_{j=l+1}^{k_h} \lambda_{h,j} B_j^{(h)} \notin Span\,(\{B_{l+1}^{(h)}, \ldots, B_{k_h}^{(h)}\}) \;, \quad h = 1, \ldots, s,$$

we have

$$\mathbf{rank}\; P = \sum_{i=1}^{s} \mathbf{rank}\; G_i \geq \sum_{i=1}^{s} d_i$$

and therefore, by lemma 8, we have

$$\mathbf{L}(S_\lambda) \geq N_F\,(l, \sum_{i=1}^{s} d_i). \tag{11}$$

Since $|V_2| = \left(\sum_{i=1}^{s} k_i\right) - s\,l$, by (10) and (11), the result follows. □

Let $i_F(n)$ denote the maximal possible number of distinct irreducible factors of a polynomial of degree n over the field F. It is known from [KB] that

Lemma 15 . For sufficient large n we have

$$i_F(n) \leq \frac{2n}{\log_{|F|} n}.$$

For integers $1 \leq j \leq m$ we define the $m \times m$ Hankel matrix

$$I_m^{(j)} = \begin{bmatrix} 0 & \cdots & 0 & 1 & 0 & \overset{j-1}{\cdots} & 0 \\ 0 & \cdots & 0 & 0 & 1 & 0 & 0 \\ \vdots & \cdots & \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 1 \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \cdots & \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \end{bmatrix}$$

i.e,

$$I_m^{(j)}[i,k] = \begin{cases} 1 & \text{if } m-i-k+2=j, \\ 0 & \text{otherwise.} \end{cases}$$

It is well known that for some basis of $\mathbf{A} = F(\alpha^n) = F[\alpha]/(\alpha^m)$, the regular matrix representation of $\mathbf{A}$ is

$$\mathbf{A} = \{I_m^{(j)} \mid j = 1, \ldots, m\}.$$

We now prove corollary I

<u>**Theorem 1 .**</u> Let $p(\alpha)$ be any polynomial of degree n. Then

$$\mathbf{L}(F(p)) \geq \left[2 + \frac{1}{|F|-1} \right] n - o(n).$$

Proof . Let $p = p_1^{d_1} \cdots p_k^{d_k}$ where $p_1, \ldots, p_k$ are distinct irreducible polynomials, $deg\ p = n$, $deg\ p_i^{d_i} = s_i = r_i d_i$, $deg\ p_i = r_i$ and $s_1 \leq \cdots \leq s_k$. Then, by (8) and (9), we have

$$F(p) = (F(\alpha^{d_1}) \otimes F(p_1)) \oplus \cdots \oplus (F(\alpha^{d_k}) \otimes F(p_k)),$$

and therefore, by lemma 4, we can choose a basis such that, the regular matrix representation of $F(p)$ is

$$F(p) = \left\{ diag\,((I_{d_1}^{(i_1)} \otimes C_{p_1}^{j_1}), \ldots, (I_{d_k}^{(i_k)} \otimes C_{p_k}^{j_k})) \;\middle|\; 1 \leq i_l \leq d_l, 0 \leq j_l \leq r_l - 1, l = 1, \ldots, k \right\},$$

and C_{p_k} is the companion matrix of p_k.

Let w be an integer such that

$$deg\ p_1^{d_1} \cdots p_w^{d_w} \geq n^{1/2} \quad , \quad deg\ p_1^{d_1} \cdots p_{w-1}^{d_{w-1}} < n^{1/2}.$$

By lemma 15, we have

$$w < \frac{2n^{1/2}}{\log_{|F|} n}.$$

Since $deg\ p_1^{d_1} \cdots p_w^{d_w} \ge n^{1/2}$, we have

$$deg\ p_w^{d_w} \ge \frac{n^{1/2}}{w} > \frac{1}{2}\log_{|F|} n,$$

which implies

$$s_i = deg\ p_i^{d_i} > \frac{1}{2}\log_{|F|} n \quad , \quad i = w, w+1, \ldots, k.$$

Let

$$m_i = \left\lceil \frac{\log_{|F|} \log n}{r_i} \right\rceil \ , i = w, \ldots, k, \tag{12}$$

$$\mathbf{B}_i = \{ I_{d_i}^{(j)} \otimes C_{p_i}^l \mid 1 \le j \le d_i\ ,\ 0 \le l \le r_i - 1 \},$$

and

$$\mathbf{W}_i = \{ I_{d_i}^{(j)} \otimes C_{p_i}^l \mid d_i - m_i + 1 \le j \le d_i\ ,\ 0 \le l \le r_i - 1 \} \ , i = w, \ldots, k.$$

Since $|\mathbf{W}_i| = m_i r_i \ge \log_{|F|} \log n$ we can find a subset $\mathbf{V}_i \subseteq \mathbf{W}_i$ such that

$$|\mathbf{V}_i| = \left\lceil \log_{|F|} \log n \right\rceil ,\ i = w, \ldots, k.$$

We shall prove now that $\mathbf{B}_i$ is $\left(s_i , \left\lceil \log_{|F|} \log n \right\rceil , s_i - m_i r_i + r_i \right)$-set for $i = w, \ldots, k$. Obviously, $|\mathbf{B}_i| = s_i = r_i d_i$. We also have, for $\delta_V \in F$ not all zero and any $\eta_V \in F$

$$P = \sum_{V \in \mathbf{V}_i} \delta_V V + \sum_{V \in \mathbf{B}_i - \mathbf{V}_i} \eta_V V \notin Span\,(\mathbf{B}_i - \mathbf{V}_i)$$

and P can be written as

$$P = \sum_{j=0}^{d} \left(I_{d_j}^{(j)} \otimes \sum_{l=0}^{r_i - 1} \lambda_{i,l,j} C_{p_i}^l \right).$$

Since δ_V are not all zero, $\sum_{l=0}^{r_i-1} \lambda_{i,l,j_0} C_{p_i}^l \ne 0$ for some $d_i - m_i + 1 \le j_0 \le d_i$ and therefore, since P is a triangular block matrix,

$$\mathbf{rank}\ (P_i) \ge \mathbf{rank} \left(I_{d_{j_0}}^{(j_0)} \otimes \sum_{l=0}^{r_i-1} \lambda_{i,l,j_0} C_{p_i}^l \right) = j_0 r_i \ge (d_i - m_i + 1) r_i = s_i - m_i r_i + r_i .$$

This prove that B_i is $\left(s_i , \left\lceil \log_{|F|} \log n \right\rceil , s_i - m_i r_i + r_i \right)$-set. Now, since $F(p)$ is Frobenuis algebra and by lemma 13 and 14, we have

$$\mathbf{L}(F(p)) = \mathbf{L}(\mathbf{B}_{F(p)}) = \mathbf{L}(\mathbf{C}_{F(p)}) \ge$$

$$\mathbf{L}(\overbrace{\{0\} \oplus \cdots \oplus \{0\}}^{w\ times} \oplus \mathbf{B}_{w+1} \oplus \cdots \oplus \mathbf{B}_k) = \mathbf{L}(\mathbf{B}_{w+1} \oplus \cdots \oplus \mathbf{B}_k) \ge \tag{*}$$

$$\sum_{i=w}^{k} s_i - (k \log_{|F|} \log n) + N_F \left(\log_{|F|} \log n , \sum_{i=w}^{k} (s_i - m_i r_i + r_i) \right).$$

We have

$$\sum_{i=w}^{k} s_i = deg\, p_w^{d_w} \cdots p_k^{d_k} \geq n - n^{1/2},$$

by lemma 14,

$$k < \frac{2n}{\log_{|F|} n},$$

and, therefore,

$$k \log_{|F|} \log n = o(n),$$

and by (12)

$$\sum_{i=w}^{k} (s_i - m_i r_i + r_i) \geq n - n^{1/2} - \sum_{i=w}^{k} (m_i - 1) r_i \geq n - n^{1/2} - k \log_{|F|} \log n.$$

$$\geq n - n^{1/2} - \frac{2n}{\log_{|F|} n} (\log_{|F|} \log n) = n - o(n).$$

Therefore,

$$\mathbf{L}(F(p)) \geq n + N_F \left(\left\lceil \log_{|F|} \log n \right\rceil , n - o(n) \right) - o(n).$$

Now, by lemma 9, we have

$$N_F \left(\left\lceil \log_{|F|} \log n \right\rceil , n - o(n) \right) \geq \left(1 + \frac{1}{|F| - 1} - \frac{1}{|F|^{\left\lceil \log_{|F|} \log n \right\rceil} - |F|} \right) (n - o(n))$$

$$= \left(1 + \frac{1}{|F| - 1} \right) n - o(n),$$

which with (*) implies

$$\mathbf{L}(F(p)) \geq \left(2 + \frac{1}{|F| - 1} \right) n - o(n). \quad \square$$

5. LOWER BOUNDS FOR ALGEBRAS WITH ONE MAXIMAL IDEAL

In this section we shall prove a general result for algebras with one maximal ideal which, in particular, implies corollary II.

Let $\mathbf{A}$ be an algebra with one maximal ideal. It is known that $\mathbf{A} / rad\, \mathbf{A} = \mathbf{M}_n \otimes \mathbf{D}$ where $\mathbf{M}_n$ is the total $n \times n$-matrix algebra and $\mathbf{D}$ is a division algebra. If F is finite field, then $\mathbf{D} = F(p)$ for some irreducible polynomial p, i.e, **D** is a field over F. For the algebra **A** we prove the following lower bound

<u>**Theorem 2 .**</u> Let A be an algebra such that $\mathbf{A}/rad\,\mathbf{A} = \mathbf{M}_n \otimes F\ (p)$ where $p\,(\alpha)$ is irreducible polynomial of degree d. Let m ,s and r be integers, $n = m\,s + r$ where $r \ge s \ge 1$ or $r = 0$, $gcd\ (s\ ,d\ ) = 1$ and if $r \ne 0$, then $gcd\ (r\ ,d\ ) = 1$. Then

$$\mathbf{R}(\mathbf{A}) \ge \Delta_{s,r}(\mathbf{A}) = \frac{1}{2}\,dim\ \mathbf{A} + dim\ rad\ \mathbf{A} + N_F\left[\,s\ deg\ p\ ,\ dim\ \mathbf{A}\right] - \frac{1}{2}(ns + r^2 - rs)\ deg\ p.$$

If **A** is Frobenuis algebra, then

$$\mathbf{L}(\mathbf{A}) \ge \Delta_{s,r}(\mathbf{A}).$$

Proof . Let

$$f : \mathbf{A} \to \mathbf{A}/rad\ \mathbf{A} = \mathbf{M}_n \otimes F(p)$$

be a canonical projection and let B be a complementary subspace for rad **A**, i.e, (here $\oplus$ is direct sum of linear spaces)

$$\mathbf{A} = rad\ \mathbf{A} \oplus B.$$

Let $a_1, \ldots, a_t$ be a basis for rad **A** and $a_{t+1}, \ldots, a_k$ be a basis for B. By lemma 11 and 13, we have, (we remind the reader that we consider the elements in the algebras **A** and $\mathbf{A}/rad$ **A** as matrices in the regular matrix representation)

$$\begin{aligned}\mathbf{R}(\mathbf{A}) = \mathbf{R}(\mathbf{B}_\mathbf{A}) &= \mathbf{R}(\mathbf{C}_\mathbf{A}) = \mathbf{R}(\{a_1, \ldots, a_t, a_{t+1}, \ldots, a_k\}) \\ &\ge dim\ rad\ \mathbf{A} + \min_{\lambda_{i,j} \in F} \mathbf{R}\left[\left\{\ a_{t+1} + \sum_{j=1}^{t}\lambda_{1,j}\,a_j\ ,\ \ldots\ ,\ a_k + \sum_{j=1}^{t}\lambda_{k-t,j}\,a_j\right\}\right]. \qquad (13)\end{aligned}$$

For some $\lambda_{i,j} \in F$, let $g_i = a_{t+i} + \sum_{j=1}^{t}\lambda_{i,j}a_j$, $i = 1, \ldots, k-t$ and $G = Span\ (\{g_1, \ldots, g_{k-t}\})$, the linear space spanned by $g_1, \ldots, g_{k-t}$. Since, also $\mathbf{A} = rad\ \mathbf{A} \oplus G$, (as linear spaces), we have $\theta = f\ |_G : G \to \mathbf{A}/rad\ \mathbf{A}$ is nonsingular linear transformation of the linear space G onto $\mathbf{A}/rad\ \mathbf{A}$. By examples 1 and 2, we have

$$\mathbf{A}/rad\ \mathbf{A} = \mathbf{M}_n \otimes F(p) \equiv \{I_n \otimes M \otimes C\ \mid M \in F^{n \times n}, C \in F\ (p\ )\}.$$

Let $n = m\,s + r$ where $gcd\ (s\ ,d\ ) = gcd\ (r\ ,d\ ) = 1$ and $r \ge s \ge 1$, (the proof for the case $r = 0$ is similar), and let $q\,(\alpha)$ and $w\,(\alpha)$ be irreducible polynomials over F of degree s and r, respectively. Consider the following subsets of $\mathbf{A}/rad$ **A**,

$$S_1 = \left\{ I_n \otimes diag\,(\overbrace{C_q^i, \ldots, C_q^i}^{m\ times}, C_w^i) \otimes C_p^j \mid i = 0, \ldots, deg\, q - 1\ ,\ j = 0, \ldots, deg\, p - 1 \right\} \quad (14)$$

and

$$S_2 = \{ I_n \otimes E_{i,k} \otimes C_p^j \mid j = 0, \ldots, deg\, p - 1\,,\ (i, k) \in \mathbf{I} \} \quad (15)$$

where $\{ E_{i,k} \}$ is the standard basis of $F^{n \times n}$ and

$$\mathbf{I} = \{ (i, k) \mid (s+1 \le i \le n-r \text{ and } 1 \le k \le (\lceil i/s \rceil - 1)s)\ or \quad (16)$$
$$(n-r+1 \le i \le n \text{ and } 1 \le k \le n-r) \}.$$

Obviously, $Span\,(S_1) \cup Span\,(S_2) \subset \mathbf{A}/rad\,\mathbf{A}$ and $Span\,(S_1) \cap Span\,(S_2) = \emptyset$. Consider the following sets

$$\Pi_1 = \theta^{-1}(S_1),\ \ \Pi_2 = \theta^{-1}(S_2).$$

Then $Span\,(\Pi_1 \cup \Pi_2)$ is a subset of $Span\,(G)$. Since θ is nonsingular, $Span\,(\Pi_1) \cap Span\,(\Pi_2) = \emptyset$, and $dim\ Span\,(\Pi_1) \oplus Span\,(\Pi_2) = |\,\Pi_1 \cup \Pi_2\,|$. Therefore, by lemma 12,

$$\mathbf{R}\left[\left\{ a_{t+1} + \sum_{j=1}^{t} \lambda_{1,j}\, a_j\ , \ldots ,\ a_k + \sum_{j=1}^{t} \lambda_{k-t,j} a_j \right\} \right] = \mathbf{R}(\{ g_1, \ldots, g_{k-t} \}) \ge \mathbf{R}(\Pi_1 \cup \Pi_2). \quad (17)$$

Let $\Pi_1 = \{ D_1, \ldots, D_{\tau_1} \}$ and $\Pi_2 = \{ \tilde{D}_1, \ldots, \tilde{D}_{\tau_2} \}$. By lemma 11, we have

$$\mathbf{R}(\Pi_1 \cup \Pi_2) \ge |\,\Pi_2\,| + \mathbf{min}_{\eta_{i,j}}\ \mathbf{R}\left[\left\{ D_1 + \sum_{j=1}^{\tau_2} \eta_{1,j} \tilde{D}_j, \ldots, D_{\tau_1} + \sum_{j=1}^{\tau_2} \eta_{\tau_1,j} \tilde{D}_j \right\} \right]. \quad (18)$$

Let $0 \ne \mathbf{D} = Span\left[\left\{ D_1 + \sum_{j=1}^{\tau_2} \eta_{1,j} \tilde{D}_j, \ldots, D_{\tau_1} + \sum_{j=1}^{\tau_2} \eta_{\tau_1,j} \tilde{D}_j \right\} \right]$. We now prove that all the the nonzero elements in $\mathbf{D}$ are nonsingular. Let $D \in \mathbf{D}$, then

$$D = \sum_{i=1}^{\tau_1} c_i D_i + \sum_{i=1}^{\tau_2} d_i \tilde{D}_i,$$

where $c_i, d_i \in F$ and not all c_i are zero. To prove that D is a nonsingular element in $\mathbf{A}$ it is suffices to show that $P = \theta(D)$ is nonsingular in $\mathbf{A}/rad\,\mathbf{A}$. We have

$$P = \theta(D) = \sum_{i=1}^{\tau_1} c_i \theta(D_i) + \sum_{i=1}^{\tau_2} d_i \theta(\tilde{D}_i).$$

Since $\theta(D_i) \in S_1$ and $\theta(\tilde{D}_i) \in S_2$, the matrix P is of the form

$$P = \sum_{i,j} e_{i,j} (I_n \otimes diag\,(\overbrace{C_q^i, \ldots, C_q^i}^{m\ times}, C_w^i) \otimes C_p^j) + \sum_{(i,k) \in \mathbf{I},\, j} f_{i,j,k} (I_n \otimes E_{i,k} \otimes C_p^j),$$

where $e_{i,j}, f_{i,j} \in F$, and not all $e_{i,j}$ are zero. Because P has the first summand in the diagonal, and, the second summand effect only below the diagonal of P (see the definition of **I**), we have

$$\det(P) = \det\left[\sum_{i,j} e_{i,j}\,(I_n \otimes diag\,(\overbrace{C_q^i,\ldots,C_q^i}^{m\ times},C_w^i)\otimes C_p^j)\right].$$

To prove that $\det(P)\neq 0$, observe that

$$diag\,(\overbrace{C_q^i,\ldots,C_q^i}^{m\ times},C_w^i)\otimes C_p^j = diag\,(\overbrace{C_q^i\otimes C_p^j,\ldots,C_q^i\otimes C_p^j}^{m\ times},C_w^i\otimes C_p^j).$$

Now, because $gcd\,(deg\ p\,, deg\ q\,) = gcd\,(deg\ p\,, deg\ w\,) = 1$ we have, by (7),

$$H = \{C_q^i \otimes C_p^j \mid i = 0,\ldots, deg\ q-1, j = 0,\ldots, deg\ p-1\}$$

is a set of independent matrices and each matrix in $Span\ (H\,)$ has rank $deg\ p\ deg\ q$. The same property also hold for

$$H' = \{C_w^i \otimes C_p^j \mid i = 0,\ldots, deg\ q-1, j = 0,\ldots, deg\ p-1\}$$

since $deg\ q = s < r = deg\ w$. In particular, since not all $e_{i,j}$ are zero, we have

$$\det\left[\sum_{i,j} e_{i,j}\,(C_q^i\otimes C_p^j)\right]\neq 0\ ,\quad \det\left[\sum_{i,j} e_{i,j}\,(C_w^i\otimes C_p^j)\right]\neq 0.$$

Hence,

$$\begin{aligned}
\det(P) &= \det\left[\sum_{i,j} e_{i,j}\,(I_n \otimes diag\,(\overbrace{C_q^i,\ldots,C_q^i}^{m\ times},C_w^i)\otimes C_p^j)\right]\\
&= \det\left[\sum_{i,j} e_{i,j}\,(I_n \otimes diag\,(\overbrace{C_q^i\otimes C_p^j,\ldots,C_q^i\otimes C_p^j}^{m\ times},C_w^i\otimes C_p^j))\right]\\
&= \det\left[I_n \otimes diag\left[\overbrace{\sum_{i,j} e_{i,j}\,(C_q^i\otimes C_p^j),\ldots,\sum_{i,j} e_{i,j}\,(C_q^i\otimes C_p^j)}^{m\ times},\sum_{i,j} e_{i,j}\,(C_w^i\otimes C_p^j)\right]\right]\\
&= \det(I_n)\det\left[\sum_{i,j} e_{i,j}(C_q^i\otimes C_p^j)\right]^m \det\left[\sum_{i,j} e_{i,j}(C_w^i\otimes C_p^j)\right]\neq 0\,.
\end{aligned}$$

This prove that all the nonzero elements in **D** are nonsingular and, therefore, has rank dim **A**. Therefore, by lemma 8, we have

$$\mathbf{R}\left[\left\{D_1+\sum_{j=1}^{\tau_2}\eta_{1,j}\tilde{D}_j\,,\ldots, D_{\tau_1,1}+\sum_{j=1}^{\tau_2}\eta_{\tau_1,1}\tilde{D}_j\right\}\right]\geq N_F\left[\,|\Pi_1|\,, dim\ \mathbf{A}\right]. \tag{19}$$

Now, by (14), (15) and (16) and since θ is nonsingular we have

$$|\Pi_1| = |S_1| = s\ deg\ p,$$

$$|\Pi_2| = |S_2| = \left[\frac{m^2-m}{2}s^2+s\,r\,m\right] deg\ p = \frac{1}{2}n^2 deg\ p - \frac{1}{2}(n\,s+r^2-r\,s\,)deg\ p\,,$$

and therefore, by (13), (14), (18) and (19) and since $n^2 deg\ p = dim\ \mathbf{A}$, we obtain

$$\mathbf{R}(\mathbf{A}) \geq \frac{1}{2} \, dim\ \mathbf{A} + dim\ rad\ \mathbf{A} + N_F \left[s\ deg\ p\ ,\ dim\ \mathbf{A} \right] - \frac{1}{2}(n\ s + r^2 - r\ s)\, deg\ p\ = \Delta_{s,r}(\mathbf{A}),$$

which implies the result.

If **A** is Frobenuis algebra, then, by lemma 13, we have, (the proof is also valid for $\mathbf{L}(\mathbf{C_A})$)

$$\mathbf{L}(\mathbf{A}) = \mathbf{L}(\mathbf{B_A}) = \mathbf{L}(\mathbf{C_A}) \geq \Delta_{s,r}(\mathbf{A}). \ \square$$

We first show that this theorem includes all the results known from the literature about lower bounds for algebras over finite fields.

<u>**Corollary 1 .**</u> [BD], [LSW] . We have

$$\mathbf{L}_{F_2}(F_{2^k}) \geq 3.52 \ , \qquad \mathbf{L}_{F_q}(F_{q^k}) \geq \left[2 + \frac{1}{q+1} \right] k - O(\log k).$$

Proof . The algebras in the corollary are $\mathbf{A} = \mathbf{M}_1 \otimes F(p)$ for irreducible polynomial p of degree k over the field $F = F_2$ and $F = F_q$, respectively. Now applying theorem 2 for $n = 1 = m\ s + r$, $m = 1$, $s = 1$, $r = 0$, we obtain

$$\mathbf{L}(\mathbf{A}) \geq \Delta_{1,0}(F(p)) = N_F(k, k),$$

which by lemmas 9 and 10 follows the result. $\square$

<u>**Corollary 2 .**</u> [B1] . We have

$$\mathbf{L}_{F_2}(\mathbf{M}_n) \geq 2.5 n^2 - \frac{1}{2} n \log n - O(n).$$

Proof . In this algebra we have $deg\ p = d = 1$. Set $s = \lfloor \log n \rfloor$ and $r = (n\ mod\ s) + s$. Then, by theorem 2, we have

$$\mathbf{L}(\mathbf{M}_n) \geq \Delta_{s,r}(\mathbf{A}) = \frac{1}{2} n^2 + N_F(\lfloor \log n \rfloor, n^2) - \frac{1}{2} n \log n + O(\log^2 n)$$
$$= 2\frac{1}{2} n^2 - \frac{1}{2} n \log n + O(n). \ \square$$

We now generalize the result in corollary 2 to simple algebras over the binary field

<u>**Corollary 3 .**</u> Let $p \in F[\alpha]$ be an irreducible polynomials of degree d. If F is the binary field, then for any n and d that satisfy $d = o(\log n)$ or $d = O(\log n)$ or $\log n = o(d)$, we have

$$\mathbf{L}(\mathbf{M}_n(F) \otimes F(p)) \geq 2.5 n^2 deg\ p - o(n^2 deg\ p).$$

Proof . Suppose $d = o(\log n)$. Let i_0 be the least positive integer such that

$$s = \left\lceil \frac{\log n}{d} \right\rceil + i_0 \equiv 1 \, (mod \; d). \qquad (20)$$

Then

$$\frac{\lfloor \log n \rfloor}{d} \le s \le \frac{\log n}{d} + d + 1 \le 2 \log n \, .$$

Suppose $n = s\,m + r_0$, $0 \le r_0 < s$. We choose $r = r_0 + s\,((1-r_0) \; mod \; d)$, where, here, $(x \; mod \; d)$ means the least *positive* integer that equal to x modulo d. Then, $r \ge s$ and $n = s\,(m-\lambda)+(r_0+s\,\lambda)$ for $\lambda = (1-r_0) \, mod \; d$. Now, since $r \equiv r_0 + s\,(1-r_0) \equiv 1 \; (mod \; d)$, with (20), we have

$$gcd\,(s\,,d\,) = gcd\,(r\,,d\,) = 1\,.$$

We also have

$$r = r_0 + s\,((1-r_0) \; mod \; d\,) \le s + s\,d \le 2(\log n + d^2 + d\,) = o\,(\log^2 n\,).$$

Now, applying theorem 2, we have

$$\mathbf{L}(\mathbf{A}) \ge \frac{1}{2} n^2 d + N_F\,(\lfloor \log n \rfloor \,, n^2 d\,) - o\,(n \log^2 n\,)$$

$$\ge 2\frac{1}{2} n^2 d - o\,(n^2).$$

If $d = O\,(\log n\,)$ or $\log n = o\,(d\,)$, then setting $s = 1$, $r = 0$, we obtain

$$\mathbf{L}(\mathbf{A}) \ge \frac{1}{2} n^2 d + N_F\,(d\,, n^2 d\,) - \frac{1}{2} n\,d$$

$$= 2\frac{1}{2} n^2 d - \frac{n^2 d}{2^{d-1}} - \frac{1}{2} n\,d = 2\frac{1}{2} n^2 d - o\,(n^2 d\,). \quad \square$$

Let $\mathbf{A}$ be an algebra such that $\mathbf{A}/rad\;\mathbf{A} = \mathbf{M}_2 \otimes F\,(p\,)$. The bound of Alder and Strassen in [AS] gives $\mathbf{R}(\mathbf{A}) \ge 2 \; dim \; \mathbf{A} - 1$. By theorem 2, we have

$$\mathbf{R}(\mathbf{A}) \ge dim \; \mathbf{A} - 3\,deg\;p + N_F\,(deg\;p\,,\, dim\;\mathbf{A})$$

and, if $deg\;p$ is odd, then we have

$$\mathbf{R}(\mathbf{A}) \ge dim \; \mathbf{A} - 4\,deg\;p + N_F\,(2\,deg\;p\,,\, dim\;\mathbf{A})$$

Then the following bounds are obtained

(i) If $\mathbf{A}/rad\;\mathbf{A} = \mathbf{M}_2$, then $\mathbf{R}(\mathbf{A}) \ge \left(2 + \frac{1}{|F|} \right) dim\;\mathbf{A} - 4$.

(ii) If $deg\;p = 2$, then $\mathbf{R}(\mathbf{A}) \ge \left(2 + \frac{1}{|F|} \right) dim\;\mathbf{A} - 3$.

(*iii*) If $deg\ p = 3$, then $\mathbf{R}(\mathbf{A}) \ge \left(2 + \frac{1}{|F|-1} - \frac{1}{|F|^5(|F|-1)} \right) dim\ \mathbf{A} - 12$.

(*iv*) If $deg\ p > O(1)$, then $\mathbf{R}(\mathbf{A}) \ge \left(2 + \frac{1}{|F|-1} \right) dim\ \mathbf{A} - o(dim\ \mathbf{A})$ □.

REFERENCES

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

[BC] W. Büchi, M. Clusen, On a class of primary algebra of minimal rank. *Linear Algebra and its Application.* **69** (1985), 249-268.

[BD] R.W. Brockett, D. Dobkin, On the number of multiplications required for a matrix multiplication, *SIAM J.Comput.* **5** (1976), 624-628.

[BF] N. H. Bshouty, H. K. Farhat, On the regular representation of algebras, TR 89/365/27, U. of Calgary.

[CC] D. V. Chudnovsky, G. V. Chudnovsky, Algebraic complexities and algebraic curves over finite fields, *Proc. Nate. Acad. Sci. USA* **84** (1987), 1739-1743.

[CR] C. W. Curtis, I. Reiner, Representation theory of finite groups and associative algebras, Wiley classics library edition published 1988.

[CW] D. Coppersmith, S. Winograd, Matrix multiplication via arithmetic progressions, Proceedings 19st Annual ACM Symposium on Theory of Computing, (May 1987).

[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.

[Gr] D. Yu. Grigorive, Multiplicative complexity of a pair of bilinear forms and of polynomial multiplication, *Lecture Note in Computer Sci. vol.* **46** , (1978), 250-256.

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

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

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

[HM] J. Heintz, J. Morgenstern, On associative algebras of minimal rank, *Proc. of the AAECC-2 Conference* (Grenoble 1984).

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

[KB] M. Kaminski, N. H. Bshouty, Multiplicative complexity of polynomial multiplication over finite field, Proceedings 28th Annual Symposium on Foundations of Computer Science, (1987).

[L] J. H. van Lint, *Introduction to Coding theory* , Springer Verlag, New York, 1980.

[LSW] A. Lempel, G. Seroussi, S. Winograd, On the Complexity of Multiplication in Finite Fields, *Theoret. Comput. Sci.* **22** (1983), 285-296.

[LW] A. Lempel, S. Winograd, A New Approach to Error-Correcting Codes, *IEEE Transactions on Information Theory* **23** (1977), 503-508.

[S] V. Strassen, Gaussian elimination is not optimal, *Numer. Math.* **13** (1969) 354-356.

[W] S. Winograd, On multiplication of 2×2 matrices, *Linear Algebra and its Applications,* **4** (1971), 381-388.