A LOWER BOUND FOR THE MULTIPLICATION OF POLYNOMIALS MODULO A POLYNOMIAL

Nader H. Bshouty

Department of Computer Science

University of Calgary

Calgary, Alberta, Canada

ABSTRACT

In [Theoretical Computer Science, 1983], Lempel, Seroussi and Winograd proved the lower bound

$$\left(2+\frac{1}{q-1}\right)n-o(n)$$

for the multiplicative complexity of the multiplication of two polynomials of degree $n-1$ modulo an **irreducible** polynomial p of degree n over a finite field F with q elements.

In this paper we prove this lower bound holds for **any** polynomial p of degree n.

Key Words - multiplicative complexity, quadratic algorithms, 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. Let $x=(x_0,\ldots,x_{n-1})^t$ and $y=(y_0,\ldots,y_{m-1})^t$ be vectors of indeterminates. A *quadratic* algorithm over F that computes the bilinear forms $x^T\mathbf{B}y=\{x^TB_1y,\ldots,x^TB_ky\}$ is a straightline algorithm over F for $x^t\mathbf{B}y$ such that its 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 an infinite field, then $\mathbf{L}_F(\mathbf{B})$ is the minimal 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 minimal number of nonscalar multiplications needed to compute $x^T\mathbf{B}y$ by a straightline algorithm without divisions.

For the vectors $x=(x_0,\ldots,x_{n-1})$ and $y=(y_0,\ldots,y_{n-1})$ we define $x(\alpha)=x_0+x_1\alpha+\cdots+x_{n-1}\alpha^{n-1}$ and $y(\alpha)=y_0+y_1\alpha+\cdots+y_{n-1}\alpha^{n-1}$. Let $p(\alpha)$ be a polynomial of degree n over F and define $\mathbf{B}(p)=\{B_0,\ldots,B_{n-1}\}$ where

$$\sum_{i=0}^{n-1}(x^TB_i\,y)\alpha^i = x(\alpha)y(\alpha)\ mod\ p(\alpha).$$

That is, $x^TB_i\,y$ is the $i+1$ coefficient of $x(\alpha)y(\alpha)\ mod\ p(\alpha)$.

In [LSW] Lemple, Seroussi and Winograd used coding theory to prove the lower bound

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

when p is an **irreducible** polynomial of degree n. In [CC], Chudnovsky and Chudnovsky proved the linear upper bound

$$\mathbf{L}_F(\mathbf{B}(p))\leq\left[2+O\left[\frac{1}{|F|^{1/2}}\right]\right]n.$$

In this paper we generalize the result in [LSW] as follows:

Theorem . Let $p\in F[\alpha]$ be **any polynomial** of degree n over a finite field F. Then

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

The method we use involves a combination of the coding method which is used in [LSW], and the substitution method used in [BD].

This paper is organized as follows. In section 2 we give some preliminary results and the connection between linear codes and the complexity of bilinear forms. In section 3 we prove the theorem.

2. PRELIMINARY RESULTS

This section contains a survey of some basic concepts that will be employed throughout the

paper.

Definition 1 . Let $\mathbf{B} = \{B_1, \ldots, B_n\}$ be an n–set of $n \times n$-matrices and M , N and $K = (K_{i,j})$ be $n \times n$-matrices. We define

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

For an n–set $\mathbf{C}$ of $n \times n$-matrices we write $\mathbf{B} \equiv \mathbf{C}$ if there exist nonsingular $n \times n$–matrices N , M and K such that

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

Definition 2 . Let $\mathbf{B} = \{B_1, \ldots, B_n\}$ be an n–set of $n \times n$ matrices and let $\mathbf{C} = \{C_1, \ldots, C_m\}$ be an m–set of $m \times m$-matrices. We define

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

where

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

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

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 an $[n\,,k\,]$ code. For $c \in C$ the *weight* of c, denoted by $wt\,(c\,)$, is the number of nonzero components of c. The *minimal weight* of C is $\mathbf{min}\ \{wt\,(c\,) \mid c \in C - \{0\}\}$. We say that C is an $[n\,,k\,,d\,]$ *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 exists an $[N_F\,(k\,,d\,),k\,,d\,]$ code. The connection between the linear codes and the complexity of bilinear forms over F is given in the following lemma.

Lemma 1 . [BD, LW] . Let $\mathbf{B} = \{B_1, \ldots, B_k\}$ be a set of $n \times m$ matrices and let $\mathbf{G} = Span_F\,(\mathbf{B})$ be the linear space over F spanned by the elements of $\mathbf{B}$. Let $d = \mathbf{min}_{B' \in \mathbf{G}-\{0\}}\ \mathbf{rank}\ B'$ and $k = dim\ Span_F\,(\mathbf{B})$. Then

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

Lemma 1 is proved in [BD, LW] for the bilinear algorithm model of computation. The proof for the quadratic algorithm model is very similar and will be omitted.

The next lemma gives a lower bound for $N_F(k,d)$.

Lemma 2. (Griesmer Bound [L, p. 59]). We have

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

Other lower bound techniques known from the literature for the complexity of quadratic algorithms are the following.

Lemma 3. [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

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

Lemma 4. Let $\mathbf{B}$ and $\mathbf{C}$ be as in lemma 3 with $k_1 = k_2 = n = m$

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

$$\mathbf{L}_F(\mathbf{B}) \leq \mathbf{L}_F(\mathbf{C}).$$

(2) If $\mathbf{B} \equiv \mathbf{C}$, then

$$\mathbf{L}_F(\mathbf{B}) = \mathbf{L}_F(\mathbf{C}).$$

(see definition 1 for $\equiv$).

3. PROOF OF THE LOWER BOUND

In this section we prove the theorem stated in section 1.

Let $\mathbf{B}$ be an independent set of matrices. We say that $\mathbf{B}$ is a (k,l,d)-set if $|\mathbf{B}| = k$ and there exists $k-l$ matrices $B_1, \ldots, B_{k-l} \in \mathbf{B}$ such that for any $B \notin Span_F(\{B_1, \ldots, B_{k-l}\})$ we have

$$\mathbf{rank}\ B \geq d.$$

We remind the reader that $Span_F(\mathbf{B})$ is the linear space spanned by the elements of $\mathbf{B}$. If $\mathbf{B}$ is a (k,l,d)-set, then $\mathbf{B}$ is a (k,l',d)-set for any $l' \leq l$. This follows from the fact that,

$\mathbf{B} \notin Span_F \{B_1, \ldots, B_{k-l'}\}$ implies that $\mathbf{B} \notin Span_F \{B_1, \ldots, B_{k-l}\}$.

The following lemma will be used to prove the theorem.

Lemma 5 . Let $\mathbf{B}^{(i)}$, be a (k_i, l_i, d_i)-set for $i = 1, \ldots, s$ and let $l = \min_{1 \le i \le s} l_i$. Then

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

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

$$\mathbf{rank}\ B \ge d_i. \qquad (*)$$

Consider the following two sets

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

and

$$\mathbf{V}_2 = (\mathbf{B}^{(1)} - \mathbf{D}^{(1)}) \oplus \cdots \oplus (\mathbf{B}^{(s)} - \mathbf{D}^{(s)}),$$

where

$$\mathbf{D}^{(i)} = \{B_1^{(i)}, \ldots, B_l^{(i)}\}.$$

Here, $diag (B_i^{(1)}, \ldots, B_i^{(s)})$ is the block matrix

$$\begin{bmatrix} B_i^{(1)} & & & \\ & \ddots & & \\ & & \ddots & \\ & & & B_i^{(s)} \end{bmatrix}.$$

Obviously, $Span_F (\mathbf{V}_1 \cup \mathbf{V}_2)$ is a subset of $Span_F (\mathbf{B}^{(1)} \oplus \cdots \oplus \mathbf{B}^{(s)})$. Therefore, by lemma 4 and lemma 3,

$$\mathbf{L}_F (\mathbf{B}^{(1)} \oplus \cdots \oplus \mathbf{B}^{(s)}) \ge \mathbf{L}_F (\mathbf{V}_1 \cup \mathbf{V}_2) \ge dim\ Span_F (\mathbf{V}_2) + \min_{\lambda \in F^{k_1 + \cdots + k_s}} \mathbf{L}_F (\mathbf{S}_\lambda) \qquad (1)$$

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

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

Every nonzero element in $Span_F(S_\lambda)$ is of the form

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

where not all δ_i are zero. Since not all δ_i are zero, we have

$$G_h = \sum_{i=1}^{l}\delta_i B_i^{(h)} + \sum_{j=l+1}^{k_h}\lambda'_{h,j}B_j^{(h)} \notin Span_F(\{B_{l+1}^{(h)}, \ldots, B_{k_h}^{(h)}\}) \quad \text{for} \quad h = 1, \ldots, s.$$

Therefore, by (*), for any $P \in Span_F(S_\lambda)$ we have

$$\textbf{rank } P = \sum_{i=1}^{s}\textbf{rank } G_i \geq \sum_{i=1}^{s} d_i.$$

Thus, by lemma 1, we have

$$\mathbf{L}_F(\mathbf{S}_\lambda) \geq N_F\left[l, \sum_{i=1}^{s} d_i\right]. \tag{2}$$

Now, it is obvious that

$$dim \ \ Span_F(\mathbf{V}_2) = \left[\sum_{i=1}^{s} k_i\right] - s\,l.$$

Combining this with (1) and (2), the result of the lemma follows. □

Let $i_F(n)$ denote the maximum possible number of distinct irreducible factors of a polynomial of degree n over the field F. The following lemma is known from [KB].

Lemma 6. For sufficiently 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

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

That is,

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

It is known that,

$$\mathbf{B}(\alpha^m) = \{I_m^{(j)} \mid j = 1, \ldots, m\}. \tag{3}$$

From [AGW], for any polynomial $p(\alpha)$ of degree n

$$\mathbf{B}(p) = \{C_p^0, C_p^1, \ldots, C_p^{n-1}\}, \tag{4}$$

where C_p is the companion matrix of p. It is well known that when p is an irreducible polynomial over F then for any nonzero $C \in Span_F(\mathbf{B}(p))$ we have

$$\mathbf{rank}\ C = deg\ p. \tag{5}$$

Another important property that will be used for the proof of the theorem is the following.

Let H_i be nonsingular $n \times n$–matrices for $i = 1, \ldots, j_0$. The matrix $\sum_{j=1}^{j_0} I_m^{(j)} \otimes H_j$ is of the shape

$$\begin{bmatrix} 0_{n\times n} & \cdots & 0_{n\times n} & H_{j_0} & \cdots & H_3 & H_2 & H_1 \\ \vdots & & & & & H_3 & H_2 & \\ \vdots & & & & & & H_3 & \\ \vdots & & \mathbf{0} & & & & \vdots & \\ & & & & & & H_{j_0} & \\ & & & & & & 0_{n\times n} & \\ & & & & & & \vdots & \\ 0_{n\times n} & \cdots & \cdots & \cdots & & & 0_{n\times n} & \end{bmatrix}$$

where $0_{n\times n}$ is the $n \times n$ zero matrix. Therefore

$$\mathbf{rank}\left[\sum_{j=1}^{j_0} I_m^{(j)} \otimes H_j\right] = n\, j_0. \tag{6}$$

We now prove the theorem.

Theorem . Let $p(\alpha)$ be any polynomial of degree n. Then

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

Proof . Let $p = p_1^{d_1} \cdots p_k^{d_k}$, where $p_1, \ldots, p_k$ are distinct irreducible polynomials. Let $deg\ p = n$, $deg\ p_i = r_i$, $deg\ p_i^{d_i} = s_i = r_i d_i$, and $s_1 \leq \cdots \leq s_k$. It is well known from [AGW1] and [AGW2] that

$$\mathbf{B}(p) \equiv (\mathbf{B}(\alpha^{d_1}) \otimes \mathbf{B}(p_1)) \oplus \cdots \oplus (\mathbf{B}(\alpha^{d_k}) \otimes \mathbf{B}(p_k)).$$

By (3) and (4),

$$\mathbf{B}(p) = \mathbf{B}_1 \oplus \cdots \oplus \mathbf{B}_k,$$

where

$$\mathbf{B}_h = \left\{ (I_{d_h}^{(i)} \otimes C_{p_h}^{j}) \;\middle|\; 1 \le i \le d_h, 0 \le j \le r_h - 1 \right\} \quad \text{for} \quad h = 1, \ldots, k,$$

and C_{p_h} is the companion matrix of p_h. We now prove the following claims.

Claim 1. There exists an integer $w \le 2\dfrac{n^{1/2}}{\log_{|F|} n}$ such that

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

Let w be an integer such that

$$deg\ p_1^{d_1} \cdots p_w^{d_w} \ge n^{1/2} \quad , \quad deg\ p_1^{d_1} \cdots p_{w-1}^{d_{w-1}} < n^{1/2}. \tag{7}$$

By lemma 6, for sufficiently large n,

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

Now, since $deg\ p_1^{d_1} \cdots p_w^{d_w} \ge n^{1/2}$ and $s_1 \le s_2 \le \cdots \le s_w$, we have that

$$s_w = deg\ p_w^{d_w} \ge \frac{n^{1/2}}{w} \ge \frac{1}{2}\log_{|F|} n.$$

Since $s_w \le s_{w+1} \le \cdots \le s_k$ we have

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

This completes the proof of claim 1.

Let

$$m_i = \left\lceil \frac{\log_{|F|} \log n}{r_i} \right\rceil \quad \text{for} \quad i = w, \ldots, k, \tag{8}$$

and

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

Claim 2. We have

$$|\mathbf{W}_i| \ge \log_{|F|} \log n \quad \text{for} \quad i = w, \ldots, k. \quad \square$$

If $\max(d_i - m_i + 1, 1) = d_i - m_i + 1$, then by (8), $|\mathbf{W}_i| = m_i r_i \ge \log_{|F|} \log n$. If $\max(d_i - m_i + 1, 1) = 1$, then $d_i - m_i + 1 \le 1$ and $|\mathbf{W}_i| = r_i$. This implies that

$$d_i \le m_i = \left\lceil \frac{\log_{|F|} \log n}{r_i} \right\rceil < \frac{\log_{|F|} \log n}{r_i} + 1.$$

We multiply the latter inequality by r_i and obtain $r_i > d_i r_i - \log_{|F|} \log n$. Now, using claim 1, for $i = w, \ldots, k$,

$$r_i > \frac{1}{2}\log_{|F|} n - \log_{|F|} \log n > \log_{|F|} \log n.$$

Now, since $| \mathbf{W}_i | = r_i$ the result of the claim follows.

Claim 3 . The set $\mathbf{B}_i$ is a $\left[s_i , | \mathbf{W}_i | , s_i - m_i r_i + r_i \right]$ – set for $i = w , \ldots , k$. □

Obviously, $| \mathbf{B}_i | = s_i = r_i d_i$. If $P \notin Span_F (\mathbf{B}_i - \mathbf{W}_i)$, then there exist constants $\{\delta_V \mid V \in \mathbf{W}_i\} \subseteq F$ not all zero and $\{\eta_V \mid V \in \mathbf{B}_i - \mathbf{W}_i\} \subseteq F$ such that

$$P = \sum_{V \in \mathbf{W}_i} \delta_V V + \sum_{V \in \mathbf{B}_i - \mathbf{W}_i} \eta_V V .$$

Then P can be written as

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

where not all $\{\lambda_{i,j,l}\}_{j = \mathbf{max}\,(d_i - m_i + 1, 1), \ldots, d_i}$ are zero. Therefore

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

Suppose j_0, where $\mathbf{max}\,(d_i - m_i + 1, 1) \le j_0 \le d_i$, is the maximal integer such that $\sum_{l=0}^{r_i-1} \lambda_{i,j_0,l} C_{p_i}^l \neq 0$. By (5) and (6)

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

This proves that $\mathbf{B}_i$ is a $\left[s_i , | \mathbf{W}_i | , s_i - m_i r_i + r_i \right]$ – set and claim 3 is proved.

Now, by claim 2, $\mathbf{min}_{w \le i \le k} | \mathbf{W}_i | \ge \log_{|F|} \log n$, and by lemma 5,

$$\mathbf{L}_F (\mathbf{B}(p)) \ge$$

$$\mathbf{L}_F (\{0\} \oplus \overset{w \text{ times}}{\cdots} \oplus \{0\} \oplus \mathbf{B}_{w+1} \oplus \cdots \oplus \mathbf{B}_k) = \mathbf{L}_F (\mathbf{B}_{w+1} \oplus \cdots \oplus \mathbf{B}_k) \ge \tag{9}$$

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

We now estimate each term in (9). By (7), we have

$$\sum_{i=w}^{k} s_i = deg\ p_w^{d_w} \cdots p_k^{d_k} \ge n - n^{1/2}. \tag{10}$$

By lemma 6,

$$k \le \frac{2n}{\log_{|F|} n}.$$

Therefore,

$$k \log_{|F|} \log n = o(n). \tag{11}$$

By (8), (10) and (11),

$$\sum_{i=w}^{k} (s_i - m_i r_i + r_i) \ge n - n^{1/2} - \sum_{i=w}^{k} (m_i - 1) r_i \ge n - n^{1/2} - k \log_{|F|} \log n = n - o(n). \tag{12}$$

Combining this with (9), (10) and (11) we get

$$\mathbf{L}_F(\mathbf{B}(p)) \ge n + N_F\left(\left\lceil \log_{|F|} \log n \right\rceil, n - o(n)\right) - o(n). \tag{13}$$

Now, by lemma 2, we have

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

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

Combining this with (13), we obtain the result

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

REFERENCES

[AGW1] A. Averbuch, Z. Galil, S. Winograd, Classification of all minimal bilinear algorithms for computing the coefficients of the product of two polynomials in the algebra $G[u]/<u^n>$, manuscript.

[AGW2] A. Averbuch, Z. Galil, S. Winograd, Classification of all minimal bilinear algorithms for computing the coefficients of the product of two polynomials in the algebra $G[u]/<Q(u)^l>$, $l > 1$, manuscript.

[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 extended direct sum conjecture. Proceedings 21st Annual ACM Symposium on Theory of Computing, (May 1989).

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

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

[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.

[KB] M. Kaminski, N. H. Bshouty, Multiplicative complexity of polynomial multiplication over finite field, *J. of ACM*, **36**, (1989), 150-170.

[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.