Multiplicative Complexity of Polynomial Multiplication over Finite Fields

MICHAEL KAMINSKI AND NADER H. BSHOUTY

Technion—Israel Institute of Technology, Haifa, Israel

Abstract. Let $M_q(n)$ denote the number of multiplications required to compute the coefficients of the product of two polynomials of degree n over a q-element field by means of bilinear algorithms. It is shown that $M_q(n) \geq 3n - o(n)$. In particular, if $q/2 < n \leq q + 1$, we establish the tight bound $M_q(n) = 3n + 1 - \lfloor q/2 \rfloor$. The technique we use can be applied to analysis of algorithms for multiplication of polynomials modulo a polynomial as well.

Categories and Subject Descriptors: F.2.1 [**Analysis of Algorithms and Problem Complexity**]: Numerical Algorithms and Problems—*computation in finite fields, computation on polynomials*

General Terms: Algorithms, Theory, Verification

Additional Key Words and Phrases: Bilinear algorithms, Hankel matrices, linear recurring sequences, polynomial multiplication

1. *Introduction*

In infinite fields it is possible to compute the coefficients of the product of two polynomials of degree n in $2n + 1$ nonscalar multiplications. It is known from [18] that each algorithm for computing the above product in $2n + 1$ nonscalar multiplications must evaluate the multiplicands at a minimum of $2n$ distinct points, multiply the samples, and interpolate the result. However, in finite fields, this method fails if $2n$ exceeds the number of field elements. Thus, in general, the above bound cannot be achieved in finite fields.

Let $\mathbf{F}_q$ denote the q-element field and let $M_q(n)$ denote the number of multiplications required to compute the coefficients of the product of two polynomials of degree n over $\mathbf{F}_q$ by means of bilinear algorithms. In this paper we prove that for any q we have $M_q(n) \geq 3n - o(n)$. The best lower bound on $M_q(n)$ known from the literature, cf. [2], [3], [9], [11], and [12], states that $M_q(n)$ is bounded from below by the minimum length of a linear code over $\mathbf{F}_q$ of dimension $n + 1$ and

A preliminary version of this paper appeared in *Proceedings of the 28th Annual IEEE Symposium on Foundations of Computer Science* (Los Angeles, Calif., Oct. 12–14). IEEE, New York, 1987, pp. 138–140.

Authors' address: Department of Computer Science, Technion—Israel Institute of Technology, Haifa 32000, Israel.

minimal distance $n + 1$,[1,2] which implies the following linear lower bounds on $M_q(n)$. $M_q(n) \geq (2 + 1/(q - 1))n - o(n)$, if $q \geq 3$, and, for large values of n, $M_2(n) \geq 3.52n$. However, an easy calculation based on the Gilbert–Varshamov upper bound on the length of linear codes, cf. [14, Theorem 4.7, p. 87], shows that for $q \geq 7$ there exist linear codes of dimension $n + 1$, minimal distance $n + 1$, and length $2.9n$, say. (Actually, it is not hard to show that there exists a linear code of dimension $n + 1$, minimal distance $n + 1$, and length $(2 + O(1/\ln q))n$. Hence, the constant factor of the linear lower bound established in [2], [3], [9], [11], and [12] tends to 2, when q tends to infinity.) Thus, if $q \geq 7$, the $3n - o(n)$ lower bound cannot be achieved by the previously known technique. For $q = 3, 4, 5$, it is unknown whether or not there exist linear codes of dimension $n + 1$, minimal distance $n + 1$, and length less than $3n$; but the best-known lower bound on the length of such codes is $(2 + 1/(q - 1))n - o(n)$. Therefore, in these cases, the $3n - o(n)$ lower bound on $M_q(n)$ can be considered as an improvement of the known one as well. The only case where the $3n - o(n)$ lower bound is worse than the bound given by the code length is that of $q = 2$. However, in this case, our technique also allows to obtain an alternative proof of the known lower bound.

If $q/2 < n \leq q + 1$, the method we use provides the tight bound of $M_q(n) = 3n + 1 - \lfloor q/2 \rfloor$. (As it has been mentioned earlier, if $n \leq q/2$, then $M_q(n) = 2n + 1$.) All these tight bounds are new and cannot be achieved by the technique based on coding theory.

Although we consider only bilinear algorithms and the lower bound we present is linear, the result seems to be of interest, since the constant factor of that bound is independent on q, and in view of quasi-linear upper bound of $f_q(n) \cdot n$, established in [11]. Here $f_q(n)$ is a very slowly growing function of n defined recursively as follows

(1) $f_q(1)$ and $f_q(2) = \frac{3}{2}$.

(2) $f_2(3) = f_3(3) = 2$ and $f_q(3) = \frac{3}{2}$, if $q > 3$.

(3) If $n \geq 4$, then $f_q(n) = 2f_q(\lceil \log_q 2(q - 1)n \rceil)$.

In fact, the asymptotic behavior of $f_q(n)$ is similar to the behavior of the function $2^{\log_q^* n}$, where $\log_q^* n$ is the inverse of the function $G_q(n)$, defined recursively by $G_q(0) = q$ and $G_q(n + 1) = q^{G_q(n)}$.

It is known from [16] that if a set of bilinear forms over an infinite field can be computed in t multiplications/divisions, then it can be computed in t multiplications by a bilinear algorithm whose total number of operations differs from that of the original one by a factor of a small constant. But it is unknown whether a similar result holds for finite fields. However, one can easily prove that bilinear algorithms for computing a set of bilinear forms are optimal within the algorithms without divisions. Also we would like to note that all the algorithms for polynomial

[1] The definitions of a linear code can be found in the end of Section 7.

[2] Actually, the bound established in [9] and [11] concerns the number of multiplications required to compute the product of two polynomials of degree n modulo an irreducible polynomial of degree $n + 1$. It is unknown whether this bound follows from the same bound on $M_q(n)$, since, unlike in the case of infinite fields, it is unknown whether computing the product modulo an irreducible polynomial requires less multiplications than computing the product itself, cf. [11]. In any case, the above bound on the number of multiplications required to compute the product of two polynomials modulo an irreducible polynomial, and even a more general result, can be easily obtained by our method, cf. Corollary 5 to Lemma 7 in the end of Section 7.

multiplication over finite fields known from the literature are bilinear, cf. [11] and [15].

The proofs are based on the theory of linear recurring sequences and an analysis of Hankel matrices[3] representing bilinear forms defined by linear combinations of the coefficients of the product of two polynomials. This technique can be also applied to analysis of algorithms for multiplication of polynomials modulo a polynomial.

The paper is organized as follows. In the next section we give the statements of the main results. In Section 3 we introduce some notation and definitions, and prove the major auxiliary technical lemmas. The proofs of the main results are presented in Sections 4, 5, and 6. In Section 7 we consider some applications of our method to analysis of algorithms for multiplication of polynomials modulo a polynomial. Finally, in Appendix A we present an upper bound on the number of distinct irreducible factors of a polynomial over a finite field, and in Appendix B we present an optimal algorithm for computing the product of two polynomials of degree not exceeding $q + 1$ over $\mathbf{F}_q$.

2. *Statements of Main Results*

In this paper we restrict ourselves to bilinear algorithms, which are defined below.

Let $\mathbf{x}$ and $\mathbf{y}$ be column vectors of indeterminates. A *bilinear algorithm* for computing a set of bilinear forms of $\mathbf{x}$ and $\mathbf{y}$ is a straight-line algorithm whose nonscalar multiplications are of the form $L(\mathbf{x}) \cdot L'(\mathbf{y})$, where $L(\mathbf{x})$ and $L'(\mathbf{y})$ are linear forms of $\mathbf{x}$ and $\mathbf{y}$, respectively, and each bilinear form is obtained by computing a linear combination of these products.

We remind the reader that $\mathbf{F}_q$ denotes the q-element field and $M_q(n)$ denotes the number of multiplications required to compute the coefficients of the product of two polynomials of degree n over $\mathbf{F}_q$ by means of bilinear algorithms.

The main results of the paper are given by Theorems 1 and 2 below.

THEOREM 1. *For any $q \geq 3$ we have $M_q(n) > 3n - n/(\log_q n - 3)$.*

We recall that it is known from [3] that for sufficiently large n we have $M_2(n) > 3.52n$.

THEOREM 2. *For any q and $q/2 < n \leq q + 1$ we have $M_q(n) = 3n + 1 - \lfloor q/2 \rfloor$.*

3. *Notation and Auxiliary Lemmas*

In this section we introduce some notation and prove the major auxiliary lemmas needed for the proofs of Theorems 1 and 2.

Let k be a positive integer and let $a_0, \ldots, a_{k-1}$ be given elements of a field F. A sequence $\sigma = s_0, s_1, \ldots, s_l$ of elements of F satisfying the relation

$$s_{n+k} = a_{k-1}s_{n+k-1} + a_{k-2}s_{n+k-2} + \cdots + a_0 s_n, \quad n = 0, 1, \ldots, l - k$$

is called a (finite kth-order homogeneous) *linear recurring sequence* in F. The terms $s_0, s_1, \ldots, s_{k-1}$ are referred to as *initial values*. The polynomial

$$f(\alpha) = \alpha^k - a_{k-1}\alpha^{k-1} - a_{k-2}\alpha^{k-2} - \cdots - a_0 \in F[\alpha]$$

is called a *characteristic polynomial* of σ. Proposition 1 below shows that if a finite linear recurring sequence is "sufficiently long," then it possesses an important property of infinite linear recurring sequences.

[3] The definition of Hankel matrices is given in Section 3.

PROPOSITION 1. *Let σ and $f(\alpha)$ be as above, and let $f_\sigma(\alpha)$ be a characteristic polynomial of σ of the minimal degree. If* $\mathbf{deg}\, f_\sigma(\alpha) + \mathbf{deg}\, f(\alpha) \le l + 1$, *then $f_\sigma(\alpha)$ divides $f(\alpha)$.*

PROOF. Let $\mathbf{deg}\, f(\alpha) = m$. Consider the system of linear equations in $w_0, w_1, \ldots, w_{m-1}$

$$\begin{pmatrix} s_0 & s_1 & \cdots & s_{m-1} \\ s_1 & s_2 & \cdots & s_m \\ \vdots & \vdots & & \vdots \\ s_{l-m} & s_{l-m+1} & \cdots & s_{l-1} \end{pmatrix} \begin{pmatrix} w_0 \\ w_1 \\ \vdots \\ w_{m-1} \end{pmatrix} = \begin{pmatrix} s_m \\ s_{m+1} \\ \vdots \\ s_l \end{pmatrix}. \tag{1}$$

Since, by definition, $f_\sigma(\alpha)$ is the minimal polynomial of the infinite sequence extending σ and satisfying the recurrence defined by $f_\sigma(\alpha)$, the rank of the $(l - m + 1) \times m$ matrix in (1) is equal to $\mathbf{deg}\, f_\sigma(\alpha)$, cf. [13, Theorem 8.51, p. 422].[4] (Here we use the condition $\mathbf{deg}\, f_\sigma(\alpha) + \mathbf{deg}\, f(\alpha) \le l + 1$.)

It follows that the dimension of the affine space of the solutions of (1) is equal to $m - \mathbf{deg}\, f_\sigma(\alpha)$. On the other hand, for each monic polynomial $Q(\alpha) = \alpha^m - \sum_{i=0}^{m-1} b_i \alpha^i$ divisible by $f_\sigma(\alpha)$, the vector $(b_0, b_1, \ldots, b_{m-1})^T$ is a solution for (1), cf. [13, Theorem 8.42, p. 418]. Since the dimension of the affine space over F consisting of such polynomials is equal to $m - \mathbf{deg}\, f_\sigma(\alpha)$, this space contains $f(\alpha)$. Hence $f(\alpha)$ is divisible by $f_\sigma(\alpha)$. □

A uniquely determined monic polynomial $f_\sigma(\alpha) \in F[\alpha]$ given by Proposition 1 is called the *minimal polynomial* of σ.

For a sequence $\sigma = \{s_0, \ldots, s_{2n}\}$ we define the $(n + 1) \times (n + 1)$ *Hankel matrix* $H(\sigma)$ by

$$\begin{pmatrix} s_0 & s_1 & \cdots & s_n \\ s_1 & s_2 & \cdots & s_{n+1} \\ \vdots & \vdots & & \vdots \\ s_n & s_{n-1} & \cdots & s_{2n} \end{pmatrix}.$$

Let H^i denote the $(i + 1)$st row of H, $i = 0, 1, \ldots, n$. If $\mathbf{rank}\, H < n + 1$, let k be the minimal positive integer such that there exist $a_0, \ldots, a_{k-1} \in F$ satisfying

$$\sum_{i=0}^{k-1} a_i H^i = H^k.$$

We define $\tilde{\sigma} = \{\tilde{s}_0, \tilde{s}_1, \ldots, \tilde{s}_{2n}\}$ by the recurrence

$$\tilde{s}_{i+k} = a_{k-1}\tilde{s}_{i+k-1} + a_{k-2}\tilde{s}_{i+k-2} + \cdots + a_0\tilde{s}_i,$$

with initial values $\tilde{s}_i = s_i$, $i = 0, \ldots, k - 1$.

Let $\bar{\sigma} = \sigma - \tilde{\sigma}$. We shall denote $H(\tilde{\sigma})$ and $H(\bar{\sigma}) = H - H(\tilde{\sigma})$ by $\tilde{H}$ and $\bar{H}$, respectively. Let $f_H(\alpha) = \alpha^k - \sum_{i=0}^{k-1} a_i \alpha^i$, that is, $f_H(\alpha)$ is a characteristic polynomial of $\tilde{\sigma}$. (In fact, $f_H(\alpha) = f_{\tilde{\sigma}}(\alpha)$, since, by definition, $f_H(\alpha)$ is a characteristic polynomial of the minimal degree.)

It follows from the above definition that $\mathbf{rank}\, H \le \mathbf{deg}\, f_H(\alpha) + \mathbf{rank}\, \bar{H}$. Proposition 2 below shows that, actually, $\mathbf{rank}\, H = \mathbf{deg}\, f_H(\alpha) + \mathbf{rank}\, \bar{H}$.

[4] The proofs in [13] do not use the finiteness of the underlying field.

PROPOSITION 2. *Let $H(\sigma)$ be an $(n+1) \times (n+1)$ Hankel matrix of rank not exceeding n. Then the set of vectors consisting of the first* **deg** $f_H(\alpha)$ *and the last* **rank** $\bar{H}$ *rows of H is linearly independent.*

PROOF. By the definition of $\tilde{H}$ and $\bar{H}$ it suffices to prove that the set of vectors consisting of the first **deg** $f_H(\alpha)$ rows of H and the last **rank** $\bar{H}$ rows of $\bar{H}$ is linearly independent. Let **deg** $f_H(\alpha) = k$. Since **deg** $f_H(\alpha) =$ **deg** $f_{\tilde{\sigma}}(\alpha)$ $(=k)$, the rank of the $k \times k$ upper left submatrix of H is equal to k, cf. [13, Theorem 8.51, p. 422]. Since $\bar{H}$ is a Hankel matrix whose first row is the zero vector, the last **rank** $\bar{H}$ rows of $\bar{H}$ are linearly independent. Now the result follows from the fact that the first k components of the rows of $\bar{H}$ are equal to zero. □

Let $\mathbf{S} = \{H_0, H_1, \ldots, H_s\}$ be an $(s+1)$-element set of $(n+1) \times (n+1)$ Hankel matrices of rank not exceeding n. Define $f_{\mathbf{S}}(\alpha) = \text{lcm}\{f_{H_i}(\alpha) \mid i = 0, 1, \ldots, s\}$,[5] $d_{\mathbf{S}} =$ **deg** $f_{\mathbf{S}}(\alpha)$ and $r_{\mathbf{S}} =$ **max**{**rank** $\bar{H}_i \mid i = 0, 1, \ldots, s$}.

The proofs of Theorems 1 and 2 are based on Lemmas 1, 2, and 3 below.

Let V be a vector space over F, $v_1, v_2, \ldots, v_m \in V$. $[v_1, v_2, \ldots, v_m]$ denotes the linear subspace of V spanned by $v_1, v_2, \ldots, v_m$.

LEMMA 1. *Let $\mathbf{S} = \{H_0, H_1, \ldots, H_s\}$ be a set of $(n+1) \times (n+1)$ Hankel matrices of rank not exceeding n. Then* **dim**[**S**] $\leq d_{\mathbf{S}} + r_{\mathbf{S}}$.

Let $\mathbf{x} = (x_0, x_1, \ldots, x_n)^{\mathrm{T}}$ and $\mathbf{y} = (y_0, y_1, \ldots, y_n)^{\mathrm{T}}$ be column vectors of indeterminates.

LEMMA 2. *Let $\mathbf{S} = \{H_0, H_1, \ldots, H_s\}$ be a set of $(n+1) \times (n+1)$ Hankel matrices of rank not exceeding n. If $d_{\mathbf{S}} + r_{\mathbf{S}} \geq n+1$, then computing the set of bilinear forms of* **x** *and* **y** *defined by $\mathbf{x}^{\mathrm{T}}H_0\mathbf{y}, \mathbf{x}^{\mathrm{T}}H_1\mathbf{y}, \ldots, \mathbf{x}^{\mathrm{T}}H_s\mathbf{y}$ requires at least $n+1$ multiplications.*

LEMMA 3. *Let $\mathbf{S} = \{H_0, H_1, \ldots, H_s\}$ be a set of $(n+1) \times (n+1)$ Hankel matrices of rank not exceeding n. If $d_{\mathbf{S}} + r_{\mathbf{S}} \leq n$, then computing the set of bilinear forms of* **x** *and* **y** *defined by $\mathbf{x}^{\mathrm{T}}H_0\mathbf{y}, \mathbf{x}^{\mathrm{T}}H_1\mathbf{y}, \ldots, \mathbf{x}^{\mathrm{T}}H_s\mathbf{y}$ requires at least $d_{\mathbf{S}} + r_{\mathbf{S}}$ multiplications.*

At this point we advise the reader to postpone reading the proofs of Lemmas 1–3 and directly move to the next sections that contain the proofs of the main results.

PROOF OF LEMMA 1. Let $H_i = H(\sigma_i)$, $i = 0, 1, \ldots, s$. Obviously, $[H_0, H_1, \ldots, H_s]$ is isomorphic to $[\sigma_0, \sigma_1, \ldots, \sigma_s]$. Since $\sigma_i = \tilde{\sigma}_i + \bar{\sigma}_i$, $i = 0, 1, \ldots, s$, it suffices to show that **dim**$[\tilde{\sigma}_0, \tilde{\sigma}_1, \ldots, \tilde{\sigma}_s] \leq d_{\mathbf{S}}$, and **dim**$[\bar{\sigma}_0, \bar{\sigma}_1, \ldots, \bar{\sigma}_s] \leq r_{\mathbf{S}}$.

To prove **dim**$[\tilde{\sigma}_0, \tilde{\sigma}_1, \ldots, \tilde{\sigma}_s] \leq d_{\mathbf{S}}$, we observe that, by Proposition 1, $f_{\mathbf{S}}(\alpha)$ is a characteristic polynomial of $\tilde{\sigma}_i$, $i = 0, 1, \ldots, s$. Hence each of those sequences is determined by the $d_{\mathbf{S}}$-dimensional vector of its first $d_{\mathbf{S}}$ elements. This proves the inequality concerning $d_{\mathbf{S}}$.

To prove **dim**$[\bar{\sigma}_0, \bar{\sigma}_1, \ldots, \bar{\sigma}_s] \leq r_{\mathbf{S}}$, we observe that the first $(2n + 1 - r_{\mathbf{S}})$ elements of $\bar{\sigma}_i$ are zero, $i = 0, 1, \ldots, s$. Hence each of the above sequences is determined by an $r_{\mathbf{S}}$-dimensional vector of its last $r_{\mathbf{S}}$ elements. This proves the inequality concerning $r_{\mathbf{S}}$. □

[5] lcm is an abbreviation for "the least common multiple".

PROOF OF LEMMA 2. Let $\mathbf{z} = (z_0, z_1, \ldots, z_s)^T$ be a column vector of new indeterminates. Consider the dual set of bilinear forms of $\mathbf{y}$ and $\mathbf{z}$ defined by the components of the vector $\sum_{j=0}^{s} z_j H_j \mathbf{y}$. Computing the above set of bilinear forms requires the same number of multiplications as computing the original set $\mathbf{x}^T H_0 \mathbf{y}$, $\mathbf{x}^T H_1 \mathbf{y}, \ldots, \mathbf{x}^T H_s \mathbf{y}$, cf. [5]. Hence for the proof of the lemma it suffices to show that the rows of the matrix $\sum_{j=0}^{s} z_j H_j$ are linearly independent over F, cf. [17]. Assume, by contradiction, that the first k rows of $\sum_{j=0}^{s} z_j H_j$ are linearly independent, but the first $(k+1)$ rows are linearly dependent:

$$\sum_{i=0}^{k} a_i (z_0 H_0^i + z_1 H_1^i + \cdots + z_s H_s^i) = 0,$$

where $a_k = 1$. Since $z_0, z_1, \ldots, z_s$ are indeterminates, the above identity is equivalent to

$$\sum_{i=0}^{k} a_i H_j^i = 0, \qquad j = 0, 1, \ldots, s. \tag{2}$$

Hence, by Proposition 2, $k < n + 1 - \mathbf{rank}\, \bar{H}_j$, $j = 0, 1, \ldots, s$, which implies

$$k < n + 1 - \mathbf{max}\{\mathbf{rank}\, \bar{H}_j \mid j = 0, 1, \ldots, s\} = n + 1 - r_S. \tag{3}$$

Since $\mathbf{deg}\, f_{\bar{\sigma}_i} \le n$, it follows from (2) and Proposition 1 that $f_{H_j}(\alpha) = f_{\bar{\sigma}_j}(\alpha)$ divides $\sum_{i=0}^{k} a_i \alpha^i$, $j = 0, 1, \ldots, s$. Thus $f_S(\alpha)$ divides $\sum_{i=0}^{k} a_i x^i$. Hence $d_S \le k$, which, together with (3), implies $d_S + r_S < n + 1$. This contradiction completes the proof of Lemma 2. □

PROOF OF LEMMA 3. By the argument at the beginning of the proof of Lemma 2, in the same notation, it suffices to show that the first d_S and the last r_S rows of $\sum_{j=0}^{s} z_j H_j$ are linearly independent over F. We break the proof of linear independence of the above set of rows into two stages. First we prove that the first d_S rows of $\sum_{j=0}^{s} z_j H_j$ are linearly independent. Then we prove that no nonzero linear combination over F of the last r_S rows of $\sum_{j=0}^{s} z_j H_j$ can be equal to a linear combination of its first d_S rows.

To show that the first d_S rows of $\sum_{j=0}^{s} z_j H_j$ are linearly independent over F we proceed exactly as in the proof of Lemma 2. Assume, by contradiction, that for some $k < d_S$ we have

$$\sum_{i=0}^{k} a_i (z_0 H_0^i + z_1 H_1^i + \cdots + z_s H_s^i) = 0,$$

where $a_k = 1$. Since $z_0, z_1, \ldots, z_s$ are indeterminates, the above identity is equivalent to

$$\sum_{i=0}^{k} a_i H_j^i = 0, \qquad j = 0, 1, \ldots, s. \tag{4}$$

By Proposition 1, it follows from (4) that $f_{H_i}(\alpha) = f_{\bar{\sigma}_i}(\alpha)$ divides $\sum_{i=0}^{k} a_i \alpha^i$, $i = 0, 1, \ldots, s$. Thus $f_S(\alpha)$ divides $\sum_{i=0}^{k} a_i \alpha^i$. Hence $d_S \le k$, which contradicts our assumption and proves that the first d_S rows of $\sum_{j=0}^{s} z_j H_j$ are linearly independent over F.

To show that no nonzero linear combination over F of the last r_S rows of $\sum_{j=0}^{s} z_j H_j$ can be equal to a linear combination of its first d_S rows, assume, by

contradiction, that

$$\sum_{i=0}^{d_S-1} a_i(z_0H_0^i + z_1H_1^i + \cdots + z_sH_s^i) + \sum_{i=n-r_S+1}^{n} b_i(z_0H_0^i + z_1H_1^i + \cdots + z_sH_s^i) = 0,$$

where not all b_i, $i = n - r_S + 1, \ldots, n$, are zero. Without loss of generality we may assume that $r_S = \mathbf{rank}\ \bar{H}_0$. Since $z_0, z_1, \ldots, z_s$ are indeterminates, in particular, we have

$$\sum_{i=0}^{d_S-1} a_iH_0^i + \sum_{i=n+1-\mathbf{rank}\bar{H}_0}^{n} b_iH_0^i = 0. \tag{5}$$

Since $\mathbf{deg}\, f_{H_0}(\alpha) \le d_S$, and $d_S + \mathbf{rank}\ \bar{H}_0 < n + 1$, it follows from the definition of $\tilde{H}_0$ and $\bar{H}_0$ that the first d_S rows of H_0 are linear combinations of its first $\mathbf{deg}\, f_{H_0}(\alpha)$ rows. Hence, by (5), we have

$$\sum_{i=0}^{\mathbf{deg}f_{H_0}(\alpha)-1} c_iH_0^i + \sum_{i=n+1-\mathbf{rank}\bar{H}_0}^{n} b_iH_0^i = 0,$$

for some constants $c_0, c_1, \ldots, c_{\mathbf{deg}f_{H_0}(\alpha)-1}$. Since not all b_i, $i = n + 1 - r_S, \ldots, n + 1$, are zero, the last equality contradicts Proposition 2. This completes the proof of Lemma 3, because each linear combination of the above rows either includes or does not include last rows. □

4. *Proof of Theorem* 1

Actually, Theorem 1 is a corollary of another general result given by Lemma 4 below. First, we introduce one more notation that will be frequently used in this section. We denote the maximal possible number of distinct factors of a polynomial of degree n over $\mathbf{F}_q$ by $\mathbf{i}_q(n)$. It is shown in Appendix A that for $q \ge 3$ we have $\mathbf{i}_q(n) < n/(\log_q n - 3)$.

LEMMA 4. *Let* $\mathbf{S} = \{H_0, H_1, \ldots, H_n\}$ *be a set of* $(n + 1) \times (n + 1)$ *Hankel matrices that are linearly independent over* $\mathbf{F}_q$. *Then there exists a subset* $\mathbf{S}'$ *of* $\mathbf{S}$ *containing* $\mathbf{i}_q(n) + 1$ *or fewer elements such that computing the set of bilinear forms defined by* $\{\mathbf{x}^T H\mathbf{y}\}_{H\in\mathbf{S}'}$ *requires at least* $n + 1$ *multiplications.*

PROOF. If some $H \in \mathbf{S}$ is of rank $n + 1$, the lemma, is, trivially, true, since we can take $\mathbf{S}' = \{H\}$. Otherwise, by Lemma 1, we have $d_S + r_S \ge n + 1$, which implies $\mathbf{deg}\, f_S(\alpha) \ge n + 1 - r_S$. Let $f_S(\alpha) = \prod_{j=1}^{l} p_j^{d_j}(\alpha)$ be the decomposition of $f_S(\alpha)$ into irreducible factors $p_1(\alpha), p_2(\alpha), \ldots, p_l(\alpha)$ such that $\mathbf{deg}\ p_1(\alpha) \ge \mathbf{deg}\ p_2(\alpha) \ge \cdots \ge \mathbf{deg}\ p_l(\alpha)$. Let $m \le l$ be such that $\mathbf{deg} \prod_{j=1}^{m} p_j^{d_j}(\alpha) \ge n + 1 - r_S$, and $\mathbf{deg} \prod_{j=1}^{m-1} p_j^{d_j}(\alpha) < n + 1 - r_S$.

We construct a subset $\mathbf{S}'$ of $\mathbf{S}$, inductively, as follows: $\mathbf{S}_0 = \{H_{i_0}\}$, where $\mathbf{rank}\ \bar{H}_{i_0} = r_S$, if $r_S > 0$, and $\mathbf{S}_0 = \emptyset$, otherwise.

Assume $\mathbf{S}_j$, $j < m$, has been constructed. Choose an $H_{i_{j+1}}$ such that $f_{H_{i_{j+1}}}(\alpha)$ is divisible by $p_{j+1}^{d_{j+1}}(\alpha)$ and put $\mathbf{S}_{j+1} = \mathbf{S}_j \cup \{H_{i_{j+1}}\}$.

Let $\mathbf{S}' = \mathbf{S}_m$. By the construction above, $f_{S'}(\alpha)$ is divisible by $\prod_{j=1}^{m} p_j^{d_j}(\alpha)$, hence $d_{S'} \ge n + 1 - r_S$. This together with $\mathbf{rank}\ \bar{H}_{i_0} = r_S = r_{S'}$ implies $d_{S'} + r_{S'} \ge n + 1$. It follows from Lemma 2 that computing the set of bilinear forms defined by $\{\mathbf{x}^T H\mathbf{y}\}_{H\in\mathbf{S}'}$ requires at least $n + 1$ multiplications.

In order to complete the proof of Lemma 4, it remains to show that the number of the elements of $\mathbf{S}'$ does not exceed $\mathbf{i}_q(n) + 1$. We contend that $m \leq \mathbf{i}_q(n + 1 - r_S)$. If $\mathbf{deg} \prod_{j=1}^{m} p_j^{d_j}(\alpha) = n + 1 - r_S$, there is nothing to prove. If $\mathbf{deg}\, p_m(\alpha) = 1$, then, by the definition of m, there exists a $1 \leq d_m' \leq d_m$ such that $\mathbf{deg}(\prod_{j=1}^{m-1} p_j^{d_j}(\alpha)) p_m^{d_m'}(\alpha) = n + 1 - r_S$, and the result follows. Otherwise, that is, $\mathbf{deg}\, p_j(\alpha) > 1, j = 1, 2, \ldots, m$, the polynomial

$$\alpha^{(n+1-r_s)} - \mathbf{deg}(\prod_{j=1}^{m-1} p_j^{d_j}(\alpha))\left(\prod_{j=1}^{m-1} p_j^{d_j}(\alpha)\right)$$

has m irreducible factors and is of degree $n + 1 - r_S$. Hence $m \leq \mathbf{i}_q(n + 1 - r_S)$, which proves our contention.

Obviously, the number of elements of $\mathbf{S}'$ is bounded by $m + 1$. Hence the number of the elements of $\mathbf{S}'$ does not exceed $\mathbf{i}_q(n + 1)$, if $r_S = 0$, and does not exceed $\mathbf{i}_q(n + 1 - r_S) + 1$, otherwise. In both cases, the number of the elements of $\mathbf{S}'$ is bounded by $m \leq \mathbf{i}_q(n) + 1$. □

Now Theorem 1 is implied by Lemma 4 in a standard manner, cf. [11] and [18], as follows.

PROOF OF THEOREM 1. We have to compute $z_k = z_k(\mathbf{x}, \mathbf{y}) = \sum_{i+j=k} x_i y_j$, $k = 0, \ldots, 2n$. Let $\mathbf{z} = (z_0, z_1, \ldots, z_{2n})^T$. Assume that $M_q(n) = t$, that is, all the bilinear forms defined by the components of $\mathbf{z}$ can be computed in t multiplications, namely there exist t linear forms $L_1(\mathbf{x}), \ldots, L_t(\mathbf{x})$ of $\mathbf{x}$ and t linear forms $L_1'(\mathbf{y}), \ldots, L_t'(\mathbf{y})$ of $\mathbf{y}$ such that each z_k is a linear combination of the products $L_1(\mathbf{x})L_1'(\mathbf{y}), \ldots, L_t(\mathbf{x})L_t'(\mathbf{y})$. It is known from [4] that $t \geq 2n + 1$. Let $\mathbf{p} = (L_1(\mathbf{x})L_1'(\mathbf{y}), \ldots, L_t(\mathbf{x})L_t'(\mathbf{y}))^T$. By the definition of bilinear algorithms there exists a $(2n + 1) \times t$ matrix U whose entries are constants from $\mathbf{F}_q$ such that $\mathbf{z} = U\mathbf{p}$.

We contend first that $\mathbf{rank}\ U = 2n + 1$. Obviously, $z_k(\mathbf{x}, \mathbf{y}) = \mathbf{x}^T A_k \mathbf{y}$, where $A_k = (a_{i,j,k})$ is an $(n + 1) \times (n + 1)$ Hankel matrix defined by

$$a_{i,j,k} = \begin{cases} 1, & \text{if } i + j = k + 2, \\ 0, & \text{otherwise.} \end{cases}$$

Since the matrices $A_0, A_1, \ldots, A_{2n}$ are linearly independent, the rows of U are independent as well. This proves our contention.

Permuting the components of $\mathbf{p}$, if necessary, we may assume that the first $(2n + 1)$ columns of U are linearly independent. Hence, there exist a nonsingular $(2n + 1) \times (2n + 1)$ matrix W and $(2n + 1) \times (t - 2n - 1)$ matrix V such that

$$W\mathbf{z} = (I_{2n+1}, V)\mathbf{p},$$

where I_{2n+1} denotes the $(2n + 1) \times (2n + 1)$ identity matrix. That is, the first $(2n + 1)$ columns of the product WU are those of I_{2n+1}.

By Lemma 4, there exist $\mathbf{i}_q(n) + 1$ components of $W\mathbf{z}$ which define bilinear forms whose multiplicative complexity is at least $n + 1$. Without loss of generality we may assume that the above bilinear forms are defined by the last components of $W\mathbf{z}$. Since the first $2n - \mathbf{i}_q(n)$ components of the last $\mathbf{i}_q(n) + 1$ rows of (I_{2n+1}, V) are zero, we have $t - (2n - \mathbf{i}_q(n)) \geq n + 1$. This implies $t \geq 3n + 1 - \mathbf{i}_q(n)$. Using the $n/(\log_q n - 3)$ upper bound on $\mathbf{i}_q(n)$, cf. Appendix A, we obtain $M_q(n) = t > 3n - n/(\log_q n - 3)$. □

Remark. Applying the argument used in the proof of Lemma 4 to $2n + 1$ linearly independent Hankel matrices $H_0, H_1, \ldots, H_{2n}$, and assuming that **deg**

$p_1^{d_1}(\alpha) \geq \deg p_2^{d_2}(\alpha) \geq \cdots \geq \deg p_l^{d_l}(\alpha)$, one can improve the lower bound given by Theorem 1 by $O(n/\log_q^2 n)$. The proof requires a more involved counting argument than that in Appendix A and will be omitted.

5. *Proof of Theorem* 2

Let $\mathbf{x}(\alpha) = \sum_{i=0}^{n} x_i \alpha^i$ and $\mathbf{y}(\alpha) = \sum_{i=0}^{n} y_i \alpha^i$. Similarly to [18], computing the coefficients of the product $\mathbf{x}(\alpha)\mathbf{y}(\alpha)$ in $3n + 1 - \lfloor q/2 \rfloor$ multiplications can be easily done by computing $\mathbf{x}(\alpha)\mathbf{y}(\alpha)$ modulo linear and quadratic polynomials, cf. Appendix B. In order to prove the lower bound we proceed as follows.

Let $\mathbf{F}_q = \{e_1, e_2, \ldots, e_q\}$. Without loss of generality we may assume that $L_i(\mathbf{x})L_i'(\mathbf{y}) = \mathbf{x}(e_i)\mathbf{y}(e_i)$, $i = 1, 2, \ldots, q$, and $L_{q+1}(\mathbf{x})L_{q+1}'(\mathbf{y}) = x_n y_n$, cf. [1, Exercise 12.9, p. 445]. Using the same notation as in the proof of Theorem 1 we have $W\mathbf{z} = (I_{2n+1}, V)\mathbf{p}$, where the first $q + 1$ rows of V are zero. Let H_i be the Hankel matrix representing the bilinear forms defined by the ith component of $W\mathbf{z}$, $i = 1, 2, \ldots, 2n + 1$. Let $\mathbf{S} = \{H_{q+2}, H_{q+3}, \ldots, H_{2n+1}\}$. The proof of the $3n + 1 - \lfloor q/2 \rfloor$ lower bound is based on the following lemma.

LEMMA 5. *Either there exists a subset* $\mathbf{S}'$ *of* $\mathbf{S}$ *containing* $\lfloor (2n - q)/2 \rfloor$ *or fewer elements such that computing the set of bilinear forms defined by* $\{\mathbf{x}^T H \mathbf{y}\}_{H \in \mathbf{S}'}$ *requires at least* $(2n - q)$ *multiplications, or there exists a subset* $\mathbf{S}'$ *of* $\mathbf{S}$ *containing* $\lceil (2n - q)/2 \rceil$ *elements such that computing the set of bilinear forms defined by* $\{\mathbf{x}^T H \mathbf{y}\}_{H \in \mathbf{S}'}$ *requires at least* $2n - q + 1$ *multiplications.*

The proof of Lemma 5 is rather long and technical, and, for the sake of continuity, is postponed to the next section.

PROOF OF THEOREM 2. The proof is similar to the proof of Theorem 1. By Lemma 5, either there exist $\lfloor (2n - q)/2 \rfloor$ components of $W\mathbf{z}$ that define bilinear forms whose multiplicative complexity is at least $2n - q$, or there exist $\lceil (2n - q)/2 \rceil$ components of $W\mathbf{z}$ that define bilinear forms whose multiplicative complexity is at least $2n - q + 1$. Without loss of generality in both cases we may restrict ourselves to the last components of $W\mathbf{z}$.

In the former case, since the first $2n + 1 - \lfloor (2n - q)/2 \rfloor$ components of the last $\lfloor (2n - q)/2 \rfloor$ rows of (I_{2n+1}, V) are zero, we have

$$M_q(n) - \left(2n + 1 - \left\lfloor \frac{2n - q}{2} \right\rfloor\right) \geq 2n - q.$$

(Recall that (I_{2n+1}, V) is a $(2n + 1) \times M_q(n)$ matrix.) Therefore

$$M_q(n) \geq 4n + 1 - q - \left\lfloor \frac{2n - q}{2} \right\rfloor = 3n + 1 - \left(q + \left\lfloor -\frac{q}{2} \right\rfloor\right) = 3n + 1 - \left\lfloor \frac{q}{2} \right\rfloor.$$

In the latter case, since the first $2n + 1 - \lceil (2n - q)/2 \rceil$ components of the last $\lceil (2n - q)/2 \rceil$ rows of (I_{2n+1}, V) are zero, we have

$$M_q(n) - \left(2n + 1 - \left\lceil \frac{2n - q}{2} \right\rceil\right) \geq 2n - q + 1.$$

Therefore

$$\begin{aligned} M_q(n) &\geq 4n + 2 - q - \left\lceil \frac{2n - q}{2} \right\rceil \\ &= 3n + 1 - \left(q + \left\lceil -\frac{q}{2} \right\rceil - 1\right) \geq 3n + 1 - \left\lfloor \frac{q}{2} \right\rfloor. \end{aligned}$$

□

6. *Proof of Lemma* 5

In order to prove Lemma 5 we need some preliminary facts. First we observe that **rank** $H_i \le n$, $i = q+2, \ldots, 2n+1$. Were there an H_i of rank $n+1$, similarly to the proof of Theorem 1, we would have $M_q(n) > 3n$, which contradicts the upper bound at the beginning of this section.

By Lemma 1, we have $d_S + r_S \ge 2n - q$, which implies $\deg f_S(\alpha) \ge 2n - q - r_S$. Let $f_S(\alpha) = \prod_{i=1}^{l} p_i^{d_i}(\alpha)$ be the decomposition of $f_S(\alpha)$ into irreducible factors $p_1(\alpha)$, $p_2(\alpha), \ldots, p_l(\alpha)$ such that $\deg p_1^{d_1}(\alpha) \ge \deg p_2^{d_2}(\alpha) \ge \cdots \ge \deg p_l^{d_l}(\alpha)$. Write

$$f_S(\alpha) = \prod_{i=1}^{l} p_i^{d_i}(\alpha) = \left(\prod_{i=1}^{k} p_i^{d_i}(\alpha)\right)\left(\prod_{i=k+1}^{l} p_i(\alpha)\right),$$

where $p_{k+1}(\alpha), p_{k+2}(\alpha), \ldots, p_l(\alpha)$ are all the linear factors of $f_S(\alpha)$ of multiplicity 1.

PROPOSITION 3. *We have* $\deg \prod_{i=1}^{k} p_i^{d_i}(\alpha) \ge 2n - q - r_S$.

PROOF. Assume, by contradiction, that $\deg \prod_{i=1}^{k} p_i^{d_i}(\alpha) < 2n - q - r_S$ and consider the set of Hankel matrices $S'' = S \cup \{H_i\}_{i=1,2,\ldots,q}$. Obviously $r_{S''} = r_S$ and $\deg f_{S''}(\alpha) \le q + \deg \prod_{i=1}^{k} p_i^{d_i}(\alpha)$. Hence $d_{S''} + r_{S''} < q + 2n - q - r_S + r_S = 2n$. The last inequality contradicts Lemma 1, because $\dim[S''] = \dim[H_1, \ldots, H_q, H_{q+2}, \ldots, H_{2n+1}] = 2n$. □

Let m be such that $\deg \prod_{i=1}^{m-1} p_i^{d_i}(\alpha) < 2n - q - r_S$, and $\deg \prod_{i=1}^{m} p_i^{d_i}(\alpha) \ge 2n - q - r_S$.

PROPOSITION 4. *If q is even, or $r_S \ge 3$, or $\deg p_1^{d_1}(\alpha) \ge 3$, then we have*

$$m \le \begin{cases} \left\lfloor \dfrac{2n-q}{2} \right\rfloor, & \text{if } \deg \prod_{i=1}^{m} p_i^{d_i}(\alpha) \ge 2n - q, \\ \left\lfloor \dfrac{2n-q}{2} \right\rfloor - 1, & \text{if } \deg \prod_{i=1}^{m} p_i^{d_i}(\alpha) \le 2n - q - 1. \end{cases}$$

PROOF. Assume that $\deg \prod_{i=1}^{m} p_i^{d_i}(\alpha) \ge 2n - q$. If $\deg p_1^{d_1}(\alpha) \ge 3$, then

$$m \le \left\lceil \frac{2n-q-3}{2} \right\rceil + 1 = \left\lceil \frac{2n-q-1}{2} \right\rceil = \left\lfloor \frac{2n-q}{2} \right\rfloor,$$

and if q is even, then

$$m \le \frac{2n-q}{2} = \left\lfloor \frac{2n-q}{2} \right\rfloor.$$

If $\deg \prod_{i=1}^{m} p_i^{d_i}(\alpha) < 2n - q$, then $r_S \ge 1$. We shall consider the cases of $r_S = 1$, $r_S = 2$, and $r_S \ge 3$ separately.

Case of $r_S = 1$. In this case $\deg \prod_{i=1}^{m} p_i^{d_i}(\alpha) = 2n - q - 1$. Assume that q is odd and $\deg p_1^{d_1}(\alpha) \ge 3$. Since q is odd, $2n - q - 1$ is even. Hence either $\deg p_1^{d_1}(\alpha) \ge 4$ or $\deg p_2^{d_2}(\alpha) = 3$. In the case of $\deg p_1^{d_1}(\alpha) \ge 4$ we have

$$m \le 1 + \left\lfloor \frac{(2n-q-1)-4}{2} \right\rfloor = \left\lfloor \frac{2n-q}{2} \right\rfloor - 1,$$

and in the case of $\mathbf{deg}\, p_2^{d_2}(\alpha) = 3$ we have

$$m \le 2 + \left\lfloor \frac{(2n-q-1)-6}{2} \right\rfloor = \left\lfloor \frac{2n-q}{2} \right\rfloor - 1.$$

If q is even, then $2n-q-1$ is odd. Hence $\mathbf{deg}\, p_1^{d_1}(\alpha) \ge 3$, which implies

$$m \le 1 + \frac{(2n-q-1)-3}{2} = \left\lfloor \frac{2n-q}{2} \right\rfloor - 1.$$

Case of $r_S = 2$. If $\mathbf{deg}\, p_1^{d_1}(\alpha) \ge 3$, then

$$m \le \left(1 + \left\lceil \frac{(2n-q-2)-3}{2} \right\rceil\right) = \left\lceil \frac{2n-q-1}{2} \right\rceil - 1 = \left\lfloor \frac{2n-q}{2} \right\rfloor - 1,$$

and if q is even, then

$$m \le \frac{2n-q-2}{2} = \left\lfloor \frac{2n-q}{2} \right\rfloor - 1.$$

Case of $r_S \ge 3$. We have

$$m \le \left\lfloor \frac{2n-q-r_S}{2} \right\rfloor \le \left\lfloor \frac{2n-q-3}{2} \right\rfloor = \left\lceil \frac{2n-q-1}{2} \right\rceil - 1 = \left\lfloor \frac{2n-q}{2} \right\rfloor - 1.$$

This completes the proof of Proposition 4. □

PROPOSITION 5. *If q is even, or $r_S \ge 3$, or $\mathbf{deg}\, p_1^{d_1}(\alpha) \ge 3$, then there exists a subset $\mathbf{S}'$ of $\mathbf{S}$ containing $\lfloor (2n-q)/2 \rfloor$ or fewer elements such that computing the set of bilinear forms defined by $\{\mathbf{x}^T H \mathbf{y}\}_{H \in \mathbf{S}'}$ requires at least $2n-q$ multiplications.*

PROOF. Since $q \ge n-1$, we have $2n-q \le n+1$. Therefore, by Lemmas 2 and 3, it suffices to show that there exists a subset $\mathbf{S}'$ of $\mathbf{S}$ containing $\lfloor (2n-q)/2 \rfloor$ or fewer elements such that $d_{S'} + r_{S'} \ge 2n-q$. Similarly to the proof of Lemma 4 we shall construct $\mathbf{S}'$ inductively as follows.

If $\mathbf{deg} \prod_{i=1}^{m} p_i^{d_i}(\alpha) \ge 2n-q$, then $\mathbf{S}_0 = \emptyset$; and if $\mathbf{deg} \prod_{i=1}^{m} p_i^{d_i}(\alpha) \le 2n-q-1$, then $\mathbf{S}_0 = \{H_{i_0}\}$, where $\mathbf{rank}\, \bar{H}_{i_0} = r_S$.

Assume $\mathbf{S}_j$, $j < m$, has been constructed. If there exists an $H \in \mathbf{S}_j$ such that $f_H(\alpha)$ is divisible by $p_{j+1}^{d_{j+1}}(\alpha)$, then $\mathbf{S}_{j+1} = \mathbf{S}_j$. Otherwise, choose an $H_{i_{j+1}}$ such that $f_{H_{i_{j+1}}}(\alpha)$ is divisible by $p_{j+1}^{d_{j+1}}(\alpha)$ and put $\mathbf{S}_{j+1} = \mathbf{S}_j \cup \{H_{i_{j+1}}\}$.

Let $\mathbf{S}' = \mathbf{S}_m$. By the construction above, $f_{S'}(\alpha)$ is divisible by $\prod_{i=1}^{m} p_i^{d_i}(\alpha)$, hence $d_{S'} \ge 2n - q - r_S$. This together with $\mathbf{rank}\, \bar{H}_{i_0} = r_S$ implies $d_{S'} + r_{S'} \ge 2n-q$.

Obviously, the number of elements of $\mathbf{S}'$ does not exceed m, if $\mathbf{deg} \prod_{i=1}^{m} p_i^{d_i}(\alpha) \ge 2n-q$; and does not exceed $m+1$, otherwise. Thus the bound on the number of the elements of $\mathbf{S}'$ follows from Proposition 4. □

PROPOSITION 6. *If $r_S = 1$, and $\mathbf{deg}\, p_1^{d_1}(\alpha) = 2$, then there exists a subset $\mathbf{S}'$ of $\mathbf{S}$ containing $\lfloor (2n-q)/2 \rfloor$ or fewer elements such that computing the set of bilinear forms defined by $\{\mathbf{x}^T H \mathbf{y}\}_{H \in \mathbf{S}'}$ requires at least $2n-q$ multiplications.*

PROOF. Like in the proof of Proposition 5, it suffices to show there exists a subset $\mathbf{S}'$ of $\mathbf{S}$ containing $\lfloor (2n-q)/2 \rfloor$ or fewer elements such that $d_{S'} + r_{S'} \ge 2n - q$. Pick an $s \in \{q+2, q+3, \ldots, 2n+1\}$ such that $\mathbf{rank}\, \bar{H}_s = 1$. We contend that there exists an i, $1 \le i \le k$ such that $f_{H_s}(\alpha)$ is divisible by $p_i^{d_i}(\alpha)$. Since any $(n+1) \times (n+1)$ Hankel matrix H with $\mathbf{rank}\, \bar{H} = 1$ such that $f_H(\alpha)$ divides

$\prod_{i=k+1}^{l} p_i(\alpha)$ belongs to $[H_1, H_2, \ldots, H_{q+1}]$, cf. [13, Theorem 8.55, p. 425], for some i, $1 \le i \le k$, $f_{H_s}(\alpha)$ is divisible by $p_i^t(\alpha)$, where $t \le d_i$ and $\deg p_i^t(\alpha) \ge 2$. Since $\deg p_1^{d_1} = 2$, we have $\deg p_i^{d_i}(\alpha) = 2$, which implies $t = d_i$. This completes the proof of our contention. Without loss of generality we may assume that $f_{H_s}(\alpha)$ is divisible by $p_1^{d_1}(\alpha)$. Then $\mathbf{S}'$ can be constructed as follows.

Let $\mathbf{S}_1 = \{H_s\}$. Assume $\mathbf{S}_j$, $j < m$, has been constructed. If there exists an $H \in \mathbf{S}_j$ such that $f_H(\alpha)$ is divisible by $p_{j+1}^{d_{j+1}}(\alpha)$, then $\mathbf{S}_{j+1} = \mathbf{S}_j$. Otherwise, choose an $H_{i_{j+1}}$ such that $f_{H_{i_{j+1}}}(\alpha)$ is divisible by $p_{j+1}^{d_{j+1}}(\alpha)$ and put $\mathbf{S}_{j+1} = \mathbf{S}_j \cup \{H_{i_{j+1}}\}$.

Let $\mathbf{S}' = \mathbf{S}_m$. By the construction above, $f_{\mathbf{S}'}(\alpha)$ is divisible by $\prod_{i=1}^{m} p_i^{d_i}(\alpha)$. Since $H_s \in \mathbf{S}'$, it follows that $d_{\mathbf{S}'} + r_{\mathbf{S}'} = d_{\mathbf{S}'} + 1 = 2n - q$. Obviously, the number of the elements of $\mathbf{S}'$ does not exceed m. Therefore, by the definition of m, we have

$$m \le \left\lceil \frac{2n - q - 1}{2} \right\rceil = \left\lfloor \frac{2n - q}{2} \right\rfloor. \qquad \square$$

PROPOSITION 7. *Let q be odd, $r_{\mathbf{S}} = 2$, and $\deg p_1^{d_1}(\alpha) = 2$. If there is an $H_s \in \mathbf{S}$ such that $\mathbf{rank}\ \bar{H}_s = 2$ and $\deg f_{H_s}(\alpha) \ge 1$, then there exists a subset $\mathbf{S}'$ of $\mathbf{S}$ containing $\lfloor (2n - q)/2 \rfloor$ or fewer elements such that computing the set of bilinear forms defined by $\{\mathbf{x}^T H \mathbf{y}\}_{H \in \mathbf{S}'}$ requires at least $2n - q$ multiplications.*

PROOF. It suffices to show there exists a subset $\mathbf{S}'$ of $\mathbf{S}$ containing $\lfloor (2n - q)/2 \rfloor$ or fewer elements such that $d_{\mathbf{S}'} + r_{\mathbf{S}'} \ge 2n - q$. Let $\mathbf{rank}\ \bar{H}_s = 2$ and $\deg f_{H_s}(\alpha) \ge 1$. If for no i, $k < i \le l$, $f_{H_s}(\alpha)$ is divisible by $p_i(\alpha)$, then, without loss of generality, we may assume that $f_{H_s}(\alpha)$ is divisible by $p_1(\alpha)$. We construct $\mathbf{S}'$ as follows.

Let $\mathbf{S}_1 = \{H_s\}$. Assume $\mathbf{S}_j$, $j < m$, has been constructed. If there exists an $H \in \mathbf{S}_j$ such that $f_H(\alpha)$ is divisible by $p_{j+1}^{d_{j+1}}(\alpha)$, then $\mathbf{S}_{j+1} = \mathbf{S}_j$. Otherwise, choose an $H_{i_{j+1}}$ such that $f_{H_{i_{j+1}}}(\alpha)$ is divisible by $p_{j+1}^{d_{j+1}}(\alpha)$ and put $\mathbf{S}_{j+1} = \mathbf{S}_j \cup \{H_{i_{j+1}}\}$.

Let $\mathbf{S}' = \mathbf{S}_m$. By the construction above, $f_{\mathbf{S}'}(\alpha)$ is divisible by $p_j(\alpha) \prod_{i=2}^{m} p_i^{d_i}(\alpha)$, where $j = 1$, or $j > k$. Since

$$\deg \prod_{i=2}^{m} p_i^{d_i}(\alpha) = 2n - q - r_{\mathbf{S}} - 1 = 2n - q - 3,$$

we have $d_{\mathbf{S}'} \ge 2n - q - 2$. Therefore, $d_{\mathbf{S}'} + r_{\mathbf{S}'} = d_{\mathbf{S}'} + 2 \ge 2n - q$. Obviously, the number of the elements of $\mathbf{S}'$ does not exceed m. Since q is odd, we have

$$m \le \left\lceil \frac{2n - q - 2}{2} \right\rceil = \left\lfloor \frac{2n - q}{2} \right\rfloor. \qquad \square$$

PROPOSITION 8. *Let q be odd, $r_{\mathbf{S}} = 0$, and $\deg p_1^{d_1}(\alpha) = 2$. If there is an $H_s \in \mathbf{S}$ such that $\deg f_{H_s}(\alpha) \ge 3$, then there exists a subset $\mathbf{S}'$ of $\mathbf{S}$ containing $\lfloor (2n - q)/2 \rfloor$ or fewer elements such that computing the set of bilinear forms defined by $\{\mathbf{x}^T H \mathbf{y}\}_{H \in \mathbf{S}'}$ requires at least $2n - q$ multiplications.*

PROOF. It suffices to show there exists a subset $\mathbf{S}'$ of $\mathbf{S}$ containing $\lfloor (2n - q)/2 \rfloor$ or fewer elements such that $d_{\mathbf{S}'} + r_{\mathbf{S}'} \ge 2n - q$. Let $\deg f_{H_s}(\alpha) \ge 3$. Exactly as in the proof of Proposition 7, one can show that there exists an i, $1 \le i \le k$, such that $f_{H_s}(\alpha)$ is divisible by $p_i^{d_i}(\alpha)$. It will be convenient to assume that $f_{H_s}(\alpha)$ is divisible by $p_2^{d_2}(\alpha)$. If for no i, $k < i \le l$, $f_{H_s}(\alpha)$ is divisible by $p_i(\alpha)$, then we may assume that $f_{H_s}(\alpha)$ is divisible by $p_1(\alpha)$. We construct $\mathbf{S}'$ as follows.

Let $\mathbf{S}_2 = \{H_s\}$. Assume $\mathbf{S}_j$, $j < m$, has been constructed. If there exists an $H \in \mathbf{S}_j$ such that $f_H(\alpha)$ is divisible by $p_{j+1}^{d_{j+1}}(\alpha)$, then $\mathbf{S}_{j+1} = \mathbf{S}_j$. Otherwise, choose an $H_{i_{j+1}}$ such that $f_{H_{i_{j+1}}}(\alpha)$ is divisible by $p_{j+1}^{d_{j+1}}(\alpha)$ and put $\mathbf{S}_{j+1} = \mathbf{S}_j \cup \{H_{i_{j+1}}\}$.

Let $\mathbf{S}' = \mathbf{S}_m$. By the construction above, $f_{\mathbf{S}'}(\alpha)$ is divisible by $p_j(\alpha) \prod_{i=2}^{m} p_i^{d_i}(\alpha)$, where $j = 1$, or $j > k$. Since $\deg \prod_{i=2}^{m} p_i^{d_i}(\alpha) = 2n - q - 1$, we have $d_{\mathbf{S}'} \ge 2n - q$.

Obviously, the number of the elements of $\mathbf{S}'$ does not exceed $m-1$. Since q is odd, we have

$$m-1 \le \left\lceil \frac{2n-q}{2} \right\rceil - 1 = \left\lceil \frac{2n-q-2}{2} \right\rceil = \left\lfloor \frac{2n-q}{2} \right\rfloor. \qquad \square$$

In view of Propositions 5–8, we may assume that q is odd, $\mathbf{deg}\, p_1^{d_1}(\alpha) = 2$, and $r_{\mathbf{S}} = 0$; or q is odd, $\mathbf{deg}\, p_1^{d_1}(\alpha) = 2$, $r_{\mathbf{S}} = 2$, and for any $H \in \mathbf{S}$, if $\mathbf{rank}\, \bar{H} = 2$, then $\bar{H} = H$. The above two cases are treated by Propositions 9 and 10 below.

PROPOSITION 9. *If q is odd, $\mathbf{deg}\, p_1^{d_1}(\alpha) = 2$, and $r_{\mathbf{S}} = 0$, then there exists a subset $\mathbf{S}'$ of $\mathbf{S}$ containing $\lceil (2n-q)/2 \rceil$ elements such that computing the set of bilinear forms defined by $\{\mathbf{x}^T H \mathbf{y}\}_{H \in \mathbf{S}'}$ requires at least $2n-q+1$ multiplications.*

PROOF. Since q is odd, we have $m = \lceil (2n-q)/2 \rceil$. We may assume that $f_{H_{2n-m+i}}(\alpha) = p_i^{d_i}(\alpha)$, $i = 1, 2, \ldots, m$.

If $2n-q = 1$, let $\mathbf{S}' = \{H_{2n}\}$. Since $\mathbf{deg}\, f_{H_{2n}}(\alpha) = 2$, it follows that $\mathbf{rank}\, H_{2n} = 2$. Hence computing $\mathbf{x}^T H_{2n} \mathbf{y}$ requires two multiplications.

If $2n-q = 3$, let $\mathbf{S}' = \{H_{2n-1}, H_{2n}\}$. The inequality $q \ge 3$, implies $n+1 \ge 4$. Hence, by Lemmas 2 and 3, computing $\{\mathbf{x}^T H_{2n-1} \mathbf{y}, \mathbf{x}^T H_{2n} \mathbf{y}\}$ requires at least four multiplications.

Let $2n-q \ge 5$. The set of bilinear forms $\{\mathbf{x}^T H \mathbf{y}\}_{H \in \mathbf{S}}$ can be computed by

$$(\mathbf{x}^T H_{2n-m+1} \mathbf{y}, \mathbf{x}^T H_{2n-m+2} \mathbf{y}, \ldots, \mathbf{x}^T H_{2n} \mathbf{y})^T = (I_m, U)\mathbf{p},$$

where U consists of the last m rows of V. (Recall that $W\mathbf{z} = (I_{2n+1}, V)\mathbf{p}$.) We have to prove that U has at least m columns. Assume, by contradiction, that U has at most $2n-q-m = m-1$ columns.[6] Let

$$U = (u_{i,j})_{\substack{i=1,\ldots,m \\ j=1,\ldots,m-1}}.$$

Since computing each $\mathbf{x}^T H_i \mathbf{y}$, $i = 2n-m+1, 2n-m+2, \ldots, 2n$, requires at least two multiplications and the number of columns of U is less than m, the matrix U has a column with two nonzero components. Permuting the columns and rows of U, if necessary, we may assume that $u_{m-1,m-1}$ and $u_{m,m-1}$ are not equal to zero. Then there exist nonzero $a_2, a_3, \ldots, a_m \in \mathbf{F}_q$ such that $\sum_{i=2}^{m} a_i u_{i,m-1} = 0$.

Consider the matrix H defined by $H = \sum_{i=2}^{m} a_i H_{2n-m+i}$. Since for $i = 2n-q+1, \ldots, 2n$, $\bar{H}_i$ is the zero matrix, $\bar{H}$ is the zero matrix as well. Then, in view of Proposition 1, we have $f_H(\alpha) = \prod_{i=2}^{m} p_i^{d_i}(\alpha)$, cf. [13, Theorem 8.57, p. 426]. It follows from Proposition 2 that $\mathbf{rank}\, H = 2n-q-1$. On the other hand, the bilinear form $\mathbf{x}^T H \mathbf{y}$ can be computed in $2n-q-2$ multiplications by

$$\mathbf{x}^T H \mathbf{y} = (0, a_2, \ldots, a_{m-1}, a_m)(I_m, U)\mathbf{p},$$

because the first and the last component of $(0, a_2, \ldots, a_{m-1}, a_m)(I_m, U)$ are zero. This contradiction completes the proof of Proposition 9. $\square$

PROPOSITION 10. *Let q be odd, $\mathbf{deg}\, p_1^{d_1}(\alpha) = 2$, $r_{\mathbf{S}} = 2$, and for any $H \in \mathbf{S}$, if $\mathbf{rank}\, \bar{H} = 2$, then $\bar{H} = H$. Then there exists a subset $\mathbf{S}'$ of $\mathbf{S}$ containing $\lceil (2n-q)/2 \rceil$ elements such that computing the set of bilinear forms defined by $\{\mathbf{x}^T H \mathbf{y}\}_{H \in \mathbf{S}'}$ requires at least $2n-q+1$ multiplications.*

[6] It follows from Lemma 2 that U has at least $2n-q-m$ columns.

PROOF. We may assume that $2n - q \geq 5$. The case of $2n - q \leq 3$ can be treated exactly as in the proof of Proposition 9. Since q is odd, we have $m = \lceil (2n - q)/2 \rceil - 1$. We may assume that for some j, $2n - m \leq j \leq 2n$, **rank** $\bar{H}_j = 2$, and that for each $i = 1, 2, \ldots, m$ there exists a j_i, $2n - m \leq j_i \leq 2n$ such that $f_{H_{j_i}}(\alpha) = p_i^{d_i}(\alpha)$. Then we have

$$(\mathbf{x}^T H_{2n-m}\mathbf{y}, \mathbf{x}^T H_{2n-m+2}\mathbf{y}, \ldots, \mathbf{x}^T H_{2n}\mathbf{y})^T = (I_{m+1}, U)\mathbf{p},$$

where U consists of the last $m + 1$ rows of V.

We have to prove that U has at least $m + 1$ columns. Assume, by contradiction, that U has $2n - q - (m + 1) = m$ columns. Let $U = (u_{i,j})_{i=1,\ldots,m+1, j=1,\ldots,m}$. Since computing each $\mathbf{x}^T H_i \mathbf{y}$, $i = 2n - m, 2n - m + 1, \ldots, 2n$, requires at least two multiplications and the number of columns of U is equal to m, the matrix U has a column with two nonzero components. Permuting the columns and rows U, if necessary, we may assume that $u_{m,m}$ and $u_{m+1,m}$ are not equal to zero. If **rank** $\bar{H}_{2n-m} = 2$, then we proceed exactly as in the proof of Proposition 9. Otherwise we may assume that $f_{H_{2n-m}}(\alpha) = p_1^{d_1}(\alpha)$ and **rank** $\bar{H}_{2n-m+1} = 2$. There exist nonzero $a_2, a_3, \ldots, a_m \in \mathbf{F}_q$ such that $\sum_{i=2}^{m} a_i u_{i,m-1} = 0$. Consider the matrix H defined by $H = \sum_{i=1}^{m} a_i H_{2n-m+i}$.

Since for $i = 2n - q - m + 1, \ldots, 2n$, **rank** $\bar{H}_i \leq 1$, it follows that **rank** $\bar{H} \leq 2$. Then $f_H(\alpha) = \prod_{i=1}^{m-1} p_i^{d_i}(\alpha)$, and, by Proposition 2, we have **rank** $H = 2n - q - 1$. On the other hand, exactly as in the proof of Proposition 9, it can be shown that the bilinear form $\mathbf{x}^T H \mathbf{y}$ can be computed in $2n - q - 2$ multiplications. This contradiction completes the proof of Proposition 10. □

Now the reader can easily convince himself that Lemma 5 follows from Propositions 5–10.

Notice that if $n = q + 1$, then in the conditions of Propositions 9 or 10 we have the tight $n + 2$ bound on the number of multiplications required to compute $\{\mathbf{x}^T H_i \mathbf{y}\}_{i=3n/2,\ldots,2n}$. This bound exceeds the lower bound given by Lemma 2.

7. *Multiplication of Polynomials Modulo a Polynomial*

Here we consider an application of the technique developed in the previous sections to multiplication of polynomials modulo a polynomial. All the results obtained in this section are easy corollaries of Lemma 6 below. To proceed we need one more notation. For polynomials $\mathbf{z}(\alpha)$ and $P(\alpha)$ we denote by $\mathbf{res}(\mathbf{z}(\alpha), P(\alpha))$ the minimal degree residue of $\mathbf{z}(\alpha)$ modulo $P(\alpha)$.

LEMMA 6. *Let* $\mathbf{x}(\alpha) = \sum_{i=0}^{n} x_i \alpha^i$ *and* $\mathbf{y}(\alpha) = \sum_{i=0}^{n} y_i \alpha^i$ *be polynomials with indeterminate coefficients, and let* $P(\alpha) = \alpha^m - \sum_{i=0}^{m-1} a_i \alpha^i$ *be a fixed polynomial over* F *of degree* $m > n$. *Let* $\mathbf{x}^T H \mathbf{y}$ *be a bilinear form defined by a linear combination of the coefficients of* $\mathbf{res}(\mathbf{x}(\alpha)\mathbf{y}(\alpha), P(\alpha))$, *If* **rank** $H \leq 2n + 1 - m$, *then* $f_H(\alpha)$ *divides* $P(\alpha)$, *and* **rank** $\bar{H} = 0$.

PROOF. Let $\mathbf{x}^T H \mathbf{y}$ be a bilinear form defined by a linear combination of the coefficients of $\mathbf{res}(\mathbf{x}(\alpha)\mathbf{y}(\alpha), P(\alpha))$. First we contend that if $H = H(\sigma)$, then $P(\alpha)$ is a characteristic polynomial of σ. Since the set of all linear recurring sequences satisfying the same recurrence is a linear space over F, we may assume that $\mathbf{x}^T H \mathbf{y}$ is defined by a coefficient of $\mathbf{res}(\mathbf{x}(\alpha), \mathbf{y}(\alpha), P(\alpha))$. Let $\mathbf{x}(\alpha)\mathbf{y}(\alpha) = \mathbf{z}(\alpha) = \sum_{i=0}^{2n} z_i \alpha^i$, and let $\mathbf{res}(\mathbf{z}(\alpha), P(\alpha)) = \sum_{i=0}^{m-1} u_i \alpha^i$, where $u_i = \sum_{j=0}^{2n} s_{i,j} z_j$, $i = 0, 1, \ldots, m - 1$. We have to prove that $P(\alpha)$ is a characteristic polynomial of $\sigma_i = s_{i,0}, s_{i,1}, \ldots, s_{i,2n}$, $i = 0, 1, \ldots, m - 1$.

Let $P(\alpha) = \alpha^m - \sum_{i=0}^{m-1} a_i \alpha^i$ and let C_P denote the companion matrix of $P(\alpha)$, that is,

$$C_P = \begin{pmatrix} 0 & 0 & \cdots & 0 & a_0 \\ 1 & 0 & \cdots & 0 & a_1 \\ 0 & 1 & \cdots & 0 & a_2 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & a_{m-1} \end{pmatrix}.$$

Let $\sigma_{i,k} = (s_{i,k}, s_{i,k+1}, \ldots, s_{i,k+m-1})$ be the kth m-dimensional state vector of σ_i, $i = 0, 1, \ldots, m-1$; $k = 0, 1, \ldots, 2n - m + 1$. In order to prove our contention it suffices to show that $\sigma_{i,k} = \sigma_{i,0} C_P^k$, or, since, trivially, $\sigma_{i,0}$ is equal to the ith row of I_m, it suffices to show that $\sigma_{i,k}$ is equal to the $(i+1)$st row of C_P^k.

Using the regular matrix representation of the algebra $F[\alpha]/(P(\alpha))$, cf. [6, p. 424], we obtain that the column vector of the coefficients of $\mathbf{res}(\mathbf{z}(\alpha), P(\alpha))$ is equal to

$$(z_0, z_1, \ldots, z_{m-2}, z_{m-1})^{\mathrm{T}} + \sum_{k=n}^{m} z_k C_P^{k-m+1} (0, 0, \ldots, 0, 1)^{\mathrm{T}}.$$

Therefore, if $k \geq m$, then $s_{i,k}$ is the ith component of the last row of C_P^{k-m+1}. Now the contention follows from the fact that the vector of the first $m-1$ components of the ith row of C_P^d is equal to the vector of the last $m-1$ components of the ith row of C_P^{d+1}.

Since, $\mathbf{rank}\ H \leq 2n - m + 1$, by Proposition 2, we have $\mathbf{deg}\, f_H(\alpha) + \mathbf{rank}\ \bar{H} \leq 2n + 1 - m$, which implies $\mathbf{deg}\, f_H(\alpha) \leq 2n + 1 - \mathbf{rank}\ \bar{H} - m = l - m + 1$. Now the divisibility of $P(\alpha)$ by $f_H(\alpha)$ follows from Proposition 1.

It remains to show that $\mathbf{rank}\ \bar{H} = 0$. $f_H(\alpha)$ divides $P(\alpha)$, which implies that $P(\alpha)$ is a characteristic polynomial of $\bar{\sigma} = \sigma - \tilde{\sigma}$, cf. [13, Theorem 8.55, p. 425]. Since σ and $\tilde{\sigma}$ have the same first m elements, $\bar{\sigma}$ is the zero sequence. Hence $\bar{H}$ is the zero matrix. □

Next we present some corollaries to Lemma 6. Whereas Corollaries 1 and 2 were established in [18] in a more general form, Corollaries 3 and 4 are new and cannot be obtained by the technique used in [18].

COROLLARY 1. *Let the field of constants be infinite, and let* $P(\alpha) = \prod_{i=1}^{k} p_i^{d_i}(\alpha)$ *be a fixed polynomial of degree* $n+1$ *with its factorization into irreducible factors* $p_1(\alpha), p_2(\alpha), \ldots, p_k(\alpha)$. *Let* $\mathbf{x}(\alpha)$ *and* $\mathbf{y}(\alpha)$ *be polynomials of degree* n *with indeterminate coefficients. Then computing* $\mathbf{res}(\mathbf{x}(\alpha)\mathbf{y}(\alpha), P(\alpha))$ *requires exactly* $(2n + 2 - k)$ *multiplications.*

PROOF. Computing $\mathbf{res}(\mathbf{x}(\alpha)\mathbf{y}(\alpha), P(\alpha))$ can be performed in $2n + 2 - k$ multiplications by means of Chinese Remainder Theorem, cf. [18]. To prove the lower bound stated in the corollary we proceed as follows. Assume that computing $\mathbf{res}(\mathbf{x}(\alpha)\mathbf{y}(\alpha), P(\alpha))$ can be performed in t multiplications. Let $\mathbf{res}(\mathbf{x}(\alpha)\mathbf{y}(\alpha), P(\alpha)) = \sum_{i=0}^{n} u_i \alpha^i$, $\mathbf{u} = (u_0, u_1, \ldots, u_n)^{\mathrm{T}}$, and let $\mathbf{p}$ be a t-dimensional vector of products of linear forms of $\mathbf{x}$ and $\mathbf{y}$ such that $\mathbf{u} = U\mathbf{p}$, where U is an $(n+1) \times t$ constant matrix. We have to prove that $t \geq 2n + 2 - k$. Exactly as in the proof of Theorem 1, it can be shown that there exists a nonsingular matrix W such that $W\mathbf{u} = (I_{n+1}, V)\mathbf{p}$.

Let $\mathbf{S} = \{H_0, H_1, \ldots, H_n\}$ be the set of Hankel matrices representing the bilinear forms defined by the components of $W\mathbf{u}$. If there exists an $H \in \mathbf{S}$ such that **rank** $H = n + 1$, then V must have at least n columns, which implies $t = 2n + 1 \geq 2n + 2 - k$. If **rank** $H_i \leq n$, $i = 0, 1, \ldots, n$, then it follows from Lemmas 1 and 6 that $f_{\mathbf{S}}(\alpha) = P(\alpha)$ and $r_{\mathbf{S}} = 0$. Exactly as in the proof of Lemma 4, we can find a subset $\mathbf{S}'$ of $\mathbf{S}$ containing at most k elements such that $d_{\mathbf{S}'} = n + 1$. Then, exactly as in the proof of Theorem 1, we have $t - (n + 1 - k) \geq n + 1$, or $t \geq 2n + 2 - k$. □

The following corollary is a partial case of the *direct sum conjecture* conjectured by Strassen in [16].

Let $\mathbf{B} = \mathbf{B}(\mathbf{x}, \mathbf{y})$ be a finite set of bilinear forms of $\mathbf{x}$ and $\mathbf{y}$ over a field F. $\mu_F(\mathbf{B})$ denotes the minimal number of multiplications required to compute all the forms of $\mathbf{B}$ by means of bilinear algorithms over F.

COROLLARY 2. *Let the field of constants F be infinite, and let $\mathbf{x}_i(\alpha)$ and $\mathbf{y}_i(\alpha)$, $i = 1, 2, \ldots, k$, be polynomials of degree n_i with disjoint set of indeterminate coefficients. Let $P_1(\alpha), P_2(\alpha), \ldots, P_k(\alpha)$ be powers of distinct irreducible polynomials,* **deg** $P_i(\alpha) = n_i$, $i = 1, 2, \ldots, k$. *Then*

$$\mu_F\left(\bigcup_{i=1}^{k} \mathbf{res}(\mathbf{x}_i(\alpha)\mathbf{y}_i(\alpha), P_i(\alpha))\right) = \sum_{i=1}^{k} \mu_F(\mathbf{res}(\mathbf{x}_i(\alpha)\mathbf{y}_i(\alpha), P_i(\alpha))) = \sum_{i=1}^{k} (2n_i + 1).$$

PROOF. The proof immediately follows from Corollary 1, because, by means of Chinese Remainder Theorem, each algorithm for computing $\bigcup_{i=1}^{k} \mathbf{res}(\mathbf{x}_i(\alpha)\mathbf{y}_i(\alpha), P_i(\alpha))$ can be transformed to an algorithm for multiplying the polynomials of degree $\sum_{i=1}^{k} n_i - 1$ modulo the product of the moduli. □

The above two proofs differ from those of Winograd in [18] in the following. In [18] the result concerning multiplication of polynomials modulo a polynomial implied by an instance of the direct sum conjecture, which was proved first.

COROLLARY 3. *Let the field of constants F be infinite, and let $P(\alpha) = \prod_{i=1}^{k} p_i^{d_i}(\alpha)$ be a fixed polynomial of degree m with its factorization into irreducible factors $p_1(\alpha), p_2(\alpha), \ldots, p_k(\alpha)$. Let $\mathbf{x}(\alpha)$ and $\mathbf{y}(\alpha)$ be polynomials of degree $n < m$ with indeterminate coefficients. If $m - k \geq n$, then computing* **res**$(\mathbf{x}(\alpha)\mathbf{y}(\alpha), P(\alpha))$ *requires $2n + 1$ multiplications.*

PROOF. Obviously, computing **res**$(\mathbf{x}(\alpha)\mathbf{y}(\alpha), P(\alpha))$ can be performed in $2n + 1$ multiplications by first computing the product $\mathbf{x}(\alpha)\mathbf{y}(\alpha)$, and then reducing it modulo $P(\alpha)$. To prove the lower bound stated in the corollary we proceed as follows. Assume that computing **res**$(\mathbf{x}(\alpha)\mathbf{y}(\alpha), P(\alpha))$ can be performed in t multiplications. Let **res**$(\mathbf{x}(\alpha)\mathbf{y}(\alpha), P(\alpha)) = \sum_{i=0}^{m-1} u_i\alpha^i$, and let $\mathbf{u} = (u_0, u_1, \ldots, u_{m-1})^{\mathrm{T}}$. Let $\mathbf{p}$ be a t-dimensional vector of products of linear forms of $\mathbf{x}$ and $\mathbf{y}$ such that $\mathbf{u} = U\mathbf{p}$, where U is an $m \times t$ constant matrix. We have to prove that $t \geq 2n + 1$. As in the previous proofs, it can be shown that there exists a nonsingular matrix W such that $W\mathbf{u} = (I_m, V)\mathbf{p}$.

Let $\mathbf{S} = \{H_0, H_1, \ldots, H_{m-1}\}$ be the set of Hankel matrices representing the bilinear forms defined by the components of $W\mathbf{z}$. If there exists an $H_i \in \mathbf{S}$ such that **rank** $H_i > 2n + 1 - m$, then V must have at least $2n - m$ columns, which implies $t \geq 2n + 1$. Otherwise, by Lemmas 1 and 6, we have $d_{\mathbf{S}} \geq m$. Then, as in the proof of Lemma 4, one can show that there exists a subset $\mathbf{S}'$ of $\mathbf{S}$ containing at most k elements such that $d_{\mathbf{S}'} \geq n + 1$. By Lemma 2, we have $\mu_F(\{\mathbf{x}^{\mathrm{T}}H\mathbf{y}\})_{H \in \mathbf{S}'} \geq$

$n + 1$. Then, exactly as in the proof of Theorem 1, we have $t - (m - k) \geq n + 1$. Since $m - k \geq n$ the above inequality implies $t \geq (m - k) + (n + 1) \geq 2n + 1$. □

COROLLARY 4. *Let the field of constants be infinite. Let n be even and let $P(\alpha) = \prod_{i=1}^{1+n/2} p_i^{d_i}(\alpha)$ be a fixed polynomial of degree $n + 2$ with its factorization into irreducible factors $p_1(\alpha), p_2(\alpha), \ldots, p_{1+n/2}(\alpha)$ such that* $\deg p_i^{d_i}(\alpha) = 2$, $i = 1, 2, \ldots, 1 + n/2$. *Let $\mathbf{x}(\alpha)$ and $\mathbf{y}(\alpha)$ be polynomials of degree n with indeterminate coefficients. Then computing $\mathbf{res}(\mathbf{x}(\alpha)\mathbf{y}(\alpha), P(\alpha))$ requires exactly $3 + 3n/2$ multiplications.*

The proof of Corollary 4 is similar to the proof of Proposition 9 and will be omitted. Notice that in Corollaries 3 and 4 the degree of the moduli is greater than $n + 1$.

In order to state one more corollary to Lemma 6 we need the following definition:

Definition. Let F^k be the k-dimensional vector space over a field F, and let $\{e_1, \ldots, e_k\}$ be a fixed basis of F^k. Let $v = \sum_{i=1}^{k} a_i e_i \in F^k$. Define $\omega(v)$, the *weight* of v, as the number of nonzero components a_i of v. If L is a subspace of F^k of dimension l, we say that L is a *linear code of dimension l and length k.* Define $\omega(L)$, the *minimal distance* of L, *by* $\omega(L) = \mathbf{min}\ \{\omega(v) \mid \overline{0} \neq v \in L\}$.

COROLLARY 5. *Let $\mathbf{x}(\alpha)$ and $\mathbf{y}(\alpha)$ be polynomials with indeterminate coefficients of degree n over a field F, and let $P(\alpha)$ be a fixed polynomial of degree $m > n$. If $P(\alpha)$ has no factors of degree less than $2n + 2 - m$, then the number of multiplications required to compute $\mathbf{res}(\mathbf{x}(\alpha)\mathbf{y}(\alpha), P(\alpha))$ by means of a bilinear algorithm over F is not smaller than the minimum code length of linear codes over F of minimal distance $2n + 2 - m$ and dimension m. In particular, if F is infinite, then computing $\mathbf{res}(\mathbf{x}(\alpha), \mathbf{y}(\alpha), P(\alpha))$ requires exactly $2n + 1$ multiplications.*

For an irreducible polynomial $P(\alpha)$ and $m = n + 1$; and for an irreducible polynomial $P(\alpha)$ and any $m \geq n + 1$ the above corollary was obtained in [11] and [9], respectively.

PROOF. Let $\mathbf{x}^T H \mathbf{y}$ be a bilinear form defined by a linear combination of the coefficients of $\mathbf{res}(\mathbf{x}(\alpha)\mathbf{y}(\alpha), P(\alpha))$. It suffices to show that $\mathbf{rank}\ H \geq 2n + 2 - m$. Were $\mathbf{rank}\ H \leq 2n + 1 - m$, by Proposition 2 and Lemma 6, $P(\alpha)$ would have a factor of degree less than $2n + 2 - m$, which contradicts the conditions of the corollary. □

Notice that the second part of Corollary 5 follows from Corollary 3 as well.

Appendix A. The Number of Distinct Factors of a Polynomial over a Finite Field

Let $\mathbf{i}_q(n)$ denote the maximal possible number of distinct irreducible factors of a polynomial of degree n over $\mathbf{F}_q$. In this appendix we prove the following upper bound on $\mathbf{i}_q(n)$.

LEMMA A1. *If $q \geq 3$, then $\mathbf{i}_q(n) \leq n/(\log_q n - 3)$.*

Let $N_q(j)$ denote the number of monic irreducible polynomials of degree j over $\mathbf{F}_q$. It is well-known that $N_q(j) = (1/j) \sum_{d|j} \mu(d) q^{j/d}$, where $\mu(d)$ is Möbius function of d, cf. [13, Theorem 3.25, p. 93].

For the proof of Lemma A1 we need some preliminary results.

PROPOSITION A1. *If $j \geq 5$ and $q \geq 3$, then $2N_q(j - 1) \leq N_q(j)$.*

PROOF. We have

$$\frac{1}{j}\,q^j - \frac{q}{j(q-1)}\,(q^{j/2}-1) \le N_q(j) \le \frac{1}{j}\,(q^j - q),$$

cf. [13, Exercises 3.26 and 3.27, p. 142]. Hence, it suffices to show that

$$\frac{2q^{j-1}}{j-1} < \frac{q^j}{j} - \frac{q}{j(q-1)}\,q^{j/2}.$$

Multiplying the above inequality of j/q^j and performing simple manipulations, we obtain that it is equivalent to

$$2\left(1 + \frac{1}{j-1}\right) < q - \frac{q}{q-1}\,q^{1-j/2}.$$

Recalling the bounds on q and j we obtain

$$2\left(1 + \frac{1}{j-1}\right) < 2\left(1 + \frac{1}{4}\right) \le 3 - \frac{3}{2}\,3^{-3/2} \le q - q^{1-j/2}. \qquad \square$$

PROPOSITION A2. *If* $q \ge 3$ *and* $k \ge 2$, *then* $\sum_{j=1}^{k} N_q(j) < 1/(k-1) \sum_{j=1}^{k} jN_q(j)$.

PROOF. We have

$$\frac{1}{k-1}\sum_{j=1}^{k} jN_q(j) = \sum_{m=3}^{k}\left(\frac{1}{m-1}\sum_{j=1}^{m} jN_q(j) - \frac{1}{m-2}\sum_{j=1}^{m-1} jN_q(j)\right) + \sum_{j=1}^{2} jN_q(j).$$

Since

$$\sum_{j=1}^{2} jN_q(j) > \sum_{j=1}^{2} N_q(j),$$

it suffices to show that if $m \ge 3$, then

$$N_q(m) < \frac{1}{m-1}\sum_{j=1}^{m} jN_q(j) - \frac{1}{m-2}\sum_{j=1}^{m-1} jN_q(j).$$

Multiplying the last inequality by $(m-1)(m-2)$ and performing simple manipulations, we obtain that it is equivalent to

$$\sum_{j=1}^{m-1} jN_q(j) < (m-2)N_q(m) = \sum_{j=5}^{m} [(j-2)N_q(j) - (j-3)N_q(j-1)] + 2N_q(4).$$

Since for $q \ge 3$ we have

$$\sum_{j=1}^{3} jN_q(j) = q + (q^2 - q) + (q^3 - q) < \frac{q^4 - q^2}{2} = 2N_q(4),$$

it suffices to prove that if $j \ge 5$, then

$$(j-1)N_q(j-1) < (j-2)N_q(j) - (j-3)N_q(j-1).$$

The last inequality is equivalent to

$$2N_q(j-1) < N_q(j),$$

and the result follows from Proposition A1. $\square$

PROOF OF LEMMA A1. Let $h(\alpha) = \prod_{i=1}^{l} p_i^{d_i}(\alpha)$ be a polynomial of degree n over $\mathbf{F}_q$ with its prime factorization. We have to prove that $l < n/(\log_q n - 3)$. Let $n = \sum_{j=1}^{k-1} jN_q(j) + km$, where $0 \le m < N_q(k)$. Increasing l, if necessary, we may assume that $\deg p_i(\alpha) \le k$ and $d_i = 1$, $i = 1, 2, \ldots, l$; and that each irreducible polynomial of degree less than k divides $h(\alpha)$. Thus m is the number of irreducible factors of $h(\alpha)$ of degree k and $l = \sum_{j=1}^{k-1} N_q(j) + m$.

By Proposition A2, we have

$$l = \sum_{j=1}^{k-1} N_q(j) + m < \frac{\sum_{j=1}^{k-1} jN_q(j) + km}{k-2} = \frac{n}{k-2}.$$

The proof of Lemma A1 will be completed if we show that $k + > \log_q n$, or, equivalently, if we show that $n < q^{k+1}$. Since $n = \sum_{j=1}^{k-1} jN_q(j) + km \le \sum_{j=1}^{k} jN_q(j)$, the desired inequality follows from the estimation below.

$$\sum_{j=1}^{k} jN_q(j) < \sum_{j=1}^{k} q^j = \frac{q^{k+1} - q}{q-1} < q^{k+1}. \qquad \square$$

Appendix B. An Optimal Algorithm for Polynomial Multiplication

In this appendix we show that for $n \le q + 1$ we have $M_q(n) \le 3n + 1 - \lfloor q/2 \rfloor$. In order to present the above bound uniformly we assume that $n \le 2$ for $q = 2$. The inequality of $M_2(3) \le 9$ follows from recursive application of the algorithm for computing the product of two linear polynomials in three multiplications, which is similar to the method of Karatsuba and Ofman, cf. [1, p. 62].

Let $\mathbf{x}(\alpha) = \sum_{i=0}^{n} x_i \alpha^i$ and $\mathbf{y}(\alpha) = \sum_{i=0}^{n} y_i \alpha^i$. Similarly to [18] computing the coefficients of the product in $\mathbf{x}(\alpha)\mathbf{y}(\alpha)$ in $3n + 1 - \lfloor q/2 \rfloor$ multiplications can be done by computing $\mathbf{x}(\alpha)\mathbf{y}(\alpha)$ modulo linear and quadratic polynomials as follows. Let $u_1(\alpha), u_2(\alpha), \ldots, u_q(\alpha)$ be all the linear monic polynomials over $\mathbf{F}_q$, and let $u_{q+1}(\alpha), u_{q+2}(\alpha), \ldots, u_{\lceil (2n+q)/2 \rceil}(\alpha)$ be $\lceil (2n - q)/2 \rceil$ quadratic monic irreducible polynomials over $\mathbf{F}_q$. Such polynomials exist, because the number of quadratic monic irreducible polynomials over $\mathbf{F}_q$ is equal to $(q^2 - q)/2$, cf. [13, Theorem 3.25, p. 93], and for $n \le q + 1$, $q \ge 3$ we have

$$\frac{q^2 - q}{2} > \frac{2(q+1) - q}{2} \ge \frac{2n - q}{2}.$$

We distinguish between the cases of odd and even q. If q is odd, then

$$\sum_{i=1}^{\lceil (2n+q)/2 \rceil} \deg u_i(\alpha) = q + 2\left\lceil \frac{2n-q}{2} \right\rceil = q + 2\,\frac{2n - q + 1}{2} = 2n + 1.$$

This allows to compute the coefficients of the product $\mathbf{x}(\alpha)\mathbf{y}(\alpha)$ as follows.

For $i = 1, 2, \ldots, \lceil (2n + q)/2 \rceil$ compute $\mathbf{z}_i(\alpha) \equiv \mathbf{x}(\alpha)\mathbf{y}(\alpha) \bmod u_i(\alpha)$ and reconstruct $\mathbf{x}(\alpha)\mathbf{y}(\alpha)$ from the residues $\{\mathbf{z}_i(\alpha)\}_{i=1,2,\ldots,\lceil (2n+q)/2 \rceil}$ by means of Chinese Remainder Theorem. Since reducing $\mathbf{x}(\alpha)$ and $\mathbf{y}(\alpha)$ modulo a fixed polynomial and reconstructing the product requires no nonscalar multiplications, the above computation can be performed in

$$q + 3\,\frac{2n - q + 1}{2} = 2n + 1 - \left\lfloor \frac{q}{2} \right\rfloor$$

multiplications: computing the product of zero degree polynomials can be performed in one multiplication, and computing the product of linear polynomials

can be performed in three multiplications over any field. Notice that $\deg \mathbf{z}_i(\alpha) = 0$, if $i \le q$, and $\deg \mathbf{z}_i(\alpha) = 1$, otherwise.

If q is even, then

$$\sum_{i=1}^{\lceil (2n+q)/2 \rceil} \deg u_i(\alpha) = q + 2\,\frac{2n-q}{2} = 2n.$$

This allows to compute the coefficients of the product of $\mathbf{x}(\alpha)\mathbf{y}(\alpha)$ as follows.

For $i = 1, 2, \ldots, (2n-q)/2$ compute $\mathbf{z}_i(\alpha) \equiv \mathbf{x}(\alpha)\mathbf{y}(\alpha) \bmod u_i(\alpha)$. Then, by means of Chinese Remainder Theorem, compute from the residues

$$\{\mathbf{z}_i(\alpha)\}_{i=1,2,\ldots,(2n-q)/2}$$

the polynomial $\bar{\mathbf{z}}(\alpha)$ such that $\bar{\mathbf{z}}(\alpha) \equiv \mathbf{x}(\alpha)\mathbf{y}(\alpha) \bmod \prod_{i=1}^{(2n+q)/2} u_i(\alpha)$. Similarly to the case of an odd q one can show that the above computation can be performed in $3n - \lfloor q/2 \rfloor$ multiplications. Notice that the polynomial $\prod_{j=1}^{(2n+q)/2} u_j(\alpha)$ has no multiple roots. Finally, compute $\mathbf{x}(\alpha)\mathbf{y}(\alpha)$ by

$$\mathbf{x}(\alpha)\mathbf{y}(\alpha) = \bar{\mathbf{z}}(\alpha) + x_n y_n \prod_{j=1}^{(2n+q)/2} u_j(\alpha).$$

This computation requires one more multiplication. Thus the total number of multiplications involved is equal to $3n + 1 - \lfloor q/2 \rfloor$. Since for any root a of $\prod_{j=1}^{(2n+q)/2} u_j(\alpha)$ we have $\mathbf{x}(a)\mathbf{y}(a) = \bar{\mathbf{z}}(a)$, the validity of the above computation follows from [18, eq. 11]. This completes the proof of the $3n + 1 - \lfloor q/2 \rfloor$ upper bound on $M_q(n)$. □

NOTE ADDED IN PROOF. Recently Joos Heintz informed us that a slightly worse bound

$$M_q(n) \ge 3n - \log_q n - \frac{n}{\log_q \log_q n}$$

has been established by Walter Baur in 1985 by a different method. This result has never been published.

REFERENCES

Note: References [7] and [8] are not cited in text.

1. AHO, A. A., HOPCROFT, J. E., AND ULLMAN, J. D. *The Design and Analysis of Computer Algorithms*. Addison-Wesley, Reading, Mass., 1974.
2. BROCKETT, R. W., AND DOBKIN, D. On the optimal evaluation of a set of bilinear forms. *Linear Alg. Applic. 19* (1978), 207–235.
3. BROWN, M. R., AND DOBKIN, D. P. An improved lower bound on polynomial multiplication. *IEEE Trans. Comput. 29* (1980), 337–340.
4. FEDUCCIA, C. M., AND ZALCSTEIN, Y. Algebras having linear multiplicative complexity. *J. ACM 24* (1977), 311–331.
5. HOPCROFT, J., AND MUNSINSKI, J. Duality applied to the complexity of matrix multiplication. *SIAM J. Comput. 2* (1973), 159–173.
6. JACOBSON, N. *Basic Algebra I*. Freeman and Co., New York, 1985.
7. JA' JA', J. Optimal evaluation of pairs of bilinear forms. *SIAM J. Comput. 8* (1979), 443–462.
8. JA' JA', J. Computation of bilinear forms over finite fields. *J. ACM 27* (1980), 822–830.
9. KAMINSKI, M. A lower bound for polynomial multiplication. *Theoret. Comput. Sci. 40* (1985), 319–322.
10. KAMINSKI, M., AND BSHOUTY, N. H. Multiplicative complexity of polynomial multiplication over finite fields. In *Proceedings of 28th Annual IEEE Symposium on Foundations of Computer Science*. IEEE, New York, 1987, pp. 138–140.

11. LEMPEL, A., SEROUSSI, G., AND WINOGRAD, S. On the complexity of multiplication in finite fields. *Theoret. Comput. Sci. 22* (1983), 285–296.
12. LEMPEL, A., AND WINOGRAD, S. A new approach to error-correcting codes. *IEEE Trans. Inf. Theory 23* (1977), 503–508.
13. LIDL, R., AND NIEDERREITER, H. Finite fields. In *Encyclopedia of Mathematics and Its Applications*, Vol. 20, G.-C. Rota, Ed. Addison-Wesley, Reading, Mass., 1983.
14. PETERSON, W. W., AND WELDON, E. J. *Error-Correcting Codes.* MIT Press, Cambridge, Mass., 1972.
15. SCHÖNHAGE, A. Schnelle Multiplikation von Polynomen über Körpern der Charakteristik 2. *Acta Inf. 7* (1977), 395–398.
16. STRASSEN, V. Vermeidung von Divisionen. *J. Reine Angew. Math. 264* (1973), 184–202.
17. WINOGRAD, S. On the number of multiplications necessary to compute certain functions. *Commun. Pure and Appl. Math. 23* (1970), 165–179.
18. WINOGRAD, S. Some bilinear forms whose multiplicative complexity depends on the field constants. *Math. Syst. Theory 10* (1976/77), 169–180.

RECEIVED JUNE 1987; REVISED JANUARY 1988; ACCEPTED APRIL 1988