POLYNOMIALS WITH 0-1 COEFFICIENTS

THAT ARE HARD TO EVALUATE

Richard J. Lipton†

Department of Computer Science
Yale University
New Haven, Connecticut 06520

ABSTRACT: We show the existence of polynomials with 0-1 coefficients that are hard to evaluate even when arbitrary preconditioning is allowed. Further we show that there are power series with 0-1 coefficients such that their initial segments are hard to evaluate.

† This represents work performed while visiting IBM Thomas J. Watson Research Center, Yorktown Heights, New York 10598. Also supported in part by the National Science Foundation under contract DCR74-12870.

1. *Introduction*

The well known results of Belaga, Motzin, and Winograd [1,4,7] demonstrate that a polynomial of degree n requires n/2 multiplications (divisions) and n additions (subtractions) when the coefficients of the polynomial are algebraically independent. The model of computation they employ allows the use of arbitrary additional complex numbers at no cost. The selection of these numbers - called "preconditioning" - can depend in any way whatever on the original polynomial. In contrast to these results, as pointed out by Paterson-Stockmeyer [5] and Strassen [6], most polynomials that one wishes to evaluate have rational coefficients, not algebraically independent ones. The known results on rational polynomial evaluation are as follows:

1. Paterson-Stockmeyer have shown that there are rational polynomials that require $\sim\sqrt{n}$ nonscalar multiplications (divisions) when complex preconditioning is allowed. When only integer preconditioning is allowed and no division they show that there are 0-1 polynomials (polynomials with 0,1 as coefficients) that require $\sim\sqrt{n}$ nonscalar multiplications. (We use $\sim f(n)$ to mean a function $g(n)$ such that $c_1 f(n) \leq g(n) \leq c_2 f(n)$ for some $c_1, c_2 > 0$.)
2. Strassen has shown that specific rational polynomials require $\sim n$ total operations when complex preconditioning is allowed.
3. Lipton-Dobkin [3] have shown that there are 0-1 polynomials that require $\sim n/\log n$ operations when finite preconditioning is allowed (that is, all scalars used must lie in some fixed finite set).

In summary, Strassen has shown that a specific polynomial is hard to

evaluate when complex preconditioning is allowed. For weaker models (integer or finite preconditioning) Paterson-Stockmeyer and Lipton-Dobkin have shown the existence of hard 0-1 polynomials.

As Strassen states [6], an interesting open question is the construction of hard 0-1 polynomials when complex preconditioning is allowed. In this direction it is interesting to note that the coefficients of Strassen's grow at double exponential rate, so they grow very fast indeed. Essentially Strassen's results are based on the fact that while his coefficients are algebraically dependent they do not satisfy any relation with "small" degree or height. Clearly this method cannot be directly applied to any 0-1 polynomial: The coefficients of a 0-1 polynomial satisfy a great number of very simple relations.

The main results of this paper are a step in the direction of answering Strassen's open question. We restrict ourselves to proving the existence of hard 0-1 polynomials. Our main results are Theorems 5 and 7. Theorem 5 shows that there are 0-1 polynomials that require $\sim n^{1/4}/\log n$ nonscalar multiplications/divisions when arbitrary complex preconditioning is allowed. Theorem 7 addresses a related question:

Can one find a 0-1 power series $\sum_{i=0}^{\infty} a_i x^i$ such that each initial segment $\sum_{i=0}^{n} a_i x^i$ is a hard 0-1 polynomial?

The motivation for this question is twofold. First, many interesting polynomials that arise naturally are the initial segments of some power series. Second, could it be that there are hard 0-1 polynomials of every

degree while all power series are easy? Theorems 7, 8, 9 show that this cannot be so. More exactly they show that:

1. There is a 0-1 power series whose initial segments require $\sim n^{1/4}/\log n$ nonscalar multiplications/divisions when arbitrary complex preconditioning is allowed.
2. There is a 0-1 power series whose initial segments require $\sim n^{1/2}$ nonscalar multiplications when integer preconditioning is allowed.
3. There is a 0-1 power series whose initial segments require $\sim n/\log n$ total operations when finite preconditioning is allowed.

It is interesting to note that these results on power series suggest a number of questions about the interplay between polynomial evaluation and language theory. These are discussed further in Section 3.

2. *Hard 0-1 Polynomials*

Our model of computation is the standard one based on "straightline programs." Suppose that $p(x)$ is a polynomial with complex coefficients. Then $S_1,\ldots,S_m$ is a computation of $p(x)$ over A where $A \subseteq \mathbb{C}$ ($\mathbb{C}$ = the set of complex numbers) provided for each step S_i either

1. $S_i \in A \cup \{x\}$ or
2. $S_i = S_j \circ S_k$ where $j,k<i$ and $\circ \in \{+,-,\times,\div\}$. And
3. $S_m = p(x)$.

The set A determines what type of preconditioning is allowed. The measure of complexity used is either the total number of operations or the operations of some specific type. A step $S_i = S_j \circ S_k$ is a *nonscalar * operation*

provided $\circ$ is $\times$ and both S_j and S_k are not in A, or $\circ$ is $\div$ and S_k is not in A.

The proof of the existence of hard 0-1 polynomials is essentially two steps.

1. First, we show that "small" polynomials α 0-1 polynomials. That is, the evaluation of polynomials with small coefficients (in a sense to be made precise) can be reduced to the evaluation of not too many (in a sense to be made precise) 0-1 polynomials. Thus α acts here as an analogy to reducibility in the sense of automata theory.
2. Second, we show that there are hard small polynomials.

Of course, Theorem 5 is then a consequence of (1) and (2).

The details of these two steps are now presented.

Definition: Say $(a_1,\ldots,a_n)$ is a *generalized 0-1 vector* provided for some x all a_i lie in $\{0,x\}$.

Definition: Suppose that $a = (a_1,\ldots,a_n)$ is a vector of natural numbers. Then define *d(a)* to be

$$\min \{k \mid \exists v^1,\ldots,v^k \text{ generalized 0-1 vectors with } v^1+\ldots+v^k \dagger = a\}$$

Lemma 1: The function d(a) satisfies the following:

1. $d(a_1,\ldots,a_n) = d(b_1,\ldots,b_n)$ if $a_1,\ldots,a_n$ is a permutation of $b_1,\ldots,b_n$.
2. $d(a_1,\ldots,a_n) \leq d(b_1,\ldots,b_m)$ if $\{a_1,\ldots,a_n\} \subseteq \{b_1,\ldots,b_m\}$.
3. $d(a_1+b_1,\ldots,a_n+b_n) \leq d(a_1,\ldots,a_n) + d(b_1,\ldots,b_n)$.

---

† We use componentwise addition.

4. $d(a_1,\ldots,a_n) \le d(1,2,3,\ldots,t)$ where $t = \max(a_1,\ldots,a_n)$.

5. $d(a_1,\ldots,a_n) \le \log^{\dagger} n+2$ provided $a_1,\ldots,a_n$ is an arithmetic progression.

6. $d(a_1,\ldots,a_n) \le \log t+2$ where $t = \max(a_1,\ldots,a_n)$.

Proof:

1. If π is a permutation of $\{1,\ldots,n\}$, then define $\pi(a_1,\ldots,a_n) = (a_{\pi(1)},\ldots,a_{\pi(n)})$. Now let us assume that $\pi(a_1,\ldots,a_n) = (b_1,\ldots,b_n)$ and also that $V^1+\ldots+V^k = (a_1,\ldots,a_n)$ for some generalized 0-1 vectors. Then since π is additive,

$$\pi(V^1)+\ldots+\pi(V^k) = \pi(a_1,\ldots,a_n) = (b_1,\ldots,b_n).$$

Therefore, it follows that $d(a_1,\ldots,a_n) \ge d(b_1,\ldots,b_n)$; the same argument with $(a_1,\ldots,a_n)$ and $(b_1,\ldots,b_n)$ interchanged shows that $d(a_1,\ldots,a_n) \le d(b_1,\ldots,b_n)$. Thus, $d(a_1,\ldots,a_n) = d(b_1,\ldots,b_n)$.

2. We need only prove that

$$d(a_1,\ldots,a_n) \le d(a_1,\ldots,a_n,b)$$

in order to prove (2): it follows by (1) and induction on n-m. Therefore, suppose that $V^1+\ldots+V^k = d(a_1,\ldots,a_n,b)$ for some generalized 0-1 vectors. Then clearly

$$W^1+\ldots+W^k = (a_1,\ldots,a_n)$$

where W^i is the projection of V^i into the first n coordinates. Hence, $d(a_1,\ldots,a_n) \le d(a_1,\ldots,a_n,b)$.

3. Suppose that $(a_1,\ldots,a_n) = V^1+\ldots+V^k$ and $(b_1,\ldots,b_n) = W^1+\ldots+W^m$. Then

$$(a_1+b_1,\ldots,a_n+b_n) = V^1+\ldots+V^k + W^1+\ldots+W^m;$$

---

† All logarithms are to base 2.

hence, $d(a_1,+b_1,\ldots,a_n+b_n) \le d(a_1,\ldots,a_n) + d(b_1,\ldots,b_n)$.

4. Clearly $\{a_1,\ldots,a_n\} \subseteq \{1,\ldots,t\}$ where $t = \max(a_1,\ldots,a_n$; hence, $d(a_1,\ldots,a_n) \le d(1,\ldots,t)$ by (2).

5. Define $f(n)$ to be the maximum value of $d(a_1,\ldots,a_n)$ provided $a_1,\ldots,a_n$ is an arithmetic progression. We first assume that n is a power of 2. Let $a_i = bi + c$ for $i=1,\ldots,n$. Then by (1),

$$d(a_1,\ldots,a_n) \le d(a_1,a_3,\ldots,a_{2m-1},a_2,a_4,\ldots,a_{2m})$$

where $n = 2m$. Moreover, by (3),

$$d(a_1,\ldots,a_n) \le d(a_1,a_3,\ldots,a_{2m-1},a_1,a_3,\ldots,a_{2m-1}) + d(\underbrace{0,0,\ldots,0}_{m \text{ copies}},\underbrace{c,c,\ldots,c}_{m \text{ copies}})$$

since $a_1+c = a_2,\ldots,a_{2m-1}+c = a_{2m}$. By (2),

$$d(a_1,a_3,\ldots,a_{2m-1},a_1,a_3,\ldots,a_{2m-1}) = d(a_1,a_3,\ldots,a_{2m-1}).$$

Therefore, $d(a_1,\ldots,a_n) \le d(a_1,a_3,\ldots,a_{2m-1}) + 1$. Clearly $a_1,a_3,\ldots,a_{2m-1}$ is an arithmetic progression of length $n/2$; hence,

$$f(n) \le f\left(\frac{n}{2}\right) + 1.$$

Since $f(1) = 1$, it follows that $f(n) \le \log n+1$ provided n is a power of 2. Next suppose that n is not a power of 2. Now $f(k)$ is clearly a nondecreasing function of k: this follows by (2) and the fact that any arithmetic progression of length k can be extended to one of length k+1. Thus $f(n) \le f(n')$ where n' is the least power of $2 \ge n$; hence, $f(n) \le f(2n) \le \log n+2$.

6. Clearly (6) is an immediate consequence of (4) and (5). □

Let $C_{01}(n)$ be the number of nonscalar * operations required to

evaluate any 0-1 polynomial of degree $\leq n$ over C.

Lemma 2: For any natural numbers $a_o,\ldots,a_n$ it follows that $C_{01}(n) \cdot d(a_o,\ldots,a_n)$ is an upper bound on the number of nonscalar * operations needed to evaluate the polynomial

$$p(n) = \sum_{i=0}^{n} a_i x^i$$

over C.

Proof: Let $d(a_o,\ldots,a_n) = m$. Then there are generalized 0-1 vectors $V^1,\ldots,V^m$ such that $V^1+\ldots+V^m = (a_o,\ldots,a_n)$. Let

$$P_i(x) = \sum_{j=0}^{n} V_j^i x^j$$

where V_j^i = the j*th* component of the vector V^i. Then

$$\sum_{i=1}^{m} P_i(x) = \sum_{i=1}^{m} \sum_{j=0}^{n} V_j^i x^j$$

$$= \sum_{j=0}^{n} x^j \sum_{i=1}^{m} V_j^i$$

$$= \sum_{j=0}^{n} x^j a_j.$$

Therefore, $p(x) = \sum_{i=1}^{m} P_i(x)$. The number of nonscalar * operations sufficient to evaluate $p(x)$ is thus bounded by the total number of nonscalar * operations required to evaluate all the $P_i(x)$ polynomials. Each $P_i(x)$ is equal to $bq(x)$ for some scalar b and some 0-1 polynomial $q(x)$ of degree $\leq n$; hence, each $P_i(x)$ can be evaluated in $C_{01}(n)$ nonscalar * operations.

Finally, the upper bound on the number of nonscalar * operations for $p(x)$ is

$$C_{01}(n) \cdot d(a_o,\ldots,a_n). \qquad \square$$

Lemma 3: There is a nontrivial polynomial $H(a_1,\ldots,a_n)$ of degree $\leq n^{18}$ (for $n > n_0$ where n_0 is some constant) such that if $H(a_1,\ldots,a_n) \neq 0$, then

$$\sum_{i=1}^{n} a_i x^i$$

requires at least $n^{1/4}$ nonscalar * operations when arbitrary preconditioning is allowed.

Proof: Following Paterson-Stockmeyer [5], we first observe that if $p(x)$ can be computed with $\leq n^{1/4}$ nonscalar * operations, then $p(x)$ can be computed by the scheme P for some m_{ij}, m'_{ij} in $\mathbb{C}$:

P: $P_{-1} = 1.$

$P_0 = x.$

For $r-1,\ldots,\lfloor 2n^{1/4} \rfloor$

$$P_r = \left(\sum_{i=-1}^{r-1} m_{r,i} P_i\right) o_r \left(\sum_{i=-1}^{r-1} m'_{r,i} P_i\right)$$

where o_r is $\times$ if r is odd and $\div$ if r is even. Finally,

$$p(x) = \sum_{i=-1}^{\lfloor 2n^{1/4} \rfloor} m_{0,i} P_i.$$

The total number of operations - scalar and nonscalar - is

$$3 + \sum_{r=1}^{\lfloor 2n^{1/4} \rfloor} (4r+5) \leq 4n^{1/2}$$

for $n > n_0$ where n_0 is some constant.

We now proceed to apply the method of Strassen's Theorem 2.5 to the scheme P with the parameters m_{ij}, m'_{ij} considered as indeterminates. Viewed this way, P computes (by Strassen's Lemma 2.4)

$$q(\bar{m}) + \sum_{i=1}^{\infty} q_i(\bar{m}) x^i$$

for some polynomials[†] q_i where $\bar{m}$ is the vector of all the parameters m_{ij}, m'_{ij}. In the notation of Strassen

$$g = n^{18}$$

$$q = n$$

$$m \leq 4n^{1/2}$$

$$s \leq 4n^{1/2}$$

$$d = n.$$

For $n > n_1$ where n_1 is some constant,

$$g^{q-m-2} = n^{18(n-4\sqrt{n}-2)}$$

$$> n^{4\sqrt{n}(4\sqrt{n}+1)} n^n$$

$$= d^{s(m+1)} q^q$$

Now let $H(a_1,\ldots,a_n)$ be the nontrivial polynomial of degree $\leq g$ that exists by Strassen's theorem.[††] Now suppose that $a_1,\ldots,a_n$ are natural numbers such that $H(a_1,\ldots,a_n) \neq 0$ and yet

---

[†] $q(\bar{m})$ need not be a polynomial, but are rational.

[††] The field k of Strassen's theorem is the complex numbers extended by the indeterminates m_{ij} and m'_{ij}.

$$p(x) = \sum_{i=1}^{n} a_i x^i$$

can be done in $< n^{1/4}$ nonscalar * operations; we will reach a contradiction. For some complex parameters $\bar{t}$ the scheme P computes $p(x)$; hence,

$$p(x) = \sum_{i=1}^{n} q_i(\bar{t}) x^i + q(\bar{t}).$$

Thus $H(a_1,\ldots,a_n) = H(q_1(\bar{t}),\ldots,q_n(\bar{t}))$. But

$$H(q_1(\bar{t}),\ldots,q_n(\bar{t})) = 0$$

by the method of Strassen's theorem; hence, $H(a_1,\ldots,a_n) = 0$. This is a contradiction. □

Lemma 4: Suppose that $q(x_1,\ldots,x_k)$ is a polynomial of degree $\leq g$ such that $q(x_1,\ldots,x_k) = 0$ for all natural numbers $0 \leq x_i \leq g$. Then $q(x_1,\ldots,x_k)$ is identically 0.

Proof: We will use induction on k. When k=1 the result is an immediate consequence of the fact that a polynomial of degree $\leq g$ can have at most g zeroes without being identically 0. Now suppose that k>1. Then

$$q(x_1,\ldots,x_k) = \sum_{i=0}^{g} P_i(x_2,\ldots,x_k) x_1^i$$

for some polynomials $P_0,\ldots,P_g$ of degree $\leq g$. Assume that $q(x_1,\ldots,x_k)$ is not identically 0. Then there is a $P_d(x_2,\ldots,x_k)$ that is not identically 0. Then

$$\exists 0\leq x_2\leq g \ \ldots \ \exists 0\leq x_k\leq g \text{ with } P_d(x_2,\ldots,x_k) \neq 0;$$

for otherwise by induction $P_d(x_2,\ldots,x_k)$ is identically 0. Let $x_2',\ldots,x_k'$ be such natural numbers. Then $q(x,x_2',\ldots,x_k')$ is a polynomial in x of degree

$\leq g$ with $g+1$ zeroes; hence $q(x,x_2',\ldots,x_k')$ is identically 0. This contradicts the fact that $P_d(x_2',\ldots,x_k') \neq 0$. □

We are finally ready to prove our main result.

Theorem 5: There are 0-1 polynomials that require $\sim n^{1/4}/\log n$ nonscalar * operations when arbitrary preconditioning is allowed.

Proof: Let $H(a_1,\ldots,a_n)$ be as in Lemma 3. Let $g = n^{18}$, the degree of H. Then by Lemma 4 there is a $(a_1,\ldots,a_n)$ such that $H(a_1,\ldots,a_n) \neq 0$ and $0 \leq a_i \leq g$ for $i=1,\ldots,n$. By Lemma 3, with $a_0 = 0$

$$\sum_{i=0}^{n} a_i x^i$$

requires $n^{1/4}$ nonscalar * operations. By Lemma 2,

$$C_{01}(n) \cdot d(a_0,\ldots,a_n) \geq n^{1/4}.$$

Therefore, by Lemma 1 part (6),

$$C_{01}(n) \geq n^{1/4}(18 \log n+2).$$ □

3. *Hard 0-1 Power Series*

In this section we study the complexity of the initial segments to power series whose coefficients are 0-1.

Definition: Let $D_A(\alpha)$ be the number of nonscalar * operations required to evaluate

$$p(x) = \alpha_0+\ldots+\alpha_k x^k$$

over A where α is a 0-1 string of length k+1. Also we will say that p(x) is the polynomial that *corresponds* to α.

Lemma 6: For any 0-1 strings α and β,[†]

$$D_A(\alpha\beta) + D_A(\alpha) + 2 \log |\alpha| + 1 \geq D_A(\beta).$$

Proof: Let $q(x) = \sum_{i=0}^{|\alpha|-1} \alpha_i x^i$ and $r(x) = \sum_{i=0}^{|\beta|-1} \beta_i x^i$. Then $p(x) = q(x) + x^{|\alpha|} r(x)$ is the polynomial that corresponds to $\alpha\beta$. Now in order to evaluate r(x), the polynomial that corresponds to β, proceed as follows:

1. Compute p(x).
2. Compute q(x).
3. Form g(x) = p(x) - q(x).
4. Compute $x^{|\alpha|}$.
5. Form $h(x) = g(x)/x^{|\alpha|}$.

The above computation clearly takes at most

$$D_A(\alpha\beta) + D_A(\alpha) + 2 \log |\alpha| + 2$$

nonscalar * operations. Now $g(x) = x^{|\alpha|} r(x)$, and so h(x) = r(x). □

Suppose that $\sum_{i=0}^{\infty} a_i x^i$ is a power series. Then the polynomials

$$\sum_{i=0}^{n} a_i x^i$$

are the initial segments of the given power series. The next theorem

---

[†] $|\alpha|$ = length of α and $\alpha\beta$ is the concatenation of α and β.

shows that there are power series with 0-1 coefficients such that their initial segments are hard infinitely often.

Theorem 7: There is a 0-1 power series whose initial segments of length n infinitely often require $\sim n^{1/4}/\log n$ nonscalar * operations when arbitrary complex preconditioning is allowed.

Proof: Let $p_k(X)$ be a 0-1 polynomial of degree 2^k that requires

$$\frac{\varepsilon\ 2^{k/4}}{k}$$

nonscalar * operations where $\varepsilon > 0$; it exists of course by Theorem 5. Then let α^k be the 0-1 string of the coefficients of $p_k(x)$. Also let

$$\alpha = \alpha^1\alpha^2\ldots$$

be the infinite 0-1 string formed by concatenating together all the α^i's. By Lemma 6 for all k,

$$D_A(\alpha^1\ldots\alpha^k) + D_A(\alpha^1\ldots\alpha^{k-1}) + 2\log|\alpha^1\ldots\alpha^{k-1}| + 2 \geq D_A(\alpha^k).$$

by the definition of α^k, $D_A(\alpha^k) \geq \frac{\varepsilon\ 2^{k/4}}{k}$. Thus,

$$D_A(\alpha^1\ldots\alpha^{k-1}) + D_A(\alpha^1\ldots\alpha^k) \geq \frac{\varepsilon'\ 2^{k/4}}{k}$$

for large k and some $\varepsilon' > 0$ since $|\alpha^1\ldots\alpha^{k-1}| \leq 2^{k+1}$. Thus either $D_A(\alpha^1\ldots\alpha^k)$ or $D_A(\alpha^1\ldots\alpha^{k-1})$ exceeds

$$m = \frac{\varepsilon'\ 2^{k/4}}{2k}.$$

In either case we have shown that there is an initial segment of length between 2^{k-1} and 2^{k+2} which requires $\geq m$ nonscalar * operations. Since

k was arbitrary the theorem is proved. □

The same type of reasoning also yields:

Theorem 8: There is a 0-1 power series whose initial segments of length n infinitely often require $\sim n^{1/2}$ nonscalar * operations when only integer preconditioning is allowed.

Theorem 9: There is a 0-1 power series whose initial segments of length n infinitely often require ~ n/log n total operations when finite preconditioning is allowed.

It is interesting to note in passing a connection between these results and language theory. Let α be the 0-1 infinite sequence that is constructed in Theorem 7. Also let

$$L = \{\alpha_0, \ldots, \alpha_i \mid i \geq 0\}.^{\dagger}$$

By construction L is recursive. (Actually one must choose αi to be lexicographically smallest 0-1 string of length 2^k such that the corresponding polynomial requires the specified number of operations.) The exact complexity of L is of some interest since it hopefully would help one understand what makes a 0-1 polynomial hard. In this direction we have

Theorem 10: L cannot be context-free (Book-Lipton [2]).

Proof: Suppose that L was context free. Then a "pumping lemma" argument

---

† α_i is the *ith* symbol in α.

shows that for some strings a and b with b nonempty,

$$ab^i \in L \text{ for all } i \geq 0.$$

Now select any $x \in L$ with $|x| \geq |a|$. Then x must be the prefix of ab^i for some i: this follows since there is exactly one string of each length in L.

Thus α is an ultimately periodic string. We will now show that the polynomial that corresponds to any initial segment is easy to evaluate. In order to prove this it is sufficient to show that for any string β the polynomial that corresponds to β^n (β concatenated n times) is easy to evaluate. Now this polynomial is equal to

$$\sum_{m=0}^{n} \sum_{i=0}^{k-1} \beta_i x^{km+i}$$

which is in turn equal to

$$\left(\sum_{m=0}^{n} x^{km} \right) \left(\sum_{i=0}^{k-1} {}_i x^i \right) .$$

This polynomial can be evaluated in log n + 0(k) total steps; hence, L cannot be context free. □

Acknowledgements:

The author wishes to thank Larry Stcomeyer for a number of helpful suggestions, and the referees for their helpful comments.

References

[1] E. G. Belaga.
Some problems involved in the computation of polynomials.
Dokl. Akad. Nauk 123:775-777, 1958.

[2] R. V. Book and R. J. Lipton.
Unpublished manuscript.

[3] R. J. Lipton and D. P. Dobkin.
Complexity measures and hierarchies for the evaluation of integers, polynomials, and N-linear forms.
In the proceedings of the Seventh Annual ACM Symposium on Theory of Computing, 1975.

[4] T. S. Motzkin.
Evaluation of polynomials and evaluation of rational functions.
Bull. Amer. Math. Soc. 61:163, 1955.

[5] M. Paterson and L. Stockmeyer.
On the number of nonscalar multiplications necessary to evaluate polynomials.
SIAM J. Computing 2:60-66, 1973.

[6] V. Strassen.
Polynomials with rational coefficients which are hard to compute.
SIAM J. Computing 3:128-148, 1974.

[7] S. Winograd.
On the number of multiplications necessary to compute certain functions.
Comm. Pure Appl. Math. 23:165-179, 1970.