ON THE NUMBER OF ADDITIONS TO COMPUTE SPECIFIC POLYNOMIALS

Preliminary Version

Allan Borodin and Stephen Cook
Department of Computer Science
University of Toronto

I Introduction

It is well known from the work of Motzkin [55], Belaga [58] and Pan [66], that "most" n^{th} degree polynomials $p \in R[x]$ require about $n/2$ $\times, \div$ ops and n $\pm$ ops and that these bounds can always be achieved within the framework of preconditioned evaluation(1). More precisely, if p can be computed using less than $\left\lceil\frac{n+1}{2}\right\rceil$ $\times, \div$ or less than n $\pm$ ops, then the coefficients of p are algebraically dependent.

However, it can be argued that only polynomials in $Q[x]$ are of any computational concern. Moreover, one would like "practical tests" to determine the complexity of a specific polynomial. With respect to non scalar * ops, Paterson and Stockmeyer [71] are able to show that approximately $\sqrt{n}$ such ops are required for "most" n^{th} degree polynomials in $Q[x]$. Also they show that every n^{th} degree polynomial can be computed in about $\sqrt{2n}$ non scalar * ops. In $Q[x]$, the scalar * ops can be simulated by (an unbounded number of) $\pm$ ops. Strassen [72] uses a careful analysis of the Motzkin-Belaga argument (and also of the corresponding development in Paterson-Stockmeyer) to exhibit specific polynomials $Z[x]$ whose required complexity is nearly that obtainable by general preconditioning methods. For example, any program for

$$p(x) = \sum_{i=0}^{n} 2^{2^{in^3}} x^i \text{ requires}$$

i) either $\frac{n}{2} - 4$ * ops and $n - 4$ $\pm$ ops or at least $n^2/\log n$ total ops.

ii) at least $\sqrt{n}$ non scalar * ops.

That is, if one chooses to tradeoff $\pm$ ops to reduce the * complexity of $p(x)$, then it can be done but only with an exorbitant cost of at least $n^2/\log n$ $\pm$ ops.

The situation when counting $\pm$ ops with the potential of unlimited * ops, is not as clear. In fact, we are not aware of any previous results which show that not all $p \in Q[x]$ are computable in (say) 4 $\pm$ ops. A "useable" characterization of precisely which polynomials are computable in 4 $\pm$ ops is more than a tedious exercise. Does an analogue of Paterson-Stockmeyer hold? That is, can the output of a program (which is computing an n^{th} degree polynomial) using k $\pm$ ops <u>but an unbounded number of * ops</u> be represented by $\sum_{i=0}^{n} q_i(\alpha_1,\ldots,\alpha_t)x^i$ for some fixed polynomials $\{q_i\}$ where the number t of parameters $\{\alpha_i\}$ is bounded by some function of k ? We shall show in section III that this is the case with $t \approx k^2$ but unlike the situation in Paterson-Stockmeyer, we do not yet know if the use of unlimited * ops can in general reduce the $\pm$ complexity of all $p \in Q[x]$.

While the arguments based on algebraic dependence provide us with our best lower bounds thus far, a different approach of independent interest is taken in section IV. Namely, we are able to show that the number of $\pm$ ops required to compute any $p \in R[x]$ is bounded below by a function of the number of distinct real zeros of p. The potential (e.g., for producing non

(1) See Knuth [69] or Revah [74] for a review. We use the following notation: R, Q, C for the field of reals, rationals, complex numbers, respectively; $F[y_1,\ldots,y_m]$ is the ring of polynomials, $F[[y_1,\ldots,y_m]]$ is the power series ring and $F(y_1,\ldots,y_m)$ the field of rational functions in $y_1,\ldots,y_m$ over F. We will also use * ops to denote either a $\times$ or $\div$ op.

linear lower bounds) and limitations of this approach will be discussed.

II The Model and a Review of Basic Results Based on Algebraic Independence

We follow informally the notation of Winograd [70] and say that we are interested in computing $p \in F[x]$ over $G(x)$ given $G \cup \{x\}$ where G is a field. That is, we think of a program P as a sequence of statements $\langle s_1, \ldots, s_m \rangle$; each s_i is of the form p_i op q_i where op $\in \{+, -, \times, \div\}$ and each operand p_i, q_i is either

i) in $G \cup \{x\}$; i.e., a scalar constant or 'x'

ii) a previously computed s_j $(j<i)$.

P computes $p \in F[x]$ if $p = s_m$ (as elements of $F[x] \subseteq G(x)$).

In III, the choice of F & G are not that essential but for definiteness we can take $F = Q$ and $G = C$. Section IV will depend essentially on the choice $G = R$.

<u>Definition 1</u>: Let H be an extension field of $F = Q$. $u_1, \ldots, u_m \in H$ are <u>algebraically dependent</u> (over Q) if $\exists$ a non trivial $f \in Z[y_1, \ldots, y_t]$ such that $f(u_1, \ldots, u_t) = 0$.

<u>Lemma 1 (see Van der Waerden [64])</u>: Let $p_1, \ldots, p_m \in Q(\alpha_1, \ldots, \alpha_t)$. If $m > t$, then $p_1, \ldots, p_m$ are alg. dep.

For the sake of completeness and motivation, let's briefly sketch the lower bound of Paterson and Stockmeyer. Assuming no $\div$, we can construct a "canonical" program using k non scalar $\times$ ops; namely:

$$s_{-1} \leftarrow 1$$

$$s_0 \leftarrow x$$

$$s_i \leftarrow \Big(\sum_{j<i} \alpha'_{j,i} s_j\Big) \times \Big(\sum_{j<i} \alpha''_{j,i} s_j\Big)$$

$$s_{k+1} \leftarrow \sum_{j\le k} \alpha_{j,k+1} s_j$$

Then $s_{k+1} = \sum_{j=0}^{r} p_j(\vec{\alpha})x^j$ where $r \le 2^k$
and $\vec{\alpha} = \langle \alpha'_{-1,1}, \alpha'_{0,1}, \alpha''_{-1,1}, \ldots, \alpha_{k,k+1} \rangle$
$= \langle \alpha_1, \ldots, \alpha_t \rangle$ where t is approximately k^2 .

<u>Theorem 1 (Paterson & Stockmeyer)</u>: If $n+1 > t$, then $\exists$ $p \in [x]$ not doable in k non scalar $\times$ ops.

<u>Proof</u>: Let $p(x) = \sum_{p=0}^{n} a_j x^j = \sum_{p=0}^{n} p_j(\vec{\alpha}) x^j$ for some choice of $\vec{\alpha}$ if p is computable in k non scalar $\times$ ops.

But $\langle p_0(\vec{\alpha}), \ldots, p_n(\vec{\alpha}) \rangle$ are alg. dep. if $n+1 > t$ and hence $\exists$ non trivial $f \in Z[y_1, \ldots, y_{n+1}]$: $f(p_0(\vec{\alpha}), \ldots, p_n(\vec{\alpha})) = 0$. If every $p \in Q[x]$ were doable in k non scalar $\times$ ops, then $f(q_0, \ldots, q_n) = 0$ for all $\langle q_0, \ldots, q_n \rangle \in Q^{n+1}$. Hence $f \equiv 0$ because Q^{n+1} is dense in R^{n+1} and f is continuous. This contradicts the assumption that f be non trivial.

As Paterson and Stockmeyer observe, if we can produce a finite number, say ℓ , of canonical programs for some measure (rather than just one) then the same type of results will follow; for the "alg. dep. of each program" is characterized by some $f_i \in Z[y_1, \ldots, y_t]$ and hence the coefficients of any n^{th} degree polynomial doable in k ops, will be a zero of $f = \prod_{i=1}^{\ell} f_i$.

From these observations, the following fact follows directly:

<u>Fact 1</u>: Let $\psi : N \to N$ be any function.

a) There are n^{th} degree polynomials in $Q[x]$ which either require $\lceil \frac{n+1}{2} \rceil$ $*$ ops or more than $\psi(n)$ $\pm$ ops.

b) There are n^{th} degree polynomials in $Q[n]$ which either require n $\pm$ ops, or more than $\psi(n)$ $*$ ops.

In either case, once $\psi(n)$ is given, there are only a finite number of canonical programs each having the appropriate number of parameters.

III A Lower Bound for $\pm$ Ops Based on Algebraic Dependence

We shall now consider the situation when the number of $*$ ops is <u>not</u> bounded by any function of the degree. One might argue that this is a totally impractical hypothesis, but we believe that the questions arising out of the developments in sections III and IV are more than academic. The difficulty in trying to bound $\pm$ ops is suggested by the simplest example. Let $s \leftarrow (x+\alpha)^u$ represent the first $\pm$ step (say $u \in N$). If we treat u as a parameter, then $s = \alpha^u + u\alpha^{u-1}x + \binom{u}{2}\alpha^{u-2}x^2 + \ldots$.

We cannot immediately view s as $\sum_{j=0} p_j(\alpha)x^j$ with the p_j being polynomials. Nor can we treat each α, α^2, α^3, ... as a parameter for then the number of parameters will not be a bounded function of ± ops. We might want to argue that u cannot be too large without introducing some inefficiency; but this is just the sort of question we cannot yet answer.

Let's consider a "canonical" k ± step program:

$$T_0 = 1$$

$$S_0 = x$$

$$\vdots$$

$$\left.\begin{aligned} T_i &= \prod_{j<i} S_j^{m_{j,i}} \\ S_i &= \gamma_i + T_i \end{aligned}\right\} 1 \le i \le k$$

$$\vdots$$

$$T_{k+1} = \gamma_{k+1} \prod_{j\le k} S_j^{m_{j,k+1}}$$ represents

the output where each $m_{j,i} \in Z$. (Allowing negative exponents accounts for ÷ and also allows a simplification in the number of parameters introduced. On the other hand, we will have to view the computation as taking place over some power series $G[[x-\theta]]$ as in Strassen [72] in order to accommodate the negative exponents.)

We want to express T_{k+1} as a polynomial in x whose coefficients are in some $H = Z(\alpha_1,\ldots,\alpha_t)$. Let's concern ourselves only with the computation of n^{th} degree polynomials. Suppose P computes p over $G[x]$. Then P correctly computes p over $G[x] \bmod (x^{n+1})$; i.e., with all higher order terms dropped throughout the computation.

The example $s \leftarrow (x+\alpha)^u$ illustrates the approach to be taken. We can consider $n+2$ cases: $u = 0, \ldots, u = n, u > n$. It is clear that for each $u = i$ $(i \le n)$ that we can represent $s \bmod (x^{n+1})$ as some $\sum_{j=0}^{n} p_j(\alpha)x^i$. For $u > n$, we have

$$s = \alpha^u + u\alpha^{u-1}x + \ldots \binom{u}{n}\alpha^{u-n}x^n$$

$$= \sum_{j=0}^{n} r_j(\alpha,\beta,u)x^j \quad \text{where } \beta = \alpha^u \text{ and}$$

$r_j \in Z(\alpha,\beta,u)$; i.e., $r_0(\alpha,\beta,u) = \beta$, $r_1(\alpha,\beta,u) = u\frac{\beta}{\alpha}$, ..., $r_n = \binom{u}{n}\frac{\beta}{\alpha^n}$. More generally, if $u \in Z$ (rather than N) we would have $2n+3$ cases: $u < -n$, $u = -n$, ..., $u = 0$, ..., $u = n$, $u > n$. Consider $u < 0$ and assume $\alpha \ne 0$. (If $\alpha = 0$, we would have to consider power series in $x - \theta$ rather than x for some appropriate θ.) Then

$$s \leftarrow 1/(\alpha+x)^{-u} = [1/(\alpha+x)]^{-u}$$

$$= [\frac{1}{\alpha} - \frac{1}{\alpha^2}x + \frac{1}{\alpha^3}x^2 - \frac{1}{\alpha^4}x^3 + \ldots]^{-u}$$

$$s \bmod (x^{n+1}) = [\frac{1}{\alpha} - \frac{1}{\alpha^2}x + \ldots (-1)^n\frac{1}{\alpha^{n+1}}x^n]^{-u}$$

$$= \sum_{j=0}^{n} r_j(\alpha,\beta,u)x^j \text{ with } \beta = \alpha^{-u}.$$

<u>Theorem 2</u>: Consider n^{th} degree polynomial p and assume that p can be computed in k ± ops (without any bound on the number of * ops). Then p can be represented as $\sum_{p=0}^{n} p_j(\alpha_1,\ldots,\alpha_t)(x-\theta)^j$ with $t \le (k+2)^2$ for some choice of $\{\alpha_i\}$ and θ.

<u>Proof</u>: To simplify the discussion we shall assume that all the exponents $\{m_{j,i}\}$ in the canonical program are non negative and hence we can take $\theta = 0$.

The proof is by induction on k, arguing by cases depending on whether or not any $m_{j,i} \le n$ or $> n$. A k ± step program introduces $v = \frac{(k+1)(k+2)}{2}$ exponents, all of which we shall treat as parameters. For every exponent there are $n+2$ cases to consider ($m_{j,i} = 0$, $m_{j,i} = 1$, ...), or $(n+2)^v$ cases in all. Each case will determine a new canonical program. For each of these (finite number of) programs, we shall characterize the statements in the desired manner.

Let's just consider the case that all exponents are $> n$ (of course, we could argue trivially that we are not computing p, but this approach shows that we are not even computing $p \bmod (x^{n+1})$ if k is too small).

<u>Induction step</u>:

Assume $S_i = \sum_{j=0}^{n} p_j^i(\alpha_1,\ldots,\alpha_{t(i)})x^j \bmod (x^{n+1})$ for $0 \le i \le r$.

Show that $S_{r+1} = \sum_{p=0}^{n} p_j^{r+1}(\alpha_1,\ldots,\alpha_{t(r+1)})x^j$ and that $t(r+1) \le t(r) + 2(r+1)$. So by induction $t = t(k+1) \le (k+2)^2$.

Introduce new parameters (and rename by $\alpha_{t(r)+1},\alpha_{t(r)+2},\ldots,\alpha_{t(r+1)}$ to represent $\gamma_{r+1},m_{0,r+1},\ldots,m_{r,r+1}$,

$[p_0^1(\alpha_1,\ldots,\alpha_{t(1)})]^{m_{1,r+1}},\ldots,$

$[p_0^r(\alpha_1,\ldots,\alpha_{t(r)})]^{m_{r,r+1}}$. We have thus introduced $2(r+1)$ parameters. Now it remains to show that $S_{r+1} = \sum p_j^{r+1}(\alpha_1, \ldots,\alpha_{t(r+1)})x^j \pmod{x^{n+1}}$

$$S_{r+1} = \prod_{j=0}^{r} S_j^{m_{j,r+1}} + \gamma_{r+1} .$$

Look at any $S_i^{m_{i,r+1}} = \left[\sum_{j=0}^{n} p_j^i(\alpha_1,\ldots,\alpha_{t(i)})x^i\right]^{m_{i,r+1}} \bmod (x^{n+1})$.

Claim: The coefficient of x^ℓ $(\ell \le n \le m_{i,r+1})$ is

$$\sum_{m_1\cdot 1+m_2\cdot 2+\ldots+m_n\cdot s=\ell} \binom{m_{i,r+1}}{m_1}\binom{m_{i,r+1}-m_1}{m_2}\cdots\binom{m_{i,r+1}-m_1-\cdots m_n}{m_n} \cdot \left[p_0^i(\alpha_1,\ldots)\right]^{m_{i,r+1}-m_1\cdots m_n} p_1^i(\ )^{m_1}\cdots p_n^i(\ )^{m_n} .$$

And as in the simple example, the expression can be written as a rational function $g(\alpha_1,\ldots,\alpha_{t(r)},m_{i,r+1},[p_0^i]^{m_{i,r+1}})$. So it follows that $\prod S_j^{m_{i,r+1}} + \gamma_{r+1} \bmod (x^{n+1})$ can be represented as desired.

Corollary 1: There exist n^{th} degree polynomials $\varepsilon\ Q[x]$ which require $\sim \sqrt{n}$ $\pm$ ops (even if we do the computation mod (x^{n+1}) ; i.e., chop off high order terms without cost).

Corollary 2: By calculating upper bounds on the degree and weight of the polynomials $\{p_j^i(\alpha_1,\ldots)\}$ we can exhibit ala Strassen [72] specific polynomials which require $\sqrt{n}$ $\pm$ ops.

At this time we do not know if such a saving (or any saving) can generally be obtained. We suspect that while it may be possible to achieve a saving when computing mod (x^{n+1}) , that the additional requirements imposed by the cancellation of high order terms will preclude any such saving. That is, $\pm$ ops in computations over $Q(x)$ cannot in general be reduced by * ops.

We state the following conjecture: There is a function $\gamma(k,n)$ satisfying the following property: If p is an n^{th} degree polynomial (say in $Q[x]$) and p is computable in k $\pm$ ops, then p is computable in k $\pm$ ops and $\le \gamma(k,n)$ * ops.

Finally, we can note that if a general saving in $\pm$ ops can be achieved for any fixed n_0 (say $\beta(n_0)$ $\pm$ ops), then a proportionate saving can be achieved for all $n \ge n_0$ (i.e., only need about $\beta(n_0)\cdot n/n_0$ $\pm$ ops).

IV A Lower Bound Based on the Number of Real Zeros

In Strassen [73], we see the first non trivial results concerning non linear lower bounds for arithmetic complexity. Algebraic geometry provides the proper notion of 'degree' for a set (rather than just one) polynomial in several variables. The geometric formulation of degree is "correct" from a complexity point of view since Strassen is able to show that the degree can at most double after a * op and is unchanged after any $\pm$ op. In this way, one can prove for example that any n^{th} degree polynomial evaluated at n arbitrary points requires $n \log n$ * ops.

For $\pm$ ops, we do not yet have an appropriate concept or property (such as degree) which can be used to derive non linear lower bounds. For example: Is polynomial multiplication non linear wrt. $\pm$ ops? Does there exist an n^{th} degree polynomial which requires $n \log n$ $\pm$ ops for computation at n arbitrary points? One type of property that may be relevant is to look at the zeros associated with the polynomials computed during a computation. If we look at all complex zeros, then we can obviously generate an n^{th} degree $p\ \varepsilon\ R[x]$ which has n distinct zeros in one $\pm$ op (of course, these zeros have a nice structure).

The approach of this section is to show that the number of distinct real zeros can not grow too fast as a function of the number of $\pm$ ops. Unfortunately, (unlike degree wrt. * ops) it is not true that if p_1 and p_2 have $\le r$ distinct real zeros, then $p_1 + p_2$ has $\le \phi(r)$ distinct real zeros (for some function $\phi: N \to N$).

We consider again the canonical program given in the last section:

$$T_0 = 1$$

$$S_0 = x$$

$$\left.\begin{array}{l} \vdots \\ T_i = \prod_{j<i} S_j^{m_{j,i}} \\ S_i = \gamma_i + T_i \\ \vdots \end{array}\right\} \begin{array}{l} 1 \le i \le k \\ m_{j,i} \in Z \\ \gamma_i \in R \end{array}$$

$$T_{k+1} = \gamma_{k+1} \prod_{j \le k} S_j^{m_{j,k+1}}$$

We want to bound the number of distinct real roots in T_n as a function of n.

To do so a more general induction hypothesis seems necessary.

<u>Theorem 3</u>: Let $p = \sum_{j=1}^{N} a_j S_0^{r_{0,j}} \ldots S_n^{r_{n,j}} \cdot Q_j(S_0,\ldots,S_m)$ with each $Q_j \in R(y_0,\ldots,y_m)$ of deg $\le M$, and $a_j \in R$ (deg. can be defined as max (deg of numerator, deg denominator)). Then p has $\le \phi(n, N, M)$ distinct real roots. The function ϕ will be defined by induction.

Note! $\phi(n, N, M)$ is independent of the exponents $r_{i,j} \in Z$.

Throughout the following, S' denotes $\frac{dS}{dx}$.

<u>Corollary 3</u>: Let $\rho(k)$ be the maximum number of distinct real roots in any polynomial computable in k $\pm$ ops. Then $\rho(k) \le \phi(k,1,0)$.

<u>Lemma 2</u>: If $f(x) \in R[x]$ has k non zero terms, then f has $\le 2k-1$ distinct real zeros.

<u>Proof</u>: Induction on k

Let $f = x^r \cdot g(x) = x^r(a_0 + \ldots)$. Note that if g has r distinct real zeros, then g' has at least $r-1$ distinct real zeros (Rolle's Theorem).

<u>Lemma 3</u>: $S'_{n+1} = T'_{n+1} = T_{n+1}\left[\sum_{i=0}^{n} m_{i,n+1} \cdot S'_i/S_i\right]$.

<u>Corollary 4</u>: $S'_{n+1} = Q(S_0,\ldots,S_{n+1})$ and deg Q can be bound by some $\psi(n)$ independent of the $\{m_{i,n+1}\}$.

<u>Proof of Theorem</u>: (double induction; main induction on n, second induction on N).

$n = 0$: $\phi(0, N, M) = 2[N(NM+M+1)] - 1$, by Lemma 2.

Assume true for n and all N, M.

Induction on N for $n+1$:

$$N = 1: \quad p = a_1 \prod_{i=0}^{n+1} S_i^{r_{i,1}} Q_1(S_0,\ldots,S_{n+1})$$
$$= a_1 S_{n+1}^{r_{n+1,1}} \prod_{i=0}^{n} S_i^{r_{i,1}} \cdot Q_1(S_0,\ldots,S_{n+1}).$$

Any zero of p is one of the following:

i) A zero of $S_{n+1}^{r_{n+1,1}}$, and hence a zero of S_{n+1}. But
$$S_{n+1} = \prod_{i=0}^{n} S_i^{m_{i,n+1}} + \gamma_{n+1}$$
and so the induction (on n with $N = 2$) can be applied.

ii) A zero of $\prod_{i=0}^{n} S_i^{r_{i,1}}$. Apply induction.

iii) A zero of $Q_1(S_0,\ldots,S_{n+1})$ and hence a zero of the numerator P_1 of Q_1. Since deg $P_1 \le M$, there are at most $(n+2)^M$ terms in P_1 and each of these terms can be expanded into the form $\sum_{j=1}^{N' \le M+1} a_j \prod_{i=0}^{n} S_i^{r_{i,j}} Q_j(S_0,\ldots,S_n)$ by making the substitution $S_{n+1} = \gamma_{n+1} + \prod_{i}^{n} S_i^{m_{i,n+1}}$. (At worst, we have to raise S_{n+1} to the M^{th} power.)

End $N = 1$.

$$N > 1: \quad p = \sum_{j=1}^{N} a_j \left(\prod_{i=0}^{n+1} S_i^{r_{i,j}}\right) \cdot Q_j(S_0,\ldots,S_{n+1}).$$

Factor out $a_1 \prod S_i^{r_{i,1}} Q_1(S_0,\ldots,S_{n+1}) = p_1$,

$$p = p_1\left(1 + \sum_{j=2}^{N} \tilde{a}_j \prod S_i^{\tilde{r}_{i,1}} \tilde{Q}_j(S_0,\ldots,S_{n+1})\right)$$
$$= p_1 p_2.$$

It suffices to show that p'_2 has a bounded number of distinct real zeros

$$p'_2 = \sum_{j=2}^{N} \tilde{a}_j S_0^{\tilde{r}_{0,j}} \ldots S_n^{\tilde{r}_{n+1,j}} \cdot \left[\left(\sum_{i=0}^{n+1} \tilde{r}_{i,j} S'_0/S_i\right) \cdot \tilde{Q}_j(S_0,\ldots,S_{n+1})\right.$$

$$+ Q_j'(S_0,\ldots,S_{n+1}) \quad .\Big]$$

Now observe

i) $\sum_{i=0}^{N} \tilde{r}_{i,j} \cdot S_0'/S_i$ has bounded deg by Lemma 2

ii) deg $\tilde{Q}_j$ is bounded

iii) $\tilde{Q}_j'(S_0,\ldots,S_{n+1}) = \sum_{i=0}^{n+1} \frac{\partial Q_j}{\partial S_i} S_i'$.

Again, by Lemma 2, $\tilde{Q}_j'(S_0,\ldots,S_{n+1})$ has bounded degree.

QED

The bound on the function $\phi(n, N, M)$ will depend on how the rational functions Q_j are represented and manipulated. To get a better bound we may want to consider $\phi(n, N, M, t)$ where t could be a bound on the number of terms in some Q_j .

Fact 2: $\rho(k) \geq 3^k$ (where $\rho(k)$ was defined in Corollary 3).

That is, the approach of section IV can at best show the existence of n^{th} degree polynomials requiring $O(\log n)$ ± ops. But this is consistent with the simple bound for * ops based on degree. Let $u(k)$ = maximum [number of distinct real roots in any polynomial computable in k * op].

Fact 3: $u(k) = 2^k$.

We conjecture that $\rho(k) \leq c^k$ (for some c) but most likely such a bound will not result from any simple modification of Theorem 3. It should also be noted that we have not yet proven any upper bound on $\rho(k)$ when complex scalars are allowed as program constants. Returning to the question of non linear lower bounds, we must also hope that appropriate bounds would hold in the context of multivariate polynomials. Here, of course, we must be careful since $p(x,y)$ can have an infinite number of zeros. Yet we can hope that an extension could be found, for example, when there are n^2 pairs $\{\langle x_i,y_j\rangle \mid 1\leq i\leq n, 1\leq j\leq n\}$ of zeros.

Acknowledgement

We would like to thank Dr. Zvi Kedem for many helpful discussions.

Bibliography

Belaga, E.C., "Some Problems in the Computation of Polynomials", Dokl. Akad. Nauk. SSSR, 123 (1958), 775-777.

Knuth, D.E., The Art of Computer Programming, Vol. II, Seminumerical Algorithms, Addison-Wesley (1969), Don Mills.

Motzkin, T.S., "Evaluation of Polynomials and Evaluation of Rational Functions", Bull. Amer. Math. Soc. 61 (1955), 163.

Pan, V.Y., "Methods of Computing Values of Polynomials", Russian Mathematical Surveys, Vol. 21, No. 1 (1966).

Paterson, M. and Stockmeyer, L., "Bounds on the Evaluation Time of Rational Functions", Proc. Twelfth Annual IEEE Symposium on Switching and Automata Theory (Oct. 1971), 140-143.

Revah, L., "On the Number of Multiplications/Divisions Evaluating a Polynomial with Auxiliary Functions", M.Sc. thesis, Technion Haifa, Isreal, (submitted to SIAM J. Comp.), (1973).

Strassen, V., "Schwer berechenbare Polynome met rationalen Koeffizienten", unpublished manuscript, University of Zürich (1972).

Strassen, V., "Die Berechnungskomplixetät von elementarysymmetrischen Funktunin und von Anterpolationskoeffizienten", Numerische Mathematik, Vol. 20, No. 3 (1973), 238-251.

Van der Waerden, B.L., "Modern Algebra", Vol. 1, Frederick Ungar Publishing Co., Third Printing (1964).

Winograd, S., "On the Number of Multiplications Necessary to Compute Certain Functions", Comm. on Pure and Applied Mathematics, Vol. 23 (1970).