AN $\Omega((n/\lg n)^{1/2})$ LOWER BOUND ON THE NUMBER OF ADDITIONS NECESSARY TO COMPUTE 0-1 POLYNOMIALS OVER THE RING OF INTEGER POLYNOMIALS

Ronald L. RIVEST
Laboratory for Computer Science, Massachusetts Institute of Technology, Cambridge, MA, U.S.A.

Jean-Paul VAN DE WIELE
Laboria, IRIA, Domaine de Voluceau, Rocquencourt, B.P. 105, 78150 Le Chesnay, France

Received 6 November 1978, revised version received 9 January 1979

Computational complexity, polynomial evaluation, lower bound, additive complexity, 0-1 polynomials, integer preconditioning

1. Introduction

An interesting open problem in arithmetic complexity is to find concrete polynomials that are both simple in form and hard to compute. In this paper we study the complexity of univariate polynomials with 0-1 coefficients in the model with integer preconditioning. In this model the free constants are the integers and the allowed operations are addition, substraction and multiplication (no division). We compute over the *ring* of integer polynomials. Using a counting argument inspired by Paterson–Stockmeyer [1], we prove a lower bound of order $(n/\lg n)^{1/2}$ on the additive complexity of 0-1 polynomials in this model. In other words there is a strictly positive real number γ such that for all natural numbers $n > 1$ there is a univariate nth degree 0-1 polynomial that requires at least $\gamma(n/\lg n)^{1/2}$ ± operations to be evaluated in $\mathbf{Z}[x] \bmod(\mathbf{Z} \cup \{x\})$. (Evaluating a polynomial $f(x)$ in $(\mathbf{Z}[x] \bmod(\mathbf{Z} \cup \{x\}))$ must begin with the variable x and the integers, and compute $f(x)$ in a sequence of steps each of which uses only +, –, or $\circ$ on the given inputs or results of previous steps.) This bound is better than the best known lower bound on the additive complexity of 0-1 polynomials in the model with general complex preconditioning, which is only $\Omega(n^{1/2}/\lg n)$. ([4]. See also this paper for a survey of results on the computational complexity of 0-1 polynomials.)

In both models the best upper bound is $O(n/\lg n)$. (See [2].) Hence a stronger lower bound may still be shown.

Paterson, Stockmeyer [1] have shown a lower bound of order $n^{1/2}$ on the non scalar multiplicative complexity of 0-1 nth degree polynomials in the model with integer preconditioning. Moreover they have shown the optimality of this bound. The question is also settled for the total number of operations. Indeed it has been shown [4] that there are nth degree 0-1 polynomials that require order of $(n/\lg n)$ total arithmetic operations to be computed over the field of complex rational functions. Like the previous one, this bound is asymptotically optimal.

2. Definitions and model of computation

Let F denote the set $\{0, 1\}$ and let $\mathbf{N}, \mathbf{Z}, \mathbf{Z}_p$ stand for the set of nonnegative natural numbers, integers and integers modulo p, respectively. For a prime p, $\mathbf{Z}_p$ is a field. Let x be an indeterminate. $F[x]$ is the set of polynomials in x with 0-1 coefficients. Let k be a ring. $k[x]$ is the ring of polynomials in x over k.

A *computation* β in $k[x] \bmod(k \cup \{x\})$ for

$p(x) \in k[x]$ is a sequence of computation steps S_i, $1 \leqslant i \leqslant l$, such that there is i_0, $1 \leqslant i_0 \leqslant l$, with $S_{i_0} = p(x)$ and either

(i) $S_i \in k \cup \{x\}$ or

(ii) $S_i = S_j \circ S_k$ with $j, k < i$ and $\circ \in \{+, -, \cdot\}$.

The polynomials S_i are the results of the computation and β is said to compute the S_i.

The *additive complexity* of a polynomial $p(x) \in k[x]$ over the ring $k[x]$ is the minimum number of addition and subtraction steps in a computation for p in $k[x] \bmod (k \cup \{x\})$.

We are now going to study the additive complexity over $\mathbf{Z}[x]$ of polynomials in $F[x]$. We denote by $L(\pm, p)$ the additive complexity over $\mathbf{Z}[x]$ of a polynomial $p(x)$ in $\mathbf{Z}[x]$.

If f and g are functions from $\mathbf{N}$ to $\mathbf{N}$, $f(n) = \Omega(g(n))$ means that there is a positive constant γ such that finally $f(n) \geqslant \gamma g(n)$. The abbreviation lg stands for $\log_2$.

3. An $\Omega((n/\lg n)^{1/2}$ lower bound on the additive complexity of 0-1 polynomials over the ring of integers

Theorem 1. *There exists a real number $\gamma > 0$ such that for any natural number $n > 1$ there is a polynomial of degree n in $F[x]$ that cannot be computed in $\mathbf{Z}[x] \bmod (\mathbf{Z} \cup \{x\})$ with less than $\gamma((n/\lg n))^{1/2}$ additive operations.*

Proof. Let n and q be natural numbers, q a prime. We shall fix q later. Consider the finite field $\mathbf{Z}_q$ and the ring homomorphism $H : \mathbf{Z} \to \mathbf{Z}_q$ given by $H(z) = z \bmod (q)$. If $p(x) = \Sigma_{i=0}^{n} z_i x^i \in \mathbf{Z}[x]$ can be evaluated by a computation in $\mathbf{Z}[x] \bmod (\mathbf{Z} \cup \{x\})$ using k additions, then certainly $\tilde{p}(x) = \Sigma_{i=0}^{n} H(z_i)\, x^i \in \mathbf{Z}_q[x]$ can be evaluated by an algorithm in $\mathbf{Z}_q[x] \bmod (\mathbf{Z}_q \cup \{x\})$ using k additions. In the rest of the paper the term additions will be employed in place of additive operations.

Any computation in $\mathbf{Z}_q[x] \bmod (\mathbf{Z}_q \cup \{x\})$ with $\leqslant k$ additions can be expressed by the following scheme $\mathcal{A}_k$, where the m_{ij}, m'_{ij} are natural numbers, and c_i and d_i are integers modulo q:

$$\mathcal{A}_k \begin{cases} s_0 = x\,, \\ s_j = c_j \prod_{i=0}^{j-1} s_i^{m_{i,j}} + d_j \prod_{i=0}^{j-1} s_i^{m'_{i,j}} \qquad \text{for } 1 \leqslant j \leqslant k, \\ p(x) = s_{k+1} = c_{k+1} \prod_{i=0}^{k} s_i^{m_{i,k+1}}\,. \end{cases}$$

Let $\mathbf{N}(k)$ be the number of different polynomials in $\mathbf{Z}_q[x]$ that are computable by at least one algorithm in $\mathcal{A}_k$. Let a be an element in $\mathbf{Z}_q$ and let b and c be natural numbers with $b \equiv c \bmod (q-1)$. Then it is well known that $a^b \equiv a^c \bmod (q)$, since q is a prime. Therefore the exponents $m_{i,j}$, $m'_{i,j}$ can be assumed to range over $\{0, 1, ..., q-2\}$ and $\mathbf{N}(k)$ is bounded above by q^s where s is the number of different parameters in $\mathcal{A}_k$.

Thus

$$\mathbf{N}(k) \leqslant q^{(\Sigma_{j=1}^{k} 2(j+1)) + k + 2} = q^{k^2 + 4k + 2}\,.$$

Let now $M(k)$ be the number of different nth degree 0-1 polynomials in $\mathbf{Z}_q[x]$. $M(k) = 2^n$ provided $q \geqslant n$. Choose the prime q such that $n \leqslant q \leqslant 2n$. Such a prime exists for all $n \geqslant 1$. (See for instance [3, p. 57, Satz 31].)

Every 0-1 polynomial of degree n can be computed by an algorithm in $\mathcal{A}_k$ only if $\mathbf{N}(k) \geqslant M(k)$. This means

$$q^{k^2 + 4k + 2} \geqslant 2^n\,.$$

Thus $k^2 + 4k + 2 \geqslant n/\lg q \geqslant n/(2 \lg n)$ for n large enough. Hence $k \geqslant (n/(2 \lg n))^{1/2} - 2 \geqslant \frac{1}{2}\cdot (n/\lg n)^{1/2}$ for n large enough. This proves that there is a positive real number γ such that for all natural numbers $n > 1$ there exists some 0-1 polynomial p of degree n such that $L(\pm, p) \geqslant \gamma(n/\lg n)$. We are done.

References

[1] M.S. Paterson and L.J. Stockmeyer, On the number of non scalar multiplications necessary to evaluate poly-

nomials, SIAM J. Comput. 2 (1) (1973) 60–66.
[2] J.E. Savage, An algorithm for the computation of linear firms, SIAM J. Comput. 3 (2) (1974) 150–158.
[3] E. Trost, Primzahlen (Birkhäuser, Basel, 1953).
[4] J.-P. van de Wiele, An optimal lower bound on the number of total operations to compute 0-1 polynomials over the field of complex numbers, Rapport Laboria No. 303 (May 1978).