PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 124, Number 5, May 1996

# THE COST OF COMPUTING INTEGERS

W. DE MELO AND B. F. SVAITER

(Communicated by William W. Adams)

Abstract. We analyse the growth rate of a number theoretic function related to the operational complexity of integers

The purpose of this note is to answer a question raised by Smale on the cost of computing integers using arithmetic operations. More precisely, let $\tau\colon \mathbf{N} \to \mathbf{N}$ be the function that associates to each number $n$ the minimum number of arithmetic operations (addition, subtraction and multiplication) one needs to obtain $n$ starting from 1 and 2. Although 2 is obtainable from 1 in one operation, we have included it as a "starting number" (like 1) to simplify our formulas and induction.

**Definition.** An *allowable list* of length $k$ is a list of $k$ integers $n_1, n_2, \dots, n_k$ such that for each $l \le k$, there exist integers $-1 \le i, j < l$ such that $n_l = op(n_i, n_j)$, where *op* is either addition, subtraction or multiplication and $n_{-1} = 1, n_0 = 2$.

It follows that $\tau(n) \le k$ if and only if there exists an allowable list of length $k$, $\{n_1, \dots, n_k\}$ with $n_k = n$. Also, $\tau(n) = k$ if $\tau(n) \le k$ but $\tau(n)$ is not less than or equal to $k-1$.

**Proposition 1.** (a) $\log\log(n) \le \tau(n) \le 2\log(n)$, *where* $\log$ *is the logarithm in base* 2.

(b) $\tau(2^{2^k}) = k = \log(\log(2^{2^k}))$.

*Proof.* Suppose that $\tau(n) = k$. Then there exists an allowable list $\{n_1, \dots, n_k\}$ with $n_k = n$. Let us consider the allowable list $\{m_1, \dots, m_k\}$, where $m_l = m_{l-1} \times m_{l-1}$. By induction we have that $n_l \le m_l$ for every $l \le k$ because $m_i \le m_j$ for $i \le j$. Therefore, $n \le m_k = 2^{2^k}$. Thus, $\log(\log(n)) \le k = \tau(n)$. This proves (b) and the first inequality in (a). To prove the second inequality we consider the binary expansion $n = 2^{k_1} + 2^{k_2} + \cdots + 2^{k_l}$, with $0 \le k_1 < \cdots < k_l$. The following is an allowable sequence:

$$\{2^2, 2^3, \dots, 2^{k_l}, 2^{k_l} + 2^{k_{l-1}}, \dots, 2^{k_l} + \cdots + 2^{k_1} = n\}.$$

Hence, $\tau(n) \le k_l + l \le 2\log(n)$.

*Remark.* $\tau(2^n) \le 2\log\log(2^n)$. In fact, if $n = 2^{k_1} + \cdots + 2^{k_l}$, then

$$\{2, 2^2, 2^{2^2}, \dots, 2^{2^{k_l}}, 2^{2^{k_l}} \times 2^{2^{k_{l-1}}}, \dots, 2^{2^{k_l} + \cdots + 2^{k_1}} = n\}$$

is an allowable list and, therefore, $\tau(n) \le k_l + l \le 2\log\log(2^n)$.

Received by the editors May 31, 1994 and, in revised form, October 24, 1994.
1991 *Mathematics Subject Classification.* Primary 11N56, 11A25, 11Y16.

**Lemma 1.** *Let $B(k) = \{n \in \mathbf{N}; \tau(n) \leq k\}$. Then the cardinality $\#B(k) \leq 3^k \times ((k+1)!)^2$.*

*Proof.* Let us consider the space $\mathcal{S}_k = \{s = (s_1, \ldots, s_k)\}$, where each $s_l = (op_l, i_l, j_l)$ and $op_l \in \{+, \times -\}$, $i_l, j_l$ are integers smaller than $l$. To each point $s \in \mathcal{S}_k$ we can associate an allowable sequence $n_1, \ldots, n_k$ by taking $n_l = op_l(n_{i_l}, n_{j_l})$, starting with $n_{-1} = 1$ and $n_0 = 2$. In particular we have a mapping $\phi: \mathcal{S}_k \to B(k)$ which associates to $s$ the integer $n_k$ constructed above. Since $\phi$ is onto, it follows that the cardinality of $B(k)$ is at most equal to the cardinality of $\mathcal{S}_k$ which is equal to $3^k \times ((k+1)!)^2$.

**Definition.** A property $P$ holds for almost all integers if the number of integers smaller than $n$ that do not satisfy $P$ is $n \times o(n)$.

**Theorem.** *If $\epsilon > 0$, then almost all integers $n$ satisfy the property:*

$$\tau(n) \geq \frac{\log(n)}{(\log\log(n))^{1+\epsilon}}.$$

*Proof.* Suppose, by contradiction, that this is not true. Let

$$\psi(n) = \frac{\log(n)}{(\log\log(n))^{1+\epsilon}}.$$

Then, there exists $0 < \rho < 1$ such that, for infinitely many values of $m$, the cardinality of the set

$$C_m = \{n \leq m; \tau(n) \leq \psi(n)\}$$

is bigger than $\rho \times m$. If $\psi(m) \leq k < \psi(m) + 1$, then $C_m \subset B_k$. Therefore, by the lemma, $\rho \times m \leq 3^k((k+1)!)^2$ for infinitely many values of $m$. Thus,

$$\rho \times m \leq 3^{\psi(m)+1}(\psi(m)+2)^{2(\psi(m)+2)}$$

which is a contradiction because a straightforward calculation shows that the above inequality cannot hold for $m$ big enough.

The above theorem answers negatively Smale's first question: does there exist a polynomial $p$ such that $\tau(n) \leq p(\log\log(n))$?

**Smales's question 2.** Is $\tau(k!) \leq p(\log k)$ for some universal polynomial $p$?

**Smale's question 3.** Does there exist a polynomial $p$ such that for each $k$ there exists an $m$ satisfying $\tau(m \times k!) \leq p(\log k)$ ? In [SS], Shub and Smale proved that a negative answer to this question implies that one cannot find an algorithm having polynomial cost to decide whether a family of polynomials have a common zero, and, by the results of [BSS], this implies that $N \neq NP$ over the complex numbers.

## References


[SS] M. Shub and S. Smale, *On the Intractability of Hilbert's Nullestellensatz and an algebraic version of "$NP \neq P$?"*, preprint.

[BSS] L. Blum, M. Shub, and S. Smale, *On a theory of computation and complexity over the real numbers: NP-completeness, recursive functions and universal machines*, Bull. Amer. Math. Soc. **21** (1989), 1–46. MR **90a:**68022



Instituto de Matematica Pura e Aplicada, Estrada Dona Castorina 110, Jardim Botanico, Rio de Janeiro, Brazil

*E-mail address*: demelo@impa.br

*E-mail address*: benar@impa.br