A Question of Smale

Peter Borwein

http://www.cecm.sfu.ca/~pborwein.

2005
Abstract

Abstract: Two problems of Smale that imply a version of $P \neq NP$ over $\mathbb{C}$.

These are from a paper of Smale entitled ”Mathematical problems for the next century.” They are problem 4.
Introduction

Smale Verbatim

Problem 4: Integer zeros of a polynomial of one variable.

A program for a polynomial $f \in \mathbb{Z}[t]$ of one variable with integer coefficients is the object $(1, t, u_1, \ldots, u_k)$ where $u_k = f$, and for all $l$, $u_l = u_i \circ u_j$, $i, j < l$ and $\circ$ is one of $+,-$ or $\ast$. Here $u_0 = t$ and $u_{-1} = 1$. Then $\tau(f)$ is the minimum of $k$ over all such programs.
Is the number of distinct integer zeros of $f$, polynomially bounded by $\tau(f)$? In other words, is

$$Z(f) \leq a\tau(f)^c \text{ for all } f \in \mathbb{Z}[t].$$

Here $Z(f)$ is the number of distinct integer zeros of $f$ with $a$, $c$ universal constants.

From earlier results of Strassen, communicated via Schönhage, Shub, and Bürgisser, it follows that the exponent $c$ has to be at least 2.
Mike Shub and I discovered this problem in our complexity studies. We proved that an affirmative answer implied the intractibility of the Nullstellensatz as a decision problem over \( \mathbb{C} \) and thus \( P \neq NP \) over \( \mathbb{C} \).

See (Shub-Smale, 1995) and also BCSS.

Since the degree of \( f \) is less than or equal to \( 2^\tau \), \( \tau = \tau f \), there are no more than \( 2^\tau \) zeros altogether.

For Chebyshev polynomials, the number of distinct real zeros grows exponentially with \( \tau \).
Many of the classic diophantine problems are in two or more variables. This problem asks for an estimate in just one variable, and nevertheless seems not so easy.

Here is a related problem. A program for an integer m is the object \((1, m_1, ..., m_l)\) where \(m_k = m\), \(m_0 = 1\) and for all \(l\), \(m_l = m_j \circ m_k\), \(j, k < l\) and \(\circ\) is one of \(+, -\) or \(*\). Then \(\tau(f)\) is the minimum of \(k\) over all such programs. Thus \(\tau(m)\) represents the shortest way to build up an integer m starting from 1 using plus, minus, and times.
**Problem:** Is there a constant $c$ such that $\tau(k!) \leq (\log k)^c$ for all integers $k$?

One might expect this to be false, so that $k!$ is hard to compute (see Shub-Smale, 1995).
A Start

As above let $S_k$ be the set of all polynomials in $\mathbb{Z}[t]$ for which there exists a program

$$(1, t, u_1, ..., u_k)$$

where $u_k = f$, and for all $l$,

$$u_l = u_i \circ u_j, \quad i, j < l$$

and $\circ$ is one of $+, -, \text{ or } *$,

Here $u_0 = t$ and $u_{-1} \in A$ where $A$ is a fixed finite set of integers.
Some programs with $k := 1$

$[1, t, 2], [1, t, 0], [1, t, 1], [1, t, t + 1],$

$[1, t, -t+1], [1, t, t], [1, t, t-1], [1, t, 2t], [1, t, t^2]$

A variety of length 3 programs are:

$[1, t, 2t, -t + 1, -t^2 + t]$

$[1, t, 0, 2t, t]$

$[1, t, t + 1, 2t, 2]$

$[1, t, t - 1, -t + 1, -2t + 1]$

$[1, t, t^2, 2t^2, 4t^4]$
One can compute that $S_1$ has cardinality 21, $S_2$ has cardinality 189 and $S_3$ has cardinality 11301.

**Theorem 1**

$$|S_k| \leq (3/2)^k(k+2)!(k+1)! \leq 2^{ck \log(k)}$$

for some absolute constant $c$.

**Proof.** This is an easy induction. Every program of length $k$ gives rise to at most $3((k+2)(k+1)/2)$ programs of length $k+1$. 

The cost of an integer $n$, denoted $\tau(n)$, is the least integer $m$ such that there exists a sequence $(s_0, \cdots, s_m)$ of integers with the property that $s_0 = 1$, $s_m = n$, and for each $l \in \{1, \cdots, m\}$ there exist $i, j \in \{0, \cdots, l-1\}$ such that $s_l = F(s_i, s_j)$ where $F$ is one of addition, subtraction, or multiplication.
In this paper, the author proves that for any $\epsilon > 0$, the ratio

$$\frac{\# \{ k \leq n \mid \tau(k) \geq \frac{\log k}{\log \log k} + (1 - \epsilon) \frac{\log k \log \log \log k}{(\log \log k)^2} \}}{n}$$

approaches 1 as $n$ goes to infinity and that for any $\epsilon > 0$,

$$\tau(n) \leq \frac{\log n}{\log \log n} + (3 + \epsilon) \frac{\log n \log \log \log n}{(\log \log n)^2}$$

for $n$ sufficiently large. He concludes that

$$\tau(n) \geq \frac{\log n}{\log \log n}$$

for almost all $n$, and that for any $\epsilon > 0$, if $n$ is large enough, then

$$\tau(n) \leq (1 + \epsilon) \frac{\log n}{\log \log n}.$$
These bounds improve on earlier results, such as those in a paper by W. de Melo and B. F. Svaiter [Proc. Amer. Math. Soc. 124 (1996), no. 5, 1377–1378; MR1307510 (96g:11150)]. The author also extends the notion of cost to a polynomial in several variables with integral coefficients and establishes bounds for this case which are analogous to those given above for the integer cost function.

The final section of the paper is devoted to a discussion of some open
problems relating to the integer cost function $\tau$. The most significant of these is to determine whether there exist a sequence of positive integers $\{n_i\}_{i=0}^{\infty}$ and a positive constant $c$ such that $\tau(n_ii!) \leq (\log i)^c$ for all $i$. In a paper by M. Shub and S. Smale [Duke Math. J. 81 (1995), no. 1, 47–54 (1996)] it is shown that if no such sequence exists, then an algebraic version of $\text{NP} \neq \text{P}$ is true.

It has long been observed that certain factorization algorithms provide a way to write products of large numbers of integers succinctly. In this paper, we study the problem of representing the product of all integers from 1 to $n$ ($n!$) by straight-line programs.

Formally, we say that a sequence of integers $a_n$ is ultimately $f(n)$-computable if there exists a nonzero integer sequence $m_n$ such that for any $n, a_n m_n$
can be computed by a straight-line pro-
gram (using only additions, subtrac-
tions and multiplications) of length at
most \( f(n) \). M. Shub and S. Smale
54 (1996); MR1381969 (97h:03067)]
showed that if \( n! \) is ultimately hard to
compute, then the algebraic version of
\( \text{NP} \neq \text{P} \) is true.
Assuming a widely believed number theory conjecture concerning the density of smooth numbers in short intervals, a subexponential upper bound

$$\exp(c \sqrt{\log n \log \log n})$$

for the ultimate complexity of $n!$ is proved in this paper, and a random subexponential algorithm constructing a correspondingly short straight-line program is presented as well.
Binomial Coefficients with Division:

Let \( N_k \) be the set of all integers \( m \) for which there exists a program \( (0, 1, u_1, \ldots, u_k) \) where \( u_k = m \) and for all \( l \),

\[
  u_l = u_i \pm u_j, \quad i, j < l
\]

or

\[
  u_l = u_i \times u_j, \quad i, j < l
\]

or

\[
  u_l = u_i / u_j, \quad i, j < l.
\]

(Here division is ”integer division” so \( a/b := q \) where \( a = bq + r \) where \( 0 \leq r < b \).)
Theorem 2 Both \( \binom{n}{m} \) and \( n! \) are in \( \mathcal{O}(\log(n)) \).

Proof

Consider

\[ F_n := (1 + 10^n)^n \]
Then $F_n$ is an integer with $n^2$ digits with $\binom{n}{m}$ embedded in the middle. Note that $\binom{n}{m}$ is of maximum size $2^n$. So in the expansion each binomial is separated by zeros.

So, for example,

\[(1 + 10^8)^8 =
\]

\[
1000000008000000028000000056000000
\]

\[
70000000560000000280000000
\]

\[
8000000001.
\]
Note that $F_n$ evaluates as a straight line program in in $O(\log(n))$ steps.

Note also that

$$(2^n)! = \left(\frac{2^n}{2^{n-1}}\right)\left(\frac{2^{n-1}}{2^{n-2}}\right)^2 \left(\frac{2^{n-2}}{2^{n-3}}\right)^4 \cdots$$

So if binomial coefficients are polynomial in $\log(n)$ then so are factorials (or at least factorials of powers of 2).

So if splitting an integer in half is $O(\log(n))$ then so is computing factorials.
Division allows for this as follows. To get the \((m+1)\)th through \(n\)th digits of \(M\) compute as follows. Let

\[
a := (m/10^m) \times 10^m.
\]

Then \(a\) has lowest \(m\) digits zero and the rest agree with those of \(M\). Now let

\[
b := (n/10^n) \times 10^n
\]

and consider \((b - a)/10^m\).
Questions and stuff.

**Question.** Does anything distinguish $S_k$ analytically/combinatorially?

**Question.** Can one tell whether an element is in $S_k$ without computing all of $S_k$?

**Question.** Is number of irreducible factors the right question?
**Question.** Find an unconditional algorithm for $n!$ that is subexponential in the sense of [?]. That is better than $e^{\sqrt{\log n}}$. And does not require assumptions on smooth numbers.

**Question.** What about binomial coefficients?


