Theoretical Computer Science 11 (1980) 331–335
© North-Holland Publishing Company

J. VON ZUR GATHEN & V. STRASSEN (1980). Some polynomials that are hard to compute. *Theoretical Computer Science* **11**, 331–335. URL http://dx.doi.org/10.1016/0304-3975(80)90020-1. Russian version in *Kiberneticeskij sbornik* (1983).
This document is provided as a means to ensure timely dissemination of scholarly and technical work on a non-commercial basis. Copyright and all rights therein are maintained by the authors or by other copyright holders, notwithstanding that these works are posted here electronically. It is understood that all persons copying any of these documents will adhere to the terms and constraints invoked by each copyright holder, and in particular use them only for noncommercial purposes. These works may not be posted elsewhere without the explicit written permission of the copyright holder. (Last update 2016/05/18-14 :21.)

NOTE

SOME POLYNOMIALS THAT ARE HARD TO COMPUTE

J. von zur GATHEN and V. STRASSEN
Seminar für Angewandte Mathematik, Universität Zürich, CH-8032 Zürich, Switzerland

Communicated by A. Schönhage
Received November 1978

Abstract. Using the result of Heintz and Sieveking [1], we show that the polynomials $\sum_{1\leqslant j\leqslant d} b^{1/i}X^i$ with b positive real different from one, and $\sum_{1\leqslant j\leqslant d} j^rX^i$ with r rational not integer, are hard to compute.

We use the following variant of the main result of Heintz and Sieveking [1]:

Let $f=\sum_{1\leqslant j\leqslant d} b_jX^i \in \mathbf{C}[X]$, k_0 a subfield of $\mathbf{C}$ such that all b_j are algebraic over k_0, and N the number of conjugates of $(b_1,\ldots,b_d)$ over k_0 (i.e. the size of the orbit of $(b_1,\ldots,b_d)$ in $\mathbf{C}^d$ under the action of the Galois group of $\mathbf{C}$ over k_0).

Let $g_1,\ldots,g_n \in k_0[T_1,\ldots,T_d]$ be polynomials of degree $\leqslant M$ such that $\{x\in\mathbf{C}^d: g_1(x)=\cdots=g_n(x)=0\}$ is finite and contains $(b_1,\ldots,b_d)$. Then

$$L(f)\geqslant\left(\frac{\log N}{24\log(dM)}\right)^{1/2}.$$

Here $L(f)$ is the minimum number of nonscalar multiplications/divisions sufficient to compute f over $\mathbf{C}\cup\{x\}$ by a straight-line program. (So arbitrary preconditioning is allowed.)

Application 1. Let b be positive real and different from one. Then

$$L\Big(\sum_{1\leqslant j\leqslant d} b^{1/i}X^i\Big)\geqslant\left(\frac{d}{\log d}\right)^{1/2}.$$

(Here $u(d)\geqslant v(d)$ means that there is a positive constant c such that $u(d)\geqslant c\cdot v(d)$ for large d. Roots of positive real numbers are understood to be positive real unless otherwise stated.)

Proof. Let $k_0=\mathbf{Q}(b,\exp(2\pi i/3),\ldots,\exp(2\pi i/d))=\mathbf{Q}(b,\exp(2\pi i/l))$, where $l=\operatorname{lcm}(1,\ldots,d)$, and let $g_j=T_j^j-b$ for $j=1,\ldots,d$. Then $\deg g_j\leqslant d=:M$. Moreover $K:=k_0(b^{1/2},\ldots,b^{1/d})$ is a Galois extension of k_0 and the orbits of $(b,b^{1/2},\ldots,b^{1/d})$ under $\operatorname{Gal}(\mathbf{C}/k_0)$ and $\operatorname{Gal}(K/k_0)$ are the same. Since only the identity element of

$\mathrm{Gal}(K/k_0)$ fixes $(b, \ldots, b^{1/d})$, we have

$$N = \text{size of orbit of } (b, b^{1/2}, \ldots, b^{1/d}) \text{ under } \mathrm{Gal}(K/k_0)$$
$$= \#\mathrm{Gal}(K/k_0) = [K: k_0].$$

Hence,

$$L\Big(\sum_{1 \leq j \leq d} b^{1/j} X^j\Big) \geq \left(\frac{\log[K: k_0]}{\log d}\right)^{1/2}.$$

We write $[K: k_0] = [K: \mathbf{Q}(b)]/[k_0: \mathbf{Q}(b)]$. If b is transcendental, then $[k_0: \mathbf{Q}(b)] = [\mathbf{Q}(\exp(2\pi \mathrm{i}/l)): \mathbf{Q}] = \varphi(l)$. If b is algebraic, then $[k_0: \mathbf{Q}(b)]$ divides

$$[k_0: \mathbf{Q}] = \varphi(l) \cdot [k_0: \mathbf{Q}(\exp(2\pi \mathrm{i}/l))].$$

Since $\varphi(l)$ has only prime divisors $< \frac{1}{2}d$ and $[k_0: \mathbf{Q}(\exp(2\pi \mathrm{i}/l))] \leq [\boldsymbol{Q}(b): \mathbf{Q}]$, which is independent of d, we obtain that in either case

$$p \nmid [k_0: \mathbf{Q}(b)]$$

for all primes p between $\frac{1}{2}d$ and d, provided d is sufficiently large.

On the other hand, we claim that

$$p \mid [K: \mathbf{Q}(b)]$$

for d sufficiently large and all primes p such that $\frac{1}{2}d \leq p \leq d$. This claim implies

$$\log[K: k_0] \geq \log\Big(\prod_{\frac{1}{2}d \leq p \leq d} p\Big) \geq d$$

by the Prime Number Theorem, and therefore Application 1.

To prove the claim it is sufficient to show

$$[\mathbf{Q}(b^{1/p}): \mathbf{Q}(b)] = p$$

for large primes p.

Let p be a prime and assume $[\mathbf{Q}(b^{1/p}): \mathbf{Q}(b)] < p$. Then $T^p - b$ has a nontrivial factor $h \in \mathbf{Q}(b)[T]$. Since $T^p - b = (T - \zeta^0 a) \cdots (T - \zeta^{p-1} a)$ over $\mathbf{C}$, where $a = b^{1/p} \in \mathbf{R}$ and $\zeta = \exp(2\pi \mathrm{i}/p)$, the constant term of h is of the form $\zeta^t a^m$ with $1 \leq m < p$. Thus $\zeta^t a^m \in \mathbf{Q}(b)$. Writing $1 = um + vp$ we get $\zeta^{tu} a \in \mathbf{Q}(b)$, and therefore $a \in \mathbf{Q}(b)$, since a and b are real. If b is transcendental, this cannot happen. If b is algebraic, consider the factorization $(b) = q_1^{e_1} \cdots q_r^{e_r}$ of the fractional ideal (b), where the q_i are prime ideals in the ring $\mathcal{O}$ of integers of $\mathbf{Q}(b)$, and $e_i \in \mathbf{Z} \setminus \{0\}$. The corresponding factorization of (a) yields that p divides every e_i. For large p this cannot happen unless $r = 0$. In this case a and b are units of $\mathcal{O}$. By Dirichlet's unit theorem, there is a unique representation $b = u \cdot v_1^{f_1} \cdots v_s^{f_s}$, where u is a root of unity in $\mathbf{Q}(b)$, $\{v_1, \ldots, v_s\}$ is a set of fundamental units of $\mathbf{Q}(b)$, and $f_1, \ldots, f_s \in \mathbf{Z}$. The corresponding representation of a yields that p divides every f_i. For large p this cannot happen, unless all f_i are zero. But then $b = 1$, which is excluded. This proves the claim.

Remark. We have stated Application 1 for positive roots of positive real b. Actually, the proof goes through for any nonzero complex b not a root of unity and arbitrary roots $b^{1/j}$. If b is a root of unity, say $b = \exp(2\pi i/t)$ for simplicity, the polynomial is hard (see [1, Corollary 1]) if one takes $b^{1/j} = \exp(2\pi i/tj)$. However, for any such b one can also choose the $b^{1/j}$ in such a way that the polynomial becomes easy:

To any j we associate the unique natural numbers f, g such that $f = \gcd(j, t^l)$ for large l, $1 \leq g < t$, and $g \cdot (j/f) \equiv 1 \pmod t$. We set $b_j = \exp(2\pi i g/ft)$. Then $b_j^j = \exp(2\pi i/t) = b$. If t has s different prime divisors, there are at most $(\log d)^s \cdot t$ possibilities for the f, g associated to the $j \in \{1, \ldots, d\}$. We split up $\sum_{1 \leq j \leq d} b_j X^j$ into subsums according to the value of f, g. Each subsum is a geometric sum and can be computed in $O(\log d)$. Therefore $L(\sum_{j \leq d} b_j X^j) = O((\log d)^{s+1})$.

Application 2. Let $r \in \mathbf{Q} \backslash \mathbf{Z}$. Then

$$L\Big(\sum_{1 \leq j \leq d} j^r X^j\Big) \geq d^{1/2}/\log d.$$

Proof. Let $r = s/t$ with $s \in \mathbf{Z}$, $t \in \mathbf{N}$ relatively prime, p a prime divisor of t, $\zeta = \exp(2\pi i/p)$, $k_0 = \mathbf{Q}(\zeta)$, and $g_j = T_j^t - j^s$ for $j = 1, \ldots, d$. Furthermore let $q_1, \ldots, q_m$ be the prime numbers $\leq d$. Then

$$\begin{aligned} N &= \#\text{ conjugates of } (1^r, 2^r, \ldots, d^r) \text{ over } k_0 \\ &= \#\text{ conjugates of } (q_1^r, \ldots, q_m^r) \text{ over } k_0 \\ &\geq \#\text{ conjugates of } ((q_1^s)^{1/p}, \ldots, (q_m^s)^{1/p}) \text{ over } k_0 \\ &= [k_0((q_1^s)^{1/p}, \ldots, (q_m^s)^{1/p}) \colon k_0]. \end{aligned}$$

The last equality follows as in the previous proof, since the extension is Galois. We claim that for every $l < m$

$$(q_{l+1}^s)^{1/p} \notin k_0((q_1^s)^{1/p}, \ldots, (q_l^s)^{1/p}).$$

Then we have $N \geq 2^m$ and therefore

$$L\Big(\sum_{1 \leq j \leq d} j^r X^j\Big) \geq (m/24 \log(dt))^{1/2} \geq d^{1/2}/\log d$$

by the Prime Number Theorem. The claim follows from a general fact:

Let $a_1, \ldots, a_l, a$ be positive rational numbers with $a^{1/p} \in k_0(a_1^{1/p}, \ldots, a_l^{1/p})$. Then there are $w \in \mathbf{Q}$, $e_1, \ldots, e_l \in \mathbf{N}$ such that

$$a = w^p a_1^{e_1} \cdots a_l^{e_l}.$$

We prove this by induction on l. For $l = 0$, we have

$$[\mathbf{Q}(a^{1/p}) \colon \mathbf{Q}] \leq [k_0 \colon \mathbf{Q}] = p - 1.$$

This implies, as in the previous proof, $w := a^{1/p} \in \mathbf{Q}$. Inductively, we may assume

$$a^{1/p} \notin k_0(a_1^{1/p}, \ldots, a_{l-1}^{1/p}) =: K.$$

Put $\theta = a_l^{1/p}$, $\eta = a^{1/p}$. Then $K(\theta)$ is a Galois extension of K, and $1, \theta, \ldots, \theta^z$ is a K-basis of $K(\theta)$ for some $z \leq p-1$. (In fact $z = p-1$.) Let

$$\eta = b_0 + b_1\theta + \cdots + b_z\theta^z$$

with $b_i \in K$, and let $\sigma \in \mathrm{Gal}(K(\theta)/K)$ with $\sigma(\theta) \neq \theta$. There exist natural numbers u, v such that

$$\sigma(\theta) = \zeta^u\theta \quad \text{and} \quad (u, p) = 1,$$
$$\sigma(\eta) = \zeta^v\eta.$$

Comparing coefficients of

$$\sigma(\eta) = b_0 + b_1\sigma(\theta) + \cdots + b_z\sigma(\theta)^z$$
$$= b_0 + b_1\zeta^u\theta + \cdots + b_z\zeta^{uz}\theta^z$$

and

$$\sigma(\eta) = \zeta^v\eta = b_0\zeta^v + b_1\zeta^v\theta + \cdots + b_z\zeta^v\theta^z,$$

and observing that the ζ^{ui} are pairwise distinct, we find that there is exactly one i with $b_i \neq 0$. Thus

$$(a/a_l^i)^{1/p} = \eta/\theta^i = b_i \in K.$$

Using the induction hypothesis we conclude

$$a/a_l^i = w^p a_1^{e_1} \cdots a_{l-1}^{e_{l-1}}.$$

Remarks. (1) For $r \in \mathbf{N}$ we have $L(\sum_{j \leq d} j^r X^j) = \mathrm{O}(\log d)$. To see this, put $f_r = \sum_{1 \leq j \leq d} j^r X^j$. From $f_r = x \cdot (\mathrm{d}/\mathrm{d}x) f_{r-1}$ it follows inductively, that $f_r = (x^{d+1} \cdot g + h)/(x-1)^{r+1}$ with polynomials g and h of degree $\leq r$. Hence $L(f_r) = \mathrm{O}(\log d)$.

(2) Since the highest complexity of polynomials of degree d has order $d^{1/2}$ (counting nonlinear operations only), the lower bounds of this paper cannot be much improved. Of course, analogous results hold in the case where all operations are counted. Slightly weaker bounds also follow from the method of Strassen [3] (taking into account the improvement of Schnorr [2]). However, the method of Heintz-Sieveking [1] is much more elegant.

References

[1] J. Heintz and M. Sieveking, Lower bounds for polynomials with algebraic coefficients, *Theoret. Comput. Sci.* **11** (1980) 321–330, this volume.

[2] C.P. Schnorr, Improved lower bounds on the number of multiplications/divisions which are necessary to evaluate polynomials, *Theoret. Comput. Sci.* **7** (1978) 251–261.

[3] V. Strassen, Polynomials with rational coefficients which are hard to compute, *SIAM J. Comput.* **3**(2) (1974) 128–149.