REND. SEM. MAT. UNIV. PADOVA, Vol. 112 (2004)

Large Integer Polynomials in Several Variables.

A. DUBICKAS (*)

ABSTRACT - For every sufficiently large positive integer D, we construct a family of irreducible integer polynomials of degree D in n variables whose Mahler measures are bounded by D and whose values at $(1, \dots, 1)$ are greater than $\exp\{(1/9n)\, D^{n/(n+1)}\}$. This shows that an upper bound for the height of integer irreducible polynomials in terms of their degree and Mahler measure obtained by Amoroso and Mignotte is sharp up to a logarithmic factor.

1. Introduction.

Let $|P|$ be the maximum of modulus of a polynomial in n variables $P(x_1, \dots, x_n)$ in the unit disc $|x_1| \leqslant 1, \dots, |x_n| \leqslant 1$, and let

$$M(P) = \exp\left\{ \int_0^1 \dots \int_0^1 \log |P(e^{2\pi i t_1}, \dots, e^{2\pi i t_n})|\, dt_1 \dots dt_n \right\}$$

be its *Mahler's measure*. Clearly,

$$M(P) \leqslant |P| \leqslant (n+1)^D M(P),$$

where D is the degree of the polynomial P. See also p. 248 in [16] for other versions of the second inequality.

Mignotte [13], [14] (see also [17]) was the first who sharpened this inequality for $n = 1$. He proved that

$$\log |P| < c\sqrt{D \log(DM(P)) \log(2D+1)} + \log M(P), \tag{1}$$

(*) Indirizzo dell'A.: Department of Mathematics and Informatics, Vilnius University, Naugarduko 24, LT-03225 Vilnius, Lithuania.
E-mail: arturas.dubickas@maf.vu.lt

which is better than $\log|P| \leqslant D\log 2 + \log M(P)$ essentially by the factor $\sqrt{D}$ if $M(P)$ is smaller than a fixed power of D. The constant c in this inequality was then sharpened by Amoroso [4] and by the author [9]. Mignotte's original proof involves a version of Siegel's lemma and an inequality on the size of the factors of univariate polynomials. Inequality (1) is the main ingredient in the estimate of the value of a univariate polynomial at an algebraic point. Such estimate is stronger than Liouville and for this reason it has other useful applications. A special version of such inequality for $|\alpha - 1|$, where α is an algebraic number of small Mahler measure, was investigated in [2], [3], [7], [8], [10], [15].

Recently, Amoroso and Mignotte managed to generalize this result to irreducible integer polynomials in several variables. They showed [6] that

$$\log|P| \leqslant 2D^{n/(n+1)}\log((n+2)^3 D^3 M(P)), \tag{2}$$

and, in case $1 + \log M(P)/\log((n+2)D) \leqslant D/4$,

$$\log|P| \leqslant \tag{3}$$

$$\leqslant (n+1)D^{n/(n+1)}\left(1 + \frac{\log M(P)}{\log((n+2)D)}\right)^{1/(n+1)}\log(4(n+2)D^2),$$

thus gaining the factor $D^{1/(n+1)}$ for polynomials with small Mahler measures. (Note that putting $n = 1$ into (3) one obtains (1), and (3) is stronger than (2) if $\log M(P) \geqslant ((3n)^{1+1/n} - 1)\log((n+2)D)$.) Their results come from a multivariate version of Siegel's lemma [5].

On the other hand, Amoroso [1] showed that Mignotte's inequality (1) is sharp up to the logarithmic factors, namely, there are irreducible polynomials $P(x) \in \mathbb{Z}[x]$ of degree D having Mahler's measure $\leqslant D^2/2$ such that $\log P(1) \sim \sqrt{2D\log D}$. In [6] Amoroso and Mignotte exhibited a family of polynomials which demonstrate that (3) is sharp up to the logarithmic factors appearing in it. Unfortunately, in their example Mahler's measure is very large ($M(P)$ is of the size $D^{D^{n/(2n+1)}}$), so it is not clear whether (2) is sharp or not. Therefore, they asked for an example of a polynomial having small Mahler measure but at the same time being large at a point on the unit disc (see p. 11 in [6]). The purpose of this note is to give an explicit family of such polynomials showing that $D^{n/(n+1)}$ is the right order in both (2) and (3). We prove the following:

THEOREM. *Let $n \geqslant 2$ be an integer. Then, for every sufficiently large positive integer D and for every prime number $p \geqslant D/n$, there is an in-*

teger irreducible polynomial P in n variables with degree D and with Mahler's measure $M(P) = p$ satisfying

$$\log |P(1, \dots, 1)| > (1/9n)\, D^{n/(n+1)}. \tag{4}$$

Of course, if p is close to D/n, say $D/n \leqslant p \leqslant 2D/n$, then for the family of polynomials of the theorem inequality (2) is stronger than (3). By (2), for them, the inequality $\log |P| < 8D^{n/(n+1)} \log ((n+1)D)$ holds, so the theorem implies that (2) is sharp up to the logarithmic factor.

In the next section we give the construction of such P which is completely explicit. Then we prove the lower bound (4) of the theorem and recall some useful results about the Mahler measure of polynomials in several variables in proving that $M(P) = p$. The proof of the theorem will be completed in Section 3, where we show that these polynomials P are irreducible. Irreducibility is the main difficulty in our proof. The reason for this is that one cannot use arguments based on Hilbert's irreducibility theorem, because we need a sharp and effective upper bound for the Mahler measure of P, which will be obtained by some «deformation» of a reducible polynomial F, in order to keep the Mahler measure of P small.

Note that the theorem is stated only for $n \geqslant 2$. In [1] and Theorem 2 of [10] slightly better results of order $\sqrt{D \log D}$ instead of just $\sqrt{D}$ as in (4) for $n = 1$ were obtained. Our theorem also implies that the multidimensional Siegel's lemma of Amoroso and David [5] or at least its version given in Proposition 3 of [6] is not far from being sharp, since (2) is derived from it. For instance, the exponent n in Proposition 3 of [6] cannot be replaced by a smaller number.

2. Construction of polynomials large at unity.

Set $F(x_1, \dots, x_n) = \prod (1 + x_1^{\lambda_1} \dots x_n^{\lambda_n})$, where the product is taken over every non-zero vector $(\lambda_1, \dots, \lambda_n) \in \mathbb{Z}^n$, $0 \leqslant \lambda_1, \dots, \lambda_n \leqslant k-1$. Then, as the Mahler measure of polynomials is multiplicative, $M(F) = 1$ (see, e.g., p. 260 in [16] or Theorem 3.10 in [11]). The degree of F is equal to $D = nk^n(k-1)/2$. Since $F(1, \dots, 1) = 2^{k^n - 1}$, for every D of the form $nk^n(k-1)/2$, where $k \in \mathbb{N}$ is sufficiently large, we obtain the inequality $\log |F(1, \dots, 1)| > D^{n/(n+1)}/n$.

Of course, the above F is reducible. We thus define $P(x_1, \dots, x_n)$ as follows. Set $k = [(D/2n)^{1/(n+1)}]$, where D is a sufficiently large integer. Let Λ be the set of vectors $\bar{\lambda} = (\lambda_1, \dots, \lambda_n) \in \mathbb{Z}^n$, where $k \leqslant \lambda_1, \dots, \lambda_n \leqslant$

$\leqslant 2k-1$ and $\gcd(\lambda_1, \lambda_2) = 1$. Suppose that the polynomial

$$Q(x_1, \dots, x_n) = \prod_{\bar{\lambda} \in \Lambda} (1 + x_1^{\lambda_1} \dots x_n^{\lambda_n})$$

has total degree q and partial degree ℓ in x_1. Then, since $|\Lambda| < k^n$, we have

$$q \leqslant n(2k-1)\,|\Lambda| < 2nk^{n+1} \leqslant D \quad \text{and} \quad \ell \leqslant (2k-1)\,|\Lambda| < (2k-1)\,k^n.$$

Now, set

$$(5) \qquad P(x_1, \dots, x_n) = \frac{1}{x_1^{r-1}} \frac{\partial(x_1^r(1 + x_1 x_2^{D-q-1})\,Q(x_1, \dots, x_n))}{\partial x_1},$$

where r is an arbitrary positive integer such that $p = 1 + \ell + r$ is a prime number. The fact that p is prime will only be used for irreducibility in Section 3.

It is clear that the degree of P is equal to D. Since the coefficients of Q are non-negative,

$$|P(1, \dots, 1)| = P(1, \dots, 1) > Q(1, \dots, 1) = 2^{|\Lambda|}.$$

Suppose that Λ_s is the set of vectors $(\lambda_1, \dots, \lambda_n) \in \mathbb{Z}^n$ such that $k \leqslant \leqslant \lambda_1, \dots, \lambda_n \leqslant 2k-1$ and $\gcd(\lambda_1, \lambda_2) = s$, so that $\Lambda_1 = \Lambda$. Note that the set $\cup_{s=1}^{2k-1} \Lambda_s$ contains precisely k^n elements. Furthermore, since the first two entries of every $\bar{\lambda} \in \Lambda_s$ are divisible by s, we can bound

$$|\Lambda_s| \leqslant ([(2k-1)/s] - [(k-1)/s])^2 k^{n-2} < (1/s + 1/k)^2 k^n.$$

It follows that

$$|\Lambda_1| \geqslant k^n - \sum_{s=2}^{2k-1} |\Lambda_s| > k^n - \sum_{s=2}^{2k-1} (1/s + 1/k)^2 k^n.$$

Since $\lim\limits_{k \to \infty} \sum\limits_{s=2}^{2k-1} (1/s + 1/k)^2 = \pi^2/6 - 1$, we have that

$$|\Lambda| = |\Lambda_1| > k^n/3 > (1/6n) D^{n/(n+1)}$$

for D sufficiently large. This yields (4):

$$\log |P(1, \dots, 1)| > |\Lambda| \log 2 > (1/9n) D^{n/(n+1)}.$$

Now, we will show that $M(P) = p = 1 + \ell + r$, where p is greater than or equal to D/n. Since

$$\ell + 1 \leqslant (2k-1)\, k^n \leqslant 2k^{n+1} - 1 \leqslant D/n - 1\,,$$

$r \in \mathbb{N}$ satisfying $r = p - 1 - \ell$ exists for every integer $p \geqslant D/n$. The degree of the polynomial

$$G(x_1, \ldots, x_n) = x_1^r (1 + x_1 x_2^{D-q-1})\, Q(x_1, \ldots, x_n)$$

in the variable x_1 is equal to p. It is easily seen that, for each choice of $x_2 = e^{2\pi i t_2}, \ldots, x_n = e^{2\pi i t_n}$ on the unit disc, $G(x_1, e^{2\pi i t_2}, \ldots, e^{2\pi i t_n})$ has its roots in the unit circle. By the theorem of Lucas claiming that the smallest closed convex set containing all zeros of a polynomial (in one variable) also contains all the zeros of the derivative of the polynomial, we have that the roots of $R(x_1) = \partial G(x_1, e^{2\pi i t_2}, \ldots, e^{2\pi i t_n})/\partial x_1$ are all in the unit circle. Since the leading coefficient of R equals p, we obtain that $M(R) = p$. This equality can be written in form

$$\int_0^1 \log |R(e^{2\pi i t}, e^{2\pi i t_2}, \ldots, e^{2\pi i t_n})|\, dt = \log p\,,$$

where $t_2, \ldots, t_n$ are arbitrary fixed real numbers. We may now integrate $n-1$ times over $t_2, \ldots, t_n$ in $[0, 1]$. This will not change the right-hand side, $\log p$, whereas on the left-hand side we will get $\log M(\partial G/\partial x_1)$, where $\partial G/\partial x_1$ is considered as a polynomial in n variables. Consequently, $M(\partial G/\partial x_1) = p$ and, by (5),

$$M(P) = M(P)\, M(x_1^{r-1}) = M(\partial G/\partial x_1) = p\,.$$

Alternatively, by Exercise 3.2 in [11] and because $M(G) = 1$,

$$M(\partial G/\partial x_1) \leqslant p M(G) = p\,.$$

On the other hand, writing $\partial G(x_1, \ldots, x_n)/\partial x_1$ in the form

$$\partial G(x_1, \ldots, x_n)/\partial x_1 = p x_1^{p-1} x_2^{u_2} \ldots x_n^{u_n} + \ldots + r x_1^{r-1} \tag{6}$$

and using precisely the same argument as in Lemma 3.7 of [11], i.e. expressing the quantity $\log M(\partial G/\partial x_1)$ as $\log M(p x_2^{u_2} \ldots x_n^{u_n}) = \log p$ plus a non-negative term, we obtain that $M(\partial G/\partial x_1) \geqslant p$. Combining upper and lower bounds for the same quantity yields $M(\partial G/\partial x_1) = p$. As above, this leads to $M(P) = p$.

REMARK. Mahler's inequality [12] $M(G')/M(G) \leqslant \deg G$, where G is an arbitrary complex polynomial in one variable was also posed as a problem by Vaaler in the Problems section of the American Mathematical Monthly and solved by Boyd using an elementary theorem of Bernstein (Advanced Problem 6613, Amer. Math. Monthly **98**, 451-452 (1991)).

3. Irreducibility of P.

By (6) we write

$$P(x_1, \dots, x_n) = px_1^{\ell+1} x_2^{u_2} \dots x_n^{u_n} + \sum_{j=1}^{\ell} x_1^j f_j(x_2, \dots, x_n) + r,$$

where $f_j \in \mathbb{Z}[x_2, \dots, x_n]$. Assume that P is reducible in $\mathbb{Z}[x_1, \dots, x_n]$. Since p is a prime number, one of the factors of P written as a polynomial in x_1 must have the leading coefficient equal to $x_2^{v_2} \dots x_n^{v_n}$ and the constant term equal to a non-zero integer r'. (Here, $v_2 \leqslant u_2, \dots, v_n \leqslant u_n$ are non-negative integers and $r' \mid r$.) Thus, for each choice of $x_2, \dots, x_n$ with $|x_2| = \dots = |x_n| = 1$, this polynomial (and so P itself as a polynomial in x_1) must have a root whose absolute value is greater than or equal to 1. However, by choosing certain $x_j = e^{2\pi i\theta_j}$, $j = 2, \dots, n$, we will prove that the polynomial $P(x_1, e^{2\pi i\theta_2}, \dots, e^{2\pi i\theta_n})$ has no such roots. Here, $\theta_2, \dots, \theta_n$ are some fixed positive numbers such that the collection $1, \theta_2, \dots, \theta_n$ is linearly independent over $\mathbb{Q}$. For instance, one can take $\theta_j = \sqrt{p_{j-1}}$, where $p_1 = 2 < p_2 = 3 < p_3 = 5 < \dots$ is the set of prime numbers.

It remains to prove that all $\ell + 1$ roots of the polynomial

$$T(x_1) = (1 + x_1 e^{2(D-q-1)\pi i\theta_2}) \prod_{\vec{\lambda} \in \Lambda} (1 + x_1^{\lambda_1} e^{2\pi i(\lambda_2\theta_2 + \dots + \lambda_n\theta_n)})$$

are distinct. Indeed, they all lie on the unit circle and the fact that the polynomial $P(x_1, e^{2\pi i\theta_2}, \dots, e^{2\pi i\theta_n})$ has all of its roots lying in $|x_1| < 1$ will follow by (5) and by the theorem of Lucas mentioned above.

We see at once that the root $x_1 = e^{-2(D-q-1)\pi i\theta_2}$ of T is simple, because the numbers $1, \theta_2, \dots, \theta_n$ are linearly independent over $\mathbb{Q}$. Clearly, all λ_1 roots of $1 + x_1^{\lambda_1} e^{2\pi i(\lambda_2\theta_2 + \dots + \lambda_n\theta_n)}$ are distinct, so these factors also have no multiple roots.

The only possibility left is that the factors $1 + x_1^{\lambda_1} e^{2\pi i(\lambda_2\theta_2 + \dots + \lambda_n\theta_n)}$ and $1 + x_1^{\mu_1} e^{2\pi i(\mu_2\theta_2 + \dots + \mu_n\theta_n)}$, where $(\lambda_1, \dots, \lambda_n) \neq (\mu_1, \dots, \mu_n)$, share a common root, say $x_1 = y$. Then $y^{\lambda_1 - \mu_1}$ is equal to $e^{-2\pi i\mu_1(\lambda_2\theta_2 + \dots + \lambda_n\theta_n)}$ and

at the same time $y^{\lambda_1\mu_1} = e^{-2\pi i\lambda_1(\mu_2\theta_2 + \ldots + \mu_n\theta_n)}$. The equality of these exponents holds if their arguments differ by $2\pi iv$ with $v \in \mathbb{Z}$. But the numbers $1, \theta_2, \ldots, \theta_n$ are $\mathbb{Q}$-linearly independent, so this is only possible if $\mu_1\lambda_j = \lambda_1\mu_j$ for every $j = 2, \ldots, n$. In particular, this implies that $\mu_1\lambda_2 = \lambda_1\mu_2$. However, $\gcd(\lambda_1, \lambda_2) = 1$, hence λ_1 divides μ_1. Since $k \leqslant \lambda_1$, $\mu_1 \leqslant 2k-1$, this can only happen if $\lambda_1 = \mu_1$. From the equalities $\mu_1\lambda_j = \lambda_1\mu_j$ we conclude that $\lambda_j = \mu_j$ for every $j = 1, 2, \ldots, n$, a contradiction. This, combined with all said above, implies that T is a separable polynomial and completes the proof of the theorem.

We remark that by splitting $x_1^{\lambda_1}\ldots x_n^{\lambda_n}$ into two «nearly equal» parts $x_1^{\lambda_1}\ldots x_m^{\lambda_m}$ and $x_{m+1}^{\lambda_{m+1}}\ldots x_n^{\lambda_n}$, where $m = [n/2]$, one can consider $\prod(x_1^{\lambda_1}\ldots x_m^{\lambda_m} + x_{m+1}^{\lambda_{m+1}}\ldots x_n^{\lambda_n})$ instead of Q. Having this product in place of Q in the definition of P and slightly modifying the definition of Λ and finding its cardinality asymptotically, one can replace the constant 9 in (4) by a smaller constant. However, similarly to the case $n = 1$, there is still a logarithmic gap between upper bound (2) and the example of the theorem.

This research was partially supported by a grant from Lithuanian Foundation of Studies and Science.

REFERENCES

[1] F. AMOROSO, *Sur des polynômes de petites mesures de Mahler*, C. R. Acad. Sci. Paris, **321** (1995), pp. 11-14.

[2] F. AMOROSO, *Algebraic numbers close to 1 and variants of Mahler's measure*, J. Number Theory, **60** (1996), pp. 80-96.

[3] F. AMOROSO, *Algebraic numbers close to 1: results and methods*, in: Number Theory, Tiruchirapalli, 1996 (V.K. Murthy, M. Waldschmidt eds.), Contemporary Mathematics **210**, Amer. Math. Soc., Providence, RI, 1998, pp. 305-316.

[4] F. AMOROSO, *Upper bounds for the resultant and diophantine applications*, in: Number Theory: Diophantine, Computational and Algebraic Aspects, Eger, 1996 (K. Győry, A. Pethö, V.T. Sós eds.), Walter de Gruyter, Berlin, 1998, pp. 23-36.

[5] F. AMOROSO - S. DAVID, *Minoration de la hauteur normalisée des hypersurfaces*, Acta Arith., **92** (2000), pp. 339-366.

[6] F. AMOROSO - M. MIGNOTTE, *Upper bounds for the coefficients of irreducible integer polynomials in several variables*, Acta Arith., **99** (2001), pp. 1-12.

[7] Y. BUGEAUD, *Algebraic numbers close to 1 in non-archimedean metrics*, The Ramanujan J., **2** (1998), pp. 449-457.

[8] A. DUBICKAS, *On algebraic numbers close to 1*, Bull. Australian Math. Soc., **58** (1998), pp. 423-434.
[9] A. DUBICKAS, *On certain geometric mean of the values of a polynomial*, Liet. Matem. Rink., **40** (2000), pp. 17-27.
[10] A. DUBICKAS, *Three problems for polynomials of small measure, Acta Arith.*, **98** (2001), pp. 279-292.
[11] G. EVEREST - T. WARD, *Heights of polynomials and entropy in algebraic dynamics*, London, Springer, 1999.
[12] K. MAHLER, *On the zeros of the derivative of a polynomial*, Proc. Roy. Soc. London, Ser. A, **264** (1961), pp. 145-154.
[13] M. MIGNOTTE, *On algebraic integers of small measure*, Colloq. Math. Soc. János Bolyai, **34** (1981), pp. 1069-1077.
[14] M. MIGNOTTE, *An inequality about irreducible factors of integer polynomials*, J. Number Theory, **30** (1988), pp. 156-166.
[15] M. MIGNOTTE - M. WALDSCHMIDT, *On algebraic numbers of small height: linear forms in one logarithm*, J. Number Theory, **47** (1994), pp. 43-62.
[16] A. SCHINZEL, *Polynomials with special regard to reducibility*, Encyclopedia of Mathematics and Its Applications **77**, Cambridge, Cambridge University Press, 2000.
[17] W. SCHMIDT, *Diophantine approximation*, Lecture Notes in Mathematics **785**, Berlin-Heidelberg-New York, Springer, 1980.

Manoscritto pervenuto in redazione il 16 aprile 2004.