ACTA ARITHMETICA
XCIX.1 (2001)

Upper bounds for the coefficients of irreducible integer polynomials in several variables

by

Francesco Amoroso (Caen) and Maurice Mignotte (Strasbourg)

1. Introduction. Let $P(\mathbf{X}) = P(X_1, \dots, X_n)$ be a polynomial over $\mathbb{C}$ in n variables. There are several measures for the growth of the coefficients of P, for instance: the "naive" height $H(P)$ (maximum modulus of the coefficients), the length $L(P)$ (sum of the absolute values of the coefficients), the euclidean norm $\|P\|$ (quadratic mean of the absolute values of the coefficients) and the maximum modulus $|P|$ over the polydisk $|z_1| = \dots = |z_n| = 1$. They are all equivalent up to a multiplicative factor which grows polynomially in the total degree $\deg P$ of the polynomial. More precisely, we have

$$H(P) \le \|P\| \le |P| \le L(P) \le \binom{\deg P + n}{n} H(P).$$

Let us introduce the *Mahler measure* $M(P)$ by the analytic formula

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

From this formula, we obtain (see [M2], Theorem 4.4 bis, for details)

$$M(P) \le \|P\|.$$

In the opposite direction, since the coefficient of the monomial $X_1^{\lambda_1} \dots X_n^{\lambda_n}$ of P is bounded by $\frac{(\deg P)!}{\lambda_1! \dots \lambda_n!} \cdot M(P)$ (see for instance [P], Lemme 1.13), we have

$$L(P) \le (n+1)^{\deg P} \cdot M(P).$$

For further references we also notice the upper bound

$$L(P) \le 2^{\deg_1 P + \dots + \deg_n P} \cdot M(P)$$

(see again [M2], Theorem 4.4 bis), where $\deg_i P = \deg_{X_i} P$ is the partial degree of P relative to X_i.

2000 *Mathematics Subject Classification*: Primary 11G50; Secondary 11J25, 26C05.

We are interested in relations between the Mahler measure and the maximum modulus of a polynomial. From the above discussion we obtain

$$M(P) \le |P| \le (n+1)^{\deg P} \cdot M(P). \tag{1}$$

These inequalities are clearly sharp when the degree is fixed and $M(P)$ grows to infinity. Moreover, the upper bound for $|P|$ is also sharp, except perhaps for the constant $n+1$, for *general polynomials* when $M(P)$ is bounded and $\deg P$ tends to infinity. To see this, consider, for a fixed multi-index $(\lambda_1, \dots, \lambda_n)$, the polynomials

$$P = (1 - X_1^{\lambda_1} \dots X_n^{\lambda_n})^D$$

having Mahler's measure 1 and maximum modulus 2^D. However, in the one-dimensional case the second author sharpened the upper bound (1) when P is an irreducible polynomial with integer coefficients having small Mahler's measure. As a special case of this result, we have (see [M1], Theorem 1)

$$\|P\| \le e^{\sqrt{D}}(D + 2\sqrt{D} + 2)^{1+\sqrt{D}} M(P)^{1+\sqrt{D}}$$

if $P \in \mathbb{Z}[X]$ is irreducible of degree D.

The aim of this paper is to generalize Mignotte's result to several variables. Our main inequality (Theorem 1) is rather technical; hence we prefer to state here a simpler result (see §4 for the proof):

Corollary 1. *Let P be an irreducible polynomial in n variables with integer coefficients and of degree D. Then*

$$|P| \le ((n+2)^3 D^3 M(P))^{2D^{n/(n+1)}}.$$

As in [M1], we can deduce from this upper bound an estimate for the coefficients of an irreducible factor of a multivariate integer polynomial. Let F be a nonzero polynomial in n variables with integer coefficients and let P be an irreducible factor of F of degree D. Then, since $M(P) \le M(F)$,

$$|P| \le ((n+2)^3 D^3 M(F))^{2D^{n/(n+1)}}.$$

Corollary 1 also has some applications in Diophantine analysis. Consider for instance the classical Liouville inequality. Let $P \in \mathbb{Z}[X_1, \dots, X_n]$ be of partial degrees $D_j = \deg_j P$ and let $\alpha_1, \dots, \alpha_n \in \overline{\mathbb{Q}}^*$ be such that $P(\alpha_1, \dots, \alpha_n) \neq 0$. Put $d = [\mathbb{Q}(\alpha_1, \dots, \alpha_n) : \mathbb{Q}]$ and let $M(\alpha_j)$ be the Mahler measure of α_j (i.e. the Mahler measure of the minimal equation of α_j over the integers) and d_j be its degree. Then (see for instance [MW], Lemma 5)

$$|P(\alpha_1, \dots, \alpha_n)| \ge L(P)^{-d+1} M(\alpha_1)^{-D_1 d/d_1} \dots M(\alpha_n)^{-D_n d/d_n}.$$

In the previous lower bound, it can be useful to have a dependence in terms of the Mahler measure of P instead of its length. To do this we may use the inequality $L(P) \le (n+1)^{\deg P} \cdot M(P)$, but then an extra factor

$(n+1)^{(-d+1)\deg P}$ will appear in the right hand side. Using Corollary 1, we obtain (see §4 for the proof):

COROLLARY 2. *Let $P \in \mathbb{Z}[\mathbf{X}]$ be an irreducible polynomial of partial degrees $D_1, \dots, D_n$ and of total degree D. Let also $\alpha_1, \dots, \alpha_n$ be nonzero algebraic numbers such that $P(\alpha_1, \dots, \alpha_n) \neq 0$. Then*

$$|P(\alpha_1, \dots, \alpha_n)| \geq ((n+2)^3 D^3 M(P))^{-2(d-1)D^{n/(n+1)}} M(\alpha_1)^{-D_1 d/d_1} \dots M(\alpha_n)^{-D_n d/d_n},$$

where $d = [\mathbb{Q}(\alpha_1, \dots, \alpha_n) : \mathbb{Q}]$ and $d_j = [\mathbb{Q}(\alpha_j) : \mathbb{Q}]$ for $j = 1, \dots, n$.

The proof of Theorem 1 (§4) is a natural extension of the proof of [M1]. The main ingredients are an inequality on the size of the factors of multivariate polynomials (§2) and a generalization of Siegel's lemma proved in [AD] (see §3). We also show (§5) that our results are essentially sharp. A generalization to several variables of a well known algorithm for the computation of the Mahler measure (§6) finishes this paper.

Acknowledgements. The authors are indebted to the referee for his interesting comments. The remark that follows the proof of Proposition 1 is due to the referee and also the first one after the proof of Theorem 1 is inspired by the referee's report.

2. Size of factors. The aim of this section is to generalize an inequality on the size of the factors of univariate polynomials due to the second author (see [M1], Theorem 3). We first recall this inequality and, for the reader's convenience, its proof.

PROPOSITION 1. *Let $P, Q \in \mathbb{C}[X]$ be nonzero polynomials with $\deg P = D$ and $\deg Q = d$. Then* [1]

$$|P| \cdot M(Q) \leq \frac{(D+d)^{D+d}}{D^D d^d} \cdot |P \cdot Q|.$$

Proof. We can assume $D, d \geq 1$ (otherwise the result is trivial). Recall that the Blaschke factor associated with a nonzero complex number α is

$$B_\alpha(z) = \frac{\overline{\alpha} z - 1}{z - \alpha}.$$

Also notice that $B_\alpha(z)$ has modulus 1 when $|z| = 1$. Define

$$\widetilde{Q} = Q(X) \cdot \prod_{\substack{\alpha;\, Q(\alpha)=0 \\ |\alpha|>1}} B_\alpha(X)$$

[1] With the convention $0^0 = 1$.

and $\widetilde{F} = P \cdot \widetilde{Q}$. By the maximum principle and by the definition of $\widetilde{Q}$, we have, for any $R > 1$,

$$|P| = \left|\frac{\widetilde{F}}{\widetilde{Q}}\right| \le \left|\frac{\widetilde{F}}{\widetilde{Q}}\right|_R \le \frac{|\widetilde{F}|R^{D+d}}{|b|(R-1)^d},$$

where b is the leading coefficient of $\widetilde{Q}$, hence $b = M(Q)$. Notice also that $|\widetilde{F}| = |P \cdot Q|$ by the above property of Blaschke factors. To conclude, choose $R = 1 + d/D$. ∎

Remark. As noticed by the referee, the inequality of Proposition 1 can be reformulated as follows. Define $\alpha : [0,1] \to [0,+\infty)$ by $\alpha(0) = \alpha(1) = 0$ and $\alpha(x) = -x\log x - (1-x)\log(1-x)$ for $x \in (0,1)$. Then $\alpha(x)$ is easily seen to be nonnegative, positive on the open interval $(0,1)$ and concave. Also define $\beta : [0,1] \to [0,+\infty)$ by $\beta(x) = x\log 2$. Then the bound in Proposition 1 can be written as

$$|P| \cdot M(Q) \le \exp\{(D+d)\alpha(\theta)\} \cdot |P \cdot Q|, \quad \text{where} \quad \theta = \frac{D}{D+d}.$$

And the basic inequality (1) (in case $n = 1$) is

$$|P| \cdot M(Q) \le \exp\{(D+d)\beta(\theta)\} \cdot |P \cdot Q|.$$

Plainly, these can be combined as

$$|P| \cdot M(Q) \le \exp\{(D+d)\min\{\alpha(\theta), \beta(\theta)\}\} \cdot |P \cdot Q|,$$

and the unique solution to $\alpha(x) = \beta(x)$ in $(0,1)$ determines when the bound of Proposition 1 is sharper than (1). It would be of considerable interest to replace $\min\{\alpha(\theta), \beta(\theta)\}$ by some more natural smooth function of the parameter θ.

From Proposition 1 we obtain, by induction:

Proposition 2. *Let P, $Q \in \mathbb{C}[\mathbf{X}]$ be nonzero polynomials. Put $D_j := \deg_j P$ for $j = 1, \dots, n$. Let also $qX_1^{d_1} \dots X_n^{d_n}$ be the monomial of Q for which $(d_1, \dots, d_n)$ is maximal with respect to the anti-lexicographic order, among the exponent vectors of all monomials appearing with nonzero coefficients in Q. Then*

$$|P| \cdot |q| \le \frac{(D_1+d_1)^{D_1+d_1}}{D_1^{D_1} d_1^{d_1}} \cdots \frac{(D_n+d_n)^{D_n+d_n}}{D_n^{D_n} d_n^{d_n}} \cdot |P \cdot Q|.$$

Proof. We write

$$Q(X_1, \dots, X_n) = Q_1(X_1, \dots, X_{n-1}) X_n^{d_n} + \text{lower order terms (with respect to } X_n).$$

Let $z_1, \ldots, z_{n-1}$ be arbitrary complex numbers and apply Proposition 1 to the univariate polynomial

$$F_0(X) = P(z_1, \ldots, z_{n-1}, X) \cdot Q(z_1, \ldots, z_{n-1}, X).$$

We obtain

$$|P(z_1, \ldots, z_{n-1}, X) \cdot Q_1(z_1, \ldots, z_{n-1})| \leq \frac{(D_n + d_n)^{D_n + d_n}}{D_n^{D_n} d_n^{d_n}} \cdot |F_0|,$$

where we have used the fact that the absolute value of the leading coefficient of a univariate polynomial is bounded by its measure. Since the previous inequality is true for any complex numbers $z_1, \ldots, z_{n-1}$ of modulus 1 and since $|F_0| \leq |P \cdot Q|$, we have

$$|P \cdot Q_1| \leq \frac{(D_n + d_n)^{D_n + d_n}}{D_n^{D_n} d_n^{d_n}} \cdot |P \cdot Q|. \tag{2}$$

Now write

$$Q_1(X_1, \ldots, X_{n-1}) = Q_2(X_1, \ldots, X_{n-2}) X_{n-1}^{d_{n-1}} + \text{lower order terms (with respect to } X_{n-1}).$$

Let $z_1, \ldots, z_{n-2}$, z_n be arbitrary complex numbers and apply Proposition 1 to the univariate polynomial

$$F_1(X) = P(z_1, \ldots, z_{n-2}, X, z_n) \cdot Q_1(z_1, \ldots, z_{n-2}, X).$$

As before, we obtain

$$|P(z_1, \ldots, z_{n-2}, X_{n-1}, z_n) \cdot Q_2(z_1, \ldots, z_{n-2})| \leq \frac{(D_{n-1} + d_{n-1})^{D_{n-1} + d_{n-1}}}{D_{n-1}^{D_{n-1}} d_{n-1}^{d_{n-1}}} \cdot |F_1|.$$

Hence, using inequality (2) gives

$$|P \cdot Q_2| \leq \frac{(D_{n-1} + d_{n-1})^{D_{n-1} + d_{n-1}}}{D_{n-1}^{D_{n-1}} d_{n-1}^{d_{n-1}}} \cdot \frac{(D_n + d_n)^{D_n + d_n}}{D_n^{D_n} d_n^{d_n}} \cdot |P \cdot Q|.$$

After n steps, we get the announced upper bound for the product $|P| \cdot |q|$. ∎

In particular, we have

COROLLARY 3. *Let $P \in \mathbb{C}[\mathbf{X}]$ and $Q \in \mathbb{Z}[\mathbf{X}]$ be nonzero polynomials. Let d, D be two integers with $D \geq \max_j \deg_j P$ and $d \geq \deg Q$. Then*

$$|P| \leq e^d (1 + D)^d \cdot |P \cdot Q|.$$

Proof. We apply Proposition 2, using the inequalities $|q| \geq 1$,

$$\frac{(x+y)^{x+y}}{x^x y^y} = \left(1 + \frac{y}{x}\right)^x \cdot \left(1 + \frac{x}{y}\right)^y \leq e^y (1 + x)^y$$

(valid for reals $x > 0$ and $y \geq 1$), and $d_1 + \ldots + d_n \leq d$. ∎

3. A generalization of Siegel's lemma. We shall need a generalization of Siegel's lemma for univariate polynomials to the multivariate case, due to the first author and S. David (indeed the quoted result is more general but for our purposes we only need a special case).

We denote by $h(F)$ the *Weil height* of the polynomial $F \in \overline{\mathbb{Q}}[\mathbf{X}]$, i.e. the Weil height of the vector of the coefficients of P in a suitable projective space.

PROPOSITION 3. *Let $P \in \mathbb{Z}[\mathbf{X}]$ be an irreducible polynomial of total degree D and let T, L be integers such that $L \geq TD$. Then there exists a nonzero polynomial $F \in \mathbb{Z}[\mathbf{X}]$ of degree $\leq L$ which is a multiple of P^T and such that*

$$h(F) \leq \left(\left(\frac{L+1}{L-TD+1} \right)^n - 1 \right) \cdot \left\{ (n+T)\log(L+1) + \frac{L}{D} \log M(P) \right\}.$$

Proof. Let $N = \binom{L+n}{n}$ and let

$$r = H(({}^{\mathrm{h}}P^T); L) = \binom{L+n}{n} - \binom{L-TD+n}{n}$$

be the value at L of the Hilbert function of the principal ideal generated by the homogenization ${}^{\mathrm{h}}P^T \in \mathbb{Z}[X_0, \ldots, X_n]$ of P^T. We apply Théorème 4.1 of [AD] to the hypersurface

$$V = \{P = 0\} \subset \mathbb{G}_m^n \subset \mathbb{P}^n.$$

Let $V(\theta)$ be the set of points of $V(\overline{\mathbb{Q}}) \subset \mathbb{P}^n(\overline{\mathbb{Q}})$ having Weil's height $\leq \theta$. We define the *essential minimum* $\widehat{\mu}_{\mathrm{ess}}(V)$ of V as the infimum of the set of $\theta > 0$ such that $V(\theta)$ is Zariski-dense in V. Then the quoted result of [AD] gives at once a nonzero polynomial $F \in \mathbb{Z}[\mathbf{X}]$ of degree $\leq L$ which vanishes on V with multiplicity $\geq T$ (hence P^T divides F) and has

$$h(F) \leq \frac{r}{N-r} \{(n+T)\log(L+1) + L\widehat{\mu}_{\mathrm{ess}}(V)\}.$$

We now notice that

$$\widehat{\mu}_{\mathrm{ess}}(V) \leq \frac{1}{D} \log M(P)$$

by a particular case of a theorem of Zhang (for an elementary proof of this inequality, see also [AD], Proposition 2.7). Finally, to simplify the upper bound for $h(F)$, we use the inequality

$$\frac{r}{N-r} = \frac{(L+n)\ldots(L+1)}{(L-TD+n)\ldots(L-TD+1)} - 1 \leq \left(\frac{L+1}{L-TD+1} \right)^n - 1. \quad \blacksquare$$

4. Upper bounds for the coefficients. Combining Proposition 3 and Corollary 3, we find the following general upper bound for the maximum modulus:

THEOREM 1. *Let P be an irreducible polynomial in n variables with integer coefficients and of degree at most D. Then, for any positive number x, we have*

$$\log|P| \le x\log(e(D+1)) + \left(1+\frac{D}{x}\right)^n \cdot \left\{(n+1)\log(D+x+1) + \left(1+\frac{x}{D}\right)\log M(P)\right\}.$$

Proof. We apply Proposition 3 choosing $T = 1$ and $L = D + d$, with $d = [x]$. Since $\log|F| \le h(F) + n\log(L+1)$, we have

$$\begin{aligned}\log|F| &\le \left(1+\frac{D}{d+1}\right)^n \cdot \left\{(n+1)\log(D+d+1) + \left(1+\frac{d}{D}\right)\log M(P)\right\} \\ &\le \left(1+\frac{D}{x}\right)^n \cdot \left\{(n+1)\log(D+x+1) + \left(1+\frac{x}{D}\right)\log M(P)\right\}.\end{aligned}$$

Now, by Corollary 3,

$$\begin{aligned}\log|P| &\le d\log(e(D+1)) + \log|F| \\ &\le x\log(e(D+1)) \\ &\quad + \left(1+\frac{D}{x}\right)^n \cdot \left\{(n+1)\log(D+x+1) + \left(1+\frac{x}{D}\right)\log M(P)\right\}. \ \blacksquare\end{aligned}$$

REMARKS. As suggested by the referee, we could prove an apparently more general result without choosing $T = 1$ at the beginning of the previous proof. More precisely, using Proposition 3 we can find a multiple of P^T of degree $\le L = TD + d$. Then, using the more precise bound for the factors given by Proposition 2 instead of Corollary 3, we obtain an upper bound for $|P^T| = |P|^T$. In this way, we can prove an inequality of the shape $\log|P| \le f(T,d)$, where

$$\begin{aligned}f(T,d) &= nD\log\left(1+\frac{d}{TD}\right) + \frac{nd}{T}\log\left(1+\frac{TD}{d}\right) \\ &\quad + \left(1+\frac{TD}{d}\right)^n \cdot \left\{(n+T)\log(TD+d+1) + \left(1+\frac{d}{TD}\right)\log M(P)\right\}.\end{aligned}$$

Both the integer parameters T and d are now at our disposal. Unfortunately, the optimal choice of T turns out to be $T = 1$. This is due to the term $\log(TD+d+1)$ in the last displayed formula, which comes from $\log(L+1)$ in Proposition 3. As noticed by the referee, this can be viewed as a signal that the argument used to obtain our main result is not the best possible. This phenomenon occurs very often in Diophantine's proofs (see, for instance, Dobrowolski's lower bound for the height).

We also notice that the main result of [M1] (Theorem 5) is just the special case $n = 1$ of Theorem 1, the proof of Theorem 1 being a natural extension of the proof of [M1]. One can also notice that the main result of

[M1] was extended to complex univariate polynomials in [A3] (under some hypothesis on the discriminant). It is an interesting open problem to extend Theorem 1 to complex polynomials (under suitable hypotheses).

Proof of Corollary 1. Assume first $D \le D_0 := (n+1)^{n+3}$ and consider the function

$$f(t) = \log((n+1)t) - t^{1/(n+1)} \log(n+1).$$

By standard analysis, we see that $\min_{t\in[1,D_0]} f(t) = \min\{f(1), f(D_0)\}$. Since $f(1) = 0$ and

$$f(D_0) = ((n+4) - (n+1)^{(n+3)/(n+1)}) \log(n+1) > 0,$$

we have

$$(n+1)^D \le ((n+1)D)^{D^{n/(n+1)}}$$

for $D \le D_0$. Hence, in this range, Corollary 1 follows directly from the inequality $L(P) \le (n+1)^D M(P)$. Assume now $D > D_0$ and choose

$$x = (n+1)^{1/(n+1)} D^{n/(n+1)}$$

in Theorem 1. Since $D > D_0$ we have

$$x \le (n+1)^{-(n+2)/(n+1)} D \le D - 1.$$

Hence $\log(D+x+1) \le \log(2D)$ and

$$1 + x/D \le 1 + (n+1)^{-(n+2)/(n+1)},$$

$$1 + \frac{D}{x} = \left(1 + \frac{x}{D}\right)\frac{D}{x} \le (1 + (n+1)^{-(n+2)/(n+1)})(n+1)^{-1/(n+1)} D^{1/(n+1)}.$$

Therefore

$$\begin{aligned}(3)\qquad (n+1)&\left(1 + \frac{D}{x}\right)^n \log(D+x+1)\\ &\le (1 + (n+1)^{-(n+2)/(n+1)})^n (n+1)^{1/(n+1)} D^{n/(n+1)} \log(2D)\\ &\le e D^{n/(n+1)} \log((n+2)D)\end{aligned}$$

and

$$\begin{aligned}(4)\qquad &\left(1 + \frac{D}{x}\right)^n \left(1 + \frac{x}{D}\right) \log M(P)\\ &\le (1 + (n+1)^{-(n+2)/(n+1)})^{n+1} (n+1)^{-n/(n+1)} D^{n/(n+1)} \log M(P)\\ &\le 2D^{n/(n+1)} \log M(P).\end{aligned}$$

Moreover, since $D_0 \ge 10$, we also have

$$\begin{aligned}(5)\qquad x \log(e(D+1)) &\le (n+1)^{1/(n+1)} D^{n/(n+1)} \log(3D)\\ &\le 2D^{n/(n+1)}((n+2)D).\end{aligned}$$

Using inequalities (3)–(5) in Theorem 1, we obtain

$$\log|P| \le 6D^{n/(n+1)}\log((n+2)D) + 2D^{n/(n+1)}\log M(P). \ \blacksquare$$

Proof of Corollary 2. Let $z_1,\dots,z_n \in \mathbb{C}$; applying the maximum principle to the polynomial

$$X_1^{D_1}\dots X_n^{D_n}P(X_1^{-1},\dots,X_n^{-1})$$

on the polydisk $X_1 = \max\{1,|z_1|\}$, …, $X_n = \max\{1,|z_n|\}$, we get

$$|P(z_1,\dots,z_n)| \le |P|\cdot\max\{1,|z_1|\}^{D_1}\dots\max\{1,|z_n|\}^{D_n}.$$

Hence, by standard arguments (see for instance [MW], Lemma 4),

$$|P(\alpha_1,\dots,\alpha_n)| \ge |P|^{-d+1}M(\alpha_1)^{-D_1 d/d_1}\dots M(\alpha_n)^{-D_n d/d_n}.$$

Now we apply Corollary 1 to get an upper bound for $|P|$. $\blacksquare$

The following result is sharper than Corollary 1 in the range

$$(3n)^{1+1/n} \le 1 + \frac{\log M(P)}{\log((n+2)D)} \le \frac{D}{4}.$$

Corollary 4. *Let P be an irreducible polynomial in n variables with integer coefficients and of degree at most D. Assume*

$$1 + \frac{\log M(P)}{\log((n+2)D)} \le \frac{D}{4}. \tag{6}$$

Then

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

Proof. To simplify the notations, put

$$c = 1 + \frac{\log M(P)}{\log((n+2)D)}$$

and choose $x = (n+1)c^{1/(n+1)}D^{n/(n+1)}$ in Theorem 2. By (6) we have $x \le (n+1)4^{-1/(n+1)}D \le nD$; hence

$$\log(D+x+1) \le \log((n+2)D), \qquad 1 + \frac{x}{D} \le n+1,$$

$$1 + \frac{D}{x} = \left(1+\frac{x}{D}\right)\frac{D}{x} \le c^{-1/(n+1)}D^{1/(n+1)}$$

and (notice that $e(1+D) \le 4D$ since $D \ge 4$) also

$$x\log(e(D+1)) \le (n+1)c^{1/(n+1)}D^{n/(n+1)}\log(4D).$$

Putting these inequalities in Theorem 1 we obtain the assertion. $\blacksquare$

5. Examples. Corollary 4 is sharp (except perhaps for a power of $\log D$) if $\log M(P) \ge D(\log((n+2)D))^{-c}$ with $c > 0$. In fact, for any polynomial

of degree D satisfying the previous inequality, we have

$$\log|P| \geq \log M(P) \geq \left(\frac{\log M(P)}{\log((n+2)D)}\right)^{1/(n+1)} D^{n/(n+1)} \log((n+2)D)^{(1-c)/(n+1)}.$$

In this section, using some ideas from [A2], §4, and from [D], §6 and §7, we construct a family of irreducible polynomials P_k ($k \in \mathbb{N}$) such that $\log M(P_k)$ is "small" and the upper bound for $|P_k|$ given by Corollary 3 is sharp (except perhaps for some power of $\log D$).

Consider the set

$$\Lambda_k = \{\boldsymbol{\lambda} = (\lambda_1, \ldots, \lambda_n) \in \mathbb{Z}^n : 0 \leq \lambda_j \leq k-1,\ j = 1, \ldots, n\}$$

of cardinality k^n. We fix an arbitrary total order $<$ on Λ_k and we introduce the polynomial

$$F_k(\mathbf{X}) = \mathrm{Det}((\mathbf{X}^{\boldsymbol{\lambda}})^j)_{\boldsymbol{\lambda}\in\Lambda_k;\, j=0,\ldots,k^n-1} = \prod_{\substack{\boldsymbol{\lambda},\boldsymbol{\mu}\in\Lambda \\ \boldsymbol{\mu}<\boldsymbol{\lambda}}} (\mathbf{X}^{\boldsymbol{\lambda}} - \mathbf{X}^{\boldsymbol{\mu}}),$$

where $\mathbf{X}^{\boldsymbol{\lambda}} = X_1^{\lambda_1} \ldots X_n^{\lambda_n}$. An easy computation shows that F_k has partial degree

$$\deg_j F_k = \frac{k^n(k-1)(4k^n + k^{n-1} - 3)}{12} \sim \frac{1}{3}k^{2n+1}.$$

Therefore $\deg F_k \lesssim (n/3)k^{2n+1}$. Moreover, by the Hadamard inequality,

$$|F_k| \leq k^{nk^n/2}.$$

We now fix a polynomial $A_k \in \mathbb{Z}[\mathbf{X}]$ of total degree $\deg A_k = \deg F_k$ and with coefficients $\in \{0, 1\}$, which is irreducible mod 2. Define

$$P_k(\mathbf{X}) := A_k(\mathbf{X}) + 2\,\frac{F_k(X_1^2, \ldots, X_n^2)}{F_k(X_1, \ldots, X_n)} = A_k(\mathbf{X}) + 2 \prod_{\substack{\boldsymbol{\lambda},\boldsymbol{\mu}\in\Lambda \\ \boldsymbol{\mu}<\boldsymbol{\lambda}}} (\mathbf{X}^{\boldsymbol{\lambda}} + \mathbf{X}^{\boldsymbol{\mu}}).$$

This polynomial is irreducible and

$$D_k := \deg P_k \lesssim \frac{n}{3}k^{2n+1}.$$

Moreover, since $M(F_k) = 1$ and $H(A_k) = 1$,

$$M(P_k) = M(A_k(\mathbf{X})F_k(\mathbf{X}) + 2F_k(X_1^2, \ldots, X_n^2)) \leq (|A_k| + 2)|F_k| \leq \left(2 + \binom{D_k + n}{n}\right) k^{nk^n/2}.$$

Therefore,

$$\log M(P_k) \lesssim \frac{n}{2}k^n \log k.$$

Corollary 4 gives the upper bound

$$\log|P_k| \le (n+1)\left(1+\frac{\log M(P_k)}{\log((n+2)D_k)}\right)^{1/(n+1)} D^{n/(n+1)}\log(4(n+2)D_k^2)$$
$$\lesssim 2(n+1)^3 k^{2n}\log k.$$

On the other hand, for large k,

$$\log|P_k| \ge \log|P_k(1,\dots,1)| \ge \log\left(2^{1+\frac{1}{2}k^n(k^n-1)} - \binom{D_k+n}{n}\right) \gtrsim \frac{\log 2}{2}k^{2n}.$$

REMARK. In [A1] there was exhibited a family of irreducible univariate polynomials $P_D(X) \in \mathbb{Z}[X]$ of degree at most D and Mahler's measure $\le \frac{1}{2}D^2$ such that

$$\log|P_D(1)| \gtrsim \sqrt{2D\log D}.$$

It would be nice to extend this construction to several variables.

6. Appendix: how to compute $M(P)$. As in the univariate case, the following algorithm is based on Graeffe's method.

Let $P(\mathbf{X})$ be a polynomial with complex coefficients. We define recursively $n+1$ polynomials $P_0, P_1, \dots, P_n \in \mathbb{C}[\mathbf{X}]$ as follows. We put $P_0 := P$. Let now j be an index with $1 \le j \le n$; write

$$P_{j-1}(\mathbf{X}) = A_j(X_1,\dots,X_{j-1},X_j^2,X_{j+1},\dots,X_n) + B_j(X_1,\dots,X_{j-1},X_j^2,X_{j+1},\dots,X_n)\cdot X_j$$

and define

$$P_j(\mathbf{X}) := A_j(\mathbf{X})^2 - B_j(\mathbf{X})^2\cdot X_j.$$

LEMMA 1. *We have* $\deg_i P_j \le 2\deg_i P_{j-1}$ *for* $i = 1,\dots,n$; *moreover* $\deg_j P_j = \deg_j P_{j-1}$. *We also have* $M(P_j) = M(P_{j-1})^2$.

Proof. The first two claims are obvious. In order to prove the third one, we remark that

$$P_j(X_1,\dots,X_{j-1},X_j^2,X_{j+1},\dots,X_n) = P_{j-1}(\mathbf{X})\cdot P_{j-1}(X_1,\dots,X_{j-1},-X_j,X_{j+1},\dots,X_n).$$

Therefore, by simple changes of variables in the integral defining the Mahler measure,

$$M(P_j) = M(P_j(X_1,\dots,X_{j-1},X_j^2,X_{j+1},\dots,X_n)) = M(P_{j-1})^2. \ \blacksquare$$

We now define a transformation $\tau : \mathbb{C}[\mathbf{X}] \to \mathbb{C}[\mathbf{X}]$ by putting $\tau P = P_n$. By the previous lemma we have

$$M(\tau P) = M(P)^{2^n}, \quad \deg_i(\tau P) \le 2^{n-1}\deg_i P \quad (i = 1,\dots,n).$$

Therefore, using the inequalities (see §1)

$$M(F) \le \|F\| \le 2^{\deg_1 F+\ldots+\deg_n F} \cdot M(F),$$

with $F = \tau^{(m)}P$, we obtain the following generalization of the main result of [CMP]:

PROPOSITION 4. *The real sequence* $\{\|\tau^{(m)}P\|^{2^{-n\cdot m}}\}_{m\in\mathbb{N}}$ *tends to* $M(P)$. *More precisely*,

$$M(P) \le \|\tau^{(m)}P\|^{2^{-n\cdot m}} \le 2^{2^{-m}\cdot(\deg_1 P+\ldots+\deg_n P)} \cdot M(P).$$

References

[A1] F. Amoroso, *Sur des polynômes de petites mesures de Mahler*, C. R. Acad. Sci. Paris Sér. I 321 (1995), 11–14.

[A2] —, *Algebraic numbers close to* 1: *results and methods*, in: Number Theory (Tiruchirapalli, 1996), Contemp. Math. 210, Amer. Math. Soc., Providence, RI, 1998, 305–316.

[A3] —, *Upper bounds for the resultant and diophantine applications*, in: Number Theory (Eger, 1996), de Gruyter, Berlin, 1998, 23–36.

[AD] F. Amoroso et S. David, *Minoration de la hauteur normalisée des hypersurfaces*, Acta Arith. 92 (2000), 339–366.

[CMP] L. Cerlienco, M. Mignotte and F. Piras, *Computing the measure of a polynomial*, J. Symbolic Comput. 4 (1987), 21–34.

[D] A. Dubickas, *On algebraic numbers close to* 1, Bull. Austral. Math. Soc. 58 (1998), 423–434.

[M1] M. Mignotte, *An inequality about irreducible factors of integer polynomials*, J. Number Theory 30 (1988), 156–166.

[M2] —, *Mathematics for Computer Algebra*, Springer, New York, 1992.

[MW] M. Mignotte and M. Waldschmidt, *On algebraic numbers of small height*: *Linear forms in one logarithm*, J. Number Theory 47 (1994), 43–62.

[P] P. Philippon, *Critères pour l'indépendance algébrique*, Inst. Hautes Etudes Sci. Publ. Math. 64 (1986), 5–52.

Département de Mathématiques
Université de Caen
Campus II, BP 5186
14032 Caen Cedex, France
E-mail: amoroso@math.unicaen.fr

Université Louis Pasteur, Strasbourg
7, rue Descartes
67084 Strasbourg, France
E-mail: mignotte@math.u-strasbg.fr

Received on 10.6.1999
and in revised form on 5.6.2000 (3618)