LEHMER'S PROBLEM FOR POLYNOMIALS WITH ODD COEFFICIENTS

Peter Borwein,
Edward Dobrowolski,
Kevin Hare
and Michael Mossinghoff

We prove that if $f(x) = \sum_{k=0}^{n-1} a_k x^k$ is a polynomial with no cyclotomic factors whose coefficients satisfy $a_k \equiv 1 \bmod 2$, then Mahler's measure of f satisfies

$$\log M(f) \geq \frac{\log 5}{4}\left(1 - \frac{1}{n}\right).$$

This resolves a problem of D. H. Lehmer for the class of polynomials with odd coefficients.

We also prove that if f has odd coefficients, degree $n-1$, and at least one noncyclotomic factor, then at least one root α of f satisfies

$$|\alpha| > 1 + \frac{\log 3}{2n},$$

resolving a conjecture of Schinzel and Zassenhaus for this class of polynomials.

Introduction

Mahler's measure of a polynomial f, denoted $M(f)$, is defined as

$$M(f) = |a| \prod_{k=1}^{d} \max\{1, |\alpha_k|\}. \qquad (1)$$

For $f \in \mathbf{Z}[x]$, clearly $M(f) \geq 1$, and by a classical theorem of Kronecker, $M(f) = 1$ precisely when $f(x)$ is a product of cyclotomic polynomials and the monomial x.

In 1933, D. H. Lehmer asked if for every $\epsilon > 0$ there exists a polynomial $f \in \mathbf{Z}[x]$ satisfying $1 < M(f) < 1 + \epsilon$.

This is known as *Lehmer's problem*. Lehmer noted that the polynomial

$$\ell(x) = x^{10} + x^9 - x^7 - x^6 - x^5 - x^4 - x^3 + x + 1$$

has $M(\ell) = 1.176280\ldots$, and this value remains the smallest known measure larger than 1 of a polynomial with integer coefficients.

Lehmer's problem has been solved for several special classes of polynomials.

Smyth shows that if $f \in \mathbf{Z}[x]$ is nonreciprocal and $f(0) \neq 0$, then

$$M(f) \geq M(x^3 - x - 1) = 1.324717\ldots.$$

Schinzel proves that if f is a monic, integer polynomial with degree d satisfying $f(0) = \pm 1$ and $f(\pm 1) \neq 0$, and all roots of f are real, then

$$M(f) \geq \gamma^{d/2}$$

where γ denotes the golden ratio, $\gamma := (1 + \sqrt{5})/2$.

The best general lower bound for Mahler's measure of an irreducible, noncyclotomic polynomial $f \in \mathbf{Z}[x]$ with degree d has the form

$$\log M(f) \gg \left(\frac{\log\log d}{\log d}\right)^3;$$

This is due to Dobrowolski.

We solve Lehmer's problem for the class of polynomials $\mathcal{D}_m$ polynomials whose coefficients are all congruent to 1 mod m,

$$\left\{\sum_{k=0}^{d} a_k x^k \in \mathbf{Z}[x] : a_k \equiv 1 \bmod m \text{ for } 0 \le k \le d\right\}. \tag{2}$$

We prove that if $f \in \mathcal{D}_m$ has degree $n-1$ and no cyclotomic factors, then

$$\log M(f) \ge c_m \left(1 - \frac{1}{n}\right),$$

with $c_2 = (\log 5)/4$ and

$$c_m = \log(\sqrt{m^2+1}/2)$$

for $m > 2$.

We provide in Theorem 1 a characterization of polynomials $f \in \mathbf{Z}[x]$ for which there exists a polynomial $F \in \mathcal{D}_p$ with $f \mid F$ and $M(f) = M(F)$, where p is a prime number.

We obtain a lower bound on a Salem number whose minimal polynomial lies in $\mathcal{D}_2$. This bound is slightly stronger than that obtained from our bound on Mahler's measure of a polynomial in this set.

The smallest Pisot number is the minimal value of Mahler's measure of a nonreciprocal polynomial, $M(x^3 - x - 1) = 1.324717\ldots$.

Previously we showed that the smallest measure of a nonreciprocal polynomial in $\mathcal{D}_2$ is the golden ratio, $M(x^2 - x - 1) = \gamma$, and therefore this value is the smallest Pisot number whose minimal polynomial lies in $\mathcal{D}_2$.

Salem proves that every Pisot number is a limit point, from both sides, of Salem numbers. We prove that the golden ratio is in fact a limit point, from both sides, of Salem numbers whose minimal polynomials are also in $\mathcal{D}_2$; in fact, they are Littlewood polynomials.

Factors of polynomials in $\mathcal{D}_p$

Let p be a prime number.

Lemma 1 *Suppose p is a prime number, and $n = p^k m$ with $p \nmid m$. Then*

$$x^n - 1 \equiv \prod_{d|m} \Phi_d^{p^k}(x) \mod p.$$

Cyclotomic polynomials whose indices are relatively prime and not divisible by p have no common factors in $\mathbf{F}_p[x]$.

Lemma 2 *Suppose m and n are distinct, relatively prime positive integers, and suppose p is a prime number that does not divide mn. Then $\Phi_n(x)$ and $\Phi_m(x)$ are relatively prime in $\mathbf{F}_p[x]$.*

Lemma 3 *Suppose $f(x) \in \mathbf{Z}[x]$ has degree $n-1$ and $\Phi_r \mid f$. If $f \in \mathcal{D}_2$, then $r \mid 2n$; if $f \in \mathcal{D}_p$ for an odd prime p, then $r \mid n$.*

We now have a simple characterization of polynomials $f \in \mathbf{Z}[x]$ that divide a polynomial with the same measure having all its coefficients congruent to 1 modulo p.

Theorem 1 *Let p be a prime number, and let $f(x)$ be a polynomial with integer coefficients.*

There exists a polynomial $F \in \mathcal{D}_p$ with $f \mid F$ and $M(f) = M(F)$ if and only if f is congruent modulo p to a product of cyclotomic polynomials.

This suggests an algorithm for determining if a given polynomial f with degree d divides a polynomial F in $\mathcal{D}_p$ with the same measure:

Construct all possible products of cyclotomic polynomials with degree d, and test if any of these are congruent to f mod p.

Using this strategy, we verify that none of the 100 smallest measure known irreducible, non-cyclotomic polynomials divides a Littlewood polynomial with the same measure.

This does not imply, however, that no Littlewood polynomials exist with these measures, since measures are not necessarily represented uniquely by irreducible integer polynomials, even discounting the simple symmetries.

Lemma 4 *Suppose $f \in \mathcal{D}_m$ with degree $n-1$, and let g be a factor of f. If* $\gcd(g(x), x^n - 1) = 1$, *then*

$$|\mathrm{Res}(g(x), x^n - 1)| \geq m^{\deg g}. \qquad (3)$$

Further, if $m = 2$, k is a nonnegative integer, and $\gcd(g(x), x^{n2^k} + 1) = 1$, *then*

$$\left|\mathrm{Res}(g(x), x^{n2^k} + 1)\right| \geq 2^{\deg g}. \qquad (4)$$

Proof Define the polynomial $s(x)$ by

$$ms(x) = (x^n - 1) + (1 - x)f(x), \qquad (5)$$

and note that $s(x) \in \mathbf{Z}[x]$ since $f \in \mathcal{D}_m$. If g has no common factor with $x^n - 1$, then $\gcd(g, s) = 1$, so $|\mathrm{Res}(g, s)| \geq 1$. Thus, computing the resultant of both sides of (5) with g we obtain (3).

Suppose $m = 2$. For $k \geq 0$, define the polynomial $t_k(x)$ by

$$2t_k(x) = (x^{n2^k} + 1) + (1 + x)f(x) \sum_{j=0}^{2^k-1} x^{jn},$$

and (4) follows by a similar argument.

Lemma 5 *For any polynomial $f \in \mathbf{C}[x]$, the value of $L(f^k)^{1/k}$ approaches $\|f\|_\infty$ from above as $k \to \infty$.*

For a polynomial $g \in \mathbf{Z}[x]$, let $\nu_k(g)$ denote the multiplicity of the cyclotomic polynomial $\Phi_{2^k}(x)$ in $g(x)$, and let $\nu(g) = \sum_{k \geq 0} \nu_k(g)$.

Theorem 2 *Suppose $f \in \mathcal{D}_m$ with degree $n-1$, and suppose $F \in \mathbf{Z}[x]$ satisfies*

$$\gcd(f(x), F(x^n)) = 1.$$

Then

$$\log M(f) \geq \begin{cases} \dfrac{\nu(F)\log 2 - \log\|F\|_\infty}{\deg F}\left(1 - \dfrac{1}{n}\right), & m = 2 \\ \dfrac{\nu_0(F)\log m - \log\|F\|_\infty}{\deg F}\left(1 - \dfrac{1}{n}\right), & m > 2. \end{cases}$$

This suggests looking for auxiliary polynomials F with high order divisibility by certain cyclotomic polynomials and with small norm on the disc.

Proof Suppose $m = 2$. Since $f(x)$ and $F(x^n)$ have no common factors, by Lemma 4 each cyclotomic factor Φ_{2^k} of F contributes a factor of 2^{n-1} to their resultant. Thus

$$|\mathrm{Res}(f(x), F(x^n))| \geq 2^{\nu(F)(n-1)}.$$

If α is a root of f, then

$$|F(\alpha^n)| \leq L(F) \max\left\{1, |\alpha|^{n \deg F}\right\},$$

so

$$|\mathrm{Res}(f(x), F(x^n))| \leq L(F)^{n-1} M(f)^{n \deg F}.$$

Therefore

$$2^{\nu(F)(n-1)} \leq L(F)^{n-1} M(f)^{n \deg F},$$

or

$$\log M(f) \geq \frac{\nu(F) \log 2 - \log L(F)}{\deg F} \left(1 - \frac{1}{n}\right). \tag{6}$$

Let k be a positive integer. Since $\nu(F^k) = k\nu(F)$ and $\deg F^k = k \deg F$, we obtain

$$\log M(f) \geq \frac{\nu(F) \log m - \log L(F^k)^{1/k}}{\deg F} \left(1 - \frac{1}{n}\right).$$

Letting $k \to \infty$ and using Lemma 5, the theorem follows. The proof for $m > 2$ is similar, using $\nu_0(F)$ in place of $\nu(F)$.

If f has all odd coefficients and no cyclotomic factors, then we may use $F(x) = x^2 - 1$ in the last theorem to obtain

$$\log M(f) \geq \frac{\log 2}{2}\left(1 - \frac{1}{n}\right). \qquad (7)$$

For $m > 2$, if $f \in \mathcal{D}_m$ has no cyclotomic factors, then using $F(x) = x - 1$ yields

$$\log M(f) \geq \log(m/2)\left(1 - \frac{1}{n}\right). \qquad (8)$$

We record here some improved bounds that arose from some fairly substantial searches.

Corollary 1 *Let f be a polynomial with degree $n-1$ having odd coefficients and no cyclotomic factors. Then*

$$\log M(f) \geq \frac{\log 5}{4}\left(1-\frac{1}{n}\right), \tag{9}$$

with equality if and only if $f(x) = \pm 1$.

Proof Let $F(x) = \left(1+x^2\right)\left(1-x^2\right)^4$. Since $\nu(F) = 9$, $\deg F = 10$, and

$$\begin{aligned}
\|F\|_\infty &= \left\|(1+y)(1-y)^4\right\|_\infty \\
&= 2^5 \max_{0\leq t\leq 1} \left|\cos(\pi t)\sin^4(\pi t)\right| \\
&= \frac{2^9}{25\sqrt{5}},
\end{aligned}$$

using the main estimate we establish the bound.

The bound of $5^{1/4} = 1.495348\ldots$ is not far from the smallest known measure of a polynomial with odd coefficients and no cyclotomic factors:

$$M(1+x-x^2-x^3-x^4+x^5+x^6) = 1.556030\ldots.$$

This number is in fact the smallest measure of a reciprocal polynomial with ± 1 coefficients having no cyclotomic factors and degree at most 72.

For the case $m > 2$, an improvement is possible.

Corollary 2 *Let $f \in \mathcal{D}_m$ have degree $n-1$ and no cyclotomic factors. Then*

$$\log M(f) \geq \log\left(\frac{\sqrt{m^2+1}}{2}\right)\left(1-\frac{1}{n}\right), \qquad (10)$$

with equality if and only if $f(x) = \pm 1$.

Proof Let $F(x) = (1+x)(1-x)^{m^2}$. Since $\nu_0(F) = m^2$, $\deg F = m^2+1$, and

$$\begin{aligned} \|F\|_\infty &= 2^{m^2+1} \max_{0\leq t\leq 1} \left|\cos(\pi t)\sin^{m^2}(\pi t)\right| \\ &= \frac{2^{m^2+1} m^{m^2}}{(m^2+1)^{(m^2+1)/2}}, \end{aligned}$$

. The main theorem now gives the result.

The bound of $\sqrt{10}/2 = 1.581138\ldots$ for $m = 3$ may be replaced by $1.582495\ldots$ by using the auxiliary polynomial $(1-x)^{425}(1-x^2)^{50}(1-x^5)$. No improvements are known for $m > 3$.

Auxiliary Polynomials

We obtain nontrivial bounds on the measure of a polynomial $f \in \mathcal{D}_m$ from Theorem 2 by using auxiliary polynomials having small degree, small supremum norm, and a high order of vanishing at 1.

We now investigate a family of polynomials having precisely these properties.

Pure product polynomials

A *pure product* of size n is a polynomial of the form

$$\prod_{k=1}^{n} (1 - x^{e_k}),$$

with each e_k a positive integer. Let $A(n)$ denote the minimal supremum over the unit disk among all pure products of size n,

$$A(n) = \min \left\{ \left\| \prod_{k=1}^{n} (1 - x^{e_k}) \right\|_{\infty} : e_k \geq 1 \right\}.$$

Erdős and Szekeres study this quantity, proving that the growth rate of $A(n)$ is subexponential:

$$\lim_{n\to\infty} A(n)^{1/n} = 1.$$

The upper bound on the asymptotic growth rate of $\log A(n)$ has since been greatly improved. Atkinson obtained $O(\sqrt{n}\log n)$, Odlyzko proved $O(n^{1/3}\log^{4/3} n)$, Kolountzakis demonstrated $O(n^{1/3}\log n)$, and Belov and Konyagin showed $O(\log^4 n)$.

The best known general lower bound on $A(n)$ is simply $\sqrt{2n}$; strengthening this would provide information on the Diophantine problem of Prouhet, Tarry, and Escott Erdős conjectured that in fact $A(n) \gg n^c$ for any $c > 0$.

Since $\nu_0(A(n)) = n$ and $\log A(n) = o(n)$, it follows that there exist pure product polynomials $F(x)$ that yield nontrivial lower bounds in Theorem 2.

Previously we exhibited some pure products of size $n \leq 20$ with very small length and degree, and these polynomials yield nontrivial lower bounds in Theorem 2.

However, these polynomials arise as optimal examples of polynomials with $\{-1, 0, 1\}$ coefficients having a root of prescribed order n at 1 and minimal degree. We obtain better bounds by designing some more specialized searches.

The Schinzel-Zassenhaus Problem

The lower bounds on $\log M(f)$ for $f \in \mathcal{D}_m$ of Corollaries 1 and 2 automatically yield lower bounds on $\max\{|\alpha| : f(\alpha) = 0\}$ for polynomials $f \in \mathcal{D}_m$ having no cyclotomic factors. The following theorem improves these results in the Schinzel-Zassenhaus problem in two ways: weakening the hypotheses and improving the constants.

Theorem 3 *Suppose $f \in \mathcal{D}_m$ is monic with degree $n-1$ having at least one noncyclotomic factor. Then there exists a root α of f satisfying*

$$|\alpha| > \begin{cases} 1 + \dfrac{\log 3}{2n}, & \text{if } m = 2, \\ 1 + \dfrac{\log(m-1)}{n}, & \text{if } m > 2. \end{cases} \tag{11}$$

Proof (for m =2) Let g denote the noncyclotomic part of f, let $d = \deg g$, and let α_1, ..., α_d denote the roots of g. Suppose that

$$\max\{|\alpha_k| : 1 \le k \le d\} < 1 + \frac{c}{n}$$

for a positive constant c, so $\left|\alpha_k^n\right| < e^c$ for each k.

Suppose $m = 2$. Since the maximum value of $\left|1 - z^2\right|$ for complex numbers z lying in the disk $\{z : |z| \le r\}$ is $1 + r^2$, with the maximum value occurring at $z = \pm ir$, we have

$$\left|1 - \alpha_k^{2n}\right| < 1 + e^{2c}$$

for each k. Consequently, using Lemma 4 with both $x^n + 1$ and $x^n - 1$, we find

$$2^{2d} \le \left|\mathrm{Res}(g(x), 1 - x^{2n})\right| < \left(1 + e^{2c}\right)^d. \quad (12)$$

Therefore $1 + e^{2c} > 4$, and the inequality for $m = 2$ follows.

No better bounds were found by using other auxiliary polynomials in place of $1 - x^{2n}$ and $1 - x^n$. However, for some m we find that the polynomials employed in Corollaries 1 and 2 do just as well. For example, let $F_{a,b}(x) = (1-x^2)^a(1+x^2)^b$, with a and b positive integers. The supremum of $F_{a,b}$ on the disk $\{z \in \mathbf{C} : |z| = r\}$ is

$$\left\|F_{a,b}\right\|_{|z|=r} = a^{a/2}b^{b/2}\left(\frac{2(1+r^4)}{a+b}\right)^{(a+b)/2},$$

and we obtain a lower bound on c from the inequality

$$2^{2a+b} < \left\|F_{a,b}\right\|_{|z|=e^c}.$$

The optimal choice of parameters is $a = 4$ and $b = 1$, as in Corollary 1, yielding $c \geq (\log 3)/2$. Likewise, for $m > 1$ the optimal choice for a and b in the auxiliary polynomial $(1-x)^a(1+x)^b$ is $a = m^2$ and $b = 1$, but this selection achieves $c \geq \log(m-1)$ only for $m = 3$.

Pisot and Salem numbers

We can slightly improve our estimates for Littlewood Salem's

Theorem 4 *Suppose f is a monic, irreducible polynomial in $\mathcal{D}_2$ with degree $n-1$ having exactly one root α outside the unit disk. Then*

$$\log|\alpha| > \frac{\log 5}{4}\left(1+\frac{1}{10n}\right).$$

It is well-known that every Pisot number is a two-sided limit point of Salem numbers. We also prove that more is true for the smallest Littlewood Pisot number.

Theorem 5 *The smallest Littlewood Pisot number is a limit point, from both sides, of Littlewood Salem numbers.*