Mahler's Measure of a Polynomial

Michael Mossinghoff

Graduate Student Seminar

UCLA Department of Mathematics

February 17, 1999

I. Mahler's Measure.

A. Definition.

Let

$$f(x) = \sum_{k=0}^{d} a_k \, x^k \,, \quad a_k \in \mathbf{C}$$

$$= a_d \prod_{k=1}^{d} (x - \alpha_k).$$

Mahler's measure of $f(x)$:

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

B. Properties.

1. $M(fg) = M(f)M(g)$.

2. $M(f) = \exp\left(\int_0^1 \log\left|f\left(e^{2\pi i t}\right)\right|\,dt\right)$.

$$\begin{aligned}\int_0^1 \log\left|f\left(e^{2\pi i t}\right)\right|\,dt &= \log|f(0)| + \sum_{|\alpha_i|\le 1} \log\frac{1}{|\alpha_i|}\\ &= \log\frac{|a_0|}{\prod_{|\alpha_i|\le 1}|\alpha_i|}\\ &= \log|a_d|\prod_{|\alpha_i|>1}|\alpha_i|\\ &= \log M(f).\end{aligned}$$

3. $M(f(x)) = M(f(-x)) = M(f(x^n)) = M(f^*(x))$, where $f^*(x) = x^d f(1/x)$ is the **reciprocal polynomial** of $f(x)$.

f is **reciprocal** if $f(x) = f^*(x)$.

4. Since

$$\frac{a_k}{a_d} = (-1)^k \sum_{i_1<i_2<\cdots<i_k} \alpha_{i_1}\alpha_{i_2}\cdots\alpha_{i_k}\,,$$

it follows that

$$|a_k| \leq \binom{d}{k} M(f).$$

Hence, given M and d, the set

$$\{f(x) \in \mathbf{Z}[x] \ : \ M(f) < M \text{ and } \deg(f) \leq d\}$$

is finite.

5. Writing

$$L(f) = \sum_{k=0}^{d} |a_k|\,,$$

$$\|f\|_2 = \left(\sum_{k=0}^{d} |a_k|^2\right)^{1/2},$$

$$\|f\|_\infty = \sup_{|z|=1} |f(z)|\,,$$

we obtain

$$M(f) \leq \|f\|_2 \leq \|f\|_\infty \leq L(f) \leq 2^d M(f).$$

6. (Kronecker) Suppose $f(x) \in \mathbf{Z}[x]$. Then $M(f) = 1 \iff f(x)$ is a product of cyclotomic polynomials, and the monomial x.

Recall: the cyclotomic polynomials are defined by:

$$\Phi_n(x) = \begin{cases} x-1\,, & \text{if } n = 1, \\ \dfrac{x^n - 1}{\prod_{\substack{m|n \\ m<n}} \Phi_m(x)}\,, & \text{otherwise.} \end{cases}$$

C. Applications.

1. Transcendental Number Theory.

Given $\alpha \neq 0$, algebraic integer, with minimal polynomial f, $\deg(f) = d$. If $g(x) \in \mathbf{Z}[x]$, $\deg(g) = n$, and $g(\alpha) \neq 0$, then

$$|g(\alpha)| \geq \frac{1}{L(g)^{d-1} M(f)^n}.$$

Example: $g(x) = x - 1$:

$$|\alpha - 1| \geq \frac{1}{2^{d-1} M(f)}\,.$$

Mignotte and Waldschmidt (1994):

$$|\alpha - 1| \geq \max\{2, M(f)\}^{-3\sqrt{d \log d}}\,.$$

2. Ergodic Theory.

Let $\mathbf{K}^n = \mathbf{R}^n/\mathbf{Z}^n$ (n-dimensional torus).

Suppose $T : \mathbf{K}^n \to \mathbf{K}^n$ is a measure-preserving automorphism, so given by an $n \times n$ integer matrix A with $\det A = \pm 1$.

Let f be the characteristic polynomial of A.

T is ergodic $\iff$ no root of f is a root of unity.

Thm (Sinai): Entropy of $T = \log_2(M(f))$.

II. Lehmer's Conjecture.

A. Statement and History.

There exists a constant $c > 1$ such that if $f(x) \in \mathbf{Z}[x]$ and $M(f) > 1$ then $M(f) \geq c$.

D. H. Lehmer (1933): Given $f(x) \in \mathbf{Z}[x]$, consider the sequence $\{\Delta_n(f)\}$:

$$\Delta_n(f) = \prod_{k=1}^{d} (\alpha_k^n - 1) .$$

Small $M(f)$ implies strong restrictions on primes that may divide $\Delta_n(f)$ and allowed construction of large prime numbers.

Best polynomial found:

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

$$M(\ell) = 1.1762808182599\ldots$$

B. Applications.

1. Ergodic Theory.

   Lehmer's conjecture does not hold if and only if:

   - Ergodic automorphisms on $\mathbf{K}^n$ with arbitrarily small entropy exist.
   - (Lind) Ergodic automorphism on $\mathbf{K}^\infty$ with finite entropy exists.

2. Number Theory.

   Let $\mu(f)$ denote the number of irreducible, noncyclotomic factors of f.

   Thm (Pinner, Vaaler): Lehmer's conjecture is equivalent to the existence of a constant c_0 such that for every $f(x) \in \mathbf{Z}[x]$,

$$\mu(f) \leq c_0 \log \|f\|_2 .$$

III. Lower Bounds.

1. Blanksby and Montgomery (1971):

$$M(f) > 1 + \frac{1}{52d \log 6d}.$$

2. Stewart (1978):

$$M(f) > 1 + \frac{1}{10^4 d \log d}.$$

3. Dobrowolski (1979):

$$M(f) > 1 + (1-\varepsilon)\left(\frac{\log\log d}{\log d}\right)^3, \quad d > d_0(\varepsilon).$$

4. Cantor and Straus (1982), Rausch (1985):

$$M(f) > 1 + (2-\varepsilon)\left(\frac{\log\log d}{\log d}\right)^3, \quad d > d_0(\varepsilon).$$

5. Louboutin (1983):

$$M(f) > 1 + \left(\frac{9}{4}-\varepsilon\right)\left(\frac{\log\log d}{\log d}\right)^3, \quad d > d_0(\varepsilon).$$

6. Smyth (1971):

If f is irreducible, nonreciprocal, and $f(x) \neq x$ or $x-1$, then

$$M(f) \geq M(x^3 - x - 1) = 1.3247179572\ldots.$$

IV. Related Conjectures.

1. Schinzel and Zassenhaus (1965).

If α is an algebraic integer with conjugates $\alpha_1, \ldots,$ α_d, let

$$\overline{|\alpha|} = \max_k |\alpha_k| \, .$$

Conjecture: there exists a constant $c > 0$ such that

$$\overline{|\alpha|} \geq 1 + \frac{c}{d}$$

whenever $\alpha \neq 0$ is an algebraic integer of degree d which is not a root of unity.

Lehmer $\implies$ Schinzel-Zassenhaus:

$$\overline{|\alpha|} \geq M(f)^{1/d} \geq (1+\delta)^{1/d} > 1 + \frac{c}{d}.$$

2. Pisot-Vijaraghavan and Salem Numbers.

Suppose α is a real algebraic integer and $\alpha > 1$.

PV number: all conjugates β of α have $|\beta| < 1$.

Salem number: all conjugates β of α have $|\beta| \leq 1$, and at least one conjugate satisfies $|\beta| = 1$.

Facts.

- The set of PV numbers is closed.
- (Siegel) The smallest PV number is $1.32471\ldots = M(x^3 - x - 1)$.
- Every PV number is a limit of Salem numbers.

Smallest known Salem number: $1.1762808\ldots = M(\ell)$.

V. Searches.

Search for f with $M(f) < 1.3$.

Restrict search to reciprocal polynomials with even d.

1. Exhaustive (Boyd, M.).
   - $O\left(C^{d^2}\right)$
   - $d \leq 24$

2. Height 1 (Boyd, M.).

   If f is irreducible and $M(f) < 2$ then there exists $g(x) \in \mathbf{Z}[x]$ such that fg has all coefficients in $\{-1, 0, 1\}$. Further, $\deg g < cd \log d$.
   - $O\left(C^{d}\right)$
   - $d \leq 40$
   - Finds all polynomials found in first search.

3. Perturbed Cyclotomic Products (Pinner, Vaaler, M.).

$$\ell(x) = \Phi_1^2(x)\Phi_2^2(x)\Phi_3^2(x)\Phi_6(x) - x^5$$

Form products of cyclotomic polynomials of degree d, then perturb middle coefficient(s).

- $O\left(C^{\sqrt{d}}\right)$
- $d \leq 64$
- Finds $> 80\%$ of those found in previous searches.
- All known measures less than 1.23 found.
- Lehmer's polynomial detected 241 times.

Measure	**Polynomial**
1.176280 . . .	$\Phi_1^2(x)\Phi_2^2(x)\Phi_3^2(x)\Phi_6(x) - x^5$
1.188368 . . .	$\Phi_1^2(x)\Phi_2^2(x)\Phi_3^2(x)\Phi_4(x)\Phi_6(x)\Phi_9(x) + x^9$
1.200026 . . .	$\Phi_1^2(x)\Phi_2^2(x)\Phi_4(x)\Phi_6(x)\Phi_7(x) + x^7$
1.201396 . . .	$(\Phi_1^2(x)\Phi_5^2(x)\Phi_7(x)\Phi_{10}(x) + x^{10})/\Phi_6(x)$
1.202616 . . .	$\Phi_1^2(x)\Phi_2^2(x)\Phi_3(x)\Phi_4(x)\Phi_6(x)\Phi_{12}(x) + x^7$
1.205019 . . .	$(\Phi_2^2(x)\Phi_{10}(x)\Phi_{16}(x)\Phi_{26}(x) - x^{13})/\Phi_{12}(x)$
1.207950 . . .	$\Phi_1^2(x)\Phi_2^2(x)\Phi_3(x)\Phi_4(x)\Phi_6(x)\Phi_7(x)\Phi_9(x)\Phi_{18}(x) + x^{14}$
1.212824 . . .	$(\Phi_1^2(x)\Phi_3(x)\Phi_8(x)\Phi_9(x)\Phi_{13}(x) + x^{13})/\Phi_{14}(x)$
1.214995 . . .	$\Phi_1^2(x)\Phi_2^2(x)\Phi_3(x)\Phi_5^2(x)\Phi_6(x)\Phi_{10}(x) + x^{10}$
1.216391 . . .	$\Phi_1^2(x)\Phi_2^2(x)\Phi_3(x)\Phi_4(x)\Phi_6(x) + x^5$
1.218396 . . .	$(\Phi_1^2(x)\Phi_3^2(x)\Phi_4(x)\Phi_6(x)\Phi_7(x)\Phi_{12}^2(x) + x^{12})/\Phi_{10}(x)$
1.218855 . . .	$\Phi_1^2(x)\Phi_2^2(x)\Phi_3(x)\Phi_4(x)\Phi_6(x)\Phi_7(x)\Phi_{10}(x)\Phi_{12}(x) + x^{12}$
1.219057 . . .	$(\Phi_1^2(x)\Phi_3(x)\Phi_4(x)\Phi_5(x)\Phi_{44}(x) + x^{15})/\Phi_{14}(x)$
1.219446 . . .	$\Phi_1^2(x)\Phi_2^2(x)\Phi_3^2(x)\Phi_4^2(x)\Phi_6(x)\Phi_{12}(x) + x^9$
1.219720 . . .	$\Phi_1^2(x)\Phi_2^2(x)\Phi_3(x)\Phi_4(x)\Phi_8(x)\Phi_9(x) + x^9$
1.220287 . . .	$(\Phi_1^2(x)\Phi_2^2(x)\Phi_7(x)\Phi_{10}(x)\Phi_{14}(x)\Phi_{19}(x) + x^{19})/\Phi_{12}(x)$
1.223447 . . .	$\Phi_1^2(x)\Phi_2^2(x)\Phi_3(x)\Phi_4(x)\Phi_5(x)\Phi_6(x)\Phi_{10}(x)\Phi_{20}(x)\Phi_{42}(x) - x^{19}$
1.223777 . . .	$(\Phi_1^2(x)\Phi_2^2(x)\Phi_4(x)\Phi_6(x)\Phi_8(x)\Phi_{17}(x)\Phi_{18}(x) + x^{17})/\Phi_{15}(x)$
1.224278 . . .	$\Phi_2^2(x)\Phi_6(x)\Phi_{18}^2(x) + x^8$
1.225503 . . .	$(\Phi_5(x)\Phi_{48}(x) + x^{10})/\Phi_4(x)$
1.225619 . . .	$\Phi_2^2(x)\Phi_4(x)\Phi_6(x)\Phi_{10}(x)\Phi_{26}(x)\Phi_{30}(x) - x^{15}$
1.225810 . . .	$(\Phi_1^2(x)\Phi_2^2(x)\Phi_5(x)\Phi_{10}(x)\Phi_{14}(x)\Phi_{17}(x) + x^{17})/\Phi_{12}(x)$
1.226092 . . .	$\Phi_2^2(x)\Phi_4(x)\Phi_6(x)\Phi_{20}(x)\Phi_{26}(x) - x^{13}$
1.226493 . . .	$\Phi_1^2(x)\Phi_2^2(x)\Phi_3(x)\Phi_6(x)\Phi_9(x)\Phi_{17}(x)\Phi_{18}(x) + x^{18}$
1.226993 . . .	$\Phi_1^2(x)\Phi_2^2(x)\Phi_3^2(x)\Phi_4(x)\Phi_6(x)\Phi_{12}^2(x) + x^{10}$
1.227785 . . .	$\Phi_1^2(x)\Phi_2^2(x)\Phi_3^2(x)\Phi_4(x)\Phi_6(x) + x^6$
1.228140 . . .	$(\Phi_1^2(x)\Phi_4(x)\Phi_5(x)\Phi_{12}(x)\Phi_{13}(x)\Phi_{36}(x) - x^{18})/\Phi_{14}(x)$
1.229482 . . .	$(\Phi_1^2(x)\Phi_2^2(x)\Phi_6(x)\Phi_{11}(x)\Phi_{13}(x)\Phi_{18}(x)\Phi_{22}(x) + x^{22})/\Phi_{15}(x)$
1.229566 . . .	$(\Phi_1^2(x)\Phi_5(x)\Phi_7(x)\Phi_{36}(x) - x^{12})/\Phi_6(x)$
1.229999 . . .	$\Phi_1^2(x)\Phi_2^2(x)\Phi_3(x)\Phi_6(x)\Phi_{17}(x)\Phi_{22}(x) + x^{17}$

VI. Limit Points.

Define

$$M(f(x,y)) = \exp\left(\int_0^1 \int_0^1 \log\left|f\left(e^{2\pi i s}, e^{2\pi i t}\right)\right| \, ds\, dt\right).$$

Applications.

- Ergodic theory.
- Factoring polynomials.
  If $g(x) \mid f(x)$ and $\deg(f) = d$ then $\|g\|_2 \leq \beta^d \|f\|_2$,
  where $\beta = M(1 + x + y) = 1.38135\ldots$.

Thm (Boyd): $\lim_{n\to\infty} M(f(x, x^n)) = M(f(x,y))$.

Smallest Known Limit Points.

$$f_1(x,y) = y^2(x+1) + y(x^2+x+1) + x(x+1),$$

$$f_2(x,y) = y^2 + y(x^2+x+1) + x^2,$$

$$f_3(x,y) = y^2(x+1) + y(x^4-x^2+1) + x^3(x+1),$$

$$f_4(x,y) = y^2(x^3-1) + y(x^5-1) + x^2(x^3-1),$$

$$M(f_1) = 1.255433866\ldots,$$

$$M(f_2) = 1.285734864\ldots,$$

$$M(f_3) = 1.309098380\ldots,$$

$$M(f_4) = 1.315692702\ldots.$$

Connections with L-functions.

Smyth:

$$\log(M(1+x+y)) = \frac{3\sqrt{3}}{4\pi}L(\chi_3, 2) = L'(\chi_3, -1)$$

where, for $\mathrm{Re}(s) > 1$,

$$L(\chi_3, s) = \sum_{n\geq 1} \frac{\left(\frac{n}{3}\right)}{n^s} = 1 - \frac{1}{2^s} + \frac{1}{4^s} - \frac{1}{5^s} + \frac{1}{7^s} - \frac{1}{8^s} + \cdots .$$

Let E denote an elliptic curve over $\mathbf{Q}$ (smooth cubic with a rational point).

L-function of E:

$$L(E, s) = \sum_{n\geq 1} \frac{a_n}{n^s}$$

converges for $\mathrm{Re}(s) > 3/2$.

Shimura-Taniyama-Weil conjecture: E is modular.

Thm (Wiles): If the conductor N of E is squarefree, then E is modular.

Define

$$\Lambda(s) = \frac{N^{s/2}}{(2\pi)^s}\Gamma(s)L(E,s).$$

If E is modular, then Λ extends to an entire function satisfying

$$\Lambda(s) = \pm\Lambda(2-s).$$

Thm (Deninger): Assuming the Bloch-Beilinson conjecture in K-theory, there exists an $r \in \mathbf{Q}$ such that

$$\begin{aligned}\log M(f_2(x,y)) &= \frac{15r}{4\pi^2}L(E,2) \\ &= rL'(E,0).\end{aligned}$$

where E is the elliptic curve with conductor 15.

Boyd:

$r = 1.000000000000000000000000000000000000000000000000000$

Boyd (1998): Hundreds of examples of polynomials $f(x,y)$ and elliptic curves E where $\log(M(f)) =_? rL'(E,0)$, where either r or $1/r$ is an integer.

Interesting: If E is the curve of conductor 11, then

$$\exp(L'(E,0)) = 1.16433154\ldots < M(\ell(x)).$$