On Lehmer’s question for integer-valued polynomials

Berend Ringeling*

Department of Mathematics, IMAPP, Radboud University,
PO Box 9010, 6500 GL Nijmegen, Netherlands

b.ringeling@math.ru.nl

July 15, 2022

We solve a Lehmer-type question about the Mahler measure of integer-valued polynomials.

1 Introduction

In the 1930s Lehmer asks, for a monic polynomial $P(x) = \prod_{j=1}^{d}(x - \alpha_j) \in \mathbb{Z}[x]$, whether the real quantity $\prod_{j=1}^{d} \max\{1,|\alpha_j|\}$ can be made arbitrarily close to but larger than 1. This quantity is called the Mahler measure of $P(x)$ [1]. More generally, for $P(x) = c\prod_{j=1}^{d}(x - \alpha_j) \in \mathbb{C}[x]$, the Mahler measure $M(P(x))$ is defined as $|c|^d \prod_{j=1}^{d} \max\{1,|\alpha_j|\}$. Conjecturally, the answer to Lehmer’s question is negative and the suspected lower bound is given by $\alpha = 1.176280818\ldots$ , the unique real zero outside the unit circle of Lehmer’s polynomial $x^{10} + x^9 - x^7 - x^6 - x^5 - x^4 - x^3 + x + 1$. Here we want to extend the original question to a bigger class of polynomials, integer-valued polynomials, that is, polynomials $P(x) \in \mathbb{Q}[x]$ such that $P(k) \in \mathbb{Z}$ for all $k \in \mathbb{Z}$. These polynomials often occur in counting problems; basic examples include binomial coefficients,

\[
\binom{x}{n} = \frac{x(x-1)(x-2)\ldots(x-n+1)}{n!} \in \mathbb{Q}[x]
\]

for $n \in \mathbb{N}$.

**Question 1.1.** Can $M(P(x))$ be made arbitrarily close to but larger than 1, when $P(x)$ is an irreducible integer-valued polynomial?

The irreducibility condition is essential here, since for a reducible integer-valued polynomial $P(x)$ the bound $M(P(x)) \geq 1$ may be violated. This is seen from the example

\[
P(x) = \frac{x^p - x}{p}
\]

*This work is supported by NWO grant OCENW.KLEIN.006.
for primes $p$. By Fermat’s little theorem $P(x)$ is integer-valued and the Mahler measure $M(P(x)) = 1/p$ tends to 0 as $p$ increases. Using this example, one can construct reducible integer-valued polynomials $P(x)$ with Mahler measure arbitrarily close to but larger than 1. The following statement demonstrates that the bound $M(P(x)) \geq 1$ in Question 1.1 is then best possible.

**Lemma 1.2.** If $P(x) \in \mathbb{Q}[x]$ is irreducible and integer-valued, then $M(P(x)) \geq 1$.

In fact, one can easily construct infinitely many (non-cyclotomic) irreducible integer-valued polynomials $P(x)$ with $M(P(x)) = 1$, this is demonstrated in Example 2.1 below. A goal of this note is to answer Question 1.1 in the affirmative. To accomplish the task, we consider the family of polynomials

$$f_p(x) = \frac{x^p - x}{p} + x^{(p+1)/2} + 1,$$

for odd integers $p$. For primes $p$, the polynomials $f_p(x)$ are integer-valued. We prove the following three statements for them.

**Theorem 1.3.** For primes $p \equiv 3 \pmod{4}$, $f_p(x)$ is irreducible.

**Theorem 1.4.** We have the following asymptotics for $M(f_p(x))$:

$$M(f_p(x)) \sim \frac{1 + \sqrt{1 + 4/p^2}}{2},$$

to all orders in $p$, as $p \to \infty$. In particular, $\lim_{p \to \infty} M(f_p(x)) = 1$.

**Theorem 1.5.** The sequence $M(f_p(x))$ is strictly decreasing in $p$.

Thus $M(f_p(x)) > 1$. Hence, the affirmative answer to Question 1.1 is given by the family $f_p$ when $p \equiv 3 \pmod{4}$. Here we tabulate a few values of $M(f_p(x))$ for small primes $p$:

| $p$ | $M(f_p(x))$ |
|-----|-------------|
| 3   | 1.17503…   |
| 7   | 1.02169…   |
| 11  | 1.00821…   |
| 19  | 1.00276…   |

## 2 Properties for the Mahler measure of integer-valued polynomials

**Proof of Lemma 1.2.** The Mahler measure of any polynomial $P(x) \in \mathbb{Q}[x]$ is bounded from below by the absolute value of the constant term. Indeed if

$$P(x) = a_dx^d + \cdots + a_0 = a_d \prod_{j=1}^{d} (x - \alpha_j),$$

then

$$M(P(x)) = |a_d| \prod_{j=1}^{d} |\alpha_j| \geq |a_d| \prod_{j=1}^{d} |\alpha_j| = |a_d| |a_0|/|a_d| = |a_0|.$$

Moreover, if $P(x)$ is integer-valued and irreducible, $P(0)$ is guaranteed to be a non-zero integer. Hence $M(P(x)) \geq 1$. \qed
The following example shows that one can find infinitely many non-cyclotomic irreducible integer-valued polynomials with Mahler measure exactly 1.

**Example 2.1.** Consider the integer-valued polynomial

\[ g_p(x) = \frac{x^p - x}{p} + 1 \]

for primes \( p > 2 \). The zeros of \( g_p(x) \) all lie outside the complex unit circle, as otherwise for any zeros \( \alpha \) of \( g_p \) inside or on the unit circle, we would have the contradictory inequality

\[ 0 = |g_p(\alpha)| = \left| 1 + \frac{\alpha^p}{p} - \frac{\alpha}{p} \right| \geq 1 - \frac{2}{p} > 0. \]

As a consequence of this, we find \( M(g_p(x)) = 1 \).

We want to show that the polynomial \( pg_p(x) \) is irreducible. If it were reducible, then at least one of the irreducible factors would have constant term 1; this is impossible since \( g_p \) has all the zeros outside the unit circle. Thus, we have found an infinite family of (non-cyclotomic) irreducible integer-valued polynomials.

### 3 Irreducibility

**Proof of Theorem 1.3.** For a polynomial \( P(x) \) of degree \( d \), write \( \tilde{P}(x) = x^d P(1/x) \) for its reciprocal. We prove the irreducibility of the polynomials \( f_p \) for primes \( p \equiv 3 \mod 4 \) following the method first used by Ljunggren in [3], also see the expository notes [2]. The irreducibility of \( f_3 \) and \( f_7 \) is immediate, so we deal with \( p > 7 \) from now on.

Write

\[ f_p^*(x) = pf_p^*(x) = x^p + px^{\frac{p+1}{2}} - x + p \]

and

\[ \tilde{f}_p^*(x) = x^p f_p^*(1/x) = px^p - x^{p-1} + px^{\frac{p-1}{2}} + 1 \]

for its reciprocal.

**Lemma 3.1.** The polynomials \( f_p^* \) and \( \tilde{f}_p^* \) have no zeros in common.

**Proof.** Suppose \( \alpha \) is a zero of both \( f_p^* \) and \( \tilde{f}_p^* \), so that

\[ \alpha^p - \alpha + pa^{\frac{p+1}{2}} + p = 0 \quad \text{and} \quad \alpha - \alpha^p + pa^{\frac{p-1}{2}} + p\alpha^{p+1} = 0. \]

The equations imply

\[ (\alpha^{\frac{p+1}{2}} + 1)^2 = 0, \]

hence \( \alpha^{\frac{p+1}{2}} = -1 \). Substituting this in the first equation we find that \( \alpha = \pm 1 \). This is impossible if \( p \equiv 3 \mod 4 \).

Suppose \( f_p^*(x) \) is reducible, i.e. \( f_p^* = gh \) for \( g, h \in \mathbb{Z}[x] \) of positive degree. Define an auxiliary polynomial

\[ k = \tilde{g}h = b_\mu x^\mu + \cdots + b_0; \]
then $\tilde{k}k = f_p^*\tilde{f}_p^*$. Note that $k \neq \pm f_p^*$ or $\pm \tilde{f}_p^*$, as otherwise $k = gh$ and $f_p^* = gh$ are equal, up to sign, hence $h$ and $h$ share a common zero, which is impossible by Lemma 3.1.

We next compute the coefficients of $k$ by comparing the coefficients in

$$\tilde{k}k = f_p^*\tilde{f}_p^* = px^{2p} - x^{2p-1} + p^2 x^{\frac{3p+1}{2}} - px^{p+1} + 2(p^2 + 1)x^p - px^{p-1} + p^2 x^{\frac{p-1}{2}} - x + p. \quad (1)$$

Reading off the $x^{2p}$-coefficient we have $b_0b_p = p$. We can assume that $b_0 = \pm p$ and $b_p = \pm 1$, possibly by interchanging $k$ and $\tilde{k}$. Further we may assume $b_0 = p$ and $b_p = 1$ by possibly replacing $k$ with $-k$.

Comparing the $x^p$-coefficient of $\tilde{k}k$ in (1), we find

$$2(p^2 + 1) = b_0^2 + \cdots + b_p^2,$$

therefore

$$p^2 + 1 = b_1^2 + \cdots + b_{p-1}^2. \quad (2)$$

Comparing the $x$-coefficient in (1) we conclude that

$$-1 = b_0b_{p-1} + b_1b_p,$$

implying $b_1 = -1 - b_{p-1}p$. The latter equality is only possible if either $b_{p-1} = 0$ and $b_1 = -1$, or $b_{p-1} = -1$ and $b_1 = p - 1$, as otherwise (2) fails. Consider the two cases separately.

**Case $b_{p-1} = -1$ and $b_1 = p - 1$.** We obtain from (2)

$$2p - 1 = b_2^2 + \cdots + b_{p-2}^2 \quad (3)$$

Compare the $x^2$-coefficient to find that

$$b_0b_{p-2} + b_1b_{p-1} + b_2b_p = 0,$$

so that $b_2 = -1 - p(b_{p-2} - 1)$. According to (3), the equality is only possible if $b_{p-2} = 1$ and $b_2 = -1$. Next compare the $x^3$-coefficient to find that

$$b_0b_{p-3} + b_1b_{p-2} + b_2b_{p-1} + b_3b_p = 0,$$

hence $p(b_{p-3} + 1) + b_3 = 0$. Again, from (3) we conclude that $b_{p-3} = -1$ and $b_3 = 0$. We claim that $b_{p-j} = (-1)^j$ and $b_j = 0$ for $2 < j < \frac{p-1}{2}$. Comparing the $x^j$-coefficient for such $j$ gives

$$b_0b_{p-j} + b_1b_{p-j+1} + b_2b_{p-j+2} + \cdots + b_jb_p = 0.$$

By induction all the terms $b_i$ vanish for $2 < i < j$, so that $b_j = -p(b_{p-j} - (-1)^j)$. From (3) and the fact that $p$ divides $b_j$, we conclude that $b_j = 0$ and $b_{p-j} = (-1)^j$. Finally, compare the coefficient of $x^{\frac{p-1}{2}}$ in (1):

$$p^2 = b_0b_{p-1} + b_1b_{p-1} + b_2b_{p-1} + \cdots + b_{p-1}b_p.$$

This translates into

$$p^2 = p(b_{p-1} + (-1)^{p-3}b_{p-1}) + b_{p-1}.$$
Therefore, $b_{\frac{p-1}{2}}$ is divisible by $p$, hence $b_{\frac{p-1}{2}} = 0$ from (3) implying $b_{\frac{p+1}{2}} = (-1)^{\frac{p-1}{2}} + p = p - 1$. This calculation contradicts (3).

Case $b_{p-1} = 0$ and $b_1 = -1$. In this case we have

$$p^2 = b_2^2 + \cdots + b_{p-2}^2.$$  \hfill (4)

We claim that $b_j = 0$ for $1 < j < \frac{p+1}{2}$. Suppose otherwise, let $1 < j' < \frac{p+1}{2}$ be the smallest integer such that $b_{j'} \neq 0$. Comparing the $x^i$-coefficient for $1 < i < j'$ in (1) results in

$$b_0 b_{p-i} + b_1 b_{p-i+1} \cdots + b_{j'} b_p = 0;$$

it follows by induction that $b_{p-i} = 0$ for all such $i$ as well.

Comparing the $x^{j'}$-coefficient in (1) we find out that

$$b_0 b_{p-j'} + b_1 b_{p-j'+1} \cdots + b_{j'} b_p = 0,$$

hence $p b_{p-j'} + b_{j'} = 0$. Since $b_{j'} \neq 0$ by our assumption, we have $|b_{j'}| \geq p$ and $|b_{p-j'}| \geq 1$. Comparing this with (4) we find this impossible. The contradiction implies that $b_j = 0$ and $b_{p-j} = 0$ for $1 < j < \frac{p+1}{2}$.

Finally, consider the $x^{\frac{p+1}{2}}$-coefficient in (1):

$$b_0 b_{p-\frac{p-1}{2}} + b_1 b_{p-\frac{p-1}{2}+1} \cdots + b_{\frac{p-1}{2}} b_p = p^2;$$

this simplifies to

$$p b_{\frac{p+1}{2}} + b_{\frac{p-1}{2}} = p^2.$$

Comparing with (4), the only solution to this equation is $b_{\frac{p+1}{2}} = p$ and $b_{\frac{p-1}{2}} = 0$. We conclude that $k = f_p^*$, which gives a contradiction.

Thus, $f_p^*$ is irreducible. This proves Theorem 1.3. \hfill \Box

4 Asymptotics

For this part, it is more convenient to work with the logarithmic Mahler measure $m(P(x)) = \log(M(P(x)))$. Jensen’s formula allows one to write it as

$$m(P(x)) = \frac{1}{2\pi i} \oint_{|z|=1} \log |P(z)| \frac{dz}{z}. \hfill (5)$$

Denote $N = (p - 1)/2$ and $Q_p(x) = (x^2 - 1)/p + x$ and define

$$m_p = m\left(\frac{x^p - x}{p} + x^{\frac{p+1}{2}} + 1\right) = m(xQ_p(x^N) + 1).$$

We will show that, for all integers $N$,

$$m_p \sim m(xQ_p(x^N)) = m(Q_p(x)) = \log \frac{1 + \sqrt{1 + 4/p^2}}{2}$$

to all orders in $p$, i.e. the difference of $m_p$ and $m(Q_p(x))$ is $O(p^n)$ for all $n \in \mathbb{Z}$. 

5
We have
\[ m_p - m(xQ_p(x^N)) = m\left(1 + \frac{1}{xQ_p(x^N)}\right) = \frac{1}{N} \cdot m\left(1 + \frac{(-1)^{N+1}}{xQ_p(x^N)}\right), \quad (6) \]
where the last equality follows from the more general observation:

**Lemma 4.1.** If \( P(x) \) is a polynomial and \( N \) an integer, then
\[ m\left(1 + \frac{(-1)^{N+1}}{xP(x)^N}\right) = N \cdot m\left(1 + \frac{1}{xP(x)}\right) \]

**Proof.** Indeed, Jensen’s formula implies that
\[ m\left(1 + \frac{\xi}{xP(x)}\right) = m\left(1 + \frac{1}{xP(x)}\right), \]
by substituting \( \xi x \) for \( x \) in the integral (5) for the corresponding Mahler measure.

Since
\[ \frac{1}{|Q_p(z)|^2} = \frac{p}{|z^2 + pz - 1|^2} = \frac{p^2}{2 + p^2 - 2 \text{Re}(z^2)} < 1 \]
for \( z \in \mathbb{C} \setminus \{\pm 1\}, |z| = 1 \), we get the convergent expansion
\[ \log\left(1 + \frac{(-1)^{N+1}}{zQ_p(z)^N}\right) = \sum_{\ell=1}^{\infty} \frac{(-1)^{\ell N-1}}{\ell z^\ell Q_p(z)^\ell N}. \]
for all such \( z \). From this we find out that
\[ m\left(1 + \frac{(-1)^{N+1}}{xQ_p(x)^N}\right) = \text{Re} \left\{ \frac{1}{2\pi i} \oint_{|z|=1} \log\left(1 + \frac{(-1)^{N+1}}{zQ_p(z)^N}\right) \frac{dz}{z} \right\} = \text{Re} \sum_{\ell=1}^{\infty} \frac{(-1)^{\ell N-1}}{\ell} F_\ell, \quad (7) \]
where
\[ F_\ell = \frac{1}{2\pi i} \oint_{|z|=1} \frac{dz}{z^{\ell+1}Q_p(z)^\ell N} = \frac{p^{\ell N}}{2\pi i} \oint_{|z|=1} \frac{dz}{z^{\ell+1}(z - \alpha_1)^{\ell N}(z - \alpha_2)^{\ell N}} \]
and \( \alpha_1, \alpha_2 \) are the zeros of \( Q_p(x) \) ordered by \( |\alpha_2| > 1 > |\alpha_1| \). We will examine the asymptotics of \( F_\ell \) for \( \ell \geq 1 \) as \( p \to \infty \). We can explicitly compute these integrals.

**Lemma 4.2.** For \( \ell \geq 1 \), we have
\[ F_\ell = (-1)^\ell p^{\ell N} \sum_{j=0}^{\ell N-1} \binom{\ell N - 1}{j} \binom{\ell + j}{\ell} \frac{1}{(\alpha_2 - \alpha_1)^{2\ell N - 1 - j} \alpha_2^{\ell + 1 + j}}. \]
Proof. This follows from Cauchy’s integral theorem. The integrand has precisely one singularity outside the unit circle. Therefore, the value of the integral is given by

$$ - \text{Res}_{z = \alpha_2} \frac{1}{z^{\ell+1}Q_p(z)\ell^N}. $$

The formula follows by expanding $1/z^{\ell+1}$ into a series in $z - \alpha_2$:

$$ 1/z^{\ell+1} = \sum_{j=0}^{\infty} (-1)^j \binom{\ell + j}{j} \frac{1}{\alpha_2^{\ell+1+j}} (z - \alpha_2)^j $$

and extracting the nonpositive powers of $z - \alpha_2$ in the Laurent expansion of $1/Q_p(z)^{\ell N}$:

$$ \frac{1}{(z - \alpha_1)^{\ell N}(z - \alpha_2)^{\ell N}} = \sum_{j=0}^{\ell N} (-1)^j \binom{\ell N + j - 1}{j} \frac{1}{(\alpha_2 - \alpha_1)^{\ell N+j}} (z - \alpha_2)^{j-\ell N} + O(z - \alpha_2). $$

Taking the product of (8) and (9) we conclude with the formula

$$ (-1)^{\ell-1} p^{\ell N} \sum_{j=0}^{\ell N-1} \binom{2\ell N - 2 - j}{\ell N - 1} \binom{\ell + j}{j} \frac{1}{(\alpha_2 - \alpha_1)^{2\ell N-j} \alpha_2^{\ell+1+j}} $$

for the coefficient of $1/(z - \alpha_2)$.

Using Lemma 4.2, we will estimate $|F_{\ell}|$ from above.

Lemma 4.3. For $\ell \geq 1$, we have

$$ |F_{\ell}| \leq \frac{1}{p^{\ell(N+1)}} \left( \frac{2\ell N + \ell - 1}{\ell N} \right). $$

Proof. The estimates $|\alpha_2 - \alpha_1| \geq p$ and $|\alpha_2| \geq p$ imply

$$ |F_{\ell}| \leq \frac{1}{p^{\ell(N+1)}} \sum_{j=0}^{\ell N-1} \binom{2\ell N - 2 - j}{\ell N - 1} \binom{\ell + j}{j} $$

$$ = \frac{p - 1}{p + 1} \frac{1}{p^{\ell(N+1)}} \left( \frac{2\ell N + \ell - 1}{\ell N} \right) \leq \frac{1}{p^{\ell(N+1)}} \left( \frac{2\ell N + \ell - 1}{\ell N} \right). $$

It follows from Lemma 4.3 that $F_{\ell}$ decays exponentially in $\ell N$.

Proof of Theorem 1.4. Using Equations (6), (7) and Lemma 4.3, we conclude that

$$ |m_p - m(Q_p(x))| \leq \frac{1}{p^{N+1}} \left( \frac{p - 1}{N} \right) =: \epsilon_p $$

meaning that the difference of the Mahler measures decays exponentially in $p$ as $p \to \infty$. This finishes the proof of Theorem 1.4.
Proof of Theorem 1.5. To show that the sequence $m_p$ for odd $p$ is decreasing, it suffices to prove the inequality

$$m(Q_p(x)) - \epsilon_p > m(Q_{p+2}(x)) + \epsilon_{p+2},$$

(10)

where $\epsilon_p$ is defined in the proof of Theorem 1.4. We can estimate $m(Q_p(x)) - m(Q_{p+2}(x))$ from below using that $\log(x) > 1 - \frac{1}{x}$ for $x > 1$. Indeed, for $p \geq 5$ we have

$$m(Q_p(x)) - m(Q_{p+2}(x)) = \log \frac{1 + \sqrt{1 + 4/p^2}}{1 + \sqrt{1 + 4/(p+2)^2}} > \frac{1 + \sqrt{1 + 4/p^2} - \sqrt{1 + 4/(p+2)^2}}{1 + \sqrt{1 + 4/p^2}} - \frac{1}{2p^2} - \frac{1}{2(p+2)^2} \geq \frac{1}{p^3}.$$

On the other hand, using $\binom{2n}{n} \leq 2^n$ for $n \geq 1$, we can estimate $\epsilon_p + \epsilon_{p+2}$ from above: for $p \geq 7$ we obtain

$$\epsilon_p + \epsilon_{p+2} \leq \frac{1}{p^{N+1}} \frac{4^N}{4} + \frac{1}{(p+2)^{N+2}} \frac{4^{N+1}}{4} \leq \frac{4}{p} \frac{N+1}{4} \leq \frac{3}{4} \frac{p}{p} \leq \frac{1}{p^3}.$$

This implies inequality (10) for $p \geq 7$. Together with $m_3 = 0.16129\ldots$, $m_5 = 0.04920\ldots$, $m_7 = 0.02145\ldots$, it concludes our proof of Theorem 1.5.

5 Discussion

The choice for the family of polynomials $f_p(x)$ is far from optimal: among integer-valued polynomials of prime degree $p \equiv 3 \mod 4$, it is not the one with smallest Mahler measure larger than 1. This can already be seen when $p = 3$: an integer-valued polynomial with the smallest Mahler measure is

$$Q_3(x) = \frac{2}{3}x^3 - \frac{1}{2}x^2 - \frac{1}{6}x - 1,$$

with the Mahler measure $1.02833\ldots$ much smaller than $M(f_3(x)) = 1.17503\ldots$.

For $d = 2, 3, \ldots$, define $Q_d(x)$ to be an irreducible integer-valued polynomial of degree $d$ with smallest Mahler measure larger than 1. Then the following questions arise.

**Question 5.1.** How to (efficiently) compute these polynomials $Q_d(x)$?

**Question 5.2.** What can be said about the asymptotics of $M(Q_d(x))$ for $d \to \infty$?

**Acknowledgements** The author would like to thank François Brunault, David Hokken and Wadim Zudilin for interesting discussions and helpful comments.
References

[1] F. Brunault and W. Zudilin, Many variations of Mahler measures: a lasting symphony, Aust. Math. Soc. Lecture Ser. 28 (Cambridge University Press, Cambridge, 2020).

[2] K. Conrad, Irreducibility of $x^n - x - 1$, unpublished note, available at https://kconrad.math.uconn.edu/blurbs/ringtheory/irredsselmerpoly.pdf.

[3] W. Ljunggren, On the irreducibility of certain trinomials and quadrinomials, Math. Scand. 8 (1960), 65–70.