HEIGHTS OF ROOTS OF POLYNOMIALS WITH ODD COEFFICIENTS

JOHN GARZA, M. I. M. ISHAK, MICHAEL J. MOSSINGHOFF, CHRISTOPHER PINNER, AND BENJAMIN WILES

Abstract. We show that the height of a non-zero non root of unity α which is the zero of a polynomial with all odd coefficients of degree n satisfies

$$h(\alpha) \geq \frac{0.4278}{n+1}.$$

More generally we obtain bounds when the coefficients are all congruent to 1 modulo m for some $m \geq 2$.

1. Introduction

We recall the Mahler measure $M(f)$ of a polynomial $f = a\prod_{i=1}^{d}(x-\alpha_i)$ in $\mathbb{C}[x]$:

$$M(f) = |a|\prod_{i=1}^{d}\max\{1,|\alpha_i|\}.$$

For a non-zero algebraic number α of degree d one defines the absolute logarithmic height $h(\alpha)$ of α to be

$$h(\alpha) = \frac{1}{d}\log M(F)$$

where F is an irreducible polynomial in $\mathbb{Z}[x]$ with $F(\alpha)=0$. That is $\log M(f)$ represents the sum of the heights of the non-zero roots of f (with multiplicity) whenever f is primitive in $\mathbb{Z}[x]$.

For an integer $m \geq 2$ let D_m denote the set of integer polynomials whose coefficients a_i all satisfy $a_i \equiv 1 \pmod{m}$. For a polynomial of degree n in D_m with no cyclotomic factors Borwein, Dobrowolski & Mossinghoff [1] proved that

$$\log M(f) \geq c_m \frac{n}{n+1}$$

with $c_2 = \frac{1}{4}\log 5 = 0.402359\ldots$, $c_3 = 0.459003$ and $c_m = \log(\sqrt{m^2+1}/2)$ for $m > 3$. These constants were improved in [2] to obtain $c_2 = 0.416230\ldots$, general bounds of strength

$$c_m = \begin{cases} \log(m/2) + (3-\log 3)/2m^2 + O(1/m^4) & \text{if } m \geq 3 \text{ odd,} \\ \log(m/2) + (4-\log 4)/m^2 + O(1/m^4) & \text{if } m \geq 4 \text{ even,} \end{cases}$$

and particular values $c_3 = 0.501026\ldots$, $c_4 = 0.832461\ldots$, $c_5 = 0.952869$, $c_6 = 1.165884$, $c_7 = 1.271775$, $c_8 = 1.425369$, $c_9 = 1.515669$, $c_{10} = 1.634836$, and $c_{11} = 1.712539$.

We show here how to more straightforwardly obtain bounds of the form

$$h(\alpha) \geq \frac{c_m}{n+1} \tag{1.1}$$

Date: February 2, 2010.

1991 *Mathematics Subject Classification.* 11L07; 11L03.

Key words and phrases. heights, Mahler measure, Lehmer problem.

The research of the third author was supported in part by NSA grant H98230-08-1-0052.

when α is a zero of a polynomial f in D_m of degree n, but not a $2(n+1)$st root of unity. Of course then

$$\log M(f) \geq c_m \frac{d}{n+1}$$

where d is the degree of the non-cyclotomic part of f (the type of bound obtained in Theorem 2.2 of [2]).

Theorem 1. *If α is a zero of a polynomial f in D_m of degree n and α is not an $2(n+1)$st root of unity (not an $n+1$st if $m \geq 3$), then (1.1) holds with*

$$c_2 = 0.427800$$

and

$$c_m = \log\left(\frac{m}{2}\right) + \frac{2.947486 - \delta/2}{m^2} + O\left(\frac{1}{m^4}\right),$$

where

$$\delta = \begin{cases} 1 & \text{if } m \geq 3 \text{ odd,} \\ 0 & \text{if } m \geq 4 \text{ even.} \end{cases}$$

For small $m \geq 3$ we show the following improvements: $c_3 = 0.620362$, $c_4 = 0.855600$, $c_5 = 1.016628$, $c_6 = 1.179916$, $c_7 = 1.307083$, $c_8 = 1.434141$, $c_9 = 1.538934$, $c_{10} = 1.640027$, and $c_{11} = 1.728890$.

We note the easily obtained (if asymptotically less precise) bound

$$c_m = \begin{cases} \frac{1}{2}\log\left(\frac{m^2+3}{4}\right) & \text{if } m \geq 3 \text{ odd,} \\ \frac{1}{2}\log\left(\frac{m^2+4}{4}\right) & \text{if } m \geq 4 \text{ even,} \end{cases} \tag{1.2}$$

(the even case having already been obtained and improved in [2]). We remark that the optimal c_m in (1.1) certainly satisfies $c_m = \log m + O(1)$:

Theorem 2. *If (1.1) holds for any non root of unity α that is a zero of a polynomial f in D_m of degree n and α, then*

$$c_2 \leq \log\left(\frac{1+\sqrt{5}}{2}\right) = 0.481211\ldots \tag{1.3}$$

(even if we further restrict to Littlewood polynomials),

$$c_3 \leq \log 2 = 0.693147\ldots,$$

$$c_4 \leq \log(1+\sqrt{2}) = 0.881373\ldots, \tag{1.4}$$

and

$$c_6 \leq \log\left(\frac{3+\sqrt{13}}{2}\right) = 1.194763\ldots. \tag{1.5}$$

For general $m \geq 3$

$$c_m \leq \log(m-1). \tag{1.6}$$

It is not clear what should be the optimal constant C_1 in a bound of the form $c_m = \log m - C_1 + o(1)$. We note that the same computation that yields c_3 immediately gives the lower bound

$$h(\alpha) \geq 0.155090$$

for abelian α (see [3]).

2. Preliminaries

Suppose that α is in an algebraic number field k, and $|\ |_v$, $v \in V_k$ a complete set of absolute values on k normalised so that $|x|_v = \|x\|_v^{d_v/d}$ where $d = [k : \mathbb{Q}]$, $d_v = [k_v : \mathbb{Q}_v]$, and $\|x\|_v$ coincides with the usual absolute value or p-adic absolute value on $\mathbb{Q}$. Then

$$h(\alpha) = \log H(\alpha), \quad H(\alpha) = \prod_{v \in V_k} \max\{1, |\alpha|_v\}.$$

The normalisations ensure that this does not depend upon k.

Lemma 1. *For $t = 1$ or $t > 1$ and $k \le 4t/(t-1)^2$*

$$\sup_{|z|=1} |(z-1)^k (z+t)| = \frac{(t+1)^{k+1}}{(k+1)^{\frac{1}{2}(k+1)}} \left(\frac{k}{t}\right)^{\frac{1}{2}k}$$

achieved at $z = -\frac{((t^2+1)k-2t)}{2t(k+1)} \pm \frac{(t+1)\sqrt{k(4t-(t-1)^2k)}}{2t(k+1)} i$. For $t > 1$ and $k \ge 4t/(t-1)^2$ the supremum is $2^k(t-1)$ achieved at $z = -1$.

Proof. Writing $z = e^{i\theta}$, $u = \cos\theta$, it is readily checked that

$$|(z-1)^k (z+t)|^2 = 2^k (1-u)^k ((t^2+1) + 2tu)$$

is maximised for $-1 \le u \le 1$ at $u = -\frac{((t^2+1)k-2t)}{2t(k+1)}$ while this is at least -1 (and at $u = -1$ when $k > 4t/(t-1)^2$). □

Define the polynomials

$$g_1(z) = \frac{1}{2}(m-\delta)z + \frac{1}{2}(m+\delta), \qquad \delta = \begin{cases} 1 & \text{if } m \text{ is odd,} \\ 0 & \text{if } m \text{ is even,} \end{cases} \tag{2.1}$$

and

$$g_2(z) = \frac{1}{4}(m^2 + (4-\delta))z^2 + \frac{1}{2}(m^2 - (4-\delta))z + \frac{1}{4}(m^2 + (4-\delta)). \tag{2.2}$$

Lemma 2. *If $m \ge 3$ is odd then $g_1(z^n)$ is irreducible in $\mathbb{Z}[z]$ for all n in $\mathbb{N}$. Further, if $m \ge 4$ is odd with $3 \nmid m$ or even with $4 \mid m$ then $g_2(z^n)$ is irreducible in $\mathbb{Z}[z]$ for all n in $\mathbb{N}$.*

Proof. If $m = 2k+1$ is odd then by Capelli's Theorem $g_1(z^n) = kz^n + (k+1)$ is irreducible unless $(k+1)/k$ is a prime power in $\mathbb{Q}$, but plainly $k+1 = a^p$, $k = b^p$ has no positive integer solutions a, b.

Observe that if $g_2(\beta) = 0$ then

$$\beta = \frac{-\frac{1}{2}(m^2 - (4-\delta)) \pm m\sqrt{(4-\delta)}i}{\frac{1}{2}(m^2 + (4-\delta))}$$

is complex, lying on the unit circle. Moreover if m is odd and $3 \nmid m$ or if $4 \mid m$ then

$$\gcd\left(\frac{1}{4}(m^2 + (4-\delta)), \frac{1}{2}(m^2 - (4-\delta))\right) = 1,$$

$g_2(z)$ is irreducible in $\mathbb{Z}[z]$, and

$$h(\beta) = \frac{1}{2}\log\left(\frac{m^2 + (4-\delta)}{4}\right).$$

Notice that if $m \ge 2$ is odd with $3 \mid m$ or if $2 \parallel m$ then we need to first factor out a common 3 or 2 and

$$h(\beta) = \frac{1}{2}\log\left(\frac{m^2+3}{12}\right) \text{ or } \frac{1}{2}\log\left(\frac{m^2+4}{8}\right). \tag{2.3}$$

Suppose then that $(m,6)=1$ or $4\mid m$, and $g_2(z^n)$ has a non-trivial factor,

$$r(z)=\sum_{i=0}^{d} a_i z^i \in \mathbb{Z}[z], \quad a_d\neq 0, \quad 0<d<2n.$$

If α is a root of $r(z)$, then

$$\frac{\log|a_d|}{d}=h(\alpha)=\frac{1}{n}h(\beta)$$

and

$$\frac{m^2+(4-\delta)}{4}=|a_d|^{2n/d}=y^p$$

for some y in $\mathbb{N}$ and prime $p\mid 2n/\gcd(2n,d)$. For $m=4l$ this reduces to $l^2+1=y^p$, a special case of Catalan's equation shown to have no solution by Lebesgue [4]. For $m=2l+1$ odd this reduces to $l^2+l+1=y^p$ shown by Nagell [6] and Ljunggren [5] to only have the solution $p=3$, $y=7$, $l=18$. This just leaves the case $m=37$, in which case

$$g_2(z^n)=7^3\left(z^n-\beta\right)\left(z^n-\beta^{-1}\right), \quad \beta=\frac{1}{2}\left(1-\sqrt{3}i\right)\left(\frac{2+\sqrt{3}i}{2-\sqrt{3}i}\right)^3.$$

Plainly then $g_2(z^n)$ is irreducible in $\mathbb{Z}[z]$ unless $(z^n-\beta)$ is reducible in $\mathbb{Q}(\sqrt{3}i)[z]$. But by Capelli's Theorem this would require $\beta=A^p$ or $-4\mu^4$ for some prime p and A or μ in $\mathbb{Q}(\sqrt{3}i)$. Considering prime factorizations in the integers of $\mathbb{Q}(\sqrt{3}i)$ the only possibility would be $p=3$, but $\frac{1}{2}(1-\sqrt{3}i)$ can not be a cube in $\mathbb{Q}(\sqrt{3}i)$ (which contains the sixth but not the eighteenth roots of unity). □

3. Proof of Theorem 1

If f is in D_m then $f(x)=\frac{x^{n+1}-1}{x-1}+mr(x)$ for some r of degree at most n in $\mathbb{Z}[x]$. Hence for $v\nmid\infty$, writing $\beta=\alpha^{n+1}$,

$$|\beta-1|_v=|m(\alpha-1)r(\alpha)|_v\le|m|_v\max\{1,|\beta|_v\}. \tag{3.1}$$

For $m=2$ we take

$$\begin{aligned}g(z)=&(z-1)^k(z+1)^l(5z^2+6z+5)^t(29z^4+60z^3+78z^2+60z+29)^w\\&\cdot(3z^2+2z+3)^c(33z^4+60z^3+70z^2+60z+33)^e\\&\cdot(169z^6+490z^5+871z^4+1036z^3+871z^2+490z+169)^s.\end{aligned}$$

Thus for $v\nmid\infty$

$$|\beta-1|_v\le|2|_v\max\{1,|\beta|_v\},\qquad |\beta+1|_v=|\beta-1+2|_v\le|2|_v\max\{1,|\beta|_v\},$$

and

$$\left|\beta^2-1\right|_v\le|2|_v^2\max\{1,|\beta|_v\}^2, \tag{3.2}$$

giving

$$\begin{aligned}|\beta^2+1|_v&=|\beta^2-1+2|_v\le|2|_v\max\{1,|\beta|_v\}^2,\\ \left|5\beta^4+6\beta^2+5\right|_v&=\left|5(\beta^2-1)^2+16\beta^2\right|_v\le|2|_v^4\max\{1,|\beta|_v\}^4,\\ \left|3\beta^4+2\beta^2+3\right|_v&=\left|3(\beta^2-1)^2+8\beta^2\right|_v\le|2|_v^3\max\{1,|\beta|_v\}^4,\end{aligned}$$

and for integer A,B,C,D (the quartic factors in $g(z)$ correspond to $(A,B,C)=(29,11,1)$ and $(33,12,1)$, and the sextic to $(A,B,C,D)=(169,94,17,1)$),

$$|A(\beta^2-1)^4+B2^4\beta^2(\beta^2-1)^2+C2^8\beta^4|_v\le|2|_v^8\max\{1,|\beta|_v\}^8,$$

$$\left|A(\beta^2-1)^6+B\cdot4^2\beta^2(\beta^2-1)^4+C\cdot4^4\beta^4(\beta^2-1)^2+D4^6\beta^6\right|_v\le|2|_v^{12}\max\{1,|\beta|_v\}^{12}.$$

Hence we have

$$|g(\beta^2)|_v\le|2|_v^{2k+l+4t+8w+3c+8e+12s}\max\{1,|\beta|_v\}^{2\deg g},\quad v\nmid\infty.$$

For $v \mid \infty$ and $|\beta|_v > 1$ we observe that $|g(\beta^2)|_v = |\beta|_v^{2\deg g}|g(\beta^{-2})|_v$ with $|\beta^{-2}|_v < 1$. Hence for $v \mid \infty$

$$|g(\beta)|_v \le \max\{1, |\beta|_v\}^{2\deg g}\left(\sup_{|z|\le 1}|g(z)|\right)^{d_v/d} = \max\{1,|\beta|_v\}^{2\deg g}\sqrt{M}^{d_v/d},$$

where, writing $z = e^{it}$ and $u = \cos t$,

$$M = \sup_{|z|=1}|g(z)|^2 = 2^{k+l+2t+4w+2c+4e+6s}L$$

with

$$L = \sup_{-1\le u\le 1}(1-u)^k(1+u)^l(5u+3)^{2t}(29u^2+30u+5)^{2w}(3u+1)^{2c} \cdot (33u^2+30u+1)^{2e}(169u^3+245u^2+91u+7)^{2s}.$$

We need to justify that $g(\beta^2) \neq 0$. By assumption $\beta^2 \neq 1$, and from (3.2) plainly $\beta^2 \neq -1$. Observe also that

$$5z^{4(n+1)} + 6z^{2(n+1)} + 5, \quad 3z^{4(n+1)} + 2z^{2(n+1)} + 3,$$
$$29z^{8(n+1)} + 60z^{6(n+1)} + 78z^{4(n+1)} + 60z^{2(n+1)} + 29,$$
$$33z^{8(n+1)} + 60z^{6(n+1)} + 70z^{4(n+1)} + 60z^{2(n+1)} + 33,$$

and the factors

$$13z^{6(n+1)} + 2z^{5(n+1)} + 19z^{4(n+1)} - 4z^{3(n+1)} + 19z^{2(n+1)} + 2z^{(n+1)} + 13,$$
$$13z^{6(n+1)} - 2z^{5(n+1)} + 19z^{4(n+1)} + 4z^{3(n+1)} + 19z^{2(n+1)} - 2z^{(n+1)} + 13$$

of $169z^{12(n+1)} + 490z^{10(n+1)} + 871z^{8(n+1)} + 1036z^{6(n+1)} + 871z^{4(n+1)} + 490z^{2(n+1)} + 169$ are all irreducible (each of their roots lies on the unit circle with the same non-trivial height so the lead coefficients of each factor would need to contain all the primes in the original lead coefficient). Since α has degree at most n the remaining factors can not vanish. Thus by the product formula

$$1 = \prod_v |g(\beta^2)|_v \le H(\beta)^{2\deg g}2^{-(2k+l+4t+8w+3c+8e+12s)}\sqrt{M},$$

and

$$h(\beta) \ge \frac{\log\left(2^{3k+l+6t+12w+4c+12e+18s}/L\right)}{4(k+l+2t+4w+2c+4e+6s)}.$$

The choice $(k,l,t,w,c,e,s) = (3977, 780, 328, 96, 24, 16, 16)$ and numerical computation of L gives the lower bound $h(\beta) \ge 0.4278003111\ldots$ claimed.

For $m = 4$ taking $g(\beta)$ in place of $g(\beta^2)$ immediately gives $h(\beta) \ge 2\cdot 0.4278003111\ldots = 0.8556006223\ldots$.

For general $m \ge 3$ we take

$$g(z) = \prod_{i=0}^{I} g_i(z)^{s_i}$$

with $I = 2$,

$$g_0(z) = (z-1),$$

and $g_1(z)$ and $g_2(z)$ as in (2.1) and (2.2). For $v \nmid \infty$ we have

$$|g_1(\beta)|_v = \left|\frac{1}{2}(m-\delta)(\beta-1)+m\right|_v \le |m|_v \max\{1,|\beta|_v\}$$

$$|g_2(\beta)|_v = \left|\frac{1}{4}(m^2+(4-\delta))(\beta-1)^2 + m^2\beta\right|_v \le |m|_v^2\max\{1,|\beta|_v\}^2,$$

and

$$|g(\beta)|_v \le \max\{1,|\beta|_v\}^{\deg g}|m|_v^{\deg g}.$$

For $v \mid \infty$ and $|\beta|_v > 1$ writing $|g(\beta)|_v = |\beta|_v^{\deg g} |g^*(\beta^{-1})|_v$, where g^* is the reciprocal of g, we have

$$\begin{aligned}|g(\beta)|_v &\leq \max\{1, |\beta|_v\}^{\deg g} \left(\sup_{|z|\leq 1} \max\{|g(z)|, |g^*(z)|\}\right)^{d_v/d}\\ &= \max\{1, |\beta|_v\}^{\deg g} \sup_{|z|=1} |g(z)|^{d_v/d}.\end{aligned}$$

Hence assuming that $g(\beta) \neq 0$ we have

$$1 = \prod_v |g(\beta)|_v \leq H(\beta)^{\deg g} m^{-\deg g} \sup_{|z|=1} |g(z)|,$$

and

$$h(\beta) \geq \log(m) - \frac{\log(\sqrt{M})}{\deg g}, \qquad M := \sup_{|z|=1} |g(z)|^2. \tag{3.3}$$

It remains to check that $g(\beta) \neq 0$. By assumption $\beta \neq 1$. For m odd $g_1(z^{n+1})$ is irreducible by Lemma 2 so can not vanish at α (which has degree at most n). From (3.1) we know that

$$\prod_{v\mid\infty} |1-\beta|_v \geq m \prod_{v\nmid\infty} \max\{1, |\beta|_v\}^{-1}. \tag{3.4}$$

So for $m > 2$ we must have $\beta \neq -1$ (else (3.4) gives $2 \geq m$). Hence $g_0(\beta)g_1(\beta) \neq 0$. Thus when $s_2 = 0$, $s_1 = 1$ (and $s_0 \leq m^2 - 1$ when m is odd) Lemma 1 gives

$$\sqrt{M} = \frac{m^{s_0+1}}{(s_0+1)^{\frac{1}{2}(s_0+1)}} \left(\frac{4s_0}{m^2-\delta}\right)^{\frac{1}{2}s_0},$$

and

$$H(\beta)^{s_0+1} \geq (s_0+1)^{\frac{1}{2}(s_0+1)} \left(\frac{m^2-\delta}{4s_0}\right)^{\frac{1}{2}s_0}.$$

The result (1.2)

$$h(\beta) \geq \frac{1}{2}\log\left(\frac{m^2+4-\delta}{4}\right) \tag{3.5}$$

follows from optimally taking $s_0 = (m^2-\delta)/4$.

Similarly degree considerations show that $g_2(\beta) \neq 0$ when $4 \mid m$ or m is odd with $3 \nmid m$ and $g_2(z^{n+1})$ is irreducible by Lemma 2. When m is odd and $3 \mid m$ or $2 \parallel m$ then $g_2(\beta) \neq 0$ from (2.3) and the lower bound (3.5).

Converting to cosines we have

$$M = \sup_{|z|=1} |g(z)|^2 = \sup_{u\in[-1,1]} \prod_{i=0}^{I} f_i(u)^{s_i}$$

with

$$\begin{aligned}f_0(u) &= 2(1-u),\\ f_1(u) &= \frac{1}{2}(m^2-\delta)u + \frac{1}{2}(m^2+\delta),\end{aligned}$$

and

$$f_2(u) = \left(\frac{1}{2}(m^2+(4-\delta))u + \frac{1}{2}(m^2-(4-\delta))\right)^2,$$

where plainly M will be achieved at $u = -1$ or at zero of

$$\sum_{i=0}^{I} s_i \frac{f_i'(u)}{f_i(u)} = 0.$$

For example, after numerical computational and experimentation, the choices $(m;s_0,s_1,s_2)=(3;107,48,17),\ (5;198,26,13),\ (6;246,21,11),\ (7;225,14,8),\ (8;151,7,4),\ (9;326,12,7),\ (10;106,3,2)$, and $(11;206,5,3)$ give us respectively $c_3=0.599206$, $c_5=1.001086$, $c_6=1.172140$, $c_7=1.298988$, $c_8=1.429512$, $c_9=1.532875$, $c_{10}=1.637694$, and $c_{11}=1.724309$.

For the asymptotic bound we take a sequence of s_0,s_1,s_2 with

$$s_0/s_2\to Am^2,\qquad s_1/s_2\to 2C,$$

for constants A, C which will be chosen optimally below. Hence M must be achieved at

$$u=\frac{-Am^6+m^2((4-\delta)(2C-A\delta)-2\delta)-2\delta(4-\delta)(C+1)\pm 2m^2\sqrt{D_1}}{(m^2-\delta)(m^2+4-\delta)(Am^2+2C+2)}$$

where

$D_1=m^4((2A+1+C)^2-8AC)+m^2((2A+1+C)(8-2\delta(C+1))+8AC\delta)+(4-\delta(1+C))^2$,

or at $u=-1$ when m is odd. Writing

$$u=-1+\frac{2}{Am^2}\left(2A+1+C-A\delta\pm\sqrt{D}\right)+O\left(\frac{1}{m^4}\right),$$

where $D=(2A+1+C)^2-8AC$, leads to

$$c_m\geq\log\left(\frac{m}{2}\right)+\frac{1}{2Am^2}\min_{\pm}\log\left(\frac{\exp\left(2A+1+C-A\delta\pm\sqrt{D}\right)}{\left(\frac{2A+1+C\pm\sqrt{D}}{4A}\right)^{2C}\left(\frac{-2A+1+C\pm\sqrt{D}}{4A}\right)^{2}}\right)+O\left(\frac{1}{m^4}\right),$$

or $\log(m/2)+\frac{1}{Am^2}\log\left(2^{2(1+C)}/3\right)+O\left(m^{-4}\right)$ if this is smaller when m is odd. For a given choice of C we can choose A to make these $\pm$ quantities equal. Choosing (after numerical experimentation) $2C=1.5799148239$ and calculating $A=0.5569260220\ldots$ gives the desired asymptotic bound.

To obtain the improved values for $m=3$ to 11 stated in the theorem we take $g(z)=\prod_{i=0}^{I}g_i(z)^{s_i}$ with $I=4$ or 5 and the auxiliary factors $g_i(z)$, and choice of exponents s_i given in Table 1. For these $g_j(z)$ we have $|g_j(\beta)|_v\leq|m|_v^{\deg g_j}\max\{1,|\beta|_v\}^{\deg g_j}$ for $v\nmid\infty$ and (3.3) holds as before (as long as $g(\beta)\neq 0$). We can argue as above that $g(\beta)\neq 0$ by irreducibility (and for $m=8$ that $\frac{1}{2}\log 9=1.0986\ldots<1.4295\ldots$ (the previous lower bound), and for $m=5$ and $m=11$ that $\frac{1}{2}\log 8>1.016628$ and $\frac{1}{2}\log 32>1.728890$). □

Additional factors could probably be added to the auxiliary polynomial $g(z)$ in the style of [2] for further improvements.

The choices $g(z)=(z^2-1)^4(z^2+1)$ and $g(z)=(z-1)^{m^2}(z+1)$ similarly recover the values $c_2=\frac{1}{4}\log 5$ and $c_m=\log(\sqrt{m^2+1}/2)$ for $m>2$ respectively (and using the auxiliary polynomials of [2] for $g(z)$ gives the improved values stated there).

4. Proof of Theorem 2

Since the golden ratio is a limit point of Salem numbers with Littlewood minimal polynomials (Theorem 6.2 of [1]) we note that the optimal c_2 certainly satisfies (1.3).

Suppose that $m\geq 3$. For (1.6) we take $n\geq 2$ and

$$f_n(x)=x^{2n}+\sum_{i=0}^{n-1}\left(x^{2i}-(m-1)x^{2i+1}\right)=\frac{x^{n+1}}{x^2-1}F_n(x),$$

with

$$F_n(x)=(x^{n+1}-x^{-(n+1)})-(m-1)(x^n-x^{-n}).$$

Since $f_n\left(\frac{1}{m-1}\right)>0$, $f_n\left(\frac{1}{m-1}\left(1+\left(\frac{2}{m-1}\right)^n\right)\right)<0$ it is clear that the $f_n(x)$ have real roots α_n, α_n^{-1} with $\alpha_n\to(m-1)$ as $n\to\infty$. Notice that $f_n(x)$ does not vanish at ± 1 or any $(2n+1)$st root of unity (so by the theorem can have no cyclotomic factors). Since

Table 1. Auxiliary factors and exponents

m	Auxiliary factors $g_3(z),\ldots$	$(s_0,s_1,s_2,s_3,\ldots)$
3	$g_3(z)=11(z-1)^4+7\cdot 3^2z(z-1)^2+3^4z^2$	$(823,178,183,48,53,7)$
	$g_4(z)=13(z-1)^4+8\cdot 3^2z(z-1)^2+3^4z^2$	
	$g_5(z)=5(z-1)^2+2\cdot 3^2z$	
5	$g_3(z)=8(z-1)^2+5^2z$	$(340,10,29,1,8,10)$
	$g_4(z)=61(z-1)^4+16\cdot 5^2z(z-1)^2+5^4z^2$	
	$g_5(z)=5(11(z-1)^4+3\cdot 5^2z(z-1)^2+5^3z^2)$	
6	$g_3(z)=109(z-1)^4+21\cdot 6^2z(z-1)^2+6^4z^2$	$(222680,19000,8000,$
	$g_4(z)=11(z-1)^2+6^2z$	$2793,2064,1000)$
	$g_5(z)=2(59(z-1)^4+11\cdot 6^2z(z-1)^2+3\cdot 6^3z^2)$	
7	$g_3(z)=181(z-1)^4+27\cdot 7^2z(z-1)^2+7^4z^2$	$(309,16,9,4,1,2)$
	$g_4(z)=193(z-1)^4+28\cdot 7^2z(z-1)^2+7^4z^2$	
	$g_5(z)=7(2z^2+3z+2)$	
8	$g_3(z)=2(9(z-1)^2+2^5z)$	$(944,45,20,5,5,2)$
	$g_4(z)=305(z-1)^4+35\cdot 8^2z(z-1)^2+8^4z^2$	
	$g_5(z)=321(z-1)^4+36\cdot 8^2z(z-1)^2+8^4z^2$	
9	$g_3(z)=461(z-1)^4+43\cdot 9^2z(z-1)^2+9^4z^2$	$(44277,0,1256,538,273)$
	$g_4(z)=481(z-1)^4+44\cdot 9^2z(z-1)^2+9^4z^2$	
10	$g_3(z)=701(z-1)^4+53\cdot 10^2z(z-1)^2+10^4z^2$	$(1029,25,10,5,3)$
	$g_4(z)=1351(z-1)^4+104\cdot 10^2z(z-1)^2+2\cdot 10^4z^2$	
11	$g_3(z)=32(z-1)^2+11^2z$	$(827,6,12,2,6,3)$
	$g_4(z)=991(z-1)^4+63\cdot 11^2z(z-1)^2+11^4z^2$	
	$g_5(z)=1021(z-1)^4+64\cdot 11^2z(z-1)^2+11^4z^2$	

$\frac{1}{2i}F(e^{2\pi it})=\sin(2\pi(n+1)t)-(m-1)\sin(2\pi nt)$ changes sign it must have a zero t_j in each interval $\left[\frac{2j-1}{4n},\frac{2j+1}{4n}\right]$, $j=1,2,\ldots,2n-1$ and the remaining $(2n-2)$ zeros $e^{2\pi it_j}$, $t_j\neq 1/2$ of $f_n(x)$ all lie on the unit circle. Since $f_n(x)$ has no monic factors with all roots on the unit circle these $f_n(x)$ are irreducible with $(\deg f_n+1)h(\alpha_n)=\left(\frac{2n+1}{2n}\right)\log\alpha_n\to\log(m-1)$ as $n\to\infty$. For (1.4) we similarly consider

$$f_{n,4}(x)=\sum_{i=0}^{4n+2}x^i-4x\sum_{i=0}^{n}x^{4i}=(1-x)(1-2x-x^2)\sum_{i=0}^{n}x^{4i}-x^{4n+3}$$

with real roots $\alpha_n,\alpha_n^{-1}\to\sqrt{2}-1,\sqrt{2}+1$ and no roots at the $(4n+3)$st roots of unity. Writing $F_{n,4}(x)=(x^4-1)f_{n,4}(x)x^{-(2n+3)}$ and observing that

$$\frac{1}{4i}F_{n,4}(e^{2\pi it})=(\cos(3\pi t)+\cos(\pi t))\sin((4n+3)\pi t)-2\sin(4(n+1)\pi t)$$

has sign changes in each of the intervals $[(2j+1)/8(n+1),(2j+3)/8(n+1)]$, $j=0,\ldots,4n+2$, (and removing the introduced fourth roots of unity) the remaining $4n$ zeros of $f_{n,4}(x)$

all lie on the unit circle. For (1.5) we take

$$f_{n,6}(x) = \sum_{i=0}^{6n+4} x^i - 6x(1-x+x^2)\sum_{i=0}^{n} x^{6i} = (1-x)(1-x+x^2)(1-3x-x^2)\sum_{i=0}^{n} x^{6i} - x^{6n+5}$$

with real roots $\alpha_n, \alpha_n^{-1} \to \frac{1}{2}(\sqrt{13}-3), \frac{1}{2}(\sqrt{13}+3)$ and no roots at the $(6n+5)$st roots of unity. Writing $F_{n,6}(x) = \frac{(x^6-1)}{(x^2-x+1)} f_{n,6}(x) x^{-(3n+4)}$ and observing that

$$\frac{1}{4i} F_{n,6}(e^{2\pi i t}) = (\cos(3\pi t) + 2\cos(\pi t))\sin((6n+5)\pi t) - 3\sin(6(n+1)\pi t)$$

has sign changes in each of the intervals $[(2j+1)/12(n+1), (2j+3)/12(n+1)]$, $j = 0, \ldots, 6n+4$, (and removing the introduced sixth roots of unity) the remaining $6n+2$ zeros of $f_{n,6}(x)$ all lie on the unit circle. □

References

[1] P. Borwein, E. Dobrowolski & M.J. Mossinghoff, *Lehmer's problem for polynomials with odd coefficients*, Ann. of Math. (2) 166 (2007), no. 2, 347–366.

[2] A. Dubickas & M.J. Mossinghoff, *Auxiliary polynomials for some problems regarding Mahler's measure.* Acta Arith. 119 (2005), no. 1, 65–79.

[3] M.I.M. Ishak, M.J. Mossinghoff, C.G. Pinner & B. Wiles, *Lower bounds for heights in cyclotomic extensions.* submitted J. Number Theory.

[4] V.A. Lebesgue, *Sur l'impossibilité, en nombres entiers, de l'équation* $x^m = y^2 + 1$, Nouv. Ann. Math. (1) 9 (1850), 178–181.

[5] W. Ljunggren, *Einige bemerkungen uber die darstellung ganzer zahlen durch binare kubische farmen mit positiver diskrimante*, Acta Math. 75 (1943), 1–21.

[6] T. Nagell, *Des equations indéterminées* $x^2+x+1 = y^n$ *et* $x^2+x+1 = 3y^n$, Norsk Matematisk Forening, Skr. (1) no. 2 (1921), 1–14.

Department of Mathematics, Kansas State University, Manhattan, KS 66506
E-mail address: johngarz@math.ksu.edu

Department of Mathematics, Kansas State University, Manhattan, KS 66506
E-mail address: mimishak@math.ksu.edu

Department of Mathematics, Davidson College, Davidson, NC 28035-6996
E-mail address: mimossinghoff@davidson.edu

Department of Mathematics, Kansas State University, Manhattan, KS 66506
E-mail address: pinner@math.ksu.edu

Department of Mathematics, Kansas State University, Manhattan, KS 66506
E-mail address: wilesb@math.ksu.edu