London Mathematical Society ISSN 1461–1570

POLYNOMIALS WITH RESTRICTED COEFFICIENTS AND PRESCRIBED NONCYCLOTOMIC FACTORS

MICHAEL J. MOSSINGHOFF

Abstract

The algorithms described in this paper were developed to investigate three problems regarding polynomials with restricted coefficients: (i) determining whether there exist polynomials with $\{0, 1\}$ coefficients and repeated noncyclotomic factors, (ii) searching for polynomials with $\{-1, 1\}$ coefficients and small Mahler measure, and (iii) finding polynomials with $\{-1, 0, 1\}$ coefficients with a root of high multiplicity off the unit circle. The results in the first problem presented here answer a question of Odlyzko and Poonen.

1. *Introduction*

Let $\mathcal{N}$ denote the set of polynomials with $\{0, 1\}$ coefficients having constant term 1:

$$\mathcal{N} = \left\{ 1 + \sum_{k=1}^{d} a_k x^k : a_k \in \{0, 1\} \right\}. \tag{1}$$

We call these the *Newman polynomials*. Similarly, let $\mathcal{L}$ denote the set of *Littlewood polynomials*,

$$\mathcal{L} = \left\{ \sum_{k=0}^{d} a_k x^k : a_k \in \{-1, 1\} \right\}, \tag{2}$$

and let $\mathcal{H}$ denote the set of *height* 1 *polynomials* with nonzero constant term,

$$\mathcal{H} = \left\{ \pm 1 + \sum_{k=1}^{d} a_k x^k : a_k \in \{-1, 0, 1\} \right\}. \tag{3}$$

We study several problems regarding noncyclotomic factors of polynomials in these sets, especially repeated factors.

In 1993, Odlyzko and Poonen [24] studied the set of zeros of polynomials in $\mathcal{N}$, proving for instance bounds on their location. They remarked that there exist polynomials in $\mathcal{N}$ with cyclotomic factors of arbitrarily high multiplicity, as follows. Let $\zeta = \exp(2\pi i/n)$ be an nth root of unity with $n > 1$, and set $\Phi(x) = (x^n - 1)/(x - 1)$. If $\{r_k\}_{k=1}^{m}$ is a sequence of positive integers satisfying $\gcd(r_k, n) = 1$ and $r_k > (n-1)\sum_{i<k} r_i$ for each k, then the polynomial $\prod_{k=1}^{m} \Phi(x^{r_k})$ is a Newman polynomial with a zero of order m at ζ. They left open the question of whether there exist polynomials in $\mathcal{N}$ with repeated noncyclotomic factors.

In Section 2 we develop some algorithms to search for Newman polynomials with prescribed factors, and we use our methods to construct several $\{0, 1\}$ polynomials with repeated

Received 30 May 2003, revised 17 September 2003; *published* 28 November 2003.
2000 Mathematics Subject Classification 11C08 (primary); 11Y35, 30C15 (secondary)

noncyclotomic factors. These algorithms take advantage of the fact that only two values are allowed as coefficients in the polynomials that we seek, and consequently our searches extend to fairly high degrees. In particular, we find 23 polynomials in $\mathcal{N}$ divisible by $\ell(x)^2$, where $\ell(x)$ is the irreducible noncyclotomic polynomial

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

This polynomial arises in many other problems.

Recall that *Mahler's measure* of a polynomial $f(x) = \sum_{k=0}^{d} a_k x^k = a_d \prod_{k=1}^{d}(x - \beta_k)$ is defined by

$$M(f) = |a_d| \prod_{k=1}^{d} \max\{1, |\beta_k|\}. \tag{5}$$

For polynomials with integer coefficients, a classical result of Kronecker implies that $M(f) = 1$ if and only if f is a product of cyclotomic polynomials and the monomial x. In 1933, D. H. Lehmer [18] asked whether the Mahler measure of a polynomial with integer coefficients can be arbitrarily close to 1, and noted that the polynomial (4) has $M(\ell) = 1.176280\ldots$. Lehmer's question remains open, and this number remains the smallest known value greater than 1 of the measure of an integer polynomial, despite several extensive searches [9, 10, 22, 23]. Lists of known irreducible polynomials with small values of Mahler's measure are available at [21].

Lehmer's polynomial, being in this sense 'nearly' cyclotomic, appears to be an attractive candidate in the problem of Odlyzko and Poonen. This polynomial has found application in other problems for the same reason; for instance, in the construction of high-order polylogarithm relations [2, 14], and in the study of algebraic integers α for which several powers α^n are exceptional units [27].

Recall that a polynomial $f(x)$ is described as *reciprocal* if $f(x) = \pm x^{\deg f} f(1/x)$. Smyth [28] proved that if $f \in \mathbb{Z}[x]$ is nonreciprocal and $f(0) \neq 0$, then $M(f) \geqslant M(x^3 - x - 1) = 1.324717\ldots$, thus answering Lehmer's question for this class of polynomials. In [6], Smyth's theorem is strengthened for polynomials with odd coefficients: in particular, if $f \in \mathcal{L}$ is nonreciprocal, then $M(f) \geqslant M(x^2 - x - 1) = (1 + \sqrt{5})/2$. Here also are found the smallest measures among reciprocal Littlewood polynomials of degree at most 72; the smallest known measure is $1.496711\ldots$, achieved by

$$x^{19} + x^{18} + x^{17} + x^{16} - x^{15} + x^{14} - x^{13} + x^{12} - x^{11} - x^{10} - x^9 - x^8 + x^7 - x^6 + x^5 - x^4 + x^3 + x^2 + x + 1.$$

In Section 3 we adapt the methods of Section 2 to search for Littlewood polynomials with prescribed factors, and then we use these methods to attempt to construct polynomials in $\mathcal{L}$ with measure smaller than 1.4967.

Section 4 studies a similar problem for height 1 polynomials. In 1973, Pathiaux [25] proved that if $f(x) \in \mathbb{Z}[x]$ is irreducible and $M(f) < 2$, then there exists a polynomial $F(x) \in \mathcal{H}$ with $f \mid F$. A remark at the end of this paper notes that the proof may be modified to establish the same result for reducible polynomials. Mignotte [20] found a simpler proof of this statement for irreducible polynomials, and derived an upper bound on the degree of F in terms of the degree and measure of f. His proof may also be extended to the reducible case. These results were generalized and strengthened by Bombieri and Vaaler in [4], as an application of their improved formulation of Siegel's lemma.

https://doi.org/10.1112/S1461157000000474 Published online by Cambridge University Press

Therefore, if one could establish an absolute upper bound B on the multiplicity of a noncyclotomic factor of a polynomial with height 1, then it would follow that the value of Mahler's measure for noncyclotomic polynomials is bounded away from 1, answering Lehmer's question. Certainly, if B exists, then $B \geqslant 4$, since $\sqrt[4]{2} = 1.189207\ldots > M(\ell)$. It is therefore of interest to study height 1 polynomials with repeated noncyclotomic factors. In Section 4 we use lattice reduction to construct some polynomials in $\mathcal{H}$ with noncyclotomic factors of multiplicity 3.

We add that similar problems regarding polynomials in $\mathcal{N}$, $\mathcal{L}$, and $\mathcal{H}$ with prescribed cyclotomic factors have also been well studied, particularly with the factor $(x \pm 1)^m$. The case of Newman polynomials is studied in [**8, 16**], Littlewood polynomials in [**11, 12**], and height 1 polynomials in [**1, 4, 5, 7, 15**].

2. *Newman polynomials*

We describe two algorithms for finding polynomials $f \in \mathcal{N}$ having a prescribed factor $g(x) \in \mathbb{Z}[x]$.

2.1. *Exhaustive search*

Given a polynomial $g(x) \in \mathbb{Z}[x]$ and a positive integer d, we wish to determine all polynomials $f(x) \in \mathcal{N}$ having $\deg(f) \leqslant d$ and $g \mid f$. In order to avoid the time-consuming operation of trial division with polynomials, we first ensure that $g(x_i) \mid f(x_i)$ for a sequence of integers $\{x_i\}$ before testing whether $g \mid f$. Choosing $x_0 = 2$ allows us to take advantage of the computer's binary representation of integers. We identify an odd positive integer w with the polynomial $f \in \mathcal{N}$ having $f(2) = w$, and clearly we can construct f from w by scanning its binary representation. Since we need only consider odd integers w divisible by $g(2)$, this reduces the search space by a factor of $2|g(2)|$.

We choose $x_1 = -2$ for a secondary screening of candidate polynomials, taking advantage of bit-selection operations to test very quickly whether $g(-2) \mid f(-2)$. Let b_+ and b_- denote the two integers between 2^{d-1} and 2^{d+1} whose binary representation consists of alternating zeros and ones:

$$b_+ = \sum_{k=0}^{d/2} 2^{2k}; \qquad b_- = \sum_{k=0}^{(d-1)/2} 2^{2k+1}.$$

Also, for positive integers $r = \sum_{i=0}^{d} r_i 2^i$ and $s = \sum_{i=0}^{d} s_i 2^i$ with $r_i, s_i \in \{0, 1\}$, let $r \star s$ denote the integer $\sum_{i=0}^{d} r_i s_i 2^i$, so $r \star s$ is the bitwise 'and' of the binary representations for r and s. This operation is available in many popular programming languages (often as the operator '&'). Finally, we define the function γ on nonnegative integers $w < 2^{d+1}$ by

$$\gamma(w) = w \star b_+ - w \star b_-.$$

Note that if $w = f(2)$ for $f \in \mathcal{N}$, then $\gamma(w) = f(-2)$. Further, computing $\gamma(w)$ from w requires only three operations per word of storage for the bits of w, so testing whether $g(-2) \mid f(-2)$ is quite fast.

We summarize our procedure in Algorithm 1

We implemented this algorithm in C++, and ran it on a MIPS R10000 processor, which supports 64-bit arithmetic, allowing fast computation of $\gamma(w)$ for $d \leqslant 63$. Using $g(x) = \ell(x)^2$, we have $u = 358801$ and $v = 1666681$, and with $d = 60$ our algorithm finds

https://doi.org/10.1112/S1461157000000474 Published online by Cambridge University Press

Input. $g(x) \in \mathbb{Z}[x]$, positive integer d.
Output. All $f \in \mathcal{N}$ with $\deg f \leqslant d$ and $g \mid f$.
Method. Set $u = g(2)$ and $v = g(-2)$.
For each odd w with $0 < w < 2^{d+1}$ and $u \mid w$ do
If $v \mid \gamma(w)$ then
Construct f from $w = f(2)$.
If $g \mid f$ then print f.
End if.
End loop.

Algorithm 1: Newman polynomials with a prescribed factor.

two polynomials in $\mathcal{N}$ having Lehmer's polynomial as a repeated factor:

$$\begin{aligned} &x^{59}+x^{58}+x^{54}+x^{51}+x^{48}+x^{47}+x^{46}+x^{45}+x^{41}+x^{37}\\ &\quad+x^{36}+x^{35}+x^{34}+x^{31}+x^{28}+x^{25}+x^{24}+x^{23}+x^{22}\\ &\quad+x^{18}+x^{14}+x^{13}+x^{12}+x^{11}+x^{8}+x^{5}+x+1\\ &\qquad\qquad = \ell(x)^2\Phi_2(x)\Phi_4(x)\Phi_7(x)\Phi_{30}(x)p_{22}(x), \end{aligned} \tag{6}$$

and

$$\begin{aligned} &x^{60}+x^{59}+x^{57}+x^{56}+x^{53}+x^{52}+x^{49}+x^{48}+x^{47}+x^{46}+x^{45}+x^{44}\\ &\quad+x^{40}+x^{37}+x^{36}+x^{34}+x^{33}+x^{30}+x^{27}+x^{26}+x^{24}+x^{23}+x^{20}\\ &\quad+x^{16}+x^{15}+x^{14}+x^{13}+x^{12}+x^{11}+x^{8}+x^{7}+x^{4}+x^{3}+x+1\\ &\qquad\qquad = \ell(x)^2\Phi_5(x)\Phi_6(x)\Phi_7(x)\Phi_{30}(x)\Phi_{66}(x). \end{aligned} \tag{7}$$

Here, $\Phi_n(x)$ denotes the nth cyclotomic polynomial, and in (6), $p_{22}(x)$ denotes the noncyclotomic polynomial $x^{22} - x^{19} + x^{18} - x^{15} + x^{14} - x^{11} + x^8 - x^7 + x^4 - x^3 + 1$.

2.2. *Reciprocal search*

Notice that the polynomials (6) and (7) are reciprocal, as we might anticipate, given that $\ell(x)$ is reciprocal. We describe a modification to Algorithm 1 to search for reciprocal $f \in \mathcal{N}$ having a prescribed reciprocal polynomial $g(x)$ as a factor.

We need to combine the arithmetic constraints on $f(\pm 2)$ with the structural requirement of reciprocality. To do this, for a polynomial $f \in \mathcal{N}$ of degree d, we partition the $d+1$ bits of the integer $f(2)$ into three parts: the k low-order bits containing an integer a, the k high-order bits containing the reversed bits of a, which we label a^*, and the m remaining bits in the middle containing an integer b. Thus $f(2) = 2^{k+m}a^* + 2^k b + a$, and since $g(2) \mid f(2)$, we require

$$b \equiv -2^m a^* - 2^{-k} a \mod g(2). \tag{8}$$

We thus need to ensure that $2^m > g(2)$, and it is clearly beneficial to select m as small as possible, subject to this constraint. The relation $2k + m = d + 1$ imposes a parity condition on m, so we choose m to satisfy $2^{m-2} < g(2) < 2^m$. Thus, for each a, we need to consider at most three values for b.

https://doi.org/10.1112/S1461157000000474 Published online by Cambridge University Press

Input. Reciprocal $g(x) \in \mathbb{Z}[x]$, positive integer d.

Output. All reciprocal $f \in \mathcal{N}$ with $\deg f = d$ and $g \mid f$.

Method.
Set $u = g(2)$ and $v = g(-2)$.
Select m and k so that $d + 1 = m + 2k$ and $2^{m-2} < u < 2^m$.
For each odd a with $0 < a < 2^k$ do
  For each b with $0 \leqslant b < 2^m$ satisfying $b \equiv -2^m a^* - 2^{-k} a \bmod u$ do
    If $\gamma(b) \equiv -(-2)^m \gamma(a^*) - (-2)^{-k} \gamma(a) \bmod v$ then do
      Construct f from a and b.
      If $g \mid f$ then print f.
    End if.
  End loop.
End loop.

Algorithm 2: Reciprocal Newman polynomials with a prescribed factor.

For the second test, because $g(-2) \mid \gamma(f(2))$ and $\gamma(2n) = -2\gamma(n)$, we require

$$\gamma(b) \equiv -(-2)^m \gamma(a^*) - (-2)^{-k} \gamma(a) \mod g(-2). \tag{9}$$

We therefore obtain Algorithm 2.

Algorithm 2 in fact performs a somewhat broader search, since it guarantees that only the leading k coefficients of f match the trailing k coefficients.

We use a Gray code in the implementation to enumerate the 2^{k-1} values for a, so that each value that is considered differs from the previous value in exactly one bit position. This allows for fast computation of the required residues in (8) and (9). For example, if the bit in position i of a changes from 1 to 0, then we need only add $2^{m+k-1-i} + 2^{i-k} \bmod u$ to the required residue for b and $(-2)^{m+k-1-i} + (-2)^{i-k} \bmod v$ to the required residue for $\gamma(b)$. By computing the values $2^{-j} \bmod u$ and $(-2)^{-j} \bmod v$ for $1 \leqslant j \leqslant k-1$, as well as $2^{m+j} \bmod u$ and $(-2)^{m+j} \bmod v$ for $0 \leqslant j \leqslant k-2$ at initialization, we may update the state for each subsequent a using only a small number of array lookups, additions, and modular reductions.

We may use the computer's native arithmetic if $\max\{m, \lceil \log_2 |v| \rceil\} \leqslant W - 1$, where W denotes the word size of the computer. This guarantees that all additions stay within integer precision. If this condition does not hold, we employ the highly optimized software package GMP [**17**] for arithmetic with arbitrary precision.

Last, we note that it is simple to create a parallel version of Algorithm 2. If we have 2^r processors available, then on each one we fix the low-order $r + 1$ bits of a to a particular odd integer between 1 and 2^{r+1}.

We implemented this algorithm in C++ and ran it on the Bugaboos, a Beowulf cluster consisting of 192 AMD Athlon 1.2 GHz processors at the High Performance Computing Centre at Simon Fraser University. We found 23 polynomials $f \in \mathcal{N}$ with degree at most 100 having $g(x) = \ell(x)^2$ as a factor. These polynomials are listed in Table 1, with the coefficients of $f(x)$ given in hexadecimal.

https://doi.org/10.1112/S1461157000000474 Published online by Cambridge University Press

Table 1: Newman polynomials f divisible by $\ell(x)^2$.

deg f	Coefficients of f (hexadecimal)
59	C49E23C93C47923
60	1B33F1364D91F99B
79	C42E67FE42427FE67423
84	1BF66C43EC4446F846CDFB
84	1A52C02D5DF1F75680694B
85	37EDB84FDB61B6FC876DFB
90	639D99136318C63644CDCE3
90	691F26C6F8BDE8FB1B27C4B
92	1A59E126B6D4A56DAC90F34B
93	310B99FFF9CC0CE7FFE67423
94	624F496C458A28D11B497923
95	DEDFE0288ECFF3711407FB7B
96	182345F5AD226C896B5F45883
96	1A52C971EF96EED3EF1D2694B
97	3722F1D73627FF91B3AE3D13B
99	DE1EE1F6A418918256F87787B
99	D92F0CB24469F96224D30F49B
99	D3AF53973A240245CE9CAF5CB
99	DEDFCA2852B7FED4A1453FB7B
99	C646A23E9776F6EE97C456263
100	1891A17715814E50351DD0B123
100	1BC3DC3ED48DFBF6256F87787B
100	1B33F1372D75EEF5D69D91F99B

It is natural to ask if other choices for $g(x)$ work as well. We tested $g(x) = p(x)^2$ for 361 other monic irreducible polynomials $p(x)$ having no positive real root:

- the 96 known polynomials with $M(\ell) < M(p) < 1.24$;
- the 50 polynomials with deg $p \leqslant 16$ and $1.24 < M(p) < 1.3$;
- 115 additional reciprocal polynomials with height 1 and deg $p \leqslant 10$;
- 100 nonreciprocal polynomials with height 1 and deg $p \leqslant 6$.

The polynomials in the first two categories may be found at [21]. For the reciprocal polynomials of the first three families, we used Algorithm 2 to test $k \leqslant 36$ when using native arithmetic and $k \leqslant 33$ when using GMP. For the last family, we used Algorithm 1 on each $p(x)$ to test $f \in \mathcal{N}$ with $f(2) < 2^{34} p(2)^2$.

Only six Newman polynomials having a square nonreciprocal factor were found in these searches; these are listed in Table 2. The first column of this table shows the ranking of $M(p)$ among known measures greater than 1 of polynomials with integer coefficients (see [21]).

https://doi.org/10.1112/S1461157000000474 Published online by Cambridge University Press

Table 2: Newman polynomials f divisible by p^2 with $M(p) > M(\ell)$.

Rank	$M(p)$	deg p	deg f	Coefficients of f (hexadecimal)
3	1.20002	14	105	`3132866EBF8EDCEDC7F5D985323`
5	1.20261	14	63	`C4F2B890091D4F23`
10	1.21639	10	60	`1A413DB2A9B7904B`
33	1.23039	10	86	`6FC955A9F52257CAD549FB`
–	1.28012	14	76	`19008ADC4DB6476A2013`
–	1.29156	14	76	`16A92F5D560D575E92AD`

The last two entries have no ranking listed because of the existence of a limit point of Mahler's measure near 1.255.

The second- and fourth-smallest known measures are both associated with polynomials of degree 18, and we verify that no $f \in \mathcal{N}$ exists with $\deg f \leqslant 120$ having one of these polynomials as a repeated factor.

The question of whether there exist Newman polynomials with noncyclotomic factors of multiplicity three or greater remains open, as does the broader question of whether there exists an upper bound on the multiplicity of a noncyclotomic factor of a Newman polynomial. We verify that no $f \in \mathcal{N}$ exists with $\deg f \leqslant 120$ having $\ell(x)^3 \mid f(x)$. In this computation, the value $u = \ell(2)^3$ is slightly larger than 2^{31}, but by performing additions mod u with some care, we are able to implement this search using native arithmetic on 32-bit processors, allowing a deeper search.

3. *Littlewood polynomials*

In [6], Borwein, Hare, and the author determined the smallest values of Mahler's measure for Littlewood polynomials of degree at most 72. The fifteen smallest values found are listed in Table 3, where d represents the minimal degree of a polynomial $f \in \mathcal{L}$ having the given measure, and d_0 is the degree of the noncyclotomic part of this polynomial.

The seventh polynomial in this table is the only one whose noncyclotomic part is reducible, factoring as $(x^{10} - x^7 - x^5 - x^3 + 1)(x^{10} - x^9 + x^5 - x + 1)$. These factors have Mahler's measure 1.23039... and 1.28358..., respectively: the third- and sixth-smallest measures among irreducible, noncyclotomic polynomials of degree 10. Since the degree of this example is close to the largest degree tested in that search, this suggests searching for more Littlewood polynomials with reducible noncyclotomic part and small measure. Fixing two polynomials g_1 and g_2 with small measure, can we find a polynomial $f \in \mathcal{L}$ having $g_1 g_2$ as a factor? We find that Algorithms 1 and 2 may be adapted to this problem with only slight modifications.

For a polynomial $f \in \mathcal{L}$ of degree d, write $f(x) = f^+(x) - f^-(x)$, with f^+ and f^- having $\{0, 1\}$ coefficients. Since $f^+(x) - f^-(x) = (x^{d+1} - 1)/(x - 1)$, we have

$$f^+(x) = \frac{1}{2}\Big(f(x) + \frac{x^{d+1} - 1}{x - 1}\Big),$$

https://doi.org/10.1112/S1461157000000474 Published online by Cambridge University Press

Table 3: Smallest known measures realized by Littlewood polynomials.

	Measure	d	d_0	Coefficients a_i, for $0 \leqslant i \leqslant d/2$.
1.	1.49671107561	19	12	++++-+-+--
2.	1.50613567955	11	6	+-+---
3.	1.50646000575	35	12	++------+++--+---+
4.	1.53691794778	23	14	++++----+-+-
5.	1.55107223951	23	12	+++++++--++-
6.	1.55603019132	6	6	++--
7.	1.57930874185	65	20	+--++--++--+--++--++--+--++--++--
8.	1.58234718368	7	6	++-+
9.	1.58501169305	35	24	++++++-------+-+-+
10.	1.59185616779	71	16	+-+--+-+--+-++-++++-+--+------++-+++
11.	1.59287323067	65	44	+-+-+-+-+-+-+-+-+-+-+-++++++++++
12.	1.59341317381	19	12	++++-++++-
13.	1.59504631133	53	36	+-+-+-+-+-+-+-+-+----------
14.	1.59700500917	17	10	++-++-++-
15.	1.59918220880	41	26	+-+-+-+-+-+-+-+++++++

and so, if $g \mid f$, then for any integer x_0,

$$f^+(x_0) \equiv \frac{x_0^{d+1}-1}{2(x_0-1)} \mod g(x_0).$$

Thus, to modify Algorithm 1 to search for Littlewood polynomials, we let w represent $f^+(2)$, replace the condition $u \mid w$ with $w \equiv (2^{d+1}-1)/2 \bmod u$, and replace $v \mid \gamma(w)$ with $\gamma(w) \equiv (1-(-2)^{d+1})/6 \bmod v$. Likewise, we modify Algorithm 2 by replacing (8) and (9) with

$$b \equiv (2^{d+1}-1)/2 - 2^m a^* - 2^{-k}a \mod g(2) \tag{10}$$

and

$$\gamma(b) \equiv (1-(-2)^{d+1})/6 - (-2)^m \gamma(a^*) - (-2)^{-k}\gamma(a) \mod g(-2). \tag{11}$$

The amended algorithms run just as fast, since only the initial values of the required residues have been changed.

We add that Algorithms 1 and 2 may be modified in a similar way to search for a polynomial f with a prescribed factor when only two fixed values are permitted as coefficients.

We use our modified Algorithm 2 to search for Littlewood multiples of the 746 known polynomials $g(x)$ satisfying $g = g_1 g_2$ with:

- g_1 and g_2 irreducible;
- $1 < M(g_1) < M(g_2)$;
- $M(g_1 g_2) < \theta = 1.496711\ldots$;
- $g(x)$ and $g(-x)$ not both selected; and
- either $M(g_2) < \sqrt{\theta}$ or $\deg(g_2) \leqslant 24$.

https://doi.org/10.1112/S1461157000000474 Published online by Cambridge University Press

The last restriction is needed to avoid considering infinitely many polynomials for g_2 when g_1 is one of the two smallest known measures. For each such g, we stop searching when a particular choice for d results in a running time exceeding two hours, resulting in an average of about eight hours of CPU time per polynomial.

Our search finds 900 Littlewood polynomials f having such a prescribed factor g. In each case, $g_1(x) = \ell(x)$, and either $g_2(x) = 1 - x^4 - x^5 - x^6 + x^{10}$, which has the second-smallest measure among irreducible noncyclotomic polynomials of degree 10, or $g_2(x) = 1 + x^2 - x^3 - x^5 - x^7 + x^8 + x^{10}$, which has the fifth-smallest such measure. All of these, however, have additional noncyclotomic factors, and none has measure less than $1.496711\ldots$.

Finally, consider the obvious algorithm for searching for $f \in \mathcal{L}$ with degree d, prescribed factor g, and $M(f) = M(g)$. Construct all polynomials of the form $g\Phi$ with $M(\Phi) = 1$ and $\deg \Phi = d - \deg g$. Boyd and Montgomery [13] determined an asymptotic estimate for the number $c(n)$ of polynomials of degree n composed entirely of cyclotomic factors, finding that

$$c(n) = \frac{A \exp(B\sqrt{n})}{n\sqrt{\log n}} \left(1 + O\left(\frac{\log\log n}{\log n}\right)\right),$$

where $A \approx .213234$ and $B \approx 3.57608$. Since $\deg g \approx m$ in Algorithm 2, our method constructs $2^{k-1} \approx 2^{(n-1)/2}$ values for $f(2)$, so clearly the simple algorithm is more efficient for large enough d. However, we compute that $c(n) > 2^{(n-1)/2}$ for $n < 64$. Further, Algorithm 2 performs very few operations for each candidate $f(2)$, so we expect it to be faster than the simple algorithm if $2^{(n-1)/2}$ is at least within an order of magnitude of the number of cyclotomic products of total degree n. The actual crossover point is thus likely to exceed $n = 80$, well past where our computations cease.

4. *Height* 1 *polynomials*

Lehmer's problem is related to the question of the existence of polynomials in $\mathcal{H}$ with roots of high order off the unit circle: if 1 is a limit point of the values of Mahler's measure, then for any $m > 0$ there exists a polynomial $f \in \mathcal{H}$ and a complex number β with $|\beta| \notin \{0, 1\}$ such that f has a root at β with multiplicity m. We describe a method of searching for polynomials with height 1 having a prescribed factor $g(x) \in \mathbb{Z}[x]$, and use it to construct some polynomials in $\mathcal{H}$ with a noncyclotomic factor of order 3. A similar method is used in [7] for the cyclotomic case $g(x) = (x-1)^m$.

We implemented Algorithm 3 in C++, using the NTL programming library [26] for its powerful and flexible implementations of lattice reduction, and we used this program to search for height 1 multiples of $g(x) = \ell(x)^m$ or $g(x) = \ell_2(x)^m$, where

$$\ell_2(x) = x^{18} + x^{17} + x^{16} + x^{15} - x^{12} - x^{11} - x^{10} - x^9 - x^8 - x^7 - x^6 + x^3 + x^2 + x + 1,$$

and $M(\ell_2) = 1.188368\ldots$. The polynomials ℓ and ℓ_2 represent the only two known measures between 1 and $\sqrt[4]{2}$.

We found solutions for $m = 2$ and $m = 3$ for both of these polynomials, and we record below an example with the smallest known degree for each case. For each polynomial, we list its degree, its sequence of coefficients (abbreviating to '+' for $+1$ and '-' for -1) and its factorization (using $p_n(x)$ to denote an irreducible, noncyclotomic polynomial of degree n).

https://doi.org/10.1112/S1461157000000474 Published online by Cambridge University Press

Input. Reciprocal $g(x) \in \mathbb{Z}[x]$ with $\deg g = d$, positive integer $D \geqslant d$.

Output. $\lfloor (D-d)/2 \rfloor + 1$ linearly independent, reciprocal polynomials with small coefficients and degree at most D, each having g as a factor.

Method. Set $n = D - d$. Set $h_k(x) = (x^{n-k} + x^k)g(x)$ for $0 \leqslant k < n/2$, and if n is even set $h_{n/2}(x) = x^{n/2}g(x)$. Write $h_k(x) = \sum_{i=0}^{D-k} c_{k,i}x^i$, and set $\mathbf{v}_k = (c_{k,0}, \ldots, c_{k,\lfloor D/2 \rfloor})$ for $0 \leqslant k \leqslant n/2$. The sequence $\{\mathbf{v}_k\}$ spans an $(\lfloor n/2 \rfloor + 1)$-dimensional lattice in $\mathbb{R}^{\lfloor D/2 \rfloor + 1}$, and vectors in this lattice correspond to reciprocal multiples of $g(x)$ with degree at most D. Use the LLL lattice basis reduction algorithm [19] to construct a reduced basis for this lattice, and report the polynomials produced.

Algorithm 3: Multiples of reciprocal polynomials with small coefficients.

- Degree 38:

```
+0-00+-0+--0+0--0-000-0--0+0--+0-+00-0+
```

$$= \ell(x)^2\ell(-x)\Phi_3(x)\Phi_4(x)\Phi_{12}(x).$$

- Degree 115:

```
--+0-000-0+---0+00-00-00-0-0+0--000-+-00+000+-+-0--00+00++
--00-00++0+-+-000-00+-+000++0-0+0+00+00+00-0+++-0+000+0-++
```

$$= \ell(x)^3\Phi_1(x)\Phi_4(x)\Phi_5(x)\Phi_6(x)\Phi_7(x)\Phi_{11}(x)\Phi_{30}(x)\Phi_{42}(x)p_{40}(x).$$

- Degree 60:

```
++++00-0------0++0+-+-+0+0-0+000+0-0+0+-+-+0++0------0-00++++
```

$$= \ell_2(x)^2\Phi_8(x)\Phi_{12}(x)p_{16}(x).$$

- Degree 200:

```
++0+000-0-0--+00+000-0-000+00+-+00+-+000-+--+-000+
++000-0+0-+-0-0000-+0000+-0--0-+0++0+-0--0-+00000+0
+00000+-0--0-+0++0+-0--0-+0000+-0000-0-+-0+0-000+++
000-+--+-000+-+00+-+00+000-0-000+00+--0-0-000+0++
```

$$\begin{aligned} &= \ell_2(x)^3\Phi_1(x)^2\Phi_2(x)^4\Phi_3(x)^2\Phi_4(x)\Phi_6(x)\Phi_8(x)\Phi_9(x)\Phi_{10}(x) \\ &\quad \cdot \Phi_{12}(x)\Phi_{15}(x)\Phi_{18}(x)\Phi_{21}(x)\Phi_{22}(x)\Phi_{27}(x)\Phi_{32}(x)\Phi_{38}(x)\Phi_{46}(x). \end{aligned}$$

The example for ℓ_2^3 has only cyclotomic auxiliary factors. No such polynomial is found for ℓ^3, although we do find a polynomial in $\mathcal{H}$ of degree 117 whose noncyclotomic factors are $\ell(x)^3\ell(-x)$. Its cyclotomic part is $\Phi_1^2\Phi_2\Phi_3\Phi_4^2\Phi_6\Phi_7\Phi_{11}\Phi_{12}\Phi_{18}\Phi_{30}\Phi_{32}\Phi_{48}$.

No height 1 multiples of ℓ^4 or ℓ_2^4 are found using this method. We remark that a result of Bombieri and Vaaler [4, Corollary 2] guarantees that such a polynomial exists for ℓ^4 with degree less than 16000, and for ℓ_2^4 with degree less than 634000.

https://doi.org/10.1112/S1461157000000474 Published online by Cambridge University Press

We add that Beaucoup, Borwein, Boyd and Pinner [3] have established bounds on the minimal absolute value of a nonzero root of prescribed multiplicity for a power series with all its coefficients in $[-1, 1]$. In particular, they proved that no height 1 polynomials exist having ℓ^7 or ℓ_2^7 as a factor.

Acknowledgments. I thank David Boyd for bringing the article [25] to my attention, Christopher Pinner for pointing out [3], and the referee for his careful reading of the manuscript. I also thank the High Performance Computing Centre at Simon Fraser University.

References

1. F. Amoroso, 'Polynomials with prescribed vanishing at roots of unity', *Boll. Un. Mat. Ital. B* (7) 9 (1995) 1021–1042. 316

2. D. H. Bailey and D. Broadhurst, 'A seventeenth-order polylogarithm ladder', arXiv:math.CA/9906134, 18 pp. 315

3. F. Beaucoup, P. Borwein, D. W. Boyd and C. Pinner, 'Multiple roots of $[-1, 1]$ power series', *J. London Math. Soc.* (2) 57 (1998) 135–147. 324

4. E. Bombieri and J. D. Vaaler, 'Polynomials with low height and prescribed vanishing', *Analytic number theory and Diophantine problems* (*Stillwater, Oklahoma*, 1984), Prog. Math. 70 (ed. A. C. Adolphson, J. B. Conrey, A. Ghosh and R. I. Yager, Birkhäuser, Basel, 1987) 53–73. 315, 316, 323

5. P. Borwein, T. Erdélyi and G. Kós, 'Littlewood-type problems on $[0, 1]$', *Proc. London Math. Soc.* (3) 79 (1999) 22–46. 316

6. P. Borwein, K. G. Hare and M. J. Mossinghoff, 'The Mahler measure of polynomials with odd coefficients', *Bull. London Math. Soc.*, to appear. 315, 320

7. P. Borwein and M. J. Mossinghoff, 'Polynomials with height 1 and prescribed vanishing at 1', *Experiment. Math.* 9 (2000) 425–433. 316, 322

8. P. Borwein and M. J. Mossinghoff, 'Newman polynomials with prescribed vanishing and integer sets with distinct subset sums', *Math. Comp.* 72 (2003) 787–800. 316

9. D. W. Boyd, 'Reciprocal polynomials having small measure', *Math. Comp.* 35 (1980) 1361–1377. 315

10. D. W. Boyd, 'Reciprocal polynomials having small measure II', *Math. Comp.* 53 (1989) 355–357, S1–S5. 315

11. D. W. Boyd, 'On a problem of Byrnes concerning polynomials with restricted coefficients', *Math. Comp.* 66 (1997) 1697–1703. 316

12. D. W. Boyd, 'On a problem of Byrnes concerning polynomials with restricted coefficients II', *Math. Comp.* 71 (2002) 1205–1217. 316

13. D. W. Boyd and H. L. Montgomery, 'Cyclotomic partitions', *Number theory* (*Banff, Alberta*, 1988), (ed. R. A. Mollin, Walter de Gruyter, Berlin, 1990) 7–25. 322

14. H. Cohen, L. Lewin and D. Zagier, 'A sixteenth-order polylogarithm ladder', *Experiment. Math.* 1 (1992) 25–34. 315

15. A. Dubickas, 'On the order of vanishing at 1 of a polynomial', *Lithuanian Math. J.* 39 (1999) 365–370. 316

16. A. Dubickas, 'Three problems for polynomials of small measure', *Acta Arith.* 98 (2001) 279–292. 316

17. 'GMP: The GNU multiple precision arithmetic library', http://www.swox.com/gmp. 318

18. D. H. Lehmer, 'Factorization of certain cyclotomic functions', *Ann. of Math.* (2) 34 (1933) 461–479. 315

19. A. K. Lenstra, H. W. Lenstra Jr. and L. Lovász, 'Factoring polynomials with rational coefficients', *Math. Ann.* 261 (1982) 515–534. 323

20. M. Mignotte, 'Sur les multiples des polynômes irréductibles', *Bull. Soc. Math. Belg.* 27 (1975) 225–229. 315

21. M. J. Mossinghoff, 'Lehmer's problem', http://www.cecm.sfu.ca/~mjm/Lehmer. 315, 319, 320

22. M. J. Mossinghoff, 'Polynomials with small Mahler measure', *Math. Comp.* 67 (1998) 1697–1705, S11–S14. 315

23. M. J. Mossinghoff, C. G. Pinner and J. D. Vaaler, 'Perturbing polynomials with all their roots on the unit circle', *Math. Comp.* 67 (1998) 1707–1726. 315

24. A. M. Odlyzko and B. Poonen, 'Zeros of polynomials with 0, 1 coefficients', *Enseign. Math.* (2) 39 (1993) 317–348. 314

25. M. Pathiaux, 'Sur les multiples de polynômes irréductibles associés à certains nombres algébriques', *Séminaire Delange–Pisot–Poitou* 14 (1972/73) 9 pp. 315, 324

26. V. Shoup, 'NTL: a library for doing number theory', http://www.shoup.net/ntl. 322

27. J. H. Silverman, 'Exceptional units and numbers of small Mahler measure', *Experiment. Math.* 4 (1995) 69–83. 315

28. C. J. Smyth, 'On the product of the conjugates outside the unit circle of an algebraic integer', *Bull. London Math. Soc.* 3 (1971) 169–175. 315

Michael J. Mossinghoff mjm@member.ams.org
http://www.davidson.edu/math/mossinghoff

Department of Mathematics
Davidson College
Davidson, NC 28035
USA

https://doi.org/10.1112/S1461157000000474 Published online by Cambridge University Press